SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

November 2025, Vol. 68, Iss. 11, 212203:1–212203:15
https://doi.org/10.1007/s11432-024-4364-4

Cycle structure and observability of two types of Galois NFSRs

Xianghan WANG[1,2], Jianghua ZHONG[1*] & Dongdai LIN[1,2]

[1] *State Key Laboratory of Cyberspace Security Defense, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100085, China*
[2] *School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China*

Received 13 June 2024/Revised 9 December 2024/Accepted 25 March 2025/Published online 20 June 2025

Abstract Galois nonlinear feedback shift registers (NFSRs) are used in many recent stream ciphers. One security criterion for the design of a stream cipher is to ensure that its keystream has a long period, which requires the used NFSR to have a long state cycle. Meanwhile, to avoid equivalent keys, the keystream's period must not be compressed compared with the NFSR's state cycle length, which can be guaranteed if the NFSR is observable. The cycle structure of a general Galois NFSR is an open hard problem, and the observability of Galois NFSRs is less studied because of the lack of efficient tools. This paper considers the cycle structure and observability of two types of Galois NFSRs, using the semi-tensor product-based Boolean network approach. It discloses that each Galois NFSR has the maximum state cycle for the first type, but has equal-length state cycles for the second. Some easily verifiable necessary and/or sufficient conditions are given for the observability of each Galois NFSR for both types, generalizing the corresponding previous results on single-cycle triangular functions. Each Galois NFSR in both types has simple feedback functions and has extensive selections for its output function to assure it to be observable, helpful for the design of stream ciphers.

Keywords shift register, state cycle, Boolean network, semi-tensor product, observability

Citation Wang X H, Zhong J H, Lin D D, et al. Cycle structure and observability of two types of Galois NFSRs. Sci China Inf Sci, 2025, 68(11): 212203, https://doi.org/10.1007/s11432-024-4364-4

1 Introduction

With the development of the Internet, big data, and artificial intelligence, there is a growing demand for higher security and efficiency in information processing. To guarantee information security, cryptographic primitives are usually used. Among these, stream ciphers have efficient advantages over other techniques. They commonly use shift registers as their main building blocks. On the basis of whether feedback functions are linear or not, shift registers are divided into linear feedback shift registers (LFSRs) and nonlinear feedback shift registers (NFSRs). Over time, the latter have replaced the former and have been used as the main building blocks in many stream ciphers, such as the two hardware-oriented finalists Grain [1] and Trivium [2] in the eSTREAM project and the finalist Acorn [3] in the CAESAR competition.

NFSRs are generally classified into Fibonacci NFSRs and Galois NFSRs, in terms of their implementation structure. A Fibonacci NFSR has feedback applied only to the last bit, and its other bits involve only shifts. However, a Galois NFSR has feedback availably applied to every bit. Clearly, a Fibonacci NFSR is a particular Galois NFSR. Moreover, all foregoing stream ciphers use Galois NFSRs as their main building blocks, and the output functions of these Galois NFSRs are Boolean functions.

An NFSR has the same mathematical model as a Boolean network, which can be described by a set of difference equations via Boolean functions. The Boolean network was first introduced by Kauffman [4] in 1969 to model a genetic network. In the control theory community, Cheng et al. [5] developed an algebraic framework for Boolean networks, using a powerful mathematical tool named semi-tensor product of matrices. Under this algebraic framework, a Boolean network is characterized by a state transition matrix, facilitating solving fundamental problems in control theory, such as the observability problem. So far, many studies have been done on the observability of Boolean networks [6–10]. By viewing NFSRs as Boolean networks, some studies have also studied NFSRs [11–14].

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

From a security perspective, NFSR-based stream ciphers should select observable NFSRs in the sense that any two distinct initial states are distinguishable from their resulting output sequences; otherwise, they may have equivalent keys, subject to weak key attacks [15]. Moreover, an observable NFSR can guarantee that the period of its output sequences is not compressed compared with its corresponding state cycle length (or equivalently, the period of its corresponding state sequence). In the cryptography community, Kalouptsidis and Limniotis [16] first introduced the observability of sequence generators from the perspective of systems theory and applied it to the generators of de Bruijn sequences. Since then, only one work addressed the observability of NFSRs (over the binary field) [17], which was soon generalized to finite fields [18], to the authors' best knowledge.

One security criterion for the design of a stream cipher is to ensure a keystream with a long period. To meet this criterion, the NFSR used in a stream cipher must have a long state cycle. However, figuring out the cycle structure of a general Galois NFSR (i.e., the pre-periods and periods of its state sequences) remains an open problem. So far, only particular Galois NFSRs have been investigated. Short state cycles were disclosed for the Galois NFSR used in the stream cipher Trivium [19]. If a Fibonacci NFSR only outputs its first state bit, then each output sequence and its corresponding state sequence have the same preperiod and period. In the existing literature, if there is no special clarification, an NFSR is always assumed to output its first state bit. Under this assumption, the period of an NFSR in a Grain-like structure was found to be a multiple of its LFSR's period if the LFSR is set to a nonzero initial state [20], and the cycle structure of a cascade connection of a maximum-period Fibonacci LFSR into a maximum-period Fibonacci NFSR was revealed [21]. Here, the period of an NFSR means the length of the longest cyclic output sequence the NFSR generates [22], whereas a maximum-period NFSR means an NFSR achieving the maximum period.

An NFSR is said to be a maximum-cycle NFSR if it has the maximum state cycle, that is, has the maximum cycle in its state diagram. Much attention has been paid to constructing maximum-cycle Fibonacci NFSRs (or equivalently, constructing maximum-period Fibonacci NFSRs or constructing de Bruijn sequences, with the condition that they output their first state bits) using the cycle joining method [23–25]. However, in practice the feedback functions of such Fibonacci NFSRs are generally hard to get. So far, only the maximum-cycle Fibonacci NFSRs with stage numbers no greater than 33 have been found [26, 27]. In contrast, much less attention has been paid to maximum-cycle Galois NFSRs, let alone maximum-period Galois NFSRs [28], although Galois NFSRs may decrease the area and increase the throughput compared with Fibonacci NFSRs [29].

A triangular function with maximum state cycle, called a single-cycle T-function for short, has been studied in [30–32]. The T-function was introduced by Klimov and Shamir in 2002 [33]. It includes arithmetic operations (negation, addition, subtraction, and multiplication) and Boolean operations (AND, OR, NOT, and XOR). A candidate of the eSTREAM project, stream cipher ABC [34], used such a single-cycle T-function. If a T-function only includes the Boolean operations AND and XOR, the algebraic normal form of a single-cycle T-function was given in [35].

For a single-cycle T-function, the periods of the sequences generated by the front state bits are small, except those generated by the last state bit achieving the maximum value [30]. To overcome this drawback, a way was proposed to refine a single-cycle T-function $\boldsymbol{f}$ to another function $\varphi\boldsymbol{f}\varphi^{-1}$ [36] by a proper bijection φ between the states of both functions, such that the sequences generated by each state bit of the latter function achieve the maximum period [37, 38]. However, this does not guarantee that the sequences generated by the output functions of the latter function can achieve the maximum period.

This paper considers the cycle structure and observability of two types of Galois NFSRs, using the semi-tensor product-based Boolean network approach. It discloses that each Galois NFSR has the maximum state cycle for the first type, but has equal-length state cycles for the second. It also gives some easily verifiable necessary and/or sufficient conditions for the observability of each Galois NFSR for both types, generalizing the corresponding previous results on single-cycle T-functions. Each Galois NFSR in both types has simple feedback functions and has extensive selections for its output function to assure it to be observable, helpful for the design of stream ciphers.

2 Preliminaries

In this section, we review some basic concepts and related results on Boolean functions, T-functions, 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 represent the i-th column of the $n \times n$ identity matrix I_n. Let $\Delta_n = \{\delta_n^i | 1 \leqslant i \leqslant n\}$. $\mathcal{L}_{m\times n}$ is the set of $m\times n$ matrices, whose columns belong to Δ_n. A matrix $A \in \mathcal{L}_{m\times n}$ can be written as $A = [\delta_m^{i_1}, \delta_m^{i_2}, \ldots, \delta_m^{i_n}]$. For convenience, we rewrite $A = \delta_m[i_1, i_2, \ldots, i_n]$ in a compact form. $\mathrm{Col}_j(A)$ represents the j-th column of a matrix A, and $\mathrm{Col}(A)$ is the set of all columns of A. $|\cdot|$ represents the cardinality for a set, whereas it represents the absolute value for a real number. $+$, $-$, and $\times$ indicate the ordinary addition, subtraction, and multiplication in the real field, while $\oplus$ and $\odot$ represent the addition and multiplication over $\mathbb{F}_2$, respectively. For two integers a and b, $a \bmod b = c$ means the remainder of a divided by b is c.

2.1 Boolean function and T-function

An n-variable Boolean function f is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Let a constant vector $\boldsymbol{a} = [a_1 \ a_2 \ \cdots \ a_n]^{\mathrm{T}} \in \mathbb{F}_2^n$. The support set of a Boolean function f is $\mathrm{supp}(f) = \{\boldsymbol{a} | f(\boldsymbol{a}) = 1, \boldsymbol{a} \in \mathbb{F}_2^n\}$. For a variable $X_i \in \mathbb{F}_2$ and a value $a_i \in \mathbb{F}_2$, define $X_i^{a_i} = X_i \oplus a_i \oplus 1$. Then, $X_i^{a_i} = 1$ if and only if $X_i = a_i$; moreover, $X_i^0 = X_i \oplus 1$. Similarly, for a Boolean function f, define $f^0 = f \oplus 1$. For a variable vector $\boldsymbol{X} = [X_1 \ X_2 \ \cdots \ X_n]^{\mathrm{T}} \in \mathbb{F}_2^n$, define $\boldsymbol{X}^{\boldsymbol{a}} = X_1^{a_1} X_2^{a_2} \cdots X_n^{a_n}$. Then, $\boldsymbol{X}^{\boldsymbol{a}} = 1$ if and only if $\boldsymbol{X} = \boldsymbol{a}$. Therefore, the Boolean function f can be expressed by minterms as [39] $f(\boldsymbol{X}) = \bigoplus_{\boldsymbol{a}\in\mathrm{supp}(f)} \boldsymbol{X}^{\boldsymbol{a}} = \bigoplus_{\boldsymbol{a}\in\mathrm{supp}(f)} X_1^{a_1} X_2^{a_2} \cdots X_n^{a_n}$.

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

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

is called the structure matrix of f [40].

The function $\boldsymbol{f} = [f_1 \ f_2 \ \cdots \ f_n]^{\mathrm{T}}$ is a vectorial function if its components $f_1, f_2, \ldots, f_n$ are all Boolean functions. A triangular function (usually called a T-function for short) is a vectorial function, in which the i-th component is only dependent on the first i variables. It is a single-cycle T-function, if it has the maximum state cycle.

For a sequence $(s_i)_{i\geqslant 1}$, if k_0 is the least nonnegative integer such that $s_{i+p} = s_i$ for any positive integer $i \geqslant k_0$, then k_0 is called the preperiod of the sequence and p is called a period of the sequence. If $k_0 = 0$, then the sequence $(s_i)_{i\geqslant 1}$ is said to be periodic. The smallest number among all the possible periods of the sequence $(s_i)_{i\geqslant 1}$ is called the least period of the sequence, usually called the period for short if there is no confusion. As usual, in this paper the period of a sequence means the least period of the sequence.

Lemma 1 ([30]). The sequence generated by the i-th state bit of a single-cycle T-function is of period 2^i, and the second half of the sequence in a period is just dual to the first half.

Lemma 2 ([35]). Let $\boldsymbol{f} = [f_1 \ f_2 \ \cdots \ f_n]^{\mathrm{T}} \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a bijective T-function. Then $\boldsymbol{f}$ is a single-cycle T-function if and only if the algebraic normal form of each component is of form:

$$f_i = X_i \oplus X_1 \cdots X_{i-1} \oplus \phi_i(X_1, X_2, \ldots, X_{i-1}) \text{ for each } i \in \{1, 2, \ldots, n\},$$

where the algebraic degree of ϕ_i is no greater than $i-2$.

For a bijection $\varphi\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$, the vectorial functions $\boldsymbol{f}$ and $\boldsymbol{g} = \varphi \boldsymbol{f} \varphi^{-1}$ are said to be isomorphic, and they have the same cycle structure if they are used as state transition functions. For a single-cycle T-function $\boldsymbol{f}$, by properly selecting the bijection φ, the sequences generated by each state bit of $\boldsymbol{g} = \varphi \boldsymbol{f} \varphi^{-1}$ was proven to be of the maximum period, as shown in the following two lemmas.

Lemma 3 ([37]). The sequences generated from each state bit of a vectorial function $\boldsymbol{g}\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ achieve the maximum period 2^n, if $\boldsymbol{g} = P\boldsymbol{f}P^{-1}$, where $\boldsymbol{f}$ is a single-cycle T-function, and P is an $n \times n$ nonsingular matrix over $\mathbb{F}_2$ with the entries at the last column taking the value of 1.

Lemma 4 ([38]). The sequences generated from each bit of a vectorial function $\boldsymbol{g}\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ achieve the maximum period 2^n, if $\boldsymbol{g} = (\boldsymbol{h}R)\boldsymbol{f}(\boldsymbol{h}R)^{-1}$, where $\boldsymbol{f}$ and $\boldsymbol{h}$ are two single-cycle T-functions, and the bijection R over $\mathbb{F}_2^n$ satisfies $R\colon [X_1 \ X_2 \ \cdots \ X_n]^{\mathrm{T}} \mapsto [X_n \ X_{n-1} \ \cdots \ X_1]^{\mathrm{T}}$.

2.2 Boolean network

Definition 1 ([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 an $\frac{n\alpha}{m} \times \frac{q\alpha}{p}$ matrix, given by $A \ltimes B = (A \otimes I_{\frac{\alpha}{m}})(B \otimes I_{\frac{\alpha}{p}})$, where $\otimes$ represents the Kronecker product [41].

Lemma 5 ([40]). For any vector $\boldsymbol{Z} = [Z_1 \ \ Z_2 \ \cdots \ Z_r]^{\mathrm{T}} \in \mathbb{F}_2^r$, let $z = [Z_1 \ \ Z_1 \oplus 1]^{\mathrm{T}} \ltimes [Z_2 \ \ Z_2 \oplus 1]^{\mathrm{T}} \ltimes \cdots \ltimes [Z_r \ \ Z_r \oplus 1]^{\mathrm{T}}$. Then the vector $z = \delta_{2^r}^j \in \Delta_{2^r}$ with $j = 2^r - (2^{r-1}Z_1 + 2^{r-2}Z_2 + \cdots + Z_r)$; moreover, $\boldsymbol{Z} \in \mathbb{F}_2^r$ and $z \in \Delta_{2^r}$ are a one-to-one correspondence.

A Boolean network with n nodes and m outputs can be described as a set of difference equations (usually called a nonlinear system):

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

where $\boldsymbol{X} = [X_1 \ \ X_2 \ \cdots \ X_n]^{\mathrm{T}} \in \mathbb{F}_2^n$ is the state, the vectorial function $\boldsymbol{g} = [g_1 \ \ g_2 \ \cdots \ g_n]^{\mathrm{T}} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is the state transition function, $\boldsymbol{Y} = [Y_1 \ \ Y_2 \ \cdots \ Y_m]^{\mathrm{T}} \in \mathbb{F}_2^m$ is the output, and $\boldsymbol{h} = [h_1 \ \ h_2 \ \cdots \ h_m]^{\mathrm{T}} : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is the output function.

According to Lemma 5 and the structure matrix of a Boolean function, Boolean network (1) can be equivalently expressed as a linear system [40]:

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

with the state $\boldsymbol{x} \in \Delta_{2^n}$, the output $\boldsymbol{y} \in \Delta_{2^m}$, 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

$$\mathrm{Col}_j(L) = \mathrm{Col}_j(G_1) \otimes \mathrm{Col}_j(G_2) \otimes \cdots \otimes \mathrm{Col}_j(G_n), \ j = 1, 2, \ldots, 2^n, \tag{3}$$

where G_i is the structure matrix of the i-th component g_i of the vectorial function $\boldsymbol{g}$ in (1) for any $i \in \{1, 2, \ldots, n\}$. The j-th column of H can be computed similarly.

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

Lemma 6 ([40]). Let $M_k = \delta_2[\underbrace{A_k, A_k, \ldots, A_k}_{2^{k-1}}]$ with $A_k = \delta_2[\underbrace{1, 1, \ldots, 1}_{2^{n-k}}, \underbrace{2, 2, \ldots, 2}_{2^{n-k}}]$, $k = 1, 2, \ldots, n$. Then, the structure matrix of g_k in (1) is $G_k = M_k L$, where L is the state transition matrix in (2).

Definition 2 ([6]). Two distinct initial states of a Boolean network are said to be indistinguishable, if their resulting output sequences are equal; otherwise, they are said to be distinguishable. A Boolean network is said to be observable if every two distinct initial states are distinguishable.

Definition 3 ([6]). The observability matrix of Boolean network (2) in N steps is defined as

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

Lemma 7 ([6]). Boolean network (2) is observable if and only if the observability matrix $\mathcal{O}_{2^n-1}$ satisfies $|\mathrm{Col}(\mathcal{O}_{2^n-1})| = 2^n$, that is, $\mathcal{O}_{2^n-1}$ has 2^n distinct columns.

2.3 Nonlinear feedback shift register

An n-stage Galois NFSR, as shown in Figure 1(a), consists of n binary storage devices, also called bits. The content of bit i is denoted as X_i, which is updated by the feedback function f_i. All X_i compose the Galois NFSR's state $\boldsymbol{X} = [X_1 \ \ X_2 \ \cdots \ X_n]^{\mathrm{T}}$, and all feedback functions f_i form the Galois NFSR's feedback $\boldsymbol{f} = [f_1 \ \ f_2 \ \cdots \ f_n]^{\mathrm{T}}$. The output of the Galois NFSR, denoted by y, is the value of a Boolean function h, which takes the current contents of all bits as input. The n-stage Galois NFSR can be expressed as the following nonlinear system:

$$\begin{cases} X_1(t+1) = f_1(X_1(t), X_2(t), \ldots, X_n(t)), \\ \quad \vdots \\ X_n(t+1) = f_n(X_1(t), X_2(t), \ldots, X_n(t)), \\ y(t) = h(X_1(t), X_2(t), \ldots, X_n(t)), \end{cases} \tag{4}$$

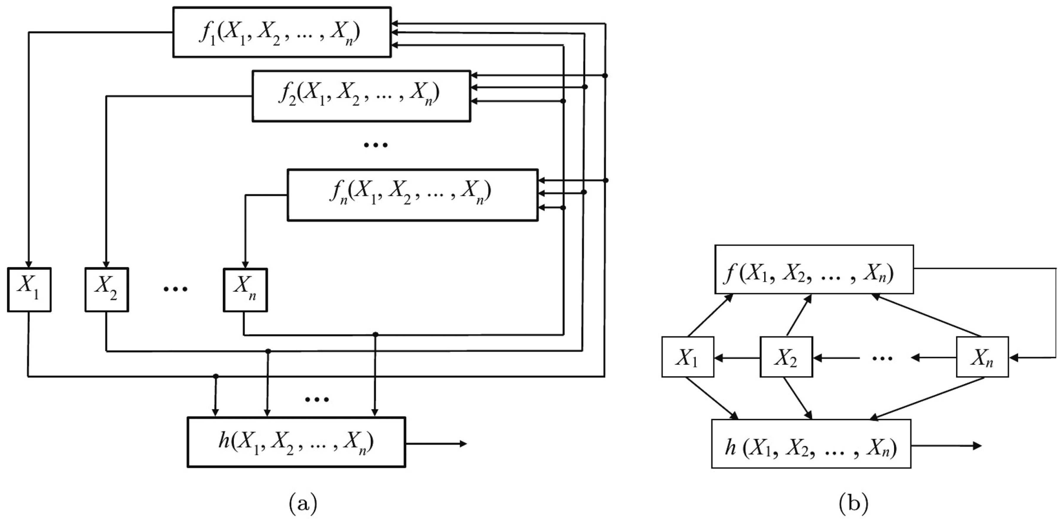

Figure 1 (a) An n-stage Galois NFSR; (b) an n-stage Fibonacci NFSR.

where t represents time instant. Eq. (4) can be rewritten in a vector form as

$$\begin{cases} \boldsymbol{X}(t+1) = \boldsymbol{f}(\boldsymbol{X}(t)), \\ y(t) = h(\boldsymbol{X}(t)). \end{cases} \tag{5}$$

If the feedback functions f_i satisfy $f_i(X_1, X_2, \dots, X_n) = X_{i+1}$ for all $i = 1, 2, \dots, n-1$, then the Galois NFSR is reduced to a Fibonacci NFSR, see Figure 1(b).

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 a state, and each directed edge represents a transition between two states. Precisely, if state $\boldsymbol{X}$ is updated to state $\boldsymbol{Y}$, then there is an edge from $\boldsymbol{X}$ to $\boldsymbol{Y}$. In this case, $\boldsymbol{X}$ is called the predecessor of $\boldsymbol{Y}$, whereas $\boldsymbol{Y}$ is called the successor of $\boldsymbol{X}$. A state sequence $\boldsymbol{X}_1, \boldsymbol{X}_2, \dots, \boldsymbol{X}_d$ forms a cycle of length d if the successor of $\boldsymbol{X}_d$ is $\boldsymbol{X}_1$. An NFSR and its state diagram are a one-to-one correspondence. An NFSR's state diagram contains only cycles if and only if its output sequences are all periodic.

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, and 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 bijection $\varphi\colon V \to \hat{V}$ such that there is an edge $E \in A$ from node N to node N' in G if and only if there is an edge $\hat{E} \in \hat{A}$ from $\varphi(N)$ to $\varphi(N')$ in $\hat{G}$. Furthermore, if the bijection $\varphi = D\colon [X_1 \ \ X_2 \ \cdots \ X_n]^{\mathrm{T}} \mapsto [X_1^0 \ \ X_2^0 \ \cdots \ X_n^0]^{\mathrm{T}}$, then G and $\hat{G}$ are said to be dual isomorphic, denoted by $\hat{G} = DG$; if the bijective mapping $\varphi = R\colon [X_1 \ \ X_2 \ \cdots \ X_n]^{\mathrm{T}} \mapsto [X_n \ \ X_{n-1} \ \cdots \ X_1]^{\mathrm{T}}$, then G and $\hat{G}$ are said to be anti-isomorphic, denoted by $\hat{G} = RG$; if the bijective mapping $\varphi = D\colon [X_1 \ \ X_2 \ \cdots \ X_n]^{\mathrm{T}} \mapsto [X_n^0 \ \ X_{n-1}^0 \ \cdots \ X_1^0]^{\mathrm{T}}$, 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, which is equivalent to saying that their feedbacks are isomorphic, or saying that they have the same cycle structure.

Lemma 8 ([42])**.** For an n-stage Galois NFSR$_1$ with feedback $\boldsymbol{f} = [f_1 \ \ f_2 \ \cdots \ f_n]^{\mathrm{T}}$,

(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 $D\boldsymbol{f}$ of the Galois NFSR$_2$ satisfies

$$D\boldsymbol{f} = [f_1^0(X_1^0, X_2^0, \dots, X_n^0) \quad f_2^0(X_1^0, X_2^0, \dots, X_n^0) \quad \cdots \quad f_n^0(X_1^0, X_2^0, \dots, X_n^0)]^{\mathrm{T}}; \tag{6}$$

(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 $R\boldsymbol{f}$ of the Galois NFSR$_3$ satisfies

$$R\boldsymbol{f} = [f_n(X_n, X_{n-1}, \dots, X_1) \quad f_{n-1}(X_n, X_{n-1}, \dots, X_1) \quad \cdots \quad f_1(X_n, X_{n-1}, \dots, X_1)]^{\mathrm{T}}; \tag{7}$$

(3) The state diagram of an n-stage Galois NFSR$_4$ is dual anti-isomorphic to that of Galois NFSR$_1$, if and only if the feedback $DR\boldsymbol{f}$ of the Galois NFSR$_4$ satisfies

$$DR\boldsymbol{f} = [f_n^0(X_n^0, X_{n-1}^0, \dots, X_1^0) \quad f_{n-1}^0(X_n^0, X_{n-1}^0, \dots, X_1^0) \quad \cdots \quad f_1^0(X_n^0, X_{n-1}^0, \dots, X_1^0)]^{\mathrm{T}}. \tag{8}$$

Lemma 9 ([16])**.** The period of the output sequence of a Galois NFSR with an arbitrary output function is a divisor of the corresponding state cycle's length.

Viewing an NFSR as a Boolean network, we can get the first equation in (5) equivalently expressed as $\boldsymbol{x}(t+1) = L\boldsymbol{x}(t)$. The NFSR is nonsingular if and only if L is nonsingular (see, Lemma 5 in the supplementary file of [43]); that is, L is a permutation matrix. Considering that a nonsingular circulant matrix is a particular permutation matrix, we herein consider Galois NFSRs with state transition matrices of form nonsingular circulant matrices $L = \delta_{2^n}[i, i+1, \ldots, 2^n, 1, 2, \ldots, i-1]$, determined by the positive integer i, which represents the position of element 1 in the first column. We study the Galois NFSRs in two types. In the first type, the position i is even, whereas in the second type, the position i is odd. However, the feedback functions of a Galois NFSR in the second type can be computed from those of a Galois NFSR in the first type, which can be seen later in Sections 3 and 4.

3 First type of Galois NFSRs

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

$$L = \delta_{2^n}[i, i+1, \ldots, 2^n, 1, 2, \ldots, i-1], \text{ where } i \text{ is even.} \tag{9}$$

We first disclose that each Galois NFSR in this type has the maximum state cycle. We then reveal the explicit form of its feedback functions, which is simple. Finally, we disclose its observability with output function that is only required to be dependent on the first state bit.

3.1 Type of maximum-cycle Galois NFSRs

Theorem 1. An n-stage Galois NFSR with state transition matrix L in (9), has the maximum state cycle.

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

$$\delta_{2^n}^1, \delta_{2^n}^i, \delta_{2^n}^{2(i-1) \bmod 2^n+1}, \ldots, \delta_{2^n}^{k(i-1) \bmod 2^n+1}, \ldots, \delta_{2^n}^{(2^n-1)(i-1) \bmod 2^n+1}, \delta_{2^n}^1, \ldots \tag{10}$$

Note that an n-stage Galois NFSR has 2^n possible states. Then, to prove the result, we are only required to prove that the state sequence in (10) has the period 2^n.

As i is even, we have $\delta_{2^n}^i \neq \delta_{2^n}^1$. Assume in (10) the state 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, we have $k(i-1) \bmod 2^n + 1 = 1$, which implies that $2^n | k(i-1)$. As i is even, $i-1$ is odd. Then there must exist $2^n | k$, which implies that the period of the state sequence in (10) is $k = 2^n$.

The proof of Theorem 1 shows that, an n-stage Galois NFSR with state transition matrix L in (9) has a 2^n-period state sequence in (10) over Δ_{2^n}, whose corresponding state sequence in $\mathbb{F}_2^n$ can be easily obtained according to Lemma 5.

Theorem 2. If an n-stage Galois NFSR has the state transition matrix L in (9), then its feedback $\boldsymbol{f} = [f_1 \ \ f_2 \ \ \cdots \ \ f_n]^{\mathrm{T}}$ satisfies the following recursive relation:

(1) $f_n = X_n^0$;

(2) For any $k \in \{2, 3, \ldots, n\}$, let $j = (i-1) \bmod 2^{n-k+2} + 1$,

(a) If $1 \leqslant j \leqslant 2^{n-k}$, then $f_{k-1} = X_k^0 f_k \oplus X_{k-1}$;

(b) If $2^{n-k} + 1 \leqslant j \leqslant 2^{n-k+1}$, then $f_{k-1} = X_k f_k^0 \oplus X_{k-1}^0$;

(c) If $2^{n-k+1} + 1 \leqslant j \leqslant 2^{n-k+1} + 2^{n-k}$, then $f_{k-1} = X_k^0 f_k \oplus X_{k-1}^0$;

(d) If $2^{n-k+1} + 2^{n-k} + 1 \leqslant j \leqslant 2^{n-k+2}$, then $f_{k-1} = X_k f_k^0 \oplus X_{k-1}$.

Proof. According to Lemma 6, we can easily see the structure matrix of f_n is

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

which implies $f_n = X_n^0$. To compute the other feedback functions f_k with $k \in \{1, 2, \ldots, n-1\}$, let $l := 2^n - (2^{n-1}X_1 + 2^{n-2}X_2 + \cdots + X_n)$. Then $[X_1 \ \ X_2 \ \ \cdots \ \ X_n]^{\mathrm{T}}$ is the l-th state if all states of the n-stage Galois NFSR are arranged in descending order according to their corresponding decimal numbers. In the following, we discuss the recursive relation between f_k and f_{k-1} with $k \in \{2, 3, \ldots, n\}$, under the different ranges of j and l as follows.

Table 1 Values of X_{k-1}, X_k, f_k, and f_{k-1} with $k \in \{2, 3, \ldots, n\}$ for the case of $1 \leqslant j \leqslant 2^{n-k}$.

Range of l	X_{k-1}	X_k	f_k	f_{k-1}
$1 \leqslant l \leqslant 2^{n-k} - j + 1$	1	1	1	1
$2^{n-k} - j + 2 \leqslant l \leqslant 2^{n-k}$	1	1	0	1
$2^{n-k} + 1 \leqslant l \leqslant 2^{n-k+1} - j + 1$	1	0	0	1
$2^{n-k+1} - j + 2 \leqslant l \leqslant 2^{n-k+1}$	1	0	1	0
$2^{n-k+1} + 1 \leqslant l \leqslant 2^{n-k+1} + 2^{n-k} - j + 1$	0	1	1	0
$2^{n-k+1} + 2^{n-k} - j + 2 \leqslant l \leqslant 2^{n-k+1} + 2^{n-k}$	0	1	0	0
$2^{n-k+1} + 2^{n-k} + 1 \leqslant l \leqslant 2^{n-k+2} - j + 1$	0	0	0	0
$2^{n-k+2} - j + 2 \leqslant l \leqslant 2^{n-k+2}$	0	0	1	1

For the case of $1 \leqslant j \leqslant 2^{n-k}$, according to Lemma 6, we can get the values of X_{k-1}, X_k, f_k, and f_{k-1} for different ranges of l, as shown in Table 1. As i is even, so is j. Thus, the number of all l in each range therein is odd. Regarding X_{k-1}, X_k, and f_k as the variables of f_{k-1}, we can deduce from Table 1 that, f_{k-1} can be expressed by minterms of form $f_{k-1} = X_{k-1}(X_k f_k \oplus X_k f_k^0 \oplus X_k^0 f_k^0) \oplus X_{k-1}^0 X_k^0 f_k = X_k^0 f_k \oplus X_{k-1}$. Similarly, we can get the recursive relation for the other cases of j.

Example 1. Consider an n-stage Galois NFSR with state transition matrix $L = \delta_{2^n}[2, 3, \ldots, 2^n, 1]$.

According to Theorem 2, we can get its feedback $\boldsymbol{f} = [f_1 \quad f_2 \quad \cdots \quad f_n]^{\mathrm{T}}$ satisfying $f_n = X_n^0$ and $f_k = X_k \oplus X_{k+1}^0 X_{k+2}^0 \cdots X_n^0$ for all $k = 1, 2, \ldots, n-1$.

If the feedback $\boldsymbol{f}$ of an n-stage Galois NFSR$_1$ with state transition matrix L in (9) is computed according to Theorem 2, then we can easily derive from Lemma 8 the feedbacks $D\boldsymbol{f}, R\boldsymbol{f}$, and $RD\boldsymbol{f}$ of the Galois NFSRs, which are dual isomorphic, anti-isomorphic, and dual anti-isomorphic to Galois NFSR$_1$, respectively. Moreover, we can observe that, each feedback $D\boldsymbol{f}$ results from $\boldsymbol{f}$ via each feedback function, and each variable is replaced by its own complement, and each feedback $R\boldsymbol{f}$ or $RD\boldsymbol{f}$ satisfies the conditions for a single-cycle T-function in Lemma 2.

3.2 Observability

In this section, we give some necessary and sufficient conditions for the observability of the first type of Galois NFSRs, and extend them to Galois NFSRs with feedbacks of single-cycle T-functions.

Lemma 10. An n-stage maximum-cycle Galois NFSR is observable if and only if there exists an initial state $\boldsymbol{X}(t_0)$ such that its resulting output sequence $(Y(t))_{t \geqslant t_0}$ satisfies $Y(t_0) \neq Y(t_0 + 2^{n-1})$.

Proof. Necessity. We prove this lemma through contradiction. If for any initial state $\boldsymbol{X}(t_0)$, the resulting output sequence $(Y(t))_{t \geqslant t_0}$ satisfies $Y(t_0) = Y(t_0 + 2^{n-1})$, then the initial states $X(t_0)$ and $X(t_0 + 2^{n-1})$ result in the same output sequences. This implies that the Galois NFSR is not observable, which is contrary to the assumption that the Galois NFSR is observable.

Sufficiency. If there exists an initial state $\boldsymbol{X}(t_0)$ such that its resulting output sequence $(Y(t))_{t \geqslant t_0}$ satisfies $Y(t_0) \neq Y(t_0 + 2^{n-1})$, then considering that the proper divisor of 2^n is 2^m with nonnegative integer $0 \leqslant m < n$, we derive from Lemma 9 that the output sequence $(Y(t))_{t \geqslant t_0}$ has the period 2^n. As the Galois NFSR has the maximum-length cycle, we can deduce that the sequence resulting from any initial state has the period 2^n, which implies that any two distinct initial states result in different output sequences. Therefore, the Galois NFSR is observable.

From Lemmas 9 and 10, we directly obtain the following results.

Corollary 1. An n-stage maximum-cycle Galois NFSR is observable if and only if there is an output sequence generated by the n-stage maximum-cycle Galois NFSR achieving the maximum period 2^n.

Corollary 2. For any positive integer k, any two distinct initial states on a cycle of length 2^k are distinguishable if and only if there is an output sequence generated by the cycle achieving the period 2^k.

Theorem 3. An n-stage Galois NFSR with state transition matrix L in (9) is observable if and only if the output function is dependent on the first state bit variable X_1.

Proof. According to Theorem 1 and its proof, an n-stage Galois NFSR with state transition matrix L in (9) is a maximum-cycle Galois NFSR and has a state sequence in (10). 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 $1 \leqslant k \leqslant 2^n$. Then, according to the state sequence in (10), $\delta_{2^n}^j$ is updated to $\delta_{2^n}^{[(2^{n-1}+k)(i-1)] \bmod 2^n+1} := \delta_{2^n}^l$

at time $t+2^{n-1}$. Note that $(a+b) \bmod n = [(a \bmod n)+(b \bmod n)] \bmod n$. Then, we have

$$l=(2^{n-1}+j-1) \bmod 2^n+1=\begin{cases} j+2^{n-1}, & \text{if } 1\leqslant j\leqslant 2^{n-1};\\ j-2^{n-1}, & \text{if } 2^{n-1}+1\leqslant j\leqslant 2^n.\end{cases}$$

Hence, $|l-j|=2^{n-1}$. Assume that the n-dimensional vector uniquely corresponding to the state $\delta_{2^n}^j$ at time t is $\boldsymbol{X}(t)=[X_1(t)\ \ X_2(t)\ \ \cdots\ \ X_n(t)]^{\mathrm{T}}$, and uniquely corresponding to the state $\delta_{2^n}^l$ at time $t+2^{n-1}$ is $\boldsymbol{X}(t+2^{n-1})=[X_1(t+2^{n-1})\ \ X_2(t+2^{n-1})\ \ \cdots\ \ X_n(t+2^{n-1})]^{\mathrm{T}}$. Thus, we deduce from Lemma 5 that

$$X_1(t)=X_1(t+2^{n-1})\oplus 1,\ X_i(t)=X_i(t+2^{n-1}) \text{ for any } t\in\mathbb{N} \text{ and any } i\in\{2,3,\ldots,n\}. \quad (11)$$

We rewrite the output function h of the Galois NFSR as

$$Y=h(X_1,X_2,\ldots,X_n)=X_1g_1(X_2,X_3,\ldots,X_n)\oplus g_2(X_2,X_3,\ldots,X_n). \quad (12)$$

Then along with (11), we have

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

Hence, there exists an initial state $\boldsymbol{X}(t_0)$ such that the resulting output sequence $(Y(t))_{t\geqslant t_0}$ satisfies $Y(t_0)\neq Y(t_0+2^{n-1})$, if and only if $g_1\not\equiv 0$, which is equivalent to saying that the output function h is dependent on the variable X_1, drawn from (12). Thus, the result follows from Lemma 10.

Example 2. Consider a 3-stage Galois NFSR with state transition matrix $L=\delta_8[2,3,\ldots,8,1]$. We can easily observe that it has a state sequence $\delta_8^1,\delta_8^2,\delta_8^3,\ldots,\delta_8^7,\delta_8^8,\delta_8^1,\ldots$. Take the output function $h=X_1$. Then we can easily compute that the output sequence resulting from the initial state δ_8^1 is an 8-period sequence 11110000, implying that the Galois NFSR is observable. On the other hand, according to Theorem 3, the Galois NFSR is observable, consistent with the fact above.

Theorem 4. An n-stage Galois NFSR with feedback of a single-cycle T-function is observable if and only if the output function is dependent on the last state bit variable X_n.

Proof. Because the feedback of the Galois NFSR is a single-cycle T-function, according to Lemma 1, the sequence $\{X_i(t)\}_{t\geqslant 0}$ generated by the i-th state bit of the Galois NFSR is of period 2^i, and $X_i(t)\oplus X_i(t+2^{i-1})=1$ for any $t\in\mathbb{N}$ and any $i\in\{1,2,\ldots,n\}$. Thus, $X_n(t)=X_n(t+2^{n-1})\oplus 1$ and $X_i(t)=X_i(t+2^{n-1})$ for any $t\in\mathbb{N}$ and any $i\in\{1,2,\ldots,n-1\}$. Regarding X_n here as X_1 in Theorem 3, we use a similar way there and conclude that the result holds.

In the following, we apply Theorem 4 to the stream cipher ABC [34], a candidate in the eSTREAM project. ABC uses three main primitives: A, B, and C. A is an LFSR, used as a counter. B is a single-cycle T-function, used as a state transition function. C is the output of B.

The single-cycle T-function B is $B(\boldsymbol{X})=\boldsymbol{d}_0+5(\boldsymbol{X}\ \text{XOR}\ \boldsymbol{d}_1)$, where $\boldsymbol{X}=[X_1\ \ X_2\ \ \cdots\ \ X_{32}]^{\mathrm{T}}\in\mathbb{F}_2^{32}$ is the state, $\boldsymbol{d}_0=[d_{0,1}\ \ d_{0,2}\ \ \cdots\ \ d_{0,32}]^{\mathrm{T}}\in\mathbb{F}_2^{32}$ and $\boldsymbol{d}_1=[d_{1,1}\ \ d_{1,2}\ \ \cdots\ \ d_{1,32}]^{\mathrm{T}}\in\mathbb{F}_2^{32}$ are two vectors, respectively dependent on the key and initialization vector (IV) determined at the initialization stage of the cipher, and XOR is a bitwise exclusive of vectors.

The output function C takes $\boldsymbol{X}$ as an argument and generates $\boldsymbol{Y}=[Y_1\ \ Y_2\ \ \cdots\ \ Y_{32}]^{\mathrm{T}}\in\mathbb{F}_2^{32}$ through two equations: $\zeta=S(\boldsymbol{X})=\boldsymbol{e}+\sum_{i=1}^{32}\boldsymbol{e}_iX_i$ and $\boldsymbol{Y}=\zeta\lll 16$, where $\cdot\lll c$ represents a left bitwise rotation by c bits for a vector, $\boldsymbol{e}=[e_1\ \ e_2\ \ \cdots\ \ e_{32}]^{\mathrm{T}}$ and $\boldsymbol{e}_i=[e_{i,1}\ \ e_{i,2}\ \ \cdots\ \ e_{i,32}]^{\mathrm{T}}$ with $i=1,2,\ldots,32$, are vectors in $\mathbb{F}_2^{32}$, dependent on the key and IV; moreover, $e_{32,17}=1$ and $e_{32,j}=0$ for all $j=1,2,\ldots,16$.

As the decimal number 5 corresponds to the binary vector $[1\ 0\ 1]^{\mathrm{T}}$, $B(\boldsymbol{X})=[B_1(\boldsymbol{X})\ B_2(\boldsymbol{X})\ \cdots\ B_{32}(\boldsymbol{X})]^{\mathrm{T}}$ defined above can be computed via a right zero-fill shift and an extra addition. Through a direct computation, we can obtain $B_1(\boldsymbol{X})=X_1\oplus d_{1,1}\oplus d_{0,1}$, $B_2(\boldsymbol{X})=X_2\oplus d_{1,2}\oplus d_{0,2}\oplus d_{0,1}(X_1\oplus d_{1,1})$, $B_3(\boldsymbol{X})=X_3\oplus d_{1,3}\oplus X_1\oplus d_{1,1}\oplus d_{0,3}\oplus d_{0,2}(X_2\oplus d_{1,2})\oplus d_{0,1}(X_1\oplus d_{1,1})(X_2\oplus d_{1,2})\oplus d_{0,1}d_{0,2}(X_1\oplus d_{1,1})$, $\ldots$, $B_{32}(\boldsymbol{X})=B_{32}(X_1,X_2,\ldots,X_{32})$. Because $e_{32,17}=1$, we can easily compute that the 17-th component of ζ is dependent on the variable X_{32}, implying Y_1 is dependent on X_{32} as well. According to Theorem 4, the Galois NFSR with feedback of a single-cycle T-function B and with output function Y_1, is observable. Thus, the output sequence generated by output function Y_1 can achieve the maximum period 2^{32}. Notably, the period of the output sequence generated by output function $\boldsymbol{Y}$ is the least common multiple of all periods p_i of the output sequences generated by output functions Y_i for all $i=1,2,\ldots,32$. Moreover, each p_i is a divisor of the state cycle length 2^{32} according to Lemma 9. Therefore, the output sequence generated by output function $\boldsymbol{Y}$ can achieve the maximum period 2^{32}, consistent with the statement in [34].

Theorem 5. For an n-stage Galois NFSR_1 with feedback $\boldsymbol{f}$ of a single-cycle T-function, let an n-stage Galois NFSR_2 have the feedback $\boldsymbol{g} = \varphi \boldsymbol{f} \varphi^{-1}$, where $\varphi = [\varphi_1 \ \ \varphi_2 \ \ \cdots \ \ \varphi_n]^{\mathrm{T}}$ is a bijection over $\mathbb{F}_2^n$. Then for any $j \in \{1, 2, \ldots, n\}$, the sequences generated by the j-th state bit of Galois NFSR_2 achieve the maximum period 2^n if and only if φ_j is dependent on the state bit variable X_n.

Proof. Let $\boldsymbol{X} = [X_1 \ \ X_2 \ \ \cdots \ \ X_n]^{\mathrm{T}}$ and $\boldsymbol{Y} = [Y_1 \ \ Y_2 \ \ \cdots \ \ Y_n]^{\mathrm{T}}$ be the states of NFSR_1 and NFSR_2, respectively. As the feedbacks of NFSR_1 and NFSR_2 satisfy $\boldsymbol{g} = \varphi \boldsymbol{f} \varphi^{-1}$, we can deduce that $\boldsymbol{Y} = \varphi(\boldsymbol{X})$, yielding $Y_j = \varphi_j(\boldsymbol{X})$ for all $j = 1, 2, \ldots, n$. Then, for any $j \in \{1, 2, \ldots, n\}$, the sequence $\{\varphi_j(\boldsymbol{X}(t))\}_{t \geqslant 0}$ can be seen as the output sequence generated by NFSR_1, with $\varphi_j : \mathbb{F}_2^n \to \mathbb{F}_2$ as its output function.

As NFSR_1 has the feedback of a single-cycle T-function, it is a maximum-cycle Galois NFSR. According to Corollary 1, the output sequences generated by NFSR_1 achieve the maximum period 2^n if and only if NFSR_1 is observable. According to Theorem 4, NFSR_1 is observable if and only if its output function is dependent on the last state bit variable X_n. Therefore, for any $j \in \{1, 2, \ldots, n\}$, the sequences generated by the j-th state bit of NFSR_2 achieve the maximum period 2^n if and only if φ_j is dependent on the state bit variable X_n.

Theorem 5 generalizes the results in Lemmas 3 and 4, as the nonsingular matrix P in Lemma 3 and the bijection $\boldsymbol{h}R$ in Lemma 4 satisfy $\varphi(\boldsymbol{X}) = P\boldsymbol{X}$ and $\varphi(\boldsymbol{X}) = \boldsymbol{h}R$, with their j-th ($1 \leqslant j \leqslant n$) components dependent on the last state bit X_n, consistent with the sufficient condition in Theorem 5.

In Theorem 5, although the sequences generated by each state bit of NFSR_2 achieve the maximum period, the sequences generated by NFSR_2 with an arbitrary output function do not necessarily achieve the maximum period. Note that the feedbacks of NFSR_1 and NFSR_2 satisfy $\boldsymbol{g} = \varphi \boldsymbol{f} \varphi^{-1}$, which means that the states of both NFSRs have the relation $\boldsymbol{Y} = \varphi(\boldsymbol{X})$. Hence, if NFSR_1 with feedback $\boldsymbol{f}$ is observable with output function h, then NFSR_2 with feedback $\boldsymbol{g} = \varphi \boldsymbol{f} \varphi^{-1}$ is observable with output function $h\varphi^{-1}$. Therefore, using Theorem 3 and the bijections, denoted by φ as well, we can get more Galois NFSRs with feedbacks of form $\varphi \boldsymbol{f} \varphi^{-1}$ and with output functions of form $h\varphi^{-1}$. Herein, $\boldsymbol{f}$ is the feedback of a Galois NFSR in the first type and h is dependent on the first state bit X_1, such that the Galois NFSRs have output sequences achieving the maximum period. Similarly, using Theorem 4 and the bijections φ, we can get more Galois NFSRs with feedbacks of form $\varphi \boldsymbol{f} \varphi^{-1}$ and with output functions of form $h\varphi^{-1}$. Herein, $\boldsymbol{f}$ is a single-cycle T-function and h is dependent on the last state bit X_n, such that the Galois NFSRs have output sequences achieving the maximum period.

4 Second type of Galois NFSRs

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

$$L = \delta_{2^n}[i, i+1, \ldots, 2^n, 1, 2, \ldots, i-1], \text{ where } i = 2^m + 1, \tag{13}$$

with positive integer m satisfying $1 \leqslant m \leqslant n-1$. We first disclose that the Galois NFSR has 2^m state cycles of length 2^{n-m}. We then reveal its explicit expression of feedback, based on what we have obtained in Section 3 for a Galois NFSR in the first type. Finally, we give some necessary and/or sufficient conditions for its observability.

4.1 Type of Galois NFSRs with equal-length state cycles

Theorem 6. An n-stage Galois NFSR with state transition matrix L in (13), has 2^m state cycles of length 2^{n-m}.

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

$$\delta_{2^n}^1, \delta_{2^n}^{2^m+1}, \delta_{2^n}^{2\cdot 2^m \bmod 2^n+1}, \ldots, \delta_{2^n}^{k\cdot 2^m \bmod 2^n+1}, \ldots, \delta_{2^n}^{(2^{n-m}-1)\cdot 2^m \bmod 2^n+1}, \delta_{2^n}^1, \ldots \tag{14}$$

Assume in (14) the state equal to $\delta_{2^n}^1$ for the first time is $\delta_{2^n}^{k\cdot 2^m \bmod 2^n+1}$; that is, k is the least positive integer such that $\delta_{2^n}^{k\cdot 2^m \bmod 2^n+1} = \delta_{2^n}^1$. Then, $k \cdot 2^m \bmod 2^n + 1 = 1$, which implies that $2^n | k2^m$. Then $k = 2^{n-m}$. Hence, there are 2^{n-m} different states in (14), yielding a cycle C_1 of length 2^{n-m}.

Moreover, we can see that the states over Δ_{2^n} on the cycle C_1 have one common characterization, that is, their superscripts divided by 2^m have a remainder of 1. Similarly, for any $k \in \{2, 3, \ldots, 2^m - 1\}$, the states whose superscripts divided by 2^m have a remainder of k, compose another one state cycle C_k of length 2^{n-m}. Therefore, the Galois NFSR has totally 2^m cycles of length 2^{n-m} in its state diagram.

Theorem 7. For an n-stage Galois NFSR$_1$ with state transition matrix $L_1 = \delta_{2^n}[i, i+1, \ldots, 2^n, 1, 2, \ldots, i-1]$, where $i = 2^m$ with positive integer m satisfying $1 \leqslant m \leqslant n-1$, and for an n-stage Galois NFSR$_2$ with state transition matrix $L_2 = \delta_{2^n}[i, i+1, \ldots, 2^n, 1, 2, \ldots, i-1]$ where $i = 2^m+1$, let $\boldsymbol{f} = [f_1\ f_2\ \cdots\ f_n]^{\mathrm{T}}$ and $\boldsymbol{g} = [g_1\ \ g_2\ \ \cdots\ \ g_n]^{\mathrm{T}}$ be their feedbacks, respectively. Then the feedback functions in $\boldsymbol{f}$ and $\boldsymbol{g}$ have the following relations:

(1) $g_n = f_n \oplus 1$;

(2) $g_{n-1} = f_{n-1} \oplus X_n$;

(3) $g_k = f_k \oplus X^0_{k+1} X^0_{k+2} \cdots X^0_{n-m} X_{n-m+1} \cdots X_n$ for all $k = 1, 2, \ldots, n-2$.

Proof. According to Lemma 6, the structure matrix of the n-th feedback function g_n of NFSR$_1$ is

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

Hence, $g_n = X_n$. From Theorem 2, we know $f_n = X^0_n$. Therefore, $g_n = f_n \oplus 1$.

Note that, if we use minterms to represent a Boolean function, we are only required to consider the states at which the Boolean function takes a value of 1. The states $\delta^1_{2^n}, \delta^2_{2^n}, \ldots, \delta^{2^{n-1}}_{2^n}$ over Δ_{2^n} correspond to those states, whose first components are 1 over $\mathbb{F}^n_2$. 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 $\delta^1_{2^n}, \delta^2_{2^n}, \ldots, \delta^{2^{n-1}}_{2^n}$. For any $j \in \{1, 2, \ldots, 2^n\}$, let $j = k(i-1) \bmod 2^n + 1$ with positive integers $k \leqslant 2^n$ and $2 \leqslant i \leqslant 2^n$. Then according to the proof of Theorem 1, we know that for an n-stage Galois NFSR with state transition matrix $L = \delta_{2^n}[i, i+1, \ldots, 2^n, 1, 2, \ldots, i-1]$, the predecessor of state $\delta^j_{2^n}$ is $\delta^{(k-1)(i-1) \bmod 2^n+1}_{2^n} := \delta^p_{2^n}$. Thus, we have

$$p = [k(i-1) \bmod 2^n + (1-i) \bmod 2^n] \bmod 2^n + 1 = (j-i) \bmod 2^n + 1. \tag{15}$$

In the above inferences, the first equation applies $(a+b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$, the second uses $j = k(i-1) \bmod 2^n + 1$ with positive integers $k \leqslant 2^n$ and $2 \leqslant i \leqslant 2^n$, and uses $a \bmod n = a + (\lfloor(-a)/n\rfloor + 1)n$ for a negative integer a, where $\lfloor(-a)/n\rfloor$ represents the positive integer no greater than $(-a)/n$, and also utilizes the property applied in the first. Note that for NFSR$_1$ and NFSR$_2$, the positive integer i respectively takes the values of two adjacent positive integers, 2^m and 2^m+1, with positive integer m satisfying $1 \leqslant m \leqslant n-1$. Then along with (15), we can deduce that the two support sets $\mathrm{supp}(f_1)$ and $\mathrm{supp}(g_1)$ have only two different states $\delta^{[1-(2^m+1)] \bmod 2^n+1}_{2^n} = \delta^{2^n-2^m+1}_{2^n}$ from NFSR$_2$ and $\delta^{(2^{n-1}-2^m) \bmod 2^n+1}_{2^n} = \delta^{2^{n-1}-2^m+1}_{2^n}$ from NFSR$_1$. Their corresponding n-dimensional vectors, respectively, are $\boldsymbol{a} = [\underbrace{0,0,\ldots,0}_{n-m}, \underbrace{1,1,\ldots,1}_{m}]^{\mathrm{T}}$ and $\boldsymbol{b} = [1, \underbrace{0,0,\ldots,0}_{n-m-1}, \underbrace{1,1,\ldots,1}_{m}]^{\mathrm{T}}$. Therefore,

$$\begin{aligned} f_1 \oplus g_1 = \boldsymbol{X}^{\boldsymbol{a}} \oplus \boldsymbol{X}^{\boldsymbol{b}} &= X^0_1 X^0_2 \cdots X^0_{n-m} X_{n-m+1} \cdots X_n \oplus X_1 X^0_2 \cdots X^0_{n-m} X_{n-m+1} \cdots X_n \\ &= X^0_2 \cdots X^0_{n-m} X_{n-m+1} \cdots X_n, \end{aligned}$$

yielding $g_1 = f_1 \oplus X^0_2 \cdots X^0_{n-m} X_{n-m+1} \cdots X_n$. Keeping the same reasoning, we can get $g_{n-1} = f_{n-1} \oplus X_n$, and $g_k = f_k \oplus X^0_{k+1} \cdots X^0_{n-m} X_{n-m+1} \cdots X_n$ for all remaining $k = 2, 3, \ldots, n-2$.

Example 3. Consider an n-stage Galois NFSR with state transition matrix $L = \delta_{2^n}[3, 4, \ldots, 2^n, 1, 2]$.

According to Theorem 7, its feedback functions can be derived from the Galois NFSR with state transition matrix $L = \delta_{2^n}[2, 3, \ldots, 2^n, 1, 2, 3]$ in Example 1 as

$$\begin{cases} g_k = X_k \oplus X^0_{k+1} X^0_{k+2} \cdots X^0_{n-1}, \quad k = 1, 2, \ldots, n-2, \\ g_{n-1} = X^0_{n-1}, \\ g_n = X_n. \end{cases} \tag{16}$$

For an n-stage Galois NFSR with state transition matrix $L = \delta_{2^n}[i, i+1, \ldots, 2^n, 1, 2, \ldots, i-1]$ with $i = 2m+1$, we can similarly get its feedback functions. However, its cycle structure and observability are related to the relation between n and m, which is much more complex and is not studied in the paper.

4.2 Observability

In this section, we give some necessary and/or sufficient conditions for the observability of the second type of Galois NFSRs.

Proposition 1. For an n-stage Galois NFSR with state transition matrix L in (13), if its output function $h(X_1, X_2, \ldots, X_n) = X_j$ for any $j \in \{1, 2, \ldots, n\}$, then the Galois NFSR is unobservable.

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

$$H = [\,\underbrace{A \;\; A \;\; \cdots \;\; A}_{2^{j-1}}\,] \text{ with } A = \delta_2[\,\underbrace{1, 1, \ldots, 1}_{2^{n-j}},\ \underbrace{0, 0, \ldots, 0}_{2^{n-j}}\,]. \tag{17}$$

According to Theorem 6, the Galois NFSR has 2^m cycles of length 2^{n-m}, which implies the order of the state transition matrix L (i.e., the least positive integer N such that $L^N = I$) is the least common multiple of 2^m occurrences of 2^{n-m}, that is, the order of L is 2^{n-m}. Thus, 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; that is,

$$|\mathrm{Col}(\mathcal{O}_{2^{n-m}+l})| = |\mathrm{Col}(\mathcal{O}_{2^{n-m}})| \text{ for any positive integer } l. \tag{18}$$

As $1 \leqslant m \leqslant n-1$, we have $n \geqslant 2$. Therefore, we can equally partition the 2^n columns of H into 2^{n-m} blocks; that is, $H = [B_1 \;\; B_2 \;\; \cdots \;\; B_{2^{n-m}}]$ with each $B_s \in \mathcal{L}_{2\times 2^m}$ for each $s \in \{1, 2, \ldots, 2^{n-m}\}$. Considering (17), we can easily observe that each B_s has the following properties:

(1) if $n - j \geqslant m$, then $|\mathrm{Col}(B_s)| = 1$;

(2) if $n - j < m$, then each $|\mathrm{Col}(B_s)| = 2$, moreover,

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

Because L is a circulant matrix, we can deduce that for any positive integer $k \leqslant 2^{n-m} - 1$, 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 in the matrix HL^k. Thus, $HL^k = [B_{k+1}, B_{k+2}, \ldots, B_{2^{n-m}}, B_1, B_2, \ldots, B_k]$ for any positive integer $k \leqslant 2^{n-m} - 1$. Therefore, if $n - j \geqslant m$, then the observability matrix $\mathcal{O}_{2^{n-m}}$ satisfies $|\mathrm{Col}(\mathcal{O}_{2^{n-m}})| \leqslant 2^{n-m}$; if $n - j < m$, then $|\mathrm{Col}(\mathcal{O}_{2^{n-m}})| = 2$.

As $m \geqslant 1$ and $n \geqslant 2$, we have $2^{n-m} < 2^n$ and $2 < 2^n$ and therefore, $|\mathrm{Col}(\mathcal{O}_{2^{n-m}})| < 2^n$. According to (18), we have $|\mathrm{Col}(\mathcal{O}_{2^n-1})| = |\mathrm{Col}(\mathcal{O}_{2^{n-m}})| < 2^n$. From Lemma 7, the Galois NFSR is unobservable.

The following lemma can be directly obtained.

Lemma 11. Let $\widetilde{d}$ be the number of d-period sequences, and $d_1, d_2, \ldots, d_m$ be the proper factors of d. Then $\widetilde{d} = 2^d - \widetilde{d_1} - \widetilde{d_2} - \cdots - \widetilde{d_m}$.

Proposition 2. For an n-stage Galois NFSR with state transition matrix L in (13), if $2^{2^{n-m}} - 2^{2^{n-m-1}} \geqslant 2^n$, then there must exist an output function such that the NFSR is observable.

Proof. Let $\widetilde{d}$ be the number of d-period sequences. Then, according to Lemma 11, $\widetilde{2^{n-m}} = 2^{2^{n-m}} - \widetilde{2^{n-m-1}} - \widetilde{2^{n-m-2}} - \cdots - \widetilde{1}$. Together with the consideration of $\widetilde{2^{n-m-1}} = 2^{2^{n-m-1}} - \widetilde{2^{n-m-2}} - \widetilde{2^{n-m-3}} - \cdots - \widetilde{1}$, we can deduce that the number of 2^{n-m}-period sequence is $\widetilde{2^{n-m}} = 2^{2^{n-m}} - 2^{2^{n-m-1}} := N$. According to $2^{2^{n-m}} - 2^{2^{n-m-1}} \geqslant 2^n$, we have $N \geqslant 2^n$. Hence, there exists an output function such that the Galois NFSR produces 2^n different output sequences that are from N sequences of period 2^{n-m}, which implies that different initial states of the Galois NFSR produce different output sequences. Therefore, the Galois NFSR is observable.

Consider an n-stage Galois NFSR with state transition matrix L in (13). For any $q \in \{1, 2, \ldots, 2^m\}$, let C_q denote the cycle formed by the states $\delta_{2^n}^{q+k\cdot 2^m}$ for all $k = 0, 1, \ldots, 2^{n-m} - 1$. As q is the remainder of $q + k \cdot 2^m$ divided by 2^m, the corresponding n-dimensional vectors of the states on 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 $[X_1 \;\; X_2 \;\; \cdots \;\; X_{n-m} \;\; q_{n-m+1} \;\; q_{n-m+2} \;\; \cdots \;\; q_n]^{\mathrm{T}}$, where

$$q = 2^m - (2^{m-1} q_{n-m+1} + 2^{m-2} q_{n-m+2} + \cdots + q_n). \tag{19}$$

Take cycle C_1 as an example. The corresponding n-dimensional vectors of the states on the C_1 are of form $[X_1 \;\; X_2 \;\; \cdots \;\; X_{n-m} \;\; \underbrace{1 \; 1 \; \cdots \; 1}_{m}\,]^{\mathrm{T}}$.

An n-variable Boolean function h can be expressed as

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

where

$$h_q = \bigoplus_{(q_1,q_2,\ldots,q_{n-m})\in\mathbb{F}_2^{n-m}} h(q_1, q_2, \ldots, q_n) X_1^{q_1} X_2^{q_2} \cdots X_{n-m}^{q_{n-m}}, \ q = 1, 2, \ldots, 2^m, \tag{20}$$

with q satisfying (19). 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

$$
\begin{aligned}
h = h_1 X_{n-m+1}^1 \cdots X_{n-1}^1 X_n^1 \oplus h_2 X_{n-m+1}^1 \cdots X_{n-1}^1 X_n^0 \oplus \cdots \oplus h_q X_{n-m+1}^{q_{n-m+1}} \cdots X_{n-1}^{q_{n-1}} X_n^{q_n}\\
\oplus \cdots \oplus h_{2^m} X_{n-m+1}^0 \cdots X_{n-1}^0 X_n^0.
\end{aligned}
\tag{21}
$$

Assume that h in (21) is an output function of the Galois NFSR with state transition matrix L in (13). Thus, if the output function h is limited to the states on the cycle C_q, then it becomes

$$
\begin{aligned}
h(X_1, X_2, \ldots, X_n) &= h_1 \odot 0 \oplus \cdots \oplus h_{q-1} \odot 0 \oplus h_q(X_1, X_2, \ldots, X_{n-m}) \odot 1 \oplus h_{q+1} \odot 0 \oplus \cdots \oplus h_{2^m} \odot 0\\
&= h_q(X_1, X_2, \ldots, X_{n-m}).
\end{aligned}
$$

Proposition 3. For an n-stage Galois NFSR with state transition matrix L in (13) and output function h in (21), each h_q in the function h is dependent on the variable X_1 for each $q \in \{1, 2, \ldots, 2^m\}$, if and only if any two distinct initial states on each cycle of the Galois NFSR are distinguishable.

Proof. Sufficiency. If any two distinct initial states on each cycle of the Galois NFSR are distinguishable, then for each $q \in \{1, 2, \ldots, 2^m\}$, the output of state $\boldsymbol{X}(t) \in \mathbb{F}_2^n$ at time t on the 2^{n-m}-length cycle C_q of the Galois NFSR is different from that of the state $\boldsymbol{X}(t+2^{n-m-1})$ at time $t+2^{n-m-1}$ for some $t \in \mathbb{N}$. That is, $h(\boldsymbol{X}(t)) \neq h(\boldsymbol{X}(t+2^{n-m-1}))$ for each $q \in \{1, 2, \ldots, 2^m\}$ and for some $t \in \mathbb{N}$. 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 in the same output sequence. Thus, the two states on the cycle C_{q_0} are indistinguishable, which is contrary to the assumption.

According to a state sequence in (14) of the Galois NFSR, the initial state $x(t) = \delta_{2^n}^q \in \Delta_{2^n}$ at time t is updated to state $x(t+2^{n-m-1}) = \delta_{2^n}^{q+2^{n-m-1}\times 2^m} = \delta_{2^n}^{q+2^{n-1}}$ at time $t+2^{n-m-1}$ for any $t \in \mathbb{N}$. Their corresponding n-dimensional vectors $\boldsymbol{X}(t)$ and $\boldsymbol{X}(t+2^{n-m-1})$ have the same other state bits except for the first state bit. Hence, h_q is dependent on the variable X_1 for any $q \in \{1, 2, \ldots, 2^m\}$. Otherwise, $h(\boldsymbol{X}(t)) = h(\boldsymbol{X}(t+2^{n-m-1}))$ for some $q_0 \in \{1, 2, \ldots, 2^m\}$, contrary to what we have proven above.

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

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

As h_q is dependent on the variable X_1, we have $h_{q_1} \not\equiv 0$. Thus, there must exist some state $\boldsymbol{X}_0 \in \mathbb{F}_2^{n-m-1}$ such that $h_{q_1}(\boldsymbol{X}_0) = 1$. Then, there exists some initial state $\boldsymbol{X}(t) = [1 \ \ \boldsymbol{X}_0 \ \ q_{n-m+1} \ \ q_{n-m+2} \ \cdots \ q_n]^{\mathrm{T}}$, whose output is different from that of the initial state $\boldsymbol{X}(t+2^{n-m-1}) = [0 \ \ \boldsymbol{X}_0 \ \ q_{n-m+1} \ \ q_{n-m+2} \ \cdots \ q_n]^{\mathrm{T}}$; that is, $h(\boldsymbol{X}(t)) \neq h(\boldsymbol{X}(t+2^{n-m-1}))$. Note that the cycle C_q of the Galois NFSR is of length 2^{n-m}. Then, according to Lemma 9, the output sequence resulting from the initial state $\boldsymbol{X}(t)$ is of period 2^{n-m}. Thus, we derive from Corollary 2 that any two distinct initial states of the cycle C_q of the Galois NFSR are distinguishable. Because of the arbitrariness of q, the result follows.

For simplicity, we introduce some notations to be used in the sequel. It is helpful to keep them in mind.

First, we define two sets: a set of the first $n-m$ bits of states on the cycle C_q such that the output function h takes the value of 1, given by

$$A_{\boldsymbol{q}_{n-m}} = \{\boldsymbol{q}_{n-m} = [q_1 \ \cdots \ q_{n-m}]^{\mathrm{T}} | \boldsymbol{q} = [q_1 \ \cdots \ q_{n-m} \ \ q_{n-m+1} \ \cdots \ q_n]^{\mathrm{T}} \text{ on the cycle } C_q \text{ and } h(\boldsymbol{q}) = 1\}, \tag{22}$$

and a set of nonnegative integers determined by the vectors from $A_{\boldsymbol{q}_{n-m}}$ as

$$\hat{A}_{\boldsymbol{q}_{n-m}} = \{\hat{q} | \hat{q} = 2^{n-m} - 1 - (2^{n-m-1}q_1 + 2^{n-m-2}q_2 + \cdots + q_{n-m}), \ [q_1 \ \ q_2 \ \cdots \ q_{n-m}]^{\mathrm{T}} = \boldsymbol{q}_{n-m} \in A_{\boldsymbol{q}_{n-m}}\}. \tag{23}$$

Next, we define a tuple

$$\hat{\boldsymbol{q}} = (\hat{q}_1, \hat{q}_2, \ldots, \hat{q}_N), \tag{24}$$

where $\hat{q}_1, \hat{q}_2, \ldots, \hat{q}_N \in \hat{A}_{\boldsymbol{q}_{n-m}}$ satisfy $0 \leqslant \hat{q}_1 < \hat{q}_2 < \cdots < \hat{q}_N \leqslant 2^{n-m} - 1$ with $N = |\hat{A}_{\boldsymbol{q}_{n-m}}|$.

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

$$\operatorname{dist}(\hat{q}) = \left((\hat{q}_1 - \hat{q}_N) \bmod 2^{n-m}, \hat{q}_2 - \hat{q}_1, \hat{q}_3 - \hat{q}_2, \ldots, \hat{q}_N - \hat{q}_{N-1}\right). \tag{25}$$

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

Lemma 12. Each component of $\operatorname{dist}(\hat{q})$ in (25) is equal to the path length of two states whose outputs are 1 on the cycle C_q.

Proof. The states of the cycle C_q are of form $\delta_{2^n}^{k\cdot 2^m + q}$ in Δ_{2^n}, where $k \in \{0, 1, \ldots, 2^{n-m} - 1\}$. Their corresponding n-dimensional vector is $[X_1 \ X_2 \ \cdots \ X_{n-m} \ q_{n-m+1} \ \cdots \ q_n]^{\mathrm{T}}$, where $q = 2^m - (2^{m-1}q_{n-m+1} + 2^{m-2}q_{n-m+2} + \cdots + q_n)$. According to Lemma 5, we have

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

yielding $k = 2^{n-m} - 1 - (2^{n-m-1}X_1 - 2^{n-m-2}X_2 + \cdots + X_{n-m}) \in \hat{A}_{\boldsymbol{q}_{n-m}}$ defined in (23). From the proof of Theorem 6, cycle C_q has a 2^{n-m}-period state sequence: $\delta_{2^n}^{q}, \delta_{2^n}^{2^m+q}, \ldots, \delta_{2^n}^{k\cdot 2^m+q}, \ldots, \delta_{2^n}^{(2^{n-m}-1)\cdot 2^m+q}$. Clearly, the path length of any two states $\delta_{2^n}^{k\cdot 2^m+q}$ and $\delta_{2^n}^{l\cdot 2^m+q}$ with positive integers k and l satisfying $k < l$, is $l - k$. Then the result follows from the definition of $\operatorname{dist}(\hat{\boldsymbol{q}})$ given in (25).

Recall that, for an n-period sequence $S = s_1 s_2 \cdots s_n$, the n-period sequence $S_i = s_i s_{i+1} \cdots s_n s_1 \cdots s_{i-1}$ with $i \in \{2, 3, \ldots, n\}$ is said to be shift equivalent to S [44].

Similarly, we define a shift equivalence for a tuple.

Definition 4. For an n-tuple $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$, the n-tuple $\boldsymbol{a}' = (a_i, a_{i+1}, \ldots, a_n, a_1, \ a_2, \ldots, a_{i-1})$ with $i \in \{2, 3, \ldots, n\}$ is said to be shift equivalent to $\boldsymbol{a}$.

Proposition 4. For an n-stage Galois NFSR with state transition matrix L in (13), there exist indistinguishable initial states on different cycles C_p and C_q, if and only if $\operatorname{dist}(\hat{p})$ is shift equivalent to $\operatorname{dist}(\hat{q})$ in (25).

Proof. Let $\operatorname{dist}(\nu) = (d_1^\nu, d_2^\nu, \ldots, d_N^\nu)$ with $\nu = \hat{\boldsymbol{p}}, \hat{\boldsymbol{q}}$. Then, from the proof of Lemma 12 and the definitions of $A_{\boldsymbol{q}_{n-m}}$ in (22) and $\hat{q}$ in (24), we know that for each $k \in \{1, 2, \ldots, N\}$, each d_k^ν uniquely corresponds to a $(d_k^\nu - 1)$-length zero run. Thus, $\operatorname{dist}(\nu)$ uniquely corresponds to all-zero runs of an output sequence S^ν generated by the cycle C_ν and thereby, uniquely corresponds to the output sequence S^ν. Hence, $\operatorname{dist}(\hat{\boldsymbol{p}})$ is shift equivalent to $\operatorname{dist}(\hat{\boldsymbol{q}})$ if and only if the output sequence $S^{\hat{\boldsymbol{q}}}$ is shift equivalent to the output sequence $S^{\hat{\boldsymbol{p}}}$. This is equivalent to saying that there exist two indistinguishable initial states separately from different cycles C_p and C_q.

Theorem 8. If an n-stage Galois NFSR with state transition matrix L in (13) is observable, then its output function h is dependent on the variables X_k for all $k = n-m+1, n-m+2, \ldots, n$.

Proof. We use the previous notations and prove the result by contradiction. If the output function h is independent of some variable X_k with some $k \in \{n-m+1, n-m+2, \ldots, n\}$, then according to (21), there exists $h_q = h_{q+2^{n-k}}$ with some $q \in \{1, 2, \ldots, 2^{m-1}\}$. Note that $h = h_q$ if h is limited to the cycle C_q. Then, according to (20) and (22)–(25), we can deduce $\operatorname{dist}(\hat{\boldsymbol{q}}) = \operatorname{dist}(\widehat{\boldsymbol{q} + 2^{n-k}})$ for some $q \in \{1, 2, \ldots, 2^{m-1}\}$. From Proposition 4, there exist two indistinguishable initial states on different cycles C_q and $C_{q+2^{n-k}}$ with some $q \in \{1, 2, \ldots, 2^{m-1}\}$, which is contrary to the assumption that the Galois NFSR is observable. Therefore, the result holds.

Theorem 9. An n-stage Galois NFSR with state transition matrix L in (13), is observable, if and only if the following two conditions are satisfied:

(1) the function h_q in (20) contains the variable X_1 for any $q \in \{1, 2, \ldots, 2^m\}$;

(2) $\mathrm{dist}(\hat{\boldsymbol{p}})$ is not shift equivalent to $\mathrm{dist}(\hat{\boldsymbol{q}})$ in (25) for any $p, q \in \{1, 2, \ldots, 2^m\}$, where $p \neq q$.

Proof. According to Proposition 3, Condition (1) holds if and only if any two distinct initial states on each cycle are distinguishable. From Proposition 4, Condition (2) holds if and only if any two distinct initial states on different cycles are distinguishable. Therefore, the result follows.

Example 4. Consider a 4-stage Galois NFSR with state transition matrix $L = \delta_{16}[3, 4, \ldots, 16, 1, 2]$. Clearly, its state diagram consists of two 8-length cycles, whose successive states are $\delta_{16}^1, \delta_{16}^3, \delta_{16}^5, \ldots, \delta_{16}^{15}, \delta_{16}^1$ and $\delta_{16}^2, \delta_{16}^4, \delta_{16}^6, \ldots, \delta_{16}^{16}, \delta_{16}^2$. We use the previous notations. Take $h_1 = X_1 \oplus X_1X_2 \oplus X_2X_3$ and $h_2 = X_1$. Then the output function of the Galois NFSR is $h = h_1X_4 \oplus h_2X_4^0 = X_1 \oplus X_1X_2X_4 \oplus X_2X_3X_4$. The output sequences resulting from the initial state δ_{16}^1 and δ_{16}^2 are easily computed as two 8-period sequences: 10111000 and 11110000, respectively. These imply that the Galois NFSR is observable. On the other hand, we can directly compute that $\mathrm{dist}(\hat{\boldsymbol{p}}) = (4, 2, 1, 1)$ and $\mathrm{dist}(\hat{\boldsymbol{q}}) = (5, 1, 1, 1)$. Along with the forms of h_1 and h_2, we can see that both conditions in Theorem 9 are satisfied. Therefore, the Galois NFSR is observable, consistent with the foregoing fact.

In particular, if $|A_{\boldsymbol{p}_{n-m}}| \neq |A_{\boldsymbol{q}_{n-m}}|$, then Condition (2) of Theorem 9 clearly holds, see the result below.

Theorem 10. For an n-stage Galois NFSR with feedback functions satisfying (16), if its output function is

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

where $b_i \in \mathbb{F}_2$ for each $i \in \{0, 1, 2, \ldots, n\}$, $g_1 \not\equiv 0$, 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 NFSR consists of two cycles of length 2^{n-1}:

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

Note that $X_n^{b_n} \oplus X_n^{b_n^0} = 1$. Then, we can rewrite the output function h as

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

Let $h_p(X_1, X_2, \ldots, X_{n-1}) = X_1^{b_0} g_1 \oplus g_2 \oplus X_1^{b_1} X_2^{b_2} \cdots X_{n-1}^{b_{n-1}}$ and $h_q(X_1, X_2, \ldots, X_{n-1}) = X_1^{b_0} g_1 \oplus g_2$. 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, and so is h_q. Thus, h_p and h_q satisfy Condition (1) in Theorem 9. Clearly, $h_p \oplus h_q = X_1^{b_1} X_2^{b_2} \cdots X_{n-1}^{b_{n-1}}$, which is equal to 1 if and only if $X_i = b_i$, $i = 1, 2, \ldots, n-1$. So, $|A_{\boldsymbol{p}_{n-1}}| - |A_{\boldsymbol{q}_{n-1}}| = 1$ or -1, where the sets $A_{\boldsymbol{p}_{n-1}}$ and $A_{\boldsymbol{q}_{n-1}}$ are defined similarly to (22). Hence, $\mathrm{dist}(\hat{\boldsymbol{p}})$ is not shift equivalent to $\mathrm{dist}(\hat{\boldsymbol{q}})$ in (25), satisfying Condition (2) in Theorem 9. Therefore, from Theorem 9, the Galois NFSR is observable.

5 Conclusion

This 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 NFSR in the first class has the maximum state cycle with simple feedback functions. Moreover, an easily verifiable necessary and sufficient condition was given to determine whether a Galois NFSR in the first class with output function is observable, which guarantees its output sequences to achieve the maximum period. Each Galois NFSR in the second class has equal-length state cycles with simple feedback functions as well. Some easily verifiable necessary/sufficient conditions were given for the observability of a Galois NFSR in the second class with output function. In future work, it is interesting to use these Galois NFSRs in both classes or their isomorphic Galois NFSRs with output functions to design new stream ciphers by accounting for their security and implementation efficiency. In addition, the cycle structure of a general NFSR is known to be an open hard problem. We conjecture that the problem of computing the period of a general NFSR is NP-hard. Proving this conjecture is an interesting avenue for future research.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 62172408, 62472417, 62372449).

References

1 Hell M, Johansson T, Maximov A, et al. The grain family of stream ciphers. In: New Stream Cipher Designs: The eSTREAM Finalists. Berlin: Springer-Verlag, 2008. 4986: 179–190
2 Cannière C D, Preneel B. Trivium. In: New Stream Cipher Designs: The eSTREAM Finalists. Berlin: Springer-Verlag, 2008. 4986: 244–266
3 Wu H. ACORN: a lightweight authenticated cipher (v3). 2016. http://competitions.cr.yp.to/round3/acornv3.pdf
4 Kauffman S A. Metabolic stability and epigenesis in randomly constructed genetic nets. J Theor Biol, 1969, 22: 437–467
5 Cheng D, Qi H, Zhao Y. An Introduction to Semi-Tensor Product of Matrices and Its Applications. Singapore: World Scientific Publishing Company, 2012
6 Fornasini E, Valcher M E. Observability, reconstructibility and state observers of Boolean control networks. IEEE Trans Automat Contr, 2013, 58: 1390–1401
7 Liu Y, Zhong J, Ho D W C, et al. Minimal observability of Boolean networks. Sci China Inf Sci, 2022, 65: 152203
8 Laschov D, Margaliot M, Even G. Observability of Boolean networks: a graph-theoretic approach. Automatica, 2013, 49: 2351–2362
9 Guo Y, Gui W, Yang C. Redefined observability matrix for Boolean networks and distinguishable partitions of state space. Automatica, 2018, 91: 316–319
10 Yu Y, Meng M, Feng J, et al. Observability criteria for Boolean networks. IEEE Trans Automat Contr, 2022, 67: 6248–6254
11 Lu J Q, Li M L, Liu Y, et al. Nonsingularity of Grain-like cascade FSRs via semi-tensor product. Sci China Inf Sci, 2018, 61: 010204
12 Liu Z, Wang Y, Cheng D. Nonsingularity of feedback shift registers. Automatica, 2015, 55: 247–253
13 Zhong J H, Lin D D. Stability of nonlinear feedback shift registers. Sci China Inf Sci, 2016, 59: 012204
14 Zhao D W, Peng H P, Li L X, et al. Novel way to research nonlinear feedback shift register. Sci China Inf Sci, 2014, 57: 092114
15 Biryukov A. Weak keys. In: Encyclopedia of Cryptography and Security. Boston: Springer, 2005
16 Kalouptsidis N, Limniotis K. Nonlinear span, minimal realizations of sequences over finite fields and de Bruijn generators. In: Proceedings of International Symposium on Information Theory and Its Applications, Chicago, 2004. 794–799
17 Kong W H, Zhong J H, Lin D D. Observability of Galois nonlinear feedback shift registers. Sci China Inf Sci, 2022, 65: 192206
18 Gao Z, Feng J, Yu Y, et al. On observability of Galois nonlinear feedback shift registers over finite fields. Front Inform Technol Electron Eng, 2022, 23: 1533–1545
19 Zhang S, Chen G. New results on the state cycles of Trivium. Des Codes Cryptogr, 2019, 87: 149–162
20 Hu H, Gong G. Periods on two kinds of nonlinear feedback shift registers with time varying feedback functions. Int J Found Comput Sci, 2011, 22: 1317–1329
21 Chang Z, Gong G, Wang Q. Cycle structures of a class of cascaded FSRs. IEEE Trans Inform Theor, 2019, 66: 3766–3774
22 Dubrova E. Finding matching initial states for equivalent NLFSRs in the Fibonacci and the Galois configurations. IEEE Trans Inform Theor, 2010, 56: 2961–2966
23 Dong J, Pei D. Construction for de Bruijn sequences with large stage. Des Codes Cryptogr, 2017, 85: 343–358
24 Mandal K, Yang B, Gong G, et al. Analysis and efficient implementations of a class of composited de Bruijn sequences. IEEE Trans Comput, 2020, 69: 1835–1848
25 Li M, Lin D. Partial cycle structure of FSRs and its applications in searching de Bruijn sequences. IEEE Trans Inform Theor, 2023, 69: 598–609
26 Dubrova E. A list of maximum-period NFSRs. Cyptology ePrint Archive, 2012. http://eprint.iacr.org/2012/166
27 Gammel B, Göttfert R, Kniffer O. Achterbahn-128/80, eSTREAM: the ECRYPT Stream Cipher Project. 2006. http://www.ecrypt.eu.org/stream/p2ciphers/achterbahn/achterbahn_p2.pdf
28 Yang Y, Zeng X, Xu Y. Periods on the cascade connection of an LFSR and an NFSR. Chin J Electron, 2019, 28: 301–308
29 Dubrova E. A transformation from the Fibonacci to the Galois NLFSRs. IEEE Trans Inform Theor, 2009, 55: 5263–5271
30 Klimov A, Shamir A. Cryptographic application of T-functions. In: Proceeding of International Workshop on Selected Areas in Cryptography (SAC), Ottawa, 2004. 3006: 248–261
31 Hong J, Lee D, Yeom Y, et al. A new class of single cycle T-functions. In: Proceedings of International Workshop on Fast Software Encryption (FSE), Paris, 2005. 3557: 68–82
32 Roy D, Chaturvedi A, Mukhopadhyay S. New constructions of T-function. In: Proceedings of Information Security Practice and Experience (ISPEC), Beijing, 2015. 9065: 395–405
33 Klimov A, Shamir A. A new class of invertible mappings. In: Proceedings of Cryptographic Hardware and Embedded Systems(CHES), Redwood Shores, 2002. 2523: 470–483
34 Anashin V, Bogdanov A, Kizhvtov I, et al. ABC: a new fast flexible stream cipher. ECRYPT Stream Cipher Project Report 2005/001, 2005. http://www.ecrypt.eu.org/stream
35 Zhang W, Wu C. The algebraic normal form, linear complexity and k-error linear complexity of single-cycle T-function. In: Proceedings of Sequences and Their Applications (SETA), Beijing, 2006. 4086: 391–401
36 Mitra J, Sarkar P. Time-memory trade-off attacks on multiplication and T-functions. In: Proceedings of Advances in Cryptology-ASIACRYPT, Jeju Island, 2004. 3329: 468–482
37 Kolokotronis N. Cryptographic properties of stream ciphers based on T-functions. In: Proceedings of IEEE International Symposium on Information Theory (ISIT), Seattle, 2006. 1604–1608
38 Anashin V S, Khrennikov Y A. Applied Algebraic Dynamics. Berlin: Walter de Gruyter, 2009
39 Wu C-K, Feng D. Boolean Functions and Their Applications in Cryptography. Heidelberg: Springer-Berlin, 2016
40 Cheng D, Qi H, Li Z. Analysis and Control of Boolean Networks. London: Springer-Verlag, 2011
41 Roger H A, Johnson R C. Topics in Matrix Analysis. Cambridge: Cambridge University Press, 1991
42 Kong W, Zhong J, Lin D. Isomorphism and equivalence of Galois nonlinear feedback shift registers. In: Proceedings of International Conference on Information Security and Cryptology (Inscrypt), Shandong, 2021. 13007: 301–315
43 Zhong J H, Lin D D. Decomposition of nonlinear feedback shift registers based on Boolean networks. Sci China Inf Sci, 2019, 62: 039110
44 Golomb S W. Shift Register Sequences. Laguna Hills: Holden-Day, 1967