SCIENCE CHINA
Information Sciences

• **Supplementary File** •

Decomposition of Nonlinear Feedback Shift Registers Based on Boolean Networks

Jianghua ZHONG* & Dongdai LIN

State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093*, China*

Appendix A Nonlinear Feedback Shift Registers

Figure A1 describes an r-stage Fibonacci nonlinear feedback shift regisger (NFSR). Here small squares represent binary storage devices, also called *bits*, whose contents are labelled as $Y_1, Y_2, \ldots, Y_r$ from left to right. They together form the state of the NFSR, denoted by $\boldsymbol{Y} = [Y_1\ Y_2 \cdots Y_r]^T$. The nonlinear Boolean function h in the rectangle is called the *feedback function* of the NFSR. If the feedback function h is degenerated to a linear Boolean function, then the NFSR is reduced to a linear feedback shift register (LFSR). The content Y_1 is the output of the NFSR. The NFSR is nonsingular if and only if its feedback function h is nonsingular, i.e., $h(Y_1, Y_2, \ldots, Y_r) = Y_1 \oplus \tilde{h}(Y_2, \ldots, Y_r)$ [1]. The function $h_c(Y_1, Y_2, \ldots, Y_{r+1}) = Y_{r+1} \oplus h(Y_1, Y_2, \ldots Y_r)$ is called the *characteristic function* of the NFSR. The NFSR can be described by the nonlinear system:

$$\begin{cases} Y_1(t+1) = Y_2(t), \\ \quad \vdots \\ Y_{r-1}(t+1) = Y_r(t), \\ Y_r(t+1) = h(Y_1(t), Y_2(t), \ldots, Y_r(t)). \end{cases} \tag{A1}$$

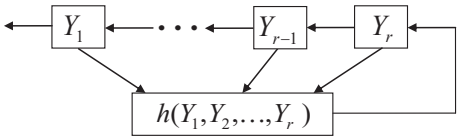

Figure A1 An r-stage Fibonacci NFSR.

A cascade connection of an m-stage NFSR1 into an n-stage NFSR2, is a particular Galois NRSR, in which NFSR1 is a Fibonacci NFSR, and NFSR2 is an NFSR with a single input, and the input of NFSR2 is just the output of NFSR1. If the input of NFSR2 holds constantly at zero, then NFSR2 is reduced to a Fibonacci NFSR. Let g_c and f_c be characteristic functions of NFSR1 and NFSR2, respectively. The cascade connection of NFSR1 into NFSR2 is equivalent to an $(m+n)$-stage Fibonacci NFSR whose characteristic function is [2]:

$$h_c(Y_1, \ldots, Y_{m+n+1}) = g_c * f_c(Y_1, \ldots, Y_{m+n+1}) = g_c(f_c(Y_1, \ldots Y_{n+1}), f_c(Y_2, \ldots Y_{n+2}), f_c(Y_{m+1}, \ldots Y_{n+m+1})).$$

Clearly, one way to solve the decomposition of a Fibonacci NFSR is to factorize its characteristic function in the sense of $*$-product decomposition, like that used in [3, 4].

The *state diagram* of an n-stage NFSR is a directed graph consisting of 2^n nodes and 2^n edges, in which each node represents a state of the NFSR, and each edge represents a transition between two states. An edge from state $\boldsymbol{X}$ to state $\boldsymbol{Y}$ means that the state $\boldsymbol{X}$ is shifted to the state $\boldsymbol{Y}$. $\boldsymbol{X}$ is called a *predecessor* of $\boldsymbol{Y}$, and $\boldsymbol{Y}$ is called the *successor* of $\boldsymbol{X}$. The state with more than one predecessors is called a *branch state*, while the state without predecessors is called a *starting state*. A sequence of p distinct states, $\boldsymbol{X}_1, \boldsymbol{X}_2, \ldots, \boldsymbol{X}_p$, is called a *cycle of length* p if $\boldsymbol{X}_1$ is the successor of $\boldsymbol{X}_p$, and $\boldsymbol{X}_{i+1}$ is a successor of $\boldsymbol{X}_i$ for any $i \in \{1, 2, \ldots, p-1\}$. Similarly, a sequence of p distinct states, $\boldsymbol{X}_1, \boldsymbol{X}_2, \ldots, \boldsymbol{X}_p$, is called a *transient of length* p, if the following conditions are satisfied: 1) none of them lies on a cycle; 2) $\boldsymbol{X}_1$ is a starting point; 3) $\boldsymbol{X}_{i+1}$ is a successor of $\boldsymbol{X}_i$ for any $i \in \{1, 2, \ldots, p-1\}$; 4) the successor of $\boldsymbol{X}_p$ lies on a cycle.

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

Appendix B Proofs of the Theorems

All proofs in this appendix are based on an algebraic framework of Boolean networks (BNs), developed by Cheng et al. via the semi-tensor product [5]. Before we provide detailed proofs, we first review some related concepts and results.

A BN with n nodes and m inputs can be described by the following nonlinear system:

$$\boldsymbol{X}(t+1)=\boldsymbol{g}_{\mathrm{u}}(\boldsymbol{U}(t),\boldsymbol{X}(t)),\ t\in\mathbb{N}, \tag{B1}$$

where $\boldsymbol{X}=[X_1\ \ X_2\ \ \cdots\ \ X_n]^T\in\mathbb{F}_2^n$ is the state, $\boldsymbol{U}=[U_1\ \ U_2\ \ \cdots\ \ U_m]^T\in\mathbb{F}_2^m$ is the input, and the vectorial function $\boldsymbol{g}_{\mathrm{u}}=[g_{\mathrm{u}1}\ \ g_{\mathrm{u}2}\ \ \ldots\ \ g_{\mathrm{u}n}]^T$ is the state transition function.

Definition 1 ([5]). Let $\boldsymbol{A}$ and $\boldsymbol{B}$ be matrices of dimensions $n\times m$ and $p\times q$, respectively, and let α be the least common multiple of m and p. The *(left) semi-tensor product* of $\boldsymbol{A}$ and $\boldsymbol{B}$ is defined as an $\frac{n\alpha}{m}\times\frac{q\alpha}{p}$ matrix, given by

$$\boldsymbol{A}\ltimes\boldsymbol{B}=(\boldsymbol{A}\otimes\boldsymbol{I}_{\frac{\alpha}{m}})(\boldsymbol{B}\otimes\boldsymbol{I}_{\frac{\alpha}{p}}). \tag{B2}$$

where $\otimes$ represents the Kronecker Product.

Definition 2 ([6]). Let $\boldsymbol{A}=(a_{ij})$ and $\boldsymbol{B}$ be matrices of dimensions $n\times m$ and $p\times q$, respectively. The *Kronecker product* of $\boldsymbol{A}$ and $\boldsymbol{B}$, is defined as an $np\times mq$ matrix, given by

$$\boldsymbol{A}\otimes\boldsymbol{B}=\begin{bmatrix}a_{11}\boldsymbol{B} & a_{12}\boldsymbol{B} & \cdots & a_{1m}\boldsymbol{B}\\ a_{21}\boldsymbol{B} & a_{22}\boldsymbol{B} & \cdots & a_{2m}\boldsymbol{B}\\ \vdots & \vdots & & \vdots\\ a_{n1}\boldsymbol{B} & a_{n2}\boldsymbol{B} & \cdots & a_{nm}\boldsymbol{B}\end{bmatrix}. \tag{B3}$$

Lemma 1 ([5]). Let $\boldsymbol{x}=[X_1\ \ X_1\oplus 1]^T\ltimes[X_2\ \ X_2\oplus 1]^T\ltimes\cdots\ltimes[X_n\ \ X_n\oplus 1]^T$ with each $X_i\in\mathbb{F}_2$. Then $\boldsymbol{x}\in\Delta_{2^n}$. Moreover, the state $\boldsymbol{X}=[X_1\ \ X_2\ \cdots\ X_n]^T\in\mathbb{F}_2^n$ and the state $\boldsymbol{x}=\delta_{2^n}^j\in\Delta_{2^n}$ with $j=2^n-(2^{n-1}X_1+2^{n-2}X_2+\cdots+X_n)$ are one-to-one correspondent.

Lemma 2 ([5]). The nonlinear system (B1) describing a BN with inputs can be equivalently expressed as a linear system

$$\boldsymbol{x}(t+1)=\boldsymbol{L}_{\boldsymbol{u}}\ltimes\boldsymbol{u}(t)\ltimes\boldsymbol{x}(t),\ t\in\mathbb{N}, \tag{B4}$$

where $\boldsymbol{x}\in\Delta_{2^n}$ is the state, $\boldsymbol{u}\in\Delta_{2^m}$ is the input, and $\boldsymbol{L}_{\boldsymbol{u}}\in\mathcal{L}_{2^n\times 2^{n+m}}$ is the state transition matrix, satisfying

$$\mathrm{Col}_j(\boldsymbol{L}_{\boldsymbol{u}})=\mathrm{Col}_j(\boldsymbol{G}_{\mathrm{u}1})\otimes\cdots\otimes\mathrm{Col}_j(\boldsymbol{G}_{\mathrm{u}n}) \tag{B5}$$

for all $j=1,2,\ldots,2^{n+m}$, with the structure matrix $\boldsymbol{G}_{\mathrm{u}i}$ of the i-th component $g_{\mathrm{u}i}$ of the vectorial function $\boldsymbol{g}_{\mathrm{u}}$ in (B1) for any $i\in\{1,2,\ldots,n\}$.

In (B1), if $U(t)\equiv 0$ for any $t\in\mathbb{N}$, which means the BN without input, then its linear system representation (B4) is reduced to $\boldsymbol{x}(t+1)=\boldsymbol{L}\boldsymbol{x}(t)$ with state transition matrix $\boldsymbol{L}\in\mathcal{L}_{2^n\times 2^n}$ [5].

Definition 3 ([5]). An $mn\times mn$ swap matrix $\boldsymbol{W}_{[m,n]}$ is defined in the following way: label its columns as $(11,12,\ldots,1n,\ldots,m1,m2,\ldots,mn)$ and its rows as $(11,21,\ldots,m1,\ldots,1n,2n,\ldots,mn)$, and assign the entry $w_{[(U,V),(u,v)]}$ at the position $[(U,V),(u,v)]$ as

$$w_{[(U,V),(u,v)]}=\begin{cases}1, & U=u \text{ and } V=v,\\ 0, & \text{otherwise.}\end{cases}$$

Lemma 3 ([5]). The semi-tensor product has the following properties.

1) Let $\boldsymbol{A}$ and $\boldsymbol{B}$ be, respectively, $m\times n$ and $p\times q$ matrices, and let $\boldsymbol{X}$ and $\boldsymbol{Y}$ be vectors of dimensions n and q, respectively. Then $(\boldsymbol{A}\boldsymbol{X})\ltimes(\boldsymbol{B}\boldsymbol{Y})=(\boldsymbol{A}\otimes\boldsymbol{B})(\boldsymbol{X}\ltimes\boldsymbol{Y})$.
2) Let $\boldsymbol{A}$ be an $m\times np$ matrix, and $\boldsymbol{B}$ be a $p\times q$ matrix. Then $\boldsymbol{A}\ltimes\boldsymbol{B}=\boldsymbol{A}(\boldsymbol{B}\otimes\boldsymbol{I}_n)$.
3) If $x\in\Delta_2$, then $x\ltimes x=\boldsymbol{M}x$ with the power-reducing matrix $\boldsymbol{M}=\delta_4[1\ 4]$.
4) Let $\boldsymbol{X}$ and $\boldsymbol{Y}$ be two column vectors of dimensions n and m, respectively. Then $\boldsymbol{X}\ltimes\boldsymbol{Y}=\boldsymbol{W}_{[m,n]}\ltimes\boldsymbol{Y}\ltimes\boldsymbol{X}=\boldsymbol{X}\otimes\boldsymbol{Y}$.
5) $\boldsymbol{W}_{[m,n]}=\boldsymbol{W}_{[n,m]}^{-1}=[\delta_n^1\ltimes\delta_m^1\ \cdots\ \delta_n^n\ltimes\delta_m^1\ \cdots\ \delta_n^1\ltimes\delta_m^m\ \cdots\ \delta_n^n\ltimes\delta_m^m]$.

Appendix B.1 Proof of Theorem 1

For a cascade connection of an m-stage NFSR1 into an n-stage NFSR2, Theorem 1 gives a linear system representation of NFSR2.

Theorem 1. NFSR2 can be equivalently expressed as a linear system

$$\boldsymbol{x}(t+1)=\boldsymbol{L}_{\mathrm{u}}\ltimes u_1(t)\ltimes\boldsymbol{x}(t),\ t\in\mathbb{N}, \tag{B6}$$

with state $\boldsymbol{x}\in\Delta_{2^n}$, input $u_1\in\Delta_2$, and state transition matrix $\boldsymbol{L}_{\mathrm{u}}\in\mathcal{L}_{2^n\times 2^{n+1}}$ satisfying

$$\mathrm{Col}_j(\boldsymbol{L}_{\mathrm{u}})=\delta_{2^n}^{2[(j-1)\bmod 2^{n-1}+1]-s_j} \tag{B7}$$

for all $j=1,2,\ldots,2^{n+1}$, where $[s_1,s_2,\ldots,s_{2^{n+1}}]$ is the truth table of the function $f_n(U_1,X_1,\ldots,X_n)=U_1\oplus f(X_1,X_2,\ldots,X_n)$, arranged in the reverse alphabet order, with NFSR2's input U_1 and feedback function f.

Proof. NFSR2 can be represented by a nonlinear system

$$\begin{cases} X_1(t+1) = X_2(t), \\ \quad \vdots \\ X_{n-1}(t+1) = X_n(t), \\ X_n(t+1) = U_1(t) \oplus f(X_1(t), X_2(t), \ldots, X_n(t)). \end{cases}$$

Let $f_i(U_1, \boldsymbol{X}) = X_{i+1}$ and let $\boldsymbol{F}_i$ be the structure matrix of f_i for any $i \in \{1, 2, \ldots, n-1\}$. Then, according to the definition of structure matrix, we can easily obtain that

$$\begin{aligned} \boldsymbol{F}_1 &= [\underbrace{\tilde{\boldsymbol{F}}_1 \cdots \tilde{\boldsymbol{F}}_1}_{2^2}], \text{where } \tilde{\boldsymbol{F}}_1 = \delta_2[\underbrace{1 \cdots 1}_{2^{n-2}} \ \underbrace{2 \cdots 2}_{2^{n-2}}], \\ \boldsymbol{F}_2 &= [\underbrace{\tilde{\boldsymbol{F}}_2 \cdots \tilde{\boldsymbol{F}}_2}_{2^3}], \text{where } \tilde{\boldsymbol{F}}_2 = \delta_2[\underbrace{1 \cdots 1}_{2^{n-3}} \ \underbrace{2 \cdots 2}_{2^{n-3}}], \\ &\vdots \\ \boldsymbol{F}_{n-1} &= [\underbrace{\tilde{\boldsymbol{F}}_{n-1} \cdots \tilde{\boldsymbol{F}}_{n-1}}_{2^n}], \text{where } \tilde{\boldsymbol{F}}_{n-1} = \delta_2[1\ 2]. \end{aligned}$$

Suppose the structure matrix of f_n to be $\boldsymbol{F}_n$. From Lemma 2, for all $j = 1, 2, \ldots, 2^{n+1}$, we have

$$\mathrm{Col}_j(\boldsymbol{L}_{\mathrm{u}}) = \mathrm{Col}_j(\boldsymbol{F}_1) \otimes \cdots \otimes \mathrm{Col}_j(\boldsymbol{F}_{n-1}) \otimes \mathrm{Col}_j(\boldsymbol{F}_n).$$

Let $\mathrm{Col}_j(\boldsymbol{B}) = \mathrm{Col}_j(\boldsymbol{F}_1) \otimes \cdots \otimes \mathrm{Col}_j(\boldsymbol{F}_{n-1})$. According to the structure feature of $\boldsymbol{F}_i$s for all $i = 1, 2, \ldots, n-1$, we can easily see that

$$\boldsymbol{B} = [\tilde{\boldsymbol{B}} \ \tilde{\boldsymbol{B}} \ \tilde{\boldsymbol{B}} \ \tilde{\boldsymbol{B}}], \tag{B8}$$

where the $2^{n-1} \times 2^{n-1}$ matrix $\tilde{\boldsymbol{B}}$ is to be determined. From Lemma 3, $\boldsymbol{X} \otimes \boldsymbol{Y} = \boldsymbol{X} \ltimes \boldsymbol{Y}$ for any two column vectors $\boldsymbol{X}$ and $\boldsymbol{Y}$. Thus, according to Lemma 1, we can easily compute that $\mathrm{Col}_j(\tilde{\boldsymbol{B}}) = \delta^j_{2^{n-1}}$ for all $j = 1, 2, \ldots, 2^{n-1}$. Since each $\mathrm{Col}_j(\boldsymbol{F}_n) = [s_j \ \ s_j \oplus 1]^T = \delta_2^{2-s_j}$, we have $\mathrm{Col}_j(\boldsymbol{L}_{\mathrm{u}}) = \mathrm{Col}_j(\tilde{\boldsymbol{B}}) \otimes \mathrm{Col}_j(\boldsymbol{F}_n) = \delta_{2^n}^{2j-s_j}$ for all $j = 1, 2, \ldots, 2^{n-1}$. Together taking Eq. (B8) into consideration, we can conclude that the result holds. □

Appendix B.2 Proof of Theorem 2

For a cascade connection of an m-stage NFSR1 into an n-stage NFSR2, Theorem 2 reveals the relation of its state transition matrix with those of both NFSRs. Before giving the detail proof of Theorem 2, we first review/give some related results.

NFSR1 can be represented by a linear system [7]:

$$\boldsymbol{u}(t+1) = \boldsymbol{L}\boldsymbol{u}(t), \ t \in \mathbb{N}, \tag{B9}$$

where $\boldsymbol{L} \in \mathcal{L}_{2^m \times 2^m}$ is the state transition matrix, satisfying

$$\begin{cases} \mathrm{Col}_{2^{m-1}+j}(\boldsymbol{L}) = \delta_{2^m}^{2j-q_{2^{m-1}+j}}, \\ \mathrm{Col}_j(\boldsymbol{L}) = \delta_{2^m}^{2j-q_j}, \ j = 1, 2, \ldots, 2^{m-1}, \end{cases} \tag{B10}$$

with the truth table $[q_1, q_2, \ldots, q_{2^m}]$ of the feedback function of NFSR1, arranged in the reverse alphabet order. $\boldsymbol{L}$ is nonsingular if and only if the feedback function of NFSR1 is nonsingular [7]. It is notable to point out that Eq. (B10) can be unified as:

$$\mathrm{Col}_j(\boldsymbol{L}) = \delta_{2^m}^{2[(j-1) \bmod 2^{m-1}+1]-q_j}, \ j = 1, 2, \ldots, 2^m. \tag{B11}$$

Similarly, NFSR2 with input holding constantly at zero can be represented by

$$\boldsymbol{x}(t+1) = \boldsymbol{L}_0\boldsymbol{x}(t), \ t \in \mathbb{N}, \tag{B12}$$

with $\boldsymbol{L}_0 \in \mathcal{L}_{2^n \times 2^n}$ satisfying

$$\mathrm{Col}_j(\boldsymbol{L}_0) = \delta_{2^n}^{2[(j-1) \bmod 2^{n-1}+1]-p_j}, \ j = 1, 2, \ldots, 2^n, \tag{B13}$$

and the truth table $[p_1, p_2, \ldots, p_{2^n}]$ of the feedback function of NFSR2, arranged in the reverse alphabet order. $\boldsymbol{L}_0$ is nonsingular if and only if the feedback function of NFSR2 is nonsingular.

Proposition 1. A cascade connection of an m-stage NFSR1 into an n-stage NFSR2 can be represented by a linear system

$$\bar{\boldsymbol{z}}(t+1) = \bar{\boldsymbol{L}}_c\bar{\boldsymbol{z}}(t), \tag{B14}$$

where $\bar{\boldsymbol{z}} \in \Delta_{2^{m+n}}$ is the state, and $\bar{\boldsymbol{L}}_c \in \mathcal{L}_{2^{m+n} \times 2^{m+n}}$ is the state transition matrix, satisfying

$$\bar{\boldsymbol{L}}_c = (\boldsymbol{L} \otimes \boldsymbol{L}_{\mathrm{u}})(\boldsymbol{A} \otimes \boldsymbol{I}_{2^n}) \tag{B15}$$

with state transition matrices $\boldsymbol{L}$ in (B9) of NFSR1 and $\boldsymbol{L}_{\mathrm{u}}$ in (B6) of NFSR2, and a $2^{m+1} \times 2^m$ matrix

$$\boldsymbol{A} = \boldsymbol{W}_{[2,2^m]}(\boldsymbol{M} \otimes \boldsymbol{I}_{2^{m-1}}), \tag{B16}$$

and a swap matrix $\boldsymbol{W}_{[2,2^m]}$, and the power-reducing matrix $\boldsymbol{M} = \delta_4[1 \ \ 4]$.

Proof. Note that NFSR1 and NFSR2 can be represented by the linear systems (B9) and (B6), respectively. Multiplying both equations in the sense of semi-tensor product, we have

$$\begin{aligned}&\boldsymbol{u}(t+1)\ltimes\boldsymbol{x}(t+1)=[\boldsymbol{L}\boldsymbol{u}(t)]\ltimes\{\boldsymbol{L}_{\rm u}[u_1(t)\ltimes\boldsymbol{x}(t)]\}=(\boldsymbol{L}\otimes\boldsymbol{L}_{\rm u})[\boldsymbol{u}(t)\ltimes u_1(t)\ltimes\boldsymbol{x}(t)]\\&=(\boldsymbol{L}\otimes\boldsymbol{L}_{\rm u})[\boldsymbol{W}_{[2,2^m]}\ltimes u_1(t)\ltimes\boldsymbol{u}(t)\ltimes\boldsymbol{x}(t)]=(\boldsymbol{L}\otimes\boldsymbol{L}_{\rm u})[\boldsymbol{W}_{[2,2^m]}\ltimes\boldsymbol{M}\ltimes\boldsymbol{u}(t)\ltimes\boldsymbol{x}(t)]\\&=(\boldsymbol{L}\otimes\boldsymbol{L}_{\rm u})\left\{[\boldsymbol{W}_{[2,2^m]}(\boldsymbol{M}\otimes\boldsymbol{I}_{2^{m-1}})]\ltimes[\boldsymbol{u}(t)\ltimes\boldsymbol{x}(t)]\right\}=(\boldsymbol{L}\otimes\boldsymbol{L}_{\rm u})(\boldsymbol{A}\otimes\boldsymbol{I}_{2^n})[\boldsymbol{u}(t)\ltimes\boldsymbol{x}(t)].\end{aligned}$$

In the above inference, the first equation uses the associative law of the semi-tensor product, the second applies Property 1 of Lemma 3, the third utilizes its Property 4, and the fourth uses its Property 3, while the fifth and sixth apply its Property 2. Set $\bar{\boldsymbol{z}}=\boldsymbol{u}\ltimes\boldsymbol{x}$. Then the result follows. □

Remark 1. In Proposition 1, the state $\bar{\boldsymbol{z}}=\boldsymbol{u}\ltimes\boldsymbol{x}\in\Delta_{2^{m+n}}$ uniquely corresponds to the state $\bar{\boldsymbol{Z}}=[\boldsymbol{U}^T\ \boldsymbol{X}^T]^T\in\mathbb{F}_2^{m+n}$. If we set $\boldsymbol{z}=\boldsymbol{x}\ltimes\boldsymbol{u}$ that uniquely corresponds to $\boldsymbol{Z}=[\boldsymbol{X}^T\ \boldsymbol{U}^T]^T$, then from Property 4 of Lemma 3, the system (B14) becomes $\boldsymbol{z}(t+1)=\boldsymbol{L}_c\boldsymbol{z}(t)$ with $\boldsymbol{L}_c=\boldsymbol{W}_{[2^m,2^n]}\bar{\boldsymbol{L}}_c\boldsymbol{W}_{[2^n,2^m]}$. As $\boldsymbol{W}_{[2^n,2^m]}=\boldsymbol{W}_{[2^m,2^n]}^{-1}$, $\boldsymbol{L}_c$ is similar to $\bar{\boldsymbol{L}}_c$. Note that, either $\boldsymbol{Z}=[\boldsymbol{X}^T\ \boldsymbol{U}^T]^T$ or $\bar{\boldsymbol{Z}}=[\boldsymbol{U}^T\ \boldsymbol{X}^T]^T$ can be viewed as the state of the cascade connection of NFSR1 into NFSR2. Hence, $\boldsymbol{L}_c$ is also a state transition matrix of the cascade connection.

In the following, we aim to further reveal the relation of the columns of the state transition matrix of a cascade connection of two NFSRs with those of the state transition matrices of both NFSRs. To achieve this goal, we first give a lemma.

Lemma 4. The matrix $\boldsymbol{A}$ in (B16) satisfies

$$\begin{cases}\mathrm{Col}_j(\boldsymbol{A})=\delta_{2^{m+1}}^{2j-1}\\ \mathrm{Col}_{2^{m-1}+j}(\boldsymbol{A})=\delta_{2^{m+1}}^{2^m+2j},\ j=1,2,\ldots,2^{m-1}.\end{cases}\tag{B17}$$

Proof. The matrix $\boldsymbol{A}$ is related to a swap matrix. First, we prove the swap matrix $\boldsymbol{W}_{[m,n]}$ satisfies

$$\mathrm{Col}_j(\boldsymbol{W}_{[m,n]})=\delta_{mn}^{[(j-1)\bmod n]m+\lceil\frac{j}{n}\rceil},\ j=1,2,\ldots,mn.$$

Partition $\boldsymbol{W}_{[m,n]}$ as $\boldsymbol{W}_{[m,n]}=[\boldsymbol{W}_1\ \ \boldsymbol{W}_2\ \cdots\ \boldsymbol{W}_m]$ with each $\boldsymbol{W}_i\in\mathcal{L}_{mn\times n}$. According to Property 5 of Lemma 3, we have $\boldsymbol{W}_i=[\delta_n^1\ltimes\delta_m^i\ \cdots\ \delta_n^n\ltimes\delta_m^i]$ for all $i=1,2,\ldots,m$. Clearly, the j-th column of $\boldsymbol{W}_{[m,n]}$ is the $[(j-1)\bmod n+1]$-th column of $\boldsymbol{W}_{\lceil\frac{j}{n}\rceil}$ for any $j\in\{1,2,\ldots,mn\}$. Therefore, $\mathrm{Col}_j(\boldsymbol{W}_{[m,n]})=\delta_n^{(j-1)\bmod n+1}\ltimes\delta_m^{\lceil\frac{j}{n}\rceil}=\delta_{mn}^{[(j-1)\bmod n]m+\lceil\frac{j}{n}\rceil}$ for all $j=1,2,\ldots,mn$.

Next, we prove Eq. (B17). Clearly,

$$\boldsymbol{A}=\boldsymbol{W}_{[2,2^m]}(\delta_4[1\ \ 4]\otimes\boldsymbol{I}_{2^{m-1}})=\boldsymbol{W}_{[2,2^m]}\delta_{2^{m+1}}[1\ \ 2\ \cdots\ 2^{m-1}\ \ \ 3\cdot2^{m-1}+1\ \ \ 3\cdot2^{m-1}+2\ \cdots\ 2^{m+1}].$$

Hence, for all $j=1,2,\ldots2^{m-1}$, we have $\mathrm{Col}_j(\boldsymbol{A})=\mathrm{Col}_j(\boldsymbol{W}_{[2,2^m]})=\delta_{2^{m+1}}^{2j-1}$, and $\mathrm{Col}_{2^{m-1}+j}(\boldsymbol{A})=\mathrm{Col}_{3\cdot2^{m-1}+j}(\boldsymbol{W}_{[2,2^m]})=\delta_{2^{m+1}}^{2^m+2j}$. □

Proposition 2. Let the state transition matrices of NFSR1 and NFSR2 be $\boldsymbol{L}=\delta_{2^m}[\eta_1\ \ \eta_2\ \ \ldots\ \ \eta_{2^m}]$ and $\boldsymbol{L}_{\rm u}=\delta_{2^n}[\zeta_1\ \ \zeta_2\ \ \ldots\ \ \zeta_{2^{n+1}}]$, respectively. Then the state transition matrix of the cascade connection of NFSR1 into NFSR2, $\bar{\boldsymbol{L}}_c$ in (B14), can be expressed as

$$\bar{\boldsymbol{L}}_c=[\bar{\boldsymbol{L}}_{c1}\ \ \bar{\boldsymbol{L}}_{c2}\ \ \ldots\ \ \bar{\boldsymbol{L}}_{c2^m}]\text{ with}$$

$$\begin{cases}\bar{\boldsymbol{L}}_{c(2^{m-1}+i)}=\delta_{2^{m+n}}[(\eta_{2^{m-1}+i}-1)2^n+\zeta_{2^n+1}\ \ (\eta_{2^{m-1}+i}-1)2^n+\zeta_{2^n+2}\ \ldots\ (\eta_{2^{m-1}+i}-1)2^n+\zeta_{2^{n+1}}],\\ \bar{\boldsymbol{L}}_{ci}=\delta_{2^{m+n}}[(\eta_i-1)2^n+\zeta_1\ \ (\eta_i-1)2^n+\zeta_2\ \ldots\ (\eta_i-1)2^n+\zeta_{2^n}],i=1,2,\ldots,2^{m-1}.\end{cases}$$

Proof. Note that $\bar{\boldsymbol{L}}_c=(\boldsymbol{L}\otimes\boldsymbol{L}_{\rm u})(\boldsymbol{A}\otimes\boldsymbol{I}_{2^n})$ with $\boldsymbol{A}$ in (B16). Then, from Lemma 4, for all $i=1,2,\ldots,2^{m-1}$, we have

$$\begin{aligned}&\mathrm{Col}_i(\boldsymbol{A})\otimes\boldsymbol{I}_{2^n}=\delta_{2^{m+n+1}}[(i-1)2^{n+1}+1\ \ (i-1)2^{n+1}+2\ \cdots\ (i-1)2^{n+1}+2^n],\text{and}\\&\mathrm{Col}_{2^{m-1}+i}(\boldsymbol{A})\otimes\boldsymbol{I}_{2^n}=\delta_{2^{m+n+1}}[(2^m+2i-1)2^n+1\ \ \ (2^m+2i-1)2^n+2\ \ \cdots\ \ (2^m+2i)2^n].\end{aligned}$$

Let $\boldsymbol{L}\otimes\boldsymbol{L}_u=[\boldsymbol{L}_1\ \ \boldsymbol{L}_2\ \cdots\ \boldsymbol{L}_{2^{m+1}}]$ with $\boldsymbol{L}_i\in\mathcal{L}_{2^{m+n}\times2^n}$ for all $i=1,2,\ldots,2^{m+1}$. Clearly, $\boldsymbol{L}\otimes\boldsymbol{L}_{\rm u}=[\delta_{2^m}^{\eta_1}\otimes\boldsymbol{L}_{\rm u}\ \ \ \delta_{2^m}^{\eta_2}\otimes\boldsymbol{L}_{\rm u}\ \ \cdots\ \ \delta_{2^m}^{\eta_{2^m}}\otimes\boldsymbol{L}_{\rm u}]$, and for all $i=1,2,\ldots,2^m$, we have

$$\delta_{2^m}^{\eta_i}\otimes\boldsymbol{L}_{\rm u}=\delta_{2^{m+n}}[(\eta_i-1)2^n+\zeta_1\ \ (\eta_i-1)2^n+\zeta_2\ \cdots\ (\eta_i-1)2^n+\zeta_{2^{n+1}}]=[\boldsymbol{L}_{2i-1}\ \ \boldsymbol{L}_{2i}].$$

Therefore, we can deduce that

$$\begin{aligned}\bar{\boldsymbol{L}}_c&=(\boldsymbol{L}\otimes\boldsymbol{L}_{\rm u})(\boldsymbol{A}\otimes\boldsymbol{I}_{2^n})=[\boldsymbol{L}_1\ \ \boldsymbol{L}_2\ \cdots\ \boldsymbol{L}_{2^{m+1}}][\mathrm{Col}_1(\boldsymbol{A})\otimes\boldsymbol{I}_{2^n}\ \ \ \mathrm{Col}_2(\boldsymbol{A})\otimes\boldsymbol{I}_{2^n}\ \cdots\ \mathrm{Col}_{2^m}(\boldsymbol{A})\otimes_{2^n}]\\&=[\boldsymbol{L}_1\ \ \boldsymbol{L}_3\ \cdots\ \boldsymbol{L}_{2^m-1}\ \ \boldsymbol{L}_{2^m+2}\ \ \boldsymbol{L}_{2^m+4}\ \cdots\ \boldsymbol{L}_{2^{m+1}}].\end{aligned}$$

Hence, $\bar{\boldsymbol{L}}_{ci}=\boldsymbol{L}_{2i-1}$ and $\bar{\boldsymbol{L}}_{c(2^{m-1}+i)}=\boldsymbol{L}_{2^m+2i}$ for all $i=1,2,\ldots,2^{m-1}$. Thus, the result follows. □

Theorem 2. Let $\boldsymbol{L}=[\boldsymbol{L}_1\ \boldsymbol{L}_2]$ with $\boldsymbol{L}_1,\boldsymbol{L}_2\in\mathcal{L}_{2^m\times2^{m-1}}$ be a state transition matrix of NFSR1, and let $\boldsymbol{L}_{\rm u}=[\boldsymbol{L}_{\rm u1}\ \boldsymbol{L}_{\rm u2}]$ with $\boldsymbol{L}_{\rm u1},\boldsymbol{L}_{\rm u2}\in\mathcal{L}_{2^n\times2^n}$ be a state transition matrix of NFSR2. Then

$$\bar{\boldsymbol{L}}_c=[\boldsymbol{L}_1\otimes\boldsymbol{L}_{\rm u1}\ \ \boldsymbol{L}_2\otimes\boldsymbol{L}_{\rm u2}].\tag{B18}$$

is a state transition matrix of the cascade connection of NFSR1 into NFSR2.

Proof. The result directly follows from Proposition 2 and the definition of Kronecker product. □

Appendix B.3 Proof of Theorem 3

Theorem 3. If an n-stage Fibonacci NFSR and an n-stage Galois NFSR are equivalent, then their state diagrams are isomorphic.

Proof. Let Ω_f and Ω_g be the sets of output sequences, respectively, of the Fibonacci NFSR and of the Galois NFSR. Since they are equivalent, we have $\Omega_f = \Omega_g$.

For any given output sequence $\boldsymbol{a} = (a_i)_{i\geqslant 0}$ of the Fibonacci NFSR, let K_a be the preperiod of $\boldsymbol{a}$, and P_a be the least period of $\boldsymbol{a}$, that is, K_a is the least nonnegative integer such that $a_{i+P_a} = a_i$ for all $i \geqslant K_a$. Since any sequence generated by an NFSR is ultimately periodic, P_a must be a positive integer. Moreover, the sequence $\boldsymbol{a}$ is formed by the first components of $K_a + P_a$ consecutive states of the Fibonacci NFSR, denoted by $\boldsymbol{X}_1, \boldsymbol{X}_2, \ldots, \boldsymbol{X}_{K_a+P_a}$. Let $\boldsymbol{b} = (b_j)_{j\geqslant K_a}$. Then $\boldsymbol{b}$ is a sequence of period P_a.

Since $\boldsymbol{a} \in \Omega_f$, we have $\boldsymbol{a} \in \Omega_g$. Hence, there exist $N_a = K_a + B_aP_a + C_aP_a$ consecutive states of the Galois NFSR such that their first components form the sequence $\boldsymbol{a}$, where B_aP_a consecutive states are on a transient with nonnegative integer $B_a \geqslant 0$, and C_aP_a consecutive states are on a cycle with positive integer $C_a \geqslant 1$, and the first components of $B_aP_a + C_aP_a$ consecutive states form the sequence $\boldsymbol{b}$.

If $B_a + C_a > 1$, then there exist two different initial states of the Galois NFSR such that the output sequences resulting from both initial states are the sequence $\boldsymbol{b}$. It implies that the cardinality of Ω_g satisfies $|\Omega_g| < 2^n$. Thus $|\Omega_f| < 2^n$ as well, which is in contradiction with the fact that an n-stage Fibonacci NFSR totally has 2^n output sequences. Hence, $B_a + C_a = 1$. Note that B_a is a nonnegative integer and C_a is a positive integer. Then, $B_a = 0$ and $C_a = 1$. It indicates that there are $K_a + P_a$ consecutive states of the Galois NFSR, denoted by $\boldsymbol{Y}_1, \boldsymbol{Y}_2, \ldots, \boldsymbol{Y}_{K_a+P_a}$, such that their first components form the sequence $\boldsymbol{a}$. Therefore, the exists a bijection mapping $\varphi : \boldsymbol{X}_i \mapsto \boldsymbol{Y}_i, i = 1, 2, \ldots, K_a + P_a$, such that for any given edge from $\boldsymbol{X}_{i_1}$ to $\boldsymbol{X}_{i_2}$ in the state diagram of the Fibonacci NFSR, there is an edge from $\varphi(\boldsymbol{X}_{i_1})$ to $\varphi(\boldsymbol{X}_{i_2})$ in the state diagram of the cascade connection. Due to the arbitrariness of the sequence $\boldsymbol{a}$, the result follows. □

Based on Theorem 3, the following corollary is immediately gotten.

Corollary 1. A cascade connection of NFSR1 into NFSR2 is nonsingular if and only if its equivalent Fibonacci NFSR is nonsingular.

Appendix B.4 Proof of Theorem 4

Proposition 3. The state transition matrix $\boldsymbol{L}_{\rm u}$ in (B6) of NFSR2 and the state transition matrix $\boldsymbol{L}_0$ in (B12) of NFSR2 with input holding constantly at zero, satisfy

1) $\mathrm{Col}_{2^n+j}(\boldsymbol{L}_{\rm u}) = \mathrm{Col}_j(\boldsymbol{L}_0),\ j = 1, 2, \ldots, 2^n$.
2) Moreover, if the feedback function of NFSR2 is nonsingular, then $\mathrm{Col}_j(\boldsymbol{L}_{\rm u}) = \mathrm{Col}_{2^{n-1}+j}(\boldsymbol{L}_0)$ and $\mathrm{Col}_{2^{n-1}+j}(\boldsymbol{L}_{\rm u}) = \mathrm{Col}_j(\boldsymbol{L}_0)$ for all $j = 1, 2, \ldots, 2^{n-1}$.

Proof. Let U_1 and f be the input and feedback function of NFSR2, respectively, and let $[p_1, p_2, \ldots, p_{2^n}]$ be the truth table of f, arranged in the reverse alphabet order. We also let $[s_1, s_2, \ldots, s_{2^{n+1}}]$ be the truth table of the function $f_n(U_1, X_1, \ldots, X_n) = U_1 \oplus f(X_1, X_2, \ldots, X_n)$, arranged in the reverse alphabet order as well. For any $j \in \{1, 2, \ldots, 2^{n+1}\}$, let $[U_1^{(j)}\ X_1^{(j)}\ \cdots\ X_n^{(j)}]^T$ denote the vector $[U_1\ X_1\ \cdots\ X_n]^T$ that corresponds to the decimal number $2^{n+1} - j$, that is, $2^nU_1^{(j)} + 2^{n-1}X_1^{(j)} + \cdots + X_n^{(j)} = 2^{n+1} - j$. Similarly, for any $k \in \{1, 2, \ldots, 2^n\}$, let $[X_1^{(k)}\ X_2^{(k)}\ \cdots\ X_n^{(k)}]^T$ denote the vector $[X_1\ X_2\ \cdots\ X_n]^T$ that corresponds to the decimal number $2^n - k$.

Clearly, $U_1^{(2^n+j)} = 0$ for all $j = 1, 2, \ldots, 2^n$. Thus, we have

$$s_{2^n+j} = f_n(U_1^{(2^n+j)}, X_1^{(2^n+j)}, \ldots, X_n^{(2^n+j)}) = f(X_1^{(2^n+j)}, \ldots, X_n^{(2^n+j)}),\ j = 1, 2, \ldots, 2^n.$$

Note that $[X_1^{(2^n+j)}\ \cdots\ X_n^{(2^n+j)}]^T = [X_1^{(k)}\ \cdots\ X_n^{(k)}]^T$ as $k = j$, and $p_k = f(X_1^{(k)}, \ldots, X_n^{(k)})$ for all $k = 1, 2, \ldots, 2^n$. Therefore, $s_{2^n+j} = p_j$ for all $j = 1, 2, \ldots, 2^n$. According to Eqs. (B13) and (B7), Item 1 follows. Item 2 can be proved in a similar way. □

Lemma 5. An n-stage NFSR represented by System $\boldsymbol{s}(t+1) = \boldsymbol{A}\boldsymbol{s}(t)$ with state $\boldsymbol{s} \in \Delta_{2^n}$ is nonsingular if and only if the state transition matrix $\boldsymbol{A}$ is nonsingular.

Proof. Since $\boldsymbol{s}(t+1) = \boldsymbol{A}\boldsymbol{s}(t)$ with $\boldsymbol{s} \in \Delta_{2^n}$, we have $\boldsymbol{A} \in \mathcal{L}_{2^n\times 2^n}$. An NFSR is nonsingular if and only if its state diagram only contains cycles, which is equivalent to that each state of the NFSR has only one predecessor and only one successor. For any two distinct states $\delta_{2^n}^{j_i}$, $i = 1, 2$, we have $\boldsymbol{A}\delta_{2^n}^{j_i} = \mathrm{Col}_{j_i}(\boldsymbol{A})$, which implies that $\delta_{2^n}^{j_i}$ is a predecessor of $\mathrm{Col}_{j_i}(\boldsymbol{A})$, and that $\mathrm{Col}_{j_i}(\boldsymbol{A})$ is the successor of $\delta_{2^n}^{j_i}$.

Sufficiency: If $\boldsymbol{A}$ is nonsingular, then all of its columns are distinct. Thus, $\mathrm{Col}_{j_1}(\boldsymbol{A}) \neq \mathrm{Col}_{j_2}(\boldsymbol{A})$. Due to the arbitrariness of the states $\delta_{2^n}^{j_i}$, $i = 1, 2$, we can conclude that each state of the NFSR has only one predecessor and only one successor.

Necessity: If an NFSRs is nonsingular, then each state of the NFSR has only one predecessor and only one successor. Therefore, $\mathrm{Col}_{j_1}(\boldsymbol{A}) \neq \mathrm{Col}_{j_2}(\boldsymbol{A})$. Due to the arbitrariness of $\mathrm{Col}_{j_1}(\boldsymbol{A})$ and $\mathrm{Col}_{j_2}(\boldsymbol{A})$, we deduce that all columns of $\boldsymbol{A}$ are distinct. Thus, $\boldsymbol{A}$ is nonsingular. □

Corollary 2. A cascade connection of NFSR1 into NFSR2 represented by System (B14) is nonsingular if and only if its state transition matrix $\bar{\boldsymbol{L}}_c$ in (B14) is nonsingular.

As stated in Remark 1, a cascade connection of NFSR1 into NFSR2 can also be represented by $\boldsymbol{z}(t+1) = \boldsymbol{L}_c\boldsymbol{z}(t)$. Thus, the cascade connection is nonsingular if and only if $\boldsymbol{L}_c$ is nonsingular, which is just the result given in [8]. However, both

state transition matrices $\boldsymbol{L}_c$ and $\bar{\boldsymbol{L}}_c$ are of large size in general. Hence, using state transition matrices is not an efficient way to the nonsingularity of a cascade connection of two NFSRs. Alternatively, the following gives an efficient way.

Theorem 4. A cascade connection of NFSR1 into NFSR2 is nonsingular if and only if the feedback functions of both NFSRs are nonsingular.

Proof. As before, we let $\boldsymbol{L} = \delta_{2^m}[\eta_1 \ \ \eta_2 \ \ \dots \ \ \eta_{2^m}]$ and $\boldsymbol{L}_{\rm u} = \delta_{2^n}[\zeta_1 \ \ \zeta_2 \ \ \dots \ \ \zeta_{2^{n+1}}]$, respectively, be the state transition matrices of NFSR1 and NFSR2. We also let $\bar{\boldsymbol{L}}_c$ in (B14) be the state transition matrix of the cascade connection.

From Proposition 2, we can deduce that all columns of $\bar{\boldsymbol{L}}_c$ are distinct if and only if the following three properties are satisfied: 1) $\eta_1, \eta_2, \dots, \eta_{2^m}$ are distinct; 2) $\zeta_1, \zeta_2, \dots, \zeta_{2^n}$ are distinct; 3) $\zeta_{2^n+1}, \zeta_{2^n+2}, \dots, \zeta_{2^{n+1}}$ are distinct. First, $\eta_1, \eta_2, \dots, \eta_{2^m}$ are distinct if and only if the feedback function of NFSR1 is nonsingular. On the other hand, according to Eq. (B7), we have $\zeta_i, \zeta_{2^n+i} \in \{2a_i - 1, 2a_i\}$ with $a_i = (i-1) \bmod 2^{n-1} + 1$ for all $i = 1, 2, \dots, 2^n$. Hence, $\zeta_1, \zeta_2, \dots, \zeta_{2^n}$ (resp. $\zeta_{2^n+1}, \zeta_{2^n+2}, \dots, \zeta_{2^{n+1}}$) are distinct if and only if they take all possible values of $1, 2, \dots, 2^n$. Therefore, 2) and 3) are equivalent. From Property 1 of Proposition 3, we can infer that that $\zeta_{2^n+1}, \zeta_{2^n+2}, \dots, \zeta_{2^{n+1}}$ are distinct if and only if the feedback function of NFSR2 is nonsingular. Thus, all columns of $\bar{\boldsymbol{L}}_c$ are distinct if and only if the feedback functions of NFSR1 and NFSR2 are nonsingular. Note that $\bar{\boldsymbol{L}}_c \in \mathcal{L}_{2^{m+n} \times 2^{m+n}}$. Then all columns of $\bar{\boldsymbol{L}}_c$ are distinct if and only if $\bar{\boldsymbol{L}}_c$ is nonsingular. Thus, the result follows from Corollary 2. □

Theorem 4 can be proved in another way. For a cascade connection of NFSR1 into NFSR2 and its equivalent Fibonacci NFSR, their characteristic functions satisfy $h_c = g_c * f_c$ [2], where g_c, f_c and h_c are the characteristic functions of NFSR1, NFSR2 and the Fibonacci NFSR, respectively. Moreover, h_c is nonsingular if and only if g_c and f_c are nonsingular [9]. Note that the characteristic function of a Fibonacci NFSR is nonsingular if and only if its feedback function is nonsingular. Hence, for a cascade connection of NFSR1 into NFSR2 and its equivalent Fibonacci NFSR, the feedback functions of NFSR1 and NFSR2 are nonsingular if and only if the feedback function of the Fibonacci NFSR is nonsingular, which is equivalent to that the Fibonacci NFSR is nonsingular. Corollary 1 has shown that a cascade connection of NFSR1 into NFSR2 is nonsingular if and only if its equivalent Fibonacci NFSR is nonsingular. Thus, Theorem 4 follows.

Example 1. Consider a cascade connection of a 3-stage NFSR1 into a 3-stage NFSR2, in which the feedback function of NFSR1 is $g(U_1, U_2, U_3) = U_1 \oplus U_3 \oplus U_2U_3 \oplus 1$, and the feedback function of NFSR2 is $f(X_1, X_2, X_3) = X_1 \oplus X_2X_3$.

By direct computations we obtain the state diagram of the cascade connection only contains two cycles: 1) a cycle of length 56, i.e., $63 \to 55 \to 39 \to 7 \to 14 \to 21 \to 43 \to 30 \to 61 \to 50 \to 37 \to 2 \to 12 \to 17 \to 42 \to 29 \to 59 \to 54 \to 36 \to 0 \to 8 \to 16 \to 40 \to 25 \to 58 \to 53 \to 34 \to 5 \to 11 \to 23 \to 46 \to 28 \to 57 \to 51 \to 38 \to 4 \to 9 \to 18 \to 44 \to 24 \to 56 \to 49 \to 35 \to 8 \to 13 \to 19 \to 47 \to 31 \to 62 \to 52 \to 32 \to 1 \to 10 \to 20 \to 41 \to 27 \to 63$; 2) and a cycle of length 8, i.e., $60 \to 48 \to 33 \to 3 \to 15 \to 22 \to 45 \to 26 \to 60$, where all integers are the decimal numbers corresponding to the states over $\mathbb{F}_2^6$. On the other hand, both g and f are, clearly, nonsingular. From Theorem 4, we deduce that the cascade connection is nonsingular, consistent with the fact that its state diagram only contains cycles.

However, if we modify the feedback function of NFSR2 as $\tilde{f}(X_1, X_2, X_3) = X_1 \oplus X_1X_2 \oplus X_2X_3$. By direct computations again, we found that both states that correspond to the decimal numbers 63 and 59 are two predecessors of the state that corresponds to the decimal number 54, which implies that the state diagram of the modified cascade connection contains some branch state. On the other hand, since $\tilde{f}$ is clearly not nonsingular, we can deduce from Theorem 4 that the modified cascade connection is singular, which is consistent with the fact that its state diagram contains some branch state.

Appendix B.5 Proof of Theorem 5

Lemma 6. A Fibonacci NFSR represented by System $\boldsymbol{Y}(t+1) = H(\boldsymbol{Y}(t))$ with state $\boldsymbol{Y} \in \mathbb{F}_2^n$ is equivalent to a cascade connection of two NFSRs represented by System $\boldsymbol{Z}(t+1) = F(\boldsymbol{Z}(t))$ with state $\boldsymbol{Z} \in \mathbb{F}_2^n$, if and only if there exists a bijective mapping $\varphi : \boldsymbol{Y} \mapsto \boldsymbol{Z}$ such that $\varphi(H(\boldsymbol{Y})) = F(\varphi(\boldsymbol{Y}))$ and $[1\ 0\ \cdots 0]\varphi(\boldsymbol{Y}) = [1\ 0\ \cdots 0]\boldsymbol{Y}$ for all $\boldsymbol{Y} \in \mathbb{F}_2^n$.

Proof. Necessity: Clearly, for each $\boldsymbol{Y} \in \mathbb{F}_2^n$, there exists an edge from state $\boldsymbol{Y}$ to state $H(\boldsymbol{Y})$ in the state diagram of the Fibonacci NFSR, Similarly, for each $\boldsymbol{Z} \in \mathbb{F}_2^n$, there exists an edge from state $\boldsymbol{Z}$ to state $F(\boldsymbol{Z})$ in the state diagram of the cascade connection. If a Fibonacci NFSR is equivalent to a cascade connection of two NFSRs, then according to Theorem 3, their state diagrams are isomorphic, which is equivalent to that there exists a bijective mapping $\varphi : \boldsymbol{Y} \mapsto \boldsymbol{Z}$ such that $\varphi(H(\boldsymbol{Y})) = F(\boldsymbol{Z}) = F(\varphi(\boldsymbol{Y}))$ for each $\boldsymbol{Y} \in \mathbb{F}_2^n$. Moreover, Since the output of an NFSR is the content of the first bit, each state $\boldsymbol{Y}$ and its correspondingly transformed state $\boldsymbol{Z}$ have the same first component, which is equivalent to $[1\ 0\ \cdots 0]\varphi(\boldsymbol{Y}) = [1\ 0\ \cdots 0]\boldsymbol{Y}$ for each $\boldsymbol{Y} \in \mathbb{F}_2^n$.

Sufficiency: If there exists a bijective mapping $\varphi : \boldsymbol{Y} \mapsto \boldsymbol{Z}$ such that $\varphi(H(\boldsymbol{Y})) = F(\varphi(\boldsymbol{Y}))$ and $[1\ 0\ \cdots 0]\varphi(\boldsymbol{Y}) = [1\ 0\ \cdots 0]\boldsymbol{Y}$ for all $\boldsymbol{Y} \in \mathbb{F}_2^n$, then according to the necessity proof, the state diagrams of the Fibonacci NFSR and the cascade connection are isomorphic, and each state and its correspondingly transformed state have the same first component. Hence, the Fibonacci NFSR and the cascade connection have the same set of output sequences. Thus, they are equivalent. □

Proposition 4. A Fibonacci NFSR represented by System $\boldsymbol{y}(t+1) = L_f\boldsymbol{y}(t)$ with state $\boldsymbol{y} \in \Delta_{2^n}$ is equivalent to a cascade connection of two NFSRs represented by System $\boldsymbol{z}(t+1) = \boldsymbol{L}_c\boldsymbol{z}(t)$ with state $\boldsymbol{z} \in \Delta_{2^n}$, if and only if there exists a permutation matrix $\boldsymbol{V} = \delta_{2^n}[j_1\ j_2\ \dots\ j_{2^n}]$ satisfying $1 \leqslant j_i \leqslant 2^{n-1}$ and $2^{n-1}+1 \leqslant j_{2^{n-1}+i} \leqslant 2^n$ for all $i = 1, 2, \dots, 2^{n-1}$, such that $\boldsymbol{L}_c = \boldsymbol{V}\boldsymbol{L}_f\boldsymbol{V}^{-1}$.

Proof. Note that the states over $\mathbb{F}_2^n$ and the states over Δ_{2^n} are one-to-one correspondent. Then we can set $\boldsymbol{z} = \boldsymbol{V}\boldsymbol{y}$, where $\boldsymbol{V}$ is a permutation matrix determined by the bijection mapping φ in Lemma 6. Since all states in the set $S_1 = \{\delta_{2^n}^j | j = 1, 2, \dots, 2^{n-1}\}$ correspond to the states over $\mathbb{F}_2^n$ whose first components are 1, and all states in the set $S_2 = \{\delta_{2^n}^j | j = 2^{n-1}+1, 2^{n-1}+2, \dots, 2^n\}$ correspond to the states over $\mathbb{F}_2^n$ whose first components are 0, we can easily infer the result from Lemma 6. □

Theorem 5. An $(m+n)$-stage Fibonacci NFSR can be decomposed into a cascade connection of an m-stage NFSR1 into an n-stage NFSR2, if and only if there exists a permutation matrix $\boldsymbol{P}=[\boldsymbol{P}_l\ \boldsymbol{P}_r]\in\mathcal{P}_{2^{m+n}}$ with $\boldsymbol{P}_l,\boldsymbol{P}_r\in\mathcal{L}_{2^{m+n-1}}$, such that $\boldsymbol{P}\boldsymbol{L}_f\boldsymbol{P}_l^{-1}=\boldsymbol{L}_1\otimes\boldsymbol{L}_{\rm u1}$ and $\boldsymbol{P}\boldsymbol{L}_f\boldsymbol{P}_r^{-1}=\boldsymbol{L}_2\otimes\boldsymbol{L}_{\rm u2}$, where $\boldsymbol{L}_f\in\mathcal{L}_{2^{m+n}\times 2^{m+n}}$ is a state transition matrix of the Fibonacci NFSR, $[\boldsymbol{L}_1\ \boldsymbol{L}_2]$ is a state transition matrix of NFSR1 with $\boldsymbol{L}_1,\boldsymbol{L}_2\in\mathcal{L}_{2^m\times 2^{m-1}}$, and $[\boldsymbol{L}_{\rm u1}\ \boldsymbol{L}_{\rm u2}]$ is a state transition matrix of NFSR2 with $\boldsymbol{L}_{\rm u1},\boldsymbol{L}_{\rm u2}\in\mathcal{L}_{2^n\times 2^n}$.

Proof. A Fibonacci NFSR can be decomposed into a cascade connection of NFSR1 into NFSR2 if and only if they are equivalent. According to Proposition 4 , we know that the Fibonacci NFSR and the cascade connection are equivalent if and only if there exists a permutation matrix $\boldsymbol{V}=\delta_{2^{m+n}}[j_1,\ \ j_2\ \cdots\ j_{2^{m+n}}]$ such that the state transition matrix $\boldsymbol{L}_c$ of the cascade connection satisfies $\boldsymbol{L}_c=\boldsymbol{V}\boldsymbol{L}_f\boldsymbol{V}^{-1}$, where $1\leqslant j_i\leqslant 2^{m+n-1}$ and $2^{m+n-1}+1\leqslant j_{2^{m+n-1}+i}\leqslant 2^{m+n}$ for all $i=1,2,\ldots,2^{m+n-1}$. According to Theorem 2, $\bar{\boldsymbol{L}}_c=[\boldsymbol{L}_1\otimes\boldsymbol{L}_{\rm u1}\ \ \boldsymbol{L}_2\otimes\boldsymbol{L}_{\rm u2}]$ is another state transition matrix of the cascade connection. From Remark 1, we know that the state transition matrix $\boldsymbol{L}_c=\boldsymbol{W}_{[2^m,2^n]}\bar{\boldsymbol{L}}_c\boldsymbol{W}_{[2^n,2^m]}$. Hence, $\bar{\boldsymbol{L}}_c=(\boldsymbol{W}_{[2^n,2^m]}\boldsymbol{V})\boldsymbol{L}_f(\boldsymbol{W}_{[2^n,2^m]}\boldsymbol{V})^{-1}$. Set $\boldsymbol{P}=\boldsymbol{W}_{[2^n,2^m]}\boldsymbol{V}$. Then $\boldsymbol{P}\boldsymbol{L}_f\boldsymbol{P}_l^{-1}=\boldsymbol{L}_1\otimes\boldsymbol{L}_{\rm u1}$, and $\boldsymbol{P}\boldsymbol{L}_f\boldsymbol{P}_r^{-1}=\boldsymbol{L}_2\otimes\boldsymbol{L}_{\rm u2}$.

The left is to prove $\boldsymbol{P}\in\mathcal{P}_{2^{m+n}}$. Clearly,

$$\boldsymbol{P}=\boldsymbol{W}_{[2^n,2^m]}\boldsymbol{V}=[{\rm Col}_{j_1}(\boldsymbol{W}_{[2^n,2^m]})\ \ {\rm Col}_{j_2}(\boldsymbol{W}_{[2^n,2^m]}\ \cdots\ {\rm Col}_{j_{2^{m+n}}}(\boldsymbol{W}_{[2^n,2^m]})].$$

According to the proof of Lemma 4, we know the explicit form of each column of $\boldsymbol{W}_{[2^n,2^m]}$. Note that $1\leqslant j_i\leqslant 2^{m+n-1}$ and $2^{m+n-1}+1\leqslant j_{2^{m+n-1}+i}\leqslant 2^{m+n}$ for all $i=1,2,\ldots,2^{m+n-1}$. Then we can easily see $\boldsymbol{P}\in\mathcal{P}_{2^{m+n}}$. □

Appendix B.6 Proof of Theorem 6

Corollary 1 have shown that a cascade connection of two NFSRs is nonsingular if and only if its equivalent Fibonacci NFSRs is nonsingular. Hence, to assure the nonsingularity of the cascade connection, the decomposed Fibonacci NFSR must be nonsingular. Theorem 6 gives a criterion to the decomposition of nonsingular Fibonacci NFSRs.

Theorem 6. An $(m+n)$-stage nonsingular Fibonacci NFSR can be decomposed into a cascade connection of an m-stage NFSR1 into an n-stage NFSR2, if and only if there exists a permutation matrix $\boldsymbol{P}\in\mathcal{P}_{2^{m+n}}$ such that $\boldsymbol{P}\boldsymbol{L}_f\boldsymbol{P}^{-1}\boldsymbol{Q}_0=\boldsymbol{L}\otimes\boldsymbol{L}_{\rm u2}$, where $\boldsymbol{L}_f\in\mathcal{L}_{2^{m+m}\times 2^{m+n}}$ is a state transition matrix of the Fibonacci NFSR, $\boldsymbol{L}\in\mathcal{R}_{2^m}$ is a state transition matrix of NFSR1, $\boldsymbol{L}_{\rm u2}\in\mathcal{R}_{2^n}$ is a state transition matrix of NFSR2 with input holding constantly at zero, and

$$\boldsymbol{Q}_0=\begin{bmatrix}\boldsymbol{I}_{2^{m-1}}\otimes\boldsymbol{P}_0 & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{I}_{2^{m+n-1}}\end{bmatrix}$$

is a permutation matrix with $\boldsymbol{P}_0=\delta_{2^n}[2^{n-1}+1\ \ 2^{n-1}+2\ \cdots\ 2^n\ \ 1\ \ 2\ \cdots\ 2^{n-1}]$.

Proof. We use the same notations as in Theorem 5. According to Proposition 3, $\boldsymbol{L}_{\rm u2}$ is the state transition matrix of NFSR2 with input holding constantly at zero. From the proof of Theorem 5, we know that the Fibonacci NFSR can be decomposed into the cascade connection of NFSR1 into NFSR2 if and only if there exists a permutation matrix $\boldsymbol{V}=\delta_{2^{m+n}}[j_1,\ \ j_2\ \cdots\ j_{2^{m+n}}]$ such that $\boldsymbol{L}_c=\boldsymbol{V}\boldsymbol{L}_f\boldsymbol{V}^{-1}$, where $1\leqslant j_i\leqslant 2^{m+n-1}$ and $2^{m+n-1}+1\leqslant j_{2^{m+n-1}+i}\leqslant 2^{m+n}$ for all $i=1,2,\ldots,2^{m+n-1}$.

According to Corollary 1 and Theorem 4, we conclude that the Fibonacci NFSR is nonsingular if and only if NFSR1 and NFSR2 with input holding constantly at zero are nonsingular, which is equivalent to $\boldsymbol{L}\in\mathcal{R}_{2^m}$ and $\boldsymbol{L}_{\rm u2}\in\mathcal{R}_{2^n}$. From Proposition 3, we know $\boldsymbol{L}_{\rm u1}=\boldsymbol{L}_{\rm u2}\boldsymbol{P}_0$. Thus, $\boldsymbol{L}_1\otimes\boldsymbol{L}_{\rm u1}=\boldsymbol{L}_1\otimes\boldsymbol{L}_{\rm u2}\boldsymbol{P}_0=(\boldsymbol{L}_1\otimes\boldsymbol{L}_{\rm u2})(\boldsymbol{I}_{2^{m-1}}\otimes\boldsymbol{P}_0)$. On the other hand, Theorem 2 has shown $\bar{\boldsymbol{L}}_c=[\boldsymbol{L}_1\otimes\boldsymbol{L}_{\rm u1}\ \ \ \boldsymbol{L}_2\otimes\boldsymbol{L}_{\rm u2}]$. Hence, we can easily compute that $\bar{\boldsymbol{L}}_c=(\boldsymbol{L}\otimes\boldsymbol{L}_{\rm u2})\boldsymbol{Q}_0$. Clearly, $\boldsymbol{P}_0$ is a permutation matrix and satisfies $\boldsymbol{P}_0^{-1}=\boldsymbol{P}_0$. Then, $\boldsymbol{Q}_0$ is also a permutation matrix and satisfies $\boldsymbol{Q}_0^{-1}=\boldsymbol{Q}_0$. From the proof of Theorem 5, we know $\bar{\boldsymbol{L}}_c=(\boldsymbol{W}_{[2^n,2^m]}\boldsymbol{V})\boldsymbol{L}_f(\boldsymbol{W}_{[2^n,2^m]}\boldsymbol{V})^{-1}$, and $\boldsymbol{P}=\boldsymbol{W}_{[2^n,2^m]}\boldsymbol{V}\in\mathcal{P}_{2^{m+n}}$. Therefore, $(\boldsymbol{L}\otimes\boldsymbol{L}_{\rm u2})\boldsymbol{Q}_0=\boldsymbol{P}\boldsymbol{L}_f\boldsymbol{P}^{-1}$, yielding $\boldsymbol{P}\boldsymbol{L}_f\boldsymbol{P}^{-1}\boldsymbol{Q}_0=\boldsymbol{L}\otimes\boldsymbol{L}_{\rm u2}$. □

Theorems 5 and 6 show that the decomposition of (nonsingular) Fibonacci NFSRs can be converted into the Kronecker product decomposition of (permutation) matrices whose columns are canonical vectors. It will be shown in later Remark 2 that using the latter lowers the time complexity of computations.

In addition, Theorems 5 and 6 show that the decomposition type of a Fibonacci NFSR (i.e., the type of a pair of NFSR1 and NFSR2 that are decomposed from the Fibonacci NFSR) is determined by the permutation matrix $\boldsymbol{P}$, which is only relative to two factors. One is the decomposition of the Fibonacci NFSR's stage number such that it can be decomposed as a sum of two positive integers that are the stage numbers of NFSR1 and NFSR2. The other is the state permutation of the Fibonacci NFSR such that its set of output sequences is preserved.

Notably, even if the decomposition of stage number is fixed for a given Fibonacci NFSR, different state permutation may result in different decomposition type, which can be easily seen from the property given in [3], namely, $D(g_c)*(f_c\oplus 1)=g_c*f_c$, where $D(g_c)(U_1,U_2,\ldots,U_m)=g_c(U_1\oplus 1,U_2\oplus 1,\ldots,U_m\oplus 1)$ for any $[U_1\ U_2\ \cdots\ U_m]\in\mathbb{F}_2^m$, with characteristic functions g_c and f_c. Summarizing all facts, we can easily see that the decomposition is not unique if a Fibonacci NFSR is decomposable. Of course, if some constraints are imposed on two NFSRs in the cascade connection, then the decomposition may be unique, like that in [4], where the feedback functions of all NFSRs are restricted to taking zero at the origin.

Appendix B.7 Proof of Theorem 7

Lemma 7. For any $m\times r$ matrix $\boldsymbol{A}$ and any $n\times s$ matrix $\boldsymbol{B}$, $\boldsymbol{A}\otimes\boldsymbol{B}\in\mathcal{L}_{mn\times rs}$ if and only if $\boldsymbol{A}\in\mathcal{L}_{m\times r}$ and $\boldsymbol{B}\in\mathcal{L}_{n\times s}$.

Proof. As each column of a matrix in $\mathcal{L}_{p\times q}$ has only one entry of 1 and the other entries of 0, the result can be easily inferred from the definition of Kronecker product. □.

Theorem 7. Let $\boldsymbol{A}=\delta_m[\alpha_1\ \alpha_2\ \cdots\ \alpha_r]\in\mathcal{L}_{m\times r}$, $\boldsymbol{B}=\delta_n[\beta_1\ \beta_2\ \cdots\ \beta_s]\in\mathcal{L}_{n\times s}$, and $\boldsymbol{P}=\delta_{mn}[\gamma_1\ \gamma_2\ \cdots\ \gamma_{rs}]\in\mathcal{L}_{mn\times rs}$. Then $\boldsymbol{P}=\boldsymbol{A}\otimes\boldsymbol{B}$ if and only if

$$\begin{cases}\beta_{(i-1)\bmod s+1}=(\gamma_i-1)\bmod n+1,\\ \alpha_{\lceil\frac{i}{s}\rceil}=\lceil\frac{\gamma_i}{n}\rceil,\quad i=1,2,\ldots,rs.\end{cases}\tag{B19}$$

Proof. Clearly, $\boldsymbol{A}\otimes\boldsymbol{B}=[\delta_m^{\alpha_1}\otimes\boldsymbol{B}\quad\delta_m^{\alpha_2}\otimes\boldsymbol{B}\ \cdots\ \delta_m^{\alpha_r}\otimes\boldsymbol{B}]$, and for all $j=1,2,\ldots,r$, we have

$$\delta_m^{\alpha_j}\otimes\boldsymbol{B}=[\delta_m^{\alpha_j}\otimes\delta_n^{\beta_1}\quad\delta_m^{\alpha_j}\otimes\delta_n^{\beta_2}\ \cdots\ \delta_m^{\alpha_j}\otimes\delta_n^{\beta_s}]=\delta_{mn}[(\alpha_j-1)n+\beta_1\ \ (\alpha_j-1)n+\beta_2\ \cdots\ (\alpha_j-1)n+\beta_s].$$

Note that each β_k satisfies $1\leqslant\beta_k\leqslant n$. Together taking Lemma 7 into consideration, we can infer that $\boldsymbol{P}=\boldsymbol{A}\otimes\boldsymbol{B}$ is equivalent to Eq. (B19). □

If $\boldsymbol{P}=\boldsymbol{A}\otimes\boldsymbol{B}$, then for the simplicity we say $\boldsymbol{A}$ and $\boldsymbol{B}$ are *factor matrices* of $\boldsymbol{P}$. For a matrix $\boldsymbol{P}\in\mathcal{L}_{m\times n}$, if $\boldsymbol{P}=\boldsymbol{A}\otimes\boldsymbol{B}=\boldsymbol{C}\otimes\boldsymbol{D}$, where $\boldsymbol{A}$ and $\boldsymbol{C}$ are of the same size, then from Theorem 7, we have $\boldsymbol{A}=\boldsymbol{C}$ and $\boldsymbol{B}=\boldsymbol{D}$. However, if $\boldsymbol{A}$ and $\boldsymbol{C}$ are not restricted to the same size, then the Kronecker product decomposition of $\boldsymbol{P}$ may be not unique, as $(\boldsymbol{M}\otimes\boldsymbol{N})\otimes\boldsymbol{K}=\boldsymbol{M}\otimes(\boldsymbol{N}\otimes\boldsymbol{K})$ for any matrices $\boldsymbol{M},\boldsymbol{N}$ and $\boldsymbol{K}$.

Remark 2. Theorem 7 provides a way to determine whether a matrix whose columns are canonical vectors is Kronecker product decomposable, and how to find its factor matrices if it is. To determine whether a matrix $\boldsymbol{P}=\delta_{mn}[\gamma_1\ \ \gamma_2\ \ldots\ \gamma_{rs}]$ can be decomposed as the Kronecker product of $\boldsymbol{A}\in\mathcal{L}_{m\times r}$ and $\boldsymbol{B}\in\mathcal{L}_{n\times s}$, we can first partition $\boldsymbol{\gamma}=[\gamma_1\ \ \gamma_2\ \ldots\ \gamma_{rs}]$ as $\boldsymbol{\gamma}=[\boldsymbol{\Gamma_1}\ \ \boldsymbol{\Gamma_2}\ \ldots\ \boldsymbol{\Gamma}_r]$, where each $\boldsymbol{\Gamma}_i=[\gamma_{(i-1)s+1}\ \ \gamma_{(i-1)s+2}\ \cdots\ \gamma_{is}]$, and then check whether $\lceil\frac{\gamma_{(i-1)s+1}}{n}\rceil=\lceil\frac{\gamma_{(i-1)s+2}}{n}\rceil=\cdots=\lceil\frac{\gamma_{is}}{n}\rceil$ for all $i=1,2,\ldots,r$, and whether $(\gamma_j-1)\bmod n=(\gamma_{s+j}-1)\bmod n=\cdots=(\gamma_{(r-1)s+j}-1)\bmod n$ for all $j=1,2\ldots,s$. If all these equations hold, then the matrix $\boldsymbol{P}$ can be decomposed as the Kronecker product of $\boldsymbol{A}$ and $\boldsymbol{B}$, moreover, $\boldsymbol{A}=\delta_m\left[\lceil\frac{\gamma_1}{n}\rceil\ \ \lceil\frac{\gamma_{s+1}}{n}\rceil\ \cdots\ \lceil\frac{\gamma_{(r-1)s+1}}{n}\rceil\right]$ and $\boldsymbol{B}=\delta_n[(\gamma_1-1)\bmod n+1\quad(\gamma_2-1)\bmod n+1\ \cdots\ (\gamma_s-1)\bmod n+1]$. Otherwise, it cannot.

Our above way is simpler than the matrix rank way [10]. The latter way is to first partition $\boldsymbol{P}$ as

$$\boldsymbol{P}=\begin{bmatrix}\boldsymbol{P}_{11}&\boldsymbol{P}_{12}&\cdots&\boldsymbol{P}_{1r}\\ \vdots&\vdots&&\vdots\\ \boldsymbol{P}_{m1}&\boldsymbol{P}_{m2}&\cdots&\boldsymbol{P}_{mr}\end{bmatrix},$$

where each $\boldsymbol{P}_{ij}$ is an $n\times s$ matrix, and then check whether the rank of the matrix $\boldsymbol{V}_P=[\boldsymbol{V}_c(\boldsymbol{P}_{11})\ \ \boldsymbol{V}_c(\boldsymbol{P}_{12})\ \cdots\ \boldsymbol{V}_c(\boldsymbol{P}_{1r})\ \cdots\ \boldsymbol{V}_c(\boldsymbol{P}_{m1})\ \ \boldsymbol{V}_c(\boldsymbol{P}_{m2})\ \cdots\ \boldsymbol{V}_c(\boldsymbol{P}_{mr})]$ is 1, where each $\boldsymbol{V}_c(\boldsymbol{P}_{ij})$ is a column vector that orderly stacks all columns of $\boldsymbol{P}_{ij}$. If the rank of $\boldsymbol{V}_P$ is 1, then $\boldsymbol{P}$ is Kronecker product decomposable. Otherwise, it is not. Clearly, our method takes advantage of the sparseness of $\boldsymbol{P}$, and only requires to consider the entries of 1 in the matrix $\boldsymbol{P}$, while the matrix rank method requires to consider all entries of $\boldsymbol{P}$. Thus, our method is simpler.

The state transition matrix of a Fibonacci NFSR has a dimension exponential in its stage number, and therefore the above method of Kronecker product decomposition is limited to those NFSRs with their stage numbers not too large. Nevertheless, Using the Kronecker product decomposition to solve the decomposition of a Fibonacci NFSR requires lower time complexity than using the $*$-product decomposition of its characteristic function. The reason is as follows. Without loss of generality, we assume the Fibonacci NFSR decomposed into a cascade connection of an m-stage NFSR1 into an n-stage NFSR2, the time complexity for the former method is mainly from $(2^{m+n-1}!)^2$ possible forms of $\boldsymbol{P}\in\mathcal{P}_{2^{m+n}}$ required to be considered, while the time complexity for the latter method is mainly from $2^{2^n+2^m}$ possible pairs of characteristic functions of NFSR1 and NFSR2 that need to be considered for a general Fibonacci NFSR, and $2^{2^{n-1}+2^{m-1}}$ possible pairs for a nonsingular Fibonacci NFSR.

Appendix C Example

Consider a 5-stage nonsingular Fibonacci NFSR given in [4]. Its feedback function is $h=Y_1\oplus Y_2\oplus Y_3\oplus Y_2Y_3\oplus Y_2Y_4\oplus Y_3Y_5\oplus Y_4Y_5$.

We can easily compute its state transitions as: $21\to11\to23\to14\to28\to24\to16\to1\to2\to4\to9\to19\to6\to13\to26\to21$, and $10\to20\to8\to17\to3\to7\to15\to30\to29\to27\to22\to12\to25\to18\to5\to10$, and $31\to31$ and $0\to0$, where all positive integers are the decimal numbers corresponding to the states $\boldsymbol{Y}=[Y_1\ \ Y_2\ \cdots\ Y_5]$s of the Fibonacci NFSR. Clearly, they produce two sequences of period 15, i.e., 101011100001001 and 010100011110110, and two sequences of period 1, i.e., 1 and 0. According to Eq. (B11), we can compute its state transition matrix as $\boldsymbol{L}_f=\delta_{32}[1\ 3\ 5\ 8\ 10\ 11\ 14\ 16\ 18\ 20\ 21\ 24\ 26\ 27\ 29\ \ 31\ 2\ 4\ 6\ 7\ 9\ 12\ 13\ 15\ 17\ 19\ 22\ 23\ 25\ 28\ 30\ 32]$.

Ref. [4] showed that it can be decomposed into a cascade connection of NFSR1 into NFSR2 in the following two types:

1) NFSR1 is a 1-stage LFSR with feedback function $g=U_1$, and NFSR2 is a 4-stage NFSR with feedback function $f=X_1\oplus X_3\oplus X_4\oplus X_2X_3\oplus X_2X_4\oplus X_3X_4$;

2) NFSR1 is a 4-stage NFSR with feedback function $\tilde{g}=\tilde{U}_1\oplus\tilde{U}_4\oplus\tilde{U}_2\tilde{U}_3\oplus\tilde{U}_3\tilde{U}_4$, and NFSR2 is a 1-stage LFSR with feedback function $\tilde{f}=\tilde{X}_1$.

For Type 1, the state transitions are: $21\to11\to23\to15\to29\to25\to17\to1\to3\to5\to9\to19\to7\to13\to27\to21$, and $10\to20\to8\to16\to2\to6\to14\to30\to28\to26\to22\to12\to24\to18\to4\to10$, and $31\to31$ and $0\to0$, where all positive integers are the decimal numbers corresponding to the states $\boldsymbol{Z}=[X_1\ \cdots\ X_4\ \ U_1]$s of the cascade connection. For Type 2, the state transitions are: $31\to14\to28\to9\to18\to20\to24\to1\to3\to6\to13\to26\to5\to11\to23\to31$, and $15\to30\to12\to25\to2\to4\to8\to17\to19\to22\to29\to10\to21\to27\to7\to15$, and $16\to16$

and $0 \to 0$, where all positive integers are the decimal numbers corresponding to the states $\tilde{\boldsymbol{Z}} = [\tilde{X}_1 \ \ \tilde{U}_1 \ \cdots \ \tilde{U}_4]$s of the cascade connection. Clearly, both types produce the same set of output sequences as the Fibonacci NFSR.

We use the previous notations. To distinguish both types, we add *tilde* to notations for Type 2. According to Lemma 1, we can easily obtain the permutation matrices

$$\boldsymbol{V} = \delta_{32}[1\ 2\ 4\ 3\ 6\ 5\ 8\ 7\ 9\ 10\ 11\ 12\ 13\ 14\ 16\ 15\ 18\ 17\ 19\ 20\ 21\ 22\ 23\ 24\ 26\ 25\ 28\ 27\ 30\ 29\ 31\ 32],$$
$$\tilde{\boldsymbol{V}} = \delta_{32}[16\ 15\ 13\ 14\ 10\ 9\ 11\ 12\ 4\ 3\ 1\ 2\ 6\ 5\ 7\ 8\ 24\ 23\ 21\ 22\ 18\ 17\ 19\ 20\ 28\ 27\ 25\ 26\ 30\ 29\ 31\ 32].$$

Since $\boldsymbol{P} = \boldsymbol{W}_{[16,2]}\boldsymbol{V}$ and $\tilde{\boldsymbol{P}} = \boldsymbol{W}_{[2,16]}\tilde{\boldsymbol{V}}$, we can easily obtain

$$\boldsymbol{P} = \delta_{32}[1\ 17\ 18\ 2\ 19\ 3\ 20\ 4\ 5\ 21\ 6\ 22\ 7\ 23\ 24\ 8\ 25\ 9\ 10\ 26\ 11\ 27\ 12\ 28\ 29\ 13\ 30\ 14\ 31\ 15\ 16\ 32],$$
$$\tilde{\boldsymbol{P}} = \delta_{32}[31\ 29\ 25\ 27\ 19\ 17\ 21\ 23\ 7\ 5\ 1\ 3\ 11\ 9\ 13\ 15\ 16\ 14\ 10\ 12\ 4\ 2\ 6\ 8\ 24\ 22\ 18\ 20\ 28\ 26\ 30\ 32].$$

Clearly, $\boldsymbol{P}, \tilde{\boldsymbol{P}} \in \mathcal{P}_{32}$ and they are distinct. Moreover, we can easily calculate

$$\boldsymbol{Q}_0 = \delta_{32}[9\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 17\ 18\ 19\ 20\ 21\ 22\ 23\ 24\ 25\ 26\ 27\ 28\ 29\ 30\ 31\ 32],$$
$$\tilde{\boldsymbol{Q}}_0 = \delta_{32}[2\ 1\ 4\ 3\ 6\ 5\ 8\ 7\ 10\ 9\ 12\ 11\ 14\ 13\ 16\ 15\ 17\ 18\ 19\ 20\ 21\ 22\ 23\ 24\ 25\ 26\ 27\ 28\ 29\ 30\ 31\ 32].$$

Hence, we directly compute $\boldsymbol{A} = \boldsymbol{P}\boldsymbol{L}_f\boldsymbol{P}^{-1}\boldsymbol{Q}_0$ and $\tilde{\boldsymbol{A}} = \tilde{\boldsymbol{P}}\boldsymbol{L}_f\tilde{\boldsymbol{P}}^{-1}\tilde{\boldsymbol{Q}}_0$ as

$$\boldsymbol{A} = \delta_{32}[2\ 3\ 5\ 7\ 10\ 12\ 14\ 15\ 1\ 4\ 6\ 8\ 9\ 11\ 13\ 16\ 18\ 19\ 21\ 23\ 26\ 28\ 30\ 31\ 17\ 20\ 22\ 24\ 25\ 27\ 29\ 32],$$
$$\tilde{\boldsymbol{A}} = \delta_{32}[3\ 4\ 7\ 8\ 11\ 12\ 13\ 14\ 17\ 18\ 21\ 22\ 27\ 28\ 29\ 30\ 1\ 2\ 5\ 6\ 9\ 10\ 15\ 16\ 19\ 20\ 23\ 24\ 25\ 26\ 31\ 32].$$

Using the method of Kronecker product decomposition provided in Remark 2, we can obtain $\boldsymbol{A} = \boldsymbol{L} \otimes \boldsymbol{L}_{\mathrm{u}2}$ and $\tilde{\boldsymbol{A}} = \tilde{\boldsymbol{L}} \otimes \tilde{\boldsymbol{L}}_{\mathrm{u}2}$, where $\boldsymbol{L} = \tilde{\boldsymbol{L}}_{\mathrm{u}2} = \delta_2[1\ 2]$, $\boldsymbol{L}_{\mathrm{u}2} = \delta_{16}[2\ 3\ 5\ 7\ 10\ 12\ 14\ 15\ 1\ 4\ 6\ 8\ 9\ 11\ 13\ 16]$, and $\tilde{\boldsymbol{L}} = \delta_{16}[2\ 4\ 6\ 7\ 9\ 11\ 14\ 15\ 1\ 3\ 5\ 8\ 10\ 12\ 13\ 16]$. Applying Eq. (B10), we easily verify that $\boldsymbol{L}$ and $\tilde{\boldsymbol{L}}$ are indeed the state transition matrices of the NFSR1, respectively, for Types 1 and 2, while $\boldsymbol{L}_{\mathrm{u}2}$ and $\tilde{\boldsymbol{L}}_{\mathrm{u}2}$ are indeed those of NFSR2 with input holding constantly at zero, respectively, for Types 1 and 2 as well. All these validate the result in Theorem 6.

References

1 Golomb S W. Shift Register Sequences. Walnut Creek, CA: Aegean Park Press, 1982
2 Green D H, Dimond K R. Nonlinear product-feedback shift registers. Proc. IEEE, 1970, 117: 681-686
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 Wang Z-X, Qi W-F. On the uniqueness of decomposition of a NFSR into a cascade connection of smaller NFSRs (in Chinese). J. Electron. Inf. Tech., 2014, 36: 1656-1660
5 Cheng D, Qi H, Li Z. Analysis and Control of Boolean Networks. London: Springer-Verlag, 2011
6 Roger A H, Johnson C R. Topics in Matrix Analysis. Cambridge: Cambridge University Press, 1991
7 Zhong J, Lin D. A new linearization method for nonlinear feedback shift registers. J. Comput. Syst. Sci., 2015, 81(4): 783-796
8 Lu J, Li M, Liu Y, et al. Nonsingualrity of Grain-like cascade FSRs via semi-tensor product. Sci. China Inf. Sci., 2018, 61(1): 010204:1-010204:12
9 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. Inf. Theory, 2015, 61(1): 645-654
10 Liu F. New Kronecker product decompositions and its applications. Int. J. Eng. and Sci., 2012, 1(11): 25-30