Cycle Structure and Observability of Two Types of Galois NFSRs

Xianghan Wang, Jianghua Zhong, Dongdai Lin

Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100085, China

Email: {wangxianghan,zhongjianghua,ddlin}@iie.ac.cn

Abstract

Nonlinear feedback shift registers (NFSRs) are used in many stream ciphers as their main building blocks. One security criterion for the design of a stream cipher is to assure its keystream has a long period. To meet this criterion, the NFSR used in a stream cipher must have a long state cycle. Further, to simultaneously avoid equivalent keys, the keystream's period is not compressed compared to the NFSR's state cycle length, which can be guaranteed if the NFSR is observable in the sense that any two distinct initial states are distinguishable from their resulting output sequences. The cycle structure of a general NFSR remains an open hard problem. Constructing Fibonacci NFSRs with maximum state cycles has therefore attracted much attention, but so far such Fibonacci NFSRs with known feedback functions have been found only for their stage numbers no greater than 33.

Considering that Galois NFSRs may decrease the area and increase the throughput compared to Fibonacci NFSRs, this paper studies two types of n-stage Galois NFSRs, whose state transition matrices are circulant matrices with only one nonzero element of 1 in each column. The cycle structure and observability of both types are disclosed using the semi-tensor product based Boolean network approach. In the first type, each Galois NFSR has the state transition matrix, in which the position of the element 1 in the first column is even. It has the maximum state cycle with an arbitrary stage number and an explicit feedback functions. It is observable if and only if its output function is dependent on the first state bit. In the second type, each Galois NFSR has the state transition matrix, in which the position of the element 1 in the first column is $2^m + 1$ with positive integer $m \leq n - 1$ for the NFSR's stage number n. It has 2^m cycles of length 2^{n-m}, and it is observable if its output function is dependent on all the state bits whose indices are no smaller than $n - m + 1$.

Keywords: shift register, stream cipher, cycle structure, observablility, semi-tensor product, Boolean network

1 Introduction

Shift registers are commonly used in stream cipher designs, due to their efficiency and good statistical properties. According to whether the feedback function is linear or not, shift registers are divided into linear feedback shift registers (LFSRs) and nonlinear feedback shift registers (NFSRs). The latter, which have taken the place of the former, are used as the main building blocks in many stream ciphers, such as the three hardware-oriented finalists Grain [1], Trivium [2], and Mickey [3] in the European eSTREAM project. According to the implementation structure, NFSRs are usually classified into Fibonacci NFSRs and Galois NFSRs. A Fibonacci NFSR has the feedback only applied to the last bit, and its other bits only involve shift, see Figure 1(a). A Galois NFSR has the feedback availably applied to every bit, shown in Figure 1(b).

An NFSR has the same mathematical model as a Boolean network, which can be described by a set of difference equations via Boolean functions. Boolean network was firstly introduced in 1969 by Kauffman to model a genetic network [4]. In the community of systems and control, Cheng and his collaborators developed an algebraic framework for Boolean networks, using a powerful mathematical tool named semi-tensor product of matrices, which builds an algebraic framework for Boolean networks [5]. This algebraic framework facilitates the solving of many fundamental problems of Boolean networks, for instance, the observability problems. Till now, much work has been done on the observability of Boolean networks, see e.g., [6]-[10] and their references therein.

From the security perspective, NFSR-based stream ciphers should select observable NFSRs; otherwise, they may have equivalent keys, subject to weak key attacks [11]. In the community of cryptography, Kalouptsidis and Limniotis in 2004

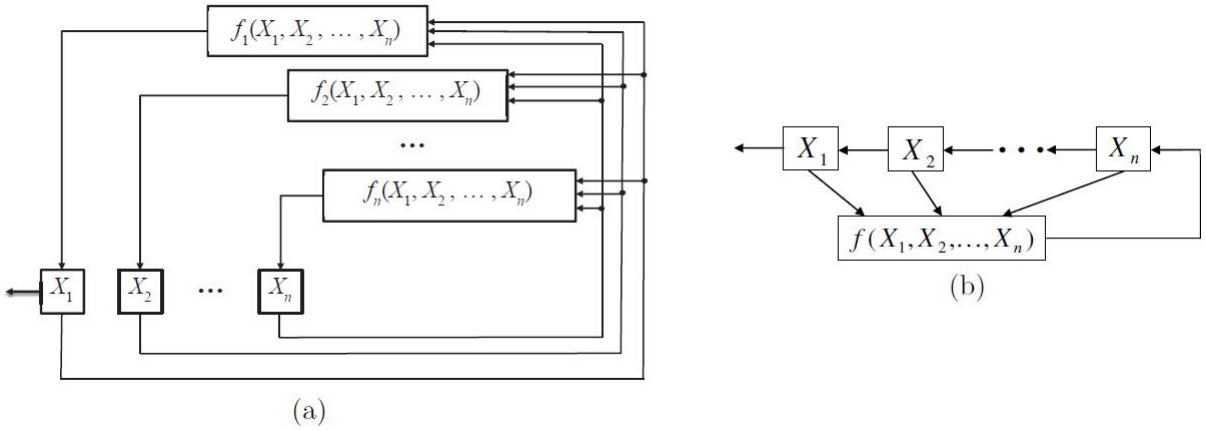

Figure 1: Galois and Fibonacci NFSRs. (a) An n-stage Galois NFSR; (b) An n-stage Fibonacci NFSR.

first proposed the notation of observability of sequence generators from the perspective of systems theory and applied it to the generators of de Bruijn sequences [12]. Since then, only one work addressed the observability of NFSRs (over the binary field) [13], which was soon generalized into the finite fields [14], the authors' best knowledge.

One of security criteria for the design of a stream cipher is to assure its keystream with long period. To meet this criterion, the NFSR used in a stream cipher must have a long state cycle. Further, to simultaneously avoid equivalent keys, the keystream's period is not compressed compared to the NFSR's state cycle length, which can be guaranteed if the NFSRs is observable in the sense that any two distinct initial states are distinguishable from their resulting output sequences.

The cycle structure of a general NFSR remains an open hard problem. LFSRs' cycle structure has been well studied [15]. However, NFSRs' cycle structure has been investigated only for some special cases. An NFSR is said to be a *maximum cycle NFSR* if it has the maximum cycle in its state diagram (or equivalently, has the maximum state cycle). The *period* of an NFSR is the length of the longest cyclic output sequence the NFSR generates. An n-stage NFSR is called a *maximum period NFSR* if it achieves the maximum period 2^n. The period of an NFSR in Grain-like structure was found to be a multiple of its LFSR's period if the LFSR is set to nonzero initial state [16]. Short state cycles were disclosed for the Galois NFSR used in the stream cipher Trivium [17]. For a cascade connection of a maximum period LFSR into a maximum period Fibonacci NFSR, its cycle structure were revealed in [18].

Much attention has been paid on constructing the maximum period Fibonacci NFSRs (or equivalently, constructing de Bruijn sequences) using the cycle joining method, for instance, see [19]-[23]. Nevertheless, in practice such Fibonacci NFSRs' feedback functions are generally hard to get. Up to now, only the maximum period Fibonacci NFSRs with stage numbers no greater than 33 have been found [24, 25]. In contrast, maximum period Galois NFSRs has been much less studied [26, 27], though Galois NFSRs may decrease the area and increase the throughput [28]

This paper considers the cycle structure and observability of two types of Galois NFSRs with circulant matrices as their state transition matrices, in which only one nonzero element of 1 in each column. In the first type, each Galois NFSR has the state transition matrix, in which the position of the element 1 is even. It is proved to be a maximum period Galois NFSR with arbitrary stage number, and to be observable if and only if its output function is dependent on the first state bit. In the second type, each Galois NFSRs has the state transition matrix, in which the position of the element 1 is $2^m + 1$ with positive integer m smaller than the Galois NFSR's stage number n. It is proved to have 2^m state cycles of length 2^{n-m}, and to be observable if its output function is dependent on all the state bits whose indices are no smaller than $n - m + 1$. Those Galois NFSRs in both types have simple feedback functions, potentially applicable to the design of new stream ciphers.

The paper is organized as follows. In Section 2, we give a brief introduction on Boolean networks and NFSRs. Our main results on the cycle structure and observability of two types of Galois NFSRs are presented in Section 3 and 4, respectively. Section 5 concludes the paper.

2 Preliminaries

In this section, we review some basic concepts and related results on Boolean networks and NFSRs. Before that, we first introduce some notations used in this paper.

Notations: $\mathbb{F}_2$ denotes the binary field, and $\mathbb{F}_2^n$ is an n-dimensional vector space over $\mathbb{F}_2$. Let δ_n^i stand for the i-th column of the $n \times n$ identity matrix I_n. Denote $\Delta_n = \{\delta_n^i | 1 \leq i \leq n\}$. $\mathcal{L}_{m\times n}$ is the set of $m \times n$ matrices. A matrix $A \in \mathcal{L}_{m\times n}$ can be written as $A = [\delta_m^{i_1}, \delta_m^{i_2}, \cdots, \delta_m^{i_n}]$. For the convenience of statements, we rewrite $A = \delta_m[i_1, i_2, \cdots, i_n]$ in a compact form. $\mathrm{Col}_j(A)$ (resp. $\mathrm{Row}_j(A)$) represents the j-th column (resp. row) of a matrix A. $+$, $-$ 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.

2.1 Boolean function

Definition 1. *An n-variable Boolean function f is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$.*

Let a constant vector $\mathbf{a} = [a_1 \ a_2 \ \dots \ a_n]^T \in \mathbb{F}_2^n$. The *support set* of a Boolean function f is

$$supp(f) = \{\mathbf{a} | f(\mathbf{a}) = 1, \mathbf{a} \in \mathbb{F}_2^n\}.$$

For a variable $X_i \in \mathbb{F}_2$ and a value $a_i \in \mathbb{F}_2$, define $X_i^{a_i} = X_i \oplus a_i \oplus 1$. Hence, $X_i^{a_i} = 1$ if and only if $X_i = a_i$. And for a binary variable vector $\mathbf{X} = [X_1 \ X_2 \ \dots \ X_n]^T$, define $\mathbf{X}^{\mathbf{a}} = X_1^{a_1} X_2^{a_2} \dots X_n^{a_n}$. Then, $\mathbf{X}^{\mathbf{a}} = 1$ if and only if $\mathbf{X} = \mathbf{a}$. Therefore, the Boolean function f can be expressed by minterms as [29]:

$$f(\mathbf{X}) = \bigoplus_{\mathbf{a}\in supp(f)} \mathbf{X}^{\mathbf{a}} = \bigoplus_{\mathbf{a}\in supp(f)} X_1^{a_1} X_2^{a_2} \dots X_n^{a_n}.$$

Let i be the decimal number corresponding to the binary $(i_1, i_2, \dots, i_n)$ via the mapping $i = i_1 2^{n-1} + i_2 2^{n-2} + \cdots + i_n$. Then i ranges from 0 to $2^n - 1$. Denote $f(i) = f(i_1, i_2, \dots, i_n)$. Then $[f(2^n - 1), f(2^n - 2), \dots, f(0)]$ is called the truth table of f, arranged in the *reverse alphabet order*. For the simplicity, throughout the paper the truth table of a Boolean function always means it is arranged in the reverse alphabet order.

Definition 2 ([30, 32])**.** *The matrix*

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

is called the structure matrix of f.

Definition 3. *The function $\mathbf{f} = [f_1 \ f_2 \ \dots \ f_n]^T$ is a vectorial function if its components $f_1, f_2, \dots, f_n$ are all Boolean functions.*

2.2 Boolean network

Definition 4 ([33])**.** *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 5 ([5])**.** *For an $n \times m$ matrix A and a $p \times q$ matrix B, let α be the least common multiple of m and p. The semi-tensor product of A and B is defined as*

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

Lemma 1 ([30])**.** *For any vector $Z = [Z_1 \quad Z_2 \quad \cdots \quad Z_r]^T \in \mathbb{F}_2^r$, let $z = [Z_1 \quad Z_1 \oplus 1]^T \ltimes [Z_2 \quad Z_2 \oplus 1]^T \ltimes \cdots \ltimes [Z_r \quad Z_r \oplus 1]^T$. Then the vector $z = \delta_{2^n}^j \in \Delta_{2^n}$ with $j = 2^r - (2^{r-1}Z_1 + 2^{r-2}Z_2 + \cdots + Z_r)$.*

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

$$\begin{cases} X(t+1) = g(X(t)), \\ Y(t) = h(X(t)), t \in \mathbb{N}. \end{cases} \tag{2}$$

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

Boolean network (2) can be equivalently expressed as a linear system [30]:

$$\begin{cases} x(t+1) = L(x(t)), \\ y(t) = H(x(t)), t \in \mathbb{N}. \end{cases} \tag{3}$$

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

$$\mathrm{Col}_j(L) = \mathrm{Col}_j(G_1) \otimes \mathrm{Col}_j(G_2) \otimes \cdots \otimes \mathrm{Col}_j(G_n), j = 1, 2, \cdots 2^n, \tag{4}$$

where G_i is the structure matrix of the i-th component g_i of the vectorial function g in (2) for any $i \in \{1, 2, \cdots, n\}$. The j-th column of H can be computed in a way similar to Equation (4) for the j-th column of L.

The following result shows how to compute the structure matrix of each Boolean function of a Boolean network from its state transition matrix.

Lemma 2 ([31]). *Let*

$$M_k = \delta_2[\underbrace{A_k, A_k, \cdots, A_k}_{2^{k-1}}] \text{ with } A_k = \delta_2[\underbrace{1, 1, \cdots, 1}_{2^{n-k}}, \underbrace{2, 2, \cdots, 2}_{2^{n-k}}].$$

Then the structure matrix of g_k in (2) is $G_k = M_k L$, where L is the state transition matrix in (3).

Definition 6 ([6]). *Two distinct initial states of a Boolean network are said to be indistinguishable, if their resulting output sequences are equal. Otherwise, the two distinct initial states are said to be distinguishable. A Boolean network is said to be observable if every two distinct initial states are distinguishable.*

Definition 7 ([6]). *The observability matrix of Boolean network (3) in N steps is defined as:*

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

Lemma 3 ([6]). *Boolean network (3) is observable if and only if the observability matrix $\mathcal{O}_{2^n-1}$ has 2^n distinct columns.*

2.3 Nonlinear feedback shift register

The n-stage Galois NFSR is composed of n binary storage devices, also called *bits*. The content of bit i is denoted as X_i, which is updated the feedback function f_i. All X_i compose the Galois NFSR's state $X = [X_1 \ X_2 \ \ldots \ X_n]^T$, and all feedback functions f_i form the Galois NFSR's feedback $F = [f_1 \ f_2 \ \cdots \ f_n]^T$. The n-stage Galois NFSR can be expressed as the following nonlinear system:

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

where t represents time instant. Equation (5) can be rewritten in a vector form as:

$$X(t+1) = F(X(t)), \tag{6}$$

where $X = [X_1 \ X_2 \ \cdots \ X_n]^T$ is the state, $F = [f_1 \ f_2 \ \cdots \ f_n]^T$ is the feedback. If the feedback functions f_i satisfy $f_i(X_1(t), X_2(t), \cdots, X_n(t)) = X_{i+1}$ for all $i = 1, 2, \cdots, n-1$, then the Galois NFSR is reduced to a Fibonacci NFSR.

The *state diagram* of an n-stage NFSR is a directed graph consisting of 2^n vertices and 2^n edges, where each vertex represents one state, and each directed edge represents a transition between two states. For instance, if state X is updated to state Y, then there is an edge from state X to state Y. In this case, X is called the predecessor of Y, and Y is called the successor of X. A state sequences $X_1, X_2, \ldots, X_d$ form a cycle of length d if the successor of X_d is X_1. An NFSR and its state diagram are a one-to-one correspondence.

Let $G = (V, A)$ and $\hat{G} = (\hat{V}, \hat{A})$ be two directed graphs, where V and $\hat{V}$ are their sets of nodes, A and $\hat{A}$ are their sets of edges. The two directed graphs G and $\hat{G}$ are said to be *isomorphic* if there exists a bijective mapping $\varphi\colon V \to \hat{V}$ such that there is an edge $E \in A$ from node N to node $\hat{N}$ in G if and only if there is an edge $\hat{E} \in \hat{A}$ from $\varphi(N)$ to $\varphi(\hat{N})$ in $\hat{G}$. Furthermore, if the bijective mapping $\varphi = D : [X_1\ X_2\ \cdots\ X_n]^T \mapsto [X_1^0\ X_2^0\ \cdots\ X_n^0]^T$, then G and $\hat{G}$ are said to be *dual isomorphic*, denoted by $\hat{G} = DG$; if the bijective mapping $\varphi = R : [X_1\ X_2\ \cdots\ X_n]^T \mapsto [X_n\ X_{n-1}\ \cdots\ X_1]^T$, then G and $\hat{G}$ are said to be *anti-isomorphic*, denoted by $\hat{G} = RG$; if the bijective mapping $\varphi = D : [X_1\ X_2\ \cdots\ X_n]^T \mapsto [X_n^0\ X_{n-1}^0\ \cdots\ X_1^0]^T$, then G and $\hat{G}$ are said to be *dual anti-isomorphic*, denoted by $\hat{G} = DRG$.

Two NFSRs of the same stage number are said to be *isomorphic* if their state diagrams are isomorphic, that is, their state diagrams are of the same cycle structure.

Lemma 4 ([34]). *For an n-stage Galois NFSR$_1$ with feedback $F = [f_1\ f_2\ \ldots\ f_n]^T$,*

1. *the state diagram of an n-stage Galois NFSR$_2$ is dual isomorphic to that of Galois NFSR$_1$, if and only if the feedback DF of the Galois NFSR$_2$ satisfies*

$$DF = [f_1(X_1^0, X_2^0, \cdots, X_n^0) \oplus 1\quad f_2(X_1^0, X_2^0, \cdots, X_n^0) \oplus 1\ \cdots\ f_n(X_1^0, X_2^0, \cdots, X_n^0) \oplus 1]^T; \tag{7}$$

2. *the state diagram of an n-stage Galois NFSR$_3$ is anti-isomorphic to that of Galois NFSR$_1$, if and only if the feedback RF of the Galois NFSR$_3$ satisfies*

$$RF = [f_n(X_n, X_{n-1}, \ldots, X_1)\quad f_{n-1}(X_n, X_{n-1}, \ldots, X_1)\ \ldots\ f_1(X_n, X_{n-1}, \ldots, X_1)]^T. \tag{8}$$

3. *the state diagram of an n-stage Galois NFSR$_4$ is dual anti-isomorphic to that of Galois NFSR1, if and only if the feedback DR of the Galois NFSR$_4$ satisfies*

$$DR = [f_n(X_n^0, X_{n-1}^0, \ldots, X_1^0) \oplus 1\quad f_{n-1}(X_n^0, X_{n-1}^0, \ldots, X_1^0) \oplus 1\ \ldots\ f_1(X_n^0, X_{n-1}^0, \ldots, X_1^0) \oplus 1]^T. \tag{9}$$

Lemma 5 ([12]). *The period of the output sequence of a Galois NFSR with an arbitrary output function is a divisor of the corresponding cycle's length.*

Viewing an NFSR as a Boolean Network, we can get the Equation (6) equivalently expressed as: $x(t+1) = Lx(t)$. The NFSR is nonsingular if and only if L is nonsingular, that is, L is a permutation matrix. In this paper, we consider the Galois NFSRs with state transition matrix of form circulant matrix $L = \delta_{2^n}[i, i+1, \cdots, 2^n, 1, 2, \cdots, i-1]$.

3 The first type of Galois NFSRs

In this section, we consider a type of n-stage Galois NFSRs with state transition matrices of form

$$L = \delta_{2^n}[i, i+1, \cdots, 2^n, 1, 2, \cdots, i-1], \text{ where } i \text{ is even.} \tag{10}$$

We first disclose that each Galois NFSR in this type has the maximum cycle in its state diagram. We then reveal its feedback functions. Finally, we disclose its observability with output functions that are only required to be dependent on the first state bit.

3.1 A type of maximum cycle Galois NFSRs

Theorem 1. *An n-stage Galois NFSR with state transition matrix L in (10), has the maximum cycle in its state diagram.*

Proof. For any state $\delta_{2^n}^i$, the positive integer i must satisfy $1 \le i \le 2^n$. Moreover, note that $L\delta_{2^n}^i = \mathrm{Col}_i(L)$. Then, we can easily obtain a state sequence of the Galois NFSR as:

$$\delta_{2^n}^1, \delta_{2^n}^i, \delta_{2^n}^{2(i-1) \bmod 2^n+1}, \cdots, \delta_{2^n}^{k(i-1) \bmod 2^n+1}, \cdots, \delta_{2^n}^{(2^n-1)(i-1) \bmod 2^n+1}, \delta_{2^n}^1, \cdots, . \tag{11}$$

An n-stage Galois NFSR has 2^n possible states. To prove the result, we are only required to prove the state sequence in (11) has the period of 2^n.

As i is even, we have $\delta_{2^n}^i \neq \delta_{2^n}^1$. Assume in (11) the state that is equal to $\delta_{2^n}^1$ for the first time is $\delta_{2^n}^{k(i-1) \bmod 2^n+1}$, that is, k is the least positive integer such that $\delta_{2^n}^{k(i-1) \bmod 2^n+1} = \delta_{2^n}^1$. Then, $k(i-1) \bmod 2^n + 1 = 1$, which implies that $2^n | k(i-1)$. Since i is even, $i-1$ is odd. Then there must exist $2^n | k$, which implies that the period of the state sequence in (11) is 2^n. □

Corollary 1. *For an n-stage Galois NFSR$_1$ with state transition matrix $L = \delta_{2^n}[i, i+1, \cdots, 2^n, 1, 2, \cdots, i-1]$, its dual isomorphic Galois NFSR$_2$ has the state transition matrix of $DL = \delta_{2^n}[2^n + 2 - i, 2^n + 3 - i, \cdots, 2^n, 1, 2, \cdots, 2^n + 1 - i]$.*

Proof. From Lemma 1, we know that a vector $[X_1 \ X_2 \ \dots \ X_n]^T \in \mathbb{F}_2^n$ uniquely corresponds to a state $\delta_{2^n}^j$, where

$$j = 2^n - (2^{n-1}X_1 + 2^{n-2}X_2 + \cdots + X_n). \tag{12}$$

The dual vector of $[X_1 \ X_2 \ \dots \ X_n]^T$ is $[X_1^0 \ X_2^0 \ \cdots \ X_n^0]^T$. Note that $X_i^0 = X_i \oplus 1 = 1 - X_i$ for all $i = 1, 2, \dots, n$. Then, we have

$$(2^{n-1}X_1 + 2^{n-2}X_2 + \cdots + X_n) + (2^{n-1}X_1^0 + 2^{n-2}X_2^0 \cdots + X_n^0) = 2^{n-1} + 2^{n-2} + \cdots + 1 = 2^n - 1. \tag{13}$$

From Equations(12) and (13), we get $2^{n-1}X_1^0 + 2^{n-2}X_2^0 \cdots + X_n^0 = j - 1$, which implies $2^n - (2^{n-1}X_1^0 + 2^{n-2}X_2^0 + \cdots + X_n^0 = 2^n - j + 1$. Hence, the dual state of $\delta_{2^n}^j$ is $\delta_{2^n}^{2^n-j+1}$ for any $j \in \{1, 2, \dots, 2^n\}$.

The Galois NFSR$_1$ has a state sequence:

$$\delta_{2^n}^1, \delta_{2^n}^i, \delta_{2^n}^{2(i-1) \bmod 2^n+1}, \cdots, \delta_{2^n}^{k(i-1) \bmod 2^n+1}, \cdots \delta_{2^n}^1, \cdots .$$

Thus, accordingly, the Galois NFSR$_2$ that is dual isomorphic to Galois NFSR$_1$ has a state sequence as:

$$\delta_{2^n}^{2^n}, \delta_{2^n}^{2^n+1-i}, \delta_{2^n}^{2^n-[2(i-1) \bmod 2^n]}, \cdots \delta_{2^n}^{2^n-[k(i-1) \bmod 2^n]}, \cdots, \delta_{2^n}^{2^n} \cdots .$$

Hence, for the Galois NFSR$_2$, its state transition matrix is $DL = \delta_{2^n}[2^n + 2 - i, 2^n + 3 - i, \cdots, 2^n, 1, 2, \cdots, 2^n + 1 - i]$. □

Corollary 1 shows that, if a Galois NFSR has the state transition matrix of form a circulant matrix, in which the position of the nonzero element of 1 in the first column is even, then so is its dual isomorphic Galois NFSR. Moreover, if the feedback $F = [f_1(X_1, \cdots, X_n) \ \ f_2(X_1, \cdots, X_n) \ \cdots \ f_n(X_1, \cdots, X_n)]^T$ of the Galois NFSR$_1$, then according to Lemma 4, the feedback DF of the dual isomorphic Galois NFSR$_2$ is of form Equation (7).

Theorem 2. *If an n-stage Galois NFSR has the state transition matrix L in (10), then its feedback function $F = [f_1 \ f_2 \ \cdots \ f_{k-1} \ f_k \ \cdots \ f_n]^T$ satisfies the recurrence relation:*

1. *if $k = n$, then $f_k = X_n^0$;*
2. *if $k \in \{1, 2, \cdots, n-1\}$, then let $j = (i-1) \bmod 2^{n-k+2} + 1$,*
   - *(a) if $1 \le j \le 2^{n-k}$, then $f_{k-1} = X_k^0 f_k \oplus X_{k-1}$;*
   - *(b) if $2^{n-k} + 1 \le j \le 2^{n-k+1}$, then $f_{k-1} = X_k f_k^0 \oplus X_{k-1}^0$;*
   - *(c) if $2^{n-k+1} + 1 \le j \le 2^{n-k+1} + 2^{n-k}$, then $f_{k-1} = X_k^0 f_k \oplus X_{k-1}^0$;*
   - *(d) if $2^{n-k+1} + 2^{n-k} + 1 \le j \le 2^{n-k+2}$, then $f_{k-1} = X_k f_k^0 \oplus X_{k-1}$.*

Proof. According to Lemma 2, we can easily see the the structure matrix of f_n is

$$M_n L = \delta_2[1, 0, 1, 0, \dots, 1, 0, 1, 0]\delta_{2^n}[i, i+1, \dots, 2^n, 1, 2, \dots, i-1] = \delta_2[0, 1, 0, 1, \dots, 0, 1, 0, 1],$$

which implies $f_n = X_n^0$.

Table 1: The corresponding values of X_k, X_{k-1}, f_k and f_{k-1}

The value range of l	X_k	X_{k-1}	f_{k-1}	f_k
$1 \le l \le 2^{n-k} - i + 1$	1	1	1	1
$2^{n-k} - i + 2 \le l \le 2^{n-k}$	1	1	1	0
$2^{n-k} + 1 \le l \le 2^{n-k+1} - i + 1$	0	1	1	0
$2^{n-k+1} - i + 2 \le l \le 2^{n-k+1}$	0	1	0	1
$2^{n-k+1} + 1 \le l \le 2^{n-k+2} - i + 1$	1	0	0	1
$2^{n-k+2} - i + 2 \le l \le 2^{n-k+2}$	1	0	0	0
$2^{n-k+2} + 1 \le l \le 2^{n-k+3} - i + 1$	0	0	0	0
$2^{n-k+3} - i + 2 \le l \le 2^{n-k+3}$	0	0	1	1

To compute the other feedback functions f_k with $k \in \{1, 2, \ldots, n-1\}$, we let $l := 2^n - (2^{n-1}X_1 + 2^{n-2}X_2 + \cdots + X_n)$ and discuss the recurrence relation between the f_k and f_{k-1} in the cases of different range of i and l as follows.

For the case of $1 \le i \le 2^{n-k}$, we can easily observe that the first values of the truth table of f_k and f_{k-1} are both 1. In the cases of different ranges of l , the values of X_k, X_{k-1}, f_k and f_{k-1} are listed in Table 3.1.

Since i is even, the numbers of ls in the above ranges are all odd. Hence, f_{k-1} can be expressed by minterms of from:

$$f_{k-1} = X_{k-1}(X_k f_k \oplus X_k f_k^0 \oplus X_k^0 f_k^0) \oplus X_{k-1}^0 X_k^0 f_k = X_k^0 f_k \oplus X_{k-1}. \tag{14}$$

In a similar way, we can get the recurrence relation the other cases of i. □

Example 1. *Consider an n-stage Galois* NFSR_1 *with state transition matrix* $L = \delta_{2^n}[2, 3, \cdots, 2^n, 1]$. *According to Theorem 2, we can get its feedback functions as:*

$$\begin{cases} f_n = X_n^0, \\ f_{n-1} = X_{n-1} \oplus X_n^0, \\ f_{n-2} = X_{n-2} \oplus X_{n-1}^0 X_n^0, \\ \quad \vdots \\ f_1 = X_1 \oplus X_2^0 X_3^0 \cdots X_n^0. \end{cases} \tag{15}$$

From Corollary 1, we can get the Galois NFSR$_2$ *that is dual isomorphic to the Galois NFSR*$_1$ *has the state transition matrix* $L = \delta_{2^n}[2^n, 1, \cdots, 2^n - 2, 2^n - 1]$, *and its feedback functions are:*

$$\begin{cases} f_n = X_n^0, \\ f_{n-1} = X_{n-1} \oplus X_n, \\ f_{n-2} = X_{n-2} \oplus X_{n-1} X_n, \\ \quad \vdots \\ f_1 = X_1 \oplus X_2 X_3 \cdots X_n, \end{cases} \tag{16}$$

which is consistent with the result of direct calculation of DF in (??).

From the feedback F of Galois NFSR_1 with state transition matrix L in (10), it is easy to get the feedbacks DF, RF, RDF of Galois NFSR_2 which are dual isomorphic, anti-isomorphic and dual anti-isomorphic to Galois NFSR_1, respectively. The explicit expressions of these feedback functions are partially shown in Table 2 in Appendix.

3.2 Observability

Lemma 6. *An n-stage maximum cycle Galois NFSR is observable if and only if there exists an initial state* $X(t_0)$ *such that its resulting output sequence* $(Y(t))_{t \ge 0}$ *satisfying* $Y(t_0) \ne Y(t_0 + 2^{n-1})$.

Proof. An n-stage maximum cycle Galois NFSR has the maximum state cycle of length 2^n. Note that the divisor of 2^n is 2^m with nonnegative integer $0 \le m \le n$. Then the result follows from Lemma 5. □

Theorem 3. *An n-stage Galois NFSR with state transition matrix L in (10) is observable if and only if the output function contains the first state bit variable X_1.*

Proof. According to the proof of Proposition 1, an n-stage Galois NFSR with state transition matrix L in (10) has a state sequence in (11). For any initial state $\delta_{2^n}^j$ with $j \in \{1, 2, \ldots, 2^n\}$ at time $t \in \mathbb{N}$, let $j = k(i-1) \bmod 2^n + 1$ for some positive integer k satisfying $1 \leq k \leq 2^n$. Then, according to state sequence in (11), $\delta_{2^n}^j$ is updated to $\delta_{2^n}^{[(2^{n-1}+k)(i-1)] \bmod 2^n+1}$ at time $t + 2^{n-1}$. Since i is even, we have $\delta_{2^n}^{[(2^{n-1}+k)(i-1)] \bmod 2^n+1} = \delta_{2^n}^{(2^{n-1}+j-1) \bmod 2^n+1}$. Assume the n-dimensional vector uniquely corresponding to the state $\delta_{2^n}^j$ is $[X_1 \ X_2 \ \cdots \ X_n]^T$. Then, according to Lemma 1, we have

$$j = 2^n - (2^{n-1}X_1 + 2^{n-2}X_2 + \cdots + X_n).$$

Note that $X_1^0 = X_0 \oplus 1 = 1 - X_0$. Then,

$$(2^{n-1} + j - 1) \bmod 2^n + 1 = 2^n - (2^{n-1}X_1^0 + 2^{n-3}X_2 + 2^{n-3}X_3 + \cdots + X_n),$$

which implies that the corresponding n-dimensional vectors of $\delta_{2^n}^j$ at time $t = 0$ and its successor at $t = 2^{n-1}$ have the different first state bits, but have the same other state bits. In other words, for any $t \in \mathbb{N}$, $X(t)$ and $X(t + 2^{n-1})$ from the state sequence over $\mathbb{F}_2^n$ that uniquely corresponds to the state sequence over Δ_{2^n} in (11), have the different first state bits, but have the same other state bits, denote by **Fact 1**.

Sufficiency: Since the output function contains the first state bit variable X_1, we can write the output function as

$$h(X_1, X_2, \cdots, X_n) = X_1 g_1(X_2, \cdots, X_n) \oplus g_2(X_2, \cdots, X_n) \text{ with } g_1(X_2, \cdots, X_n) \neq 0. \tag{17}$$

According to **Fact 1**, we have

$$h(X(t)) \oplus h(X(t + 2^{n-1})) = g_1(X_2(t), \cdots, X_n(t)) \text{ for any } t \in \mathbb{N}.$$

As $g_1(X_2, \cdots, X_n) \neq 0$, there must exist some $t_0 \in \mathbb{N}$ such that such that $g_1(X_2(t_0), \cdots, X_n(t_0)) \neq 0$, which implies that there exists some state $X(t_0)$ such that the resulting output sequence $(Y(t))_{t \geq 0}$ satisfying $Y(t_0) \neq Y(t_0 + 2^{n-1})$. According to Lemma 6, the result follows.

Necessity: Since for any initial state at time t_0 and its successor at $t_0 + 2^{n-1}$, their corresponding n-dimensional vectors have the different first state bits, but have the same other state bits. Assume the output function h is independent of the first state bit variable X_1. Then according to Equation 17, there must be $Y(t) = Y(t + 2^{n-1})$ for any $t \in \mathbb{N}$. According to Lemma 6, this Galois NFSR is unobservable, which is in contradiction with the assumption that to the Galois NFSR is observable. □

4 The second type of Galois NFSRs

In this section, we consider the n-stage Galois NFSR with state transition matrix

$$L = \delta_{2^n}[i, i+1, \cdots, 2^n, 1, 2, \cdots, i-1] \text{ where } i = 2^m + 1 \tag{18}$$

with positive integer m satisfying $1 \leq m \leq n - 1$.

First, we will disclose that each Galois NFSR in this type has 2^m cycles of length 2^{n-m} in its state diagram. Then, We will reveal its the feedback functions. Finally, we will give some necessary and/or sufficient conditions for its observability. In particular, we will show that it is observable if its output function is dependent on all the state bits whose indices are no smaller than $n - m + 1$.

4.1 A type of Galois NFSRs with equi-length state cycles

Theorem 4. *For an n-stage Galois NFSR with the state transition matrix L in (18), there are 2^m cycles of length 2^{n-m} in its state diagram.*

Proof. Similar to the proof of Theorem 1, we can easily observe that the Galois NFSR has a state sequence as:

$$\delta_{2^n}^1, \delta_{2^n}^{2^m+1}, \delta_{2^n}^{2\cdot 2^m \bmod 2^n+1}, \cdots, \delta_{2^n}^{k\cdot 2^m \bmod 2^n+1}, \cdots, \delta_{2^n}^{(2^{n-m}-1)\cdot 2^m \bmod 2^n+1}, \delta_{2^n}^1, \cdots, \tag{19}$$

which contains 2^{n-m} different states, yielding a cycle of length 2^{n-m}. Moreover, we can see that the states contained in this cycle has one same characterization: their superscripts divided by 2^m have a remainder of 1.

Similarly, the states whose superscripts divided by 2^m have the same other remainder compose another one state cycle of length 2^{n-m}. Therefore, the Galois NFSR has totally 2^m cycles of length 2^{n-m} in its state diagram. □

Theorem 5. *For an n-stage Galois NFSR$_1$ with state transition matrix $L_1 = \delta_{2^n}[i, i+1, \cdots, 2^n, 1, 2, \cdots, i-1]$ where $i = 2^m$, and for an n-stage Galois NFSR$_2$ with state transition matrix $L_2 = \delta_{2^n}[i, i+1, \cdots, 2^n, 1, 2, \cdots, i-1]$ where $i = 2^m + 1$, let $F = [f_1\ f_2\ \cdots\ f_n]^T$ and $G = [g_1\ \ g_2\ \cdots\ g_n]^T$ be their feedbacks, respectively. The feedback functions in F and G have the following relation:*

1. *if $k = n$, then $g_k = f_k \oplus 1$;*
2. *if $k = n-1$, then $g_k = f_k \oplus X_n$;*
3. *if $k \in \{1, 2, \cdots, n-2\}$, then $g_k = f_k \oplus X_{k+1}^0 X_{k+2}^0 \cdots X_{n-m}^0 X_{n-m+1} \cdots X_n$.*

Proof. According to Lemma 2, the structure matrix of the n-th feedback function g_n of NFSR$_1$ is

$$G_n = M_n L_1 = \delta_2[1\ \ 0\ \ 1\ \ 0\ \ \ldots\ 1\ \ 0\ \ 1\ \ 0]\delta_{2^n}[2^m+1, 2^m+2, \cdots, 2^n, 1, 2, \cdots, 2^m] = \delta_2[1\ \ 0\ \ 1\ \ 0\ \ \ldots\ 1\ \ 0\ \ 1\ \ 0].$$

Hence, $g_n = X_n = f_n \oplus 1$.

If we use minterms to represent a Boolean function, we are only required to consider the state at which the Boolean function takes value 1. The states $\delta_{2^n}^1, \delta_{2^n}^2, \cdots, \delta_{2^n}^{2^{n-1}}$ over Δ_{2^n} corresponds to those states whose first components are 1 over $\mathbb{F}_2^n$. To compute the support set of the first feedback function f_1 of Galois NFSR$_1$, we only need to compute the predecessors of states $\delta_{2^n}^1, \delta_{2^n}^2, \cdots, \delta_{2^n}^{2^{n-1}}$. Note that $(a+b) \bmod n = [(a \bmod n)+(b \bmod n)] \bmod n$. Then, according to the state sequence in (11) of Galois NFSR$_1$, the predecessor of state $\delta_{2^n}^j$ for any $j \in \{1, 2, \ldots, 2^n\}$ is

$$\delta_{2^n}^{[(2^n-1)(2^m-1)+j-1] \bmod 2^n+1} = \delta_{2^n}^{(j-2^m) \bmod 2^n+1} = \begin{cases} 2^n - 2^m + j + 1, & \text{if } 1 \le j \le 2^m, \\ j - 2^m + 1, & \text{if } 2^m + 1 \le j \le 2^n. \end{cases}$$

Taking into account $1 \le m \le n-1$, yielding $2 \le 2^m \le 2^{n-1}$, we can deduce that the support set of the first feedback function f_1 of Galois NFSR$_1$ is:

$$supp(f_1) = \{\delta_{2^n}^{2^n-2^m+2}, \delta_{2^n}^{2^n-2^m+3}, \delta_{2^n}^{(3-2^m) \bmod 2^n+1}, \cdots, \delta_{2^n}^{(2^{n-1}-1-2^m) \bmod 2^n+1}, \delta_{2^n}^{2^{n-1}-2^m+1}\}. \tag{20}$$

Similarly, according to the state sequence in (19) of Galois NFSR$_2$, the predecessor of state $\delta_{2^n}^j$ for any $j \in \{1, 2, \ldots, 2^n\}$ is

$$\delta_{2^n}^{[(2^{n-m}-1)2^m+j-1] \bmod 2^n+1} = \delta_{2^n}^{(j-2^m-1) \bmod 2^n+1} = \begin{cases} 2^n - 2^m + j, & \text{if } 1 \le j \le 2^m + 1, \\ j - 2^m, & \text{if } 2^m + 2 \le j \le 2^n. \end{cases}$$

Hence, the support set of the first feedback function g_1 of Galois NFSR$_2$ is:

$$supp(g_1) = \{\delta_{2^n}^{2^n-2^m+1}, \delta_{2^n}^{2^n-2^m+2}, \delta_{2^n}^{2^n-2^m+3}, \delta_{2^n}^{(3-2^m) \bmod 2^n+1}, \cdots, \delta_{2^n}^{(2^{n-1}-1-2^m) \bmod 2^n+1}\}. \tag{21}$$

From Equations (20) and (21), we can easily see that the support sets $supp(f_1)$ and $supp(g_1)$ of f_1 and g_1 have only two different states $\delta_{2^n}^{2^n+1-2^m}$ and $\delta_{2^n}^{2^{n-1}+1-2^m}$, whose corresponding n-dimensional vectors, respectively, are $\mathbf{a} = [\underbrace{0, 0, \cdots, 0}_{n-m}, \underbrace{1, 1, \cdots, 1}_{m}]^T$ and $\mathbf{b} = [1, \underbrace{0, 0, \cdots, 0}_{n-m-1}, \underbrace{1, 1, \cdots, 1}_{m}]^T$. Therefore,

$$f_1 \oplus g_1 = \mathbf{X^a} \oplus \mathbf{X^b} = X_1^0 X_2^0 \cdots X_{n-m}^0 X_{n-m+1} \cdots X_n \oplus X_1 X_2^0 \cdots X_{n-m}^0 X_{n-m+1} \cdots X_n = X_2^0 \cdots X_{n-m}^0 X_{n-m+1} \cdots X_n,$$

yielding $g_1 = f_1 \oplus X_2^0 \cdots X_{n-m}^0 X_{n-m+1} \cdots X_n$.

keeping the same reasoning, we can get $g_{n-1} = f_{n-1} \oplus X_n$, and $g_k = f_k \oplus X_{k+1}^0 \cdots X_{n-m}^0 X_{n-m+1} \cdots X_n$ for all $k = 2, 3, \cdots, n-2$. □

The feedback functions of Galois NFSR$_1$ whose state transition matrix is a circulant matrix $L = \delta_{2^n}[i, i+1, \ldots, 2^n, 1, 2, \ldots, i-1]$ with $i = 2^m$ have been given in the Appendix. So, it is easy to get the feedback functions of Galois NFSR$_2$ whose state transition matrix is a circulant matrix L with $i = 2^m + 1$.

Example 2. *For an n-stage Galois NFSR with state transition matrix $L = \delta_{2^n}[3, 4, \cdots, 2^n, 1, 2]$, according to Theorem 5, its feedback functions can be derived from the Galois NFSR in Example 1 as:*

$$\begin{cases} g_n = f_n \oplus 1 = X_n^0 \oplus 1, \\ g_{n-1} = f_{n-1} \oplus X_n = X_{n-1} \oplus X_n^0 \oplus X_n, \\ g_{n-2} = f_{n-2} \oplus X_{n-1}^0 X_n = X_{n-2} \oplus X_{n-1}^0 X_n^0 \oplus X_{n-1}^0 X_n, \\ g_{n-3} = f_{n-3} \oplus X_{n-2}^0 X_{n-1}^0 X_n = X_{n-3} \oplus X_{n-2}^0 X_{n-1}^0 X_n^0 \oplus X_{n-2}^0 X_{n-1}^0 X_n, \\ \vdots \\ g_1 = f_1 \oplus X_2^0 \cdots X_{n-1}^0 X_n = X_1 \oplus X_2^0 X_3^0 \cdots X_n^0 \oplus X_2^0 \cdots X_{n-1}^0 X_n. \end{cases} , \tag{22}$$

yielding

$$\begin{cases} g_n = X_n, \\ g_{n-1} = X_{n-1}^0, \\ g_{n-2} = X_{n-2} \oplus X_{n-1}^0, \\ g_{n-3} = X_{n-3} \oplus X_{n-2}^0 X_{n-1}^0, \\ \vdots \\ g_1 = X_1 \oplus X_2^0 X_3^0 \cdots X_{n-1}^0. \end{cases} \tag{23}$$

For an n-stage NFSR whose state transition matrix is a circulant matrix $L = \delta_{2^n}[i, i+1, \ldots, 2^n, 1, 2, \ldots, i-1]$ with $i = 2m + 1$, we can get its feedback function in a similar way. But its cycle structure and observability is related to the relation between n and m, which is much more complicated to discuss. We do not discuss this case in the paper.

4.2 Observability

Proposition 1. *For an n-stage Galois NFSR with state transition matrix L in (18), if its output function $h(X_1, X_2, \cdots, X_n) = X_j$ for any $j \in \{1, 2, \cdots n\}$, then the Galois NFSR is unobservable.*

Proof. For any $j \in \{1, 2, \cdots n\}$, the function $h(X_1, X_2, \cdots, X_n) = X_j$ has the structure matrix

$$H = [\underbrace{A \ A \ \ldots \ A}_{2^{j-1}}] \text{ with } A = \delta_2[\underbrace{1, 1, \ldots, 1}_{2^{n-j}}, \underbrace{0, 0, \ldots, 0}_{2^{n-j}}]. \tag{24}$$

According to Theorem 4, the Galois NFSR has 2^m cycles of length 2^{n-m}, which implies the order of the state transition matrix L is the least common multiple of 2^m repeated numbers of 2^{n-m}, namely, the order of L is 2^{n-m}. Therefore, for any positive integer l, the observability matrices $\mathcal{O}_{2^{n-m}+l}$ and $\mathcal{O}_{2^{n-m}}$ have the same number of different columns, denoted by **Fact 2**.

Since L is a circulant matrix, we can infer that for any positive integer $k \leq 2^{n-m} - 1$, at the k-th iteration the matrix HL^{k-1} multiplies the circulant matrix L, and the column vectors of HL^{k-1} circularly move to the left by 2^m, resulting the matrix HL^k. Note that H has totally 2^n columns. As $1 \leq m \leq n-1$, we have $n \geq 2$ and therefore, we can equally partition the 2^n columns into 2^{n-m} blocks, that is, we rewrite H as

$$H = [B_1 \ B_2 \ \ldots \ B_{2^{n-m}}]$$

with each $B_s \in \mathcal{L}_{2 \times 2^m}$ for each $s \in \{1, 2, \ldots, 2^{n-m}\}$. Taking into count Equation (24), we can easily observe the following facts.

1) If $n - j \geq m$, then each B_s has only one different column.

2) If $n - j < m$, then each B_s has two different columns; moreover,

$$B_1 = B_2 = \ldots = B_{2^{m-n}} = [\underbrace{A \ A \ \ldots \ A}_{2^{m-n+j-1}}].$$

Note that $HL^k = [B_{k+1}, B_{k+2}, \ldots, B_{2^{n-m}}, B_1, B_2, \ldots, B_k]$ for any positive integer $k \leq 2^{n-m} - 1$. Therefore, if $n - j \geq m$, then the observability matrix $\mathcal{O}_{2^{n-m}}$ has at most 2^{n-m} different columns; if $n - j < m$, then $\mathcal{O}_{2^{n-m}}$ has 2 different columns. Since $m \geq 1$ and $n \geq 2$, we have $2^{n-m} < 2^n$ and $2 < 2^n$. Together considering **Fact 2**, we can deduce that the number of difference columns of the observability matrix $\mathcal{O}_{2^n-1}$ is smaller than 2^n. According to Lemma 3, the Galois NFSR is unobservable. □

The following lemma can be directly obtained.

Lemma 7. *Denote the number of d-period binary sequences as $\widetilde{d}$. Then $\widetilde{d} = 2^d - \widetilde{d_1} - \widetilde{d_2} - \cdots - \widetilde{d_m}$, where $d_1, d_2, \cdots, d_m$ is the proper factor of d.*

Proposition 2. *For an n-stage Galois NFSR with state transition matrix L in (18), if*

$$2^{2^{n-m}} - 2^{2^{n-m-1}} \geq 2^n, \tag{25}$$

then there must exist an output function such that the NFSR is observable.

Proof. There are $\widetilde{2^{n-m}}$ binary sequences of period 2^{n-m} in total. According to the lemma 7,

$$\widetilde{2^{n-m}} = 2^{2^{n-m}} - \widetilde{2^{n-m-1}} - \widetilde{2^{n-m-2}} - \cdots - \widetilde{1}.$$

Since $\widetilde{2^{n-m-1}} = 2^{2^{n-m-1}} - \widetilde{2^{n-m-2}} - \widetilde{2^{n-m-3}} - \cdots - \widetilde{1}$, there is $N = \widetilde{2^{n-m}} = 2^{2^{n-m}} - 2^{2^{n-m-1}}$ different 2^{n-m}-period sequences. According to Equation (25), we have $N \geq 2^n$. Hence, there exists an output function h such that the Galois NFSR produces 2^n different output sequences that are from N sequences of period 2^{n-m}, which implies different initial states of the Galois NFSR produces different output sequences as according Theorem 4 and Lemma 5, the period of the Galois NFSR's output sequences is the devisor of 2^{n-m} . Therefore, the Galois is observable.

□

Consider an n-stage Galois NFSR with state transition matrix L in (18). For for any $q \in \{1, 2, \cdots, 2^m\}$, denote by C_q the cycle that is formed by the states $\delta_{2^n}^{q+k\cdot 2^m}$ for all $k = 0, 1, \cdots, 2^{n-m} - 1$. Since q is the remainder divided by 2^m, the corresponding n-dimensional vectors of the states contained in cycle C_q have the same last m bits, which implies that the corresponding n-dimensional vectors of the states on the C_q are of form

$$[X_1 \ X_2 \ \cdots \ X_{n-m} \ q_{n-m+1} \ q_{n-m+2} \ \cdots \ q_n]^T,$$

where

$$q = 2^m - (2^{m-1}q_{n-m+1} + 2^{m-2}q_{n-m+2} + \cdots + q_n). \tag{26}$$

Take cycle C_1 as an example. The corresponding n-dimensional vectors of the states on the C_1 are of form

$$[X_1 \ X_2 \ \cdots \ X_{n-m} \ \underbrace{1\,1 \ \cdots \ 1}_{m}]^T.$$

An n-variable Boolean function h can be expressed as

$$\begin{aligned}
& h(X_1, X_2, \ldots, X_n) \\
= & \sum_{(q_1, q_2, \ldots q_n) \in \mathbb{F}_2^n} h(q_1, q_2, \ldots q_n) X_1^{q_1} X_2^{q_2} \ldots X_n^{q_n} \\
= & \sum_{(q_{n-m+1}, q_{n-m+2}, \ldots q_n) \in \mathbb{F}_2^m} \left[\sum_{(q_1, q_2, \ldots q_{n-m}) \in \mathbb{F}_2^{n-m}} h(q_1, q_2, \ldots q_n) X_1^{q_1} X_2^{q_2} \ldots X_{n-m}^{q_{n-m}} \right] X_{n-m+1}^{q_{n-m+1}} X_{n-m+2}^{q_{n-m+2}} \ldots X_n^{q_n} \\
:= & \sum_{(q_{n-m+1}, q_{n-m+2}, \ldots q_n) \in \mathbb{F}_2^m} h_q X_{n-m+1}^{q_{n-m+1}} X_{n-m+2}^{q_{n-m+2}} \ldots X_n^{q_n},
\end{aligned}$$

where

$$h_q = \sum_{(q_1, q_2, \ldots q_{n-m}) \in \mathbb{F}_2^{n-m}} h(q_1, q_2, \ldots q_n) X_1^{q_1} X_2^{q_2} \ldots X_{n-m}^{q_{n-m}}, \ q = 1, 2, \ldots, 2^{n-m} \tag{27}$$

with q satisfying Equation (26). Clearly, each h_q is an $(n-m)$-variable Boolean function, and it is unique for a given Boolean function h. For the convenience, we rewrite the Boolean function h as

$$h = h_1 X_{n-m+1}^1 \cdots X_{n-1}^1 X_n^1 + h_2 X_{n-m+1}^1 \cdots X_{n-1}^1 X_n^0 + \cdots + h_q X_{n-m+1}^{q_{n-m+1}} \cdots X_{n-1}^{q_{n-1}} X_n^{q_n} + \cdots + h_{2^m} X_{n-m+1}^0 \cdots X_{n-1}^0 X_n^0. \quad (28)$$

Assume h in (28) is an output function of the Galois NFSR with transition matrix L in (18). Thus, if the output function h is limited to the states on the cycle C_q, then it becomes:

$$h(X_1, X_2, \cdots, X_n) = h_1 \cdot 0 + \cdots + h_{q-1} \cdot 0 + h_q(X_1, X_2, \cdots, X_{n-m}) \cdot 1 + h_{q+1} \cdot 0 + \cdots + h_{2^m} \cdot 0 = h_q(X_1, X_2, \cdots, X_{n-m}).$$

Proposition 3. *For an n-stage Galois NFSR with state transition matrix L in (*18*) and output function h in (28), each h_q in the function h is dependent on the variable X_1 for each $q \in \{1, 2, \cdots, 2^m\}$, if and only if any two distinct states on each cycle are distinguishable.*

Proof. Sufficiency: If the any two distinct states on each cycle are distinguishable, there must exist a state $X(t) \in \mathbb{F}_2^n$ at time t on each cycle whose output is different from that of the state $X(t + 2^{n-m-1})$ at time $t + 2^{n-m-1}$, namely, $h_q(X(t)) \neq h(X(t + 2^{n-m-1})$. Otherwise, the output sequence of a cycle C_{q_0} is a divisor of 2^{n-m}. Then, there are two distinct initial states from the cycle C_{q_0} resulting the same output sequence. Thus, the two states on the cycle C_{q_0} are indistinguishable, which is contrary.

According to a state sequence in (19) of the Galois NFSR, the initial state $x(t) = \delta_{2^n}^q \in \Delta_{2^n}$ at time t is updated to $x(t + 2^{n-m-1}) = \delta_{2^n}^{q+2^{n-m-1}\times 2^m} = \delta_{2^n}^{q+2^{n-1}}$ at time $t + 2^{n-m-1}$. Their corresponding n-dimensional vectors $X(t)$ and $X(t + 2^{n-m-1})$ have the same other bits except the first bit. Hence, h_q is dependent on the variable X_1 for any $q \in \{1, 2, \cdots, 2^m\}$; Otherwise, $h_q(X(t)) = h(X(t + 2^{n-m-1})$, a contradiction.

Necessity: If the output function h is limited to the states on the cycle C_q, then h becomes

$$h(X_1, X_2, \cdots, X_n) = h_q(X_1, X_2, \cdots, X_{n-m}) = h_{q_1}(X_2, \cdots, X_{n-m})X_1 + h_{q_2}(X_2, \cdots, X_{n-m}).$$

As h_q is dependent on the variable X_1, we can deduce that $h_{q_1} \not\equiv 0$.

Since the first $n-m$ variables of states on cycle C_q go through all states in $\mathbb{F}_2^{n-m}$, there must exist state $X_0 \in F_2^{n-m-1}$ such $h_{q_1}(X_0) = 1$. Then there exists initial state $X(t) = [1 \ X_0 \ q_{n-m+1} \ q_{n-m+2} \ \cdots \ q_n]^T$ at time t whose output is different from that of the state $X(t + 2^{n-m-1}) = [0 \ X_0 \ q_{n-m+1} \ q_{n-m+2} \ \cdots \ q_n]^T$ at time $t + 2^{n-m-1}$. Therefore, the states in each cycle are distinguishable separately. □

For the statement ease, we introduce some notations, which will be used in the sequence. It is helpful to keep them in mind.

First, we define two sets:

$$A_{\mathbf{q}_{n-m}} = \{\mathbf{q}_{n-m} = [q_1 \ q_2 \ \ldots \ q_{n-m}]^T | \mathbf{q} = [q_1 \ q_2 \ \ldots \ q_{n-m} \ q_{n-m+1} \ \ldots \ q_n]^T \text{ on the cycle } C_q \text{ and } h(\mathbf{q}) = 1\}, \quad (29)$$

and

$$\hat{A}_{\mathbf{q_{n-m}}} = \{\hat{q} | \hat{q} = 2^{n-m} - 1 - (2^{n-m-1}q_1 + 2^{n-m-2}q_2 + \cdots + q_{n-m}), \ [q_1 \ q_2 \ \ldots \ q_{n-m}]^T = \mathbf{q}_{n-m} \in A_{\mathbf{q}_{n-m}}\}. \quad (30)$$

Next, we define a vector

$$\hat{\mathbf{q}} = (\hat{q}_1, \hat{q}_2, \ldots, \hat{q}_N), \quad (31)$$

where $\hat{q}_1, \hat{q}_2, \ldots, \hat{q}_N \in \hat{A}_{\mathbf{q_{n-m}}}$ satisfy $\hat{q}_1 < \hat{q}_2 < \ldots < \hat{q}_N$, and N is the cardinality of the set $\hat{A}_{\mathbf{q_{n-m}}}$.

Finally, we define the *distance tuple* of $\hat{\mathbf{q}}$ as

$$\text{dist}(\hat{\mathbf{q}}) = ((\hat{q}_1 - \hat{q}_N) \bmod 2^{n-m}, \hat{q}_2 - \hat{q}_1, \hat{q}_3 - \hat{q}_2, \cdots, \hat{q}_N - \hat{q}_{N-1}). \quad (32)$$

Similarly, we can define $\text{dist}(\hat{\mathbf{p}})$ for the cycle C_p.

Lemma 8. *Each component of* $\text{dist}(\hat{\mathbf{q}})$ *is equal to the path length of two states from two neighboring components of the vector* $\hat{\mathbf{q}}$.

Proof. The states of the cycle C_q are of form $\delta_{2^n}^{2^m k+q}$ in Δ_{2^n}, where $k \in \{0, 1, \cdots, 2^{n-m}-1\}$. Their corresponding n-dimensional vector is $(X_1, X_2, \cdots, X_{n-m}, q_{n-m+1}, \cdots, q_n)$, where $q = 2^m - (2^{m-1}a_{n-m+1} + 2^{m-2}a_{n-m+2} + \cdots + a_n)$. According to Lemma 1 and Equation (30) , we have

$$2^m k + q = 2^n - (2^{n-1}X_1 + 2^{n-2}X_2 + \cdots + 2^m X_{n-m} + 2^{m-1}q_{n-m+1} + 2^{m-2}q_{n-m+2} + \cdots + q_n),$$

yielding

$$k = 2^{n-m} - 1 - (2^{n-m-1}X_1 - 2^{n-m-2}X_2 + \cdots + X_{n-m}) \in \hat{A}_{\mathbf{q}_{n-m}}.$$

The cycle C_q has a 2^{n-m}-period state sequence:

$$\delta_{2^n}^{q}, \delta_{2^n}^{2^m+q}, \delta_{2^n}^{2\cdot 2^m+q}, \cdots, \delta_{2^n}^{k\cdot 2^m+q}, \cdots, \delta_{2^n}^{(2^{n-m}-1)\cdot 2^m+q}.$$

Clearly, the path length of any two states $\delta_{2^n}^{2^m k+q}$ and $\delta_{2^n}^{2^m l+q}$ with positive integers k, l satisfying $k < l$, is $l - k$. Then the result follows from the definition of $\mathrm{dist}(\hat{\mathbf{q}})$ in (32). □

Proposition 4. *For an n-stage Galois NFSR with state transition matrix L in (18), there exist indistinguishable states on different cycles C_p and C_q, if and only if* $\mathrm{dist}(\hat{\mathbf{p}})$ *is shift equivalent to* $\mathrm{dist}(\hat{\mathbf{q}})$.

Proof. Let $\mathrm{dist}(\nu) = (d_1^\nu, d_2^\nu, \ldots, d_N^\nu)$ with $\nu = \hat{\mathbf{p}}, \hat{\mathbf{q}}$. Then, from the proof of Lemma 8, we know that for each $k \in \{1, 2, \ldots, N\}$, each d_k^ν uniquely corresponds to an output sequences $1\ \underbrace{00\ldots0}_{d_k^\nu - 1}\ 1$ of length d_k^ν. Thus, $\mathrm{dist}(\nu)$ uniquely corresponds to an output sequence S^ν of length $d^\nu = d_1^\nu + d_2^\nu + \ldots + d_N^\nu$. Hence, $\mathrm{dist}(\hat{\mathbf{p}})$ is shift equivalent to $\mathrm{dist}(\hat{\mathbf{q}})$ if and only if the output sequence $S^{\hat{\mathbf{q}}}$ uniquely corresponds to $\mathrm{dist}(\hat{\mathbf{q}})$ is shift equivalent to the output sequence $S^{\hat{\mathbf{p}}}$ uniquely corresponds to $\mathrm{dist}(\hat{\mathbf{p}})$, which is equivalent to saying that there exist two indistinguishable states on different cycles C_p and C_q as both cycles has the same length. □

Corollary 2. *For an n-stage Galois NFSR with state transition matrix L in (18), if it is observable, then its output function h is dependent on the variables X_k for any $k \in \{n-m+1, n-m+2, \cdots, n\}$.*

Proof. If the output function h is not dependent on some variable X_k with some $k \in \{n-m+1, n-m+2, \cdots, n\}$, then there exists $h_q = h_{q+2^{n-k}}$ for $q = 1$. According to Equations (27) and (29)-(32), we can deduce $\mathrm{dist}(\hat{\mathbf{q}}) = \mathrm{dist}(\widehat{\mathbf{q} + 2^{n-k}})$ for $q = 1$. From Proposition 4, there exist two indistinguishable states on different cycles C_q and $C_{q+2^{n-k}}$ for $q = 1$, which is contrary. Hence, the result holds. □

Theorem 6. *For an n-stage Galois NFSR with state transition matrix L in (18) satisfying the equation(25), it is observable if and only if:*

1) The h_q contains the variable X_1 for any $q \in \{1, 2, \cdots, 2^m\}$;

2) $\mathrm{dist}(\hat{\mathbf{p}})$ *is not shift equivalent to* $\mathrm{dist}(\hat{\mathbf{q}})$ *for any $p, q \in \{1, 2, \cdots, 2^m\}$, where $p \neq q$.*

Proof. According to Proposition 3, Condition 1) holds if and only if any two distinct states in each cycle are distinguishable. From Proposition 4, Condition 2) holds if and only if any two distinct states on different cycles are distinguishable. □

Corollary 3. *For an n-stage Galois NFSR with feedback function satisfying Equation (23), if its output function is*

$$h(X_1, X_2, \cdots, X_n) = X_1^{b_0} g_1(X_2, \cdots, X_{n-1}) \oplus g_2(X_2, \cdots, X_{n-1}) \oplus X_1^{b_1} X_2^{b_2} \cdots X_n^{b_n},$$

where each $b_i \in \mathbb{F}_2$ for each $i \in \{0, 1, 2, \cdots, n\}$, $g_1 \not\equiv 0$ and $g_1 \neq X_2^{b_2} \cdots X_{n-1}^{b_{n-1}}$, then the Galois NFSR is observable.

Proof. The state diagram of the Galois consists of two cycles of length 2^{n-1}:

$$\begin{aligned}
&\text{Cycle } C_1 : \delta_{2^n}^1 \to \delta_{2^n}^3 \to \delta_{2^n}^5 \to \cdots \to \delta_{2^n}^{2k-1} \to \cdots \to \delta_{2^n}^{2^n-1} \to \delta_{2^n}^1;\\
&\text{Cycle } C_2 : \delta_{2^n}^2 \to \delta_{2^n}^4 \to \delta_{2^n}^6 \to \cdots \to \delta_{2^n}^{2k} \to \cdots \to \delta_{2^n}^{2^n} \to \delta_{2^n}^2.
\end{aligned}$$

Rewrite the output function h as:

$$\begin{aligned}
h(X_1, X_2, \cdots, X_n) &= X_1^{b_0} g_1(X_2, \cdots, X_{n-1})(X_n^{b_n} \oplus X_n^{b_n^0}) \oplus g_2(X_2, \cdots, X_{n-1})(X_n^{b_n} \oplus X_n^{b_n^0}) \oplus X_1^{b_1} X_2^{b_2} \cdots X_n^{b_n}\\
&= (X_1^{b_0} g_1 \oplus g_2 \oplus X_1^{b_1} X_2^{b_2} \cdots X_{n-1}^{b_{n-1}}) X_n^{b_n} \oplus (X_1^{b_0} g_1 \oplus g_2) X_n^{b_n^0}.
\end{aligned} \tag{33}$$

Let $h_p(X_1, X_2, \cdots, X_{n-1}) = X_1^{b_0} g_1 \oplus g_2 \oplus X_1^{b_1} X_2^{b_2} \cdots X_{n-1}^{b_{n-1}}$ and $h_q(X_1, X_2, \cdots, X_{n-1}) = X_1^{b_0} g_1 \oplus g_2$. As $g_1 \not\equiv 0$ and $g_1 \neq X_2^{b_2} \cdots X_{n-1}^{b_{n-1}}$, we easily observe that h_p is dependent on the variable X_1. Clearly, h_q is also dependent on the variable X_1. So, h_p and h_q satisfy Condition 1) in Theorem 6. Clearly, $h_p \oplus h_q = X_1^{b_1} X_2^{b_2} \cdots X_{n-1}^{b_{n-1}}$, which indicates $|A_{\mathbf{p}_{n-1}}| - |A_{\mathbf{q}_{n-1}}| = 1$ or -1, where $|A_{\mathbf{p}_{n-1}}|$ and $|A_{\mathbf{q}_{n-1}}|$ are the cardinality of $A_{\mathbf{p}_{n-1}}$ and $A_{\mathbf{q}_{n-1}}$. Hence, dist($\hat{\mathbf{p}}$) is not shift equivalent to dist($\hat{\mathbf{q}}$), which satisfies Condition 2) in Theorem 6. Therefore, according to Theorem 6, the Galois NFSR is observable. □

5 Conclusion

The paper considered two classes of Galois NFSRs. Their cycle structure and observability were disclosed using the semi-tensor product based Boolean network approach. Each Galois NFSRs in the first classes has the maximum state cycle with an arbitrary stage number and explicit feedback functions, which breaks the longstanding dilemma that it is quite difficult to construct a maximum cycle NFSR (even if a maximum cycle Fibonacci NFSR) with an arbitrary state number and explicit feedback functions; moreover, an easily verifiable necessary and sufficient condition was given to determine whether a Galois NFSR in the first class with an output function is observable, which guarantees the period of output sequences is maximum as well, namely, is equal to the length of the maximum state cycle. Each Galois NFSR in the second class has equi-length state cycles with an arbitrary stage number and explicit feedback functions as well. Some (easily verifiable) necessary and sufficient conditions were given to determine whether a Galois NFSR in the second class with an output function is observable. In the future work, it is interesting to use those Galois NFSRs in both classes or their isomorphic Galois NFSRs or their variant Galois NFSRs with output functions to design new stream ciphers by taking into account their security and implementation efficiency.

References

[1] M. Hell, T. Johansson and W. Meier, "Grain-a stream cipher for constrained environments," *M. Robshaw and O. Billet (eds) Lecture Notes in Computer Science (LCNS)*, 2008, 4986: 179-190.

[2] C. Canniere De and B. Preneel, "Trivium specifications," *M. Robshaw and O. Billet (eds) Lecture Notes in Computer Science (LCNS)*, 2008, 4986: 244-266.

[3] S. Babbage and M. Dodd,"The stream cipher MICKEY (version 1)," *M. Robshaw and O. Billet (eds) Lecture Notes in Computer Science (LCNS)*, 2008, 4986: 191-209.

[4] Kauffman, S.A,"Metabolic stability and epigenesis in randomly constructed genetic nets," *J. Theor. Biol.*, vol. 22, no. 3, pp. 437-467, 1969.

[5] D. Cheng, H. Qi and Y Zhao,"An introduction to semi-tensor product of matrices and its applications," *World Scientific*, vol.8, pp. 610-612, 2012.

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

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

[8] D. Laschov, M. Margaliot and G. Even, "Observability of Boolean networks: a graph-theoretic approach," *Automatica*, vol. 49, no. 8, pp. 2351–2362, 2013.

[9] Y. Guo, W. Gui and C. Yang, "Redefined observability matrix for Boolean networks and distinguishable partitions of state space," *Automatica*, vol. 91, no. 5, pp. 316-319, 2018.

[10] Y. Yu, M. Meng, J. Feng and G. Chen, "Observability criteria for Boolean networks," *IEEE Trans. Autom. Control*, vol. 67, no. 11, 6248-6254, 2022.

[11] A. Biryukov, "Weak keys," In: H.C.A. van Tilborg, S. Jajodia (eds), *Encyclopedia of Cryptography and Security*, Springer, Boston, MA., pp. 1366–1367, 2011.

[12] N. Kalouptsidis and K. Limniotis, "Nonlinear span, minimal realizations of sequences over finite fields and De Brujin generators," in *International Symposium on Information Theory and its Applications (ISITA 2004)*, Parma, Italy, Oct. 2004, pp. 794-799.

[13] W. Kong, J. Zhong and D. Lin, "Observability of Galois nonlinear feedback shift registers," *Science China Information Sciences*, vol. 65, no. 9, pp. 192206: 1–192206:16, 2022.

[14] Z. Gao, J. Feng, Y. Yu and Y. Cui, "On observability of Galois nonlinear feedback shift registers over finite fields," *Frontiers Inf. Technol. Electon. Eng.*, vol. 23, no. 10, pp. 1533-1545, 2022.

[15] Z. Chang, M. F. Ezerman, S. Ling, and H. Wang, "The cycle structure of LFSR with arbitrary characteristic polynomial over finite fields," *Cryptogr. Commun.*, vol. 10, no. 6, pp. 1183-1202, 2018.

[16] H. Hu and G. Guang, "Periods on two kinds of nonlinear feedback shift registers with time varying feedback functions," *Int. J. Found. Comput. Sci.*, vol. 22, no. 6, pp. 1317-1329, 2011.

[17] S. Zhang and G. Chen, "New results on the state cycles of Trivium," *Design Code Cryptogr.*, vol. 87, no. 5, pp. 149-162, 2019.

[18] Z. Chang, G. Gong and Q. Wang, "Cycle structures of a class of cascaded FSRs," *IEEE Trans. Inf. Theory*, vol. 66, no. 6, pp. 3766 –3774, 2019.

[19] J. Dong and D. Pei, "Construction for De Bruijn sequences with large stage," *Des. Code Cryptogr.*, vol. 85, no. 2, pp. 343-358, 2017.

[20] M. Li and D. Lin, "De Bruijn sequences, adjacency graphs, and cyclotomy," *IEEE Trans. Inf. Theory*, vol. 64, no. 4, pp. 2941-2952, 2018.

[21] K. Mandal, B. Yang, G. Gong, and M. Aagaard, "Analysis and efficient implementations of a class of composited de Bruijn sequences", *IEEE Trans. Comput.*, vol. 69, no. 12, pp. 1835-1848, 2020.

[22] K. Mandal, B. Yang, G. Gong, and M. Aagaard, "Analysis and efficient implementations of a class of composited de Bruijn sequences", *IEEE Trans. Comput.*, vol. 69, no. 12, pp. 1835-1848, 2020.

[23] M. Li, D. Lin, "Partial cycle structure of FSRs and its applications in searching de Bruijn sequences," *IEEE Trans. Inf. Theory*, vol. 69, no. 1, pp. 598-609, 2023.

[24] E. Dubrova, "A list of maximum-period NFSRs," *Cyptology ePrint Archive*, Report 2012/166, 2012. http://eprint.iacr.org/2012/166

[25] B. M. Gammel, R. Göttfert, and O. Kniffer, "Achterbahn-128/80," eSTREAM: the ECRYPT Stream Cipher Project, 2006. http://www.ecrypt.eu.org/stream/p2ciphers/achterbahn/achterbahn_p2.pdf.

[26] Y. Yang, X. Zeng and Y. Xu, "Periods on the cascade connection of an LFSR and an NFSR," *Chinese J. Electronics*, vol. 28, no. 2, pp. 301-308, 2019.

[27] Z. Wang, Q. Zheng, X. Zhao and X. Feng, "Grain-like structures with minimal and maximal period sequences," *Des. Codes Crpt.*, vol. 89, no. 1, pp. 679-693, 2021.

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

[29] C.-K. Wu and D. Feng, *Boolean Functions and Their Applications in Cryptography*, Springer Berlin, Heidelberg, 2016.

[30] D. Cheng, H. Qi and Z. Li, *Analysis and Control of Boolean Networks*, Springer-Verlag, 2011.

[31] D. Cheng, H. Qi and Z. Li, "Model contruction of Boolean network via observed data," *IEEE Trans. Neural Network*, vol. 22, no. 4, pp. 525-536, 2011.

[32] H. Qi and D. Cheng,"Logic and logic-based control," *J. Contr. Theory*, vol.6, no.1, pp. 123-133, 2008.

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

[34] W. Kong, J. Zhong and D. Lin, "Isomorphism and equivalence of Galois nonlinear feedback shift registers," *Inscrypt 2021, Lecture Notes in Computer Science, LNCS* 13007, pp. 301–315, 2021.

Appendix

Table 2: The feedback functions.

i	feedback	explicit expression of feedback function
2	F	$\begin{cases} f_n = X_n^0, \\ f_{n-1} = X_{n-1} \oplus X_n^0, \\ f_{n-2} = X_{n-2} \oplus X_{n-1}^0 X_n^0, \\ \quad \vdots \\ f_1 = X_1 \oplus X_2^0 X_3^0 \cdots X_n^0. \end{cases}$
	DF	$\begin{cases} f_n = X_n^0, \\ f_{n-1} = X_{n-1} \oplus X_n, \\ f_{n-2} = X_{n-2} \oplus X_{n-1} X_n, \\ \quad \vdots \\ f_1 = X_1 \oplus X_2 X_3 \cdots X_n. \end{cases}$
	RF	$\begin{cases} f_1 = X_1^0, \\ f_2 = X_2 \oplus X_1^0, \\ f_3 = X_3 \oplus X_2^0 X_1^0, \\ \quad \vdots \\ f_n = X_n \oplus X_{n-1}^0 X_{n-2}^0 \cdots X_1^0. \end{cases}$
	RDF	$\begin{cases} f_1 = X_1^0, \\ f_2 = X_2 \oplus X_1, \\ f_3 = X_3 \oplus X_2 X_1, \\ \quad \vdots \\ f_n = X_n \oplus X_{n-1} X_{n-2} \cdots X_1. \end{cases}$
4	F	$\begin{cases} f_n = X_n^0, \\ f_{n-1} = X_{n-1} \oplus X_n, \\ f_{n-2} = X_{n-2}^0 \oplus X_{n-1} X_n, \\ f_{n-3} = X_{n-3} \oplus X_{n-2}^0 \oplus X_{n-2}^0 X_{n-1} X_n, \\ f_{n-4} = X_{n-4} \oplus X_{n-3}^0 X_{n-2}^0 \oplus X_{n-3}^0 X_{n-2}^0 X_{n-1} X_n, \\ \quad \vdots \\ f_1 = X_1 \oplus X_2^0 X_3^0 \cdots X_{n-2}^0 \oplus X_2^0 X_3^0 \cdots X_{n-2}^0 X_{n-1} X_n. \end{cases}$
	DF	$\begin{cases} f_n = X_n^0, \\ f_{n-1} = X_{n-1} \oplus X_n^0, \\ f_{n-2} = X_{n-2}^0 \oplus X_{n-1}^0 X_n^0, \\ f_{n-3} = X_{n-3} \oplus X_{n-2} \oplus X_{n-2} X_{n-1}^0 X_n^0, \\ f_{n-4} = X_{n-4} \oplus X_{n-3} X_{n-2} \oplus X_{n-3} X_{n-2} X_{n-1}^0 X_n^0, \\ \quad \vdots \\ f_1 = X_1 \oplus X_2 X_3 \cdots X_{n-2} \oplus X_2 X_3 \cdots X_{n-2} X_{n-1}^0 X_n^0. \end{cases}$

i	feedback	explicit expression of feedback function
6	RF	$f_1 = X_1^0,$ $f_2 = X_2 \oplus X_1,$ $f_3 = X_3^0 \oplus X_2X_1,$ $f_4 = X_4 \oplus X_3^0 \oplus X_3^0X_2X_1,$ $f_5 = X_5 \oplus X_4^0X_3^0 \oplus X_4^0X_3^0X_2X_1,$ $\vdots$ $f_n = X_n \oplus X_{n-1}^0X_{n-2}^0 \cdots X_3^0 \oplus X_{n-1}^0X_{n-2}^0 \cdots X_3^0X_2X_1.$
	RDF	$f_1 = X_1^0,$ $f_2 = X_2 \oplus X_1^0,$ $f_3 = X_3^0 \oplus X_2^0X_1^0,$ $f_4 = X_4 \oplus X_3 \oplus X_3X_2^0X_1^0,$ $f_4 = X_5 \oplus X_4X_3 \oplus X_4X_3X_2^0X_1^0,$ $\vdots$ $f_n = X_n \oplus X_{n-1}X_{n-2} \cdots X_3 \oplus X_{n-1}X_{n-2} \cdots X_3X_2^0X_1^0.$
	F	$f_n = X_n^0,$ $f_{n-1} = X_{n-1} \oplus X_n^0,$ $f_{n-2} = X_{n-2}^0 \oplus X_{n-1}^0X_n^0,$ $f_{n-3} = X_{n-3}^0 \oplus X_{n-2} \oplus X_{n-2}X_{n-1}^0X_n^0,$ $f_{n-4} = X_{n-4} \oplus X_{n-3}^0X_{n-2}^0 \oplus X_{n-3}^0X_{n-2}X_{n-1}^0X_n^0,$ $\vdots$ $f_1 = X_1 \oplus X_2^0X_3^0 \cdots X_{n-2}^0 \oplus X_2^0 \cdots X_{n-3}^0X_{n-2}X_{n-1}^0X_n^0.$
	DF	$f_n = X_n^0,$ $f_{n-1} = X_{n-1} \oplus X_n,$ $f_{n-2} = X_{n-2}^0 \oplus X_{n-1}X_n,$ $f_{n-3} = X_{n-3}^0 \oplus X_{n-2}^0 \oplus X_{n-2}^0X_{n-1}X_n,$ $f_{n-4} = X_{n-4} \oplus X_{n-3}X_{n-2} \oplus X_{n-3}X_{n-2}^0X_{n-1}X_n,$ $\vdots$ $f_1 = X_1 \oplus X_2X_3 \cdots X_{n-2} \oplus X_2 \cdots X_{n-3}X_{n-2}^0X_{n-1}X_n.$
	RF	$f_1 = X_1^0,$ $f_2 = X_2 \oplus X_1^0,$ $f_3 = X_3^0 \oplus X_2^0X_1^0,$ $f_4 = X_4^0 \oplus X_3 \oplus X_3X_2^0X_1^0,$ $f_5 = X_5 \oplus X_4^0X_3^0 \oplus X_4^0X_3X_2^0X_1^0,$ $\vdots$ $f_n = X_n \oplus X_{n-1}^0X_{n-2}^0 \cdots X_3^0 \oplus X_{n-1}^0 \cdots X_4^0X_3X_2^0X_1^0.$
	RDF	$f_1 = X_1^0,$ $f_2 = X_2 \oplus X_1,$ $f_3 = X_3^0 \oplus X_2X_1,$ $f_4 = X_4^0 \oplus X_3^0 \oplus X_3^0X_2X_1,$ $f_5 = X_5 \oplus X_4X_3 \oplus X_4X_3^0X_2X_1,$ $\vdots$ $f_n = X_n \oplus X_{n-1}X_{n-2} \cdots X_3 \oplus X_{n-1} \cdots X_4X_3^0X_2X_1.$

i	feedback	explicit expression of feedback function
8	F	$f_n = X_n^0,$ $f_{n-1} = X_{n-1} \oplus X_n,$ $f_{n-2} = X_{n-2} \oplus X_{n-1}X_n,$ $f_{n-3} = X_{n-3}^0 \oplus X_{n-2}X_{n-1}X_n,$ $f_{n-4} = X_{n-4} \oplus X_{n-3}^0 \oplus X_{n-3}^0X_{n-2}X_{n-1}X_n,$ $\vdots$ $f_1 = X_1 \oplus X_2^0X_3^0 \cdots X_{n-3}^0 \oplus X_2^0 \cdots X_{n-3}^0X_{n-2}X_{n-1}X_n.$
	DF	$f_n = X_n^0,$ $f_{n-1} = X_{n-1} \oplus X_n^0,$ $f_{n-2} = X_{n-2} \oplus X_{n-1}^0X_n^0,$ $f_{n-3} = X_{n-3}^0 \oplus X_{n-2}^0X_{n-1}^0X_n^0,$ $f_{n-4} = X_{n-4} \oplus X_{n-3} \oplus X_{n-3}X_{n-2}^0X_{n-1}^0X_n^0,$ $\vdots$ $f_1 = X_1 \oplus X_2X_3 \cdots X_{n-3} \oplus X_2 \cdots X_{n-3}X_{n-2}^0X_{n-1}^0X_n^0.$
	RF	$f_1 = X_1^0,$ $f_2 = X_2 \oplus X_1,$ $f_3 = X_3 \oplus X_2X_1,$ $f_4 = X_4^0 \oplus X_3X_2X_1,$ $f_5 = X_5 \oplus X_4^0 \oplus X_4^0X_3X_2X_1,$ $\vdots$ $f_n = X_n \oplus X_{n-1}^0X_{n-2}^0 \cdots X_4^0 \oplus X_{n-1}^0 \cdots X_4^0X_3X_2X_1.$
	RDF	$f_1 = X_1^0,$ $f_2 = X_2 \oplus X_1^0,$ $f_3 = X_3 \oplus X_2^0X_1^0,$ $f_4 = X_4^0 \oplus X_3^0X_2^0X_1^0,$ $f_5 = X_5 \oplus X_4 \oplus X_4X_3^0X_2^0X_1^0,$ $\vdots$ $f_n = X_n \oplus X_{n-1}X_{n-2} \cdots X_4 \oplus X_{n-1} \cdots X_4X_3^0X_2^0X_1^0.$
$\vdots$		
2^{n-1}	F	$f_n = X_n^0,$ $f_{n-1} = X_{n-1} \oplus X_n,$ $f_{n-2} = X_{n-2} \oplus X_{n-1}X_n,$ $f_{n-3} = X_{n-3} \oplus X_{n-2}X_{n-1}X_n,$ $\vdots$ $f_2 = X_2 \oplus X_3X_4 \cdots X_n,$ $f_1 = X_1^0 \oplus X_2X_3 \cdots X_n.$
	DF	$f_n = X_n^0,$ $f_{n-1} = X_{n-1} \oplus X_n^0,$ $f_{n-2} = X_{n-2} \oplus X_{n-1}^0X_n^0,$ $f_{n-3} = X_{n-3} \oplus X_{n-2}^0X_{n-1}^0X_n^0,$ $\vdots$ $f_2 = X_2 \oplus X_{n-3}^0X_{n-2}^0X_{n-1}^0X_n^0,$ $f_1 = X_1^0 \oplus X_2^0X_3^0 \cdots X_n^0.$

i	feedback	explicit expression of feedback function
	RF	$\begin{cases} f_1 = X_1^0, \\ f_2 = X_2 \oplus X_1, \\ f_3 = X_3 \oplus X_2X_1, \\ f_4 = X_4 \oplus X_3X_2X_1, \\ \quad \vdots \\ f_{n-1} = X_{n-1} \oplus X_{n-2}X_{n-3} \cdots X_1, \\ f_n = X_n^0 \oplus X_{n-1}X_{n-2} \cdots X_1. \end{cases}$
	RDF	$\begin{cases} f_1 = X_1^0, \\ f_2 = X_2 \oplus X_1^0, \\ f_3 = X_3 \oplus X_2^0X_1^0, \\ f_4 = X_4 \oplus X_3^0X_2^0X_1^0, \\ \quad \vdots \\ f_{n-1} = X_{n-1} \oplus X_{n-2}^0X_{n-3}^0 \cdots X_1^0, \\ f_n = X_n^0 \oplus X_{n-1}^0X_{n-2}^0 \cdots X_1^0. \end{cases}$
End of Table		