SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

September 2022, Vol. 65 192206:1–192206:16
https://doi.org/10.1007/s11432-021-3346-6

Observability of Galois nonlinear feedback shift registers

Wenhui KONG[1,2], Jianghua ZHONG[1*] & Dongdai LIN[1]

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

Received 11 April 2021/Revised 26 June 2021/Accepted 1 September 2021/Published online 29 August 2022

Abstract Nonlinear feedback shift registers (NFSRs) have been used in many recent stream ciphers. They are generally classified into Fibonacci NFSRs and Galois NFSRs according to their implementation configurations. An NFSR is observable if any two distinct initial states can be distinguished from their corresponding output sequences. From the security perspective, NFSR-based stream ciphers should select observable NFSRs; otherwise, they will be subject to weak key attacks. Any Fibonacci NFSR is observable as the first n bits of its output sequence is just its initial state, where n is the stage number of the Fibonacci NFSR. This paper considers the observability of Galois NFSRs. Some necessary and/or sufficient conditions are presented, using the semi-tensor product-based Boolean network theory. In particular, a new observability matrix is proposed to facilitate the observability determination.

Keywords shift register, stream cipher, observability, Boolean network, semi-tensor product

Citation Kong W H, Zhong J H, Lin D D. Observability of Galois nonlinear feedback shift registers. Sci China Inf Sci, 2022, 65(9): 192206, https://doi.org/10.1007/s11432-021-3346-6

1 Introduction

Nonlinear feedback shift registers (NFSRs), which have taken the place of linear feedback shift registers (LFSRs), have become popular in the design of stream ciphers. Recently, NFSRs 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 and one of the finalists Acorn [4] in the CAESAR competition. In contrast to the well-developed theory of LFSRs, the theory of NFSRs is far from being well-understood due to its complexity and lack of efficient mathematical tools. The large gap between the NFSR theory and practical demand urges to find new tools to develop the cryptographic properties of NFSRs.

NFSRs are generally classified into Fibonacci NFSRs and Galois NFSRs based on their implementation configurations. A Fibonacci NFSR applies its feedback only to the last bit, whereas a Galois NFSR applies its feedback availability to every bit [5]. Compared with Fibonacci NFSRs, Galois NFSRs may decrease the propagation time and increase the throughput [5]. Many stream ciphers like the foregoing ones use Galois NFSRs as their main building blocks. However, previous studies focused mainly on Fibonacci NFSRs, whereas much less concern has been shown to Galois NFSRs.

Furthermore, NFSRs are the most used sequence generators. In 2004, the cryptographers Kalouptsidis and Limniotis [6] 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. The observability of a sequence generator therein means that two distinct initial states can be distinguished from their corresponding output sequences. In other words, an output sequence of the generator can uniquely determine its initial state. However, since then, no cryptographers have addressed the observability of sequence generators. According to the definition of observability of sequence generators, it is easy to see that NFSR-based

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

stream ciphers should avoid unobservable Galois NFSRs from the security viewpoint and select observable ones; otherwise, they are vulnerable to weak key attacks [7].

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 introduced in 1969 by Kauffman [8] to model a genetic network. Since then, it has been developed in many communities, ranging from biology and physics to systems and control. In the community of systems and control, Cheng and his collaborators [9] developed an algebraic framework for Boolean networks, using a powerful mathematical tool called the semi-tensor product of matrices. This algebraic framework facilitates solving fundamental problems in control theory, such as controllability, observability, and stabilization [10]. Here, it is worthy to point out that the notion of the observability of Boolean networks is the same as that of sequence generators. Interestingly, till now, much work has been done on the observability of Boolean networks [11–17]. Nevertheless, there is still extensive recent work on other aspects, such as stability and stabilization [18–20], pinning control [21–23], and optimal control [24, 25].

Some studies [26–31] regarded an NFSR as a Boolean network and applied the semi-tensor product-based Boolean network theory to investigate NFSRs. Specifically, Ref. [31] defined an observability matrix for a Fibonacci NFSR's cycle, which orderly accumulates output sequences resulting from initial states that are the cycle's consecutive states. This construction approach of the observability matrix for a Fibonacci NFSR's cycle is the same as that of the state transition matrix under the canonical form for a Boolean network, where the consecutive states on the same branch (also called transient) and its connected cycle (i.e., attractor) are accumulated into a block [32]. The construction method of both matrices motivated us to propose a new observability matrix for a Galois NFSR.

In this paper, we also view an NFSR as a Boolean network and use the observability matrix to analyze its observability. First, we give some necessary and/or sufficient conditions for the observability, using the observability matrix introduced in the community of systems and control. Then, we propose a new observability matrix for a Galois NFSR, which accumulates output sequences resulting from initial states on the same branch and its connected cycle into a block. Finally, based on the new observability matrix, we again give some new necessary and/or sufficient conditions for the observability of Galois NFSRs.

The rest of this paper is organized as follows. Section 2 gives some preliminaries in Boolean networks and NFSRs. Sections 3 and 4 present some necessary and/or sufficient conditions for the observability of Galois NFSRs, using the original observability matrix and a proposed new one, respectively. Section 5 is the conclusion.

2 Preliminaries

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

Notations. $\mathbb{F}_2$ denotes the binary Galois field and $\mathbb{F}_2^n$ represents an n-dimensional vector space over $\mathbb{F}_2$. $\mathbb{N}$ is the set of nonnegative integers. δ_n^i stands for the i-th column of the $n \times n$ identity matrix I_n. The set of all columns of I_n is denoted by Δ_n. Let $\mathcal{L}_{n\times m}$ be the set of all $n \times m$ matrices whose columns belong to the set Δ_n. A matrix $A = [\delta_n^{i_1}\ \delta_n^{i_2}\ \cdots\ \delta_n^{i_m}] \in \mathcal{L}_{n\times m}$ is simply denoted by $A = \delta_n[i_1\ i_2\ \cdots\ i_m]$. $\mathrm{Col}_j(A)$ (resp. $\mathrm{Row}_j(A)$) represents the j-th column (resp. row) of a matrix A.

In addition, some commonly used notations are illustrated for clarity. The operators $+, -$ and $\times$, respectively, denote the ordinary addition, subtraction and multiplication in the real field. The operations $\oplus$ and $\odot$, respectively, represent the addition and multiplication modulo 2 over $\mathbb{F}_2$. Precisely, $1 \oplus 1 = 0, 1 \oplus 0 = 1, 0 \oplus 1 = 1, 0 \oplus 0 = 0$ for the addition $\oplus$; and $1 \odot 1 = 1, 1 \odot 0 = 0, 0 \odot 1 = 0, 0 \odot 0 = 0$ for the multiplication $\odot$. For an $n \times n$ matrix $B = (b_{ij})$, $\det(B)$ denotes its determinant, and $\mathrm{tr}(B)$ represents its trace, and if B is a nonsingular matrix, then $\mathrm{ord}(B)$ stands for its order, that is, the least power p of B such that $B^p = I_n$.

2.1 Boolean network

Definition 1 ([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 2 ([9]). 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

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

Notably, the semi-tensor product works for any two matrices. Moreover, if $m = p$ in Definition 2, then the semi-tensor product of matrices degenerates to the conventional matrix product, whereas it preserves all fundamental properties of the conventional matrix product.

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

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

is called the structure matrix of f [10,34]. The function $\boldsymbol{f} = [f_1 \ \ f_2 \ \ \ldots \ \ f_n]^{\mathrm{T}}$ is called a vectorial function if all f_is are Boolean functions.

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

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

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, 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.

Lemma 1 ([10]). For any vector $\boldsymbol{Z} = [Z_1 \ \ Z_2 \ \cdots \ Z_r]^{\mathrm{T}} \in \mathbb{F}_2^r$, let $\boldsymbol{z} = [Z_1 \ \ Z_1 \oplus 1]^{\mathrm{T}} \ltimes [Z_2 \ \ Z_2 \oplus 1]^{\mathrm{T}} \ltimes \cdots \ltimes [Z_r \ \ Z_r \oplus 1]^{\mathrm{T}}$. Then the vector $\boldsymbol{z} = \delta_{2^n}^j \in \Delta_{2^r}$ with $j = 2^r - (2^{r-1}Z_1 + 2^{r-2}Z_2 + \cdots + Z_r)$.

From Lemma 1, we can easily observe that the vector $\boldsymbol{Z} = [Z_1 \ \ Z_2 \ \cdots \ Z_r]^{\mathrm{T}} \in \mathbb{F}_2^r$ and the vector $\boldsymbol{z} = \delta_{2^r}^j \in \Delta_{2^r}$ with $j = 2^r - (2^{r-1}Z_1 + 2^{r-2}Z_2 + \cdots + Z_r)$ are one-to-one correspondence.

Boolean network (3) can be equivalently expressed as the linear system [10]:

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

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

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

with G_i being the structure matrix of the i-th component g_i of the vectorial function $\boldsymbol{g}$ in (3) for any $i \in \{1, 2, \ldots, n\}$. The j-th column of H can be computed in a way similar to (5) for the j-th column of L.

Lemma 2 ([9,10]). Let $L \in \mathcal{L}_{2^n \times 2^n}$ be the state transition matrix of Boolean network (4). Then the number N_k of cycles of length k of the Boolean network is

$$\begin{cases} N_1 = \mathrm{tr}(L), \\ N_k = \dfrac{1}{k}\left[\mathrm{tr}(L^k) - \displaystyle\sum_{q|k, 0<q<k} qN_q\right], \quad 2 \leqslant k \leqslant 2^n. \end{cases} \tag{6}$$

Notably, two sequences $(a_i)_{i \geqslant 1}$ and $(b_i)_{i \geqslant 1}$ are equal if and only if $a_i = b_i$ for any positive integer $i \geqslant 1$.

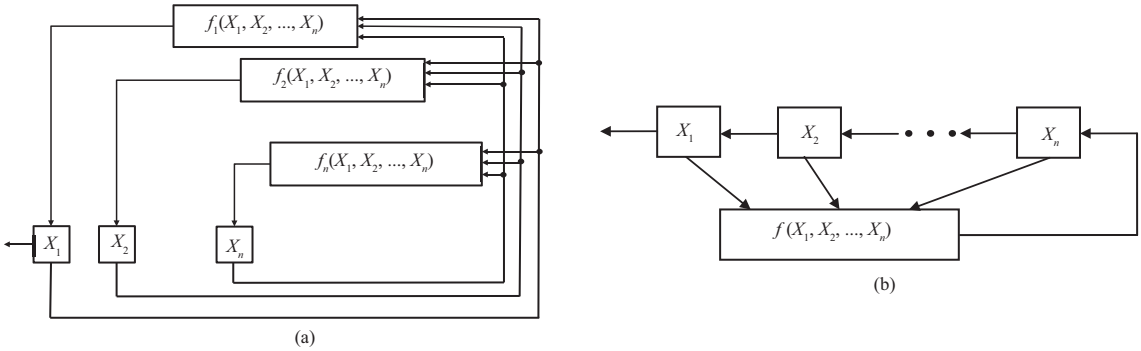

Figure 1 Galois and Fibonacci NFSRs. (a) An n-stage Galois NFSR; (b) an n-stage Fibonacci NFSR.

Definition 3 ([12])**.** Two distinct initial states of a Boolean network are said to be indistinguishable, if their corresponding 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 4 ([12])**.** The observability matrix of Boolean network (4) in N steps is defined as

$$\mathcal{O}_N = [H^{\mathrm{T}} \ \ (HL)^{\mathrm{T}} \ \cdots \ (HL^{N-1})^{\mathrm{T}}]^{\mathrm{T}}. \tag{7}$$

Lemma 3 ([12])**.** Boolean network (4) is observable if and only if the observability matrix $\mathcal{O}_{2^n-1}$ has 2^n distinct columns.

Recall that a sequence $(s_i)_{i\geqslant 1}$ is of period k if k is the least positive integer such that $s_{i+k} = s_i$ for all positive integer i. Moreover, any state of a Boolean network will finally reach a cycle and stay on this cycle forever.

Lemma 4 ([12])**.** Boolean network (4) is observable if and only if

(1) (states distinguishable before their merging) for any two distinct states $\boldsymbol{x}_1$ and $\boldsymbol{x}_2$, condition $L\boldsymbol{x}_1 = L\boldsymbol{x}_2$ implies $H\boldsymbol{x}_1 \neq H\boldsymbol{x}_2$;

(2) (states distinguishable for those on the same or different cycles) for any two distinct state sequences $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_k$ and $\bar{\boldsymbol{x}}_1, \bar{\boldsymbol{x}}_2, \ldots, \bar{\boldsymbol{x}}_k$ of period k, their corresponding output sequences $H\boldsymbol{x}_1, H\boldsymbol{x}_2, \ldots, H\boldsymbol{x}_k$ and $H\bar{\boldsymbol{x}}_1, H\bar{\boldsymbol{x}}_2, \ldots, H\bar{\boldsymbol{x}}_k$ are distinct and are of period k.

2.2 Nonlinear feedback shift register

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

$$\begin{cases} X_1(t+1) = f_1(X_1(t), X_2(t), \ldots, X_n(t)), \\ X_2(t+1) = f_2(X_1(t), X_2(t), \ldots, X_n(t)), \\ \quad \vdots \\ X_n(t+1) = f_n(X_1(t), X_2(t), \ldots, X_n(t)), \end{cases} \tag{8}$$

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

If a Galois NFSR's feedback $\boldsymbol{f} = [f_1 \ \ f_2 \ \cdots \ f_n]^{\mathrm{T}}$ satisfies $f_i(X_1, X_2, \ldots, X_n) = X_{i+1}$ for all $i = 1, 2, \ldots, n-1$, then the n-stage Galois NFSR becomes an n-stage Fibonacci NFSR. Figure 1(b) describes an n-stage Fibonacci NFSR, which is nonsingular if and only if its feedback function f is nonsingular, that is, $f = X_1 \oplus \overline{f}(X_2, X_3, \ldots, X_n)$, where $\overline{f}$ is an $(n-1)$-variable Boolean function [35].

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

$\boldsymbol{Y}$. In this case, $\boldsymbol{X}$ is called a predecessor of $\boldsymbol{Y}$, and $\boldsymbol{Y}$ is called the successor of $\boldsymbol{X}$. A state has or has no predecessors. A state without predecessors is called a starting state. Distinct consecutive states $\boldsymbol{X}_1, \boldsymbol{X}_2, \ldots, \boldsymbol{X}_p$ and their edges between them form a cycle of length p if $\boldsymbol{X}_1$ is the successor of $\boldsymbol{X}_p$. Similarly, distinct consecutive states $\boldsymbol{X}_1, \boldsymbol{X}_2, \ldots, \boldsymbol{X}_p$ and their edges between them form a branch (or transient) of length p, if three conditions below are satisfied: (1) none lies on a cycle; (2) $\boldsymbol{X}_1$ is a starting state; (3) the successor of $\boldsymbol{X}_p$ is on a cycle.

Definition 5 ([35])**.** For an n-period sequence $S = s_1 s_2 s_3 \cdots s_n$, the n-period sequence $S_i = s_i s_{i+1} \cdots s_n s_1 s_2 \cdots s_{i-1}$ with $i \in \{2, 3, \ldots, n\}$ is said to be shift equivalent to S.

Similarly, we define the column-shift equivalence for matrices.

Definition 6. For an $m \times n$ matrix A, the $m \times n$ matrix $B = [\mathrm{Col}_i(A)\ \mathrm{Col}_{i+1}(A)\ \cdots\ \mathrm{Col}_n(A)\ \mathrm{Col}_1(A)\ \cdots\ \mathrm{Col}_{i-1}(A)]$ with $i \in \{2, 3, \ldots, n\}$ is said to be column-shift equivalent to matrix A.

From Definition 5, we can easily obtain the following result.

Lemma 5. An $m \times n$ matrix B is column-shift equivalent to an $m \times n$ matrix A if and only if there exists an $n \times n$ circulant matrix P such that $B = AP$.

3 Determining the observability of Galois NFSRs via the original observability matrix

In this section, we give some necessary and/or sufficient conditions for Galois NFSRs, which are particular Boolean networks that use the contents of their lowest bits as their outputs, via the observability matrix of Boolean networks introduced by Fornasini and Valcher in [12].

Proposition 1. If the state transition matrix $L \in \mathcal{L}_{2^n \times 2^n}$ of an n-stage Galois NFSR satisfies $\mathrm{tr}(L) \geqslant 3$, then the Galois NFSR is not observable.

Proof. Let the state transition matrix $L = (a_{ij})$, where $i, j \in \{1, 2, \ldots, 2^n\}$. If $\mathrm{tr}(L) \geqslant 3$, then we have $a_{11} + a_{22} + \cdots + a_{2^n 2^n} \geqslant 3$. Hence, there exist at least three distinct positive integers p, q, r such that $a_{pp} = a_{qq} = a_{rr} = 1$. According to the pigeonhole principle, we must have two of p, q, r in $\{1, 2, \ldots, 2^{n-1}\}$ or in $\{2^{n-1} + 1, 2^{n-1} + 2, \ldots, 2^n\}$. Without loss of generality, we assume $p, q \in \{1, 2, \ldots, 2^{n-1}\}$ and $r \in \{2^{n-1} + 1, 2^{n-1} + 2, \ldots, 2^n\}$. Note that the content of the lowest bit is always used as the output of a Galois NFSR, which means its output Y over $\mathbb{F}_2$ satisfies $Y(t) = X_1(t), t \in \mathbb{N}$, with X_1 being the first component of its state $\boldsymbol{X}$. Then the output matrix of the n-stage Galois NFSR is

$$H = \delta_2[\underbrace{1\ \ 1\ \cdots\ 1}_{2^{n-1}}\ \ \underbrace{2\ 2\ \cdots\ 2}_{2^{n-1}}]. \tag{9}$$

Thus, we can get $\mathrm{Col}_p(HL) = \mathrm{Col}_p(H), \mathrm{Col}_q(HL) = \mathrm{Col}_q(H)$. For the observability matrix $\mathcal{O}_N = [H^{\mathrm{T}}\ \ (HL)^{\mathrm{T}}\ \cdots\ (HL^{N-1})^{\mathrm{T}}]^{\mathrm{T}}$ of the Galois NFSR, we have $\mathrm{Col}_p(\mathcal{O}_2) = \mathrm{Col}_q(\mathcal{O}_2)$ since $\mathrm{Col}_p(H) = \mathrm{Col}_q(H)$. By the same reasoning, we can get $\mathrm{Col}_p(\mathcal{O}_{2^n-1}) = \mathrm{Col}_q(\mathcal{O}_{2^n-1})$. So, the observability matrix $\mathcal{O}_{2^n-1}$ contains at most $2^n - 1$ distinct columns. According to Lemma 3, we can conclude that the Galois NFSR is not observable.

Corollary 1. If the feedback $\boldsymbol{f} = [f_1\ f_2\ \cdots\ f_n]^{\mathrm{T}}$ of an n-stage Galois NFSR has at least three fixed points, then the Galois NFSR is not observable.

Theorem 1. Let $\boldsymbol{f} = [f_1\ f_2\ \cdots\ f_n]^{\mathrm{T}}$ be the feedback of an n-stage Galois NFSR. If $f_1, f_2, \ldots, f_n$ have no constant term and only f_n has a term x_n, then the Galois NFSR is not observable.

Proof. If $f_1, f_2, \ldots, f_n$ have no constant term, then $\boldsymbol{f}(0, 0, \ldots, 0) = [0\ \ 0\ \cdots\ 0]^{\mathrm{T}}$. Thus, there is a unit cycle containing the state $[0\ \ 0\ \cdots\ 0]^{\mathrm{T}}$ in the state diagram of the Galois NFSR. So, the state transition matrix L of the Galois NFSR satisfies $\mathrm{Col}_{2^n}(L) = \delta_{2^n}^{2^n}$. Moreover, if only f_n has a term x_n, then $\boldsymbol{f}(0, 0, \ldots, 0, 1) = [0\ \ 0\ \cdots\ 0\ \ 1]^{\mathrm{T}}$. It implies that there is another unit cycle containing the state $[0\ \ 0\ \cdots\ 0\ \ 1]^{\mathrm{T}}$. Hence, the state transition matrix L of the Galois NFSR satisfies $\mathrm{Col}_{2^n-1}(L) = \delta_{2^n-1}^{2^n-1}$. Thus, the $(2^n - 1)$-th column and the 2^n-th column of the observability matrix $\mathcal{O}_{2^n-1}$ are the same, and thereby $\mathcal{O}_{2^n-1}$ has not 2^n distinct columns. According to Lemma 3, the Galois NFSR is not observable.

Theorem 2. If the state transition matrix $L \in \mathcal{L}_{2^n\times 2^n}$ of an n-stage Galois NFSR satisfies

$$L = \begin{bmatrix} D_1 & & & \\ & D_2 & & \\ & & \ddots & \\ & & & D_r \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} & & & D_1 \\ & & D_2 & \\ & \iddots & & \\ D_r & & & \end{bmatrix}, \tag{10}$$

where each D_i is a square matrix with $i \in \{1, 2, \ldots, r\}$ and $r > 1$, then the Galois NFSR is not observable.

Proof. If L satisfies (10), then there must exist a $D_i, i \in \{1, 2, \ldots, r\}$ such that the columns of D_i lie at the left-half columns or at the right-half columns of L. Then, for the output matrix H in (9) of the Galois NFSR, D_i keeps some left-half columns or right-half columns of H lying at the left-half columns or the right-half columns of HL^k for any positive integer $k \leqslant 2^n - 1$. So we cannot get 2^n distinct columns for the observability matrix $\mathcal{O}_{2^n-1}$. Thus, according to Lemma 3, this Galois NFSR is not observable.

Reducing the rows of observability matrix. From (9), we know the 2×2^n output matrix H of an n-stage Galois NFSR can be rewritten as

$$H = \begin{bmatrix} 1 & 1 & \cdots & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 1 & 1 & \cdots & 1 \end{bmatrix}. \tag{11}$$

We can easily observe that the second row of the output matrix H in (11) is the complementary of the first row. Hence, for the observability matrix $\mathcal{O}_N$ in (7), the number of distinct columns is equal to that of the matrix formed by the odd rows of $\mathcal{O}_N$. In other words, we can only consider the first row of HL^k for each $k \in \{0, 1, \ldots, N-1\}$ to count the number of distinct columns of $\mathcal{O}_N$ in (7). We define the matrix formed by the odd rows of $\mathcal{O}_N$ as $\mathcal{O}_N^\sharp$.

Lemma 6. For an n-stage Galois NFSR, let $\mathcal{N}_k$ be the number of distinct columns of its observability matrix $\mathcal{O}_k$. Then $\mathcal{N}_k \leqslant 2^k$ for any positive integer $k \leqslant 2^n - 1$.

Proof. Firstly, we can easily observe that $\mathcal{O}_1 = H = \delta_2[1\ \ 1\ \cdots\ 1\ \ 2\ \ 2\ \cdots\ 2]$ has two distinct columns. Since the row reduced observability matrix $\mathcal{O}_2^\sharp$ is a matrix of two rows, $\mathcal{O}_2^\sharp$ has at most four distinct columns, namely, $[1\ 0]^{\mathrm{T}}, [1\ 1]^{\mathrm{T}}, [0\ 1]^{\mathrm{T}}, [0\ 0]^{\mathrm{T}}$. For a general case, there are only 0 and 1 elements in every column, and the row reduced observability matrix $\mathcal{O}_k^\sharp$ has totally k rows. Then, according to the combinations of all components of each column, we can easily obtain that $\mathcal{O}_k^\sharp$ has at most 2^k distinct columns and therefore, the observability matrix $\mathcal{O}_k$ has at most 2^k distinct columns as well.

Corollary 2. If the state transition matrix L of an n-stage Galois NFSR satisfies $\mathrm{ord}(L) < n$, then the Galois NFSR are not observable.

Proof. If $\mathrm{ord}(L) < n$, then the observability matrix $\mathcal{O}_{2^n-1}$ has the same number of distinct columns as the observability matrix $\mathcal{O}_{\mathrm{ord}(L)}$, and according to Lemma 6, $\mathcal{O}_{\mathrm{ord}(L)}$ has at most $2^{\mathrm{ord}(L)}$ distinct columns. Since $\mathrm{ord}(L) < n$, we have $2^{\mathrm{ord}(L)} < 2^n$. Hence, $\mathcal{O}_{2^n-1}$ has less than 2^n distinct columns. Therefore, according to Lemma 3, the Galois NFSR is not observable.

Lemma 7. Let H in (11) be the output matrix of an n-stage Galois NFSR. If its state transition matrix $L \in \mathcal{L}_{2^n\times 2^n}$ is a circulant matrix, then for any positive integer k, the matrix HL^k is column-shift equivalent to the matrix H.

Proof. According to the properties of circulant matrix, if matrix L is a circulant matrix, then L^k is also a circulant matrix for any positive integer k. According to Lemma 5, the result holds.

Theorem 3. If the state transition matrix L of an n-stage Galois NFSR satisfies $L = \delta_{2^n}[i\ \ i+1\ \cdots\ 2^n\ \ 1\ \ 2\ \cdots\ i-1]$ and i is even, then the Galois NFSR is observable.

Proof. Let H be the output matrix of the Galois NFSR. Then, for any positive integer k, we have

$$\begin{aligned} HL^k &= (HL^{k-1})L = (HL^{k-1})\delta_{2^n}[i\ \ i+1\ \cdots\ 2^n\ \ 1\ \ 2\ \cdots\ i-1] \\ &= [\mathrm{Col}_i(HL^{k-1})\ \ \mathrm{Col}_{i+1}(HL^{k-1})\ \cdots\ \mathrm{Col}_{2^n}(HL^{k-1})\ \underbrace{\mathrm{Col}_1(HL^{k-1})\ \cdots\ \mathrm{Col}_{i-1}(HL^{k-1})}_{(2^n-i+2)\text{-th}}], \end{aligned}$$

which yields

$$\begin{cases} \mathrm{Col}_{2^n+j-i+1}(HL^k) = \mathrm{Col}_j(HL^{k-1}), & \text{if } 1 \leqslant j \leqslant i-1, \\ \mathrm{Col}_{j-i+1}(HL^k) = \mathrm{Col}_j(HL^{k-1}), & \text{if } i \leqslant j \leqslant 2^n. \end{cases}$$

Combining the above equations, we obtain

$$\mathrm{Col}_{(2^n+j-i) \bmod 2^n+1}(HL^k) = \mathrm{Col}_j(HL^{k-1}) \tag{12}$$

for any positive integer k. Thus, according to (12), we have

$$\mathrm{Col}_{[2\times 2^n+2(1-i)] \bmod 2^n+1}(HL^2) = \mathrm{Col}_{(2^n+1-i) \bmod 2^n+1}(HL) = \mathrm{Col}_1(H).$$

By the same reasoning, we can infer that

$$\begin{aligned}\mathrm{Col}_{[k2^n+k(1-i)] \bmod 2^n+1}(HL^k) &= \mathrm{Col}_{[(k-1)2^n+(k-1)(1-i)] \bmod 2^n+1}(HL^{k-1}) = \cdots \\ &= \mathrm{Col}_{(2^n+1-i) \bmod 2^n+1}(HL) = \mathrm{Col}_1(H)\end{aligned}$$

for any positive integer $k \leqslant 2^n - 2$.

Now, we prove $(2^n + 1 - i) \bmod 2^n + 1, [2 \times 2^n + 2(1 - i)] \bmod 2^n + 1, \ldots, [k2^n + k(1 - i)] \bmod 2^n + 1$ are pairwise distinct. Using a proof by contradiction, we assume that there exist two distinct integers $k_1, k_2 \leqslant k$ such that $[k_1 2^n + k_1(1 - i)] \bmod 2^n + 1 = [k_2 2^n + k_2(1 - i)] \bmod 2^n + 1$. Then we get $(k_1 - k_2)(1 - i) \bmod 2^n = 0$. Since i is an even number, $1 - i$ is an odd number. Hence, $k_1 - k_2 = 0$ or $k_1 - k_2$ is the multiple of 2^n. According to $k_1, k_2 \leqslant k \leqslant 2^n - 2$, we have $k_1 - k_2 = 0$. It is contrary with $k_1 \neq k_2$. Thus, $(2^n + 1 - i) \bmod 2^n + 1, [2 \times 2^n + 2(1 - i)] \bmod 2^n + 1, \ldots, [k2^n + k(1 - i)] \bmod 2^n + 1$ are pairwise distinct. Therefore, we can infer that $H, HL, \ldots, HL^{2^n-2}$ are pairwise distinct.

Next, we assume that the observability matrix $\mathcal{O}_{2^n-1}$ has not 2^n distinct columns. So there must exist two equal columns in $\mathcal{O}_{2^n-1}$. If the two equal columns are adjacent, then without loss of generality, we can assume that the first and the second columns are the same in $\mathcal{O}_{2^n-1}$. On the other hand, notably, all possible columns that keep the first column equal to the second column in the row reduced observability matrix $\mathcal{O}_N^\sharp$ with $N \leqslant 2^n - 1$ are as follows:

$$\mathcal{O}_N^\sharp = \begin{bmatrix} 1111 \cdots 1100 \cdots 0000 \\ 1111 \cdots 1000 \cdots 0001 \\ 1111 \cdots 0000 \cdots 0011 \\ \vdots \quad\quad \vdots \quad\quad \vdots \\ 1100 \cdots 0000 \cdots 1111 \\ 0000 \cdots 0011 \cdots 1111 \\ 0000 \cdots 0111 \cdots 1110 \\ 0000 \cdots 1111 \cdots 1100 \\ \vdots \quad\quad \vdots \quad\quad \vdots \\ 0011 \cdots 1111 \cdots 0000 \end{bmatrix}.$$

Together taking into consideration Lemma 7, HL^k is column-shift equivalent to H for any positive integer $k \leqslant 2^n$. We can deduce that there are at most $2^n - 4$ rows keeping the first column equal to the second column in the row reduced observability matrix $\mathcal{O}_{2^n-1}^\sharp$. If the two same columns are not adjacent, then we get the number of rows is less than $2^n - 4$. However, according to our assumption of $\mathcal{O}_{2^n-1}$ not having 2^n distinct columns, which is equivalent to $\mathcal{O}_{2^n-1}^\sharp$ not having 2^n distinct columns, we can infer that $\mathcal{O}_{2^n-1}^\sharp$ (or equivalently, $\mathcal{O}_{2^n-1}$) has $2^n - 1$ rows keeping its first column equal to the second column. This induces a contradiction, so the observability matrix $\mathcal{O}_{2^n-1}$ has 2^n distinct columns. Therefore, according to Lemma 3, the Galois NFSR is observable.

The following result can be directly obtained from the definition of observability of Galois NFSRs.

Lemma 8. An n-stage Galois NFSR is observable if and only if the Galois NFSR has 2^n output sequences.

Theorem 4. If a Galois NFSR with nonsingular state transition matrix L is observable, then the Galois NFSR with state transition matrix L^{T} is also observable.

Proof. Since L is nonsingular, L is a permutation matrix. So, we only need to concern the position of the entry 1 in each column of L. Without loss of generality, we assume the (i, j)-th entry of L is 1,

denoted by $L_{ij}=1$. It means $\mathrm{Col}_j(L)=\delta^i_{2^n}$, where n is the stage number of the Galois NFSR. Hence, according to the linear system representation $\boldsymbol{x}(t+1)=L\boldsymbol{x}(t)$ of the Galois NFSR, we can easily see that the state transition matrix L is nonsingular if and only if the Galois NFSR is nonsingular, which means its state diagram contains only cycles; moreover, we can easily observe from $L\delta^j_{2^n}=\mathrm{Col}_j(L)=\delta^i_{2^n}$ that the state $\boldsymbol{x}_1=\delta^j_{2^n}$ is updated to the state $\boldsymbol{x}_2=\delta^i_{2^n}$. But in the state transition matrix L^{T}, L_{ji} means the state $\boldsymbol{x}_2=\delta^i_{2^n}$ is updated to the state $\boldsymbol{x}_1=\delta^j_{2^n}$. Together considering that the state diagram of the Galois NFSR with state transition matrix L contains only cycles, we can deduce that the state diagram of the Galois NFSR with state transition matrix L^{T} has a reverse direction to the state diagram of the Galois NFSR with state transition matrix L. Moreover, as the Galois NFSR is observable, according to Lemma 8, we know the Galois NFSR has 2^n output sequences. Hence, the Galois NFSR with state transition matrix L^{T} also has 2^n output sequences. Therefore, according to Lemma 8 again, the Galois NFSR with state transition matrix L^{T} is observable.

4 Determining the observability of Galois NFSRs via a new observability matrix

In this section, we propose a new observability matrix. Thanks to its induced convenience, we give some new necessary and/or sufficient conditions for the observability of Galois NFSRs. Before that, we first give two results below.

Proposition 2. For a positive integer N, let $\mathcal{O}_N$ be the observability matrix of an n-stage Galois NFSR. Then $\mathrm{Col}_i(\mathcal{O}_N)$ with $i\in\{1,2,\ldots,2^n\}$ is an output sequence of length N over Δ_2 resulting from the initial states $\boldsymbol{x}=\delta^i_{2^n}$.

Proof. Let the n-stage Galois NFSR be represented by the linear system:

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

where $\boldsymbol{x}\in\Delta_{2^n}$ is the state and $\boldsymbol{y}\in\Delta_2$ is the output. Then, we can easily obtain

$$\begin{bmatrix}\boldsymbol{y}(t)\\ \boldsymbol{y}(t+1)\\ \vdots\\ \boldsymbol{y}(t+N-1)\end{bmatrix}=\begin{bmatrix}H\\ HL\\ \vdots\\ HL^{N-1}\end{bmatrix}\boldsymbol{x}(t)=\mathcal{O}_N\boldsymbol{x}(t).$$

If the initial state $\boldsymbol{x}=\delta^i_{2^n}$, then we can get the output sequence is $\mathrm{Col}_i(\mathcal{O}_N)$ and its length is N.

Corollary 3. For a positive integer N, let $\mathcal{O}^\sharp_N$ be the row reduced observability matrix of an n-stage Galois NFSR. Then $\mathrm{Col}_i(\mathcal{O}^\sharp_N)$ with $i\in\{1,2,\ldots,2^n\}$ is an output sequence of length N over $\mathbb{F}_2$ resulting from the initial state $[i_1\ \ i_2\ \cdots\ i_n]^{\mathrm{T}}\in\mathbb{F}_2^n$, where $(i_1,i_2,\ldots,i_n)$ is the binary of 2^n-i.

Proof. Note that $\mathcal{O}^\sharp_N$ is a row reduced matrix formed by the odd rows of the observability matrix $\mathcal{O}_N$. Then the result follows from Proposition 2 and Lemma 1 and the relation between $\mathcal{O}_N$ and $\mathcal{O}^\sharp_N$.

Corollary 3 shows that the columns of the row reduced observability matrix $\mathcal{O}^\sharp_N$ of a Galois NFSR are arranged in the reverse alphabetic order. We can properly change this order according to the state diagram of the Galois NFSR, for the convenience of counting the number of its distinct columns.

4.1 New observability matrix

4.1.1 *For nonsingular Galois NFSRs*

If an n-stage Galois NFSR is nonsingular, then its state diagram consists of only cycles without branches. We assume it has M cycles, denoted by $C_1,C_2,\ldots,C_M$. Their lengths are $l_{C_1},l_{C_2},\ldots,l_{C_M}$, respectively. For each $i\in\{1,2,\ldots,M\}$, let $s^i_1,s^i_2,\ldots,s^i_{l_{C_i}}$ be the states on cycle C_i, where the successor of s^i_r is s^i_{r+1} with $r\in\{1,2,\ldots,l_{C_i}-1\}$ and the successor of $s^i_{l_{C_i}}$ is s^i_1. Then there exists a permutation P of dimension 2^n, such that

$$\mathcal{O}^\sharp_N P=\mathcal{O}^*_N=[{}^{C_1}\mathcal{O}^*_N\quad {}^{C_2}\mathcal{O}^*_N\quad\cdots\quad {}^{C_M}\mathcal{O}^*_N],\tag{13}$$

where $\mathrm{Col}_r({}^{C_i}\mathcal{O}_N^*)$ and $\mathrm{Col}_{r+1}({}^{C_i}\mathcal{O}_N^*)$ are the output sequences resulting from the initial states s_r^i and s_{r+1}^i, respectively, for each $i \in \{1,2,\ldots,M\}$ and for each $r \in \{1,2,\ldots,l_{C_i}\}$. We call the matrix $\mathcal{O}_N^*$ in (13) a new observability matrix of an n-stage nonsingular Galois NFSR.

Let

$$ {}^{C_i}\mathcal{S}_N^* = \begin{bmatrix} s_1^i & s_2^i & \cdots & s_{l_{C_i}-1}^i & s_{l_{C_i}}^i \\ s_2^i & s_3^i & \cdots & s_{l_{C_i}}^i & s_1^i \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ s_{l_{C_i}}^i & s_1^i & \cdots & s_{l_{C_i}-2}^i & s_{l_{C_i}-1}^i \\ s_1^i & s_2^i & \cdots & s_{l_{C_i}-1}^i & s_{l_{C_i}}^i \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ s^i_{(N-1) \bmod l_{C_i}+1} & s^i_{N \bmod l_{C_i}+1} & \cdots & s^i_{(N-3) \bmod l_{C_i}+1} & s^i_{(N-2) \bmod l_{C_i}+1} \end{bmatrix}. \tag{14} $$

Note that an NFSR usually uses the content of the lowest bit as its output. Then, the output sequence of an NFSR is formed by the first components of its corresponding consecutive states. Thus, we have the following statement.

Fact 1. $\mathrm{Col}_r({}^{C_i}\mathcal{S}_N^*)$ is the state sequence corresponding to the output sequence $\mathrm{Col}_r({}^{C_i}\mathcal{O}_N^*)$ for each $r \in \{1,2,\ldots,l_{C_i}\}$.

Let a_{pq}^i be the (p,q)-th entry of ${}^{C_i}\mathcal{O}_N^*$. Then, according to Fact 1 and (14), for the matrix ${}^{C_i}\mathcal{O}_N^*$, we have the following two properties:

$$ a_{pq}^i = \begin{cases} a^i_{(p-1)(q+1)}, & p = 2,3,\ldots,N, \quad q = 1,2,\ldots,l_{C_i}-1, \\ a^i_{(p-1)1}, & p = 2,3,\ldots,N, \quad q = l_{C_i}, \end{cases} \tag{15} $$

$$ \mathrm{Col}_j({}^{C_i}\mathcal{O}_{l_{C_i}}^*) = \mathrm{Row}_j({}^{C_i}\mathcal{O}_{l_{C_i}}^*), \quad i = 1,2,\ldots,M, \quad j = 1,2,\ldots,l_{C_i}. \tag{16} $$

Because of $\mathcal{O}_N^* = \mathcal{O}_N^\sharp P$, $\mathcal{O}_N^*$ has the same number of the distinct columns as $\mathcal{O}_N^\sharp$, and thereby as $\mathcal{O}_N$. Thus, an n-stage Galois NFSR is observable if and only if its new observability matrix $\mathcal{O}_N^*$ has 2^n distinct columns.

Example 1. Consider a 3-stage Galois NFSR with state transition matrix $L = \delta_8[1\ 6\ 7\ 3\ 2\ 4\ 5\ 8]$. Using Definition 4 of the observability matrix $\mathcal{O}_N$, we get the row reduced observability matrix:

$$ \mathcal{O}_3^\sharp = \begin{bmatrix} 1&1&1&1&0&0&0&0 \\ 1&0&0&1&1&1&0&0 \\ 1&1&0&0&0&1&1&0 \end{bmatrix} $$

which has 8 distinct columns. It implies that the Galois NFSR is observable. On the other hand, by direct computation, we get its state diagram consisting of three cycles:

$$ C_1 : 110 \to 010 \to 100 \to 101 \to 001 \to 011 \to 110; $$
$$ C_2 : 111 \to 111; \quad C_3 : 000 \to 000. $$

According to our method of constructing the new observability matrix, we obtain

$$ \mathcal{O}_3^* = \begin{bmatrix} 1&0&1&1&0&0&1&0 \\ 0&1&1&0&0&1&1&0 \\ 1&1&0&0&1&0&1&0 \end{bmatrix}. $$

Clearly, $\mathcal{O}_3^* = \mathcal{O}_3^\sharp P$, where $P = \delta_8[2\ 6\ 4\ 3\ 7\ 5\ 1\ 8]$. It also takes only three steps to achieve 8 distinct columns, and thereby we can conclude that the Galois NFSR is observable, consist with the foregoing conclusion drawn by the row reduced observability matrix $\mathcal{O}_3^\sharp$.

Remark 1. Our proposed new observability matrix $\mathcal{O}_N^*$ for a nonsingular Galois NFSR accumulates output sequences resulting from initial states on the same cycle into a column block. Notably, here the

initial states are only restricted to the same cycle, but not restricted to the reverse alphabetic order. If the initial states are restricted to the same cycle and to the reverse alphabetic order, then our proposed new observability matrix $\mathcal{O}_N^*$ becomes the original observability matrix $\mathcal{O}_N$ under the canonical form [32] of the nonsingular Galois NFSR. The reason is that the state transition matrix under the canonical form of the nonsingular Galois NFSR is block diagonal with each block nonsingular, and it accumulates consecutive states on each cycle in the reverse alphabetic order into a column block.

4.1.2 *For singular Galois NFSRs*

If an n-stage Galois NFSR is singular, then its state diagram consists of some cycles and some branches. We assume that this Galois NFSR has M starting states. The branches that start from these starting states are denoted by $B_1, B_2, \ldots, B_M$ and their lengths are $l_{B_1}, l_{B_2}, \ldots, l_{B_M}$, respectively. Since any branch connects only one cycle, the cycles $C_1, C_2, \ldots, C_M$ are connected with $B_1, B_2, \ldots, B_M$, respectively. Notably, here some C_ks may be the same. $l_{C_1}, l_{C_2}, \ldots, l_{C_M}$ are the lengths of cycles $C_1, C_2, \ldots, C_M$, respectively. For each $i \in \{1, 2, \ldots, M\}$, let $s_1^i, s_2^i, \ldots, s_{l_{B_i}+l_{C_i}}^i$ be the states on the branch B_i and its connected cycle C_i. Moreover, for each $i \in \{1, 2, \ldots, M\}$ and each $r \in \{1, 2, \ldots, l_{B_i}+l_{C_i}\}$, let $\mathrm{Col}_r({}^{B_i}\mathcal{O}_N^*)$ and $\mathrm{Col}_{r+1}({}^{B_i}\mathcal{O}_N^*)$ be the output sequences, respectively, resulting from the initial state s_r^i and s_{r+1}^i on the branch B_i, while let $\mathrm{Col}_r({}^{C_i}\mathcal{O}_N^*)$ and $\mathrm{Col}_{r+1}({}^{C_i}\mathcal{O}_N^*)$ be the output sequences, respectively, resulting from the initial states s_r^i and s_{r+1}^i on the cycle C_i. Then there exists a matrix $P^* \in \mathcal{L}_{2^n \times v}$ with

$$v = \sum_{i=1}^{M} (l_{B_i} + l_{C_i}),$$

such that

$$\mathcal{O}_N^\sharp P^* = \mathcal{O}_N^* = [{}^{B_1}\mathcal{O}_N^* \quad {}^{C_1}\mathcal{O}_N^* \quad {}^{B_2}\mathcal{O}_N^* \quad {}^{C_2}\mathcal{O}_N^* \quad \cdots \quad {}^{B_M}\mathcal{O}_N^* \quad {}^{C_M}\mathcal{O}_N^*]. \tag{17}$$

We call $\mathcal{O}_N^*$ in (17) a new observability matrix of an n-stage singular Galois NFSR.

Let

$$[{}^{B_i}\mathcal{S}_N^* \ {}^{C_i}\mathcal{S}_N^*] = \begin{bmatrix} s_1^i & s_2^i & \cdots & s_{l_{B_i}+1}^i & \cdots & s_{l_{B_i}+l_{C_i}}^i \\ s_2^i & s_3^i & \cdots & s_{l_{B_i}+2}^i & \cdots & s_{l_{B_i}+1}^i \\ \vdots & \vdots & & \vdots & & \vdots \\ s_{l_{B_i}+1}^i & s_{l_{B_i}+2}^i & \cdots & s_{(l_{B_i} \bmod l_{C_i})+l_{B_i}+1}^i & \cdots & s_{(l_{B_i}-1 \bmod l_{C_i})+l_{B_i}+1}^i \\ \vdots & \vdots & & \vdots & & \vdots \\ s_{(N-l_{B_i}-1) \bmod l_{C_i}+l_{B_i}+1}^i & s_{(N-l_{B_i}) \bmod l_{C_i}+l_{B_i}+1}^i & \cdots & s_{(N-1) \bmod l_{C_i}+l_{B_i}+1}^i & \cdots & s_{(N-2) \bmod l_{C_i}+l_{B_i}+1}^i \end{bmatrix}. \tag{18}$$

Similar to the nonsingular case, we have the following statement.

Fact 2. $\mathrm{Col}_r([{}^{B_i}\mathcal{S}_N^* \ {}^{C_i}\mathcal{S}_N^*])$ is the state sequence corresponding to the output sequence $\mathrm{Col}_r([{}^{B_i}\mathcal{O}_N^* \ {}^{C_i}\mathcal{O}_N^*])$ for each $r \in \{1, 2, \ldots, l_{B_i} + l_{C_i}\}$.

Let a_{pq}^i be the (p, q)-th entry of $[{}^{C_i}\mathcal{O}_N^* \ {}^{B_i}\mathcal{O}_N^*]$. Note that any state on a branch will finally reach a cycle and stay on this cycle forever. Then, according to Fact 2 and (18), for the matrix $[{}^{B_i}\mathcal{O}_N^* \ {}^{C_i}\mathcal{O}_N^*]$, we obtain the following two properties:

$$a_{pq}^i = \begin{cases} a_{(p-1)(q+1)}^i, & p = 2, 3, \ldots, N, \quad q = 1, 2, \ldots, l_{B_i} + l_{C_i} - 1, \\ a_{(p-1)(l_{B_i}+1)}^i, & p = 2, 3, \ldots, N, \quad q = l_{B_i} + l_{C_i}; \end{cases} \tag{19}$$

$$\mathrm{Col}_j([{}^{B_i}\mathcal{O}_{l_{B_i}+l_{C_i}}^* \quad {}^{C_i}\mathcal{O}_{l_{B_i}+l_{C_i}}^*]) = \mathrm{Row}_j([{}^{B_i}\mathcal{O}_{l_{B_i}+l_{C_i}}^* \quad {}^{C_i}\mathcal{O}_{l_{B_i}+l_{C_i}}^*]) \tag{20}$$

for all $i = 1, 2, \ldots, M$ and for all $j = 1, 2, \ldots, l_{B_i} + l_{C_i}$. Hence, if we know the first row of the new observability matrix $\mathcal{O}_N^*$, then we can get all rows of $\mathcal{O}_N^*$.

The matrix $\mathcal{O}_N^*$ is a column permutation and column extension of the observability matrix $\mathcal{O}_N^\sharp$ because the sequences resulting from different initial states on the same branch and their connected common cycle are arranged together; moreover, different branches may have some common states and different branches

may connect the same circle. The expanded columns of $\mathcal{O}_N^*$ are all those of $\mathcal{O}_N^\sharp$. So, $\mathcal{O}_N^*$ has 2^n distinct columns if and only if $\mathcal{O}_N^\sharp$ (or equivalently, $\mathcal{O}_N$) has 2^n distinct columns. Hence, an n-stage Galois NFSR is observable if and only if $\mathcal{O}_N^*$ has 2^n distinct columns.

Example 2. Consider a 3-stage Galois NFSR with state transition matrix $L = \delta_8[1\ 3\ 4\ 5\ 6\ 7\ 4\ 8]$. Using Definition 4 of the observability matrix $\mathcal{O}_N$, we get the row reduced observability matrix:

$$\mathcal{O}_4^\sharp = \begin{bmatrix} 1&1&1&1&0&0&0&0\\ 1&1&1&0&0&0&1&0\\ 1&1&0&0&0&1&0&0\\ 1&0&0&0&1&0&0&0 \end{bmatrix},$$

which has 8 distinct columns. It implies that the Galois NFSR is observable. On the other hand, by direct computation, we get its state diagram consisting of one branch and three cycles:

$$B_1: 110 \to 101 \to 100; \quad C_1: 100 \to 011 \to 010 \to 001 \to 100;$$
$$C_2: 111 \to 111; \quad C_3: 000 \to 000.$$

According to our construction of the new observability matrix, we obtain

$$\mathcal{O}_4^* = \left[{}^{B_1}\mathcal{O}_4^* \ \ {}^{C_1}\mathcal{O}_4^* \ \ {}^{C_2}\mathcal{O}_4^* \ \ {}^{C_3}\mathcal{O}_4^*\right] = \begin{bmatrix} 1&1&1&0&0&0&1&0\\ 1&1&0&0&0&1&1&0\\ 1&0&0&0&1&0&1&0\\ 0&0&0&1&0&0&1&0 \end{bmatrix}.$$

Clearly, $\mathcal{O}_4^* = \mathcal{O}_4^\sharp P$, where $P = \delta_8[2\ 3\ 4\ 5\ 6\ 7\ 1\ 8]$. It also takes only four steps to achieve 8 distinct columns, and thereby we can infer that the Galois NFSR is observable, consist with the foregoing conclusion drawn by the row reduced observability matrix $\mathcal{O}_4^\sharp$.

Remark 2. The new observability matrix $\mathcal{O}_N^*$ of a Galois NFSR is constructed by accumulating output sequences resulting from initial states on the same branch and its connected cycle into a block. Compared with the original observability matrix $\mathcal{O}_N$ that is actually constructed by accumulating output sequences resulting from initial states in the reverse alphabetic order, the new observability matrix $\mathcal{O}_N^*$ has some advantages. First, the adjacent columns/rows of each block of the new observability matrix $\mathcal{O}_N^*$ have the shift property (15) for a nonsingular Galois NFSR and have the shift property (19) for a singular Galois NFSR. Second, the new observability matrix $\mathcal{O}_N^*$ has the symmetric property (16) of each block for a nonsingular Galois NFSR and has symmetric property (20) for a singular Galois NFSR as well. Last but most importantly, the above shift property and symmetric property, especially the former, facilitate to count the distinct columns of the new observability matrix, which is the key point of the observability determination for Galois NFSRs and therefore, benefit us to get some new interesting results, which will be shown in Subsection 4.2.

4.2 Applications of the new observability matrix

Lemma 9. If $\mathrm{Row}_1({}^{C_{i_1}}\mathcal{O}_N^*)$ is shift-column equivalent to $\mathrm{Row}_1({}^{C_{i_2}}\mathcal{O}_N^*)$, where cycles C_{i_1} and C_{i_2} have the same length, then the Galois NFSR is not observable.

Proof. Let $\mathrm{Row}_1({}^{C_{i_1}}\mathcal{O}_N^*) = [a_{11}^{i_1} \ \ a_{12}^{i_1} \ \ \cdots \ \ a_{1(l_{C_{i_1}})}^{i_1}]$ and $\mathrm{Row}_1({}^{C_{i_2}}\mathcal{O}_N^*) = [a_{11}^{i_2} \ \ a_{12}^{i_2} \ \ \cdots \ \ a_{1(l_{C_{i_2}})}^{i_2}]$. Since the cycles C_{i_1} and C_{i_2} have the same length, we conclude that $l_{C_{i_1}} = l_{C_{i_2}}$. If $\mathrm{Row}_1({}^{C_{i_1}}\mathcal{O}_N^*)$ is column-shift equivalent to $\mathrm{Row}_1({}^{C_{i_2}}\mathcal{O}_N^*)$, then according to the foregoing definition of column-shift equivalence of matrices, we know that there exists a positive integer k satisfying $1 \leqslant k \leqslant l_{C_{i_1}}$, such that

$$a_{1k}^{i_1} = a_{11}^{i_2}, \quad a_{1(k+1)}^{i_1} = a_{12}^{i_2}, \ldots, a_{1(l_{C_i})}^{i_1} = a_{1(1+l_{C_i}-k)}^{i_2}, \quad a_{11}^{i_1} = a_{1(2+l_{C_i}-k)}^{i_2}, \ldots, a_{1(k-1)}^{i_1} = a_{1(l_{C_i})}^{i_2}.$$

According to the shift property of O_N^* described in (15) for nonsingular Galois NFSR or in (19) for singular one, we have

$$\mathrm{Col}_1\left({}^{C_{i_2}}\mathcal{O}_{l_{C_{i_2}}}^*\right) = \begin{bmatrix} a_{11}^{i_2} & a_{21}^{i_2} & \cdots & a_{(l_{C_{i_2}})1}^{i_2} \end{bmatrix}^{\mathrm{T}} = \begin{bmatrix} a_{11}^{i_2} & a_{12}^{i_2} & \cdots & a_{1(l_{C_{i_1}})}^{i_2} \end{bmatrix}^{\mathrm{T}}$$

$$= \begin{bmatrix} a_{1k}^{i_1} & a_{1(k+1)}^{i_1} & \cdots & a_{1(k-1)}^{i_1} \end{bmatrix}^{\mathrm{T}} = \begin{bmatrix} a_{1k}^{i_1} & a_{2k}^{i_1} & \cdots & a_{(l_{C_{i_1}})k}^{i_1} \end{bmatrix}^{\mathrm{T}} = \mathrm{Col}_k \left({}^{C_{i_1}}\mathcal{O}_{l_{C_{i_1}}}^* \right).$$

It implies that there exist two distinct state sequences on different cycles corresponding to the same output sequences. According to Lemma 4, the Galois NFSR is not observable.

Theorem 5. Let $\mathcal{N}_k$ be the number of distinct columns of the observability matrix $\mathcal{O}_k$ of an n-stage Galois NFSR. Then the Galois NFSR is observable if and only if $\mathcal{N}_{k+1} - \mathcal{N}_k \geqslant 1$ for all positive integer k satisfying $\mathcal{N}_k < 2^n$.

Proof. (Sufficiency) The 2×2^n output matrix $H = \delta_2[1 \ \ 1 \cdots 1 \ \ 2 \ \ 2 \cdots 2]$ of an n-stage Galois NFSR has two distinct columns. So $\mathcal{N}_1 = 2$. Since $\mathcal{N}_{k+1} - \mathcal{N}_k \geqslant 1$, we have $\mathcal{N}_2 \geqslant \mathcal{N}_1 + 1 = 3$, $\mathcal{N}_3 \geqslant \mathcal{N}_2 + 1 = 4$, …, $\mathcal{N}_{2^n-1} \geqslant \mathcal{N}_{2^n-2} + 1 \geqslant (2^n - 1) + 1 = 2^n$. On the other hand, as the observability matrix $\mathcal{O}_{2^n-1}$ has only 2^n columns, we have $\mathcal{N}_{2^n-1} \leqslant 2^n$. Hence, $\mathcal{N}_{2^n-1} = 2^n$. Therefore, according to Lemma 3, this Galois NFSR is observable.

(Necessary) If an n-stage Galois NFSR is observable, then according to Lemma 3, its observability matrix $\mathcal{O}_{2^n-1}$ has 2^n distinct columns. Hence, to assure $\mathcal{N}_{k+1} - \mathcal{N}_k \geqslant 1$ with $\mathcal{N}_k < 2^n$, k must satisfy $k \leqslant 2^n - 2$.

Case 1. The Galois NFSR is nonsingular. Since the Galois NFSR is nonsingular, its state diagram contains only cycles. Assume that there are M cycles denoted by $C_1, C_2, \ldots, C_M$. Let $\mathcal{N}_k^{C_i}$ represent the number of distinct columns of ${}^{C_i}\mathcal{O}_k^*$. Let a_{pq}^i be the (p,q)-th entry of ${}^{C_i}\mathcal{O}_{k+1}^*$ in (13) with therein $N = k+1$. If $\mathcal{N}_k < 2^n$, then there are two cases.

Case 1(a). There exist two equal columns on the cycle C_i, say, $\mathrm{Col}_p({}^{C_i}\mathcal{O}_k^*) = \mathrm{Col}_q({}^{C_i}\mathcal{O}_k^*)$ with $1 \leqslant p, q \leqslant l_{C_i}$. Then, according to the shift property described by (15) for $\mathcal{O}_k^*$ with any positive integer $k \leqslant 2^n - 2$, we can get $a_{1(p+1)}^i = a_{2p}^i, a_{2(p+1)}^i = a_{3p}^i, \ldots, a_{k(p+1)}^i = a_{(k+1)p}^i$ and $a_{1(q+1)}^i = a_{2q}^i, a_{2(q+1)}^i = a_{3q}^i, \ldots, a_{k(q+1)}^i = a_{(k+1)q}^i$. It yields $\mathrm{Col}_{p+1}({}^{C_i}\mathcal{O}_k^*) = \mathrm{Col}_{q+1}({}^{C_i}\mathcal{O}_k^*)$. Assume $\mathcal{N}_{k+1} - \mathcal{N}_k = 0$, then we have $a_{(k+1)(p+1)}^i = a_{(k+1)(q+1)}^i$. So we get $\mathrm{Col}_{p+1}({}^{C_i}\mathcal{O}_{k+1}^*) = \mathrm{Col}_{q+1}({}^{C_i}\mathcal{O}_{k+1}^*)$. By the same reasoning, we get $\mathrm{Col}_{p+2}({}^{C_i}\mathcal{O}_{k+1}^*) = \mathrm{Col}_{q+2}({}^{C_i}\mathcal{O}_{k+1}^*)$, …, $\mathrm{Col}_1({}^{C_i}\mathcal{O}_{k+1}^*) = \mathrm{Col}_{(q+l_{C_i}-p) \mod l_{C_i}+1}({}^{C_i}\mathcal{O}_{k+1}^*)$. Thereby, we have $\mathrm{Col}_1({}^{C_i}\mathcal{O}_{k+1}^*) = \mathrm{Col}_{(q-p) \mod l_{C_i}+1}({}^{C_i}\mathcal{O}_{k+1}^*)$. Thus, the sequence $a_{11}^i a_{12}^i \cdots a_{1(l_{C_i})}^i$ is of period $q-p$. Since the Galois NFSR is observable and $a_{11}^i a_{12}^i \cdots a_{1(l_{C_i})}^i$ is an output sequence corresponding to the cycle C_i, the period of this sequence is l_{C_i}. Thus, $q - p = l_{C_i}$. However, as $1 \leqslant p, q \leqslant l_{C_i}$, we have $q - p \neq l_{C_i}$, a contradiction. Hence, $\mathcal{N}_{k+1} - \mathcal{N}_k \geqslant 1$ in this case.

Case 1(b). There exist two equal columns on two distinct cycles C_i and C_r, say, $\mathrm{Col}_p({}^{C_i}\mathcal{O}_k^*) = \mathrm{Col}_q({}^{C_r}\mathcal{O}_k^*)$ with $1 \leqslant p \leqslant l_{C_i}$ and $1 \leqslant q \leqslant l_{C_r}$. From the shift property described by (15) for $\mathcal{O}_k^*$ with any positive integer $k \leqslant 2^n - 2$, we can get $a_{1(p+1)}^i = a_{2p}^i, a_{2(p+1)}^i = a_{3p}^i, \ldots, a_{k(p+1)}^i = a_{(k+1)p}^i$ and $a_{1(q+1)}^r = a_{2q}^r, a_{2(q+1)}^r = a_{3q}^r, \ldots, a_{k(q+1)}^r = a_{(k+1)q}^r$. It means $\mathrm{Col}_{p+1}({}^{C_i}\mathcal{O}_k^*) = \mathrm{Col}_{q+1}({}^{C_r}\mathcal{O}_k^*)$. Suppose $\mathcal{N}_{k+1} - \mathcal{N}_k = 0$, yielding $a_{(k+1)(p+1)}^i = a_{(k+1)(q+1)}^r$. So we get $\mathrm{Col}_{p+1}({}^{C_i}\mathcal{O}_{k+1}^*) = \mathrm{Col}_{q+1}({}^{C_r}\mathcal{O}_{k+1}^*)$. By the same reasoning, we get $\mathrm{Col}_{p+2}({}^{C_i}\mathcal{O}_{k+1}^*) = \mathrm{Col}_{q+2}({}^{C_r}\mathcal{O}_{k+1}^*), \ldots, \mathrm{Col}_1({}^{C_i}\mathcal{O}_{k+1}^*) = \mathrm{Col}_{(q+l_{C_i}-p) \mod l_{C_r}+1}({}^{C_r}\mathcal{O}_{k+1}^*), \ldots$. Thus, we can infer that the sequence $a_{1p}^i a_{1(p+1)}^i a_{1(p+2)}^i \cdots$ is equal to the sequence $a_{1q}^r a_{1(q+1)}^r a_{1(q+2)}^r \cdots$. If $l_{C_i} = l_{C_r}$, then we can easily find that $\mathrm{Col}_1({}^{C_i}\mathcal{O}_{k+1}^*) = \mathrm{Col}_{(q-p) \mod l_{C_r}+1}({}^{C_r}\mathcal{O}_{k+1}^*), \mathrm{Col}_2({}^{C_i}\mathcal{O}_{k+1}^*) = \mathrm{Col}_{(q-p+1) \mod l_{C_r}+1}({}^{C_r}\mathcal{O}_{k+1}^*), \ldots$. Hence, we can deduce that $\mathrm{Row}_1({}^{C_i}\mathcal{O}_{k+1}^*)$ is column-shift equivalent to $\mathrm{Row}_1({}^{C_r}\mathcal{O}_{k+1}^*)$, and therefore according to Lemma 9, the Galois NFSR is not observable, which is in contradiction with the assumption that the Galois NFSR is observable. If $l_{C_i} \neq l_{C_r}$, then without loss of generality, we assume $l_{C_r} > l_{C_i}$. Since the sequence $a_{1q}^r a_{1(q+1)}^r a_{1(q+2)}^r \cdots$ on the cycle C_r, its period is l_{C_r}. Similarly, the period of sequence $a_{1p}^i a_{1(p+1)}^i a_{1(p+2)}^i \cdots$ is l_{C_i}. Since $a_{1p}^i a_{1(p+1)}^i a_{1(p+2)}^i \cdots$ is equal to the sequence $a_{1q}^r a_{1(q+1)}^r a_{1(q+2)}^r \cdots$, we can infer that l_{C_i} is also a period of the sequence $a_{1q}^r a_{1(q+1)}^r a_{1(q+2)}^r \cdots a_{1(q-1)}^r \cdots$ on C_r. Because of $l_{C_i} \neq l_{C_r}$, this output sequence's period is not equal to the length of its corresponding cycle, and contrary with the observability of the Galois NFSR. So $\mathcal{N}_{k+1} - \mathcal{N}_k \geqslant 1$ in this case.

Case 2. The Galois NFSR is singular. Let a_{pq}^i be the (p,q)-th entry of $[{}^{B_i}\mathcal{O}_{k+1}^* \ \ {}^{C_i}\mathcal{O}_{k+1}^*]$ in (17) with therein $N = k+1$. If $\mathcal{N}_k < 2^n$, then there are six cases.

Case 2(a). There exist two equal columns on a branch B_i and its connected cycle C_i. Without loss of generality, we assume that the p-th column in ${}^{B_i}\mathcal{O}_k^*$ is equal to the q-th column in ${}^{C_i}\mathcal{O}_k^*$. Assume $\mathcal{N}_{k+1} - \mathcal{N}_k = 0$. Then, there are two equal columns in the above matrix, say, $\mathrm{Col}_p({}^{B_i}\mathcal{O}_{k+1}^*) = \mathrm{Col}_q({}^{C_i}\mathcal{O}_{k+1}^*)$. According to the shift property described in (19) for the matrix $[{}^{B_i}\mathcal{O}_k^* \ \ {}^{C_i}\mathcal{O}_k^*]$ with $k \leqslant 2^n - 2$, we

get $\mathrm{Col}_{p+1}({}^{B_i}\mathcal{O}^*_{k+1}) = \mathrm{Col}_{q+1}({}^{C_i}\mathcal{O}^*_{k+1})$. By the same reasoning, we can obtain $\mathrm{Col}_{p+2}({}^{B_i}\mathcal{O}^*_{k+1}) = \mathrm{Col}_{q+2}({}^{C_i}\mathcal{O}^*_{k+1}), \ldots, \mathrm{Col}_1({}^{C_i}\mathcal{O}^*_{k+1}) = \mathrm{Col}_{(q+l_{B_i}-p) \mod l_{C_i}+1}({}^{C_i}\mathcal{O}^*_{k+1})$. It means that there are two equal columns on the cycle C_i. According to Case 1(a), we know the result holds.

Case 2(b). There exist two equal columns on a branch B_i. Without loss of generality, we assume that the p-th column of ${}^{B_i}\mathcal{O}^*_k$ is the same as the q-th column of ${}^{B_i}\mathcal{O}^*_k$. Assume $\mathcal{N}_{k+1} - \mathcal{N}_k = 0$. Then, there are two equal columns in the the above matrix, say, $\mathrm{Col}_p({}^{B_i}\mathcal{O}^*_{k+1}) = \mathrm{Col}_q({}^{B_i}\mathcal{O}^*_{k+1})$. According to the shift property described in (19) for the matrix $[{}^{B_i}\mathcal{O}^*_k \ {}^{C_i}\mathcal{O}^*_k]$ with $k \leqslant 2^n-2$, similar to the proof of Case 2(a), we get $\mathrm{Col}_{p+1}({}^{B_i}\mathcal{O}^*_{k+1}) = \mathrm{Col}_{q+1}({}^{B_i}\mathcal{O}^*_{k+1})$. Again, similar to the proof of Case 2(a), by the same reasoning, we get $\mathrm{Col}_{p+2}({}^{B_i}\mathcal{O}^*_{k+1}) = \mathrm{Col}_{q+2}({}^{B_i}\mathcal{O}^*_{k+1}), \ldots, \mathrm{Col}_1({}^{C_i}\mathcal{O}^*_{k+1}) = \mathrm{Col}_{(q-p) \mod l_{C_i}+1}({}^{C_i}\mathcal{O}^*_{k+1})$. It means that there are two equal columns on the cycle C_i. From Case 1(a), the result follows.

Case 2(c). There exist two equal columns on a branch B_i and a cycle C_r. Without loss of generality, we assume that the p-th column of ${}^{B_i}\mathcal{O}^*_k$ is the same as the q-th column of ${}^{C_r}\mathcal{O}^*_k$. Similar to the proof of Case 2(a), we obtain $\mathrm{Col}_{p+1}({}^{B_i}\mathcal{O}^*_{k+1}) = \mathrm{Col}_{q+1}({}^{C_r}\mathcal{O}^*_{k+1})$. Again, by the same reasoning, we can obtain $\mathrm{Col}_{p+2}({}^{B_i}\mathcal{O}^*_{k+1}) = \mathrm{Col}_{q+2}({}^{C_r}\mathcal{O}^*_{k+1}), \ldots, \mathrm{Col}_1({}^{C_i}\mathcal{O}^*_{k+1}) = \mathrm{Col}_{(q+l_{B_i}-p) \mod l_{C_r}+1}({}^{C_r}\mathcal{O}^*_{k+1})$. It means that there are two equal columns on the two distinct cycles C_i and C_r. From Case 1(b), the result holds.

Case 2(d). There exist two equal columns on a branch B_i and another branch B_r. Without loss of generality, we assume that the p-th column of ${}^{B_i}\mathcal{O}^*_k$ is the same as the q-th column of ${}^{B_r}\mathcal{O}^*_k$. Similar to the proof of Case 2(a), we obtain $\mathrm{Col}_{p+1}({}^{B_i}\mathcal{O}^*_{k+1}) = \mathrm{Col}_{q+1}({}^{B_r}\mathcal{O}^*_{k+1})$. If $l_{B_i} - p \geqslant l_{B_r} - q$, we can get $\mathrm{Col}_{p+2}({}^{B_i}\mathcal{O}^*_{k+1}) = \mathrm{Col}_{q+2}({}^{B_r}\mathcal{O}^*_{k+1}), \ldots, \mathrm{Col}_1({}^{C_i}\mathcal{O}^*_{k+1}) = \mathrm{Col}_{(q+l_{B_i}-p) \mod l_{C_r}+1}({}^{C_r}\mathcal{O}^*_{k+1})$. If $l_{B_i} - p < l_{B_r} - q$, we have $\mathrm{Col}_{p+2}({}^{B_i}\mathcal{O}^*_{k+1}) = \mathrm{Col}_{q+2}({}^{B_r}\mathcal{O}^*_{k+1}), \ldots, \mathrm{Col}_{(p+l_{B_r}-q) \mod l_{C_i}+1}({}^{C_i}\mathcal{O}^*_{k+1}) = \mathrm{Col}_1({}^{C_r}\mathcal{O}^*_{k+1})$. Therefore, for both above branch length cases, we can observe that there are two equal columns on the two distinct cycles C_i and C_r. According to Case 1(b), the result follows.

Case 2(e). There exist two equal columns on a cycle C_i. From Case 1(a), the result follows.

Case 2(f). There exist two equal columns on two distinct cycles C_i and C_r. According to Case 1(b), the result holds.

Summarizing the above argument, we can conclude that an n-stage Galois NFSR is observable if and only if $\mathcal{N}_{k+1} - \mathcal{N}_k \geqslant 1$ for all positive integer k satisfying $\mathcal{N}_k < 2^n$.

Theorem 6. An n-stage Galois NFSR is observable if and only if its observability matrix $\mathcal{O}_{2^n-2}$ has 2^n distinct columns.

Proof. (Sufficiency) Note that $\mathcal{O}_{2^n-2}$ and $\mathcal{O}_{2^n-1}$ are matrices with 2^n columns. Thus, if $\mathcal{O}_{2^n-2}$ has 2^n distinct columns, then so has $\mathcal{O}_{2^n-1}$. Hence, according to Lemma 3, the result holds.

(Necessary) Since $\mathcal{O}_1 = H = \delta_2[1 \ \ 1 \ \cdots \ 1 \ \ 2 \ \ 2 \ \cdots \ 2]$, where H is the output matrix of the Galois NFSR, $\mathcal{N}_1$ has two distinct columns. By Lemma 6 and Theorem 5, we have $N_2 = 3$ or 4. If $\mathcal{N}_2 = 3$, we can assume that the row reduced observability matrix $\mathcal{O}_2^\sharp$ has not column $[1 \ 1]^{\mathrm{T}}$, which implies that there are only columns $[1 \ 0]^{\mathrm{T}}$, $[0 \ 0]^{\mathrm{T}}$, $[0 \ 1]^{\mathrm{T}}$. We define a, b, c as the number of $[1 \ 0]^{\mathrm{T}}$, $[0 \ 0]^{\mathrm{T}}$, $[0 \ 1]^{\mathrm{T}}$. In the first row of H, since the number of 0's is equal to the number of 1's, we can infer that $a = b + c$. HL is a column permutation of H, so the first row of HL keeps the number of 0's equal to the number of 1's. Thus, we have $c = b + a$. Therefore, $b = 0$, which is contrary with $\mathcal{N}_2 = 3$. So we have $\mathcal{N}_2 = 4$. According to Theorem 5, we have $\mathcal{N}_3 \geqslant \mathcal{N}_2 + 1 = 5, \mathcal{N}_4 \geqslant 6, \ldots, \mathcal{N}_{2^n-2} \geqslant 2^n$. Since $\mathcal{O}_{2^n-2}$ has only 2^n columns, we can conclude that $\mathcal{N}_{2^n-2} = 2^n$.

Theorem 6 reveals that, as a particular Boolean network, an n-stage Galois NFSR that usually uses the content of the lowest bit as its output, needs at most $2^n - 2$ steps (only one step less than a general Boolean network) to determine whether its observability matrix $\mathcal{O}_N$ has 2^n distinct columns and therefore, to determine whether the Galois NFSR is observable. The following example shows that the upper bound $2^n - 2$ for the observability matrix $\mathcal{O}_N$ is compact.

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

$$\begin{cases} f_1 = x_2 \oplus x_3 \oplus x_1x_2 \oplus x_2x_3 \oplus x_1x_3, \\ f_2 = x_1 \oplus x_1x_2 \oplus x_2x_3, \\ f_3 = x_1 \oplus x_3 \oplus 1. \end{cases}$$

We can easily get its state diagram consisting of two cycles:

$$C_1 : 000 \to 001 \to 100 \to 010 \to 101 \to 011 \to 110 \to 000, \quad C_2 : 111 \to 111.$$

Hence, the Galois NFSR can produce a sequence 0010101 of period 7 and a sequence 1 of period 1. Therefore, according to our construction, we can easily obtain the new observability matrix $\mathcal{O}_6^*$ as

$$\mathcal{O}_6^* = [{}^{C_1}\mathcal{O}_6^* \ {}^{C_2}\mathcal{O}_6^*] = \begin{bmatrix} 0&0&1&0&1&0&1&1 \\ 0&1&0&1&0&1&0&1 \\ 1&0&1&0&1&0&0&1 \\ 0&1&0&1&0&0&1&1 \\ 1&0&1&0&0&1&0&1 \\ 0&1&0&0&1&0&1&1 \end{bmatrix}.$$

This Galois observability matrix takes 6 steps to get 8 distinct columns. It implies that some n-stage Galois NFSR cannot be determined its observability until its observability matrix reaching 2^n-2 steps, though Theorem 6 shows that an n-stage Galois NFSR can be determined its observability by its observability matrix at most in 2^n-2 steps.

Lemma 10. Let $L \in \mathcal{L}_{2^n\times 2^n}$ be the state transition matrix of an n-stage Galois NFSR. Then the Galois NFSR has a cycle of length 2^n in its state diagram if and only if $\mathrm{tr}(L^i)=0$ for all $i=1,2,\ldots,2^n-1$ and $L^{2^n}=I_{2^n}$.

Proof. (Sufficiency) If $\mathrm{tr}(L^i)=0$ for all $i=1,2,\ldots,2^n-1$ and $L^{2^n}=I_{2^n}$, then according to Lemma 2, we have $N_1=N_2=\cdots=N_{2^n-1}=0$ and $\mathrm{tr}(L^{2^n})=2^n$. Hence, according to Lemma 2 again, we have $N_{2^n}=1$. So this Galois NFSR has a cycle of length 2^n in its state diagram.

(Necessary) Note that an n-stage Galois NFSR has totally 2^n possible states. Thus, if an n-stage nonsingular Galois NFSR has a cycle of length 2^n in its state diagram, we can get $N_1=N_2=\cdots=N_{2^n-1}=0$ and $N_{2^n}=1$. According to Lemma 2, we have $\mathrm{tr}(L^i)=0$ for all $i=1,2,\ldots,2^n-1$ and $\mathrm{tr}(L^{2^n})=2^n$. Together considering $L\in\mathcal{L}_{2^n\times 2^n}$, we can deduce that $L^{2^n}=I_{2^n}$.

Lemma 10 gives a necessary and sufficient condition for a Galois NFSR with maximum length cycle in its state diagram. In the following, we present a sufficient condition for the observability of such Galois NFSRs.

Theorem 7. If an n-stage Galois NFSR has a cycle of length 2^n in its state diagram and its state transition matrix $L=\delta_{2^n}[r_1\ r_2\ \cdots\ r_{2^n}]$ satisfies only one element of $\{r_1,r_2,\ldots,r_{2^{n-1}}\}$ is in $\{2^{n-1}+1,2^{n-1}+2,\ldots,2^n\}$ and only one element of $\{r_{2^{n-1}+1},r_{2^{n-1}+2},\ldots,r_{2^n}\}$ is in $\{1,2,\ldots,2^{n-1}\}$, then this Galois NFSR is observable.

Proof. Since only one of the first 2^{n-1} columns of L takes the value from $\{\delta_{2^n}^{2^{n-1}+1},\delta_{2^n}^{2^{n-1}+2},\ldots,\delta_{2^n}^{2^n}\}$, it means over $\mathbb{F}_2^n$ only one state whose first component is 1 is updated to a state whose first component is 0. By the same reasoning, we have only one state whose first component is 0 is updated to a state $\boldsymbol{S}_1$ whose first component is 1. Since this Galois NFSR has a cycle of length 2^n, we can get all states with their first components of 1 except for the state $\boldsymbol{S}_1$ and all states with their first components of 0 are concatenated, respectively. If we choose $\boldsymbol{S}_1$ as the initial state, then we have $\mathrm{Row}_1({}^c\mathcal{O}_1^*)=[1\ 1\ \cdots\ 1\ 1\ 0\ 0\ \cdots\ 0\ 0]$, which has 2^{n-1} entries of 1 and 2^{n-1} entries of 0. Moreover, according to the shift property described in (15) for the new observability matrix $\mathcal{O}_N^*$, we can get $\mathrm{Row}_2({}^c\mathcal{O}_2^*)=[1\ 1\ \cdots\ 1\ 0\ 0\ 0\ \cdots\ 0\ 1]$. We can see that $\mathrm{Col}_{2^{n-1}}(\mathcal{O}_2^*)$ and $\mathrm{Col}_{2^n}(\mathcal{O}_2^*)$ are new distinct columns. Similarly, we get $\mathrm{Col}_{2^{n-1}-1}(\mathcal{O}_3^*)$ and $\mathrm{Col}_{2^n-1}(\mathcal{O}_3^*)$ are new distinct columns at the second iteration. Keeping the same reasoning, we can obtain that this Galois NFSR's observability matrix $\mathcal{O}_k^*$ keeps $\mathcal{N}_{k+1}-\mathcal{N}_k=2$ for all positive integer k satisfying $\mathcal{N}_k<2^n$. Thus, according to Theorem 5, we can infer that this Galois NFSR is observable.

Example 4. Consider a 3-stage Galois NFSR with feedback $\boldsymbol{f}=[f_1\ \ f_2\ \ f_3]^{\mathrm{T}}$ satisfying

$$\begin{cases} f_1 = x_1\oplus x_2\oplus x_3\oplus x_2x_3\oplus 1, \\ f_2 = x_2\oplus x_3\oplus 1, \\ f_3 = x_3\oplus 1. \end{cases}$$

We can easily obtain its state diagram consisting of only one cycle:

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

Hence, the Galois NFSR can only produce a sequence 11110000 of period 8. Therefore, according to our

construction, we can easily get the new observability matrix is

$$\mathcal{O}_4^* = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix},$$

which has 8 distinct columns. Hence, the Galois NFSR is observable. On the other hand, according to the state diagram of the Galois NFSR, we can obtain the state transition matrix of the Galois NFSR as $L = \delta_8[2 \;\; 3 \;\; 4 \;\; 5 \;\; 6 \;\; 7 \;\; 8 \;\; 1]$. It satisfies the conditions of Theorem 7, so this Galois NFSR is observable, consistent with the above conclusion drawn by the new observability matrix $\mathcal{O}_4^*$.

Remark 3. This paper establishes a series of criteria for the observability of Galois NFSRs. First, using the original observability matrix, Proposition 1 and Theorems 2–4 provide some sufficient conditions for observable or unobservable Galois NFSRs from the perspective of state transition matrix that actually requires high computational complexity. Nevertheless, Theorem 1 gives a sufficient condition for observable Galois NFSRs from the perspective of feedback, which can be directly used for observability determination. Second, using our proposed new observability matrix, from the viewpoint of state transition matrix, Theorems 5 and 6 provide two necessary and sufficient conditions for the observability of Galois NFSRs, while Theorem 7 presents a sufficient condition for observable Galois NFSRs. In particular, Theorem 6 shows that Galois NFSRs need one step less than general Boolean networks to determine their observability.

5 Conclusion

In this paper, the method of the semi-tensor product-based Boolean network is used to study the observability of Galois NFSRs. We found a series of necessary and/or sufficient conditions for the observability of Galois NFSRs via the observability matrix introduced in the semi-tensor product-based Boolean network theory. Furthermore, a new observability matrix was established. The new observability matrix of a Galois NFSR is constructed by accumulating output sequences resulting from initial states on the same branch and its connected cycle into a block. As a result, adjacent columns/rows of each block of the new observability matrix have a shift property. Thanks to the convenience induced by the shift property, we obtained some new necessary and/or sufficient conditions for the observability of Galois NFSRs. The new observability matrix provides a promising approach to further study the observability of Galois NFSRs in future work.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61772029, 62172408, 61872359).

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 Babbage S, Dodd M. The MICKEY stream ciphers. In: New eStream Cipher Designs: The eSTREAM Finalists. Berlin: Springer-Verlag, 2008. 4986: 191–209
4 Wu H. ACORN: a lightweight authenticated cipher (v3). 2016. http://competitions.cr.yp.to/round3/acornv3.pdf
5 Dubrova E. A transformation from the fibonacci to the Galois NLFSRs. IEEE Trans Inform Theor, 2009, 55: 5263–5271
6 Kalouptsidis N, Limniotis K. Nonlinear span, minimal realizations of sequences over finite fields and de Brujin generators. In: Proceedings of International Symposium on Information Theory and Its Applications. Piscataway: IEEE Press, 2004. 794–799
7 Biryukov A. Weak keys. In: Encyclopedia of Cryptography and Security. Boston: Springer, 2005
8 Kauffman S A. Metabolic stability and epigenesis in randomly constructed genetic nets. J Theor Biol, 1969, 22: 437–467
9 Cheng D, Qi H, Zhao Y. An Introduction to Semi-Tensor Product of Matrices and Its Applications. Singapore: World Scientific Publishing Company, 2012
10 Cheng D, Qi H, Li Z. Analysis and Control of Boolean Networks. London: Springer-Verlag, 2011
11 Cheng D, Qi H. Controllability and observability of Boolean control networks. Automatica, 2009, 45: 1659–1667
12 Fornasini E, Valcher M E. Observability, reconstructibility and state observers of Boolean control networks. IEEE Trans Automat Contr, 2013, 58: 1390–1401
13 Laschov D, Margaliot M, Even G. Observability of Boolean networks: a graph-theoretic approach. Automatica, 2013, 49: 2351–2362
14 Zhang K, Zhang L. Observability of Boolean control networks: a unified approach based on finite automata. IEEE Trans Automat Contr, 2016, 61: 2733–2738

15 Cheng D, Li C, He F. Observability of Boolean networks via set controllability approach. Syst Control Lett, 2018, 115: 22–25
16 Guo Y, Gui W, Yang C. Redefined observability matrix for Boolean networks and distinguishable partitions of state space. Automatica, 2018, 91: 316–319
17 Yu Y, Meng M, Feng J. Observability of Boolean networks via matrix equations. Automatica, 2020, 111: 108621
18 Li H, Yang X, Wang S. Perturbation analysis for finite-time stability and stabilization of probabilistic Boolean networks. IEEE Trans Cybern, 2021, 51: 4623–4633
19 Li H, Yang X, Wang S. Robustness for stability and stabilization of boolean networks with stochastic function perturbations. IEEE Trans Automat Contr, 2021, 66: 1231–1237
20 Li R, Zhang Q, Chu T. Input-output-to-state stability of systems related through simulation relations. SIAM J Control Optim, 2021, 59: 614–634
21 Liu Z, Cheng D, Liu J. Pinning control of Boolean networks via injection mode. IEEE Trans Control Netw Syst, 2021, 8: 749–756
22 Jia G, Meng M, Lam J, et al. Further results for pinning stabilization of Boolean networks. IEEE Trans Control Netw Syst, 2021, 8: 897–905
23 Lu J, Liu R, Lou J, et al. Pinning stabilization of Boolean control networks via a minimum number of controllers. IEEE Trans Cybern, 2021, 51: 373–381
24 Gao S, Sun C, Xiang C, et al. Finite-horizon optimal control of Boolean control networks: a unified graph-theoretical approach. IEEE Trans Neural Netw Learn Syst, 2022, 33: 157–171
25 Toyoda M, Wu Y. Mayer-type optimal control of probabilistic Boolean control network with uncertain selection probabilities. IEEE Trans Cybern, 2021, 51: 3079–3092
26 Liu Z, Wang Y, Cheng D. Nonsingularity of feedback shift registers. Automatica, 2015, 55: 247–253
27 Zhong J, Lin D. Driven stability of nonlinear feedback shift registers with inputs. IEEE Trans Commun, 2016, 64: 2274–2284
28 Zhong J, Lin D. On minimum period of nonlinear feedback shift registers in grain-like structure. IEEE Trans Inform Theor, 2018, 64: 6429–6442
29 Lu J, Li M, Huang T, et al. The transformation between the Galois NLFSRs and the Fibonacci NLFSRs via semi-tensor product of matrices. Automatica, 2018, 96: 393–397
30 Lu J Q, Li B W, Zhong J. A novel synthesis method for reliable feedback shift registers via Boolean networks. Sci China Inf Sci, 2021, 64: 152207
31 Zhao X, Wang B, Zhu S, et al. On degeneracy problem of NFSRs via semi-tensor product. In: Proceedings of the 39th Chinese Control Conference, Shenyang, 2020. 146–151
32 Liu Z, Cheng D. Canonical form of Boolean networks. In: Proceedings of the 38th Chinese Control Conference, 2019. 1801–1806
33 Roger A H, Johnson C R. Topics in Matrix Analysis. Cambridge: Cambridge University Press, 1991
34 Qi H S, Cheng D Z. Logic and logic-based control. J Control Theor Appl, 2008, 6: 26–36
35 Golomb S W. Shift Register Sequences. Laguna Hills: Holden-Day, 1967