

More constructions of n -cycle permutations

Tailin Niu, Kangquan Li, Longjiang Qu and Bing Sun

Abstract

n -cycle permutations with small n have the advantage that their compositional inverses are efficient in terms of implementation. They can be also used in constructing Bent functions and designing codes. Since the AGW Criterion was proposed, the permuting property of several forms of polynomials has been studied. In this paper, characterizations of several types of n -cycle permutations are investigated. Three criteria for n -cycle permutations of the form $xh(\lambda(x))$, $h(\psi(x))\varphi(x) + g(\psi(x))$ and $g(x^{q^t} - x + \delta) + bx$ with general n are provided. We demonstrate these criteria by providing explicit constructions. For the form of $x^r h(x^s)$, several new explicit triple-cycle permutations are also provided. Finally, we also consider triple-cycle permutations of the form $x^t + c\text{Tr}_{q^m/q}(x^s)$ and provide one explicit construction. Many of our constructions are both new in the n -cycle property and the permutation property.

Index Terms

Finite Field, Permutation Polynomial, the AGW Criterion, n -cycle Permutation.

1. INTRODUCTION

Let q be a prime power and \mathbb{F}_q be the finite field with q elements. A polynomial $f(x) \in \mathbb{F}_q[x]$ is called a *permutation polynomial* (PP) and f^{-1} denotes the compositional inverse of f , if the map $f : a \mapsto f(a)$ is a bijection on \mathbb{F}_q . If there exists a positive integer n such that $f^{(n)} = I$ is the identity map, f is called an *n -cycle permutation*, where the n -th functional power of f is defined inductively by $f^{(n)} = f \circ f^{(n-1)} = f^{(n-1)} \circ f$ and $f^{(1)} = f, f^{(0)} = I, f^{(-n)} = (f^{-1})^{(n)}$ with our notation. In this paper, n -cycle permutations are called *low-cycle permutations* for a small n . When $n = 2$ or 3 , f is also called an *involution*, or a *triple-cycle permutation* respectively.

Permutation polynomials over finite fields have wide applications in coding theory, cryptography, and combinatorial design theory, and we refer the readers to [2, 5, 18, 28, 30, 35] and the references therein for more details of the recent advances and contributions to the area. It is a challenging task to find new classes

This work is supported in part by the National Natural Science Foundation of China (NSFC) under Grant 62032009 and Grant 62172427, in part by the State Key Development Program for Basic Research of China under Grant 2019-JCJQ-ZD-351-00, in part by the Natural Science Foundation of Hunan Province of China under Grant 2021JJ40701, and in part by the Research Fund of National University of Defense Technology under Grant ZK22-14 and Grant ZK20-42. (*Corresponding author: Longjiang Qu.*)

The authors are with the College of Science, National University of Defense Technology, Changsha, 410073, China (e-mail: runningniu@outlook.com; likangquan11@nudt.edu.cn; ljqu_happy@hotmail.com; happy_come@163.com). They are also with Hunan Engineering Research Center of Commercial Cryptography Theory and Technology Innovation, Changsha 410073, China.

of permutation polynomials. However in 2011, Akbary et al. [1] provided a powerful method for constructing PPs over finite fields, which is called the AGW Criterion now. It both provided a unified explanation of earlier constructions of PPs and served a method to construct many new classes of PPs. After then, permutation polynomials of the form $x^r h(x^s)$ over \mathbb{F}_q were constructed by some researchers; see [6, 14, 17, 19, 21, 23–27, 33, 36, 38, 41, 45] etc. for more details. Similarly, PPs of the form $xh(\lambda(x))$, $h(\psi(x))\varphi(x) + g(\psi(x))$ and $g(x^{q^i} - x + \delta) + bx$ were studied in [1, 34, 39, 40, 44] etc. In addition, several authors researched constructions of the PPs $x + c\text{Tr}_{q^m/q}(x^s)$; see e.g. [9, 16, 20, 22, 42] for more details. In engineering, if both the permutation and its compositional inverse are efficient in terms of implementation, it is beneficial for the designer. This motivates the use of low-cycle permutations in the S-box of block ciphers. That the implementation of its inverse does not require much resources is a direct practical advantage of a low-cycle permutation. In devices with limited resources as a part of a block cipher, this is very useful. For instance, involutions have been used frequently in block cipher designs, in AES [13], Khazad [4], Anubis [3] and PRINCE [7]. Furthermore, low-cycle permutations (such as involutions) have been also used to construct Bent functions over finite fields [12, 15] and to design codes [15]. In [8], behaviors of permutations of an affine equivalent class have been analyzed with respect to some cryptanalytic attacks, and it is shown that low-cycle permutations (such as involutions) are nice candidates against these attacks. In addition, in classifying permutations in the view of cycle, the research of n -cycle permutations will be quite helpful, since each permutation over finite sets must be an n -cycle permutation for at least one positive integer n . Because of the importance of n -cycle permutations, in recent years, there are several studies about them. Charpin et al. [10] started the explicit study of involutions for finite fields with even characteristic. Since then, a lot of attentions had been drawn in this direction. In 2019, a more concise criterion for involutory permutations of the form $x^r h(x^s)$ over \mathbb{F}_q was given by Zheng et al. [43], where $s \mid (q - 1)$. By using this criterion, from a cyclotomic perspective, they proposed a general method to construct involutions of such form from given involutions over some subgroups of \mathbb{F}_q^* by solving congruent and linear equations over finite fields. Niu et al. [31] started from the AGW Criterion, and proposed an involutory version of the AGW Criterion, independently. They also provided several explicit involutions of the forms $x^r h(x^s)$ and $g(x^{q^i} - x + \delta) + cx$. Monomial, Dickson polynomial and Linearized triple-cycle permutations over binary fields were studied by [29]. In 2020, Wu et al. [37] generalized the work of [43] and obtained some characterizations of triple-cycle permutations of the form $x^r h(x^s)$. After that, Chen et al. [11] generalized the work of [31, 37, 43, 43] and obtained criteria for n -cycle permutations, which mainly are of the form $x^r h(x^s)$. Chen et al. [11] also proposed other constructing tools and several explicit triple-cycle permutations of the form $x^r h(x^s)$ from both usual perspective and cyclotomic perspective.

There are a lot of researches about the permutation property of several forms of polynomials $x^r h(x^s)$, $xh(\lambda(x))$, $h(\psi(x))\varphi(x) + g(\psi(x))$, $g(x^{q^i} - x + \delta) + bx$ and $x + c\text{Tr}_{q^m/q}(x^s)$. However, n -cycle permutation of the form $x^r h(x^s)$ have not been well investigated so far, and there are few studies about n -cycle property of other forms. Furthermore, explicit constructions of n -cycle permutations for general n and $n = 3$ is rarely found. New constructions that both new in n -cycle property and permutation property can also be

obtained by researching n -cycle permutations. These motivate us to consider the characterizations of n -cycle property for several forms and to provide several new explicit constructions. The main purpose of this paper is to investigate general criteria for n -cycle permutations of several forms over finite fields, and provides a way to acquire cycle permutations from constructing non-identity mappings over subsets of finite fields. First, motivated by the AGW Criterion, we propose three criteria for n -cycle permutations of the form $xh(\lambda(x))$, $h(\psi(x))\varphi(x) + g(\psi(x))$ and $g(x^{q^i} - x + \delta) + bx$ with general n . We also demonstrate these criteria by constructing explicit n -cycle permutations with general n and $n = 3$. Then, for $x^r h(x^s)$ over \mathbb{F}_q , we provide several explicit triple-cycle permutations by considering different $g(x) = x^r h(x)^s$ over $\mu_\ell = \{x \in \mathbb{F}_q^* \mid x^\ell = 1\}$, where $\ell = (q-1)/s$. Finally, we consider triple-cycle permutations of the form $x^t + c\text{Tr}_{q^m/q}(x^s)$ and provide one construction. Many of explicit constructions in this paper are both new in n -cycle property and permutation property, especially those in Section 4.

The rest of this paper is organized as follows. In Section 2, we introduce some basic knowledge about n -cycle permutations. Criteria for n -cycle permutations of the form $xh(\lambda(x))$, $h(\psi(x))\varphi(x) + g(\psi(x))$ and $g(x^{q^i} - x + \delta) + bx$ are proposed in Section 3. Triple-cycle permutations of the form $x^r h(x^s)$ are constructed in Section 4. Furthermore, we provide an explicit triple-cycle permutations of the form $x^t + c\text{Tr}_{q^m/q}(x^s)$.

2. PRELIMINARIES

In this section, we introduce some basic knowledge.

Definition 2.1. *If there exists a positive integer such that $f^{(n)} = I$, we call f an n -cycle permutation.*

Monomial n -cycle permutations by Lemma 2.2 will be basic components in obtaining some constructions.

Lemma 2.2. *Let $f(x) = x^d$ be a monomial polynomial over \mathbb{F}_q . Then f is n -cycle over \mathbb{F}_q if and only if $d^n \equiv 1 \pmod{q-1}$.*

Lemma 2.3. *Assume $f(x) \in \mathbb{F}_q[x]$ is an n -cycle permutation over \mathbb{F}_{q^m} . If $m \mid ni$, then $g(x) = f(x)^{q^i}$ is also an n -cycle permutation over \mathbb{F}_{q^m} .*

Proof. We have $f^{(n)}(x) = x$ and $f(x)^{q^i} = f(x^{q^i})$. Clearly, $g^{(n)}(x) = f^{(n)}(x^{q^{ni}}) = x^{q^{ni}}$. Thus, g is also n -cycle. \square

Let m be a positive integer. We use $\text{Tr}_{q^m/q}(\cdot)$ to denote the trace function from \mathbb{F}_{q^m} to \mathbb{F}_q , i.e.,

$$\text{Tr}_{q^m/q}(x) = x + x^q + x^{q^2} + \cdots + x^{q^{m-1}}.$$

We use A^* to denote a set containing all nonzero elements of a set A . The cardinality of a set A is denoted by $|A|$. For a mapping f , the kernel of f is denoted by $\ker(f)$.

Let $F : \mathbb{F}_{p^m} \rightarrow \mathbb{F}_{p^m}$ be a mapping, and ω be a p -th primitive unit root, where p is a prime and m is a positive integer. The Walsh transform of F at $(u, v) \in \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ equals by definition the Walsh transform of the so-called component function $\text{Tr}_{p^n/p}(vF(x))$ at u , that is:

$$W_F(u, v) := \sum_{x \in \mathbb{F}_{p^m}} \omega^{\text{Tr}_{p^m/p}(vF(x)) + \text{Tr}_{p^m/p}(ux)}.$$

We have a proposition for involutions by the Walsh transform.

Proposition 2.4. *Assume F permutes \mathbb{F}_{p^m} . Then, F is an involution if and only if $W_F(u, v) = W_F(v, u)$ for each $(u, v) \in \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$.*

Proof. Assume F is an involution. Then, we have

$$W_F(u, v) = \sum_{x \in \mathbb{F}_{p^m}} \omega^{\text{Tr}_{p^m/p}(vF(x)) + \text{Tr}_{p^m/p}(ux)} = \sum_{x \in \mathbb{F}_{p^m}} \omega^{\text{Tr}_{p^m/p}(vF(F(x))) + \text{Tr}_{p^m/p}(uF(x))} = W_F(v, u).$$

Conversely, we assume $W_F(u, v) = W_F(v, u)$. Since

$$W_{F^{-1}}(v, u) = \sum_{x \in \mathbb{F}_{p^m}} \omega^{\text{Tr}_{p^m/p}(uF^{-1}(x)) + \text{Tr}_{p^m/p}(vx)} = \sum_{x \in \mathbb{F}_{p^m}} \omega^{\text{Tr}_{p^m/p}(ux) + \text{Tr}_{p^m/p}(vF(x))} = W_F(u, v),$$

we arrive at $W_{F^{-1}}(v, u) = W_F(v, u)$, for each $(u, v) \in \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$. Thus, F is an involution. \square

When we construct cycle permutations, the following result is inspiring and useful.

Lemma 2.5. (*[1], AGW Criterion*) *Let A, S , and \bar{S} be finite sets with $\#S = \#\bar{S}$, and let $f : A \rightarrow A$, $g : S \rightarrow \bar{S}$, $\lambda : A \rightarrow S$ and $\bar{\lambda} : A \rightarrow \bar{S}$ be maps such that $\bar{\lambda} \circ f = g \circ \lambda$. If both λ and $\bar{\lambda}$ are surjective, then the following statements are equivalent:*

- (1) f is a bijection and
- (2) g is a bijection from S to \bar{S} and f is injective on $\lambda^{-1}(s)$ for each $s \in S$.

The AGW Criterion can be illustrated as the following commutative diagram:

$$\begin{array}{ccc} A & \xrightarrow{f} & A \\ \lambda \downarrow & & \downarrow \bar{\lambda} \\ S & \xrightarrow{g} & \bar{S} \end{array}$$

Since the AGW Criterion was put forward, a lot of families of PPs were constructed by it. In this paper, a permutation polynomial is called an *AGW-PP* if it is based on the AGW Criterion.

3. n -CYCLE PERMUTATIONS OF THREE TYPES OF AGW-PPS

In this section, we present three constructions of n -cycle permutations of the form $xh(\lambda(x))$, $h(\psi(x))\varphi(x) + g(\psi(x))$ and $g(x^{q^i} - x + \delta) + bx$. Most of them are new in n -cycle property.

A. n -cycle permutations of the form $xh(\lambda(x))$

In [1, Theorem 6.3], Akbary et al. studied the permutation property of $xh(\lambda(x))$. In this subsection, we consider the n -cycle property of permutations with the form $xh(\lambda(x))$, and several constructions are provided.

Theorem 3.1. *Let q be any power of a prime number p , m be any positive integer, and S be any subset of \mathbb{F}_{q^m} containing 0. Let $h, k \in \mathbb{F}_{q^m}$ be any polynomials such that $h(0) \neq 0$, $k(0) = 0$ and $g(x) = xk(h(x))$ permuting $\lambda(\mathbb{F}_{q^m})$. Let $\lambda(x) \in \mathbb{F}_{q^m}[x]$ be any polynomial satisfying*

- (1) $h(\lambda(\mathbb{F}_{q^m})) \subseteq S$; and
- (2) $\lambda(a\alpha) = k(a)\lambda(\alpha)$ for all $a \in S$ and all $\alpha \in \mathbb{F}_{q^m}$.

Then the polynomial $f(x) = xh(\lambda(x))$ is an n -cycle permutation if and only if

$$\prod_{i=0}^{n-1} h(g^{(i)}(y)) = 1 \quad (1)$$

holds for any $y \neq 0 \in \lambda(\mathbb{F}_{q^m})$. Furthermore,

$$\prod_{i=0}^{n-1} k(h(g^{(i)}(y))) = 1 \quad (2)$$

is necessary for f being an n -cycle permutation.

Proof. Let $0 < s < n$. For any $x \in \mathbb{F}_{q^m}$ and $y \in \lambda(\mathbb{F}_{q^m})$ satisfying $y = \lambda(x)$, we have

$$\begin{aligned} f^{(n)}(x) &= f^{(n-1)}(f(x)) \\ &= f^{(n-2)}(f(x)h(\lambda(f(x)))) \\ &= f^{(n-2)}(xh(\lambda(x))h(\lambda(xh(\lambda(x))))), \end{aligned} \quad (3)$$

by plugging $f(x) = xh(\lambda(x))$ into $f^{(n)}(x)$. After that, apply $\lambda(h(\lambda(x))x) = k(h(\lambda(x)))\lambda(x)$ into Eq. (3) and we obtain

$$\begin{aligned} f^{(n)}(x) &= f^{(n-2)}(xh(\lambda(x))h(k(h(\lambda(x)))\lambda(x))) \\ &= f^{(n-2)}(xh(\lambda(x))h(g(\lambda(x)))) \\ &= f^{(n-2)}\left(x \prod_{i=0}^1 h(g^{(i)}(\lambda(x)))\right). \end{aligned}$$

So on and so forth, we arrive at the following

$$f^{(n)}(x) = f^{(n-s+1)}\left(x \prod_{i=0}^{s-2} h(g^{(i)}(\lambda(x)))\right), \quad (4)$$

where s is a positive integer. After plugging $f(x) = xh(\lambda(x))$ into Eq. (4), we acquire

$$f^{(n)}(x) = f^{(n-s)} \left(xh(\lambda(x)) \prod_{i=0}^{s-2} h \left(g^{(i)}(\lambda(xh(\lambda(x)))) \right) \right). \quad (5)$$

Plugging $\lambda(xh(\lambda(x))) = k(h(\lambda(x)))\lambda(x)$ and $g(x) = xk(h(x))$ into Eq. (5), one can get

$$\begin{aligned} f^{(n)}(x) &= f^{(n-s)} \left(xh(\lambda(x)) \prod_{i=0}^{s-2} h \left(g^{(i)}(\lambda(x)k(h(\lambda(x)))) \right) \right) \\ &= f^{(n-s)} \left(xh(\lambda(x)) \prod_{i=0}^{s-2} h \left(g^{(i+1)}(\lambda(x)) \right) \right) \\ &= f^{(n-s)} \left(x \prod_{i=0}^{s-1} h \left(g^{(i)}(\lambda(x)) \right) \right). \end{aligned}$$

Similarly, we finally arrive at

$$f^{(n)}(x) = f \left(x \prod_{i=0}^{n-2} h \left(g^{(i)}(\lambda(x)) \right) \right) = x \prod_{i=0}^{n-1} h \left(g^{(i)}(\lambda(x)) \right). \quad (6)$$

On the one hand, assume for any $y \in \lambda(\mathbb{F}_{q^m})$, $\prod_{i=0}^{n-1} h(g^{(i)}(y)) = 1$. Then, according to Eq. (6), f is an n -cycle permutation over \mathbb{F}_{q^m} . On the other hand, assume that f is an n -cycle permutation over \mathbb{F}_{q^m} . For each $y \in \lambda(\mathbb{F}_{q^m})^*$, there exists an $x_0 \in \mathbb{F}_q^*$ such that $\lambda(x_0) = y$. According to Eq. (6), we have $\prod_{i=0}^{n-1} h(g^{(i)}(y)) = 1$. Thus f is an n -cycle permutation if and only if Eq. (1) holds.

Furthermore, we assume f is an n -cycle permutation. For each $y \in \lambda(\mathbb{F}_{q^m})$, there exists an $x_0 \in \mathbb{F}_q$ such that $\lambda(x_0) = y$. For any $x \in \mathbb{F}_{q^m}$, we have the following equation according to Eq. (6):

$$\lambda \left(x_0 \prod_{i=0}^{n-1} h \left(g^{(i)}(y) \right) \right) = \lambda(x_0).$$

Since $\prod_{i=0}^{n-1} h(g^{(i)}(y)) \in S$, one can obtain

$$\prod_{i=0}^{n-1} k \left(h \left(g^{(i)}(y) \right) \right) \lambda(x_0) = \lambda(x_0).$$

Thus, Eq. (2) is necessary for f being an n -cycle permutation. \square

Proposition 3.2. *Assume q is a prime power, m, n are positive integers, and $h(x) \in \mathbb{F}_q[x]$ is a polynomial such that for any $y \in \mathbb{F}_q$, $h(y)^n = 1$. Let $\lambda(x) \in \mathbb{F}_{q^m}[x]$ be either $\lambda_1(x) = \text{Tr}_{q^m/q}(x^n)$ or $\lambda_2(x) = \sum_{0 \leq i_1 < i_2 < \dots < i_n \leq m-1} x^{q^{i_1} + q^{i_2} + \dots + q^{i_n}}$. Then the polynomial $f(x) = xh(\lambda(x))$ is an n -cycle permutation over \mathbb{F}_{q^m} .*

Proof. In Theorem 3.1, we have $\lambda(\mathbb{F}_{q^m}) = \mathbb{F}_q$ and $\lambda(a\alpha) = a^n\lambda(\alpha)$ for all $a \in \mathbb{F}_q$ and $\alpha \in \mathbb{F}_{q^m}$. Since $h(y)^n = 1$ holds for $y \in \mathbb{F}_q$, $g(y) = yh(y)^n = y$ is an n -cycle permutation over \mathbb{F}_q . Plugging $h(y)^n = 1$

and $g(y) = y$ into Eq. (1), one can get that f is an n -cycle permutation, according to Theorem 3.1. \square

There are a lot of polynomials h satisfying $h(y)^n = 1$, for any $y \in \mathbb{F}_q$. Below are some examples.

Corollary 3.3. *Let q be a prime power, n be a positive integer satisfying $n \mid (q - 1)$. Then, the polynomial*

$$f(x) = x \left(1 + \theta \lambda(x)^{(q-1)/n} - \lambda(x)^{q-1} \right)$$

is an n -cycle permutation over \mathbb{F}_{q^m} , where λ is either λ_1 or λ_2 in Proposition 3.2, θ is an n -th primitive unit root and m is a positive integer.

Proof. Let $h(y) = 1 + \theta y^{(q-1)/n} - y^{q-1}$ and $f(x)$ can be written as $xh(\lambda(x))$. In the following, we will prove $h(y)^n = 1$, for $y \in \mathbb{F}_q$. First, $h(0) = 1$. Next, for $y \neq 0$, we have $h(y)^n = (1 + \theta y^{(q-1)/n} - 1)^n = y^{q-1} = 1$. Thus, f is an n -cycle permutation according to Proposition 3.2. \square

When $n = 2$, there are also some involutions that easy to be obtained.

Corollary 3.4. *Let q be an odd prime power. The polynomial*

$$f(x) = x (1 - 2\lambda(x)^{q-1})$$

is an involution on \mathbb{F}_{q^m} , where λ is either λ_1 or λ_2 in Proposition 3.2 and m is a positive integer.

Proof. Let $h(y) = 1 - 2y^{q-1}$. Then $f(x)$ can be written as $xh(\lambda(x))$. We have $h(0) = 1$ and $h(y) = -1$, for $y \neq 0$. Thus, f is an involution according to Proposition 3.2. \square

Corollary 3.4 is a generalization of Example 5.5 in [32].

Corollary 3.5. *Let q be a power of odd prime p . Assume a, b, c are integers satisfying $a^2 + b^2 \equiv 0 \pmod{p}$ and $4c \equiv 0 \pmod{q - 1}$. Then, the polynomial*

$$f(x) = x (1 + a\lambda(x)^c + b\lambda(x)^{q-c-1} - \lambda(x)^{q-1})$$

is an involution on \mathbb{F}_{q^m} , where λ is either λ_1 or λ_2 in Proposition 3.2 and m is a positive integer.

Proof. Let $h(y) = 1 + ay^c + by^{q-c-1} - y^{q-1}$ and $f(x)$ can be written as $xh(\lambda(x))$. For $y \neq 0$, we have $h(y)^2 = (ay^c + by^{q-c-1})^2 = a^2y^{2c} + b^2y^{-2c} + 2ab = 1$, where $a^2y^{2c} + b^2y^{-2c} = 0$ according to $4c \equiv 0 \pmod{q - 1}$ and $a^2 \equiv -b^2 \pmod{p}$. Thus $h(y)^2 = 1$ holds for $y \in \mathbb{F}_q$. Thus, f is an involution according to Proposition 3.2. \square

Here, we provide simple examples for Corollary 3.5. Let $h(y) = 1 + y + 3y^3 + 4y^4$. Then $f(x)$ can be written as $xh(\lambda(x))$. We have $h(y) = 1$, for $y = 0, 2, 4$ and $h(y) = -1$ for $y = 1, 3, 5$. Thus, the polynomial $f(x) = x (1 + \lambda(x) + 3\lambda(x)^3 + 4\lambda(x)y^4)$ is an involution on \mathbb{F}_{5^m} according to Proposition 3.2, where $\lambda(x) = \sum_{0 \leq i < j \leq m-1} x^{5^i + 5^j}$ and m is a positive integer.

B. n -cycle permutations of the form $h(\psi(x))\varphi(x) + g(\psi(x))$

In [1, Theorem 5.1], Akbary et al. investigated the permutation property of $h(\psi(x))\varphi(x) + g(\psi(x))$. In this subsection, we consider the n -cycle property of permutations with the form of $h(\psi(x))\varphi(x) + g(\psi(x))$. Several constructions are given.

Theorem 3.6. *Consider any polynomial $g \in \mathbb{F}_{q^m}[x]$, any q -polynomials $\varphi, \psi \in \mathbb{F}_{q^m}[x]$ satisfying that φ is an n -cycle permutation over \mathbb{F}_{q^m} and $\varphi \circ \psi = \psi \circ \varphi$. Then*

$$f(x) = \varphi(x) + g(\psi(x))$$

is an n -cycle permutation over \mathbb{F}_{q^m} if and only if

$$\sum_{k=0}^{n-1} \varphi^{(n-1-k)} \left(g(\bar{f}^{(k)}(y)) \right) = 0 \quad (7)$$

holds for any $y \in \psi(\mathbb{F}_{q^m})$, where $\bar{f}(x) = \varphi(x) + \psi(g(x))$.

Proof. For any $x \in \mathbb{F}_{q^m}$, and $y \in \psi(\mathbb{F}_{q^m})$ such that $y = \psi(x)$, we have

$$\begin{aligned} f^{(n)}(x) &= \varphi(f \circ f^{(n-2)}(x)) + g(\psi \circ f \circ f^{(n-2)}(x)) \\ &= \varphi(\varphi(f^{(n-2)}(x))) + \varphi(g(\psi(f^{(n-2)}(x)))) + g(\bar{f} \circ \psi \circ f^{(n-2)}(x)) \\ &= \sum_{k=0}^1 \varphi^{(1-k)} \left(g(\bar{f}^{(k)}(\psi(f^{(n-2)}(x)))) \right) + \varphi^{(2)}(f^{(n-2)}(x)). \end{aligned}$$

So on and so forth, this will lead to

$$f^{(n)}(x) = \sum_{k=0}^2 \varphi^{(2-k)} \left(g(\bar{f}^{(k)}(\psi(f^{(n-3)}(x)))) \right) + \varphi^{(3)}(f^{(n-3)}(x)),$$

and finally arrive at

$$\begin{aligned} f^{(n)}(x) &= \sum_{k=0}^{n-1} \varphi^{(n-1-k)} \left(g(\bar{f}^{(k)}(\psi(x))) \right) + \varphi^{(n)}(x), \\ &= \sum_{k=0}^{n-1} \varphi^{(n-1-k)} \left(g(\bar{f}^{(k)}(y)) \right) + x, \end{aligned} \quad (8)$$

which indicates that f is an n -cycle permutation over \mathbb{F}_{q^m} .

On the one hand, assume that Eq. (7) holds for any $y \in \psi(\mathbb{F}_{q^m})$. Then, according to Eq. (8), f is an n -cycle permutation over \mathbb{F}_{q^m} . On the other hand, assume that f is an n -cycle permutation over \mathbb{F}_{q^m} . For each $y \in \psi(\mathbb{F}_{q^m})$, there exists an $x_0 \in \mathbb{F}_q$ such that $\psi(x_0) = y$. According to Eq. (8), we have $\sum_{k=0}^{n-1} \varphi^{(n-1-k)} \left(g(\bar{f}^{(k)}(y)) \right) = 0$. Thus f is an n -cycle permutation if and only if Eq. (7) holds for any $y \in \psi(\mathbb{F}_{q^m})$. \square

The proposition below is a generalization of involutory criterion in [32].

Proposition 3.7. Define ψ, g as in Theorem 3.6. Consider any q -polynomial $\psi \in \mathbb{F}_{q^m}[x]$ satisfying $g(\psi(\mathbb{F}_{q^m})) \neq \{0\}$. Assume $g(x) \in \mathbb{F}_{q^m}[x]$ is nonzero such that $g(\mathbb{F}_{q^m}) \subseteq \ker(\psi)$. Then,

$$f(x) = x + g(\psi(x))$$

is an n -cycle permutation over \mathbb{F}_{q^m} if and only if p is of n , where p is the characteristic of \mathbb{F}_{q^m} .

Proof. Clearly $\ker(\varphi) \cap \ker(\psi) = \{0\}$, where $\varphi(x) = x$. Together with $g(\mathbb{F}_{q^m}) \subseteq \ker(\psi)$, we have $\bar{f}(x) = x + \psi(g(x)) = x$. According to Theorem 3.6, f is an n -cycle permutation if and only if $ng(y) = 0$, which is equivalent to the condition that p is a factor of n . \square

Generally speaking, it is not hard to obtain φ and ψ satisfying $\varphi \circ \psi = \psi \circ \varphi$. For example, both ψ and φ are q -polynomials over \mathbb{F}_q . In the corollary below, note that $\varphi(x)$ permutes \mathbb{F}_q due to $\sum_{i=0}^{m-1} \alpha_i \neq 0$.

Corollary 3.8. Assume q -polynomial ψ satisfying $\psi(\mathbb{F}_q) = \{0\}$. Let $H(x)$ be a nonzero polynomial over \mathbb{F}_{q^m} and $g(x)$ be either $g_1(x) = \text{Tr}_{q^m/q}(H(x))$ with $H(\psi(\mathbb{F}_{q^m})) \not\subseteq \ker(\text{Tr}_{q^m/q})$ or $g_2(x) = H(x)^s$ with $H(\psi(\mathbb{F}_{q^m})) \neq \{0\}$, where positive integer s satisfies $s(q-1) \equiv 0 \pmod{q^m-1}$. Then,

$$f(x) = x + g(\psi(x))$$

is an n -cycle permutation over \mathbb{F}_{q^m} if and only if p is a factor of n , where p is the characteristic of \mathbb{F}_{q^m} .

Proof. One can obtain $g(\mathbb{F}_{q^m}) \subseteq \ker(\psi)$ by the expression of g . Thus f is an n -cycle permutation if and only if p is a factor of n . \square

Such conditions in Corollary 3.8 are not hard to meet.

Example 3.9. Let q be a power of 3. Then $x + \text{Tr}_{q^m/q}((x^q - x)^2)$ is a triple-cycle permutation over \mathbb{F}_{q^m} .

Corollary 3.10. Assume s is an integer and $c \in \mathbb{F}_{q^2}^*$ satisfying $c + c^q = 0$. Then, $f(x) = x + c\text{Tr}_{q^2/q}(x)^s$ is a triple-cycle permutation over \mathbb{F}_{q^2} if and only if q is a power of 3.

Proof. We have

$$\bar{f}(y) = y + \text{Tr}_{q^2/q}(cx^s) = y + cx^s + c^q x^s = y.$$

Then, $\sum_{k=0}^{2-1} g(\bar{f}^{(k)}(y)) = 3cy^s$. According to Proposition 3.7, the result is established. \square

Proposition 3.11. Consider any polynomial $g(x) = \sum_{t=0}^{q^3-2} a_t x^t \in \mathbb{F}_{q^3}[x]$, and for each t , $\text{Tr}_{q^3/q}(a_t) = 0$. Then

$$f(x) = x^q + g(\text{Tr}_{q^3/q}(x))$$

is a triple-cycle permutation over \mathbb{F}_{q^3} .

Proof. In Theorem 3.6, let $\varphi(x) = x^q$ and $\psi(x) = \text{Tr}_{q^3/q}(x)$. Clearly we have $\varphi \circ \psi = \psi \circ \varphi$. Then, one can verify that $\text{Tr}_{q^3/q}(g(x)) = 0$ holds for any $x \in \mathbb{F}_q$, since $\text{Tr}_{q^3/q}(a_t) = 0$. Thus, $\bar{f}(x) = x^q + \text{Tr}_{q^3/q}(g(x)) = x^q$. Then, for any $y \in \mathbb{F}_q$,

$$(g(y))^{q^2} + (g(y^q))^q + g(y^{q^2}) = \text{Tr}_{q^3/q}(g(y)) = 0,$$

which is equivalent to

$$\sum_{k=0}^2 \varphi^{(2-k)}(g(\bar{f}^{(k)}(y))) = 0.$$

According to Theorem 3.6, f is a triple-cycle permutation over \mathbb{F}_{q^3} . □

C. n -cycle permutations of the form $g(x^{q^i} - x + \delta) + bx$

In [44, Proposition 3], Zheng et al. investigated the permutation property between $g(x^{q^i} - x + \delta) + bx$ and $g(x)^{q^i} - g(x) + bx$. Niu et al. [31] got an involutory version using compositional inverses. In this subsection, we consider the n -cycle property of permutations with the form $g(x^{q^i} - x + \delta) + bx$. Some constructions are also provided.

For their n -cycle properties, we have the following results, similarly with above subsections.

Theorem 3.12. Let \mathbb{F}_{q^m} be the degree m extension of the finite field \mathbb{F}_q and $\delta \in \mathbb{F}_{q^m}$, $g(x) \in \mathbb{F}_{q^m}[x]$. Then $f(x) = g(x^{q^i} - x + \delta) + x$ is an n -cycle permutation over \mathbb{F}_{q^m} if and only if

$$\sum_{k=0}^{n-1} g(h^{(k)}(y)) = 0 \tag{9}$$

holds for any $y \in S_\delta = \{x^{q^i} - x + \delta \mid x \in \mathbb{F}_{q^m}\}$, where $h(y) = g(y)^{q^i} - g(y) + y$ is on S_δ , i is an integer with $1 \leq i \leq m - 1$ and $\ell = \text{gcd}(i, m)$.

Proof. Its proof is similar with that in Theorem 3.6, and thus it is omitted. □

Proposition 3.13. Let m, i be integers with $1 \leq i \leq m - 1$, $\ell = \text{gcd}(i, m)$ and \mathbb{F}_{q^m} be the finite field containing q^m elements. Assume $\delta \in \mathbb{F}_{q^m}$ and nonzero polynomial $g(x) \in \mathbb{F}_{q^m}[x]$ satisfying $g(\mathbb{F}_{q^m}) \subseteq \mathbb{F}_{q^i}$ and $g(S_\delta) \neq \{0\}$, where $S_\delta = \{x^{q^i} - x + \delta \mid x \in \mathbb{F}_{q^m}\}$. Then,

$$f(x) = x + g(x^{q^i} - x + \delta)$$

is an n -cycle permutation over \mathbb{F}_{q^m} if and only if p is a factor of n , where p is the characteristic of \mathbb{F}_{q^m} .

Proof. Its proof follows in a similar manner with that in Proposition 3.7, and thus it is omitted. \square

Corollary 3.14. *Assume integers m, i satisfy $1 \leq i \leq m - 1$. Let $H(x)$ be a nonzero polynomial over \mathbb{F}_{q^m} and $g(x)$ be either $g_1(x) = \text{Tr}_{q^m/q^i}(H(x))$ (with $H(S_\delta) \notin \ker(\text{Tr}_{q^m/q^i})$) or $g_2(x) = H(x)^s$ (with $H(S_\delta) \neq \{0\}$), where positive integer s satisfies $s(q^i - 1) \equiv 0 \pmod{q^m - 1}$. Then, for any $\delta \in \mathbb{F}_{q^m}$,*

$$f(x) = x + g(x^{q^i} - x + \delta)$$

is an n -cycle permutation if and only if p is a factor of n , where p is the characteristic of \mathbb{F}_{q^m} .

Example 3.15. *Let q be a power of 3, integers m, i satisfy $1 \leq i \leq m - 1$, and $s = 1 + q^i + q^{2i} + \dots + q^{m-i}$. For any $\delta \in \mathbb{F}_{q^m}$, $x + (x^{q^i} - x + \delta)^s$ is a triple-cycle permutation of \mathbb{F}_{q^m} , where $c \in \mathbb{F}_{q^m}^* \setminus \{1\}$.*

4. TRIPLE-CYCLE PERMUTATIONS OF THE FORM $x^r h(x^s)$

In this section, we provide triple-cycle permutations of the form $x^r h(x^s)$. First, we recall a lemma and simply derive another one.

Lemma 4.1. [37, Theorem 1] *Let q be a prime power and $f(x) = x^r h(x^s) \in \mathbb{F}_q[x]$, where $s \mid (q - 1)$, $\gcd(r, s) = 1$. Assume that $g(x) = x^r h(x^s)$ is a polynomial on $\mu_\ell = \{x \in \mathbb{F}_q^* \mid x^\ell = 1\}$, where $\ell = (q - 1)/s$. Then, f is a triple-cycle permutation over \mathbb{F}_q if and only if*

- (1) $r^3 \equiv 1 \pmod{s}$ and
- (2) $\varphi(y) = y^{(r^3-1)/s} h(y)^{r^2} h(g(y))^r h(g(g(y))) = 1$ for all $y \in \mu_\ell$.

The lemma below is not hard to obtain.

Lemma 4.2. *Let q be a prime power, $s \mid (q - 1)$, $\gcd(r, s) = 1$ and $r^3 \equiv 1 \pmod{s}$. Assume that $h(x) \in \mathbb{F}_q[x]$ such that $h(y)^s = ay^{v-r}$ holds for any $y \in \mu_\ell = \{x \in \mathbb{F}_q^* \mid x^\ell = 1\}$, where $v^3 \equiv 1 \pmod{\ell}$, $a^{v^2+v+1} = 1$ and $\ell = (q - 1)/s$. Then $f(x) = x^r h(x^s)$ is a triple-cycle permutation over \mathbb{F}_q if and only if for any $y \in \mu_\ell$,*

$$y^{(r^3-1)/s} h(y)^{r^2} h(ay^v)^r h(a^{v+1}y^{v^2}) = 1.$$

Note that if $f(x) \in \mathbb{F}_q[x]$ is a triple-cycle permutation over \mathbb{F}_{q^3} , then so does $f(x)^{q^i}$ for $i \in \{0, 1, 2\}$, according to Lemma 2.3.

Proposition 4.3. *Let $q = 2^{3m}$, where m is a positive integer. Assume that integer k satisfies $7k \equiv 0 \pmod{q - 1}$ and $k \equiv 3 \pmod{7}$. Then,*

$$f(x) = x \left(1 + x^{k(q^2+q+1)} + x^{2k(q^2+q+1)} \right)$$

is a triple-cycle permutation over \mathbb{F}_{q^3} .

Proof. First, we acquire several equations for preparations. Note $7 \mid (q-1)$ by $q = 2^{3m}$. For any $y \in \mathbb{F}_8$, we have

$$\begin{aligned} (1 + y + y^3 + y^5 + y^6)^3 &= (1 + y + y^3 + y^5 + y^6) (1 + y^2 + y^3 + y^5 + y^6) \\ &= 1 + y^2 + y^4, \end{aligned} \quad (10)$$

and

$$\begin{aligned} (1 + y + y^3)^3 &= (1 + y + y^3) (1 + y^2 + y^6) \\ &= 1 + y + y^2 + y^3 + y^4. \end{aligned} \quad (11)$$

Clearly, for any $x \in \mathbb{F}_q^*$, we have $x^k \in \mathbb{F}_8^*$ by $7k \equiv 0 \pmod{q-1}$. Let $\sigma(x) = 1 + x^k + x^{3k} + x^{5k} + x^{6k}$. According to Eq. (10) and Eq. (11) respectively, we obtain that for any $x \in \mathbb{F}_q^*$,

$$\sigma(x)^k = 1 + x^{2k} + x^{4k} \quad (12)$$

and

$$\left(1 + x^{3k} + x^{6k}\right)^k = 1 + x^k + x^{2k} + x^{3k} + x^{4k}, \quad (13)$$

since $k \equiv 3 \pmod{7}$. Then, by raising Eq. (12) to the power of 2, 3, 5 and 6 respectively, we acquire

$$\sigma(x)^{2k} = \left(1 + x^{2k} + x^{4k}\right)^2 = 1 + x^k + x^{4k}, \quad (14)$$

$$\begin{aligned} \sigma(x)^{3k} &= \left(1 + x^{2k} + x^{4k}\right) \left(1 + x^{2k} + x^{4k}\right)^2 \\ &= \left(1 + x^{2k} + x^{4k}\right) \left(1 + x^k + x^{4k}\right) \\ &= 1 + x^{2k} + x^{3k} + x^{5k} + x^{6k}, \end{aligned} \quad (15)$$

$$\begin{aligned} \sigma(x)^{5k} &= \left(1 + x^{2k} + x^{4k}\right)^4 \left(1 + x^{2k} + x^{4k}\right) \\ &= 1 + x^k + x^{3k} + x^{5k} + x^{6k}, \end{aligned} \quad (16)$$

$$\begin{aligned} \sigma(x)^{6k} &= \left(x^{6k} + x^{5k} + x^{3k} + x^{2k} + 1\right)^2 \\ &= 1 + x^{3k} + x^{4k} + x^{5k} + x^{6k}. \end{aligned} \quad (17)$$

And, by raising Eq. (13) to the power of 2, we get

$$\left(1 + x^{3k} + x^{6k}\right)^{2k} = 1 + x^k + x^{2k} + x^{4k} + x^{6k}. \quad (18)$$

After the preparation above, we now prove the theorem by Corollary 4.1. Let $h(x) = 1 + x^k + x^{2k}$ and

$$g(x) = xh(x)^{q^2+q+1} = x(1 + x^k + x^{2k})^{q^2+q+1}. \quad (19)$$

Then, $f(x)$ can be written as $xh(x^{q^2+q+1})$. To apply Corollary 4.1, we will compute $g(g(x))$ and verify $g(g(g(x))) = x$ in the below, for any $x \in \mathbb{F}_q^*$. After that, we verify $\varphi(x) = h(x)h(g(x))h(g(g(x))) = 1$, for any $x \in \mathbb{F}_q^*$.

By expanding Eq. (19), one can obtain for each $x \in \mathbb{F}_q^*$,

$$\begin{aligned} g(x) &= x \left(1 + x^k + x^{2k}\right)^3 = x \left(1 + x^k + x^{2k}\right) \left(1 + x^{2k} + x^{4k}\right) \\ &= x \left(1 + x^k + x^{3k} + x^{5k} + x^{6k}\right). \\ &= x\sigma(x). \end{aligned} \quad (20)$$

Thus, we have

$$g(g(x)) = x\sigma(x) \left(1 + x^k \sigma(x)^k + x^{3k} \sigma(x)^{3k} + x^{5k} \sigma(x)^{5k} + x^{6k} \sigma(x)^{6k}\right). \quad (21)$$

By plugging Eqs. (14), (15), (16) and (17) into Eq. (21), one can arrive at

$$g(g(x)) = x\sigma(x) \left(1 + x^k + x^{6k}\right) = x \left(1 + x^{3k} + x^{6k}\right). \quad (22)$$

By plugging Eq. (22) into $g(x) = x \left(1 + x^k + x^{3k} + x^{5k} + x^{6k}\right)$, one can obtain

$$g(g(g(x))) = x\sigma(x) \left(1 + x^{3k} \sigma(x)^{3k} + x^{6k} \sigma(x)^{6k}\right). \quad (23)$$

After plugging Eqs. (15) and (17) into Eq. (23), we have

$$\begin{aligned} g(g(g(x))) &= x(1 + x^k + x^{3k} + x^{5k} + x^{6k}) \left(1 + x^k + x^{4k}\right) \\ &= x(x^{2k} + x^{4k} + x^{6k} + 1 + x^k + x^{5k} + 1 + x^{2k} + x^{3k} + x^{4k} \\ &\quad + x^k + x^{3k} + x^{5k} + x^{6k} + 1) \\ &= x, \end{aligned}$$

for each $x \in \mathbb{F}_q^*$.

Finally, for each $x \in \mathbb{F}_q^*$, we have

$$\begin{aligned} \varphi(x) &= (1 + x^k + x^{2k})h(x\sigma(x))h\left(x(1 + x^{3k} + x^{6k})\right) \\ &= (1 + x^k + x^{2k}) \left(1 + x^k \sigma(x)^k + x^{2k} \sigma(x)^{2k}\right) \\ &\quad \cdot \left(1 + (x(1 + x^{3k} + x^{6k}))^k + (x(1 + x^{3k} + x^{6k}))^{2k}\right). \end{aligned} \quad (24)$$

By plugging Eqs. (13), (14), (15), (16), (17) and (18) into Eq. (24) and simplifying it, one can obtain

$$\varphi(x) = (1 + x^k + x^{2k}) \left(1 + x^k + x^{5k} + x^{2k} + x^{6k}\right) \left(1 + x^{5k} + x^{6k}\right). \quad (25)$$

After expanding Eq. (25), one will get

$$\begin{aligned} \varphi(x) &= \left(1 + x^k + x^{2k}\right) \left(1 + x^{2k} + x^{3k} + x^{5k} + x^{6k}\right) \\ &= 1 + x^{2k} + x^{3k} + x^{5k} + x^{6k} + x^k + x^{3k} + x^{4k} + x^{6k} + 1 + x^{2k} + x^{4k} + x^{5k} + 1 + x^{8k} \\ &= 1. \end{aligned} \quad (26)$$

Thus, f is a triple-cycle permutation over \mathbb{F}_{q^3} , according to Corollary 4.1. \square

Example 4.4. Let $q = 2^6$. Then $k = 45$ satisfies $7 \times 45 \equiv 0 \pmod{63}$ and $45 \equiv 3 \pmod{7}$. Thus, $f(x) = x(1 + x^{45 \times 4161} + x^{90 \times 4161})$ is a triple-cycle permutation over $\mathbb{F}_{2^{18}}$.

Theorem 4.5. Let q be a prime power. Assume for any $x \in \mu_{q^2+q+1}$, $h(x)^{q-1} = 1$. Then $f(x) = x^q h(x^{q-1})$ is a triple-cycle permutation over \mathbb{F}_{q^3} if and only if $h(x)h(x^q)h(x^{q^2}) = 1$ holds for any $x \in \mu_{q^2+q+1}$.

Proof. The proof is easy by Lemma 4.2, and we omit it. \square

Proposition 4.6. Let $q = 2^{2m}$. Assume $h(x) = 1 + \alpha x^{\frac{q^2+q+1}{3}} + x^{\frac{2q^2+2q+2}{3}}$, where $\alpha \in \mathbb{F}_q$ satisfying $\alpha^3 = 1$. Then $f(x) = x^q h(x^{q-1})$ is a triple-cycle permutation over \mathbb{F}_{q^3} .

Proof. Clearly $3 \mid (q^2 + q + 1)$ by $q = 2^{2m}$. For each $x \in \mu_{q^2+q+1}$, let $y = x^{\frac{q^2+q+1}{3}}$. We have $y^3 = 1$ and $y^q = y$.

Below, we prove that $h(x)^3 = 1$ for any $x \in \mu_{q^2+q+1}$. After expanding and simplifying $(1 + \alpha y + y^2)^3$, we obtain

$$(1 + \alpha y + y^2)^3 = \alpha^2 y + \alpha^3 + \alpha^2 y^2 + \alpha y^2 + \alpha y + 1 + y + y^2 + 1. \quad (27)$$

Eq. (27) equals to

$$(\alpha^2 + \alpha + 1)y^2 + (\alpha^2 + \alpha + 1)y + \alpha^3 = 1. \quad (28)$$

Then, we have $h(x)^{q-1} = 1$ due to $3 \mid (q-1)$. Note $\alpha \in \mathbb{F}_q$. Thus $h(x^q) = h(x)^q = h(x)$, which leads to

$$h(x)h(x^q)h(x^{q^2}) = h(x)^3 = 1. \quad (29)$$

Thus, f is a triple-cycle permutation over \mathbb{F}_{q^3} , according to Theorem 4.5. \square

Theorem 4.7. Let q be a prime power, $\phi(x) \in \mathbb{F}_{q^2}[x]$ and $h(x) = \phi(x) + x^{(v-1)q}\phi(x)^q + \psi(x)$, where $v^3 \equiv 1 \pmod{q+1}$ and $\psi(x)$ satisfying $\psi(x)^{q-1} = x^{v-1}$. Then $f(x) = xh(x^{q-1})$ is a triple-cycle permutation over \mathbb{F}_{q^2} if and only if $h(x)h(x^v)h(x^{v^2}) = 1$ holds for any $x \in \mu_{q+1}$.

Proof. If there exists an $x_0 \in \mu_{q+1}$ such that $h(x_0) = 0$. Then $h(x_0)^3 = 0 \neq 1$. Furthermore, $f(x_0) = x_0 h(x_0^{q-1}) = 0$, thus f is not a triple-cycle permutation.

If for any $x \in \mu_{q+1}$, $h(x) \neq 0$. Then we have

$$h(x)^{q-1} = \frac{\phi(x)^q + x^{(v-1)q}\phi(x) + \psi(x)^q}{\phi(x) + x^{(v-1)q}\phi(x)^q + \psi(x)} = x^{v-1}.$$

This lead to $g(x) = xh(x)^{q-1} = x^v$, which is a triple-cycle permutation over μ_{q+1} . Then by plugging $a = 1, r = 1, v = 1, s = q-1$ and $g(x) = x$ into the condition in Lemma 4.2, we have $f(x)$ is a triple-cycle permutation over \mathbb{F}_{q^2} if and only if $h(x)h(x^v)h(x^{v^2}) = 1$ for any $x \in \mu_{q+1}$. \square

Proposition 4.8. Let $q = 2^{12k-6}$ and $-6t + 12t^2 - 8t^3 \equiv 0 \pmod{q+1}$, where k is a positive integer.

Assume m is an integer such that

$$-3m + 6mt - 4mt^2 \equiv 0 \pmod{q+1}, \quad (30a)$$

$$-m - mt + t + t^2 \equiv 0 \pmod{q+1} \text{ and} \quad (30b)$$

$$13m - 13t \equiv 0 \pmod{q+1} \quad (30c)$$

are all established. Then $f(x) = xh(x^{q-1})$ is a triple-cycle permutation over \mathbb{F}_{q^2} , where

$$h(x) = x^m + x^{mq-2tq} + x^t.$$

Proof. In this proof, first we will derive some useful congruences from Congruences (30a), (30b), (30c). Then, we will further handle these useful congruences (Congruences (30a), (31), (33) and (34)) to obtain Congruences (35), (36), (37) and (38) that can be directly used to prove f being triple-cycle.

We have $13 \mid (q+1)$ by $q = 2^{12k-6}$. By simplifying $2 \times$ Congruence (30b) – Congruence (30a), we have

$$m + 2t - 8mt + 2t^2 + 4mt^2 \equiv 0 \pmod{q+1}. \quad (31)$$

Then, by simplifying $8 \times$ Congruence (30b) + Congruence (30c), we have

$$5t - 5m + 8mt - 8t^2 \equiv 0 \pmod{q+1}. \quad (32)$$

After simplifying $(-2) \times$ Congruence (30a) + Congruence (32), one can obtain

$$m + 5t - 4mt - 8t^2 + 8mt^2 \equiv 0 \pmod{q+1}. \quad (33)$$

By simplifying – Congruence (33) – Congruence (30b), we get

$$m - 7t + 6mt + 6t^2 - 8mt^2 \equiv 0 \pmod{q+1}. \quad (34)$$

After obtaining Congruences (30a), (31), (33) and (34), we will further handle them below. Assume $v = 1 - 2t$. Then, $v^2 + v + 1 = 3 - 6t + 4t^2$ and according to Congruence (30a), we arrive at

$$\left\{ \begin{array}{l} m(v^2 + v + 1) \equiv v(v^2 + v + 1) \equiv -3m + 6mt - 4mt^2 \equiv 0 \pmod{q+1}, \\ -mv^2 - m + tv + v^2 - v \equiv mv + tv^2 + t \pmod{q+1}, \\ -mv - m + tv^2 - v^2 + 1 \equiv mv^2 + tv + t \pmod{q+1}, \\ mv^2 + mv + t \equiv -m + tv^2 + tv - v + 1 \pmod{q+1}, \\ -mv^2 - mv + t + v - 1 \equiv m + tv^2 + tv \pmod{q+1}, \\ mv + m + tv^2 \equiv -mv^2 + tv + t + v^2 - 1 \pmod{q+1} \text{ and} \\ -mv + tv^2 + t - v^2 + v \equiv mv^2 + m + tv \pmod{q+1}. \end{array} \right. \quad (35)$$

According to Congruence (31), one can get

$$-mv + m + tv^2 - v^2 + v \equiv mv^2 + mv - m - v + 1. \quad (36)$$

According to Congruence (33), we obtain

$$mv^2 - mv + m - v^2 + v \equiv -mv^2 + mv + t + v^2 - 1. \quad (37)$$

According to Congruence (34), we have

$$-mv^2 + mv + m + v^2 - 1 \equiv mv^2 - m + tv - v + 1. \quad (38)$$

Finally, we expand $h(x)h(x^v)h(x^{v^2})$ for any $x \in \mu_{q+1}$ and get

$$\begin{aligned} & \left(x^m + x^{mq+(v-1)q} + x^t\right) \left(x^{mv} + x^{(mq+(v-1)q)v} + x^{tv}\right) \left(x^{mv^2} + x^{(mq+(v-1)q)v^2} + x^{tv^2}\right) \\ = & x^{-mv^2-mv+t+v-1} + x^{-mv^2+mv+t+v^2-1} + x^{-mv^2+m+tv+v^2-1} + x^{-mv^2+tv+t+v^2-1} \\ & + x^{-mv^2-m+tv+v^2-v} + x^{mv^2+mv+t} + x^{mv^2+m+tv} + x^{mv^2+tv+t} + x^{mv^2-m+tv-v+1} \\ & + x^{mv^2-mv+t-v^2+v} + x^{mv+m+tv^2} + x^{mv+tv^2+t} + x^{mv-m+tv^2-v+1} + x^{m+tv^2+tv} \\ & + x^{-m+tv^2+tv-v+1} + x^{-mv-m+tv^2-v^2+1} + x^{-mv+m+tv^2-v^2+v} + x^{-mv+tv^2+t-v^2+v} \\ & + x^{-mv^2-mv-m} + x^{-mv^2-mv+m+v-1} + x^{-mv^2+mv+m+v^2-1} + x^{-mv^2+mv-m+v^2-v} \\ & + x^{mv^2+mv+m} + x^{mv^2+mv-m-v+1} + x^{mv^2-av-m-v^2+1} + x^{mv^2-mv+m-v^2+v} + x^{tv^2+tv+t} \\ = & 1, \end{aligned}$$

where the last equation holds by Congruences (35), (36), (37) and (38). Thus f is a triple-cycle permutation. \square

Example 4.9. Let $q = 2^6, t = 25, m = 5$ in Proposition 4.8. Then Congruences (30a), (30b) and (30c) are all satisfied. Then, according to Proposition 4.8, $f(x) = xh(x^{q-1})$ is a triple-cycle permutation over $\mathbb{F}_{2^{12}}$, where $h(x) = x^5 + x^{45} + x^{25}$. This is also verified by Magma.

In the end of this paper, we provide an explicit triple-cycle permutation of the form $x^t + c\text{Tr}_{q^m/q}(x^s)$.

Proposition 4.10. Let $q = 2^{2k}$, where k is a positive integer. Put $\theta \in \mathbb{F}_q$ satisfying $\theta^3 = 1, \theta \neq 1$. Then, the compositional inverse of

$$f(x) = x + \theta \text{Tr}_{q^3/q} \left(x^{\frac{q^2+q}{2}} \right)$$

is $f^{-1}(x) = x + \theta^2 \text{Tr}_{q^3/q} \left(x^{\frac{q^2+q}{2}} \right)$. Furthermore, f is a triple-cycle permutation over \mathbb{F}_{q^3} .

Proof. Clearly $\theta + \theta^2 = 1$ and $\theta^{q/2} = \theta^2$. Then, after expanding $\left(x + \theta \text{Tr}_{q^3/q} \left(x^{\frac{q^2+q}{2}} \right) \right)^{\frac{q^2+q}{2}}$ and simplifying

it, we have

$$\begin{aligned} \left(x + \theta \operatorname{Tr}_{q^3/q}(x^{\frac{q^2+q}{2}})\right)^{\frac{q^2+q}{2}} &= \left(x^{q^2/2} + \theta^{q^2/2} \operatorname{Tr}_{q^3/q}(x^{\frac{q^2+q}{2}})^{q^2/2}\right) \left(x^{q/2} + \theta^{q/2} \operatorname{Tr}_{q^3/q}(x^{\frac{q^2+q}{2}})^{q/2}\right) \\ &= x^{\frac{q^2+q}{2}} + x^{q^2/2} \theta^2 \operatorname{Tr}_{q^3/q}(x^{\frac{q^2+q}{2}})^{q/2} + x^{q/2} \theta^2 \operatorname{Tr}_{q^3/q}(x^{\frac{q^2+q}{2}})^{q/2} \\ &\quad + \theta \operatorname{Tr}_{q^3/q}(x^{\frac{q^2+q}{2}}). \end{aligned} \quad (39)$$

It is clear that

$$\operatorname{Tr}_{q^3/q}(x^{q^2/2} + x^{q/2}) = 0.$$

Thus,

$$\begin{aligned} \operatorname{Tr}_{q^3/q} \left(\left(x + \theta \operatorname{Tr}_{q^3/q}(x^{\frac{q^2+q}{2}})\right)^{\frac{q^2+q}{2}} \right) &= \operatorname{Tr}_{q^3/q} \left(x^{\frac{q^2+q}{2}} + \theta \operatorname{Tr}_{q^3/q}(x^{\frac{q^2+q}{2}}) \right) \\ &= \operatorname{Tr}_{q^3/q}(x^{\frac{q^2+q}{2}}) + \theta \operatorname{Tr}_{q^3/q}(x^{\frac{q^2+q}{2}}). \end{aligned} \quad (40)$$

We consider $f(f(x))$ for any $x \in \mathbb{F}_{q^3}$. After plugging Eq. (40) into

$$f(f(x)) = x + \theta \operatorname{Tr}_{q^3/q}(x^{\frac{q^2+q}{2}}) + \theta \operatorname{Tr}_{q^3/q} \left(\left(x + \theta \operatorname{Tr}_{q^3/q}(x^{\frac{q^2+q}{2}})\right)^{\frac{q^2+q}{2}} \right),$$

we have

$$f(f(x)) = x + \theta^2 \operatorname{Tr}_{q^3/q}(x^{\frac{q^2+q}{2}}). \quad (41)$$

Then, we simplify $f(f(f(x)))$ for any $x \in \mathbb{F}_{q^3}$ below. By plugging Eq. (40) into

$$f(f(f(x))) = x + \theta \operatorname{Tr}_{q^3/q}(x^{\frac{q^2+q}{2}}) + \theta^2 \operatorname{Tr}_{q^3/q} \left(\left(x + \theta \operatorname{Tr}_{q^3/q}(x^{\frac{q^2+q}{2}})\right)^{\frac{q^2+q}{2}} \right),$$

one can obtain

$$\begin{aligned} f(f(f(x))) &= x + \theta \operatorname{Tr}_{q^3/q}(x^{\frac{q^2+q}{2}}) + \theta^2 \left(\operatorname{Tr}_{q^3/q}(x^{\frac{q^2+q}{2}}) + \theta \operatorname{Tr}_{q^3/q}(x^{\frac{q^2+q}{2}}) \right) \\ &= x + \theta \operatorname{Tr}_{q^3/q}(x^{\frac{q^2+q}{2}}) + \theta^2 \operatorname{Tr}_{q^3/q}(x^{\frac{q^2+q}{2}}) + \operatorname{Tr}_{q^3/q}(x^{\frac{q^2+q}{2}}) \\ &= x. \end{aligned}$$

Thus, $f^{-1}(x) = x + \theta^2 \operatorname{Tr}_{q^3/q}(x^{\frac{q^2+q}{2}})$, and f is a triple-cycle permutation over \mathbb{F}_{q^3} . \square

REFERENCES

- [1] Amir Akbary, Dragos Ghioca, and Qiang Wang. On constructing permutations of finite fields. *Finite Fields and Their Applications*, 17(1):51–67, 2011.
- [2] Nurdagül Anbar, Almasa Odžak, Vandita Patel, Luciane Quoos, Anna Somoza, and Alev Topuzoğlu. On the Carlitz rank of permutation polynomials over finite fields: recent developments. *Women in numbers Europe II*, pages 39–55, 2018.
- [3] Paulo Barreto. The Anubis block cipher. *NESSIE*, 2000.

- [4] Paulo Barreto and Vincent Rijmen. The Khazad legacy-level block cipher. *Primitive submitted to NESSIE*, 97, 2000.
- [5] Daniele Bartoli. Hasse-Weil type theorems and relevant classes of polynomial functions. *Surveys in Combinatorics 2021*, 470:43, 2021.
- [6] Daniele Bartoli and Marco Timpanella. A family of permutation trinomials over \mathbb{F}_{q^2} . *Finite Fields and Their Applications*, 70:101781, 2021.
- [7] Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knezevic, Lars R Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, et al. Prince—a low-latency block cipher for pervasive computing applications. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 208–225. Springer, 2012.
- [8] Anne Canteaut and Joëlle Roué. On the behaviors of affine equivalent S-boxes regarding differential and linear attacks. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 45–74. Springer, 2015.
- [9] Pascale Charpin and Gohar Kyureghyan. Monomial functions with linear structure and permutation polynomials. In *Finite fields: theory and applications*, volume 518, pages 99–111. AMS Providence, RI, USA, 2010.
- [10] Pascale Charpin, Sihem Mesnager, and Sumanta Sarkar. Involutions over the Galois Field \mathbb{F}_{2^n} . *IEEE Transactions on Information Theory*, 62(4):2266–2276, 2016.
- [11] Yuting Chen, Liqi Wang, and Shixin Zhu. On the constructions of n -cycle permutations. *Finite Fields and Their Applications*, 73:101847, 2021.
- [12] Robert S. Coulter and Sihem Mesnager. Bent functions from involutions over \mathbb{F}_{2^n} . *IEEE Transactions on Information Theory*, 64(4):2979–2986, 2018.
- [13] Joan Daemen and Vincent Rijmen. *The design of Rijndael: AES—the advanced encryption standard*. Springer Science & Business Media, 2013.
- [14] Cunsheng Ding, Longjiang Qu, Qiang Wang, Jin Yuan, and Pingzhi Yuan. Permutation trinomials over finite fields with even characteristic. *SIAM Journal on Discrete Mathematics*, 29(1):79–92, 2015.
- [15] Robert Gallager. Low-density parity-check codes. *IRE Transactions on Information Theory*, 8(1): 21–28, 1962.
- [16] Daniel Gerike and Gohar M. Kyureghyan. Permutations on finite fields with invariant cycle structure on lines. *Designs, Codes and Cryptography*, 88(9):1723–1740, 2020.
- [17] Rohit Gupta and RK Sharma. Some new classes of permutation trinomials over finite fields with even characteristic. *Finite Fields and Their Applications*, 41:89–96, 2016.
- [18] Xiangdong Hou. Permutation polynomials over finite fields—a survey of recent advances. *Finite Fields and Their Applications*, 32:82–119, 2015.
- [19] Xiangdong Hou, Ziran Tu, and Xiangyong Zeng. Determination of a class of permutation trinomials in characteristic three. *Finite Fields and Their Applications*, 61:101596, 2020.
- [20] Gohar Kyureghyan and Michael Zieve. Permutation polynomials of the form $x + \gamma\text{Tr}(x^k)$. In *Con-*

temporary developments in finite fields and applications, pages 178–194. World Scientific Singapore, 2016.

- [21] Kangquan Li, Longjiang Qu, and Xi Chen. New classes of permutation binomials and permutation trinomials over finite fields. *Finite Fields and Their Applications*, 43:69–85, 2017.
- [22] Kangquan Li, Longjiang Qu, Xi Chen, and Chao Li. Permutation polynomials of the form $cx + \text{Tr}_{q^n/q}(x^a)$ and permutation trinomials over finite fields with even characteristic. *Cryptography and Communications*, 10(3):531–554, 2018.
- [23] Kangquan Li, Longjiang Qu, Chao Li, and Shaojing Fu. New permutation trinomials constructed from fractional polynomials. *Acta Arithmetica*, 183:101–116, 2018.
- [24] Lisha Li, Qiang Wang, Yunge Xu, and Xiangyong Zeng. Several classes of complete permutation polynomials with Niho exponents. *Finite Fields and Their Applications*, 72:101831, 2021.
- [25] Nian Li. On two conjectures about permutation trinomials over $\mathbb{F}_{3^{2k}}$. *Finite Fields and Their Applications*, 47:1–10, 2017.
- [26] Nian Li and Tor Helleseeth. Several classes of permutation trinomials from Niho exponents. *Cryptography and Communications*, 9(6):693–705, 2017.
- [27] Nian Li and Tor Helleseeth. New permutation trinomials from Niho exponents over finite fields with even characteristic. *Cryptography and Communications*, 11(1):129–136, 2019.
- [28] Nian Li and Xiangyong Zeng. A survey on the applications of Niho exponents. *Cryptography and Communications*, 11(3):509–548, 2019.
- [29] Xianping Liu, Yuan Chen, Yunge Xu, and Zhimin Sun. Triple-cycle permutations over finite fields of characteristic two. *International Journal of Foundations of Computer Science*, 30(2):275–292, 2019.
- [30] Gary Lee Mullen and Qiang Wang. Permutation polynomials of one variable. In *Handbook of Finite Fields*, pages 215–230. CRC, 2014.
- [31] Tailin Niu, Kangquan Li, Longjiang Qu, and Qiang Wang. New constructions of involutions over finite fields. *Cryptography and Communications*, 12(2):165–185, 2020.
- [32] Tailin Niu, Kangquan Li, Longjiang Qu, and Qiang Wang. Finding compositional inverses of permutations from the AGW criterion. *IEEE Transactions on Information Theory*, 67(8):4975–4985, 2021.
- [33] Ziran Tu and Xiangyong Zeng. Two classes of permutation trinomials with Niho exponents. *Finite Fields and Their Applications*, 53:99–112, 2018.
- [34] Aleksandr Tuxanidy and Qiang Wang. On the inverses of some classes of permutations of finite fields. *Finite Fields and Their Applications*, 28:244–281, 2014.
- [35] Qiang Wang. Polynomials over finite fields: an index approach. In *Combinatorics and Finite Fields. Difference Sets, Polynomials, Pseudorandomness and Applications*, pages 319–348. Degruyter, 2019.
- [36] Danyao Wu, Pingzhi Yuan, Cunsheng Ding, and Yuzhen Ma. Permutation trinomials over \mathbb{F}_{2^m} . *Finite Fields and Their Applications*, 46:38–56, 2017.
- [37] Mengna Wu, Chengju Li, and Zilong Wang. Characterizations and constructions of triple-cycle

- permutations of the form $x^r h(x^s)$. *Designs, Codes and Cryptography*, 88(10):2119–2132, 2020.
- [38] Guangkui Xu, Xiwang Cao, and Jingshui Ping. Some permutation pentanomials over finite fields with even characteristic. *Finite Fields and Their Applications*, 49:212–226, 2018.
- [39] Jin Yuan and Cunsheng Ding. Four classes of permutation polynomials of \mathbb{F}_{2^m} . *Finite fields and their applications*, 13(4):869–876, 2007.
- [40] Zhengbang Zha and Lei Hu. Some classes of permutation polynomials of the form $(x^{p^m} - x + \delta)^s + x$ over \mathbb{F}_p^{2m} . *Finite Fields and Their Applications*, 40:150–162, 2016.
- [41] Zhengbang Zha, Lei Hu, and Shuqin Fan. Further results on permutation trinomials over finite fields with even characteristic. *Finite Fields and Their Applications*, 45:43–52, 2017.
- [42] Zhengbang Zha, Lei Hu, and Zhizheng Zhang. Permutation polynomials of the form $x + \gamma \text{Tr}_q^{q^n}(h(x))$. *Finite Fields and Their Applications*, 60:101573, 2019.
- [43] Dabin Zheng, Mu Yuan, Nian Li, Lei Hu, and Xiangyong Zeng. Constructions of involutions over finite fields. *IEEE Transactions on Information Theory*, 65(12):7876–7883, 2019.
- [44] Dabin Zheng, Mu Yuan, and Long Yu. Two types of permutation polynomials with special forms. *Finite Fields and Their Applications*, 56:1–16, 2019.
- [45] Lijing Zheng, Haibin Kan, Jie Peng, and Deng Tang. Two classes of permutation trinomials with Niho exponents. *Finite Fields and Their Applications*, 70:101790, 2021.