Stability of (n,k) nonlinear feedback shift registers

Meilin Li, Jianquan Lu

***Abstract*—In this paper, the (n,k) nonlinear feedback shift register (NFSR) is regarded as a Boolean network (BN). Semi-tensor product (STP) of matrices is used to convert (n,k) NFSR into an equivalent algebraic equation. Based on STP of matrices, a novel way is proposed to study stability of (n,k) NFSR and the periodicity of (n,k) NFSR. First, the stability of the (n,k) NFSR is investigated, and we propose an algorithm to judge the stability of an (n,k) NFSR. Second, we reveal relationship between the minimal period of output sequence of a cycle for an (n,k) NFSR and the length of the cycle. Third, we investigate the period of (n,k) NFSR. Some existing methods can only be used to investigate the cycle of the (n,k) NFSR, while in this paper, we can simultaneously investigate stability of an (n,k) NFSR and the period of (n,k) NFSR by using the method of STP.**

***Index Terms*—(n,k) NFSR, stability, minimal period, period, semi-tensor product, Boolean networks**

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 [1]. The main building blocks of stream cipher is nonlinear feedback 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 $n-1, n-2, ..., 1, 0$. The value of the i-th $(0 \leq i \leq n-2)$ bit is updated by the value of $(i+1)$-th bit, and the value of $(n-1)$-th bit is updated by feedback function f which depends 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 its 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 [2]. The period of Fibonacci NFSR is equal to the largest length of its state cycle. 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. E. Dubrova also provided a method to increase the period of output sequence of an (n,k) NFSR by composing m smaller (n_i, k_i) $(1 \leq i \leq m)$ NFSRs. But there is a weakness for the (n,k) NFSR. The period of an (n,k) NFSR is not necessary equal to the length of longest cycle of (n,k) NFSR, and this would cause some problems to observe the period of output sequences of an (n,k) NFSR. The advantages of (n,k) NFSR are shown as follows:

- (n,k) NFSR can potentially improve the speed of the generation of the pseudo-random sequence.
- (n,k) NFSR can generate the pseudo-random sequence with good statistical properties which can not be generated by Fibonacci NFSR.

In order to solve the above mentioned problems, in this paper, we provide a new method to investigate the period of output sequences of a cycle of an (n,k) NFSR by using the method of semi-tensor product (STP) of matrices. The method of STP was proposed by Cheng *et al.* in [3][4][5]. After the proposal of method of STP, it has been used in many fields, such as large-scale systems [6][7], graph coloring [8][9], Petri nets [10], Boolean networks (BNs) [11][12] and NFSR [13][14]. By using the method of STP, some fundamental problems of BNs have been solved, such as synchronization [15][16], stability [17][18][12], stabilization[19][20], controllability [21][22][23][24][25], observability [26][27] and so on.

In this paper, we treat the (n,k) NFSR as a Boolean network (BN). The (n,k) NFSR can be transformed into a finite-value linear system by using the method of STP. In [13], Zhong *et al.* investigated stability of NFSR and the cycle of NFSR by using the method of STP. In [29], based on STP, Cheng *et al.* studied the stability of BN. The method of STP is powerful to deal with the system with finite value. Based on the method of STP, the (n,k) NFSR can be transformed to an algebraic linear system. STP is an powerful method to investigate stability and period of (n,k) NFSR.

In the following, we will first define the minimal period of output sequence of a cycle for an (n,k) NFSR to better study the output sequence of an (n,k) NFSR. The method of STP is used to investigate the stability of (n,k) NFSR. We focus on the stability of (n,k) NFSR, the period of output sequence of (n,k) NFSR. The main contributions of this paper are listed as follows:

- We find out the relationship between the minimal period of output sequence of a cycle of an (n,k) NFSR and the length of the cycle.
- We propose an algorithm to judge the stability of an (n,k) NFSR.
- We propose an new algorithm to find all cycles of an (n,k) NFSR.

The remainder of this paper is organized as follows. Section 2 gives some preliminaries on STP and (n,k) NFSR. Based on the method of STP, we obtain the multi-linear forms of (n,k) NFSR. Section 3 investigates the stability of (n,k) NFSR, the period of an (n,k) NFSR. In Section 4, two examples are given to illustrate our theoretical results. At last, a conclusion

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

Jianquan Lu is with the School of Mathematics, Southeast University, Nanjing 210096, China `jqluma@seu.edu.cn`

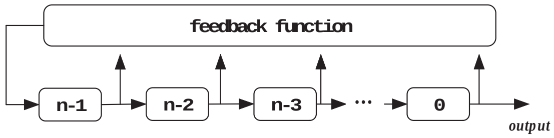

Fig. 1: The Fibonacci NLFSR

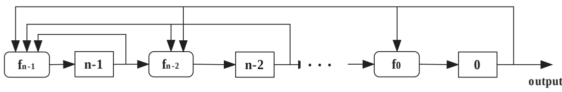

Fig. 2: The Fibonacci NLFSRs

is given.

II. PRELIMINARIES

In this section, we first review the STP of matrices briefly. Then the multi-linear form of Boolean function 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 form. We first give some notations which will be used in this paper.

- $\mathscr{D}=\{0,1\}$.
- I_n : the identity matrix of dimension n.
- $\delta_{2^n}^i$: the i-th column of identity matrix I_n.
- $\Delta_{2^n}=\{\delta_{2^n}^i|i=1,2,3,...,2^n\}$.
- $\mathscr{L}_{n\times m}$: the set of $n\times m$ matrices, whose column belong to Δ_n. For a matrix $L\in(L)_{n\times m}$, and $L=[\delta_n^{i_1}\ \delta_n^{i_2}\ ...\ \delta_n^{i_m}]$, 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 positive integers.
- $\star$: the least common multiple.
- $\diamond$: the greatest common divisor.
- $\times$: Cartesian product.
- $|S|$: the number of elements in set S.

A. Semi-tensor product of matrices

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

Definition 1: [5] 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 1, then the STP of A and B is reduced to their conventional matrix product AB.

We identify $\Delta_2\sim\mathscr{D}$ i.e $(\delta_2^1\sim 1,\delta_2^2\sim 0)$, and $\delta_2^1(\delta_2^2)$ is called the vector form of logical value $1(0)$.

Lemma 1: [5] 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) NFSR

An (n,k) NFSR consists n binary memories device called bits. The output of an (n,k) NFSR is the value of the 0-th bit. An (n,k) NFSR is defined as follows. Let $x_i(t),\ 0\le i\le n-1$ be variable representing the value of the i-th bit at time t. Let $f_i:\mathscr{D}^k\to\mathscr{D}$, $1\le k\le n$, be the next value function of 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 value 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 (n,k) NFSR can be described as a BN shown as follows:

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

where $x_i(t)\in\mathscr{D},\ 0\le i\le n-1,\ t=1,2,....$ Let $x(t)=(x_0(t),x_1(t),...,x_{n-1}(t))$ denote the state of (n,k) NFSR and $f=[f_0,f_1,...,f_{n-1}]$ be the vectorial function. So system (8) can be expressed as follows:

$$x(t+1)=f(x(t)). \tag{6}$$

Definition 2: 1) A state x_0 is called an *equilibrium state* of (n,k) NFSR (6), if $fx_0=x_0$.

2) $x_0,f(x_0),...,f^p(x_0)$ is called a cycle of (n,k) NFSR (6) with length p, if $f^p(x_0)=x_0$, and the elements in set $\{x_0,f(x_0),...,f^p(x_0)\}$ 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 x after in k steps.

Next, we give the definition of *globally stable*, *locally stable* and the period of (n,k) NFSR.

Definition 3: (n,k) NFSR (6) is called *globally stable* with respect to (w.r.t.) the equilibrium state x_0, if for any state $x\in\mathscr{D}^n$, there exist a positive integer N such that $f^Nx=x_0$.

Definition 4: (n,k) NFSR (6) is called *locally stable* w.r.t. the equilibrium state x_0, if there exist some states $x\in\mathscr{D}^n\setminus x_0$, such that $f^Nx=x_0$ for some positive integer N.

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 (8) can be converted into following system:

$$x(t+1)=Lx(t),\ t\in N, \tag{7}$$

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 5: [2] The period of an (n,k) NFSR is the length of the longest cyclic output sequence it produces.

To better study the period of (n,k) NFSR, we propose the definition of minimal period of output sequence of a state in cycle of (n,k) NFSR.

Definition 6: For arbitrary state x in a cycle $\mathscr{C}$ with length $l_{\mathscr{C}}$ of an (n,k) NFSR, the minimal period of output sequence $O_x = \{O_1, O_2, ...\}$ of x as an initial state is the minimal positive integer p_x such that $O_i = O_{i+kp_x}$, $k = 1,2,3,....$

Remark 1: For simplification, in the following, the output sequence of x means that the output sequence of x as an initial state, and x is in a cycle of (n,k) NFSR.
In order to investigate the cycle of an (n,k) NFSR, we need the following definition.

Definition 7: For an (n,k) NFSR, if the state x is shifted to the state y, then the state x is called the *predecessor* of state y, while state y is called the *successor* of state x. The state without predecessor is called a *starting state*.
Let S denote the set of starting states of (n,k) NFSR (6).

III. MAIN RESULTS

In this section, the stability of system (7) is firstly investigated. Then the period of output sequence of system (7) is studied. At last, we investigate the period of output sequence of an composed (n,k) NFSR.

A. Stability of (n,k) NFSR

Clearly, in an (n,k) NFSR, the equilibrium state can be any state. Assume the equilibrium state of (n,k) NFSR is $\delta_{2^n}^i \sim (i_0, i_1, ..., i_{n-1})$. We can make a coordinate transformation

$$\begin{cases} y_j = \neg x_j, \ i_j = 1, \\ y_j = x_j, \ i_j = 0, \end{cases} \tag{8}$$

then system (7) is converted into a system with equilibrium state $\delta_{2^n}^{2^n} \sim (0,0,...,0)$ as follows:

$$y(t+1) = \bar{L} y(t), \tag{9}$$

where $y(t) = \ltimes_{i=0}^{n-1} y_i(t)$. Then equilibrium state of system (9) is $\delta_{2^n}^{2^n} \sim (0,0,...,0)$.

Since the form of system (7) is similar to the form of system in [13], we can obtain the same result about the global stability of system (7).

Theorem 1: (n,k) NFSR (9) is globally stable with respect 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 (9) is globally stable with respect to $\delta_{2^n}^{2^n}$, if and only if $R(\delta_{2^n}^{2^n}) = \Delta_{2^n}$.

Remark 2: If an (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.

Theorem 2: (n,k) NFSR (9) is locally stable with respect to state $\delta_{2^n}^{2^n}$ if and only if there exist state $x \in \Delta_{2^n} \setminus \delta_{2^n}^{2^n}$ and a positive integer $1 \le N \le 2^n - 1$ such that $L^N x = \delta_{2^n}^{2^n}$. (i. e there exist state $x \in \Delta_{2^n} \setminus \delta_{2^n}^{2^n}$ which can reach equilibrium state $\delta_{2^n}^{2^n}$.)

In the next, we will give an algorithm to decide if an (n,k) NFSR is globally stable under the knowledge of state transition matrix of an (n,k) NFSR.

Algorithm 1 The global stability of an (n,k) NFSR.

initial set $\Delta = \{1, 2, ..., 2^n\}$
for $i = 1$ to 2^n **do**
  for $j = 1$ to 2^n **do**
    if $col_j(L) = \delta_{2^n}^{2^n}$ **then**
      $R^i(\delta_{2^n}^{2^n}) = R^i(\delta_{2^n}^{2^n}) \cup \delta_{2^n}^j$
    end if
  end for
  if $R^{i-1}_{\delta_{2^n}^{2^n}} = R^i_{\delta_{2^n}^{2^n}}$ **then**
    $num = i - 1$
    break.
  end if
end for
if $R^{num}_{\delta_{2^n}^{2^n}} = \Delta_{2^n}$ **then**
  the (n,k) NFSR is globally stable.
else
  the (n,k) NFSR is not globally stable.
end if

Lemma 2: The set of starting states of an (n,k) NFSR (7), S is equal to $\Delta_{2^n} \setminus col(L)$.

Proof: From the definition of starting state, we can know that for every starting state x, there does not exist state y, such that $Ly = x$, $Ly \in Col(L)$.Hence, we can conclude that the starting state $x \notin Col(L)$, and set $S = \Delta_{2^n} \setminus col(L)$. ∎

In the next, we will give an algorithm to find all cycles of (n,k) NFSR (7). We firstly give some notations in Algorithm 2. S_i denote the i-th state in set S. V_i denotes the set of states which start from state S_i have been visited. V_i^k denotes the k-th element in set V_i. $\mathscr{C}_i$ denote the i-th cycle of (n,k) NFSR. In Algorithm 2, we will firstly find the cycles which start from starting states. Then the cycles without branches will be found.

B. The period of (n,k) NFSR

In this section, we firstly give the following lemma before investigating the period of (n,k) NFSR.

Since the number of states in an (n,k) NFSR is finite, we can obtain the following lemma.

Lemma 3: For arbitrary initial state $\delta_{2^n}^i$ of an (n,k) NFSR, $\delta_{2^n}^i$ always can reach a cycle or an equilibrium point.

From Lemma 3, in the following, we only need to investigate the output sequence of state within a cycle. So in this paper, the minimal period of output sequence of a state in (n,k) NFSR means that the minimal period is only for the states within a cycle of (n,k) NFSR.

In [2], E. Dubrova *et al.* proposed that the minimal period of the output sequence of a state x in an (n,k) NFSR is not necessary equal to the length of the cycle which contains the state x. But they only provide a method to compute the cycle of an (n,k) NFSR. Hence, in the following, we will provide Algorithm 3 to compute the minimal period of the

Algorithm 2 All cycles of (n,k) NFSR (7)

Initialize set $V_i = \varnothing$
for $i = 1$ to $|S|$ **do**
    $V_i = S_i$
    $x = S_i$
    for $j = 1$ to 2^n **do**
        $x = Lx$
        if $x \notin V_i$ **then**
            $V_i = V_i \cup x$
            if $i > 1$ and $x \in V_{i-1} \cup V_{i-2} \cup \ldots \cup V_1$ **then**
                continue
            end if
        else
            There exist V_i^k such that V_i^k equal to x
            The i-th cycle of (n,k) NFSR is $\mathscr{C}_i = \{V_i^k, V_i^{k+1}, \ldots, V_i^{j-1}\}$.
            continue
        end if
    end for
end for
$Re = \Delta_{2^n} \setminus V_1 \cup V_2 \cup \ldots \cup V_{|S|}$
$i = 0$
while $Re \neq \varnothing$ **do**
    $i = i + 1$
    Let x denote the first number of set Re, there exist $L^k x = x$.
    The $|S| + i$-th cycle is $\mathscr{C}_{|S|+i} = \{x, Lx, \ldots, L^{k-1}x\}$
    $Re = Re \setminus \mathscr{C}_{|S|+i}$
end while

output sequence of a state in an (n,k) NFSR. Before presenting Algorithm 3, we give a theorem to show the relationship between the period of output sequence of the state in a cycle and the length of the cycle of an (n,k) NFSR.

Theorem 3: If the length of a cycle $\mathscr{C} = \{e_0, e_1, \ldots, e_{l-1}\}$ in (n,k) NFSR (7) is l, then the minimal period of output sequence of cycle $\mathscr{C}$ is one of the divisor of l, and the minimal period of output sequence of every state e_i, $0 \le i \le l-1$ in cycle $\mathscr{C}$ is equal to the minimal period of output sequence of cycle $\mathscr{C}$.

Proof: Let $p_{\mathscr{C}}$ denote the minimal period of the output sequence of cycle $\mathscr{C}$, and let p_i denote the minimal period of output sequence of initial state e_i, and l_i denote the output sequence of initial state e_i. Let $O_{\mathscr{C}} = \{O_{\mathscr{C}}^0, {}^1_{\mathscr{C}}, \ldots, O_{\mathscr{C}}^{l-1}\}$ with length l denote the output sequence of cycle $\mathscr{C}$ which start at state e_0.

Because $\mathscr{C}$ is a cycle, l is one of period of the output sequence of cycle $\mathscr{C}$. Apparently, the multiple of l is the period of output sequence of cycle $\mathscr{C}$. We also can know that one of the divisor of l can be the period of the output sequence of cycle $\mathscr{C}$. Since $e_i \in \mathscr{C}$, p_i must be a divisors of l. The output sequence of e_i is equivalent to the output sequence of cycle $\mathscr{C}$ after i times shifts. So the minimal period of output sequence e_i is equal to $p_{\mathscr{C}}$. ■

From Theorem 3, we can know that the minimal period of every state in a cycle is the same, so the investigation of minimal period of output sequence of a state can be called the investigation of minimal period of a cycle of an (n,k) NFSR.

Now, based on Theorem 3, we give an algorithm to compute the minimal period of output sequence of an initial state of (n,k) NFSR (7). The following algorithm is based on the fact that all cycles of (n,k) NFSR (7) are known. Algorithm 3 can be used to find out the period of output sequence of given cycle. For the given cycle, the length of the cycle is denoted by l, and the period of the output sequence of the cycle is denoted by p. Algorithm 3 only can compute the minimal period of output sequence of a cycle. So if we want to compute the minimal period of all cycles, Algorithm 3 should be used repeatedly.

Algorithm 3 The period of output sequence of a cycle of (n,k) NFSR (7).

initial $p = l$
for $i = 1$ to l **do**
    flag=true
    if i is a divisor of l **then**
        I_1 is a subsequence which formed by the 1-th element to i-th element of cycle $\mathscr{C}$
        for $j = 1$ to $l/p - 1$ **do**
            I_2 is a subsequence which formed by the $j * i$-th element to $(j+1) * i - 1$-th element of cycle $\mathscr{C}$.
            if $I_1 \neq I_2$ **then**
                flag=false
            end if
        end for
    end if
    if flag=true **then**
        if $i < p$ **then**
            $p = i$
        end if
    end if
end for

So the period of (n,k) NFSR (7) can be found by the following steps:

- Finding all cycles of the (n,k) NFSR (7).
- Finding the minimal periods of all cycles of the (n,k) NFSR (7) by using Algorithm 3.
- Finding the maximum value of minimal periods of all the cycles of (n,k) NFSR (7).

IV. EXAMPLES

In this section, we give two examples to illustrate our theoretical results.

Example 1: Consider an $(3,3)$ NFSR with following equations:

$$\begin{cases} x_0(t+1) &= (x_0(t)\wedge x_2(t))\vee(\neg x_0(t)\wedge x_1(t)), \\ x_1(t+1) &= (x_0(t)\wedge(\neg x_1(t)\vee\neg x_2(t)))\vee(\neg x_0(t) \\ & \quad \wedge(\neg x_1(t)\wedge x_2(t))), \\ x_2(t+1) &= (x_0(t)\wedge(\neg x_2(t)\wedge\neg x_1(t)))\vee(\neg x_0(t) \\ & \quad \wedge(\neg x_1(t)\vee\neg x_2(t))) \end{cases} \tag{10}$$

By using the method of STP, we can transfer system (10) into following multi-linear form:

$$x(t+1) = L_1 x(t), \tag{11}$$

where $L_1 = \delta_8[4\ 6\ 2\ 5\ 8\ 7\ 1\ 3]$, $x(t) = x_0(t)x_1(t)x_2(t) \in \Delta_{2^3}$.

In (n,k) NFSR (10), there is no equilibrium state, so it is not globally stable or locally stable.

We know that there is a cycle of (n,k) NFSR (10), and the cycle is $\delta_8^1 \to \delta_8^4 \to \delta_8^5 \to \delta_8^8 \to \delta_8^3 \to \delta_8^2 \to \delta_8^6 \to \delta_8^7 \to \delta_8^1$. The output sequence of the cycle is 11001100.... The period of this output sequence is 4, which is coincident with the result of Theorem 3. So we can conclude that the period of (n,k) NFSR (10) is 3.

Example 2: Consider an $(3,3)$ NFSR with following equations:

$$\begin{cases} x_0(t+1) &= (x_0(t)\wedge\neg x_2(t))\vee(\neg x_0(t)\wedge x_1(t)\wedge 1), \\ x_1(t+1) &= (x_0(t)\wedge(\neg x_1(t)\vee x_2(t)))\vee(\neg x_0(t)\wedge \\ & \quad (x_1(t)\wedge x_2(t))), \\ x_2(t+1) &= (x_0(t)\wedge(x_1(t)\vee\neg x_2(t)))\vee(\neg x_0(t)\wedge \\ & \quad (\neg x_1(t)\wedge\neg x_2(t))). \end{cases} \tag{12}$$

By using the method of STP, we can turn system (10) into following multi-linear form:

$$x(t+1) = L_2 x(t), \tag{13}$$

where $L_2 = \delta_8[5\ 3\ 6\ 1\ 2\ 4\ 8\ 7]$, $x(t) = x_0(t)x_1(t)x_2(t) \in \Delta_{2^3}$. In (n,k) NFSR (12), there is no equilibrium state, so (n,k) NFSR (12) is not globally stable or locally stable.

We can know that there are two cycles denoted by $\mathscr{C}_{21}, \mathscr{C}_{22}$. $\mathscr{C}_{21} = \delta_8^1 \to \delta_8^5 \to \delta_8^2 \to \delta_8^3 \to \delta_8^6 \to \delta_8^4 \to \delta_8^1$, $\mathscr{C}_{22} = \delta_8^7 \to \delta_8^8 \to \delta_8^7$. The output sequence of $\mathscr{C}_{21}$ is 101101101101.... The output sequence of $\mathscr{C}_{22}$ is 00.... So we can know that the minimal period of output sequence of $\mathscr{C}_{21}$ is 3, and the minimal period of output sequence of $\mathscr{C}_{22}$ is 1. So we can get that the period of (n,k) NFSR (12) is 3.

V. CONCLUSION

This paper investigated the stability of (n,k) NFSR, the period of (n,k) NFSR and the period of composed (n,k) NFSR. First, we treated the (n,k) NFSR as a BN. By using the method of STP, the (n,k) NFSR was transformed into a multi-linear system. Then an algorithm was proposed to judge the stability of an (n,k) NFSR. After that, we proposed an algorithm to find the minimal period of output sequence of a cycle of an (n,k) NFSR. Finally, two examples were given to verify the results obtained in this paper.

ACKNOWLEDGMENT

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, Jiangsu Province Six Talent Peaks Project under Grant 2015-ZNDW-002.

REFERENCES

[1] S. W. Golomb, *Shift Register Sequences*. Springer US, 2002.

[2] 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.

[3] D. Cheng, H. Qi, and Y. Zhao, *An Introduction to Semi-Tensor Product of Matrices and Its Applications*. WORLD SCIENTIFIC, 2012.

[4] D. Cheng and H. Qi, "A linear representation of dynamics of Boolean networks," *Automatic Control IEEE Transactions on*, vol. 55, no. 10, pp. 2251–2258, 2010.

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

[6] Y. Zhao, J. Kim, and M. Filippone, "Aggregation algorithm towards large-scale Boolean network analysis," *IEEE Transactions on Automatic Control*, vol. 58, no. 8, pp. 1976–1985, 2013.

[7] Y. Zhao, B. K. Ghosh, and D. Cheng, "Control of large-scale Boolean networks via network aggregation," *IEEE Transactions on Neural Networks & Learning Systems*, vol. 27, no. 7, pp. 1527–1536, 2016.

[8] 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*, vol. 48, no. 7, pp. 1227–1236, 2012.

[9] J. Zhong, J. Lu, C. Huang, L. Li, and J. Cao, "Finding graph minimum stable set and core via semi-tensor product approach," *Neurocomputing*, vol. 174, pp. 588–596, 2015.

[10] X. Han, Z. Chen, Z. Liu, and Q. Zhang, "Calculation of siphons and minimal siphons in Petri nets based on semi-tensor product of matrices," *IEEE Transactions on Systems Man & Cybernetics Systems*, pp. 1–6, 2015.

[11] Y. Guo, P. Wang, W. Gui, and C. Yang, "Set stability and set stabilization of Boolean control networks based on invariant subsets ," *Automatica*, vol. 61, pp. 106–112, 2015.

[12] E. Fornasini and M. E. Valcher, "On the periodic trajectories of Boolean control networks ," *Automatica*, vol. 49, no. 5, p. 1506C1509, 2013.

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

[14] D. W. Zhao, H. P. Peng, L. X. Li, S. L. Hui, and Y. X. Yang, "Novel way to research nonlinear feedback shift register," *Science China Information Sciences*, vol. 57, no. 9, pp. 1–14, 2014.

[15] J. Zhong, J. Lu, T. Huang, and J. Cao, "Synchronization of mastercslave Boolean networks with impulsive effects: Necessary and sufficient criteria," *Neurocomputing*, vol. 143, no. 143, pp. 269–274, 2014.

[16] H. Zhang, X. Wang, and X. Lin, "Synchronization of Boolean networks with different update schemes," *IEEE/ACM Transactions on Computational Biology & Bioinformatics*, vol. 11, no. 5, p. 965, 2014.

[17] Y. Liu, J. Cao, L. Sun, and J. Lu, "Sampled-data state feedback stabilization of Boolean control networks," *Neural Computation*, vol. 28, no. 4, pp. 778–799, 2016.

[18] H. Li, Y. Wang, and Z. Liu, "Stability analysis for switched Boolean networks under arbitrary switching signals," *IEEE Transactions on Automatic Control*, vol. 59, no. 7, pp. 1978–1982, 2014.

[19] F. Li and Z. Yu, "Feedback control and output feedback control for the stabilisation of switched Boolean networks," *International Journal of Control*, vol. 89, no. 2, pp. 337–342, 2016.

[20] N. Bof, E. Fornasini, and M. E. Valcher, "Output feedback stabilization of Boolean control networks ," *Automatica*, vol. 57, no. C, pp. 21–28, 2015.

[21] Y. Liu and J. L. B. Wu, "Some necessary and sufficient conditions for the output controllability of temporal Boolean control networks," *Esaim Control Optimisation & Calculus of Variations*, vol. 20, no. 20, pp. 158–173, 2014.

[22] J. Lu, J. Zhong, D. W. C. Ho, Y. Tang, and J. Cao, "On controllability of delayed Boolean control networks," *Siam Journal on Control & Optimization*, vol. 54, no. 2, pp. 475–494, 2016.

[23] J. Zhong, J. Lu, T. Huang, and D. W. Ho, "Controllability and synchronization analysis of identical-hierarchy mixed-valued logical control networks.," *IEEE Transactions on Cybernetics*, doi:10.1109/TCYB.2016.2560240, in press.

[24] Y. Liu, H. Chen, J. Lu, and B. Wu, "Controllability of probabilistic Boolean control networks based on transition probability matrices ," *Automatica*, vol. 52, no. C, pp. 340–345, 2015.

[25] H. Li, L. Xie, and Y. Wang, "On robust control invariance of Boolean control networks," *Automatica*, vol. 68, no. C, pp. 392–396, 2016.

[26] D. Laschov, M. Margaliot, and G. Even, "Observability of Boolean networks: A graph-theoretic approach ," *Automatica*, vol. 49, no. 8, pp. 2351–2362, 2013.

[27] L. Zhang and K. Zhang, "Controllability and observability of Boolean control networks with time-variant delays in states," *IEEE Transactions on Neural Networks & Learning Systems*, vol. 24, no. 9, p. 1478, 2013.

[28] D. Cheng, H. Qi, Z. Li, and J. B. Liu, "Stability and stabilization of Boolean networks," *International Journal of Robust & Nonlinear Control*, vol. 21, no. 2, pp. 134–156, 2011.