SCIENCE CHINA
Information Sciences

• LETTER •

March 2019, Vol. 62 039110:1–039110:3
https://doi.org/10.1007/s11432-017-9460-4

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*

Received 15 December 2017/Accepted 26 April 2018/Published online 3 January 2019

Citation Zhong J H, Lin D D. Decomposition of nonlinear feedback shift registers based on Boolean networks. Sci China Inf Sci, 2019, 62(3): 039110, https://doi.org/10.1007/s11432-017-9460-4

Dear editor,

The Boolean network (BN) was introduced by Kauffman [1] to model a genetic network . In such a network, the nodes (genes, proteins, or other molecules) assume only two values, 1 (ON) and 0 (OFF), and the interactions between nodes are determined by Boolean functions. Owing to the complexity of nonlinear logical relations, a convenient tool has been lacking until an algebraic framework was developed by Cheng et al. [2] via a semi-tensor product; further, extensive studies on BNs have been performed in the past decade from the perspective of system and control, e.g., the monography [2].

A nonlinear feedback shift register (NFSR) is a finite automaton and has the same mathematical model as the BN. To assure information security, NFSRs have been used in many stream ciphers. Grain [3], a hardware-oriented finalist in the eSTREAM Stream Cipher Project, uses a cascade connection of a linear feedback shift register (LFSR) into an NFSR. Based on Grain, some new stream ciphers such as Plantlet [4] and Lizard [5] were recently designed. However, unlike Grain and Plantlet, Lizard uses a cascade connection of an NFSR into another NFSR.

NFSRs are generally implemented in the Fibonacci or Galois configuration. Two NFSRs are equivalent if their sets of output sequences are equal [6]. As a particular Galois NFSR, a cascade connection of two NFSRs is equivalent to a Fibonacci NFSR, but it is preferable owing to its potentially shorter propagation time and higher throughput [6]. An NFSR is nonsingular if its state diagram only contains cycles. To avoid state collisions, NFSR-based stream ciphers must use nonsingular NFSRs. A Fibonacci NFSR is nonsingular if and only if its feedback function is nonsingular; but this is not true for a general Galois NFSR [7].

An NFSR is said to be decomposable if it is equivalent to a cascade connection of two NFSRs. Decomposing an NFSR as a cascade connection of an NFSR into an LFSR was studied using the linearity of the LFSR to factorize the characteristic function of the former NFSR [8]. However, the linear methods involved are not applicable to a general cascade connection. As in [8], the decomposition of NFSRs herein means the decomposition of Fibonacci NFSRs.

This study views NFSRs as Boolean networks to address the decomposition of an NFSR into a cascade connection of two NFSRs. It first shows that a cascade connection of two NFSRs is nonsingular if and only if the feedback functions of both NFSRs are nonsingular, which is an easily verifiable condition. It then reduces the decomposition of (nonsingular) NFSRs to the Kronecker product decomposition of (permutation) matrices whose columns are canonical vectors. A new and simple method is proposed to the Kronecker product decomposition of such matrices. This letter also reveals that only two factors affect the decomposition type and indicates that the decomposition is not unique if an NFSR is decomposable.

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

Notations. Let $\mathbb{N}$ denote the set of nonnegative integers, and $\boldsymbol{I}_n$ represent the identity matrix of dimension n. δ_n^i stands for the i-th canonical vector of size n, i.e., the i-th column of $\boldsymbol{I}_n$ with $i \in \{1, 2, \ldots, n\}$. Δ_n denotes the set of all canonical vectors of size n. $\mathcal{L}_{n\times m}$ is the set of $n \times m$ matrices, whose columns belong to Δ_n. If $\boldsymbol{L} \in \mathcal{L}_{n\times m}$, then $\boldsymbol{L} = [\delta_n^{i_1}\ \delta_n^{i_2}\ \cdots\ \delta_n^{i_m}]$. For simplicity, we write $\boldsymbol{L}$ in a compact form, as $\boldsymbol{L} = \delta_n[i_1\ i_2\ \cdots\ i_m]$. $\mathrm{Col}_j(\boldsymbol{A})$ stands for the j-th column of matrix $\boldsymbol{A}$. $\lceil r \rceil$ denotes the smallest integer no less than a real number r. $\oplus$ and $\odot$ are, respectively, the addition and multiplication over the binary field $\mathbb{F}_2$.

Boolean function. A Boolean function f with n variables is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Let i be the decimal number corresponding to the binary $(i_1, i_2, \ldots, i_n)$ via the mapping $i = i_1 2^{n-1} + i_2 2^{n-2} + \cdots + i_n$. Subsequently, i ranges from 0 to $2^n - 1$. Let $f(i) = f(i_1, i_2, \ldots, i_n)$. $[f(2^n - 1), f(2^n - 2), \ldots, f(0)]$ is called the truth table of f, arranged in the reverse alphabet order. The matrix

$$\boldsymbol{F} = \begin{bmatrix} f(2^n-1) & f(2^n-2) & \ldots & f(0) \\ 1-f(2^n-1) & 1-f(2^n-2) & \ldots & 1-f(0) \end{bmatrix}$$

is called the structure matrix of f [2]. $\boldsymbol{f} = [f_1\ \ f_2\ \ \ldots\ \ f_n]^{\mathrm{T}}$ is a vectorial function if its components $f_1, f_2, \ldots, f_n$ are all Boolean functions.

Mathematical model of BNs. A BN with n nodes and m inputs can be described by the following nonlinear system:

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

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

Definition 1 ([2])**.** 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

$$\boldsymbol{A} \ltimes \boldsymbol{B} = \left(\boldsymbol{A} \otimes \boldsymbol{I}_{\frac{\alpha}{m}}\right)\left(\boldsymbol{B} \otimes \boldsymbol{I}_{\frac{\alpha}{p}}\right), \tag{2}$$

where $\otimes$ represents the Kronecker product.

Lemma 1 ([2])**.** Let $\boldsymbol{x} = [X_1\ \ X_1 \oplus 1]^{\mathrm{T}} \ltimes [X_2\ \ X_2 \oplus 1]^{\mathrm{T}} \ltimes \cdots \ltimes [X_n\ \ X_n \oplus 1]^{\mathrm{T}}$ with each $X_i \in \mathbb{F}_2$. Then $\boldsymbol{x} \in \Delta_{2^n}$. Moreover, the state $\boldsymbol{X} = [X_1\ \ X_2\ \ \cdots\ \ X_n]^{\mathrm{T}} \in \mathbb{F}_2^n$ 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 ([2])**.** The nonlinear system (1) describing a BN with inputs can be equivalently expressed as a linear system:

$$\boldsymbol{x}(t+1) = \boldsymbol{L}_{\boldsymbol{u}} \ltimes \boldsymbol{u}(t) \ltimes \boldsymbol{x}(t), \quad t \in \mathbb{N}, \tag{3}$$

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

$$\mathrm{Col}_j(\boldsymbol{L}_{\boldsymbol{u}}) = \mathrm{Col}_j(\boldsymbol{G}_{\mathrm{u}1}) \otimes \cdots \otimes \mathrm{Col}_j(\boldsymbol{G}_{\mathrm{u}n}) \tag{4}$$

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 (1) for any $i \in \{1, 2, \ldots, n\}$.

In (1), if $U(t) \equiv 0$ for any $t \in \mathbb{N}$, which means a BN without input, then its linear system representation (3) is reduced to $\boldsymbol{x}(t+1) = \boldsymbol{L}\boldsymbol{x}(t)$ with state transition matrix $\boldsymbol{L} \in \mathcal{L}_{2^n\times 2^n}$ [2].

NFSRs. Figure 1 describes a cascade connection of an m-stage NFSR1 into an n-stage NFSR2, in which the Boolean functions g and f are, respectively, their feedback functions. Here, NFSR1 is a Fibonacci NFSR, while NFSR2 is an NFSR with a single input, described by the nonlinear system:

$$\begin{cases} X_1(t+1) = X_2(t), \\ \vdots \\ X_{n-1}(t+1) = X_n(t), \\ X_n(t+1) = U_1(t) \oplus f(X_1(t), X_2(t), \ldots, X_n(t)). \end{cases} \tag{5}$$

NFSR1 can be represented by the linear system [9]:

$$\boldsymbol{u}(t+1) = \boldsymbol{L}\boldsymbol{u}(t), \quad t \in \mathbb{N}, \tag{6}$$

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

$$\begin{cases} \mathrm{Col}_{2^{m-1}+j}(\boldsymbol{L}) = \delta_{2^m}^{2j-q_{2^{m-1}+j}}, \\ \mathrm{Col}_j(\boldsymbol{L}) = \delta_{2^m}^{2j-q_j}, \quad j = 1, 2, \ldots, 2^{m-1}, \end{cases} \tag{7}$$

with the truth table $[q_1, q_2, \ldots, q_{2^m}]$ of g, arranged in the reverse alphabet order.

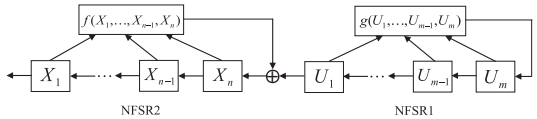

Figure 1 A cascade connection of an m-stage NFSR1 into an n-stage NFSR2.

Let $G = (V, A)$ and $\bar{G} = (\bar{V}, \bar{A})$ be the state diagrams of two n-stage NFSRs, where V and $\bar{V}$ are the sets of their states, while A and $\bar{A}$ are the sets of their edges. G and $\bar{G}$ are said to be isomorphic if there exists a bijection mapping $\varphi : V \to \bar{V}$ such that for any edge $E \in A$ from state $\boldsymbol{X}$ to $\boldsymbol{Y}$, there exists an edge $\bar{E} \in \bar{A}$ from $\varphi(\boldsymbol{X})$ to $\varphi(\boldsymbol{Y})$.

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

$$\boldsymbol{x}(t+1) = \boldsymbol{L}_{\mathrm{u}} \ltimes u_1(t) \ltimes \boldsymbol{x}(t), \quad t \in \mathbb{N}, \tag{8}$$

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

$$\mathrm{Col}_j(\boldsymbol{L}_{\mathrm{u}}) = \delta_{2^n}^{2[(j-1) \bmod 2^{n-1}+1]-s_j} \tag{9}$$

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.

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

$$\bar{\boldsymbol{L}}_c = [\boldsymbol{L}_1 \otimes \boldsymbol{L}_{\rm u1} \ \ \boldsymbol{L}_2 \otimes \boldsymbol{L}_{\rm u2}] \tag{10}$$

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

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

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

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

Define $\mathcal{J}_1 = \{(i-1)2^n + j | i = 1, 2, \ldots, 2^m, j = 1, 2, \ldots, 2^{n-1}\}$ and $\mathcal{J}_2 = \{1, 2, \ldots, 2^{m+n}\} \backslash \mathcal{J}_1$. Let $\mathcal{Q}_{2^n}$ be the set of permutation matrices of dimension 2^n; further, we define two sets as follows:

$$\begin{aligned}\mathcal{P}_{2^{m+n}} = \{&\delta_{2^{m+n}}[i_1 \ i_2 \ \cdots \ i_{2^{m+n}}] \in \mathcal{Q}_{2^{m+n}} | i_k \in \mathcal{J}_1 \\ &\text{and } i_{2^{m+n-1}+k} \in \mathcal{J}_2 \\ &\text{for all } k = 1, 2, \ldots, 2^{m+n-1}\},\end{aligned}$$

$$\begin{aligned}\mathcal{R}_{2^r} = \{&\delta_{2^r}[i_1 \ \ i_2 \ \cdots \ i_{2^r}] \in \mathcal{Q}_{2^r} | i_s, i_{2^{r-1}+s} \\ &\in \{2s-1, 2s\} \text{ for all } s = 1, 2, \ldots, 2^{r-1}\}.\end{aligned}$$

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 the state transition matrix of the Fibonacci NFSR, $[\boldsymbol{L}_1 \ \boldsymbol{L}_2]$ is the 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 the state transition matrix of NFSR2 with $\boldsymbol{L}_{\rm u1}, \boldsymbol{L}_{\rm u2} \in \mathcal{L}_{2^n \times 2^n}$.

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 the state transition matrix of the Fibonacci NFSR, $\boldsymbol{L} \in \mathcal{R}_{2^m}$ is the state transition matrix of NFSR1, $\boldsymbol{L}_{\rm u2} \in \mathcal{R}_{2^n}$ is the state transition matrix of NFSR2 with its input maintained 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 $\boldsymbol{P}_0 = \delta_{2^n}[2^{n-1} + 1 \ \ 2^{n-1} + 2 \ \cdots \ 2^n \ \ 1 \ \ 2 \ \cdots \ 2^{n-1}]$.

Theorems 5 and 6 demonstrate that the decomposition type of a Fibonacci NFSR is only relative to two factors: the stage number decomposition and the state permutation of the Fibonacci NFSR. Even if the stage number decomposition is fixed, different state permutations may result in different decomposition types, which can be easily seen from Property 4 of Lemma 1 in [8]. All these facts demonstrate that the decomposition is not unique if an NFSR is decomposable.

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

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

For more details, please refer to Appendixes A–C.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61772029, 61379139).

Supporting information Appendixes A–C. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Kauffman S A. Metabolic stability and epigenesis in randomly constructed genetic nets. J Theor Biol, 1969, 22: 437–467
2 Cheng D, Qi H, Li Z. Analysis and Control of Boolean Networks. London: Springer-Verlag, 2011
3 Hell M, Johansson T, Meier W. Grain: a stream cipher for constrained environments. Int J Wirel Mobile Comput, 2007, 2: 86–93
4 Mikhalev V, Armknecht F, Müller C. On ciphers that continuously access the non-volatile key. IACR Trans Symmetric Cryptol, 2016, 2016: 52–79
5 Hamann M, Krause M, Meier W. Lizard: a lightweight stream cipher for power-constrained devices. IACR Trans Symmetric Cryptol, 2017, 2017: 45–79
6 Dubrova E. A transformation from the Fibonacci to the Galois NLFSRs. IEEE Trans Inform Theor, 2009, 55: 5263–5271
7 Golomb S W. Shift Register Sequences. Walnut Creek: Aegean Park Press, 1982
8 Ma Z, Qi W F, Tian T. On the decomposition of an NFSR into the cascade connection of an NFSR into an LFSR. J Complex, 2013, 29: 173–181
9 Zhong J, Lin D. A new linearization method for nonlinear feedback shift registers. J Comput Syst Sci, 2015, 81: 783–796