SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

May 2021, Vol. 64 152207:1–152207:14
https://doi.org/10.1007/s11432-020-2981-4

A novel synthesis method for reliable feedback shift registers via Boolean networks

Jianquan LU[1*], Bowen LI[2] & Jie ZHONG[3]

[1]*School of Mathematics, Southeast University, Nanjing* 210096*, China;*
[2]*School of Information Science and Engineering, Southeast University, Nanjing* 210096*, China;*
[3]*College of Mathematics and Computer Science, Zhejiang Normal University, Jinhua* 321004*, China*

Received 6 March 2020/Revised 30 April 2020/Accepted 19 June 2020/Published online 25 March 2021

Abstract A random fault or a malicious attack can compromise the security of decryption systems. Using a stable and monotonous feedback shift register (FSR) as the main building block in a convolutional decoder can limit some error propagation. This work focuses on the synthesis of reliable (i.e., globally stable and monotonous) FSRs using the Boolean networks (BNs) method. First, we obtain an algebraic expression of the FSRs, based on which one necessary and sufficient condition for the monotonicity of the FSRs is given. Then, we obtain the upper bound of the number of cyclic attractors for monotonous FSRs. Furthermore, we propose one method of constructing n-stage reliable FSRs, and figure out that the number of reliable FSRs is $\frac{2^{2^{n-4}}}{\phi(n)}$ $(n>5)$ times of that constructed by the existing method, where ϕ denotes the Euler's totient function. Finally, the proposed method and the obtained results are verified by some examples.

Keywords feedback shift register, Boolean networks, semi-tensor product, global stability, monotonicity

Citation Lu J Q, Li B W, Zhong J. A novel synthesis method for reliable feedback shift registers via Boolean networks. Sci China Inf Sci, 2021, 64(5): 152207, https://doi.org/10.1007/s11432-020-2981-4

1 Introduction

Information security is of immense importance to the development of our society and has a great influence on our everyday lives. Investigation of information security such as attacks, cryptographic methods, decoding algorithms, and secure communication has attracted much attention. However, some attacks potentially lead to infinite decoding errors. To limit the spread of decoding errors, a driven stable feedback shift register (FSR) as the main building block in a convolutional decoder has been proposed [1]. Moreover, the FSRs with stability and monotonicity are alternatives to minimize the propagation of these errors. Especially, in [2], $\phi(n)2^{2^{n-2}-1}$ n-stage globally stable and monotonous FSRs were constructed, where ϕ denotes the Euler's totient function. One FSR consists of n binary storage elements called stages, and then the stages are numbered from left to right as $1,2,\ldots,n$. At each clock cycle, the value of the i-th stage is transmitted to the $(i+1)$-th stage, and the value of the first stage is regarded as the output of the FSR. In particular, the value of the n-th bit depends on the feedback function denoted by $f(x_1,x_2,\ldots,x_n)$, where x_i, $i=1,2,\ldots,n$ refers to the value of the i-th stage. If feedback functions are linear, then the FSRs are called linear feedback shift registers (LFSRs); otherwise, the FSRs are called nonlinear feedback shift registers (NLFSRs). Refs. [3,4] have obtained many interesting findings regarding NLFSRs. For example, in [3], an NLFSR was broken down into a cascade connection of an NLFSR and an LFSR. The decomposition has been further investigated in [4], where more reliable LFSR candidates can be identified and computational complexity is reduced compared with [3].

As mentioned above, only $\phi(n)2^{2^{n-2}-1}$ n-stage reliable FSRs have been constructed in [2]. Also, some other reliable FSRs still exist that have not been discovered. Motivated by this, in this paper, FSRs are regarded as Boolean networks (BNs), and then more reliable FSRs can be constructed. The BN, which was first proposed by Kauffman to model genetic regulatory networks in 1969 [5], is a logical network,

* Corresponding author (email: jqluma@seu.edu.cn)

and different from typical complex networks [6, 7]. In BNs, each gene's expression has two states as "1" and "0" to represent "expressed" and "not expressed", respectively. With each clock, each gene's status is updated by a logical function of neighboring gene states. Cheng et al. [8] have suggested that the semi-tensor product (STP) of matrices translates logical systems into corresponding algebraic forms. In other words, we can obtain the algebraic expression of BNs, and great progress has been made in BNs on the basis of this finding such as controllability [9–11], stabilization [12–15], feedback invariant subspace [16], observability [17, 18], and synchronization [19]. Also, STP can be applied to the petri net [20] and fault detection of combinational circuits [21]. Ref. [22] have introduced the application of STP in engineering in detail. FSRs can be interpreted as BNs since the feedback functions are logical. By resorting to STP, some new results for FSRs have been obtained [23–25]. In [26], an analysis of the corresponding transition matrices has been used to derive more necessary and adequate non-singularity conditions for Grain-like cascade FSRs. Zhong et al. [24] have studied the stability of NLFSRs using the method of BNs, and the computational complexity was considerably reduced compared with the exhaustive quest and Lyapunov's direct method. Compared with [27], some algorithms of building equivalent NLFSRs were obtained by resorting to STP without the presumption of the uniform form in [28]. Compared to the conventional methods such as exhaustive search and the De Bruijn-Good graph method, the method of STP is an effective tool to investigate FSRs.

The contributions of this paper can be summarized as follows:

• By considering FSRs as BNs, we obtained the general type of structure matrix for monotonous FSRs using STP and then exposed some of the transition matrix features of monotonous FSRs, which is of great importance for building reliable FSRs.

• According to the features of monotonous FSRs, the total number of cyclic attractors for an n-stage monotonous FSR is not greater than 2^{n-2}. Also, it provides some criteria for observing the existence of cyclic attractors.

• An effective method for constructing reliable FSRs in n-stage is proposed. We can build $2^{2^{n-2}-1+2^{n-4}}$ n-stage reliable FSRs, and the total number is $\frac{2^{2^{n-4}}}{\phi(n)}$ $(n > 5)$ times of that obtained in [2].

The rest of this paper is organized as follows. Section 2 contains some preliminaries on the STP and some key steps to transform logical systems into the respective discrete-time systems. Section 3 considers the construction of reliable FSRs. Section 4 concludes the paper.

2 Preliminaries

First, some commonly-used notations in BNs are listed. The matrix set $M_{m\times n}$ represents the set of $m \times n$ real matrices and $\Delta_n := \{\delta_n^k : 1 \leqslant k \leqslant n\}$, where δ_n^k is the k-th column of identity matrix I_n with dimension n. Let $\mathcal{D} = \{1,\ 0\}$ and

$$\mathcal{D}^n = \underbrace{\mathcal{D} \times \cdots \times \mathcal{D}}_{n}.$$

Let $\mathcal{B}_{m\times n}$ be the set of Boolean matrices with its entries being 1 or 0. A matrix $B \in M_{m\times n}$ is called a logical matrix, if the column set of B, expressed by $\mathrm{Col}(B)$, satisfies $\mathrm{Col}(B) \subseteq \Delta_m$. Let $\mathrm{col}_i(B)$ be the i-th column of matrix B. Let $\mathcal{L}_{m\times n}$ be the set of $m\times n$ logical matrices, and $B = [\delta_m^{i_1}\ \delta_m^{i_2}\ \cdots\ \delta_m^{i_n}] \in \mathcal{L}_{m\times n}$, which can be also denoted by $B = \delta_m[i_1\ i_2 \cdots\ i_n]$. Let $[a, b]$ denote the set $\{a, a+1, \ldots, b\}$ for integers $b > a$. Assume that the set $X = \{\delta_{2^n}^{\alpha_1}, \delta_{2^n}^{\alpha_2}, \ldots, \delta_{2^n}^{\alpha_n}\}$, and then $[X] := \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$. Let $(A)_i$ be the i-th element of vector A. Given a non-empty set $\mathcal{I}$, let $|\mathcal{I}|$ be the number of elements in $\mathcal{I}$. Let $\lceil s\rceil$ denote the smallest integer larger than or equals to s. Vector $\mathbf{1}_n$ represents the n-dimensional row vector whose entries are 1.

In BNs, we always let δ_2^1 and δ_2^2 be equivalent to 1 and 0, respectively. Based on this equivalence, $\mathcal{D}$ ($\mathcal{D}^n$) and Δ_2 (Δ_{2^n}) can be used interchangeably. In general, we say X is in a scalar form if $X \in \mathcal{D}^n$. Inversely, X is in a vector form if $X \in \Delta_{2^n}$. In the following, to distinguish these two different forms, X represents the scalar form and x represents the vector form. The following lemma reveals the relation between X and x.

Lemma 1 ([8])**.** Assume that $X = (x_1, x_2, \ldots, x_n)^{\mathrm{T}} \in \mathcal{D}^n$. The vector $x = \delta_{2^n}^i$ with $i = 2^n - (x_1 2^{n-1} + x_2 2^{n-2} + \cdots + x_n)$ is one-to-one with X. Moreover, vector $x = \delta_{2^n}^i$ can be also decomposed into $\delta_{2^n}^i = \delta_2^{i_1} \ltimes \delta_2^{i_2} \ltimes \cdots \ltimes \delta_2^{i_n}$ satisfying $(i_1-1)2^{n-1} + (i_2-1)2^{n-2} + \cdots + (i_{n-1}-1)2 + i_n = i$, $\delta_{2^n}^{i_j} \in \Delta_2$, $j \in [1, n]$.

For example, assume that $X = (1, 0, 1, 0)^{\mathrm{T}}$, and then one has that $x = \delta_{2^4}^6$ and $\delta_{2^4}^6 \sim (1, 0, 1, 0)^{\mathrm{T}}$ by Lemma 1. Moreover, $\delta_{2^4}^6$ can be uniquely decomposed into $\delta_{2^4}^6 = \delta_2^1 \ltimes \delta_2^2 \ltimes \delta_2^1 \ltimes \delta_2^2$.

2.1 Semi-tensor product of matrices

It is mentioned in Section 1 that the STP breaks through the traditional dimension matching criterion for the multiplication of two matrices, and it implies that two matrices can be multiplied regardless of their dimensions in the framework of STP. Therefore, we first review the the definition of STP.

Definition 1 ([8]). The STP of two matrices $A \in M_{m\times n}$ and $B \in M_{p\times q}$ is defined as

$$A \ltimes B = (A \otimes I_{\frac{s}{n}})(B \otimes I_{\frac{s}{p}}),$$

where $\otimes$ is the Kronecker product and $s = \operatorname{lcm}(n, p)$ is the least common multiple of n and p.

Some differences among the traditional product, Kronecker product, and STP can be found. For the traditional product, the product is element-to-element. The Kronecker product can be regarded as that every element of matrix A multiplies matrix B. For the STP, the product is one element of matrix A multiplies a block of matrix B by Definition 1. It can be noted that STP satisfies all the fundamental properties of the traditional matrix product, and the STP degenerates to the traditional matrix product when $n = p$. Thus, symbol $\ltimes$ is omitted when there is no confusion.

Next, we review some matrices, which will be used in the framework of STP.

Proposition 1 ([8]). Let x be an n-dimension column vector and M be a matrix with arbitrary dimension, and then we have

$$x \ltimes M = (I_{2^n} \otimes M) \ltimes x.$$

Proposition 2 ([8]). Let $x_i \in \Delta_2$, $i \in [1, n]$, and $\ltimes_{i=1}^n x_i = x$, and then $x_i, i \in [1, n]$ can be uniquely determined by

$$x_i = \mathbf{1}_{2^{i-1}}(I_{2^i} \otimes \mathbf{1}_{2^{n-i}})x.$$

2.2 The algebraic expression of BNs

We firstly review how logical networks can be converted into the corresponding algebraic expressions by STP. Consider the following BN with n nodes:

$$\begin{cases} x_1(t+1) = g_1(x_1(t), x_2(t), \ldots, x_n(t)), \\ x_2(t+1) = g_2(x_1(t), x_2(t), \ldots, x_n(t)), \\ \qquad\vdots \\ x_n(t+1) = g_n(x_1(t), x_2(t), \ldots, x_n(t)), \end{cases} \tag{1}$$

where $x_i(t) \in \mathcal{D}$ is a state variable at $t \geqslant 0$, and $g_i : \mathcal{D}^n \to \mathcal{D}$, $i \in [1, n]$ is a logical network.

The following lemma is of great importance to obtain the algebraic expression of logical functions.

Lemma 2 ([8]). Consider logical function $f(x_1, x_2, \ldots, x_n)$ with logical variables $x_1, x_2, \ldots, x_n \in \mathcal{D}$. There exists a unique matrix $M_f \in \mathcal{L}_{2\times 2^n}$, called the structure matrix of f, such that

$$f(x_1, x_2, \ldots, x_n) = M_f \ltimes_{i=1}^n x_i, \tag{2}$$

where $x_i \in \Delta_2$, $i \in [1, n]$.

Actually, the structure matrix of one logical function can be obtained from the corresponding truth table. For example, $x_1(t+1) = x_1(t) \wedge x_2(t)$ with $x_i \in \mathcal{D}$, $i \in [1, 2]$. By considering four cases that (1) $x_1(t) = x_2(t) = 1$, (2) $x_1(t) = 1$ and $x_2(t) = 0$, (3) $x_1(t) = 0$ and $x_2(t) = 1$, and (4) $x_1(t) = 0$ and $x_2(t) = 0$, we have $x_1(t+1) = 1, 0, 0$, and 0 successively. Since $\delta_2^1 \sim 1$ and $\delta_2^2 \sim 0$, the corresponding structure matrix $M_g = \delta_2[1\ 2\ 2\ 2]$, which implies that $x_1(t+1) = M_g x_1(t) x_2(t)$, $x_i \in \Delta_2$, $i \in [1, 2]$. Now, considering system (1), the corresponding structure matrix of $g_i, i \in [1, n]$, is denoted by M_{g_i}, based on which the component-wise algebraic form of system (1) is shown as follows:

$$x_i(t+1) = M_{g_i} x(t), \quad i \in [1, n]. \tag{3}$$

By letting $x(t) = \ltimes_{i=1}^{n} x_i \in \Delta_{2^n}$, and multiplying all the equations in (3), then system (1) can be further expressed as the following linear system:

$$x(t+1) = L_g x(t), \tag{4}$$

where $L_g \in \mathcal{L}_{2^n \times 2^n}$ is called the transition matrix of system (4), and $\mathrm{col}_i(L_g) = \mathrm{col}_i(M_{g_1}) \otimes \mathrm{col}_i(M_{g_2}) \otimes \cdots \otimes \mathrm{col}_i(M_{g_n}), i \in [1, 2^n]$.

It follows from (1)–(4) that logical systems can be converted into linear systems, based on which many problems such as controllability and stability can be investigated. In the following, we regard FSRs as BNs to consider the synthesis of FSRs. The STP method has more advantages in studying some problems of FSRs than the exhaustive search and De Bruijn graph methods. For example, in 2011, Hu et al. [29] proposed a problem about the existence of the minimum period of the sequences generated by NLFSRs in Grain-like structure. Very recently, Zhong et al. [30] has proved that the probability of achieving minimum period is 2^{-n} with n being the number of shifted registers by STP. Therefore, the method of STP is an efficient way to further investigate FSRs. It was mentioned in Section 1 that constructing reliable FSRs is very important to realize relative cryptographic secure. In [2], $\phi(n)2^{2^{n-2}-1}$ n-stage reliable FSRs have been constructed, where ϕ denotes the Euler's totient function. In the following, we will construct more reliable FSRs by the method of STP.

3 Main results

One n-stage FSR can be described as follows:

$$\begin{cases} x_i(t+1) = x_{i+1}(t), & i \in [1, n-1], \\ x_n(t+1) = f(X(t)). \end{cases} \tag{5}$$

Here, the associated state variable of each stage $i \in [1, n]$ is denoted by x_i, and $x_i(t) \in \mathcal{D}$, $i \in [1, n]$ refers to the value of state variable x_i at time t. Define $X(t) = (x_1(t), \ldots, x_n(t))^{\mathrm{T}} \in \mathcal{D}^n$. Function $f(X(t))$ is called the feedback function of FSR (5). Then the value of the n-th stage depends on $f(X(t))$. The state of FSR (5) is the ordered set of values of its state variables $(x_1, x_2, \ldots, x_n)^{\mathrm{T}}$. At each time, the state $(x_1(t), \ldots, x_{n-1}(t), x_n(t))^{\mathrm{T}}$ is shifted to the state $(x_2(t), \ldots, x_n(t), f(X(t)))^{\mathrm{T}}$. Especially, if $f(X(t))$ can satisfy $f(X(t)) = c_1x_1(t) \oplus c_2x_2(t) \oplus \cdots \oplus c_nx_n(t)$ with $c_i \in \mathcal{D}, i \in [1, n]$, then the feedback function $f(X(t))$ is linear; otherwise, it is nonlinear.

For any $i \in [1, n-1]$, the corresponding Boolean function of x_i, denoted by $f_i(X(t))$, can be regarded as $f_i(X(t)) = x_{i+1}(t+1)$ in system (5). Then by Proposition 2, we can also obtain the corresponding structure matrix denoted by M_{f_i}. For example, the corresponding structure matrix for $f_1(X(t)) = x_2(t+1)$ is

$$M_{f_1} = \delta_2[\underbrace{1 \cdots 1}_{2^{n-2}} \; \underbrace{2 \cdots 2}_{2^{n-2}} \; \underbrace{1 \cdots 1}_{2^{n-2}} \; \underbrace{2 \cdots 2}_{2^{n-2}}].$$

Therefore, the component-wise algebraic form of system (5) is derived as follows:

$$x_i(t+1) = M_{f_i} x(t), \quad i \in [1, n],$$

where $x(t) = \ltimes_{i=1}^{n} x_i(t)$, $x_i(t) \in \Delta_2$.

In a similar way of the transformation from (3) to (4), one has that

$$x(t+1) = L_f x(t), \tag{6}$$

where $L_f \in \mathcal{L}_{2^n \times 2^n}$ and $\mathrm{col}_i(L_f) = \mathrm{col}_i(M_{f_1}) \otimes \mathrm{col}_i(M_{f_2}) \otimes \cdots \otimes \mathrm{col}_i(M_{f_n})$, $i \in [1, 2^n]$.

Definition 2 ([31]). For system (5), if state X is shifted to state X', then state X is called the predecessor of state X', and state X' is called the successor of state X.

Definition 3 ([8]). Consider system (5). If there exist $t_0 \geqslant 0$ and an integer number $p \geqslant 1$ such that $X(t_0+p) = X(t_0)$ and the states in the set $\{X(t_0), X(t_0+1), \ldots, X(t_0+p-1)\}$ are pairwise distinct, then $\{X(t_0), X(t_0+1), \ldots, X(t_0+p-1)\}$ is an attractor with period p. If $X(t_0) = X(t_0+1) = \cdots = X(t_0+p-1)$, then the state $X(t_0)$ is called a fixed point; otherwise, $\{X(t_0), X(t_0+1), \ldots, X(t_0+p-1)\}$ is said to be a cyclic attractor.

Definition 4 ([8])**.** System (5) is globally stable if the system globally converges to a fixed point.

Definition 5 ([2])**.** Consider system (5). It can be said that system (5) is monotonous if for any state $X(t) \in \mathcal{D}^n$, $w(X(t+1)) \leqslant w(X(t))$, i.e., $f(X(t)) \leqslant x_1(t)$, where $w(X(t))$ is called the Hamming weight of $X(t)$, and represents the number of one in vector $X(t)$.

In order to construct n-stage reliable FSRs, we firstly analyze the monotonicity of FSRs. Consider system (5), and assume that $M_{f_n} = \delta_2[b_1\ b_2\ \cdots\ b_{2^n}]$. By Definition 5, we have the following theorem.

Theorem 1. The n-stage FSR (5) is monotonous if and only if the structure matrix M_{f_n} of feedback function $f(X(t))$ is in the form of

$$M_{f_n} = \delta_2[b_1 \cdots b_{2^{n-1}} \underbrace{2\ 2 \cdots 2}_{2^{n-1}}], \tag{7}$$

where $b_i \in [1,2]$, $i \in [1, 2^{n-1}]$.

Proof. (Necessity) Assume that state $S = (a_1, \ldots, a_{n-1}, a_n) \sim \delta_{2^n}^{\kappa}$, $\kappa \in [1, 2^n]$. By Definition 5, if system (5) is monotonous, then $f(S) \leqslant a_1$. When $\kappa \in [1, 2^{n-1}]$, i.e., $a_1 = 1$, one has that $f(S) = 1$ or 0, which implies that the κ-th column of M_{f_n} is δ_2^1 or δ_2^2. Similarly, if $\kappa \in [2^{n-1}+1, 2^n]$, then the κ-th column of M_{f_n} is equivalent to δ_2^2. Therefore, structure matrix M_{f_n} should be in the type of

$$\delta_2[b_1 \cdots b_{2^{n-1}} \underbrace{2\ 2 \cdots 2}_{2^{n-1}}].$$

(Sufficiency) The proof of sufficiency is similar to that of necessity, so we omit it here.

Remark 1. By Theorem 1, if the n-stage FSR (5) is monotonous, then the structure matrix M_{f_n} must be in the form of

$$\delta_2[b_1 \cdots b_{2^{n-1}} \underbrace{2\ 2 \cdots 2}_{2^{n-1}}].$$

Moreover, we can see that the first 2^{n-1} columns of M_{f_n} can be δ_2^1 or δ_2^2. Then we can get that the total number of n-stage monotonous FSRs is $2^{2^{n-1}}$.

Based on Lemma 1, some properties about the transition matrix of n-stage monotonous FSRs denoted by L_f can be revealed.

Lemma 3. Consider an n-stage monotonous FSR. The corresponding transition matrix has the following property:

$$\mathrm{col}_i(L_f) = \begin{cases} \delta_{2^n}^{2(i-1)+b_i}, & i \in [1, 2^{n-1}], \\ \delta_{2^n}^{2(i-2^{n-1})}, & i \in [2^{n-1}+1, 2^n]. \end{cases} \tag{8}$$

Proof. Assume that the state of an n-stage monotonous FSR with structure matrix M_{f_n} satisfying (7) is equal to $\delta_{2^n}^i$ at time t, and $\delta_{2^n}^i = \delta_2^{i_1}\delta_2^{i_2}\cdots\delta_2^{i_n}$, which implies that $x_j(t) = \delta_2^{i_j}, j \in [1, n]$. Then one has that $x_j(t+1) = \delta_2^{i_{j+1}}, j \in [1, n-1]$ and $x_n(t+1) = \delta_2^{b_i}$. Further assume that $\delta_{2^n}^j = \delta_2^{i_2}\delta_2^{i_3}\cdots\delta_2^{b_i}$, and then by Lemma 1, one has that

$$\begin{cases} (i_1-1)2^{n-1} + (i_2-1)2^{n-2} + \cdots + (i_{n-1}-1)2 + i_n = i, \\ (i_2-1)2^{n-1} + (i_3-1)2^{n-2} + \cdots + (i_n-1)2 + b_i = j. \end{cases}$$

By reduction, we have $i_1 2^n = 2^n + 2i - 2 - j + b_i$. Further considering these two cases: $i_1 = 1$ and $i_1 = 2$, equation (8) holds.

For any two Boolean vectors $x = \delta_{2^n}^{\alpha}$ and $y = \delta_{2^n}^{\beta}$, we say that $x < y$ if and only if $\alpha < \beta$. For example, $x = \delta_{2^3}^3$ and $y = \delta_{2^3}^5$, then we have $x < y$. From Lemma 3, we can summarize two features of transition matrices of monotonous FSRs as:

• The values of the first 2^{n-1} columns of L_f depend on $b_i, i \in [1, 2^{n-1}]$, but the values of last 2^{n-1} columns are deterministic;

• For any $j \in [1, 2^{n-1}-1]$, $\mathrm{col}_j(L_f) < \mathrm{col}_{j+1}(L_f)$, and $\mathrm{col}_{2^{n-1}+j}(L_f) < \mathrm{col}_{2^{n-1}+j+1}(L_f)$.

The above two properties of transition matrices for monotonous FSRs are of great importance in constructing monotonous and stable FSRs. It was shown in [24, 32] that states $\delta_{2^n}^1$ and $\delta_{2^n}^{2^n}$ are the only two possible fixed points of FSR (5). Then by (8), the successor of $\delta_{2^n}^1$ is either $\delta_{2^n}^1$ or $\delta_{2^n}^2$, and the successor of $\delta_{2^n}^{2^n}$ can only be itself. Therefore, $\delta_{2^n}^1$ is not necessary to be a fixed point, but $\delta_{2^n}^{2^n}$ must be a fixed point for monotonous FSRs. By the above analysis, we consider the case of n-stage monotonous FSRs globally stable at $\delta_{2^n}^{2^n}$.

By Theorem 1, a total of $2^{2^{n-1}}$ monotonous FSRs can be constructed. Based on these monotonous FSRs, we need to add some constraints on $b_i, i \in [1, 2^{n-1}]$ to achieve global stability. Zhong et al. [24] presented one necessary and sufficient condition for global stability of n-stage FSRs by using STP, that is, n-stage FSRs are globally stable if and only if there exists a positive integer $T \leqslant 2^n - 1$ such that $\mathrm{Col}(L^T) = \{\delta_{2^n}^{2^n}\}$, where L represents the transition matrix of n-stage FSRs. Unfortunately, it is quite difficult to use the above condition to find constraints about $b_i, i \in [1, 2^{n-1}]$ due to the exponent T. In this paper, we mainly use Definition 4 and Theorem 1 to construct n-stage reliable FSRs. To this end, we give some definitions about graph theory.

Definition 6. A state transition graph of n-stage FSRs, $T(V, E)$, consists of 2^n vertices and 2^n edges. The vertex set is $V = \mathcal{D}^n$, and each vertex is one of the states of FSRs. The set E is the set of 2^n edges, and each edge points from a state to its unique successor.

Definition 7. A pseudo-state transition graph of n-stage monotonous FSRs, denoted by $PT(V, E')$, consists of 2^n vertices and $2^n + 2^{n-1}$ edges. Each vertex represents one of the states of monotonous FSRs, and the vertex set is $V = \mathcal{D}^n$. If state y is one of the successors of state x, then there exists an edge pointing from x to y.

Remark 2. Compared with the state transition graph $T(V, E)$, the main difference is that there exist two successors rather than a unique successor for any vertex $x \in \{(1\ a_2\ a_3\ \cdots\ a_n)^{\mathrm{T}} | a_i \in \mathcal{D}, i \in [2, n]\}$ in $PT(V, E')$. The reason is that the first 2^{n-1} columns of M_f (or L_f) in n-stage monotonous FSRs are indeterminate, leading to that there exist two possible successors for any vertex $x \in \{(1\ a_2\ a_3\ \cdots\ a_n)^{\mathrm{T}} | a_i \in \mathcal{D}, i \in [2, n]\}$. Therefore, the state transition graph $T(V, E)$ can be regarded as a spanning subgraph of the $PT(V, E')$.

Example 1. Consider the following 4-stage FSR:

$$\begin{cases} x_1(t+1) = x_2(t), \\ x_2(t+1) = x_3(t), \\ x_3(t+1) = x_4(t), \\ x_4(t+1) = x_1(t) \wedge ((x_2(t) \wedge (x_3(t) \to x_4(t))) \vee \neg x_2(t) \wedge x_3(t)). \end{cases} \tag{9}$$

By Lemma 2, we can obtain the structure matrix of the feedback function, that is, $M_f = \delta_2[1\ 2\ 1\ 1\ 1\ 1\ 2\ 2\ 2\ 2\ 2\ 2\ 2\ 2\ 2\ 2]$. Therefore, system (9) is monotonous by Theorem 1. Moreover, it follows from Theorem 1 that the total number of 4-stage monotonous FSRs is 2^{2^3}. The state transition graph $T(V, E)$ can be depicted as Figure 1. Based on Definition 7 and Eq. (7), the pseudo-state transition graph $PT(V, E')$ of 4-stage monotonous FSRs can be obtained as Figure 2. Additionally, all of the possible trajectories of 4-stage monotonous FSRs can be observed from Figure 2.

Lemma 4. If n-stage FSRs are reliable at $\delta_{2^n}^{2^n}$, i.e.,

$$(\underbrace{0\ 0\ \cdots\ 0}_{n})^{\mathrm{T}},$$

then the corresponding structure matrix of feedback functions satisfies that $b_1 = b_{2^{n-1}} = 2$.

Proof. Assume that L_f is the transition matrix of an n-stage reliable FSR. If $b_1 = 1$, then by Eq. (8), we have $\mathrm{col}_1(L_f) = \delta_{2^n}^1$, which implies that $\delta_{2^n}^1$ is a fixed point of the n-stage FSR, and this contradicts with that the n-stage FSR is globally stable at $\delta_{2^n}^{2^n}$. Therefore, we have $b_1 = 2$. Let $R_i(\delta_{2^n}^{2^n})$ be the set of states satisfying that it reaches $\delta_{2^n}^{2^n}$ at the i-th step. Assume that $b_{2^{n-1}} = 1$, and then it implies that $R_1(\delta_{2^n}^{2^n}) = \{\delta_{2^n}^{2^n}\}$ by (8). If $R_1(\delta_{2^n}^{2^n}) = \{\delta_{2^n}^{2^n}\}$, then the n-stage FSR cannot be globally stable at $\delta_{2^n}^{2^n}$. As a result, the conclusion holds.

By Definition 4, when the system is globally stable at $\delta_{2^n}^{2^n}$, there only exists a unique fixed point $\delta_{2^n}^{2^n}$ without any cyclic attractor. If Lemma 4 can be satisfied, then monotonous FSRs only has one fixed point, that is $\delta_{2^n}^{2^n}$. Therefore, if we want to construct reliable FSRs, then not only Lemma 4 should be satisfied, but the FSRs should guarantee that there is no any cyclic attractor. For better analysis, we use $\mathcal{O}_1$ and $\mathcal{O}_2$ to denote the sets $\{\delta_{2^n}^1, \delta_{2^n}^2, \ldots, \delta_{2^n}^{2^{n-1}}\}$ and $\{\delta_{2^n}^{2^{n-1}+1}, \delta_{2^n}^{2^{n-1}+2}, \ldots, \delta_{2^n}^{2^n}\}$, respectively.

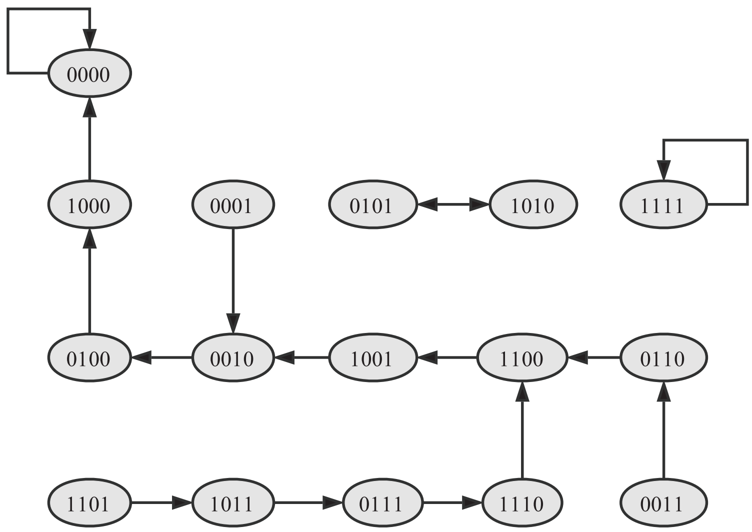

Figure 1 The state transition graph $T(V,E)$ of system (9), where each 4-tuple represents a state $(x_1,x_2,x_3,x_4)^{\mathrm{T}}$.

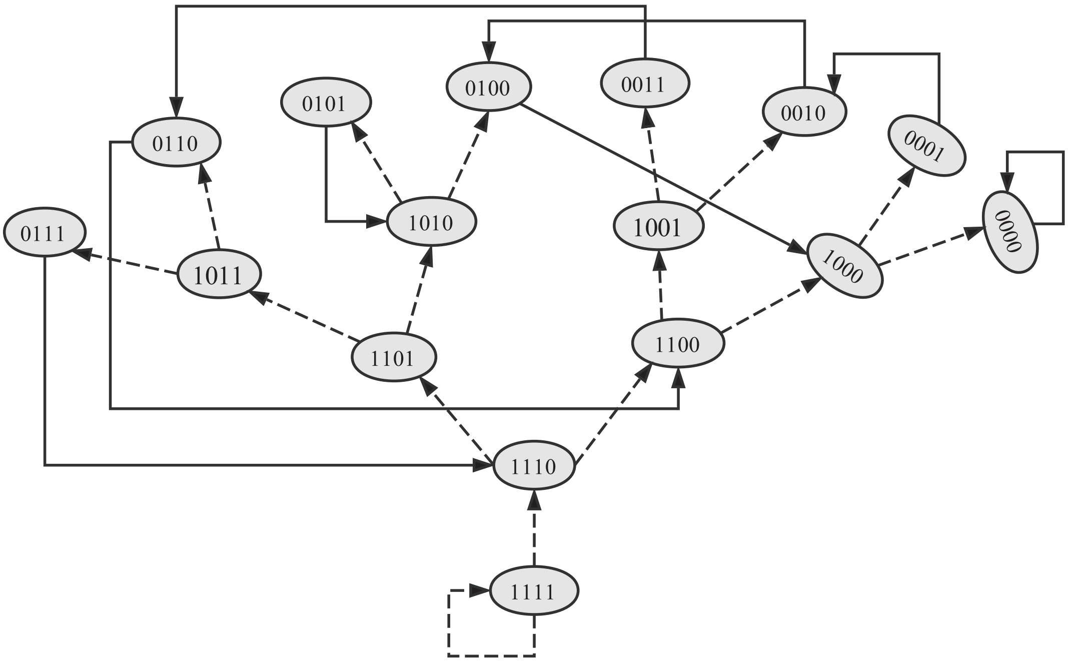

Figure 2 The $PT(V,E')$ of a 4-stage monotonous FSR, where each 4-tuple represents a state $(x_1,x_2,x_3,x_4)^{\mathrm{T}}$. A node with an arrow in a solid line (or two arraws in dotted lines) represents that it has one successor (or two potential successors).

Lemma 5. Consider an n-stage monotonous FSR. Assume that there exist m cyclic attractors represented by $C^1 \sim \{\delta_{2^n}^{r_1^1}, \delta_{2^n}^{r_2^1}, \ldots, \delta_{2^n}^{r_{l_1}^1}\}, \ldots, C^m \sim \{\delta_{2^n}^{r_1^m}, \delta_{2^n}^{r_2^m}, \ldots, \delta_{2^n}^{r_{l_m}^m}\}$, with lengths $l_1,\ldots,l_m$, respectively. Then the following two results hold:

- For any $i \in [1,m]$, C^i is neither a subset of $\mathcal{O}_1$ nor a subset of $\mathcal{O}_2$;
- For any cyclic attractor C^i, $i \in [1,m]$, there must exist two states $\delta_{2^n}^{r_{\alpha_1}^i}$ and $\delta_{2^n}^{r_{\alpha_2}^i}$ satisfying $\mathrm{col}_{r_{\alpha_2}^i}(L_f) = \delta_{2^n}^{r_{\alpha_1}^i}$, where $\delta_{2^n}^{r_{\alpha_1}^i} \in C^i \cap \mathcal{O}_1$ and $\delta_{2^n}^{r_{\alpha_2}^i} \in C^i \cap \mathcal{O}_2$.

Proof. For any cyclic attractor C^i, $i \in [1,m]$, one has that $x(t_0+l_i) = x(t_0)$, $x(t_0) \in C^i$ by Definition 3. If C^i is a subset of $\mathcal{O}_1$, i.e., $C^i \subseteq \mathcal{O}_1$, then $x(t_0+l_i) = x(t_0) \in \mathcal{O}_1$. But for any $j \in [1, 2^{n-1}-1]$, $\mathrm{col}_j(L_f) < \mathrm{col}_{j+1}(L_f)$, which implies that it does not exist l_i such that $x(t_0+l_i) = x(t_0)$. The same conclusion can be also obtained considering the case $C^i \subseteq \mathcal{O}_2$. Thus, C^i is not a subset of $\mathcal{O}_1$ or $\mathcal{O}_2$. According to (8), we have $\mathrm{col}_{2^{n-1}+j}(L_f) < \mathrm{col}_{2^{n-1}+j+1}(L_f)$, $j \in [1, 2^{n-1}-1]$ and $\mathrm{col}_{2^{n-1}+1}(L_f) = \delta_{2^n}^2$. Based on the properties, for cyclic attractor C^i, there must exist two states $\delta_{2^n}^{r^i_{\alpha_1}} \in C^i \cap \mathcal{O}_1$ and $\delta_{2^n}^{r^i_{\alpha_2}} \in C^i \cap \mathcal{O}_2$ satisfying $\mathrm{col}_{r^i_{\alpha_2}}(L_f) = \delta_{2^n}^{r^i_{\alpha_1}}$, $i \in [1, m]$, that is, $x(t_0+l_i) = x(t_0) = \delta_{2^n}^{r^i_{\alpha_1}}$. Therefore, the above two results hold.

Based on Lemma 5, the upper bound of the total number of cyclic attractors of n-stage monotonous FSRs can be obtained.

Theorem 2. For any n-stage monotonous FSR, the total number of cyclic attractors is not larger than 2^{n-2}.

Proof. On one hand, for any odd integer $\beta \in [\mathcal{O}_2]$, the state $\delta_{2^n}^{\beta}$ has a unique predecessor and a unique successor by (8), i.e., $\delta_{2^n}^{\lceil \frac{\beta}{2} \rceil}$ and $\delta_{2^n}^{2(\beta-2^{n-1})}$. Then, states $\delta_{2^n}^{\lceil \frac{\beta}{2} \rceil}$, $\delta_{2^n}^{\beta}$ and $\delta_{2^n}^{2(\beta-2^{n-1})}$ must be in the same cyclic attractor. Considering an even integer $\alpha \in [\mathcal{O}_2]$, state $\delta_{2^n}^{\alpha}$ has two potential predecessors $\delta_{2^n}^{\frac{\alpha}{2}}$ and $\delta_{2^n}^{2^{n-1}+\frac{\alpha}{2}}$, and a unique successor $\delta_{2^n}^{2(\alpha-2^{n-1})}$. Then, there exist two cyclic attractors containing $\delta_{2^n}^{\alpha}$ as: $\delta_{2^n}^{\frac{\alpha}{2}} \to \delta_{2^n}^{\alpha} \to \delta_{2^n}^{2(\alpha-2^{n-1})} \to \cdots \to \delta_{2^n}^{\frac{\alpha}{2}}$ and $\delta_{2^n}^{2^{n-1}+\frac{\alpha}{2}} \to \delta_{2^n}^{\alpha} \to \delta_{2^n}^{2(\alpha-2^{n-1})} \to \cdots \to \delta_{2^n}^{2^{n-1}+\frac{\alpha}{2}}$. In fact, the cyclic attractor $\delta_{2^n}^{\frac{\alpha}{2}} \to \delta_{2^n}^{\alpha} \to \delta_{2^n}^{2(\alpha-2^{n-1})} \to \cdots \to \delta_{2^n}^{\frac{\alpha}{2}}$ does not exist. The proof will be given at Appendix A.

On the other hand, let $\mathcal{S}_1 = \{\delta_{2^n}^{2^{n-1}+1}, \delta_{2^n}^{2^{n-1}+2}, \ldots, \delta_{2^n}^{2^{n-1}+2^{n-2}}\}$ and $\mathcal{S}_2 = \mathcal{O}_2 \backslash \mathcal{S}_1$. For any $\delta_{2^n}^i \in \mathcal{S}_2$, it follows from (8) that there exists a unique path from $\delta_{2^n}^i$ to $\delta_{2^n}^{\alpha} \in \mathcal{S}_1$, which indicates that states $\delta_{2^n}^i$ and $\delta_{2^n}^{\alpha}$ are in the same cyclic attractor. Therefore, for any n-stage monotonous FSR, the total number of cyclic attractors is not larger than $|\mathcal{S}_1|$, i.e., 2^{n-2}.

Remark 3. Considering n-stage monotonous FSRs, the successor of state $x \in \mathcal{O}_1$ is nondeterministic, which is dependent on $b_i, i \in [\mathcal{O}_1]$. This fact causes that the total number of cyclic attractors is also not deterministic. Inversely, for state $x \in \mathcal{O}_2$, its successor is determined by (8). Therefore, we can deduce the range of the total number of cyclic attractors for n-stage monotonous FSRs, i.e., Theorem 2. Taking Figure 2 as an example, the successors of states $\delta_{16}^{10} \sim (0\ 1\ 1\ 0)^{\mathrm{T}}$ and $\delta_{16}^{13} \sim (0\ 0\ 1\ 1)^{\mathrm{T}}$ with $\delta_{16}^{10}, \delta_{16}^{13} \in \mathcal{O}_2 = \{\delta_{16}^9, \delta_{16}^{10}, \delta_{16}^{11}, \delta_{16}^{12}, \delta_{16}^{13}, \delta_{16}^{14}, \delta_{16}^{15}, \delta_{16}^{16}\}$ are determined, that is, $(0\ 1\ 1\ 0)^{\mathrm{T}} \to (1\ 1\ 0\ 0)^{\mathrm{T}}$ and $(0\ 0\ 1\ 1)^{\mathrm{T}} \to (0\ 1\ 1\ 0)^{\mathrm{T}}$. Thus, the trajectory $(0\ 0\ 1\ 1)^{\mathrm{T}} \to (0\ 1\ 1\ 0)^{\mathrm{T}} \to (1\ 1\ 0\ 0)^{\mathrm{T}}$ is deterministic. If there exists a cyclic attractor containing $(0\ 1\ 1\ 0)^{\mathrm{T}}$, then the cyclic attractor must contain $(0\ 0\ 1\ 1)^{\mathrm{T}}$ and $(1\ 1\ 0\ 0)^{\mathrm{T}}$ simultaneously. However, another predecessor of $(0\ 1\ 1\ 0)^{\mathrm{T}}$ is nondeterministic, and has two cases: equal to $(1\ 0\ 1\ 1)^{\mathrm{T}}$ or nonexistent by (8). Actually, it does not exist a cyclic attractor including $(0\ 1\ 1\ 0)^{\mathrm{T}}$ and $(1\ 0\ 1\ 1)^{\mathrm{T}}$. The proof will be given at Appendix A.

In the following, Algorithm 1 is provided to find all the states in set $\mathcal{S}_2$ which can reach $\mathcal{S}_1$. As for any $\delta_{2^n}^i \in \mathcal{S}_1$, all the states that reach $\delta_{2^n}^i$ are saved as a tuple denoted by F_i where $\delta_{2^n}^i$ is also included.

Algorithm 1 Find all the states in set $\mathcal{S}_2$ that can reach $\mathcal{S}_1$.

Initial set $\mathcal{S}_1 = \{\delta_{2^n}^{2^{n-1}+1}, \delta_{2^n}^{2^{n-1}+2}, \ldots, \delta_{2^n}^{2^{n-1}+2^{n-2}}\}$;
for $i = 2^{n-1}+1$ to $2^{n-1}+2^{n-2}$ **do**
  $x = i$, $F_i = \emptyset$;
  $F_i = F_i \cup \delta_{2^n}^x$;
  while $(x < 2^n) \wedge$ (x is even) **do**
    $x = \frac{x}{2} + 2^{n-1}$;
    $F_i \leftarrow \delta_{2^n}^x$;
  end while
  Output F_i;
end for

By Algorithm 1, we can obtain $F_{2^{n-1}+1}, F_{2^{n-1}+2}, \ldots, F_{2^{n-1}+2^{n-2}}$. Further, we define a new set denoted by $\bar{\mathcal{S}}$ as $\bar{\mathcal{S}} = (F_{2^{n-1}+1})_{|F_{2^{n-1}+1}|} \cup (F_{2^{n-1}+2})_{|F_{2^{n-1}+2}|} \cup \cdots \cup (F_{2^{n-1}+2^{n-2}})_{|F_{2^{n-1}+2^{n-2}}|}$. Therefore, for any state in set $\bar{\mathcal{S}}$, its predecessor is in set $\mathcal{O}_1$.

Lemma 6. Consider an n-stage monotonous FSR. Assume that $\bar{\mathcal{S}} = \{\delta_{2^n}^{\mu_1}, \delta_{2^n}^{\mu_2}, \ldots, \delta_{2^n}^{\mu_\varphi}\}$. Then the following statements can be obtained.

- Set $[\bar{\mathcal{S}}]$ is the set of all the odd integers in set $[\mathcal{O}_2]$.
- For any $\mu_i, i \in [1, \varphi]$, if state $\delta_{2^n}^{\mu_i}$ has a predecessor, then the predecessor must be $\delta_{2^n}^{\lceil \frac{\mu_i}{2} \rceil}$ with $\lceil \frac{\mu_i}{2} \rceil \in [\mathcal{O}_1]$.
- If for any $i \in [1, \varphi]$, let $b_{\lceil \frac{\mu_i}{2} \rceil} = 2$, then there does not exist any cyclic attractor in the n-stage monotonous FSR.

Proof. For any $x \in [\mathcal{S}_1]$, the x is always less than 2^n when performing the command $x = \frac{x}{2} + 2^{n-1}$. Then the fact implies that the command will be terminated only when x is an odd integer. Therefore, for any $i \in [2^{n-1}+1, 2^{n-1}+2^{n-2}]$, the last element of set F_i must be odd. Followed by (8), for any state $\delta_{2^n}^i \in \mathcal{O}_2$, its successor must be an even integer. While, all the states in set $\bar{\mathcal{S}}$ are odd integers, which implies that their predecessors must not be in set $\mathcal{O}_2$. Therefore, if state $\delta_{2^n}^{\mu_i}, i \in [1, \varphi]$ has predecessor, then the predecessor $\delta_{2^n}^{\lceil \frac{\mu_i}{2} \rceil}$ must be in set $\mathcal{O}_1$.

By Theorem 2, any cyclic attractor must contain at least one of states of the set $\mathcal{S}_1$. If we break all trajectories that might form cyclic attractors, then n-stage monotonous FSRs do not have any cyclic attractor. On one hand, for any odd integer $\alpha \in [\mathcal{S}_1]$, we have $F_\alpha = \{\delta_{2^n}^\alpha\}$ with $\delta_{2^n}^\alpha \in \bar{\mathcal{S}}$, and $\delta_{2^n}^\alpha$ has a unique successor and a unique predecessor, i.e., $\delta_{2^n}^{2(\alpha-2^{n-1})}$ and $\delta_{2^n}^{\lceil \frac{\alpha}{2} \rceil}$. Therefore, states $\delta_{2^n}^{\lceil \frac{\alpha}{2} \rceil}$, $\delta_{2^n}^\alpha$, and $\delta_{2^n}^{2(\alpha-2^{n-1})}$ are in the same cyclic attractor. If let $b_{\lceil \frac{\alpha}{2} \rceil} = 2$, then state $\delta_{2^n}^{\lceil \frac{\alpha}{2} \rceil}$ is not the predecessor of $\delta_{2^n}^\alpha$ but the predecessor of $\delta_{2^n}^{\alpha+1}$ with $\alpha+1$ being an even integer, which implies that the unique possible cyclic attractor containing $\delta_{2^n}^\alpha$ is damaged. Then we have $\delta_{2^n}^{\lceil \frac{\alpha}{2} \rceil} \to \delta_{2^n}^{\alpha+1}$ when let $b_{\lceil \frac{\alpha}{2} \rceil} = 2$. However, it is impossible that these exists a cyclic attractor containing $\delta_{2^n}^{\lceil \frac{\alpha}{2} \rceil}$ and $\delta_{2^n}^{\alpha+1}$. The proof will be provided in Appendix A.

On the other hand, for any odd integer $\beta \in [\mathcal{S}_2]$ and any even integer $i \in [\mathcal{S}_1]$, there always exists a unique path from $\delta_{2^n}^\beta$ to $\delta_{2^n}^i$ by (8). Therefore, $\delta_{2^n}^\beta$ and $\delta_{2^n}^i$ are in the same cyclic attractor. Similarly, let $b_{\lceil \frac{\beta}{2} \rceil} = 2$, and then state $\delta_{2^n}^{\lceil \frac{\beta}{2} \rceil}$ is not the predecessor of $\delta_{2^n}^\beta$ but the predecessor of $\delta_{2^n}^{\beta+1}$ with $\beta+1$ being an even integer, which implies that the unique possible cyclic attractor containing $\delta_{2^n}^\beta$ is damaged. Moreover, it is impossible that these exists a cyclic attractor containing $\delta_{2^n}^{\lceil \frac{\beta}{2} \rceil}$ and $\delta_{2^n}^{\beta+1}$ (see Appendix A). Therefore, based on Theorem 2, if for any $i \in [1, \varphi]$, let $b_{\lceil \frac{\mu_i}{2} \rceil} = 2$, then any n-stage monotonous FSR has no cyclic attractor.

Example 2. Reconsider the $PT(V, E')$ of the 4-stage monotonous FSR depicted in Figure 2 with $\mathcal{O}_1 = \{\delta_{16}^i : i \in [1, 8]\}$ and $\mathcal{O}_2 = \{\delta_{16}^i : i \in [9, 16]\}$. There exist four possible cyclic attractors depending on $b_i, i \in [\mathcal{O}_1]$, denoted by $\mathcal{C}_1$, $\mathcal{C}_2$, $\mathcal{C}_3$, $\mathcal{C}_4$, and two fixed points denoted by $\mathcal{F}_1$, $\mathcal{F}_2$, respectively, where

$$\begin{aligned}
&\mathcal{C}_1 : \delta_{16}^2 \sim (1\ 1\ 1\ 0)^{\mathrm{T}} \to \delta_{16}^3 \sim (1\ 1\ 0\ 1)^{\mathrm{T}} \to \delta_{16}^5 \sim (1\ 0\ 1\ 1)^{\mathrm{T}} \to \delta_{16}^9 \sim (0\ 1\ 1\ 1)^{\mathrm{T}} \to \delta_{16}^2 \sim (1\ 1\ 1\ 0)^{\mathrm{T}},\\
&\mathcal{C}_2 : \delta_{16}^4 \sim (1\ 1\ 0\ 0)^{\mathrm{T}} \to \delta_{16}^7 \sim (1\ 0\ 0\ 1)^{\mathrm{T}} \to \delta_{16}^{13} \sim (0\ 0\ 1\ 1)^{\mathrm{T}} \to \delta_{16}^{10} \sim (0\ 1\ 1\ 0)^{\mathrm{T}} \to \delta_{16}^4 \sim (1\ 1\ 0\ 0)^{\mathrm{T}},\\
&\mathcal{C}_3 : \delta_{16}^8 \sim (1\ 0\ 0\ 0)^{\mathrm{T}} \to \delta_{16}^{15} \sim (0\ 0\ 0\ 1)^{\mathrm{T}} \to \delta_{16}^{14} \sim (0\ 0\ 1\ 0)^{\mathrm{T}} \to \delta_{16}^{12} \sim (0\ 1\ 0\ 0)^{\mathrm{T}} \to \delta_{16}^8 \sim (1\ 0\ 0\ 0)^{\mathrm{T}},\\
&\mathcal{C}_4 : \delta_{16}^6 \sim (1\ 0\ 1\ 0)^{\mathrm{T}} \to \delta_{16}^{11} \sim (0\ 1\ 0\ 1)^{\mathrm{T}} \to \delta_{16}^6 \sim (1\ 0\ 1\ 0)^{\mathrm{T}},\\
&\mathcal{F}_1 = \delta_{16}^1 \sim (1\ 1\ 1\ 1)^{\mathrm{T}},\ \text{and}\ \mathcal{F}_1 = \delta_{16}^{16} \sim (0\ 0\ 0\ 0)^{\mathrm{T}}.
\end{aligned}$$

We can see that for any cyclic attractor $\mathcal{C}_i, i \in [1, 4]$, there always exist $\delta_{16}^\alpha \in \mathcal{C}_i \cap \mathcal{O}_1$ and $\delta_{16}^\beta \in \mathcal{C}_i \cap \mathcal{O}_2$ satisfying $\delta_{16}^\beta \to \delta_{16}^\alpha$, which verifies Lemma 5. Moreover, one has that $\mathcal{S}_1 = \{\delta_{16}^9, \delta_{16}^{10}, \delta_{16}^{11}, \delta_{16}^{12}\}$. Then it can be obtained that $F_9 = \{\delta_{16}^9\}, F_{10} = \{\delta_{16}^{10}, \delta_{16}^{13}\}, F_{11} = \{\delta_{16}^{11}\}$, and $F_{12} = \{\delta_{16}^{12}, \delta_{16}^{14}, \delta_{16}^{15}\}$ by Algorithm 1. Further, we have $\bar{\mathcal{S}} = \{\delta_{16}^9, \delta_{16}^{13}, \delta_{16}^{11}, \delta_{16}^{15}\}$ satisfying $9\%2 = 11\%2 = 13\%2 = 15\%2 = 1$. Let $b_{\lceil \frac{9}{2} \rceil} = 2$, $b_{\lceil \frac{11}{2} \rceil} = 2$, $b_{\lceil \frac{13}{2} \rceil} = 2$, and $b_{\lceil \frac{15}{2} \rceil} = 2$ as shown in Figure 3. Then by Lemma 6, there does not exist any cyclic attractor in 4-stage monotonous FSRs.

By Lemma 6, to guarantee no cyclic attractor in n-stage monotonous FSRs, we need to fix $b_{\lceil \frac{\mu_1}{2} \rceil}, b_{\lceil \frac{\mu_2}{2} \rceil}, \ldots, b_{\lceil \frac{\mu_\varphi}{2} \rceil}$. However, it is possible that there exist some states belonging to $\bar{\mathcal{S}}$ under the assumption that $\delta_{2^n}^{\mu_i}$ and $\delta_{2^n}^{\mu_j}$ are in the same cyclic attractor. Then we only need to fix either $b_{\lceil \frac{\mu_i}{2} \rceil}$ or $b_{\lceil \frac{\mu_j}{2} \rceil}$ instead of both. If $\delta_{2^n}^{\mu_i}$ and $\delta_{2^n}^{\mu_j}$ are in the same cyclic attractor, then $\delta_{2^n}^{\mu_i}$ and $\delta_{2^n}^{\mu_j}$ are saved as a binary array denoted by $(\delta_{2^n}^{\mu_i}, \delta_{2^n}^{\mu_j})$. Based on the above analysis, either $b_{\lceil \frac{\mu_i}{2} \rceil}$ or $b_{\lceil \frac{\mu_j}{2} \rceil}$ is equal to 2, so it is impossible to form a cyclic attractor containing $\delta_{2^n}^{\mu_i}$ and $\delta_{2^n}^{\mu_j}$. Therefore, the following lemma is given to find the arrays to reduce the number of b_i which needs to be fixed.

Lemma 7. Consider an n-stage monotonous FSR. Supposing that $\bar{\mathcal{S}} = \{\delta_{2^n}^{\mu_1}, \delta_{2^n}^{\mu_2}, \ldots, \delta_{2^n}^{\mu_\varphi}\}$, we have the following results:

- In set $\bar{\mathcal{S}}$, there must exist some different states which belong to the same cyclic attractor when $n \geqslant 5$.
- If $(2^{n-1}+1) \bmod 3 \neq 0$, then there exist 2^{n-4} binary arrays such that the states in an array are in the same cyclic attractor. If $(2^{n-1}+1) \bmod 3 = 0$, then there exist $2^{n-4}-1$ binary arrays.

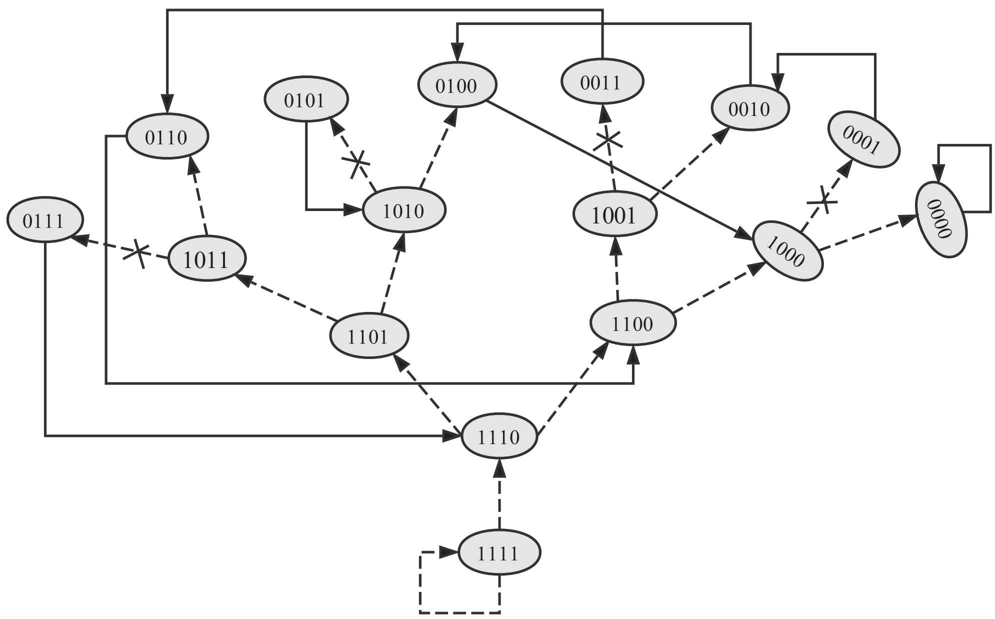

Figure 3 The $PT(V,E')$ of a 4-stage monotonous FSR after deleting some edges based on Lemma 6, where each 4-tuple represents a state $(x_1,x_2,x_3,x_4)^{\mathrm{T}}$, and the dashed line with a "×" means the path has been deleted.

The binary arrays are given as follows: $(\delta_{2^n}^{2^{n-1}+2^{n-3}+1},\delta_{2^n}^{4(2^{n-3}+1)-1})$, $(\delta_{2^n}^{2^{n-1}+2^{n-3}+3},\delta_{2^n}^{4(2^{n-3}+3)-1})$,..., $(\delta_{2^n}^{2^{n-1}+2^{n-3}+1+(2^{n-4}-1)2}, \delta_{2^n}^{4(2^{n-3}+1+(2^{n-4}-1)2)-1})$. Let Γ denote the set of these binary arrays for simplicity. If $(2^{n-1}+1) \bmod 3 = 0$, then the binary arrays are $\Gamma\backslash\{(\delta_{2^n}^{2^{n-1}+\frac{2^{n-1}+1}{3}}, \delta_{2^n}^{4\frac{2^{n-1}+1}{3}-1})\}$.

Proof. If we can find $\mu_{\alpha_1},\mu_{\alpha_2}$ and λ with $\mu_{\alpha_1},\mu_{\alpha_2}\in[\bar{\mathcal{S}}]$ and $\lambda\in[\mathcal{O}_1]$ satisfying $\delta_{2^n}^{\mu_{\alpha_1}}\rightarrow\delta_{2^n}^{\lambda}\rightarrow\delta_{2^n}^{\mu_{\alpha_2}}$, then in set $\bar{\mathcal{S}}$, there must exist different states which belong to the same cyclic attractor. Clearly, if there exists a path $\delta_{2^n}^{\mu_{\alpha_1}}\rightarrow\delta_{2^n}^{\lambda}\rightarrow\delta_{2^n}^{\mu_{\alpha_2}}$, then $\lambda=2(\mu_{\alpha_1}-2^{n-1})$ by Eq. (8). Since $\mu_{\alpha_1},\mu_{\alpha_2}\in[\bar{\mathcal{S}}]$ and $\lambda\in[\mathcal{O}_1]$, one has that $\mu_{\alpha_1}>2^{n-1}$, $\mu_{\alpha_2}>2^{n-1}$ and $\lambda\leqslant 2^{n-1}$. Let $\mu_{\alpha_1}-2^{n-1}=\bar{\mu}_{\alpha_1}$, and then $\lambda=2\bar{\mu}_{\alpha_1}$, which indicates that $\bar{\mu}_{\alpha_1}\leqslant 2^{n-2}$. Since $\delta_{2^n}^{\lambda}$ is the unique predecessor of $\delta_{2^n}^{\mu_{\alpha_2}}$, $\mu_{\alpha_2}=2(2\bar{\mu}_{\alpha_1}-1)+1=4\bar{\mu}_{\alpha_1}-1$. Moreover, $\mu_{\alpha_2}>2^{n-1}$, and then one has that $4\bar{\mu}_{\alpha_1}-1>2^{n-1}\Longrightarrow\bar{\mu}_{\alpha_1}>2^{n-3}+\frac{1}{4}$. Due to $\mu_{\alpha_1}\neq\mu_{\alpha_2}$, it can be obtained that $\bar{\mu}_{\alpha_1}\neq\frac{2^{n-1}+1}{3}$. Additionally, μ_{α_1} is an odd integer by Lemma 6, so that $\bar{\mu}_{\alpha_1}$ must be also an odd integer. Based on the above analysis, some restrained conditions on $\bar{\mu}_{\alpha_1}$ can be derived:

$$\begin{cases} 2^{n-3}<\bar{\mu}_{\alpha_1}<2^{n-2}, \\ \bar{\mu}_{\alpha_1}\neq\dfrac{2^{n-1}+1}{3}, \\ \bar{\mu}_{\alpha_1} \bmod 2\neq 0. \end{cases}$$

If we can find $\bar{\mu}_{\alpha_1}$ satisfying the above conditions, then μ_{α_1}, μ_{α_2} and λ can be determined. When $n=4$, there does not exist $\bar{\mu}_{\alpha_1}$ satisfying the above conditions. When $n\geqslant 5$ and $(2^{n-1}+1) \bmod 3\neq 0$, there exist 2^{n-4} binary arrays satisfying the above conditions, that is, $\bar{\mu}_{\alpha_1}=2^{n-3}+1, 2^{n-3}+1+2,\ldots,2^{n-3}+1+(2^{n-4}-1)2$. If $(2^{n-1}+1) \bmod 3=0$, then there exist $2^{n-4}-1$ binary arrays excluding $\bar{\mu}_{\alpha_1}=\frac{2^{n-1}+1}{3}$. Therefore, Lemma 7 holds when $\mu_{\alpha_1}=2^{n-1}+\bar{\mu}_{\alpha_1}$ and $\mu_{\alpha_2}=4\bar{\mu}_{\alpha_1}-1$.

Remark 4. It can be learned from Lemma 7 that we only consider the case $\delta_{2^n}^{\mu_{\alpha_1}}\rightarrow\delta_{2^n}^{\lambda}\rightarrow\delta_{2^n}^{\mu_{\alpha_2}}$ with $\mu_{\alpha_1},\mu_{\alpha_2}\in[\bar{\mathcal{S}}]$ and $\lambda\in[\mathcal{O}_1]$, because the number of states of $T(V,E)$ or $PT(V,E')$ grows exponentially with the increase of nodes. If we consider longer paths such as $\delta_{2^n}^{\mu_{\alpha_1}}\rightarrow\delta_{2^n}^{\lambda}\rightarrow\delta_{2^n}^{\lambda'}\rightarrow\delta_{2^n}^{\mu_{\alpha_2}}$ with $\lambda'\in[\mathcal{O}_1]$, then the number of binary arrays that satisfy the condition that the states in a same array are in the same cyclic attractor, will be more than the case considered in Lemma 7. As a result, the analysis will be more difficult.

In the following, we make a pre-treatment for these binary arrays obtained in Lemma 7. Let Γ' be the set of the first element of all these arrays, that is, $\Gamma'=\{\delta_{2^n}^{2^{n-1}+2^{n-3}+1},\ldots,\delta_{2^n}^{2^{n-1}+2^{n-3}+1+(2^{n-4}-1)2}\}$. If $(2^{n-1}+1) \bmod 3=0$, then let $\hat{\Gamma}=\Gamma'\backslash\{\delta_{2^n}^{2^{n-1}+\frac{2^{n-1}+1}{3}}\}$.

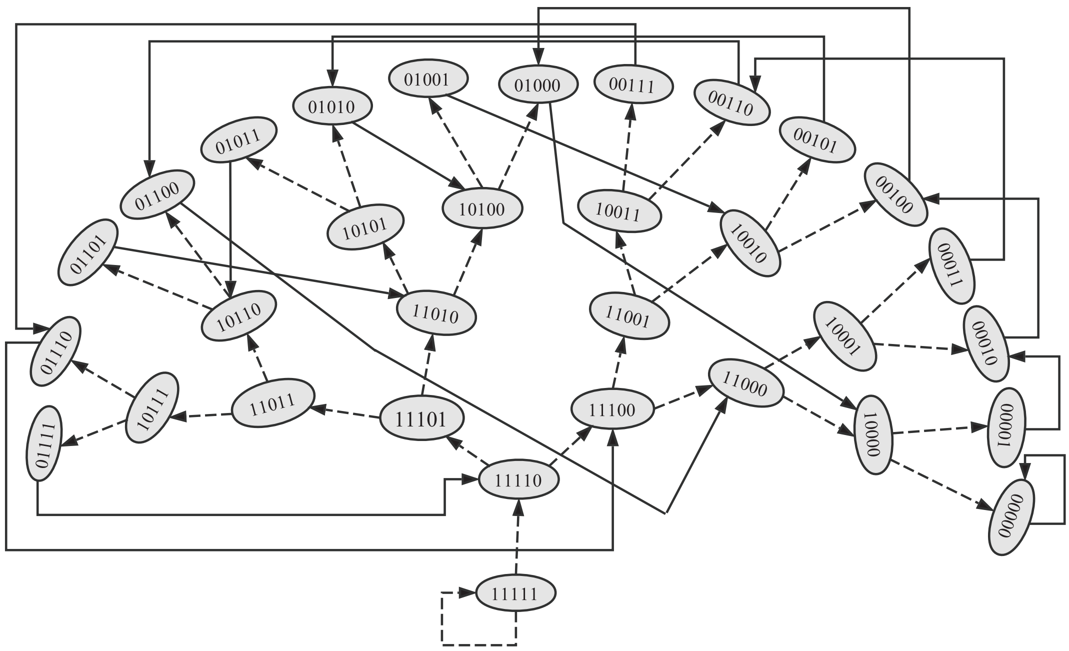

Figure 4 The pseudo-state transition graph of a 5-stage monotonous FSR, where each 5-tuple represents a state $(x_1, x_2, x_3, x_4, x_5)^{\mathrm{T}}$.

Theorem 3. An n-stage ($n \geqslant 5$) reliable FSR can be obtained if M_f in (7) is constructed as follows:

- Let $b_1 = 2$;
- If $(2^{n-1}+1) \bmod 3 \neq 0$, then let $b_{\lceil \frac{\omega}{2} \rceil} = 2$, $\omega \in [\bar{\mathcal{S}}] \backslash [\Gamma']$;
- If $(2^{n-1}+1) \bmod 3 = 0$, then let $b_{\lceil \frac{\omega}{2} \rceil} = 2$, $\omega \in [\bar{\mathcal{S}}] \backslash [\hat{\Gamma}]$.

Proof. It can be observed that $\delta_{2^n}^{2^{n-1}+\cdots+2+1} \in \bar{\mathcal{S}} \backslash \Gamma'$ or $\delta_{2^n}^{2^{n-1}+\cdots+2+1} \in \bar{\mathcal{S}} \backslash \hat{\Gamma}$. Moreover, we have $b_{\lceil \frac{2^{n-1}+\cdots+2+1}{2} \rceil} = b_{2^{n-1}}$. Therefore, if the above two conditions hold, then Lemma 4 must be satisfied and the n-stage monotonous FSR only has one fixed point, i.e., $\delta_{2^n}^{2^n}$.

Assume that $\bar{\mathcal{S}} = \{\delta_{2^n}^{\mu_1}, \delta_{2^n}^{\mu_2}, \ldots, \delta_{2^n}^{\mu_\varphi}\}$. Let $b_{\lceil \frac{\mu_i}{2} \rceil} = 2$, and then all the potential cyclic attractors will be damaged by Lemma 6. Since for any state $\delta_{2^n}^{c_i} \in \Gamma'$ (or $\delta_{2^n}^{c_i} \in \hat{\Gamma}$), we always find another state $\delta_{2^n}^{c_j} \in \bar{\mathcal{S}}$ such that $\delta_{2^n}^{c_i}$ and $\delta_{2^n}^{c_j}$ are in the same cyclic attractor when $(2^{n-1}+1) \bmod 3 \neq 0$ (or $(2^{n-1}+1) \bmod 3 = 0$). The fact implies that either $b_{\lceil \frac{c_i}{2} \rceil} = 2$ or $b_{\lceil \frac{c_j}{2} \rceil} = 2$, so that the possible cyclic attractors containing $\delta_{2^n}^{c_i}$ and $\delta_{2^n}^{c_j}$ will be damaged. Therefore, if M_f defined by (7) satisfies the above two conditions, then the n-stage FSR with structure matrix M_f is monotonous and globally stable.

Remark 5. Wan et al. [2] constructed $\phi(n)2^{2^{n-2}-1}$ n-stage reliable FSRs, where ϕ denotes the Euler's totient function. Compared with [2], while $n \geqslant 5$ and $(2^{n-1}+1) \bmod 3 \neq 0$, $2^{2^{n-2}-1+2^{n-4}}$ n-stage reliable FSRs can be constructed by Theorem 3. If $(2^{n-1}+1) \bmod 3 = 0$, then there are $2^{2^{n-2}-2+2^{n-4}-1}$ n-stage reliable FSRs can be constructed. When $n = 5$, we have $\phi(n)2^{2^{n-2}-1} = 2^{2^{n-2}-1+2^{n-4}}$, while when $n > 5$, $\phi(n)2^{2^{n-2}-1} < 2^{2^{n-2}-1+2^{n-4}}$. Therefore, the number of n-stage reliable FSRs constructed by Theorem 3 is $\frac{2^{2^{n-4}}}{\phi(n)}$ ($n > 5$) times of that obtained by the method in [2].

Example 3. In the following, we will construct 5-stage monotonous and globally stable FSRs by Theorem 3. The pseudo-state transition graph of a 5-stage monotonous FSR is shown in Figure 4, where $\mathcal{S}_1 = \{\delta_{32}^{17} \sim (0\ 1\ 1\ 1\ 1)^{\mathrm{T}}, \delta_{32}^{18} \sim (0\ 1\ 1\ 1\ 0)^{\mathrm{T}}, \delta_{32}^{19} \sim (0\ 1\ 1\ 0\ 1)^{\mathrm{T}}, \delta_{32}^{20} \sim (0\ 1\ 1\ 0\ 0)^{\mathrm{T}}, \delta_{32}^{21} \sim (0\ 1\ 0\ 1\ 1)^{\mathrm{T}}, \delta_{32}^{22} \sim (0\ 1\ 0\ 1\ 0)^{\mathrm{T}}, \delta_{32}^{23} \sim (0\ 1\ 0\ 0\ 1)^{\mathrm{T}}, \delta_{32}^{24} \sim (0\ 1\ 0\ 0\ 0)^{\mathrm{T}}\}$. By Algorithm 1, one has that $F_{17} = \{\delta_{32}^{17}\}$, $F_{18} = \{\delta_{32}^{18}, \delta_{32}^{25} \sim (0\ 0\ 1\ 1\ 1)^{\mathrm{T}}\}$, $F_{19} = \{\delta_{32}^{19}\}$, $F_{20} = \{\delta_{32}^{20}, \delta_{32}^{26} \sim (0\ 0\ 1\ 1\ 0)^{\mathrm{T}}, \delta_{32}^{29} \sim (0\ 0\ 0\ 1\ 1)^{\mathrm{T}}\}$, $F_{21} = \{\delta_{32}^{21}\}$, $F_{22} = \{\delta_{32}^{22}, \delta_{32}^{27} \sim (0\ 0\ 1\ 0\ 1)^{\mathrm{T}}\}$, $F_{23} = \{\delta_{32}^{23}\}$, and $F_{24} = \{\delta_{32}^{24}, \delta_{32}^{28} \sim (0\ 0\ 1\ 0\ 0)^{\mathrm{T}}, \delta_{32}^{30} \sim (0\ 0\ 0\ 1\ 0)^{\mathrm{T}}, \delta_{32}^{31} \sim (0\ 0\ 0\ 0\ 1)^{\mathrm{T}}\}$. Then $\bar{\mathcal{S}} = \{\delta_{32}^{17}, \delta_{32}^{19}, \delta_{32}^{21}, \delta_{32}^{23}, \delta_{32}^{25}, \delta_{32}^{27}, \delta_{32}^{29}, \delta_{32}^{31}\}$. When $n = 5$, we have $(2^{5-1}+1) \bmod 3 \neq 0$, $\Gamma = \{(\delta_{32}^{21}, \delta_{32}^{19}), (\delta_{32}^{23}, \delta_{32}^{27})\}$ and $\Gamma' = \{\delta_{32}^{21}, \delta_{32}^{23}\}$. Therefore, $[\bar{\mathcal{S}}] \backslash [\Gamma'] = \{17, 19, 25, 27, 29, 31\}$. By Theorem 3, let $b_1 = b_9 = b_{10} = b_{13} = b_{14} = b_{15} = b_{16} = 2$, and then we can obtain the pseudo-state transition graph by deleting some edges as shown in Figure 5. From

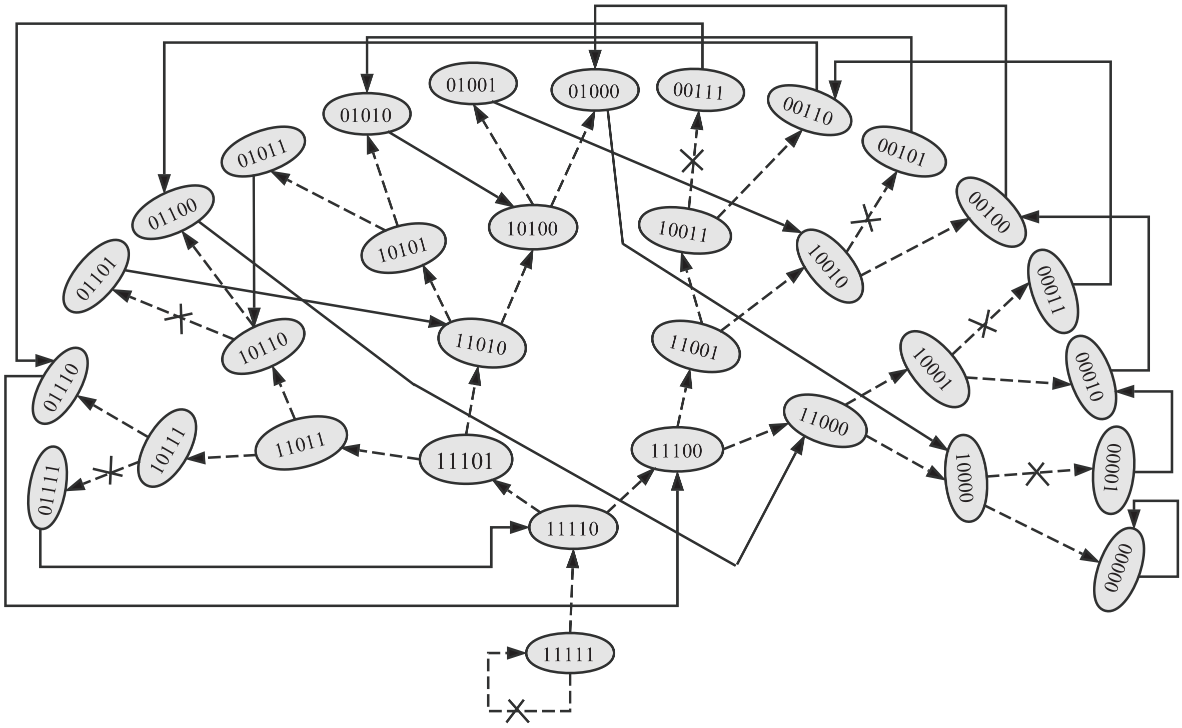

Figure 5 The $PT(V, E')$ of a 5-stage monotonous FSR by deleting some edges based on Theorem 3, where each 5-tuple represents a state $(x_1, x_2, x_3, x_4, x_5)^{\mathrm{T}}$, and the dashed line with a "×" means the path has been deleted.

Figure 5 we can observe that there does not exist any cyclic attractor. Moreover, by Theorem 3, if M_f is in the form of $\delta_2[2\ b_2\ b_3\ b_4\ b_5\ b_6\ b_7\ b_8\ 2\ 2\ b_{11}\ b_{12}\ 2\ 2\ 2\ 2\ 2\ 2\ 2\ 2\ 2\ 2\ 2\ 2\ 2\ 2\ 2\ 2\ 2\ 2\ 2\ 2]$, $b_i \in \mathcal{D}$, $i \in [2, 8] \cup \{11, 12\}$, then FSRs with structure matrix M_f are monotonous and globally stable. Moreover, the total number of 5-stage monotonous and global stability FSRs is 2^9. If we follow the method in [2] to construct the monotonous and globally stable FSRs, then the same number of monotonous and globally stable FSRs can be constructed.

Now, we construct 6-stage monotonous and globally stable FSRs. Note that the $T(V, E')$ and $PT(V, E')$ of a 6-stage monotonous FSR occupy a lot of space, so the graphs are omitted. Then, we have $(2^{6-1} + 1) \bmod 3 = 0$, $\Gamma = \{(\delta_{64}^{41}, \delta_{64}^{35}), (\delta_{64}^{43}, \delta_{64}^{43}), (\delta_{64}^{45}, \delta_{64}^{51}), (\delta_{64}^{47}, \delta_{64}^{59})\}$ and $\hat{\Gamma} = \{\delta_{64}^{41}, \delta_{64}^{45}, \delta_{64}^{47}\}$. Therefore, let $b_{17} = b_{18} = b_{19} = b_{20} = b_{22} = b_{25} = b_{26} = b_{27} = b_{28} = b_{29} = b_{30} = b_{31} = 2$, and 2^{19} 6-stage monotonous and globally stable FSRs can be constructed. If followed by the algorithm in [2], there are 2^{16} 6-stage monotonous and globally stable FSRs in total.

4 Conclusion

In this paper, the FSRs were investigated and considered as BNs for evaluating the corresponding structure matrix and transition matrix by STP. One necessary and sufficient condition was obtained for monotonous FSRs, and the upper bound of the number of cyclic attractors was given for one monotonous FSR. Also, $2^{2^{n-2}-1+2^{n-4}}$ n-stage reliable FSRs were constructed by the proposed method in this paper, and the number of n-stage reliable FSRs was greater than that in Ref. [2]. Finally, some examples have been provided to illustrate the effectiveness of the proposed method.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61973078, 61903339), Natural Science Foundation of Jiangsu Province of China (Grant No. BK20170019), Jiangsu Province Six Talent Peaks Project (Grant No. 2015-ZNDW-002), Fundamental Research Funds for the Central Universities (Grant No. 2242019k1G013), and Postgraduate Research & Practice Innovation Program of Jiangsu Province (Grant No. KYCX19_0111).

References

1 Massey J, Liu R. Application of Lyapunov's direct method to the error-propagation effect in convolutional codes. IEEE Trans Inform Theor, 1964, 10: 248–250
2 Wan Z X, Dai Z D, Liu M L, et al. Nonlinear Feedback Shift Registers (in Chinese). Beijing: Science Press, 1978

3 Ma Z, Qi W F, Tian T. On the decomposition of an NFSR into the cascade connection of an NFSR into an LFSR. J Complexity, 2013, 29: 173–181
4 Zhang J M, Qi W F, Tian T, et al. Further results on the decomposition of an NFSR into the cascade connection of an NFSR into an LFSR. IEEE Trans Inform Theor, 2015, 61: 645–654
5 Kauffman S A. Metabolic stability and epigenesis in randomly constructed genetic nets. J Theor Biol, 1969, 22: 437–467
6 Zhang Y, Liu Y. Nonlinear second-order multi-agent systems subject to antagonistic interactions without velocity constraints. Appl Math Comput, 2020, 364: 124667
7 Li N, Cao J D. Synchronization criteria for multiple memristor-based neural networks with time delay and inertial term. Sci China Tech Sci, 2018, 61: 612–622
8 Cheng D Z, Qi H S, Li Z Q. Analysis and Control of Boolean Networks: A Semi-tensor Product Approach. Berlin: Springer, 2010
9 Cheng D Z, Qi H S. Controllability and observability of Boolean control networks. Automatica, 2009, 45: 1659–1667
10 Liang S, Li H T, Wang S L. Structural controllability of Boolean control networks with an unknown function structure. Sci China Inf Sci, 2020, 63: 219203
11 Hou B Y, Li X, Chen G R. Structural controllability of temporally switching networks. IEEE Trans Circ Syst I, 2016, 63: 1771–1781
12 Zhu S Y, Liu Y, Lou Y J, et al. Stabilization of logical control networks: an event-triggered control approach. Sci China Inf Sci, 2020, 63: 112203
13 Xu M X, Liu Y, Lou J G, et al. Set stabilization of probabilistic Boolean control networks: a sampled-data control approach. IEEE Trans Cybern, 2020, 50: 3816–3823
14 Lin L, Cao J D, Rutkowski L. Robust event-triggered control invariance of probabilistic Boolean control networks. IEEE Trans Neural Netw Learn Syst, 2020, 31: 1060–1065
15 Zhong J, Li B W, Liu Y, et al. Output feedback stabilizer design of Boolean networks based on network structure. Front Inform Technol Electron Eng, 2020, 21: 247–259
16 Liu A X, Li H T. On feedback invariant subspace of Boolean control networks. Sci China Inf Sci, 2020, 63: 229201
17 Zhu Q X, Liu Y, Lu J Q, et al. Observability of Boolean control networks. Sci China Inf Sci, 2018, 61: 092201
18 Liu H C, Liu Y, Li Y Y, et al. Observability of Boolean networks via STP and graph methods. IET Control Theor Appl, 2018, 13: 1031–1037
19 Chen H W, Liang J L, Huang T W, et al. Synchronization of arbitrarily switched Boolean networks. IEEE Trans Neural Netw Learn Syst, 2017, 28: 612–619
20 Zhao J T, Chen Z Q, Liu Z X. Modeling and analysis of colored petri net based on the semi-tensor product of matrices. Sci China Inf Sci, 2018, 61: 010205
21 Li H T, Wang Y Z. Boolean derivative calculation with application to fault detection of combinational circuits via the semi-tensor product method. Automatica, 2012, 48: 688–693
22 Li H T, Zhao G D, Meng M, et al. A survey on applications of semi-tensor product method in engineering. Sci China Inf Sci, 2018, 61: 010202
23 Liu Z B, Wang Y Z, Cheng D Z. Nonsingularity of feedback shift registers. Automatica, 2015, 55: 247–253
24 Zhong J H, Lin D D. Stability of nonlinear feedback shift registers. Sci China Inf Sci, 2016, 59: 012204
25 Li B W, Lu J Q. Boolean-network-based approach for construction of filter generators. Sci China Inf Sci, 2020, 63: 212206
26 Lu J Q, Li M L, Liu Y, et al. Nonsingularity of Grain-like cascade FSRs via semi-tensor product. Sci China Inf Sci, 2018, 61: 010204
27 Dubrova E. Finding matching initial states for equivalent NLFSRs in the Fibonacci and the Galois configurations. IEEE Trans Inform Theor, 2010, 56: 2961–2966
28 Lu J Q, Li M L, Huang T W, et al. The transformation between the Galois NLFSRs and the Fibonacci NLFSRs via semi-tensor product of matrices. Automatica, 2018, 96: 393–397
29 Hu H G, Gong G. Periods on two kinds of nonlinear feedback shift registers with time varying feedback functions. Int J Found Comput Sci, 2011, 22: 1317–1329
30 Zhong J H, Lin D D. On minimum period of nonlinear feedback shift registers in Grain-like structure. IEEE Trans Inform Theor, 2018, 64: 6429–6442
31 Golomb S. Shift Register Sequences. Laguna Hills: Aegean Park Press, 1982
32 Mowle F J. An algorithm for generating stable feedback shift registers of order n. J ACM, 1967, 14: 529–542

Appendix A

In Theorem 2, we proved that for any n-stage monotonous FSR, the total number of cyclic attractors is no more than 2^{n-2}, but we did not prove that there exists a cyclic attractor including $\delta_{2^n}^{\alpha}$ and $\delta_{2^n}^{\frac{\alpha}{2}+2^{n-1}}$ rather than including $\delta_{2^n}^{\alpha}$ and $\delta_{2^n}^{\frac{\alpha}{2}}$ for any even integer $\alpha \in [\mathcal{O}_2]$. In the following, we prove that there is definitely no such cycle $\delta_{2^n}^{\alpha} \rightarrow \delta_{2^n}^{2(\alpha-2^{n-1})} \rightarrow \cdots \rightarrow \delta_{2^n}^{\frac{\alpha}{2}} \rightarrow \delta_{2^n}^{\alpha}$ but there possibly exists the cycle $\delta_{2^n}^{\alpha} \rightarrow \delta_{2^n}^{2(\alpha-2^{n-1})} \rightarrow \cdots \rightarrow \delta_{2^n}^{\frac{\alpha}{2}+2^{n-1}} \rightarrow \delta_{2^n}^{\alpha}$.

Assume that there exists a cyclic attractor with length κ in an n-stage monotonous FSR: $X_1 \rightarrow X_2 \rightarrow \cdots \rightarrow X_\kappa$. Then by Definition 5, we have that $w(X_\kappa) \leqslant w(X_{\kappa-1}) \leqslant \cdots \leqslant w(X_1) \leqslant w(X_\kappa)$. Therefore, $w(X_\kappa) = w(X_{\kappa-1}) = \cdots = w(X_1) = w(X_\kappa)$ [2]. If there exists the cycle $\delta_{2^n}^{\alpha} \rightarrow \delta_{2^n}^{2(\alpha-2^{n-1})} \rightarrow \cdots \rightarrow \delta_{2^n}^{\frac{\alpha}{2}} \rightarrow \delta_{2^n}^{\alpha}$, then $w(X_\alpha) = w(X_{\frac{\alpha}{2}})$, where $X_\alpha = (a_1, a_2, \ldots, a_n)^{\mathrm{T}} \sim \delta_{2^n}^{\alpha}$, $X_{\frac{\alpha}{2}} = (a'_1, a'_2, \ldots, a'_n)^{\mathrm{T}} \sim \delta_{2^n}^{\frac{\alpha}{2}}$, and α satisfies the following condition:

$$\alpha = 2^n - (a_1 2^{n-1} + a_2 2^{n-2} + \cdots + a_n). \tag{A1}$$

Multipling both sides of Eq. (A1) by $\frac{1}{2}$ results in

$$\begin{aligned}\frac{\alpha}{2} &= 2^{n-1} - (a_1 2^{n-2} + a_2 2^{n-3} + \cdots + a_{n-1} + \frac{a_n}{2}) \\ &= 2^n - (2^{n-1} + a_1 2^{n-2} + a_2 2^{n-3} + \cdots + a_{n-1}),\end{aligned} \tag{A2}$$

which implies that $X_{\frac{\alpha}{2}} = (1, a_1, \ldots, a_{n-1})^{\mathrm{T}}$ by Lemma 1, and then we have $a_i = a'_{i+1}$, $i \in [1, n-1]$. It follows from Lemma 6 that α is an even integer, and then we have $a_n = 0$, and $X_\alpha = (a_1, a_2, \ldots, a_{n-1}, 0)^{\mathrm{T}}$. Based on the analysis, we have that $w(X_\alpha) \neq w(X_{\frac{\alpha}{2}})$ and $w(X_\alpha) - w(X_{\frac{\alpha}{2}}) = 1$, which contradicts with $w(X_\alpha) = w(X_{\frac{\alpha}{2}})$. Therefore, there does not exist the cycle $\delta_{2^n}^{\alpha} \to \delta_{2^n}^{2(\alpha-2^{n-1})} \to \cdots \to \delta_{2^n}^{\frac{\alpha}{2}} \to \delta_{2^n}^{\alpha}$.

But for another sequence $\delta_{2^n}^{\alpha}, \delta_{2^n}^{2(\alpha-2^{n-1})}, \ldots, \delta_{2^n}^{\frac{\alpha}{2}+2^{n-1}}, \delta_{2^n}^{\alpha}$, it is possible to form a cycle. The proof is given as follows. Based on Eq. (8) and Lemma 6, the subpaths $\delta_{2^n}^{\alpha} \to \delta_{2^n}^{2(\alpha-2^{n-1})}$ and $\delta_{2^n}^{\frac{\alpha}{2}+2^{n-1}} \to \delta_{2^n}^{\alpha}$ are determined, but the rest path $\delta_{2^n}^{2(\alpha-2^{n-1})} \to \cdots \to \delta_{2^n}^{\frac{\alpha}{2}+2^{n-1}}$ with $\delta_{2^n}^{2(\alpha-2^{n-1})} \in \mathcal{O}_1$ is indeterminate, and depends on $b_i, i \in [1, 2^{n-1}]$. Therefore, we only consider these two determined subpaths. That is, if $w(X_\alpha) = w(X_{2(\alpha-2^{n-1})})$ and $w(X_\alpha) = w(X_{\frac{\alpha}{2}+2^{n-1}})$, then the cycle is possible; otherwise, it must be impossible.

By doubling both sides of Eq. (A1), one has that

$$2\alpha = 2^{n+1} - (a_1 2^n + a_2 2^{n-1} + \cdots + 2a_n).$$

Then subtracting both sides of the above equation by 2^{n-1} results in

$$2(\alpha - 2^{n-1}) = 2^n - (a_1 2^n + a_2 2^{n-1} + \cdots + 2a_n). \tag{A3}$$

Since $\alpha \in [\mathcal{S}_1]$, which means $a_1 = 0$, Eq. (A3) can be rewritten as

$$2(\alpha - 2^{n-1}) = 2^n - (a_2 2^{n-1} + \cdots + 2a_n + 0), \tag{A4}$$

which implies that $X_{2(\alpha-2^{n-1})} = (a_2, a_3, \ldots, a_n, 0)^{\mathrm{T}}$. Therefore, $w(X_\alpha) = w(X_{2(\alpha-2^{n-1})})$.

On the other hand, adding both sides of Eq. (A1) by 2^{n-1} results in

$$\begin{aligned}\frac{\alpha}{2} + 2^{n-1} =& 2^n - (a_1 2^{n-2} + a_2 2^{n-3} + \cdots + a_{n-1}) \\ =& 2^n - (0 \cdot 2^{n-1} + a_1 2^{n-2} + a_2 2^{n-3} + \cdots + a_{n-1}),\end{aligned} \tag{A5}$$

which implies that $X_{\frac{\alpha}{2}+2^{n-1}} = (0, a_1, a_2, \ldots, a_{n-1})^{\mathrm{T}}$, and $w(X_\alpha) = w(X_{\frac{\alpha}{2}+2^{n-1}})$. Therefore, $w(X_\alpha) = w(X_{\frac{\alpha}{2}+2^{n-1}}) = w(X_{2(\alpha-2^{n-1})})$.

Based on the above analysis, we can conclude that for any even integer $\alpha \in [\mathcal{O}_2]$, the cycle $\delta_{2^n}^{\alpha} \to \delta_{2^n}^{2(\alpha-2^{n-1})} \to \cdots \to \delta_{2^n}^{\frac{\alpha}{2}} \to \delta_{2^n}^{\alpha}$ cannot exist but the cycle $\delta_{2^n}^{\alpha} \to \delta_{2^n}^{2(\alpha-2^{n-1})} \to \cdots \to \delta_{2^n}^{\frac{\alpha}{2}+2^{n-1}} \to \delta_{2^n}^{\alpha}$ may exist. Therefore, for any n-stage monotonous FSR, the total number of cyclic attractors is no more than 2^{n-2}. Additionally, the above analysis also proved that it is impossible to have a cyclic attractor including $(0\ 1\ 1\ 0)^{\mathrm{T}}$ and $(1\ 0\ 1\ 1)^{\mathrm{T}}$ in Remark 3.