Hindawi
IET Information Security
Volume 2024, Article ID 3219604, 17 pages
https://doi.org/10.1049/2024/3219604

Research Article

Deciding Irreducibility/Indecomposability of Feedback Shift Registers Is NP-Hard

Lin Wang

Science and Technology on Communication Security Laboratory, Chengdu 610041, Sichuan, China

Correspondence should be addressed to Lin Wang; wanglin4math@outlook.com

Received 14 June 2023; Revised 24 July 2023; Accepted 20 December 2023; Published 7 March 2024

Academic Editor: Guowen Xu

Feedback shift registers (FSRs) are used as a fundamental component in electronics and confidential communication. A FSR f is said to be reducible if all the output sequences of another FSR g can also be generated by f and the FSR g costs less memory than f. A FSR is said to be decomposable if it has the same set of output sequences as a cascade connection of two FSRs. Two polynomial-time computable transformations from Boolean circuits to FSRs are proposed such that the output FSR of the first (resp. second) transformation is irreducible (resp. indecomposable) if and only if the input Boolean circuit is satisfiable. Through the two transformations, it is proved that deciding irreducibility (indecomposability) of FSRs is **NP**-hard. Additionally, FSRs are constructed to show that there exist infinitely many irreducible (resp. indecomposable) FSRs which are decomposable (resp. reducible).

1. Introduction

Feedback shift registers (FSRs) are broadly used in spread spectrum radio, control engineering, and confidential digital communication. As a result, this subject has attracted comprehensive research over half a century. Particularly, FSRs play a significant role in the stream cipher finalists of the eSTREAM project [1].

As shown in Figure 1, an n-stage FSR consists of n-bit registers $x_0, x_1, \dots, x_{n-1}$ and an n-input feedback logic f. A vector $\mathbf{x} \in \mathbb{F}_2^n$ is called a *state* of this FSR, and the values stored in bit registers update themselves along with clock impulses as follows:

$$(x_0, x_1, \dots, x_{n-1}) \mapsto (x_1, \dots, x_{n-1}, f(x_0, x_1, \dots, x_{n-1})), \quad (1)$$

and the mapping defined by Equation (1) is called the *state transformation* of this FSR. As the stage n and the feedback logic f uniquely determine the FSR, we denote the FSR in Figure 1 by $\mathrm{FSR}_n(f)$. Let $\mathrm{Seq}_n(f)$ denotes the set of sequences generated by $\mathrm{FSR}_n(f)$, i.e.,

$$\mathrm{Seq}_n(f) = \{s = (s_0, s_1, \dots) \in \mathbb{F}_2^\infty : \forall t \geq 0, s_{t+n} = f(s_t, s_{t+1}, \dots, s_{t+n-1})\}, \quad (2)$$

where $\mathbb{F}_2^\infty$ is the set of all binary sequences. The subscript n in $\mathrm{FSR}_n(f)$ and $\mathrm{Seq}_n(f)$ is neglected if the stage n is unambiguous or unnecessary in the context.

If $f(x_0, x_1, \dots, x_{n-1}) = c_0x_0 \oplus c_1x_1 \oplus \cdots \oplus c_{n-1}x_{n-1}$, where $c_0, c_1, \dots, c_{n-1} \in \mathbb{F}_2$, then $\mathrm{FSR}(f)$ is called a *linear feedback shift register (LFSR)*, and $p(x) = x^n \oplus c_{n-1}x^{n-1} \oplus \cdots \oplus c_1x \oplus c_0$ is called its *characteristic polynomial*. This FSR is also denoted by $\mathrm{LFSR}(p)$. For the above linear function f and $b \in \mathbb{F}_2$, $\mathrm{FSR}(f \oplus b)$ is said to be *affine*. A nonaffine FSR is called a *nonlinear feedback shift register (NFSR)*.

For $\mathrm{FSR}_n(f)$, if there exists $\mathrm{FSR}_m(g)$, such that $m < n$ and $\mathrm{Seq}(g) \subseteq \mathrm{Seq}(f)$, then $\mathrm{FSR}(f)$ is said to be *reducible* and $\mathrm{FSR}(g)$ is called a *subFSR* of $\mathrm{FSR}(f)$. Otherwise, $\mathrm{FSR}(f)$ is said to be *irreducible*. Informally, the subFSR $\mathrm{FSR}(g)$ of $\mathrm{FSR}(f)$ costs less memory than $\mathrm{FSR}(f)$ and the sequences generated by $\mathrm{FSR}(g)$ can also be generated by $\mathrm{FSR}(f)$.

The finite state machine in Figure 2 is called the *cascade connection* of $\mathrm{FSR}_n(f)$ into $\mathrm{FSR}_m(g)$. The Grain family ciphers use the cascade connection of a LFSR into a NFSR [2] and such cascade is called the grain-like structure, and the lightweight stream cipher LIZARD employs the cascade connection of two NFSRs [3]. Green and Dimond [4] defined the *product FSR* (the product of FSRs is denoted by "." in [4],

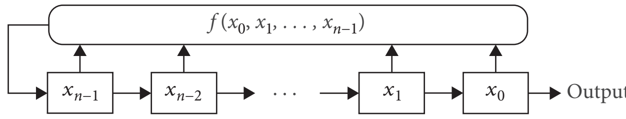


FIGURE 1: A feedback shift register with feedback logic f.

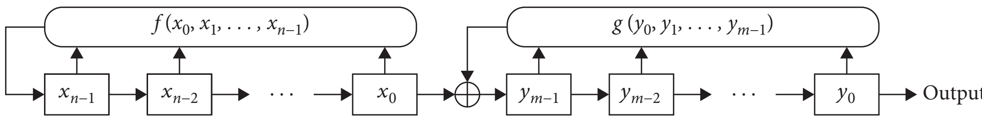


FIGURE 2: The cascade connection of $\mathrm{FSR}_n(f)$ into $\mathrm{FSR}_m(g)$.

while by "$*$" in [5]. We follow the latter in order to avoid ambiguity with the period or conventional multiplication.) of FSR(f) and FSR(g), denoted by FSR(f)$*$FSR(g), to be characterized by its feedback logic as follows:

$$(x_0, x_1, \ldots, x_{n+m-1}) \mapsto f(g(x_0, x_1, \ldots, x_{m-1}) \oplus x_m, g(x_1, x_2, \ldots, x_m) \oplus x_{m+1}, \ldots, g(x_{n-1}, x_n, \ldots, x_{n+m-2}) \oplus x_{n+m-1}) \oplus g(x_n, x_{n+1}, \ldots, x_{n+m-1}), \quad (3)$$

and showed that FSR(f)$*$FSR(g) generates exactly the same set of sequences as the device in Figure 2. Given any FSR(h), if there exist FSR(f) and FSR(g) satisfying FSR(h) = FSR(f)$*$FSR(g), then FSR(h) is said to be *decomposable* and FSR(f) (resp. FSR(g)) is called its left (resp. right) $*$-factor [6]. Otherwise, FSR(h) is said to be *indecomposable*. It is known that decomposable FSRs outputting the zero sequence are also reducible [4].

It is appealing to decide whether a FSR is (ir)reducible or (in)decomposable for the following three reasons. First, it enables a new perspective on analysis of stream ciphers. A reducible/decomposable FSR in unaware use may undermine the claimed security of stream ciphers, e.g., causing inadequate period of the output sequences. Dependent on specific ciphers, the divide-and-conquer method [7, 8] possibly decreases the cost of a brute force attack on a product FSR $\mathrm{FSR}_n(f)*\mathrm{FSR}_m(g)$. Moreover, note that all sequences generated by FSR(g) is also generated by FSR(f)$*$FSR(g) if FSR(f) outputs the zero sequence; and if FSR(g) is particularly a LFSR in this case, then FSR(f)$*$FSR(g) generates a family of linear recurring sequences, vulnerable to the Berlekamp–Massey algorithm [9, 10]. Second, deciding (ir) reducibility/(in)decomposability is applied for efficiently implementing FSRs. On the one hand, it costs less memory to replace a FSR with its large-stage subFSR (if there is one) while generating part of its output sequences. On the other hand, similar to the idea of Dubrova [11], implementing a decomposable FSR by its corresponding cascade connection as in Figure 2 possibly reduces the circuit depth of the feedback logics, in favor of less propagation time and higher data throughput. Third, an algorithm testing (ir)reducibility/(in) decomposability helps to design useful FSRs. Since the density of irreducible FSRs is lower-bounded by 0.4461 for $n \geq 6$ [12], a great number of irreducible NFSRs can be found if deciding irreducibility of FSRs is feasible; a kind of FSRs generating maximal-length sequences were also constructed based on the inherent structure of decomposable FSRs [5].

1.1. Our Contribution. This correspondence addresses irreducibility and indecomposability of FSRs from the perspective of worst-case computational complexity. Instead of representing FSRs by ANFs of their characteristic functions, we use Boolean circuits to characterize feedback logics of FSRs and measure the size of a FSR by the number of gates in its corresponding Boolean circuit.

PROBLEM: FSR IRREDUCIBILITY
INSTANCE: A FSR(f) with its feedback logic f as a Boolean circuit of size SIZE(f).
QUESTION: Is FSR(f) irreducible?

PROBLEM: FSR INDECOMPOSABILITY
INSTANCE: A FSR(f) with its feedback logic f as a Boolean circuit of size SIZE(f).
QUESTION: Is FSR(f) indecomposable?

NP is the class of all problems computed by polynomial-time nondeterministic Turing machines. A problem is **NP**-*hard* if it is at least as hard as all **NP** problems. This paper gives two polynomial-time computable algorithms transforming Boolean circuits to FSRs such that the input Boolean circuit is satisfiable if and only if the output FSR is, respectively, irreducible and indecomposable. Because the Boolean circuit satisfiability problem is **NP**-complete, the two transformations derive the main results of this paper:

Theorem 1. *The FSR IRREDUCIBILITY problem is* **NP**-*hard.*

Theorem 2. *The FSR INDECOMPOSABILITY problem is* **NP**-*hard.*

It is broadly believed that **NP**-hard problems could not be solved by quantum algorithms in the polynomial time [25], partially supported by some evidence [26]. Under this hypothesis, even a quantum computer cannot efficiently decide whether any given FSR is irreducible (or indecomposable).

Additionally, infinitely many instances of FSRs are given to show that irreducible FSRs do not include all indecompsobale FSRs and vice versa.

1.2. Related Work. It is a hot topic to address security issues of FSRs and their cascade connections, and progress has been made in recent years. Until now it is unknown how difficult deciding irreducible FSRs is, and special algorithms were proposed to search linear/affine subFSRs of NFSRs [13]. By Jiang and Lin [14], if $\mathrm{FSR}(h)=\mathrm{LFSR}_n(f)*\mathrm{FSR}_m(g)$, where $n\geq m$ and any nonzero $s\in\mathrm{Seq}(f)$ is of maximal period 2^n-1, then all affine subFSRs of $\mathrm{FSR}(h)$ are actually those of $\mathrm{FSR}(g)$. Whether a LFSR is indecomposable is completely determined by its characteristic polynomial [4, 6, 15]. In contrast, decomposing NFSRs seems much more challenging. Ma et al. [16] proposed a decomposing algorithm for NFSRs with a linear right $*$-factor using algebraic normal forms (ANFs) of Boolean functions, and Zhong and Lin [17] characterized several properties of general cascade connection using the language of state transition matrices of Boolean networks. Noteworthily, Tian et al. [6] proposed a method to find nonlinear left and right $*$-factors of NFSRs, and their algorithm efficiently and successfully decomposed 80-stage NFSRs in their experiments. So far it remains open to determine the asymptotic computational complexity of the algorithm in [6]. Instead of considering general decomposition, a practical algorithm has been proposed to find $*$-factors for the special case $\mathrm{FSR}(h)=\mathrm{FSR}(g)*\mathrm{FSR}(g)$ [18]. Zhong and Lin [19] gave strong results on uniqueness of cascade decomposition $\mathrm{FSR}(f)*\mathrm{FSR}(g)$. Additionally, the periods of sequences generated by the grain-like structures are studied [20–24].

1.3. Organization. The rest of this paper is organized as follows: in Section 2, we prepare facts and results for our main theorems. Section 2.1 is some notations. Sections 2.2 and 2.3, respectively, present some basic facts on Boolean circuits and cycles of FSRs. Section 2.4 includes some results on the cascade connection into $\mathrm{FSR}_1(x_0)$. In Section 2.5, we consider cycles and subFSRs of specific LFSRs. In Section 2.6, we use the cycle joining method to study subFSRs. Section 3 shows some relations between (ir)reducibility and (in)decomposability. **NP**-hardness of FSR irreducibility and FSR indecomposability is given in Sections 4 and 5, respectively. The last section includes a summary.

2. Preliminaries

2.1. Notations. Throughout this paper, let $\mathbb{Z}$ denote the set of integers, $\mathbb{F}_2$ the binary field, $+$ the addition of integers, $\oplus$ the exclusive-or (XOR), $\mathbf{1}^m$ (resp. $\mathbf{0}^m$) consecutive m 1's (resp. 0's).

Vectors are written in bold and upright letters or digits.

For $\mathbf{u}\in\mathbb{F}_2^m$ and $k\leq m$, let $\lceil\mathbf{u}\rceil_k$ denote the most significant k bits of $\mathbf{u}$.

Let $\overline{b}$ denote the dual of a bit b, and this notation naturally extends to vectors, i.e., for $\mathbf{u}\in\mathbb{F}_2^m$, $\overline{\mathbf{u}}=\mathbf{u}\oplus\mathbf{1}^m$.

The conjugate of $\mathbf{u}=(u_0,u_1,\dots,u_{m-1})$, denoted by $\widehat{\mathbf{u}}$, is $(\overline{u_0},u_1,\dots,u_{m-1})$.

Using the reverse lexicographic order, we take a vector $\mathbf{u}=(u_0,u_1,\dots,u_{m-1})$ as the nonnegative integer $\sum_{i=0}^{m-1}2^iu_i$. In this way,

$$(u_0,u_1,\dots,u_{m-1})<(v_0,v_1,\dots,v_{m-1}), \tag{4}$$

if and only if $\sum_{i=0}^{m-1}2^iu_i<\sum_{i=0}^{m-1}2^iv_i$.

Definition 1. For a Boolean logic $f(x_0,\dots,x_{n-1})$, its *associated logic* is as follows:

$$f^*(x_0,\dots,x_{n-1})=f(x_0\oplus1,\dots,x_{n-1}\oplus1)\oplus1. \tag{5}$$

Following from Definition 1, we have:

$$f^*(\overline{\mathbf{u}})=\overline{f(\mathbf{u})}\text{ for any }\mathbf{u}\in\mathbb{F}_2^n. \tag{6}$$

2.2. Boolean Circuits and Circuit Satisfiability Problem. An m-input *Boolean circuit* f is a directed acyclic graph with m sources and one sink [25]. The value(s) of source(s) is(are) input(s) of the Boolean circuit. Any nonsource vertex, called a *gate*, is one of the logical operations OR($\vee$), AND ($\wedge$), and NOT($\neg$), where the fan-in of OR and AND is 2 and that of NOT is 1. The value outputted from a gate is obtained by applying its logical operation on the value(s) inputted into it. The value outputted from the sink is the output of the Boolean circuit f. The size of the circuit f, denoted by $\mathrm{SIZE}(f)$, is the number of vertices in it. An m-input Boolean circuit f is *satisfiable*, if there exists $\mathbf{v}\in\mathbb{F}_2^m$ such that $f(\mathbf{v})=1$.

PROBLEM: CIRCUIT SATISFIABILITY
INSTANCE: A Boolean circuit f with its size $\mathrm{SIZE}(f)$.
QUESTION: Is f satisfiable?

A decision problem in **NP** class is **NP**-*complete* if it is not less difficult than any other **NP** problem.

Theorem 3 (see [25], Lemma 6.10). *The CIRCUIT SATISFIABILITY problem is* **NP**-*complete.*

A FSR is completely characterized by its feedback logic. We use Boolean circuits to characterize the feedback logic of FSRs for the following two reasons. First, FSRs are mostly implemented with silicon chips, and the Boolean circuit is an abstract model of the feedback logics of FSRs in silicon chips [25]. Second, the Boolean circuit is a generalization of Boolean formula [25]. For example, the Boolean function $f(x_1,x_2,\dots,x_n)=\prod_{i=1}^n(x_i\oplus1)$ can be implemented by a Boolean circuit with $2n-1$ gates, while expressing it with the ANF needs 2^n terms. Therefore, in this paper the size of a FSR is measured by the size of its feedback logic as a Boolean circuit.

2.3. Cycles of FSRs

Lemma 1 [27, 28]. *The following three statements are equivalent:*

(i) *The state transformation of* $\mathrm{FSR}_n(f)$ *is a bijection on* $\mathbb{F}_2^n$.
(ii) *Any sequence generated by* $\mathrm{FSR}_n(f)$ *is periodic.*

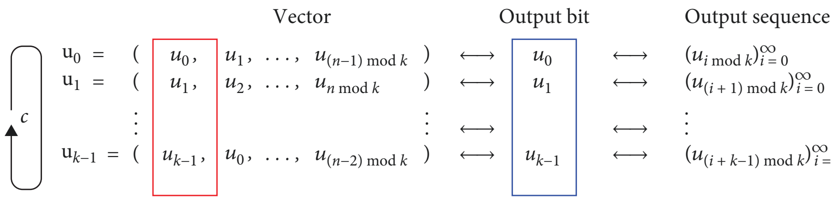


FIGURE 3: A k-cycle $\boldsymbol{c}$ and its corresponding ring bit sequence.

(iii) $f(x_0, x_1, \ldots, x_{n-1}) = x_0 \oplus g(x_1, x_2, \ldots, x_{n-1})$ *for some Boolean logic g.*

If any of the statements in Lemma 1 holds, FSR(f) is said to be *nonsingular*. In the sequel, we only refer to nonsingular FSRs.

For vectors $\mathbf{u} = (u_0, u_1, \ldots, u_{n-1})$ and $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$, $\mathbf{u}$ is said to precede $\mathbf{v}$ if $u_{i+1} = v_i$ for all $0 \le i \le n-2$.

Definition 2. (In this paper, cycles are written in bold and italic letters while vectors in bold and upright letters or digits.) [29] A k-cycle $\boldsymbol{c}$ in $\mathbb{F}_2^n$ is a ring sequence of k distinct n-bit vectors:

$$[\mathbf{u}_0, \mathbf{u}_1, \ldots, \mathbf{u}_{k-1}], \tag{7}$$

such that $\mathbf{u}_i$ precedes $\mathbf{u}_{(i+1) \bmod k}$ for all $0 \le i < k$.

Cycles interpret the relation between FSRs and periodic binary sequences.

On the one hand, as in Figure 3, the first column lists the vectors $\mathbf{u}_i$'s in the cycle $\boldsymbol{c}$; the second column shows the most significant bits of $\mathbf{u}_i$'s, representing a periodic sequence downwards in the boxes. Thus, the cycle $\boldsymbol{c}$ in Figure 3 is also written as the ring bit sequence:

$$[u_0, u_1, \ldots, u_{k-1}]. \tag{8}$$

Two cycles represented by the same ring bit sequence are said to be *equivalent*, for they correspond to the same set of periodic sequences which are equivalent by shifting.

Example 1. The following two cycles:

$$\boldsymbol{c}_1 = [(01), (11), (10)] \text{ and } \boldsymbol{c}_2 = [(011), (110), (101)], \tag{9}$$

correspond to the same ring bit sequence $[0, 1, 1]$, and are hence equivalent.

Without ambiguity in the context, we do not distinguish a cycle $\boldsymbol{c}$ from its ring bit sequence. Whether $m = n$ or not, an m-bit vector $\mathbf{v}$ occurring (contained) in the cycle Equation (7) means that $\mathbf{v}$ is consecutive m bits in the ring bit sequence Equation (8). Let len$(\boldsymbol{c})$ denote the number of distinct vectors in the cycle $\boldsymbol{c}$, i.e., the period of the binary sequence it represents.

On the other hand, if FSR$_n(f)$, with its state transformation denoted by F, generates the periodic sequence Equation (8), then $F(\mathbf{u}_i) = \mathbf{u}_{(i+1) \bmod k}$, $0 \le i < k$. If so, $\boldsymbol{c}$ is called a cycle of FSR(f), and this is denoted by $\boldsymbol{c} \in$ FSR(f). Actually, the cycle $\boldsymbol{c}$ is an orbit of the permutation F acting on $\mathbb{F}_2^n$. In Figure 3, the second column is the bit outputted by FSR(f) and the third column shows the sequences which FSR(f) generates from the initial state $\mathbf{u}_i$'s. Since all the cycles of a FSR uniquely determine its state transformation and hence its feedback logic, we also use FSR(f) to denote the set of all cycles of this FSR.

Example 2. Let $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$ be cycles given in Example 1. Then

$$\boldsymbol{c}_1 \in \text{LFSR}(x^2 \oplus x \oplus 1) \text{ and } \boldsymbol{c}_2 \in \text{LFSR}(x^3 \oplus 1). \tag{10}$$

Both LFSR$(x^2 \oplus x \oplus 1)$ and LFSR$(x^3 \oplus 1)$ output the sequence $(0, 1, 1)$ of period 3, and it is unambiguous to write $\boldsymbol{c}_1 \in$
LFSR$(x^3 \oplus 1)$.

As explained above, cycles of a nonsingular FSR essentially characterize its periodic sequences, and the following statements

$$\text{FSR}(g) \subset \text{FSR}(f), \tag{11}$$

$$\text{Seq}(g) \subset \text{Seq}(f), \tag{12}$$

$$\text{FSR}(g) \text{ is a subFSR of FSR}(f), \tag{13}$$

are equivalent. Immediately, we have

Lemma 2. *FSR(g) is a subFSR of FSR(f) if and only if FSR$(g) \subset$ FSR(f).*

Since the state transformation of an n-stage FSR is a permutation on $\mathbb{F}_2^n$, all its cycles exhaust $\mathbb{F}_2^n$ once, and hence the lengths of its cycles sum to 2^n.

Lemma 3. *It holds that* $\sum_{\boldsymbol{c} \in \text{FSR}_n(f)} \text{len}(\boldsymbol{c}) = 2^n$.

Lemma 4. *If both $\mathbf{u}$ and its conjugate $\widehat{\mathbf{u}}$ occur as n-bit vectors in the same cycle $\boldsymbol{c}$, then for any $k < n$, $\boldsymbol{c}$ is not a cycle of any nonsingular k-stage FSR.*

Proof. Assume $\boldsymbol{c} \in$ FSR$_k(g)$, $k < n$. Note that the cycle $\boldsymbol{c}$ contains two n-bit vectors $(u_0, u_1, \ldots, u_{n-1})$ and $(\overline{u_0}, u_1, \ldots, u_{n-1})$. Since $k < n$, the state transformation G of FSR(g) satisfies:

$$G(u_0, u_1, \ldots, u_{k-1}) = (u_1, u_2, \ldots, u_k) = G(\overline{u_0}, u_1, \ldots, u_{k-1}), \tag{14}$$

which is contradictory to Lemma 1. Thus, $\boldsymbol{c} \in \mathrm{FSR}_k(g)$ is not true. □

For a cycle $\boldsymbol{c}$, let $\min_n(\boldsymbol{c})$ be the minimal n-bit vector occurring in $\boldsymbol{c}$.

Definition 3. Let $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$ be two cycles in $\mathbb{F}_2^n$. If there exists an n-bit vector $\mathbf{u}$ occurring in $\boldsymbol{c}_1$ such that $\widehat{\mathbf{u}}$ occurs in $\boldsymbol{c}_2$, then $\boldsymbol{c}_1$ is said to be *adjacent to* $\boldsymbol{c}_2$ (at $\mathbf{u}$). If $\boldsymbol{c}_1$ is adjacent to $\boldsymbol{c}_2$ at $\min_n(\boldsymbol{c}_1)$, then $\boldsymbol{c}_1$ is said to be *min-adjacent to* $\boldsymbol{c}_2$.

Lemma 5. *Let* $\boldsymbol{c}_1, \boldsymbol{c}_2 \in \mathrm{FSR}_n(f)$ *and* $\mathbf{u} = \min_n(\boldsymbol{c}_1)$. *If* $\boldsymbol{c}_1$ *is min-adjacent to* $\boldsymbol{c}_2$ *and* $\mathbf{u} \notin \{\mathbf{0}^n, \mathbf{1}\mathbf{0}^{n-1}\}$, *then* $\min_n(\boldsymbol{c}_2) < \min\{\mathbf{u}, \widehat{\mathbf{u}}\}$.

Proof. Denote $\mathbf{u} = (u_0, u_1, \ldots, u_{n-1})$. By Statement (iii) of Lemma 1, the next states of $\mathbf{u}$ and $\widehat{\mathbf{u}}$ are $(u_1, \ldots, u_{n-1}, 0)$ and $(u_1, \ldots, u_{n-1}, 1)$.

Recall that vectors are in the reverse lexicographic order. If $\mathbf{u} \notin \{\mathbf{0}^n, \mathbf{1}\mathbf{0}^{n-1}\}$, i.e., $u_1, \ldots, u_{n-1}$ are not all 0, then $(u_1, \ldots, u_{n-1}, 0) < \min\{\mathbf{u}, \widehat{\mathbf{u}}\}$ since $(u_1, \ldots, u_{n-1}, 0)$ is the left shift of $\mathbf{u}$ and $\widehat{\mathbf{u}}$.

Furthermore, since $\mathbf{u} = \min_n(\boldsymbol{c}_1)$ as in Definition 3, we conclude that $(u_1, \ldots, u_{n-1}, 0)$ is in the same cycle as $\widehat{\mathbf{u}}$ (i.e., in $\boldsymbol{c}_2$), implying

$$\min_n(\boldsymbol{c}_2) \le (u_1, \ldots, u_{n-1}, 0) < \min\{\mathbf{u}, \widehat{\mathbf{u}}\}. \tag{15}$$

□

Corollary 1. *Let* $\boldsymbol{c} \in \mathrm{FSR}_n(f)$. *If* $\min_n(\boldsymbol{c}) \neq \mathbf{0}^n$, *then* $\boldsymbol{c}$ *is not min-adjacent to itself.*

Proof. Let $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$ be as in Lemma 5. Note that the proof of Lemma 5 also holds even if $\boldsymbol{c}_1 = \boldsymbol{c}_2$. If $\min_n(\boldsymbol{c}) \notin \{\mathbf{0}^n, \mathbf{1}\mathbf{0}^{n-1}\}$, then $\min_n(\boldsymbol{c}_1) = \min_n(\boldsymbol{c}_2) < \min\{\mathbf{u}, \widehat{\mathbf{u}}\}$ does not hold, and we conclude that $\boldsymbol{c}$ is not min-adjacent to itself.

Furthermore, suppose $\min_n(\boldsymbol{c}) = \mathbf{1}\mathbf{0}^{n-1}$. Then $\mathbf{0}^n$, the conjugate of $\mathbf{1}\mathbf{0}^{n-1}$, is not contained in $\boldsymbol{c}$. Thus, $\boldsymbol{c}$ is not min-adjacent to itself. □

Lemma 6. *Let G be a directed graph defined as follows: the vertices of G are cycles of* $\mathrm{FSR}_n(f)$, *and an arc is incident from* $\boldsymbol{c}_1$ *to* $\boldsymbol{c}_2$ *if* $\boldsymbol{c}_1$ *is min-adjacent to* $\boldsymbol{c}_2$ *and* $\min_n(\boldsymbol{c}_1) \neq \mathbf{0}^n$. *Then G is acyclic.*

Proof. By Corollary 1, the only cycle min-adjacent to itself has $\mathbf{0}^n$ as its minimal n-bit vector. Hence, G, as defined above, is loopless.

Now assume that G is not acyclic. Then there is a cyclic walk of length $m > 1$ in G, i.e., there exist cycles $\boldsymbol{c}_i$'s, such that $\boldsymbol{c}_i$ is min-adjacent to $\boldsymbol{c}_{(i+1) \bmod m}$ at $\min_n(\boldsymbol{c}_i)$, $0 \le i < m$.

As G is defined, we have $\min_n(\boldsymbol{c}_i) \neq \mathbf{0}^n$ for any $0 \le i < m$. Additionally, we also have $\min_n(\boldsymbol{c}_i) \neq \mathbf{1}\mathbf{0}^{n-1}$ for any $0 \le i < m$. Otherwise, $\min_n(\boldsymbol{c}_i) = \mathbf{1}\mathbf{0}^{n-1}$ for some $0 \le i < m$, then $\min_n(\boldsymbol{c}_{(i+1) \bmod m}) = \mathbf{0}^n$ and $\boldsymbol{c}_{(i+1) \bmod m}$ is hence a sink instead of a vertex in the cyclic walk. Thus, by Lemma 5:

$$\min_n(\boldsymbol{c}_0) > \min_n(\boldsymbol{c}_1) > \cdots > \min_n(\boldsymbol{c}_{m-1}) > \min_n(\boldsymbol{c}_0), \tag{16}$$

which does not hold. Therefore, G has no cyclic walk in it. □

The cycle $\boldsymbol{c}$ in Figure 3 is said to be *even* if $\bigoplus_{i=0}^{k-1} u_i = 0$ (equivalently, $\bigoplus_{i=0}^{k-1} \mathbf{u}_i = \mathbf{0}^n$). Otherwise, $\boldsymbol{c}$ is said to be *odd* [29].

For the cycle $\boldsymbol{c}$ in (7), let $\overline{\boldsymbol{c}}$ denote the cycle $[\overline{\mathbf{u}_0}, \overline{\mathbf{u}_1}, \ldots, \overline{\mathbf{u}_{k-1}}]$. A cycle $\boldsymbol{c}$ is said to be *self-dual* if $\boldsymbol{c} = \overline{\boldsymbol{c}}$ [29]. The cycle $\boldsymbol{c}$ in Equation (7) is said to be *primitive* if $\boldsymbol{c}$ and $\overline{\boldsymbol{c}}$ have no n-bit vector in common [29].

2.4. The D-Morphism. For any $0 < n \in \mathbb{Z}$, the D-morphism [29] is a mapping as below:

$$\begin{aligned} D:\ & \mathbb{F}_2^{n+1} && \to \mathbb{F}_2^n \\ & (u_0, u_1, \ldots, u_n) && \mapsto (u_0 \oplus u_1, u_1 \oplus u_2, \ldots, u_{n-1} \oplus u_n). \end{aligned} \tag{17}$$

Notice that if $\mathbf{u}$ precedes $\mathbf{v}$, then $D(\mathbf{u})$ also precedes $D(\mathbf{v})$. Hence, the D-morphism is also a natural mapping on cycles.

Lempel [29] gave the following results on D-morphism.

Theorem 4 ([29], Corollaries 1 and 2). *There exists a one-to-one correspondence between the even k-cycles* $\boldsymbol{d}$ *in* $\mathbb{F}_2^n$ *and the primitive pairs of dual k-cycles* $\boldsymbol{c}$ *and* $\overline{\boldsymbol{c}}$ *in* $\mathbb{F}_2^{n+1}$ *under which* $\boldsymbol{d} = D(\boldsymbol{c}) = D(\overline{\boldsymbol{c}})$. *There exists a one-to-one correspondence between the odd k-cycles* $\boldsymbol{d}$ *in* $\mathbb{F}_2^n$ *and the self-dual 2k-cycles* $\boldsymbol{c}$ *in* $\mathbb{F}_2^{n+1}$ *under which* $\boldsymbol{d} = D(\boldsymbol{c})$.

The D-morphism connects $\mathrm{FSR}(f) * \mathrm{FSR}_1(x_0)$ and its left $*$-factor.

Corollary 2. *Let* $\mathrm{FSR}_{n+1}(h) = \mathrm{FSR}_n(f) * \mathrm{FSR}_1(x_0)$. *Then the following two statements hold: (i) for any cycle* $\boldsymbol{d} \in \mathrm{FSR}(h)$, $D(\boldsymbol{d})$ *is a cycle of* $\mathrm{FSR}(f)$; *(ii) for any odd (resp. even) cycle* $\boldsymbol{c} \in \mathrm{FSR}(f)$, *its D-morphic preimage(s) is (resp. are) cycle(s) of* $\mathrm{FSR}(h)$.

Proof. Substitute $\mathrm{FSR}_1(x_0)$ for $\mathrm{FSR}(g)$ in Figure 2. Let H and F be, respectively, the state transformations of $\mathrm{FSR}(h)$ and $\mathrm{FSR}(f)$. As shown in the following commutative diagram

$$\begin{array}{ccccc} \xrightarrow{H} & \mathbb{F}_2^{n+1} & \xrightarrow{H} & \mathbb{F}_2^{n+1} & \xrightarrow{H} \\ & D \downarrow & & \downarrow D & \\ \xrightarrow{F} & \mathbb{F}_2^{n} & \xrightarrow{F} & \mathbb{F}_2^{n} & \xrightarrow{F} \end{array}$$

it follows from Equation (3) that $D(H(\mathbf{v})) = F(D(\mathbf{v}))$ for any $\mathbf{v} \in \mathbb{F}_2^{n+1}$. Thus, Statement (i) holds, and any $\boldsymbol{d} \in \mathrm{FSR}(h)$ is a D-morphic preimage of $D(\boldsymbol{d}) \in \mathrm{FSR}(f)$. By Theorem 4, under the D-morphism, a k-cycle of $\mathrm{FSR}(f)$ has one $2k$-cycle as its preimage or two k-cycles as its preimages. If $\mathrm{FSR}(h)$

does not include all D-morphic preimages of cycles in $\text{FSR}(f)$, then the length of cycles of $\text{FSR}(h)$ sum to less than 2^{n+1}, contradictory to Lemma 3. Therefore, Statement (ii) immediately follows. □

Example 3. Let $\boldsymbol{c}_2 = [0, 1, 1]$, $\overline{\boldsymbol{c}_2} = [0, 0, 1]$, and $\boldsymbol{c}_4 = [0, 0, 0, 1, 1, 1]$. We have $\text{LFSR}(x^4 \oplus x^3 \oplus x \oplus 1) = \text{LFSR}(x^3 \oplus 1) * \text{FSR}_1(x_0)$,

$$\begin{aligned} &\boldsymbol{c}_2, \overline{\boldsymbol{c}_2} \in \text{LFSR}(x^4 \oplus x^3 \oplus x \oplus 1), \\ &\boldsymbol{c}_4 \in \text{LFSR}(x^4 \oplus x^3 \oplus x \oplus 1), \\ &\boldsymbol{c}_2 = D(\boldsymbol{c}_2) = D(\overline{\boldsymbol{c}_2}) \in \text{LFSR}(x^3 \oplus 1), \\ &\text{and } \overline{\boldsymbol{c}_2} = D(\boldsymbol{c}_4) \in \text{LFSR}(x^3 \oplus 1). \end{aligned} \tag{18}$$

In Example 3, the even cycle $\boldsymbol{c}_2$ has two D-morphic preimages $\boldsymbol{c}_2$ and $\overline{\boldsymbol{c}_2}$, and the odd cycle $\overline{\boldsymbol{c}_2}$ has a unique D-morphic preimage $\boldsymbol{c}_4$.

2.5. Cycles and Properties of Certain LFSRs. In the rest of this paper, we use the following polynomials over $\mathbb{F}_2$:

$$\begin{aligned} p_0(x) &= x^{2n} \oplus x^n \oplus 1, \\ p_1(x) &= (x \oplus 1) \cdot p_0(x) = x^{2n+1} \oplus x^{2n} \oplus x^{n+1} \oplus x^n \oplus x \oplus 1, \\ p_2(x) &= x^{4n} \oplus x^{2n} \oplus 1, \end{aligned} \tag{19}$$

where n is a power of 3. For simplicity, let ${p_0}^*$ denote the associated logic of the feedback logic of $\text{LFSR}(p_0)$, i.e., ${p_0}^*(x_0, x_1, \ldots, x_{2n-1}) = x_n \oplus x_0 \oplus 1$.

In all that follows, L_0, L_1, and L_2, respectively, denote the state transformations of $\text{LFSR}(p_0)$, $\text{LFSR}(p_1)$, and $\text{LFSR}(p_2)$ as in Equation (20).

$$\begin{aligned} L_0: \quad & \mathbb{F}_2^{2n} \to \mathbb{F}_2^{2n} \\ & (x_0, x_1, \ldots, x_{2n-2}, x_{2n-1}) \mapsto (x_1, x_2, \ldots, x_{2n-1}, x_0 \oplus x_n), \\ L_1: \quad & \mathbb{F}_2^{2n+1} \to \mathbb{F}_2^{2n+1} \\ & (x_0, x_1, \ldots, x_{2n-1}, x_{2n}) \mapsto (x_1, x_2, \ldots, x_{2n}, x_0 \oplus x_1 \oplus x_n \oplus x_{n+1} \oplus x_{2n}), \\ L_2: \quad & \mathbb{F}_2^{4n} \to \mathbb{F}_2^{4n} \\ & (x_0, x_1, \ldots, x_{4n-2}, x_{4n-1}) \mapsto (x_1, x_2, \ldots, x_{4n-1}, x_0 \oplus x_{2n}). \end{aligned} \tag{20}$$

Cycles of LFSRs are well-understood.

Lemma 7. *If n is a power of 3, then the cycles of $\text{LFSR}(p_0)$ are $[0]$ and $(2^{2n}-1)/(3n)$ $3n$-cycles β_i, $1 \le i \le (2^{2n}-1)/(3n)$; the cycles of $\text{LFSR}(p_1)$ are the cycles of $\text{LFSR}(p_0)$ and their duals $\overline{\beta_i}$, $1 \le i \le (2^{2n}-1)/(3n)$; the cycles of $\text{LFSR}(p_2)$ are the cycles of $\text{LFSR}(p_0)$ and $(2^{4n}-2^{2n})/(6n)$ $6n$-cycles.*

Proof. Let $n = 3^t$. Since $p_0(x) \cdot (x^{3^t} \oplus 1) = x^{3^{t+1}} \oplus 1$ and $\gcd(p_0, x^{3^t} \oplus 1) = 1$, the roots of p_0 are exactly primitive 3^{t+1}-th roots of unity in the algebraic closure of $\mathbb{F}_2$. Furthermore, because $2 \cdot 3^t = \min\{0 < i \in \mathbb{Z} : 3^{t+1} | (2^i - 1)\}$, an extension of $\mathbb{F}_2$ containing a primitive 3^{t+1}-th root of unity is of degree at least $2 \cdot 3^t$. Thus, the polynomial p_0 is irreducible over $\mathbb{F}_2$.

Then the cycles of $\text{LFSR}(p_0)$, $\text{LFSR}(p_1)$, and $\text{LFSR}(p_2)$ are given by Lidl and Niederreiter [15, Theorem 8.53, 8.55, 8.63]. □

In the rest of this paper, let $\mathfrak{B}_{6n}$ denote the set of $6n$-cycles of $\text{LFSR}(p_2)$.

In the rest of Section 2.5, we give some properties of $\text{LFSR}(p_0)$ and $\text{LFSR}(p_1)$ in Lemma 9, and study their subFSRs in Theorems 5 and 6.

Theorem 5. $\text{LFSR}(p_0)$ *is an irreducible FSR.*

Proof. As given in Lemma 7, $\text{LFSR}(p_0)$ exactly includes one 1-cycle and $(2^{2n}-1)/(3n)$ $3n$-cycles. Let $n = 3^t$.

Suppose $\text{FSR}_m(f)$ to be a subFSR of $\text{LFSR}(p_0)$, where $1 \le m < 2n$. By Lemma 2, the cycles of $\text{FSR}(f)$ are contained in $\text{LFSR}(p_0)$. Then let $\text{FSR}(f)$ have exactly k 1-cycle and l $3n$-cycles. Thus, by Lemma 3, the lengths of cycles in $\text{FSR}(f)$ sum to 2^m, i.e.,

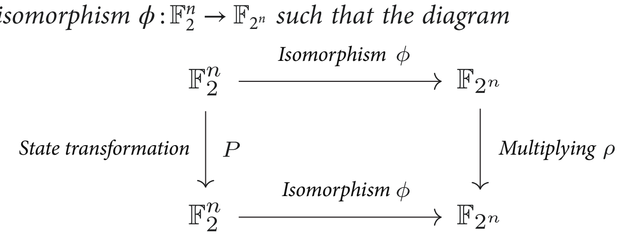
$$k + 3nl = 2^m, \tag{21}$$

where $k \in \{0, 1\}$ and $l \in \{0, 1, \cdots, (2^{2n}-1)/(3n)\}$. In Equation (21), letting $k = 0$ results in the contradiction $3 | 2^m$; letting $k = 1$ leads to $2^m \equiv 1 \bmod 3^{t+1}$, where $m < 2n$, contradictory to the fact that 2 is primitive in the residue ring $\mathbb{Z}/3^{t+1}\mathbb{Z}$, i.e., $2n = 2 \cdot 3^t = \min\{i > 0 : 3^{t+1} | (2^i - 1)\}$.

Hence, our supposition does not hold and $\text{LFSR}(p_0)$ has no subFSR. □

It is well-known that LFSRs with irreducible characteristic polynomials are also described using finite fields [15, Theorem 8.24].

Lemma 8. *Let $p(x)$ be an irreducible polynomial of degree n over $\mathbb{F}_2$, ρ a root of $p(x)$ in the finite field $\mathbb{F}_{2^n}$, and P the state transformation of $\text{LFSR}(p)$. Then there exists a linear-space isomorphism $\phi : \mathbb{F}_2^n \to \mathbb{F}_{2^n}$ such that the diagram*



is commutative.

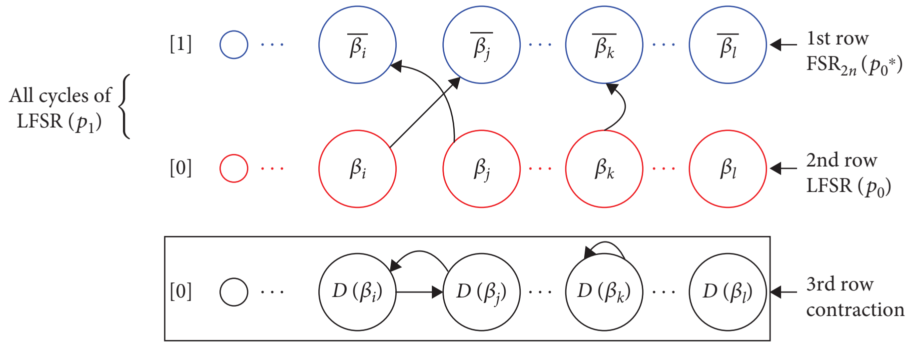


FIGURE 4: Cycles of LFSR(p_1) and their D-morphic images.

Proof. Let Tr be the trace function of $\mathbb{F}_{2^n}$ and define a linear homomorphism:

$$\begin{array}{llll}\psi: & \mathbb{F}_{2^n} & \rightarrow & \mathbb{F}_2^n \\ & x & \mapsto & (\mathrm{Tr}(x), \mathrm{Tr}(x\rho), \ldots, \mathrm{Tr}(x\rho^{n-1})).\end{array} \tag{22}$$

Since $1, \rho, \ldots, \rho^{n-1}$ are a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, ψ is an isomorphism of linear spaces. Let ϕ to be the inverse of ψ and the rest of proof is by direct computation similar to [15, Theorem 8.24]. □

By Equation (6) and Lemma 7, LFSR(p_1) = LFSR(p_0) $\cup$ FSR$({p_0}^*)$. In Figure 4, we sketch cycles of LFSR(p_0), FSR$({p_0}^*)$, and LFSR(p_1), and a cycle in the (boxed) third row is the D-morphic image of the two cycles of LFSR(p_1) in the same column.

Lemma 9. *Let $p(x) = x^n \oplus c_{n-1}x^{n-1} \oplus \cdots \oplus c_1 x \oplus 1$ be an irreducible polynomial of degree $n > 1$ over $\mathbb{F}_2$. Denote the logic $p^* = c_{n-1}x_{n-1} \oplus \cdots \oplus c_1 x_1 \oplus x_0 \oplus 1$. Then the following statements hold:*

(i) *Any cycle of* LFSR(p) *is even and any cycle in* FSR(p^*) *is odd.*

(ii) *The D-morphism is a permutation on cycles of* LFSR(p).

(iii) *For any pair of $(n+1)$-bit conjugate vectors $\mathbf{v}, \widehat{\mathbf{v}} \in \mathbb{F}_2^{n+1}$, one occurs in some cycle $\boldsymbol{c} \in$* LFSR(p) *and the other occurs in some cycle $\boldsymbol{d} \in$* FSR(p^*).

Proof. As $p(x)$ is irreducible and deg$p(x) > 1$, then $p(x)$ has no factor $x \oplus 1$ and hence $c_1 \oplus \cdots \oplus c_{n-1} = 1$. So, p^* is the associated logic of the feedback logic of LFSR(p).

By Lemma 8, the states of a nonzero cycle $\boldsymbol{c}$ in LFSR(p) correspond to a coset of a multiplicative cyclic group, and hence summing them up yields $\mathbf{0}^n$, and $\boldsymbol{c}$ is hence even. Furthermore, Equation (6) implies FSR$(p^*) = \{\overline{\boldsymbol{c}} : \boldsymbol{c} \in$ LFSR$(p)\}$, and it is known that len$(\boldsymbol{c})$ is odd for any $\boldsymbol{c} \in$ LFSR(p) [15]. Hence, any cycle of FSR(p^*) is odd. Statement (i) holds.

Summing a sequence $(s_0, s_1, s_2, \ldots)$ generated by LFSR(p) and its left-shift $(s_1, s_2, s_3, \ldots)$ derives a sequence $(s_0 \oplus s_1, s_1 \oplus s_2, s_2 \oplus s_3, \ldots)$ also generated by LFSR(p). Thus, the D-morphism is a well-defined mapping on LFSR(p). As shown above, any $\boldsymbol{c} \in$ LFSR(p) is even and len$(\boldsymbol{c})$ is odd. Then by Theorem 4, the D-morphic preimages of $\boldsymbol{c} \in$ LFSR(p) are exactly one even cycle $\boldsymbol{e}$ and its odd dual cycle $\overline{\boldsymbol{e}}$, where $\overline{\boldsymbol{e}} \notin$ LFSR(p). In other words, the D-morphism is injective on LFSR(p) and hence Statement (ii) holds.

For $\mathbf{v} = (v_0, v_1, \ldots, v_n) \in \mathbb{F}_2^{n+1}$, $\mathbf{v}$ is generated by LFSR(p) (resp. FSR(p^*)) if and only if $v_0 \oplus c_1 v_1 \oplus \cdots \oplus c_{n-1}v_{n-1} \oplus v_n = 0$ (resp. 1). Then Statement (iii) holds. □

Theorem 6. *The subFSRs of* LFSR(p_1) *are exactly* FSR$_1(x_0)$, LFSR(p_0), *and* FSR$({p_0}^*)$.

To prove Theorem 6, we prepare Lemma 10 and Corollary 3 below.

Lemma 10. *Let $p(x)$ be an irreducible polynomial of degree n over $\mathbb{F}_2$, and P the state transformation of* LFSR(p). *Then for any $\mathbf{u}_0, \mathbf{u}_n \in \mathbb{F}_2^n$, there exist $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_{n-1}$ such that for any $0 \le i < n$, $\mathbf{u}_{i+1} \in \{P(\mathbf{u}_i), \overline{P(\mathbf{u}_i)}\}$.*

Proof. Due to the isomorphism ϕ in Lemma 8, we consider the counterparts of $\mathbf{u}_i$'s in the finite field $\mathbb{F}_{2^n}$. Denote $v_0 = \phi(\mathbf{u}_0)$, $v_n = \phi(\mathbf{u}_n)$, and $c = \phi(\mathbf{1}^n)$. Clearly, $c \neq 0$. Since $c, c\rho, \ldots, c\rho^{n-1}$ is a linear basis of $\mathbb{F}_{2^n}$, $v_n \oplus \rho^n v_0 = a_0 c \oplus a_1 c\rho \oplus \cdots \oplus a_{n-1}c\rho^{n-1}$ for some $a_0, a_1, \ldots, a_{n-1} \in \mathbb{F}_2$. Let $v_{i+1} = v_i\rho \oplus a_{n-1-i}c$, $0 \le i < n-1$. Then it is verified that $v_n = v_0\rho^n \oplus (\oplus_{i=0}^{n-1} a_{n-i}\rho^{n-i}c) = v_{n-1}\rho \oplus a_0 c$.

Let $\mathbf{u}_i = \phi^{-1}(v_i)$, $0 < i < n$. Using the commutative diagram in Lemma 8, for any $0 \le i < n$, we have:

$$\begin{aligned}\mathbf{u}_{i+1} &= \phi^{-1}(v_i\rho \oplus a_{n-1-i}c) \\ &= P(\mathbf{u}_i) \oplus a_{n-1-i} \cdot \mathbf{1}^n \\ &\in \left\{P(\mathbf{u}_i), \overline{P(\mathbf{u}_i)}\right\}.\end{aligned} \tag{23}$$

□

Corollary 3. *Let $\{\boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell\} \subsetneq$* LFSR$(p)$, *where $p(x)$ is an irreducible polynomial of degree n over $\mathbb{F}_2$. Let S be the set of n-bit vectors in $\boldsymbol{c}_i$, $1 \le i \le \ell$. Then $\{\overline{\mathbf{v}} : \mathbf{v} \in S\} \nsubseteq S$.*

Proof. See that $S \neq \mathbb{F}_2^n$ and choose any $\mathbf{u}_0 \in S$ and $\mathbf{u}_n \in \mathbb{F}_2^n \setminus S$. By Lemma 10, there exist $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_{n-1}$ such that for any

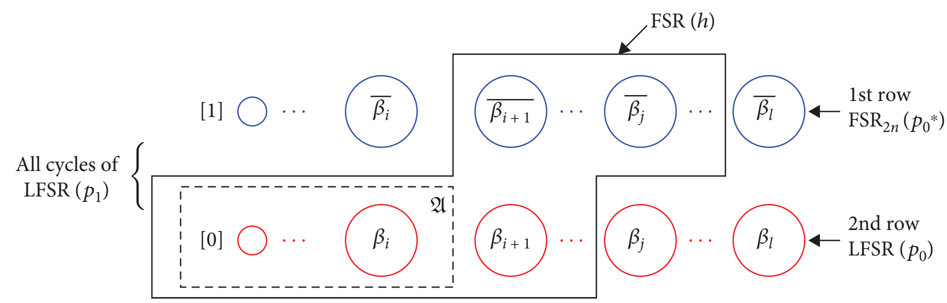


Figure 5: The assumed $2n$-stage subFSR $\mathrm{FSR}(h)$ of $\mathrm{LFSR}(p_1)$.

$0 \le i < n$, either $\mathbf{u}_{i+1}$ or $\overline{\mathbf{u}_{i+1}}$ is in the same cycle as $\mathbf{u}_i$. Note that if $\mathbf{u}_i \in S$ and $\mathbf{u}_{i+1}$ is in the same cycle as $\mathbf{u}_i$, then $\mathbf{u}_{i+1} \in S$. Thus, there exist some $1 \le j \le n$ such that $\mathbf{u}_j \notin S$ and $\overline{\mathbf{u}_j} \in S$, implying $\{\overline{\mathbf{v}} : \mathbf{v} \in S\} \nsubseteq S$. □

Proof of Theorem 6. By Lemma 2, Figure 4 shows that $\mathrm{FSR}_1(x_0)$, $\mathrm{LFSR}(p_0)$, and $\mathrm{FSR}(p_0{}^*)$ are subFSRs of $\mathrm{LFSR}(p_1)$. It remains to show that there exist no other subFSRs.

Let $\mathrm{FSR}_m(h)$ be a subFSR of $\mathrm{LFSR}(p_1)$.

First, Lemma 2 ensures $\mathrm{FSR}(h) \subset \mathrm{LFSR}(p_1)$. Due to Lemma 7, let k (resp. l) be the number of $3n$-cycles (resp. 1-cycles) of $\mathrm{FSR}(h)$. Lemma 3 derives the following integer equation:

$$3nk + l = 2^m, \tag{24}$$

where $1 \le m \le 2n$, $0 \le k \le 2(2^{2n} - 1)/(3n)$, and $0 \le l \le 2$. Letting $l = 0$ contradicts to $3 \nmid 2^m$. Because $2n = \min\{0 < i \in \mathbb{Z} : 3n \mid (2^i - 1)\}$, where n is a power of 3, Equation (24) holds only if (i) $l = 2$ and $m = 1$, or (ii) $l = 1$ and $m = 2n$.

Case (i) $l = 2$ and $m = 1$. The cycles of $\mathrm{FSR}(h)$ are exactly [0] and [1], i.e., $\mathrm{FSR}(h) = \mathrm{FSR}_1(x_0)$.

Case (ii) $l = 1$ and $m = 2n$. $\mathrm{FSR}(h)$ is of stage $2n$. Notice that $\mathrm{FSR}(h) \subset \mathrm{LFSR}(p_1)$ if and only if $\mathrm{FSR}(h^*) \subset \mathrm{LFSR}(p_1)$. We only have to consider $[0] \in \mathrm{FSR}(h)$, i.e., $\mathrm{FSR}(h)$ has [0] and $(2^{2n} - 1)/(3n)$ $3n$-cycles. Let $\mathfrak{A} = \{\boldsymbol{c} : \boldsymbol{c} \in \mathrm{FSR}(h), \overline{\boldsymbol{c}} \notin \mathrm{FSR}(h), \boldsymbol{c} \in \mathrm{LFSR}(p_0)\}$. Clearly, $[0] \in \mathfrak{A}$ and $\mathfrak{A}$ is not empty.

Assume $\mathrm{FSR}(h) \ne \mathrm{LFSR}(p_0)$. As shown in Figure 5, cycles in $\mathrm{FSR}(h)$ are partitioned into $\mathfrak{A}$ and $\mathrm{FSR}(h) \setminus \mathfrak{A}$ and cycles in $\mathrm{LFSR}(p_0)$ are partitioned into $\mathfrak{A}$ and $\mathrm{LFSR}(p_0) \setminus \mathfrak{A}$. Let

$$\begin{aligned} S &= \{\mathbf{v} : \mathbf{v} \text{ is a } 2n\text{-bit vector of } \boldsymbol{c}, \boldsymbol{c} \in \mathrm{FSR}(h) \setminus \mathfrak{A}\}, \\ S' &= \{\mathbf{v} : \mathbf{v} \text{ is a } 2n\text{-bit vector of } \boldsymbol{c}', \boldsymbol{c}' \in \mathrm{LFSR}(p_0) \setminus \mathfrak{A}\}. \end{aligned} \tag{25}$$

On the one hand, since a $2n$-stage FSR exhausts $\mathbb{F}_2^{2n}$ as its states:

$$S = S' = \mathbb{F}_2^{2n} \setminus \{\mathbf{v} : \mathbf{v} \text{ is a } 2n\text{-bit vector of } \boldsymbol{a}, \boldsymbol{a} \in \mathfrak{A}\}. \tag{26}$$

On the other hand, as the way $\mathfrak{A}$ is defined, we have:

$$\{\overline{\boldsymbol{c}} : \boldsymbol{c} \in \mathrm{FSR}(h) \setminus \mathfrak{A}\} \subseteq \{\boldsymbol{c} : \boldsymbol{c} \in (\mathrm{LFSR}(p_0) \cup \mathrm{FSR}(h)) \setminus \mathfrak{A}\}, \tag{27}$$

implying $\{\overline{\mathbf{v}} : \mathbf{v} \in S\} \subseteq S \cup S' = S$, i.e., $\{\overline{\mathbf{v}} : \mathbf{v} \in S\} \subseteq S$, contradictory to $\{\overline{\mathbf{v}} : \mathbf{v} \in S\} \nsubseteq S$ derived by Corollary 3.

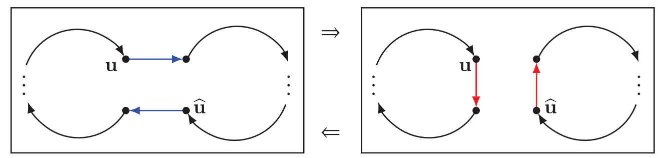


Figure 6: Interchanging next-states of $\mathbf{u}$ and $\hat{\mathbf{u}}$.

Therefore, the above assumption is not true, i.e., the $2n$-stage subFSR with the zero cycle is $\mathrm{LFSR}(p_0)$. □

2.6. The Cycle Joining Method

Theorem 7 (see [27, 28]) and (see [29], Theorem 2). *Let $\mathbf{u} = (u_0, u_1, \ldots, u_{m-1})$. Let $f(x_0, \ldots, x_{m-1})$ be an m-variable Boolean logic and $g(x_0, \ldots, x_{m-1}) = f(x_0, \ldots, x_{m-1}) \oplus \prod_{i=1}^{m-1} (x_i \oplus \overline{u_i})$. Then $\mathrm{FSR}_m(g)$ differs from $\mathrm{FSR}_m(f)$ only by interchanging the next-states of $\mathbf{u}$ and $\hat{\mathbf{u}}$. Specifically, as shown in Figure 6, if $\mathbf{u}$ and $\hat{\mathbf{u}}$ are in the same cycle $\boldsymbol{c} \in \mathrm{FSR}(f)$, then $\boldsymbol{c}$ is split into two adjacent cycles of $\mathrm{FSR}(g)$; if $\mathbf{u}$ and $\hat{\mathbf{u}}$ are in two distinct cycles $\boldsymbol{c}_1, \boldsymbol{c}_2 \in \mathrm{FSR}(f)$, then $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$ are joined into a single cycle of $\mathrm{FSR}(g)$.*

Definition 4. Given $\mathrm{FSR}_m(g)$ and a set $\Lambda \subset \mathbb{F}_2^m$, the *associated graph*, denoted by G_g^Λ, is a directed graph defined as follows: the vertices are cycles of $\mathrm{FSR}(g)$, and an arc is incident from $\boldsymbol{c}_1$ to $\boldsymbol{c}_2$ if and only if $\boldsymbol{c}_1$ is adjacent to $\boldsymbol{c}_2$ at $\mathbf{u} \in \Lambda$.

Definition 5. $\Lambda \subset \mathbb{F}_2^m$ is said to be a *potential set* of $\mathrm{FSR}_m(g)$ if the following two statements hold:

(i) Any cycle of $\mathrm{FSR}(g)$ has at most one vector in Λ;

(ii) The associated graph G_g^Λ is acyclic.

Remark 1. In Definition 5, the acyclic associated graph G_g^Λ implies that Λ contains no pair of conjugate vectors.

Definition 6. Given a set $\Lambda \subset \mathbb{F}_2^m$, its *characteristic function* $\lambda : \mathbb{F}_2^m \to \mathbb{F}_2$ is:

$$\lambda(\mathbf{u}) = \begin{cases} 1, & \mathbf{u} \in \Lambda; \\ 0, & \mathbf{u} \notin \Lambda. \end{cases} \tag{28}$$

1: Let $\mathfrak{G}_0$ be an empty set.
2: $\mathfrak{L}_0 \leftarrow [\boldsymbol{c}_0, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_{\ell-1}]$ is a list of cycles in a topological ordering of G_g^Λ, where $\mathfrak{L}_0$ exhaust cycles of FSR(g) with a state in $\{\mathbf{u} : \mathbf{u} \in \Lambda \text{ or } \widehat{\mathbf{u}} \in \Lambda\}$.
3: **for** $i = 0$ to $\ell - 1$ **do**
4: Denote $\mathfrak{L}_i = [\boldsymbol{c}_i^{(i)}, \boldsymbol{c}_{i+1}^{(i)}, \ldots, \boldsymbol{c}_{\ell-1}^{(i)}]$.
5: **if** $\boldsymbol{c}_i$ has a state $\mathbf{u}_i \in \Lambda$ **then**
6: As in Theorem 7, let $\boldsymbol{c}_i^{(i)}$ and $\boldsymbol{c}_k^{(i)}$ join into $\boldsymbol{c}_k^{(i+1)}$ by interchanging the next-states of $\mathbf{u}_i$ and $\widehat{\mathbf{u}}_i$, where $\boldsymbol{c}_k$ $(i < k \leq \ell - 1)$ contains $\widehat{\mathbf{u}}_i$.
7: $\mathfrak{L}_{i+1} \leftarrow [\boldsymbol{c}_{i+1}^{(i+1)}, \boldsymbol{c}_{i+2}^{(i+1)}, \ldots, \boldsymbol{c}_{\ell-1}^{(i+1)}]$, where $\boldsymbol{c}_j^{(i+1)} = \boldsymbol{c}_j^{(i)}$ for $j \neq k$.
8: $\mathfrak{G}_{i+1} \leftarrow \mathfrak{G}_i$
9: **else**
10: $\mathfrak{L}_{i+1} \leftarrow [\boldsymbol{c}_{i+1}^{(i)}, \boldsymbol{c}_{i+2}^{(i)}, \ldots, \boldsymbol{c}_{\ell-1}^{(i)}]$.
11: $\mathfrak{G}_{i+1} \leftarrow \mathfrak{G}_i \cup \{\boldsymbol{c}_i^{(i)}\}$
12: **end if**
13: **end for**
14: **return** $\mathfrak{G}_\ell \cup (\text{FSR}(g) \setminus \{\boldsymbol{c}_0, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_{\ell-1}\})$.

ALGORITHM 1: Cycle transition from FSR(g) to FSR(f).

Example 4. Let $\text{FSR}_m(f)$ be nonsingular and $\Lambda = \{\min_m(\boldsymbol{c}) \neq \mathbf{0}^m : \boldsymbol{c} \in \text{FSR}(f)\}$. Each cycle of FSR$(f)$ has a unique minimal m-bit vector. Furthermore, by Lemma 6, the associated graph G_f^Λ is acyclic. Thus, Λ is a potential set of FSR(f).

Note that for a subset $\Lambda' \subset \Lambda$, $G_g^{\Lambda'}$ is a subgraph of G_g^Λ. Hence, a subset of a potential set of FSR(g) is also potential for FSR(g).

Theorem 8 is the key tool of this paper.

Theorem 8. *Let* $\text{FSR}_m(g)$ *be nonsingular,* Λ *a potential set of* FSR(g), λ *the characteristic function of* Λ, *and* $f(\mathbf{x}) = g(\mathbf{x}) \oplus \lambda(\mathbf{x}) \oplus \lambda(\widehat{\mathbf{x}})$. *Then, the following statements hold:*

(i) $\text{FSR}_m(f)$ *is a nonsingular FSR.*
(ii) *A cycle of* FSR(f) *is joined by cycles of* FSR(g) *which form a weakly connected component in* G_g^Λ.
(iii) *If* FSR(h) *is a subFSR of this* $\text{FSR}_m(f)$, *then any cycle of* FSR(h) *is equivalent to a cycle* $\boldsymbol{c}$ *of* FSR(g) *such that* $\boldsymbol{c}$ *contains no vectors in* $\{\mathbf{u} : \mathbf{u} \in \Lambda \text{ or } \widehat{\mathbf{u}} \in \Lambda\}$.

Proof. Let

$$\begin{aligned}\lambda(\mathbf{x}) &= \lambda(x_0, x_1, \ldots, x_{m-1}) \\ &= x_0 \cdot \lambda_1(x_1, \ldots, x_{m-1}) \oplus (1 \oplus x_0) \cdot \lambda_2(x_1, \ldots, x_{m-1}).\end{aligned} \tag{29}$$

Then, the Boolean logic:

$$\begin{aligned}\lambda(\mathbf{x}) \oplus \lambda(\widehat{\mathbf{x}}) = &(x_0 \oplus 1 \oplus x_0) \cdot \lambda_1(x_1, \ldots, x_{m-1}) \\ &\oplus (1 \oplus x_0 \oplus x_0) \cdot \lambda_2(x_1, \ldots, x_{m-1}) \\ = &\lambda_1(x_1, \ldots, x_{m-1}) \oplus \lambda_2(x_1, \ldots, x_{m-1}),\end{aligned} \tag{30}$$

is independent of the first coordinate x_0 of $\mathbf{x}$. Thus, by Lemma 1, since $f(\mathbf{x}) = x_0 \oplus g_1(x_1, \ldots, x_{m-1}) \oplus (\lambda(\mathbf{x}) \oplus \lambda(\widehat{\mathbf{x}})) \oplus (\lambda(\mathbf{x}) \oplus \lambda(\widehat{\mathbf{x}}))$ for some Boolean function g_1, it characterizes a nonsingular FSR. Statement (i) of Theorem 8 is proved.

Due to Remark 1, we have:

$$\lambda(\mathbf{x}) \oplus \lambda(\widehat{\mathbf{x}}) = \begin{cases} 1, & \mathbf{x} \in \Lambda \text{ or } \widehat{\mathbf{x}} \in \Lambda; \\ 0, & \text{otherwise.} \end{cases} \tag{31}$$

Algorithm 1 obtains cycles of FSR(f) from those of FSR(g). □

Notice that, the Boolean logic f differs from g only at the vectors in Λ and their conjugates. Use notations in Algorithm 1. On the one hand, cycles of FSR(g) other than $\boldsymbol{c}_j$'s $(0 \leq j < \ell)$ are isolated vertices in G_g^Λ, and are hence cycles both for FSR(g) and for FSR(f). On the other hand, Algorithm 1 shows that each cycle of FSR(f) with a state in $\{\mathbf{u} : \mathbf{u} \in \Lambda \text{ or } \widehat{\mathbf{u}} \in \Lambda\}$ is joined by at least two cycles of FSR(g). Specifically, those cycles in the set $\mathfrak{G}_i$, in the list $\mathfrak{L}_i$, or in $\text{FSR}(g) \setminus \{\boldsymbol{c}_0, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_{\ell-1}\}$ are exactly cycles of FSR(f_i), where the Boolean logic f_i satisfies Equation (32). Notice that, $\mathbf{u}_i \in \Lambda$ occurs in $\boldsymbol{c}_i$ and hence in $\boldsymbol{c}_i^{(j)}$ for $0 \leq j \leq i$. In Lines 6–8, Algorithm 1 changes valuation at $\mathbf{u}_i$ in the cycle $\boldsymbol{c}_i$ (also in $\boldsymbol{c}_i^{(i)}$), and at its conjugate $\widehat{\mathbf{u}}_i$, and hence derives f_{i+1} from f_i.

$$f_i(\mathbf{x}) = \begin{cases} g(\mathbf{x}), & \{\mathbf{x}, \widehat{\mathbf{x}}\} \cap \{\mathbf{u} \in \Lambda : \exists j, 0 \leq j < i, \mathbf{u} \text{ occurs in } \boldsymbol{c}_j\} = \emptyset \text{ and } \{\mathbf{x}, \widehat{\mathbf{x}}\} \cap \Lambda \neq \emptyset; \\ f(\mathbf{x}), & \{\mathbf{x}, \widehat{\mathbf{x}}\} \cap \{\mathbf{u} \in \Lambda : \exists j, 0 \leq j < i, \mathbf{u} \text{ occurs in } \boldsymbol{c}_j\} \neq \emptyset; \\ f(\mathbf{x}) = g(\mathbf{x}), & \mathbf{x} \notin \Lambda \text{ and } \widehat{\mathbf{x}} \notin \Lambda. \end{cases} \tag{32}$$

Because G_g^{Λ} is acyclic and each vertex has at most one outdegree, G_g^{Λ} is a forest and a weakly connected component in it is a tree. Furthermore, due to the topological ordering, only cycle joining is used in Algorithm 1 and no cycle splitting occurs; and each vector in Λ causes a once joining. Thus, k cycles forming a tree in G_g^{Λ} is connected by $k-1$ arcs, and $k-1$ joinings compose them into a cycle in $\mathfrak{G}_{\ell}$, i.e., a cycle of $\mathrm{FSR}(f)$. Statement (ii) of Theorem 8 holds.

Furthermore, if a cycle $\boldsymbol{c} \in \mathrm{FSR}(f)$ is derived from joining more than one cycles of $\mathrm{FSR}(c)$, then $\boldsymbol{c}$ includes conjugate m-vectors and is hence not a cycle of any subFSR of $\mathrm{FSR}(f)$ by Lemma 4. Therefore, Statement (iii) of Theorem 8 is proved.

Statement (iii) in Theorem 8 implies Corollary 4 below.

Corollary 4. *Let* $\mathrm{FSR}(g)$ *and* $\mathrm{FSR}(f)$ *be defined as in Theorem 8. Then any subFSR of* $\mathrm{FSR}(f)$ *is also a subFSR of* $\mathrm{FSR}(g)$.

3. Some Relations between (Ir)Reducible and (In)Decomposable FSRs

Fisrt, we consider LFSRs. As for LFSRs, (note that in this paper LFSRs are defined to be homogeneous, i.e., their feedback logics in ANF do not have nonzero constant) reducibility is equivalent to decomposability. On the one hand, whether a LFSR is decomposable if and only if its characteristic polynomial is reducible [4, 6, 15]. On the other hand, $\mathrm{LFSR}(q(x)) \subset \mathrm{LFSR}(p(x))$ if and only if $q(x)|p(x)$ [15]. Thus, deciding indecomposability of LFSRs completely converts to irreducibility of their chracteristic polynnomials.

Second, we consider FSRs with the zero cycle.

Figure 2 straightforwardly yields Proposition 1 below.

Proposition 1. *If* $\mathrm{FSR}(h) = \mathrm{FSR}_n(f) * \mathrm{FSR}(g)$ *and* $f(\mathbf{0}^n) = 0$, *then* $\mathrm{FSR}(g)$ *is a subFSR of* $\mathrm{FSR}(h)$.

Proposition 2 (see [4]). *Let* $\mathrm{FSR}_d(h)$ *be a decomposable FSR satisfying* $h(\mathbf{0}^d) = 0$. *Then there exist* $\mathrm{FSR}_{d-m}(h_1)$ *and* $\mathrm{FSR}_m(h_2)$ *for some* $1 \le m < d$ *such that* $\mathrm{FSR}(h) = \mathrm{FSR}_{d-m}(h_1) * \mathrm{FSR}_m(h_2)$ *and* $h_1(\mathbf{0}^{d-m}) = h_2(\mathbf{0}^m) = 0$. *Particularly,* $\mathrm{FSR}(h_2)$ *is a subFSR of* $\mathrm{FSR}(h)$ *and* $\mathrm{FSR}(h)$ *is reducible.*

Proof. Assume $\mathrm{FSR}(h) = \mathrm{FSR}_{d-m}(f) * \mathrm{FSR}_m(g)$ for some $1 \le m < d$. Denote $\delta = g(\mathbf{0}^m)$. Then using Equation (3) yields:

$$h(\mathbf{0}^d) = f(\delta, \delta, \ldots, \delta) \oplus \delta = 0. \tag{33}$$

Thereafter we take h_1 and h_2 as follows:

$$\begin{cases} h_1 = f, h_2 = g, & \text{if } \delta = 0; \\ h_1 = f^*, h_2 = g \oplus 1, & \text{if } \delta = 1. \end{cases} \tag{34}$$

Immediately, we have $h_1(\mathbf{0}^{d-m}) = h_2(\mathbf{0}^m) = 0$.

Moreover, because $\mathrm{FSR}(f) * \mathrm{FSR}(g) = \mathrm{FSR}(f^*) * \mathrm{FSR}(g \oplus 1)$ [16, Lemma 1], it always holds that $\mathrm{FSR}(h) = \mathrm{FSR}(h_1) * \mathrm{FSR}(h_2)$. The rest of proof is completed by Proposition 1. □

The idea of Proposition 2 was given by Green and Dimond [4] and here we reinterpret it.

Third, note that there are infinitely many irreducible and indecomposable FSRs, and below we answer the question whether all irreducible (resp. indecomposable) FSRs are indecomposable (resp. irreducible).

Theorem 9. *There exist infinitely many reducible and indecomposable FSRs.*

Proof. We give a family of reducible and indecomposable FSRs as below.

Consider any even $n \ge 6$. Since the finite field $\mathbb{F}_{2^n}$ has a cyclic multiplicative group $\mathbb{F}_{2^n}^*$, we choose $p(x) = c_0 \oplus c_1 x \oplus \cdots \oplus c_{n-1} x^{n-1} \oplus x^n$ to be the minimal polynomial of ρ over $\mathbb{F}_2$, where $\rho \in \mathbb{F}_{2^n}^*$ is of order $(2^n - 1)/3$. Let

$$h(x_0, \ldots, x_{n-1}) = \left(\bigoplus_{j=0}^{n-1} c_j x_j \right) \oplus \left(\prod_{j=1}^{n-1} x_j \right). \tag{35}$$

It is known that $\mathrm{LFSR}(p) = \{[0], \boldsymbol{c}_1, \boldsymbol{c}_2, \boldsymbol{c}_3\}$, where $\boldsymbol{c}_i$'s are three $(2^n - 1)/3$-cycles [15]. Without loss of generality, assume that $\mathbf{1}^n$ occurs in $\boldsymbol{c}_1$. Then in $\boldsymbol{c}_1$, $0\mathbf{1}^{n-1}$ precedes $\mathbf{1}^n$ and $\mathbf{1}^n$ precedes $\mathbf{1}^{n-1}0$. By Theorem 7, in $\mathrm{FSR}(h)$, $\boldsymbol{c}$ is split to $[1]$ and a $(2^n - 4)/3$-cycle $\boldsymbol{c}_1'$, and hence $\mathrm{FSR}(h) = \{[0], [1], \boldsymbol{c}_1', \boldsymbol{c}_2, \boldsymbol{c}_3\}$.

Consider subFSR(s) of $\mathrm{FSR}(h)$. $\mathrm{FSR}_1(x_0) \subset \mathrm{FSR}(h)$, and other possible subFSR(s) should be of stage $n-1$ since

$$\mathrm{len}(\boldsymbol{c}_2) = \mathrm{len}(\boldsymbol{c}_3) > \mathrm{len}(\boldsymbol{c}_1') = (2^n - 4)/3 > 2^{n-2}. \tag{36}$$

However, because the integer equation:

$$a \frac{2^n - 1}{3} + b \frac{2^n - 4}{3} + c = 2^{n-1}, \tag{37}$$

where $a, c \in \{0, 1, 2\}$ and $b \in \{0, 1\}$, has no solution, by Lemma 3, $\mathrm{FSR}(h)$ has no subFSR of stage $n-1$. Thus, $\mathrm{FSR}_1(x_0)$ is the unique subFSR of $\mathrm{FSR}(h)$.

Assume that $\mathrm{FSR}(h)$ is decomposable. By Proposition 2, $\mathrm{FSR}(h) = \mathrm{FSR}_{n-1}(f) * \mathrm{FSR}_1(x_0)$, where $[0] \in \mathrm{FSR}(f)$. Note that $p(x)$ is an irreducible polynomial over $\mathbb{F}_2$. By Corollary 3, the cycle $\boldsymbol{c}_2$ is not self-dual. Moreover, by Statement (i) of Lemma 9, the cycle $\boldsymbol{c}_2$ is even. If so, by Corollary 2 and Theorem 4, $\boldsymbol{c}_3$ is the dual of $\boldsymbol{c}_2$ and $D(\boldsymbol{c}_3) = D(\boldsymbol{c}_2)$, implying:

Require: A Boolean circuit f_0.
Ensure: FSR(f).
1: Read the fan-in r of f_0.
2: Compute $n=3^k$, where $k=\min\{i\in\mathbb{Z}:i>\log_3(r/2)\}$.
3: Construct a $4n$-input Boolean circuit $f(x_0,x_1,\ldots,x_{4n-1})=x_0\oplus x_{2n}\oplus\lambda(x_0,x_1,\ldots,x_{4n-1})\oplus\lambda(\overline{x_0},x_1,\ldots,x_{4n-1})$ with λ described in Figure 8.
4: **return** FSR$_{4n}(f)$.

Algorithm 2: Transforming a Boolean circuit to a FSR (a reduction for Theorem 1).

$$\{\overline{\mathbf{v}}\in\mathbb{F}_2^n:\mathbf{v}\text{ occurs in }\boldsymbol{c}_2\text{ or }\boldsymbol{c}_3\}=\{\mathbf{v}\in\mathbb{F}_2^n:\mathbf{v}\text{ occurs in }\boldsymbol{c}_2\text{ or }\boldsymbol{c}_3\},\tag{38}$$

contradictory to Corollary 3. Therefore, FSR(h) is indecomposable. □

Theorem 10. *There exist infinitely many decomposable and irreducible FSRs.*

Proof. We construct a family of decomposable and irreducible FSRs as below.

Consider any $n>2$. There exist FSR$_n(f)$ outputting a de Bruijn sequence [27], i.e., FSR$_n(f)$ has only one 2^n-cycle $\boldsymbol{c}$. Let FSR$(h)=$ FSR$(f)*$FSR$_1(x_0)$. Clearly, FSR(h) is decomposable. Furthermore, by Theorem 4 and Corollary 2, FSR(h) has exactly two cycles $\boldsymbol{d}$ and $\overline{\boldsymbol{d}}$, implying that $\mathbf{0}^{n+1}$ and $\mathbf{1}^{n+1}$ do not occur in the same cycle. Since no FSR of stage less than $n+1$ generates $\mathbf{0}^{n+1}$ or $\mathbf{1}^{n+1}$, neither $\boldsymbol{d}$ nor $\overline{\boldsymbol{d}}$ defines a subFSR. Therefore, FSR(h) is irreducible. □

4. NP-Hardness of Deciding Irreducible FSRs

This section proves Theorem 1. Above all, we sketch our idea. Our way is to give a polynomial-time Karp reduction (detailed in Algorithm 2) from the CIRCUIT SATISFIABILITY problem to the FSR IRREDUCIBILITY problem. Using the cycle joining method in Theorem 8, we choose FSR$(g)=$ LFSR(p_2) and construct a potential set Λ_2 such that in the associated graph $G_{p_2}^{\Lambda_2}$ (i) all $6n$-cycles of LFSR(p_2) are not isolated (by Lemma 15) and (ii) all cycles in LFSR(p_0) are sources (by Lemma 14). The Boolean circuit f_0 (the input of the Karp reduction) is used to tune Λ_2 such that all cycles in LFSR(p_0) are isolated in $G_{p_2}^{\Lambda_2}$ if and only if f_0 is unsatisfiable. The parameters are chosen such that there exists no subFSR of stage less than $2n$ (by Theorem 5). Because a nonisolated cycle in $G_{p_2}^{\Lambda_2}$ does not admit a subFSR of f (by Lemma 4), p_0 is the only possible subFSR of f and it occurs if and only if f_0 is unsatisfiable (by Lemma 16). Additionally, the transformation itself is polynomial-time computable (detailed in Lemma 17). Below we give details of this proof.

In this section, for $\mathbf{v}\in\mathbb{F}_2^{4n}$, $\mathbf{Cycle}(\mathbf{v})$ denotes the unique cycle of LFSR(p_2) containing $\mathbf{v}$.

Definition 7. Let $\mathfrak{C}$ denote the set of cycles of LFSR(p_2) min-adjacent to a cycle of LFSR(p_0); and let $\mathfrak{D}$ denote the set of cycles $\boldsymbol{c}$ in $\mathfrak{C}$ such that any cycle in $\mathfrak{B}_{6n}$ is not min-adjacent to $\boldsymbol{c}$. Formally,

$$\begin{aligned}\mathfrak{C}&=\{\boldsymbol{c}\in\text{LFSR}(p_2):\mathbf{Cycle}((\mathbf{10}^{4n-1})\oplus\min_{4n}(\boldsymbol{c}))\in\text{LFSR}(p_0)\};\\ \mathfrak{D}&=\{\boldsymbol{c}\in\mathfrak{C}:\text{for any }\mathbf{v}\in\mathbb{F}_2^{4n}\text{ in }\boldsymbol{c},\mathbf{Cycle}(\widehat{\mathbf{v}})\notin\mathfrak{B}_{6n}\text{ or }\widehat{\mathbf{v}}\neq\min_{4n}(\mathbf{Cycle}(\widehat{\mathbf{v}}))\}.\end{aligned}\tag{39}$$

Lemma 11 shows that in LFSR(p_2), a cycle $\boldsymbol{c}\in$ LFSR(p_0) is adjacent only to $6n$-cycles.

Lemma 11. *Let $\boldsymbol{c}_1,\boldsymbol{c}_2\in$ LFSR(p_2). If $\boldsymbol{c}_1$ is adjacent to $\boldsymbol{c}_2$ and $\boldsymbol{c}_1\in$ LFSR(p_0), then $\boldsymbol{c}_2\in\mathfrak{B}_{6n}$.*

Proof. Let $\mathbf{v}$ be a $4n$-bit vector in $\boldsymbol{c}_1$. Suppose $\boldsymbol{c}_2\in$ LFSR(p_0). Note that $\widehat{\mathbf{v}}$ is a $4n$-bit vector in $\boldsymbol{c}_2$. By Lemma 7, we have $L_2^{3n}(\widehat{\mathbf{v}})=\widehat{\mathbf{v}}$ and $L_2^{3n}(\mathbf{v})=\mathbf{v}$. Since L_2 is a linear transformation and $\mathbf{10}^{4n-1}=\mathbf{v}\oplus\widehat{\mathbf{v}}$, we have $L_2^{3n}(\mathbf{10}^{4n-1})=\mathbf{10}^{4n-1}$, contradictory to the fact $L_2^{3n}(\mathbf{10}^{4n-1})=(\mathbf{0}^n\mathbf{10}^{2n-1}\mathbf{10}^{n-1})\neq(\mathbf{10}^{4n-1})$. Therefore, the above supposition does not hold and hence $\boldsymbol{c}_2\in$ LFSR$(p_2)\setminus$ LFSR$(p_0)=\mathfrak{B}_{6n}$. □

By Definition 7 and Lemma 11, we have $\mathfrak{D}\subseteq\mathfrak{C}\subseteq\mathfrak{B}_{6n}$.

Example 5. Let $p_2(x)=x^{12}\oplus x^6\oplus 1$. For LFSR$(p_2)$,

$$\begin{aligned}\mathfrak{C}=\{&[1,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0],\\ &[1,0,0,0,1,0,0,1,0,0,0,0,1,1,0,0,1,0],\\ &[1,0,0,0,1,1,0,1,1,0,0,0,1,1,1,0,1,1]\}\end{aligned}\tag{40}$$

and $\mathfrak{D}$ includes only one cycle:

$$[1,0,0,0,1,1,0,1,1,0,0,0,1,1,1,0,1,1].\tag{41}$$

In this section, for a Boolean logic $f_0:\mathbb{F}_2^r\rightarrow\mathbb{F}_2$, $r<2n$, we define four subsets of $\mathbb{F}_2^{4n}$:

$$\begin{cases} \Lambda_{3n,f_0} = \{\min_{4n}(\boldsymbol{c}) : [0] \neq \boldsymbol{c} \in \mathrm{LFSR}(p_0), \exists \mathbf{v} \in \mathbb{F}_2^{2n} \text{ in } \boldsymbol{c}, f_0(\lceil \mathbf{v} \rceil_r) = 1\}, \\ \Lambda_{\overline{\mathfrak{C}}} = \{\min_{4n}(\boldsymbol{c}) : \boldsymbol{c} \in \mathfrak{B}_{6n} \backslash \mathfrak{C}\}, \\ \Lambda_{\mathfrak{D}} = \{L_2^{5n}(\min_{4n}(\boldsymbol{c})) : \boldsymbol{c} \in \mathfrak{D}\}, \\ \Lambda_2 = \Lambda_{3n,f_0} \cup \Lambda_{\overline{\mathfrak{C}}} \cup \Lambda_{\mathfrak{D}}. \end{cases} \quad (42)$$

Theorem 11. *Λ_2 is a potential set of* LFSR(p_2).

To prove Theorem 11, we need Lemmas 12–14.
To some extent, Lemma 12 describes the cycles in $\mathfrak{C}$.

Lemma 12. *If $\boldsymbol{c} \in \mathfrak{C}$, then*

$$\boldsymbol{c} = [1\mathbf{u}_0 0\mathbf{u}_1 0\mathbf{u}_2 0\mathbf{u}_0 1\mathbf{u}_1 0\mathbf{u}_2], \quad (43)$$

where $\mathbf{u}_0, \mathbf{u}_1, \mathbf{u}_2 \in \mathbb{F}_2^{n-1}$, $\mathbf{u}_2 = \mathbf{u}_0 \oplus \mathbf{u}_1$, *and* $(1\mathbf{u}_0 0\mathbf{u}_1 0\mathbf{u}_2 0\mathbf{u}_0) = \min_{4n}(\boldsymbol{c})$.

Proof. As $\boldsymbol{c} \in \mathfrak{C} \subseteq \mathfrak{B}_{6n}$, we denote

$$\boldsymbol{c} = [a_0\mathbf{u}_0 a_1\mathbf{u}_1 a_2\mathbf{u}_2 a_3\mathbf{u}_3 a_4\mathbf{u}_4 a_5\mathbf{u}_5], \quad (44)$$

where

$$\begin{cases} a_i \in \mathbb{F}_2, 0 \leq i \leq 5; \\ \mathbf{u}_i \in \mathbb{F}_2^{n-1}, 0 \leq i \leq 5; \\ (a_0\mathbf{u}_0 a_1\mathbf{u}_1 a_2\mathbf{u}_2 a_3\mathbf{u}_3) = \min_{4n}(\boldsymbol{c}). \end{cases} \quad (45)$$

Note that, the cycle $[\mathbf{1}\mathbf{0}^{4n-1}\mathbf{1}\mathbf{0}^{2n-1}] \in \mathrm{LFSR}(p_2)$ contains $\mathbf{1}\mathbf{0}^{4n-1}$. Then the $6n$-bit sequence of LFSR(p_2) containing $(\mathbf{1}\mathbf{0}^{4n-1}) \oplus \min_{4n}(\boldsymbol{c})$ is:

$$(\overline{a_0}\mathbf{u}_0 a_1\mathbf{u}_1 a_2\mathbf{u}_2 a_3\mathbf{u}_3 \overline{a_4}\mathbf{u}_4 a_5\mathbf{u}_5), \quad (46)$$

since L_2 is a linear transformation. By Lemma 7, If the sequence Equation (46) is generated by LFSR(p_0), then its period divides $3n$, and hence $a_2 = a_0 \oplus a_1 \oplus 1$, $\mathbf{u}_2 = \mathbf{u}_0 \oplus \mathbf{u}_1$, $a_3 = \overline{a_0}$, $\mathbf{u}_3 = \mathbf{u_0}$, $\overline{a_4} = a_1$, $\mathbf{u}_4 = \mathbf{u}_1$, $a_5 = a_2$, and $\mathbf{u}_5 = \mathbf{u}_2$. Thus, we get

$$\boldsymbol{c} = [a_0\mathbf{u}_0 a_1\mathbf{u}_1 a_2\mathbf{u}_2 \overline{a_0}\mathbf{u}_0 \overline{a_1}\mathbf{u}_1 a_2\mathbf{u}_2]. \quad (47)$$

Due to Equation (45), we have:

$$(a_0\mathbf{u}_0 a_1\mathbf{u}_1 a_2\mathbf{u}_2 \overline{a_0}\mathbf{u}_0) < (\overline{a_0}\mathbf{u}_0 \overline{a_1}\mathbf{u}_1 a_2\mathbf{u}_2 a_0\mathbf{u}_0), \quad (48)$$

and hence $a_0 = 1$. Similarly, we have:

$$(a_0\mathbf{u}_0 a_1\mathbf{u}_1 a_2\mathbf{u}_2 \overline{a_0}\mathbf{u}_0) < (\mathbf{u}_0 a_1\mathbf{u}_1 a_2\mathbf{u}_2 \overline{a_0}\mathbf{u}_0 \overline{a_1}), \quad (49)$$

and hence $a_1 = 0$. Immediately, $a_2 = a_0 \oplus a_1 \oplus 1 = 0$. The proof is complete. □

Lemma 13 describes in which cycles the conjugates of vectors in $\Lambda_{\mathfrak{D}}$ are located.

Lemma 13. *For any $\mathbf{v} \in \Lambda_{\mathfrak{D}}$, $\widehat{\mathbf{v}}$ is contained in a cycle in $\mathfrak{B}_{6n} \setminus \mathfrak{C}$.*

Proof. Let $\boldsymbol{c} \in \mathfrak{D}$ and $\mathbf{v} = L_2^{5n}(\min_{4n}(\boldsymbol{c}))$. Since $\mathfrak{D} \subseteq \mathfrak{C}$, $\boldsymbol{c}$ is of the form Equation (43) given in Lemma 12. Then,

$$\widehat{\mathbf{v}} = (\mathbf{1}\mathbf{0}^{4n-1}) \oplus L_2^{5n}(\min_{4n}(\boldsymbol{c})) = (1\mathbf{u}_2 1\mathbf{u}_0 0\mathbf{u}_1 0\mathbf{u}_2), \quad (50)$$

and hence,

$$\mathbf{Cycle}\ (\widehat{\mathbf{v}}) = [1\mathbf{u}_2 1\mathbf{u}_0 0\mathbf{u}_1 0\mathbf{u}_2 1\mathbf{u}_0 1\mathbf{u}_1]. \quad (51)$$

For a $6n$-cycle $[b_0, b_1, \ldots, b_{6n-1}]$,

$$\left(b_i, b_{(i+n) \bmod 6n}, b_{(i+2n) \bmod 6n}, \ldots, b_{(i+5n) \bmod 6n}\right) \quad (52)$$

is called an *n-sampling* of $[b_0, b_1, \ldots, b_{6n-1}]$, $0 \leq i < 6n$.

On the one hand, see that len$(\mathbf{Cycle}(\widehat{\mathbf{v}})) \notin \{1, 3n\}$. Thus, by Lemma 7, $\mathbf{Cycle}(\widehat{\mathbf{v}}) \in \mathfrak{B}_{6n}$.

On the other hand, by Lemma 12, (100010) occurs as an n-sampling of any cycle in $\mathfrak{C}$. However, as shown in (51), (100010) is not an n-sampling of $\mathbf{Cycle}(\widehat{\mathbf{v}})$. Therefore, $\mathbf{Cycle}\ (\widehat{\mathbf{v}}) \notin \mathfrak{C}$. □

Lemma 14. *The cycles of* LFSR(p_0) *are sources in the associated graph $G_g^{\Lambda_2}$, and $G_g^{\Lambda_2}$ is acyclic.*

Proof. Recall that an arc is incident from $\boldsymbol{c}_1$ to $\boldsymbol{c}_2$ if $\boldsymbol{c}_1$ is adjacent to $\boldsymbol{c}_2$ at some $\mathbf{v} \in \Lambda_2$.

First, consider cycles of LFSR(p_0). By Lemma 11, the successor of any cycle of LFSR(p_0) in $G_g^{\Lambda_2}$, if there is one, is a cycle in $\mathfrak{B}_{6n}$. Moreover, by Definition 7 and Lemma 13, no cycle in $(\mathfrak{B}_{6n} \setminus \mathfrak{C}) \cup \mathfrak{D}$ is adjacent to a cycle in LFSR(p_0) at some $\mathbf{v} \in \Lambda_2$. Thus, cycles of LFSR(p_0) are sources in $G_{p_2}^{\Lambda_2}$.

Second, consider cycles in $\mathfrak{D}$. By Definition 7 (resp. Lemma 13), in $G_{p_2}^{\Lambda_2}$ there exists no arc incident from any cycle in $\mathfrak{B}_{6n} \setminus \mathfrak{C}$ (resp. in $\mathfrak{D}$) to a cycle in $\mathfrak{D}$. Hence, due to Definition 4 and Equation (42), in $G_{p_2}^{\Lambda_2}$, a cycle in $\mathfrak{D}$ is either a source or a successor of a cycle of LFSR(p_0). Therefore, in either case any $\boldsymbol{d} \in \mathfrak{D}$ is not a vertex in a cyclic walk in $G_{p_2}^{\Lambda_2}$.

Thus, $G_{p_2}^{\Lambda_2}$ is acyclic if and only if $G_{p_2}^{\Lambda_{3n,f_0} \cup \Lambda_{\overline{\mathfrak{C}}}}$ is acyclic.

Because any $\mathbf{v} \in \Lambda_{3n,f_0} \cup \Lambda_{\overline{\mathfrak{C}}}$ is the nonzero minimal $4n$-vector in $\mathbf{Cycle}(\mathbf{v})$, $G_{p_2}^{\Lambda_{3n,f_0} \cup \Lambda_{\overline{\mathfrak{C}}}}$ is loopless by Corollary 1, and is furthermore acyclic by Lemma 6. The proof is complete. □

Incorporating the proof of Lemma 14 and Definition 7, we present Figure 7 to show (possible) directions of arcs in $G_{p_2}^{\Lambda_2}$.

Proof of Theorem 11. By (42) and $\mathfrak{D} \subseteq \mathfrak{C} \subseteq \mathfrak{B}_{6n}$, any cycle of LFSR$(p_2)$ has at most one vector in Λ_2. By Lemma 14, $G_{p_2}^{\Lambda_2}$ is

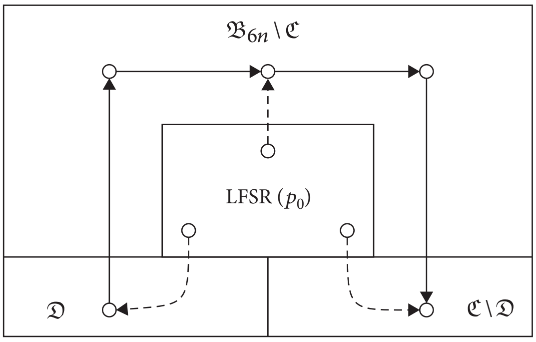


FIGURE 7: A sketch of (possible) directions of arcs in $G_{p_2}^{\Lambda_2}$.

acyclic. Therefore, Λ_2 satisfies Statements (i) and (ii) in Definition 5. □

Lemma 15. *No cycle in $\mathfrak{B}_{6n}$ is an isolated vertex in $G_{p_2}^{\Lambda_2}$.*

Proof. Note that $\mathfrak{B}_{6n} = (\mathfrak{B}_{6n} \setminus \mathfrak{C}) \cup \mathfrak{D} \cup (\mathfrak{C} \setminus \mathfrak{D})$. See Figure 7.

By Definition 4 and Equation (42), any cycle in $(\mathfrak{B}_{6n} \setminus \mathfrak{C}) \cup \mathfrak{D}$ is not isolated in $G_{p_2}^{\Lambda_2}$.

Moreover, by Definition 7, for $\boldsymbol{c} \in \mathfrak{C} \setminus \mathfrak{D}$, there exists $\boldsymbol{d} \in \mathfrak{B}_{6n}$ such that $\boldsymbol{c}$ contains the conjugate of $\min_{4n}(\boldsymbol{d})$. Then $\boldsymbol{d} \notin \mathfrak{C}$ by Definition 7, and hence $\min_{4n}(\boldsymbol{d}) \in \Lambda_{\overline{\mathfrak{C}}}$. Thus, there exists $\boldsymbol{d} \in \mathfrak{B}_{6n} \setminus \mathfrak{C}$ min-adjacent to $\boldsymbol{c}$. Therefore, any cycle in $\mathfrak{C} \setminus \mathfrak{D}$ is not isolated in $G_{p_2}^{\Lambda_2}$. □

Lemma 16. *Let Λ_2 be defined in Equation (42) and λ its characteristic function. Let*

$$f(x_0, x_1, \ldots, x_{4n-1}) = x_0 \oplus x_{2n} \oplus \lambda(x_0, x_1, \ldots, x_{4n-1}) \oplus \lambda(\overline{x_0}, x_1, \ldots, x_{4n-1}). \tag{53}$$

Then $\mathrm{FSR}_{4n}(f)$ *is irreducible if and only if the Boolean circuit f_0 is satisfiable.*

Proof. By Theorem 11, Λ_2 is a potential set of LFSR(p_2).

By Theorem 8, FSR(f) is nonsingular and it is reducible if and only if there exists $\mathrm{FSR}_m(h)$, $m < 4n$, such that all its cycles essentially belong to LFSR(p_2) and all m-bit vectors generated by FSR(h) are not in $\{\mathbf{v} : \mathbf{v} \in \Lambda_2 \text{ or } \widehat{\mathbf{v}} \in \Lambda_2\}$. Furthermore, by Lemma 15, any cycle in $\mathfrak{B}_{6n}$ has a state in $\{\mathbf{v} : \mathbf{v} \in \Lambda_2 \text{ or } \widehat{\mathbf{v}} \in \Lambda_2\}$, and hence we only have to consider such FSR(h) with its cycles in LFSR(p_0).

Suppose f_0 to be unsatisfiable. Then Λ_{3n, f_0} is empty as defined in Equation (42). By Definition 4 and Lemma 14, all cycles of LFSR(p_0) are isolated vertices in $G_{p_2}^{\Lambda_2}$. Therefore, LFSR(p_0) is a subFSR of FSR(f).

Suppose f_0 to be satisfiable. Since the nonzero cycles of LFSR(p_0) exhaust all nonzero $2n$-bit vectors and $r < 2n$, there exists at least one nonzero cycle $\boldsymbol{c} \in$ LFSR(p_0) containing a $2n$-bit vector $\mathbf{v}$ such that $f_0(\lceil \mathbf{v} \rceil_r) = 1$. Then Λ_{3n, f_0} is not empty as defined in Equation (42). In this case, all cycles in $\mathfrak{B}_{6n}$ and some cycle(s) of LFSR(p_0) are not isolated vertices in $G_{p_2}^{\Lambda_2}$. Thus, by Theorem 8, a subFSR of FSR(f) should be a subFSR of LFSR(p_0). Anyhow, LFSR(p_0) has no subFSR by Theorem 5, and hence FSR(f) is irreducible. □

Lemma 17. *There exists a polynomial-time algorithm for the transformation defined by Algorithm 2.*

Proof. In Figure 8, the characteristic functions of Λ_{3n, f_0}, $\Lambda_{\overline{\mathfrak{C}}}$, $\Lambda_{\mathfrak{D}}$ and Λ_2 are given in peudocodes. Note that in $\mathsf{Test}_{\Lambda_{\mathfrak{D}}}$, $\mathbf{v}_0 = L_2^n(\mathbf{x})$ is equivalent to $\mathbf{x} = L_2^{5n}(\mathbf{v}_0)$.

First, the linear transformations L_0, L_1 and L_2 have complexity $\mathcal{O}(1)$. Second, the subprocedure $\mathsf{IsNonzero}_k$ decides whether $\mathbf{x}$ is a nonzero k-bit vector and $\mathsf{IsNonzero}_{4n}$ costs $\mathcal{O}(n)$; $\mathsf{IsMin}_{T,l}$ decides whether $\mathbf{x}$ is the minimal vector in the sequence $\mathbf{x}, T(\mathbf{x}), \ldots, T^k(\mathbf{x})$, where T is the state transformation, and $\mathsf{IsMin}_{L_2, 6n}$ costs $\mathcal{O}(n^2)$; $\mathsf{IsInB6n}$ decides whether $\mathbf{Cycle}(\mathbf{x}) \in \mathfrak{B}_{6n}$, and costs $\mathcal{O}(n)$; $\mathsf{IsSol3n}$ decides whether f_0 is evaluated 1 at some r-bit vector in the cycle $\boldsymbol{c} \in$ LFSR(p_0) containing $\mathbf{x}$, and costs $\mathcal{O}(n \cdot \mathrm{SIZE}(f_0))$. Thus, the time complexity of $\mathsf{Test}_{\Lambda_{3n, f_0}}$, $\mathsf{Test}_{\Lambda_{\overline{\mathfrak{C}}}}$, $\mathsf{Test}_{\Lambda_{\mathfrak{D}}}$, and λ are, respectively, $\mathcal{O}(n^2 + n \cdot \mathrm{SIZE}(f_0))$, $\mathcal{O}(n^2)$, $\mathcal{O}(n^3)$ and $\mathcal{O}(n^3 + n \cdot \mathrm{SIZE}(f_0))$. Third, Line 2 of Algorithm 2 costs $\mathcal{O}(\log r \cdot \log n)$, and ensures $r < 2n \le 3r$. Moreover, the fan-in is not greater than the circuit size, i.e., $r \le \mathrm{SIZE}(f_0)$. Therefore, the time complexity of λ, and hence that of f, is polynomial in SIZE(f_0).

Furthermore, incorporating Figure 9 we give a branchless interpretation of the logic λ via standard instructions and the input circuit f_0. Additionally, the nesting depth of loop structures is not greater than three, and each loop structure has a controlling counter upper-bounded by $6n$, including implicit loops in $\mathsf{IsNonzero}$, L_2^n and L_2^{3n}. Thus, we conclude that Figures 8 and 9 enable to express the feedback logic f as a straight-line program scaling up its size up to n (essentially dependent on SIZE(f_0)), with at most $\mathsf{poly}(n)$ instructions, where $\mathsf{poly}(n)$ is a polynomial in n. Moreover, the parameter $n \le 3 \cdot \mathrm{SIZE}(f_0)/2$ is efficiently decided in Line 2 of Algorithm 2. Therefore, given a Boolean circuit f_0, there exists a polynomial-time algorithm characterizing the above FSR(f). □

Proof of Theorem 1. By Theorem 3, Lemmas 16 and 17, Algorithm 2 gives a polynomial-time Karp reduction from the **NP**-complete problem CIRCUIT SATISFIABILITY to FSR IRREDUCIBILITY. Therefore, we conclude that FSR IRREDUCIBILITY is **NP**-hard. □

5. NP-Hardness of Deciding Indecomposable FSRs

This section proves Theorem 2. Above all, we sketch our idea. Similar to the proof of Theorem 1, we give a Karp reduction (detailed in Algorithm 3) from the CIRCUIT SATISFIABILITY problem to the FSR INDECOMPOSABILITY problem. Using the cycle joining method in Theorem 8, we take FSR$(g) =$ LFSR(p_1) and construct a potential set Λ_{p_0, f_0} of LFSR(p_1) in the following way. The potential set of LFSR(p_0) defined in

Require: A Boolean circuit f_0.
Ensure: $\mathrm{FSR}(f)$.
Read the fan-in r of f_0.
Compute $n = 3^k$, where $k = \min\{i \in \mathbb{Z} : i > \log_3(r/2)\}$.
Construct a $(2n+1)$-input Boolean circuit $f(x_0, x_1, \ldots, x_{2n}) = x_0 \oplus x_1 \oplus x_n \oplus x_{n+1} \oplus x_{2n} \oplus \lambda(x_0, x_1, \ldots, x_{2n}) \oplus \lambda(\overline{x_0}, x_1, \ldots, x_{2n})$ with λ described in Figure 10.
return $\mathrm{FSR}_{2n+1}(f)$.

ALGORITHM 3: Transforming a Boolean circuit to a FSR (a reduction for Theorem 2).

Line 2 of Algorithm 2

$n \leftarrow 1$
repeat $n \leftarrow 3n$ **until** $n > r/2$
return n

$\mathsf{IsNonzero}_k(\mathbf{x})$

$(x_0, x_1 \ldots, x_{k-1}) \leftarrow \mathbf{x}$
return $x_0 \vee x_1 \vee \cdots \vee x_{k-1}$

$\mathsf{IsMin}_{T,k}(\mathbf{x})$

$\mathbf{v}_0 \leftarrow \mathbf{x}$
for $i = 1$ to k **do**
  $\mathbf{v}_i \leftarrow T(\mathbf{v}_{i-1})$
  if $\mathbf{v}_i < \mathbf{v}_0$ **then return** 0
endfor
return 1

$\mathsf{IsInB6n}(\mathbf{x})$

$\mathbf{v}_{3n} \leftarrow L_2^{3n}(\mathbf{x})$
if $\mathbf{v}_{3n} = \mathbf{x}$ **then**
  return 0
else
  return 1
endif

$\mathsf{IsSol3n}(\mathbf{x}, f_0)$

$\mathbf{v}_0 \leftarrow \lceil \mathbf{x} \rceil_{2n}$ and $a_0 \leftarrow 0$
for $i = 1$ to $3n$ **do**
  $\mathbf{v}_i \leftarrow L_0(\mathbf{v}_{i-1})$
  $a_i \leftarrow a_{i-1} \vee f_0(\lceil \mathbf{v}_i \rceil_r)$
endfor
return a_{3n}

$\mathsf{Test}_{\Lambda_{3n,f_0}} : \mathbb{F}_2^{4n} \rightarrow \mathbb{F}_2$, the characteristic function of Λ_{3n,f_0}

return $\mathsf{IsNonzero}_{4n}(\mathbf{x}) \wedge \mathsf{IsMin}_{L_2,6n}(\mathbf{x}) \wedge (\neg \mathsf{IsInB6n}(\mathbf{x})) \wedge \mathsf{IsSol3n}(\mathbf{x}, f_0)$

$\mathsf{Test}_{\Lambda_{\overline{\mathfrak{C}}}} : \mathbb{F}_2^{4n} \rightarrow \mathbb{F}_2$, the characteristic function of $\Lambda_{\overline{\mathfrak{C}}}$

return $\mathsf{IsMin}_{L_2,6n}(\mathbf{x}) \wedge \mathsf{IsInB6n}(\mathbf{x}) \wedge \mathsf{IsInB6n}(\widehat{\mathbf{x}})$

$\mathsf{Test}_{\Lambda_{\mathfrak{D}}} : \mathbb{F}_2^{4n} \rightarrow \mathbb{F}_2$, the characteristic function of $\Lambda_{\mathfrak{D}}$

$\mathbf{v}_0 \leftarrow L_2^n(\mathbf{x})$
if $\mathsf{IsMin}_{L_2,6n}(\mathbf{v}_0) \wedge \mathsf{IsInB6n}(\mathbf{x}) \wedge (\neg \mathsf{IsInB6n}(\widehat{\mathbf{v}_0})) = 0$ **then return** 0
for $i = 1$ to $6n$ **do**
  $\mathbf{v}_i \leftarrow L_2(\mathbf{v}_{i-1})$
  if $\mathsf{IsInB6n}(\widehat{\mathbf{v}}_i) \wedge \mathsf{IsMin}_{L_2,6n}(\widehat{\mathbf{v}}_i) = 1$ **then return** 0
endfor
return 1

$\lambda : \mathbb{F}_2^{4n} \rightarrow \mathbb{F}_2$, the characteristic function of Λ_2

return $\mathsf{Test}_{\Lambda_{3n,f_0}}(\mathbf{x}) \vee \mathsf{Test}_{\Lambda_{\overline{\mathfrak{C}}}}(\mathbf{x}) \vee \mathsf{Test}_{\Lambda_{\mathfrak{D}}}(\mathbf{x})$

FIGURE 8: Subprocedures for Algorithm 2 and the logic of $\mathrm{FSR}(f)$.

Example 4 is tuned by the Boolean circuit f_0 (the input of the Karp-reduction), and then Λ_{p_0,f_0} includes their D-morphic pre-images generated by $\mathrm{LFSR}(p_0)$. If f_0 is unsatisfiable, $\mathrm{FSR}(f)$ is equivalent to $\mathrm{LFSR}(p_0) * \mathrm{FSR}_1(x_0)$. If $\mathrm{FSR}(f)$ is decomposable, a possible right $*$-factor of $\mathrm{FSR}(f)$ is a subFSR of $\mathrm{LFSR}(p_1)$ (by Proposition 2 and Corollary 4), which turns out to be either $\mathrm{LFSR}(p_0)$ or $\mathrm{FSR}_1(x_0)$ (by Theorem 6). If f_0 is satisfiable, Theorem 8 ensures that $\mathrm{LFSR}(p_0)$ is not a right $*$-factor of $\mathrm{FSR}(f)$, and Lemma 6 does not admit $\mathrm{FSR}_1(x_0)$ as a right $*$-factor of $\mathrm{FSR}(f)$ (detailed in the proof of Lemma 19). That is, f is

IsInB6n (x)

$v_{3n} \leftarrow L_2^{3n}(x)$
return $\text{IsNonzero}_{4n}(v_{3n} \oplus x)$

$\text{IsMin}_{T,l}(x)$

$v_0 \leftarrow x$
$a_0 \leftarrow 1$
for $i = 1$ to l do
    $v_i \leftarrow T(v_i - 1)$
    $a_i \leftarrow a_{i-1} \wedge \text{IsNonzero2}(1 - \text{Sign}(v_0 - v_i))$
  /v_i and v_0 are taken as integers and $\text{Sign}(v_0 - v_i)$ gives the sign of $v_0 - v_i$.
return a_l

$\text{Test}_{\Lambda_{\mathfrak{D}}} : \mathbb{F}_2^{4n} \to \mathbb{F}_2$, the characteristic function of $\Lambda_{\mathfrak{D}}$

$v_0 \leftarrow L_2^n(x)$
$w_0 = \text{IsMin}_{L_2,6n}(v_0) \wedge \text{IsInB6n}(x) \wedge (\neg \text{IsInB6n}(\widehat{v_0}))$
for $i = 1$ to $6n$ do
    $v_i \leftarrow L_2(v_i - 1)$
    $w_i = w_{i-1} \wedge (\neg(\text{IsInB6n}(\widehat{v_i}) \wedge \text{IsMin}_{L_2,6n}(\widehat{v_i})))$
endfor
return w_{6n}

FIGURE 9: Branchless interpretation of some subprocedures for λ.

indecomposable if and only if f_0 is satisfiable. Additionally, the transformation itself is polynomial-time computable (by Lemma 20). Below we give details of this proof.

In this section, for $\mathbf{v} \in \mathbb{F}_2^{2n+1}$, $\mathbf{Cycle}(\mathbf{v})$ denotes the unique cycle of $\text{LFSR}(p_1)$ containing $\mathbf{v}$.

For a Boolean logic $f_0 : \mathbb{F}_2^r \to \mathbb{F}_2$, $r < 2n$, we define a subset of $\mathbb{F}_2^{2n+1}$:

$$\Lambda_{p_0,f_0} = \left\{ \mathbf{v} \in \mathbb{F}_2^{2n+1} \;\middle|\; \begin{array}{c} [0] \neq \mathbf{Cycle}(\mathbf{v}) \in \text{LFSR}(p_0), \\ D(\mathbf{v}) = \min_{2n}(D(\mathbf{Cycle}(\mathbf{v}))), \\ \exists \mathbf{u} \in \mathbb{F}_2^{2n} \text{ in } D(\mathbf{Cycle}(\mathbf{v})),\ f_0(\lceil \mathbf{u} \rceil_r) = 1 \end{array} \right\}. \tag{54}$$

Theorem 12. *Λ_{p_0,f_0} is a potential set of* $\text{LFSR}(p_1)$.

Proof. As Statement (ii) of Lemma 9, the D-morphism is a permutation on $\text{LFSR}(p_0)$, and hence $D(\mathbf{Cycle}(\mathbf{v})) \in \text{LFSR}(p_0)$. Note that any cycle of $\text{LFSR}(p_0)$ has a unique minimal $2n$-bit vector. Thus, $\min_{2n}(D(\mathbf{Cycle}(\mathbf{v})))$ is well-defined and its D-morphic preimages are a pair of dual vectors. By Statement (i) of Lemma 9 and Theorem 4, as shown in Figure 4, one of the preimages occurs in a cycle of $\text{LFSR}(p_0)$, and the other in a cycle of $\text{FSR}(p_0{}^*)$. Thus, the preimage in a cycle of $\text{LFSR}(p_0)$ is uniquely determined. Therefore, each nonzero cycle of $\text{LFSR}(p_0)$ has at most one $(2n+1)$-bit vector in Λ_{p_0,f_0}, and any cycle of $\text{FSR}(p_0{}^*)$ has no vector in Λ_{p_0,f_0}.

By Definition 4, Equation (54) and Statement (iii) of Lemma 9, an arc in the associated graph $G_{p_1}^{\Lambda_{p_0,f_0}}$ always goes from a cycle in $\text{LFSR}(p_0)$ to a cycle in $\text{FSR}(p_0{}^*)$. Then $G_{p_1}^{\Lambda_{p_0,f_0}}$ is therefore acyclic.

In summary, Λ_{p_0,f_0} satisfies Statements (i) and (ii) of Definition 5 and is hence a potential set of $\text{LFSR}(p_1)$. □

We define a directed graph G as follows: the vertices of G are cycles of $\text{LFSR}(p_0)$, and an arc is incident from $\boldsymbol{c}_1$ to $\boldsymbol{c}_2$ if and only if $\boldsymbol{c}_1 \neq [0]$ is min-adjacent to $\boldsymbol{c}_2$ at $\min_{2n}(\boldsymbol{c}_1)$ and $\exists \mathbf{u} \in \mathbb{F}_2^{2n}$ in $\boldsymbol{c}_1$ such that $f_0(\lceil \mathbf{u} \rceil_r) = 1$.

Lemma 18. *G is a contraction graph of $G_{p_1}^{\Lambda_{p_0,f_0}}$, where for all $\beta \in \text{LFSR}(p_0)$, two vertices β and $\overline{\beta}$ of $G_{p_1}^{\Lambda_{p_0,f_0}}$ are identified as one vertex $D(\beta)$ in G.*

Proof. The pair of vertices β_l and $\overline{\beta_l}$ contract to $D(\beta_l)$ in G, $1 \leq l \leq (2^{2n} - 1)/(3n)$, and the pair of 1-cycles $[0]$ and $[1]$ contract to $[0]$.

On the one hand, the same as in the proof of Theorem 12, if an arc in $G_{p_1}^{\Lambda_{p_0,f_0}}$ goes from some cycle in $\{\beta_i, \overline{\beta_i}\}$ to some cycle in $\{\beta_j, \overline{\beta_j}\}$, then this arc is necessarily incident from β_i to $\overline{\beta_j}$. By Definition 4 and Equation (54), an arc in $G_{p_1}^{\Lambda_{p_0,f_0}}$ is incident from a nonzero cycle β_i to $\overline{\beta_j}$ if and only if there exists $\mathbf{v} \in \mathbb{F}_2^{2n+1}$ satisfying the following four statements: (i) $\mathbf{v} \neq \mathbf{0}^{2n+1}$ is $(2n+1)$-bit vector in β_i; (ii) $D(\mathbf{v})$ is the minimal $2n$-bit vector in $D(\beta_i)$; (iii) f_0 is evaluated 1 at an r-bit vector in $D(\beta_i)$; and (iv) $\widehat{\mathbf{v}}$ occurs in $\overline{\beta_j}$.

On the other hand, the vertices of G are $[0]$ and β_i's, $1 \leq i \leq (2^{2n} - 1)/(3n)$, and an arc in G is incident from the nonzero cycle $D(\beta_i)$ to $D(\beta_j)$ if and only if there exists $\mathbf{w} \in \mathbb{F}_2^{2n}$ satisfying the following three statements: (i) $\mathbf{w} \neq 0^{2n}$ is the minimal $2n$-bit vector in $D(\beta_i)$; (ii) f_0 is evaluated 1 at an r-bit vector in $D(\beta_i)$; and (iii) $\widehat{\mathbf{w}}$ occurs in $D(\beta_j)$.

Let $\mathbf{w} = D(\mathbf{v})$. Then $\widehat{\mathbf{w}} = D(\widehat{\mathbf{v}})$. Note that $\widehat{\mathbf{v}}$ is a $(2n+1)$-bit vector generated by $\text{FSR}(p_0{}^*)$ by Statement (iii) of Lemma 9. Considering $D(\beta_j) = D(\overline{\beta_j})$, we conclude that $\widehat{\mathbf{w}}$ is contained in $D(\beta_j)$ if and only if $\widehat{\mathbf{v}}$ is contained in $\overline{\beta_j}$. Therefore, the D-morphism determines a one–one correspondence between $\mathbf{v}$'s and $\mathbf{w}$'s as above.

Thus, an arc in $G_{p_1}^{\Lambda_{p_0,f_0}}$ is incident from some cycle in $\{\beta_i, \overline{\beta_i}\}$ to some cycle in $\{\beta_j, \overline{\beta_j}\}$ if and only if an arc in G is incident from the nonzero cycle $D(\beta_i)$ to $D(\beta_j)$. Therefore, G is a contraction of $G_{p_1}^{\Lambda_{p_0,f_0}}$. □

Lemma 19. *Let Λ_{p_0,f_0} be as in Equation (54) and λ its characteristic function. Let*

$$\begin{aligned} f(x_0, x_1, \ldots, x_{2n}) &= x_0 \oplus x_1 \oplus x_n \oplus x_{n+1} \oplus x_{2n} \\ &\oplus \lambda(x_0, x_1, \ldots, x_{2n}) \oplus \lambda(\overline{x_0}, x_1, \ldots, x_{2n}). \end{aligned} \tag{55}$$

Then $\text{FSR}_{2n+1}(f)$ is indecomposable if and only if the Boolean circuit f_0 is satisfiable.

$\lambda : \mathbb{F}_2^{2n+1} \to \mathbb{F}_2$, the characteristic function of Λ_{p_0,f_0}

return $\mathsf{IsNonzero}_{2n+1}(\mathbf{x}) \wedge (\neg(x_0 \oplus x_n \oplus x_{2n})) \wedge \mathsf{IsMin}_{L_0,3n}(D(\mathbf{x})) \wedge \mathsf{IsSol3n}(D(\mathbf{x}), f_0)$

FIGURE 10: A subprocedure for the logic of FSR(f) (IsNonzero, IsMin, and IsSol3n given in Figure 8).

Proof. By Theorem 12, Λ_{p_0,f_0} is a potential set of LFSR(p_1). By Theorem 8, FSR(f) is nonsingular.

Suppose f_0 to be unsatisfiable. Then Λ_{p_0,f_0} is empty as defined in (54), and hence the Boolean function λ is constant zero. In this case, FSR(f) is equivalent to LFSR(p_1) = LFSR(p_0)∗FSR$_1$(x_0) and is hence decomposable.

Now suppose f_0 to be satisfiable.

Since $r<2n$ and the nonzero cycles of LFSR(p_0) contain all r-bit vectors, there exists at least one nonzero cycle $\beta \in$ LFSR(p_0) such that $D(\beta)$ contains an r-bit vector $\mathbf{x}$ such that $f_0(\mathbf{x}) = 1$. Then the $(2n+1)$-bit vector $\mathbf{v}$ in β with its D-morphic image $D(\mathbf{v})$ minimal in $D(\beta)$ is a vector in Λ_{p_0,f_0}. Thus, Λ_{p_0,f_0} is not empty and $G_{p_1}^{\Lambda_{p_0,f_0}}$ has at least one arc.

Assume that FSR(f) is decomposable. Note that $\mathbf{0}^{2n+1} \notin \Lambda_{p_0,f_0}$ and then [0] is an isolated vertex in $G_{p_1}^{\Lambda_{p_0,f_0}}$, implying [0] ∈ FSR($f$) by Theorem 8. Then by Proposition 2, FSR(f) = FSR(g)∗FSR(h), where FSR(h) ⊂ FSR(f) and [0] ∈ FSR(h). By Corollary 4, FSR(h) is also a subFSR of LFSR(p_1). Thus, by Theorem 6, FSR(h) is either LFSR(p_0) or FSR$_1$(x_0). Anyhow, as shown above, $G_{p_1}^{\Lambda_{p_0,f_0}}$ has at least one arc, i.e., at least one nonzero cycle of LFSR(p_0) is not an isolated vertex in $G_{p_1}^{\Lambda_{p_0,f_0}}$. Then it follows from Theorem 8 that LFSR(p_0) is not a subFSR of FSR(f). Therefore, below we only have to consider FSR(h) = FSR$_1$(x_0), i.e., FSR(f) = FSR(g)∗FSR$_1$(x_0).

First, we claim that each odd cycle (i.e. any cycle in FSR($p_0{}^*$)) has indegree at most 1. Otherwise, suppose that $\overline{\beta_j}$ has indegree >1 in $G_{p_1}^{\Lambda_{p_0,f_0}}$. Let $\mathfrak{A} \subset$ LFSR(p_1) be the weakly connected component containing $\overline{\beta_j}$ and denote the set of the dual cycles $\overline{\mathfrak{A}} = \{\overline{\boldsymbol{c}} : \boldsymbol{c} \in \mathfrak{A}\}$. On the one hand, recall that each even cycle (i.e., any cycle in LFSR(p_0)) has outdegree ≤1 in $G_{p_1}^{\Lambda_{p_0,f_0}}$. Hence, even cycles outnumber odd cycles in $\mathfrak{A}$. On the other hand, by Theorem 4 and Corollary 2, since cycles in $\mathfrak{A}$ and those in $\overline{\mathfrak{A}}$ have the same D-morphic images, $\overline{\mathfrak{A}}$ is also a weakly connected component in $G_{p_1}^{\Lambda_{p_0,f_0}}$ and its cycles are joined into one cycle of FSR(f) since we have assumed FSR(f) = FSR(g)∗FSR$_1$(x_0). However, odd cycles outnumber even cycles in $\overline{\mathfrak{A}}$, and cycles in $\overline{\mathfrak{A}}$ are hence not weakly connected since each even cycle has outdegree at most 1, yielding contradiction. So, the claim is proved.

Second, we conclude that for any $1 \le k \le (2^{2n}-1)/(3n)$, β_k and $\overline{\beta_k}$ are in different weakly connected components. Otherwise, there is an undirected path connecting β_k with $\overline{\beta_k}$. In $G_{p_1}^{\Lambda_{p_0,f_0}}$, each cycle in LFSR($p_0$) has 0 indegree and at most 1 outdegree, and each cycle in FSR($p_0{}^*$) has 0 outdegree and at most 1 indegree as in the above claim. Thus, the only possible undirected path from β_k to $\overline{\beta_k}$ is an arc from β_k to $\overline{\beta_k}$. However, there exists no arc from β_k to $\overline{\beta_k}$. Otherwise, in the contraction graph G there is a self-loop of $D(\beta_k)$ (see Figure 4), contradictory to Lemma 6. So, by Theorem 8, there are no self-dual cycles in FSR(f).

Therefore, a weakly connected component in $G_{p_1}^{\Lambda_{p_0,f_0}}$ (as shown in Figure 4) is of the form $\{\beta_i, \overline{\beta_j}\}$ with an arc incident from β_i to $\overline{\beta_j}$, where β_i and β_j are distinct nonzero cycles of LFSR(p_0). Notice that,

$$\begin{aligned} &\left\{\mathbf{v} \in \mathbb{F}_2^n : \mathbf{v} \text{ in } D(\beta_i) \text{ or } D\left(\overline{\beta_j}\right)\right\} \\ &= \left\{\mathbf{v} \in \mathbb{F}_2^n : \mathbf{v} \text{ in } D\left(\overline{\beta_i}\right) \text{ or } D(\beta_j)\right\}. \end{aligned} \quad (56)$$

The same as above, because we assume FSR(f) = FSR(g)∗FSR$_1$(x_0), by Equation (56), Theorem 4 and Corollary 2, we conclude that β_j and $\overline{\beta_i}$ also join into one cycle of FSR(f), i.e., there is an arc from β_j to $\overline{\beta_i}$. Consider the contraction graph G. If so, in G, an arc goes from $D(\beta_i)$ to $D(\beta_j)$ and another from $D(\beta_j)$ to $D(\beta_i)$, implying that G is not acyclic, contradictory to Lemma 6.

Thus, our assumption does not hold and FSR(f) is indecomposable. □

Lemma 20. *There exists a polynomial-time algorithm for the transformation defined by Algorithm 3.*

Note that $\mathbf{x} = (x_0, x_1, \ldots, x_{2n})$ occurs in a cycle of LFSR(p_0) if and only if $x_0 \oplus x_n \oplus x_{2n} = 0$. Then Figure 10 presents the peudocode of the characteristic function of Λ_{p_0,f_0}. The proof of Lemma 20 is similar to that of Lemma 17, and we omit it here.

Proof of Theorem 2. By Theorem 3, Lemmas 19 and 20, Algorithm 3 gives a polynomial-time Karp-reduction from the **NP**-complete problem CIRCUIT SATISFIABILITY to FSR INDECOMPOSABILITY. Therefore, we conclude that FSR INDECOMPOSABILITY is **NP**-hard. □

6. Conclusion

Deciding irreducibility/indecomposability of FSRs is interesting for sophisticated circuit implementation and security analysis of stream ciphers. We studied both problems from the standing point of the worst-case computational complexity, and by now have proved that both the decision problems are **NP**-hard. Constructive examples are also given to show that there exist infinitely many irreducible (resp. indecomposable) FSRs that are decomposable (resp. reducible). We hope that this theoretical work serves as an inspiration to further explore the underlying obstacles to generally finding subFSRs or decomposing FSRs. To find subFSRs and ∗-factors of FSRs with no help of groundbreaking computing, it is therefore recommended to make good use of their specific feedback logics. Additionally, it is also interesting and challenging to study the average-case computational complexity of irreducibility and indecomposability of FSRs in future.

Data Availability

The data used to support the findings of this study are included within the article.

Disclosure

A preprint of this paper has previously been published [30]. Differing from the earlier version, this paper gives a new proof of Theorem 2 using the language of graph theory, and also shows that irreducible (resp. indecomposable) FSRs do not exclude decomposable (resp. reducible) FSRs.

Conflicts of Interest

The author declares that he has no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

The author would like to express sincere gratitude to Prof. Dr. Klaus Pommerening for his invaluable and encouraging suggestions to improve the manuscript. This work is supported by the National Key R&D Program of China (Grant No. 2021YFB3100200) and the National Natural Science Foundation of China (Grant No. 61502441).

References

[1] M. Robshaw and O. Billet, *New Stream Cipher Designs: The eSTREAM Finalists*, Springer-Verlag, Heidelberg, 2008.

[2] M. Hell, T. Johansson, A. Maximov, and W. Meier, “The grain family of stream ciphers,” in *New Stream Cipher Designs*, M. Robshaw and O. Billet, Eds., vol. 4986 of *Lecture Notes in Computer Science*, pp. 179–190, Springer, Berlin, Heidelberg, 2008.

[3] M. Hamann, M. Krause, and W. Meier, “Lizard—a lightweight stream cipher for power-constrained devices,” *IACR Transactions on Symmetric Cryptology*, vol. 2017, no. 1, pp. 45–79, 2017.

[4] D. H. Green and K. R. Dimond, “Nonlinear product-feedback shift registers,” in *Proceedings of the Institution of Electrical Engineers*, vol. 117, pp. 681–686, IET Digital Library, 1970.

[5] J. Mykkeltveit, M. K. Siu, and P. Tong, “On the cycle structure of some nonlinear shift register sequences,” *Information and Control*, vol. 43, no. 2, pp. 202–215, 1979.

[6] T. Tian, J. M. Zhang, C. D. Ye, and W. F. Qi, “A survey and new results on the decomposition of an nfsr into a cascade connection of two smaller nfsrs,” Cryptology ePrint Archive, Paper 2014/536, 2014.

[7] A. Klein, *Stream Ciphers*, Springer Publishing Company, Incorporated, 2013.

[8] B. Zhang, C. Xu, and W. Meier, “Fast near collision attack on the grain v1 stream cipher,” in *Advances in Cryptology—EUROCRYPT 2018*, J. B. Nielsen and V. Rijmen, Eds., pp. 771–802, Springer International Publishing, Cham, 2018.

[9] E. R. Berlekamp, *Algorithmic Coding Theory*, McGraw-Hill, New York, 1968.

[10] J. Massey, “Shift-register synthesis and BCH decoding,” *IEEE Transactions on Information Theory*, vol. 15, no. 1, pp. 122–127, 1969.

[11] E. Dubrova, “A transformation from the fibonacci to the galois NLFSRs,” *IEEE Transactions on Information Theory*, vol. 55, no. 11, pp. 5263–5271, 2009.

[12] Y. Jiang and D. Lin, “Lower and upper bounds on the density of irreducible NFSRs,” *IEEE Transactions on Information Theory*, vol. 64, no. 5, pp. 3944–3952, 2018.

[13] T. Tian and W.-F. Qi, “On the largest affine sub-families of a family of nfsr sequences,” *Designs, Codes and Cryptography*, vol. 71, no. 1, pp. 163–181, 2014.

[14] Y. Jiang and D. Lin, “On affine sub-families of grain-like structures,” *Designs, Codes and Cryptography*, vol. 82, no. 3, pp. 531–542, 2017.

[15] R. Lidl and H. Niederreiter, *Finite Fields*, Vol. 20, Cambridge Univ. Press, Cambridge, U.K, 1997.

[16] Z. Ma, W.-F. Qi, and T. Tian, “On the decomposition of an NFSR into the cascade connection of an NFSR into an LFSR,” *Journal of Complexity*, vol. 29, no. 2, pp. 173–181, 2013.

[17] J. Zhong and D. Lin, “Decomposition of nonlinear feedback shift registers based on Boolean networks,” *Science China Information Sciences*, vol. 62, no. 3, Article ID 39110, 2019.

[18] Z. Wang, X. Zhao, Q. Zheng, X. Feng, and Z. Sun, “The decomposition of an nfsr into the cascade connection of two smaller nfsrs revisited,” *Designs, Codes and Cryptography*, vol. 91, pp. 1889–1910, 2023.

[19] J. Zhong and D. Lin, “On equivalence of cascade connections of two nonlinear feedback shift registers,” *The Computer Journal*, vol. 62, no. 12, pp. 1793–1804, 2019.

[20] H. Hu and G. Gong, “Periods on two kinds of nonlinear feedback shift registers with time varying feedback functions,” *International Journal of Foundations of Computer Science*, vol. 22, pp. 1317–1329, 2011.

[21] J. Zhong and D. Lin, “On minimum period of nonlinear feedback shift registers in grain-like structure,” *IEEE Transactions on Information Theory*, vol. 64, no. 9, pp. 6429–6442, 2018.

[22] Y. Yang, X. Zeng, and Y. Xu, “Periods on the cascade connection of an LFSR and an NFSR,” *Chinese Journal of Electronics*, vol. 28, no. 2, pp. 301–308, 2019.

[23] Z. Wang, Q. Zheng, X. Zhao, and X. Feng, “Grain-like structures with minimal and maximal period sequences,” *Designs, Codes and Cryptography*, vol. 89, no. 4, pp. 679–693, 2021.

[24] Y. Jiang, “Weak grain-like structures,” *IEEE Transactions on Information Theory*, vol. 66, no. 12, pp. 7717–7723, 2020.

[25] S. Arora and B. Barak, *Computational Complexity: A Modern Approach*, Cambridge University Press, 2012.

[26] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, “Strengths and weaknesses of quantum computing,” *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1510–1523, 1997.

[27] S. W. Golomb, *Shift Register Sequences*, Aegean Park Press, Laguna Hills, CA, USA, 1981.

[28] Z. Wan, Z. Dai, M. Liu, and X. Feng, *Nonlinear Feedback Shift Registers*, Science Press, Beijing, 1978.

[29] A. Lempel, “On a homomorphism of the de bruijn graph and its applications to the design of feedback shift registers,” *IEEE Transactions on Computers*, vol. C-19, no. 12, pp. 1204–1209, 1970.

[30] L. Wang, “Deciding irreducibility/indecomposability of feedback shift registers is np-hard,” 1702.01423, 2017.