Isomorphism and Equivalence of Galois Nonlinear Feedback Shift Registers

Wenhui Kong[1,2], Jianghua Zhong[1], and Dongdai Lin[1]

[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 Science, Beijing 100049, China

Abstract. Nonlinear feedback shift registers (NFSRs) have been used in many recent stream ciphers. They are generally classified as Fibonacci NFSRs and Galois NFSRs in terms of their implementation configurations. Two NFSRs are said to be isomorphic if their state diagrams are isomorphic, and two NFSRs are equivalent if their sets of output sequences are equal. Equivalent NFSRs must be isomorphic NFSRs, but not the vice versa. Previous work has been done on the isomorphism and equivalence of Fibonacci NFSRs. This paper continues this research for Galois NFSRs. It first gives some characterizations for several kinds of isomorphic Galois NFSRs, which improves and generalizes the previous corresponding results for Fibonacci NFSRs. It then presents some characterizations for two kinds of equivalent Galois NFSRs, helpful to the design of NFSR-based stream ciphers.

Keywords: Nonlinear feedback shift register · Boolean function · Stream cipher · Isomorphism · Equivalence.

1 Introduction

Nonlinear feedback shift registers (NFSRs) have been used as the main building blocks in many stream ciphers, such as the finalists Grain [1] and Trivium [2] in the eSTREAM project. An NFSR can be generally implemented in Fibonacci or Galois configuration. In Fibonacci configuration, the feedback is only applied to the last bit, while in the Galois configuration, the feedback can be applied to every bit. NFSRs in Fibonacci configuration are called Fibonacci NFSRs, and those in Galois configuration are called Galois NFSRs. Compared to Fibonacci NFSRs, Galois NFSRs may shorten propagation time and improve throughput [3]. Notably, the foregoing stream ciphers Grain and Trivium use the Galois NFSRs. Precisely, both are Galois NFSRs with terminal bits, which have the first several bits involved only shifts.

An NFSR has the same mathematical model as a Boolean network, which is a finite automaton evolving through Boolean functions. Boolean networks have been well developed in the community of systems and control [4] via a powerful mathematical tool called semi-tensor product of matrices [5]. As mentioned in

literature [6]-[10], NFSRs can be regarded as Boolean networks, and their cryptographic properties can be facilitated to some extent to analyze by using the semi-tensor product based Boolean network theory.

Two NFSRs are said to be isomorphic if their state diagrams are isomorphic, and two NFSRs are said to be equivalent if their sets of output sequences are equal. Equivalent NFSRs must be isomorphic, but not the vice versa. Some kinds of isomorphic Fibonacci NFSRs were studied and the relation between their feedback functions were revealed [9]. Some isomorphic Galois NFSRs equivalent to Fibonacci ones were found [11].

Some work has been done on the equivalence of NFSRs. A Fibonacci NFSR can be equivalent to "uniform" Galois NFSRs [3], and their initial states were matched in [12]. "Lower triangular" Galois NFSRs [13] and cascade connections of two Fibonacci NFSRs [14] were found equivalent to Fibonacci NFSRs. In addition, some characterizations of the feedback of Galois NFSRs equivalent to Fibonacci ones was revealed [15]. The Galois NFSRs with terminal bits that are equivalent to Fibonacci ones were enumerated [16].

Contribution. This paper considers the isomorphism and equivalence of Galois NFSRs. It first presents several kinds of isomorphic Galois NFSRs and reveals the relation of their feedbacks, which improves and generalizes the corresponding results for Fibonacci NFSRs. It then gives some characterizations of two kinds of Galois NFSRs equivalent to Fibonacci ones from the perspective of feedbacks and numbers, benefiting the design of NFSR-based stream ciphers.

Organization. The paper is organized as follows. Section 2 gives some preliminaries, including some basic concepts and related results on Boolean networks and NFSRs. Our main results on isomorphism and equivalence of Galois NFSRs are presented in Sections 3 and 4, respectively. The paper concludes in Section 5.

2 Preliminaries

In this section, we review some basic concepts and related results on the semi-tensor product of matrices and NFSRs. Before that, we first introduce some notations used throughout the paper.

Notations: $\mathbb{F}_2$ denotes the binary Galois field, and $\mathbb{F}_2^n$ is an n-dimensional vector space over $\mathbb{F}_2$. $\mathbb{N}$ is the set of nonnegative integers. δ_n^i stands for the i-th column of the $n \times n$ identity matrix I_n. The set of all columns of I_n is denoted by Δ_n. Let $\mathcal{L}_{n\times m}$ be the set of all $n \times m$ matrices whose columns belong to the set Δ_n. For a matrix $A = [\delta_n^{i_1}\ \delta_n^{i_2}\ \cdots\ \delta_n^{i_m}] \in \mathcal{L}_{n\times m}$, we simply denote it as $A = \delta_n[i_1\ i_2\ \cdots\ i_m]$. The operators $+, -$ and $\times$, respectively, denote the ordinary addition, subtraction and multiplication in the real field. The operations $\oplus$ and $\odot$, respectively, represent the addition and multiplication over $\mathbb{F}_2$.

2.1 Boolean network

Definition 1 ([17]). *For an $n \times m$ matrix $A = (a_{ij})$ and a $p \times q$ matrix B, their Kronecker product is defined as*

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

Definition 2 ([5]). *For an $n \times m$ A and a $p \times q$ matrix B, let α be the least common multiple of m and p. The semi-tensor product of A and B is defined as*

$$A \ltimes B = (A \otimes I_{\frac{\alpha}{m}})(B \otimes I_{\frac{\alpha}{p}}). \tag{1}$$

We can easily observe that if $m = p$ in Definition 2 , then the semi-tensor product is degenerated into the conventional matrix product.

An n-variable Boolean function f is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. The decimal number of a binary $(i_1, i_2, \ldots, i_n)$ is $i = i_1 2^{n-1} + i_2 2^{n-2} + \cdots + i_n$. We simply write $f(i_1, i_2, \ldots, i_n)$ as $f(i)$. $[f(2^n - 1), f(2^n - 2), \cdots, f(0)]$ is called the *truth table* of f, arranged in the reverse alphabet order. The matrix

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

is named the *structure matrix* of f [18, 4]. The function $\mathbf{f} = [f_1 \;\; f_2 \;\; \ldots \;\; f_n]^T$ is called a *vectorial function* if all f_is are Boolean functions.

The Hamming weight of a binary string α of finite length is the number of ones in α, denoted by $wt(\alpha)$. The Hamming weight of a Boolean function f, denoted by $wt(f)$, is the Hamming weight of its truth table. The Hamming weight is one of the most basic properties of a Boolean function, and is a crucial criterion in cryptography [19]. If an n-variable Boolean function f satisfies $wt(f) = 2^{n-1}$, then the Boolean function f is said to be balanced. An n-variable Boolean function f is said to be linear with respect to the variable X_i if $f(X_1, X_2, \cdots, X_n) = X_i \oplus \tilde{f}(X_1, X_2, \cdots, X_{i-1}, X_{i+1}, \cdots, X_n)$ for some i satisfying $1 \leq i \leq n$. If a Boolean function f is linear with respect to some variable, then it is balanced.

A Boolean network with n nodes and m outputs can be described in general as the nonlinear system:

$$\begin{cases} \mathbf{X}(t+1) = \mathbf{g}(\mathbf{X}(t)), \\ \mathbf{Y}(t) = \mathbf{h}(\mathbf{X}(t)), t \in \mathbb{N}, \end{cases} \tag{3}$$

where $\mathbf{X} = [X_1 \;\; X_2 \;\; \ldots \;\; X_n]^T \in \mathbb{F}_2^n$ is the state, and the vectorial function $\mathbf{g} = [g_1 \;\; g_2 \;\; \cdots \;\; g_n]^T : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is the state transition function, and $\mathbf{h} = [h_1 \;\; h_2 \;\; \ldots \;\; h_n]^T : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is the output function.

Lemma 1 ([4]). *For any state* $\mathbf{X} = [X_1 \ \ X_2 \ \cdots \ X_n]^T \in \mathbb{F}_2^n$, *let* $\mathbf{x} = [X_1 \ \ X_1 \oplus 1]^T \ltimes [X_2 \ \ X_2 \oplus 1]^T \ltimes \cdots \ltimes [X_n \ \ X_n \oplus 1]^T$. *Then* $\mathbf{x} = \delta_{2^n}^j \in \Delta_{2^n}$ *with* $j = 2^n - (2^{n-1}X_1 + 2^{n-2}X_2 + \cdots + X_n)$.

From Lemma 1, we can easily see that 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 (3) can be equivalently expressed as the linear system (6):

$$\begin{cases} \mathbf{x}(t+1) = L\mathbf{x}(t), \\ \mathbf{y}(t) = H\mathbf{x}(t), \ t \in \mathbb{N}, \end{cases} \tag{4}$$

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

$$Col_j(L) = Col_j(G_1) \otimes Col_j(G_2) \otimes \cdots \otimes Col_j(G_n), \ j = 1, 2, \ldots, 2^n, \tag{5}$$

with G_i being the the structure matrix of the i-th component g_i of the vectorial function $\mathbf{g}$ in (3) for any $i \in \{1, 2, \ldots, n\}$. The j-th column of H can be computed in a similar way.

2.2 Nonlinear feedback shift register

Fig.1 shows the diagram of an n-stage Galois NFSR, in which each small square represents a binary storage device, also called *bit*. The content of bit i is labelled as X_i. All X_is together form the Galois NFSR's state $[X_1 \ \ X_2 \ \ldots \ X_n]^T$. Every bit i has its own feedback function f_i. They all form the Galois NFSR's feedback $\mathbf{f} = [f_1 \ \ f_2 \ \ldots \ f_n]^T$. At each periodic interval determined by a master clock, the content X_i is updated by the value of f_i taking at the previous contents of all X_is. The n-stage Galois NFSR can be described by the nonlinear system:

$$\begin{cases} X_1(t+1) = f_1(X_1(t), X_2(t), \ldots, X_n(t)), \\ X_2(t+1) = f_2(X_1(t), X_2(t), \ldots, X_n(t)), \\ \quad \vdots \\ X_n(t+1) = f_n(X_1(t), X_2(t), \ldots, X_n(t)), \end{cases} \tag{6}$$

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

If a Galois NFSR's feedback $\mathbf{f} = [f_1 \ \ f_2 \ \ldots \ f_n]^T$ satisfies $f_i(X_1, X_2, \cdots, X_n) = X_{i+1}$ for all $i = 1, 2, \cdots, n-1$, then the n-stage Galois NFSR becomes an n-stage Fibonacci NFSR. Fig. 2 describes an n-stage Fibonacci NFSR, which is nonsingular if and only if its feedback function f is nonsingular, that is, $f = X_1 \oplus \tilde{f}(X_2, X_3, \cdots, X_n)$ [20].

The state diagram of an n-stage NFSR is a directed graph consisting of 2^n vertices and 2^n edges, in which each vertex represents a state of the NFSR, and each edge represents a transition between two states. Precisely, if state $\mathbf{X}$ is updated to state $\mathbf{Y}$, then there is an edge from state $\mathbf{X}$ to state $\mathbf{Y}$. In this case,

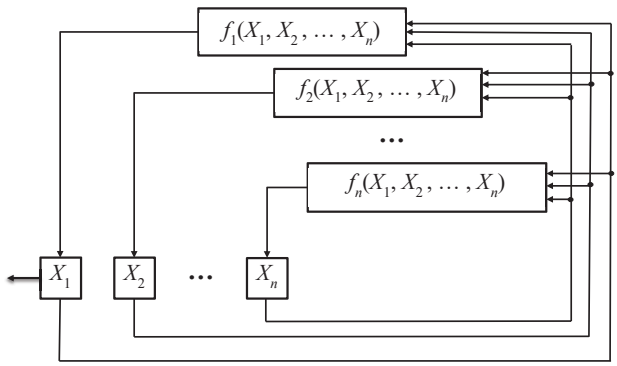

Fig. 1. An n-stage Galois NFSR.

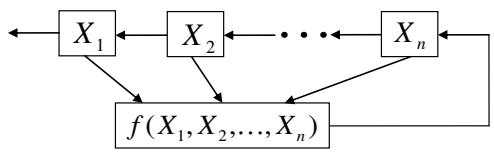

Fig. 2. An n-stage Fibonacci NFSR.

$\mathbf{X}$ is a *predecessor* of $\mathbf{Y}$, and $\mathbf{Y}$ is the *successor* of $\mathbf{X}$. Consecutive distinct states $\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_p$ and their edges between them form a *cycle* of length p if $\mathbf{X}_1$ is the successor of $\mathbf{X}_p$.

For any $X \in \mathbb{F}_2$, denote $\bar{X} = X \oplus 1$. Let $G_i = (V_i, A_i)$ with $i \in \{1, 2\}$, be the state diagram of an n-stage NFSRi, where V_i is the set of states, while A_i is the set of edges. G_1 and G_2 are said to be *isomorphic* if there exists a bijective mapping $\varphi : V_1 \to V_2$ such that for any edge $E_1 \in A_1$ from $\mathbf{X}$ to state $\mathbf{Y}$, there exists an edge $E_2 \in A_2$ from $\varphi(\mathbf{X})$ to $\varphi(\mathbf{Y})$. In this case, NFSR1 and NFSR2 are said to be *isomorphic NFSRs*. Furthermore, if the bijective mapping φ satisfies $\varphi = D : [X_1 \;\; X_2 \;\; \ldots \;\; X_n]^T \mapsto [\bar{X}_1 \;\; \bar{X}_2 \;\; \ldots \;\; \bar{X}_n]^T$, then G_1 and G_2 are said to be *dual isomorphic*, denoted by $G_2 = DG_1$; if φ satisfies $\varphi = R : [X_1 \;\; X_2 \;\; \ldots \;\; X_n]^T \mapsto [X_n \;\; X_{n-1} \;\; \ldots \;\; X_1]^T$, then G_1 and G_2 are said to be *anti-isomorphic*, denoted by $G_2 = RG_1$; if φ satisfies $\varphi = DR : [X_1 \;\; X_2 \;\; \ldots \;\; X_n]^T \mapsto [\bar{X}_n \;\; \bar{X}_{n-1} \;\; \ldots \;\; \bar{X}_1]^T$, then G_1 and G_2 are said to be *dual anti-isomorphic*, denoted by $G_2 = DRG_1$.

Lemma 2 ([9]). *For an n-stage Fibonacci NFSR1 with feedback function f,*

1. *if the state diagram of an n-stage Fibonacci NFSR2 is dual isomorphic to that of the Fibonacci NFSR1, then the feedback function of the Fibonacci NFSR2 is D_f satisfying $D_f(X_1, X_2, \ldots, X_n) = \overline{f(\bar{X}_1, \bar{X}_2, \ldots, \bar{X}_n)}$;*
2. *if the state diagram of an n-stage Fibonacci NFSR2 is anti-isomorphic to that of the Fibonacci NFSR1, then the feedback function of the Fibonacci NFSR2 is R_f satisfying $R_f(X_1, X_2, \ldots, X_n) = f(X_n, X_{n-1}, \ldots, X_1)$;*

3. *if the state diagram of an n-stage Fibonacci NFSR2 is dual anti-isomorphic to that of the Fibonacci NFSR1, then the feedback function of the Fibonacci NFSR2 is DR_f satisfying $DR_f(X_1, X_2, \ldots, X_n) = \overline{f(\bar{X}_n, \bar{X}_{n-1}, \ldots, \bar{X}_1)}$.*

Lemma 3 ([21]). *If an n-stage Fibonacci NFSR and an n-stage Galois NFSR are equivalent, then their state diagrams are isomorphic.*

Definition 3 ([16]). *For a positive integer τ satisfying $1 \le \tau \le n-1$, an n-stage Galois NFSR with feedback $\mathbf{f} = [f_1 \ \ f_2 \ \ \ldots \ \ f_n]^T$ 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.*

Lemma 4 ([16]). *Suppose τ to be a positive integer satisfying $1 \le \tau \le n-1$. An n-stage τ-terminal-bit Galois NFSR represented by a nonlinear 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 a nonlinear 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*

$$diag(\underbrace{1 \ 1 \cdots 1}_{\tau+1} \ 0 \cdots 0)\varphi(\mathbf{X}) = diag(\underbrace{1 \ 1 \cdots 1}_{\tau+1} \ 0 \cdots 0)\mathbf{X} \tag{7}$$

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

Lemma 5 ([15]). *An n-stage Galois NFSR with feedback $\mathbf{f} = [f_1 \ \ f_2 \cdots f_n]^T$ can be equivalently expressed as a linear system:*

$$\mathbf{x}(t+1) = L_g \mathbf{x}(t), t \in \mathbb{N},$$

where $\mathbf{x} \in \Delta_{2^n}$ is the state, and $L_g = \delta_{2^n}[\xi_1 \ \xi_2 \ \cdots \ \xi_{2^n}] \in \mathcal{L}_{2^n \times 2^n}$ is the state transition matrix, satisfying

$$\xi_i = 2^n - 2^{n-1} f_1(2^n - i) - 2^{n-2} f_2(2^n - i) - \cdots - 2 f_{n-1}(2^n - i) - f_n(2^n - i),$$
$$j = 1, 2, \cdots, 2^n.$$

Lemma 6 ([10]). *An n-stage Fibonacci NFSR with a feedback function f, can be expressed as the following linear system:*

$$\mathbf{x}(t+1) = L\mathbf{x}(t), \ t \in \mathbb{N},$$

where $\mathbf{x} \in \Delta_{2^n}$ is the state, $L \in \mathcal{L}_{2^n \times 2^n}$ is the state transition matrix, satisfying

$$L = \delta_{2^n}[\eta_1 \ \cdots \ \eta_{2^{n-1}} \ \eta_{2^{n-1}+1} \ \cdots \ \eta_{2^n}]$$

with

$$\begin{cases} \eta_i = 2i - s_i, \ i = 1, 2, \cdots, 2^{n-1}, \\ \eta_{2^{n-1}+i} = 2i - s_{2^{n-1}+i}, \end{cases}$$

and $[s_1, s_2, \cdots, s_{2^n}]$ being the truth table of f, arranged in the reverse alphabet order.

3 Isomorphism of Galois NFSRs

In this section, we will reveal some characterizations of several kinds of isomorphic Galois NFSRs.

Theorem 1. *For an n-stage Galois NFSR1 with feedback* $\mathbf{f} = [f_1 \;\; f_2 \;\; \dots \;\; f_n]^T$,

1. *the state diagram of an n-stage Galois NFSR2 is dual isomorphic to that of Galois NFSR1, if and only if the feedback* $D_{\mathbf{f}}$ *of the Galois NFSR2 satisfies*

$$D_{\mathbf{f}} = [\overline{f_1(\bar{X}_1, \bar{X}_2, \cdots, \bar{X}_n)} \quad \overline{f_2(\bar{X}_1, \bar{X}_2, \cdots, \bar{X}_n)} \;\; \cdots \;\; \overline{f_n(\bar{X}_1, \bar{X}_2, \cdots, \bar{X}_n)}]^T; \tag{8}$$

2. *the state diagram of an n-stage Galois NFSR3 is anti-isomorphic to that of Galois NFSR1, if and only if the feedback* $R_{\mathbf{f}}$ *of the Galois NFSR3 satisfies*

$$R_{\mathbf{f}} = [f_n(X_n, X_{n-1}, \dots, X_1) \quad f_{n-1}(X_n, X_{n-1}, \dots, X_1) \;\; \dots \;\; f_1(X_n, X_{n-1}, \dots, X_1)]^T. \tag{9}$$

3. *the state diagram of an n-stage Galois NFSR4 is dual anti-isomorphic to that of Galois NFSR1, if and only if the feedback* $DR_{\mathbf{f}}$ *of the Galois NFSR4 satisfies*

$$DR_{\mathbf{f}} = [\overline{f_n(\bar{X}_n, \bar{X}_{n-1}, \dots, \bar{X}_1)} \quad \overline{f_{n-1}(\bar{X}_n, \bar{X}_{n-1}, \dots, \bar{X}_1)} \;\; \dots \;\; \overline{f_1(\bar{X}_n, \bar{X}_{n-1}, \dots, \bar{X}_1)}]^T. \tag{10}$$

Proof. Let $[a_0 \;\; a_1 \;\; \dots \;\; a_n]^T$ be a vertex in the state diagram of Galois NFSR1. Then, there is an edge from $[a_0 \;\; a_1 \;\; \dots \;\; a_n]^T$ to $[f_1(a_1, a_2, \dots, a_n) \;\; f_2(a_1, a_2, \dots, a_n) \;\; \dots \;\; f_n(a_1, a_2, \dots, a_n)]^T$ in the state diagram of Galois NFSR1.

Case 1: If the state diagram of the Galois NFSR2 is dual isomorphic to that of the Galois NFSR1, then there is an edge from $[\bar{a}_1 \;\; \bar{a}_2 \;\; \dots \;\; \bar{a}_n]^T$ to $[\overline{f_1(a_1, a_2, \dots, a_n)} \quad \overline{f_2(a_1, a_2, \dots, a_n)} \;\; \dots \;\; \overline{f_n(a_1, a_2, \dots, a_n)}]^T$ in the state diagram of Galois NFSR2. Let $b_i = \bar{a}_i$ for all $i = 1, 2, \cdots, n$. Then, there is an edge from $[b_1 \;\; b_2 \;\; \dots \;\; b_n]^T$ to $[\overline{f_1(\bar{b}_1, \bar{b}_2, \cdots, \bar{b}_n)} \;\; \overline{f_2(\bar{b}_1, \bar{b}_2, \cdots, \bar{b}_n)} \;\; \dots \;\; \overline{f_n(\bar{b}_1, \bar{b}_2, \cdots, \bar{b}_n)}]^T$ in the state diagram of Galois NFSR2. Thus, the feedback $D_{\mathbf{f}}$ of Galois NFSR2 satisfies Equation (8).

Conversely, if the feedback $D_{\mathbf{f}}$ of Galois NFSR2 satisfies Equation (8), then there is an edge from $[b_1 \;\; b_2 \;\; \dots \;\; b_n]^T$ to $[\overline{f_1(\bar{b}_1, \bar{b}_2, \cdots, \bar{b}_n)} \;\; \overline{f_2(\bar{b}_1, \bar{b}_2, \cdots, \bar{b}_n)} \;\; \dots \;\; \overline{f_n(\bar{b}_1, \bar{b}_2, \cdots, \bar{b}_n)}]^T$ in the state diagram of Galois NFSR2. Let $a_i = \bar{b}_i$ for all $i = 1, 2, \cdots, n$. Then there is an edge from $[\bar{a}_1 \;\; \bar{a}_2 \;\; \dots \;\; \bar{a}_n]^T$ to $[\overline{f_1(a_1, a_2, \dots, a_n)} \;\; \overline{f_2(a_1, a_2, \dots, a_n)} \;\; \dots \;\; \overline{f_n(a_1, a_2, \dots, a_n)}]^T$ in the state diagram of Galois NFSR2. Therefore, the state diagram of Galois NFSR2 is dual isomorphic to that of Galois NFSR1.

Case 2: If the state diagram of Galois NFSR3 is anti-isomorphic to that of Galois NFSR1, then there is an edge from $[a_n \;\; a_{n-1} \;\; \dots \;\; a_1]^T$ to $[f_n(a_1, a_2, \dots, a_n) \;\; f_{n-1}(a_1, a_2, \dots, a_n) \;\; \cdots \;\; f_1(a_1, a_2, \dots, a_n)]^T$ in the state diagram of the Galois NFSR3. Let $b_i = a_{n-i+1}$ for all $i = 1, 2, \dots, n$. Then, there is an edge from $[b_1 \;\; b_2 \;\; \dots \;\; b_n]^T$ to $[f_n(b_n, b_{n-1}, \dots, b_1) \;\; f_{n-1}(b_n, b_{n-1}, \dots, b_1) \;\; \dots \;\; f_1(b_n, b_{n-1}, \dots,$

$b_1)]^T$ in the state diagram of the Galois NFSR3. Thereby, the feedback $R_{\mathbf{f}}$ of Galois NFSR3 satisfies Equation (9).

Conversely, if the feedback $R_{\mathbf{f}}$ of Galois NFSR3 satisfies Equation (9), then there is edge from $[b_1 \ \ b_2 \ \ldots \ b_n]^T$ to $[f_n(b_n, b_{n-1}, \ldots, b_1) \ \ f_{n-1}(b_n, b_{n-1}, \ldots, b_1) \ \ldots \ f_1(b_n, b_{n-1}, \ldots, b_1)]^T$ in the state diagram of the Galois NFSR3. Let $a_i = b_{n-i+1}$ for all $i = 1, 2, \ldots, n$. Thus, there is an edge from $[a_n \ \ a_{n-1} \ \ldots \ a_1]^T$ to $[f_n(a_1, a_2, \ldots, a_n) \ \ f_{n-1}(a_1, a_2, \ldots, a_n) \ \cdots \ f_1(a_1, a_2, \ldots, a_n)]^T$ in the state diagram of Galois NFSR3. Therefore, the state diagram of Galois NFSR3 is anti-isomorphic to that of Galois NFSR1.

Case 3: From Cases 1 and 2, we can easily follow Case 3. □

Theorem 1 generalizes the results of Lemma 2 for Fibonacci NFSRs to Galois ones, and improves the necessary condition to the necessary and sufficient condition, using the proof method similar to that in [9].

Theorem 2. *For an n-stage nonsingular Galois NFSR1 with feedback $\mathbf{f}$, the state diagram of an n-stage nonsingular Galois NFSR2 has a direction opposite to that of the Galois NFSR1, if and only if Galois NFSR2 has the feedback $\mathbf{f}^{-1}$.*

Proof. Since the Galois NFSR1 is nonsingular, its feedback $\mathbf{f}$ is invertible, and each state has unique predecessor and unique successor.

If the state diagram of an n-stage nonsingular Galois NFSR2 has a direction opposite to that of NFSR1, then for any state $\mathbf{X}$, its successor $\mathbf{Y}$ (i.e., $\mathbf{Y} = \mathbf{f}(\mathbf{X})$) in the state diagram of NFSR1 becomes its predecessor (i.e., $\mathbf{X} = \mathbf{f}^{-1}(\mathbf{Y})$) in the sate diagram of NFSR2. Due to the arbitrariness of state $\mathbf{X}$, we can infer that the Galois NFSR2 has the feedback $\mathbf{f}^{-1}$.

Conversely, if Galois NFSR2 has the feedback $\mathbf{f}^{-1}$, then the for any state $\mathbf{Y}$, its successor $\mathbf{X}$ (i.e., $\mathbf{X} = \mathbf{f}^{-1}(\mathbf{Y})$) in the state diagram of NFSR2 becomes its predecessor (i.e., $\mathbf{Y} = \mathbf{f}(\mathbf{X})$)) in the sate diagram of NFSR1. Due the arbitrariness of state $\mathbf{Y}$, we can conclude that the state diagram of Galois NFSR2 has a direction opposite to that of NFSR1. □

Corollary 1. *For an n-stage nonsingular Fibonacci NFSR1 with feedback function $f = X_1 + \tilde{f}(X_2, X_3, \cdots, X_n)$, the state diagram of an n-stage Galois NFSR2 has a direction opposite to that of NFSR1 if and only if the Galois NFSR2 has the feedback $\mathbf{g} = [g_1 \ \ g_2 \ \ldots \ g_n]^T$ satisfying*

$$\begin{cases} g_1 = X_n + \tilde{f}(X_1, X_2, \cdots, X_{n-1}), \\ g_2 = X_1, \\ g_3 = X_2, \\ \quad \vdots \\ g_n = X_{n-1}. \end{cases} \tag{11}$$

Proof. As a particular nonsingular Galois NFSR, the nonsingular Fibonacci NFSR1 with feedback function $f = X_1 + \tilde{f}(X_2, X_3, \cdots, X_n)$ has the feedback

$\mathbf{f} = [f_1 \ \ f_2 \ \ \dots \ \ f_n]^T$ satisfying

$$\begin{cases} f_1 = X_2, \\ f_2 = X_3, \\ \quad \vdots \\ f_{n-1} = X_n, \\ f_n = X_1 \oplus f(X_2, X_3, \dots, X_n). \end{cases}$$

By direct computation, we can deduce that $\mathbf{f}^{-1} = \mathbf{g}$ satisfying Equation (11). Then the result follows from Theorem 2. □

Remark 1. The n-stage Galois NFSR2 with feedback $\mathbf{g} = [g_1 \ \ g_2 \ \ \dots \ \ g_n]^T$ satisfying (11) is actually an n-stage Fibonacci NFSR with feedback function $R_f(X_1, X_2, \dots, X_n) = f(X_n, X_{n-1}, \dots, X_1)$, where f is the feedback function of the Fibonacci NFSR in Corollary 1. It implies that two n-stage anti-isomorphic Fibonacci NFSRs, actually, have their state diagrams with directions opposite to each other.

4 Equivalence of Galois NFSRs

In this section, we give some characterizations for two kinds of equivalent Galois NFSRs.

Theorem 3. *If an n-stage τ-terminal-bit Galois NFSR with feedback $\mathbf{f} = [f_1 \ \ f_2 \ \ \dots \ \ f_n]^T$ is equivalent to an n-stage Fibonacci NFSR, then its feedback function $f_{\tau+1}$ satisfies*

$$\begin{aligned} & wt\left([f_{\tau+1}(2^n-1), f_{\tau+1}(2^n-2), \cdots, f_{\tau+1}(2^n-2^{n-\tau-1})]\right) \\ & = wt\left([f_{\tau+1}(2^n-2^{n-\tau-1}-1), f_{\tau+1}(2^n-2^{n-\tau-1}-2), \cdots, f_{\tau+1}(2^n-2^{n-\tau})]\right) \\ & = \cdots \\ & = wt\left([f_{\tau+1}(2^{n-\tau-1}-1), f_{\tau+1}(2^{n-\tau-1}-2), \cdots, f_i(0)]\right) = 2^{n-\tau-2}. \end{aligned}$$

Proof. We use the semi-tensor product based Boolean network theory. Then, the Galois NFSR represented by nonlinear system $\mathbf{X}(t+1) = \mathbf{f}(\mathbf{X}(t))$ with $\mathbf{X} \in \mathbb{F}_2^n$ has a linear system representation $\mathbf{x}(t+1) = L_g\mathbf{x}(t)$ with $\mathbf{x} \in \Delta_{2^n}$, and the Fibonacci NFSR represented by nonlinear system $\mathbf{Y}(t+1) = \mathbf{h}(\mathbf{Y}(t))$ with state $\mathbf{Y} \in \mathbb{F}_2^n$ has a linear system representation $\mathbf{y}(t+1) = L_f\mathbf{y}(t)$ with $\mathbf{y} \in \Delta_{2^n}$.

If the n-stage τ-terminal-bit Galois NFSR is equivalent to an n-stage Fibonacci NFSR, then according to Lemma 4, there exists a bijection $\varphi : \mathbf{X} \mapsto \mathbf{Y}$ such that $\varphi(\mathbf{f}(\mathbf{X})) = \mathbf{h}(\varphi(\mathbf{X}))$ and Equation (7) holds. It means there is a transformation $\mathbf{y} = P\mathbf{x}$ such that $L_g = P^T L_f P$, and $P = \delta_{2^n}[j_1 \ j_2 \ \cdots \ j_{2^n}]$ satisfies $1 \le j_i \le 2^{n-\tau-1}, 1 + 2^{n-\tau-1} \le j_{2^{n-\tau-1}+i} \le 2^{n-\tau}, \cdots, 1 + 2^n - 2^{n-\tau-1} \le j_{2^n-2^{n-\tau-1}+i} \le 2^n$ for all $i = 1, 2, \cdots, 2^{n-\tau-1}$.

Let $L_f = \delta[\eta_1 \ \eta_2 \ \cdots \ \eta_{2^n}]$ and $L_g = \delta_{2^n}[\xi_1 \ \xi_2 \ \cdots \ \xi_{2^n}]$. Then,

$$\begin{aligned} L_g &= P^T L_f P = P^T \delta_{2^n}[\eta_1 \ \eta_2 \ \cdots \ \eta_{2^n}]\delta_{2^n}[j_1 \ j_2 \ \cdots \ j_{2^n}] \\ &= (\delta_{2^n}[j_1 \ j_2 \ \cdots \ j_{2^n}])^T \delta[\eta_{j_1} \ \eta_{j_2} \ \cdots \ \eta_{j_{2^n}}], \end{aligned}$$

which yields,

$$\delta_{2^n}^{\xi_i} = (\delta[j_1\ j_2\ \cdots\ j_{2^n}])^T\, \delta_{2^n}^{\eta_{j_i}}, i = 1, 2, \cdots, 2^n,$$

that is,

$$[0\ \cdots\ \underset{\xi_i-th}{0\ 1\ 0}\ \cdots\ 0]^T = (\delta_{2^n}[j_1\ j_2\ \cdots\ j_{2^n}])^T\, [0\ \cdots\ \underset{\eta_{j_i}-th}{0\ 1\ 0}\ \cdots\ 0]^T.$$

From the above equation, we can see that the column vector $[0\ \cdots\ \underset{\xi_i-th}{0\ 1\ 0}\ \cdots\ 0]^T$ is just a row permutation of $[0\ \cdots\ \underset{\eta_{j_i}-th}{0\ 1\ 0}\ \cdots\ 0]^T$ via the permutation $(j_1\ j_2\ \cdots j_{2^n})$. Clearly, if $1 \le j_i \le 2^{n-\tau-1}$, then $1 \le \eta_{j_i} \le 2^{n-\tau-1}$ and thereby $1 \le \xi_i \le 2^{n-\tau-1}$. Similarly, if $1 + k2^{n-\tau-1} \le j_i \le (k+1)2^{n-\tau-1}$, then $1 + k2^{n-\tau-1} \le \eta_{j_i} \le (k+1)2^{n-\tau-1}$ and thereby $1 + k2^{n-\tau-1} \le \xi_i \le (k+1)2^{n-\tau-1}$ for all $k = 0, 1, 2, \cdots, 2^{\tau+1} - 1$.

According to Lemma 6, we deduce that there are $2^{n-\tau-2}$ η_is satisfying $1 \le \eta_i \le 2^{n-\tau-1}$, and 2^{n-3} η_is satisfying $1 + 2^{n-\tau-1} \le \eta_i \le 2^{n-\tau}$ with $1 \le i \le 2^{n-\tau-1}$. Similarly, there are $2^{n-\tau-2}$ η_is satisfying $1 + k2^{n-\tau-1} \le \eta_i \le (k+1)2^{n-\tau-1}$, $2^{n-\tau-2}$ η_is satisfying $1 + (k+1)2^{n-\tau-1} \le \eta_i \le (k+2)2^{n-\tau-1}$ with $1 + k2^{n-\tau-1} \le i \le (k+1)2^{n-\tau-1}$, $k = 0, 1, 2, \cdots, 2^{\tau+1} - 1$. Hence, there are $2^{n-\tau-2}$ ξ_is satisfying $1 + k2^{n-\tau-1} \le \xi_i \le (k+1)2^{n-\tau-1}$, $2^{n-\tau-2}$ ξ_is satisfying $1 + (k+1)2^{n-\tau-1} \le \xi_i \le (k+2)2^{n-\tau-1}$, with $1 + k2^{n-\tau-1} \le i \le (k+1)2^{n-\tau-1}$, $k = 0, 1, 2, \cdots, 2^{\tau+1} - 1$.

From Lemma 5, we know

$$\xi_i = 2^n - 2^{n-1} f_1(2^n - i) - 2^{n-2} f_2(2^n - i) - \cdots - 2f_{n-1}(2^n - i) - f_n(2^n - i)$$

for all $j = 1, 2, \cdots, 2^n$. Clearly, $1 \le \xi_i \le 2^{n-\tau-1}$ yields

$$2^n - 2^{n-\tau-1} \le 2^{n-1} f_1(2^n - i) + 2^{n-2} f_2(2^n - i) + \cdots + f_n(2^n - i) \le 2^n - 1.$$

It means $f_{\tau+1}(2^n - i) = 1$. Similarly, if $1 + 2^{n-\tau-1} \le \xi_i \le 2^{n-\tau}$, then $f_{\tau+1}(2^n - i) = 0$; and if $1 + 2^{n-\tau} \le \xi_i \le 3 \times 2^{n-\tau-1}$, then $f_{\tau+1}(2^n - i) = 1$. Keeping the same reasoning, we can infer that, if $1 + (2^{\tau+1} - 2)2^{n-\tau-1} \le \xi_i \le (2^{\tau+1} - 1)2^{n-\tau-1}$, then $f_{\tau+1}(2^n - i) = 0$, and if $1 + (2^{\tau+1} - 1)2^{n-\tau-1} \le \xi_i \le 2^n$, then $f_{\tau+1}(2^n - i) = 1$. Therefore, there are $2^{n-\tau-2}$ ones in $[f_{\tau+1}(2^{n-\tau-1} - 1), f_{\tau+1}(2^{n-\tau-1} - 2), \cdots, f_{\tau+1}(0)]$, and in $[f_{\tau+1}(2^{n-\tau} - 1), f_{\tau+1}(2^{n-\tau} - 2), \cdots, f_{\tau+1}(2^{n-\tau-1})]$, till in $[f_{\tau+1}(2^n - 1), f_{\tau+1}(2^n - 2), \cdots, f_{\tau+1}(2^n - 2^{n-\tau-1})]$. □

Example 1. Consider a 4-stage 2-terminal-bit Galois NFSR with feedback $\mathbf{f} = [f_1\ \ f_2\ \ f_3\ \ f_4]^T$ satisfying

$$\begin{cases} f_1 = X_2, \\ f_2 = X_3, \\ f_3 = X_4 \oplus X_1X_2X_3, \\ f_4 = 1 \oplus X_1 \oplus X_2 \oplus X_2X_3 \oplus X_2X_4 \oplus X_1X_2X_3. \end{cases}$$

Table 1. the truth table of f_3 tables.

X	1111	1110	1101	1100	1011	1010	1001	1000
$f_3(X)$	0	1	1	0	1	0	1	0
X	0111	0110	0101	0100	0011	0010	0001	0000
$f_3(X)$	1	0	1	0	1	0	1	0

This Galois NFSR is equivalent to a 4-stage Fibonacci NFSR with feed back function $f = 1 \oplus X_1 \oplus X_2 \oplus X_2X_3 \oplus X_2X_4 \oplus X_2X_3X_4$. We can get the truth table of f_3, listed in Table 1.

It satisfies $wt([f_3(15), f_3(14)]) = wt([f_3(13), f_3(12)]) = \cdots = wt([f_3(1), f_3(0)]) = 1$, consistent with the result in Theorem 3.

The following result gives some Boolean functions satisfying the necessary condition of Theorem 3.

Proposition 1. *The Boolean function*

$$f(X_1, X_2, \cdots, X_n) = X_{i+1} \oplus g(X_{i+2}, X_{i+3}, \cdots, X_n) \ \ or$$

$$f(X_1, X_2, \cdots, X_n) = X_{i+1} \oplus u(X_1, X_2, \cdots, X_i, X_{i+2}, \cdots, X_n)$$

satisfies

$$wt([f(2^n - 1), \cdots, f(2^n - 2^{n-i})]) = \cdots = wt([f(2^{n-i} - 1), \cdots, f(0)]) = 2^{n-i-1}.$$

Proof. For the first case of $f(X_1, X_2, \cdots, X_n) = X_{i+1} \oplus g(X_{i+2}, X_{i+3}, \cdots, X_n)$, we note that f is actually not relative to $X_1, X_2, \ldots, X_i$. For this case, we set $Y_j = X_{i+j}$ for all $j = 1, 2, \cdots, n-i$, and set $h = f$. Then, $h(Y_1, Y_2, \cdots, Y_{n-i}) = Y_1 \oplus g(Y_2, Y_3, \cdots, Y_{n-i})$. The function h is, clearly, an $(n-i)$-variable function and is linear with respect to the variable Y_1. Hence, h is balanced, and thereby $wt(h) = 2^{n-i-1}$.

On the other hand, note that $f(2^n - 1), f(2^n - 2), \cdots, f(2^n - 2^{n-i})$ are the possible values of $f(1, 1, \cdots, 1, 1, X_{i+1}, \cdots, X_n)$. Similarly, we can get $f(2^n - 2^{n-i} - 1), f(2^n - 2^{n-i} - 2), \cdots, f(2^n - 2 \times 2^{n-i})$ are the possible values of $f(1, 1, \cdots, 1, 0, X_{i+1}, \cdots, X_n)$. By the same reasoning, we have $f(2^{n-2}-1), f(2^{n-2} -2), \cdots, f(0)$ are the possible values of $f(0, 0, \cdots, 0, 0, X_{i+1}, \cdots, X_n)$. Together considering $f(1, 1, \cdots, 1, 1, X_{i+1}, \cdots, X_n) = f(1, 1, \cdots, 1, 0, X_{i+1}, \cdots, X_n) = \cdots = f(0, 0, \cdots, 0, 0, X_{i+1}, \cdots, X_n)$, we can infer that the result holds for the first case.

For the second case of $f(X_1, X_2, \ldots, X_n) = X_{i+1} \oplus u(X_1, X_2, \ldots, X_i, X_{i+2}, \ldots, X_n)$, any one of $\{u(1, 1, \cdots, 1, 1, X_{i+2}, \cdots, X_n), u(1, 1, \cdots, 1, 0, X_{i+2}, \cdots, X_n), \cdots, u(0, 0, \cdots, 0, 0, X_{i+2}, \cdots, X_n)\}$ has a function $g(X_{i+2}, X_{i+3}, \cdots, X_n)$ equal to it. Keeping the reasoning similar to the first case, we can prove the result holds for the second case. □

Let a sequence set $S = \{(s_i)_{i\geq 1} | s_i \in \mathbb{F}_2\}$, and $\bar{S} = \{(\bar{s}_i)_{i\geq 1} | (s_i)_{i\geq 1} \in S\}$. $\bar{S}$ is called the complementary set of S.

Proposition 2. *The output sequence set S of an n-stage Fibonacci NFSR is equal to its complementary set $\overline{S}$, if and only if the feedback function f of the Fibonacci NFSR satisfies $f = D_f$.*

Proof. Clearly, an output sequence $(s_i)_{i\geq 1} \in S$ if and only if $(\bar{s_i})_{i\geq 1} \in \overline{S}$. In an n-stage Fibonacci NFSR, $S_i = [s_i \quad s_{i+1} \quad \dots \quad s_{i+n-1}]^T$ with $i \geq 1$ is a state of the Fibonacci NFSR. Therefore, $S = \bar{S}$ means that, there is a path $S_1, S_2, \cdots, S_k (k \leq 2^n)$ in a Fibonacci state diagram if and only if there is also a path $\bar{S}_1, \bar{S}_2, \cdots, \bar{S}_k$. The mapping $D : S_r \mapsto \bar{S}_r$ with $1 \leq r \leq k$ is a dual mapping. Therefore, we can get the Fibonacci NFSR's state diagram G satisfies $G = DG$, where DG is a dual graph of G. According to Theorem 1, the result follows. □

Remark 2. From the security perspective, those Fibonacci NFSR with output sequence set equal to its complementary set should be avoided in the design of NFSR-based stream ciphers, due to the "bad" randomness of output sequences.

Example 2. For a 3-bit Fibonacci NFSR with feedback function $f(X_1, X_2, X_3) = X_1X_2 \oplus X_2X_3 \oplus X_1X_3$, we get its state diagram as:

$$110 \to 101 \to 011 \to 111 \circlearrowleft;$$
$$001 \to 010 \to 100 \to 000 \circlearrowleft .$$

Obviously, the feedback function f of the Fibonacci NFSR satisfies $f = D_f$, and its output sequence set is equal to its complementary set, consistent with the result in Proposition 4.

Corollary 2. *For two n-stage Fibonacci NFSRs with feedback functions f and $f^{'}$ satisfying $f^{'} = f \oplus 1$. If one Fibonacci NFSR satisfies its output sequence set equal to its complementary set, then the other also satisfies this property.*

Proof. Without loss of generality, we assume the Fibonacci NFSR with feedback function f satisfies its output sequence set equal to its complementary set. Then, according to Proposition 2, we know $D_f = f$. Together taking into consideration $f^{'} = f \oplus 1$, we have

$$\begin{aligned} &D_{f'}(X_1, X_2, \cdots, X_n) = \overline{f'(\bar{X}_1, \bar{X}_2, \cdots, \bar{X}_n)} = f(\bar{X}_1, \bar{X}_2, \cdots, \bar{X}_n) \\ &= D_f(X_1, X_2, \cdots, X_n) \oplus 1 = f(X_1, X_2, \cdots, X_n) \oplus 1 = f^{'}(X_1, X_2, \cdots, X_n). \end{aligned}$$

According to Proposition 2 again, we know Corollary 2 holds. □

Proposition 3. *Suppose an n-stage Fibonacci NFSR represented by a nonlinear system $\mathbf{Y}(t+1) = \mathbf{h}(\mathbf{Y}(t))$ with $\mathbf{Y} \in \mathbb{F}_2^n$ satisfies its output sequences set equal to its the complementary set. An n-stage Galois NFSR represented by a nonlinear system $\mathbf{X}(t+1) = \mathbf{f}(\mathbf{X}(t))$ with $\mathbf{Y} \in \mathbb{F}_2^n$ is equivalent to the n-stage Fibonacci NFSR 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 $[1 \quad 0 \quad \dots \quad 0]\varphi(\mathbf{X}) = \mathbf{X}$ or $[1 \quad 0 \quad \dots \quad 0]\varphi(\mathbf{X}) = \mathbf{X} \oplus 1$ for all $\mathbf{X} \in \mathbb{F}_2^n$.*

Proof. Let S be the set of output sequences of the n-stage Fibonacci NFSR. Then $S = \bar{S}$ means for any sequence $(s_i)_{i\geq 1} \in S$, we have $(s_i \oplus 1)_{i\geq 1} \in S$ as well, denoted by **Property 1**.

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 3, their state diagrams are isomorphic, which is equivalent to that there exists a bijective mapping $\varphi : \mathbf{X} \mapsto \mathbf{Y}$ such that $\varphi(\mathbf{f}(\mathbf{X})) = \mathbf{h}(\mathbf{Y}) = \mathbf{h}(\varphi(\mathbf{X}))$ for all $\mathbf{X} \in \mathbb{F}_2^n$. Note that an NFSR usually uses the content of the lowest bit as its output. Together taking into consideration Property 1, we can infer that the mapping φ must make the first component $\mathbf{Y}$ equal or complementary to the first component of $\mathbf{X}$, that is, $[1\ \ 0\ \ \ldots\ \ 0]\varphi(\mathbf{X}) = \mathbf{X}$ or $[1\ \ 0\ \ \ldots\ \ 0]\varphi(\mathbf{X}) = \mathbf{X} \oplus 1$ for all $\mathbf{X} \in \mathbb{F}_2^n$.

Sufficiency: If there exists a bijective mapping $\varphi : \mathbf{X} \mapsto \mathbf{Y}$ such that $\varphi(\mathbf{f}(\mathbf{X})) = \mathbf{h}(\varphi(\mathbf{X}))$, 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 $[1\ \ 0\ \ \ldots\ \ 0]\varphi(\mathbf{X}) = \mathbf{X}$ or $[1\ \ 0\ \ \ldots\ \ 0]\varphi(\mathbf{X}) = \mathbf{X} \oplus 1$ for all $\mathbf{X} \in \mathbb{F}_2^n$, then their sets of output sequences are equal or complementary provided that Property 1 holds. □

Theorem 4. *If an n-stage Fibonacci NFSR satisfies its output sequences set equal to its the complementary set, then there are $2 \times (2^{n-1}!)^2$ Galois NFSRs are equivalent to the Fibonacci NFSR.*

Proof. Different diagrams correspond to different Galois NFSRs. According to Proposition 3, we can only count the number of bijective mappings φ. Suppose the bijective mapping $\varphi : \mathbf{X} \mapsto \mathbf{Y}$ making the first component $\mathbf{Y}$ equal to the first component of $\mathbf{X}$. Thereby, if the first component of $\mathbf{X}$ is given, then the first component of $\mathbf{Y}$ is given as well. Clearly, the first component of $\mathbf{X}$ has two possible forms: 0 or 1, say, $\mathbf{X} = [0\ \ X_2\ \ \ldots\ \ X_n]^T$. Then $\mathbf{Y} = [0\ \ Y_2\ \ \ldots\ \ Y_n]^T$. The mapping $\varphi : \mathbf{X} = [0\ \ X_2\ \ \ldots\ \ X_n]^T \mapsto \mathbf{Y} = [0\ \ Y_2\ \ \ldots\ \ Y_n]^T$ has $(2^{n-1}!)$ possible forms. Thus, the bijective mapping $\varphi : \mathbf{X} \mapsto \mathbf{Y}$ making the first component $\mathbf{Y}$ equal to the first component of $\mathbf{X}$ has $(2^{n-1}!)^2$ possible forms. Similarly, we can easily observe that the bijective mapping $\varphi : \mathbf{X} \mapsto \mathbf{Y}$ making the first component $\mathbf{Y}$ complementary to the first component of $\mathbf{X}$ has $(2^{n-1}!)^2$ possible forms as well. Therefore, the result follows. □

5 Conclusion

This paper considered the isomorphism and equivalence of Galois NFSRs. It characterized the feedback of several kinds of isomorphic Galois NFSRs. In addition, the characterizations of two kinds of equivalent Galois NFSRs were revealed from the perspectives of their feedback functions and numbers. In the future, it will be interesting to find more characterizations of isomorphic and/or equivalent Galois NFSRs to benefit the design of NFSR-based stream ciphers.

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

References

1. Hell M., Johansson T., Meier W.: The Grain Family of Stream ciphers. LNCS **4986**, 179-190 (2008)
2. Cannièere De C., Preneel B.: Trivium. LNCS **4986**, 244-266 (2008)
3. Dubrova E.: A transformation from the Fibonacci to the Galois NLFSRs. IEEE Trans. Inf. Theory, **55**, 5263-5271 (2009)
4. Cheng D., Qi H., Li Z.: Analysis and Control of Boolean Networks. Springer-Verlag, London, U. K. (2011)
5. Cheng D., Qi H., Zhao Y.: An Introduction To Semi-Tensor Product of Matrices And Its Applications. World Scientific Publishing Company, Singapore (2012)
6. Zhao D., Peng H., Li L., Hui S., Yang Y.: Novel way to research nonlinear feedback shift register. Science China Information Sciences **57**(9), 1-14 (2014)
7. Zhong J., Lin D.: Driven stability of nonlinear feedback shift registers. IEEE Trans. Communications **64**(6), 2274-2284 (2016)
8. Zhong J., Lin D.: On minimum period of nonlinear feedback shift registers in Grain-like structure. IEEE Trans. Inf. Theory **64**(9), 6429-6442 (2018)
9. Wan Z., Dai Z., Liu M. et al.: Nonlinear shift register (in Chinese), Science Press, 1978.
10. Zhong J., Lin D.: A new linearization method of nonlinear feedback shift registers. J. Comput. Syst. Sci. **81**(4), 783-796 (2015)
11. X.-X. Zhao, Q.-X. Zheng, Z.-X. Wang, W.-F. Qi: On a class of isomorphic NFSRs. Des. Codes Cryptogr. **88**(6), 1205-1226 (2020)
12. Dubrova E.: Finding matching initial states for equivalent NLFSRs in the Fibonacci and the Galois configurations. IEEE Trans. Inf. Theory, **56**, 2961-2966 (2010)
13. Lin Z.: The transformation from the Galois NLFSR to the Fibonacci Configuration. In: EI-DWT 2013, USA, NJ, Piscataway: IEEE Press, 2013, pp. 335-339
14. Mykkeltveit J., Siu M.-K. and Ton P.: On the cylcle structure of some nonlinear shift register sequences. Inf. Control, **43**(2), 202-215 (1979)
15. Zhong J., Pan Y., Lin D. (2021) On Galois NFSRs Equivalent to Fibonacci Ones. In: Wu Y., Yung M. (eds) Information Security and Cryptology. Inscrypt 2020. LNCS **12612**, 433-449 (2021)
16. Pan Y., Zhong J. and Lin D.: On Galois NFSRs with terminal bits. In: 2021 IEEE International Symposium on Information Theory (ISIT 2021), to appear.
17. Roger A.H., Johnson C.R.: Topics in Matrix Analysis. Cambridge University Press, UK, (1991)
18. Qi H. and Cheng D.: Logic and logic-based control. J. Contr. Theory Appl, **6**(1), 123-133 (2008)
19. Barbier M., Cheballah H., Bars Le J.-M.: On the computation of the Mobius transform. Theoretical Computer Sciences **809**, 171-188 (2020)
20. Golomb S. W.: Shift Register Sequences. Holden-Day, Laguna Hills, CA, USA, (1967)
21. Zhong J. and Lin D.: Decomposition of nonlinear feedback shift registers based on Boolean networks. Science China Information Sciences, **62**(3), 39110:1-39110:3 (2019)