Necessary and Sufficient Conditions for Galois NFSRs Equivalent to Fibonacci Ones and Their Application to the Stream Cipher Trivium

Jianghua Zhong, Yingyin Pan, Wenhui Kong, and Dongdai Lin

Abstract

Many recent stream ciphers use Galois NFSRs as their main building blocks, such as the hardware-oriented finalists Grain and Trivium in the eSTREAM project. Previous work has found some types of Galois NFSRs equivalent to Fibonacci ones, including that used in Grain. Based on the observability of an NFSR on $[0, N-1]$, which means any two initial states of an NFSR are distinguishable from their corresponding output sequences of length N, the paper first presents two easily verifiable necessary and sufficient conditions for Galois NFSRs equivalent to Fibonacci ones. It then validates both conditions by the Galois NFSRs previously found (not) equivalent to Fibonacci ones. As an application, the paper finally reveals that the 288-stage Galois NFSR used in Trivium is neither equivalent to a 288-stage Fibonacci NFSR, nor observable on $[0, 287]$, theoretically verifying Trivium's good design criteria of confusion and diffusion.

Index Terms

Shift register, Boolean function, stream cipher, Trivium, equivalence, observability, Boolean network.

I. Introduction

Nonlinear feedback shift registers (NFSRs) are generally implemented in Fibonacci or Galois configuration. The NFSRs in Fibonacci configuration are called Fibonacci NFSRs, in which the feedback is

The authors are with the State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China. Yingyin Pan and Wenhui Kong are also with the School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China. (e-mail: {zhongjianghua, panyingyin, kongwenhui, ddlin}@iie.ac.cn).

This work was supported by the National Natural Science Foundation of China under Grant Nos. 61772029 and 61872359.

only applied to the last bit. The NFSRs in Galois configuration are called Galois NFSRs, in which the feedback can be applied to every bit. Compared to Fibonacci NFSRs, Galois NFSRs may reduce the depth of circuits implementing their feedback functions, and therefore may improve the throughput [1]. Many recently designed stream ciphers use Galois NFSRs as their main building blocks, such as the hardware-oriented finalists Grain [2] and Trivium [3] in the European eSTREAM project. Grain uses as its main building block a 160-stage Galois NFSR formed by a cascade connection of two Fibonacci NFSRs, while Trivium uses as its main building block a 288-stage Galois NFSR formed by three pairwise controlled Fibonacci NFSRs.

Two NFSRs are said to be equivalent if their sets of output sequences are equal [1]. Studying the equivalence of NFSRs is helpful to select preferable NFSRs according to requirement criteria, such as low cost of hardware implementation, good hardware performance, and high security level. Some work has been done on the equivalence of NFSRs. First, for the equivalence between Galois NFSRs, a Galois NFSR in which the i-th bit feedback function satisfies $f_i(X_1, X_2, \ldots, X_n) = X_{(i+1) \bmod n} \oplus g_i(X_1, \ldots, X_i, X_{i+2}, \ldots, X_n)$ was found equivalent to a class of Galois NFSRs [4]. Second, for the equivalence between Galois and Fibonacci NFSRs, the Galois NFSRs in which the same feedback output can be added to every bit were found equivalent to Fibonacci NFSRs [5]. Cascade connections of two Fibonacci NFSRs were shown equivalent to Fibonacci ones as well [6]. Dubrova disclosed “uniform” Galois NFSRs equivalent to Fibonacci ones [1], and matched their initial states [7]. Recently, “lower triangular” Galois NFSRs [8], nonsingular triangulation-I and triangulation-II Galois NFSRs [9] were also found equivalent to Fibonacci ones. Those are actually some *sufficient* conditions for Galois NFSRs equivalent to Fibonacci ones. Third, some *necessary* conditions were provided for Galois NFSRs equivalent to Fibonacci ones from the perspectives of their stage number and feedback functions [10]. It was disclosed therein that if a Galois NFSR is equivalent to a Fibonacci NFSR, then its stage number is no less than that of the Fibonacci NFSR. In addition, some properties of cascade connections of two Fibonacci NFSRs were revealed from the viewpoint of feedback functions in [11].

An NFSR has the same mathematical model as a Boolean network that evolves as a finite automaton through Boolean functions. As the literature [12]–[15], we apply some concepts and results (especially, those of observability) on Boolean network in the community of systems and control [16] to analyze the cryptographical properties of NFSRs. An NFSR is said to be observable on $[0, N-1]$ if any two initial states of the NFSR can be distinguishable from their corresponding output sequences of length N. Based on the observability of an NFSR on $[0, N-1]$, this paper first presents two easily verifiable necessary and sufficient conditions for Galois NFSRs equivalent to Fibonacci ones. It then uses the Galois NFSRs found (not) equivalent to Fibonacci ones in previous work to validate those conditions. Finally, as an application of those theoretical results, the paper reveals that the 288-stage Galois NFSRs used in the stream cipher Trivium is neither equivalent to a 288-stage Fibonacci NFSR, nor observable on $[0, 287]$, theoretically verifying Trivium's good design criteria of confusion and diffusion.

The remainder of this paper is organized as follows. Section II gives some preliminaries, followed by a brief review of related work on equivalence between Galois and Fibonacci NFSR in Section III. Section IV presents our main results. The paper concludes in Section V.

II. Preliminaries

In this section, we first review some concepts on Boolean functions and matrix products, followed by the representation and observability of Boolean networks. Finally, we recall some related concepts and results on the Galois and Fibonacci NFSRs. Before that, we first introduce some notations used throughout the paper.

Notations: $\mathbb{F}_2$ denotes the binary field, and $\mathbb{F}_2^n$ is an n-dimensional vector space over $\mathbb{F}_2$. $\mathbb{N}$ represents the set of nonnegative integers. Let I_n be the identity matrix of dimension n, and δ_n^i be the i-th column of the matrix I_n with $i \in \{1, 2, \ldots, n\}$, and Δ_n be the set of all columns of the matrix I_n. Denote by $\mathcal{L}_{n\times m}$ the set of $n \times m$ matrices, whose columns belong to Δ_n. If $L \in \mathcal{L}_{n\times m}$, then $L = [\delta_n^{i_1} \ \delta_n^{i_2} \ \cdots \ \delta_n^{i_m}]$. For simplicity, we write L in a compact form, as $L = \delta_n[i_1 \ i_2 \ \cdots \ i_m]$. $\mathrm{Col}_j(A)$ stands for the j-th column of a matrix A. $\otimes$ and $\ltimes$ are, respectively, the Kronecker product and semi-tensor product. $+$, $-$ and $\times$ are the ordinary addition, subtraction and multiplication in the real field, while $\oplus$ and $\odot$ are the addition and multiplication over $\mathbb{F}_2$, respectively.

A. Boolean Function

An n-variable Boolean function f 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 $i = i_1 2^{n-1} + i_2 2^{n-2} + \cdots + i_n$. Then i ranges from 0 to $2^n - 1$. For the simplicity, we denote $f(i) = f(i_1, i_2, \ldots, i_n)$. The matrix

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

is called the *structure matrix* of f [16], [17]. $\mathbf{f} = [f_1 \ \ f_2 \ \ldots \ f_n]^T$ is a *vectorial function* if f_is are Boolean functions for all $i = 1, 2, \ldots, n$.

B. Matrix Product

In this subsection, we review the Kronecker product and semi-tensor product. Both matrix products work for any two matrices.

Definition 2.1 ([18]): Let $A = (a_{ij})$ and B be matrices of dimensions $n \times m$ and $p \times q$, respectively. The *Kronecker product* of A and B, is defined as an $np \times mq$ matrix, given by

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

Definition 2.2 ([19]): For an $n \times m$ matrix A and a $p \times q$ matrix B, let α be the least common multiple of m and p. The *(left) semi-tensor product* of A and B is defined as an $\frac{n\alpha}{m} \times \frac{q\alpha}{p}$ matrix, given by

$$A \ltimes B = (A \otimes I_{\frac{\alpha}{m}})(B \otimes I_{\frac{\alpha}{p}}).$$

Clearly, in Definition 2.2 if $m = p$, then the semi-tensor product $A \ltimes B$ is reduced to the conventional matrix product AB. In fact, the semi-tensor product is a generalization of the conventional matrix product, but it preserves all major properties of the conventional matrix product, such as the associative law and the distributive law [19].

C. Representation of Boolean Networks

A Boolean network can be mathematically modeled by a set of difference equations, called a *system*, via a vectorial function, revealing the relation of its states at time instants t and $t+1$. If each component of the vectorial function is a linear Boolean function, then such a system is called a *linear system*. Otherwise, it is called a *nonlinear system*. In general, a Boolean network with n nodes can be described by the following nonlinear system:

$$\begin{aligned} &\mathbf{X}(t+1) = \mathbf{f}(\mathbf{X}(t)), \\ &\mathbf{Y}(t) = \mathbf{h}(\mathbf{X}(t)),\ t \in \mathbb{N}, \end{aligned} \tag{1}$$

where $\mathbf{X} = [X_1 \ \ X_2 \ \ \ldots \ \ X_n]^T \in \mathbb{F}_2^n$ is the state, and $\mathbf{Y} = [Y_1 \ \ Y_2 \ \ \ldots \ \ Y_m]^T \in \mathbb{F}_2^m$ is the output, the vectorial functions $\mathbf{f}$ and $\mathbf{h}$ are state transition function and output function, respectively.

Lemma 2.3 ([16]): Let $\mathbf{x} = [X_1 \ \ X_1 \oplus 1]^T \ltimes [X_2 \ \ X_2 \oplus 1]^T \ltimes \cdots \ltimes [X_n \ \ X_n \oplus 1]^T$ with $X_i \in \mathbb{F}_2$, $i = 1, 2, \ldots, n$. Then $\mathbf{x} \in \Delta_{2^n}$. Moreover, the state $\mathbf{X} = [X_1 \ \ X_2 \ \ \cdots \ \ X_n]^T \in \mathbb{F}_2^n$ and the state $\mathbf{x} = \delta_{2^n}^j \in \Delta_{2^n}$ with $j = 2^n - (2^{n-1}X_1 + 2^{n-2}X_2 + \cdots + X_n)$ are one-to-one correspondent.

Boolean network (1) can be equivalently expressed as the linear system [16]:

$$\begin{aligned} &\mathbf{x}(t+1) = L\mathbf{x}(t), \\ &\mathbf{y}(t) = H\mathbf{x}(t),\ t \in \mathbb{N}, \end{aligned} \tag{2}$$

where the state $\mathbf{x} \in \Delta_{2^n}$ and the output $\mathbf{y} \in \Delta_{2^m}$, the state transition matrix $L \in \mathcal{L}_{2^n \times 2^n}$, and the output coefficient matrix $H \in \mathcal{L}_{2^m \times 2^n}$. The j-th column of L satisfies

$$\mathrm{Col}_j(L) = \mathrm{Col}_j(F_1) \otimes \mathrm{Col}_j(F_2) \otimes \cdots \otimes \mathrm{Col}_j(F_n),\ j = 1, 2, \ldots, 2^{n+m}, \tag{3}$$

with the structure matrix F_i of the i-th component f_i of the vectorial function $\mathbf{f}$ in (1) for any $i \in \{1, 2, \ldots, n\}$. The j-th column of H can be computed in a similar way.

D. Observability of Boolean Networks

Definition 2.4 ([20]): Two initial states $\mathbf{X}_1$ and $\mathbf{X}_2$ of Boolean network (1) are said to be indistinguishable, if the outputs of the Boolean network starting from the two initial states coincide at every time instant. Otherwise, the two initial states $\mathbf{X}_1$ and $\mathbf{X}_2$ are said to be distinguishable. Boolean network (1) is said to be observable if every two distinct initial states are distinguishable.

The observability of a Boolean network means any two distinct initial states are distinguishable from their corresponding output sequences, or equivalently, the initial state of the Boolean network can be uniquely determined by its output sequence. An NFSR has the same mathematical model as a Boolean network and therefore, it can be viewed as a Boolean network. Reference [21] gave the definition of observability of a feedback shift register from the viewpoint of systems theory, which is in essence the same as the observability definition for a Boolean network. To emphasis the length of an output sequence required to uniquely determine the initial state of a Boolean network, a further definition was given below.

Definition 2.5 ([22]): Two initial states $\mathbf{X}_1$ and $\mathbf{X}_2$ of Boolean network (1) are said to be distinguishable on $[0, N-1]$ if the outputs starting from the two initial states do not coincide at the time instant $t = N-1$. Boolean network (1) is said to be observable on $[0, N-1]$ if any two distinct initial states are distinguishable on $[0, N-1]$

Definition 2.6 ([20], [22]): The observability matrix of Boolean network (1) on $[0, N-1]$ is defined as

$$\mathcal{O}_N = [H^T \ \ (HL)^T \ \cdots \ (HL^{N-1})^T]^T. \tag{4}$$

Lemma 2.7 ([22], [23]): Boolean network (1) is observable on $[0, N-1]$ if and only if the observability matrix $\mathcal{O}_N$ has 2^n distinct columns.

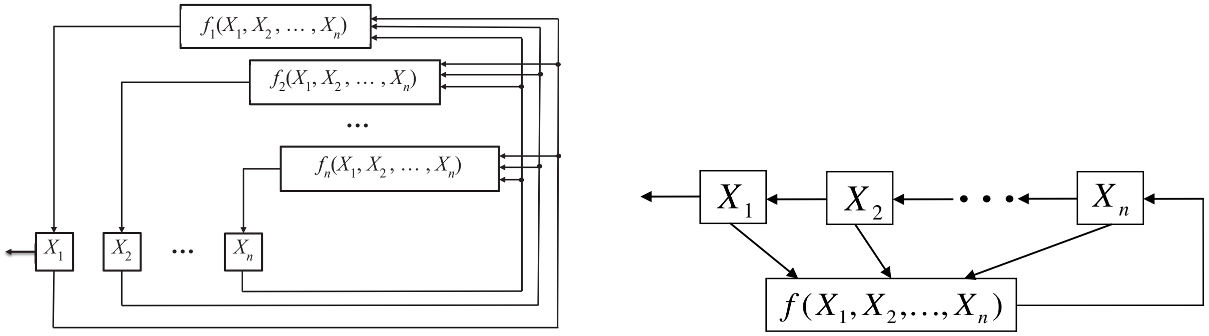
Notably, a Boolean network observable on $[0, N-1]$ means that the initial state of a Boolean network can be uniquely determined by an output sequence of length N.

E. Galois and Fibonacci NFSRs

Fig. 1(a) gives the diagram of an n-stage Galois NFSR, in which each small square represents a binary storage device, also called *bit*. Each i-th bit has a feedback function f_i. All these feedback functions $f_1, f_2, \dots, f_n$ form the feedback $\mathbf{f} = [f_1 \quad f_2 \quad \dots \quad f_n]^T$ of the Galois NFSR. At each periodic interval determined by a master clock, the content of each bit is updated by the value of its feedback function taking at the previous contents of all bits. The n-stage Galois NFSR can be described as the following nonlinear system:

$$\begin{cases} X_1(t+1) = f_1(X_1, X_2, \dots, X_n), \\ X_2(t+1) = f_2(X_1, X_2, \dots, X_n), \\ \vdots \\ X_n(t+1) = f_n(X_1, X_2, \dots, X_n), \end{cases} \tag{5}$$

where $t \in \mathbb{N}$ represents time instant.


$f_1(X_1, X_2, \dots, X_n)$
$f_2(X_1, X_2, \dots, X_n)$
$f_n(X_1, X_2, \dots, X_n)$
X_1
X_2
X_n
X_1
X_2
X_n
$f(X_1, X_2, \dots, X_n)$

(a) An n-stage Galois NFSR.

(b) An n-stage Fibonacci NFSR.

Fig. 1: Galois and Fibonacci NFSRs.

In particular, if there are only shifts between neighbouring bits for the first $n-1$ bits, i.e., $f_i(X_1, X_2, \dots, X_n) = X_{i+1}$ for all $i = 1, 2, \dots, n-1$, then the n-stage Galois NFSR is reduced to an n-stage Fibonacci NFSR. Fig. 1(b) shows the diagram of an n-stage Fibonacci NFSR, in which the Boolean function f is called the *feedback function* of the Fibonacci NFSR. A Fibonacci NFSR is *nonsingular* if and only if its feedback function f is nonsingular, that is, $f(X_1, X_2, \dots, X_n) = X_1 \oplus \tilde{f}(X_1, X_2, \dots, X_n)$ [24]. In the sequel, if there is no special clarification, then an NFSR means it can be a Galois or Fibonacci NFSR.

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 states. An edge from a state $\mathbf{X}$ to a state $\mathbf{Y}$ means that $\mathbf{X}$ is updated to $\mathbf{Y}$.

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 their sets of states, while A and $\bar{A}$ are their sets of 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 $\mathbf{X}$ to state $\mathbf{Y}$, there exists an edge $\bar{E} \in \bar{A}$ from $\varphi(\mathbf{X})$ to $\varphi(\mathbf{Y})$.

Lemma 2.8 ([25]): If an n-stage Fibonacci NFSR and an n-stage Galois NFSR are equivalent, then their state diagrams are isomorphic.

Lemma 2.9 ([10]): An n-stage Galois NFSR represented by System $\mathbf{X}(t+1) = \mathbf{f}(\mathbf{X}(t))$ with state $\mathbf{X} \in \mathbb{F}_2^n$ is equivalent to an n-stage Fibonacci NFSR represented by System $\mathbf{Y}(t+1) = \mathbf{h}(\mathbf{Y}(t))$ with state $\mathbf{Y} \in \mathbb{F}_2^n$, if and only if there exists a bijective mapping $\varphi : \mathbf{X} \mapsto \mathbf{Y}$ such that $\varphi(\mathbf{f}(\mathbf{X})) = \mathbf{h}(\varphi(\mathbf{X}))$ and $[1\ 0\ \cdots\ 0]\varphi(\mathbf{X}) = [1\ 0\ \cdots\ 0]\mathbf{X}$ for all $\mathbf{X} \in \mathbb{F}_2^n$.

III. Related Work

In this section, we review all types of Galois NFSRs previously found equivalent to Fibonacci ones.

Lemma 3.1 ([5]): If an n-stage Galois NFSR with feedback $\mathbf{f} = [f_1\ \ f_2\ \ \dots\ \ f_n]^T$ satisfies

$$\begin{cases} f_i = X_{i+1} \oplus c_i g(X_1, X_2, \dots, X_n), i = 1, 2, \dots, n-1, \\ f_n = g(X_1, X_2, \dots, X_n), \end{cases} \tag{6}$$

where $c_i \in \{0, 1\}$ and g is a Boolean function, then there exists a linear transformation $Q : \mathbf{X} = [X_1\ \ X_2\ \ \dots\ \ X_n]^T \to \mathbf{Y} = [Y_1\ \ Y_2\ \ \dots\ \ Y_n]^T$ such that the Galois NFSR is transformed to an n-stage Fibonacci NFSR, where $\mathbf{X}$ and $\mathbf{Y}$ are the states of the Galois NFSR and its equivalent Fibonacci NFSR, respectively, and Q satisfies

$$Q = \begin{bmatrix} 1 & q_1 & q_2 & \cdots & q_{n-1} \\ 0 & 1 & q_1 & \cdots & q_{n-2} \\ & & \ddots & & \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}. \tag{7}$$

Notably, a Galois NFSR is uniquely determined by its feedback, which updates the state of the Galois NFSR. Then, we can easily see that Equation (6) implies

$$\begin{cases} X_i(t+1) = X_{i+1}(t) \oplus c_i g(X_1(t), X_2(t), \ldots, X_n(t)), i = 1, 2, \ldots, n-1, \\ X_n(t+1) = g(X_1(t), X_2(t), \ldots, X_n(t)), t \in \mathbb{N}, \end{cases} \tag{8}$$

which is actually a nonlinear system representation of the Galois NFSR. Moreover, without special clarification, we always regard an NFSR using the content of the first bit as its output. However, from Equation (7), we can easily see that the Galois NFSR in Lemma 3.1, which uses the content of the *last* bit as its output, is equivalent to a Fibonacci NFSR that also uses the content of the *last* bit as its output.

Lemma 3.2: If an n-stage Galois NFSR with feedback $\mathbf{f} = [f_1 \quad f_2 \quad \ldots \quad f_n]^T$ satisfies one of the following conditions:

1) Cascade connection [6]:

$$\begin{cases} f_i = X_{i+1}, i \neq m, n \text{ with } m < n, \\ f_m = X_{m+1} \oplus g_m(X_1, X_2, \ldots, X_m), \\ f_n = g_n(X_{m+1}, X_{m+2}, \ldots, X_n), \end{cases} \tag{9}$$

2) Uniform Galois NFSR [1]:

$$\begin{cases} f_i = X_{i+1}, i = 1, 2, \ldots, \tau, \\ f_i = X_{i+1 \text{ mod } n} \oplus g_i(X_1, X_2, \ldots, X_{\tau+1}), i = \tau+1, \tau+2, \ldots, n, \end{cases}$$

3) Lower triangular Galois NFSR [8]:

$$\begin{cases} f_i = X_{i+1} \oplus g_i(X_1, X_2, \ldots, X_i), i = 1, 2, \ldots, n-1, \\ f_n = g_n(X_1, X_2, \ldots, X_{\tau+1}), \end{cases}$$

4) Nonsingular triangulation-I Galois NFSR [9]:

$$\begin{cases} f_1 = X_n \oplus g_1(X_1, X_2, \ldots, X_{n-1}), \\ f_i = X_{i-1} \oplus g_i(X_1, X_2, \ldots, X_{i-1}, f_1), i = 2, 3, \ldots, n, \end{cases}$$

5) Nonsingular triangulation-II Galois NFSR [9]:

$$\begin{cases} f_i = X_{i+1} \oplus g_i(X_1, X_2, \ldots, X_i), i = 1, 2, \ldots, n-1, \\ f_n = X_1 \oplus g_n(f_1, f_2, \ldots, f_{n-1}), \end{cases}$$

where g_is are Boolean functions, then the n-stage Galois NFSR is equivalent to an n-stage Fibonacci NFSR.

Among the six types of Galois NFSRs equivalent to Fibonacci ones, listed in Lemmas 3.1 and 3.2, we can easily see that the types of cascade connection and uniform Galois NFSRs are two particular types of lower triangular Galois NFSRs. Reference [9] showed a nonsingular triangulation-I Galois NFSR π-equivalent to the Galois with feedback in Equation (6) if it is nonsingular, while a nonsingular triangulation-II Galois NFSR π-equivalent to a nonsingular uniform Galois NFSR.

IV. Main Results

In this section, we give some necessary and sufficient conditions for Galois NFSRs equivalent to Fibonacci ones, followed by their validations via the Galois NFSRs found equivalent or not equivalent to Fibonacci ones in previous work. Finally, we apply those theoretical results to the stream cipher Trivium.

A. Necessary and Sufficient Conditions

If the initial state of a Fibonacci NFSR is given, then the output sequence is uniquely determined. Notably, whether a Galois NFSR is equivalent to a Fibonacci NFSR depends on their sets of output sequences are equal. Among the previous work on Galois NFSRs found equivalent to Fibonacci ones [1], [5], [6], [8], [9], each equivalent Fibonacci NFSR used the content of the first bit as its output, except that in [5] using the content of the last bit as its output. Actually, if a Fibonacci NFSR uses different bit's content as its output, then its set of output sequences may be different, which can be shown by the following result.

Proposition 4.1: Let $\Omega_i(f)$ be the set of output sequences of the i-th bit of an n-stage Fibonacci NFSR with $i \in \{1, 2, \ldots, n\}$. Then $\Omega_1(f) \supseteq \Omega_2(f) \supseteq \cdots \supseteq \Omega_n(f)$; moreover, the equality holds if and only if the Fibonacci NFSR is nonsingular.

Proof: Let $X_i(t)$ be the content of the i-th bit at time instant t with $i \in \{1, 2, \ldots, n\}$ and $t \in \mathbb{N}$. Thus, $(X_i(t))_{t\geq 0}$ be an output sequence of the i-th bit of the Fibonacci NFSR, and $\Omega_i(f) = \{(X_i(t))_{t\geq 0} | [X_i(0) \;\; X_i(1) \;\; \cdots \;\; X_i(n-1)]^T \in \mathbb{F}_2^n\}$. Notably, for the Fibonacci NFSR, we have $X_i(t+1) = X_{i+1}(t)$ for all $i = 1, 2, \ldots, n-1$ and for all $t \in \mathbb{N}$. Hence, we can easily observe that

$$\Omega_i(f) = \Omega_{i+1}(f) \bigcup \{S_i\}, \; i = 1, 2, \ldots, n-1, \tag{10}$$

where S_i is the output sequence resulted from the initial state $[X_i(0) \;\; X_i(1) \;\; \cdots \;\; X_i(n-1)]^T$. Therefore, we have $\Omega_1(f) \supseteq \Omega_2(f) \supseteq \cdots \supseteq \Omega_n(f)$. The left is to prove that, the equality holds if and only if the Fibonacci NFSR is nonsingular.

If the Fibonacci is nonsingular, then according to the definition of S_i, we can infer that the output sequences S_is are periodic for all $i = 1, 2, \ldots, n-1$; moreover, they have the same period P. Thus,

$X_i(t) = X_i(t+P) = X_{i+1}(t+P-1)$ for all $i = 1, 2, \ldots, n-1$ and for all $t \in \mathbb{N}$. Thereby, for any $i \in \{1, 2, \ldots, n-1\}$, the output sequence S_i can also be resulted from the initial state $[X_{i+1}(P-1) \quad X_{i+1}(P) \quad \cdots \quad X_{i+1}(P+n-2)]^T$, which implies $S_i \in \Omega_{i+1}(f)$. Taking into consideration Equation (10), we have $\Omega_i(f) = \Omega_{i+1}(f)$ for all $i = 1, 2, \ldots, n-1$.

Conversely, assume $\Omega_i(f) = \Omega_{i+1}(f)$ for all $i = 1, 2, \ldots, n-1$. Then from Equation (10), we have $S_i \in G_{i+1}(f)$. According to the foregoing definition of S_i for any $\in \{1, 2, \ldots, n-1\}$, we know $S_i \in G_i(f)$. On one hand, $S_i \in G_i(f)$ implies that S_i is resulted from the initial state $[X_i(0) \quad X_i(1) \quad \cdots \quad X_i(n-1)]^T$. On the other hand, $S_i \in G_{i+1}(f)$ implies that there exists an initial state $[X_{i+1}(t_1-1) \quad X_{i+1}(t_1) \quad \cdots \quad X_{i+1}(t_1+n-2)]^T$ with some positive integer t_1, such that the resulting sequence is S_i. Note that $X_i(t+1) = X_{i+1}(t)$ for all $i = 1, 2, \ldots, n-1$ and for all $t \in \mathbb{N}$. Then, the initial state

$$[X_{i+1}(t_1-1) \quad X_{i+1}(t_1) \quad \cdots \quad X_{i+1}(t_1+n-2)]^T = [X_i(t_1) \quad X_i(t_1) \quad \cdots \quad X_i(t_1+n-1)]^T$$

for all $i = 1, 2, \ldots, n-1$. Thereby, we can deduce that the initial states $[X_i(t_1) \quad X_i(t_1+1) \quad \cdots \quad X_i(t_1+n-1)]^T$ and $[X_i(0) \quad X_i(1) \quad \cdots \quad X_i(n-1]^T$ result in the same output sequence S_i for any $i \in \{1, 2, \ldots, n-1\}$. Hence, the output sequences S_i is periodic, and has period t_1. Note that the initial state $[X_i(0) \quad X_i(1) \quad \cdots \quad X_i(n-1)]^T$ can be arbitrarily selected over $\mathbb{F}_2^n$. Then the output sequence S_i is arbitrary. Thus, we can deduce that all output sequences of the Fibonacci NFSR are periodic. Therefore, the Fibonacci NFSR is nonsingular. □

Corollary 4.2: Let $\Omega_i(f)$ be the set of output sequences of the i-th bit of an n-stage Fibonacci NFSR with $i \in \{1, 2, \ldots, n\}$. Then the cardinality of $\Omega_i(f)$s satisfies $2^n = |\Omega_1(f)| \geq |\Omega_2(f)| \geq \cdots \geq |\Omega_n(f)| \geq 1$; moreover, if the feedback of the Fibonacci NFSR is nonsingular, then $|\Omega_1(f)| = |\Omega_2(f)| = \cdots = |\Omega_n(f)| = 2^n$.

In the sequel, for an n-stage Fibonacci NFSR, we always assume that the $(i+1)$-th bit shifts its content to the i-th bit for all $i = 1, 2, \ldots, n-1$. Moreover, if there is no special clarification,we always assume an NFSR uses the content of the *lowest* bit as its output.

Let $(s_i)_{i\geq 1}$ be an output sequences of an n-stage NFSR. Then $(s_{i+1}, s_{i+2}, ..., s_{i+n})$ for any $i \in \mathbb{N}$ is said to be an *n-tuple* of the sequence $(s_i)_{i\geq 1}$. The output sequences of an n-stage Galois NFSR may not contain all n-tuples. We take a simple example below to illustrate.

Example 4.3: Consider a 3-stage Galois NFSR with feedback $\mathbf{f} = [f_1 \;\; f_2 \;\; f_3]^T$ satisfying

$$\begin{cases} f_1 = X_1X_3 \oplus X_2 \oplus X_3, \\ f_2 = X_1X_2 \oplus X_2X_3 \oplus X_2 \oplus X_3, \\ f_3 = X_2X_3 \oplus X_1 \oplus X_2. \end{cases}$$

Fig. 2 describes its state diagram. We can easily observe that the Galois NFSR can produce an output sequence 1001 of period 4, an output sequence 110 of period 3, and an output sequence 0 of period 1. Clearly, the output sequences of the Galois NFSR contain seven 3-tuples: $(1,0,0),(0,0,1),(0,1,1),(1,1,0),$ $(1,0,1),(0,1,1),(0,0,0)$, but do not contain the 3-tuple $(1,1,1)$.

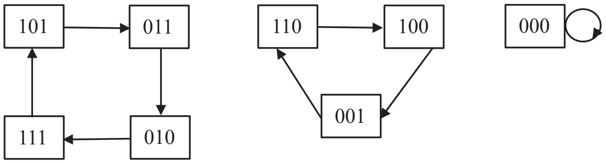


Fig. 2: The state diagram of a 3-stage Galois NFSR.

Proposition 4.4: An n-stage Galois NFSR is equivalent to an m-stage Fibonacci NFSR if and only if the output sequences of the Galois NFSR contain all m-tuples with $m \leq n$, and every m-tuple appears once.

Proof: Sufficiency. Let $(s_i)_{i\geq 1}$ be an output sequence of the n-stage Galois NFSR. Thus, $(s_i)_{i\geq 1}$ is an ultimately periodic sequence. Let k and T, respectively, be preperiod and period of the $(s_i)_{i\geq 1}$, that is, $s_{i+T} = s_i$ for any positive integer $i \geq k$.

The Galois NFSR is equivalent to a Fibonacci NFSR if and only if their sets of output sequences are equal. Let f be the feedback function of an m-stage Fibonacci NFSR. By the output sequence $(s_i)_{i\geq 1}$ of the Galois NFSR, we can determine the value of the feedback function f at the state $[s_{i+1} \;\; s_{i+2} \;\; \cdots \;\; s_{i+n}]^T$ for all $i = 0, 1, \ldots, k+T-1$, precisely, $f(s_{i+1}, s_{i+2}, \ldots, s_{i+m}) = s_{i+m+1}$. The output sequences of the n-stage Galois NFSR contain all m-tuples with $m \leq n$ is equivalent to that, those output sequences totally contain 2^m possible state over $\mathbb{F}_2^m$. Note that every m-tuples appears once. Thus, keeping the above reasoning, we can determine the values of f at 2^m possible states over $\mathbb{F}_2^m$, and simultaneously preserve all these output sequences. Therefore, the feedback function f is determined and thus, the m-stage Fibonacci is determined; moreover, the Fibonacci NFSR and the Galois NFSR have the same set of output sequences.

Necessity. If an n-stage Galois NFSR can be equivalent to an m-stage Fibonacci NFSR, then the Galois NFSR and the Fibonacci NFSR has the same set of output sequences, and therefore they have the same number of output sequences. Since an m-stage Fibonacci NFSR has 2^m output sequences, so has the n-stage Galois NFSR. Different initial states of a Galois NFSR may result in the same output sequence. Thereby, the number of the output sequences of an n-stage Galois NFSR is no greater than 2^n, which implies $2^m \leq 2^n$. Thus, we have $m \leq n$. The m-stage Fibonacci NFSR has 2^m possible states, contained in its output sequences, and each state appears once. As the Galois NFSR and the Fibonacci NFSR have the same set of output sequences, the output sequences of the Galois NFSR contain 2^m possible states over $\mathbb{F}_2^m$ as well, i.e., contain all m-tuples, and every m-tuple appears once. □

Corollary 4.5: An n-stage Galois NFSR can be equivalent to an n-stage Fibonacci NFSR if and only if the output sequences of the Galois NFSR contain all n-tuples.

Proof: Necessity. The result directly follows from the necessity of Proposition 4.4.

Sufficiency. An n-stage Galois NFSR has totally 2^n possible states and thereby, its output sequences at most contain 2^n possible n-tuples. If the output sequences of an n-stage Galois NFSR contain all n-tuples, then every n-tuple must appear once. Thus, according to the sufficiency of Proposition 4.4, the result holds. □.

Lemma 4.6: The output sequences of an n-stage Galois NFSR contain all n-tuples if and only if the n-stage Galois NFSR is observable on $[0, n-1]$.

Proof: Sufficiency. View the Galois NFSR as a Boolean network. Thus, the Galois NFSR can be represented by a linear system:

$$\begin{cases} \mathbf{x}(t+1) = L\mathbf{x}(t), \\ \mathbf{y}(t) = H\mathbf{x}(t),\ t \in \mathbb{N}, \end{cases}$$

where $\mathbf{x}(t) \in \Delta_{2^n}$ is the state, $\mathbf{y} \in \Delta_2$ is the output, $L \in \mathcal{L}_{2^n \times 2^n}$ is the state transition matrix, and $H \in \mathcal{L}_{2 \times 2^n}$ is the output coefficient matrix. Hence, we have

$$\begin{bmatrix} \mathbf{y}(t) \\ \mathbf{y}(t+1) \\ \vdots \\ \mathbf{y}(t+n-1) \end{bmatrix} = \mathcal{O}_n \mathbf{x}(t),\ t \in \mathbb{N}, \tag{11}$$

where $\mathcal{O}_n = [H^T \ \ (HL)^T \ \ldots \ (HL^{n-1})^T]^T$ is the observability matrix. We arbitrarily take $\mathbf{x}(t) = \delta_{2^n}^i$ for some initial instant time instant $t \in \mathbb{N}$ and any $i \in \{1, 2, \ldots, 2^n\}$, then Equation (11) becomes

$$\begin{bmatrix} \mathbf{y}(t) \\ \mathbf{y}(t+1) \\ \vdots \\ \mathbf{y}(t+n-1) \end{bmatrix} = \mathrm{Col}_i(\mathcal{O}_n). \tag{12}$$

If the Boolean network is observable on $[0, n-1]$, then the observability matrix $\mathcal{O}_n$ has 2^n distinct columns, which implies $\mathrm{Col}_i(\mathcal{O}_n)$s in (12) are pairwise distinct for all $i = 1, 2, \ldots, 2^n$. Therefore, from Equation (12), we can infer that the output sequences of the Galois NFSR contain all n-tuples.

Necessity. If the output sequences of the n-stage Galois NFSR contain all n-tuples, then according to Corollary 4.5, the n-stage Galois NFSR is equivalent to an n-stage Fibonacci NFSR. Hence, according to Lemma 2.9, there exists a bijective mapping φ from the states of the Fibonacci NFSR to the states of the Galois NFSR, such that their edges in their state diagrams are one-to-one correspondent. It is known that for any initial state $\mathbf{X}_0$ of the Fibonacci NFSR, there is an output sequence of length n such that it can uniquely determine the initial state $\mathbf{X}_0$ and therefore, can uniquely determine the initial state $\mathbf{Y}_0 = \varphi(\mathbf{X}_0)$ of the Galois NFSR. Since $\mathbf{X}_0$ is arbitrary, so is $\mathbf{Y}_0$. Hence, the n-stage Galois NFSR is observable on $[0, n-1]$. □

Theorem 4.7: The following conditions are equivalent.

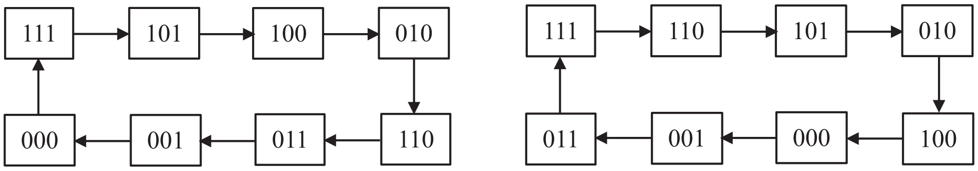
1) An n-stage Galois NFSR can be equivalent to an n-stage Fibonacci NFSR.
2) The output sequences of the n-stage Galois NFSR contain all n-tuples.
3) The n-stage Galois NFSR is observable on $[0, n-1]$.

Proof: The results follow from Corollary 4.5 and Lemma 4.6. □

Example 4.8: Consider a 3-stage Galois NFSR with feedback $\mathbf{f} = [f_1 \ \ f_2 \ \ f_3]^T$ satisfying

$$\begin{cases} f_1 = X_1 \oplus X_3 \oplus 1, \\ f_2 = X_3, \\ f_3 = X_1X_3 \oplus X_1 \oplus X_2 \oplus X_3 \oplus 1. \end{cases}$$

and a 3-stage Fibonacci NFSR with feedback function $f = X_2X_3 \oplus X_1 \oplus X_1 \oplus 1$. Their state diagrams are shown in Fig. 3, from which we can see that each NFSR contains only one cycle in its state diagram, and both NFSRs can generate the same sequence $\mathbf{s} = 11101000$ of period 8. Thereby, they have the same set of output sequences. Hence, the Galois NFSR and the Fibonacci NFSR are equivalent.



(a) State diagram of the 3-stage Galois NFSR.

(b) State diagram of the 3-stage Fiboacci NFSR.

Fig. 3: State diagrams of the Galois and Fibonacci NFSRs in Example 4.8

Clearly, the sequence $\mathbf{s}$ contains all 3-tuples: $(1,1,1),(1,1,0),(1,0,1),(0,1,0),(1,0,0),(0,0,0),(0,0,1),$ $(0,1,1)$. According to Item 2 of Theorem 4.7, the 3-stage Galois NFSR is equivalent to a 3-stage Fibonacci NFSR, consistent with the above equivalent fact. On the other hand, from Lemma 2.3 and the state diagram of the Galois NFSR, we know the successor of the state δ_8^1 (or equivalently, $[1\ 1\ 1]^T$) is the state δ_8^3 (or equivalently, $[1\ 0\ 1]^T$), which implies $\delta_8^3 = L\delta_8^1 = \mathrm{Col}_1(L)$, yielding $\mathrm{Col}_1(L) = \delta_8^3$. Keeping the same reasoning, we can obtain the state transition matrix of the Galois NFSR is $L = \delta_8[3\ \ 5\ \ 4\ \ 6\ \ 7\ \ 2\ \ 8\ \ 1]$. As usual, we use the content of the lowest bit of the Galois NFSR as its output, namely, the output $y(t) = x_1(t),\ t \in \mathbb{N}$. Then, the output coefficient matrix H of the Galois NFSR is just the structure matrix of the Boolean function $h(X_1, X_2, X_3) = X_1$, that is, $H = \delta_2[1\ \ 1\ \ 1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0]$. By direct computation, we can easily get

$$\mathcal{O}_3 = \begin{bmatrix} H \\ HL \\ HL^2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix},$$

which clearly has 8 distinct columns. According to Lemma 2.7, the Galois NFSR is observable on $[0, 2]$. Thus, from Item 3 of Theorem 4.7, the 3-stage Galois NFSR is equivalent to a 3-stage Fibonacci NFSR, consistent with the above fact of equivalence.

Theorem 4.7 converts the equivalence problem of Galois NFSRs into their observability problem, which requires high computational complexity if their stage numbers are large. Nevertheless, based on this conversion, we can obtain two easily verifiable necessary and sufficient conditions for Galois NFSRs equivalent to Fibonacci ones, shown in the sequel.

Theorem 4.9: An n-stage Galois NFSR with state $\mathbf{X} = [X_1\ \ X_2\ \ \cdots\ \ X_n]^T \in \mathbb{F}_2^n$ is equivalent to an n-stage Fibonacci NFSR if and only if there exists a unique bijection $\mathbf{h} = [h_1\ \ h_2\ \ \ldots\ \ h_n]^T$ over $\mathbb{F}_2^n$ such that

$$X_i(t) = h_i(X_1(t), X_1(t+1), \ldots, X_1(t+n-1)) \tag{13}$$

for all $i = 1, 2, \ldots, n$ and for all $t \in \mathbb{N}$.

Proof: Note that we usually use the content of the first bit of an NFSR as its output. Then, for any initial instant $t_0 \in \mathbb{N}$, we can easily see that $\mathbf{X}(t_0) = [X_1(t_0) \;\; X_2(t_0) \;\; \cdots \;\; X_n(t_0)]^T$ is an initial state, and $X_1(t_0), X_1(t_0+1), \ldots, X_1(t_0+n-1)$ is an output sequence of length n of the Galois NFSR.

Sufficiency: If Equation (13) holds for any initial time instant $t_0 \in \mathbb{N}$, then all $X_i(t_0)$s with $i = 1, 2, \ldots, n$ can be uniquely determined by the output sequence $X_1(t_0), X_1(t_0+1), \ldots, X_1(t_0+n-1)$ of length n and therefore, the initial state $\mathbf{X}(t_0)$ is determined. As $\mathbf{h}$ is a bijection, $\mathbf{h}$ is surjective. So we can deduce that any initial state $\mathbf{X}(t_0) \in \mathbb{F}_2^n$ can be uniquely determined by an output sequence $X_1(t_0), X_1(t_0+1), \ldots, X_1(t_0+n-1)$ of length n, which means the Galois NFSR is observable on $[0, n-1]$. According to Theorem 4.7, the n-stage Galois NFSR is equivalent to an n-stage Fibonacci NFSR.

Necessity: If the n-stage Galois NFSR is equivalent to an n-stage Fibonacci NFSR, then the Galois NFSR has the same set of output sequences as the n-stage Fibonacci NFSR, which implies that the Galois NFSR has 2^n output sequences. Moreover, from Theorem 4.7, we know that if the n-stage Galois NFSR is equivalent to an n-stage Fibonacci NFSR, then the Galois NFSR is observable on $[0, n-1]$, which means an output sequence of length n of the Galois NFSR can be uniquely determine its initial state. Thereby, the 2^n initial states of the Galois NFSR and its 2^n output sequences of length n are one-to-one correspondence, and such a correspondence is unique. Hence, there exists a unique bijection $\mathbf{h} = [h_1 \;\; h_2 \;\; \cdots \;\; h_n]^T$ mapping from the 2^n output sequences of length n to the 2^n initial states, that is, $X_i(t_0) = h_i(X_1(t_0), X_1(t_0+1), \ldots, X_1(t_0+n-1))$ for all $i = 1, 2, \ldots, n$ and for any $t_0 \in \mathbb{N}$. Thus, the result follows. □

Remark 4.10: Theorem 4.9 shows that, an n-stage Galois NFSR is equivalent to an n-stage Fibonacci NFSR if and only if there exists a unique bijection $\mathbf{h} = [h_1 \;\; h_2 \;\; \ldots \;\; h_n]^T$ over $\mathbb{F}_2^n$ such that the state at time instant t of the Galois NFSR can be expressed by an n-tuples of successive outputs starting from the time instant t via the bijection $\mathbf{h}$. Moreover, from the proof of Theorem 4.9, we can easily see that Boolean function h_1 satisfies $h_1(X_1(t), X_1(t+1), \ldots, X_1(t+n-1)) = X_1(t)$ for any $t \in \mathbb{N}$, where $(X_1(t), X_1(t+1), \ldots, X_1(t+n-1))$ is the n-tuples of successive outputs staring from time instant t. Hence, to find this unique bijection $\mathbf{h} = [h_1 \;\; h_2 \;\; \ldots \;\; h_n]^T$, we are only required to find the remaining

$n-1$ Boolean functions $h_2, h_3, \ldots, h_n$, which can be derived from the nonlinear system representation

$$\begin{cases} X_1(t+1) = f_1(X_1(t), X_2(t), \ldots, X_n(t)) \\ X_2(t+1) = f_2(X_1(t), X_2(t), \ldots, X_n(t)) \\ \quad\vdots \\ X_n(t+1) = f_n(X_1(t), X_2(t), \ldots, X_n(t)) \end{cases}$$

of the Galois NFSR by equivalent transformations. In other word, we need to solve $n-1$ variables $X_2(t), X_3(t), \ldots, X_n(t)$ from the above n equations by equivalent transformations. Notably, it implies that one equation among the n equations is naturally not used.

Remark 4.11: 1) If the Galois NFSR uses the content of the last bit as its output, then Equation (13) changes to

$$X_i(t) = h_i(X_n(t), X_n(t+1), \ldots, X_n(t+n-1)) \tag{14}$$

for all $i = 1, 2, \ldots, n$ and for all $t \in \mathbb{N}$.

2) Note that a mapping $\mathbf{h} = [h_1 \;\; h_2 \;\; \ldots \;\; h_n]^T$ from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ is bijective, if and and if it is surjective. Hence, to verify $\mathbf{h}$ is bijective, it is enough to prove it is surjective. Precisely, for any $\mathbf{b} = [b_1 \;\; b_2 \;\; \ldots \;\; b_n]^T \in \mathbb{F}_2^n$, we are only required to prove the equation

$$\begin{cases} h_1(X_1, X_2, \ldots, X_n) = b_1 \\ h_2(X_1, X_2, \ldots, X_n) = b_2 \\ \quad\vdots \\ h_n(X_1, X_2, \ldots, X_n) = b_n \end{cases}$$

has a solution $\mathbf{X} = [X_1 \;\; X_2 \;\; \ldots \;\; X_n]^T$ over $\mathbb{F}_2^n$.

Two types of nonsingular Galois NFSRs were found equivalent to Fibonacci ones in [9]. The following result further gives a necessary and sufficient condition for nonsingular Galois NFSRs equivalent to Fibonacci ones.

Theorem 4.12: An n-stage nonsingular Galois NFSR with state $\mathbf{X} = [X_1 \;\; X_2 \;\; \cdots \;\; X_n]^T \in \mathbb{F}_2^n$ is equivalent to an n-stage Fibonacci NFSR if and only if there exists a unique bijection $\varphi = [\varphi_1 \;\; \varphi_2 \;\; \ldots \;\; \varphi_n]^T$ over $\mathbb{F}_2^n$ such that

$$X_i(t) = \varphi_i(X_1(t-n+1), X_1(t-n+2), \ldots, X_1(t)) \tag{15}$$

for all $i = 1, 2, \ldots, n$ and for all positive integer $t \geq n-1$.

Proof: Let the Galois NFSR be represented by a nonlinear system $\mathbf{X}(t+1) = \mathbf{f}(\mathbf{X}(t))$ with $t \in \mathbf{N}$ and the feedback $\mathbf{f} = [f_1 \;\; f_2 \;\; \dots \;\; f_n]^T$. The Galois NFSR is nonsingular if and only if its feedback $\mathbf{f}$ is invertible. Let $\mathbf{f}^{-1}$ be the inverse of $\mathbf{f}$. Then, we have $\mathbf{X}(t) = \mathbf{f}^{-1}(\mathbf{X}(t+1))$.

Sufficiency: If Equation (15) holds, then the output sequence $X_1(t-n+1), X_1(t-n+2), \dots, X_1(t)$ of length n over the time interval $[t-n+1, t]$ can uniquely determine the final state $\mathbf{X}(t) = [X_1(t) \;\; X_2(t) \;\; \dots \;\; X_n(t)]^T$ and therefore, can uniquely determine the initial state $\mathbf{X}(t_0) = [X_1(t_0) \;\; X_2(t_0) \;\; \dots \;\; X_n(t_0)]^T$ with any initial time instant t_0 satisfying $0 \leq t_0 < t$ by the inverse of $\mathbf{f}$, precisely, $\mathbf{X}(t_0) = (\mathbf{f}^{-1})^{t-t_0}\mathbf{X}(t)$. As φ is bijective, φ is surjective. So, any $\mathbf{X}(t) \in \mathbb{F}_2^n$ can be uniquely determined by an output sequence $X_1(t-n+1), X_1(t-n+2), \dots, X_1(t)$ of length n and thereby, any initial state $\mathbf{X}(t_0) \in \mathbb{F}_2^n$ can be uniquely determined by an output sequence of length n as well. It means that the Galois NFSR is observable on $[0, n-1]$. According to Theorem 4.7, the Galois NFSR is equivalent to an n-stage Fibonacci NFSR.

Necessity: If the n-stage Galois NFSR is equivalent to an n-stage Fibonacci NFSR, then from the necessity of Theorem 4.9, we know that there exists a unique bijection $\mathbf{h} = [h_1 \;\; h_2 \;\; \dots \;\; h_n]^T$ such that

$$X_i(t-n+1) = h_i(X_1(t-n+1), X_1(t-n+2), \dots, X_1(t)) \tag{16}$$

for all $i = 1, 2, \dots, n$ and for all positive integer $t \geq n-1$. Let $\mathbf{X}(t-n+1) = [X_1(t-n+1) \;\; X_2(t-n+1) \;\; \dots \;\; X_n(t-n+1)]^T$ and $\mathbf{X}_1(t) = [X_1(t-n+1) \;\; X_1(t-n+2) \;\; \dots \;\; X_1(t)]^T$. Then from Equation (16), we have $\mathbf{X}(t-n+1) = \mathbf{h}(\mathbf{X}_1(t))$ for all positive integer $t \geq n-1$. Thus, $\mathbf{X}_1(t) = \mathbf{h}^{-1}(\mathbf{X}(t-n+1)) = \mathbf{h}^{-1}((\mathbf{f}^{-1})^{n-1}\mathbf{X}(t)) = (\mathbf{h}^{-1}(\mathbf{f}^{-1})^{n-1})(\mathbf{X}(t))$ for all positive integer $t \geq n-1$. It yields $\mathbf{X}(t) = (\mathbf{f}^{n-1}\mathbf{h})(\mathbf{X}_1(t)) = (\mathbf{f}^{n-1}\mathbf{h})(X_1(t-n+1), X_1(t-n+2), \dots, X_1(t))$ for all positive integer $t \geq n-1$. Let $\varphi = \mathbf{f}^{n-1}\mathbf{h}$. As $\mathbf{f}$ is invertible, $\mathbf{f}$ is bijective. Thus, $\varphi = \mathbf{f}^{n-1}\mathbf{h}$ is bijective as well. Therefore, the result follows. □

B. Validating Necessary and Sufficient Conditions

We use the Galois NFSRs previously found equivalent or not equivalent to Fibonacci ones, to validate our necessary and sufficient conditions for Galois NFSRs presented in Theorems 4.9 and 4.12.

In fact, the Galois NFSRs found equivalent to Fibonacci ones in [1], [6], [8], [9] satisfy Equation (13) in Theorem 4.9 or Equation (15) in Theorem 4.12, which can be easily observed by the substitution and elimination of state's components. Precisely speaking, the Galois NFSRs found equivalent to Fibonacci ones in [1], [6], [8] satisfy Equation (13). We simply take the Galois NFSR in [6] as an example. That Galois NFSR is actually a cascade connection of two NFSRs, and the stream cipher Grain just uses such a Galois NFSR as its main building block. From Equation 9 in Lemma 3.2, we can easily see that the Galois NFSR therein can be described by the following nonlinear system:

$$\begin{cases} X_i(t+1) = X_{i+1}(t), i \neq m, n \text{ with } m < n \\ X_m(t+1) = X_{m+1}(t) \oplus g_m(X_1(t), X_2(t), \ldots, X_m(t)), \\ X_n(t+1) = g_n(X_{m+1}(t), X_{m+2}(t), \ldots, X_n(t)), t \in \mathbb{N}. \end{cases}$$

By the substitution and elimination on the above equations, we have

$$\begin{cases} X_1(t) = X_1(t) := h_1(X_1(t)), \;\; t \in \mathbb{N}, \\ X_i(t) = X_1(t+i-1) := h_i(X_1(t+i-1)), \;\; 2 \leq i \leq m, \\ X_{m+1}(t) = X_1(t+m) \oplus g_m(X_1(t), X_1(t+2), \ldots, X_1(t+m-1) \\ \qquad\qquad := h_{m+1}(X_1(t), X_1(t+1), \ldots X_1(t+m)), \\ X_i(t) = X_{m+1}(t+i-m-1) \\ \qquad := h_i(X_1(t+i-m-1), X_1(t+i-m), \ldots X_1(t+i-1)), \;\; m+2 \leq i \leq n, \end{cases}$$

which satisfies Equation (13). Let $\mathbf{h} = [h_1 \;\; h_2 \;\; \ldots \;\; h_n]^T$. Then, for any $\mathbf{b} = [b_1 \;\; b_2 \;\; \ldots \;\; b_n]^T \in \mathbb{F}_2^n$, it is easily seen that the equation $\mathbf{h}(X_1(t), X_1(t+1), \ldots, X_1(t+n-1)) = \mathbf{b}$ has a solution with resect to the unknown vector $[X_1(t) \;\; X_1(t+1) \;\; \ldots \;\; X_1(t+n-1)]^T$ over $\mathbb{F}_2^n$. All these are consistent with the results in Theorem 4.9.

The Galois NFSR considered in [9] has some feedback function f_is appearing in some other feedback function f_is. Actually, if we observe that $f_i(\mathbf{X}(t)) = X_i(t+1)$ for all $i = 1, 2, \ldots, n$, then we can easily see that the nonsingular "Triangular-I" Galois NFSRs found equivalent to Fibonacci ones satisfy Equation (15), while the nonsingular "Triangular-II" Galois NFSRs found equivalent to Fibonacci ones satisfy Equation (13). All these verify Theorems 4.9 and 4.12.

The Galois NFSR considered in [5] uses the content of the last bit as its output, resulting the same set of output sequences as a Fibonacci NFSR with the same stage number, which uses the content of the last bit as its output as well. This can be easily seen from Lemma 3.1 that the linear transformation Q from the Galois NFSR to its equivalent Fibonacci NFSR preserves the last components of their corresponding states. According to Lemma 2.8 and Proposition 4.1, the n-stage Galois NFSR therein is equivalent to an n-stage Fibonacci NFSR that uses the content of the lowest bit as its output if and only if the Galois NFSR is nonsingular. From [9], by a permutation $(n, n-1, \ldots, 1)$, the Galois NFSR therein can be transformed to a new Galois NFSR whose lowest bit is just the last bit of the original one; moreover, if the new Galois NFSR is nonsingular, then it is a particular case of the nonsingular “Triangular-I” Galois NFSR, which satisfies Equation (15) as foregoing mentioned. It validates Theorem 4.12 as well.

Example 4.13: Consider a 4-stage Galois NFSR with feedback $\mathbf{f} = [f_1 \quad f_2 \quad f_3 \quad f_4]^T$ satisfying [1]

$$\begin{cases} f_1 = X_2 \oplus X_1X_2, \\ f_2 = X_3 \oplus X_1 \oplus X_1X_3 \oplus X_1X_2X_3, \\ f_3 = X_4 \oplus X_1 \oplus X_2 \oplus X_3 \oplus X_1X_3 \oplus X_2X_3, \\ f_4 = X_1 \oplus X_2X_4. \end{cases} \tag{17}$$

It was found *not* equivalent to Fibonacci NFSRs [1].

According to Equation (17), we know the Galois NFSR can be represented by a nonlinear system:

$$\begin{cases} X_1(t+1) = X_2(t) \oplus X_1(t)X_2(t), \\ X_2(t+1) = X_3(t) \oplus X_1(t) \oplus X_1(t)X_3(t) \oplus X_1(t)X_2(t)X_3(t), \\ X_3(t+1) = X_4(t) \oplus X_1(t) \oplus X_2(t) \oplus X_3(t) \oplus X_1(t)X_3(t) \oplus X_2(t)X_3(t), \\ X_4(t+1) = X_1(t) \oplus X_2(t)X_4(t). \end{cases} \tag{18}$$

We can easily observe that $X_i(t)$ with $i = 1, 2, 3, 4$, can neither be expressed by $X_1(t), X_1(t+1), X_1(t+2), X_1(t+3)$ for all $t \in \mathbb{N}$, nor be expressed by $X_1(t-3), X_1(t-2), X_1(t-1), X_1(t)$ for all $t \geq 3$, by the computations of substitution and elimination on Equation (18). According to Theorems 4.9 and 4.12, the 3-stage Galois NFSR cannot be equivalent to a 3-stage Fibonacci NFSR, consistent with the fact found in [1].

Remark 4.14: The point of using Theorems 4.9 (or Theorem 4.12) to determine whether an n-stage Galois NFSR (or nonsingular Galois NFSR) is equivalent to an n-stage Fibonacci NFSR, is how to determine whether the bijective mapping in Theorems 4.9 (or Theorem 4.12) exists, and how to find it if it exists. By the above validations, we see that both questions can be answered via the computations of substitute and elimination on the nonlinear system representation of the Galois NFSR.

C. Application to Stream Cipher Trivium

Trivium [3] is the first stream cipher based on confusion and diffusion principles that block cipher designs always use. Trivium uses three pairwise controlled Fibonacci NFSRs. The stage numbers of the three NFSRs are 93, 84, 111. The feedback $\mathbf{f} = [f_1 \quad f_2 \ \dots \ f_{288}]^T$ of the Galois NFSR formed by the three pairwise controlled Fibonacci NFSRs, satisfies the following relation:

$$\begin{cases} f_1 = X_{243} \oplus X_{286}X_{287} \oplus X_{288} \oplus X_{69}, \\ f_{94} = X_{66} \oplus X_{91}X_{92} \oplus X_{93} \oplus X_{171}, \\ f_{178} = X_{162} \oplus X_{175}X_{176} \oplus X_{177} \oplus X_{264}, \\ f_{i+1} = X_i, \;\; i \neq 1, 94, 178, \end{cases}$$

where $\mathbf{X} = [X_1 \;\; X_2 \;\; \ldots \;\; X_{288}]^T$ is the state of the Galois NFSR. Thus, we can easily observe that the Galois NFSR used in Trivium can be described by the nonlinear system:

$$\begin{cases} X_1(t+1) = X_{243}(t) \oplus X_{286}(t)X_{287}(t) \oplus X_{288}(t) \oplus X_{69}(t), \\ X_{94}(t+1) = X_{66}(t) \oplus X_{91}(t)X_{92}(t) \oplus X_{93}(t) \oplus X_{171}(t), \\ X_{178}(t+1) = X_{162}(t) \oplus X_{175}(t)X_{176}(t) \oplus X_{177}(t) \oplus X_{264}(t), \\ X_{i+1}(t+1) = X_i(t), \;\; i \neq 1, 94, 178, \;\; t \in \mathbb{N}. \end{cases} \tag{19}$$

Notably, different to the usual shift occurring from the $(i+1)$-th bit to the i-th bit, the shift in Trivium occurs from the i-th bit to the $(i+1)$-bit, due to its different order of bits. Precisely, in Trivium $X_{i+1}(t) = X_i(t)$ for all $i \neq 1, 94, 178$ and all $t \in \mathbb{N}$. Hence, for the computation ease of substitute and elimination, here we use the content of the 288-th bit as the output of the Galois NFSR to validate. By direct computations of substitution and elimination on Equation (19), we have

$$\begin{cases} X_i(t) = X_{93}(t+93-i), \;\; 1 \leq i \leq 92, \\ X_{93}(t) = X_{177}(t+84) \oplus X_{93}(t+2)X_{93}(t+1) \oplus X_{177}(t+6), \\ X_i(t) = X_{177}(t+177-i), \;\; 94 \leq i \leq 176, \\ X_{177}(t) = X_{288}(t+111) \oplus X_{177}(t+15) \oplus X_{177}(t+2)X_{177}(t+1) \oplus X_{288}(t+24), \\ X_i(t) = X_{288}(t+288-i), \;\; 178 \leq i \leq 287, \; t \in \mathbb{N}. \end{cases} \tag{20}$$

Clearly, $X_i(t) = X_{288}(t+288-i)$ for all $i = 178, 179, \ldots, 287$ and for all $t \in \mathbb{N}$. However, the variables $X_i(t)$ are relative to the variables $X_{177}(t+177-i)$ for all $i = 94, 95, \ldots, 176$ and for all $t \in \mathbb{N}$. In the following, we mainly concern the variable X_{177}. Note that each variable X_i with $i \in \{1, 2, \ldots, 288\}$ appears in some feedback function f_j only once. Then, we can easily see that $X_{177}(t)$ only appears at the right-hand side of the third equation of (19), and $X_{177}(t+1)$ only appears at the left-hand side of the fourth equation of (19). Hence, $X_{177}(t)$ can be derived only from either of the above two equations by equivalent transformations.

For the former case, from the fourth equation of (20), we can see that $X_{177}(t)$ cannot expressed by $X_{288}(t), X_{288}(t+1), \ldots, X_{288}(t+287)$. For the latter case, we have $X_{177}(t) = X_{176}(t-1)$. However, in this case, we discard the third equation of $X_{178}(t+1)$ in (19) and use the other 177 equations to derive the 177 variables $X_i(t)$ with $i = 1, 2, \ldots, 177$. Again, we note each variable X_i with $i \in \{1, 2, \ldots, 288\}$ appearing in some feedback function f_j only once. Then, from Equation(19), we have $X_{i+1}(t) = X_i(t-1)$ for all i satisfying $94 \leq i \leq 176$ and $1 \leq i \leq 92$, while $X_{94}(t) = X_{66}(t-1) \oplus X_{91}(t-1)X_{92}(t-1) \oplus X_{93}(t-1) \oplus X_{171}(t-1)$. Hence, summarizing the above equations for the latter case, we can conclude that $X_{177}(t)$ is relative to the variables $X_1, X_2, \ldots, X_{176}$, for which $X_1(t), X_2(t), \ldots, X_{176}(t)$ cannot be expressed by $X_{288}(t), X_{288}(t+1), \ldots, X_{288}(t+287)$ and therefore, $X_{177}(t)$ cannot be expressed by $X_{288}(t), X_{288}(t+1), \ldots, X_{288}(t+287)$ either for the latter case.

Summarizing the above cases, we know that $X_{177}(t)$ cannot be expressed by $X_{288}(t), X_{288}(t+1), \ldots, X_{288}(t+287)$. According to Item 1 of Remark 4.11, the Galois NFSR used in the stream cipher Trivium cannot be equivalent to a 288-stage Fibonacci NFSR. Thus, from Theorem 4.7, Trivium is not observable on $[0, 287]$, which means the initial state of Trivium cannot be uniquely determined by an output sequence of length 288, theoretically verifying its good design criteria of confusion and diffusion.

V. Conclusion

Based on the observability of an NFSR, the paper gave two easily verifiable necessary and sufficient conditions for Galois NFSRs equivalent to Fibonacci ones, covering and improving the previous results on this research. As an application of those theoretical results, the paper revealed that the 288-stage Galois NFSR used in the stream cipher Trivium is neither equivalent to a 288-stage Fibonacci NFSR, nor observable on $[0, 287]$, theoretically verifying Trivium's good design criterion of confusion and diffusion. In the future, it is interesting to use our necessary and sufficient conditions to find more types of Galois NFSRs equivalent to Fibonacci ones, and to find more types of Galois NFSRs not equivalent to Fibonacci ones but having other good cryptographical properties.

References

[1] E. Dubrova, "A transformation from the Fibonacci to the Galois NLFSRs," *IEEE Trans. Information Theory*, vol. 55, no. 11, pp. 5263-5271, Nov. 2009.

[2] M. Hell, T. Johansson, and W. Meier, "Grain-a stream cipher for constrained environments," eSTREAM, ECRYPT Stream Cipher Project, London, U.K., Tech. Rep. 2005/010, 2005.

[3] C. De Cannière and B. Preneel, "Trivium Specifications," eSTREAM, ECRYPT Stream Cipher Project, London, U.K., Tech. Rep. 2005/030, 2005.

[4] E. Dubrova, “An equivalence-preserving tranformation of shift register,” in *Proceedings of Squences and Their Applications (SETA 2014)*, eds. K.-U. Schmidt and A. Winterhof, LNCS 8865, 2014, pp. 187-199.

[5] J. L. Massey and R. W. Liu, Equivalence of nonlinear shift-register, IEEE Press, 10(4) (1964) 378-379.

[6] J. Mykkeltveit, M.-K. Siu, and P. Ton, “On the cylcle structure of some nonlinear shift register sequences,” *Information and Control*, vol. 43, pp. 202-215, 1979.

[7] E. Dubrova E, “Finding matching initial states for equivalent NLFSRs in the Fibonacci and the Galois configurations,” *IEEE Trans. Inf. Theory*, vol. 56, no. 6, pp. 2961-2966, 2010.

[8] Z. Lin, “The transformation from the Galois NLFSR to the Fibonacci Configuration,” *2013 Fourth International Conference on Emerging Intelligent Data and Web Technologies*, Xi’an, China, Sept. 2013, pp. 335-339.

[9] X.-X. Zhao, W.-F. Qi, and J.-M. Zhang, “Further results on the equivalence between Galois NFSRs and Fibonacci NFSRs,” *Designs, Codes and Cryptography*, vol. 88, no. 1, pp. 153-171, 2020.

[10] J. Zhong, Y. Pan and D. Lin, “On Galois NFSRs equivalent to Fibonacci ones,” *The 16th International Conference on Information Security and Cryptology (Inscrypt 2020)*, Guangzhou, China, Dec. 11-14, 2020.

[11] J. Zhong, “On equivalence of cascade connections of two nonlinear feedback shift registers,” *The Computer Journal*, vol. 62, no. 12, pp. 1793-1804, 2019.

[12] D. Zhao, H. Peng, L. Li, S. Hui, and Y. Yang, “Novel way to research nonlinear feedback shift register,” *Science China Information Sciences*, vol. 57, no. 9, pp. 1-14, Sept. 2014.

[13] J. Zhong and D. Lin, “A new linearization method of nonlinear feedback shift registers,” *J. Comput. Syst. Sci.*, vol. 81, no. 4, pp. 783-796, 2015.

[14] J. Zhong and D. Lin, “Driven stability of nonlinear feedback shift registers,” *IEEE Trans. Communications*, vol. 64, no. 6, pp. 2274-2284, Jun. 2016.

[15] J. Zhong and D. Lin, “On minimum period of nonlinear feedback shift registers in Grain-like structure,” *IEEE Trans. Inf. Theory*, vol. 64, no. 99, pp. 6429-6442, 2018.

[16] D. Cheng, H. Qi, and Z. Li, *Analysis and Control of Boolean Networks*, London, U. K.: Springer-Verlag, 2011.

[17] H. Qi and D. Cheng, “Logic and logic-based control,” *J. Contr. Theory Appl.*, vol. 6, no. 1, pp. 123-133, Jan. 2008.

[18] A. H. Roger and C. R. Johnson, *Topics in Matrix Analysis*, U.K.: Cambridge University Press, 1991.

[19] D. Cheng, H. Qi, and Y. Zhao, *An Introduction To Semi-Tensor Product of Matrices And Its Applications*, World Scientific Publishing Company, Singapore, 2012.

[20] E. Fornasini and M. E. Valche, “Observability, reconstructibility and state observers of Boolean control networks,” *IEEE Trans. Automat. Control*, vol. 58, no. 6, pp. 1390-1401, 2013.

[21] N. Kalouptsidis and K. Limniotis, “Nonlinear span, minimal realizations of sequences over finite fields and de Brujin generators,” *International Symposium on Information Theory and its Applications, ISITA 2004*, IEEE Press, Piscataway, NJ, USA, 2004, pp. 794-799.

[22] D. Cheng and H. Hong, “Controllability and observability of Boolean control networks,” *Automatica*, vol. 45, no. 7, pp. 1657-1667, 2009.

[23] Y. Guo, W. Gui, and C. Yang, “Redefined observability matrix for Boolean networks and distinguishable partitions of state spaces,” *Automatica*, vol. 91, pp. 316-319, 2018.

[24] S. W. Golomb, *Shift Register Sequences*, Holden-Day, Laguna Hills, CA, USA, 1967.

[25] J. Zhong and D. Lin, “Decomposition of nonlinear feedback shift registers based on Boolean networks,” *Science China Information Sciences*, vol. 62, no. 3, pp. 39110:1-39110:3, 2019.