

The compositional inverses of three classes of permutation polynomials over finite fields

Danyao Wu^{1*} and Pingzhi Yuan²

^{1*}School of Computer Science and Technology, Dongguan University of Technology, Dongguan, 523808, China.

²School of Mathematics, South China Normal University, Guangzhou, 510631, China.

*Corresponding author(s). E-mail(s): wudanyao111@163.com;
Contributing authors: yuanpz@scnu.edu.cn;

Abstract

Recently, P. Yuan presented a local method to find permutation polynomials and their compositional inverses over finite fields. The work of P. Yuan inspires us to compute the compositional inverses of three classes of the permutation polynomials: (a) the permutation polynomials of the form $\mathbf{a}x^q + \mathbf{b}x + (x^q - x)^k$ over \mathbb{F}_{q^2} , where $\mathbf{a} + \mathbf{b} \in \mathbb{F}_q^*$ or $\mathbf{a}^q = \mathbf{b}$; (b) the permutation polynomials of the forms $\mathbf{f}(x) = -x + x^{(q^2+1)/2} + x^{(q^3+q)/2}$ and $\mathbf{f}(x) + x$ over \mathbb{F}_{q^3} ; (c) the permutation polynomial of the form $\mathbf{A}^m(x) + \mathbf{L}(x)$ over \mathbb{F}_{q^n} , where $\mathbf{Im}(\mathbf{A}(x))$ is a vector space with dimension 1 over \mathbb{F}_q and $\mathbf{L}(x)$ is not a linearized permutation polynomial.

Keywords: finite fields, polynomials, permutation polynomials, compositional inverses, local method

MSC Classification: 11T06; 12E10

1 Introduction

Let \mathbb{F}_q be the finite field with q elements and \mathbb{F}_q^* denote the multiplicative group with the nonzero element in \mathbb{F}_q , where q is a prime power. Let $\mathbb{F}_q[x]$ be the ring of polynomials in a single indeterminate x over \mathbb{F}_q . A polynomial $f \in \mathbb{F}_q[x]$ is called a *permutation polynomial* (PP) of \mathbb{F}_q if its associated polynomial mapping $f : c \mapsto$

$f(x)$ from \mathbb{F}_q to itself is bijective. A polynomial $f(x) \in \mathbb{F}_q[x]$ is called a complete permutation polynomial (CPP) if both $f(x)$ and $f(x) + x$ are permutations of \mathbb{F}_q . The unique polynomial denoted by $f^{-1}(x)$ over \mathbb{F}_q such that $f(f^{-1}(x)) \equiv f^{-1}(f(x)) \equiv x \pmod{x^q - x}$ is called the compositional inverse of $f(x)$. Furthermore, $f(x)$ is called an involution when $f^{-1}(x) = f(x)$.

The study of permutation polynomials and their compositional inverses over finite fields in terms of their coefficients is a classical and difficult subject which attracts people's interest partially due to their wide applications in coding theory [1–3], cryptography [4, 5], combinatorial design theory [6], and other areas of mathematics and engineering [7, 8]. For instance, in block ciphers, a permutation polynomial is usually used as an S-box to build the confusion layer and the compositional inverse of S-box comes into picture while decrypting the cipher. Both the permutation polynomial and its compositional inverse are implemented. Therefore, the explicit and efficient permutation polynomial and its compositional inverse are desired for designers. Indeed, the better understanding of permutation polynomials and their compositional inverses in explicit format is not only meaningful, but also important for these applications.

In general, it is difficult to discover new classes of permutation polynomials. In 2011, Akbrary, Ghioca and Wang [9] proposed a powerful method called the AGW criterion for constructing permutation polynomials—that is, construct mappings $\bar{\lambda}(x)$, $\lambda(x)$, $h(x)$ that satisfy certain condition such that $\bar{\lambda}(x) \circ f(x) = h(x) \circ \lambda(x)$, to discuss whether $f(x)$ is a permutation polynomial. Many classes of permutation polynomials have been constructed up to now, see [9–18]. Computing the coefficients of the compositional inverse of a permutation polynomial seems to be even more difficult, except for several classical classes such as monomials, linearized polynomials, Dickson polynomials, which have nice structure. Wang [19] surveyed on the results and methods in the study of compositional inverses of permutation polynomials over finite fields. More recent results are included in [20–25] for more details.

The coauthor gave the dual diagram of the AGW criterion [25] and a local method [26] to find permutation polynomials and their compositional inverses, which the latter result proposed the framework to obtain the permutation polynomials and their compositional inverses. This inspires us to merge these two conclusions to study the compositional inverses of permutation polynomials, as established by the AGW criterion. In this paper, we will examine the compositional inverses of permutation polynomials of the form $ax^q + bx + (x^q - x)^k$ over \mathbb{F}_{q^2} as discussed in [15].

Furthermore, the authors [20] considered three classes of permutation trinomials over \mathbb{F}_{q^3} using the local method. Using the techniques outlined in [20], we will investigate the compositional inverse of permutation polynomials of the form $f(x) = -x + x^{(q^2+1)/2} + x^{(q^3+q)/2}$ over \mathbb{F}_{q^3} .

Based on the local method, the authors [23] examined a class of permutation polynomials of the form

$$A_1^{m_1}(x) + \sum_{i=2}^n u_i A_i^{m_i}(x) \quad (1)$$

and their compositional inverses over \mathbb{F}_{q^n} , where $\text{Im}(A_i(x))$ is a vector space with dimension 1 over \mathbb{F}_q and $u_i \in \mathbb{F}_{q^n}$, m_i are a positive integers for $i = 1, 2, \dots, n$. Hasan and Kaur [27] considered six specific forms given by (1) over \mathbb{F}_{q^3} , setting $m_1 = m_2 =$

$u_2 = u_3 = 1$ and $A_3(x) = x + x^q + x^{q^2}$. In this case, we have $\sharp\text{Im}(A_1(x) + A_2(x)) \leq \sharp\text{Im}(A_1(x)) \cdot \sharp\text{Im}(A_2(x)) = q^2$, indicating that $A_1(x) + A_2(x)$ does not permute \mathbb{F}_{q^3} . In this paper, we refine the result of Hasan and Kaur [27] by considering a class of permutation polynomials of the form

$$A^m(x) + L(x),$$

and its compositional inverse over \mathbb{F}_{q^n} , where $\text{Im}(A(x))$ is a vector space with dimension 1 over \mathbb{F}_q and $L(x)$ is not a linearized permutation polynomial.

The remainder of this paper is organized as follows. In Section 2, some basic concepts are introduced and the local method is presented which is used in the sequels. In Section 3, we the compositional inverses of permutation polynomials of the form $ax^q + bx + (x^q - x)^k$ over \mathbb{F}_{q^2} . In Section 4, we investigate the compositional inverses of the permutation polynomials of the forms $f(x) = -x + x^{(q^2+1)/2} + x^{(q^3+q)/2}$ and $f(x) + x$ over \mathbb{F}_{q^3} . In Section 5, we study the permutation behavior of the form $A^m(x) + L(x)$ and its compositional inverse over \mathbb{F}_{q^n} , where $\text{Im}(A(x))$ is a vector space with dimension 1 over \mathbb{F}_q and $L(x)$ is not a linearized permutation polynomial.

2 Preliminaries

The following lemma was developed by Akbary, Ghioca and Wang [9].

Lemma 1. [9, AGW criterion] *Let A, S and \bar{S} be finite sets with $\sharp S = \sharp \bar{S}$, and let $f(x) : A \rightarrow A$, $h(x) : S \rightarrow \bar{S}$, $\lambda(x) : A \rightarrow S$, and $\bar{\lambda}(x) : A \rightarrow \bar{S}$ be maps such that $\bar{\lambda}(x) \circ f(x) = h(x) \circ \lambda(x)$. If both $\lambda(x)$ and $\bar{\lambda}(x)$ are surjective, then the following statements are equivalent:*

- (i) $f(x)$ is bijective (a permutation of A); and
- (ii) $h(x)$ is bijective from S to \bar{S} and $f(x)$ is injective on $\lambda^{-1}(s)$ for each $s \in S$.

$$\begin{array}{ccc} A & \xrightarrow{f(x)} & A \\ \lambda(x) \downarrow & & \downarrow \bar{\lambda}(x) \\ S & \xrightarrow{h(x)} & \bar{S} \end{array}$$

We give the dual diagram of the AGW criterion.

Lemma 2. [25, Theorem 2.6] *Let the notations be defined as in Lemma 1. If $f(x) : A \rightarrow A$ is a bijection, $f^{-1}(x)$ and $h^{-1}(x)$ are the compositional inverses of $f(x)$ and $h(x)$, respectively, then we have*

$$\lambda(x) \circ f^{-1}(x) = h^{-1}(x) \circ \bar{\lambda}(x),$$

i.e., the following diagram commutes

$$\begin{array}{ccc} A & \xrightarrow{f^{-1}(x)} & A \\ \bar{\lambda}(x) \downarrow & & \downarrow \lambda(x) \\ \bar{S} & \xrightarrow{h^{-1}(x)} & S \end{array}$$

Yuan [26] presented a local method to find the permutation polynomials and their compositional inverses over finite fields. We will use the local method frequently.

Lemma 3. [26, Theorem 2.2] *Let q be a prime power and $f(x)$ be a polynomial over \mathbb{F}_q . Then $f(x)$ is a permutation polynomial over \mathbb{F}_q if and only if there exist nonempty finite subsets S_i , $i = 1, 2, \dots, t$ of \mathbb{F}_q and maps $\psi_i(x) : \mathbb{F}_q \rightarrow S_i$, $i = 1, 2, \dots, t$ such that $\psi_i(x) \circ f(x) = \varphi_i(x)$, $i = 1, 2, \dots, t$ and $x = F(\varphi_1(x), \varphi_2(x), \dots, \varphi_t(x))$, where $F(x_1, x_2, \dots, x_t) \in \mathbb{F}_q[x_1, x_2, \dots, x_t]$. Moreover, the compositional inverse of $f(x)$ is given by*

$$f^{-1}(x) = F(\psi_1(x), \psi_2(x), \dots, \psi_t(x)).$$

Next, we will give a result about linearized permutation polynomial over \mathbb{F}_{q^n} . It is well-known that $L(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \in \mathbb{F}_{q^n}[x]$ is a permutation polynomial if and only if the associated Dickson matrix

$$D = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1}^q & a_0^q & \cdots & a_{n-2}^q \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{q^{n-1}} & a_2^{q^{n-1}} & \cdots & a_0^{q^{n-1}} \end{pmatrix}$$

is non-singular.

Wu and Liu [28] obtained the compositional inverse of a linearized permutation polynomial over \mathbb{F}_{q^n} . Recently, the authors also obtained such result in [24] by the local method.

Lemma 4. [24, 28] *Let $L(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \in \mathcal{D}_n(\mathbb{F}_{q^n})$ be a linearized permutation polynomial and D_L be its associated Dickson matrix. Then*

$$L^{-1}(x) = (\det(D_L))^{-1} \sum_{i=0}^{n-1} \bar{a}_i x^{q^i},$$

where \bar{a}_i is the $(i, 0)$ -th cofactor of D_L , and the determinant of D_L is $\det(D_L) = a_0 \bar{a}_0 + \sum_{i=1}^{n-1} a_{n-i}^{q^i} \bar{a}_i$.

3 The compositional inverses of the PPs of the form $ax^q + bx + (x^q - x)^k$ over \mathbb{F}_{q^2}

Yuan [15] studied the permutation behavior of the polynomials of the form $ax^q + bx + (x^q - x)^k$ over \mathbb{F}_{q^2} by applying the AGW criterion and gave the following result.

Theorem 1. [15, Theorem 6.4] Let q be a prime power.

(a) If $k \geq 2$ is an even integer or k is odd and q is even, then $f_{a,b,k}(x) = ax^q + bx + (x^q - x)^k$, $a, b \in \mathbb{F}_{q^2}$ with $a + b \in \mathbb{F}_q^*$ permutes \mathbb{F}_{q^2} if and only if $b \neq a^q$.

(b) If k and q are odd positive integers, then $f_{a,k}(x) = ax^q + a^q x + (x^q - x)^k$, $a \in \mathbb{F}_{q^2}^*$ and $a + a^q \neq 0$ permutes \mathbb{F}_{q^2} if and only if $\gcd(k, q-1) = 1$.

We will compute the compositional inverse of $f_{a,b,k}(x)$ and $f_{a,k}(x)$ in Theorem 1 by the dual diagram of the AGW criterion and the local method. We give a lemma at first.

Lemma 5. Let q be an odd prime power and k be an odd positive integer. Let $S = \{\alpha^q - \alpha \mid \alpha \in \mathbb{F}_{q^2}\}$ and $\bar{S} = \{-2s^k \mid s \in S\}$ be two subsets of \mathbb{F}_{q^2} . Assume that the polynomial $h(x) = -2x^k$ is a polynomial from S to \bar{S} . If there exist two integers u, v such that $uk + v(q-1) = 1$, then the compositional inverse of $h(x)$ from \bar{S} to S is given by

$$h^{-1}(x) = (-1)^v (-2)^{-u} x^u.$$

Proof. Since $\alpha^q - \alpha = 0$ if $\alpha \in \mathbb{F}_q$, and $\alpha^q - \alpha \neq 0$ if $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, we have $S = \{\alpha^q - \alpha \mid \alpha \in \mathbb{F}_{q^2}\} = \{\alpha^q - \alpha \mid \alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q\} \cup \{0\}$. Moreover, Since q is odd, we have

$$(x^q - x)^{q-1} = \begin{cases} 0, & \text{if } x \in \mathbb{F}_q, \\ -1, & \text{if } x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q, \end{cases} \quad (2)$$

and so for any $x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, we obtain

$$\begin{aligned} ((-1)^v (-2)^{-u} x^u) \circ h(x^q - x) &= ((-1)^v (-2)^{-u} x^u) \circ (-2(x^q - x)^k) \\ &= (-1)^v (x^q - x)^{uk} \\ &= (x^q - x)^{v(q-1)+uk} \\ &= x^q - x \end{aligned}$$

as $uk + v(q-1) = 1$. Moreover, The value of $(-1)^v (-2)^{-u} x^u$ at $x = 0$ is also equal to zero. Hence, the compositional inverse of $h(x)$ is

$$h^{-1}(x) = (-1)^v (-2)^{-u} x^u.$$

We are done. □

Theorem 2. (i) Using the notations as in Theorem 1 (a). If the polynomial $f_{a,b,k}(x) = ax^q + bx + (x^q - x)^k$ permutes \mathbb{F}_{q^2} , then the compositional inverse of $f_{a,b,k}(x)$ over \mathbb{F}_{q^2} is given by

$$f_{a,b,k}^{-1}(x) = (a+b)^{-1} ((b-a^q)^{-k} (x^q - x)^k - a(b-a^q)^{-1} (x^q - x) - x).$$

(ii) Using the notations as in Theorem 1 (b). If the polynomial $f_{a,k}(x) = ax^q + a^q x + (x^q - x)^k$ permutes \mathbb{F}_{q^2} , then the compositional inverse of $f_{a,k}(x)$ over \mathbb{F}_{q^2} is given by

$$f_{a,k}^{-1}(x) = (a+a^q)^{-1} ((-1)^{kv} (-2)^{-ku} (x^q - x)^{ku} - (-1)^v (-2)^{-u} a(x^q - x)^u - x),$$

where u, v are intergers with $uk + v(q - 1) = 1$.

Proof. (i) As it have been shown in [15] that

$$(x^q - x) \circ f_{a,b,k} = (b - a^q)x \circ (x^q - x),$$

we have

$$x^q - x = (b - a^q)^{-1}x \circ (x^q - x) \circ f_{a,b,k}$$

by Lemma 2.

Let $\psi_1(x) = x^q - x = (b - a^q)^{-1}x \circ (x^q - x) \circ f_{a,b,k}$, $\psi_2(x) = f_{a,b,k}(x)$, $\varphi_1(x) = (b - a^q)^{-1}(x^q - x)$, and $\varphi_2(x) = x$. Then we have the system of the equations

$$\begin{cases} ax^q + bx &= \psi_1^k(x) - \psi_2(x), \\ x^q - x &= \psi_1(x). \end{cases}$$

By eliminating the indeterminate x^q using the above system, we obtain

$$x = (a + b)^{-1} (\psi_1^k(x) - \psi_2(x) - a\psi_1(x)).$$

It follows from Lemma 3 that the compositional inverse of $f_{a,b,k}(x)$ over \mathbb{F}_{q^2} is given by

$$f_{a,b,k}^{-1}(x) = (a + b)^{-1} ((b - a^q)^{-k}(x^q - x)^k - a(b - a^q)^{-1}(x^q - x) - x).$$

(ii) Let $S = \{\alpha^q - \alpha \mid \alpha \in \mathbb{F}_{q^2}\}$, $\bar{S} = \{-2s^k \mid s \in S\}$ be two subsets of \mathbb{F}_{q^2} and $h(x) = -2x^k$ be a polynomial from S to \bar{S} . As it have been shown in [15] that

$$(x^q - x) \circ f_{a,k} = h(x) \circ (x^q - x),$$

we have

$$x^q - x = h^{-1}(x) \circ (x^q - x) \circ f_{a,k}$$

according to Lemma 2.

Let $\psi_1(x) = x^q - x = h^{-1}(x) \circ (x^q - x) \circ f_{a,k}$, $\psi_2(x) = f_{a,k}(x)$, $\varphi_1(x) = h^{-1}(x) \circ (x^q - x)$, and $\varphi_2(x) = x$. Then we have the system of the equations

$$\begin{cases} ax^q + a^q x &= \psi_1^k(x) - \psi_2(x), \\ x^q - x &= \psi_1(x). \end{cases}$$

By eliminating the indeterminate x^q using the above system, we obtain

$$x = (a + a^q)^{-1} (\psi_1^k(x) - \psi_2(x) - a\psi_1(x)).$$

It follows from Lemmas 3 and 5 that the compositional inverse of $f_{a,k}(x)$ over \mathbb{F}_{q^2} is given by

$$f_{a,k}^{-1}(x) = (a + a^q)^{-1} ((-1)^{kv}(-2)^{-ku}(x^q - x)^{ku} - (-1)^v(-2)^{-u}a(x^q - x)^u - x).$$

□

4 The compositional inverse of a class of CPP over \mathbb{F}_{q^3}

Ma et al. [29] studied a class of complete permutation polynomial and gave the following result.

Theorem 3. [29, Theorem 4.1] *Let q be an odd prime power, $f(x) = -x + x^{(q^2+1)/2} + x^{(q^3+q)/2}$ is a CPP over \mathbb{F}_{q^3} .*

To compute the composition inverse of $f(x)$ and $f(x)$ in Theorem 3, we give a lemma first.

Lemma 6. *Let q be an odd prime. For any $a \in \mathbb{F}_{q^3}^*$, the unique solution of the equation $a^q x^q + a^{q^2} x - 2 = 0$ over \mathbb{F}_{q^3} is $x = a^{-(q^2+q+1)}(a^{q+1} - a^{2q} + a^{q^2+q})$.*

Proof. Let $A(x) = a^q x^q + a^{q^2} x - 2 = (x - 2) \circ L(x)$, where $L(x) = a^q x^q + a^{q^2} x$ is a linearized polynomial over \mathbb{F}_{q^3} . Since the determinant of Dickson matrix of $L(x)$ is $2a^{q^2+q+1} \neq 0$, we have that $L(x)$ permutes \mathbb{F}_{q^3} , and so $A(x)$ permutes \mathbb{F}_{q^3} , that is to say, that the equation $a^q x^q + a^{q^2} x - 2 = 0$ has a unique solution over \mathbb{F}_{q^3} . Moreover, according to Lemma 4, we have that the compositional inverse of $L(x)$ over \mathbb{F}_{q^3} is

$$L^{-1}(x) = (2a^{q^2+q+1})^{-1}(a^{q+1}x - a^{2q}x^q + a^{q^2+q}x^{q^2}).$$

This yields that the compositional inverse of $A(x)$ over \mathbb{F}_{q^3} is

$$A^{-1}(x) = L^{-1}(x) \circ (x+2) = (2a^{q^2+q+1})^{-1}(a^{q+1}(x+2) - a^{2q}(x+2)^q + a^{q^2+q}(x+2)^{q^2}).$$

Therefore, $A^{-1}(0) = a^{-(q^2+q+1)}(a^{q+1} - a^{2q} + a^{q^2+q})$. We complete the proof. □

Theorem 4. *Using the notations as in Theorem 3, if $f(x) = -x + x^{(q^2+1)/2} + x^{(q^3+q)/2}$ is a CPP over \mathbb{F}_{q^3} . Then the compositional inverse of $f(x) + x$ over \mathbb{F}_{q^3} is*

$$(f(x) + x)^{-1} = \left((x - x^q + x^{q^2})/2 \right)^{q^3 - q^2 + q}.$$

and the compositional inverse of $f(x)$ over \mathbb{F}_{q^3} is

$$f^{-1}(x) = \left(x^{q^2+q+1}(x^{q+1} - x^{2q} + x^{q^2+q})^{q^3-2} \right)^{q^3 - q^2 + q}.$$

Proof. Note that

$$f(x) + x = x^{(q^2+1)/2} + x^{(q^3+q)/2} = g(x^{(q^2+1)/2}), \quad (3)$$

where are $g(x) = x + x^q$.

Since $g(x)$ is a linearized polynomial over \mathbb{F}_{q^3} and the determinant of Dickson matrix of $g(x)$ is 2, it implies by Lemma 4 that the compositional inverse of $g(x)$ over \mathbb{F}_{q^3} is

$$g^{-1}(x) = (x - x^q + x^{q^2})/2. \quad (4)$$

Moreover, since $(q^3 - q^2 + q)(q^2 + 1)/2 - ((q^2 - q + 2)/2)(q^3 - 1) = 1$, it follows from Eqs. (3) and (4) that

$$\begin{aligned} (f(x) + x)^{-1} &= \left(x^{(q^2+1)/2}\right)^{-1} \circ g^{-1}(x) \\ &= \left((x - x^q + x^{q^2})/2\right)^{q^3 - q^2 + q}. \end{aligned}$$

Now we will study the compositional inverse of $f(x)$ over \mathbb{F}_{q^3} . Put $h(x) = x + x^q - x^{1+q-q^2}$. Then we have

$$f(x) = h(x) \circ x^{(q^2+1)/2} \quad (5)$$

Therefore, it is crucial to calculate the compositional inverse of $h(x)$ over \mathbb{F}_{q^3} .

Let $\psi_1(x) = x, \psi_2(x) = x^q, \psi_3(x) = x^{q^2}, \varphi_1(x) = \psi_1(x) \circ h(x) = h(x), \varphi_2(x) = \psi_2(x) \circ h(x) = h^q(x)$, and $\varphi_3(x) = \psi_3(x) \circ h(x) = h^{q^2}(x)$. For simplicity, put $\varphi_1(x) = a, \varphi_2(x) = b, \varphi_3(x) = c$. Then $c = b^q = a^{q^2}$. As it has been shown in [29] that $f(x)$ has a unique root 0 in \mathbb{F}_{q^3} , we assume that $x \neq 0$ so that $abc \neq 0$. By substituting $y = x^q, z = y^q$, we obtain the system of equations

$$\begin{cases} x + y + \frac{xy}{z} = a, \\ y + z + \frac{yz}{x} = b, \\ z + x + \frac{xz}{y} = c, \end{cases}$$

which can be rewritten as

$$\begin{cases} xz + yz - xy = az, \\ xy + xz - yz = bx, \\ yz + xy - xz = cy. \end{cases} \quad (6)$$

By adding the last two equations of Eq. (6), we have

$$2xy = bx + cy,$$

or, equivalently,

$$2x^q = a^q + a^{q^2}x^{q-1}$$

because $c = b^q = a^{q^2}, y = x^q$ and $x \neq 0$. Setting $t = 1/x$, we obtain

$$a^q t^q + a^{q^2} t - 2 = 0$$

by the above equation. According to Lemma 6, we have $t = a^{-(q^2+q+1)}(a^{q+1} - a^{2q} + a^{q^2+q})$, and so $x = a^{q^2+q+1}(a^{q+1} - a^{2q} + a^{q^2+q})^{q^3-2}$. Hence, by Lemma 3, the

compositional inverse of $f(x)$ over \mathbb{F}_{q^3} is

$$\begin{aligned} f^{-1}(x) &= \left(x^{(q^2+1)/2}\right)^{-1} \circ h^{-1}(x) \\ &= \left(x^{q^2+q+1}(x^{q+1} - x^{2q} + x^{q^2+q})^{q^3-2}\right)^{q^3-q^2+q}. \end{aligned}$$

We are done. \square

5 The permutation polynomial of the form $A(x)^m + L(x)$ and its inverse over \mathbb{F}_{q^n}

In this section, we investigate the permutation behavior of the form the form $A(x)^m + L(x)$ and its inverse over \mathbb{F}_{q^n} .

We give a property of linearized polynomial over \mathbb{F}_{q^n} at first.

Lemma 7. [28, Proposition 4.4] *For any linearize polynomial $L(x)$ over \mathbb{F}_{q^n} , then $\text{rank}(L) = \text{rank}(D)$, where $\text{rank}(L)$ is the rank of the linear transformation induced by $L(x)$, and D is the Dickson matrix associated to $L(x)$.*

We investigate a property of a linearized polynomial $L(x)$ over \mathbb{F}_{q^n} with $\text{rank}(L) = n - 1$ in the following result.

Lemma 8. *Let $L(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \in \mathbb{F}_{q^n}[x]$ and D be the associated Dickson matrix. If $\text{rank}(D) = n - 1$, then any $n - 1$ row vectors of the matrix D are linearly independent.*

Proof. Suppose, on the contrary, that there exist $n - 1$ row vectors being linear dependent. In fact, we can assume that the first $n-1$ rows vectors of matrix D are linearly dependent, and other cases can be similarly proved. Suppose that the vectors $(a_0, a_1, \dots, a_{n-1})$, $(a_{n-1}^q, a_0^q, \dots, a_{n-2}^q)$, \dots , $(a_2^{q^{n-2}}, a_3^{q^{n-2}}, \dots, a_1^{q^{n-2}})$ are linear dependent, and so we get a relation

$$k_1 \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix}^T + k_2 \begin{pmatrix} a_{n-1}^q \\ a_0^q \\ \vdots \\ a_{n-2}^q \end{pmatrix}^T + \dots + k_n \begin{pmatrix} a_2^{q^{n-2}} \\ a_3^{q^{n-2}} \\ \vdots \\ a_1^{q^{n-2}} \end{pmatrix}^T = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}^T \quad (7)$$

with $k_i \in \mathbb{F}_{q^n}$ not all being 0. Raising Eq.(7) to the power of q , and then rearranging the row vectors components suitably, we obtain

$$k_1^q \begin{pmatrix} a_{n-1}^q \\ a_0^q \\ \vdots \\ a_{n-2}^q \end{pmatrix}^T + k_2^q \begin{pmatrix} a_{n-2}^{q^2} \\ a_{n-1}^q \\ \vdots \\ a_{n-3}^{q^3} \end{pmatrix}^T + \dots + k_n^q \begin{pmatrix} a_1^{q^{n-1}} \\ a_2^{q^{n-1}} \\ \vdots \\ a_0^{q^{n-1}} \end{pmatrix}^T = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}^T, \quad (8)$$

which means except for the first row vector of matrix D , the last $n-1$ rows vectors of matrix D are linearly dependent. Similarly, raising Eq.(7) to the q^2 -th power and then properly permuting the positions of the row vectors components, we obtain

$$k_1^{q^2} \begin{pmatrix} a_{n-2}^{q^2} \\ a_{n-1}^{q^2} \\ \dots \\ a_{n-3}^{q^3} \end{pmatrix}^T + \dots + k_{n-1}^{q^2} \begin{pmatrix} a_1^{q^{n-1}} \\ a_2^{q^{n-1}} \\ \vdots \\ a_0^{q^{n-1}} \end{pmatrix}^T + k_n^{q^2} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix}^T = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}^T.$$

That is, except for the vector in the second row, the remaining $n-1$ row vectors of matrix D are linearly dependent. We keep repeating the steps by raising Eq.(8) to the power q^3, \dots, q^{n-1} and then properly permuting the positions of row vectors components. Then we have that any $n-1$ row vectors of the matrix D are linearly dependent, which is a contraction to $\text{rank}(D) = n-1$. We are done. \square

For be a prime power q and a positive integer $n > 1$, let $b \in \mathbb{F}_{q^n}$ with $b^{q^{n-1}+q^{n-2}+\dots+q^2+q+1} = 1$ and the polynomial

$$A(x) = x^{q^{n-1}} + bx^{q^{n-2}} + b^{1+q^{n-1}}x^{q^{n-3}} + \dots + b^{1+\sum_{i=1}^j q^{n-i}}x^{q^{n-j-2}} + \dots + b^{1+\sum_{i=1}^{n-2} q^{n-i}}x.$$

We demonstrate that $\text{Im}(A(x))$ is a vector space with dimension 1. Furthermore, we present a necessary and sufficient condition for $\text{Im}(A(x))^m$ to also be a vector space with dimension 1, as shown in the following lemma.

Lemma 9. [23, Lemma 2] *Let the notation $A(x)$ be defined as above, then*

- (i) $A(x)^q = b^q A(x)$;
- (ii) $\text{Im}(A(x)) = \{cg^{qt} \mid c \in \mathbb{F}_q\}$ is a one-dimensional vector space over \mathbb{F}_q , where $g \in \mathbb{F}_{q^n}$ is a primitive element of \mathbb{F}_{q^n} and t is a positive integer with $b = g^{(q-1)t}$.
- (iii) For a positive integer m , $\text{Im}(A^m(x))$ is a one-dimensional vector space over \mathbb{F}_q if and only if $\text{gcd}(m, q-1) = 1$.

Theorem 5. *For a prime power q and positive integers $n > 1$ and m , let $b \in \mathbb{F}_{q^n}$ with $b^{q^{n-1}+q^{n-2}+\dots+q^2+q+1} = 1$ and the polynomial*

$$A(x) = x^{q^{n-1}} + bx^{q^{n-2}} + b^{1+q^{n-1}}x^{q^{n-3}} + \dots + b^{1+\sum_{i=1}^j q^{n-i}}x^{q^{n-j-2}} + \dots + b^{1+\sum_{i=1}^{n-2} q^{n-i}}x.$$

Assume that $L(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$ is a linearized polynomial over \mathbb{F}_{q^n} . If $L(x)$ is not a permutation polynomial over \mathbb{F}_{q^n} , then the polynomial

$$f(x) = A^m(x) + L(x)$$

is a permutation polynomial over \mathbb{F}_{q^n} if and only if $\text{gcd}(m, q-1) = 1$, $\text{rank}(D) = n-1$, $\alpha_1 + \alpha_2 b^{qm} + \alpha_3 b^{q^2 m + qm} + \dots + \alpha_n b^{m \sum_{i=1}^{n-1} q^i} \neq 0$ and the determinant of the matrix

$$B = \begin{pmatrix} b^{1+\sum_{i=1}^{n-2} q^{n-i}} & a_0 & a_{n-1}^q & a_{n-2}^{q^2} & \cdots & a_2^{q^{n-2}} \\ b^{1+\sum_{i=1}^{n-3} q^{n-i}} & a_1 & a_0^q & a_{n-1}^{q^2} & \cdots & a_3^{q^{n-2}} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ b & a_{n-2} & a_{n-3}^q & a_{n-4}^{q^2} & \cdots & a_0^{q^{n-2}} \\ 1 & a_{n-1} & a_{n-2}^q & a_{n-3}^{q^2} & \cdots & a_1^{q^{n-2}} \end{pmatrix}$$

is non-zero, where the matrix D is the associate Dickson matrix of $L(x)$, and $(\alpha_1, \alpha_2, \dots, \alpha_n)$ is a non-zero solution of the system of linear equations $D^T x = O$.

Proof. We first prove the necessity. Put $\text{rank}(D) = r$. Since $L(x)$ is not a permutation polynomial over \mathbb{F}_{q^n} , we have $\text{rank}(D) \leq n - 1$ by Lemma 7.

If $\gcd(m, q - 1) \neq 1$ or $\text{rank}(D) = r < n - 1$, then it follows from lemma 9 that

$$\#\text{Im}(f(x)) \leq \#\text{Im}(A^m(x)) \cdot q^r \leq q \cdot q^r < q^n, \quad (9)$$

and so $f(x)$ is not a permutation polynomial over \mathbb{F}_{q^n} .

Now we assume that $\text{rank}(D) = n - 1$, and $\gcd(m, q - 1) = 1$. Suppose that the determinant of B is zero. it follows that n column vectors of B are linearly dependent. Additionally, since the rank of D is $n - 1$, by Lemma 8 we have that the first $n - 1$ row vectors of D are linear independent. Furthermore, since the transpose of the last $n - 1$ column vectors of the matrix B form the first $n - 1$ row vectors of the matrix D , these last $n - 1$ column vectors of the matrix B are linear independent. Given that the determinant of B is zero, it follows that the first column vector of B can be expressed as a linear combination of the last $n - 1$ column vectors of the matrix B . Therefore, there exist scalars $k_2, \dots, k_n \in \mathbb{F}_{q^n}$ not all zero, such that

$$\begin{pmatrix} b^{1+\sum_{i=1}^{n-2} q^{n-i}} \\ b^{1+\sum_{i=1}^{n-3} q^{n-i}} \\ \vdots \\ 1 \end{pmatrix} = k_2 \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} + \cdots + k_n \begin{pmatrix} a_2^{q^{n-2}} \\ a_3^{q^{n-2}} \\ \vdots \\ a_1^{q^{n-2}} \end{pmatrix}.$$

This implies

$$\begin{aligned} & \begin{pmatrix} b^{1+\sum_{i=1}^{n-2} q^{n-i}} \\ b^{1+\sum_{i=1}^{n-3} q^{n-i}} \\ \vdots \\ 1 \end{pmatrix}^T \begin{pmatrix} x \\ x^q \\ \vdots \\ x^{q^{n-1}} \end{pmatrix} \\ &= \begin{pmatrix} k_2 \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix}^T + \cdots + k_n \begin{pmatrix} a_2^{q^{n-2}} \\ a_3^{q^{n-2}} \\ \vdots \\ a_1^{q^{n-2}} \end{pmatrix}^T \end{pmatrix} \begin{pmatrix} x \\ x^q \\ \vdots \\ x^{q^{n-1}} \end{pmatrix} \end{aligned}$$

$$= k_2 \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix}^T \begin{pmatrix} x \\ x^q \\ \vdots \\ x^{q^{n-1}} \end{pmatrix} + \cdots + k_n \begin{pmatrix} a_2^{q^{n-2}} \\ a_3^{q^{n-2}} \\ \vdots \\ a_1^{q^{n-2}} \end{pmatrix}^T \begin{pmatrix} x \\ x^q \\ \vdots \\ x^{q^{n-1}} \end{pmatrix}. \quad (10)$$

Note that

$$\left(b^{1+\sum_{i=1}^{n-2} q^{n-i}}, b^{1+\sum_{i=1}^{n-3} q^{n-i}}, \dots, 1 \right) \left(x, x^q, \dots, x^{q^{n-1}} \right)^T = A(x), \quad (11)$$

and

$$\begin{pmatrix} L(x) \\ L(x)^q \\ \vdots \\ L(x)^{q^{n-1}} \end{pmatrix} = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1}^q & a_0^q & \cdots & a_{n-2}^q \\ \vdots & \vdots & \vdots & \vdots \\ a_1^{q^{n-1}} & a_2^{q^{n-1}} & \cdots & a_0^{q^{n-1}} \end{pmatrix} \begin{pmatrix} x \\ x^q \\ \vdots \\ x^{q^{n-1}} \end{pmatrix} = D \begin{pmatrix} x \\ x^q \\ \vdots \\ x^{q^{n-1}} \end{pmatrix}, \quad (12)$$

or we can rewrite as

$$\left(a_{n-j}^{q^j}, \dots, a_{n-1}^{q^j}, a_0^{q^j}, \dots, a_{n-j-1}^{q^j} \right)^T \left(x, x^q, \dots, x^{q^{n-1}} \right) = L(x)^{q^j}, \quad (13)$$

for $j = 1, 2, \dots, n$.

Substituting (11) and (13) into (10) yields

$$A(x) = k_2 L(x) + k_3 L^q(x) + k_4 L^{q^2}(x) + \cdots + k_n L^{q^{n-2}}(x),$$

Consequently, we can conclude that

$$f(x) = A^m(x) + L(x) = \left((k_2 x + k_3 x^q + k_4 x^{q^2} + \cdots + k_n x^{q^{n-2}})^m + x \right) \circ L(x). \quad (14)$$

Since $L(x)$ is not a permutation polynomial over \mathbb{F}_{q^n} , it follows from (14) that $f(x)$ is not a permutation polynomial.

Now we assume that the martrix of B is non-singular. Since the rank of D is $n-1$, the system of homogeneous linear equations

$$D^T x = O, \quad (15)$$

has a nontrivial solutions. Let $(\alpha_1, \alpha_2, \dots, \alpha_n)^T$ be a non-zero solution of (15). Then we have

$$(\alpha_1, \alpha_2, \dots, \alpha_n) D = (0, 0, \dots, 0). \quad (16)$$

Let $\psi_1(x) = \alpha_1 x + \alpha_2 x^q + \dots + \alpha_n x^{q^{n-1}}$, $\psi_2(x) = x$, $\varphi_1(x) = A(x)$ and $\varphi_2(x) = f(x)$. It follows from (12) and (16) that

$$\begin{aligned}
& \psi_1(x) \circ f(x) \\
&= (\alpha_1, \alpha_2, \dots, \alpha_n) \begin{pmatrix} x \\ x^q \\ \vdots \\ x^{q^{n-1}} \end{pmatrix} \circ A^m(x) + (\alpha_1, \alpha_2, \dots, \alpha_n) \begin{pmatrix} x \\ x^q \\ \vdots \\ x^{q^{n-1}} \end{pmatrix} \circ L(x) \\
&= (\alpha_1, \alpha_2, \dots, \alpha_n) \begin{pmatrix} A^m(x) \\ A^{mq}(x) \\ \vdots \\ A^{mq^{n-1}}(x) \end{pmatrix} + (\alpha_1, \alpha_2, \dots, \alpha_n) \begin{pmatrix} L(x) \\ L(x)^q \\ \vdots \\ L(x)^{q^{n-1}} \end{pmatrix} \\
&= A^m(x) (\alpha_1, \alpha_2, \dots, \alpha_n) \begin{pmatrix} 1 \\ b^{qm} \\ \vdots \\ b^{m \sum_{i=1}^{n-1} q^i} \end{pmatrix} + (\alpha_1, \alpha_2, \dots, \alpha_n) D \begin{pmatrix} x \\ x^q \\ \vdots \\ x^{q^{n-1}} \end{pmatrix} \\
&= (\alpha_1 + \alpha_2 b^{qm} + \alpha_3 b^{q^2 m + qm} + \dots + \alpha_n b^{m \sum_{i=1}^{n-1} q^i}) A^m(x). \tag{17}
\end{aligned}$$

If $\alpha_1 + \alpha_2 b^{qm} + \alpha_3 b^{q^2 m + qm} + \dots + \alpha_n b^{m \sum_{i=1}^{n-1} q^i} = 0$, then $f(x)$ is not a permutation polynomial over \mathbb{F}_{q^n} .

Suppose that $\alpha_1 + \alpha_2 b^{qm} + \alpha_3 b^{q^2 m + qm} + \dots + \alpha_n b^{m \sum_{i=1}^{n-1} q^i} \neq 0$. For simplicity, we put $s = \alpha_1 + \alpha_2 b^{qm} + \alpha_3 b^{q^2 m + qm} + \dots + \alpha_n b^{m \sum_{i=1}^{n-1} q^i}$. Since $\gcd(m, q-1) = 1$, there exist integers u and v such that $mu \equiv 1 + v(q-1) \pmod{q^n - 1}$, and so by (17), that we get

$$b^{-qv} (s^{-1}(\psi_1(x) \circ f(x)))^u = A^{mu}(x) = A^{1+v(q-1)}(x) = A(x) = \varphi_1(x).$$

Thus, we obtain

$$\varphi_2(x) - \varphi_1^m(x) = L(x). \tag{18}$$

On the other hand, since the determinant of B is not zero, the system of non-homogeneous linear equations

$$Bx = (1, 0, \dots, 0)^T, \tag{19}$$

has a unique solution. Let $(\beta_1, \beta_2, \dots, \beta_n)^T$ be the unique solution of the system of non-homogeneous linear equations (19). Then we have

$$(\beta_1, \beta_2, \dots, \beta_n) B^T = (1, 0, \dots, 0). \tag{20}$$

Put $D = (\eta_1, \eta_2, \dots, \eta_m)$ and $\beta^T = (\beta_2, \beta_3, \dots, \beta_n, 0)$, where η_i is the i -th column vector of the matrix D , It follows from Eq. (20) that

$$\begin{aligned}
& \beta_1(b^{1+\sum_{i=1}^{n-2} q^{n-i}}, b^{1+\sum_{i=1}^{n-3} q^{n-i}}, \dots, 1) + (\beta_2, \beta_3, \dots, \beta_n, 0)D \\
&= \beta_1(b^{1+\sum_{i=1}^{n-2} q^{n-i}}, b^{1+\sum_{i=1}^{n-3} q^{n-i}}, \dots, 1) + \beta^T(\eta_1, \eta_2, \dots, \eta_m) \\
&= (\beta_1 b^{1+\sum_{i=1}^{n-2} q^{n-i}} + \beta^T \eta_1, \beta_1 b^{1+\sum_{i=1}^{n-3} q^{n-i}} + \beta^T \eta_2, \dots, \beta_1 + \beta^T \eta_m) \\
&= (\beta_1, \beta_2, \dots, \beta_n) B^T \\
&= (1, 0, \dots, 0),
\end{aligned}$$

and so by (12), that

$$\begin{aligned}
& \beta_1 \varphi_1(x) + \left((\beta_2 x + \beta_3 x^q + \dots + \beta_n x^{q^{n-2}}) \circ (\varphi_2(x) - \varphi_1^m(x)) \right) \\
&= \beta_1 \varphi_1(x) + \left((\beta_2 x + \beta_3 x^q + \dots + \beta_n x^{q^{n-2}}) \circ L(x) \right) \\
&= \beta_1(b^{1+\sum_{i=1}^{n-2} q^{n-i}}, b^{1+\sum_{i=1}^{n-3} q^{n-i}}, \dots, 1) \begin{pmatrix} x \\ x^q \\ \vdots \\ x^{q^{n-1}} \end{pmatrix} + (\beta_2, \beta_3, \dots, \beta_n, 0) \begin{pmatrix} L(x) \\ L(x)^q \\ \vdots \\ L(x)^{q^{n-1}} \end{pmatrix} \\
&= \beta_1(b^{1+\sum_{i=1}^{n-2} q^{n-i}}, b^{1+\sum_{i=1}^{n-3} q^{n-i}}, \dots, 1) \begin{pmatrix} x \\ x^q \\ \vdots \\ x^{q^{n-1}} \end{pmatrix} + (\beta_2, \beta_3, \dots, \beta_n, 0) D \begin{pmatrix} x \\ x^q \\ \vdots \\ x^{q^{n-1}} \end{pmatrix} \\
&= x.
\end{aligned}$$

It follows from Lemma (3) that the polynomial $f(x)$ permutes \mathbb{F}_{q^n} and the compositional inverse of $f(x)$ over \mathbb{F}_{q^n} is

$$\begin{aligned}
f^{-1}(x) &= \beta_1 b^{-qv} s^{-u} \left(\alpha_1 x + \alpha_2 x^q + \dots + \alpha_n x^{q^{n-1}} \right)^u + \\
& (\beta_2 x + \beta_3 x^q + \dots + \beta_n x^{q^{n-2}}) \circ \left(x - b^{-qvm} s^{-um} (\alpha_1 x + \alpha_2 x^q + \dots + \alpha_n x^{q^{n-1}})^{um} \right).
\end{aligned}$$

This completes the proof. \square

Declarations

- The works is partially supported by the National Natural Science Foundation of China (Grant Nos. 12171163 and 11901083) and the Guangdong Basic and Applied Basic Research Foundation (Grant Nos. 2020A1515111090 and 2024A1515010589).

References

- [1] Ding, C.: Cyclic codes from some monomials and trinomials. *SIAM Journal on Discrete Mathematics* **27**(4), 1977–1994 (2013)
- [2] Ding, C., Zhou, Z.: Binary cyclic codes from explicit polynomials over $GF(2m)$. *Discrete Mathematics* **321**, 76–89 (2014)
- [3] Laigle-Chapuy, Y.: Permutation polynomials and applications to coding theory. *Finite Fields and Their Applications* **13**(1), 58–70 (2007)
- [4] Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM* **21**(2), 120–126 (1978)
- [5] Schwenk, J., Huber, K.: Public key encryption and digital signatures based on permutation polynomials. *Electronics Letters* **34**(8), 759–760 (1998)
- [6] Ding, C., Yuan, J.: A family of skew hadamard difference sets. *Journal of Combinatorial Theory, Series A* **113**(7), 1526–1535 (2006)
- [7] Lidl, R., Niederreiter, H.: *Finite Fields* vol. 20. Cambridge University Press, New York (1997)
- [8] Lidl, R., Niederreiter, H.: *Introduction to Finite Fields and Their Applications*. Cambridge University press, New York (1994)
- [9] Akbary, A., Ghioca, D., Wang, Q.: On constructing permutations of finite fields. *Finite Fields and Their Applications* **17**(1), 51–67 (2011)
- [10] Cepak, N., Charpin, P., Pasalic, E.: Permutations via linear translators. *Finite Fields and Their Applications* **45**, 19–42 (2017)
- [11] Li, K., Qu, L., Chen, X.: New classes of permutation binomials and permutation trinomials over finite fields. *Finite Fields and Their Applications* **43**, 69–85 (2017)
- [12] Tu, Z., Zeng, X.: Two classes of permutation trinomials with Niho exponents. *Finite Fields and Their Applications* **53**, 99–112 (2018)
- [13] Wu, D., Yuan, P.: Some classes of permutation polynomials of the form $b(x^q + ax + \delta)^{i(q^2-1)/d+1} + c(x^q + ax + \delta)^{j(q^2-1)/d+1} + L(x)$ over \mathbb{F}_{q^2} . *Applicable Algebra in Engineering, Communication and Computing* **33**(2), 135–149 (2022)
- [14] Wu, D., Yuan, P.: Further results on permutation polynomials from trace functions. *Applicable Algebra in Engineering, Communication and Computing* **33**(4), 341–351 (2022)
- [15] Yuan, P., Ding, C.: Permutation polynomials over finite fields from a powerful

- lemma. *Finite Fields and Their Applications* **17**(6), 560–574 (2011)
- [16] Yuan, P., Zheng, Y.: Permutation polynomials from piecewise functions. *Finite Fields and Their Applications* **35**, 215–230 (2015)
- [17] Zheng, Y., Yuan, P., Pei, D.: Large classes of permutation polynomials over \mathbb{F}_{q^2} . *Designs, Codes and Cryptography* **81**, 505–521 (2016)
- [18] Zheng, D., Yuan, M., Yu, L.: Two types of permutation polynomials with special forms. *Finite Fields and Their Applications* **56**, 1–16 (2019)
- [19] Wang, Q.: A survey of compositional inverses of permutation polynomials over finite fields. *Designs, codes and cryptography* <https://doi.org/10.1007/s10623-024-01436-4>
- [20] Wu, D., Yuan, P., Guan, H., Li, J.: The compositional inverses of three classes of permutation polynomials over finite fields (2024). <https://arxiv.org/abs/2409.18517>
- [21] Wu, D., Yuan, P.: The compositional inverses of permutation polynomials from trace functions over finite fields (2024). <https://arxiv.org/abs/2409.20000>
- [22] Wu, D., Yuan, P., Guan, H., Li, J.: The compositional inverses of permutation polynomials of the form $\sum_{i=1}^k b_i(x^{p^m} + x + \delta)^{s_i} - x$ over $\mathbb{F}_{p^{2m}}$ (2024). <https://arxiv.org/abs/2409.18662>
- [23] Wu, D., Yuan, P.: Permutation polynomials and their compositional inverses over finite fields by a local method. *Des. Codes Cryptogr.* **92**(2), 267–276 (2024) <https://doi.org/10.1007/S10623-023-01308-3>
- [24] Wu, D., Yuan, P.: Permutation polynomials over finite fields by the local criterion (2024). <https://arxiv.org/abs/2409.18758>
- [25] Yuan, P.: Compositional inverses of agw-pps. *Advances in Mathematics of Communications* **16**(4), 1185–1195 (2022)
- [26] Yuan, P.: Local method for compositional inverses of permutation polynomials. *Communications in Algebra* **52**(7), 3070–3080 (2024)
- [27] Hasan, S.U., Kaur, R.: Some new classes of permutation polynomials and their compositional inverses (2024). <https://arxiv.org/abs/2407.12688>
- [28] Wu, B., Liu, Z.: Linearized polynomials over finite fields revisited. *Finite Fields and Their Applications* **22**, 79–100 (2013)
- [29] Ma, J., Zhang, T., Feng, T., Ge, G.: Some new results on permutation polynomials over finite fields. *Des. Codes Cryptogr.* **83**(2), 425–443 (2017) <https://doi.org/10.1007/S10623-016-0236-1>