On the Nonsingularity and Equivalence of NFSRs

Yingyin Pan[1 2], Jianghua Zhong[1 ✉], and Dongdai Lin [1]

Abstract

Nonlinear feedback shift registers (NFSRs) are used in many stream ciphers as their main building blocks. In particular, Galois NFSRs with terminal bits are used in the typical stream ciphers Grain and Trivium. One security criterion for the design of stream ciphers is to assure their used NFSRs are nonsingular. The nonsingularity is well solved for Fibonacci NFSRs, whereas it is not for Galois NFSRs. In addition, some types of Galois NFSRs equivalent to Fibonacci ones have been found. However, whether there exist new types of such Galois NFSRs remains unknown. The paper first considers the nonsingularity of Galois NFSRs. Some necessary/sufficient conditions are presented. The paper then concentrates on the equivalence between Galois NFSRs and Fibonacci ones. Some necessary conditions for Galois NFSRs equivalent to Fibonacci ones are provided. The Galois NFSRs with terminal bits equivalent to a given Fibonacci one are enumerated. Moreover, two classes of nonsingular Galois NFSRs with terminal bits are found to be the new types of Galois NFSRs equivalent to Fibonacci ones.

keywords Nonlinear feedback shift register, Stream cipher, Boolean function, Nonsingularity, Equivalence

Yingyin Pan
panyingyin@iie.ac.cn
Jianghua Zhong
zhongjianghua@iie.ac.cn
Dongdai Lin
ddlin@iie.ac.cn

1 State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
2 School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

This paper was presented in part at the 2021 IEEE International Symposium on Information Theory (ISIT 2021).

1 Introduction

Our society greatly depends on security of information. To protect the confidential information from unauthorized or accidental disclosure, cryptographic methods are applied. Stream cipher is a one-time pad approach, and has been widely used in communication, diplomacy, military and other fields, due to its efficient encryption and decryption, simple hardware implementation and low error-propagation rate. In many recent stream ciphers, such as the finalists Grain [1] and Trivium [2] in the eSTREAM project, and the finalist Acorn [3] in the CAESAR competition, nonlinear feedback shift registers (NFSRs) have been used as their main building blocks.

An NFSR can be generally implemented in Fibonacci or Galois configuration. In Fibonacci configuration, the NFSR's feedback is only applied to the last bit, while in the Galois configuration, the feedback can be applied to every bit. Compared with Fibonacci NFSRs, Galois ones may decrease the propagation time and increase the throughput [4]. Notably, the foregoing stream ciphers use Galois NFSRs as their main building blocks. More precisely, they use Galois NFSRs with terminal bits, which have the first several bits involved only shifts, as their building blocks.

An NFSR is nonsingular if every state has one unique predecessor, which means that the NFSR's state diagram consists of only pure cycles without branches, or equivalently, all sequences generated by the NFSR are periodic. One security criterion in the design of NFSR-based stream ciphers is to assure their used NFSRs are nonsingular. If an NFSR is singular, then there must exist two different states producing the same successor, and hence, equivalent secret keys probably exist. Thus, it might encounter weak attacks [5]. So far, some work has been done on the nonsingularity of NFSRs. A Fibonacci NFSR is nonsingular if and only if its feedback function is nonsingular [6]. As a particular Galois NFSR, a cascade connection of two Fibonacci NFSR is nonsingular if and only if the feedback functions of both Fibonacci NFSRs are nonsingular [7]. However, all nonsingular feedback functions cannot guarantee a general Galois NFSR to be nonsingular. In [8], it stated that all feedback functions of an n-stage Galois NFSR satisfy $f_i = X_{i+1} \oplus g_i(X_1, X_2, \ldots, X_i, X_{i+2}, \ldots, X_n)$ with $i = 1, 2, \ldots, n$ is a necessary condition for the nonsingularity of Galois NFSR. Compared to the well-solved nonsingularity of Fibonacci NFSRs, the nonsingularity of Galois NFSRs is far from being understood.

Two NFSRs are said to be equivalent if their sets of output sequences are equal [4]. Studying the equivalence of NFSRs is helpful to select preferable ones in the design of NFSR-based stream ciphers according to requirement criteria, such as low cost of hardware implementation, good hardware performance, and high security level. So far, 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 $f_i(X_1, X_2, \ldots, X_n) = X_{(i+1) \ mod \ n} \oplus g_i(X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n)$ was found equivalent to a class of Galois NFSRs [8]. In addition, as particular Galois NFSRs, cascade connections of two NFSRs were characterized from the perspectives of feedback functions if they are equivalent [9]. Second, for the equivalence between Galois NFSRs and Fibonacci ones, it was found that any given Fibonacci NFSR can be equivalent to uniform Galois one with the same stage number [4], and their initial states were matched [10]; moreover, lower triangular Galois NFSRs [11] and cascade connections of two NFSRs [12] were revealed equivalent to Fibonacci NFSRs. Meanwhile, it discovered a new type of Galois NFSRs (called Type-IV, therein) that can be transformed to Fibonacci NFSRs [13]. In fact, these are some sufficient conditions for Galois NFSRs equivalent to Fibonacci ones.

The paper first considers the nonsingularity of Galois NFSRs. Some necessary/sufficient conditions are presented. The paper then concentrates on the equivalence between Galois NFSRs and Fibonacci ones. It gives some necessary conditions for Galois NFSRs that are equivalent to Fibonacci ones, from the perspectives of their feedback functions. It also enumerates the Galois NFSRs with terminal bits equivalent to a given Fibonacci one with the same stage number. Moreover, it discloses two new types of nonsingular Galois NFSRs with terminal bits that are equivalent to Fibonacci NFSRs. All of these are helpful to the design of NFSR-based stream ciphers.

The reminder of this paper is organized as follows. Sction 2 introduces some preliminaries on NFSRs. Section 3 reviews some previous work on the equivalence of NFSRs. Section 4 presents our results on the nonsingularity of NFSRs, followed by those on the equivalence in Section 5. The paper concludes in Section 6.

2 Nonlinear Feedback Shift Registers

In this section, we review some basic concepts and related results on 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. $+$, $-$ 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.

Galois and Fibonacci NFSRs: Figure 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 $f_1, f_2, \ldots, f_n$ form the feedback $F = [f_1 \;\; f_2 \;\; \ldots \;\; f_n]^T$ 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 at the previous contents of all bits. The n-stage Galois NFSR can be described as the following set of difference equations, also called *nonlinear system*:

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

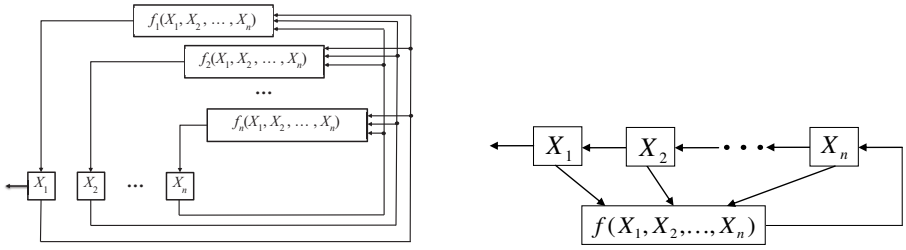
or equivalently described by a system of vector form as:

$$\mathbf{X}(t+1) = F(\mathbf{X}(t)), \tag{2}$$

where $\mathbf{X} = [X_1 \;\; X_2 \;\; \ldots \;\; X_n]^T \in \mathbb{F}_2^n$ is the state of the Galois NFSR, the feedback F is also called *state transition function*, and $t \in \mathbb{N}$ represents time instant. Throughout the paper, without specification, the content of the lowest bit is always used as the output of the Galois NFSR.

In particular, if there are only shifts between the first $n-1$ neighboring bits, that is, $f_i(X_1, X_2, \ldots, X_n) = X_{i+1}$ for all $i = 1, 2, \ldots, n-1$, then the n-stage Galois NFSR is reduced to an n-stage Fibonacci NFSR, whose diagram is shown in Figure 1(b), in which the Boolean function f is called *feedback function* of the Fibonacci NFSR.

State Diagram of NFSRs: 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



(a) An n-stage Galois NFSR. (b) An n-stage Fibonacci NFSR.

Figure 1: Galois and Fibonacci NFSRs.

each edge represents a transition between states. An edge from state $\mathbf{X}$ to state $\mathbf{Y}$ means that the state $\mathbf{X}$ is updated to the state $\mathbf{Y}$. $\mathbf{X}$ is called a *predecessor* of $\mathbf{Y}$, and $\mathbf{Y}$ is called the *successor* of $\mathbf{X}$. A sequence of p distinct states, $\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_p$, is called a *cycle of length* p if $\mathbf{X}_1$ is the successor of $\mathbf{X}_p$, and $\mathbf{X}_{i+1}$ is a successor of $\mathbf{X}_i$ for any $i \in \{1, 2, \ldots, p-1\}$.

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 1 ([7]) *If an n-stage Fibonacci NFSR and an n-stage Galois NFSR are equivalent, then their state diagrams are isomorphic.*

Definition 1 ([14]) *Suppose F and F_π to be the feedback of two n-stage Galois NFSRs. Let $F(\mathbf{X}) = [f_1(X_1, \ldots, X_n)\ f_2(X_1, \ldots, X_n)\ \ldots\ f_n(X_1, \ldots, X_n)]^T$ and let π be a permutation of $\{1, 2, \ldots, n\}$. The Galois NFSR with feedback F_π is said to be π-equivalent to the Galois NFSR with feedback F if $F_\pi(\mathbf{X}) = [f_{\pi(1)}(X_{\pi(1)}, \ldots, X_{\pi(n)})\ f_{\pi(2)}(X_{\pi(1)}, \ldots, X_{\pi(n)}) \cdots f_{\pi(n)}\ (X_{\pi(1)}, \ldots, X_{\pi(n)})]^T$.*

Definition 2 *Given a positive integer τ satisfying $1 \leq \tau \leq n-1$, an n-stage Galois NFSR with feedback $F = [f_1\ \ f_2\ \ \ldots\ \ f_n]^T$ is said to have the terminal bit τ if $f_i(\mathbf{X}) = X_{i+1}$ for all $i = 1, 2, \ldots, \tau$ and for all $\mathbf{X} = [X_1\ \ X_2\ \ \ldots\ \ X_n]^T \in \mathbb{F}_2^n$. Such an NFSR with terminal bit τ is called an n-stage τ-terminal-bit Galois NFSR.*

Notably, if an n-stage Galois NFSR has the terminal bit $n-1$, then it is reduced to an n-stage Fibonacci NFSR.

3 Previous Work

In this section, we review some previous work regarding the equivalence of NFSRs since they are necessary for the discussion in Section 5.

Lemma 2 ([4]) *For an n-stage Galois NFSR with state $\mathbf{X} = [X_1 \ X_2 \ \dots \ X_n]^T$ and feedback $F(\mathbf{X}) = [f_1(\mathbf{X}) \ f_2(\mathbf{X}) \ \dots \ f_n(\mathbf{X})]^T$, if there exists a recurrence relation of order n describing each output sequence of the i-th bit X_i with some $i \in \{1, 2, \dots, n\}$, then the set of output sequences of the i-th bit of the Galois NFSR is a subset of the set of output sequences of an n-stage Fibonacci NFSR.*

Lemma 3 ([14]) *For an n-stage nonsingular Galois NFSR with state $\mathbf{X} = [X_1 \ X_2 \ \cdots \ X_n]^T$, if it uses the content of the i-th bit as its output, and there exists a recurrence relation of order n describing each output sequence of the i-th bit X_i with some $i \in \{1, 2, \dots, n\}$, then this n-stage nonsingular Galois NFSR is equivalent to an n-stage Fibonacci NFSR.*

Lemma 4 ([15]) *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 $\mathbf{h} = [h_1 \ h_2 \ \cdots \ h_n]^T$ over $\mathbb{F}_2^n$ such that*

$$X_i(t) = h_i(X_1(t), X_1(t+1), \dots, X_1(t+n-1)) \tag{3}$$

for all $i = 1, 2, \dots, n$ and for all $t \in \mathbb{N}$; moreover $h_1(X_1(t), X_1(t+1), \dots, X_1(t+n-1)) = X_1(t)$ for all $t \in \mathbb{N}$.

Lemma 5 *If an n-stage Galois NFSR with feedback $F = [f_1 \ f_2 \ \cdots \ f_n]^T$ satisfies one of the following conditions:*

1) Cascade connection [16]:

$$\begin{cases} f_i = X_{i+1}, \ i \neq m, n \text{ with } m < n, \\ f_m = X_{m+1} \oplus g_m(X_1, X_2, \dots, X_m), \\ f_n = g_n(X_{m+1}, X_{m+2}, \dots, X_n), \end{cases} \tag{4}$$

2) Uniform Galois NFSR [4]:

$$\begin{cases} f_i = X_{i+1}, \ i = 1, 2, \dots, \tau, \\ f_i = X_{(i+1) \bmod n} \oplus g_i(X_1, X_2, \dots, X_{\tau+1}), \ i = \tau+1, \tau+2, \dots, n, \end{cases} \tag{5}$$

3) Lower triangular Galois NFSR [11]:

$$\begin{cases} f_i = X_{i+1} \oplus g_i(X_1, X_2, \ldots, X_i), \ i = 1, 2, \ldots, n-1, \\ f_n = g_n(X_1, X_2, \ldots, X_n), \end{cases} \tag{6}$$

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

Clearly, cascade connections and uniform Galois NFSR are two particular types of lower triangular Galois NFSRs.

4 Nonsingularity of NFSRs

In this section, we give some necessary/sufficient conditions for the nonsingualarity of Galois NFSRs.

Theorem 1 *Suppose τ to be a positive integer satisfying $1 \leq \tau \leq n-1$. An n-stage τ-terminal-bit Galois NFSR is nonsingular, if its feedback $F = [f_1 \ \ f_2 \ \ \ldots \ \ f_n]^T$ satisfies*

$$\begin{cases} f_i = X_{i+1}, i = 1, 2, \ \ \ldots, \tau, \\ f_i = X_{j_i} \oplus g_i(X_2, \ldots, X_{\tau+1}, X_{j_{\tau+1}}, \ldots, X_{j_{i-1}}, h_n), \ i = \tau+1, \ldots, n-1, \\ f_n = h_n \oplus g_n(X_2, \ldots, X_{\tau+1}), \end{cases} \tag{7}$$

where $h_n = X_{j_n} \oplus \widetilde{g}_n(X_2, \ldots, X_{\tau+1}, X_{j_{\tau+1}}, X_{j_{\tau+2}}, \ldots, X_{j_{n-1}})$, $\{X_{j_{\tau+1}}, X_{j_{\tau+2}}, \ldots, X_{j_n}\} = \{X_1, X_{\tau+2}, \ldots, X_n\}$, or the feedback $F = [\widetilde{f}_1 \ \ \widetilde{f}_2 \ \ \ldots \ \ \widetilde{f}_n]^T$ satisfies

$$\begin{cases} \widetilde{f}_i = X_{i+1}, i = 1, 2, \ \ \ldots, \tau \\ \widetilde{f}_i = f_{\rho(i)}(\mathbf{X}), \ i = \tau+1, \tau+2, \ldots, n, \end{cases} \tag{8}$$

where ρ is a permutation of $\{\tau+1, \tau+2, \ldots, n\}$.

Proof. A Galois NFSR is nonsingular, if and only if its feedback F is bijection. Hence, we only need to prove that for any $\mathbf{a} = [a_1 \ \ a_2 \ \ \ldots \ \ a_n]^T \in \mathbb{F}_2^n$, the equation $F(X_1, X_2, \ldots, X_n) = \mathbf{a}$ has a unique solution $[X_1 \ \ X_2 \ \ \ldots \ \ X_n]^T \in \mathbb{F}_2^n$.

Consider the solution of the following system derived from Equation (7) by setting $f_i = a_i$ for all $i = 1, 2, \ldots, n$:

$$\begin{cases} a_1 = X_2, \\ \quad \vdots \\ a_\tau = X_{\tau+1}, \\ a_{\tau+1} = X_{j_{\tau+1}} \oplus g_{\tau+1}(X_2, \ldots, X_{\tau+1}, h_n), \\ a_{\tau+2} = X_{j_{\tau+2}} \oplus g_{\tau+2}(X_2, \ldots, X_{\tau+1}, X_{j_{\tau+1}}, h_n), \\ \quad \vdots \\ a_{n-1} = X_{j_{n-1}} \oplus g_{n-1}(X_2, \ldots, X_{\tau+1}, X_{j_{\tau+1}}, \ldots, X_{j_{n-2}}, h_n), \\ a_n = h_n \oplus g_n(X_2, \ldots, X_{\tau+1}). \end{cases} \tag{9}$$

First, it can be seen that X_is for $2 \leq i \leq \tau+1$ are determined by the first τ equations. Then, we can determine the value of $g_n(X_2, \ldots, X_{\tau+1})$, denoted by c_n. Therefore, according to the last equation of (9), we have $h_n = a_n \oplus c_n$. Substituting h_n and X_i with $2 \leq i \leq \tau+1$ to the equations from the $(\tau+1)$-th to the $(n-1)$-th of Equation (9), we have

$$\begin{cases} a_{\tau+1} = X_{j_{\tau+1}} \oplus g_{\tau+1}(X_2, \ldots, X_{\tau+1}, a_n \oplus c_n), \\ a_{\tau+2} = X_{j_{\tau+2}} \oplus g_{\tau+2}(X_2, \ldots, X_{\tau+1}, X_{j_{\tau+1}}, a_n \oplus c_n), \\ \quad \vdots \\ a_{n-1} = X_{j_{n-1}} \oplus g_{n-1}(X_2, \ldots, X_{\tau+1}, X_{j_{\tau+1}}, \ldots, X_{j_{n-2}}, a_n \oplus c_n), \\ a_n = h_n \oplus g_n(X_2, \ldots, X_{\tau+1}). \end{cases} \tag{10}$$

Based on this, $X_{j_{\tau+1}}$ is determined by the $(\tau+1)$-th equation. Continuing this process, we see that each X_{j_i} with $i \in \{\tau+1, \ldots, n-1\}$ is determined by the i-th equation under the condition that $X_2, \ldots, X_{\tau+1}, X_{j_{\tau+1}}, \ldots, X_{j_{i-1}}$ have already been determined. Thus, the value of $\widetilde{g}_n(X_2, \ldots, X_{\tau+1}, X_{j_{\tau+1}}, \ldots, X_{j_{n-1}})$ in the function h_n is determined, denoted by b_n. Substituting this to the last equation of (10), we have $a_n = X_{j_n} \oplus b_n \oplus c_n$. Thus, X_{j_n} is determined. Hence, all X_is are determined.

Using the process similar to the above, for the feedback F satisfying Equation (8), the equation $F(X_1, X_2, \ldots, X_n) = \mathbf{a}$ also has a unique solution for any $\mathbf{a} \in \mathbb{F}_2^n$, but only the order and value of the solution are different. Thus, the proof is complete. □

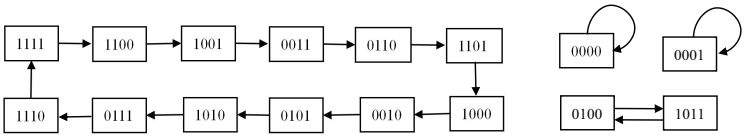


Figure 2: State diagram of the Galois NFSR in Example 1.

Example 1 *Consider a 4-stage 2-terminal-bit Galois NFSR given by Theorem 1, whose feedback* $F = [f_1 \;\; f_2 \;\; f_3 \;\; f_4]^T$ *satisfies*

$$\begin{cases} f_1 = X_2, \\ f_2 = X_3, \\ f_3 = X_1 \oplus X_2 \oplus X_2X_3 \oplus X_3X_4, \\ f_4 = X_2 \oplus X_3 \oplus X_4 \oplus X_2X_3. \end{cases} \tag{11}$$

We use the notations in Theorem 1. Then, based on Equations (7) and (11), we can easily get that $X_{j_3} = X_1, X_{j_4} = X_4, g_3(X_2, X_3, h_4) = X_2 \oplus X_3h_4, h_4 = X_4 \oplus X_2X_3$ *and* $g_4 = X_2 \oplus X_3$. *Figure 2 shows that the state diagram of the Galois NFSR contains only cycles, which means the Galois NFSR is nonsingular. This result is consistent with Theorem 1.*

Remark 1 *Theorem 1 gives a sufficient condition for an n-stage Galois NFSR to be nonsingular. However, this nonsingular Galois NFSR, clearly, does not satisfy the stated necessary condition for the nonsingularity of an n-stage Galois NFSR [8], that is, all feedback functions of the Galois NFSR satisfy* $f_i = X_{(i+1) \bmod n} \oplus g_i(X_1, X_2, \ldots, X_i, X_{i+2}, \ldots, X_n)$ *with* $i = 1, 2, \ldots, n$. *Actually, in Example 1, we can easily know that* f_3 *and* f_4 *does not contain the linear term* X_4 *and* X_1, *respectively. Therefore, that stated necessary condition therein is not reasonable. Nevertheless, we give some necessary conditions as follows.*

Theorem 2 *If an n-stage Galois NFSR with feedback* $F = [f_1 \;\; f_2 \;\; \ldots \;\; f_n]^T$ *is nonsingular, then all linear terms* X_i*s with* $i = 1, 2, \ldots, n$, *appear in the feedback* F *of the Galois NFSR.*

Proof. If the Galois NFSR is nonsingular, then F is invertible. Thereby, F is bijective. Hence, for any $\mathbf{a} = [a_1 \;\; a_2 \;\; \ldots \;\; a_n]^T \in \mathbb{F}_2^n$, the equation $F(X_1, X_2, \ldots, X_n) = \mathbf{a}$ has a unique solution $[X_1 \;\; X_2 \;\; \ldots \;\; X_n]^T \in \mathbb{F}_2^n$.

We assume there exists a linear term X_{i_0} with some $i_0 \in \{1, 2, \ldots, n\}$ does not appear in feedback function f_i for any $i \in \{1, 2, \ldots, n\}$. Since the function f_i can be written as

$$\begin{aligned} &f_i(X_1, \ldots, X_n) = h_i(X_1, X_2, \ldots, X_{i_0-1}, X_{i_0+1}, \ldots, X_n)X_{i_0} \\ &\oplus p_i(X_1, X_2, \ldots, X_{i_0-1}, X_{i_0+1}, \ldots, X_n), \end{aligned} \tag{12}$$

where h_i and p_i are Boolean functions, we can infer that $h_i(0, 0, \ldots, 0) = 0$ for any $i \in \{1, 2, \ldots, n\}$. Then, according to Equation (12), we have

$$f_i(0, \ldots, 0, X_{i_0}, 0, \ldots, 0) = p_i(0, 0 \ldots, 0) := c_i \tag{13}$$

for any $i \in \{1, 2, \ldots, n\}$ and for any $X_{i_0} \in \mathbb{F}_2$, which has two solutions $[0 \ \ldots \ 0 \ \underset{i_0}{0} \ 0 \ \ldots \ 0]^T$ and $[0 \ \ldots \ 0 \ \underset{i_0}{1} \ 0 \ \ldots \ 0]^T$. Then, for $\mathbf{c} = [c_1 \ c_2 \ \ldots \ c_n]^T \in \mathbb{F}_2^n$, the equation $F(X_1, X_2, \ldots, X_n) = \mathbf{c}$ has two solutions $[0 \ \ldots \ 0 \ \underset{i_0}{0} \ 0 \ \ldots \ 0]^T$ and $[0 \ \ldots \ 0 \ \underset{i_0}{1} \ 0 \ \ldots \ 0]^T$, a contradiction. □

Corollary 1 *If an n-stage Galois NFSR with feedback $F = [f_1 \ \ f_2 \ \cdots \ f_n]^T$ is nonsingular, then for the binary variable X_i with any $i \in \{1, 2 \ldots, n\}$, there exists a feedback function f_{j_i} with some $j_i \in \{1, 2, \ldots, n\}$ such that the linear term X_i appears in $f_{j_i}(X_1, X_2, \ldots, X_n)$.*

In [17], it gave the following result. For the necessity of later statements, we list its proof below as well.

Theorem 3 (Theorem 4 in [17]) *If an n-stage Galois NFSR with feedback $F = [f_1 \ \ f_2 \ \ldots \ f_n]^T$ is nonsingular, then there exists at least one feedback function f_i satisfies*

$$f_i(X_1, \ldots, X_n) = X_j \oplus g_i(X_1, X_2, \ldots, X_{j-1}, X_{j+1}, \ldots, X_n).$$

Proof. If the Galois NFSR is nonsingular, then for any pair of states $(\alpha_1, \alpha_2, \ldots, \alpha_{j-1}, 0, \alpha_{j+1}, \ldots, \alpha_n) \in \mathbb{F}_2^n$ and $(\alpha_1, \alpha_2, \ldots, \alpha_{j-1}, 1, \alpha_{j+1}, \ldots, \alpha_n) \in \mathbb{F}_2^n$, their successors are distinct, which means there exists at least one feedback function f_i such that

$$f_i(\alpha_1, \alpha_2, \ldots, \alpha_{j-1}, 0, \alpha_{j+1}, \ldots, \alpha_n) = f_i(\alpha_1, \alpha_2, \ldots, \alpha_{j-1}, 1, \alpha_{j+1}, \ldots, \alpha_n) \oplus 1, \tag{14}$$

where i may be relative to $(\alpha_1, \alpha_2, \ldots, \alpha_{j-1}, \alpha_{j+1}, \ldots, \alpha_n)$.

The function f_i can be written as:

$$\begin{aligned} &f_i(X_1, \ldots, X_n) = g_i(X_1, X_2, \ldots, X_{j-1}, X_{j+1}, \ldots, X_n)X_j \\ &\oplus h_i(X_1, X_2, \ldots, X_{j-1}, X_{j+1}, \ldots, X_n), \end{aligned} \tag{15}$$

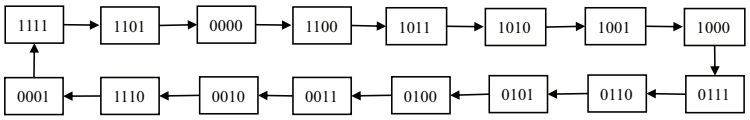


Figure 3: State diagram of the Galois NFSR in Example 2.

where g_i and h_i are Boolean functions. We shall prove that $g_i = (X_1, \ldots, X_{j-1}, X_{j+1}, \ldots, X_n) \equiv 1$. If $g_i(X_1, X_2, \ldots, X_{j-1}, X_{j+1}, \ldots, X_n) \not\equiv 1$, then there exists some $(a_1, a_2, \ldots, a_{j-1}, a_{j+1}, \ldots, a_n) \in \mathbb{F}_2^{n-1}$ such that $g_i(a_1, a_2, \ldots, a_{j-1}, a_{j+1}, \ldots, a_n) = 0$. Thus

$$f_i(a_1, a_2, \ldots, a_{j-1}, 0, a_{j+1}, \ldots, a_n) = f_i(a_1, a_2, \ldots, a_{j-1}, 1, a_{j+1}, \ldots, a_n), \tag{16}$$

which is contrary with Equation (14). Hence, $g_i = (X_1, X_2, \ldots, X_{j-1}, X_{j+1}, \ldots, X_n) \equiv 1$. According to Equation (15), the result follows. □

Actually, the following example shows that the result in Theorem 3 is not reasonable.

Example 2 *Consider a 4-stage Galois NFSR with a feedback* $F = [f_1 \;\; f_2 \;\; f_3 \;\; f_4]^T$ *satisfying*

$$\begin{cases} f_1 = X_1 \oplus X_2 \oplus X_1X_3 \oplus X_1X_4 \oplus X_3X_4 \oplus X_2X_3X_4 \oplus 1, \\ f_2 = X_2 \oplus X_1X_3 \oplus X_1X_4 \oplus X_2X_3 \oplus X_2X_4 \oplus X_3X_4 \oplus 1, \\ f_3 = X_1 \oplus X_2 \oplus X_3 \oplus X_4 \oplus X_1X_2 \oplus X_3X_4 \oplus X_1X_3X_4 \oplus X_2X_3X_4, \\ f_4 = X_1 \oplus X_2 \oplus X_4 \oplus X_1X_2 \oplus X_3X_4 \oplus X_1X_3X_4 \oplus X_2X_3X_4. \end{cases}$$

From Figure 3, we can see that the state diagram of the Galois NFSR contains only cycles, which means the Galois NFSR is nonsingular. However, all the feedback functions of this Galois NFSR do not satisfy the result in Theorem 3. Therefore, the result in Theorem is not reasonable.

Remark 2 *In the proof of Theorem 3, the statement "where i may be relative to* $(\alpha_1, \alpha_2, \ldots, \alpha_{j-1}, \alpha_{j+1}, \ldots, \alpha_n)$*" implies that not all* $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_{j-1}, \alpha_{j+1}, \ldots, \alpha_n)$ *satisfy Equation (14). For simplicity, we denote the set* $S = \{\boldsymbol{\alpha} | \boldsymbol{\alpha}$ *satisfies Equation (14)}. Unfortunately,* $(a_1, a_2, \ldots, a_{j-1}, a_{j+1}, \ldots, a_n)$ *in Equation (16) may not belong to* S*. Hence, the statement of Equation (16) contrary with Equation (14) is not correct. Therefore, the proof of Theorem 3 is problematic. Nevertheless, we have given Theorem 2 and Corollary 1, which are similar to Theorem 3 and are easily shown correct by Example 2.*

Theorem 4 *If an n-stage Galois NFSR with feedback $F = [f_1 \ \ f_2 \ \ \dots \ \ f_n]^T$ is nonsingualr, then the f_k's Hamming weight $wt(f_k) = 2^{n-1}$ for all $k = 1, 2, \dots, n$.*

Proof. An n-stage Galois NFSR with feedback $F = [f_1 \ \ f_2 \ \ \dots \ \ f_n]^T$ is nonsingualr if and only if F is inverse, which is equivalent to saying that the set $S = \{\mathbf{Y} | \mathbf{Y} = F(\mathbf{X}), \mathbf{X} \in \mathbb{F}_2^n\}$ has 2^n elements, which means $S = \mathbb{F}_2^n$ and $\mathbf{Y} \in \mathbb{F}_2^n$. Clearly, there are 2^{n-1} possible forms of $\mathbf{Y}$ over $\mathbb{F}_2^n$ whose i-th components are 1 for $i = 1, 2, \dots, n$.

Assume there exists a feedback function f_i whose $wt(f_i) \neq 2^{n-1}$. Thus, $wt(f_i) = 2^{n-1} \pm a$, where $a = 1, 2, \dots, 2^{n-1}$. This is equivalent to saying that there are $2^{n-1} \pm a$ possible forms of $\mathbf{Y}$ over $\mathbb{F}_2^n$ whose i-th components are 1, where $a = 1, 2, \dots, 2^{n-1}$. It is a contradiction, and the result follows. □

Corollary 2 *If an n-stage Galois NFSR with feedback $F = [f_1 \ \ f_2 \ \ \dots \ \ f_n]^T$ is nonsingular, then the degree of f_i for all $i = 1, 2, \dots, n$, is no more than $n - 1$.*

Proof. According to Theorem 4 and the process of computing the algebraic normal form of a Boolean function by its truth table, the result follows. □

5 Equivalence of NFSRs

In this section, we study the equivalence between Galois NFSRs and Fibonacci ones.

According to Lemma 4, we know that if an n-stage Galois NFSR represented by a linear system $\mathbf{X}(t+1) = F(\mathbf{X}(t))$ with $\mathbf{X} = [X_1 \ \ X_2 \ \cdots \ X_n]^T$ is equivalent to an n-stage Fibonacci one, then for any $i \in \{1, 2, \dots, n\}$, $X_i(t)$ can be uniquely expressed by $X_1(t), X_1(t+1), \dots, X_1(t+n-1)$ for all $t \in \mathbb{N}$. Moreover, as stated in [15], such a unique expression of $X_i(t)$ for any $i \in \{1, 2, \dots, n\}$ and for all $t \in \mathbb{N}$, can be derived from the nonlinear system represention $\mathbf{X}(t+1) = F(\mathbf{X}(t))$ by equivalent transformations. Notably, in Galois NFSR, $X_1(t)$ can always expressed by $X_1(t)$ for all $t \in \mathbb{N}$. Based on this result, in the following we obtain some necessary conditions for the Galois NFSRs equivalent to Fibonacci ones, from the perspectives of their feedback functions.

Theorem 5 *If an n-stage Galois NFSR with feedback $F = [f_1 \ \ f_2 \ \cdots \ f_n]^T$ is equivalent to an n-stage Fibonacci one, then for any $i \in \{2, 3, \dots, n\}$, the linear term X_i must appear in the feedback $F = [f_1 \ \ f_2 \ \cdots \ f_n]^T$ of the Galois NFSR.*

Proof. Assume there exists a linear term X_j with some $j \in \{2, \ldots, n\}$ does not appear in the feedback function f_i for any $i \in \{1, 2, \ldots, n\}$. Since there is no division in binary field, we cannot derive $X_j(t)$ from any bit but the j-th bit feedback function of the Galois NFSR, which can be described as

$$X_j(t+1) = f_j(X_1(t), X_2(t), \ldots, X_n(t)),\ t \in \mathbb{N}. \tag{17}$$

As this Galois NFSR is equivalent to a Fibonaaci one, then according to Lemma 4, there exists a unique bijection $\mathbf{h} = [h_1 \ \ h_2 \ \cdots \ h_n]^T$ over $\mathbb{F}_2^n$ such that

$$X_k(t) = h_k(X_1(t), X_1(t+1), \ldots, X_1(t+n-1)) \tag{18}$$

for each $k \in \{1, 2, \ldots, n\}$ and for any $t \in \mathbb{N}$. From Equations (17) and (18), we have

$$X_j(t+1) = g_j(X_1(t), X_1(t+1), \ldots, X_1(t+n-1)),\ t \in \mathbb{N},$$

for some Boolean function g_j, which implies

$$X_j(t) = g_j(X_1(t-1), X_1(t), \ldots, X_1(t+n-2)),\ t \geq 1,$$

contrary with Lemma 4. Hence, for any $j \in \{2, \ldots, n\}$, the linear term X_j must appear in the feedback $F = [f_1 \ \ f_2 \ \ldots \ f_n]^T$ of the Galois NFSR. □

Theorem 6 *If an n-stage Galois NFSR with feedback $F = [f_1 \ \ f_2 \ \ldots \ f_n]^T$ is equivalent to an n-stage Fibonacci one, and some linear term X_i with $i \in \{2, \ldots, n\}$ appears in only one feedback function f_j with $j \in \{1, 2, \ldots, n\}$ of the Galois NFSR, then*

$$f_j(X_1, X_2, \ldots, X_n) = X_i \oplus h_j(X_1, X_2, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n),\ j \neq i.$$

Proof. Note that

$$\begin{aligned} &X_j(t+1) = f_j(X_1(t), X_2(t), \ldots, X_n(t)) \\ &= g_j(X_1(t), \ldots, X_{i-1}(t), X_{i+1}(t), \ldots, X_n(t))X_i(t) \\ &\oplus h_j(X_1(t), \ldots, X_{i-1}(t), X_{i+1}(t), \ldots, X_n(t)),\ t \in \mathbb{N}. \end{aligned} \tag{19}$$

Then, we can claim $g_j(X_1(t), X_2(t), \ldots, X_{i-1}(t), X_{i+1}(t), \ldots, X_n(t)) \equiv 1$. Otherwise, there exists some $t_0 \in \mathbb{N}$ such that

$$g_j(X_1(t_0), X_2(t_0), \ldots, X_{i-1}(t_0), X_{i+1}(t_0), \ldots, X_n(t_0)) = 0.$$

Together taking into consideration Equation (19), we have

$$X_j(t_0+1) = h_j(X_1(t_0), X_2(t_0), \ldots, X_{i-1}(t_0), X_{i+1}(t_0), \ldots, X_n(t_0)),\ t_0 \in \mathbb{N},$$

which does not contain $X_i(t_0)$. As the linear term X_i only appears in f_j and there is no division in binary field, we cannot derive $X_i(t_0)$ from any bit but the i-th bit feedback function of the Galois NFSR, which can be described as

$$X_i(t_0+1) = f_i(X_1(t_0), X_2(t_0), \ldots, X_n(t_0)),\ t_0 \in \mathbb{N}. \tag{20}$$

As this Galois NFSR is equivalent to Fibonacci one, then according to Lemma 4, there exists a unique bijection $\mathbf{h} = [h_1 \ \ h_2 \ \cdots \ h_n]^T$ over $\mathbb{F}_2^n$ such that

$$X_k(t) = h_k(X_1(t), X_1(t+1), \ldots, X_1(t+n-1)) \tag{21}$$

for each $k \in \{1, 2, \ldots, n\}$ and for any $t \in \mathbb{N}$. From Equation (20) and (21), we have

$$X_i(t_0+1) = g_j(X_1(t_0), X_1(t_0+1), \ldots, X_1(t_0+n-1)),\ t_0 \in \mathbb{N},$$

for some Boolean function g_j, which implies

$$X_i(t_0) = g_j(X_1(t_0-1), X_1(t_0), \ldots, X_1(t_0+n-2)),\ t_0 \geq 1.$$

Thus, $X_i(t_0)$ cannot be expressed by $X_1(t_0), X_1(t_0+1), \ldots, X_1(t_0+n-1)$, contrary with Lemma 4. Hence, we have

$$g_j(X_1(t), X_2(t), \ldots, X_{i-1}(t), X_{i+1}(t), \ldots, X_n(t)) \equiv 1,\ t \in \mathbb{N},$$

which implies

$$X_j(t+1) = X_i(t) \oplus h_j(X_1(t), \ldots, X_{i-1}(t), X_{i+1}(t), \ldots, X_n(t)),\ t \in \mathbb{N}.$$

The remaining is to prove $j \neq i$. We assume that $j = i$. Then the above Equation can be of the form

$$X_i(t+1) = X_i(t) \oplus h_i(X_1(t), \ldots, X_{i-1}(t), X_{i+1}(t), \ldots, X_n(t)),\ t \in \mathbb{N}.$$

Similar to the foregoing proof, we can get a contraction. Thus, we have $j \neq i$. □

Corollary 3 *An n-stage $(n-2)$-terminal-bit Galois NFSR with feedback $F = [f_1 \ \ f_2 \ \cdots \ f_n]^T$ be of the form*

$$\begin{aligned} &(a) \quad f_i = X_{i+1}, \quad i = 1, 2, \ldots, n-2, \\ &(b) \quad f_{n-1} = f_{n-1}(X_1, X_2, \ldots, X_n), \\ &(c) \quad f_n = f_n(X_1, X_2, \ldots, X_n), \end{aligned} \tag{22}$$

is equivalent to an n-stage Fibonacci NFSR if and only if the feedback function f_{n-1} can be written in the form

$$f_{n-1} = X_n \oplus g_{n-1}(X_1, X_2, \ldots, X_{n-1}). \tag{23}$$

Proof. *Sufficiency:* If (b) of Equation (22) can be written as Equation (23), we can easily know that this Galois NFSR is a particular lower triangular Galois NFSR. Then according to Lemma 5, this n-stage Galois NFSR is equivalent to an n-stage Fibonacci NFSR.

Necessity: From (a) in Equation (22), we can derive $X_i(t) = X_1(t + i - 1)$ for any $i \in \{2, 3, \ldots, n-1\}$. As the linear term X_n does not appear in (a) of Equation (22), then according to Theorems 5 and 6, the result follows. □

Remark 3 *Corollary 3 shows that an n-stage $(n-2)$-terminal-bit Galois NFSR is equivalent an n-stage Fibonacci NFSR if and only if the n-stage $(n-2)$-terminal-bit Galois NFSR is a lower triangular Galois NFSR.*

Lemma 6 *Suppose τ to be a positive integer satisfying $1 \leq \tau \leq n-1$. Let an n-stage Galois NFSR with feedback $F = [f_1 \ \ f_2 \ \ldots \ f_n]^T$ be of the form*

$$\begin{aligned} &(a) \quad f_i = X_{i+1}, \quad i = 1, 2, \ldots, \tau, \\ &(b) \quad f_{\tau+1} = g_{\tau+1}(X_1, X_2, \ldots, X_n), \\ &(c) \quad f_i = g_i(X_1, X_2, \ldots, X_{i-1}), \ i = \tau+2, \tau+3, \ldots, n. \end{aligned} \tag{24}$$

Then, $\Omega_g \subseteq \Omega_f$, where Ω_g and Ω_f are the sets of output sequences of the Galois NFSR and an n-stage Fibonacci NFSR, respectively.

Proof. It follows from (a) in Equation (24) that $X_i(t+1) = X_{i+1}(t)$ for $1 \leq i \leq \tau$ and for any $t \in \mathbb{N}$. Thus, we have

$$X_i(t) = X_1(t + i - 1), \ i = 1, 2, \ldots, \tau + 1, \ t \in \mathbb{N}. \tag{25}$$

(c) in Equation (24) means

$$\begin{cases} X_{\tau+2}(t+1) = g_{\tau+2}(X_1(t), X_2(t), \ldots, X_{\tau+1}(t)), \\ X_{\tau+3}(t+1) = g_{\tau+3}(X_1(t), X_2(t), \ldots, X_{\tau+2}(t)), \\ \quad \vdots \\ X_n(t+1) = g_n(X_1(t), X_2(t), \ldots, X_{n-1}(t)),\ t \in \mathbb{N}. \end{cases} \tag{26}$$

Taking Equation (25) into the first equation of (26), we have $X_{\tau+2}(t+1) = g_{\tau+2}(X_1(t), X_1(t+1), \ldots, X_1(t+\tau))$. Thus,

$$X_{\tau+2}(t) = g_{\tau+2}(X_1(t-1), X_1(t), \ldots, X_1(t+\tau-1)) \tag{27}$$

for all $t \geq 1$. Here $t \geq 1$ is to ensure that the time of every parameter is nonnegative. Taking Equations (25) and (27) into the second equation of (26), we have $X_{\tau+3}(t+1) = \widetilde{g}_{\tau+3}(X_1(t-1), \ldots, X_1(t+\tau))$ for some Boolean function $\widetilde{g}_{\tau+3}$ and for all $t \geq 1$. Thus, $X_{\tau+3}(t) = \widetilde{g}_{\tau+3}(X_1(t-2), \ldots, X_1(t+\tau-1))$ for all $t \geq 2$. Keeping similar substitutions, the last equation of (26) can be rewritten as $X_n(t) = \widetilde{g}_n(X_1(t+\tau-n+1), \ldots, X_1(t+\tau-1))$ for some Boolean function $\widetilde{g}_n$ and for all $t \geq n-\tau-1$. Therefore, we have

$$X_i(t) = \widetilde{g}_i(X_1(t+\tau-i+1), \ldots, X_1(t+\tau-1)) \tag{28}$$

for some Boolean function $\widetilde{g}_i$ with $\tau+2 \leq i \leq n$ and for all $t \geq i-\tau-1$. Together taking into consideration (b) in Equation (24), we can infer that

$$X_{\tau+1}(t+1) = g_{\tau+1}(X_1(t), X_2(t), \ldots, X_n(t)),\ t \in \mathbb{N}. \tag{29}$$

Replacing $X_1(t), X_2(t), \ldots, X_n(t)$ in (29) by Equations (25) and (28), we get $X_1(t+\tau+1) = \widetilde{g}_{\tau+1}(X_1(t+\tau-n+1), \ldots, X_1(t+\tau))$ for some Boolean function $\widetilde{g}_{\tau+1}$ and for all $t \geq n-\tau-1$. Thus, $X_1(t) = \widetilde{g}_{\tau+1}(X_1(t-n), X_1(t-n+1), \ldots, X_1(t-1))$ for all $t \geq n$, which formulates a recurrence relation of order n. According to Lemma 2, the proof is complete. □

Remark 4 *Neither the Galois NFSRs in Lemma 6 nor their π-equivalent ones belong to the class of lower triangular Galois NFSRs in [11]. The reason is as follows.*

The feedback function $f_{\tau+1}$ of the Galois NFSR in Lemma 6 is a function of n variables that has no restriction. However, each feedback function f_i of a lower triangular Galois NFSR is a function with variable indices no greater than $i+1$. Thus, the Galois NFSR in Lemma 6 is clearly not contained in the class of lower triangular NFSRs.

Table 1: The Output Sequences of length 8 of Two NFSRs in Example 3

Sequences of the Galois NFSR												Sequences of the Fibonacci NFSR															
1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	0	1	1	1	1	0	1	0	1	0	0	0	0	1	1	1	1	0	1	0	1	0	0	**1**	**0**	**0**	**1**
0	1	1	1	1	0	1	0	0	0	1	0	0	1	1	1	1	0	1	0	0	0	1	0	**0**	**1**	**0**	**1**
1	1	1	1	0	1	0	0	0	1	1	1	1	1	1	1	0	1	0	0	0	1	1	1	**0**	**0**	**0**	**0**
1	1	1	0	1	0	0	0	0	1	0	0	1	1	1	0	1	0	0	0	0	1	0	0	**1**	**1**	**1**	**0**
1	1	0	1	0	0	0	0	0	0	1	0	1	1	0	1	0	0	0	0	0	0	1	0	**1**	**1**	**0**	**0**
1	0	1	0	0	0	0	0	0	1	0	0	1	0	1	0	0	0	0	0	0	1	0	0	**1**	**0**	**0**	**0**
0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	**1**	**1**	**0**	**0**
1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	**0**	**0**	**0**	**0**

For a lower triangular Galois NFSR, only f_n is a function of n variables without any restriction. For the Galois NFSR in Lemma 6, $f_{\tau+1}$ is such a function. If a π-equivalent one of the Galois NFSR in Lemma 6 belongs to the class of lower triangular Galois NFSRs, then $\pi(\tau+1) = n$. Thus, for the permuted Galois NFSR, its feedback functions of the last $n-\tau$ bits are related to the variable X_n, a contradiction. Therefore, the π-equivalent ones of the Galois NFSR in Lemma 6 are not contained in the class of lower triangular Galois NFSRs.

Example 3 *Consider a 4-stage 2-terminal-bit Galois NFSR given by Equation (24), whose feedback $F = [f_1 \quad f_2 \quad f_3 \quad f_4]^T$ satisfies $f_1 = X_2, f_2 = X_3, f_3 = X_1X_2 \oplus X_3X_4, f_4 = X_1 \oplus X_2 \oplus X_3$. Similar to the substitution in the Proof of Lemma 6, we can easily get $X_1(t) = X_1(t-3)X_1(t-2) \oplus X_1(t-1)X_1(t-4) \oplus X_1(t-1)X_1(t-3) \oplus X_1(t-1)X_1(t-2)$, which formulates a recurrence relation of order 4. In other words, each output sequence of this Galois NFSR can be generated by a 4-stage Fibonacci NFSR with feedback function $f = X_2X_3 \oplus X_1X_4 \oplus X_2X_4 \oplus X_3X_4$. There are totally 12 and 16 output sequences of the Galois NFSR and the Fibonacci NFSR, respectively. For simplicity, Table 1 lists their output sequences of length 8. We observe that the set of output sequences of the Galois NFSR is a subset of, but not equal to, the set of the output sequences of the Fibonacci NFSR.*

Remark 5 *Example 3 shows that the Galois NFSRs with terminal bits satisfying Equation (24) may not be equivalent to Fibonacci ones. Actually, the existence of a recurrence relation of order n only implies their sets of output sequences satisfying $\Omega_g \subseteq \Omega_f$, but does not*

guarantee $\Omega_g = \Omega_f$.

In the following, we give a necessary and sufficient condition for the equivalence between Galois NFSRs with terminal bits and Fibonacci ones.

Proposition 1 *Suppose* τ *to be a positive integer satisfying* $1 \leq \tau \leq n-1$. *An* n*-stage* τ*-terminal-bit Galois NFSR represented by System* $\mathbf{X}(t+1) = F(\mathbf{X}(t))$ *with state* $\mathbf{X} \in \mathbb{F}_2^n$ *is equivalent to an* n*-stage Fibonacci NFSR represented by System* $\mathbf{Y}(t+1) = H(\mathbf{Y}(t))$ *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* $\varphi(F(\mathbf{X})) = H(\varphi(\mathbf{X}))$ *and*

$$diag(\underbrace{1\ 1\cdots 1}_{\tau+1}\ 0\cdots 0)\varphi(\mathbf{X}) = diag(\underbrace{1\ 1\cdots 1}_{\tau+1}\ 0\cdots 0)\mathbf{X} \tag{30}$$

for all $\mathbf{X} \in \mathbb{F}_2^n$, *where* $diag(\cdot)$ *denotes a diagonal matrix with diagonal elements of* 1 *and* 0.

Proof. *Necessity:* Clearly, for each $\mathbf{X} \in \mathbb{F}_2^n$, there exists an edge from state $\mathbf{X}$ to state $F(\mathbf{X})$ in the state diagram of the Galois NFSR. Similarly, for each $\mathbf{Y} \in \mathbb{F}_2^n$, there exists an edge from state $\mathbf{Y}$ to state $H(\mathbf{Y})$ in the state diagram of the Fibonacci NFSR. If a Galois NFSR is equivalent to a Fibonacci NFSR, then according to Lemma 1, their state diagrams are isomorphic, which is equivalent to that there exists a bijective mapping $\varphi : \mathbf{X} \mapsto \mathbf{Y}$ such that

$$\varphi(F(\mathbf{X})) = H(\mathbf{Y}) = H(\varphi(\mathbf{X})) \ \text{ for each } \ \mathbf{X} \in \mathbb{F}_2^n. \tag{31}$$

Let

$$F = [f_1 \ \ f_2 \ \ \ldots \ \ f_n]^T, \tag{32}$$

$$H = [h_1 \ \ h_2 \ \ \ldots \ \ h_n]^T, \tag{33}$$

$$\varphi = [\varphi_1 \ \ \varphi_2 \ \ \ldots \ \ \varphi_n]^T. \tag{34}$$

Moreover, we let $\mathbf{X} = [X_1 \ \ X_2 \ \ \ldots \ \ X_n]^T$ and $\mathbf{Y} = [Y_1 \ \ Y_2 \ \ \ldots \ \ Y_n]^T$. Since F is the state transition function of the n-stage τ-terminal-bit Galois NFSR with τ satisfying $1 \leq \tau \leq n-1$, we have

$$f_i(\mathbf{X}) = X_{i+1},\ i = 1, 2, \ldots, \tau. \tag{35}$$

Similarly, as H is the state transition function of the Fibonacci NFSR, we have

$$\begin{cases} h_i(\mathbf{Y}) = Y_{i+1},\ i = 1, 2, \ldots, n-1, \\ h_n(\mathbf{Y}) = f(Y_1, Y_2, \ldots, Y_n), \end{cases} \tag{36}$$

where f is the feedback function of the Fibonacci NFSR. Since the output of an NFSR is the content of the first bit, and the first τ bits of the Fibonacci NFSR and its equivalent Galois NFSR are involved only shifts, we can deduce that each state $\mathbf{X}$ and its correspondingly transformed state $\mathbf{Y}$ have the same first τ components, which means

$$\varphi_i(\mathbf{X}) = X_i,\ i = 1, 2, \ldots, \tau. \tag{37}$$

From Equations (32), (35) and (37), we have

$$\begin{aligned}
&\varphi(F(\mathbf{X})) = \varphi(f_1(\mathbf{X}), f_2(\mathbf{X}), \ldots, f_n(\mathbf{X})) = \varphi(X_2, \ldots, X_{\tau+1}, f_{\tau+1}(\mathbf{X}), \ldots, f_n(\mathbf{X})) \\
&= [\varphi_1(X_2, \ldots, X_{\tau+1}, f_{\tau+1}(\mathbf{X}) \cdots f_n(\mathbf{X})), \ldots, \varphi_n(X_2, \ldots, X_{\tau+1}, f_{\tau+1}(\mathbf{X}), \ldots, f_n(\mathbf{X}))]^T \\
&= [X_2\ \cdots\ X_\tau\ X_{\tau+1}\ \ \varphi_{\tau+1}(X_2, \ldots, X_{\tau+1}, f_{\tau+1}(\mathbf{X}), \ldots, f_n(\mathbf{X}))\ \cdots \\
&\quad \varphi_n(X_2, \ldots, X_{\tau+1}, f_{\tau+1}(\mathbf{X}), \ldots, f_n(\mathbf{X}))]^T
\end{aligned} \tag{38}$$

for all $\mathbf{X} \in \mathbb{F}_2^n$. Similarly, according to Equations (33)-(34) and (36)-(37), we have

$$\begin{aligned}
&H(\varphi(\mathbf{X})) = H(\varphi_1(\mathbf{X}), \varphi_2(\mathbf{X}), \ldots, \varphi_n(\mathbf{X})) \\
&= [h_1(\varphi_1(\mathbf{X}), \varphi_2(\mathbf{X}), \ldots, \varphi_n(\mathbf{X}))\ \ \cdots\ \ h_n(\varphi_1(\mathbf{X}), \varphi_2(\mathbf{X}), \ldots, \varphi_n(\mathbf{X}))]^T \\
&= [\varphi_2(\mathbf{X})\ \cdots\ \varphi_n(\mathbf{X})\ \ f(\varphi_1(\mathbf{X}), \varphi_2(\mathbf{X}), \ldots, \varphi_n(\mathbf{X}))]^T \\
&= [X_2\ \cdots\ X_\tau\ \ \varphi_{\tau+1}(\mathbf{X})\ \cdots\ \varphi_n(\mathbf{X})\ \ f(X_1, \ldots, X_\tau, \varphi_{\tau+1}(\mathbf{X}), \ldots, \varphi_n(\mathbf{X}))]^T
\end{aligned} \tag{39}$$

for all $\mathbf{X} \in \mathbb{F}_2^n$. Based on Equations (31), (38) and (39), we can deduce that $\varphi_{\tau+1}(\mathbf{X}) = X_{\tau+1}$ for all $\mathbf{X} \in \mathbb{F}_2^n$. Hence, $\varphi_i(\mathbf{X}) = X_i$ for all $i = 1, 2, \ldots, \tau+1$ and for all $\mathbf{X} \in \mathbb{F}_2^n$, which is equivalent to Equation (30) for all $\mathbf{X} \in \mathbb{F}_2^n$.

Sufficiency: If there exists a bijective mapping $\varphi : \mathbf{X} \mapsto \mathbf{Y}$ such that $\varphi(F(\mathbf{X})) = H(\varphi(\mathbf{X}))$, then according to the necessity proof, the state diagrams of the Galois NFSR and the Fibonacci NFSR are isomorphic. Moreover, if the bijection φ satisfies Equation (30) for all $\mathbf{X} \in \mathbb{F}_2^n$, then

$$\varphi_i(\mathbf{X}) = X_i,\ i = 1, 2, \ldots, \tau+1,\ \mathbf{X} \in \mathbb{F}_2^n. \tag{40}$$

Thus, each state and its correspondingly transformed state have the same first $\tau+1$ components, and thereby the Galois NFSR is equivalent to the Fibonacci NFSR. In the following, we need to prove that the Galois NFSR has the terminal bit τ.

By Equations (32)-(34), (36) and (40), we have

$$\begin{aligned}
&H(\varphi(\mathbf{X})) = H(\varphi_1(\mathbf{X}), \varphi_2(\mathbf{X}), \ldots, \varphi_n(\mathbf{X})) \\
&= [h_1(\varphi_1(\mathbf{X}), \varphi_2(\mathbf{X}), \ldots, \varphi_n(\mathbf{X})) \ \cdots \ h_n(\varphi_1(\mathbf{X}), \varphi_2(\mathbf{X}), \ldots, \varphi_n(\mathbf{X}))]^T \\
&= [\varphi_2(\mathbf{X}) \ \cdots \ \varphi_n(\mathbf{X}) \ \ f(\varphi_1(\mathbf{X}), \varphi_2(\mathbf{X}), \ldots, \varphi_{n-1}(\mathbf{X}))]^T \\
&= [X_2 \ \cdots \ X_{\tau+1} \ \ \varphi_{\tau+2}(\mathbf{X}) \ \cdots \ \varphi_n(\mathbf{X}) \ \ f(\varphi_1(\mathbf{X}), \varphi_2(\mathbf{X}), \ldots, \varphi_{n-1}(\mathbf{X}))]^T
\end{aligned}$$

and

$$\varphi(F(\mathbf{X})) = \varphi(f_1(\mathbf{X}), \ldots, f_n(\mathbf{X})) = [f_1(\mathbf{X}) \ \cdots \ f_{\tau+1}(\mathbf{X}) \ \varphi_{\tau+2}(F(\mathbf{X})) \ \cdots \ \varphi_n(F(\mathbf{X}))]^T$$

for all $\mathbf{X} \in \mathbb{F}_2^n$. Together taking into consideration $\varphi(F(\mathbf{X})) = H(\varphi(\mathbf{X}))$ for all $\mathbf{X} \in \mathbb{F}_2^n$, we can infer that $f_i(\mathbf{X}) = X_{i+1}$ for all $i = 1, 2, \ldots, \tau$ and for all $\mathbf{X} \in \mathbb{F}_2^n$. Thus, the Galois NFSR has the terminal bit τ. □

Lemma 7 *An n-stage Galois NFSR and its state diagram is one-to-one correspondent.*

Proof. If an n-stage Galois NFSR is given, which means its feedback $F = [f_1 \ \ f_2 \ \ldots \ f_n]^T$ is fixed, then its state diagram is, clearly, uniquely determined. Conversely, if a state diagram with 2^n nodes is given, then for any given state $\mathbf{X} = [X_1 \ \ X_2 \ \ldots \ X_n]^T$, its successor $\mathbf{Y} = [Y_1 \ \ Y_2 \ \ldots \ Y_n]^T$ is uniquely determined. It means the feedback $F = [f_1 \ \ f_2 \ \ldots \ f_n]^T$ of the Galois NFSR satisfies $F(\mathbf{X}) = \mathbf{Y}$, i.e., $f_i(\mathbf{X}) = Y_i$, for all $i = 1, 2, \ldots, n$. Note that for the given state $\mathbf{X}$, it has totally 2^n possible values. Thus, for each $i \in \{1, 2, \ldots, n\}$, there are totally 2^n equations satisfying $f_i(\mathbf{X}) = \mathbf{Y}_i$ and $\mathbf{X}$ takes all 2^n possible values. This means that for each $i \in \{1, 2, \ldots, n\}$, the truth table of f_i is uniquely determined by the sate diagram, and therefore the algebraic normal form of f_i is uniquely determined. Thus, the Galois NFSR is uniquely determined. □

Theorem 7 *Suppose τ to be a positive integer satisfying $1 \leq \tau \leq n-1$. For any given n-stage Fibonacci NFSR, there are $(2^{n-\tau-1}!)^{2^{\tau+1}}$ n-stage τ-terminal-bit Galois NFSR equivalent to the Fibonacci NFSR.*

Proof. Let the n-stage Fibonacci NFSR be represented by System $\mathbf{Y}(t+1) = H(\mathbf{Y}(t))$ with state $\mathbf{Y} \in \mathbb{F}_2^n$, and its n-stage τ-terminal-bit equivalent Galois NFSR be represented by System $\mathbf{X}(t+1) = F(\mathbf{X}(t))$ with state $\mathbf{X} \in \mathbb{F}_2^n$. According to Proposition 1, the n-stage τ-terminal-bit Galois NFSR is equivalent to the given n-stage Fibonacci NFSR, if and only

if there exists a bijective mapping $\varphi : \mathbf{X} \mapsto \mathbf{Y}$ such that $\varphi(F(\mathbf{X})) = H(\varphi(\mathbf{X}))$ and Equation (30) holds for all $\mathbf{X} \in \mathbb{F}_2^n$.

Equation (30) means that the state $\mathbf{X} = [X_1 \ \ X_2 \ \ \ldots \ \ X_n]^T$ and its transformed state $\mathbf{Y} = [Y_1 \ \ Y_2 \ \ \ldots \ \ Y_n]^T$ satisfy $X_i = Y_i$ for all $i = 1, 2, \ldots, \tau + 1$. Hence, for any given state $\mathbf{X}$, $[Y_1 \ \ Y_2 \ \ \ldots \ \ Y_{\tau+1}]^T = [X_1 \ \ X_2 \ \ \ldots \ \ X_{\tau+1}]^T$ is fixed. Clearly, there are $2^{\tau+1}$ possible forms of $[X_1 \ \ X_2 \ \ \ldots \ \ X_{\tau+1}]^T$. Without loss of generality, say $[X_1 \ \ X_2 \ \ \ldots \ \ X_{\tau+1}]^T = [\underbrace{0 \ \ldots \ 0}_{\tau+1}]^T$. Then, there are $2^{n-\tau-1}$ possible forms of $[\underbrace{0 \ \ldots \ 0}_{\tau+1} \ \ X_{\tau+2} \ \ldots \ X_n]^T$, and there are $2^{n-\tau-1}$ possible forms of $[\underbrace{0 \ \ldots \ 0}_{\tau+1} \ \ Y_{\tau+2} \ \ldots \ Y_n]^T$ as well. Thereby, there are $2^{n-\tau-1}!$ possible forms of the bijection $\varphi : [\underbrace{0 \ \ldots \ 0}_{\tau+1} \ \ X_{\tau+2} \ \ldots \ X_n]^T \to [\underbrace{0 \ \ldots \ 0}_{\tau+1} \ \ Y_{\tau+2} \ \ldots \ Y_n]^T$. Therefore, we can deduce that there are totally $(2^{n-\tau-1}!)^{2^{\tau+1}}$ possible forms of the bijection $\varphi : \mathbf{X} = [X_1 \ \ X_2 \ \ \ldots \ \ X_n]^T \mapsto \mathbf{Y} = [Y_1 \ \ Y_2 \ \ \ldots \ \ Y_n]^T$ such that $\varphi(F(\mathbf{X})) = H(\varphi(\mathbf{X}))$ and Equation (30) holds for all $\mathbf{X} \in \mathbb{F}_2^n$.

Different bijective mappings φs result in different state diagrams of equivalent Galois NFSRs, and according to Lemma 7, different state diagrams result in different Galois NFSRs. Therefore, there are $(2^{n-\tau-1}!)^{2^{\tau+1}}$ n-stage τ-terminal-bit equivalent Galois NFSRs. □

Example 4 *A 3-stage Fibonacci NFSR with a feedback function* $f = X_1 \oplus X_2X_3 \oplus X_2 \oplus 1$ *generates the output sequence* 01110100 *which has the period* 8. *There are totally* 16 *3-stage 1-terminal-bit Galois NFSRs equivalent to this Fibonacci NFSR. Actually, they are all lower triangular Galois NFSRs. Table 2 in Appendix gives their feedback functions, in which each first-bit feedback function satisfies* $f_1 = X_2$. *Figure 7 in Appendix gives their state diagrams, which are isomorphic; moreover, their corresponding sates have the same first two components. All of these are consistent with the results in Theorems 5, 7 and Corollary 3.*

Theorem 8 *Suppose* τ *to be a positive integer satisfying* $1 \le \tau \le n-1$. *An* n*-stage Galois NFSR is equivalent to an* n*-stage Fibonacci NFSR if its feedback* $F = [f_1 \ \ f_2 \ \ \ldots \ \ f_n]^T$ *satisfies*

$$\begin{aligned}
&(a) \quad f_i = X_{i+1}, \quad i = 1, 2, \ldots, \tau, \\
&(b) \quad f_{\tau+1} = X_n \oplus g_{\tau+1}(X_1, X_2, \ldots, X_{n-1}), \\
&(c) \quad f_{\tau+2} = X_1 \oplus g_{\tau+1}(X_2, \ldots, X_{\tau+1}), \\
&(d) \quad f_i = X_{i-1} \oplus g_i(X_1, X_2, \ldots, X_{i-2}), \ i = \tau+3, \tau+4, \ldots, n.
\end{aligned} \tag{41}$$

Proof. Because of the Galois NFSR whose feedback satisfies Equation (41) is a particular Galois NFSR whose feedback satisfies Equation (24), then according to the proof of Lemma

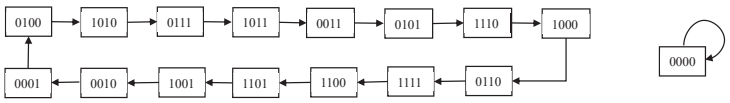
6, we know that there exists a recurrence relation of order n describing each output sequence of the i-th bit X_i with $i \in \{1, 2, \ldots, n\}$. In the following, we prove that the Galois NFSR is nonsingular.

A Galois NFSR is nonsingular, if and only if its feedback F is bijection. Hence, we only need to prove that for any $\mathbf{a} = [a_1 \ \ a_2 \ \ \ldots \ \ a_n]^T \in \mathbb{F}_2^n$, the equation $F(X_1, X_2, \ldots, X_n) = \mathbf{a}$ has a unique solution $[X_1 \ \ X_2 \ \ \ldots \ \ X_n]^T \in \mathbb{F}_2^n$. Consider the solution of the following system derived from Equation (41) by setting $f_i = a_i$ for all $i = 1, 2, \ldots, n$:

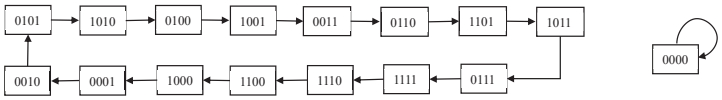
$$\begin{cases} a_1 = X_2, \\ \quad \vdots \\ a_\tau = X_{\tau+1}, \\ a_{\tau+1} = X_n \oplus g_{\tau+1}(X_1, X_2, \ldots, X_{n-1}), \\ a_{\tau+2} = X_1 \oplus g_{\tau+2}(X_2, \ldots, X_{\tau+1}), \\ a_{\tau+3} = X_{\tau+2} \oplus g_{\tau+3}(X_1, X_2, \ldots, X_{\tau+1}), \\ \quad \vdots \\ a_{n-1} = X_{n-2} \oplus g_{n-1}(X_1, X_2 \ldots, X_{n-3}), \\ a_n = X_{n-1} \oplus g_n(X_1, X_2 \ldots, X_{n-2}). \end{cases} \tag{42}$$

First, it can be seen that X_is for $2 \le i \le \tau + 1$ are determined by the first τ equations. Then, we can determine the value of X_1 from the $(\tau + 2)$-th equation of (42). Based on these, we can determine each X_i with $i \in \{\tau + 2, \tau + 3, \ldots, n - 1\}$ according to the equations from the $(\tau + 3)$-th to the n-th of Equation (42). Finally, X_n is determined by the $(\tau + 1)$-th equation under the condition that all $X_1, X_2, \ldots, X_{n-1}$ have been determined. Thus, the Galois NFSR is nonsingular. Then, according to Lemma 3, the result follows. □

Example 5 *Consider a 4-stage 1-terminal-bit Galois NFSR given by Equation (41), whose feedback* $F = [f_1 \ \ f_2 \ \ f_3 \ \ f_4]^T$ *satisfies* $f_1 = X_2, f_2 = X_4 \oplus X_1 \oplus X_2X_3, f_3 = X_1 \oplus X_2, f_4 = X_3 \oplus X_1X_2$. *In fact, this 4-stage Galois NFSR is equivalent to a 4-stage Fibonacci NFSR with feedback function* $f = X_1 \oplus X_2 \oplus X_3 \oplus X_2X_3 \oplus X_2X_4 \oplus X_3X_4$. *Figure 4(a) and Figure 4(b), respectively, show their state diagrams. We can easily see that each NFSR has one all-zero sequence and one 15-period sequence of 010100110111100. So, the Galois NFSR and the Fibonacci NFSR are indeed equivalent, consistent with our result in Theorem 8.*



(a) State diagram of the Galois NFSR in Example 5.



(b) State diagram of the Fibonacci NFSR in Example 5.

Figure 4: State diagrams of the Galois NFSR and the Fibonacci NFSR in Example 5.

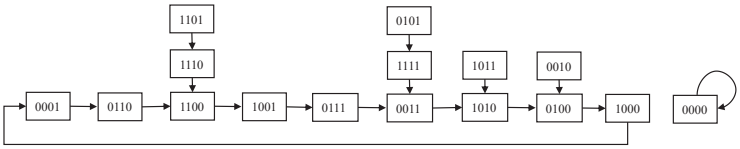


Figure 5: State diagram of the Galois NFSR in Example 6.

In [13], it discovered that the set of output sequences of the last bit of Galois NFSR(called Type-IV), is equal to the set of output sequences of Fibonacci NFSR. The feedback $F = [f_1 \;\; f_2 \;\; \cdots \;\; f_n]^T$ of the Type-IV Galois NFSR satisfies

$$\begin{aligned} &(a) \quad f_i = X_{i+1} \oplus g_i(X_{i+2}, X_{i+3}, \ldots, X_n), \quad i = 1, 2, \ldots, n-2, \\ &(b) \quad f_{n-1} = X_n, \\ &(c) \quad f_n = X_1 \oplus g_n(X_1, X_2, \ldots, X_n). \end{aligned} \tag{43}$$

Actually, the result about Type-IV Galois NFSRs equivalent to Fibonacci ones in [13] is not reasonable, which can be shown by the following example.

Example 6 *Consider a* 4*-stage Galois NFSR given by Equation (43), whose feedback* $F = [f_1 \;\; f_2 \;\; f_3 \;\; f_4]^T$ *satisfies* $f_1 = X_2 \oplus X_3X_4, f_2 = X_3 \oplus X_4, f_3 = X_4, f_4 = X_1 \oplus X_1X_3 \oplus X_2X_4$. *From Figure 5, we can see that the sequence* 100111000 *can be generated from initial state* [0 0 0 1] *and initial state* [1 1 0 1]. *Thus, this Galois NFSR is not equivalent to Fibonacci NFSR. Therefore, the result about Type-IV Galois NFSRs in [13] is not reasonable.*

Proposition 2 *A Type-IV Galois NFSR in [13] is equivalent to a Fibonacci NFSR if and*

only if its feedback functions satisfy

$$\begin{aligned}
&(a) \quad f_i = X_{i+1} \oplus g_i(X_{i+2}, X_{i+3}, \ldots, X_n), \quad i = 1, 2, \ldots, n-2, \\
&(b) \quad f_{n-1} = X_n, \\
&(c) \quad f_n = X_1 \oplus g_n(X_2, \ldots, X_n).
\end{aligned} \tag{44}$$

Poof. Similar to the poof of Lemma 6 and Theorem 8, we can prove the result holds. □

Remark 6 *The π-equivalent NFSRs of Galois ones in Lemma 2 belong to the class of Galois NFSRs in Theorem 8, where the permutation $\pi : (1, 2, 3, \ldots, n-2, n-1, n) \to (n, n-1, n-2 \ldots 3, 1, 2)$. We show the transformation process below.*

$$\begin{array}{ll}
f_n = X_1 \oplus g_n(X_2, X_3, \ldots, X_n), & f_1 = X_2, \\
f_{n-1} = X_n, & f_2 = X_n \oplus g_2(X_1, X_2, \ldots, X_{n-1}), \\
f_{n-2} = X_{n-1} \oplus g_{n-2}(X_n), & f_3 = X_2 \oplus g_3(X_1), \\
f_{n-3} = X_{n-2} \oplus g_{n-3}(X_{n-1}, X_n), & f_4 = X_3 \oplus g_4(X_1, X_2), \\
\quad \vdots & \xrightarrow{\pi} \quad \vdots \\
f_3 = X_4 \oplus g_3(X_5, X_6, \ldots, X_n), & f_{n-2} = X_{n-3} \oplus g_{n-2}(X_1, X_2, \ldots, X_{n-4}), \\
f_2 = X_3 \oplus g_2(X_4, X_5, \ldots, X_n), & f_{n-1} = X_{n-2} \oplus g_{n-1}(X_1, X_2, \ldots, X_{n-3}), \\
f_1 = X_2 \oplus g_1(X_3, X_4, \ldots, X_n), & f_n = X_{n-1} \oplus g_{n-1}(X_1, X_2, \ldots, X_{n-2}).
\end{array} \tag{45}$$

Clearly, the permuted Galois NFSR in the right column of Equation (45) is an n-stage 1-terminal-bit Galois NFSR in Theorem 8. Therefore, the π-equivalent NFSRs of Galois ones in Proposition 2 belong to the class of Galois NFSRs in Theorem 8.

Theorem 9 *Suppose τ to be a positive integer satisfying $1 \le \tau \le n-1$. An n-stage Galois NFSR is equivalent to an n-stage Fibonacci NFSR if its feedback $F = [f_1 \ \ f_2 \ \ \ldots \ \ f_n]^T$ satisfies*

$$\begin{aligned}
&(a) \quad f_i = X_{i+1}, \quad i = 1, 2, \ldots, \tau, \\
&(b) \quad f_{\tau+1} = X_1 \oplus g_{\tau+1}(X_2, \ldots, X_{\tau+1}) \oplus h_n, \\
&(c) \quad f_i = X_{i+1} \oplus g_i(X_1, X_2, \ldots, X_{\tau+1}, h_n), \ i = \tau+2, \tau+3, \ldots, n-1 \\
&(d) \quad f_n = g_n(X_2, \ldots, X_{\tau+1}) \oplus h_n,
\end{aligned} \tag{46}$$

where $h_n = X_{\tau+2} \oplus \tilde{h}(X_1, X_2, \ldots, X_{\tau+1}, X_{\tau+3}, \ldots, X_n)$.

Proof. We use the notations in Theorem 1. Then, based on Equation (7) and (46), we can easily get that $X_{j_{\tau+1}} = X_1$, $X_{j_n} = X_{\tau+2}$ and $X_{j_i} = X_{i+1}$ for all $i = \{\tau+2, \tau+2, \ldots, n-1\}$.

Thus, the Galois NFSR whose feedback satisfies Equation (46) is a particular Galois NFSR whose feedback satisfies Equation (7), then according to the proof of Theorem 1, we know that this Galois NFSR is nonsingular.

In the following, we prove that there exists a recurrence relation of order n describing each output sequence of the i-th bit X_i with $i \in \{1, 2, \ldots, n\}$. Similar to the proof of Lemma 6, we have

$$X_i(t) = X_1(t+i-1),\ i = 1, 2, \ldots, \tau+1,\ t \in \mathbb{N}. \tag{47}$$

Notably, h_n is relative to the variables $X_1, X_2, \ldots, X_n$, which change with time instant t. For the statement ease, we denote h_n as $h_n(t)$ in the sequel. Thus, from (b) in Equation (46), we can obtain

$$X_{\tau+1}(t+1) = X_1(t) \oplus g_{\tau+1}(X_2(t), X_3(t), \ldots, X_{\tau+1}(t)) \oplus h_n(t),\ t \in \mathbb{N}. \tag{48}$$

Taking Equation (47) into (48), we have

$$h_n(t) = \tilde{h}_n(t)(X_1(t), X_1(t+1), \ldots, X_1(t+\tau+1)), t \in \mathbb{N}. \tag{49}$$

(c) and (d) mean that

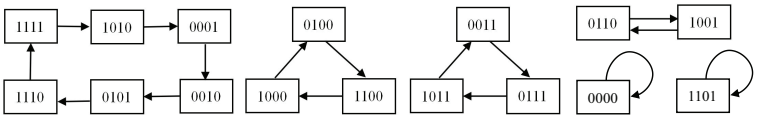
$$\begin{cases} X_{\tau+2}(t+1) = X_{\tau+3}(t) \oplus g_{\tau+2}(X_1(t), X_2(t), \ldots, X_{\tau+1}(t), h_n(t)), \\ X_{\tau+3}(t+1) = X_{\tau+4}(t) \oplus g_{\tau+3}(X_1(t), X_2(t), \ldots, X_{\tau+1}(t), h_n(t)), \\ \quad \vdots \\ X_{n-1}(t+1) = X_n(t) \oplus g_{n-1}(X_1(t), X_2(t), \ldots, X_{\tau+1}(t), h_n(t)), \\ X_n(t+1) = g_n(X_1(t), X_2(t), \ldots, X_{\tau+1}(t)) \oplus h_n(t), t \in \mathbb{N}. \end{cases} \tag{50}$$

Taking Equations (47) and (48) into the last equation of (50), we have $X_n(t+1) = \tilde{g}_n(X_1(t), X_1(t+1), \ldots, X_1(t+\tau+1))$ for some Boolean functions $\tilde{g}_n$ and for all $t \in \mathbb{N}$. Thus, $X_n(t) = \tilde{g}_n(X_1(t-1), X_1(t+1), \ldots, X_1(t+\tau))$ for all $t \geq 1$. Keeping similar substitutions, the first equation of (50) can be rewritten as $X_{\tau+2}(t) = \tilde{g}_{\tau+2}(X_1(t+\tau-n+1), X_1(t+\tau-n+2), \ldots, X_1(t+\tau))$ for some Boolean function $\tilde{g}_{\tau+2}$ and for all $t \geq n-\tau-1$. Therefore, we have

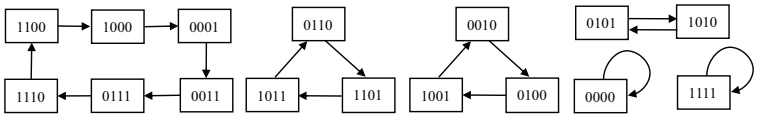
$$X_i(t) = \tilde{g}_i(X_1(t-n+i-1), X_1(t+n-i), \ldots, X_1(t+\tau)) \tag{51}$$

for some Boolean function $\tilde{g}_i$ with $\tau+2 \leq i \leq n$ and for all $t \geq n-i+1$. Taking $h_n = X_{\tau+2} \oplus \tilde{h}(X_1, X_2, \ldots, X_{\tau+1}, X_{\tau+3}, \ldots, X_n)$ into (48), we can infer that

$$\begin{aligned} &X_{\tau+1}(t+1) = X_1(t) \oplus g_{\tau+1}(X_2(t), X_3(t), \ldots, X_{\tau+1}(t)) \oplus \\ &X_{\tau+2}(t) \oplus \tilde{h}(X_1(t), X_2(t), \ldots, X_{\tau+1}(t), X_{\tau+3}(t), \ldots, X_n(t)),\ t \in \mathbb{N}. \end{aligned} \tag{52}$$



(a) State diagram of the Galois NFSR in Example 7.



(b) State diagram of the Fibonacci NFSR in Example 7.

Figure 6: State diagrams of the Galois NFSR and the Fibonacci NFSR in Example 7.

Replacing $X_1(t), X_2(t), \ldots, X_n(t)$ in (52) by Equations (47) and (51), we get $X_1(t+\tau+1) = \tilde{g}_{\tau+1}(X_1(t+\tau-n+1), X_1(t+\tau-n+2), \ldots, X_1(t+\tau))$ for some Boolean function $\tilde{g}_{\tau+1}$ and for all $t \geq n-\tau-1$. Thus, $X_1(t) = \tilde{g}_{\tau+1}(X_1(t-n), X_1(t-n+1), \ldots, X_1(t-1))$ for all $t \geq n$, which formulates a recurrence relation of order n. Then according to Lemma 3, the result follows. □

Example 7 *Consider a* 4*-stage* 1*-terminal-bit Galois NFSR given by Equation (46), whose feedback* $F = [f_1 \quad f_2 \quad f_3 \quad f_4]^T$ *satisfies* $f_1 = X_2, f_2 = X_1 \oplus X_2 \oplus X_3 \oplus X_1X_2X_4, f_3 = X_4 \oplus X_1X_2X_3 \oplus X_1X_2X_4, f_4 = X_3 \oplus X_1X_2X_4$*. In fact, this* 4*-stage Galois NFSR is equivalent to a* 4*-stage Fibonacci NFSR with feedback function* $f = X_1 \oplus X_2 \oplus X_4$*. Figure 6(a) and Figure 6(b), respectively, show their state diagrams. We can easily see that each NFSR has one all-zero and all-one sequence, one 2-period sequence of 01, two 3-period sequences of 011 and 001, one 6-period sequence of 110001. So, the Galois NFSR and the Fibonacci NFSR are indeed equivalent, consistent with our result in Theorem 9.*

Remark 7 *Similar to Remark 4, we can know that neither the Galois NFSRs in Theorem 8(resp. Theorem 9) nor their* π*-equivalent ones belong to lower triangular Galois NFSRs. Moreover, from Equations (41) and (46), we can know that the Galois NFSRs in Theorems 8 and 9 are not covered by each other. So, the Galois NFSRs with terminal bits in Theorems 8 and 9 are actually two new types of Galois NFSRs which are nonsingular and equivalent to Fibonacci ones.*

6 Conclusion

This paper first considered the nonsingularity of Galois NFSRs. Some necessary/sufficient conditions were presented. The paper then concentrated on the equivalence between Galois NFSRs and Fibonacci ones. It gave some necessary conditions for Galois NFSRs that are equivalent to Fibonacci ones, from the perspectives of their feedback functions. Is also enumerated the Galois NFSRs with terminal bits equivalent to a given Fibonacci one. Moreover, it provided two new types of nonsingular Galois NFSRs with terminal bits that are equivalent to Fibonacci NFSRs. In future work, it is interesting to find new necessary and/or sufficient conditions for the nonsingularity of Galois NFSRs, and find new types of Galois NFSRs with terminal bits that are equivalent to Fibonacci ones.

Appendix

Table 2: The Feedback Functions of 3-stage 1-terminal-bit Galois NFSR in Example 4

Number	f_2	f_3
1	$X_3 \oplus X_1X_2 \oplus X_2$	$X_1 \oplus X_1X_2 \oplus X_3 \oplus 1$
2	$X_3 \oplus X_1X_2$	$X_1 \oplus X_2 \oplus 1$
3	$X_3 \oplus X_1X_2 \oplus X_1$	$X_1 \oplus 1$
4	$X_3 \oplus X_1X_2 \oplus X_1 \oplus X_2 \oplus 1$	$X_1X_2 \oplus X_2 \oplus X_3 \oplus 1$
5	$X_3 \oplus X_2$	$X_1 \oplus X_2X_3 \oplus X_2 \oplus X_3 \oplus 1$
6	$X_3 \oplus X_1 \oplus X_2$	$X_1X_2 \oplus X_2X_3 \oplus X_3 \oplus 1$
7	$X_3 \oplus X_1 \oplus X_2$	$X_1 \oplus X_1X_2 \oplus X_2X_3 \oplus X_2$
8	$X_3 \oplus X_1$	$X_1 \oplus X_1X_2 \oplus X_2X_3 \oplus 1$
9	$X_3 \oplus X_1 \oplus X_2 \oplus 1$	$X_1X_2 \oplus X_2X_3 \oplus X_2 \oplus X_3 \oplus 1$
10	$X_3 \oplus X_2 \oplus 1$	$X_1 \oplus X_2X_3 \oplus X_3 \oplus 1$
11	$X_3 \oplus X_1X_2 \oplus X_2 \oplus X_1$	$X_1X_2 \oplus X_3 \oplus X_2 \oplus 1$
12	$X_3 \oplus X_1X_2 \oplus 1$	$X_1 \oplus X_2$
13	$X_3 \oplus X_1X_2 \oplus X_1 \oplus 1$	X_1
14	$X_3 \oplus X_1X_2 \oplus X_2 \oplus 1$	$X_1 \oplus X_1X_2 \oplus X_3 \oplus 1$
15	$X_3 \oplus 1$	$X_1 \oplus X_2X_3$
16	X_3	$X_1 \oplus X_2X_3 \oplus X_2 \oplus 1$

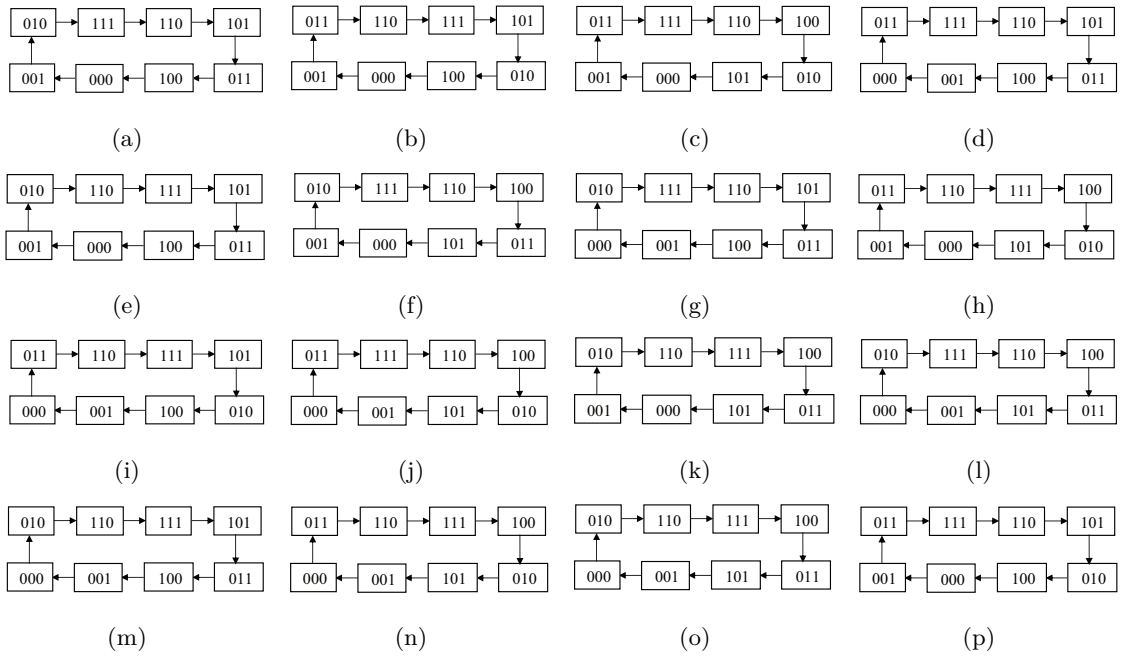


Figure 7: State diagrams of the 3-stage 1-terminal-bit Galois NFSR in Example 4

Acknowledgments

This work was support by the National Nature Science Foundation of China Grant Nos. 61772029 and 61872359.

References

[1] Hell M., Johansson T., Meier W.: Grain-a stream cipher for constrained environments. LNCS **4986**, 179-190 (2005).

[2] Cannière C.D., Preneel B.: Trivium Specifications. LNCS **4986**, 244-266 (2005).

[3] Wu H.: ACORN: A lightweight authenticated cipher (v3). Submission to CAESAR (2016). http://competitions.cr.yp.to/round3/acornv3.pdf

[4] Dubrova E.: A transformation from the Fibonacci to the Galois NLFSRs. IEEE Trans. Inf. Theory. **55**(11), 5263-5271 (2009).

[5] Biryukov A.: Weak keys. In: H.C.A. van Tilborg (eds.) Encyclopedia of Cryptography and Security, Springer, Boston, MA. (2005).

[6] Golomb S.W.: Shift Register Sequences. Holden-Dan Inc, San Francisco (1967).

[7] Zhong J., Lin D.: Decomposition of nonlinear feedback shift registers based on Boolean networks. Science China Information Sciences. **62**(3), 39110:1-39110:3 (2019).

[8] Dubrova E.: An equivalence-preserving transformation of shift registers. In: Schmidt K.-U. and Winterhof A. (eds.) Proceedings of Sequences and Their applications (SETA 2014), LNCS, vol.8865, pp. 187-199. Springer, Heidelberg (2014).

[9] Zhong J.: On equivalence of cascade connections of two nonlinear feedback shift registers. The Comput. J., **62**(12), 1793-1804 (2019).

[10] Dubrova E.: Finding matching initial states for equivalent NLFSRs in the Fibonacci and the Galois configurations. IEEE Trans. Inf. Theory **56**(6), 2961-2966 (2010).

[11] Lin Z.: The transformation from the Galois NLFSR to the Fibonacci configuration. In: 2013 Fourth International Conference on Emerging Intelligent Data and Web Technologies, pp. 335-339 (2013).

[12] Mykkeltveit J., Siu M.-K., and Ton P.: On the cylcle structure of some nonlinear shift register sequences. Inf. Control **43**, 202-215 (1979).

[13] Yao G., Parampalli U.: Improved transformation algorithms for generalized Galois NLFSRs. Cryptogr. Commun. (2021).

[14] Zhao X-X., Qi W-F., Zhang J-M.: Further results on the equivalence between Galois NFSRs and Fibonacci NFSRs. Des. Codes Cryptogr. **88**(1), 153-171 (2019).

[15] Zhong J., Pan Y., Kong W., Lin D.: Necessary and sufficient conditions for Galois NFSRs equivalent to Fibonacci ones and their application to the stream cipher Trivium. Cryptol. ePrint Archive. https://eprint.iacr.org/2021/928.

[16] Mykkeltveit J., Siu M.K., Tong P.: On the cycle structure of some nonlinear shift register sequences. Inf. Control. **43**(2), 202–215 (1979).

[17] Pan Y., Zhong J., Lin D.: On Galois NFSRs with terminal bits. In: 2021 IEEE International Symposium on Information Theory (ISIT 2021), Melbourne, Australia (2021).