Noname manuscript No.
(will be inserted by the editor)

A Generic Method for Investigating Nonsingular Galois NFSRs

Xiao-Juan Wang · Tian Tian · Wen-Feng Qi

Received: date / Accepted: date

Abstract Let n be a positive integer. An n-stage Galois NFSR has n registers and each register is updated by a feedback function. Then a Galois NFSR is called nonsingular if every register generates (strictly) periodic sequences, i.e., no branch points. In this paper, a generic method for investigating nonsingular Galois NFSRs is provided. Two fundamental concepts that are standard Galois NFSRs and the simplified feedback function of a standard Galois NFSR are proposed. Based on the new concepts, a sufficient condition is given for nonsingular Galois NFSRs. In particular, for the class of Galois NFSRs with linear simplified feedback functions, a necessary and sufficient condition is presented. Hopefully, some new insights are provided on determining nonsingular Galois NFSRs.

Keywords Stream ciphers · nonlinear feedback shift registers · Galois configuration · periodic sequences

1 Introduction

Shift registers, including linear feedback shift registers (LFSRs) and nonlinear feedback shift registers (NFSRs), were popular building blocks for hardware-oriented stream ciphers. Since primitive linear feedback shift register sequences were proven to have large periods and balancedness, early stream ciphers such as A5/1 used in the GSM, E0 used in the Bluetooth protocol, and SNOW-3G which is one of 3GPP LTE cryptographic algorithms were designed based on LFSRs. Over the years, it

This work was supported by the National Natural Science Foundation of China under Grants (61672533, 61521003).

X.-J. Wang · T. Tian · W.-F. Qi
PLA Strategic Support Force Information Engineering University, Zhengzhou 450001, China.
Tian Tian
E-mail: tiantian_d@126.com

Xiao-Juan Wang
E-mail: Xiaojuan_Wang0@163.com

Wen-Feng Qi
E-mail: wenfeng.qi@263.net

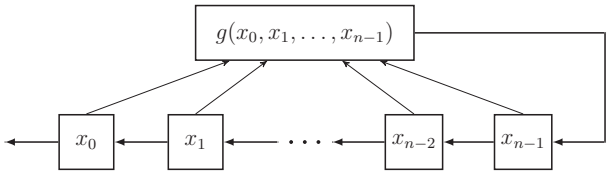

Fig. 1: An n-stage Fibonacci NFSR

is found that LFSR-based stream ciphers were susceptible to correlation attacks [1–4] and algebraic attacks [5,6]. Therefore, recent lightweight stream ciphers all turn to nonlinear feedback shift registers (NFSRs). Trivium, an International Standard of lightweight stream ciphers (ISO/IEC 29192-3:2012) and one of eSTREAM hardware-oriented finalists, is built on a 288-stage NFSR [7]. Grain-128a [8], an International Standard for air interface for RFID systems (ISO/IEC 29167-13:2015), is built on a 256-stage NFSR. Besides, Kreyvium [9], Grain-v1 [10], and Acorn [11] are all well-known NFSR-based stream ciphers.

There are two configurations to implement NFSRs, say the Fibonacci configuration and the Galois configuration. Let n be a positive integer. A typical n-stage Fibonacci NFSR is depicted in Figure 1, where the Boolean function $g(x_0, x_1, \ldots, x_{n-1})$ is called the feedback function of this Fibonacci NFSR. It can be seen that for the Fibonacci NFSR in Figure 1, at each time instance, the content of x_i is transferred into x_{i-1} for $1 \leq i \leq n-1$ and a new bit computed by the feedback function g is used to update x_{n-1}. Thus for a Fibonacci NFSR which is not a cycling register, there is one and only one register updated by a feedback function while all the other registers are updated by shifting. A diagram of an n-stage Galois NFSR is shown in Figure 2, and the vector Boolean function

$$F = (f_0(x_0, x_1, \ldots, x_{n-1}), f_1(x_0, x_1, \ldots, x_{n-1}), \ldots, f_{n-1}(x_0, x_1, \ldots, x_{n-1}))$$

is called the feedback function of this Galois NFSR. It can be seen from Figure 2 that the Galois configuration is more complex and generalized than the Fibonacci configuration, since for a Galois NFSR every register could be updated by a nontrivial feedback function. This yields that Galois NFSRs are more difficult to analyze.

Recall that for a binary sequence $\underline{s} = (s(t))_{t=0}^{\infty}$, it is called a (strictly) periodic sequence if there is a positive integer T such that $s(t+T) = s(t)$ for all $t \geq 0$. We say a Galois NFSR is nonsingular if and only if the outputting sequence of every register is periodic. It is a fundamental principal in stream ciphers that only nonsingular Galois NFSRs could be used as a main register. Although so far all particular Galois NFSRs used in stream ciphers, such as Trivium and Grain-128a, were shown to be nonsingular, there is no general theory on the problem how to determine a Galois NFSR is nonsingular from a mathematical standpoint.

In [12, Chapter VI], Golomb gave a classic result on nonsingular Fibonacci NFSRs. It was proved in [12, Chapter VI] that a Fibonacci NFSR with the feedback function $g(x_0, x_1, \ldots, x_{n-1})$ shown in Figure 1 is nonsingular if and only if

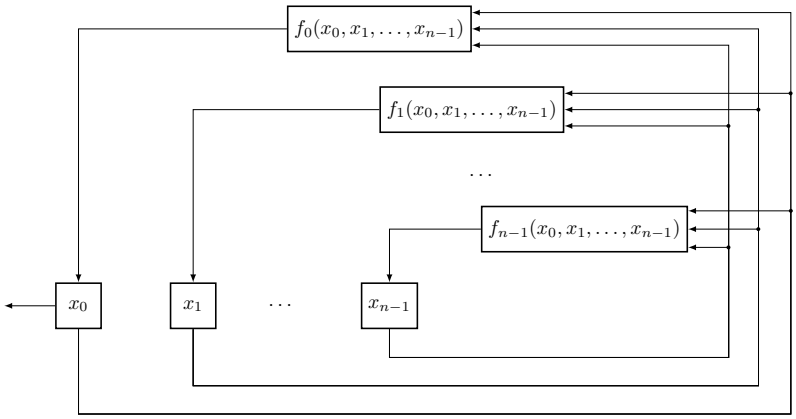

Fig. 2: An n-stage Galois NFSR

$g(x_0, x_1, \ldots, x_{n-1})$ can be decomposed into

$$g(x_0, x_1, \ldots, x_{n-1}) = x_0 \oplus g_1(x_1, x_2, \ldots, x_{n-1}).$$

As for identifying nonsingular Galois NFSRs, Golomb just mentioned two criteria in [12, Page 22][1]. One criterion is that the "Jacobian" of the feedback function is nonzero. The other one is very vague which said that there was a criterion which involves conditions on expressions of the type $f_j(x_1, x_2, \ldots, x_n) \oplus x_i$. Since the nonsingular property of Fibonacci NFSR is adequately understood, if a Galois NFSR is equivalent to a Fibonacci NFSR, then the nonsingularity property inherently follows from the Fibonacci NFSR. In [13], the author proposed a transformation from a given Fibonacci NFSR to a Galois NFSR. When the given Fibonacci NFSR is nonsingular, a class of nonsingular Galois NFSRs can be obtained. Very recently, in [14] the authors proposed two types of Galois NFSRs called Triangulation-I and Triangulation-II and identified nonsingular NFSRs included in them respectively.

In this paper, we will give a generic method for investigating nonsingular Galois NFSRs, which is distinct from the two criteria mentioned in [12, Page 22] and also distinct from Triangulation-I and -II given in [14]. The basic idea is properly classifying Galois NFSRs and describing some kind of standard forms. This facilitates us to formulate some reasonable conditions. First, we give the definition for two Galois NFSRs being equivalent and introduce the concept of standard feedback functions. For a class of equivalent Galois NFSRs, it suffices to consider the standard NFSR. Furthermore, simplified feedback functions and critical matrices whose entries are Boolean functions are proposed. Second, based on some observations on the algebraic normal form of a general standard feedback function, a sufficient condition for nonsingular Galois NFSRs is given. Finally, for standard NFSRs with linear simplified feedback functions, they are proved to be nonsingular if and only if the determinants of their critical matrices are equal to 1. Generally, a critical matrix is very small whose size is independent of the bit length of the

[1] A Galois NFSR is called an autonomous binary machine in [12]. Please refer to Fig. II-14 in [12].

NFSR, and so its determinant is easy to compute. Some practical examples of the application of the criterion are provided.

The paper is constructed as follows. In Sect. 2, we give some necessary introductions to Boolean functions and Galois NFSRs. Two fundamental concepts that are standard Galois NFSRs and the simplified feedback function of a standard Galois NFSR are proposed in Sect. 3. Meanwhile, a sufficient condition for general Galois NFSRs is given in Sect. 4. Sect. 5 is largely devoted to the proof of our necessary and sufficient condition for Galois NFSRs with linear simplified feedback functions. Some applications of our main results are discussed in Sect. 6. Sect. 7 shows that our criteria are distinct from previous results. Finally, conclusions are drawn in Sect. 8.

Throughout the paper we use the following notations. Let $\mathbb{N}^*$ denote the set of positive integers. The operations "+" and "−" denote the ordinary integer addition and subtraction, respectively. The operation "$\oplus$" denotes the addition modulo 2. The finite field of two elements is denoted by $\mathbb{F}_2$ and for any positive integer n, the n-dimensional vector space over $\mathbb{F}_2$ is denoted by $\mathbb{F}_2^n$.

2 Preliminaries

In this section, we give some basic definitions and notations on Boolean functions and NFSRs.

2.1 Boolean functions

Let $n \in \mathbb{N}^*$. An n-variable Boolean function $f(x_0, x_1, \ldots, x_{n-1})$ is a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2$. In particular, 0 and 1 are constant Boolean functions. The set of all n-variable Boolean functions is denoted by $\mathbb{B}_n$, and the set of all Boolean functions is denoted by $\mathbb{B}$, i.e., $\mathbb{B} = \bigcup_{n\in\mathbb{N}^*} \mathbb{B}_n$. The algebraic normal form (ANF) of a Boolean function $f(x_0, x_1, \ldots, x_{n-1})$ is given by

$$f(x_0, x_1, \ldots, x_{n-1}) = \bigoplus_{\boldsymbol{\alpha}=(\alpha_0,\alpha_1,\ldots,\alpha_{n-1})\in\{0,1\}^n} u_{f,\boldsymbol{\alpha}} \cdot \left(\prod_{j=0}^{n-1} x_j^{\alpha_j} \right),$$

where $u_{f,\boldsymbol{\alpha}} \in \mathbb{F}_2$ and $x_0^{\alpha_0} x_1^{\alpha_1} \cdots x_{n-1}^{\alpha_{n-1}}$ is called a term. The algebraic degree of f, denoted by $\deg(f)$, is defined by

$$\deg(f) = \max\{wt(\boldsymbol{\alpha}) | u_{f,\boldsymbol{\alpha}} \neq 0\},$$

where $wt(\boldsymbol{\alpha})$ is the Hamming weight of $\boldsymbol{\alpha}$. If $\deg(f) = 1$, then f is called affine; furthermore, if $f(0, 0, \ldots, 0) = 0$, then f is called linear.

The set of Boolean functions together with Boolean function multiplication and addition is a ring, called the Boolean function ring. A matrix over the Boolean function ring implies that every entry of the matrix is a Boolean function. Since 0 and 1 are constant Boolean function, it follows that the set of matrices over the Boolean function ring includes the set of binary matrices. For a $k \times k$ square matrix $M = (f_{i,j})_{k\times k}$, where $f_{i,j}$ is an n-variable Boolean function, the determinant of M is denoted by $\det(M)$ and the rank of M is denoted by $\mathrm{rank}(M)$. A square

matrix over the Boolean function ring is invertible if and only if its determinant is equal to 1.

Let σ be a permutation on the set $\{0, 1, \ldots, n-1\}$. Then define

$$\sigma(f) = f(x_{\sigma(0)}, x_{\sigma(1)}, \ldots, x_{\sigma(n-1)}),$$

and

$$\sigma(M) = (\sigma(f_{i,j}))_{k\times k}.$$

We note that $\sigma(0) = 0$ and $\sigma(1) = 1$, that is to say, $\sigma(f) = f$ if f is a constant Boolean function.

Finally, a mapping F from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$ is called an n-variable vector Boolean function and is represented by

$$F = (f_0(x_0, x_1, \ldots, x_{n-1}), f_1(x_0, x_1, \ldots, x_{n-1}), \ldots, f_{n-1}(x_0, x_1, \ldots, x_{n-1})),$$

where $f_0, f_1, \ldots, f_{n-1}$ are Boolean functions.

2.2 Galois NFSRs

Let $n \in \mathbb{N}^*$ and let

$$F = (f_0(x_0, x_1, \ldots, x_{n-1}), f_1(x_0, x_1, \ldots, x_{n-1}), \ldots, f_{n-1}(x_0, x_1, \ldots, x_{n-1}))$$

be a vector Boolean function. An n-stage Galois NFSR with the feedback function F is shown in Figure 2, where $x_0, x_1, \ldots, x_{n-1}$ are n binary registers and f_i is the feedback function of the register x_i for $0 \le i \le n-1$. Since a feedback function could uniquely determine the architecture of a Galois NFSR, the NFSR in Figure 2 is denoted by NFSR(F). For $t \ge 0$, the n registers of NFSR(F) are updated as follows:

$$\begin{aligned}&(x_0(t+1), x_1(t+1), \ldots, x_{n-1}(t+1))\\ &= (f_0(x_0(t), \ldots, x_{n-1}(t)), f_1(x_0(t), \ldots, x_{n-1}(t)), \ldots, f_{n-1}(x_0(t), \ldots, x_{n-1}(t))),\end{aligned}$$

where $(x_0(t), x_1(t), \ldots, x_{n-1}(t))$ is the state of NFSR(F) at the time instance t. If $f_i \neq x_j$ for every $0 \le j \le n-1$, then the ith register of NFSR(F) is called *a feedback register* in NFSR(F). Otherwise, the ith register of NFSR(F) is called *a shift register* in NFSR(F). If the outputting sequence of each register x_i is always periodic for $0 \le i \le n-1$, then we call NFSR(F) a nonsingular Galois NFSR. It is clear that NFSR(F) is nonsingular if and only if F is a one-to-one mapping from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$, or in other words, F is invertible, i.e., for every $(y_0, y_1, \ldots, y_{n-1}) \in \mathbb{F}_2^n$ there is a unique $\boldsymbol{a} = (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{F}_2^n$ such that

$$F(\boldsymbol{a}) = (f_0(\boldsymbol{a}), f_1(\boldsymbol{a}), \ldots, f_{n-1}(\boldsymbol{a})) = (y_0, y_1, \ldots, y_{n-1}).$$

This observation will be used in the later proof.

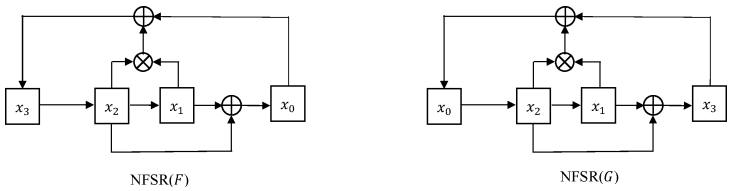

Fig. 3: NFSR(F) and NFSR(G)

3 Standard representations of Galois NFSRs and critical matrices

Note that for a Galois NFSR, every register could be updated by a feedback function, and so the position of each register in a Galois NFSR seems to be rather arbitrary. Thus, two Galois NFSRs with distinct feedback functions in ANFs may be completely the same by exchanging the positions of some registers.

Example 1 Let $F = (f_0, f_1, f_2, f_3)$ be the feedback function of a Galois NFSR with

$$\begin{aligned} f_0 &= x_1 \oplus x_2 \\ f_1 &= x_2 \\ f_2 &= x_3 \\ f_3 &= x_0 \oplus x_1x_2. \end{aligned}$$

Let $G = (g_0, g_1, g_2, g_3)$ be the feedback function of a Galois NFSR with

$$\begin{aligned} g_0 &= x_1x_2 \oplus x_3 \\ g_1 &= x_2 \\ g_2 &= x_0 \\ g_3 &= x_1 \oplus x_2. \end{aligned}$$

It can be seen that exchanging the labels of x_0 and x_3 in NFSR(F) leads to NFSR(G). This can also be observed from Figure 3.

Therefore, it is necessary to define equivalent Galois NFSRs which are different only in register order.

Definition 1 Let $F = (f_0, f_1, \ldots, f_{n-1})$ and $G = (g_0, g_1, \ldots, g_{n-1})$ be the feedback functions of two n-stage Galois NFSRs, respectively. If there is a permutation σ on the set $\{0, 1, \ldots, n-1\}$ such that $\sigma(F) = G$, then NFSR(F) and NFSR(G) are called equivalent, where

$$\sigma(F) = (f_{\sigma^{-1}(0)}(\sigma(X)), f_{\sigma^{-1}(1)}(\sigma(X)), \ldots, f_{\sigma^{-1}(n-1)}(\sigma(X)))$$

with $\sigma(X) = (x_{\sigma(0)}, x_{\sigma(1)}, \ldots, x_{\sigma(n-1)})$.

By this definition, NFSR(F) and NFSR(G) in Example 1 are equivalent. It is clear that two equivalent n-stage Galois NFSRs have the same n sets of sequences outputted from n registers not considering the order. Hence, the following property is clear and we omit the proof.

Proposition 1 *Let* NFSR(F) *and* NFSR(G) *be two equivalent n-stage Galois NFSRs. Then* NFSR(F) *is nonsingular if and only if* NFSR(G) *is nonsingular.*

Next, we define a type of standard representations for Galois NFSRs, which is very useful for investigating whether a Galois NFSR is nonsingular or not. Note that if a Galois NFSR only involves shifting, then it is a cycling register. Otherwise, a Galois NFSR has at least one register which is not updated by shifting. Hence, the following definition is reasonable.

Definition 2 Let $n \in \mathbb{N}^*$ and $F = (f_0, f_1, \ldots, f_{n-1})$ be the feedback function of an n-stage Galois NFSR. If the following two conditions are satisfied

(1) $f_{n-1} \neq x_0$,
(2) $f_i = x_j \Rightarrow j = i + 1, 0 \leq i \leq n - 2$,

then $F = (f_0, f_1, \ldots, f_{n-1})$ is called a standard feedback function and NFSR(F) is called a standard (Galois) NFSR.

The idea behind Definition 2 is putting two registers with the shifting relation into adjacent registers. This concept is inspired by Fibonacci NFSRs. The feedback function of a Fibonacci NFSR is a standard feedback function. Besides, we note that for a standard feedback function of an n-stage NFSR, the $(n-1)$th register could not be updated by shifting, and so it at least has one register updated by nontrivial feedback function. For example, NFSR(F) in Example 1 is a standard NFSR, but NFSR(G) in Example 1 is not a standard one.

Definition 3 Let $\mathcal{C}$ be an equivalent class of Galois NFSRs. If there exists a Galois NFSR in $\mathcal{C}$ with a standard feedback function, then we call $\mathcal{C}$ a normal class.

Most of equivalent classes of Galois NFSRs are normal. An equivalent class which is not normal is very uninteresting. Here are two examples.

Example 2 The class of NFSRs including the cycling register is not normal.

Example 3 Let F be the feedback function of an n-state Galois NFSR satisfying

$$f_0 = x_j, f_1 = x_j$$

for some integer j, then the equivalent class $\mathcal{C}$ of Galois NFSRs including this NFSR(F) is not normal. It can be seen that every NFSR in $\mathcal{C}$ has two registers always outputting the same bit.

For a standard feedback function, it is easier to distinguish a shifting register and a feedback register. Let $n \in \mathbb{N}^*$ and NFSR(F) be an n-stage Galois NFSR with a standard feedback function $F = (f_0, f_1, \ldots, f_{n-1})$. For $0 \leq i \leq n-1$, if $f_i = x_{i+1}$, then the ith register is a shifting register; otherwise, the ith register is a feedback register. Hence if NFSR(F) has k feedback registers, then we could use

$$\Omega(F) = [i_k + l_k, \ldots, i_k] \parallel [i_{k-1} + l_{k-1}, \ldots, i_{k-1}] \parallel \cdots \parallel [i_1 + l_1, \ldots, i_1]$$

to denote that $x_{i_k+l_k}, x_{i_{k-1}+l_{k-1}}, \ldots, x_{i_1+l_1}$ are k feedback registers in NFSR(F) where $l_j \geq 0$ for $1 \leq j \leq k$ and $i_k > i_{k-1} > \cdots > i_1 = 0$. If NFSR($F$) is an n-stage Fibonacci NFSR, then

$$\Omega(F) = [n-1, n-2, \ldots, 0].$$

From $\Omega(F)$ it can be clearly seen that a standard Galois NFSR could be divided into several feedback shift registers each of which is somewhat like Fibonacci configuration except that the feedback function could depend on every bit of the whole Galois NFSR not only the particular feedback shift register that it belongs to.

Remark 1 If $l_j = 0$ in $\Omega(F)$ for some integer $1 \leq j \leq k$, then x_{i_j} is a feedback register.

Definition 4 Let $n \in \mathbb{N}^*$ and NFSR(F) be an n-stage Galois NFSR with a standard feedback function $F = (f_0, f_1, \ldots, f_{n-1})$. Suppose there are exactly $k \geq 1$ feedback registers in NFSR(F) given by

$$\Omega(F) = [i_k + l_k, \ldots, i_k] \parallel [i_{k-1} + l_{k-1}, \ldots, i_{k-1}] \parallel \cdots \parallel [i_1 + l_1, \ldots, i_1].$$

Let $Y = X \setminus \{x_{i_1}, x_{i_2}, \ldots, x_{i_k}\}$ and

$$f_{i_j+l_j}(x_0, \ldots, x_{n-1}) = D_{i_j}(Y) \oplus \left(\sum_{u=1}^{k} C_{j,u}(Y) \cdot x_{i_u} \right) \oplus \left(\sum_{\boldsymbol{\alpha} \in \mathbb{F}_2^k} E_{\boldsymbol{\alpha},j}(Y) \cdot \prod_{j=0}^{n-1} x_j^{\alpha_j} \right)$$

for $j = 1, 2, \ldots, k$, where $D_{i_j}(Y), C_{j,1}(Y), \ldots, C_{j,k}(Y), E_{\boldsymbol{\alpha},j}(Y)$ are Boolean functions on Y. Then $F_s = (f_{i_1+l_1}, f_{i_2+l_2}, \ldots, f_{i_k+l_k})$ is called the simplified feedback function and the matrix

$$\begin{pmatrix} C_{1,1}(Y) & C_{1,2}(Y) & \cdots & C_{1,k}(Y) \\ C_{2,1}(Y) & C_{2,2}(Y) & \cdots & C_{2,k}(Y) \\ \cdots & \cdots & \cdots & \cdots \\ C_{k,1}(Y) & C_{k,2}(Y) & \cdots & C_{k,k}(Y) \end{pmatrix}$$

is called the critical matrix for NFSR(F), denoted by $\mathcal{M}(F)$.

If F_s contains some nonlinear terms on the variables $x_{i_1}, x_{i_2}, \ldots, x_{i_k}$, then F_s is called a nonlinear simplified feedback function. Otherwise, F_s is called a linear simplified feedback function.

Remark 2 When F_s is linear, F could still be a complex nonlinear feedback function.

4 A sufficient condition for general Galois NFSRs

In this section, we will give a sufficient condition for general Galois NFSRs. For convenience, we can write the simplified feedback function of NFSR(F) as follows

$$\begin{pmatrix} f_{i_1+l_1} \\ f_{i_2+l_2} \\ \vdots \\ f_{i_k+l_k} \end{pmatrix} = \begin{pmatrix} D_{i_1}(Y) \\ D_{i_2}(Y) \\ \vdots \\ D_{i_k}(Y) \end{pmatrix} \oplus \mathcal{M}(F) \begin{pmatrix} x_{i_1} \\ x_{i_2} \\ \vdots \\ x_{i_k} \end{pmatrix} \oplus \left(\bigoplus_{j=1}^{n_0} \begin{pmatrix} E_{j,1}(Y) \\ E_{j,2}(Y) \\ \vdots \\ E_{j,k}(Y) \end{pmatrix} x_{i_{m_{j,1}}} \cdots x_{i_{m_{j,d_j}}} \right). \quad (1)$$

In the following, let n_0 be a positive integer, i.e., F_s is nonlinear. The case of $n_0 = 0$ will be discussed in Sect. 5. For $1 \leq j \leq n_0$, let $S_j = \{m_{j,1}, m_{j,2}, \ldots, m_{j,d_j}\}$ and $S = \bigcup_{j=1}^{n_0} S_j$. The degree of jth nonlinear term is denoted by d_j and it is easy to see that $\max\{d_j | 1 \leq j \leq n_0\} = d$.

For $0 \leq j \leq k$, let $E(Y) = (E_1(Y), E_2(Y), \ldots, E_k(Y))^\top$ be a column vector over Boolean function ring and $C_j(Y) = (C_{1,j}(Y), C_{2,j}(Y), \ldots, C_{k,j}(Y))^\top$ be the jth column of $\mathcal{M}(F)$. Let

$$M_{E,j}(Y) = (C_1(Y), \ldots, C_j(Y) \oplus E(Y), \ldots, C_k(Y))$$

be the matrix obtained by adding $E(Y)$ to the jth column of $\mathcal{M}(F)$. It is obvious that $M_{E,0}(Y) = \mathcal{M}(F)$. If $\det(\mathcal{M}(F)) = 1$, then $(C_1(\boldsymbol{b}), C_2(\boldsymbol{b}), \ldots, C_k(\boldsymbol{b}))$ is a basis of the vector space $\mathbb{F}_2^k$ for every $\boldsymbol{b} \in \mathbb{F}_2^{n-k}$. Therefore, $E(\boldsymbol{b})$ can be expressed as $E(\boldsymbol{b}) = \bigoplus_{u=1}^{k} \beta_u C_u(\boldsymbol{b})$, where $\beta_u \in \mathbb{F}_2$. Then we have an $(n-k)$-variable Boolean function φ_u satisfying $\varphi_u(\boldsymbol{b}) = \beta_u$ by letting $\boldsymbol{b}$ run through $\mathbb{F}_2^{n-k}$. Thus $E(Y)$ can be expressed as $E(Y) = \bigoplus_{u=1}^{k} \varphi_u C_u(Y)$. Before proving the main results in this section, we first give Lemma 1.

Lemma 1 *Let* $\det(\mathcal{M}(F)) = 1$ *and* $E(Y) = \bigoplus_{u=1}^{k} \varphi_u C_u(Y)$. *Then for* $1 \leq j \leq k$, $\det(M_{E,j}(Y)) = 1$ *if and only if* $\varphi_j(Y) = 0$.

Proof Suppose $\det(M_{E,j}(Y)) = 1$ and there exists $\boldsymbol{b} \in \mathbb{F}_2^{n-k}$ such that $\beta_j = \varphi_j(\boldsymbol{b}) = 1$. Then we have

$$\begin{aligned} M_{E,j}(\boldsymbol{b}) &= (C_1(\boldsymbol{b}), \ldots, C_j(\boldsymbol{b}) \oplus E(\boldsymbol{b}), \ldots, C_k(\boldsymbol{b})) \\ &= (C_1(\boldsymbol{b}), \ldots, \bigoplus_{u=1, u\neq j}^{k} \beta_u C_u(\boldsymbol{b}), \ldots, C_k(\boldsymbol{b})). \end{aligned}$$

It is clear that there is a linearly correlation between $\bigoplus_{u=1,u\neq j}^{k} \beta_u C_u(\boldsymbol{b})$ and $C_1(\boldsymbol{b})$,
$\ldots, C_{j-1}(\boldsymbol{b}), C_{j+1}(\boldsymbol{b}), \ldots, C_k(\boldsymbol{b})$. Therefore, $\det(M_{E,j}(\boldsymbol{b})) = 0$, which is a contradiction to the assumption that $\det(M_{E,j}(\boldsymbol{b})) = 1$.

Conversely, suppose $\varphi_j(Y) = 0$ and $\det(M_{E,j}(Y)) \neq 1$. Then $\det(M_{E,j}(Y)) = 0$ or $\det(M_{E,j}(Y))$ is a Boolean function on Y which is not a constant, say $\det(M_{E,j}(Y)) = h(Y)$. There exists at least one evaluation of $Y = \boldsymbol{b}$ such that $\det(M_{E,j}(\boldsymbol{b})) = 0$. Thus there is a linearly correlation between $C_1(\boldsymbol{b}), \ldots, C_j(\boldsymbol{b}) \oplus E(\boldsymbol{b}), \ldots, C_k(\boldsymbol{b})$, i.e., there exist $a_1, \ldots, a_k \in \mathbb{F}_2$ such that

$$a_1 C_1(\boldsymbol{b}) \oplus \cdots \oplus a_j(C_j(\boldsymbol{b}) \oplus E(\boldsymbol{b})) \oplus \cdots \oplus a_k C_k(\boldsymbol{b}) = 0.$$

Considering that $(C_1(\boldsymbol{b}), \ldots, C_k(\boldsymbol{b}))$ is a basis of $\mathbb{F}_2^k$, we have $a_j \neq 0$ and then $C_j(\boldsymbol{b}) \oplus E(\boldsymbol{b}) = \bigoplus_{1\leq u\leq k, u\neq j}^{k} a_u C_u(\boldsymbol{b})$. Hence $E(\boldsymbol{b}) = C_j(\boldsymbol{b}) \bigoplus_{1\leq u\leq k, u\neq j}^{k} a_u C_u(\boldsymbol{b})$, a contradiction. □

We define an order for the coefficient vectors of the simplified feedback function F_s in the following.

Definition 5 The simplified feedback function F_s of NFSR(F) is given by (1) and $E_i(Y)$ is the coefficient vector of the ith nonlinear term of F_s for $1 \leq i \leq n_0$. When $\det(\mathcal{M}(F)) = 1$, let

$$S_{E_i} = \{m_{j,1}, \ldots, m_{j,d_j} | 1 \leq j \leq n_0 \text{ and } \det(M_{E_i, m_{j,r}}(Y)) = 1 \text{ for } 1 \leq r \leq d_j\}$$

be an index set. If there is a permutation σ on the set $\{0, 1, \ldots, n_0\}$ such that $S_{E_{\sigma(1)}} \subseteq S_{E_{\sigma(2)}} \subseteq \cdots \subseteq S_{E_{\sigma(n_0)}}$, then the coefficient vectors $E_1(Y), \ldots, E_{n_0}(Y)$ are called ordered.

If the coefficient vectors are ordered, then they can be sorted to satisfy that $S_{E_1} \subseteq S_{E_2} \subseteq \cdots \subseteq S_{E_{n_0}}$. Sometimes, there may not exist the permutation σ. Therefore, $E_1(Y), E_2(Y), \ldots, E_{n_0}(Y)$ cannot be sorted by Definition 5. In this case, we say that the coefficient vectors of F_s are disordered. It is worth noting that Definition 5 only makes sense under the condition that $\det(\mathcal{M}(F)) = 1$. Here is an example to explain Definition 5.

Example 4 Let the following system of quadratic equations

$$\begin{pmatrix} f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \end{pmatrix} = \begin{pmatrix} 1\,0\,0\,0\,0 \\ 0\,0\,1\,0\,0 \\ 0\,1\,0\,0\,0 \\ 0\,0\,0\,1\,0 \\ 0\,0\,0\,0\,1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} \oplus \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} x_1x_2 \oplus \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} x_2x_3 \oplus \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} x_1x_4$$

be the function F, where $a_j \in \mathbb{F}_2$ for $1 \leq j \leq 5$. It is clear that the critical matrix satisfies that $\det(\mathcal{M}(F)) = 1$ and $S_{E_1} = \{1, 2, 3\}, S_{E_2} = \{2, 3\}, S_{E_3} = \{1, 2, 3, 4\}$. Then the coefficient vectors of F are ordered for $S_{E_2} \subseteq S_{E_1} \subseteq S_{E_3}$.

In the following, we will give the main results in this section. Before this, let us recall that an n-stage Galois NFSR with a feedback function F is nonsingular if and only if F is an invertible function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. Therefore, we shall show that the internal state update function

$$(x_0(t+1), x_1(t+1), \ldots, x_{n-1}(t+1)) = F(x_0(t), x_1(t), \ldots, x_{n-1}(t)), t \geq 0,$$

is invertible.

For an integer $t \geq 0$, let $X(t) = (x_0(t), x_1(t), \ldots, x_{n-1}(t))$ be the internal state of NFSR(F) at the time instance t. Suppose there are exactly $k \geq 1$ feedback registers in NFSR(F) given by

$$\Omega(F) = [i_k + l_k, \ldots, i_k] \parallel [i_{k-1} + l_{k-1}, \ldots, i_{k-1}] \parallel \cdots \parallel [i_1 + l_1, \ldots, i_1],$$

where $l_j \geq 0$ for $1 \leq j \leq k$ and $i_k > i_{k-1} > \cdots > i_1 = 0$. Let $\tilde{X}(t)$ denote the vector derived from $X(t)$ by removing $x_{i_1}(t), x_{i_2}(t), \ldots, x_{i_k}(t)$ from $X(t)$, i.e.,

$$\tilde{X}(t) = (x_{i_1+1}(t), \ldots, x_{i_2-1}(t), x_{i_2+1}(t), \ldots, x_{i_3-1}(t), \ldots, x_{i_k+1}(t), \ldots, x_{n-1}(t)).$$

Let

$$\hat{X}(t+1) = (x_{i_1}(t+1), \ldots, x_{i_2-2}(t+1), x_{i_2}(t+1), \ldots, x_{i_3-2}(t+1), \ldots, x_{i_k}(t+1), \ldots, x_{n-2}(t+1)),$$

which is completely determined by $\tilde{X}(t)$ because of the shifting relation. Then we have

$$\begin{pmatrix} x_{i_1+l_1}(t+1) \\ x_{i_2+l_2}(t+1) \\ \vdots \\ x_{i_k+l_k}(t+1) \end{pmatrix} = \begin{pmatrix} D_1(\tilde{X}(t)) \\ D_2(\tilde{X}(t)) \\ \vdots \\ D_k(\tilde{X}(t)) \end{pmatrix} \oplus M(\tilde{X}(t)) \cdot \begin{pmatrix} x_{i_1}(t) \\ x_{i_2}(t) \\ \vdots \\ x_{i_k}(t) \end{pmatrix} \oplus \left(\bigoplus_{\boldsymbol{\alpha} \in \mathbb{F}_2^k} \begin{pmatrix} E_{\boldsymbol{\alpha},1}(\tilde{X}(t)) \\ E_{\boldsymbol{\alpha},2}(\tilde{X}(t)) \\ \vdots \\ E_{\boldsymbol{\alpha},k}(\tilde{X}(t)) \end{pmatrix} x_{i_1}^{\alpha_1}(t) \cdots x_{i_k}^{\alpha_k}(t) \right).$$

Since $\tilde{X}(t) = \hat{X}(t+1)$, we only need to prove that $(x_{i_1}(t), x_{i_2}(t), \ldots, x_{i_k}(t))$ could be uniquely determined by $X(t+1)$. Thus, NFSR(F) is nonsingular if and only if F_s is invertible. Let

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_k \end{pmatrix} = \begin{pmatrix} D_{i_1}(\tilde{X}(t)) \\ D_{i_2}(\tilde{X}(t)) \\ \vdots \\ D_{i_k}(\tilde{X}(t)) \end{pmatrix} \oplus \begin{pmatrix} x_{i_1+l_1}(t+1) \\ x_{i_2+l_2}(t+1) \\ \vdots \\ x_{i_k+l_k}(t+1) \end{pmatrix}.$$

It is clear that $(a_1, a_2, \ldots, a_k)^\top$ is completely determined by $X(t+1)$.

Lemma 2 *If a general Galois NFSR whose simplified feedback function F_s given by (1) has only one nonlinear term satisfies the condition that the determinant of the matrix $M_{E,j}(F)$ is equal to 1, i.e., $\det(M_{E,j}(F)) = 1$ for $j \in S \cup \{0\}$, then NFSR(F) is nonsingular.*

Proof It suffices to consider the case $d = 2$ since the general case follows easily by induction. Without loss of generality, let $x_{i_k} x_{i_{k-1}}$ be the quadratic term of F_s. For every $X(t+1) \in \mathbb{F}_2^n$, we distinguish two cases.

In the first case, let $x_{i_k}(t) = 0$. Then we have

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_k \end{pmatrix} = \begin{pmatrix} C_{1,1}(\tilde{X}(t)) & \cdots & C_{1,k-1}(\tilde{X}(t)) \\ C_{2,1}(\tilde{X}(t)) & \cdots & C_{2,k-1}(\tilde{X}(t)) \\ \vdots & \ddots & \vdots \\ C_{k,1}(\tilde{X}(t)) & \cdots & C_{k,k-1}(\tilde{X}(t)) \end{pmatrix} \begin{pmatrix} x_{i_1}(t) \\ x_{i_2}(t) \\ \vdots \\ x_{i_{k-1}}(t) \end{pmatrix}. \tag{2}$$

Let $\tilde{M}_0$ be the coefficient matrix of (2). Since $\det(\mathcal{M}(F)) = 1$ and $\tilde{X}(t) = \hat{X}(t+1)$, there exists a matrix P_1 over $\mathbb{F}_2$ such that

$$P_1 \begin{pmatrix} C_{1,1}(\tilde{X}(t)) & \cdots & C_{1,k}(\tilde{X}(t)) \\ C_{2,1}(\tilde{X}(t)) & \cdots & C_{2,k}(\tilde{X}(t)) \\ \vdots & \ddots & \vdots \\ C_{k,1}(\tilde{X}(t)) & \cdots & C_{k,k}(\tilde{X}(t)) \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}_{k \times k}.$$

Let

$$\begin{pmatrix} \tilde{a}_1 \\ \tilde{a}_2 \\ \vdots \\ \tilde{a}_k \end{pmatrix} = P_1 \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_k \end{pmatrix}.$$

Then we have

$$\begin{pmatrix} \tilde{a}_1 \\ \tilde{a}_2 \\ \vdots \\ \tilde{a}_k \end{pmatrix} = \begin{pmatrix} 1\ 0 \cdots\ 0 \\ 0\ 1 \cdots\ 0 \\ \vdots\ \vdots\ \ddots\ \vdots \\ 0\ 0 \cdots\ 0 \end{pmatrix} \begin{pmatrix} x_{i_1}(t) \\ x_{i_2}(t) \\ \vdots \\ x_{i_{k-1}}(t) \end{pmatrix}$$

by multiplying P_1 to (2). If $\tilde{a}_k = 0$, then there exists only one solution of (2) because $\mathrm{rank}(\tilde{M}_0) = k-1$. If $\tilde{a}_k = 1$, then there exists no solutions of (2).

In the remaining case, let $x_{i_k}(t) = 1$ and $R_{k-1}(\tilde{X}(t)) = C_{k-1}(\tilde{X}(t)) \oplus E(\tilde{X}(t))$. Then we have

$$\begin{pmatrix} a_1 \oplus C_{1,k}(\tilde{X}(t)) \\ a_2 \oplus C_{2,k}(\tilde{X}(t)) \\ \vdots \\ a_k \oplus C_{k,k}(\tilde{X}(t)) \end{pmatrix} = \begin{pmatrix} C_{1,1}(\tilde{X}(t)) \cdots\ R_{k-1,1}(\tilde{X}(t)) \\ C_{2,1}(\tilde{X}(t)) \cdots\ R_{k-1,2}(\tilde{X}(t)) \\ \vdots\ \ddots\ \vdots \\ C_{k,1}(\tilde{X}(t)) \cdots\ R_{k-1,k}(\tilde{X}(t)) \end{pmatrix} \begin{pmatrix} x_{i_1}(t) \\ x_{i_2}(t) \\ \vdots \\ x_{i_{k-1}}(t) \end{pmatrix}. \quad (3)$$

It follows from Lemma 1 that $E(\tilde{X}(t)) = \bigoplus_{u=1}^{k-2} \beta_u C_u(\tilde{X}(t))$, and so $R_{k-1}(\tilde{X}(t)) = \bigoplus_{u=1}^{k-1} \beta_u C_u(\tilde{X}(t))$ for $\beta_{k-1} = 1$. Then we have

$$\begin{pmatrix} \tilde{a}_1 \\ \tilde{a}_2 \\ \vdots \\ \tilde{a}_k \oplus 1 \end{pmatrix} = \begin{pmatrix} 1\ 0 \cdots\ \beta_1 \\ 0\ 1 \cdots\ \beta_2 \\ \vdots\ \vdots\ \ddots\ \vdots \\ 0\ 0 \cdots\ 0 \end{pmatrix} \begin{pmatrix} x_{i_1}(t) \\ x_{i_2}(t) \\ \vdots \\ x_{i_{k-1}}(t) \end{pmatrix}$$

by multiplying P_1 to (3). Similar to the case of $x_{i_k}(t) = 0$, if $\tilde{a}_k = 1$, then there exists only one solution of (3). If $\tilde{a}_k = 0$, then there exists no solutions of (3). Meanwhile, because the value of $\tilde{a}_k$ only depends on the value of $X(t+1)$, it is impossible that the system of equations has a solution for $x_{i_k}(t) = 0$ and $x_{i_k}(t) = 1$ simultaneously.

Therefore, for every $X(t+1) \in \mathbb{F}_2^n$, there exists only one value of $X(t)$ such that $(x_0(t+1), x_1(t+1), \ldots, x_{n-1}(t+1)) = F(x_0(t), x_1(t), \ldots, x_{n-1}(t))$, i.e., the feedback function F is invertible. □

Lemma 3 *If a quadratic Galois NFSR with simplified feedback function F_s given by (1) satisfies the following three conditions:*

(1) $\det(\mathcal{M}(F)) = 1$,
(2) $S_j = \{m_{j,1}, m_{j,2}\} \subseteq S_{E_j}$, $1 \le j \le n_0$,
(3) the coefficient vectors of F_s are ordered,

then the quadratic Galois NFSR is nonsingular.

Proof We proceed by induction on n_0 and note that the case $n_0 = 1$ follows from Lemma 2. Suppose the proposition is true for F_s with quadratic terms less than n_0. When F_s has n_0 quadratic terms, we distinguish the cases of $x_{i_r}(t) = 0$ and $x_{i_r}(t) = 1$ for $r \in S$. Since the proof is similar to that of Lemma 2, we omit it. □

Similar to Lemma 3, we give a sufficient condition to determine whether a general Galois NFSR is nonsingular or not.

Theorem 1 *If a general Galois NFSR with the simplified feedback function F_s given by (1) satisfies the following three conditions:*

(1) $\det(\mathcal{M}(F)) = 1$,
(2) $S_j = \{m_{j,1}, \ldots, m_{j,d_j}\} \subseteq S_{E_j}$, $1 \le j \le n_0$,
(3) the coefficient vectors of F_s are ordered,

then the Galois NFSR is nonsingular.

Proof It follows from Lemmas 2 and 3 that if either $n_0 = 1$ or $d = 2$, then the result is clearly true. We proceed now by double induction. Suppose $d > 2$, $n_0 > 1$ and that the result is true for the simplified feedback function F_s with at most n_0 nonlinear terms of degree less than d and for F_s with less than n_0 nonlinear terms of degree at most d.

Without loss of generality, let $S_{E_1} \subseteq S_{E_2} \subseteq \cdots \subseteq S_{E_{n_0}}$. Let $d_r = \min\{d_j | 1 \le j \le n_0\}$ and we use induction on d_r. For every $X(t+1) \in \mathbb{F}_2^n$, when $d_r = 2$, let $x_{i_{m_{r,1}}} x_{i_{m_{r,2}}} = x_{i_k} x_{i_{k-1}}$. We distinguish two cases. Let $x_{i_k}(t) = 0$. Then we have

$$\begin{pmatrix} a_1(\tilde{X}(t)) \\ a_2(\tilde{X}(t)) \\ \vdots \\ a_k(\tilde{X}(t)) \end{pmatrix} = \begin{pmatrix} C_{1,1}(\tilde{X}(t)) & \cdots & C_{1,k-1}(\tilde{X}(t)) \\ C_{2,1}(\tilde{X}(t)) & \cdots & C_{2,k-1}(\tilde{X}(t)) \\ \vdots & \ddots & \vdots \\ C_{k,1}(\tilde{X}(t)) & \cdots & C_{k,k-1}(\tilde{X}(t)) \end{pmatrix} \begin{pmatrix} x_{i_1}(t) \\ x_{i_2}(t) \\ \vdots \\ x_{i_{k-1}}(t) \end{pmatrix} \oplus \begin{pmatrix} \bigoplus_{j=1, j\neq r}^{n_0} \begin{pmatrix} E_{j,1}(\tilde{X}(t)) \\ E_{j,2}(\tilde{X}(t)) \\ \vdots \\ E_{j,k}(\tilde{X}(t)) \end{pmatrix} x_{i_{m_{j,1}}}(t) \cdots x_{i_{m_{j,d_j}}}(t) \end{pmatrix}. \quad (4)$$

Since $\det(\mathcal{M}(F)) = 1$, i.e., $\operatorname{rank}(M(\tilde{X}(t))) = k$, there exists a matrix P_2 over $\mathbb{F}_2$ such that

$$P_2 \cdot \begin{pmatrix} C_{1,1}(\tilde{X}(t)) & \cdots & C_{1,k}(\tilde{X}(t)) \\ C_{2,1}(\tilde{X}(t)) & \cdots & C_{2,k}(\tilde{X}(t)) \\ \vdots & \ddots & \vdots \\ C_{k,1}(\tilde{X}(t)) & \cdots & C_{k,k}(\tilde{X}(t)) \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}_{k\times k}.$$

Meanwhile, since $S_{E_1} \subseteq S_{E_2} \subseteq \cdots \subseteq S_{E_{n_0}}$, it follows from Lemma 1 and Definition 5 that for $1 \le j \le n_0$, $E_j(\tilde{X}(t)) = \bigoplus_{u=1}^{k} \beta_{j,u} C_u(\tilde{X}(t))$, where $\beta_{j,u} = 0$ for $u \in S_{E_j}$. Let

$$\begin{pmatrix} g_1 \\ g_2 \\ \vdots \\ g_k \end{pmatrix} = \left(\bigoplus_{j=1}^{r-1} \begin{pmatrix} \beta_{j,1} \\ \beta_{j,2} \\ \vdots \\ \beta_{j,k} \end{pmatrix} \cdot \left(\prod_{m\in S_j} x_{i_m} \right) \right) \oplus \left(\bigoplus_{j=r+1}^{n_0} \begin{pmatrix} \beta_{j,1} \\ \beta_{j,2} \\ \vdots \\ 0 \end{pmatrix} \cdot \left(\prod_{m\in S_j} x_{i_m} \right) \right).$$

Then we have

$$\begin{pmatrix} \tilde{a}_1 \\ \tilde{a}_2 \\ \vdots \\ \tilde{a}_k \end{pmatrix} = \begin{pmatrix} 1\ 0 \cdots\ 0 \\ 0\ 1 \cdots\ 0 \\ \vdots\ \vdots\ \ddots\ \vdots \\ 0\ 0 \cdots\ 0 \end{pmatrix} \begin{pmatrix} x_{i_1}(t) \\ x_{i_2}(t) \\ \vdots \\ x_{i_{k-1}}(t) \end{pmatrix} \oplus \begin{pmatrix} g_1 \\ g_2 \\ \vdots \\ g_k \end{pmatrix}.$$

Using the induction hypothesis, if $\tilde{a}_k = g_k$, then the equation has one solution. Otherwise, the equation has no solutions.

Let $x_{i_k}(t) = 1$. Thus, similar to the case of $x_{i_k}(t) = 0$, we have

$$\begin{pmatrix} \tilde{a}_1 \\ \tilde{a}_2 \\ \vdots \\ \tilde{a}_k \oplus 1 \end{pmatrix} = \begin{pmatrix} 1\ 0 \cdots\ \beta_{r,1} \\ 0\ 1 \cdots\ \beta_{r,2} \\ \vdots\ \vdots\ \ddots\ \vdots \\ 0\ 0 \cdots\ 0 \end{pmatrix} \begin{pmatrix} x_{i_1}(t) \\ x_{i_2}(t) \\ \vdots \\ x_{i_{k-1}}(t) \end{pmatrix} \oplus \begin{pmatrix} g_1 \\ g_2 \\ \vdots \\ g_k \end{pmatrix},$$

where $\beta_{r,u} = 0$ for $u \in S_{E_r}$. For $u \in S_{E_{r-1}}$, we have

$$\tilde{a}_u = x_{i_u}(t) \oplus g_u = x_{i_u}(t) \oplus (\bigoplus_{j=1}^{r-1} \beta_{j,u} \cdot x_{i_{m_{j,1}}}(t) \cdots x_{i_{m_{j,d_j}}}(t)),$$

which implies that the value of $x_{i_u}(t)$ is independent of the value of $x_{i_k}(t)$. Then the value of g_k is not dependent on the value of $x_{i_k}(t)$. Using the induction hypothesis, if $\tilde{a}_k \oplus 1 = g_k$, then the equation has one solution. If $\tilde{a}_k = g_k$, then the equation has no solutions. Since the values of $\tilde{a}_k$ and g_k are independent of the value of $x_{i_k}(t)$, it is impossible that the system of equations has a solution for $x_{i_k}(t) = 0$ and $x_{i_k}(t) = 1$ simultaneously. Therefore, F_s is invertible when $d_r = 2$.

Suppose that the result holds for $d_r \leq N-1$. When $d_r = N$, let $x_{i_{m_{r,1}}}(t) = 0$. Then the number of nonlinear terms is not greater than $n-1$. Using the induction hypothesis, if the system of equations has a solution, then it has only one solution. If the system of equations has no solution, then we let $x_{i_{m_{r,1}}}(t) = 1$ and d'_r of new function is less than or equal to $N-1$. By the induction hypothesis, it has only one solution. Meanwhile, for the same $X(t+1) \in \mathbb{F}_2^n$, it is impossible that the system of equations has a solution for $x_{i_k}(t) = 0$ and $x_{i_k}(t) = 1$ simultaneously. □

Theorem 1 is not a necessary condition. In the following, we will give an example of F which is invertible but not satisfy the condition.

Example 5 Let NFSR(F) be a standard Galois NFSR with a quadratic simplified feedback function F_s given by

$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \end{pmatrix} = \begin{pmatrix} 1\ 0\ 0\ 0\ 0 \\ 0\ 1\ 0\ 0\ 0 \\ 0\ 0\ 1\ 0\ 0 \\ 0\ 0\ 0\ 1\ 0 \\ 0\ 0\ 0\ 0\ 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} \oplus \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} x_1x_2 \oplus \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} x_1x_5$$
$$\oplus \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} x_2x_3 \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} x_2x_5 \oplus \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} x_3x_4 \oplus \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} x_4x_5,$$

where $a_j \in \mathbb{F}_2$ for $1 \leq j \leq 5$. It is easy to check that F_s is invertible while does not satisfy the conditions of Theorem 1.

5 A necessary and sufficient condition for Galois NFSRs with linear simplified feedback functions

In this section, we give a necessary and sufficient condition for determining the nonsingularity of a large class of Galois NFSRs with linear simplified feedback functions. It means that there is no product term on the variables $x_{i_1}, x_{i_2}, \ldots, x_{i_k}$ occurring in every feedback computation, which is a very weak restriction on NFSRs. This type of Galois NFSRs will be shown to have potential usage in practice in Sect. 6.

Theorem 2 *A Galois* NFSR(F) *with a linear simplified feedback function is nonsingular if and only if the determinant of the matrix* $\mathcal{M}(F)$ *is equal to 1, i.e.,* $\det(\mathcal{M}(F)) = 1$*, which is a constant independent of* Y*.*

Proof Suppose there are exactly $k \geq 1$ feedback registers in NFSR(F) given by

$$\Omega(F) = [i_k + l_k, \ldots, i_k] \parallel [i_{k-1} + l_{k-1}, \ldots, i_{k-1}] \parallel \cdots \parallel [i_1 + l_1, \ldots, i_1].$$

Let

$$f_{i_j+l_j}(x_0, \ldots, x_{n-1}) = D_{i_j}(Y) \oplus \left(\sum_{u=1}^{k} C_{j,u}(Y) \cdot x_{i_u} \right), j = 1, 2, \ldots, k, \quad (5)$$

be the simplified feedback function F_s. Since $\tilde{X}(t)$ can be completely determined by $\hat{X}(t+1)$ for the shifting relation, NFSR(F) is nonsingular if and only if F_s is invertible. Then we have

$$\begin{pmatrix} x_{i_1+l_1}(t+1) \\ x_{i_2+l_2}(t+1) \\ \vdots \\ x_{i_k+l_k}(t+1) \end{pmatrix} = \begin{pmatrix} D_{i_1}(\tilde{X}(t)) \\ D_{i_2}(\tilde{X}(t)) \\ \vdots \\ D_{i_k}(\tilde{X}(t)) \end{pmatrix} \oplus M(\tilde{X}(t)) \cdot \begin{pmatrix} x_{i_1}(t) \\ x_{i_2}(t) \\ \vdots \\ x_{i_k}(t) \end{pmatrix}.$$

Since $\det(\mathcal{M}(F)) = 1$, it follows that $M(\tilde{X}(t))$ is invertible. Consequently

$$\begin{pmatrix} x_{i_1}(t) \\ x_{i_2}(t) \\ \vdots \\ x_{i_k}(t) \end{pmatrix} = (M(\hat{X}(t+1)))^{-1} \cdot \begin{pmatrix} x_{i_1+l_1}(t+1) - D_1(\hat{X}(t+1)) \\ x_{i_2+l_2}(t+1) - D_2(\hat{X}(t+1)) \\ \vdots \\ x_{i_k+l_k}(t+1) - D_k(\hat{X}(t+1)) \end{pmatrix}.$$

Therefore, this shows that F_s is invertible.

Assume the simplified feedback function F_s is invertible. Suppose $\det(\mathcal{M}(F)) \neq 1$. Then $\det(\mathcal{M}(F)) = 0$ or $\det(\mathcal{M}(F))$ is a Boolean function on Y which is not a constant, say $\det(\mathcal{M}(F)) = h(Y)$. Since $h(Y)$ is not a constant function, there is at least one evaluation of Y, say $Y = P$, such that $h(P) = 0$. Thus, in either case, there exists one evaluation of $Y = P$ such that $\det(M(P)) = 0$.

Let $X(t+1)$ be a state such that $\hat{X}(t+1) = P$. Then $\det(M(\hat{X}(t+1))) = 0$. Since $\tilde{X}(t) = \hat{X}(t+1)$, we have the following system of linear equations

$$M(\hat{X}(t+1)) \cdot \begin{pmatrix} x_{i_1}(t) \\ x_{i_2}(t) \\ \vdots \\ x_{i_k}(t) \end{pmatrix} = \begin{pmatrix} x_{i_1+l_1}(t+1) \\ x_{i_2+l_2}(t+1) \\ \vdots \\ x_{i_k+l_k}(t+1) \end{pmatrix} \oplus \begin{pmatrix} D_1(\hat{X}(t+1)) \\ D_2(\hat{X}(t+1)) \\ \vdots \\ D_k(\hat{X}(t+1)) \end{pmatrix} \tag{6}$$

in the variables $x_{i_1}(t), x_{i_2}(t), \ldots, x_{i_k}(t)$. Since $\det(M(\hat{X}(t+1))) = 0$, it follows that the system of equations (6) has more than one solution, a contradiction to the assumption that F_s is invertible. Hence, we have $\det(\mathcal{M}(F)) = 1$. □

For a Fibonacci NFSR(F), there is only one feedback register, and so its critical matrix $\mathcal{M}(F)$ is just given by

$$\mathcal{M}(F) = (h(y)), \tag{7}$$

which is a 1×1 matrix. Then by Theorem 2, this NFSR(F) is nonsingular if and only if $h(y) = 1$, a constant Boolean function. That is to say, a Fibonacci NFSR(F) is nonsingular if and only if the feedback function F can be written as $F = f(x_1, \ldots, x_{n-1}) \oplus x_0$. This is just the result given by Golomb in [12, Chapter VI, Theorem 1]. Hence, Theorem 2 can be seen as a generalization of Golomb's classic result on Fibonacci NFSRs to Galois NFSRs.

6 Applications

In this section, we apply our results to some known and new NFSRs, to show the validity of our results. In the following, let k and n be positive integers and a matrix is always over the Boolean function ring.

6.1 Trivium

Trivium is a bit-oriented stream cipher designed by Canniére and Preneel [7]. It was selected as one of the eSTREAM portfolio ciphers in 2008. Trivium attracted lots of cryptanalysis because of its simple design. The main building block of Trivium is a 288-stage NFSR, see Figure 4. Let us denote its feedback function by $F_{\text{Trivium}} = (f_0, f_1, \ldots, f_{287})$ where

$$\begin{aligned} f_{110} &= x_{24} \oplus x_{126} \oplus \boldsymbol{x_{111}} \oplus x_{112}x_{113} \\ f_{194} &= x_{117} \oplus x_{222} \oplus \boldsymbol{x_{195}} \oplus x_{196}x_{197} \\ f_{287} &= x_{219} \oplus x_{45} \oplus \boldsymbol{x_0} \oplus x_1x_2 \\ f_i &= x_{i+1}, i \notin \{110, 194, 287\}. \end{aligned}$$

It can be seen that

$$\Omega(F_{\text{Trivium}}) = [287, \ldots, 195] \parallel [194, \ldots, 111] \parallel [110, \ldots, 0],$$

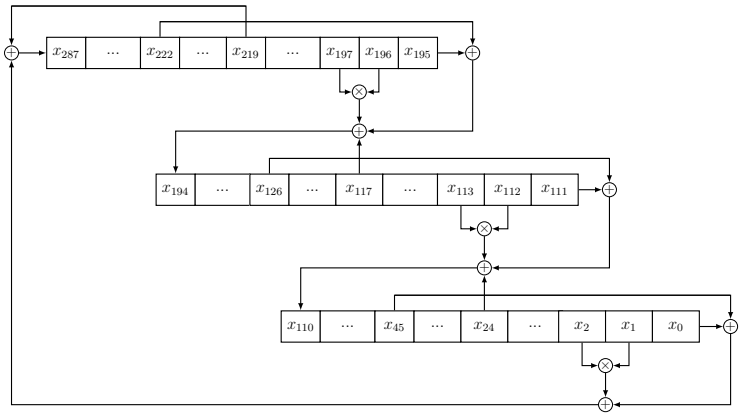

Fig. 4: The main register of Trivium

and the simplified feedback function of Trivium is linear. The critical matrix of F_{TRIVIUM} is clearly given by

$$\mathcal{M}(F_{\text{TRIVIUM}}) = \begin{pmatrix} 0\,1\,0 \\ 0\,0\,1 \\ 1\,0\,0 \end{pmatrix}.$$

It is obvious that $\det(\mathcal{M}(F_{\text{TRIVIUM}})) = 1$, and so the main register of Trivium is nonsingular by Theorem 2.

We note that the nonsingularity of the main register of Trivium is not a new result, see [7, 15–17]. But here we just want to show that our new method is valid and simple.

6.2 SPRING

SPRING is a lightweight block cipher based on NFSRs proposed in [18], where the name SPRING means an **SP**N cipher with **ring**-like cascade connection of NFSRs. In particular, the Sbox used in SPRING is a 32-stage Galois NFSR called NFSR-SR, see Figure 5, whose feedback function $F_{\text{SPRING}} = (f_0, f_1, \ldots, f_{31})$ is given by

$$\begin{aligned} f_7 &= x_4x_5 \oplus \boldsymbol{x_0} \oplus x_2 \oplus \boldsymbol{x_8} \oplus \boldsymbol{x_{16}} \\ f_{15} &= x_{12}x_{13} \oplus \boldsymbol{x_8} \oplus x_{11} \oplus \boldsymbol{x_{16}} \oplus \boldsymbol{x_{24}} \\ f_{23} &= x_{19}x_{20} \oplus \boldsymbol{x_{16}} \oplus x_{21} \oplus \boldsymbol{x_0} \oplus \boldsymbol{x_{24}} \\ f_{31} &= x_{27}x_{28} \oplus \boldsymbol{x_{24}} \oplus x_{30} \oplus \boldsymbol{x_0} \oplus \boldsymbol{x_8} \\ f_i &= x_{i+1}, i \notin \{7, 15, 23, 31\}. \end{aligned}$$

It can be seen that

$$\Omega(F_{\text{SPRING}}) = [31, \ldots, 24] \parallel [23, \ldots, 16] \parallel [15, \ldots, 8] \parallel [7, \ldots, 0],$$

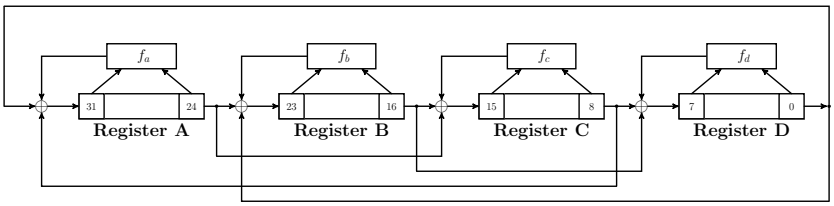

Fig. 5: An overview of NFSR-SR in SPRING

and the simplified feedback function of SPRING is linear. The critical matrix of F_{SPRING} is given by

$$\mathcal{M}(F_{\text{SPRING}}) = \begin{pmatrix} 1\,1\,1\,0 \\ 0\,1\,1\,1 \\ 1\,0\,1\,1 \\ 1\,1\,0\,1 \end{pmatrix}.$$

It can be seen that $\det(\mathcal{M}(F_{\text{SPRING}})) = 1$, and so NFSR-SR is nonsingular by Theorem 2. Also this is not a new result, it was proved that NFSR-SR is nonsingular in [18].

6.3 A large class of nonsingular Galois NFSRs with linear simplified feedback functions

In the following, we show that starting from an identity matrix, we can construct various nonsingular Galois NFSRs.

We are concerned with the following two elementary operations which does not change the determinant of a matrix.

- Interchange two columns (or rows) of a matrix A.
- A multiple of the kth column (or row) is added to the jth column (or row) of a matrix A. We remark that here all the entries of the kth column (or row) is multiplied by a Boolean function.

Proposition 2 *Let* NFSR(F) *be an n-stage Galois NFSR with a linear simplified feedback function. If the critical matrix $\mathcal{M}(F)$ could be reduced to an identity matrix by performing a sequence of elementary operations, then* NFSR(F) *is nonsingular.*

Proof Since an elementary operation does not change the determinant, it is clear that $\det(\mathcal{M}(F)) = \det(I_n) = 1$, where I_n is an $n \times n$ identity matrix. Thus, by Theorem 2, NFSR(F) is nonsingular. □

A. An upper triangular case

Let NFSR(F_{upper}) be an n-stage Galois NFSR with a linear simplified feedback function, and let its critical matrix $\mathcal{M}(F_{\text{upper}})$ be an upper triangular matrix, say

$$\mathcal{M}(F_{\text{upper}}) = \begin{pmatrix} 1 & * & \cdots & * \\ 0 & 1 & \cdots & * \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}_{k\times k}$$

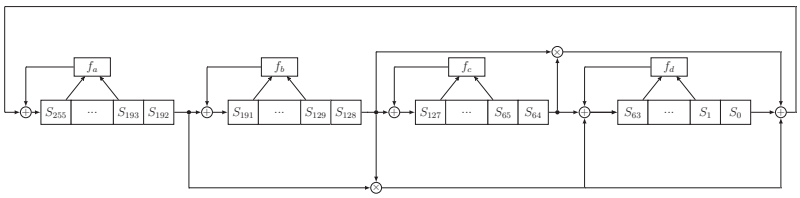

Fig. 6: A 256-stage nonsingular Galois NFSR

where $*$ can be either 0 or 1 or a Boolean function in $Y = X \setminus \{x_{i_1}, x_{i_2}, \ldots, x_{i_k}\}$. Then NFSR($F_{\text{upper}}$) is nonsingular by Theorem 2 since $\det(\mathcal{M}(F_{\text{upper}})) = 1$.

B. A lower anti-triangle case

As an analogy, if an n-stage Galois NFSR(F_{lower}) with a linear simplified feedback function has the critical matrix of the form

$$\mathcal{M}(F_{\text{lower}}) = \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 0 & \cdots & 1 & * \\ \vdots & \vdots & \vdots & \vdots \\ 1 & * & \cdots & * \end{pmatrix}_{k \times k},$$

where $*$ can be either 0 or 1 or a Boolean function in $Y = X \setminus \{x_{j_1}, x_{j_2}, \ldots, x_{j_k}\}$, then NFSR($F_{\text{lower}}$) is nonsingular by Theorem 2 since $\det(\mathcal{M}(F_{\text{lower}})) = 1$.

NFSR(F_{upper}) and NFSR(F_{lower}) are inequivalent NFSRs, whose proof is given in Appendix.

6.4 A large class of nonsingular Galois NFSRs with quadratic simplified feedback functions

Let NFSR(F_{order}) be an n-stage Galois NFSR with k feedback registers labeled by $\{x_{i_1}, x_{i_2}, \ldots, x_{i_k}\}$, and the simplified feedback function F_s be given by

$$\begin{pmatrix} f_{i_1+l_1} \\ f_{i_2+l_2} \\ \vdots \\ f_{i_k+l_k} \end{pmatrix} = \begin{pmatrix} D_{i_1}(Y) \\ D_{i_2}(Y) \\ \vdots \\ D_{i_k}(Y) \end{pmatrix} \oplus \mathcal{M}(F_{\text{order}}) \begin{pmatrix} x_{i_1} \\ x_{i_2} \\ \vdots \\ x_{i_k} \end{pmatrix} \oplus \left(\bigoplus_{j=1}^{n_0} \begin{pmatrix} E_{j,1}(Y) \\ E_{j,2}(Y) \\ \vdots \\ E_{j,k}(Y) \end{pmatrix} x_{i_j} x_{i_{j+1}} \right),$$

where $1 \le n_0 \le k-2$. If F_{order} satisfies the following conditions:

- The determinant of $\mathcal{M}(F_{\text{order}})$ is equal to 1, i.e., $\det(\mathcal{M}(F_{\text{order}})) = 1$,
- $E_j(Y) = \bigoplus_{m=j+2}^{n_0+1} C_m(Y)$ for $1 \le j \le n_0 - 1$, and $E_{n_0}(Y) = C_{n_0+2}(Y)$, where $C_m(Y) = (C_{m,1}(Y), C_{m,2}(Y), \ldots, C_{m,k}(Y))^\top$ is the mth column of $\mathcal{M}(F_{\text{order}})$ and $E_j(Y) = (E_{j,1}(Y), E_{j,2}(Y), \ldots, E_{j,k}(Y))^\top$ is the coefficient vector of term $x_j x_{j+1}$,

then NFSR(F_{order}) is nonsingular by Theorem 1.

Example 6 A 256-stage Galois NFSR with 4 feedback registers is depicted in Figure 6. Let $Y = X \setminus \{x_0, x_{64}, x_{128}, x_{192}\}$. The feedback function F could be written as

$$\begin{aligned} f_{191} &= f_b(Y) \oplus x_{192}, \\ f_{127} &= f_c(Y) \oplus x_{128}, \\ f_{63} &= f_d(Y) \oplus x_{64} \oplus x_{192}x_{128}, \\ f_{255} &= f_a(Y) \oplus x_{192}x_{128} \oplus x_{128}x_{64} \oplus x_0, \\ f_l &= x_{l+1}, l \in Y. \end{aligned}$$

The simplified feedback function F_s is

$$\begin{pmatrix} f_{191} \\ f_{127} \\ f_{63} \\ f_{255} \end{pmatrix} = \begin{pmatrix} f_a(Y) \\ f_b(Y) \\ f_c(Y) \\ f_d(Y) \end{pmatrix} \oplus \begin{pmatrix} 1\,0\,0\,0 \\ 0\,1\,0\,0 \\ 0\,0\,1\,0 \\ 0\,0\,0\,1 \end{pmatrix} \begin{pmatrix} x_{192} \\ x_{128} \\ x_{64} \\ x_0 \end{pmatrix} \oplus \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} x_{192}x_{128} \oplus \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} x_{128}x_{64}.$$

It is easy to check that NFSR(F) is nonsingular by Theorem 1.

7 Discussion

In the previous sections, we give some new results on nonsingular Galois NFSRs. In this section, we demonstrate the relation between the previous works [13, 14] and ours and prove that the Galois classes given in [13, 14] and this paper are not covered by each other.

In [14], the authors proposed two types of Galois NFSRs called Triangulation-I and Triangulation-II, and presented the necessary and sufficient conditions for their nonsingularity. It was proved in [14] that a Galois NFSR(F) belonging to Triangulation-I is nonsingular if and only if it can be written

$$\begin{aligned} f_0 &= g_0(x_0, x_1, \cdots, x_{n-2}) \oplus x_{n-1}, \\ f_i &= g_i(x_0, x_1, \cdots, x_{i-2}, f_0) \oplus x_{i-1}, \text{ for } 1 \le i \le n-1. \end{aligned}$$

Then there is a permutation σ on set $\{0, 1, \ldots, n-1\}$ satisfying $\sigma(i) = n-1-i$ such that $\sigma(F)$ is a standard feedback function. Let $F' = \sigma(F)$. Then we have

$$\begin{aligned} f'_i &= g'_i(x_{i+2}, x_{i+3}, \cdots, x_{n-1}, f'_{n-1}) \oplus x_{i+1}, \text{ for } 0 \le i \le n-2, \\ f'_{n-1} &= g'_{n-1}(x_1, x_2, \cdots, x_{n-1}) \oplus x_0. \end{aligned} \tag{8}$$

If $g'_i = 0$, then the $(\sigma^{-1}(i))$th register is a shift register; otherwise, the $(\sigma^{-1}(i))$th register is a feedback register. Then let

$$\Omega(F') = [i_k + l_k, \ldots, i_k] \parallel [i_{k-1} + l_{k-1}, \ldots, i_{k-1}] \parallel \cdots \parallel [i_1 + l_1, \ldots, i_1],$$

where $l_j \geq 0$, $g'_{i_j+l_j} \neq 0$ for $1 \leq j \leq k$ and $i_k > i_{k-1} > \cdots > i_1 = 0$. For $0 \leq j \leq k-1$, let $X_j = \{x_{i_{j+2}}, x_{i_{j+3}}, \ldots, x_{i_k}\}$ and

$$\begin{aligned} f'_{i_j+l_j} &= D_{i_j}(Y) \oplus g'_j(X_j) \oplus (R_j(Y) \oplus h_j(X_j)) f'_{n-1} \oplus x_{i_{j+1}}, \\ f'_{n-1} &= D_{i_k}(Y) \oplus \left(\sum_{u=2}^{k} C_{k,u}(Y) \cdot x_{i_u} \right) \oplus x_0. \end{aligned}$$

Then F' has the critical matrix $\mathcal{M}(F')$ of the form

$$\begin{pmatrix} R_1(Y) & 1 + R_1 C_{k,2}(Y) & \cdots & * & * \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ R_{k-2}(Y) & R_{k-2} C_{k,2}(Y) & \cdots & 1 + R_{k-2} C_{k,k-1}(Y) & * \\ R_{k-1}(Y) & R_{k-1} C_{k,2}(Y) & \cdots & R_{k-1} C_{k,k-1}(Y) & 1 + R_{k-1} C_{k,k}(Y) \\ 1 & C_{k,2}(Y) & \cdots & C_{k,k-1}(Y) & C_{k,k}(Y) \end{pmatrix}.$$

It can be seen that by the elementary operations mentioned in Subsection 6.3, $\mathcal{M}(F')$ is an upper triangular matrix and $\det(\mathcal{M}(F')) = 1$. Since the critical matrix of the nonsingular Galois classes given in this paper is a matrix over the Boolean function ring satisfies that the determination is equal to 1 without any other restrictions, then we have that our works are not covered by Triangulation-I.

In [13], Dubrova introduced the notion of the feedback graph of an NFSR, and proved that the output sequences of an n-stage Galois NFSR can be equivalent to an n-stage Fibonacci NFSR if its feedback graph can be reduced to a single vertex. Meanwhile, a sufficient condition for a feedback graph to be reducible to a single vertex is presented. In [14], the authors proved that the feedback graph of an n-stage nonsingular NFSR(F) can be reduced to a single vertex if and only if the feedback function F satisfies the form

$$\begin{aligned} f_i &= g_i(x_{i+2}, x_{i+3}, \ldots, x_{n-1}) \oplus x_{i+1}, \text{ for } 0 \leq i \leq n-2, \\ f_{n-1} &= g_{n-1}(x_1, x_2, \ldots, x_{n-1}) \oplus x_0. \end{aligned} \tag{9}$$

It can be observed that (9) satisfies the form given in (8). The only difference between them is that in (9), f'_i does not depend on f_{n-1} for $0 \leq i \leq n-2$. Therefore, the Galois class in [13] is included in Triangulation-I and cannot cover our works.

Conversely, a simplified feedback function of the Galois NFSR whose feedback function is given by (9) may be not linear or its coefficient vectors may be not ordered, even though the determination of its critical matrix is equal to 1. For example, consider an n-stage NFSR(F) defined by (9) with $f'_{n-1} = x_0$, $f'_{n-2} = x_{n-1}$, $f'_{n-3} = x_{n-2}$ and $f'_i = x_{i+3}x_{i+2} + x_{i+1}$ for all $0 \leq i \leq n-4$. Since there exist nonlinear terms on the variables $x_1, x_2, \ldots, x_{n-3}$, the simplified feedback function is nonlinear. Meanwhile, it is easy to check that its coefficient vectors are not ordered.

Similarly, it also can be proved that our works and Triangulation-II are not covered by each other.

8 Conclusions

In this paper, a new method for investigating nonsingular Galois NFSRs is proposed. This method is independent of the bit length of the NFSR, greatly reducing the computational complexity of determining the nonsingularity. A necessary and sufficient condition for nonsingular Galois NFSRs with linear simplified feedback functions is proposed. Meanwhile, a new class of general nonsingular Galois NFSRs is presented, which is distinct from previous works. It is expected that those Galois NFSR classes will be useful candidates for designing stream ciphers.

Appendix

In the following, we prove that NFSR(F_{upper}) and NFSR(F_{lower}) are inequivalent NFSRs.

Proposition 3 *If $k > 1$, then* NFSR(F_{upper}) *and* NFSR(F_{lower}) *are inequivalent.*

Proof Suppose NFSR(F_{upper}) and NFSR(F_{lower}) are equivalent. Then there is a permutation σ on the set $\{0, 1, \ldots, n-1\}$ such that $\sigma(F_{\text{upper}}) = F_{\text{lower}}$. Let

$$\Omega(F_{\text{upper}}) = [i_k + l_k, \ldots, i_k] \parallel [i_{k-1} + l_{k-1}, \ldots, i_{k-1}] \parallel \cdots \parallel [i_1 + l_1, \ldots, i_1],$$

and

$$\Omega(F_{\text{lower}}) = [j_k + m_k, \ldots, j_k] \parallel [j_{k-1} + m_{k-1}, \ldots, j_{k-1}] \parallel \cdots \parallel [j_1 + m_1, \ldots, j_1].$$

Note that both NFSR(F_{upper}) and NFSR(F_{lower}) are standard NFSRs, and so σ only permutes the order of $[i_1 + l_1, \ldots, i_1], \ldots, [i_k + l_k, \ldots, i_k]$. Then for $1 \le u \le k$ we have

$$(\sigma(i_u), \sigma(i_u + l_u)) \in \{(j_1, j_1 + m_1), (j_2, j_2 + m_2), \ldots, (j_k, j_k + m_k)\}.$$

Since the entry $a_{u,v}$ in $\mathcal{M}(F_{\text{upper}}) = (a_{u,v})_{k\times k}$ is the coefficient of x_{i_v} in $f_{i_u+l_u}$, it follows that there is a $k \times k$ permutation matrix A such that

$$\mathcal{M}(F_{\text{lower}}) = A \cdot \sigma(\mathcal{M}(F_{\text{upper}})) \cdot A^T. \tag{10}$$

Since

$$A \cdot \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \cdot A^T = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix},$$

we have

$$A \cdot \sigma(\mathcal{M}(F_{\text{upper}})) \cdot A^T = \begin{pmatrix} 1 & \cdots & * & * \\ * & 1 & \cdots & * \\ \vdots & \vdots & \vdots & \vdots \\ * & * & \cdots & 1 \end{pmatrix},$$

i.e., multiplying A on the left and A^T on the right of $\sigma(\mathcal{M}(F_{\text{upper}}))$ will not change the main diagonal. It can be seen that when $k > 1$, the first entry in $\mathcal{M}(F_{\text{lower}})$ is 0 while the first entry in $A \cdot \sigma(\mathcal{M}(F_{\text{upper}})) \cdot A^T$ is 1, a contradiction to (10). Hence, NFSR(F_{upper}) and NFSR(F_{lower}) are inequivalent when $k > 1$. □

References

1. Thomas Johansson and Fredrik Jönsson. Fast correlation attacks through reconstruction of linear polynomials. In Mihir Bellare, editor, *Advances in Cryptology - CRYPTO 2000, 20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2000, Proceedings*, volume 1880 of *Lecture Notes in Computer Science*, pages 300–315. Springer, 2000.
2. Anne Canteaut and Michaël Trabbia. Improved fast correlation attacks using parity-check equations of weight 4 and 5. In Bart Preneel, editor, *Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding*, volume 1807 of *Lecture Notes in Computer Science*, pages 573–588. Springer, 2000.
3. Philippe Chose, Antoine Joux, and Michel Mitton. Fast correlation attacks: An algorithmic point of view. In Lars R. Knudsen, editor, *Advances in Cryptology - EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, April 28 - May 2, 2002, Proceedings*, volume 2332 of *Lecture Notes in Computer Science*, pages 209–221. Springer, 2002.
4. Yi Lu and Serge Vaudenay. Faster correlation attack on bluetooth keystream generator E0. In Matthew K. Franklin, editor, *Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings*, volume 3152 of *Lecture Notes in Computer Science*, pages 407–425. Springer, 2004.
5. Nicolas T. Courtois. Fast algebraic attacks on stream ciphers with linear feedback. In Dan Boneh, editor, *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, volume 2729 of *Lecture Notes in Computer Science*, pages 176–194. Springer, 2003.
6. Nicolas Courtois and Willi Meier. Algebraic attacks on stream ciphers with linear feedback. In Eli Biham, editor, *Advances in Cryptology - EUROCRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4-8, 2003, Proceedings*, volume 2656 of *Lecture Notes in Computer Science*, pages 345–359. Springer, 2003.
7. Christophe De Cannière and Bart Preneel. Trivium. In Robshaw and Billet [19], pages 244–266.
8. Martin Ågren, Martin Hell, Thomas Johansson, and Willi Meier. Grain-128a: a new version of grain-128 with optional authentication. *IJWMC*, 5(1):48–59, 2011.
9. Anne Canteaut, Sergiu Carpov, Caroline Fontaine, Tancrède Lepoint, María Naya-Plasencia, Pascal Paillier, and Renaud Sirdey. Stream ciphers: A practical solution for efficient homomorphic-ciphertext compression. *J. Cryptology*, 31(3):885–916, 2018.
10. Martin Hell, Thomas Johansson, Alexander Maximov, and Willi Meier. The grain family of stream ciphers. In Robshaw and Billet [19], pages 179–190.
11. Hong-Jun Wu. Acorn: a lightweight authenticated cipher (v3). *Candidate for the CAESAR Competition (2016)*.
12. S. Golomb. *Shift Register Sequences*. Aegean Park Press, 1982.
13. Elena Dubrova. A transformation from the fibonacci to the galois nlfsrs. *IEEE Trans. Inf. Theory*, 55(11):5263–5271, 2009.
14. Xiao-Xin Zhao, Wen-Feng Qi, and Jia-Min Zhang. Further results on the equivalence between galois nfsrs and fibonacci nfsrs. *Des. Codes Cryptogr.*, 88(1):153–171, 2020.
15. Honggang Hu and Guang Gong. Periods on two kinds of nonlinear feedback shift registers with time varying feedback functions. *Int. J. Found. Comput. Sci.*, 22(6):1317–1329, 2011.
16. Leonie Simpson and Serdar Boztas. State cycles, initialization and the trivium stream cipher. *Cryptogr. Commun.*, 4(3-4):245–258, 2012.
17. Shiyong Zhang and Gongliang Chen. New results on the state cycles of trivium. *Des. Codes Cryptogr.*, 87(1):149–162, 2019.
18. Tian Tian, Wen-Feng Qi, Chen-Dong Ye, and Xiao-Feng Xie. Spring: A family of small hardware-oriented block ciphers based on nfsrs. *Journal of Cryptologic Research*, 6(6):815–834, 2019.
19. Matthew J. B. Robshaw and Olivier Billet, editors. *New Stream Cipher Designs - The eSTREAM Finalists*, volume 4986 of *Lecture Notes in Computer Science*. Springer, 2008.