Necessary and Sufficient Conditions for Galois NFSRs Conditionally Equivalent to Fibonacci Ones and Their Application to the Stream Cipher Trivium

Jianghua Zhong, Yingyin Pan, Wenhui Kong, and Dongdai Lin

Abstract

Grain and Trivium are two typical stream ciphers based on nonlinear feedback shift registers (NFSRs). The 160-stage Galois NFSR used in Grain was found conditionally equivalent to a 160-stage Fibonacci NFSR before Grain was introduced. But it remains unknown whether the 288-stage Galois NFSR used in Trivium is conditionally equivalent to a Fibonacci NFSR, though Trivium exists for over ten years and several types of Galois NFSRs have been found conditionally equivalent to Fibonacci ones with same stage number over the last decades.

This paper applies the NFSR's dynamic system description, and obtains some necessary and sufficient conditions for Galois NFSRs to be conditionally equivalent to Fibonacci ones with same stage number, covering and improving the previous work on this research. As an application, the paper reveals that the 288-stage Galois NFSR used in Trivium is not conditionally equivalent to any Fibonacci NFSR, indicating the infeasibility of applying a conditionally equivalent Fibonacci NFSR to simplify its cryptanalysis, and indicating the good confusion and diffusion of the initial state to the output sequence generated from the Galois NFSR's 288-th bit that is used as one of inputs of Trivium's filtering function. This provides a formal extra justification of Trivium's good design, and allows future designs to be built by the same principle.

Index Terms

Shift register, Boolean function, stream cipher, Trivium, equivalence.

The authors are with the State Key Laboratory of Cyberspace Security Defense, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China. (e-mail: zhongjianghua@iie.ac.cn).

I. Introduction

A stream cipher is a common cryptographic primitive for protecting confidential information from unauthorized or accidental disclosure. It combines a plaintext with a pseudorandom sequence, which can be generated using a feedback shift register. Due to the inherent linearity of linear feedback shift registers (LFSRs), nonlinear filtering functions are introduced to the stream ciphers based on LFSRs in order to improve the ciphers' security. Nevertheless, such stream ciphers may still be vulnerable to correlation attacks [1] and algebraic attacks [2]. In contrast, stream ciphers based on nonlinear feedback shift registers (NFSRs) are more resistent to all kinds of cryptanalytic attacks.

NFSRs are generally implemented in Fibonacci or Galois configuration. The NFSRs in Fibonacci configuration are called Fibonacci NFSRs, whose feedback is only applied to the last bit. The NFSRs in Galois configuration are called Galois NFSRs, whose feedback can be applied to every bit [3]. Notably, Galois NFSRs are used as the main building blocks of many recent stream ciphers, such as the European eSTREAM project's hardware-oriented finalists Grain [4] and Trivium [5], which are also two typical NFSR-based stream ciphers. In particular, Trivium is the first stream cipher based on the confusion and diffusion principles that block ciphers always use. Grain's internal state is from a 160-stage Galois NFSR, formed by a cascade connection of one 80-stage Fibonacci LFSRs and one 80-stage Fibonacci NFSRs. Trivium's internal state is from a 288-stage Galois NFSR, formed by three pairwise controlled Fibonacci NFSRs with their stage numbers 93, 84, and 111.

Two different NFSRs may be equivalent. But the equivalence definition has been kept refining. It was first introduced embryonically by Massey and Liu in 1964 [6], in the sense that the state diagrams of NFSRs only differ in the labelling of states, in order to simplify the analysis of a type of NFSRs used in convolutional codes. Their definition is in essence the isomorphism of NFSRs' state diagrams, involving only individual NFSRs, but not involving their output functions. Nevertheless, the two NFSRs discussed there have the same set of output sequences if they only output their *last* bits (i.e., they use their last bits' values as their outputs). The equivalence definition was then introduced explicitly by Dubrova in 2009 [3], in the sense that two NFSRs have the same set of output sequences, but implicitly with the condition that they only output their *first* bits, in order to potentially increase the throughput of NFSRs' implemented circuits and to potentially simplify the cryptanalysis of NFSR-based stream ciphers.

In practice, a stream cipher usually uses NFSR's multiple bits as the inputs of its filtering function. As a result, Dubrova's equivalence definition was clarified as *conditionally equivalent* by Yao and Parampalli in 2022 [7], to indeed simplify the cryptanalysis of stream cipher Espresso [8], by using the state

transformation between conditionally equivalent NFSRs to transform the conditional equivalence problem to their so-called unconditional equivalence problem, which is defined as, for an NFSR with an output function h, there is another suitable output function $\bar{h}$ for its conditionally equivalent NFSR such that both NFSRs have the same set of output sequences. Moreover, it was verified that transforming a Fibonacci or Galois NFSR to a conditionally equivalent Galois can indeed improve the throughput of the stream ciphers Grain and Trivium [9]–[11].

Some efforts have been done on the conditional equivalence of NFSRs. First, for the conditional equivalence between Galois NFSRs, the Galois NFSR whose i-th bit feedback function of form $f_i(X_1, X_2, \ldots, X_n) = X_{(i+1) \bmod n} \oplus g_i(X_1, \ldots, X_i, X_{i+2}, \ldots, X_n)$ was found conditionally equivalent to many Galois NFSRs [11]. Second, for the conditional equivalence between Galois and Fibonacci NFSRs, seven types of Galois NFSRs were revealed conditionally equivalent to Fibonacci ones with same stage number [3], [6], [12]–[15], which are actually some *sufficient* conditions for Galois NFSRs conditionally equivalent to Fibonacci NFSRs. They will be dealt with later in this paper. Among them, the type of cascade connections of two Fibonacci NFSRs were shown conditionally equivalent to Fibonacci NFSRs [12], which implies that the 160-stage Galois NFSR used in the stream cipher Grain is conditionally equivalent to a 160-stage Fibonacci NFSR. The transformations between conditionally equivalent NFSRs were recently disclosed for four types, as well as their initial state matches [15], [16]. In addition, some *necessary* conditions were provided for Galois NFSRs conditionally equivalent to Fibonacci NFSRs in [17], and some properties of cascade connections of two Fibonacci NFSRs were revealed in [18].

This paper continues the research of conditional equivalence between Galois and Fibonacci NFSRs, by using their nonlinear dynamic system descriptions. The main contributions of this paper are twofold. First, we present some necessary and sufficient conditions for Galois NFSRs to be conditionally equivalent to Fibonacci NFSRs, covering and improving the previous results on this research. More precisely, an n-stage Galois NFSR with feedback $\mathbf{f} = [f_1 \;\; f_2 \;\; \ldots \;\; f_n]$ is conditionally equivalent to an n-stage Fibonacci NFSR, if and only if either of the following conditions is satisfied.

1) The state of the n-stage Galois NFSR at time t can be determined from the n consecutive outputs starting from time t.
2) The vectorial function $\mathbf{g} = [g_1 \;\; g_2 \;\; \ldots \;\; g_n]^T$ is a bijection, where Boolean functions $g_1(X_1, X_2, \ldots, X_n) = X_1$, $g_i = f_1(\mathbf{f}^{i-2}(X_1, X_2, \ldots, X_n))$ for all $i = 2, 3, \ldots, n$.

Further, an n-stage *nonsingular* Galois NFSR is conditionally equivalent to an n-stage Fibonacci NFSR, if and only if the Galois NFSR's state at time t can be determined from any given n consecutive outputs.

Second, as an application, we reveal that the 288-stage Galois NFSR used in the stream cipher

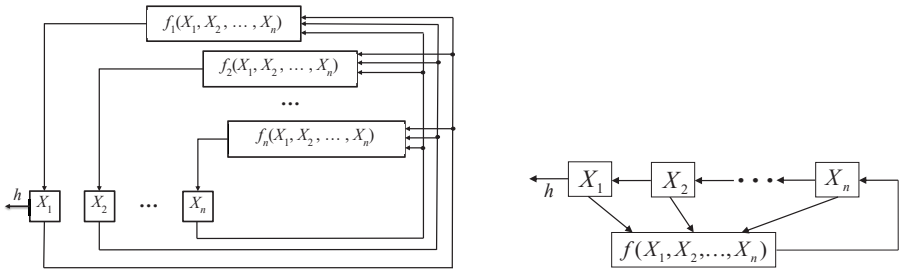
Trivium is not conditionally equivalent to any Fibonacci NFSR. It indicates the infeasibility of applying a conditionally equivalent Fibonacci NFSR to simplify Trivium's cryptanalysis, and also indicates the good confusion and diffusion of the initial state to the output sequence generated from the Galois NFSR's 288-th bit that is used as one of inputs of Trivium's filtering function. This provides a formal extra justification of Trivium's good design and allows future designs to be built by the same principle.

The remainder of this paper is organized as follows. Section II gives some preliminaries on Galois and Fibonacci NFSRs, followed by a brief review of related work on the conditional equivalence between Galois and Fibonacci NFSRs in Section III. Section IV presents our main results. The paper concludes in Section V.

II. Galois and Fibonacci NFSRs

In this section, we review some related concepts and results on the Galois and Fibonacci NFSRs. Before that, we first introduce some notations used in the paper.

Notations: $\mathbb{F}_2$ denotes the binary field, and $\mathbb{F}_2^n$ is an n-dimensional vector space over $\mathbb{F}_2$. $\mathbb{N}$ represents the set of nonnegative integers. $+$, $-$ and $\times$ are the ordinary addition, subtraction and multiplication in the real field, while $\oplus$ and $\odot$ are the addition and multiplication over $\mathbb{F}_2$, respectively.



(a) An n-stage Galois NFSR. (b) An n-stage Fibonacci NFSR.

Fig. 1: Galois and Fibonacci NFSRs.

Fig. 1(a) gives the diagram of an n-stage Galois NFSR. Here each small square represents a binary storage device, also called *bit*. Each i-th bit has a feedback function f_i, updating the bit's value at every periodic interval determined by a master clock. All feedback functions $f_1, f_2, \ldots, f_n$ form the Galois NFSR's feedback $\mathbf{f} = [f_1 \quad f_2 \quad \ldots \quad f_n]^T$. The n-stage Galois NFSR can be described as the following nonlinear dynamic system (usually called nonlinear system for short):

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

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

If there are only shifts between neighbouring bits for the first $n-1$ bits, i.e., $f_i(X_1, X_2, \ldots, X_n) = X_{i+1}$ for all $i = 1, 2, \ldots, n-1$, then the n-stage Galois NFSR is reduced to an n-stage Fibonacci NFSR. Fig. 1(b) shows the diagram of an n-stage Fibonacci NFSR, in which the Boolean function f is called the Fibonacci NFSR's *feedback function*. From now on, if there is no special clarification, then an NFSR means it can be a Galois or Fibonacci NFSR, and it is assumed to only output its first bit as usual, shown as Fig. 1, that is, its output function $h(X_1, X_2, \ldots, X_n) = X_1$.

An output sequence (or simply, a sequence) $(s_i)_{i\geq 1}$ is said to be *ultimately periodic* if there exists a positive integer p and a nonnegative integer k such that $s_i = s_{i+p}$ for any positive integer $i \geq k$. In this case, k and p are, respectively, called the *preperiod* and *period* of $(s_i)_{i\geq 1}$, and the least positive integer p is called the *minimum period* of the sequence $(s_i)_{i\geq 1}$, or simply called *period* of $(s_i)_{i\geq 1}$ for short if there is no confusion. Further, if $k = 0$, then $(s_i)_{i\geq 1}$ is said to be *periodic*. Notably, any output sequence of an NFSR is ultimately periodic.

The *state diagram* of an n-stage NFSR is a directed graph consisting of 2^n nodes and 2^n edges, in which each node represents a state of the NFSR, and each edge represents a transition between states. If state $\mathbf{X}$ is updated to state $\mathbf{Y}$, then there is an edge from state $\mathbf{X}$ to state $\mathbf{Y}$. In this case, $\mathbf{X}$ is called a *predecessor* of $\mathbf{Y}$, and $\mathbf{Y}$ is called the *successor* of $\mathbf{X}$. Distinct consecutive states $\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_p$ and their edges between them form a *cycle* of length p if $\mathbf{X}_1$ is the successor of $\mathbf{X}_p$.

An NFSR is said to be *nonsingular* if its stage diagram contains only cycles. An NFSR is nonsingular if and only if all its output sequences are periodic. In particular, a Fibonacci NFSR is nonsingular if and only if its feedback function f is nonsingular, that is, $f(X_1, X_2, \ldots, X_n) = X_1 \oplus \tilde{f}(X_2, X_3, \ldots, X_n)$ [19].

Definition 2.1 ([20]): Let $G = (V, A)$ and $\bar{G} = (\bar{V}, \bar{A})$ be two directed graphs, where V and $\bar{V}$ are their sets of nodes, A and $\bar{A}$ are their sets of edges. The two directed graphs G and $\bar{G}$ are said to be isomorphic if there exists a bijection $\varphi\colon V \to \bar{V}$ such that an edge $E \in A$ from node N to node $\hat{N}$ exists in G if and only if an edge $\bar{E} \in \bar{A}$ from $\varphi(N)$ to $\varphi(\hat{N})$ exists in $\bar{G}$.

Clearly, two isomorphic directed graphs have the same cycle structure, whereas differ only in a labelling of nodes.

Definition 2.2 ([3]): Two NFSRs are said to be *conditionally equivalent* if their sets of output sequences are equal under the condition that they only output their first bits.

The condition that an NFSR only outputs its first bit in the definition of conditional equivalence, limits the state transformation between NFSRs to preserving the first state bit. This condition is in some sense reasonable. First, it does not affect to use conditionally equivalent NFSRs to simplify cryptanalysis, which was verified by the foregoing Yao and Parampalli's work [7]. Second, it can apply the Fibonacci NFSRs' existing results to their conditionally equivalent Galois NFSRs, as up to now there is a considerable body of theory about Fibonacci NFSRs under this condition.

Lemma 2.3 ([17]): If a Galois NFSR is conditionally equivalent to a Fibonacci NFSR, then the stage number of the Galois NFSR is no less than that of the Fibonacci NFSR.

We know from Lemma 2.3 that, to determine whether a Galois NFSR is conditionally equivalent to a Fibonacci NFSR, we can only concern the Fibonacci NFSRs whose stage numbers are no greater than that of the Galois NFSR.

Lemma 2.4 ([21]): If an n-stage Galois NFSR and an n-stage Fibonacci NFSR are conditionally equivalent, then their state diagrams are isomorphic.[1]

Lemma 2.5 ([17]): An n-stage Galois NFSR represented by a nonlinear system $\mathbf{X}(t+1) = \mathbf{f}(\mathbf{X}(t))$ with state $\mathbf{X} \in \mathbb{F}_2^n$ is conditionally equivalent to an n-stage Fibonacci NFSR represented by a nonlinear system $\mathbf{Y}(t+1) = \mathbf{f}_0(\mathbf{Y}(t))$ with state $\mathbf{Y} \in \mathbb{F}_2^n$, if and only if there exists a bijection $\varphi\colon \mathbf{X} \mapsto \mathbf{Y}$ such that $\varphi(\mathbf{f}(\mathbf{X})) = \mathbf{f}_0(\varphi(\mathbf{X}))$ and $[1\ 0\ \cdots\ 0]\varphi(\mathbf{X}) = [1\ 0\ \cdots\ 0]\mathbf{X}$ for all $\mathbf{X} \in \mathbb{F}_2^n$.

Lemma 2.5 shows that, an n-stage Galois NFSR is conditionally equivalent to an n-stage Fibonacci NFSR if and only if their state diagrams are isomorphic under a bijection between their states that preserves the first state bit.

III. Related Work

In this section, we review all types of Galois NFSRs found conditionally equivalent to Fibonacci ones, that we know of, see [3], [6], [12]–[14]. Before that, we first introduce a concept related to equivalence.

[1]Detailed proof of Lemma 2.4 (i.e., Theorem 3 of Reference [21]) is provided in the reference's electronic supplementary material, available at the website:
https://static-content.springer.com/esm/art%3A10.1007%2Fs11432-017-9460-4/ MediaObjects/11432_2017_9460_MOESM1_ESM.pdf.

Definition 3.1 ([14]): Let π be a permutation of $\{1, 2, \ldots, n\}$. An n-stage Galois NFSR is said to be π-equivalent to an n-stage Galois NFSR with state $\mathbf{X} = [X_1 \ X_2 \ \ldots \ X_n]^T$ and feedback $\mathbf{f} = [f_1 \ f_2 \ \ldots \ f_n]^T$, if the former Galois NFSR's state is $\mathbf{X}_\pi = [X_{\pi(1)} \ X_{\pi(2)} \ \ldots \ X_{\pi(n)}]^T$ and feedback is $\mathbf{f}_\pi = \varphi_\pi \mathbf{f} \varphi_\pi^{-1}$, where $\varphi_\pi \colon [X_1 \ X_2 \ \ldots \ X_n]^T \mapsto [X_{\pi(1)} \ X_{\pi(2)} \ \ldots \ X_{\pi(n)}]^T$.

It is not hard to see that, for a permutation π of $\{1, 2, \ldots, n\}$, two NFSRs are π-equivalent if and only if their state diagrams are isomorphic under the bijection φ_π between their states that only reorders the state bits.

Lemma 3.2 ([6]): If an n-stage Galois NFSR with feedback $\mathbf{f} = [f_1 \ f_2 \ \ldots \ f_n]^T$ satisfies

$$\begin{cases} f_i = X_{i+1} \oplus c_i g(X_1, X_2, \ldots, X_n), \ c_i \in \{0, 1\}, \ i = 1, 2, \ldots, n-1, \\ f_n = g(X_1, X_2, \ldots, X_n), \end{cases} \tag{2}$$

where g is a Boolean function, then there exists a linear transformation mapping $\mathbf{Y} = Q\mathbf{X}$ from the Galois NFSR's state $\mathbf{X}$ to an n-stage Fibonacci NFSR's state $\mathbf{Y}$, so that the Galois NFSR is transformed to the Fibonacci NFSR, and Q satisfies

$$Q = \begin{bmatrix} 1 & q_1 & q_2 & \cdots & q_{n-1} \\ 0 & 1 & q_1 & \cdots & q_{n-2} \\ & & \ddots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix} \tag{3}$$

with $q_i \in \{0, 1\}$ for all $i = 1, 2, \ldots, n-1$.

As mentioned before, conditional equivalence assumes that an NFSR only outputs its first bit. However, from Equation (3), we can easily see that the Galois NFSR in Lemma 3.2, which only outputs the *last* bit, has the same set of output sequences as a Fibonacci NFSR that only outputs the *last* bit as well.

Lemma 3.3: If an n-stage Galois NFSR with feedback $\mathbf{f} = [f_1 \ f_2 \ \ldots \ f_n]^T$ satisfies one of the following conditions:

1) Cascade connection [12]:

$$\begin{cases} f_i = X_{i+1}, \ i \neq m, n \text{ with } \ m < n, \\ f_m = X_{m+1} \oplus g_m(X_1, X_2, \ldots, X_m), \\ f_n = g_n(X_{m+1}, X_{m+2}, \ldots, X_n), \end{cases} \tag{4}$$

2) Uniform Galois NFSR [3]:

$$\begin{cases} f_i = X_{i+1}, i = 1, 2, \ldots, \tau, \ \ 1 \leq \tau \leq n-1, \\ f_i = X_{(i+1) \bmod n} \oplus g_i(X_1, X_2, \ldots, X_{\tau+1}), i = \tau+1, \tau+2, \ldots, n, \end{cases}$$

3) Lower triangular Galois NFSR [13]:

$$\begin{cases} f_i = X_{i+1} \oplus g_i(X_1, X_2, \ldots, X_i), i = 1, 2, \ldots, n-1, \\ f_n = g_n(X_1, X_2, \ldots, X_n), \end{cases}$$

4) Nonsingular triangulation-I Galois NFSR [14]: [2]

$$\begin{cases} f_1 = X_n \oplus g_1(X_1, X_2, \ldots, X_{n-1}), \\ f_2 = X_1 \oplus g_2(f_1) \text{ with } g_2 = g_2(X_1), \\ f_i = X_{i-1} \oplus g_i(X_1, X_2, \ldots, X_{i-2}, f_1), i = 3, 4, \ldots, n, \end{cases}$$

5) Nonsingular triangulation-II Galois NFSR [14]:

$$\begin{cases} f_i = X_{i+1} \oplus g_i(X_1, X_2, \ldots, X_i), i = 1, 2, \ldots, n-1, \\ f_n = X_1 \oplus g_n(f_1, f_2, \ldots, f_{n-1}), \end{cases}$$

6) Type-IV Galois NFSR [15]:

$$\begin{cases} f_i = X_{i+1} \oplus g_i(X_{i+2}, X_{i+3}, \ldots, X_n), \ i = 1, 2, \ldots, n-2, \\ f_{n-1} = X_n, \\ f_n = X_1 \oplus g_n(X_2, \ldots, X_n), \end{cases} \tag{5}$$

then the n-stage Galois NFSR is conditionally equivalent to an n-stage Fibonacci NFSR.

The seven types of Galois NFSRs listed in Lemmas 3.2 and 3.3, are clearly related as follows.

1) A cascade connection, or a uniform Galois NFSR or a nonsingular triangulation-II Galois NFSR, is an example of a lower triangular Galois NFSR.
2) A uniform Galois NFSR is π_1-equivalent to a particular nonsingular triangulation-I Galois NFSR, with $\pi_1 \colon (1, 2, \ldots, \tau+1, \tau+2, \ldots, n) \to (\tau+1, \tau, \ldots, 1, n, \ n-1, \ldots, \tau+2)$ [14].
3) A nonsingular Galois NFSR, as in Lemma 3.2, is π_2-equivalent to some nonsingular triangulation-I Galois NFSR, with $\pi_2 \colon (1, 2, \ldots, n-1, n) \to (n, n-1, \ldots, 2, 1)$ [14].
4) A type-IV Galois NFSR is also π_2-equivalent to some nonsingular triangulation-I Galois NFSR.

IV. Main Results

In this section, we first give some necessary and sufficient conditions for Galois NFSRs to be conditionally equivalent to Fibonacci ones. We then show that those conditions cover the Galois NFSRs found (not) conditionally equivalent to Fibonacci NFSRs in previous work. Finally, we apply the theoretical results to the stream cipher Trivium.

[2]Suppose $g_2 = g_2(X_1) = c_1 X_1 \oplus c_2$ with $c_1, c_2 \in \{0, 1\}$. Then the notation $g_2(f_1)$ means $g_2(f_1) = c_1 f_1 \oplus c_2$.

A. Necessary and Sufficient Conditions

In this subsection, we provide some necessary and sufficient conditions for Galois NFSRs to be conditionally equivalent to Fibonacci NFSRs. To illustrate these conditions, some examples are provided as well.

Theorem 4.1: An n-stage Galois NFSR with state $\mathbf{X} = [X_1 \;\; X_2 \;\; \cdots \;\; X_n]^T \in \mathbb{F}_2^n$ is conditionally equivalent to an n-stage Fibonacci NFSR if and only if there exists a bijection $\mathbf{h} = [h_1 \;\; h_2 \;\; \ldots \;\; h_n]^T$ over $\mathbb{F}_2^n$ such that

$$X_i(t) = h_i(X_1(t), X_1(t+1), \ldots, X_1(t+n-1)) \tag{6}$$

for all $i = 1, 2, \ldots, n$ and for all $t \in \mathbb{N}$.

Proof. In the following, we will prove the result from the perspective of dynamic systems, by applying Lemma 2.5 and a property that an n-length output sequence generated from the first bit of an n-stage Fibonacci NFSR just forms the Fibonacci NFSR's initial state.

According to Lemma 2.5, we know that, an n-stage Galois NFSR is conditionally equivalent to an n-stage Fibonacci NFSR if and only if there exists a bijection $\mathbf{h} = \varphi^{-1}$ that maps the state $\mathbf{Y}(t)$ of the Fibonacci NFSR at time t for any $t \in \mathbb{N}$ to the state $\mathbf{X}(t)$ of the n-stage Galois NFSR at time t, so that the state diagrams of both NFSRs are isomorphic and the first bits $Y_1(t)$ and $X_1(t)$ of both states are equal (i.e., $Y_1(t) = X_1(t)$), which means that for any $t \in \mathbb{N}$, the output sequence $(X_1(t+k))_{k\geq 0}$ resulting from state $\mathbf{X}(t)$ of the Galois NFSR is also the output sequence resulting from the corresponding state $\mathbf{Y}(t)$ of the Fibonacci NFSR. Note that the first n bits of output sequence $(X_1(t+k))_{k\geq 0}$ form the state $[X_1(t) \;\; X_1(t+1) \;\; \ldots \;\; X_1(t+n-1)]^T$ of the Fibonacci NFSR at time t, that is, $\mathbf{Y}(t) = [X_1(t) \;\; X_1(t+1) \;\; \ldots \;\; X_1(t+n-1)]^T$. Therefore, an n-stage Galois NFSR is conditionally equivalent to an n-stage Fibonacci NFSR if and only if there exists a bijection $\mathbf{h} = [h_1 \;\; h_2 \;\; \ldots \;\; h_n]^T$ on $\mathbb{F}_2^n$ such that $\mathbf{X}(t) = \mathbf{h}(X_1(t), X_1(t+1), \ldots, X_1(t+n-1))$ for any $t \in \mathbb{N}$. □

Theorem 4.1 shows that, an n-stage Galois NFSR is conditionally equivalent to an n-stage Fibonacci NFSR if and only if there exists a bijection $\mathbf{h} = [h_1 \;\; h_2 \;\; \ldots \;\; h_n]^T$ on $\mathbb{F}_2^n$ such that the state at time t of the Galois NFSR can be expressed by n consecutive outputs starting from the time t via the bijection $\mathbf{h}$.

For the bijection $\mathbf{h}$ in Theorem 4.1, there are two points we need to concern. One is how to find it. The other is how to check whether it is bijective.

First, to find this bijection $\mathbf{h} = [h_1 \;\; h_2 \;\; \ldots \;\; h_n]^T$, as

$$h_1(X_1(t), X_1(t+1), \ldots, X_1(t+n-1)) = X_1(t) \text{ for any } t \in \mathbb{N},$$

we are only required to find the remaining $n-1$ Boolean functions $h_2, h_3, \ldots, h_n$, that may be derived from the nonlinear system representation

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

of the Galois NFSR by identical deformations. In other words, we need to solve $n-1$ variables $X_2(t), X_3(t), \ldots, X_n(t)$ from the above n equations by identical deformations including addition and multiplication of equations, and substitution of variables.

Second, to verify that $\mathbf{h}$ is bijective, we are only required to prove that, for any constant vector $\mathbf{c} = [c_1 \ \ c_2 \ \ \ldots \ \ c_n]^T \in \mathbb{F}_2^n$, the system of equations

$$\begin{cases} h_1(Z_1, Z_2, \ldots, Z_n) = c_1 \\ h_2(Z_1, Z_2, \ldots, Z_n) = c_2 \\ \quad \vdots \\ h_n(Z_1, X_2, \ldots, Z_n) = c_n \end{cases}$$

has a unique solution $\mathbf{Z} = [Z_1 \ \ Z_2 \ \ \ldots \ \ Z_n]^T$ on $\mathbb{F}_2^n$. Here, it is worth pointing out that, determining whether a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ is bijective is still a hard problem in general, except if the mapping is of a particular form.

Example 4.2: Consider a 4-stage Galois NFSR with feedback $\mathbf{f} = [f_1 \ \ f_2 \ \ f_3 \ \ f_4]^T$ satisfying

$$\begin{cases} f_1 = X_2 \oplus X_1, \\ f_2 = X_3, \\ f_3 = X_4, \\ f_4 = X_1 \oplus X_3 X_4, \end{cases} \tag{7}$$

which was found conditionally equivalent to a 4-stage Fibonacci NFSR [3].

In fact, from Equation (7), we know that the 4-stage Galois NFSR can be described by the following

nonlinear system:

$$\begin{cases} X_1(t+1) = X_2(t) \oplus X_1(t), \\ X_2(t+1) = X_3(t), \\ X_3(t+1) = X_4(t), \\ X_4(t+1) = X_1(t) \oplus X_3(t)X_4(t),\ t \in \mathbb{N}, \end{cases} \tag{8}$$

which yields

$$\begin{cases} X_1(t) = X_1(t) \\ \qquad := h_1(X_1(t), X_1(t+1), X_1(t+2), X_1(t+3)), \\ X_2(t) = X_1(t+1) \oplus X_1(t) \\ \qquad := h_2(X_1(t), X_1(t+1), X_1(t+2), X_1(t+3)), \\ X_3(t) = X_2(t+1) = X_1(t+2) \oplus X_1(t+1) \\ \qquad := h_3(X_1(t), X_1(t+1), X_1(t+2), X_1(t+3)), \\ X_4(t) = X_3(t+1) = X_1(t+3) \oplus X_1(t+2) \\ \qquad := h_4(X_1(t), X_1(t+1), X_1(t+2), X_1(t+3)),\ t \in \mathbb{N}. \end{cases}$$

Thus, we obtain the mapping $\mathbf{h} = [h_1 \ \ h_2 \ \ h_3 \ \ h_4]^T$ from the nonlinear system representation of the Galois NFSR by identical transformations. Moreover, for any constant vector $\mathbf{c} = [c_1 \ \ c_2 \ \ c_3 \ \ c_4]^T$, the system of equations $\mathbf{h}(Z_1, Z_2, Z_3, Z_4) = \mathbf{c}$ is: $h_1 = Z_1 = c_1, h_2 = Z_2 \oplus Z_1 = c_2, h_3 = Z_3 \oplus Z_2 = c_3, h_4 = Z_4 \oplus Z_3 = c_4$, which has a unique solution $Z_1 = c_1, Z_2 = c_1 \oplus c_2, Z_3 = c_3 \oplus c_2 \oplus c_1, Z_4 = c_4 \oplus c_3 \oplus c_2 \oplus c_1$. It implies that the mapping $\mathbf{h}$ is bijective. Thus, according to Theorem 4.1, the 4-stage Galois NFSR is conditionally equivalent to a 4-stage Fibonacci NFSR, consistent with the fact found in [3].

Considering that a bijection is invertible, we derive from Theorem 4.1 the following result.

Corollary 4.3: An n-stage Galois NFSR with feedback $\mathbf{f} = [f_1 \ \ f_2 \ \ \dots \ \ f_n]^T$ and state $\mathbf{X} = [X_1 \ \ X_2 \ \ \dots \ \ X_n]^T \in \mathbb{F}_2^n$ is equivalent to an n-stage Fibonacci NFSR if and only if the vectorial function $\mathbf{g} = [g_1 \ \ g_2 \ \ \dots \ \ g_n]^T \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$, defined by

$$\begin{cases} g_1(\mathbf{X}) = X_1, \\ g_i(\mathbf{X}) = f_1(\mathbf{f}^{i-2}(\mathbf{X})),\ i = 2, 3, \dots, n, \end{cases} \tag{9}$$

is bijective.

Proof. We will prove the result by computing the inverse of the bijection $\mathbf{h}$ in Theorem 4.1, precisely, by computing $\mathbf{h}^{-1} = \mathbf{g}$.

From Theorem 4.1, an n-stage Galois NFSR with state $\mathbf{X} = [X_1 \ \ X_2 \ \ \dots \ \ X_n]^T \in \mathbb{F}_2^n$ is conditionally equivalent to an n-stage Fibonacci NFSR if and only if there exists a bijection $\mathbf{h} = [h_1 \ \ h_2 \ \ \dots \ \ h_n]^T$ over $\mathbb{F}_2^n$ such that

$$X_i(t) = h_i(X_1(t), X_1(t+1), \dots, X_1(t+n-1)),\ i = 1, 2, \dots, n,\ t \in \mathbb{N}. \tag{10}$$

Let $\bar{\mathbf{X}}_1(t) = [X_1(t) \ \ X_1(t+1) \ \ \dots \ \ X_1(t+n-1)]^T$. Then, Equation (10) can be rewritten as $\mathbf{X}(t) = \mathbf{h}(\bar{\mathbf{X}}_1(t))$. Since $\mathbf{h}$ is bijective, we can denote its inverse as $\mathbf{h}^{-1} = [h_1^{-1} \ \ h_2^{-1} \ \ \dots \ \ h_n^{-1}]^T$. Thus, $\bar{\mathbf{X}}_1(t) = \mathbf{h}^{-1}(\mathbf{X}(t))$, yielding

$$X_1(t+i-1) = h_i^{-1}(\mathbf{X}(t)),\ i = 1, 2, \dots, n,\ t \in \mathbb{N}. \tag{11}$$

Notably, the Galois NFSR with feedback $\mathbf{f}$ and state $\mathbf{X}$ can be represented by a nonlinear system $\mathbf{X}(t+1) = \mathbf{f}(\mathbf{X}(t))$. Hence, we can obtain

$$\begin{cases} X_1(t+1) = f_1(\mathbf{X}(t)), \\ X_1(t+2) = f_1(\mathbf{X}(t+1)) = f_1(\mathbf{f}(\mathbf{X}(t))), \\ \quad \vdots \\ X_1(t+n-1) = f_1(\mathbf{X}(t+n-2)) = f_1(\mathbf{f}^{n-2}(\mathbf{X}(t))). \end{cases} \tag{12}$$

Combining Equations (11) and (12), we have

$$\begin{cases} h_1^{-1}(\mathbf{X}(t)) = X_1(t), \\ h_i^{-1}(\mathbf{X}(t)) = f_1(\mathbf{f}^{i-2}(\mathbf{X}(t))),\ i = 2, 3, \dots, n,\ t \in \mathbb{N}. \end{cases}$$

Let $g_i = h_i^{-1}$. As $\mathbf{h}$ is bijective, so is $\mathbf{g} = \mathbf{h}^{-1}$. □

From the proofs of Theorem 4.1 and Corollary 4.3, we know that the bijection $\mathbf{g}$ in Corollary 4.3 satisfies $\mathbf{g} = \mathbf{h}^{-1} = \varphi$, where $\mathbf{h}^{-1}$ and φ are from Theorem 4.1 and Lemma 2.5, respectively. The significant difference between Corollary 4.3 and Lemma 2.5 is that, Lemma 2.5 only points out the existence of the bijection, whereas Corollary 4.3 gives its explicit form, which is expressed by the feedback functions of the Galois NFSR.

Corollary 4.3 simplifies Theorem 2.1.1 in [22], which states that an n-stage Galois NFSR with feedback $\mathbf{f} = [f_1 \ \ f_2 \ \ \dots \ \ f_n]^T$ is conditionally equivalent to an n-stage Fibonacci NFSR with feedback $\mathbf{f}_0$ if and only if there exists a bijection $\mathbf{g} = [g_1 \ \ g_2 \ \ \dots \ \ g_n]^T$ such that $\mathbf{g}\mathbf{f}\mathbf{g}^{-1} = \mathbf{f}_0$ and $g_1 = X_1$; further, if such a mapping $\mathbf{g}$ exists, then $g_i = f_1\mathbf{f}^{i-2}$, $i = 2, 3, \dots, n$. Moreover, Corollary 4.3 uses a proof way different to that of the result therein.

Theorem 4.1 shows the state transformation $\mathbf{h}$ that maps the state at time t of a Fibonacci NFSR to that of its conditionally equivalent Galois NFSR, while Corollary 4.3 shows the reversed transformation $\mathbf{g}$; moreover, both transformations preserve the first state bit. Applying either of state transformations, we can make both conditionally equivalent NFSRs become Yao and Parampalli's unconditionally equivalent NFSRs if we use one NFSR's output function to properly select the other's.

More precisely, if a Galois NFSR has an output function f_z taking inputs from multiple state bits, then its conditionally equivalent Fibonacci NFSR becomes unconditionally equivalent to the Galois NFSR if we correspondingly choose the Fibonacci NFSR's output function as $f_z\mathbf{h}$. Similarly, if a Fibonacci NFSR has an output function $\bar{f}_z$ taking inputs from multiple state bits, then its conditionally equivalent Galois NFSR becomes unconditionally equivalent to the Fibonacci NFSR if we correspondingly choose the Galois NFSR's output function as $\bar{f}_z\mathbf{g}$.

Example 4.4: Consider a 4-stage Galois NFSR with feedback $\mathbf{f} = [f_1 \quad f_2 \quad f_3 \quad f_4]^T$ satisfying [3]:

$$\begin{cases} f_1 = X_2 \oplus X_1X_2, \\ f_2 = X_3 \oplus X_1 \oplus X_1X_3 \oplus X_1X_2X_3, \\ f_3 = X_4 \oplus X_1 \oplus X_2 \oplus X_3 \oplus X_1X_3 \oplus X_2X_3, \\ f_4 = X_1 \oplus X_2X_4. \end{cases} \tag{13}$$

It was proven *not* to be conditionally equivalent to any 4-stage Fibonacci NFSR [3].

According to Equation (13), we know that the Galois NFSR can be represented by a nonlinear system:

$$\begin{cases} X_1(t+1) = X_2(t) \oplus X_1(t)X_2(t), \\ X_2(t+1) = X_3(t) \oplus X_1(t) \oplus X_1(t)X_3(t) \oplus X_1(t)X_2(t)X_3(t), \\ X_3(t+1) = X_4(t) \oplus X_1(t) \oplus X_2(t) \oplus X_3(t) \oplus X_1(t)X_3(t) \oplus X_2(t)X_3(t), \\ X_4(t+1) = X_1(t) \oplus X_2(t)X_4(t), \ t \in \mathbb{N}. \end{cases} \tag{14}$$

It is not easy to observe that $X_1(t), X_2(t), X_3(t), X_4(t)$ cannot be expressed by $X_1(t), X_1(t+1), X_1(t+2), X_1(t+3)$ via identical deformations as the foregoing Galois NFSRs found conditionally equivalent to Fibonacci ones. Below we use Corollary 4.3 to determine whether the Galois NFSR is conditionally equivalent to a Fibonacci NFSR. We use the same notations as those therein.

We immediately have $g_1 = X_1$ and $g_2 = f_1 = X_2 \oplus X_1X_2$ by the definition of g_i in Equation (9) with $i = 1, 2$. Let $\mathbf{g} = [g_1 \quad g_2 \quad g_3 \quad g_4]^T$ with $g_3 = f_1\mathbf{f}$ and $g_4 = f_1\mathbf{f}^2$. Then, for any constant vector $\mathbf{c} = [c_1 \quad c_2 \quad c_3 \quad c_4]^T \in \mathbb{F}_2^4$, we consider the solution of the system of equations $\mathbf{g}(X_1, X_2, X_3, X_4) = \mathbf{c}$. Clearly, $g_1 = X_1 = c_1$ yields $X_1 = c_1$. Moreover, $g_2 = X_2 \oplus X_1X_2 = (c_1 \oplus 1)X_2 = c_2$. If we select

$c_1 = 1$ and $c_2 = 0$, then X_2 can be 0 or 1. It implies that, for the vector $\mathbf{c} = [c_1 \ \ c_2 \ \ c_3 \ \ c_4]^T$ with $c_1 = 1$ and $c_2 = 0$, the system of equations $\mathbf{g}(X_1, X_2, X_3, X_4) = \mathbf{c}$ has at least two solutions. So, $\mathbf{g}$ is not bijective. From Corollary 4.3, the Galois NFSR is not conditionally equivalent to any 4-stage Fibonacci NFSR, consistent with the fact found in [3].

Theorem 4.1 and Corollary 4.3 work for any Galois NFSR regardless of its nonsingularity, with respect to their conditionally equivalence problem. Considering that two types of nonsingular Galois NFSRs were found equivalent to Fibonacci NFSRs in [14], in the following we give some necessary and sufficient conditions for nonsingular Galois NFSRs.

Theorem 4.5: An n-stage nonsingular Galois NFSR with state $\mathbf{X} = [X_1 \ \ X_2 \ \ \cdots \ X_n]^T \in \mathbb{F}_2^n$ is conditionally equivalent to an n-stage Fibonacci NFSR if and only if there exists a bijection $\varphi = [\varphi_1 \ \ \varphi_2 \ \ \ldots \ \varphi_n]^T$ over $\mathbb{F}_2^n$ such that

$$X_i(t) = \varphi_i(X_1(t-n+1), X_1(t-n+2), \ldots, X_1(t)) \tag{15}$$

for all $i = 1, 2, \ldots, n$ and for all nonnegative integers $t \geq n-1$.

Proof. We will prove the result, by Theorem 4.1 and a property that a Galois NFSR is nonsingular if and only if its feedback is invertible, which makes available for computing the final state from the initial state on a time interval.

Let the Galois NFSR be represented by a nonlinear system:

$$\mathbf{X}(t+1) = \mathbf{f}(\mathbf{X}(t)), \ t \in \mathbb{N},$$

where $\mathbf{f} = [f_1 \ \ f_2 \ \ \ldots \ f_n]^T$ is the feedback of the Galois NFSR. The Galois NFSR is nonsingular if and only if its feedback $\mathbf{f}$ is bijective. Let $\mathbf{f}^{-1}$ be the inverse of $\mathbf{f}$. Then, we have $\mathbf{X}(t) = \mathbf{f}^{-1}(\mathbf{X}(t+1))$, which implies

$$\mathbf{X}(t-n+1) = (\mathbf{f}^{-1})^{n-1}(\mathbf{X}(t)), \ t \geq n-1. \tag{16}$$

In addition, note that $X_1(t-n+1), X_1(t-n+2), \ldots, X_1(t)$ is an output sequence of length n over the time interval $[t-n+1, t]$. Denote

$$\mathbf{X}_1(t-n+1) = [X_1(t-n+1) \ \ X_1(t-n+2) \ \ \ldots \ X_1(t)]^T.$$

Sufficiency: If Equation (15) holds, then

$$\mathbf{X}(t) = \varphi(\mathbf{X}_1(t-n+1)), \ t \geq n-1. \tag{17}$$

Hence, combining Equations (16) and (17) yields

$$\mathbf{X}(t-n+1) = ((\mathbf{f}^{-1})^{n-1}\varphi)(\mathbf{X}_1(t-n+1) := \mathbf{h}(\mathbf{X}_1(t-n+1)), \ t \geq n-1.$$

Since $\mathbf{f}$ and φ are bijective, so is $\mathbf{h} = (\mathbf{f}^{-1})^{n-1}\varphi$. According to Theorem 4.1, the sufficiency holds.

Necessity: If the n-stage Galois NFSR is conditionally equivalent to an n-stage Fibonacci NFSR, then from the necessity of Theorem 4.1, we know that there exists a bijection $\mathbf{h} = [h_1 \ \ h_2 \ \ \dots \ \ h_n]^T$ such that

$$X_i(t-n+1) = h_i(X_1(t-n+1), X_1(t-n+2), \dots, X_1(t)) \tag{18}$$

for all $i = 1, 2, \dots, n$ and for all nonnegative integers $t \geq n-1$. Equation (18) can be written as $\mathbf{X}(t-n+1) = \mathbf{h}(\mathbf{X}_1(t-n+1))$, which implies

$$\mathbf{X}_1(t-n+1) = \mathbf{h}^{-1}(\mathbf{X}(t-n+1)), \ t \geq n-1.$$

Thus, along with Equation (16), we have $\mathbf{X}_1(t-n+1) = (\mathbf{h}^{-1}(\mathbf{f}^{-1})^{n-1})(\mathbf{X}(t))$, yielding

$$\mathbf{X}(t) = (\mathbf{f}^{n-1}\mathbf{h})(\mathbf{X}_1(t-n+1)), \ t \geq n-1.$$

Let $\varphi = \mathbf{f}^{n-1}\mathbf{h}$. As $\mathbf{f}$ is bijective, so is $\varphi = \mathbf{f}^{n-1}\mathbf{h}$. Thus, the result follows. □

Theorem 4.5 shows that, the state at time t of an n-stage nonsingular Galois NFSR that is conditionally equivalent to an n-stage Fibonacci NFSR, can be expressed by n consecutive outputs ending at time t. Actually, such a state can be expressed by any given n consecutive outputs. More precisely, Theorem 4.5 can be generalized to the following result.

Theorem 4.6: An n-stage nonsingular Galois NFSR with state $\mathbf{X} = [X_1 \ \ X_2 \ \ \cdots \ \ X_n]^T \in \mathbb{F}_2^n$ is conditionally equivalent to an n-stage Fibonacci NFSR, if and only if for any integer k, there exists a bijection $\psi_k = [\psi_{k,1} \ \ \psi_{k,2} \ \ \dots \ \ \psi_{k,n}]^T$ over $\mathbb{F}_2^n$ such that

$$X_i(t) = \psi_{k,i}(X_1(t-k), X_1(t-k+1), \dots, X_1(t-k+n-1)) \tag{19}$$

for all $i = 1, 2, \dots, n$ and for all nonnegative integers $t \geq k$.

Proof. Note that $X_1(t-k), X_1(t-k+1), \dots, X_1(t-k+n-1)$ is an output sequence of length n over the time interval $[t-k, t-k+n-1]$. Then, the proof is similar to that of Theorem 4.5. □

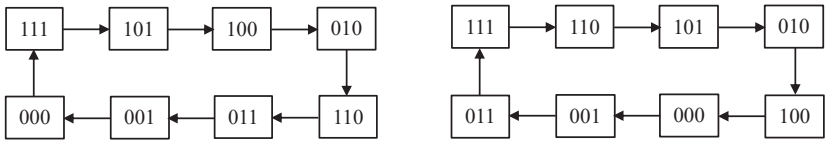
Example 4.7: Consider a 3-stage Galois NFSR with feedback $\mathbf{f} = [f_1 \ \ f_2 \ \ f_3]^T$ satisfying

$$\begin{cases} f_1 = X_1 \oplus X_3 \oplus 1, \\ f_2 = X_3 \oplus 1, \\ f_3 = X_1X_3 \oplus X_1 \oplus X_2 \oplus X_3 \oplus 1, \end{cases} \tag{20}$$

and a 3-stage Fibonacci NFSR with feedback function $f = X_2X_3 \oplus X_1 \oplus X_2 \oplus 1$.

Their state diagrams are shown in Fig. 2. Thus, we can see that, each NFSR contains only one cycle in its state diagram, which implies both NFSRs are nonsingular; moreover, both NFSRs can generate the

same sequence $\mathbf{S} = 11101000$ of period 8 if they only output their first bits. Hence, they have the same set of output sequences and therefore, they are conditionally equivalent.



(a) State diagram of the 3-stage Galois NFSR.

(b) State diagram of the 3-stage Fiboacci NFSR.

Fig. 2: State diagrams of the Galois and Fibonacci NFSRs in Example 4.7

In the following, we will use Theorem 4.6 to show this conditional equivalence. From Equation (20), we know the Galois NFSR can be represented by the nonlinear system:

$$\begin{cases} X_1(t+1) = X_1(t) \oplus X_3(t) \oplus 1, \\ X_2(t+1) = X_3(t) \oplus 1, \\ X_3(t+1) = X_1(t)X_3(t) \oplus X_1(t) \oplus X_2(t) \oplus X_3(t) \oplus 1, \ t \in \mathbb{N}. \end{cases} \tag{21}$$

According to the first equation of (21), we can obtain

$$X_3(t) = X_1(t) \oplus X_1(t+1) \oplus 1.$$

Based on this, we derive from the second equation of (21) that

$$X_2(t) = X_3(t-1) \oplus 1 = X_1(t-1) \oplus X_1(t) \oplus 1, \ t \geq 1.$$

Note that $X_1(t-1), X_1(t), X_1(t+1)$ are 3 consecutive outputs for any positive integer $t \geq 1$. Then, we can take the integer k in Theorem 4.6 as $k = 1$, and let the mapping ψ_k therefore be $\psi_1 = [\psi_{1,1} \ \ \psi_{1,2} \ \ \psi_{1,3}]^T$ satisfying

$$\begin{cases} \psi_{1,1}(X_1(t-1), X_1(t), X_1(t+1)) = X_1(t), \\ \psi_{1,2}(X_1(t-1), X_1(t), X_1(t+1)) = X_1(t-1) \oplus X_1(t) \oplus 1, \\ \psi_{1,3}(X_1(t-1), X_1(t), X_1(t+1)) = X_1(t) \oplus X_1(t+1) \oplus 1, \ t \geq 1. \end{cases}$$

For any constant vector $\mathbf{c} = [c_1 \ \ c_2 \ \ c_2]^T$, the system of equations

$$\psi_1(Z_1, Z_2, Z_3) = \mathbf{c}$$

is: $Z_2 = c_1, Z_1 \oplus Z_2 \oplus 1 = c_2, Z_2 \oplus Z_3 \oplus 1 = c_3$, which has a unique solution $Z_1 = c_1 \oplus c_2 \oplus 1, Z_2 = c_1, Z_3 = c_1 \oplus c_3 \oplus 1$. Hence, the mapping ψ_1 is bijective. Therefore, by Theorem 4.6, the 3-stage Galois

NFSR is conditionally equivalent to a 3-stage Fibonacci NFSR, consistent with the foregoing conditional equivalence fact.

B. Covering of Necessary and Sufficient Conditions

In this subsection, we will show that our necessary and sufficient conditions for Galois NFSRs presented in Theorems 4.1-4.5 in Section IV-A cover the types of Galois NFSRs previously found conditionally equivalent to Fibonacci ones.

In fact, the Galois NFSRs found conditionally equivalent to Fibonacci ones in [3], [12]–[14] satisfy Equation (6) in Theorem 4.1 or Equation (15) in Theorem 4.5, which can be easily observed by the substitution and elimination of state's bits. Below, we specify them in order in more detail.

The Galois NFSRs found conditionally equivalent to Fibonacci ones in [3], [12], [13] satisfy Equation (6). We take the Galois NFSR in [12] as an example. That Galois NFSR is actually a cascade connection of two Fibonacci NFSRs, e.g., the stream cipher Grain just uses such a Galois NFSR as its main building block. From Equation (4) in Lemma 3.3, we can easily see that, a cascade connection of two Fibonacci NFSRs can be described by the following nonlinear system:

$$\begin{cases} X_i(t+1) = X_{i+1}(t), i \neq m, n \ \text{ with } \ m < n, \\ X_m(t+1) = X_{m+1}(t) \oplus g_m(X_1(t), X_2(t), \ldots, X_m(t)), \\ X_n(t+1) = g_n(X_{m+1}(t), X_{m+2}(t), \ldots, X_n(t)), t \in \mathbb{N}. \end{cases} \tag{22}$$

By substitution and elimination on the above equations, we have

$$\begin{cases} X_1(t) = X_1(t) := h_1(X_1(t), X_2(t), \ldots, X_n(t)), \ \ t \in \mathbb{N}, \\ X_i(t) = X_1(t+i-1) := h_i(X_1(t), X_2(t), \ldots, X_n(t)), \ \ 2 \leq i \leq m < n, \\ X_{m+1}(t) = X_1(t+m) \oplus g_m(X_1(t), X_1(t+2), \ldots, X_1(t+m-1) \\ \qquad\qquad := h_{m+1}(X_1(t), X_2(t), \ldots, X_n(t)), \\ X_i(t) = X_{m+1}(t+i-m-1) := h_i(X_1(t), X_2(t), \ldots, X_n(t)), \ \ m+2 \leq i \leq n, \end{cases}$$

which satisfies Equation (6). Let a mapping $\mathbf{h} = [h_1 \ \ h_2 \ \ \ldots \ \ h_n]^T$. Then, for any constant vector $\mathbf{c} = [c_1 \ \ c_2 \ \ \ldots \ \ c_n]^T \in \mathbb{F}_2^n$, it is easily seen that the system of equations $\mathbf{h}(Z_1, Z_2, \ldots, Z_n) = \mathbf{c}$ has a unique solution over $\mathbb{F}_2^n$. Hence, $\mathbf{h}$ is bijective. All these agree with from Theorem 4.1.

The Galois NFSR found conditionally equivalent to a Fibonacci NFSR in [14] has some feedback functions f_i appearing in some other feedback functions f_i. Actually, if we observe $f_i(\mathbf{X}(t)) = X_i(t+1)$ for all $i = 1, 2, \ldots, n$, then we can easily see that the nonsingular Triangular-I Galois NFSRs found

conditionally equivalent to Fibonacci ones satisfy Equation (15), while the nonsingular Triangular-II Galois NFSRs found conditionally equivalent to Fibonacci ones satisfy Equation (6). All these agree with Theorems 4.1 and 4.5.

As mentioned in Section III, different to the Galois NFSRs studied in other previous work that only output their first bits, the Galois NFSR in [6] only outputs its last bit, producing the same set of output sequences as a Fibonacci NFSR, which only outputs the last bit as well. To illustrate this case agreeing with our results, we first give a property about the output sequences of Fibonacci NFSRs, which will show that a Fibonacci NFSR using a different bit's value as its output may result in a different set of output sequences.

Proposition 4.8: Let Ω_i be the set of output sequences of the i-th bit of an n-stage Fibonacci NFSR for any $i \in \{1, 2, \ldots, n\}$. Then $\Omega_1 \supseteq \Omega_2 \supseteq \cdots \supseteq \Omega_n$; moreover, the equality holds if and only if the Fibonacci NFSR is nonsingular.

Proof. We will prove this proposition by two points. 1)Apply the property that an n-stage Fibonacci NFSR's initial state just forms the n-length output sequence generated from the Fibonacci NFSR's first bit, and define a mapping from the Fibonacci NFSR's i-th state to the $(i+1)$-th state. 2)Utilize the property that a Fibonacci NFSR is nonsingular if and only if any state of the Fibonacci NFSR has a unique predecessor, which is equivalent to saying that the mapping defined above is bijective.

For any $i \in \{1, 2, \ldots, n\}$, let $(a_k)_{k\geq i}$ be an output sequence of Ω_i, which results from the initial state $[a_i \;\; a_{i+1} \;\; a_{i+2} \;\; \ldots \;\; a_{i+n-1}]^T$. Then, we can easily see that $(a_k)_{k\geq i+1}$ is an output sequence of Ω_{i+1}, which results from the initial state $[a_{i+1} \;\; a_{i+2} \;\; a_{i+3} \;\; \ldots \;\; a_{i+n}]^T$. Moreover, if $(a_k)_{k\geq i} \in \Omega_i$, then $(a_k)_{k\geq j} \in \Omega_i$ for any positive integer $j \geq i+1$. Thus, we have

$$\Omega_i = \Omega_{i+1} \cup \{(a_k)_{k\geq i}\},\ i = 1, 2, \ldots, n-1, \tag{23}$$

which implies

$$\Omega_1 \supseteq \Omega_2 \supseteq \cdots \supseteq \Omega_n.$$

We can see from Equation (23) that, the left is to prove: for any $i \in \{1, 2, \ldots, n\}$, $\Omega_i = \Omega_{i+1}$ if and only if the Fibonacci NFSR is nonsingular.

Let a mapping $\mathbf{p} = [p_1 \;\; p_2 \;\; \ldots \;\; p_n]^T \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ satisfying

$$\mathbf{p}(a_i, a_{i+1}, a_{i+2}, \ldots, a_{i+n-1}) = [a_{i+1} \;\; a_{i+2} \;\; a_{i+3} \;\; \ldots \;\; a_{i+n}]^T,$$

where p_n is the feedback function of the Fibonacci NFSR. Then the state $[a_i \;\; a_{i+1} \;\; a_{i+2} \;\; \ldots \;\; a_{i+n-1}]^T$ is the predecessor of state $[a_{i+1} \;\; a_{i+2} \;\; a_{i+3} \;\; \ldots \;\; a_{i+n}]^T$.

On one hand, it is known that, a Fibonacci NFSR is nonsingular if and only if any state of the Fibonacci NFSR has a unique predecessor, which is equivalent to saying that the mapping $\mathbf{p}$ is bijective. On the other hand, note that the initial state $[a_i \quad a_{i+1} \quad a_{i+2} \quad \dots \quad a_{i+n-1}]^T$ uniquely corresponds to the output sequence $(a_k)_{k\geq i} \in \Omega_i$, and $[a_{i+1} \quad a_{i+2} \quad a_{i+3} \quad \dots \quad a_{i+n}]^T$ uniquely corresponds to the output sequence $(a_k)_{k\geq i+1} \in \Omega_{i+1}$. Then, from Equation (23), $\mathbf{p}$ is bijective if and only if $\Omega_i = \Omega_{i+1}$ for any $i \in \{1, 2, \dots, n\}$. Combing the above two hands, we can conclude that, $\Omega_i = \Omega_{i+1}$ for any $i \in \{1, 2, \dots, n\}$ if and only if the Fibonacci NFSR is nonsingular. □

According to Lemma 2.4 and Proposition 4.8, the n-stage Galois NFSR in [6] is conditionally equivalent to an n-stage Fibonacci NFSR if and only if the Galois NFSR is nonsingular. From [14], by a permutation $\pi\colon (1, 2, \dots, n) \to (n, n-1, \dots, 2, 1)$, the Galois NFSR in [6] can be transformed to a new Galois NFSR whose first bit is just the last bit of the original one; moreover, if the new Galois NFSR is nonsingular, then it is a particular nonsingular Triangular-I Galois NFSR, which satisfies Equation (15) as mentioned earlier. It agrees with Theorem 4.5 as well.

C. Application to the Stream Cipher Trivium

The stream cipher Trivium [5], designed by De Cannière and Preneel, is one of three hardware-oriented finalists in the European eSTREAM projection. It is the first stream cipher based on the confusion and diffusion principles that block ciphers always use. Trivium has a simple structure. However, to date very little has been known about its cryptographic properties and no feasible attack has been found against it, though considerable cryptanalysis has been conducted since its submission.

Trivium uses as the main building block three pairwise controlled Fibonacci NFSRs with stage numbers 93, 84, 111. These three Fibonacci NFSRs together form a 288-stage Galois NFSR, whose feedback $\mathbf{f} = [f_1 \quad f_2 \quad \dots \quad f_{288}]^T$ satisfies the following relation:

$$\begin{cases} f_1 = X_{243} \oplus X_{286}X_{287} \oplus X_{288} \oplus X_{69}, \\ f_{94} = X_{66} \oplus X_{91}X_{92} \oplus X_{93} \oplus X_{171}, \\ f_{178} = X_{162} \oplus X_{175}X_{176} \oplus X_{177} \oplus X_{264}, \\ f_i = X_{i-1}, \quad i \neq 1, 94, 178, \end{cases} \tag{24}$$

where $\mathbf{X} = [X_1 \quad X_2 \quad \dots \quad X_{288}]^T$ is the state of the Galois NFSR. In the following, we concern whether the Galois NFSR is conditionally equivalent to a Fibonacci NFSR.

To make the Galois NFSR's shift be from the $(i+1)$-th to the i-th bit as is usual, we relabel all bits and their corresponding feedback functions via a permutation $\pi\colon (1, 2, \dots, 287, 288) \to (288, 287, \dots, 2, 1)$,

that is,

$$\pi(i) = 289 - i,\ i = 1, 2, \ldots, 288.$$

Then, the permuted Galois NFSR has the feedback

$$\bar{\mathbf{f}} = [\bar{f}_1 \ \ \bar{f}_2 \ \ \ldots \ \ \bar{f}_{288}]^T = [f_{\pi(1)} \ \ f_{\pi(2)} \ \ \ldots \ \ f_{\pi(288)}]^T$$

satisfying

$$\begin{cases} \bar{f}_{288} = \bar{X}_{46} \oplus \bar{X}_2\bar{X}_3 \oplus \bar{X}_1 \oplus \bar{X}_{220}, \\ \bar{f}_{195} = \bar{X}_{223} \oplus \bar{X}_{197}\bar{X}_{198} \oplus \bar{X}_{196} \oplus \bar{X}_{118}, \\ \bar{f}_{111} = \bar{X}_{127} \oplus \bar{X}_{113}\bar{X}_{114} \oplus \bar{X}_{112} \oplus \bar{X}_{25}, \\ \bar{f}_i = \bar{X}_{i+1}, \ \ i \neq 111, 195, 288, \end{cases} \tag{25}$$

where

$$\bar{\mathbf{X}} = [\bar{X}_1 \ \ \bar{X}_2 \ \ \ldots \ \ \bar{X}_{288}]^T = [X_{\pi(1)} \ \ X_{\pi(2)} \ \ \ldots \ \ X_{\pi(288)}]^T$$

is the state.

In the following, we apply Corollary 4.3 to determine whether the permuted Galois NFSR is conditionally equivalent to a Fibonacci NFSR. We use the same notations as used there. From Corollary 4.3, we know

$$g_1 = \bar{X}_1, \tag{26}$$

$$g_i = \bar{f}_1(\bar{\mathbf{f}}^{i-2}(\bar{\mathbf{X}})),\ i = 2, 3, \ldots, n. \tag{27}$$

Combining both equations above, we have $g_{i+1} = g_i(\bar{\mathbf{f}}(\bar{\mathbf{X}}))$ for all $i = 1, 2, \ldots, 288$. Along with Equations (25) and (26), we directly compute $g_1, g_2, \ldots, g_{198}$, shown in Appendix A.

As in Corollary 4.3, let $\mathbf{g} = [g_1 \ \ g_2 \ \ \ldots \ \ g_{288}]^T$. For any constant vector $\mathbf{c} = [c_1 \ \ c_2 \ \ \ldots \ \ c_{288}]^T \in \mathbb{F}_2^{288}$, we consider the solution of the system of equations $\mathbf{g}(\bar{\mathbf{X}}) = \mathbf{c}$, based on the explicit expressions of $g_1, g_2, \ldots, g_{198}$ in Appendix A.

Clearly, for all $i = 1, 2, \ldots, 111$, the variable $\bar{X}_i$ can be uniquely determined by the i-th equation $\mathbf{g}_i(\bar{\mathbf{X}}) = c_i$. In the following, we consider the variables $\bar{X}_{112}$, $\bar{X}_{113}$, $\bar{X}_{114}$, $\bar{X}_{115}$.

The variable $\bar{X}_{112}$ only appears in the monomial $\bar{X}_{112}$ of the function $\bar{f}_{111}(\bar{\mathbf{X}})$. The variable $\bar{X}_{113}$ appears in only two monomials: $\bar{X}_{113}\bar{X}_{114}$ of the function $\bar{f}_{111}(\bar{\mathbf{X}})$ and $\bar{X}_{113}$ of the function $\bar{f}_{111}(\bar{\mathbf{f}}(\bar{\mathbf{X}}))$. The variable $\bar{X}_{114}$ appears in only three monomials: $\bar{X}_{113}\bar{X}_{114}$ of the function $\bar{f}_{111}(\bar{\mathbf{X}})$, $\bar{X}_{114}\bar{X}_{115}$ of the function $\bar{f}_{111}(\bar{\mathbf{f}}(\bar{\mathbf{X}}))$ and $\bar{X}_{114}$ of the function $\bar{f}_{111}(\bar{\mathbf{f}}^2(\bar{\mathbf{X}}))$. Similarly, the variable X_{115} also appears

in only three monomials: $\bar{X}_{114}\bar{X}_{115}$ of the function $\bar{f}_{111}(\bar{\mathbf{f}}(\bar{\mathbf{X}}))$, $\bar{X}_{115}\bar{X}_{116}$ of the function $\bar{f}_{111}(\bar{\mathbf{f}}^2(\bar{\mathbf{X}}))$ and $\bar{X}_{115}$ of the function $\bar{f}_{111}(\bar{\mathbf{f}}^3(\bar{\mathbf{X}}))$.

Furthermore, $\bar{f}_{111}(\bar{\mathbf{X}})$ appears in the functions g_{112} and g_{199}, and therefore appears in g_{286} as $g_{i+1} = g_i(\bar{\mathbf{f}}(\bar{\mathbf{X}}))$ for all $i = 1, 2, \ldots, n$. Keeping the same reasoning, $\bar{f}_{111}(\bar{\mathbf{f}}(\bar{\mathbf{X}}))$ appears in the functions g_{113}, g_{200} and g_{287}, while $\bar{f}_{111}(\bar{\mathbf{f}}^2(\bar{\mathbf{X}}))$ appears in the functions g_{114}, g_{201} and g_{288}. Notably, $\bar{f}_{111}(\bar{\mathbf{X}}) = g_{112}$, while $\bar{f}_{111}(\bar{\mathbf{X}})$ is only a part of g_{199} and g_{286}. Similarly, $\bar{f}_{111}(\bar{\mathbf{f}}(\bar{\mathbf{X}})) = g_{113}$, whereas $\bar{f}_{111}(\bar{\mathbf{f}}(\bar{\mathbf{X}}))$ is only a part of g_{200} and g_{287}. $\bar{f}_{111}(\bar{\mathbf{f}}^2(\bar{\mathbf{X}})) = g_{114}$, but $\bar{f}_{111}(\bar{\mathbf{f}}^2(\bar{\mathbf{X}}))$ is only a part of g_{201} and g_{288}. In addition, $\bar{f}_{111}(\bar{\mathbf{f}}^3(\bar{\mathbf{X}})) = g_{115}$.

Based on the above facts, we know that the variable $\bar{X}_{113}$ appears not only in g_{112} and g_{113}, but also in g_{199}, g_{200}, g_{286} and g_{287}; moreover, g_{112} appears in g_{199} and g_{286}, while g_{113} appears in g_{200} and g_{287}, and g_{114} appears in g_{201} and g_{288}. Therefore, the variable $\bar{X}_{113}$ is determined by two equations $g_{112} = c_{112}$ and $g_{113} = c_{113}$, while the variable $\bar{X}_{114}$ is determined by three equations $g_{112} = c_{112}$, $g_{113} = c_{113}$ and $g_{114} = c_{114}$. Recall that, for a positive integer $i \in \{1, 2, \ldots, n\}$, an n-variable Boolean function f is said to be linear with respect to the variable X_i if $f(X_1, X_2, \ldots, X_n) = X_i \oplus g(X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n)$. Then g_{288} is linear with respect to the variable $\bar{X}_{114}$. In addition, the variable $\bar{X}_{115}$ is determined by three equations $g_{113} = c_{113}$, $g_{114} = c_{114}$ and $g_{115} = c_{115}$. Below, we mainly focus on the four equations: $g_i = c_i$ with $i = 112, 113, 114, 115$.

We claim that $\mathbf{g}$ is not bijective. For a proof by contradiction, we assume $\mathbf{g}$ is bijective, which means for any constant vector $\mathbf{c} = [c_1 \;\; c_2 \;\; \ldots \;\; c_{288}]^T \in \mathbb{F}_2^{288}$, the system of equations $\mathbf{g}(\bar{\mathbf{X}}) = \mathbf{c}$ has a unique solution. Note that $\mathbf{g}$ is a mapping from $\mathbb{F}_2^{288}$ to $\mathbb{F}_2^{288}$. Then $\mathbf{g}$ is surjective. Hence, there exists an $\mathbf{a} = [a_1 \;\; a_2 \;\; \ldots \;\; a_{288}]^T \in \mathbb{F}_2^{288}$ with proper $a_{112}, a_{113}, a_{114}, a_{115}$ such that the equation $\mathbf{g}(\bar{\mathbf{X}}) = \mathbf{a}$ has $\bar{X}_{113} = 1, \bar{X}_{115} = 1$ and the remaining $\bar{X}_i$ to be determined for all $i \in \{1, 2, \ldots, 288\} \setminus \{113, 115\}$. Clearly, such an $\mathbf{a}$ is not unique. Notably, X_{114} is determined by three equations $g_{112} = a_{112}$, $g_{113} = a_{113}$ and $g_{114} = a_{114}$; moreover, we have computed

$$\begin{aligned} g_{112} &= \bar{X}_{127} \oplus \bar{X}_{113}\bar{X}_{114} \oplus \bar{X}_{112} \oplus \bar{X}_{25}, \\ g_{113} &= \bar{X}_{128} \oplus \bar{X}_{114}\bar{X}_{115} \oplus \bar{X}_{113} \oplus \bar{X}_{26}, \\ g_{114} &= \bar{X}_{129} \oplus \bar{X}_{115}\bar{X}_{116} \oplus \bar{X}_{114} \oplus \bar{X}_{27}. \end{aligned}$$

Thus, we have

$$\begin{aligned} &\bar{X}_{127} \oplus \bar{X}_{114}(\bar{X}_{113} \oplus \bar{X}_{115}) \oplus \bar{X}_{112} \oplus \bar{X}_{25} \oplus \bar{X}_{128} \oplus \bar{X}_{113} \oplus \bar{X}_{26} = a_{112} \oplus a_{113}, \\ &\bar{X}_{128} \oplus \bar{X}_{114}(\bar{X}_{115} \oplus 1) \oplus \bar{X}_{113} \oplus \bar{X}_{26} \oplus \bar{X}_{129} \oplus \bar{X}_{115}\bar{X}_{116} \oplus \bar{X}_{27} = a_{113} \oplus a_{114}. \end{aligned}$$

It is easily observed that $\bar{X}_{114} \in \{0, 1\}$ satisfies the above two equations as $\bar{X}_{113} = 1$ and $\bar{X}_{115} = 1$. It implies that the system of equations $\mathbf{g}(\bar{\mathbf{X}}) = \mathbf{a}$ has at least two solutions, which is contrary to our

assumption that $\mathbf{g}$ is bijective. So, $\mathbf{g}$ is not bijective. Thus, according to Corollary 4.3, the permutated Galois NFSR (or equivalently, the 288-stage Galois NFSR used in the stream cipher Trivium) is not conditionally equivalent to any 288-stage Fibonacci NFSR.

On the other hand, it was revealed that the 288-stage Galois NFSR used in the stream cipher Trivium has 21 cycles of length 3 in its state diagram [23]. Note that a sequence of length 3 has 8 possible forms in total. Then, there must exist some initial states from those 21 cycles resulting in the same output sequence, no matter what output function the Galois NFSR has. Therefore, we can conclude that, the 288-stage Galois NFSR used in the stream cipher Trivium is not conditionally equivalent to any 288-stage Fibonacci NFSR, either, consistent with our above conclusion. Otherwise, if it is conditionally equivalent to some 288-stage Fibonacci NFSR, then there must also exist some initial states of the Fibonacci NFSR resulting in the same output sequences of period 3, which is in contradiction with the fact that different initial states of a Fibonacci NFSR results in different output sequences generated from the Fibonacci NFSR's first bit.

Further, using what we have obtained from the explicit expressions of $g_1, g_2, \ldots, g_{198}$, we will show that the permutated Galois NFSR is not equivalent to any m-stage Fibonacci NFSR with any positive integer $m \leq 287$. First, we note that $g_1(\bar{\mathbf{X}}), g_2(\bar{\mathbf{X}}), \ldots, g_{288}(\bar{\mathbf{X}})$ are the first 288 bits of output sequences resulting from the initial state $\bar{\mathbf{X}}$. Together considering that the system of equations $\mathbf{g}(\bar{\mathbf{X}}) = \mathbf{a}$ has been shown having at least two solutions, we can deduce that the 288-length output sequence $a_1, a_2, \ldots, a_{288}$ appears at least twice. In particular, for any positive integer m satisfying $1 \leq m \leq 287$, the m-length output sequence $a_{287-m+1}, a_{287-m+2}, \ldots, a_{287}$ appears at least twice. Second, as mentioned before, $g_{288}(\bar{\mathbf{X}})$ is linear with respect to the variable $\bar{X}_{114}$, which can be 1 or 0. Then, we have

$$g_{288}(\bar{X}_1, \ldots, \bar{X}_{113}, 1, \bar{X}_{115}, \ldots, \bar{X}_{288}) \neq g_{288}(\bar{X}_1, \ldots, \bar{X}_{113}, 0, \bar{X}_{115}, \ldots, \bar{X}_{288})$$

for any $[\bar{X}_1, \ldots, \bar{X}_{113}, \bar{X}_{115}, \ldots, \bar{X}_{288}]^T \in \mathbb{F}_2^{287}$. As $a_{288} = g_{288}(\bar{\mathbf{X}})$, we can conclude that a_{288} can be 1 or 0. Assume that the permutated Galois NFSR is conditionally equivalent to an m-stage Fibonacci NFSR with any positive integer $m \leq 287$. Then the state $[a_{287-m+1} \;\; a_{287-m+2} \;\; \ldots \;\; a_{287}]^T$ of the Fibonacci NFSR has two successors $[a_{287-m+2} \;\; \ldots \;\; a_{287} \;\; 1]$ and $[a_{287-m+2} \;\; \ldots \;\; a_{287} \;\; 0]^T$, which is in contradiction with the fact that every state of an NFSR has a unique successor. Therefore, for any positive integer m satisfying $1 \leq m \leq 287$, the 288-stage permutated Galois NFSR (or equivalently, the 288-stage Galois NFSR used in the stream cipher Trivium) is not conditionally equivalent to any m-stage Fibonacci NFSR.

Summarizing above, the 288-stage Galois NFSR used in the stream cipher Trivium is not conditionally equivalent to any m-stage Fibonacci NFSR with any positive integer m satisfying $1 \leq m \leq 288$.

Therefore, from Lemma 2.3, we can conclude that, the 288-stage Galois NFSR used in the stream cipher Trivium is not conditionally equivalent to any Fibonacci NSFR. It indicates the infeasibility of applying a conditionally equivalent Fibonacci NFSR to simplify its cryptanalysis, as an n-stage Fibonacci NFSR has the first $n-1$ bits only involved shifts that may simplify the cryptanalysis.

In the following, we will analyze the effect of the initial state on the output sequences generated from Trivium's Galois NFSR. We first give a lemma, which can be directly deduced from Theorem 3 in [24].

Lemma 4.9: An n-stage Galois NFSR is conditionally equivalent to an n-stage Fibonacci NFSR, if and only if different initial states of the Galois NFSR result in different n-length output sequences generated from the Galois NFSR's first bit. [3]

Clearly, for an n-stage Fibonacci NFSR, its different initial states result in different n-length output sequences that are generated from its first bit. Lemma 4.9 shows that, such a property of an n-stage Fibonacci NFSR is preserved to its conditionally equivalent n-stage Galois NFSR.

Proposition 4.10: If an n-stage Galois NFSR is not conditionally equivalent to any n-stage Fibonacci NFSR, then for any positive integer $m \leq n$, there are at least two distinct initial states of the Galois NFSR such that they result in the same m-length output sequence generated from the Galois NFSR's first bit.

Proof. Clearly, there are 2^n states of an n-stage Galois NFSR that can be selected as the initial state, and there are 2^m forms of an m-length output sequence for any positive integer m. So, for any positive integer $m < n$, there are at least two distinct initial states of the Galois NFSR that result in the same m-length output sequence. If an n-stage Galois NFSR is not conditionally equivalent to any n-stage Fibonacci NFSR, then from Lemma 4.9, there are at least two distinct initial states of the Galois NFSR that result in the same n-length output sequence generated from the Galois NFSR's first bit. Summarizing the above two cases of $m < n$ and $m = n$, we can conclude that the result holds. □

Proposition 4.10 indicates that, if an n-stage Galois NFSR is not conditionally equivalent to any n-stage Fibonacci NFSR, then some initial state needs the Galois NFSR's first bit generated output sequence of length longer than n, to distinguish the remaining possible initial states. Such an initial has a more complex relation with the Galois NFSR's first bit generated output sequence, and affects more bits of the output sequence than any initial state of an n-stage Galois NFSR conditionally equivalent to an n-stage Fibonacci NFSR. We say such a property *the good confusion and diffusion of the initial state to the*

[3]The necessity of Lemma 4.9 is different from that of Theorem 3 in [24], but they are equivalent according to the definitions of an NFSR's observability and observability matrix there, which might not be familiar to most readers in the community of cryptography. For their reference, we provide our different proof of Lemma 4.9 in Appendix B.

output sequence generated from the first bit of the Galois NFSR. In this case, if the first bit of the Galois NFSR is selected as one of inputs of the filtering function in an NFSR-based stream cipher, then the cipher security may be improved or the filtering function's security burden may be relaxed.

In Trivium, the 288-stage Galois NFSR is not conditionally equivalent to any Fibonacci NFSR as mentioned above, the filtering function is linear, and the 288-th bit of the Galois NFSR (i.e., the first bit of the above permuted Galois NFSR) is one of inputs of the filtering function. Nevertheless, up to now there is no feasible attack against Trivium. All these coincide with our above arguments. It inspires us that, a future design could be built by the same principle of using as a pseudorandom sequence generator the Galois NFSR not conditionally equivalent to a Fibonacci NFSR and using the Galois NFSR's first bit as one of inputs of the stream cipher's filtering function.

V. Conclusion

The paper gave some necessary and sufficient conditions for Galois NFSRs conditionally equivalent to Fibonacci ones, covering and improving the previous results on this research. As an application, the paper disclosed that the 288-stage Galois NFSR used in the stream cipher Trivium is not conditionally equivalent to any Fibonacci NFSR. It indicates the infeasibility of applying a conditionally equivalent Fibonacci NFSR to simplify its cryptanalysis. It also indicates the good confusion and diffusion of the initial state to the output sequence generated from the Galois NFSR's 288-th bit that is used as one of inputs of Trivium's filtering function. A future design could be built by the same principle of using as a pseudorandom sequence generator the Galois NFSR not conditionally equivalent to a Fibonacci NFSR and using the Galois NFSR's first bit (as usual, here bits labelled in descending order in the direction of bit shifting) as one of inputs of the stream cipher's filtering function.

This paper only concerned the equivalence of NFSRs with the condition that their output functions take inputs only from their first bits. In future work, it is interesting to theoretically and practically study the equivalence of NFSRs with output functions taking inputs from multiple state bits. In particular, it is interesting to determine whether the Galois NFSR used in the stream cipher Trivium has an equivalent Fibonacci NFSR if the Galois NFSR is considered together with Trivium's filtering function. In addition, it is interesting to determine whether Trivium's key is from an initial state of the Galois NFSR, which can be distinguished from the remaining possible initial states by their resulting output sequences. They are nontrivial generalizations of this paper, but may give deeper insights into Trivium.

APPENDIX

The vectorial function $\mathbf{g}$ in Corollary 4.3 for the 288-stage Galois NFSR used in the stream cipher Trivium is computed as follows:

$$
\begin{aligned}
&g_1 = \bar{X}_1,\\
&g_2 = \bar{f}_1(\bar{\mathbf{X}}) = \bar{X}_2,\\
&\quad\vdots\\
&g_{111} = \bar{f}_1(\bar{\mathbf{f}}^{109}(\bar{\mathbf{X}})) = \bar{f}_2(\bar{\mathbf{f}}^{108}(\bar{\mathbf{X}})) = \ldots = \bar{f}_{109}(\bar{\mathbf{f}}(\bar{\mathbf{X}})) = \bar{f}_{110}(\bar{\mathbf{X}}) = \bar{X}_{111},\\
&g_{112} = \bar{f}_{110}(\bar{\mathbf{f}}(\bar{\mathbf{X}})) = \bar{f}_{111}(\bar{\mathbf{X}}) = \bar{X}_{127} \oplus \bar{X}_{113}\bar{X}_{114} \oplus \bar{X}_{112} \oplus \bar{X}_{25},\\
&g_{113} = \bar{f}_{111}(\bar{\mathbf{f}}(\bar{\mathbf{X}})) = \bar{f}_{127} \oplus \bar{f}_{113}\bar{f}_{114} \oplus \bar{f}_{112} \oplus \bar{f}_{25}\\
&\qquad = \bar{X}_{128} \oplus \bar{X}_{114}\bar{X}_{115} \oplus \bar{X}_{113} \oplus \bar{X}_{26},\\
&g_{114} = \bar{f}_{111}(\bar{\mathbf{f}}^2((\bar{\mathbf{X}}))) = \bar{f}_{111}(\bar{\mathbf{f}}(\bar{\mathbf{f}}(\bar{\mathbf{X}}))) = \bar{f}_{128} \oplus \bar{f}_{114} \oplus \bar{f}_{115} \oplus \bar{f}_{113} \oplus \bar{f}_{26}\\
&\qquad = \bar{X}_{129} \oplus \bar{X}_{115}\bar{X}_{116} \oplus \bar{X}_{114} \oplus \bar{X}_{27},\\
&g_{115} = \bar{f}_{111}(\bar{\mathbf{f}}^{\mathbf{3}}(\bar{\mathbf{X}})) = \bar{f}_{111}(\bar{\mathbf{f}}^2((\mathbf{f}(\bar{\mathbf{X}})))) = \bar{f}_{129} \oplus \bar{f}_{115}\bar{f}_{116} \oplus \bar{f}_{114} \oplus \bar{f}_{27}\\
&\qquad = \bar{X}_{130} \oplus \bar{X}_{116}\bar{X}_{117} \oplus \bar{X}_{115} \oplus \bar{X}_{28},\\
&\quad\vdots\\
&g_{180} = \bar{f}_{111}(\bar{\mathbf{f}}^{\mathbf{68}}(\bar{\mathbf{X}})) = \ldots = \bar{X}_{195} \oplus \bar{X}_{181}\bar{X}_{182} \oplus \bar{X}_{180} \oplus \bar{X}_{93},\\
&g_{181} = \bar{f}_{111}(\bar{\mathbf{f}}^{\mathbf{68}}(\mathbf{f}(\bar{\mathbf{X}}))) = \bar{f}_{195} \oplus \bar{f}_{181}\bar{f}_{182} \oplus \bar{f}_{180} \oplus \bar{f}_{93}\\
&\qquad = (\bar{X}_{223} \oplus \bar{X}_{197}\bar{X}_{198} \oplus \bar{X}_{196} \oplus \bar{X}_{118}) \oplus \bar{X}_{182}\bar{X}_{183} \oplus \bar{X}_{181} \oplus \bar{X}_{94},\\
&\quad\vdots\\
&g_{193} = \bar{X}_{235} \oplus \bar{X}_{209}\bar{X}_{210} \oplus \bar{X}_{208} \oplus \bar{X}_{130} \oplus \bar{X}_{194}\bar{X}_{195} \oplus \bar{X}_{193} \oplus \bar{X}_{106}\\
&g_{194} = \bar{f}_{235} \oplus \bar{f}_{209}\bar{f}_{210} \oplus \bar{f}_{208} \oplus \bar{f}_{130} \oplus \bar{f}_{194}\bar{f}_{195} \oplus \bar{f}_{193} \oplus \bar{f}_{106}\\
&\qquad = \bar{X}_{236} \oplus \bar{X}_{210}\bar{X}_{211} \oplus \bar{X}_{209} \oplus \bar{X}_{131} \oplus \bar{X}_{195}(\bar{X}_{223} \oplus \bar{X}_{197}\bar{X}_{198} \oplus \bar{X}_{196} \oplus \bar{X}_{118})\\
&\qquad\quad \oplus \bar{X}_{194} \oplus \bar{X}_{107},\\
&g_{195} = \bar{f}_{236} \oplus \bar{f}_{210}\bar{f}_{211} \oplus \bar{f}_{209} \oplus \bar{f}_{131} \oplus \bar{f}_{195}(\bar{f}_{223} \oplus \bar{f}_{197}\bar{f}_{198} \oplus \bar{f}_{196} \oplus \bar{f}_{118})\\
&\qquad\quad \oplus \bar{f}_{194} \oplus \bar{f}_{107}\\
&\qquad = \bar{X}_{237} \oplus \bar{X}_{211}\bar{X}_{212} \oplus \bar{X}_{210} \oplus \bar{X}_{132}\\
&\qquad\quad \oplus (\bar{X}_{223} \oplus \bar{X}_{197}\bar{X}_{198} \oplus \bar{X}_{196} \oplus \bar{X}_{118})(\bar{X}_{224} \oplus \bar{X}_{198}\bar{X}_{199} \oplus \bar{X}_{197} \oplus \bar{X}_{119})\\
&\qquad\quad \oplus \bar{X}_{195} \oplus \bar{X}_{108},\\
&g_{196} = \bar{f}_{237} \oplus \bar{f}_{211}\bar{f}_{212} \oplus \bar{f}_{210} \oplus \bar{f}_{132}\\
&\qquad\quad \oplus (\bar{f}_{223} \oplus \bar{f}_{197}\bar{X}_{198} \oplus \bar{f}_{196} \oplus \bar{f}_{118})(\bar{f}_{224} \oplus \bar{f}_{198}\bar{f}_{199} \oplus \bar{f}_{197} \oplus \bar{f}_{119})\\
&\qquad\quad \oplus \bar{f}_{195} \oplus \bar{f}_{108}\\
&\qquad = \bar{X}_{238} \oplus \bar{X}_{212}\bar{X}_{213} \oplus \bar{X}_{211} \oplus \bar{X}_{133}\\
&\qquad\quad \oplus (\bar{X}_{224} \oplus \bar{X}_{198}\bar{X}_{199} \oplus \bar{X}_{197} \oplus \bar{X}_{119})(\bar{X}_{225} \oplus \bar{X}_{199}\bar{X}_{200} \oplus \bar{X}_{198} \oplus \bar{X}_{120})\\
&\qquad\quad \oplus (\bar{X}_{223} \oplus \bar{X}_{197}\bar{X}_{198} \oplus \bar{X}_{196} \oplus \bar{X}_{118}) \oplus \bar{X}_{109},\\
&\quad\vdots
\end{aligned}
$$

$$
\begin{aligned}
g_{198} = {} & \bar{X}_{240} \oplus \bar{X}_{214}\bar{X}_{215} \oplus \bar{X}_{213} \oplus \bar{X}_{135} \\
& \oplus (\bar{X}_{226} \oplus \bar{X}_{200}\bar{X}_{201} \oplus \bar{X}_{199} \oplus \bar{X}_{121})(\bar{X}_{227} \oplus \bar{X}_{201}\bar{X}_{202} \oplus \bar{X}_{200} \oplus \bar{X}_{122}) \\
& \oplus (\bar{X}_{225} \oplus \bar{X}_{199}\bar{X}_{200} \oplus \bar{X}_{198} \oplus \bar{X}_{120}) \oplus \bar{X}_{111}, \\
g_{199} = {} & \bar{X}_{241} \oplus \bar{X}_{215}\bar{X}_{216} \oplus \bar{X}_{214} \oplus \bar{X}_{136} \\
& \oplus (\bar{X}_{227} \oplus \bar{X}_{201}\bar{X}_{202} \oplus \bar{X}_{200} \oplus \bar{X}_{122})(\bar{X}_{228} \oplus \bar{X}_{202}\bar{X}_{203} \oplus \bar{X}_{201} \oplus \bar{X}_{123}) \\
& \oplus (\bar{X}_{226} \oplus \bar{X}_{200}\bar{X}_{201} \oplus \bar{X}_{199} \oplus \bar{X}_{121}) \oplus \bar{f}_{111}(\bar{\mathbf{X}}).
\end{aligned}
$$

We will prove Lemma 4.9 in an n-dimensional vector space $\mathbb{F}_2^n$ of the binary field $\mathbb{F}_2$. It is different to that of Theorem 3 in [24], which is proved in a set Δ_{2^n} of 2^n-dimensional canonical vectors that are a one-to-one correspondence to the vectors in $\mathbb{F}_2^n$.

First, we will prove the necessity by applying the definition of conditional equivalence of NFSRs and the property of an n-stage Fibonacci NFSR having 2^n output sequences generated from the Fibonacci NFSR's first bit. Then, we will prove the sufficiency by finding the feedback function of an Fibonacci NFSR that is conditionally equivalent to the given Galois NFSR.

Necessity: If an n-stage Galois NFSR is conditionally equivalent to an n-stage Fibonacci NFSR, then they have the same set of output sequences. Clearly, an n-stage Fibonacci NFSR has 2^n different n-length output sequences generated from the Fibonacci NFSR's first bit. Therefore, the n-stage Galois NFSR has also 2^n different n-length output sequences generated from the Galois NFSR's first bit. Since the n-stage Galois NFSR has 2^n different states that can be selected as initial states, we can conclude that different initial states of the Galois NFSR result in different n-length output sequences generated from the Galois NFSR's first bit.

Sufficiency: For the convenience of subsequent statements, we label all states of the n-stage Galois NFSR according to their order appearing in the state diagram. Precisely, for any two consecutive states on the same subgraph that consists of a branch and its connected cycle or consists of only one cycle, label the predecessor as $\mathbf{X}_j$ with $j \in \{1, 2, ..., 2^n - 1\}$, and label its successor as $\mathbf{X}_{j+1}$. In particular, for the subgraph consisting of only one cycle, any state of the cycle can be labeled as the minimum-subscript state among those states on the cycle. Thus, all states on the same subgraph are arranged together into a set of states. The order of those sets can be arbitrarily arranged. For the case of one more branches connecting the same cycle, the states on the cycle are not repeatedly labeled.

An n-stage Galois NFSR has 2^n states that can be selected as the initial state. Hence, if different initial states of the Galois NFSR result in different n-length output sequences generated from the Galois NFSR's first bit, then the Galois NFSR can produce 2^n different output sequences $S^j = (s_i^j)_{i\geq 1}$, and their n-length output sequences $S_n^j = s_1^j s_2^j \dots s_n^j$ are pairwise distinct for all $j = 1, 2, \dots, 2^n$, where

each S^j represents the output sequence resulting from the initial state $\mathbf{X}_j$.

For any positive integer $i \geq 1$ and for any positive integer $j \in \{1, 2, \ldots, 2^n\}$, let $E_i^j = s_i^j s_{i+1}^j \ldots s_{i+n}^j$. Thus, $E_1^j = S_n^j s_{n+1}^j$. As those S_n^j are pairwise distinct for all $j = 1, 2, \ldots, 2^n$, all E_1^j uniquely determines a Boolean function f satisfying $s_{n+1}^j = f(s_1^j, s_2^j, \ldots, s_n^j)$ for all $j = 1, 2, \ldots, 2^n$. On the other hand, we can easily observe that, except the state $\mathbf{X}_{j+l_j}$ on an l_j-length cycle that contains states $\mathbf{X}_{j+1}, \mathbf{X}_{j+2}, \ldots, \mathbf{X}_{j+l_j}$ satisfies $E_{i+1}^{j+l_j} = E_i^{j+1}$, all the remaining states $\mathbf{X}_j$ on the same cycle or on the same cycle-connected branch satisfy $E_{i+1}^j = E_i^{j+1}$ for all positive integer $i \geq 1$. So, we have $s_{i+n+1}^j = f(s_{i+1}^j, s_{i+2}^j, \ldots, s_{i+n}^j)$ for all positive integer $i \geq 1$ and for all $j = 1, 2, \ldots, 2^n$. Take this Boolean function f as the feedback function of an n-stage Fibonacci NFSR. Then, this n-stage Fibonacci NFSR generates the same set of output sequences as the n-stage Galois NFSR with the condition that both NFSRs output their first bits. Therefore, the n-stage Galois NFSR and the n-stage Fibonacci NFSR are conditionally equivalent. □

ACKNOWLEDGMENT

This research was supported by National Natural Science Foundation of China under Grant Nos. 62172408, 62472417 and 62372449.

REFERENCES

[1] T. Siegenthale, Correlation immunity of nonlinear combining functions for cryptographic applications, IEEE Trans. Information Theory 30 (5) (1984) 776-779.

[2] N. T. Courtois, W. Meier, Algebraic attacks on stream ciphers with linear feedback, in: Biham, E. (eds), EUROCRYPT 2003, LNCS 2656 (2003) 345-359.

[3] E. Dubrova, A transformation from the Fibonacci to the Galois NLFSRs, IEEE Trans. Information Theory 55 (11) (2009) 5263-5271.

[4] M. Hell, T. Johansson, W. Meier, The Grain family of stream ciphers, in: M. Robshaw and O. Billet (eds.), New Stream Cipher Designs, LNCS 4986 (2008) 179-190.

[5] C. De Cannière, B. Preneel, Trivium, in: M. Robshaw and O. Billet (eds.), New Stream Cipher Designs, LNCS 4986 (2008) 244-266.

[6] J. L. Massey, R. W. Liu, Equivalence of nonlinear shift-register, IEEE Trans, Inf. Theory 10 (4) (1964) 378-379.

[7] G. Yao, U. Parampalli, Cryptanalysis of the class of maximum period galois NLFSR-based stream ciphers, Crypt. Commun. 13 (5) (2021) 847-864.

[8] E. Dubrova, M. Hell, Espresso: A stream cipher for 5G wireless communication systems, Cryptogr. Commun. 9 (2) (2017) 273-289.

[9] S. S. Mansouri, E. Dubrova, An improved hardware implementation of the grain stream cipher, in: 2010 13th Euromicro Conference on Digital System Design: Architectures, Methods and Tools, Lille, France, Nov. 2010, pp. 433-440.

[10] S. S. Mansouri, E. Dubrova, An improved hardware implementation of the Grain-128a stream cipher, in: International Conference on Information Security and Cryptology, LNSC 78392012 (2012) 278-292.

[11] E. Dubrova, An equivalence-preserving tranformation of shift register, in: K.-U. Schmidt and A. Winterhof (eds.), in: Proceedings of Squences and Their Applications (SETA 2014), LNCS 8865 (2014) 187-199.

[12] J. Mykkeltveit, M.-K. Siu, P. Tong, On the cylcle structure of some nonlinear shift register sequences, Information and Control 43 (2) (1979) 202-215.

[13] Z. Lin, The transformation from the Galois NLFSR to the Fibonacci Configuration, in: 2013 Fourth International Conference on Emerging Intelligent Data and Web Technologies, Xi'an, China, Sept. 2013, 335-339.

[14] X.-X. Zhao, W.-F. Qi, J.-M. Zhang, Further results on the equivalence between Galois NFSRs and Fibonacci NFSRs, Des. Codes Cryptogr. 88 (1) (2020) 153-171.

[15] G. Yao, U. Parampalli, Improved transformation algorithms for generalized Galois NLFSRs, Cryptogr. Commun. 14 (2) (2022) 229-258.

[16] E. Dubrova, Finding matching initial states for equivalent NLFSRs in the Fibonacci and the Galois configurations, IEEE Trans. Inf. Theory 56 (6) (2010) 2961-2966.

[17] J. Zhong, Y. Pan, D. Lin, On Galois NFSRs equivalent to Fibonacci ones, in: Y. Wu, M. Yung (eds), Information Security and Cryptology, Inscrypt 2020, LNCS 12612 (2020) 11-14.

[18] J. Zhong, D. Lin, On equivalence of cascade connections of two nonlinear feedback shift registers, The Computer Journal 62 (12) (2019) 1793-1804.

[19] S. W. Golomb, Shift Register Sequences, Holden-Day, Laguna Hills, CA, USA, 1967.

[20] J. A. Bondy, U. S. R. Murty, Graph Theory with Applications, New York, USA, 1976.

[21] J. Zhong, D. Lin, Decomposition of nonlinear feedback shift registers based on Boolean networks, Sci. China Inf. Sci. 62 (3) (2019) 39110:1-39110:3.

[22] J.-M. Zhang, *Research on equivalence between Galois NFSRs and Fibonacci NFSRs*, master thesis (in Chinese), PLA Information Engineering University, Zhengzhou, China, 2012.

[23] S. Zhang, G. Chen, New results on the state cycles of Trivium, Des. Codes Cryptogr. 87 (1) (2019) 149-162.

[24] X. Zhao, B. Wang, Y. Yan, J. Feng, The equivalence transformation between Galois NFSRs and Fibonacci NFSRs, Asia J. Control 23 (6) (2020) 2865-2873.