A family of invertible shift-invariant maps with strong arithmetic properties

Xiao-Xin Zhao, Deng Tang, and Zhong-Xiao Wang

Abstract

Shift-invariant maps have been employed to design nonlinear layers in many symmetric cryptographic schemes, such as the χ-map used in Keccak. In this paper, we study a family of shift-invariant maps on $\mathbb{F}_2^n$ which exhibit strong arithmetic properties with respect to the composition. The set of their defining functions, which we denote by $\Omega_{\underline{a}}$, is induced by a so-called "bifix-free" sequence $\underline{a} = (a_1, a_2, \ldots, a_m) \in \mathbb{F}_2^m$ with $2 \leq m < n$. It is shown that $\Omega_{\underline{a}}$ forms a commutative monoid with respect to the composition. If $m \nmid n$, then $\Omega_{\underline{a}}$ is isomorphic to the unit group of $\mathbb{F}_2[x]/(x^{\lceil \frac{n}{m} \rceil})$; if $m \mid n$, then the unit group of $\Omega_{\underline{a}}$ is isomorphic to that of $\mathbb{F}_2[x]/(x^{\frac{2n}{m}} + x^{\frac{n}{m}})$. The isomorphic relation transforms the composition of functions in $\Omega_{\underline{a}}$ into the multiplication of polynomials in the quotient ring of $\mathbb{F}_2[x]$, where the algebraic properties of the latter are well-understood. As a straightforward application, we focus on the algebraic properties of a particular class of functions in $\Omega_{\underline{a}}$, denoted by ρ_k for $k \geq 1$, which include the χ-map as well as several other known maps studied in earlier literature. It is shown that ρ_k is invertible if and only if $m \nmid n$. Also the inverse and the cycle structure of ρ_k (if invertible) can be fully characterized.

As different bifix-free sequences $\underline{a}$ typically induce different families of functions $\Omega_{\underline{a}}$ with pairwise trivial intersections, this work offers abundant parameter flexibility for designing invertible shift-invariant maps as well as deep insights into their algebraic properties.

Index Terms

Symmetric cryptography, Boolean function, Sequence, Shift-invariant map

I. Introduction

A shift-invariant map $F = (f_0, f_1, \ldots, f_{n-1}) : \mathbb{F}_2^n \to \mathbb{F}_2^n$ can be uniquely defined by a single n-variable Boolean function $f(X) : \mathbb{F}_2^n \to \mathbb{F}_2$ in the sense that $f_i(X) = f(\tau^i(X))$ for $0 \leq i \leq n-1$, where τ is the cyclic-shift operator on $\mathbb{F}_2^n$. Shift-invariant maps have been used to design nonlinear layers in many symmetric cryptographic schemes. In software, such maps enable bit-sliced implementations free of table-lookup operations; in hardware, their regularity enables low area per bit and minimal propagation latency. One of the most well-known shift-invariant maps used in practice is the χ-map, defined by $x_0+(x_1+1)x_2 : \mathbb{F}_2^n \to \mathbb{F}_2$, which is invertible if and only if n is odd. The χ-map was first introduced in Daemen's thesis [1] as an efficient nonlinear component, and then adopted in the design of numerous cryptographic algorithms, such as Keccak [2] (the permutation in SHA-3), Ascon [3] (the NIST standard for lightweight cryptography), Rasta [4], Xoodoo [5], and Subterranean 2.0 [6], where n varies across different schemes. Recall that in many cryptographic application scenarios, the lengths of both input and output of permutations are typically even. To meet this, some cryptographic algorithms adopt the cascade of two χ-maps as the permutations. For example, for ultra-low-latency decryption requirements, Belkheyar et al. [7] proposed ChiChi, a novel family of even-dimensional nonlinear layers which are extended affine equivalent to the cascade of two χ-maps. Then Andreoli et al. [8] subsequently extended ChiChi's design parameters to support nonlinear layers of arbitrary even dimensions. In addition, driven by the rapid development of technologies such as fully homomorphic encryption (FHE), secure multi-party computation (MPC), and zero-knowledge proofs (ZKP), numerous arithmetization-oriented symmetric primitives that minimize the number of field multiplications have been proposed over the past years, such as HadesMiMC [9], Poseidon [10], Neptune [11], [12], Monolith [13] and so on. The nonlinear layers adopted by these schemes include both the simple power map $x \mapsto x^d$ and shift-invariant maps. Focusing on the invertibility of quadratic shift-invariant maps on $\mathbb{F}_p^n$ with p odd, Grassi et al. [11] proved that the map defined by a quadratic 2-variable polynomial (resp. 3-variable polynomial) over $\mathbb{F}_p$ is non-invertible for every $n \geq 3$ (resp. $n \geq 5$). Then in [14], the non-invertible quadratic shift-invariant maps on $\mathbb{F}_p^n$, called bounded surjective maps, were further studied for applications in some FHE-friendly and MPC-friendly schemes.

Although more than three decades have passed since the χ-map was proposed, research on it has never ceased. Particularly in recent years, algebraic properties of χ and its variants have gained growing attention. In [15], Liu et al. presented a compact formula for the inverse of χ. By exploiting the structural properties of χ^{-1}, they performed algebraic analysis on Rasta-type algorithms through constructing low-degree equations in terms of the key. Then in [16], Liu et al. further refined the idea of formulating χ^{-1}, and generalized it for finding the inverses of some other invertible shift-invariant maps proposed in Daemen's

This work was supported by the National Natural Science Foundation of China (Grant 62572305, 12371526, and 62202494), and the National Key Research and Development Project of China (Grant 2025YFA1017202 and 2024YFB4504700)

Xiao-Xin Zhao and Zhong-Xiao Wang are with Information Engineering University, Zhengzhou 450000, China. Xiao-Xin Zhao and Deng Tang are with Shanghai Jiao Tong University, Shanghai 201100, China. Xiao-Xin Zhao is with Key Laboratory of Cyberspace Security Defense, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100085, China. (e-mail: zhaoxiaoxin46@126.com; dtang@foxmail.com; zhongxiao_wang@126.com)

thesis, whose algebraic expressions are of the form analogous to χ. In [17] and [18], Schoone and Daemen studied the algebraic properties of χ from two aspects: the univariate representation and the state diagram. They introduced an innovative approach to characterizing the action of χ on $\mathbb{F}_2^n$ via multiplication over a specific quotient ring. This approach provides a new proof of the invertibility of χ, as well as a characterization of its cycle structure. In [19], Graner et al. addressed the conjecture in [17], proving that the defining function of χ over finite fields, i.e., $x_0+(x_1+1)x_2 : \mathbb{F}_q^n \to \mathbb{F}_q$, is invertible if and only if $q = 2$ and n is odd. In [20], Kriepke and Kyureghyan studied χ from a new perspective. It was found that the iteration of χ admits a linear representation with respect to a family of specific vectorial Boolean functions. Based on this, they extended χ to generalized χ-maps, and proved that if n is odd, then such maps form an abelian group isomorphic to the unit group of $\mathbb{F}_2[x]/(x^{\frac{n+1}{2}})$; if n is even, then the invertible ones of such maps form an abelian group isomorphic to the unit group of $\mathbb{F}_2[x]/(x^n + x^{\frac{n}{2}})$ [21]. This transformed the study of χ into the study of a specific polynomial in a quotient ring of $\mathbb{F}_2[x]$, making it clear to understand the algebraic properties of χ, including the calculations of its inverse and order. Recently, based on the idea in [20], Lyu et al. [22] studied a variant of χ, written as $\chi_{n,m}$, which is defined by $x_0+(x_1+1)(x_2+1)\cdots(x_{m-1}+1)x_m : \mathbb{F}_2^n \to \mathbb{F}_2$, where $m < n, m \nmid n$. They extended $\chi_{n,m}$ to a family of maps, which form an abelian group isomorphic to the unit group of $\mathbb{F}_2[x]/(x^{\lceil \frac{n}{m} \rceil})$.

A common feature of previous works [20], [21], [22] is that the families of maps studied therein exhibit favorable arithmetic properties, in the sense that the composition of such maps corresponds to the multiplication of polynomials in a specific quotient ring of $\mathbb{F}_2[x]$, which facilitates a clear analysis of their algebraic properties. This raises some natural questions: are there other families of maps enjoying analogous properties, and what connections exist between these families? These serve as the original motivation of our work.

In this paper, we propose and study a family of shift-invariant maps on $\mathbb{F}_2^n$, whose defining functions are induced by a so-called "bifix-free" sequence $\underline{a} = (a_1, a_2, \ldots, a_m) \in \mathbb{F}_2^m$ with $2 \le m < n$. Recall that $\underline{a}$ is called bifix-free if its k-length prefix differs from its k-length suffix for any $0 < k < m$, see [23]. Let $\Omega_{\underline{a}}$ be the set of defining functions of our proposed shift-invariant maps. The construction of $\Omega_{\underline{a}}$ relies on a sequence of n-variable Boolean functions $\theta_1, \theta_2, \ldots$ induced by $\underline{a}$ (see (4) for the definition). Specifically, $\Omega_{\underline{a}} = x_0 + \langle \theta_1, \theta_2, \ldots \rangle$, where $\langle \theta_1, \theta_2, \ldots \rangle$ is the linear span of $\theta_1, \theta_2, \ldots$ over $\mathbb{F}_2$. It can be seen that if $\underline{a} = (0, 1)$ (resp. $\underline{a} = (0, 0, \ldots, 0, 1) \in \mathbb{F}_2^m$), then $\Omega_{\underline{a}}$ is exactly the set of defining functions of the family of shift-invariant maps studied in [20], [21] (resp. [22]). It is shown that $\Omega_{\underline{a}}$ forms a commutative monoid with respect to the composition. If $m \nmid n$, then $\Omega_{\underline{a}}$ is isomorphic to the unit group of $\mathbb{F}_2[x]/(x^{\lceil \frac{n}{m} \rceil})$; if $m \mid n$, then the unit group of $\Omega_{\underline{a}}$ is isomorphic to that of $\mathbb{F}_2[x]/(x^{\frac{2n}{m}} + x^{\frac{n}{m}})$. Such isomorphism transforms the composition of functions in $\Omega_{\underline{a}}$ into the multiplication of polynomials in the quotient ring of $\mathbb{F}_2[x]$, which allows many algebraic properties of functions in $\Omega_{\underline{a}}$ to be read directly from the quotient-ring multiplication. Moreover, it is also shown that such isomorphism is not valid if $\underline{a}$ is not bifix-free for $n \ge 2m$. As a straightforward application, we study the algebraic properties of $\rho_k = x_0 + \theta_k \in \Omega_{\underline{a}}$ for $k \ge 1$, which includes the defining functions of χ, $\chi_{n,m}$, and several other functions proposed in Daemen's thesis [1, Table A.1]. It is shown that ρ_k is invertible if and only if $m \nmid n$. Also its inverse as well as its cycle structure can be fully characterized. In particular, a compact formula for the inverse of the nonlinear layer of a hash function called Monolith [13] is presented via the derived results.

Different bifix-free sequences $\underline{a}$ typically induce different families of functions $\Omega_{\underline{a}}$ with pairwise trivial intersections. Since bifix-free sequences exist in vast quantities, the number of invertible functions derived from $\Omega_{\underline{a}}$ via different $\underline{a}$ is enormous. As a result, our proposed construction provides a large structured parameter space for designing invertible shift-invariant maps, together with an explicit algebraic framework for analyzing them.

This paper is organized as follows. Section II introduces the basic definitions and notation that will be used throughout the paper. Section III studies the arithmetic properties of $\Omega_{\underline{a}}$ with respect to the composition and establishes the connection between $\Omega_{\underline{a}}$ and the quotient ring of $\mathbb{F}_2[x]$. Section IV characterizes the algebraic properties of ρ_k including the invertibility and the cycle structure. Section V reveals the inherent relation between $\Omega_{\underline{a}}$ and $\Omega_{\underline{a}'}$, and demonstrates the necessity of the precondition "bifix-free". Finally, conclusions are drawn in Section VI.

II. Preliminaries

In this section, we briefly review the basic definitions and notation that will be used throughout the paper.

Let n be a positive integer. An n-variable Boolean function $f(x_0, x_1, \ldots, x_{n-1})$ is a map from the n-dimension vector space $\mathbb{F}_2^n$ to the finite field $\mathbb{F}_2$. The set of all n-variable Boolean functions is denoted by $\mathcal{B}_n$. It is known that $f(x_0, x_1, \ldots, x_{n-1})$ can be uniquely expressed in the Algebraic Normal Form (ANF), i.e.,

$$f(x_0, x_1, \ldots, x_{n-1}) = \bigoplus_{I \subseteq \{0,1,\ldots,n-1\}} c_I \cdot \prod_{i \in I} x_i, \ \ c_I \in \mathbb{F}_2.$$

The product of the form $\prod_{i \in I} x_i$ is called a term of f if $c_I \neq 0$. The algebraic degree of nonzero f is the global degree of the ANF of f, defined as $\deg(f) = \max\{\#I \mid c_I \neq 0\}$. If f has no constant term and $\deg(f) = 1$, then f is called linear.

Definition 1: A map $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called shift-invariant if it is commutative with the cyclic-shift operator τ on $\mathbb{F}_2^n$, i.e., $\tau F = F\tau$, where $\tau : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is defined by

$$(x_0, x_1, \ldots, x_{n-1}) \mapsto (x_1, x_2, \ldots, x_{n-1}, x_0).$$

For $i \geq 0$, the i-th iterate of τ is expressed as $\tau^i : \mathbb{F}_2^n \to \mathbb{F}_2^n$,

$$(x_0, x_1, \ldots, x_{n-1}) \mapsto (x_i, x_{1+i}, \ldots, x_{n-1+i}),$$

where the variable indices are taken modulo n.

Let $F = (f_0, f_1, \ldots, f_{n-1}) : \mathbb{F}_2^n \to \mathbb{F}_2^n$ where $f_i \in \mathcal{B}_n$ for $0 \leq i \leq n-1$. By Definition 1, it is not hard to see that if F is shift-invariant, then each f_i can be represented by f_0 in the sense that

$$f_i = f_0(\tau^i(x_0, x_1, \ldots, x_{n-1})), 0 \leq i \leq n-1,$$

which is abbreviated to $\tau^i(f_0)$ for notational simplicity in the following paper. Since F can be uniquely expressed by a single n-variable Boolean function f_0, we say that F is defined by f_0, and denote such F by F_{f_0}.

Let F_f, F_g be two shift-invariant maps on $\mathbb{F}_2^n$ defined by $f, g \in \mathcal{B}_n$, respectively. Then it is not hard to see that their composition is still a shift-invariant map on $\mathbb{F}_2^n$. To describe its defining function, we introduce a binary operation "$\circ$" on $\mathcal{B}_n$, defined by

$$f \circ g = f(g, \tau(g), \ldots, \tau^{n-1}(g)) \in \mathcal{B}_n.$$

It can be seen that

$$F_f(F_g(X)) = F_{f \circ g}(X), \tag{1}$$

namely, the composition of two shift-invariant maps is equivalent to the $\circ$-product of their defining functions. Since $f \cdot f = f$, we write f^k to denote the k-th iterate of f under the $\circ$-product when no confusion arises. Note that the $\circ$-product is not commutative, i.e., $f \circ g \neq g \circ f$ in general. For instance, consider $f = x_0x_1 + x_2, g = x_0 + x_1 + x_2 \in \mathcal{B}_3$. It can be seen that $f \circ g = 0, g \circ f = x_0x_1x_2 + x_0x_1 + x_0x_2 + x_1x_2 + x_0 + x_1 + x_2, f \circ f = x_0x_1 + x_1x_2 + x_1, g \circ g = g$. Moreover, the $\circ$-product meets the associative law, and the left distributive law with respect to both the addition and the multiplication of Boolean functions, shown below.

Proposition 1: Let $f, g, h \in \mathcal{B}_n, i \geq 0$. Then

(i) $(f \circ g) \circ h = f \circ (g \circ h)$;
(ii) $(f + g) \circ h = f \circ h + g \circ h$;
(iii) $(f \cdot g) \circ h = (f \circ h) \cdot (g \circ h)$;
(iv) $\tau^i(f) = x_i \circ f = f \circ x_i$;
(v) $\tau^i(f \circ g) = \tau^i(f) \circ g = f \circ \tau^i(g)$.

It can be seen that $\mathcal{B}_n$ forms a finite monoid with respect to $\circ$, whose identity element is x_0. If $f, g \in \mathcal{B}_n$ satisfy $f \circ g = g \circ f = x_0$, then **we say that f, g are invertible**. The collection of all invertible functions in $\mathcal{B}_n$ forms a finite group with respect to $\circ$. In general, it is difficult to identify the invertibility of a given $f \in \mathcal{B}_n$, except for linear cases.

Let π be a one-to-one correspondence between n-variable linear Boolean functions and polynomials over $\mathbb{F}_2$ with degrees less than n, defined by

$$\pi(f) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1} \in \mathbb{F}_2[x],$$

where $f = c_0x_0 + c_1x_1 + \cdots + c_{n-1}x_{n-1} \in \mathcal{B}_n$. Moreover, $\pi(0)$ is defined to be 0 as an extension. It can be seen that

$$\pi(f \circ g) \equiv \pi(f) \cdot \pi(g) \mod x^n + 1 \tag{2}$$

for linear $f, g \in \mathcal{B}_n$. In other words, the $\circ$-product of n-variable linear Boolean functions can be treated as the multiplication of polynomials in $\mathbb{F}_2[x]/(x^n + 1)$. It follows that f is invertible if and only if $\gcd(\pi(f), x^n + 1) = 1$, whose inverse (if invertible) can be formulated by the extended Euclidean algorithm. This idea has been shown in [1, Proposition 6.2].

In fact, there are families of nonlinear Boolean functions which exhibit linear properties similar to (2) under the $\circ$-product. In [20], Kriepke and Kyureghyan proposed generalized χ-maps on $\mathbb{F}_2^n$. It is remarkable that the composition of such maps can be treated as the multiplication on $\mathbb{F}_2[x]/(x^{\frac{n+1}{2}})$ if n is odd, and on $\mathbb{F}_2[x]/(x^n + x^{\frac{n}{2}})$ if n is even [21], respectively. Then in [22], Lyu et al. further extended this work by considering a family of maps whose composition can be treated as the multiplication on $\mathbb{F}_2[x]/(x^{\lceil \frac{n}{m} \rceil})$. Inspired by previous works, we propose and study families of functions in a more general form, the $\circ$-product on which corresponds to the multiplication on the quotient ring of $\mathbb{F}_2[x]$. The construction is based on the so-called "bifix-free" sequences, specified as follows.

Let $\underline{a} = (a_1, a_2, \ldots, a_m)$ be a binary sequence of length $m \geq 2$. If there is an integer $0 < T < m$ such that $a_i = a_{i+T}$ for $1 \leq i \leq m - T$, then T is called a period of $\underline{a}$. In particular, m is naturally viewed as a period of $\underline{a}$. We say that $\underline{a}$ is bifix-free if its least period is exactly m. A bifix-free sequence of length m should satisfy that for any $0 < k < m$, its k-length prefix differs from its k-length suffix. For instance, it can be seen that $(0, 0, 1)$, $(1, 1, 0, 0)$, and $(1, 1, 0, 1, 0)$ are bifix-free, whereas $(0, 1, 0)$, $(0, 1, 0, 1)$, and $(1, 1, 0, 1, 1)$ are not. The study of bifix-free sequences can be traced back to the work in [23], where a systematic way of generating all such sequences and a recursive way to determine their number were presented.

Theorem 1: [23, Theorem 1] Let u_m be the number of binary bifix-free sequences of length $m \geq 1$. Then

$$u_m = \begin{cases} 2u_{m-1} - u_{\frac{m}{2}} & \text{if } m \text{ is even,} \\ 2u_{m-1} & \text{otherwise,} \end{cases}$$

where $u_0 = 1$. Moreover, let $v_m = \frac{u_m}{2^m}$. Then the sequence $(v_m)_{m\geq 1}$ is monotonically nonincreasing, which converges to a constant v_∞ with $v_\infty \geq \frac{1}{4}$.

Remark 1: In [23, Table II], it is shown that $v_\infty \approx 0.267786$. In other words, among all binary sequences of length m, the proportion of bifix-free ones is roughly $\frac{1}{4}$ when m is large enough.

Let $\underline{a} = (a_1, a_2, \ldots, a_m) \in \mathbb{F}_2^m$ be bifix-free with $2 \leq m < n$. Let

$$\lambda = x_1^{a_1} x_2^{a_2} \cdots x_{m-1}^{a_{m-1}} \in \mathcal{B}_n, \tag{3}$$

where $x_i^{a_i} = x_i + a_i + 1$ for $1 \leq i \leq m-1$. For $k \geq 1$, let

$$\theta_k = x_{km}^{a_m} \prod_{0\leq i\leq k-1} \tau^{im}(\lambda), \tag{4}$$

where the variable indices are taken modulo n, and so θ_k can be treated as a function in $\mathcal{B}_n$. In particular, $\theta_1 = \lambda x_m^{a_m} = x_1^{a_1} x_2^{a_2} \cdots x_m^{a_m}$. It can be seen that θ_k satisfies the recursion relation

$$\theta_{k+1} = \lambda \cdot \tau^m(\theta_k), k \geq 1. \tag{5}$$

Since $\mathcal{B}_n$ is finite, so is $\{\theta_1, \theta_2, \ldots\}$. In this paper, we fix n and study a family of n-variable Boolean functions given by

$$\Omega_{\underline{a}} = x_0 + \langle \theta_1, \theta_2, \ldots \rangle,$$

where $\langle \theta_1, \theta_2, \ldots \rangle$ is the linear span of $\theta_1, \theta_2, \ldots$ over $\mathbb{F}_2$. It can be seen that $x_0 \notin \langle \theta_1, \theta_2, \ldots \rangle$, and $\Omega_{\underline{a}}$ is exactly the coset of $\langle \theta_1, \theta_2, \ldots \rangle$ containing x_0. Recall that x_0 is the identity element in the monoid $\langle \mathcal{B}_n, \circ \rangle$. The choice of the coset containing x_0 is not merely notational: it is the setting in which one can hope for a closed arithmetic structure under the $\circ$-product.

Remark 2: It can be seen that if $\underline{a} = (0, 1)$, then $\Omega_{\underline{a}}$ is exactly the set of defining functions of the family of shift-invariant maps studied in [20], [21], where it is denoted by G and G_n, respectively. If $\underline{a} = (0, 0, \ldots, 0, 1) \in \mathbb{F}_2^m$, then $\Omega_{\underline{a}}$ is exactly the set of defining functions of the family of shift-invariant maps studied in [22], where it is denoted by $G_{n,m}$.

III. Main results

This section is divided into three parts. Subsection III-A characterizes the periodicity of $(\theta_k)_{k\geq 1}$ for $m \nmid n$ and $m \mid n$, respectively, which further clarify the representation of $\Omega_{\underline{a}}$. Subsection III-B reveals the closure of $\Omega_{\underline{a}}$ under the $\circ$-product, showing that $\Omega_{\underline{a}}$ forms a commutative monoid. Based on the first two parts, Subsection III-C establishes a connection between the $\circ$-product on $\Omega_{\underline{a}}$ and the multiplication on the quotient ring of $\mathbb{F}_2[x]$. It is shown that if $m \nmid n$, then $\Omega_{\underline{a}}$ is isomorphic to the unit group of $\mathbb{F}_2[x]/(x^{\lceil \frac{n}{m} \rceil})$; if $m \mid n$, then the unit group of $\Omega_{\underline{a}}$ is isomorphic to that of $\mathbb{F}_2[x]/(x^{\frac{2n}{m}} + x^{\frac{n}{m}})$.

In the following paper, for $f, g \in \mathcal{B}_n$, we say that g divides f, written as $g \mid f$, if there is $h \in \mathcal{B}_n$ such that $f = g \cdot h$. Furthermore, if there is another $g' \in \mathcal{B}_n$ such that $g' \mid f$, then $g \cdot g' \mid f$. In particular, if $0 \mid f$, then $f = 0$.

A. The periodicity of $(\theta_k)_{k\geq 1}$

Recall that an infinite sequence $\underline{s} = (s_i)_{i\geq 1}$ is called ultimately periodic if there exist integers $r, t \geq 1$ such that $s_{i+r} = s_i$ for each $i \geq t$. The least such t is called the preperiod of $\underline{s}$, and r is called a period of $\underline{s}$. It can be seen from (5) that $(\theta_k)_{k\geq 1}$ is ultimately periodic, whose periodicity is shown below.

Lemma 1: Let $m \nmid n$. Then $\theta_k = 0$ if and only if $k \geq \lceil \frac{n}{m} \rceil$.

Proof: Assume that $k < \lceil \frac{n}{m} \rceil$. It can be observed that the largest variable index of θ_k is km, which is less than n. This implies that θ_k can not be zero, a contradiction.

Conversely, by the recursion relation in (5), to prove the sufficiency, it suffices to show that $\theta_k = 0$ for $k = \lceil \frac{n}{m} \rceil$. Write $km = n + r$. Then $0 < r < m$. On the one hand, it can be seen that

$$(x_1, x_2, \ldots, x_r) = (x_{1+km-r}, x_{2+km-r}, \ldots, x_{km}),$$

where the variable indices are taken modulo n. On the other hand, since $\underline{a}$ is bifix-free, we have

$$(a_1, a_2, \ldots, a_r) \neq (a_{1+m-r}, a_{2+m-r}, \ldots, a_m),$$

i.e., there is $1 \leq i \leq r$ such that $a_i \neq a_{i+m-r}$. If $i < r$, then it can be seen from (3) that $x_i^{a_i} \mid \lambda$ and $x_{i+km-r}^{a_{i+m-r}} \mid \tau^{(k-1)m}(\lambda)$. Since $\lambda \cdot \tau^{(k-1)m}(\lambda) \mid \theta_k$ by (4), it follows from $x_i^{a_i} x_{i+km-r}^{a_{i+m-r}} = 0$ that $\theta_k = 0$. If $i = r$, then it follows that $\theta_k = 0$ as well since both $x_r^{a_r}, x_{km}^{a_m}$ divide θ_k and $x_r^{a_r} x_{km}^{a_m} = 0$.

■

Lemma 2: Let $m \mid n$. Then

(i) for $1 \le k < \frac{n}{m}$, there is no $k' > k$ such that $\theta_{k'} = \theta_k$;

(ii) for $k \ge \frac{n}{m}$, we have $\theta_{k+\frac{n}{m}} = \theta_k$, and $\frac{n}{m}$ is the least positive integer for which this equality holds.

Proof: Let $t = \frac{n}{m} > 1$. Note first that $\tau^{im}(\lambda) = \tau^{jm}(\lambda) \Leftrightarrow im \equiv jm \mod n \Leftrightarrow i \equiv j \mod t$. It can be seen from

$$\begin{aligned}
\theta_1 &= \lambda \cdot x_m^{a_m} \\
\theta_2 &= \lambda \cdot \tau^m(\lambda) \cdot x_{2m}^{a_m} \\
&\vdots \\
\theta_t &= \lambda \cdot \tau^m(\lambda) \cdots \tau^{(t-1)m}(\lambda) \cdot x_{tm}^{a_m}
\end{aligned}$$

that $\theta_1, \theta_2, \ldots, \theta_t$ are pairwise distinct. Then for $k \ge t$, we have

$$\begin{aligned}
\theta_k &= \lambda \cdot \tau^m(\lambda) \cdots \tau^{(k-1)m}(\lambda) \cdot x_{km}^{a_m} \\
&= \lambda \cdot \tau^m(\lambda) \cdots \tau^{(t-1)m}(\lambda) \cdot x_{km}^{a_m}.
\end{aligned} \tag{6}$$

In (6), the variable indices of $\lambda \cdot \tau^m(\lambda) \cdots \tau^{(t-1)m}(\lambda)$ are all non-zero modulo m, except for $x_{km}^{a_m}$. Thus for $k \ge t$ and positive integer l, it can be seen from (6) that $\theta_{k+l} = \theta_k \Leftrightarrow x_{km+lm}^{a_m} = x_{km}^{a_m} \Leftrightarrow lm \equiv 0 \mod n$. Finally the desired results follow. ■

Denote $\bar{*} = * + 1$ for $* \in \mathbb{F}_2$. A toy example is given for Lemmas 1 and 2.

Example 1: Let $\underline{a} = (0, 1, 1)$. When $n = 7$, it can be seen that $\theta_1 = \bar{x}_1 x_2 x_3, \theta_2 = \bar{x}_1 x_2 \bar{x}_4 x_5 x_6, \theta_3 = 0, \theta_4 = 0, \ldots$ When $n = 6$, it can be seen that $\theta_1 = \bar{x}_1 x_2 x_3, \theta_2 = \bar{x}_1 x_2 \bar{x}_4 x_5 x_0, \theta_3 = \bar{x}_1 x_2 \bar{x}_4 x_5 x_3$, and $\theta_{k+2} = \theta_k$ for $k \ge 2$.

When $m \nmid n$, it follows from Lemma 1 that the preperiod and the least period of $(\theta_k)_{k \ge 1}$ are $\lceil \frac{n}{m} \rceil$ and 1, respectively. For $1 \le k \le \lfloor \frac{n}{m} \rfloor$, it can be seen from (4) that θ_k has only one highest-degree term,

$$x_{km} \prod_{0 \le i \le k-1} x_{1+im} x_{2+im} \cdots x_{m-1+im}, \tag{7}$$

and so $\deg(\theta_k) = k(m-1) + 1$. It follows that

$$\deg(\theta_1) < \deg(\theta_2) < \cdots < \deg(\theta_{\lfloor \frac{n}{m} \rfloor}). \tag{8}$$

Since $\theta_1, \theta_2, \ldots, \theta_{\lfloor \frac{n}{m} \rfloor}$ have pairwise different algebraic degrees, it implies that they are linearly independent over $\mathbb{F}_2$. Thus in this case, we have

$$\Omega_{\underline{a}} = x_0 + \langle \theta_1, \theta_2, \ldots, \theta_{\lfloor \frac{n}{m} \rfloor} \rangle.$$

When $m \mid n$, it follows from Lemma 2 that the preperiod and the least period of $(\theta_k)_{k \ge 1}$ are both $\frac{n}{m}$. For $1 \le k \le \frac{n}{m}$, θ_k has only one highest-degree term as shown in (7), and so $\deg(\theta_k) = k(m-1)+1$. For $k \ge \frac{n}{m}$, θ_k has only one highest-degree term

$$x_{km} \prod_{0 \le i \le \frac{n}{m}-1} x_{1+im} x_{2+im} \cdots x_{m-1+im}, \tag{9}$$

and so $\deg(\theta_k) = \frac{n}{m}(m-1) + 1$. It can be seen that

$$\deg(\theta_1) < \cdots < \deg(\theta_{\frac{n}{m}}) = \deg(\theta_{\frac{n}{m}+1}) = \cdots = \deg(\theta_{\frac{2n}{m}-1}), \tag{10}$$

and $\theta_{\frac{n}{m}}, \theta_{\frac{n}{m}+1}, \ldots, \theta_{\frac{2n}{m}-1}$ have pairwise different highest-degree terms. This implies that $\theta_1, \theta_2, \ldots, \theta_{\frac{2n}{m}-1}$ are linearly independent over $\mathbb{F}_2$. Thus in this case, we have

$$\Omega_{\underline{a}} = x_0 + \langle \theta_1, \theta_2, \ldots, \theta_{\frac{2n}{m}-1} \rangle.$$

B. The closure of $\Omega_{\underline{a}}$ under the $\circ$-product

In this subsection, we show that $\Omega_{\underline{a}}$ is closed under the $\circ$-product with the help of the following auxiliary Lemmas.

Lemma 3: For $1 \le i < j \le m$ and $k, k' \ge 1$,

$$\tau^i(\theta_k) \cdot \tau^j(\theta_{k'}) = 0.$$

Proof: Let $s = j - i$. Then $0 < s < m$. We discuss the following two cases.

Case 1: when $k \le k'$, it can be seen from (4) that $\tau^{(k-1)m+i}(\lambda) x_{km+i}^{a_m} \mid \tau^i(\theta_k)$, where

$$\tau^{(k-1)m+i}(\lambda) x_{km+i}^{a_m} = x_{1+(k-1)m+i}^{a_1} x_{2+(k-1)m+i}^{a_2} \cdots x_{m-1+(k-1)m+i}^{a_{m-1}} x_{km+i}^{a_m}. \tag{11}$$

On the other hand, since $k \leq k'$, it can be seen that $\tau^{(k-1)m+i+s}(\lambda) \mid \tau^{i+s}(\theta_{k'})$, where

$$\tau^{(k-1)m+i+s}(\lambda) = x_{1+(k-1)m+i+s}^{a_1} x_{2+(k-1)m+i+s}^{a_2} \cdots x_{m-1+(k-1)m+i+s}^{a_{m-1}}. \tag{12}$$

Since $\underline{a}$ is bifix-free, we have

$$(a_1, a_2, \ldots, a_{m-s}) \neq (a_{1+s}, a_{2+s}, \ldots, a_m),$$

i.e., there is $1 \leq t \leq m-s$ such that $a_t \neq a_{t+s}$. It can be seen from (12) that $x_{t+(k-1)m+i+s}^{a_t} \mid \tau^{(k-1)m+i+s}(\lambda)$, and from (11) that $x_{t+s+(k-1)m+i}^{a_{t+s}} \mid \tau^{(k-1)m+i}(\lambda) x_{km+i}^{a_m}$. Since $x_{t+(k-1)m+i+s}^{a_t} x_{t+s+(k-1)m+i}^{a_{t+s}} = 0$, it follows that $\tau^i(\theta_k) \cdot \tau^{i+s}(\theta_{k'}) = 0$.

Case 2: when $k > k'$, it can be seen from (4) that $\tau^{k'm+i}(\lambda) \mid \tau^i(\theta_k)$, where

$$\tau^{k'm+i}(\lambda) = x_{1+k'm+i}^{a_1} x_{2+k'm+i}^{a_2} \cdots x_{m-1+k'm+i}^{a_{m-1}}. \tag{13}$$

On the other hand, it can be seen that $\tau^{(k'-1)m+i+s}(\lambda) x_{k'm+i+s}^{a_m} \mid \tau^{i+s}(\theta_{k'})$, where

$$\tau^{(k'-1)m+i+s}(\lambda) x_{k'm+i+s}^{a_m} = x_{1+(k'-1)m+i+s}^{a_1} x_{2+(k'-1)m+i+s}^{a_2} \cdots x_{m-1+(k'-1)m+i+s}^{a_{m-1}} x_{k'm+i+s}^{a_m}. \tag{14}$$

Similarly, since $\underline{a}$ is bifix-free, we have

$$(a_1, a_2, \ldots, a_s) \neq (a_{1+m-s}, a_{2+m-s}, \ldots, a_m),$$

i.e., there is $1 \leq t' \leq s$ such that $a_{t'} \neq a_{t'+m-s}$. It can be seen from (13) that $x_{t'+k'm+i}^{a_{t'}} \mid \tau^{k'm+i}(\lambda)$, and from (14) that $x_{t'+m-s+(k'-1)m+i+s}^{a_{t'+m-s}} \mid \tau^{(k'-1)m+i+s}(\lambda) x_{k'm+i+s}^{a_m}$. Since $x_{t'+k'm+i}^{a_{t'}} x_{t'+m-s+(k'-1)m+i+s}^{a_{t'+m-s}} = 0$, it follows that $\tau^i(\theta_k) \cdot \tau^{i+s}(\theta_{k'}) = 0$. ■

Lemma 4: Let $f = x_0 + \sum_{1 \leq i \leq s} c_i \theta_i \in \Omega_{\underline{a}}$, where $c_i \in \mathbb{F}_2, s \geq 1$. Then

$$\lambda \circ f = \lambda + \sum_{1 \leq j \leq m-1} \frac{x_1^{a_1} x_2^{a_2} \cdots x_{m-1}^{a_{m-1}}}{x_j^{a_j}} \sum_{1 \leq i \leq s} c_i \tau^j(\theta_i).$$

Proof: Let us write

$$\begin{aligned}
\lambda \circ f &= (x_1^{a_1} x_2^{a_2} \cdots x_{m-1}^{a_{m-1}}) \circ f \\
&= (x_1^{a_1} \circ f)(x_2^{a_2} \circ f) \cdots (x_{m-1}^{a_{m-1}} \circ f) \\
&= (x_1^{a_1} + \sum_{1 \leq i \leq s} c_i \tau(\theta_i))(x_2^{a_2} + \sum_{1 \leq i \leq s} c_i \tau^2(\theta_i)) \cdots (x_{m-1}^{a_{m-1}} + \sum_{1 \leq i \leq s} c_i \tau^{m-1}(\theta_i)).
\end{aligned}$$

It follows from Lemma 3 that the expression above can be further simplified to

$$\lambda \circ f = x_1^{a_1} x_2^{a_2} \cdots x_{m-1}^{a_{m-1}} + \sum_{1 \leq j \leq m-1} \frac{x_1^{a_1} x_2^{a_2} \cdots x_{m-1}^{a_{m-1}}}{x_j^{a_j}} \sum_{1 \leq i \leq s} c_i \tau^j(\theta_i).$$

This completes the proof. ■

Lemma 5: Let $1 \leq j \leq m-1, i \geq 1$. Then

$$\frac{x_1^{a_1} x_2^{a_2} \cdots x_m^{a_m}}{x_j^{a_j}} \tau^j(\theta_i) = 0.$$

Proof: Since $\underline{a}$ is bifix-free, we have

$$(a_1, a_2, \ldots, a_{m-j}) \neq (a_{1+j}, a_{2+j}, \ldots, a_m),$$

i.e., there is $1 \leq t \leq m-j$ such that $a_t \neq a_{t+j}$. It can be seen that $x_{t+j}^{a_{t+j}} \mid \frac{x_1^{a_1} x_2^{a_2} \cdots x_m^{a_m}}{x_j^{a_j}}$. On the other hand, it can be seen from (3) and (4) that $x_{t+j}^{a_t} \mid \tau^j(\lambda)$ and $\tau^j(\lambda) \mid \tau^j(\theta_i)$, respectively. Then the desired result follows from $x_{t+j}^{a_{t+j}} x_{t+j}^{a_t} = 0$. ■

Based on Lemmas 3, 4, 5, we now present an essential result of this section, which shows that $\Omega_{\underline{a}}$ possesses remarkable arithmetic properties under the $\circ$-product. We remark that this key property was first found in [20, Lemma 7] for $\underline{a} = (0, 1)$.

Lemma 6: Let $f = x_0 + \sum_{1 \leq i \leq s} c_i \theta_i \in \Omega_{\underline{a}}$, where $c_i \in \mathbb{F}_2, s \geq 1$. Then for $k \geq 1$,

$$\theta_k \circ f = \theta_k + \sum_{1 \leq i \leq s} c_i \theta_{i+k}.$$

Proof: We prove it by induction on k. When $k=1$, it can be seen that

$$\begin{aligned}\theta_1 \circ f &= (\lambda x_m^{a_m}) \circ f \\ &= (\lambda \circ f)(x_m^{a_m} \circ f) \\ &= (\lambda + \sum_{1\le j\le m-1} \frac{x_1^{a_1}x_2^{a_2}\cdots x_{m-1}^{a_{m-1}}}{x_j^{a_j}} \sum_{1\le i\le s} c_i\tau^j(\theta_i))(x_m^{a_m} + \sum_{1\le i\le s} c_i\tau^m(\theta_i)),\end{aligned} \tag{15}$$

where the last equality follows from Lemma 4. By Lemmas 3 and 5, (15) can be simplified to

$$\begin{aligned}\theta_1 \circ f &= \lambda(x_m^{a_m} + \sum_{1\le i\le s} c_i\tau^m(\theta_i)) \\ &= \lambda x_m^{a_m} + \sum_{1\le i\le s} c_i\lambda\tau^m(\theta_i) \\ &= \theta_1 + \sum_{1\le i\le s} c_i\theta_{i+1},\end{aligned}$$

where the last equality follows from the recursion relation in (5). This shows that the assertion holds for $k=1$.

Assume that the assertion holds for some $k \ge 1$, i.e.,

$$\theta_k \circ f = \theta_k + \sum_{1\le i\le s} c_i\theta_{i+k}.$$

By (5) and Lemma 4, we have

$$\begin{aligned}\theta_{k+1} \circ f &= (\lambda \cdot \tau^m(\theta_k)) \circ f \\ &= (\lambda \circ f) \cdot \tau^m(\theta_k \circ f) \\ &= (\lambda + \sum_{1\le j\le m-1} \frac{x_1^{a_1}x_2^{a_2}\cdots x_{m-1}^{a_{m-1}}}{x_j^{a_j}} \sum_{1\le i\le s} c_i\tau^j(\theta_i)) \cdot \tau^m(\theta_k + \sum_{1\le i\le s} c_i\theta_{i+k}) \\ &= (\lambda + \sum_{1\le j\le m-1} \frac{x_1^{a_1}x_2^{a_2}\cdots x_{m-1}^{a_{m-1}}}{x_j^{a_j}} \sum_{1\le i\le s} c_i\tau^j(\theta_i)) \cdot (\tau^m(\theta_k) + \sum_{1\le i\le s} c_i\tau^m(\theta_{i+k})).\end{aligned}$$

By Lemma 3, the expression above can be simplified to

$$\begin{aligned}\theta_{k+1} \circ f &= \lambda(\tau^m(\theta_k) + \sum_{1\le i\le s} c_i\tau^m(\theta_{i+k})) \\ &= \lambda\tau^m(\theta_k) + \sum_{1\le i\le s} c_i\lambda\tau^m(\theta_{i+k}) \\ &= \theta_{k+1} + \sum_{1\le i\le s} c_i\theta_{i+k+1}.\end{aligned}$$

This completes the proof. ∎

One may wonder if we remove the single variable x_0 from f in Lemma 6 such that $f = \sum_{1\le i\le s} c_i\theta_i$, then whether $\theta_k \circ f = \sum_{1\le i\le s} c_i\theta_{i+k}$ holds? The answer is negative, see below.

Example 2: Let $\underline{a} = (1,0)$. Then $\theta_1 = x_1\bar{x}_2, \theta_2 = x_1x_3\bar{x}_4, \theta_3 = x_1x_3x_5\bar{x}_6$. For $n > 2$, it can be checked that $\theta_1 \circ (x_0+\theta_1) = \theta_1 + \theta_2$ and $\theta_1 \circ (x_0 + \theta_1 + \theta_2) = \theta_1 + \theta_2 + \theta_3$, whereas $\theta_1 \circ \theta_1 = x_2\bar{x}_3 \ne \theta_2$ and $\theta_1 \circ (\theta_1 + \theta_2) = x_2\bar{x}_3 + x_2x_4\bar{x}_5 \ne \theta_2 + \theta_3$.

Theorem 2: Let $f, g \in \Omega_{\underline{a}}$. Then $f \circ g = g \circ f \in \Omega_{\underline{a}}$, namely, $\Omega_{\underline{a}}$ is a commutative monoid.

Proof: Let $f = x_0 + \sum_{1\le i\le s} c_i\theta_i, g = x_0 + \sum_{1\le j\le t} d_j\theta_j$. Then it follows from Lemma 6 that

$$\begin{aligned}f \circ g &= (x_0 + \sum_{1\le i\le s} c_i\theta_i) \circ g \\ &= g + \sum_{1\le i\le s} c_i(\theta_i \circ g) \\ &= x_0 + \sum_{1\le j\le t} d_j\theta_j + \sum_{1\le i\le s} c_i(\theta_i + \sum_{1\le j\le t} d_j\theta_{j+i}) \\ &= x_0 + \sum_{1\le j\le t} d_j\theta_j + \sum_{1\le i\le s} c_i\theta_i + \sum_{1\le i\le s, 1\le j\le t} c_id_j\theta_{j+i},\end{aligned} \tag{16}$$

which shows that $f \circ g \in \Omega_{\underline{a}}$. Moreover, by expanding the expression of $g \circ f$ in the same way, one will see that $f \circ g = g \circ f$. ∎

C. The connection between the $\circ$-product on $\Omega_{\underline{a}}$ and the multiplication on the quotient ring of $\mathbb{F}_2[x]$

Theorem 2 reveals the closure of $\Omega_{\underline{a}}$ under the $\circ$-product. Moreover, the explicit expansion in (16) suggests a stronger statement: the indices of θ_i's behave like the exponents of polynomials in $\mathbb{F}_2[x]$. We now make this observation precise. Let $\mathcal{R} \subset \mathbb{F}_2[x]$ be the collection of polynomials with the constant term 1, i.e.,

$$\mathcal{R} = \{1 + \sum_{1 \le i \le s} c_i x^i \mid c_i \in \mathbb{F}_2, s \ge 1\}.$$

Then $\mathcal{R}$ forms a commutative monoid with respect to the multiplication. It can be observed from (16) that the $\circ$-product of functions in $\Omega_{\underline{a}}$ behaves like the multiplication of polynomials in $\mathcal{R}$. Specifically, let $\psi : \mathcal{R} \to \Omega_{\underline{a}}$ be defined by

$$1 + \sum_{1 \le i \le s} c_i x^i \mapsto x_0 + \sum_{1 \le i \le s} c_i \theta_i.$$

Then it can be seen that ψ is well-defined and surjective. Moreover, it is not hard to verify that

$$\psi(l_1 \cdot l_2) = \psi(l_1) \circ \psi(l_2)$$

for $l_1, l_2 \in \mathcal{R}$. That is to say, ψ is a surjective homomorphism. Recall that the kernel of ψ is an equivalence relation on $\mathcal{R}$, defined by $l_1 \ker \psi \ l_2 \Leftrightarrow \psi(l_1) = \psi(l_2)$ for $l_1, l_2 \in \mathcal{R}$. A well-known result regarding the monoid isomorphism says that

$$\mathcal{R}/\ker\psi \cong \Omega_{\underline{a}}, \tag{17}$$

where every element of $\mathcal{R}/\ker\psi$ is an equivalence class of $\mathcal{R}$ with respect to $\ker\psi$.

Let $\Omega^*_{\underline{a}}$ be the unit group of $\Omega_{\underline{a}}$, i.e., the collection of all invertible functions in $\Omega_{\underline{a}}$. Then the main results of this paper are given below, which clarify $\ker\psi$ by the periodicity of $(\theta_k)_{k\ge1}$ for $m \nmid n$ and $m \mid n$, respectively.

Theorem 3: If $m \nmid n$, then $\Omega^*_{\underline{a}} = \Omega_{\underline{a}}$, which is an abelian group isomorphic to the unit group of $\mathbb{F}_2[x]/(x^{\lceil \frac{n}{m} \rceil})$.

Proof: By (17), it suffices to show that $\mathcal{R}/\ker\psi$ is isomorphic to the unit group of $\mathbb{F}_2[x]/(x^{\lceil \frac{n}{m} \rceil})$. Since $m \nmid n$, it follows from Lemma 1 that $\theta_k = 0$ if $k \ge \lceil \frac{n}{m} \rceil$. Recall that $\theta_1, \theta_2, \ldots, \theta_{\lfloor \frac{n}{m} \rfloor}$ are linearly independent over $\mathbb{F}_2$. Let

$$l_1 = 1 + \sum_{1 \le i \le s} c_i x^i, l_2 = 1 + \sum_{1 \le i \le t} d_i x^i \in \mathcal{R}.$$

It can be seen that

$$\begin{aligned} \psi(l_1) = \psi(l_2) &\Leftrightarrow x_0 + \sum_{1 \le i \le s} c_i \theta_i = x_0 + \sum_{1 \le i \le t} d_i \theta_i \\ &\Leftrightarrow c_i = d_i, 1 \le i \le \lfloor \frac{n}{m} \rfloor \\ &\Leftrightarrow l_1 \equiv l_2 \mod x^{\lceil \frac{n}{m} \rceil}, \end{aligned}$$

This means that an element of $\mathcal{R}/\ker\psi$ is an equivalence class of $\mathcal{R}$ modulo $x^{\lceil \frac{n}{m} \rceil}$. Recall that an element in the unit group of $\mathbb{F}_2[x]/(x^{\lceil \frac{n}{m} \rceil})$ is an equivalence class of $\mathbb{F}_2[x]$ modulo $x^{\lceil \frac{n}{m} \rceil}$, whose representative has the constant term. Thus there is a natural isomorphism between $\mathcal{R}/\ker\psi$ and the unit group of $\mathbb{F}_2[x]/(x^{\lceil \frac{n}{m} \rceil})$. ∎

Theorem 4: If $m \mid n$, then $\Omega^*_{\underline{a}}$ is an abelian group isomorphic to the unit group of $\mathbb{F}_2[x]/(x^{\frac{2n}{m}} + x^{\frac{n}{m}})$.

Proof: By (17), it suffices to show that the unit group of $\mathcal{R}/\ker\psi$ is isomorphic to that of $\mathbb{F}_2[x]/(x^{\frac{2n}{m}} + x^{\frac{n}{m}})$. Let l_1, l_2 be defined as in the proof of Theorem 3. Then by Lemma 2, it can be seen that

$$\psi(l_1) = x_0 + \sum_{1 \le i \le s} c_i \theta_i = x_0 + \sum_{1 \le j < \frac{2n}{m}} c'_j \theta_j,$$

$$\psi(l_2) = x_0 + \sum_{1 \le i \le t} d_i \theta_i = x_0 + \sum_{1 \le j < \frac{2n}{m}} d'_j \theta_j,$$

where $c'_j = c_j, d'_j = d_j$ for $1 \le j < \frac{n}{m}$, and $c'_j = \sum_{0 \le s' \le \lfloor \frac{(s-j)m}{n} \rfloor} c_{j+\frac{n}{m}s'}, d'_j = \sum_{0 \le t' \le \lfloor \frac{(t-j)m}{n} \rfloor} d_{j+\frac{n}{m}t'}$ for $\frac{n}{m} \le j < \frac{2n}{m}$. Then it can be seen that

$$\begin{aligned} \psi(l_1) = \psi(l_2) &\Leftrightarrow c'_j = d'_j \text{ for } 1 \le j < \frac{2n}{m} \\ &\Leftrightarrow l_1 \equiv l_2 \mod x^{\frac{2n}{m}} + x^{\frac{n}{m}}. \end{aligned}$$

This means that an element of $\mathcal{R}/\ker\psi$ is an equivalence class of $\mathcal{R}$ modulo $x^{\frac{2n}{m}} + x^{\frac{n}{m}}$. In particular, an element of $\mathcal{R}/\ker\psi$ is invertibe if and only if its representative is relatively prime to $x^{\frac{2n}{m}} + x^{\frac{n}{m}}$. Then it can be seen that there is a natural isomorphism between the unit group of $\mathcal{R}/\ker\psi$ and that of $\mathbb{F}_2[x]/(x^{\frac{2n}{m}} + x^{\frac{n}{m}})$.

∎

If $m \nmid n$, then we define $\varphi : \Omega_{\underline{a}} \to \mathbb{F}_2[x]/(x^{\lceil \frac{n}{m} \rceil})$ by

$$\varphi(x_0 + \sum_{1 \le i \le s} c_i \theta_i) = [1 + \sum_{1 \le i \le s} c_i x^i],$$

where $[l(x)]$ denote the coset of the ideal $(x^{\lceil \frac{n}{m} \rceil})$ in $\mathbb{F}_2[x]$ containing $l(x) \in \mathbb{F}_2[x]$. By Theorem 3, φ is an embedding, and $\mathrm{im}(\varphi) = \{[l(x)] \mid l(x) \in \mathbb{F}_2[x], l(0) = 1\}$, which is the unit group of $\mathbb{F}_2[x]/(x^{\lceil \frac{n}{m} \rceil})$.

If $m \mid n$, then we define $\varphi' : \Omega_{\underline{a}} \to \mathbb{F}_2[x]/(x^{\frac{2n}{m}} + x^{\frac{n}{m}})$ by

$$\varphi'(x_0 + \sum_{1 \le i \le s} c_i \theta_i) = [1 + \sum_{1 \le i \le s} c_i x^i]',$$

where $[l(x)]'$ denote the coset of the ideal $(x^{\frac{2n}{m}} + x^{\frac{n}{m}})$ in $\mathbb{F}_2[x]$ containing $l(x) \in \mathbb{F}_2[x]$. It can be seen from the proof of Theorem 4 that φ' is an embedding, and $\mathrm{im}(\varphi') = \{[l(x)]' \mid l(x) \in \mathbb{F}_2[x], l(0) = 1\}$.

Through φ or φ', one can treat the $\circ$-product on $\Omega_{\underline{a}}$ as the multiplication on the quotient ring of $\mathbb{F}_2[x]$, where the algebraic properties of the latter are well-understood. For instance, if $f \in \Omega_{\underline{a}}$ is invertible, then its inverse can be formulated by calculating the multiplicative inverse of $\varphi(f)$ if $m \nmid n$ or $\varphi'(f)$ if $m \mid n$, by means of the extended Euclidean algorithm. We remark that every function in $\Omega_{\underline{a}}$ is invertible if $m \nmid n$ by Theorem 3, whereas it is not true if $m \mid n$ by Theorem 4. This is formally stated as follows.

Theorem 5: Let $f = x_0 + \sum_{1 \le i \le s} c_i \theta_i \in \Omega_{\underline{a}}$. If $m \nmid n$, then f is invertible. If $m \mid n$, then f is invertible if and only if

$$\gcd(1 + \sum_{1 \le i \le s} c_i x^i, x^{\frac{2n}{m}} + x^{\frac{n}{m}}) = \gcd(1 + \sum_{1 \le i \le s} c_i x^i, x^d + 1) = 1,$$

where d is the largest odd divisor of $\frac{n}{m}$.

Proof: The first assertion follows directly from Theorem 3. Write $\frac{n}{m} = 2^s d$ with d odd, $s \ge 0$. Then the second assertion follows from Theorem 4 and $x^{\frac{2n}{m}} + x^{\frac{n}{m}} = x^{\frac{n}{m}}(x^d + 1)^{2^s}$. ∎

Theorem 6: If $m \nmid n$, then $\#\Omega_{\underline{a}} = \#\Omega^*_{\underline{a}} = 2^{\lfloor \frac{n}{m} \rfloor}$. If $m \mid n$, then $\#\Omega_{\underline{a}} = 2^{\frac{2n}{m} - 1}$, and

$$\#\Omega^*_{\underline{a}} = 2^{n-2} \prod_{k \mid d, k \neq 1} (1 - 2^{-\mathrm{ord}_k(2)})^{\frac{\phi(k)}{\mathrm{ord}_k(2)}},$$

where d is the largest odd divisor of $\frac{n}{m}$, $\mathrm{ord}_k(2)$ is the multiplicative order of 2 modulo k, and ϕ is the Euler's totient function.

Proof: If $m \nmid n$, then it follows from Theorem 3 that $\Omega^*_{\underline{a}} = \Omega_{\underline{a}} = x_0 + \langle \theta_1, \theta_2, \ldots, \theta_{\lfloor \frac{n}{m} \rfloor} \rangle$, where $\theta_1, \theta_2, \ldots, \theta_{\lfloor \frac{n}{m} \rfloor}$ are linearly independent over $\mathbb{F}_2$ as shown in Subsection III-A. Hence $\#\Omega^*_{\underline{a}} = \#\Omega_{\underline{a}} = 2^{\lfloor \frac{n}{m} \rfloor}$. If $m \mid n$, then $\Omega_{\underline{a}} = x_0 + \langle \theta_1, \theta_2, \ldots, \theta_{\frac{2n}{m} - 1} \rangle$, where $\theta_1, \theta_2, \ldots, \theta_{\frac{2n}{m} - 1}$ are linearly independent over $\mathbb{F}_2$. Hence $\#\Omega_{\underline{a}} = 2^{\frac{2n}{m} - 1}$. Moreover, $\#\Omega^*_{\underline{a}}$ is equal to the number of polynomials in $\mathbb{F}_2[x]$ that are of degrees smaller than $\frac{2n}{m}$ as well as relatively prime to $x^{\frac{2n}{m}} + x^{\frac{n}{m}}$, which can be explicitly calculated by means of Chinese remainder theorem via factoring $x^{\frac{2n}{m}} + x^{\frac{n}{m}}$ over $\mathbb{F}_2$, see [24, Lemma 3.69]. Specifically, let $\frac{n}{m} = 2^s d$ with d odd, $s \ge 0$. Then $x^{\frac{2n}{m}} + x^{\frac{n}{m}} = x^{\frac{n}{m}}(x^d + 1)^{2^s}$. Recall that $x^d + 1$ can be written as $x^d + 1 = \prod_{k \mid d} Q_k(x)$, where the k-th cyclotomic polynomial $Q_k(x)$ can be further written as the product of $\frac{\phi(k)}{\mathrm{ord}_k(2)}$ pairwise distinct irreducible polynomials over $\mathbb{F}_2$ of degree $\mathrm{ord}_k(2)$ if $k > 1$. Then the desired result follows directly from [24, Lemma 3.69]. ∎

IV. Algebraic properties of $\rho_k = x_0 + \theta_k$

In this section, we focus on the algebraic properties of a particular class of functions in $\Omega_{\underline{a}}$, written as $\rho_k = x_0 + \theta_k$ for $k \ge 1$, mainly from two aspects: the invertibility and the cycle structure. This specialization is useful as many known shift-invariant maps studied in earlier literature are defined by a single local "nonlinear term" added to x_0, and hence fall into the form ρ_k for a suitable choice of $\underline{a}$ and k. We remark that part of the results derived in this section constitute straightforward generalizations of the findings in [20, Section 4] and [22, Section IV].

A. The invertibility of ρ_k

Theorem 7: ρ_k is invertible if and only if $m \nmid n$. Moreover, if ρ_k is invertible, then $\mathrm{ord}(\rho_k) = 2^{\lceil \log_2(\frac{n}{km}) \rceil}$ and its inverse can be expressed as

$$\rho_k^{-1} = x_0 + \theta_k + \theta_{2k} + \cdots + \theta_{sk},$$

where $s = \lfloor \frac{n}{km} \rfloor$, and $\deg(\rho_k^{-1}) = sk(m-1) + 1$.

Proof: Assume that $m \mid n$. Then it follows from Theorem 5 that ρ_k is not invertible since $\varphi'(\rho_k) = [1 + x^k]' \in \mathbb{F}_2[x]/(x^{\frac{2n}{m}} + x^{\frac{n}{m}})$ is not invertible, a contradiction.

Let $m \nmid n$. Then it follows from Theorem 5 that ρ_k is invertible. Note that the order and the inverse of ρ_k can be described by the order and the inverse of $\varphi(\rho_k) = [1 + x^k] \in \mathbb{F}_2[x]/(x^{\lceil \frac{n}{m} \rceil})$. By Theorem 6 and Lagrange's theorem, the order of ρ_k is a power of 2, so is that of $[1 + x^k]$. Let 2^t be the order of $[1 + x^k]$ for $t \geq 0$. It can be seen from

$$(1 + x^k)^{2^t} = 1 + x^{k2^t} \equiv 1 \mod x^{\lceil \frac{n}{m} \rceil}$$

that t is the least non-negative integer such that $k2^t \geq \lceil \frac{n}{m} \rceil$, i.e., $k2^t \geq \frac{n}{m}$, and hence $t = \lceil \log_2(\frac{n}{km}) \rceil$. Moreover, let $s = \lfloor \frac{n}{km} \rfloor$. Then $s < \frac{n}{km} < s + 1$, and so $sk < \lceil \frac{n}{m} \rceil \leq (s + 1)k$. It can be seen from

$$(1 + x^k)(1 + x^k + x^{2k} + \cdots + x^{sk}) = 1 + x^{(s+1)k} \equiv 1 \mod x^{\lceil \frac{n}{m} \rceil}$$

that the inverse of $[1 + x^k]$ is $[1 + x^k + x^{2k} + \cdots + x^{sk}]$. This formulates the inverse of ρ_k. Then since $\deg(\theta_k) < \deg(\theta_{2k}) < \cdots < \deg(\theta_{sk})$ by (8), we have $\deg(\rho_k^{-1}) = \deg(\theta_{sk}) = sk(m - 1) + 1$. ∎

Let $m \nmid n$. It follows from Lemma 1 that $\rho_k \neq x_0$ if and only if $k \leq \lfloor \frac{n}{m} \rfloor$. Moreover, for $k \leq \lfloor \frac{n}{m} \rfloor$, it can be seen from Theorem 7 that ρ_k is an involution, i.e., $\rho_k = \rho_k^{-1}$ if and only if $\frac{n}{2} < km < n$.

In Daemen's thesis [1, Table A.1], it can be seen that there are several shift-invariant maps whose defining functions are of the form $\rho_1 = x_0 + x_1^{a_1} x_2^{a_2} \cdots x_m^{a_m} \in \Omega_{\underline{a}}$ for $\underline{a} \in \{(0, 1), (0, 0, 1), (1, 0, 0), (0, 1, 1), (0, 1, 1, 1), (0, 0, 0, 1), (0, 0, 1, 1)\}$, and one shift-invariant map whose defining function is of the form $\rho_2 = x_0 + \theta_2 \in \Omega_{\underline{a}}$ for $\underline{a} = (0, 1)$, i.e., $x_0 + \bar{x}_1 \bar{x}_3 x_4$. In particular, two of them have been used in practice: one is the well-known χ-map defined by $x_0 + \bar{x}_1 x_2$, and the other is used in a hash function called Monolith defined by $x_0 + \bar{x}_1 x_2 x_3$. Since the algebraic properties of the former have been well-studied, see, for example, [1], [15], [20], [18], we employ the results derived in this subsection to analyze those of the latter.

Recall that the inverse of the nonlinear layer used in Monolith was first formulated in [16, Theorem 4]. Here we would like to present an alternative one in a more concise form, which is an immediate consequence of Theorem 7.

Theorem 8: Let $\rho_1 = x_0 + \bar{x}_1 x_2 x_3 \in \Omega_{\underline{a}}$ for $\underline{a} = (0, 1, 1)$, which is the defining function of the nonlinear layer used in Monolith. Then ρ_1 is invertible if and only if $3 \nmid n$. Moreover, let $3 \nmid n$. Then $\mathrm{ord}(\rho_1) = 2^{\lceil \log_2(\frac{n}{3}) \rceil}$, and the inverse of ρ_1 is

$$\begin{aligned} \rho_1^{-1} &= x_0 + \theta_1 + \theta_2 + \cdots + \theta_{\lfloor \frac{n}{3} \rfloor} \\ &= x_0 + \sum_{1 \leq i \leq \lfloor \frac{n}{3} \rfloor} x_{3i} \prod_{0 \leq j \leq i-1} \bar{x}_{1+3j} x_{2+3j}, \end{aligned}$$

where $\deg(\rho_1^{-1}) = 2\lfloor \frac{n}{3} \rfloor + 1$.

B. The cycle structure of ρ_k

In this subsection, we always assume that $m \nmid n$, in which case ρ_k is invertible. Recall that the shift-invariant map on $\mathbb{F}_2^n$ defined by ρ_k is expressed as

$$F_{\rho_k} = (\rho_k, \tau(\rho_k), \ldots, \tau^{n-1}(\rho_k)).$$

For $S \in \mathbb{F}_2^n$, let $\mathcal{O}_{\rho_k}(S) = \{F_{\rho_k}^d(S) \mid d \geq 0\}$ be the orbit of S under F_{ρ_k}. Since F_{ρ_k} is invertible, there exists $l \geq 1$ such that $F_{\rho_k}^l(S) = S$, and the least such l is called the length of the cycle of F_{ρ_k} containing S, which is equal to $\#\mathcal{O}_{\rho_k}(S)$. For a positive integer d, it is not hard to see that

$$F_{\rho_k}^d(S) = S \Leftrightarrow \#\mathcal{O}_{\rho_k}(S) \mid d. \tag{18}$$

Below we show how to determine $\#\mathcal{O}_{\rho_k}(S)$ for each $S \in \mathbb{F}_2^n$, which provides a full description for the cycle structure of F_{ρ_k}.

The order of F_{ρ_k} is the least positive integer l such that $F_{\rho_k}^l$ is the identity map, i.e., $F_{\rho_k}^l(S) = S$ for each $S \in \mathbb{F}_2^n$, which equals the least common multiple of all cycle lengths of F_{ρ_k}. On the other hand, it can be seen from (1) that the order of F_{ρ_k} equals the order of ρ_k with respect to the $\circ$-product. Hence by Theorem 7, we have

$$\mathrm{lcm}\{\#\mathcal{O}_{\rho_k}(S) \mid S \in \mathbb{F}_2^n\} = 2^{\lceil \log_2(\frac{n}{km}) \rceil}. \tag{19}$$

For $S \in \mathbb{F}_2^n$, it can be seen from (19) that $\#\mathcal{O}_{\rho_k}(S) = 2^t$ for some $0 \leq t \leq \lceil \log_2(\frac{n}{km}) \rceil$, which also implies that there is at least one cycle of F_{ρ_k} whose length achieves the maximum $2^{\lceil \log_2(\frac{n}{km}) \rceil}$. To further characterize $\#\mathcal{O}_{\rho_k}(S)$, we introduce the following notation.

Let $\Delta = (a_1, a_2, \ldots, a_{m-1}) \in \mathbb{F}_2^{m-1}$, and let

$$\Gamma_k = \{(\underbrace{\Delta, *, \Delta, *, \ldots, \Delta, *}_{(k-1)m \text{ bits}}, \underbrace{\Delta, a_m}_{m \text{ bits}}) \mid * \in \mathbb{F}_2\} \subset \mathbb{F}_2^{km}, k \geq 1.$$

We say that $S = (s_0, s_1, \ldots, s_{n-1}) \in \mathbb{F}_2^n$ has a substring in Γ_k if there is $0 \leq i \leq n-1$ such that $(s_i, s_{i+1}, \ldots, s_{i+km-1}) \in \Gamma_k$, where the indices are taken modulo n.

Lemma 7: If $S \in \mathbb{F}_2^n$ has a substring in Γ_k, then $k \leq \lfloor \frac{n}{m} \rfloor$.

Proof: Assume that $k > \lfloor \frac{n}{m} \rfloor$. Let $k' = \lceil \frac{n}{m} \rceil$. Then $k' \leq k$. Since S has a substring in Γ_k, it also has a substring in $\Gamma_{k'}$. Without loss of generality, assume that $(s_1, s_2, \ldots, s_{k'm}) \in \Gamma_{k'}$. Let $k'm = n + r$ with $0 < r < m$. By the definition of $\Gamma_{k'}$, it can be seen that

$$(s_1, s_2, \ldots, s_r) = (a_1, a_2, \ldots, a_r)$$

and

$$(s_{k'm-r+1}, s_{k'm-r+2}, \ldots, s_{k'm}) = (a_{m-r+1}, a_{m-r+2}, \ldots, a_m),$$

which leads to $(a_1, a_2, \ldots, a_r) = (a_{m-r+1}, a_{m-r+2}, \ldots, a_m)$, a contradiction since $\underline{a}$ is bifix-free. ■

For $1 \leq k \leq \lfloor \frac{n}{m} \rfloor$, it can be seen from (4) that

$$\theta_k = 1 \Leftrightarrow (x_1, x_2, \ldots, x_{km}) \in \Gamma_k. \tag{20}$$

This leads to the following result.

Lemma 8: For $S \in \mathbb{F}_2^n$ and $1 \leq k \leq \lfloor \frac{n}{m} \rfloor$, $F_{\rho_k}(S) = S$ if and only if S has no substring in Γ_k.

Proof: It can be seen from (20) that $F_{\rho_k}(S) = S$ if and only if $\theta_k(\tau^i(S)) = 0$ for $0 \leq i \leq n-1$ if and only if $(s_{i+1}, s_{i+2}, \ldots, s_{i+km}) \notin \Gamma_k$ for $0 \leq i \leq n-1$, i.e., S has no substring in Γ_k. ■

Theorem 9: For $S \in \mathbb{F}_2^n$, if S has no substring in Γ_k, then $\#\mathcal{O}_{\rho_k}(S) = 1$; otherwise, $\#\mathcal{O}_{\rho_k}(S) = 2^{d+1}$, where d is the largest integer such that S has a substring in $\Gamma_{2^d k}$ with $0 \leq d \leq \lfloor \log_2(\frac{n}{km}) \rfloor$.

Proof: By Lemma 8, it follows that $F_{\rho_k}(S) = S$, i.e., $\#\mathcal{O}_{\rho_k}(S) = 1$, if and only if S has no substring in Γ_k. Assume that S has a substring in Γ_k, and d is the largest integer such that S has a substring in $\Gamma_{2^d k}$. Then by Lemma 7, $2^d k \leq \lfloor \frac{n}{m} \rfloor$, i.e., $2^d k \leq \frac{n}{m}$, which shows that $d \leq \lfloor \log_2(\frac{n}{km}) \rfloor$. According to (19), we can write $\#\mathcal{O}_{\rho_k}(S) = 2^t$ for $1 \leq t \leq \lceil \log_2(\frac{n}{km}) \rceil$. It can be seen from

$$\varphi({\rho_k}^{2^d}) = \varphi(\rho_k)^{2^d} = [1 + x^k]^{2^d} = [1 + x^{2^d k}]$$

and (1) that $F_{\rho_k}^{2^d} = F_{\rho_k^{2^d}} = F_{\rho_{2^d k}}$. Since S has a substring in $\Gamma_{2^d k}$, it follows from Lemma 8 that $F_{\rho_{2^d k}}(S) \neq S$, i.e., $F_{\rho_k}^{2^d}(S) \neq S$. Then by (18), $2^t \nmid 2^d$, and so $t > d$. If $d = \lfloor \log_2(\frac{n}{km}) \rfloor$, then we immediately derive that $t = d + 1$ due to $t \leq \lceil \log_2(\frac{n}{km}) \rceil$. Otherwise, since S has no substring in $\Gamma_{2^{d+1} k}$, it follows from Lemma 8 that $F_{\rho_{2^{d+1} k}}(S) = S$, i.e., $F_{\rho_k}^{2^{d+1}}(S) = S$. Then by (18), $2^t \mid 2^{d+1}$. Hence $t \leq d + 1$, and so $t = d + 1$. ■

For any $S \in \mathbb{F}_2^n$, it follows from Theorem 9 that the length of the cycle of F_{ρ_k} containing S can be determined via finding the largest integer d for which S has a substring in $\Gamma_{2^d k}$. In particular, if the cycle length $\#\mathcal{O}_{\rho_k}(S) = 1$, then S is called a fixed point of F_{ρ_k}. In general, permutations employed in cryptographic algorithms are expected to have as few fixed points as possible. Focusing on $k = 1$, we next derive the enumeration of fixed points of F_{ρ_1} via a combinatorial method.

Proposition 2: The number of fixed points of F_{ρ_1} is $2^n - N$, where

$$N = \sum_{1 \leq t \leq \lfloor \frac{n}{m} \rfloor} (-1)^{t-1} \frac{n}{t} \binom{n - tm + t - 1}{t - 1} 2^{n - tm}.$$

Proof: See Appendix A. ■

Remark 3: Generally, a counting formula for the fixed points of F_{ρ_k} for $k \geq 1$ can be derived in a similar way as Proposition 2, which takes a more complicated form accordingly. It is worth noting that the count of fixed points of F_{ρ_k} enables us to further determine its cycle number. Specifically, let M_{ρ_k} be the set of fixed points of F_{ρ_k}, which is also the set of states $S \in \mathbb{F}_2^n$ with no substring in Γ_k by Lemma 8. By the definition of Γ_k, it is not hard to see that

$$M_{\rho_k} \subset M_{\rho_{2k}} \subset \cdots \subset M_{\rho_{2^t k}},$$

where $t = \lfloor \log_2(\frac{n}{km}) \rfloor$ (if $t > \lfloor \log_2(\frac{n}{km}) \rfloor$, then $\rho_{2^t k} = x_0$, i.e., $F_{\rho_{2^t k}}$ is the identity map, in which case $M_{\rho_{2^t k}} = \mathbb{F}_2^n$). For $0 \leq d \leq t$, it can be seen that $M_{\rho_{2^{d+1} k}} - M_{\rho_{2^d k}}$ is exactly the set of states $S \in \mathbb{F}_2^n$, each of which has a substring in $\Gamma_{2^d k}$, but has no subtring in $\Gamma_{2^{d+1} k}$. In other words, $M_{\rho_{2^{d+1} k}} - M_{\rho_{2^d k}}$ is exactly the set of states $S \in \mathbb{F}_2^n$ such that $\#\mathcal{O}_{\rho_k}(S) = 2^{d+1}$ by Theorem 9. Then

$$\frac{\#(M_{\rho_{2^{d+1} k}} - M_{\rho_{2^d k}})}{2^{d+1}} = \frac{\#M_{\rho_{2^{d+1} k}} - \#M_{\rho_{2^d k}}}{2^{d+1}}$$

is the number of cycles of length 2^{d+1} of F_{ρ_k}. In this way, the cycle structure of F_{ρ_k} can be completely determined, not only the cycle lengths, but also the corresponding cycle numbers.

Recall that the cycle structure of the χ-map has been studied in [18], [20]. As for the cycle structure of ρ_1 given in Theorem 8, it can be fully characterized via the results above.

V. Further discussion

Every bifix-free sequence $\underline{a}$ can induce a family of functions $\Omega_{\underline{a}}$. Then a natural question arises: what are inherent connections between $\Omega_{\underline{a}}$ and $\Omega_{\underline{a}'}$ if $\underline{a} \neq \underline{a}'$? Moreover, if $\underline{a}$ is not bifix-free, does the connection between $\Omega_{\underline{a}}$ and the quotient ring of $\mathbb{F}_2[x]$ still holds? Focusing on these two aspects, this section is divided into two parts. In Subsection V-A, we derive a necessary and sufficient condition for $\Omega_{\underline{a}}$ and $\Omega_{\underline{a}'}$ to be isomorphic, and another for them to possess a nontrivial intersection. In Subsection V-B, we show that the isomorphism established in (17) is not valid if $\underline{a}$ is not bifix-free, which also explains why the bifix-free hypothesis is built into the definition of $\Omega_{\underline{a}}$.

A. Relations between $\Omega_{\underline{a}}$ and $\Omega_{\underline{a}'}$

Theorem 10: Let $\underline{a} \in \mathbb{F}_2^m, \underline{a}' \in \mathbb{F}_2^{m'}$ be bifix-free with $\underline{a} \neq \underline{a}'$ and $2 \leq m, m' < n$. Then $\Omega_{\underline{a}} \cong \Omega_{\underline{a}'}$ if and only if both $m, m' \nmid n$ and $\lfloor \frac{n}{m} \rfloor = \lfloor \frac{n}{m'} \rfloor$ or both $m, m' \mid n$ and $m = m'$.

Proof: If $m, m' \nmid n$ and $\lfloor \frac{n}{m} \rfloor = \lfloor \frac{n}{m'} \rfloor$, then it follows from Theorem 3 that $\Omega_{\underline{a}} \cong \Omega_{\underline{a}'}$ since both of them are isomorphic to the unit group of $\mathbb{F}_2[x]/(x^{\lceil \frac{n}{m} \rceil})$. If $m, m' \mid n$ and $m = m'$, then it can be seen from the proof of Theorem 4 that $\Omega_{\underline{a}} \cong \Omega_{\underline{a}'}$ since both of them are isomorphic to the multiplicative monoid $\{[l(x)]' \in \mathbb{F}_2[x]/(x^{\frac{2n}{m}} + x^{\frac{n}{m}}) \mid l(0) = 1\}$.

Conversely, assume that $\Omega_{\underline{a}} \cong \Omega_{\underline{a}'}$. Then $\#\Omega_{\underline{a}} = \#\Omega_{\underline{a}'}$. By Theorem 6, if both $m, m' \nmid n$, then it follows from $\#\Omega_{\underline{a}} = 2^{\lfloor \frac{n}{m} \rfloor}$ and $\#\Omega_{\underline{a}'} = 2^{\lfloor \frac{n}{m'} \rfloor}$ that $\lfloor \frac{n}{m} \rfloor = \lfloor \frac{n}{m'} \rfloor$. If both $m, m' \mid n$, then it follows from $\#\Omega_{\underline{a}} = 2^{\frac{2n}{m}-1}$ and $\#\Omega_{\underline{a}'} = 2^{\frac{2n}{m'}-1}$ that $m = m'$. In addition, if exactly one of m, m' divides n, say $m \nmid n$ and $m' \mid n$, then we will derive a contradiction since all functions in $\Omega_{\underline{a}}$ are invertible, whereas not all functions in $\Omega_{\underline{a}'}$ are invertible by Theorem 5. ∎

The intersection of $\Omega_{\underline{a}}$ and $\Omega_{\underline{a}'}$ is said to be trivial if it consists only of the identity element x_0, where $\underline{a} \neq \underline{a}'$. We remark that their intersection is typically trivial except for two extreme cases. To see this, we introduce the following auxiliary lemmas.

For $f \in \mathcal{B}_n$, let $\mathrm{Index}(f)$ be the set of variable indices of f. For instance, it can be seen from (3) that $\mathrm{Index}(\lambda) = \{1, 2, \ldots, m-1\}$.

Lemma 9: Let $h_1 = f_1 \cdot g_1, h_2 = f_2 \cdot g_2 \in \mathcal{B}_n$, where $\mathrm{Index}(f_1) \cap \mathrm{Index}(g_1) = \emptyset$, $\mathrm{Index}(f_2) \cap \mathrm{Index}(g_2) = \emptyset$. If $h_1 = h_2 \neq 0$ and $\mathrm{Index}(f_1) = \mathrm{Index}(f_2)$, then $f_1 = f_2, g_1 = g_2$.

Proof: Without loss of generality, assume that $\mathrm{Index}(f_1) = \mathrm{Index}(f_2) = \{0, 1, \ldots, k\}$ for $0 \leq k < n-1$. Let

$$h_1 = f_1(x_0, x_1, \ldots, x_k) g_1(x_{k+1}, x_{k+2}, \ldots, x_{n-1}),$$
$$h_2 = f_2(x_0, x_1, \ldots, x_k) g_2(x_{k+1}, x_{k+2}, \ldots, x_{n-1}).$$

Since $h_1 = h_2 \neq 0$, there is $(c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_2^n$ such that $h_1(c_0, c_1, \ldots, c_{n-1}) = h_2(c_0, c_1, \ldots, c_{n-1}) = 1$, and so $g_1(c_{k+1}, c_{k+2}, \ldots, c_{n-1}) = g_2(c_{k+1}, c_{k+2}, \ldots, c_{n-1}) = 1$. It can be seen from

$$h_1(x_0, x_1, \ldots, x_k, c_{k+1}, c_{k+2}, \ldots, c_{n-1}) = f_1(x_0, x_1, \ldots, x_k),$$
$$h_2(x_0, x_1, \ldots, x_k, c_{k+1}, c_{k+2}, \ldots, c_{n-1}) = f_2(x_0, x_1, \ldots, x_k),$$

that $f_1 = f_2$. Similarly, it can be deduced that $g_1 = g_2$. ∎

Lemma 10: For $k \geq 1$, if $\theta_k \neq 0$, then we can write $\theta_k = \lambda \cdot f$ for some $f \in \mathcal{B}_n$ such that $\mathrm{Index}(\lambda) \cap \mathrm{Index}(f) = \emptyset$.

Proof: If $m \nmid n$ and $1 \leq k \leq \lfloor \frac{n}{m} \rfloor$, then $\theta_k \neq 0$ by Lemma 1. By (4), we can write $\theta_k = \lambda \cdot f$ for $f = x_{km}^{a_m} \prod_{1 \leq i \leq k-1} \tau^{im}(\lambda)$, where $\mathrm{Index}(\lambda) \cap \mathrm{Index}(f) = \emptyset$.

If $m \mid n$, then by the proof of Lemma 2, it can be seen that $\theta_k \neq 0$ for $k \geq 1$, and $\theta_k = \lambda \cdot f$, where $f = x_{km}^{a_m} \prod_{1 \leq i \leq k-1} \tau^{im}(\lambda)$ if $1 \leq k \leq \frac{n}{m}$, and $f = x_{km}^{a_m} \prod_{1 \leq i \leq \frac{n}{m}-1} \tau^{im}(\lambda)$ if $k \geq \frac{n}{m}$. In both cases, we have $\mathrm{Index}(\lambda) \cap \mathrm{Index}(f) = \emptyset$. ∎

Theorem 11: Let $\underline{a} \in \mathbb{F}_2^m, \underline{a}' \in \mathbb{F}_2^{m'}$ be bifix-free with $\underline{a} \neq \underline{a}'$ and $2 \leq m, m' < n$. Then $\Omega_{\underline{a}} \cap \Omega_{\underline{a}'} \neq \{x_0\}$ if and only if $n = 4$ and $\{\underline{a}, \underline{a}'\} = \{(1,0,0),(1,0)\}$ or $\{(0,1,1),(0,1)\}$.

Proof: Let $n = 4$. If $\underline{a} = (1,0,0), \underline{a}' = (1,0)$, then it can be seen from Subsection III-A that $\Omega_{\underline{a}} \cap \Omega_{\underline{a}'} = \Omega_{\underline{a}} = \{x_0, x_0 + x_1\bar{x}_2\bar{x}_3\}$. Similarly, if $\underline{a} = (0,1,1), \underline{a}' = (0,1)$, then it can be seen that $\Omega_{\underline{a}} \cap \Omega_{\underline{a}'} = \Omega_{\underline{a}} = \{x_0, x_0 + \bar{x}_1 x_2 x_3\}$.

Conversely, let $\Omega_{\underline{a}} \cap \Omega_{\underline{a}'} \neq \{x_0\}$. For notational distinction below, we use λ, θ_k and λ', θ_k' defined in (3), (4) to denote the functions induced by $\underline{a}$ and $\underline{a}'$, respectively. Then $\langle \theta_1, \theta_2, \ldots \rangle \cap \langle \theta_1', \theta_2', \ldots \rangle \neq \{0\}$, namely, there are a collection of linearly independent $\theta_{i_1}, \theta_{i_2}, \ldots, \theta_{i_s}$ as well as a collection of linearly independent $\theta_{j_1}', \theta_{j_2}', \ldots, \theta_{j_e}'$ such that

$$\theta_{i_1} + \theta_{i_2} + \cdots + \theta_{i_s} = \theta_{j_1}' + \theta_{j_2}' + \cdots + \theta_{j_e}', \tag{21}$$

where $1 \leq i_1 < \cdots < i_s, 1 \leq j_1 < \cdots < j_e$.

When $m = m'$, by repeatedly applying Lemma 10, we can write (21) in the form

$$\lambda \cdot g = \lambda' \cdot g'$$

for some $g, g' \in \mathcal{B}_n$, where $\mathrm{Index}(\lambda) \cap \mathrm{Index}(g) = \emptyset$ and $\mathrm{Index}(\lambda') \cap \mathrm{Index}(g') = \emptyset$. Since $\mathrm{Index}(\lambda) = \mathrm{Index}(\lambda')$, it follows from Lemma 9 that $\lambda = \lambda'$, i.e.,

$$x_1^{a_1} x_2^{a_2} \cdots x_{m-1}^{a_{m-1}} = x_1^{a_1'} x_2^{a_2'} \cdots x_{m-1}^{a_{m-1}'}.$$

It follows that $a_i = a'_i$ for $1 \le i \le m-1$. Since both $\underline{a}, \underline{a}'$ are bifix-free, we have $a_m \neq a_1, a'_m \neq a'_1$. Then it follows from $a_1 = a'_1$ that $a_m = a'_m$. Thus $\underline{a} = \underline{a}'$, a contradiction to the claim that $\underline{a} \neq \underline{a}'$.

When $m \neq m'$**,** recall that the highest-degree terms of $\theta_{i_1}, \ldots, \theta_{i_s}$ (resp. $\theta'_{j_1}, \ldots, \theta'_{j_e}$) are pairwise distinct and $\deg(\theta_{i_1}) \le \cdots \le \deg(\theta_{i_s})$ (resp. $\deg(\theta'_{j_1}) \le \cdots \le \deg(\theta'_{j_e})$), as shown in Subsection III-A. For ease of notation below, let T and T' be the highest-degree terms of θ_{i_s} and θ'_{j_e}, respectively. We discuss the following three cases.

Case 1: if both $m, m' \nmid n$, then $i_s \le \lfloor \frac{n}{m} \rfloor, j_e \le \lfloor \frac{n}{m'} \rfloor$ by Lemma 1. It follows from (8) that $\deg(\theta_{i_1}) < \cdots < \deg(\theta_{i_s})$ and $\deg(\theta'_{j_1}) < \cdots < \deg(\theta'_{j_e})$. This implies that $T = T'$ by (21). Moreover, it can be seen from (7) that

$$T = x_{i_s m} \prod_{0 \le i \le i_s - 1} x_{1+im} x_{2+im} \cdots x_{m-1+im} \tag{22}$$

and

$$T' = x_{j_e m'} \prod_{0 \le i \le j_e - 1} x_{1+im'} x_{2+im'} \cdots x_{m'-1+im'}. \tag{23}$$

Since $\deg(T) = \deg(T')$, i.e., $i_s(m-1)+1 = j_e(m'-1)+1$, it follows that $i_s \neq j_e$, and hence $i_s m \neq j_e m'$. This leads to a contradiction to $T = T'$ since their largest variable indices $i_s m$ and $j_e m'$ are not equal.

Case 2: if both $m, m' \mid n$, write $t = \frac{n}{m}, t' = \frac{n}{m'}$, where $t \neq t'$. It can be seen from (10) that

$$\deg(\theta_1) < \cdots < \deg(\theta_t) = \deg(\theta_{t+1}) = \cdots = \deg(\theta_{2t-1}) = n - t + 1,$$

and

$$\deg(\theta'_1) < \cdots < \deg(\theta'_{t'}) = \deg(\theta'_{t'+1}) = \cdots = \deg(\theta'_{2t'-1}) = n - t' + 1.$$

Since $n-t+1 \neq n-t'+1$, it implies that $i_s < t$ or $j_e < t'$ (if $i_s \ge t, j_e \ge t'$, then the two sides of (21) have different algebraic degrees, a contradiction). Without loss of generality, assume that $i_s < t$. Then T is as in (22). Since $\deg(\theta_{i_1}) < \cdots < \deg(\theta_{i_s})$, the left side of (21) has only one highest-degree term, so does the right side of (21). This implies that $T = T'$. If $j_e < t'$, then T' is as in (23). With the similar discussion as in Case 1, we will arrive at a contradiction to $T = T'$. If $t' \le j_e \le 2t' - 1$, then it can be seen from (9) that

$$T' = x_{j_e m'} \prod_{0 \le i \le t' - 1} x_{1+im'} x_{2+im'} \cdots x_{m'-1+im'}, \tag{24}$$

whose largest variable index is $n-1$. On the other hand, it can be seen from (22) that the largest variable index of T is $i_s m$. Then $T = T'$ leads to $i_s m = n - 1$, and so $m \mid n-1$, a contradiction to $m \mid n$.

Case 3: if $m \nmid n$ and $m' \mid n$, write $t' = \frac{n}{m'}$. Then $i_s \le \lfloor \frac{n}{m} \rfloor$ by Lemma 1, and T is as in (22). Since $\deg(\theta_{i_1}) < \cdots < \deg(\theta_{i_s})$, the left side of (21) has only one highest-degree term, so does the right side of (21), which implies that $T = T'$. If $j_e < t'$, then T' is as in (23). With the similar discussion as in Case 1, we will arrive at a contradiction to $T = T'$. If $t' \le j_e \le 2t' - 1$, then T' is as in (24), whose largest variable index is $n-1$. Since the largest variable index of T is $i_s m$, we have $i_s m = n - 1$. Then $m \mid n-1$, and so $\gcd(m, m') = 1$. Let

$$I = \{0, m, 2m, \ldots, (i_s - 1)m\}, I' = \{m', 2m', \ldots, t'm' \mod n\} - \{j_e m' \mod n\}.$$

Then it can be observed that

$$\text{Index}(T) = \{0, 1, \ldots, n-1\} - I, \text{Index}(T') = \{0, 1, \ldots, n-1\} - I',$$

which leads to $I = I'$ due to $T = T'$. It follows from $\deg(T) = i_s(m-1)+1 = n - i_s$ and $\deg(T') = n - t' + 1$ that $i_s = t' - 1$. If $i_s \ge 2$, then $t' \ge 3$, it follows from $I = I'$ that $m \in I'$, a contradiction to $\gcd(m, m') = 1$. If $i_s = 1$, then $t' = 2$, and $m = n - 1, 2m' = n$, in which case $I = \{0\}, I' = \{m', 2m' \mod n\} - \{j_e m' \mod n\}$. It follows from $I = I'$ that $j_e m' \equiv m' \mod n$, i.e., $j_e \equiv 1 \mod t'$. Then $j_e = 3$ due to $t' \le j_e \le 2t' - 1$, i.e., $2 \le j_e \le 3$. In this case, we can write (21) as

$$\theta_1 = c_1 \theta'_1 + c_2 \theta'_2 + c_3 \theta'_3,$$

where $c_1, c_2, c_3 \in \mathbb{F}_2$, and

$$\theta'_2 = x_0^{a'_{m'}} x_1^{a'_1} x_2^{a'_2} \cdots x_{m'-1}^{a'_{m'-1}} x_{m'+1}^{a'_1} x_{m'+2}^{a'_2} \cdots x_{2m'-1}^{a'_{m'-1}},$$

$$\theta'_3 = x_1^{a'_1} x_2^{a'_2} \cdots x_{m'-1}^{a'_{m'-1}} x_{m'}^{a'_{m'}} x_{m'+1}^{a'_1} x_{m'+2}^{a'_2} \cdots x_{2m'-1}^{a'_{m'-1}}.$$

It can be observed that the variable x_0 appears in θ'_2 , but does not appear in $\theta_1, \theta'_1, \theta'_3$. Thus $c_2 = 0$. Moreover, it can be seen that $\theta_1 \neq \theta'_1$ since $m \neq m'$, and $\theta_1 \neq \theta'_3$ since otherwise we would have

$$\underline{a} = (a'_1, a'_2, \ldots, a'_{m'-1}, a'_{m'}, a'_1, a'_2, \ldots, a'_{m'-1}),$$

a contradiction to the claim that $\underline{a}$ is bifix-free. This leaves only the case $\theta_1 = \theta'_1 + \theta'_3$, where

$$\theta'_1 + \theta'_3 = x_1^{a'_1} x_2^{a'_2} \cdots x_{m'-1}^{a'_{m'-1}} x_{m'}^{a'_{m'}} (1 + x_{m'+1}^{a'_1} x_{m'+2}^{a'_2} \cdots x_{2m'-1}^{a'_{m'-1}}).$$

Recall that $m = n-1, 2m' = n$. It can be seen that the truth table of θ_1 contains 2 ones, whereas that of $\theta'_1 + \theta'_3$ contains $2^{m'} - 2$ ones. Thus we have $m' = 2$, and hence $n = 4, m = 3$. It follows from $\theta_1 = \theta'_1 + \theta'_3$ that $(a_1, a_2, a_3) = (a'_1, a'_2, a'_1 + 1)$. Recall that there are exactly two binary bifix-free sequences of length 2, i.e., $(1, 0)$ and $(0, 1)$. It follows that $\underline{a} = (1, 0, 0)$ (resp. $\underline{a} = (0, 1, 1)$) if $\underline{a}' = (1, 0)$ (resp. $\underline{a}' = (0, 1)$).

■

Theorem 11 indicates that different $\underline{a}$ typically result in different $\Omega_{\underline{a}}$, for which the intersection of any two of them is $\{x_0\}$ except for two extreme cases. As shown in Remark 1, the number of bifix-free sequences is enormous, so is the number of invertible functions derived from $\Omega_{\underline{a}}$ via different $\underline{a}$.

Moreover, we would like to mention that the $\circ$-product of functions between $\Omega_{\underline{a}}$ and $\Omega_{\underline{a}'}$ will result in more invertible functions. Specifically, if $f \in \Omega_{\underline{a}}, g \in \Omega_{\underline{a}'}$ are invertible, then so is $f \circ g$, whose inverse is $g^{-1} \circ f^{-1}$, where f^{-1}, g^{-1} can be formulated by the extended Euclidean algorithm as shown in Section III. It is clear that $f \circ g \notin \Omega_{\underline{a}}, \Omega_{\underline{a}'}$ if $f, g \neq x_0$. However, the algebraic expression of $f \circ g$ would be generally very complicated, and cannot be given explicitly.

B. When $\underline{a}$ is not bifix-free

Recall that the validity of the isomorphism in (17) relies on Lemma 6. Below we shall show that Lemma 6 is false if $\underline{a}$ is not bifix-free. This is done by showing that one specific case of Lemma 6 does not hold, i.e., $\theta_1 \circ (x_0 + \theta_1) \neq \theta_1 + \theta_2$ for $n \geq 2m$. To see this, we introduce the following notation and results.

Let $\mathcal{P}_{\underline{a}}$ be the collection of all periods of $\underline{a} \in \mathbb{F}_2^m$. Recall that $m \in \mathcal{P}_{\underline{a}}$, and $\underline{a}$ is bifix-free if and only if $\mathcal{P}_{\underline{a}} = \{m\}$. For instance, let $\underline{a} = (1, 0, 1, 1, 0, 0)$ and $\underline{a}' = (1, 0, 1, 1, 0)$. Then $\mathcal{P}_{\underline{a}} = \{6\}$ and $\mathcal{P}_{\underline{a}'} = \{3, 5\}$, where $\underline{a}$ is bifix-free, but $\underline{a}'$ is not.

Lemma 11: Let $\underline{a} = (a_1, a_2, \ldots, a_m) \in \mathbb{F}_2^m$ and $\underline{a}' = (a_1, a_2, \ldots, a_{m-1})$ for $m \geq 2$. Then $\mathcal{P}_{\underline{a}} - \{m\} \subset \mathcal{P}_{\underline{a}'}$.

Proof: Assume that $\mathcal{P}_{\underline{a}} - \{m\} \neq \emptyset$, and $k \in \mathcal{P}_{\underline{a}} - \{m\}$, where $0 < k < m$. If $k = m - 1$, then it follows immediately that $k \in \mathcal{P}_{\underline{a}'}$. Otherwise, it follows from $a_1 = a_{1+k}, a_2 = a_{2+k}, \ldots, a_{m-1-k} = a_{m-1}$ that $k \in \mathcal{P}_{\underline{a}'}$ as well. ■

Lemma 12: Let $\underline{a} = (a_1, a_2, \ldots, a_m) \in \mathbb{F}_2^m$ and $\underline{a}' = (a_1, a_2, \ldots, a_{m-1})$ for $m \geq 2$. Let

$$g_j = \frac{x_1^{a_1} x_2^{a_2} \cdots x_{m-1}^{a_{m-1}}}{x_j^{a_j}} \tau^j(\theta_1),$$

where $1 \leq j \leq m-1, m \geq 2$. If $n \geq 2m$, then $g_j \neq 0 \Leftrightarrow j \in \mathcal{P}_{\underline{a}'}$.

Proof: Let us write

$$g_j = \frac{x_1^{a_1} x_2^{a_2} \cdots x_{m-1}^{a_{m-1}}}{x_j^{a_j}} x_{j+1}^{a_1} x_{j+2}^{a_2} \cdots x_{j+m}^{a_m}. \tag{25}$$

For $j \in \mathcal{P}_{\underline{a}'}$, if $j = m-1$, then it can be seen from (25) that $g_j \neq 0$ since its largest variable index meets $j+m < 2m \leq n$. If $0 < j < m-1$, then $(a_1, a_2, \ldots, a_{m-1-j}) = (a_{1+j}, a_{2+j}, \ldots, a_{m-1})$, and hence $x_{j+1}^{a_{j+1}} x_{j+2}^{a_{j+2}} \cdots x_{m-1}^{a_{m-1}} = x_{j+1}^{a_1} x_{j+2}^{a_2} \cdots x_{m-1}^{a_{m-1-j}}$. Then (25) can be written as

$$g_j = \frac{x_1^{a_1} x_2^{a_2} \cdots x_{m-1}^{a_{m-1}}}{x_j^{a_j}} x_m^{a_{m-j}} x_{1+m}^{a_{1+m-j}} \cdots x_{j+m}^{a_m}. \tag{26}$$

Similarly, it can be seen from (26) that $g_j \neq 0$.

Conversely, assume that $j \notin \mathcal{P}_{\underline{a}'}$. Then $(a_1, a_2, \ldots, a_{m-1-j}) \neq (a_{j+1}, a_{j+2}, \ldots, a_{m-1})$, i.e., there is $1 \leq i \leq m-1-j$ such that $a_i \neq a_{j+i}$. Then since $x_{j+i}^{a_{j+i}} \mid \frac{x_1^{a_1} x_2^{a_2} \cdots x_{m-1}^{a_{m-1}}}{x_j^{a_j}}$ and $x_{j+i}^{a_i} \mid \tau^j(\theta_1)$, it follows from $x_{j+i}^{a_{j+i}} x_{j+i}^{a_i} = 0$ that $g_j = 0$, a contradiction.

■

Proposition 3: If $\underline{a} \in \mathbb{F}_2^m$ is not bifix-free and $n \geq 2m$, then $\theta_1 \circ (x_0 + \theta_1) \neq \theta_1 + \theta_2$.

Proof: Let $\underline{a}', g_j$ be defined as in Lemma 12. Let k be the least period of $\underline{a}$, where $0 < k < m$. Then $k \in \mathcal{P}_{\underline{a}'}$ by Lemma 11. By setting $f = x_0 + \theta_1$ in (15), it can be seen that

$$\begin{aligned}
\theta_1 \circ (x_0 + \theta_1) &= (\lambda + \sum_{1 \leq j \leq m-1} \frac{x_1^{a_1} x_2^{a_2} \cdots x_{m-1}^{a_{m-1}}}{x_j^{a_j}} \tau^j(\theta_1))(x_m^{a_m} + \tau^m(\theta_1)) \\
&= \lambda(x_m^{a_m} + \tau^m(\theta_1)) + \sum_{1 \leq j \leq m-1} g_j \cdot (x_m^{a_m} + \tau^m(\theta_1)) \\
&= \theta_1 + \theta_2 + \sum_{j \in \mathcal{P}_{\underline{a}'}} g_j \cdot (x_m^{a_m} + \tau^m(\theta_1)),
\end{aligned}$$

where the last equality follows from (5) and Lemma 12. Let $h_j = g_j \cdot (x_m^{a_m} + \tau^m(\theta_1))$ for $j \in \mathcal{P}_{\underline{a}'}$. Then our goal is to show that $\sum_{j \in \mathcal{P}_{\underline{a}'}} h_j \neq 0$. Since k is a period of $\underline{a}$, we have $a_{m-k} = a_m$. It can be seen from (26) that $g_k x_m^{a_m} = g_k$, and hence $h_k = g_k + g_k \tau^m(\theta_1)$. Note that $x_{2m}^{a_m} \mid \tau^m(\theta_1)$. We assign variables as follows: $x_i = a_i$ for $i \in \{1, 2, \ldots, m-1\} - \{k\}$, $x_k = \bar{a}_k$, $x_l = a_{l-k}$ for $l \in \{m, 1+m, \ldots, k+m\}$, $x_{2m} = \bar{a}_m$, and the rest of the variables are assigned arbitrarily. Under

this assignment, it can be seen that the value of h_k is 1, and the value of h_j is 0 for $j \in \mathcal{P}_{\underline{a}'} - \{k\}$ due to $x_k^{a_k} \mid g_j$ as shown in (26). Therefore, $\sum_{j \in \mathcal{P}_{\underline{a}'}} h_j \neq 0$.

■

We remark that if $n < 2m$, then $\theta_1 \circ (x_0 + \theta_1) = \theta_1 + \theta_2$ may hold when $\underline{a}$ is not bifix-free, see below.

Example 3: Let $\underline{a} = (1, 0, 1, 0)$ which is not bifix-free. Let $\theta_1 = x_1\bar{x}_2x_3\bar{x}_4, \theta_2 = x_1\bar{x}_2x_3x_5\bar{x}_6x_7\bar{x}_8$ be defined as in (4). When $n = 5$, it can be checked that $\theta_2 = 0$, and $\theta_1 \circ (x_0 + \theta_1) = \theta_1 + \theta_2$. When $n = 6$ (resp. $n = 7$), it can be checked that $\theta_2 = x_1\bar{x}_2x_3x_5\bar{x}_0 \neq 0$ (resp. $\theta_2 = 0$), and $\theta_1 \circ (x_0 + \theta_1) \neq \theta_1 + \theta_2$. Generally, when $n \geq 8$, it follows from Proposition 3 that $\theta_1 \circ (x_0 + \theta_1) \neq \theta_1 + \theta_2$.

VI. Conclusion

In this paper, we study families of shift-invariant maps on $\mathbb{F}_2^n$ whose defining functions $\Omega_{\underline{a}}$ are induced by bifix-free sequences $\underline{a} \in \mathbb{F}_2^m$ with $2 \leq m < n$. It is shown that $\Omega_{\underline{a}}$ is closed under the $\circ$-product, which exhibits strong arithmetic properties analogous to linear Boolean functions as shown in (2). Specifically, for $f, g \in \Omega_{\underline{a}}$, if $m \nmid n$, then

$$\varphi(f \circ g) \equiv \varphi(f) \cdot \varphi(g) \mod x^{\lceil \frac{n}{m} \rceil},$$

and $\Omega_{\underline{a}}$ is isomorphic to the unit group of $\mathbb{F}_2[x]/(x^{\lceil \frac{n}{m} \rceil})$. If $m \mid n$, then

$$\varphi'(f \circ g) \equiv \varphi'(f) \cdot \varphi'(g) \mod x^{\frac{2n}{m}} + x^{\frac{n}{m}},$$

and the unit group of $\Omega_{\underline{a}}$ is isomorphic to that of $\mathbb{F}_2[x]/(x^{\frac{2n}{m}} + x^{\frac{n}{m}})$. The isomorphism transforms the $\circ$-product on $\Omega_{\underline{a}}$ into the multiplication on the quotient ring of $\mathbb{F}_2[x]$, which makes the analysis of invertibility, inverses, and orders substantially more explicit. Moreover, it is also shown that such isomorphism is not valid if $\underline{a}$ is not bifix-free for $n \geq 2m$. As a straightforward application, we use the derived results to study the algebraic properties of $\rho_k \in \Omega_{\underline{a}}$, which includes the χ-function, the function used in the nonlinear layer of Monolith, and several other functions proposed in earlier literature. It is shown that ρ_k is invertible if and only if $m \nmid n$. Moreover, the inverse and the cycle structure of ρ_k can be fully characterized if it is invertible.

Building on the function families studied in [20], [21], [22], this work generalizes them to $\Omega_{\underline{a}}$ by introducing bifix-free sequences. It is shown that different bifix-free sequences $\underline{a}$ result in different $\Omega_{\underline{a}}$, where the intersection of any two of them is typically trivial. As bifix-free sequences are plentiful, there exists an enormous collection of invertible functions from $\Omega_{\underline{a}}$ via different $\underline{a}$. This offers a rich parameter space for designing invertible shift-invariant maps, together with a clear algebraic framework for analyzing them.

From the perspective of cryptographic algorithm design, deriving explicit expressions for function inverses carries both theoretical and practical significance. This work inspires a heuristic idea: given an invertible function $f \in \mathcal{B}_n$, if there exists a submonoid G of $\mathcal{B}_n$ containing f, such that the composition on G corresponds to the multiplication on a certain quotient ring of $\mathbb{F}_2[x]$, then f^{-1} can be computed via the extended Euclidean algorithm. Nevertheless, it remains unclear whether any function families other than $\Omega_{\underline{a}}$ enjoy this desirable property, which will be one subject for future work.

Appendix A
A proof for Proposition 2

To prove Proposition 2, we introduce the following notation and results for preparation. We say that $S \in \mathbb{F}_2^n$ is a moving point of F_{ρ_1} if it is not a fixed one, i.e., $F_{\rho_1}(S) \neq S$, which is equivalent to saying that S has a substring in Γ_1 by Lemma 8, where $\Gamma_1 = \{(a_1, a_2, \ldots, a_m)\}$. Let

$$A_0 = \{(a_1, a_2, \ldots, a_m, \underbrace{*, *, \cdots, *}_{n-m}) \mid * \in \mathbb{F}_2\} \subset \mathbb{F}_2^n,$$

and let $A_i = \{\tau^i(S) \mid S \in A_0\}$ for $0 \leq i \leq n-1$, where $\#A_i = 2^{n-m}$. Let

$$A = \bigcup_{0 \leq i \leq n-1} A_i.$$

Then it is not hard to see that A is exactly the set of moving points of F_{ρ_1}. Below our goal is to determine $\#A$, which can be written as (by the inclusion-exclusion principle)

$$\#A = \sum_{1 \leq t \leq n} (-1)^{t-1} \sum_{0 \leq i_1 < i_2 < \ldots < i_t \leq n-1} \#(A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_t}). \tag{27}$$

For $0 \leq i, j \leq n-1$, let $d(i, j)$ be the cyclic distance between i, j modulo n which is defined by

$$d(i, j) = \min\{(i - j)_n, (j - i)_n\},$$

where $(k)_n$ denotes the least nonnegative residue modulo n of k. Then $d(i, j) \leq \frac{n}{2}$.

Lemma 13: For $0 \leq i < j \leq n-1$, $A_i \cap A_j = \emptyset \Leftrightarrow d(i, j) < m$.

Proof: Let $d = d(i,j) < m$. Assume that $S \in A_i \cap A_j$. If $d = j - i$, then it follows from

$$(s_i, s_{i+1}, \ldots, s_{i+m}) = (a_1, a_2, \ldots, a_m)$$

and

$$(s_j, s_{j+1}, \ldots, s_{j+m}) = (a_1, a_2, \ldots, a_m)$$

that

$$(a_1, a_2, \ldots, a_{m-d}) = (a_{1+d}, a_{2+d}, \ldots, a_m),$$

a contradiction since $\underline{a}$ is bifix-free. Similarly, if $d = n-j+i$, then we will arrive at a contradiction in the same way. Therefore, $A_i \cap A_j = \emptyset$.

Conversely, assume that $m \le d(i,j) \le \frac{n}{2}$. Choose $S \in \mathbb{F}_2^n$ such that $(s_i, s_{i+1}, \ldots, s_{i+m}) = (s_j, s_{j+1}, \ldots, s_{j+m}) = (a_1, a_2, \ldots, a_m)$. Then $S \in A_i \cap A_j$, a contradiction. ∎

Lemma 14: Let $I = \{i_1, i_2, \ldots, i_t\} \subset \{0, 1, \ldots, n-1\}$, where $t \le \lfloor \frac{n}{m} \rfloor$ and the pairwise cyclic distances among integers in I are all $\ge m$. Then the number of such I is

$$\frac{n}{t}\binom{n - tm + t - 1}{t - 1}.$$

Proof: Consider an n-length cycle $(0, 1, \ldots, n-1)$. Let us pick t vertices $i_1, i_2, \ldots, i_t$ from it in order whose pairwise cyclic distances are all $\ge m$. Specifically, let

$$d_1 = (i_2 - i_1)_n, d_2 = (i_3 - i_2)_n, \ldots, d_{t-1} = (i_t - i_{t-1})_n, d_t = (i_1 - i_t)_n.$$

Then

$$\begin{cases} d_1, d_2, \ldots, d_t \ge m, \\ d_1 + d_2 + \cdots + d_t = n. \end{cases} \tag{28}$$

Let $z_j = d_j - m \ge 0$ for $1 \le j \le t$. Then the number of nonnegative integer solutions of $z_1 + z_2 + \cdots + z_t = n - tm$ is known to be

$$\binom{n - tm + t - 1}{t - 1}, \tag{29}$$

which is larger than 0 due to $t \le \lfloor \frac{n}{m} \rfloor$. This is also the number of solutions of (28). Given $d_1, d_2, \ldots, d_t$ and i_1, it can be seen that $i_2, i_3, \ldots, i_t$ can be determined in order. Multiplying (29) by n (since there are n choices for the starting vertex i_1) and then dividing by t (because i_j for each $1 \le j \le t$ may serve as the starting vertex, and thus the number of subsets $\{i_1, i_2, \ldots, i_t\}$ is overcounted by a factor of t) yields the desired result. ∎

Proof of Proposition 2. We count the number of moving points of F_{ρ_1} by (27). When $t > \lfloor \frac{n}{m} \rfloor$, it implies that there exists at least one pair (i_e, i_r) for $1 \le e < r \le t$ such that $d(i_e, i_r) < m$, in which case it follows from Lemma 13 that $\cap_{1 \le j \le t} A_{i_j} = \emptyset$. When $t \le \lfloor \frac{n}{m} \rfloor$, if the pairwise cyclic distances among $i_1, i_2, \ldots, i_t$ are all $\ge m$, then for $S \in \cap_{1 \le j \le t} A_{i_j}$, it can be seen that there are tm coordinates of S being fixed. This implies that $\# \cap_{1 \le j \le t} A_{i_j} = 2^{n-tm}$. Finally, it follows from (27) and Lemma 14 that the number of moving points of F_{ρ_1} is

$$\sum_{1 \le t \le \lfloor \frac{n}{m} \rfloor} (-1)^{t-1} \frac{n}{t} \binom{n - tm + t - 1}{t - 1} 2^{n-tm}.$$

The number of fixed points equals 2^n minus the number of moving points.

REFERENCES

[1] J. Daemen, Cipher and hash function design strategies based on linear and differential cryptanalysis, Ph.D. thesis, Doctoral Dissertation, KU Leuven, 1995.

[2] G. Bertoni, J. Daemen, M. Peeters, and G. V. Assche, KECCAK specifications, NIST SHA-3 Submission, 2008.

[3] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, Ascon v1.2: Lightweight authenticated encryption and hashing, J. Cryptol., vol. 34, no. 3, 2021.

[4] C. Dobraunig et al., Rasta: A Cipher with Low ANDdepth and Few ANDs per Bit, in: H. Shacham, A. Boldyreva (eds) Advances in Cryptology - CRYPTO 2018, vol 10991, Springer, pp. 662-692, 2018.

[5] J. Daemen, S. Hoffert, G. Van Assche, and R. Van Keer, The design of Xoodoo and Xoofff, IACR Trans. Symmetric Cryptol., vol. 2018, no. 4, pp. 1-38, 2018.

[6] J. Daemen, P. M. C. Massolino, A. Mehrdad, and Y. Rotella, The Subterranean 2.0 cipher suite, IACR Trans. Symmetric Cryptol., vol. 2020, no. S1, pp. 262-294, 2020.

[7] Y. Belkheyar et al., ChiLow and ChiChi, New Constructions for Code Encryption, In: S. Fehr, PA. Fouque (eds) Advances in Cryptology - EUROCRYPT 2025, vol. 15601, Springer, pp. 212-243, 2025.

[8] S. Andreoli, G. Leander, E. Piccione, and L. Stennes, Generalizations of ChiChi: Families of Low-Latency Permutations in Any Even Dimension, IACR Trans. Symmetric Cryptol. vol. 2025, no. 3, pp. 800-826, 2025.

[9] L. Grassi, R. Lüftenegger, C. Rechberger, D. Rotaru, and M. Schofnegger, On a Generalization of Substitution-Permutation Networks: The HADES Design Strategy, In: A. Canteaut, Y. Ishai (eds) Advances in Cryptology - EUROCRYPT 2020, vol. 12106, Springer, pp. 674-704, 2020.

[10] L. Grassi, D. Khovratovich, C. Rechberger, A. Roy, and M. Schofnegger, Poseidon: A New Hash Function for Zero-Knowledge Proof Systems, In: USENIX Security Symposium 2021, pp. 519-535, 2021.
[11] L. Grassi, S. Onofri, M. Pedicini, and L. Sozzi, Invertible Quadratic Non-Linear Layers for MPC-/FHE-/ZK-Friendly Schemes over $\mathbb{F}_p^n$: Application to Poseidon, IACR Trans. Symmetric Cryptol. vol. 2022, no. 3, pp. 20-72, 2022.
[12] M. Urani and L. Grassi, Corrigendum to "Invertible Quadratic Non-Linear Layers for MPC-/FHE-/ZK-Friendly Schemes over $\mathbb{F}_p^n$: Application to Poseidon," IACR Trans. Symmetric Cryptol. vol. 2026, no. 1, pp. 527-532, 2026.
[13] L. Grassi et al., Monolith: Circuit-Friendly Hash Functions with New Nonlinear Layers for Fast and Constant-Time Implementations, IACR Trans. Symmetric Cryptol. vol. 2024, no. 3, pp. 44-83, 2024.
[14] L. Grassi, Bounded Surjective Quadratic Functions over $\mathbb{F}_p^n$ for MPC-/ZK-/FHE-Friendly Symmetric Primitives, IACR Trans. Symmetric Cryptol. vol. 2023, no. 2, pp. 94-131, 2023.
[15] F. Liu, S. Sarkar, W. Meier, and T. Isobe, The Inverse of χ and Its Applications to Rasta-Like Ciphers, J. Cryptol., vol. 35, no. 4, 2022.
[16] F. Liu,V. Dixit,S. Sarkar,W. Meier, and T. Isobe, Finding the Inverse of some shift-invariant Transformations, J. Cryptol., vol. 39, no. 1, 2026.
[17] J. Schoone and J. Daemen, Algebraic properties of the maps χ_n, Des. Codes Cryptogr., vol. 92, no. 8, pp. 2341-2365, 2024.
[18] J. Schoone and J. Daemen, The state diagram of χ, Des. Codes Cryptogr., vol. 92, no. 5, pp. 1393-1421, 2024.
[19] A. M. Graner, B. Kriepke, L. Krompholz, and G. Kyureghyan, On the bijectivity of the map χ, Cryptogr. Commun., vol. 18, pp. 97-105, 2026.
[20] B. Kriepke and G. M. Kyureghyan, Algebraic Structure of the Iterates of χ, In: L. Reyzin, D. Stebila (eds) Advances in Cryptology -CRYPTO 2024, vol. 14923, Springer, pp. 412-424, 2024.
[21] B. Kriepke and G. M. Kyureghyan, There are siblings of χ which are permutations for n even, Des. Codes Cryptogr., vol. 94, no. 125, 2026.
[22] C. Lyu, M. Yuan, D. Zheng, S. Sun, and S. Li, A Generalized χ_n-Function, IEEE Trans. Inf. Theory, vol. 72, no. 4, pp. 2543-2556, 2026.
[23] P. T. Nielsen, A note on bifix-free sequences, IEEE Trans. Inf. Theory, vol. IT-19, no. 5, pp. 704-706, 1973.
[24] R. Lidl and H. Niederreiter, Finite Fields, Encyclopedia of Mathematics and its Applications, vol. 20. Cambridge, U.K.: Cambridge Univ. Press, 1997.