Frontiers of Information Technology & Electronic Engineering
www.jzus.zju.edu.cn; engineering.cae.cn; www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

On observability of Galois nonlinear feedback shift registers over finite fields*

Zhe GAO[1], Jun'e FENG[‡1], Yongyuan YU[1], Yanjun CUI[2]

[1]*School of Mathematics, Shandong University, Jinan 250100, China*

[2]*Department of Computer Science & Engineering, University of Minnesota Twin Cities, Minneapolis, MN 55455, USA*

E-mail: gaoz_0202@163.com; fengjune@sdu.edu.cn; yyyu@sdu.edu.cn; cui00022@umn.edu

Received May 24, 2022; Revision accepted Aug. 17, 2022; Crosschecked Sept. 7, 2022; Published online Sept. 28, 2022

Abstract: Observability ensures that any two distinct initial states can be uniquely determined by their outputs, so the stream ciphers can avoid unobservable nonlinear feedback shift registers (NFSRs) to prevent the occurrence of equivalent keys. This paper discusses the observability of Galois NFSRs over finite fields. Galois NFSRs are treated as logical networks using the semi-tensor product. The vector form of the state transition matrix is introduced, by which a necessary and sufficient condition is proposed, as well as an algorithm for determining the observability of general Galois NFSRs. Moreover, a new observability matrix is defined, which can derive a matrix method with lower computation complexity. Furthermore, the observability of two special types of Galois NFSRs, a full-length Galois NFSR and a nonsingular Galois NFSR, is investigated. Two methods are proposed to determine the observability of these two special types of NFSRs, and some numerical examples are provided to support these results.

Key words: Observability; Nonlinear feedback shift registers (NFSRs); Galois NFSRs; Semi-tensor product; Finite fields; Logical networks

https://doi.org/10.1631/FITEE.2200228 **CLC number:** O23

1 Introduction

As a pseudo-random sequence generator, feedback shift registers (FSRs) are widely used in many scenarios, such as classical stream ciphers, cryptographic systems, secure communication, delay measurement, and spread spectrum communication generators (Golomb, 1967; Hellebrand et al., 1995). In recent years, many studies have focused on FSRs, especially after the eSTREAM project in Europe (Aumasson et al., 2009; Deepthi and Sathidevi, 2009). From the perspective of feedback functions, FSRs can be divided into linear FSRs (LFSRs) and nonlinear FSRs (NFSRs). Originally, LFSRs have become the major block of several classical stream ciphers, error detection, and correction codes owing to their efficient implementation and outstanding cryptographic properties. However, due to the linear constraint among LFSR output signals (Meier and Staffelbach, 1989), at present NFSR design has gradually developed into an important stream cipher design method (Massey, 1969; Lai, 1987). From a structural point of view, NFSRs can be divided into Fibonacci NFSRs and Galois NFSRs. The feedback of Fibonacci NFSRs is applied only to the last bit, while the feedback of Galois NFSRs is applied to every bit. Due to the advantages of shorter propagation time and higher throughput (Dubrova, 2009), Galois NFSRs have been widely used and studied (Dubrova, 2010; Wang XJ et al., 2022). However, due to research tool limitation and complexity, the theory of Galois NFSRs has not been well established.

Observability is a fundamental property in

‡ Corresponding author

* Project supported by the National Natural Science Foundation of China (No. 61877036)

ORCID: Zhe GAO, https://orcid.org/0000-0002-9464-977X; Jun'e FENG, https://orcid.org/0000-0003-3881-3042

control theory, which can ensure that any two distinct initial states can be uniquely determined by their outputs. That is, starting from two distinct initial states, the NFSR does not produce two identical outputs. Limniotis et al. (2006, 2008) introduced the concept of observability into the research of sequence generators for the first time, and studied the linear complexity and the de Brujin generator problem accordingly. Zhao et al. (2021) investigated the equivalence transformation between Galois NFSRs and Fibonacci NFSRs based on observability. According to the definition of sequence generator observability, NFSR-based stream ciphers should avoid unobservable Galois NFSRs from the security viewpoint and select observable ones (Kong et al., 2022). Kong et al. (2022) investigated the observability of binary Galois NFSRs using a new observability matrix, but it cannot be applied directly to finite fields.

In recent years, a mathematical tool called the semi-tensor product of matrices has been developed, which can multiply two matrices with any dimensions (Cheng et al., 2011, 2012). As soon as the semi-tensor product of matrices came out, it was quickly applied to the study of Boolean networks (Wang B and Feng, 2019; Li YF and Zhu, 2020; Zheng and Feng, 2020; Zhong J et al., 2020; Shen et al., 2021; Yu et al., 2021; Zhang et al., 2021; Huang et al., 2022). A Boolean network is a finite state automaton that evolves through Boolean functions. Many recent works have treated an NFSR as a Boolean network because both are modeled as finite state automata, which is undoubtedly a good solution to the lack of research tools for NFSRs. For instance, NFSRs have been regarded as Boolean networks and many issues about NFSRs have been studied such as linearization representation (Zhong JH and Lin, 2015), stability (Zhong JH and Lin, 2016b), driven stability (Zhong JH and Lin, 2016a), the minimum period problem (Zhong JH and Lin, 2018), decomposition (Zhong JH and Lin, 2019a), and equivalence analysis (Zhong JH and Lin, 2019b). Lu and his team used the semi-tensor product method to study transformation between Galois NFSRs and Fibonacci NFSRs (Lu et al., 2018a), nonsingularity, reliability (Lu et al., 2018b, 2021), and other NFSR issues. Furthermore, in modern stream cipher algorithms, to consider software implementation, some research is now based on finite fields (Wang QY and Jin, 2013; Wang HY et al., 2017), which motivates us to study NFSRs over finite fields. On the other hand, a logical network, as an extension of a Boolean network that replaces the original binary values in the Boolean network with multi-values, is certainly a good research tool for studying NFSRs over finite fields.

In this work, we study the observability of Galois NFSRs over $\mathbb{F}_p$. Galois NFSRs are treated as logical networks using the semi-tensor product of matrices. We discuss the observability of general Galois NFSRs using two methods that are based on the state pair trajectory and a new observability matrix. Then we study two special types of Galois NFSRs, full-length Galois NFSRs and nonsingular Galois NFSRs. The main contributions can be summarized as follows:

1. For general Galois NFSRs, a vector form of the state transition matrix is introduced. An algorithm based on the vector form is proposed to draw the state pair trajectory table, by which a necessary and sufficient condition for the observability of this type of NFSR is obtained.

2. For general Galois NFSRs, another matrix method is proposed. Inspired by the work of Li R et al. (2014), a new observability matrix is defined, by which a necessary and sufficient condition with a lower computation complexity is derived.

3. For full-length Galois NFSRs, a simpler method is proposed to judge the observability according to the characteristic that the state transition graph has only one cycle, which can greatly narrow the scope of the research subjects for the first method in this paper. For nonsingular Galois NFSRs, a state pair transition diagram is defined to judge whether a nonsingular Galois NFSR is observable or not.

The notations used in this paper are shown in Table 1.

2 Preliminaries

In this section, some necessary information is introduced, including the definition and properties of the semi-tensor product and the algebraic expression of Galois NFSRs over finite fields.

2.1 Semi-tensor product of matrices

This subsection provides the definition and some properties of the semi-tensor product and the algebraic expression of logical networks.

Definition 1 (Roger and Johnson, 1991) Let $\boldsymbol{A} \in \mathbb{R}^{m\times n}$ and $\boldsymbol{B} \in \mathbb{R}^{p\times q}$. The Kronecker product

Table 1 Notations used in this paper

Notation	Definition
$\mathbb{N}$	Set of all nonnegative integers
$\mathbb{N}^+$	Set of all positive integers
$\mathbb{R}^{m\times n}$	Set of $m\times n$ real matrices
$\mathbb{F}_p$	Galois field of p elements
$\mathbb{F}_p^n$	Set of all n-dimensional vectors over $\mathbb{F}_p$
$\boldsymbol{I}_n$	Identity matrix of dimension n
$\boldsymbol{\delta}_n^i$	The i^{th} column of $\boldsymbol{I}_n$
Δ_p	$\{\boldsymbol{\delta}_p^i \mid i=1,2,\cdots,p\}$
Δ_p^n	Set of all n-dimensional vectors over Δ_p
$\mathcal{L}_{n\times r}$	Set of $n\times r$ logical matrices
mod	Modulo q division
$\mathrm{Col}_i(\boldsymbol{M})$	The i^{th} column of matrix $\boldsymbol{M}$
$\mathrm{Row}_i(\boldsymbol{M})$	The i^{th} row of matrix $\boldsymbol{M}$
$M_{(i,j)}$	Element of the i^{th} row and j^{th} column of matrix $\boldsymbol{M}$
C_n^m	Number of ways to select m numbers from n numbers
$\min\{a,b\}$	The minimum between a and b

of matrices $\boldsymbol{A}$ and $\boldsymbol{B}$ is defined as

$$\boldsymbol{A}\otimes\boldsymbol{B}=\begin{bmatrix} A_{(1,1)}\boldsymbol{B} & A_{(1,2)}\boldsymbol{B} & \cdots & A_{(1,n)}\boldsymbol{B}\\ A_{(2,1)}\boldsymbol{B} & A_{(2,2)}\boldsymbol{B} & \cdots & A_{(2,n)}\boldsymbol{B}\\ \vdots & \vdots & & \vdots\\ A_{(m,1)}\boldsymbol{B} & A_{(m,2)}\boldsymbol{B} & \cdots & A_{(m,n)}\boldsymbol{B}\end{bmatrix}.$$

Definition 2 (Cheng et al., 2011) Let $\boldsymbol{A}\in\mathbb{R}^{m\times n}$ and $\boldsymbol{B}\in\mathbb{R}^{p\times q}$. The semi-tensor product of matrices $\boldsymbol{A}$ and $\boldsymbol{B}$ is defined as

$$\boldsymbol{A}\ltimes\boldsymbol{B}:=(\boldsymbol{A}\otimes\boldsymbol{I}_{s/n})(\boldsymbol{B}\otimes\boldsymbol{I}_{s/p}),\tag{1}$$

where s is the least common multiple of n and p.

Without loss of generality, we usually omit "$\ltimes$" in the following for simplicity.

Definition 3 (Ljung and Sèoderstrèom, 1983) Let $\boldsymbol{A}\in\mathbb{R}^{m\times n}$ and $\boldsymbol{B}\in\mathbb{R}^{p\times n}$. The Khatri–Rao product of $\boldsymbol{A}$ and $\boldsymbol{B}$ is defined as an $mp\times n$-dimensional matrix, given by

$$\begin{aligned}\boldsymbol{A}*\boldsymbol{B}=&[\mathrm{Col}_1(\boldsymbol{A})\otimes\mathrm{Col}_1(\boldsymbol{B})\ \mathrm{Col}_2(\boldsymbol{A})\otimes\mathrm{Col}_2(\boldsymbol{B})\\ &\cdots\ \mathrm{Col}_n(\boldsymbol{A})\otimes\mathrm{Col}_n(\boldsymbol{B})].\end{aligned}\tag{2}$$

Lemma 1 (Cheng et al., 2011) Using the semi-tensor product of matrices, any logical function $f(X_1,X_2,\cdots,X_n)$ with $X_i\in\mathbb{F}_q$, $i=1,2,\cdots,n$, can be expressed in an equivalent form as

$$\boldsymbol{y}=f(\boldsymbol{x}_1,\boldsymbol{x}_2,\ldots,\boldsymbol{x}_n)=\boldsymbol{M}_f\ltimes_{i=1}^n\boldsymbol{x}_i,\tag{3}$$

where $\boldsymbol{x}_i,\ \boldsymbol{y}\in\Delta_q$, and $\boldsymbol{M}_f\in\mathcal{L}_{q\times q^n}$ is unique and is called the structural matrix of f.

A logical network with n nodes and m outputs over Δ_q can be expressed as

$$\begin{cases}\boldsymbol{x}_1(t+1)=g_1(\boldsymbol{x}_1(t),\boldsymbol{x}_2(t),\cdots,\boldsymbol{x}_n(t)),\\ \boldsymbol{x}_2(t+1)=g_2(\boldsymbol{x}_1(t),\boldsymbol{x}_2(t),\cdots,\boldsymbol{x}_n(t)),\\ \quad\vdots\\ \boldsymbol{x}_n(t+1)=g_n(\boldsymbol{x}_1(t),\boldsymbol{x}_2(t),\cdots,\boldsymbol{x}_n(t)),\\ \boldsymbol{y}_j(t)=h_j(\boldsymbol{x}_1(t),\boldsymbol{x}_2(t),\cdots,\boldsymbol{x}_n(t)),\end{cases}\tag{4}$$

with $\boldsymbol{x}_i(t)\in\Delta_q$ $(i=1,2,\cdots,n)$, $\boldsymbol{y}_j(t)\in\Delta_q$ $(j=1,2,\cdots,m)$, $g_i:\Delta_q^n\to\Delta_q$, and $h_j:\Delta_q^m\to\Delta_q$. Let $\boldsymbol{G}_i$ and $\boldsymbol{H}_j$ be the structural matrices of g_i and h_j, respectively. Denote $\boldsymbol{x}(t)=\ltimes_{i=1}^n\boldsymbol{x}_i(t)$ and $\boldsymbol{y}(t)=\ltimes_{j=1}^m\boldsymbol{y}_j(t)$. Then we have $\boldsymbol{x}_i(t+1)=\boldsymbol{G}_i\boldsymbol{x}(t)$ by Lemma 1. We can obtain an equivalent linear form (Cheng et al., 2012) as

$$\begin{aligned}\boldsymbol{x}(t+1)&=\boldsymbol{F}\boldsymbol{x}(t),\\ \boldsymbol{y}(t)&=\boldsymbol{H}\boldsymbol{x}(t),\end{aligned}$$

with

$$\boldsymbol{F}=\boldsymbol{G}_1*\boldsymbol{G}_2*\cdots*\boldsymbol{G}_n\in\mathcal{L}_{q^n\times q^n}$$

being the state transition matrix.

2.2 Algebraic expression of Galois NFSRs

In an n-stage Galois NFSR over $\mathbb{F}_p$, there are n storage devices represented by small square nodes in Fig. 1. The content of node i at time t is denoted as $X_i(t)$, $i=1,2,\cdots,n$. The state of the Galois NFSR at time t is denoted by $\boldsymbol{X}(t)=(X_1(t),X_2(t),\cdots,X_n(t))^{\mathrm{T}}$. Each node i is subject to a feedback function $f_i:\mathbb{F}_p^n\to\mathbb{F}_p$. The feedback function of the Galois NFSR is denoted by $\boldsymbol{f}=(f_1,f_2,\cdots,f_n)^{\mathrm{T}}$. Then the state updating

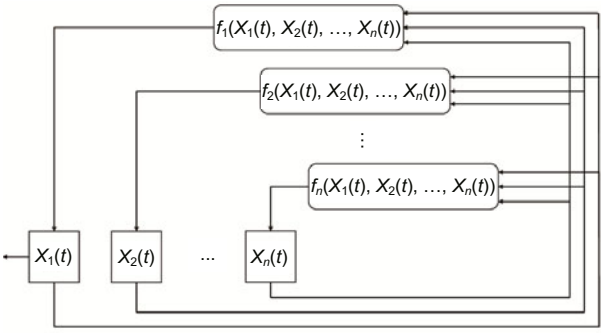

Fig. 1 Diagram of an n-stage Galois nonlinear feedback shift register (NFSR)

transformation from $\boldsymbol{X}(t)$ to $\boldsymbol{X}(t+1)$ can be expressed as a nonlinear system:

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

Let $p-i \sim \boldsymbol{\delta}_p^i$, where $p-i \in \mathbb{F}_p$ and $\boldsymbol{\delta}_p^i \in \Delta_p$, $i = 1, 2, \ldots, p$; for example, $0 \sim \boldsymbol{\delta}_p^p$ and $1 \sim \boldsymbol{\delta}_p^{p-1}$. In the following, we say a variable $X \in \mathbb{F}_p$ is in a scalar form, and say the corresponding variable $\boldsymbol{x} \in \Delta_p$ is in a vector form. For instance, the vector form of $X_i(t)$ is $\boldsymbol{x}_i(t)$. Using the vector form, logical function f_i is changed to $f_i : \Delta_p^n \to \Delta_p$. Then Eq. (5) can be regarded as a logical network and can be equivalently expressed as a linear form using the semi-tensor product:

$$\boldsymbol{x}(t+1) = \boldsymbol{L}\boldsymbol{x}(t), \tag{6}$$

where $\boldsymbol{x}(t) = \ltimes_{i=1}^n \boldsymbol{x}_i(t) \in \Delta_{p^n}$, and $\boldsymbol{L} \in \mathcal{L}_{p^n \times p^n}$ is called the state transition matrix of the Galois NFSR.

The state $\boldsymbol{x}(0)$ from which the Galois NFSR starts its work is called the initial state. The output at each moment is $\boldsymbol{y}(t) = \boldsymbol{x}_1(t)$. Hence, the output sequence generated by an n-stage Galois NFSR is $\boldsymbol{x}_1(0), \boldsymbol{x}_1(1), \boldsymbol{x}_1(2), \cdots$. Due to the output characteristics of the Galois NFSR, the form of the output matrix can be obtained:

$$\boldsymbol{H} = \boldsymbol{\delta}_p[\underbrace{1 \cdots 1}_{p^{n-1}} \ \underbrace{2 \cdots 2}_{p^{n-1}} \ \cdots \ \underbrace{p \cdots p}_{p^{n-1}}].$$

Definition 4 A directed graph consisting of p^n nodes and p^n directed edges is called the state transition diagram (ST-diagram) of an n-stage NFSR, if each of its nodes corresponds to a state of the NFSR, and each edge from state X to state Y means that X is shifted to Y.

Simultaneously, X is called a predecessor of Y, and Y is called the successor of X. Every state has a unique successor, but may have only one predecessor, several predecessors, or even no predecessor. A state without predecessors is called a starting state. A series of consecutive distinct states $\boldsymbol{x}_1, \boldsymbol{x}_2, \cdots, \boldsymbol{x}_q$ is called a cycle of length q if $\boldsymbol{x}_1$ is the successor of $\boldsymbol{x}_q$. Simultaneously, a series of consecutive distinct states $\boldsymbol{x}_1, \boldsymbol{x}_2, \cdots, \boldsymbol{x}_q$ is called a branch of length q if it satisfies the following three conditions: (1) none lies on a cycle, (2) $\boldsymbol{x}_1$ is a starting state, and (3) the successor of $\boldsymbol{x}_q$ is on a cycle.

3 Observability criteria for Galois NFSRs over finite fields

3.1 Observability determining for general Galois NFSRs via a trajectory table method

Observability means that the initial state can be uniquely determined by the output sequence. From another point of view, observability can also be defined as the distinguishability of the output sequences. The relevant definition is as follows:

Definition 5 (1) Two initial states $\boldsymbol{x}_0, \boldsymbol{x}_0' \in \Delta_{p^n}$ ($\boldsymbol{x}_0 \neq \boldsymbol{x}_0'$) are said to be indistinguishable if their corresponding output sequences are equal (Fornasini and Valcher, 2013). Otherwise, the two distinct initial states are said to be distinguishable.

(2) A Galois NFSR is said to be observable if every two distinct initial states are distinguishable.

Consider an n-stage Galois NFSR over $\mathbb{F}_p$. Let $\boldsymbol{L}$ be the state transition matrix of this Galois NFSR, denoted by

$$\boldsymbol{L} = \boldsymbol{\delta}_{p^n}[\alpha_1 \ \alpha_2 \cdots \alpha_{p^n}] \in \mathcal{L}_{p^n \times p^n},$$
$$\alpha_i \in \{1, 2, \cdots, p^n\}, \ i = 1, 2, \cdots, p^n.$$

Define a new matrix based on $\boldsymbol{L}$, called the vector form of matrix $\boldsymbol{L}$, as

$$\boldsymbol{V}_{\boldsymbol{L}} = [\alpha_1 \ \alpha_2 \cdots \alpha_{p^n}]. \tag{7}$$

A Galois NFSR can be determined uniquely by its state transition matrix $\boldsymbol{L}$, and naturally, it can also be uniquely determined by its vector form $\boldsymbol{V}_{\boldsymbol{L}}$. $\mathrm{Col}_i(\boldsymbol{V}_{\boldsymbol{L}}) = \alpha_i$ means that the successor of state $\boldsymbol{\delta}_{p^n}^i$ is $\boldsymbol{\delta}_{p^n}^{\alpha_i}$. This process can be expressed by a mapping $\varphi : \{1, 2, \cdots, p^n\} \to \{1, 2, \cdots, p^n\}$, specifically, $1 \to \alpha_1, \ 2 \to \alpha_2, \ \cdots, \ p^n \to \alpha_{p_n}$.

We define some sets that will be used later as follows:

(1) The set of all distinct state pairs of an n-stage Galois NFSR over $\mathbb{F}_p$ is denoted by

$$\Phi = \{(\boldsymbol{\delta}_{p^n}^i, \boldsymbol{\delta}_{p^n}^j) | 1 \leq i < j \leq p^n\}. \tag{8}$$

(2) The set of all indistinguishable initial state pairs is denoted by

$$\Omega = \{(\boldsymbol{\delta}_{p^n}^i, \boldsymbol{\delta}_{p^n}^j) | (k-1)p^{n-1} + 1 \leq i < j \leq kp^{n-1}, \ k = 1, 2, \cdots, p\}.$$

(3) The set of all distinguishable initial state pairs is denoted by $\Phi\backslash\Omega$, whose elements are in Φ but not in Ω.

Because the number of states of an FSR is finite, the number of state pairs composed of distinct states is also finite. The set Φ contains all distinct state pairs of an n-stage Galois NFSR, where the order of the states in each state pair is not considered; that is, (a,b) and (b,a) are counted as the same state pairs. Obviously, the number of elements in Φ is

$$|\Phi| = \mathrm{C}_{p^n}^2 = \frac{p^{2n}-p^n}{2}.$$

On the other hand, Ω is derived from the properties of the output matrix $\boldsymbol{H}$. We can easily see from $\boldsymbol{H}$ that the outputs corresponding to states $\boldsymbol{\delta}_{p^n}^1, \boldsymbol{\delta}_{p^n}^2, \cdots, \boldsymbol{\delta}_{p^n}^{p^{n-1}}$ are the same. Similarly, the outputs corresponding to states $\boldsymbol{\delta}_{p^n}^{p^{n-1}+1}, \boldsymbol{\delta}_{p^n}^{p^{n-1}+2}, \cdots, \boldsymbol{\delta}_{p^n}^{2p^{n-1}}$ are the same, and the latter states are also like this. As a result, the number of elements in Ω is

$$|\Omega| = p \cdot \mathrm{C}_{p^{n-1}}^2 = \frac{p^{2n-1}-p^n}{2}.$$

Clearly, we need only to consider whether the elements in Ω can reach $\Phi\backslash\Omega$ in finite steps. Accordingly, we can design an algorithm to judge whether the indistinguishable initial state pair can be distinguished after finite steps. The output of the algorithm is a state pair trajectory table, the first line of which contains all indistinguishable initial state pairs, and each successive line below is the state reached after each step of state transition.

In Algorithm 1, as the steps proceed, all state pairs in Ω may eventually enter two situations. One is to enter a cycle and never enter $\Phi\backslash\Omega$, which means that these state pairs will never be distinguished. The other is to enter set $\Phi\backslash\Omega$, which means that these indistinguishable initial state pairs can be distinguished after finite steps. The fourth and sixth steps correspond to the above two scenarios, which are shown in the state pair trajectory table by ending with an asterisk and a checkmark, respectively. Hence, the inner "while" loop statement will stop after at most $|\Omega|-1$ steps. Hence, the computation complexity of determining the observability for an n-stage Galois NFSR over $\mathbb{F}_p$ using Algorithm 1 is $O(|\Omega|(|\Omega|-1))$ in the worst case, where $|\Omega| = \frac{p^{2n-1}-p^n}{2}$.

Algorithm 1 Observability judgment of an n-stage Galois NFSR over $\mathbb{F}_p$

Require: the vector form of the state transition matrix of the Galois NFSR and its indistinguishable initial state set Ω

Ensure: a state pair trajectory table

```
k = 1
for all (δ^i_{p^n}, δ^j_{p^n}) ∈ Ω do
    while k ≠ 0 do
        if (φ(i), φ(j)) = (i, j) then
            R_k = ∗, k = 0
        else if (φ(i), φ(j)) ∈ Φ\Ω then
            R_k = √, k = 0
        else
            k = k + 1, (i, j) = (φ(i), φ(j))
        end if
    end while
end for
```

Theorem 1 An n-stage Galois NFSR is observable if and only if each column of the state pair trajectory table constructed by Algorithm 1 can reach $\Phi\backslash\Omega$.

Proof Because set Ω contains all indistinguishable initial state pairs, if all state pairs in Ω can reach the state pairs in $\Phi\backslash\Omega$ after finite steps, then all state pairs are distinguishable after finite steps. That is to say, the Galois NFSR is observable. On the other hand, if the Galois NFSR is observable, then all state pairs are distinguishable after finite steps. This means that all state pairs in Ω will reach $\Phi\backslash\Omega$, which demonstrates that each column of the state pair table constructed by Algorithm 1 ends with a checkmark.

Next, an example is presented to illustrate the effectiveness of Algorithm 1 as well as Theorem 1.

Example 1 Consider a two-stage Galois NFSR over $\mathbb{F}_3$ with the state transition matrix

$$\boldsymbol{L} = \boldsymbol{\delta}_9[2\ 3\ 4\ 5\ 7\ 9\ 1\ 2\ 3]$$

and output matrix

$$\boldsymbol{H} = \boldsymbol{\delta}_3[1\ 1\ 1\ 2\ 2\ 2\ 3\ 3\ 3].$$

The vector form of $\boldsymbol{L}$ and the corresponding mapping are

$$\boldsymbol{V}_{\boldsymbol{L}} = [2\ 3\ 4\ 5\ 7\ 9\ 1\ 2\ 3],$$

$$\varphi(1)=2,\ \varphi(2)=3,\ \varphi(3)=4,\ \varphi(4)=5,$$

$$\varphi(5)=7,\ \varphi(6)=9,\ \varphi(7)=1,\ \varphi(8)=2,\ \varphi(9)=3.$$

By the features of $\boldsymbol{H}$, the indistinguishable initial set is

$$\begin{aligned}\Omega =&\{(\boldsymbol{\delta}_9^1,\boldsymbol{\delta}_9^2),(\boldsymbol{\delta}_9^1,\boldsymbol{\delta}_9^3),(\boldsymbol{\delta}_9^2,\boldsymbol{\delta}_9^3),(\boldsymbol{\delta}_9^4,\boldsymbol{\delta}_9^5),(\boldsymbol{\delta}_9^4,\boldsymbol{\delta}_9^6),\\&(\boldsymbol{\delta}_9^5,\boldsymbol{\delta}_9^6),(\boldsymbol{\delta}_9^7,\boldsymbol{\delta}_9^8),(\boldsymbol{\delta}_9^7,\boldsymbol{\delta}_9^9),(\boldsymbol{\delta}_9^8,\boldsymbol{\delta}_9^9)\}.\end{aligned}$$

Using the above information, we can draw the state pair trajectory table constructed by Algorithm 1 in Table 2. As we can see from Table 2, each column ends with a checkmark, which implies that each column of the state pair trajectory table constructed by Algorithm 1 can reach $\Phi\backslash\Omega$. Consequently, this Galois NFSR is observable by Theorem 1.

Table 2 State pair trajectory table of Galois NFSR in Example 1

Step	Indistinguishable initial state pair								
	(1,2)	(1,3)	(2,3)	(4,5)	(4,6)	(5,6)	(7,8)	(7,9)	(8,9)
R_1	(2,3)	√	√	√	√	(7,9)	(1,2)	(1,3)	(2,3)
R_2	√					(1,3)	(2,3)	√	√
R_3						√	√		

Next, we analyze the method in Kong et al. (2022) to illustrate the simplicity of our method. If we use the observability matrix method in Kong et al. (2022), we first need to calculate

$$\begin{aligned}\boldsymbol{HL}&=\boldsymbol{\delta}_3[1\ 1\ 2\ 2\ 3\ 3\ 1\ 1\ 1],\\ \boldsymbol{HL}^2&=\boldsymbol{\delta}_3[1\ 2\ 2\ 3\ 1\ 1\ 1\ 1\ 2],\\ \boldsymbol{HL}^3&=\boldsymbol{\delta}_3[2\ 2\ 3\ 1\ 1\ 2\ 1\ 2\ 2],\end{aligned}$$

to obtain the observability matrix:

$$\boldsymbol{\mathcal{O}}_4=\begin{bmatrix}1&1&1&0&0&0&0&0&0\\0&0&0&1&1&1&0&0&0\\0&0&0&0&0&0&1&1&1\\1&1&0&0&0&0&1&1&1\\0&0&1&1&0&0&0&0&0\\0&0&0&0&1&1&0&0&0\\1&0&0&0&1&1&1&1&0\\0&1&1&0&0&0&0&0&1\\0&0&0&1&0&0&0&0&0\\0&0&0&1&1&0&1&0&0\\1&1&0&0&0&1&0&1&1\\0&0&1&0&0&0&0&0&0\end{bmatrix}.$$

Then we need to verify that each column of $\boldsymbol{\mathcal{O}}_4$ is different in pairs. Intuitively, our approach is simpler than the observability matrix method in Kong et al. (2022). Moreover, Kong et al. (2022) proposed a matrix $\boldsymbol{\mathcal{O}}_N^\sharp$ formed by the odd rows of the observability matrix $\boldsymbol{\mathcal{O}}_N$ and another new observability matrix by exchanging the order of the columns of matrix $\boldsymbol{\mathcal{O}}_N^\sharp$. However, these two methods cannot be applied directly to Galois NFSRs over finite fields.

3.2 Observability determining for general Galois NFSRs via a matrix method

This subsection presents another method, called the matrix method, for determining the observability for general Galois NFSRs over a finite field. This method is inspired by the work of Li R et al. (2014), and we improve it significantly by reducing the computation complexity. First, we give a lemma that will be used later:

Lemma 2 For any integers $a_i,b_i\in\{1,2,\cdots,p\}$, $i=0,1,\cdots,k$, we have

$$a_0+pa_1+p^2a_2+\cdots+p^ka_k=b_0+pb_1+\cdots+p^kb_k,\quad(9)$$

if and only if

$$(a_0,a_1,\cdots,a_k)=(b_0,b_1,\cdots,b_k).$$

Proof We prove only the necessity because the sufficiency is obvious. Performing the modulo operation on both sides of Eq. (9) at the same time, we have

$$\begin{aligned}&(a_0+pa_1+p^2a_2+\cdots+p^ka_k)\bmod p\\=&(b_0+pb_1+p^2b_2+\cdots+p^kb_k)\bmod p,\end{aligned}\quad(10)$$

and we can obtain $a_0=b_0$. Then Eq. (9) can be simplified to

$$\begin{aligned}&a_1+pa_2+p^2a_3\cdots+p^{k-1}a_k\\=&b_1+pb_2+p^2b_3\cdots+p^{k-1}b_k.\end{aligned}\quad(11)$$

Continue to perform the same modulo operation on Eq. (11), and we can find that $a_i=b_i$ holds for all $i=0,1,\cdots,k$.

Denote the state transition matrix and the output matrix of the n-stage Galois NFSR as

$$\begin{aligned}\boldsymbol{L}&=\boldsymbol{\delta}_{p^n}[\alpha_1\ \alpha_2\ldots\alpha_{p^n}],\\ \boldsymbol{H}&=\boldsymbol{\delta}_p[\underbrace{1\cdots1}_{p^{n-1}}\ \underbrace{2\cdots2}_{p^{n-1}}\ \cdots\ \underbrace{p\cdots p}_{p^{n-1}}],\end{aligned}$$

where $\alpha_i\in\{1,2,\cdots,p^n\}$. Define

$$\boldsymbol{M}_0=[\underbrace{1\cdots1}_{p^{n-1}}\ \underbrace{2\cdots2}_{p^{n-1}}\ \cdots\ \underbrace{p\cdots p}_{p^{n-1}}]^{\mathrm{T}},$$

and

$$\boldsymbol{M}_{k+1}=[\mathrm{Row}_{\alpha_1}(\boldsymbol{M}_k)\,\mathrm{Row}_{\alpha_2}(\boldsymbol{M}_k)\,\cdots\,\mathrm{Row}_{\alpha_{p^n}}(\boldsymbol{M}_k)]^{\mathrm{T}},$$

where $k>0$. It is easy to see that $\mathrm{Row}_i(\boldsymbol{M}_k)$ represents the output of state $\boldsymbol{\delta}_{p^n}^i$ at the k^{th} step.

Define

$$\boldsymbol{Q}_l=\sum_{k=0}^{l}p^k\boldsymbol{M}_k,\ l=0,1,2,\cdots,$$

which is called the new observability matrix. Note that $\boldsymbol{Q}_l$ is a p^n-dimensional column vector and the element of each row is an integer. The i^{th} row represents the integration of the output sequence of the first l steps of state $\boldsymbol{\delta}_{p^n}^i$. Through the above analysis, we can draw the following conclusion:

Theorem 2 An n-stage Galois NFSR is observable if and only if there exists an integer $l\in\mathbb{N}$ such that the corresponding new observability matrix $\boldsymbol{Q}_l$ has p^n distinct rows. Moreover, if such an l exists, and the smallest l is denoted as l^*, then $l^*\le\min\{p^n-p,\frac{p^{2n-1}-p^n}{2}\}$ must hold.

Proof We abbreviate $\mathrm{Row}_i(\boldsymbol{M}_k)$ as r_k^i. According to the previous analysis, the i^{th} row and the j^{th} row of $\boldsymbol{Q}_l$ are $r_0^i+pr_1^i+p^2r_2^i+\cdots+p^lr_l^i$ and $r_0^j+pr_1^j+p^2r_2^j+\cdots+p^lr_l^j$, respectively.

First, we assume that there exists an integer $l\in\mathbb{N}$ such that $\boldsymbol{Q}_l$ has p^n distinct rows. That is, for any distinct $i,j\in\{1,2,\cdots,p^n\}$, we have

$$\begin{aligned}&r_0^i+pr_1^i+p^2r_2^i+\cdots+p^lr_l^i\\ \neq&r_0^j+pr_1^j+p^2r_2^j+\cdots+p^lr_l^j.\end{aligned}$$

By the inverse negation of Lemma 2,

$$(r_0^i,r_1^i,\cdots,r_l^i)\neq(r_0^j,r_1^j,\cdots,r_l^j)$$

holds for any distinct $i,j\in\{1,2,\cdots,p^n\}$. Therefore, for any distinct initial states $\boldsymbol{\delta}_{p^n}^i$, $\boldsymbol{\delta}_{p^n}^j$, the corresponding output sequences are different after l steps, which implies that this n-stage Galois NFSR is observable.

Next, we assume that the n-stage Galois NFSR is observable. Any distinct initial states $\boldsymbol{\delta}_{p^n}^i$, $\boldsymbol{\delta}_{p^n}^j$ can be distinguished after finite steps. Assume that the finite step number is l. Then the output sequences corresponding to distinct initial states are different after l steps. Hence, $\boldsymbol{Q}_l$ has p^n distinct rows.

Moreover, we assume that integer $l^*\in\mathbb{N}$ is the smallest integer such that the corresponding new observability matrix $\boldsymbol{Q}_{l^*}$ has p^n distinct rows. Because any two distinct initial states can be distinguished within $|\Omega|-1$ steps or never be distinguished, where $|\Omega|=\frac{p^{2n-1}-p^n}{2}$, it is obvious that $l^*\le\frac{p^{2n-1}-p^n}{2}$ holds. Next, we prove $l^*\le p^n-p$. If two states $\boldsymbol{x}_1$ and $\boldsymbol{x}_2$ are indistinguishable in k steps, we denote this as an equivalent relation $\boldsymbol{x}_1\sim_k\boldsymbol{x}_2$. The equivalent relation "$\sim_k$" can partition Δ_{p^n} into disjoint classes. Let $\tilde{\Lambda}_k$ be the set of such equivalent classes. It is obvious that these sets satisfy the following three conditions:

(1) $|\tilde{\Lambda}_0|=p$;

(2) $|\tilde{\Lambda}_0|\le|\tilde{\Lambda}_1|\le|\tilde{\Lambda}_2|\le\cdots$;

(3) if for some $k\in\mathbb{N}^+$, $|\tilde{\Lambda}_k|=|\tilde{\Lambda}_{k+1}|$, then $\tilde{\Lambda}_k=\tilde{\Lambda}_{k+1}$ and $\tilde{\Lambda}_k=\tilde{\Lambda}_{k+l}$ hold for any $l\in\mathbb{N}^+$.

From the above conditions, it can be known that if $\tilde{\Lambda}_k$ is strictly increasing as k increases, then $|\tilde{\Lambda}_k|\ge k+p$. However, $|\tilde{\Lambda}_k|\le p^n$ must hold. That deduces $k+p\le p^n$, i.e., $k\le p^n-p$, which guarantees that $|\tilde{\Lambda}_{p^n-p}|=|\tilde{\Lambda}_{p^n-p+1}|$. This means that if two states are indistinguishable in p^n-p steps, then they will never be indistinguishable. This corresponds to the condition in the theorem that $l^*\le p^n-p$.

The current matrix method is a great improvement on the method in Li R et al. (2014). We need only to compare p^n integers, avoiding the discussion of the pairwise distinctness among rows of a $p^n\times(l+1)$-dimensional matrix, whose elements are coefficients of polynomials. In addition, this matrix method has a lower computation complexity than that of the trajectory table method in Section 3.1. Specifically, Theorem 2 has found an upper bound for l^*, and l^* takes $\min\{p^n-p,\frac{p^{2n-1}-p^n}{2}\}$ in the worst case. $\boldsymbol{Q}_{l^*}$ has p^n rows and the element of each row is an integer. Thus, taking the iteration of the matrix into account, the computation complexity of determining observability for an n-stage Galois NFSR over $\mathbb{F}_p$ using the new observability matrix is $O(p^nl^*)$ in the worst case, where $l^*=\min\{p^n-p,\frac{p^{2n-1}-p^n}{2}\}$. Next, we illustrate this with the previous example.

Example 2 Continue to consider the Galois NFSR in Example 1. According to the analysis in this subsection, we calculate

$$\begin{aligned}\boldsymbol{M}_0&=\begin{bmatrix}1&1&1&2&2&2&3&3&3\end{bmatrix}^{\mathrm{T}},\\ \boldsymbol{M}_1&=\begin{bmatrix}1&1&2&2&3&3&1&1&1\end{bmatrix}^{\mathrm{T}},\\ \boldsymbol{M}_2&=\begin{bmatrix}1&2&2&3&1&1&1&1&2\end{bmatrix}^{\mathrm{T}},\\ \boldsymbol{M}_3&=\begin{bmatrix}2&2&3&1&1&2&1&2&2\end{bmatrix}^{\mathrm{T}}.\end{aligned}$$

Hence, we have

$$\boldsymbol{Q}_4 = \begin{bmatrix} 1+3\times1+9\times1+27\times2 \\ 1+3\times1+9\times2+27\times2 \\ 1+3\times2+9\times2+27\times3 \\ 2+3\times2+9\times3+27\times1 \\ 2+3\times3+9\times1+27\times1 \\ 2+3\times3+9\times1+27\times2 \\ 3+3\times1+9\times1+27\times1 \\ 3+3\times1+9\times1+27\times2 \\ 3+3\times1+9\times2+27\times2 \end{bmatrix} = [67\ 76\ 106\ 62\ 47\ 74\ 42\ 69\ 78]^{\mathrm{T}}. \tag{12}$$

As we can see, $\boldsymbol{Q}_4$ has nine distinct rows. By Theorem 2, this Galois NFSR is observable. This method is simpler than the method in Example 1, whereas the advantage of Example 1 is that the trajectory table method looks more intuitive and is easier to understand.

3.3 Observability determining for two special types of Galois NFSRs

The methods in the previous subsections obviously can be used to determine the observability of full-length Galois NFSRs and nonsingular Galois NFSRs because they are two special types of general Galois NFSRs, but there exist simpler methods for these two special types. This subsection will consider simpler methods for determining the observability of full-length Galois NFSRs and nonsingular Galois NFSRs.

3.3.1 Full-length Galois NFSRs

First, we introduce the definition of a full-length Galois NFSR:

Definition 6 An n-stage Galois NFSR over $\mathbb{F}_p$ is called a full-length Galois NFSR if its ST-diagram consists only of a cycle of length p^n.

To make the method simpler, a set is defined as

$$P_i = \left\{(\boldsymbol{\delta}^i_{p^n}, \boldsymbol{L}\boldsymbol{\delta}^i_{p^n}), (\boldsymbol{\delta}^i_{p^n}, \boldsymbol{L}^2\boldsymbol{\delta}^i_{p^n}), \cdots, (\boldsymbol{\delta}^i_{p^n}, \boldsymbol{L}^{\lfloor \frac{p^n}{2} \rfloor}\boldsymbol{\delta}^i_{p^n})\right\}, \tag{13}$$

where $\lfloor \frac{p^n}{2} \rfloor$ represents the largest integer no larger than $\frac{p^n}{2}$. Then the following result can be obtained:

Theorem 3 For an n-stage full-length Galois NFSR over $\mathbb{F}_p$, $\boldsymbol{L}$ is the state transition matrix of this Galois NFSR. Then the Galois NFSR is observable if and only if there exists $i \in \{1, 2, \cdots, p^n\}$, such that the state pairs in $P_i \cap \Omega$ can be distinguished.

Proof (Necessity) If the Galois NFSR is observable, then all state pairs are distinguishable. Obviously, the state pairs in $P_i \cap \Omega$ can also be distinguished.

(Sufficiency) First we consider the case where p^n is even. The fact that $(\boldsymbol{\delta}^i_{p^n}, \boldsymbol{L}\boldsymbol{\delta}^i_{p^n})$ is distinguishable implies that $(\boldsymbol{L}\boldsymbol{\delta}^i_{p^n}, \boldsymbol{L}^2\boldsymbol{\delta}^i_{p^n})$, $(\boldsymbol{L}^2\boldsymbol{\delta}^i_{p^n}, \boldsymbol{L}^3\boldsymbol{\delta}^i_{p^n}), \cdots, (\boldsymbol{L}^{p^n-1}\boldsymbol{\delta}^i_{p^n}, \boldsymbol{\delta}^i_{p^n})$ are all distinguishable. This is because the ST-diagram of the NFSR has only one cycle, and these state pairs will reach $(\boldsymbol{\delta}^i_{p^n}, \boldsymbol{L}\boldsymbol{\delta}^i_{p^n})$ after an appropriate number of steps, i.e.,

$$\begin{aligned} &\left(\boldsymbol{\delta}^i_{p^n}, \boldsymbol{L}\boldsymbol{\delta}^i_{p^n}\right) \to \left(\boldsymbol{L}\boldsymbol{\delta}^i_{p^n}, \boldsymbol{L}^2\boldsymbol{\delta}^i_{p^n}\right) \to \left(\boldsymbol{L}^2\boldsymbol{\delta}^i_{p^n}, \boldsymbol{L}^3\boldsymbol{\delta}^i_{p^n}\right) \\ &\to \cdots \to \left(\boldsymbol{L}^{p^n-1}\boldsymbol{\delta}^i_{p^n}, \boldsymbol{\delta}^i_{p^n}\right) \to \left(\boldsymbol{\delta}^i_{p^n}, \boldsymbol{L}\boldsymbol{\delta}^i_{p^n}\right). \end{aligned}$$

At this point, we have verified that there are p^n distinct state pairs that are distinguishable. Similarly, for any $j = 1, 2, \cdots, \frac{p^n}{2}-1$, the fact that $(\boldsymbol{\delta}^i_{p^n}, \boldsymbol{L}^j\boldsymbol{\delta}^i_{p^n})$ is distinguishable can show that p^n distinct state pairs are distinguishable, which confirms that there are a total of $p^n(\frac{p^n}{2}-1)$ state pairs that are distinguishable. Moreover, The fact that $(\boldsymbol{\delta}^i_{p^n}, \boldsymbol{L}^{\frac{p^n}{2}}\boldsymbol{\delta}^i_{p^n})$ is distinguishable can show that $(\boldsymbol{L}\boldsymbol{\delta}^i_{p^n}, \boldsymbol{L}^{\frac{p^n}{2}+1}\boldsymbol{\delta}^i_{p^n})$, $(\boldsymbol{L}^2\boldsymbol{\delta}^i_{p^n}, \boldsymbol{L}^{\frac{p^n}{2}+2}\boldsymbol{\delta}^i_{p^n}), \cdots, (\boldsymbol{L}^{\frac{p^n}{2}-1}\boldsymbol{\delta}^i_{p^n}, \boldsymbol{L}^{p^n-1}\boldsymbol{\delta}^i_{p^n})$ can be distinguished, because

$$\begin{aligned} &(\boldsymbol{\delta}^i_{p^n}, \boldsymbol{L}^{\frac{p^n}{2}}\boldsymbol{\delta}^i_{p^n}) \to (\boldsymbol{L}\boldsymbol{\delta}^i_{p^n}, \boldsymbol{L}^{\frac{p^n}{2}+1}\boldsymbol{\delta}^i_{p^n}) \to \cdots \\ &\to (\boldsymbol{L}^{\frac{p^n}{2}-1}\boldsymbol{\delta}^i_{p^n}, \boldsymbol{L}^{p^n-1}\boldsymbol{\delta}^i_{p^n}) \to (\boldsymbol{L}^{\frac{p^n}{2}}\boldsymbol{\delta}^i_{p^n}, \boldsymbol{\delta}^i_{p^n}) \end{aligned}$$

without considering the order of two states in a state pair, and the number of these state pairs is $\frac{p^n}{2}$. We have shown that the number of state pairs that can be distinguished is

$$p^n\left(\frac{p^n}{2}-1\right) + \frac{p^n}{2} = \frac{p^{2n}-p^n}{2}.$$

Due to the characteristics of the full-length Galois NFSR, these $\frac{p^{2n}-p^n}{2}$ state pairs are indeed different, and they are exactly all the state pairs in set Φ. Thus, by the definition of observability, this Galois NFSR is observable.

When p^n is odd, $\lfloor \frac{p^n}{2} \rfloor = \frac{p^n-1}{2}$. Similarly, the fact that $(\boldsymbol{\delta}^i_{p^n}, \boldsymbol{L}\boldsymbol{\delta}^i_{p^n})$ is distinguishable implies that $(\boldsymbol{L}\boldsymbol{\delta}^i_{p^n}, \boldsymbol{L}^2\boldsymbol{\delta}^i_{p^n}), (\boldsymbol{L}^2\boldsymbol{\delta}^i_{p^n}, \boldsymbol{L}^3\boldsymbol{\delta}^i_{p^n}), \cdots, (\boldsymbol{L}^{p^n-1}\boldsymbol{\delta}^i_{p^n}, \boldsymbol{\delta}^i_{p^n})$ are all distinguishable. Actually, for any $j = 1, 2, \cdots, \frac{p^n-1}{2}$, the fact that $(\boldsymbol{\delta}^i_{p^n}, \boldsymbol{L}^j\boldsymbol{\delta}^i_{p^n})$ is distinguishable illustrates that p^n distinct state pairs are distinguishable. $p^n\left(\frac{p^n-1}{2}\right) = \frac{p^{2n}-p^n}{2}$ confirms that

there are a total of $\frac{p^{2n}-p^n}{2}$ state pairs that are distinguishable. Thus, by the definition of observability, this Galois NFSR is observable.

Theorem 3 actually narrows down the number of state pairs that we need to consider. In Section 3.1, we need to examine whether all state pairs in set Ω are distinguishable, and for full-length Galois NFSRs, Theorem 3 shows that we need only to judge whether all state pairs in set $P_i \cap \Omega$ are distinguishable. As for how to judge whether a state pair is distinguishable, we still use the method of Algorithm 1 in Section 3.1. Below we illustrate this with an example:

Example 3 Consider a three-stage Galois NFSR over $\mathbb{F}_3$ with state transition matrix

$$\boldsymbol{L} = \boldsymbol{\delta}_{27}[2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17\ 18\ 19\ 20\ 21\ 22\ 23\ 24\ 25\ 26\ 27\ 1],$$

and the corresponding vector form of $\boldsymbol{L}$ is

$$\boldsymbol{V_L} = [2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17\ 18\ 19\ 20\ 21\ 22\ 23\ 24\ 25\ 26\ 27\ 1].$$

The output matrix is

$$\boldsymbol{H} = \boldsymbol{\delta}_3[1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 2\ 2\ 2\ 2\ 2\ 2\ 2\ 2\ 2\ 3\ 3\ 3\ 3\ 3\ 3\ 3\ 3\ 3].$$

According to the state transition matrix, we can obtain the ST-diagram of this Galois NFSR in Fig. 2 (for convenience, we abbreviate state $\boldsymbol{\delta}_{27}^i$ as i in the figure). Through the ST-diagram, we know that this Galois NFSR is full-length because there is only a cycle with length 27.

By the analysis in the previous subsection, the set of indistinguishable initial state pairs is

$$\Omega = \{(\boldsymbol{\delta}_{27}^i, \boldsymbol{\delta}_{27}^j) | 9(k-1)+1 \le i < j \le 9k,\ k=1,2,3\}, \tag{14}$$

and the number of elements in Ω is

$$|\Omega| = 3 \times \mathrm{C}_9^2 = 108. \tag{15}$$

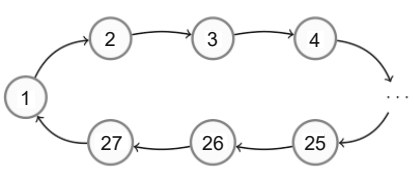

Fig. 2 ST-diagram of the Galois NFSR in Example 3

If we analyze the observability according to the method in the previous subsection, then we need to examine whether the 108 state pairs can be distinguished. However, because this is a full-length Galois NFSR, we can use Theorem 3. Considering $\lfloor \frac{3^3}{2} \rfloor = 13$, and

$$\begin{aligned} P_1 &= \left\{(\boldsymbol{\delta}_{27}^1, \boldsymbol{L}\boldsymbol{\delta}_{27}^1), (\boldsymbol{\delta}_{27}^1, \boldsymbol{L}^2\boldsymbol{\delta}_{27}^1), \cdots, (\boldsymbol{\delta}_{27}^1, \boldsymbol{L}^{13}\boldsymbol{\delta}_{27}^1)\right\} \\ &= \left\{(\boldsymbol{\delta}_{27}^1, \boldsymbol{\delta}_{27}^2), (\boldsymbol{\delta}_{27}^1, \boldsymbol{\delta}_{27}^3), \cdots, (\boldsymbol{\delta}_{27}^1, \boldsymbol{\delta}_{27}^{14})\right\}, \end{aligned}$$

we have

$$P_1 \cap \Omega = \left\{(\boldsymbol{\delta}_{27}^1, \boldsymbol{\delta}_{27}^2), (\boldsymbol{\delta}_{27}^1, \boldsymbol{\delta}_{27}^3), \cdots, (\boldsymbol{\delta}_{27}^1, \boldsymbol{\delta}_{27}^9)\right\}. \tag{16}$$

We need only to check whether these eight state pairs in $P_1 \cap \Omega$ can be distinguished.

Using Algorithm 1, we can construct Table 3, each column of which ends with a checkmark $\surd$. Hence, this Galois NFSR is observable by Theorem 3. The fact that these eight state pairs in $P_i \cap \Omega$ can be distinguished implies the following facts:

(1) The fact that $(\boldsymbol{\delta}_{27}^1, \boldsymbol{\delta}_{27}^2)$ can be distinguished means that $(\boldsymbol{\delta}_{27}^2, \boldsymbol{\delta}_{27}^3)$, $(\boldsymbol{\delta}_{27}^3, \boldsymbol{\delta}_{27}^4)$, $\cdots$, $(\boldsymbol{\delta}_{27}^{26}, \boldsymbol{\delta}_{\boldsymbol{27}}^{27})$, $(\boldsymbol{\delta}_{27}^{27}, \boldsymbol{\delta}_{27}^1)$ can all be distinguished;

(2) The fact that $(\boldsymbol{\delta}_{27}^1, \boldsymbol{\delta}_{27}^3)$ can be distinguished means that $(\boldsymbol{\delta}_{27}^2, \boldsymbol{\delta}_{27}^4)$, $(\boldsymbol{\delta}_{27}^3, \boldsymbol{\delta}_{27}^5), \cdots, (\boldsymbol{\delta}_{27}^{26}, \boldsymbol{\delta}_{27}^1)$, $(\boldsymbol{\delta}_{27}^{27}, \boldsymbol{\delta}_{27}^2)$ can all be distinguished;

$\vdots$

(8) The fact that $(\boldsymbol{\delta}_{27}^1, \boldsymbol{\delta}_{27}^9)$ can be distinguished means that $(\boldsymbol{\delta}_{27}^2, \boldsymbol{\delta}_{27}^{10})$, $(\boldsymbol{\delta}_{27}^3, \boldsymbol{\delta}_{27}^{11}), \cdots, (\boldsymbol{\delta}_{27}^{26}, \boldsymbol{\delta}_{27}^7)$, $(\boldsymbol{\delta}_{27}^{27}, \boldsymbol{\delta}_{27}^8)$ can all be distinguished;

(9) The fact that $(\boldsymbol{\delta}_{27}^1, \boldsymbol{\delta}_{27}^{10})$ can be distinguished means that $(\boldsymbol{\delta}_{27}^2, \boldsymbol{\delta}_{27}^{11})$, $(\boldsymbol{\delta}_{27}^3, \boldsymbol{\delta}_{27}^{12}), \cdots, (\boldsymbol{\delta}_{27}^{26}, \boldsymbol{\delta}_{27}^8)$, $(\boldsymbol{\delta}_{27}^{27}, \boldsymbol{\delta}_{27}^9)$ can all be distinguished;

$\vdots$

(13) The fact that $(\boldsymbol{\delta}_{27}^1, \boldsymbol{\delta}_{27}^{14})$ can be distinguished means that $(\boldsymbol{\delta}_{27}^2, \boldsymbol{\delta}_{27}^{15})$,

Table 3 State pair trajectory table in Example 3

Step	Indistinguishable initial state pair							
	(1,2)	(1,3)	(1,4)	(1,5)	(1,6)	(1,7)	(1,8)	(1,9)
R_1	(2,3)	(2,4)	(2,5)	(2,6)	(2,7)	(2,8)	(2,9)	$\surd$
R_2	(3,4)	(3,5)	(3,6)	(3,7)	(3,8)	(3,9)	$\surd$	
R_3	(4,5)	(4,6)	(4,7)	(4,8)	(4,9)	$\surd$		
R_4	(5,6)	(5,7)	(5,8)	(5,9)	$\surd$			
R_5	(6,7)	(6,8)	(6,9)	$\surd$				
R_6	(7,8)	(7,9)	$\surd$					
R_6	(8,9)	$\surd$						
R_7	$\surd$							

$(\boldsymbol{\delta}_{27}^{3},\boldsymbol{\delta}_{27}^{16}),\cdots,(\boldsymbol{\delta}_{27}^{26},\boldsymbol{\delta}_{27}^{12})$, $(\boldsymbol{\delta}_{27}^{27},\boldsymbol{\delta}_{27}^{13})$ can all be distinguished.

The last five facts hold because $(\boldsymbol{\delta}_{27}^{1},\boldsymbol{\delta}_{27}^{10}),(\boldsymbol{\delta}_{27}^{1},\boldsymbol{\delta}_{27}^{11}),\cdots,(\boldsymbol{\delta}_{27}^{1},\boldsymbol{\delta}_{27}^{14})$ are initially distinguishable. The above 13 facts can prove that a total of $13\times 27=351$ state pairs are distinguishable, and the Galois NFSR has only 351 distinct state pairs. So, the system is observable.

Remark 1 In Example 3, we choose P_1 for investigation. In fact, for P_i, no matter which i is chosen, the final results will not be affected, because as long as there is an i such that the state pairs in $P_i\cap\Omega$ can be distinguished, then for all i's, $P_i\cap\Omega$ can be distinguished. Therefore, the choice of P_i does not affect the subsequent analysis.

3.3.2 Nonsingular Galois NFSRs

Next, we consider nonsingular Galois NFSRs. An NFSR is said to be nonsingular if its ST-diagram contains only cycles. Nonsingularity is a significant property in stream cipher design, and is a fundamental demand to guarantee that NFSRs avoid generating equivalent keys. To analyze whether a nonsingular Galois NFSR is observable, the definition of a state pair transition diagram (SPT-diagram) is introduced:

Definition 7 A directed graph consisting of $\frac{p^{2n}-p^n}{2}$ nodes and $\frac{p^{2n}-p^n}{2}$ directed edges is called the SPT-diagram of an n-stage FSR over $\mathbb{F}_p$, if each node of it is an element in set $\Phi=\{(\boldsymbol{\delta}_{p^n}^{i},\boldsymbol{\delta}_{p^n}^{j})|1\leq i<j\leq p^n\}$, and an edge from node $(\boldsymbol{\delta}_{p^n}^{a},\boldsymbol{\delta}_{p^n}^{b})$ to node $(\boldsymbol{\delta}_{p^n}^{\alpha},\boldsymbol{\delta}_{p^n}^{\beta})$ means $\boldsymbol{L}\boldsymbol{\delta}_{p^n}^{a}=\boldsymbol{\delta}_{p^n}^{\alpha}$, $\boldsymbol{L}\boldsymbol{\delta}_{p^n}^{b}=\boldsymbol{\delta}_{p^n}^{\beta}$ or $\boldsymbol{L}\boldsymbol{\delta}_{p^n}^{a}=\boldsymbol{\delta}_{p^n}^{\beta}$, $\boldsymbol{L}\boldsymbol{\delta}_{p^n}^{b}=\boldsymbol{\delta}_{p^n}^{\alpha}$.

According to the above definition, a certain relationship between the ST-diagram and SPT-diagram can be obtained:

Proposition 1 The ST-diagram contains only cycles if and only if the SPT-diagram contains only cycles.

Proof (Necessity) First we assume that the ST-diagram contains only cycles and that states $\boldsymbol{x}_1$ and $\boldsymbol{x}_2$ are on the same cycle. Denote the length of this cycle as c, so we have $\boldsymbol{L}^{c}\boldsymbol{x}_1=\boldsymbol{x}_1$ and $\boldsymbol{L}^{c}\boldsymbol{x}_2=\boldsymbol{x}_2$. Then

$$(\boldsymbol{x}_1,\boldsymbol{x}_2)\to(\boldsymbol{L}\boldsymbol{x}_1,\boldsymbol{L}\boldsymbol{x}_2)\to\cdots\to(\boldsymbol{L}^{c-1}\boldsymbol{x}_1,\boldsymbol{L}^{c-1}\boldsymbol{x}_2)\to(\boldsymbol{x}_1,\boldsymbol{x}_2)$$

forms a cycle. Next, suppose that states $\boldsymbol{x}_1$ and $\boldsymbol{x}_2$ are on two different cycles. Denote the lengths of these two cycles as c_1 and c_2. Then

$$(\boldsymbol{x}_1,\boldsymbol{x}_2)\to(\boldsymbol{L}\boldsymbol{x}_1,\boldsymbol{L}\boldsymbol{x}_2)\to\cdots\to(\boldsymbol{L}^{c^*-1}\boldsymbol{x}_1,\boldsymbol{L}^{c^*-1}\boldsymbol{x}_2)\to(\boldsymbol{x}_1,\boldsymbol{x}_2)$$

forms a cycle, where c^* is the least common multiple of c_1 and c_2. However, any two states are either on the same cycle or on two different cycles, and only these two cases are possible. Thus, all state pairs are on cycles.

(Sufficiency) Assume that the ST-diagram contains other things besides cycles. In this case, the ST-diagram may also contain branches connected with cycles. Assume that $\boldsymbol{y}_1$ is the starting state of a branch and $\boldsymbol{y}$ is an arbitrary state different from $\boldsymbol{y}_1$. Then state pair $(\boldsymbol{y}_1,\boldsymbol{y})$ will never be reached. In other words, $(\boldsymbol{y}_1,\boldsymbol{y})$ is a starting node in the SPT-diagram, which contradicts the SPT-diagram containing only cycles. It is easy to know that the SPT-diagram of a nonsingular FSR contains only cycles. Next, we naturally have a necessary and sufficient condition for the observability of nonsingular Galois NFSRs according to the SPT-diagram:

Theorem 4 An n-stage nonsingular Galois NFSR over $\mathbb{F}_p$ is observable if and only if each cycle of the SPT-diagram contains a state pair in set $\Phi\backslash\Omega$.

Proof The elements in set $\Phi\backslash\Omega$ are all states that can be distinguished initially. If each cycle of the SPT-diagram contains a state pair in set $\Phi\backslash\Omega$, then all state pairs on this cycle can reach this state pair after a suitable number of steps. In other words, all state pairs of this Galois NFSR can reach the state pairs in set $\Phi\backslash\Omega$ eventually. Hence, the Galois NFSR is observable.

Conversely, if there exists a cycle in the SPT-diagram on which no state pair belongs to set $\Phi\backslash\Omega$, then all state pairs on this cycle can never reach the state pairs that can be distinguished; i.e., they can never be distinguished. That is to say, the Galois NFSR is unobservable.

An example is offered to demonstrate the effectiveness of the above results:

Example 4 Consider a two-stage Galois NFSR over $\mathbb{F}_3$ with the state transition matrix $\boldsymbol{L}=\boldsymbol{\delta}_9[4\ 3\ 7\ 5\ 9\ 6\ 2\ 1\ 8]$, output matrix $\boldsymbol{H}=\boldsymbol{\delta}_3[1\ 1\ 1\ 2\ 2\ 2\ 3\ 3\ 3]$, and the corresponding vector form $\boldsymbol{V_L}=[4\ 3\ 7\ 5\ 9\ 6\ 2\ 1\ 8]$.

According to $\boldsymbol{V_L}$, we can obtain the SPT-diagram and the ST-diagram of this Galois matrix

in Figs. 3 and 4, respectively (for convenience, we abbreviate state $\boldsymbol{\delta}_9^i$ as i in the figures).

As we can see, the ST-diagram and the SPT-diagram contain only cycles, so this Galois NFSR is nonsingular.

Set $\Omega = \{(\boldsymbol{\delta}_9^1, \boldsymbol{\delta}_9^2), (\boldsymbol{\delta}_9^1, \boldsymbol{\delta}_9^3), (\boldsymbol{\delta}_9^2, \boldsymbol{\delta}_9^3), (\boldsymbol{\delta}_9^4, \boldsymbol{\delta}_9^5), (\boldsymbol{\delta}_9^4, \boldsymbol{\delta}_9^6), (\boldsymbol{\delta}_9^5, \boldsymbol{\delta}_9^6), (\boldsymbol{\delta}_9^7, \boldsymbol{\delta}_9^8), (\boldsymbol{\delta}_9^7, \boldsymbol{\delta}_9^9), (\boldsymbol{\delta}_9^8, \boldsymbol{\delta}_9^9)\}$. Actually, in the SPT-diagram, $(\boldsymbol{\delta}_9^1, \boldsymbol{\delta}_9^5)$, $(\boldsymbol{\delta}_9^3, \boldsymbol{\delta}_9^7)$, $(\boldsymbol{\delta}_9^2, \boldsymbol{\delta}_9^6)$, $(\boldsymbol{\delta}_9^1, \boldsymbol{\delta}_9^4)$, $(\boldsymbol{\delta}_9^4, \boldsymbol{\delta}_9^3)$ belong to set $\Phi\backslash\Omega$. By Theorem 4, each cycle of the SPT-diagram contains a state pair in set $\Phi\backslash\Omega$. Hence, this Galois NFSR is observable.

This method can also be applied to general Galois NFSRs. Here we give a necessary and sufficient condition that a general Galois NFSR is unobservable:

Corollary 1 An n-stage Galois NFSR over $\mathbb{F}_p$ is unobservable if and only if there exists a cycle in the SPT-diagram on which all state pairs belong to set Ω.

Proof If there exists a cycle in the SPT-diagram on which all state pairs belong to set Ω, then all state pairs on this cycle can never be distinguished, which means that this Galois NFSR is unobservable.

On the contrary, assume that this Galois NFSR is unobservable. Then there exists a state pair that can never be distinguished. If this state pair is on a cycle, then all state pairs on this cycle must belong to set Ω; otherwise, the state pair will be distinguishable after finite steps. If this state pair is on a branch, then all state pairs on the cycle connected with this branch must belong to set Ω.

In addition, it should be noted that the matrix method in Section 3.2 can be applied directly to these two special types of Galois NFSRs. l in $\boldsymbol{Q}_l$ of these two special types will be smaller than that of general Galois NFSRs, and it is often necessary to compare the output sequence of no more than $|\Omega| - 1$ steps to distinguish it because the ST-diagram contains only cycles. The specific operation is similar to that in Example 2, so it is omitted here.

4 Conclusions

In this paper, the observability of Galois NFSRs over finite fields was investigated. First, we introduced a simpler representation of a state transition matrix called the vector form. Using this form, we researched the observability of general Galois NFSRs and gave a necessary and sufficient condition for determining the observability. Then we proposed another matrix method with a lower computation complexity to determine the observability of general Galois NFSRs over finite fields. Finally, we studied two special types of Galois NFSRs, full-length Galois NFSRs and nonsingular Galois NFSRs. For each type of NFSRs, we proposed one simpler method to study the observability. Meanwhile, some numerical examples were delivered to support the results in this paper. In the future, the observability of Galois NFSRs with inputs will be studied, and reducing computation complexity will be explored.

Contributors

Zhe GAO and Yongyuan YU designed the research. Zhe GAO and Jun'e FENG processed the data. Zhe GAO drafted

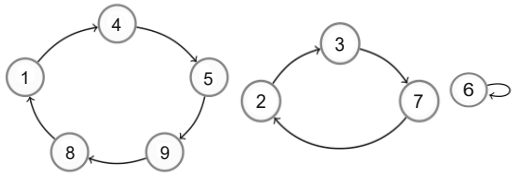

Fig. 4 ST-diagram of the Galois NFSR in Example 4

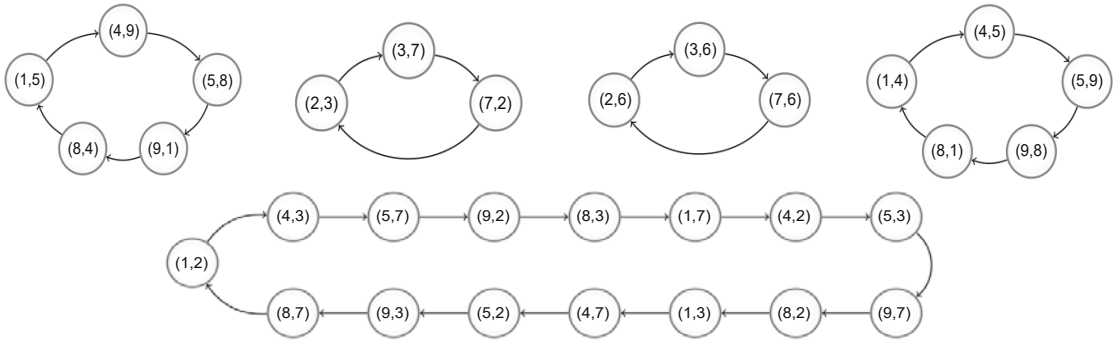

Fig. 3 SPT-diagram of the Galois NFSR in Example 4

the paper. Jun'e FENG and Yanjun CUI helped organize the paper. Zhe GAO and Yongyuan YU revised and finalized the paper.

Compliance with ethics guidelines

Zhe GAO, Jun'e FENG, Yongyuan YU, and Yanjun CUI declare that they have no conflict of interest.

References

Aumasson JP, Dinur I, Meier W, et al., 2009. Cube testers and key recovery attacks on reduced-round MD6 and Trivium. Int Workshop on Fast Software Encryption, p.1-22. https://doi.org/10.1007/978-3-642-03317-9_1

Cheng DZ, Qi HS, Li ZQ, 2011. Analysis and Control of Boolean Networks: a Semi-tensor Product Approach. Springer London. https://doi.org/10.1007/978-0-85729-097-7

Cheng DZ, Qi HS, Zhao Y, 2012. An Introduction to Semi Tensor Product of Matrices and Its Applications. Hackensack: World Scientific. https://doi.org/10.1142/8323

Deepthi PP, Sathidevi PS, 2009. Design, implementation and analysis of hardware efficient stream ciphers using LFSR based hash functions. *Comput Secur*, 28(3-4):229-241. https://doi.org/10.1016/j.cose.2008.11.006

Dubrova E, 2009. A transformation from the Fibonacci to the Galois NLFSRs. *IEEE Trans Inform Theory*, 55(11):5263-5271. https://doi.org/10.1109/TIT.2009.2030467

Dubrova E, 2010. Finding matching initial states for equivalent NLFSRs in the Fibonacci and the Galois configurations. *IEEE Trans Inform Theory*, 56(6):2961-2966. https://doi.org/10.1109/TIT.2010.2046250

Fornasini E, Valcher ME, 2013. Observability, reconstructibility and state observers of Boolean control networks. *IEEE Trans Autom Contr*, 58(6):1390-1401. https://doi.org/10.1109/TAC.2012.2231592

Golomb SW, 1967. Shift Register Sequences. San Francisco: Holden-Day.

Hellebrand S, Rajski J, Tarnick S, et al., 1995. Built-in test for circuits with scan based on reseeding of multiple-polynomial linear feedback shift registers. *IEEE Trans Comput*, 44(2):223-233. https://doi.org/10.1109/12.364534

Huang C, Ho DWC, Lu JQ, et al., 2022. Synchronization of an array of coupled probabilistic Boolean networks. *IEEE Trans Syst Man Cybern Syst*, 52(6):3834-3846. https://doi.org/10.1109/TSMC.2021.3073201

Kong WH, Zhong JH, Lin DD, 2022. Observability of Galois nonlinear feedback shift registers. *Sci China Inform Sci*, 65(9):192206. https://doi.org/10.1007/s11432-021-3346-6

Lai XJ, 1987. Condition for the nonsingularity of a feedback shift-register over a general finite field (Corresp.). *IEEE Trans Inform Theory*, 33(5):747-749. https://doi.org/10.1109/TIT.1987.1057338

Li R, Yang M, Chu TG, 2014. Observability conditions of Boolean control networks. *Int J Robust Nonl Contr*, 24(17):2711-2723. https://doi.org/10.1002/rnc.3019

Li YF, Zhu JD, 2020. Cascading decomposition of Boolean control networks: a graph-theoretical method. *Front Inform Technol Electron Eng*, 21(2):304-315. https://doi.org/10.1631/FITEE.1900422

Limniotis K, Kolokotronis N, Kalouptsidis N, 2006. New results on the linear complexity of binary sequences. Proc IEEE Int Symp on Information Theory, p.2003-2007. https://doi.org/10.1109/ISIT.2006.261900

Limniotis K, Kolokotronis N, Kalouptsidis N, 2008. On the linear complexity of sequences obtained by state space generators. *IEEE Trans Inform Theory*, 54(4):1786-1793. https://doi.org/10.1109/TIT.2008.917639

Ljung L, Sèoderstrèom T, 1983. Theory and Practice of Recursive Identification. Cambridge: MIT Press.

Lu JQ, Li ML, Liu Y, et al., 2018a. Nonsingularity of Grain-like cascade FSRs via semi-tensor product. *Sci China Inform Sci*, 61(1):010204. https://doi.org/10.1007/s11432-017-9269-6

Lu JQ, Li ML, Huang TW, et al., 2018b. The transformation between the Galois NLFSRs and the Fibonacci NLFSRs via semi-tensor product of matrices. *Automatica*, 96:393-397. https://doi.org/10.1016/j.automatica.2018.07.011

Lu JQ, Li BW, Zhong J, 2021. A novel synthesis method for reliable feedback shift registers via Boolean networks. *Sci China Inform Sci*, 64(5):152207. https://doi.org/10.1007/s11432-020-2981-4

Massey J, 1969. Shift-register synthesis and BCH decoding. *IEEE Trans Inform Theory*, 15(1):122-127. https://doi.org/10.1109/TIT.1969.1054260

Meier W, Staffelbach O, 1989. Fast correlation attacks on certain stream ciphers. *J Cryptol*, 1(3):159-176. https://doi.org/10.1007/BF02252874

Roger AH, Johnson CR, 1991. Topics in Matrix Analysis. Cambridge University Press. https://doi.org/10.1017/CBO9780511840371

Shen YW, Guo YQ, Gui WH, 2021. Stability of Boolean networks with state-dependent random impulses. *Front Inform Technol Electron Eng*, 22(2):222-231. https://doi.org/10.1631/FITEE.1900454

Wang B, Feng JE, 2019. On detectability of probabilistic Boolean networks. *Inform Sci*, 483:383-395. https://doi.org/10.1016/j.ins.2019.01.055

Wang HY, Zhong JH, Lin DD, 2017. Linearization of multi-valued nonlinear feedback shift registers. *J Syst Sci Complexity*, 30(2):494-509. https://doi.org/10.1007/s11424-016-5156-7

Wang QY, Jin CH, 2013. Nonsingularity decision of Trivium-like cascade connection of feedback shift registers. *J Inform Eng Univ*, 14(5):519-523 (in Chinese). https://doi.org/10.3969/j.issn.1671-0673.2013.05.002

Wang XJ, Tian T, Qi WF, 2022. A necessary and sufficient condition for a class of nonsingular Galois NFSRs. *Finit Fields Their Appl*, 77:101952. https://doi.org/10.1016/j.ffa.2021.101952

Yu YY, Meng M, Feng JE, et al., 2021. Observability criteria for Boolean networks. *IEEE Trans Autom Contr*, early access. https://doi.org/10.1109/TAC.2021.3131436

Zhang QL, Wang B, Feng JE, 2021. Solution and stability of continuous-time cross-dimensional linear systems. *Front Inform Technol Electron Eng*, 22(2):210-221. https://doi.org/10.1631/FITEE.1900504

Zhao XY, Wang B, Yan YY, et al., 2021. The equivalence transformation between Galois NFSRs and Fibonacci NFSRs. *Asian J Contr*, 23(6):2865-2873. https://doi.org/10.1002/asjc.2390

Zheng YT, Feng JE, 2020. Output tracking of delayed logical control networks with multi-constraint. *Front Inform Technol Electron Eng*, 21(2):316-323. https://doi.org/10.1631/FITEE.1900376

Zhong J, Li BW, Liu Y, et al., 2020. Output feedback stabilizer design of Boolean networks based on network structure. *Front Inform Technol Electron Eng*, 21(2):247-259. https://doi.org/10.1631/FITEE.1900229

Zhong JH, Lin DD, 2015. A new linearization method for nonlinear feedback shift registers. *J Comput Syst Sci*, 81(4):783-796. https://doi.org/10.1016/j.jcss.2014.12.030

Zhong JH, Lin DD, 2016a. Driven stability of nonlinear feedback shift registers with inputs. *IEEE Trans Commun*, 64(6):2274-2284. https://doi.org/10.1109/TCOMM.2016.2557330

Zhong JH, Lin DD, 2016b. Stability of nonlinear feedback shift registers. *Sci China Inform Sci*, 59(1):1-12. https://doi.org/10.1007/s11432-015-5311-0

Zhong JH, Lin DD, 2018. On minimum period of nonlinear feedback shift registers in Grain-like structure. *IEEE Trans Inform Theory*, 64(9):6429-6442. https://doi.org/10.1109/TIT.2018.2849392

Zhong JH, Lin DD, 2019a. Decomposition of nonlinear feedback shift registers based on Boolean networks. *Sci China Inform Sci*, 62(3):39110. https://doi.org/10.1007/s11432-017-9460-4

Zhong JH, Lin DD, 2019b. On equivalence of cascade connections of two nonlinear feedback shift registers. *Comput J*, 62(12):1793-1804. https://doi.org/10.1093/comjnl/bxz057