

New classes of permutation polynomials of special form*

Research Article

Pooja Gahlyan , Rohit Gupta , Rajendra Kumar Sharma 

Abstract: In this paper, we propose six new classes of permutation polynomials. Precisely, for $p = 3$ or $p = 5$, three new classes of permutation polynomials over $\mathbb{F}_{p^{2m}}$ of the form $(x^{p^m} - x + \delta)^s + L(x)$, and three new classes of permutation polynomials over $\mathbb{F}_{p^{2m}}$ of the form $(x^{p^m} - x + \delta)^{s_1} + (x^{p^m} - x + \delta)^{s_2} + L(x)$, are given where $L(x) = ax^{p^m} + ax$ with $a \in \mathbb{F}_{p^m}^*$. We use a method based on the AGW criterion and the determination of the number of solutions of certain type of equations. The sufficient conditions on $\delta \in \mathbb{F}_{p^{2m}}$ are shown to be necessary.

2020 MSC: 11T06, 11T55

Keywords: Finite field, Permutation polynomial, Linearized polynomial, Trace function

1. Introduction

For a prime power q , let $\mathbb{F}_q$ denote the finite field with q elements. A polynomial $f(x) \in \mathbb{F}_q[x]$ is said to be a *permutation polynomial* over $\mathbb{F}_q$ if the associated polynomial function $f : c \rightarrow f(c)$ from $\mathbb{F}_q$ into $\mathbb{F}_q$

* This work was supported by the University Grants Commission(UGC), India, under the grant number 1089/(CSIR-UGC NET DEC. 2016).

Pooja Gahlyan (Corresponding Author); Department of Mathematics, IIT Delhi, New Delhi, 110016, India, (poo-jagahlyan1995@gmail.com).

Rohit Gupta; Department of Mathematics, Birla Institute of Technology and Science-Pilani, Hyderabad Campus, Hyderabad, Telangana, 500078, India, (rohittgupta20@gmail.com).

Rajendra Kumar Sharma; Department of Mathematics, Delhi Technological University(DTU), New Delhi, 110042, India, (rksharmaiitd@gmail.com).

is a bijection. Permutation polynomials over finite fields have been an active area of research because of its applications in various areas like cryptography [13, 16], coding theory [3, 7] and combinatorial designs [4]. Constructions of new classes of permutation polynomials over finite fields is an area of tremendous interest.

Helleseth and Zinoviev [6] established new Kloosterman sum identities over $\mathbb{F}_{2^n}$ by using permutation polynomials of the form

$$\left(\frac{1}{x^2 - x + \delta}\right)^{2^l} + x$$

where δ in $\mathbb{F}_{2^n}$ and $l = 0, 1$ with absolute trace $Tr(\delta) = 1$. Motivated by this work, Yuan and Ding [25, 27] studied permutation polynomials of the form

$$(x^{p^k} - x + \delta)^s + L(x)$$

over $\mathbb{F}_{p^m}$, where $L(x)$ is a linearized polynomial over $\mathbb{F}_{p^m}$, $\delta \in \mathbb{F}_{p^m}$ and k, m, s are positive integers. Subsequently, many classes of permutation polynomials with the form $(x^{p^m} - x + \delta)^s + L(x)$ over $\mathbb{F}_{p^{2m}}$ for exponent s satisfying $s(p^m + 1) \equiv p^m + 1 \pmod{p^{2m} - 1}$ or $s(p^m - 1) \equiv p^m - 1 \pmod{p^{2m} - 1}$, has been constructed in [17, 18, 30]. For different values of s , many more classes of this type have been obtained in [5, 9, 10, 12, 19, 20, 22, 26, 28, 29, 31, 32] for even as well as odd characteristic. Recently, Xu, Luo and Cao [24] proposed four classes of permutation polynomials of the form

$$(x^{p^m} - x + \delta)^s + L(x)$$

with $L(x) = x$ for even characteristic. They have also found several classes of permutation polynomials over finite fields of odd characteristic of the above form, some of which are complete permutation polynomials over $\mathbb{F}_{3^{2m}}$. Very recently, Wu and Yuan [21] determined several classes of permutation polynomials of the form $b(x^q + ax + \delta)^s - ax$ over $\mathbb{F}_{2^{2m}}$ and three classes of permutation polynomials of the form $b(x^q - x + \delta)^s + x$ over $\mathbb{F}_{p^{2m}}$ with infinitely many odd primes p .

Further, by using AGW criterion and determining the number of solutions of certain type of equations, Xu, Feng and Zeng [23] investigated several classes of complete permutation polynomials of the form

$$(x^{p^m} - x + \delta)^s + ax^{p^m} + bx$$

over $\mathbb{F}_{p^n}$, for exponent $s = i(p^m \pm 1) + p^j$ and $a, b, \delta \in \mathbb{F}_{p^n}$, where m, n are positive integers. Recently, Li and Cao [8], among several other classes of polynomials, proposed two classes of permutation polynomials of the form $(x^{p^m} - x + \delta)^s + ax^{p^m} + bx$ over $\mathbb{F}_{p^{2m}}$. Very recently, Chen, Kan, Li, Peng and Zheng [2] constructed six classes of permutation polynomials of the form $(x^{p^m} - x + \delta)^s + ax^{p^m} + bx$ over $\mathbb{F}_{p^{2m}}$, where p is an odd prime.

By using a link between two classes of permutation polynomials over finite fields, Li, Qu and Zhou [11], constructed four classes of permutation polynomials of the form $(x^2 + x + \delta)^{s_1} + (x^2 + x + \delta)^{s_2} + x$ over $\mathbb{F}_{2^n}$. Very Recently, Liu, Xie, Liu, and Zou [15] gave nine classes of permutation polynomials over $\mathbb{F}_{p^n}$ of the form

$$(x^{p^m} - x + \delta)^{s_1} + (x^{p^m} - x + \delta)^{s_2} + x$$

over $\mathbb{F}_{p^n}$, where exponents s_1 and s_2 are positive integers, $m|n$ and $\delta \in \mathbb{F}_{p^n}$ and five classes of complete permutation polynomials over $\mathbb{F}_{p^{2m}}$ of the form $ax^{p^m} + bx + h(x^{p^m} - x)$ with the help of AGW criterion and determining the number of solutions to certain equations over finite fields.

In this paper, we further study the permutation behavior of polynomials of the form $(x^{p^m} - x + \delta)^s + L(x)$ and $(x^{p^m} - x + \delta)^{s_1} + (x^{p^m} - x + \delta)^{s_2} + L(x)$ over finite fields of odd characteristic. More precisely, three classes of permutation polynomials of the form $(x^{p^m} - x + \delta)^s + L(x)$ and three classes of permutation polynomials of the form $(x^{p^m} - x + \delta)^{s_1} + (x^{p^m} - x + \delta)^{s_2} + L(x)$ over the finite field $\mathbb{F}_{p^{2m}}$ are given, where $p = 3$ or $p = 5$, $L(x) = ax^{p^m} + ax$ and $a \in \mathbb{F}_{p^m}^*$. The method used in this paper has also

been used in [15]. Determining the number of solutions of certain lower degree equations in a subset of $\mathbb{F}_{p^{2m}}$ plays a key role in our constructions.

The rest of the paper is organized as follows. In Section 2, some basic definitions and useful lemmas are given. Section 3 includes the main results of this paper. In Section 4, we state the conclusion.

2. Preliminaries

Hereby, we clarify the notation used in the paper. We always use p for an arbitrary odd prime and m, n for positive integers. Let $\mathbb{F}_{p^n}$ denote finite field with p^n elements. For each element δ in the finite field $\mathbb{F}_{p^{2m}}$, we denote δ^{p^m} by $\bar{\delta}$ in analogy with the usual complex conjugation. Obviously, $\delta + \bar{\delta} \in \mathbb{F}_{p^m}$ and $\delta\bar{\delta} \in \mathbb{F}_{p^m}$. For $m|n$, we use $Tr_m^n(\cdot)$ to denote the trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$, i.e.,

$$Tr_m^n(x) = x + x^{p^m} + x^{p^{2m}} + \cdots + x^{p^{(n-m)m}}.$$

Define $J = \{\alpha^{p^m} - \alpha : \alpha \in \mathbb{F}_{p^n}\} = \{\alpha \in \mathbb{F}_{p^n} : \alpha^{p^m} + \alpha = 0\}$. First we recall the definition of q -polynomial as follows:

Definition 2.1. [14] Let q denote a prime power. A polynomial of the form

$$L(x) = \sum_{i=0}^n a_i x^{q^i}$$

with coefficients in an extension field $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$ is called a q -polynomial over $\mathbb{F}_{q^n}$.

We recall a result followed from the AGW criterion.

Lemma 2.2. [1] For positive integers m, n with $m|n$, let $\phi(x)$ be a p^m -polynomial over $\mathbb{F}_{p^m}$, $h(x) \in \mathbb{F}_{q^n}[x]$ be any polynomial such that $h(x^{p^m} - x) \in \mathbb{F}_{p^m} \setminus \{0\}$ for all $x \in \mathbb{F}_{p^n}$, and let $g(x) \in \mathbb{F}_{p^n}[x]$ be any polynomial. Then $h(x^{p^m} - x)\phi(x) + g(x^{p^m} - x)$ is a permutation of $\mathbb{F}_{p^n}$ if and only if the following two conditions hold:

- (i) $\phi(x)$ induces a permutation of $\mathbb{F}_{p^m}$;
- (ii) $h(x)\phi(x) + g(x)^{p^m} - g(x)$ permutes J .

By taking $g(x) = \sum_{j=1}^t (x + \delta)^{s_j}$, $h(x) = 1$ and $\phi(x) = ax^{p^m} + ax$, where $a \in \mathbb{F}_{p^m}^*$, in Lemma 2.2, we obtain the following lemma.

Lemma 2.3. For given positive integers m, n, t with $m|n$, non negative integers s_j for $1 \leq j \leq t$, $a \in \mathbb{F}_{p^m}^*$ and a fixed $\delta \in \mathbb{F}_{p^n}$, the polynomial

$$\sum_{j=1}^t (x^{p^m} - x + \delta)^{s_j} + ax^{p^m} + ax$$

permutes $\mathbb{F}_{p^n}$ if and only if $\sum_{j=1}^t ((x + \delta)^{p^m s_j} - (x + \delta)^{s_j}) + ax^{p^m} + ax$ permutes J .

3. Permutation polynomials over finite fields with odd characteristic

In this section, six classes of permutation polynomials over the finite field $\mathbb{F}_{p^{2m}}$ are proposed, where $p = 3$ or $p = 5$.

Theorem 3.1. For any $a \in \mathbb{F}_{3^m}^*$ and $\delta \in \mathbb{F}_{3^{2m}}$, the polynomial

$$f(x) = (x^{3^m} - x + \delta)^{2 \cdot 3^m + 1} + ax^{3^m} + ax$$

is a permutation polynomial over $\mathbb{F}_{3^{2m}}$.

Proof. From Lemma 2.3, it is enough to show that for each $d \in J$, the equation

$$(x + \delta)^{3^m(2 \cdot 3^m + 1)} - (x + \delta)^{2 \cdot 3^m + 1} + ax^{3^m} + ax = d \quad (1)$$

has at most one solution in J . Since $x + x^{3^m} = 0$ for $x \in J$, the left-hand side of equation (1) can be simplified as

$$\begin{aligned} (x + \delta)^{3^m(2 \cdot 3^m + 1)} - (x + \delta)^{2 \cdot 3^m + 1} + ax^{3^m} + ax &= (x + \delta)^2(-x + \bar{\delta}) - (-x + \bar{\delta})^2(x + \delta) \\ &= (x + \delta)(-x + \bar{\delta})(2x + \delta - \bar{\delta}) \\ &= (-x^2 + (\bar{\delta} - \delta)x + \delta\bar{\delta})(2x + \delta - \bar{\delta}) \\ &= x^3 + (2\delta\bar{\delta} - (\bar{\delta} - \delta)^2)x + \delta\bar{\delta}(\delta - \bar{\delta}) \\ &= x^3 - (Tr_m^{2m}(\delta))^2x + \delta\bar{\delta}(\delta - \bar{\delta}). \end{aligned}$$

Thus, it suffices to prove that the equation

$$x^3 - (Tr_m^{2m}(\delta))^2x + \delta\bar{\delta}(\delta - \bar{\delta}) = d \quad (2)$$

has at most one solution in J . Suppose on the contrary that Eq. (2) has two solutions x and $x + b$, where $0 \neq b \in J$. Then we have

$$(x + b)^3 - (Tr_m^{2m}(\delta))^2(x + b) + \delta\bar{\delta}(\delta - \bar{\delta}) = d. \quad (3)$$

By subtracting Eq. (2) from Eq. (3), we get

$$b^3 - (Tr_m^{2m}(\delta))^2b = 0. \quad (4)$$

Since $b \neq 0$, the above equation leads to

$$b = \pm Tr_m^{2m}(\delta). \quad (5)$$

Taking 3^m -th power on both sides, we get

$$-b = \pm Tr_m^{2m}(\delta). \quad (6)$$

By adding Eq. (5) and Eq. (6), we get $b = 0$, which is a contradiction. This completes the proof. $\square$

Theorem 3.2. For any $a \in \mathbb{F}_{3^m}^*$ and $\delta \in \mathbb{F}_{3^{2m}}$, the polynomial

$$f(x) = (x^{3^m} - x + \delta)^{3^{2m} + 3^m + 1} + (x^{3^m} - x + \delta)^{3^{m+1} + 1} + ax^{3^m} + ax$$

is a permutation polynomial of $\mathbb{F}_{3^{2m}}$ if and only if $Tr_m^{2m}(\delta) \neq 1$.

Proof. From lemma 2.3, the polynomial $f(x)$ permutes $\mathbb{F}_{3^{2m}}$ if and only if for each $d \in J$, the equation

$$(x + \delta)^{3^m(3^{2m} + 3^m + 1)} - (x + \delta)^{3^{2m} + 3^m + 1} + (x + \delta)^{3^m(3^{m+1} + 1)} - (x + \delta)^{3^{m+1} + 1} + ax^{3^m} + ax = d \quad (7)$$

has at most one solution in J . Since $x + x^{3^m} = 0$ for $x \in J$, the left-hand side of equation (7) can be simplified as

$$\begin{aligned} & (x + \delta)^{3^m(3^{2m}+3^m+1)} - (x + \delta)^{3^{2m}+3^m+1} + (x + \delta)^{3^m(3^{m+1}+1)} - (x + \delta)^{3^{m+1}+1} + ax^{3^m} + ax \\ &= (x + \delta)^{2 \cdot 3^m+1} - (x + \delta)^{3^m+2} + (x + \delta)^{3^m+3} - (x + \delta)^{3^{m+1}+1} \\ &= (x + \delta)(-x + \bar{\delta})^2 - (-x + \bar{\delta})(x + \delta)^2 + (x + \delta)^3(-x + \bar{\delta}) - (-x + \bar{\delta})^3(x + \delta) \\ &= (x + \delta)(-x + \bar{\delta})(-2x + 2x(\bar{\delta} + \delta) - \bar{\delta}^2 + \delta^2 + (\bar{\delta} - \delta)) \\ &= (x + \delta)(-x + \bar{\delta})(2x(\delta + \bar{\delta} - 1) + (\bar{\delta} - \delta) - \bar{\delta}^2 + \delta^2) \\ &= (Tr_m^{2m}(\delta) - 1)(x + \delta)(-x + \bar{\delta})(2x - \bar{\delta} + \delta). \end{aligned}$$

If $Tr_m^{2m}(\delta) = 1$, then the left hand side of Eq. (7) is equal to 0 and this implies that Eq. (7) clearly has more than one solution if $d = 0$. Therefore $f(x)$ is not a permutation polynomial if $Tr_m^{2m}(\delta) = 1$.

Next, we assume $Tr_m^{2m}(\delta) \neq 1$. It is enough to show that the equation

$$x^3 - (Tr_m^{2m}(\delta))^2 x + \delta \bar{\delta}(-\bar{\delta} + \delta) = \frac{d}{Tr_m^{2m}(\delta) - 1} \quad (8)$$

has at most one solution in J . Suppose on the contrary that Eq. (8) has two solutions x and $x + b$, where $0 \neq b \in J$. Then we have

$$(x + b)^3 - (Tr_m^{2m}(\delta))^2(x + b) + \delta \bar{\delta}(\delta - \bar{\delta}) = \frac{d}{Tr_m^{2m}(\delta) - 1}. \quad (9)$$

By subtracting Eq. (8) from Eq. (9), we get that

$$b^3 - (Tr_m^{2m}(\delta))^2 b = 0,$$

which is same as Eq. (4). By following the same arguments as in the proof Theorem 3.1, we get a contradiction. This completes the proof. $\square$

Theorem 3.3. For any $a \in \mathbb{F}_{3^m}^*$ and $\delta \in \mathbb{F}_{3^{2m}}$, the polynomial

$$f(x) = (x^{3^m} - x + \delta)^{3^m+3} + (x^{3^m} - x + \delta)^{2 \cdot 3^m+1} + ax^{3^m} + ax$$

is a permutation polynomial of $\mathbb{F}_{3^{2m}}$ if and only if $Tr_m^{2m}(\delta) \neq 1$.

Proof. From lemma 2.3, the polynomial $f(x)$ permutes $\mathbb{F}_{3^{2m}}$ if and only if for each $d \in J$, the equation

$$(x + \delta)^{3^m(3^m+3)} - (x + \delta)^{3^m+3} + (x + \delta)^{3^m(2 \cdot 3^m+1)} - (x + \delta)^{2 \cdot 3^m+1} + ax^{3^m} + ax = d \quad (10)$$

has at most one solution in J . Since $x + x^{3^m} = 0$ for $x \in J$, the left-hand side of equation (10) can be simplified as

$$\begin{aligned} & (x + \delta)^{3^m(3^m+3)} - (x + \delta)^{3^m+3} + (x + \delta)^{3^m(2 \cdot 3^m+1)} - (x + \delta)^{2 \cdot 3^m+1} + ax^{3^m} + ax \\ &= (x + \delta)^{1+3^{m+1}} - (x + \delta)^{3^m+3} + (x + \delta)^{3^m+2} - (x + \delta)^{2 \cdot 3^m+1} \\ &= (x + \delta)(-x + \bar{\delta})^3 - (-x + \bar{\delta})(x + \delta)^3 + (x + \delta)^2(-x + \bar{\delta}) - (-x + \bar{\delta})^2(x + \delta) \\ &= (x + \delta)(-x + \bar{\delta})(2x - 2x(\bar{\delta} + \delta) + \bar{\delta}^2 - \delta^2 + (-\bar{\delta} + \delta)) \\ &= (x + \delta)(-x + \bar{\delta})(-2x(\delta + \bar{\delta} - 1) + (-\bar{\delta} + \delta) + \bar{\delta}^2 - \delta^2) \\ &= -(Tr_m^{2m}(\delta) - 1)(x + \delta)(-x + \bar{\delta})(2x - \bar{\delta} + \delta). \end{aligned}$$

If $Tr_m^{2m}(\delta) = 1$, then Eq. (10) reduces to $0 = d$ which clearly has more than one solution if $d = 0$. Therefore $f(x)$ is not a permutation polynomial if $(Tr_m^{2m}(\delta) - 1) = 0$.

Next, we assume $Tr_m^{2m}(\delta) \neq 1$. It is enough to show that the equation

$$x^3 - (Tr_m^{2m}(\delta))^2 x + \delta \bar{\delta}(-\bar{\delta} + \delta) = \frac{d}{1 - Tr_m^{2m}(\delta)} \quad (11)$$

has at most one solution in J . Suppose on the contrary that Eq. (11) has two solutions x and $x + b$, where $0 \neq b \in J$. Then we have

$$(x + b)^3 - (Tr_m^{2m}(\delta))^2(x + b) + \delta \bar{\delta}(\delta - \bar{\delta}) = \frac{d}{1 - Tr_m^{2m}(\delta)}. \quad (12)$$

Subtracting equation (11) from equation (12), we get

$$b^3 - (Tr_m^{2m}(\delta))^2 b = 0.$$

which is same as Eq. (4). By following the same arguments as in the proof Theorem 3.1, we get a contradiction. $\square$

Theorem 3.4. For any $a \in \mathbb{F}_{5^m}^*$ and $\delta \in \mathbb{F}_{5^{2m}}$, the polynomial

$$f(x) = (x^{5^m} - x + \delta)^{2.5^m+3} + ax^{5^m} + ax$$

is a permutation polynomial of $\mathbb{F}_{5^{2m}}$.

Proof. From Lemma 2.3, it is enough to show that for each $d \in J$, the equation

$$(x + \delta)^{5^m(2.5^m+3)} - (x + \delta)^{2.5^m+3} + ax^{5^m} + ax = d \quad (13)$$

has at most one solution in J . Since $x + x^{5^m} = 0$ for $x \in J$, the left-hand side of equation (13) can be simplified as

$$\begin{aligned} & (x + \delta)^{5^m(2.5^m+3)} - (x + \delta)^{2.5^m+3} + ax^{5^m} + ax \\ &= (x + \delta)^2(-x + \bar{\delta})^3 - (-x + \bar{\delta})^2(x + \delta)^3 \\ &= (x + \delta)^2(-x + \bar{\delta})^2(-2x - \delta + \bar{\delta}) \\ &= (x^2 + \delta^2 + 2x\delta)(x^2 + \bar{\delta}^2 - 2x\bar{\delta})(-2x - \delta + \bar{\delta}) \\ &= (x^4 + 2(\delta - \bar{\delta})x^3 + (\delta^2 + \bar{\delta}^2 - 4\delta\bar{\delta})x^2 + 2\delta\bar{\delta}(\bar{\delta} - \delta)x + \delta^2\bar{\delta}^2)(-2x - \delta + \bar{\delta}). \end{aligned}$$

Thus, it suffices to prove that the equation

$$-2x^5 + Tr_m^{2m}(\delta)^2 x^3 + (\bar{\delta} - \delta)Tr_m^{2m}(\delta)^2 x^2 + 2\delta\bar{\delta}Tr_m^{2m}(\delta)^2 x + \delta^2\bar{\delta}^2(\bar{\delta} - \delta) = d \quad (14)$$

has unique solution in J . Suppose on the contrary that Eq. (14) has two solutions x and $x + b$, where $0 \neq b \in J$. Then we have

$$-2(x + b)^5 + Tr_m^{2m}(\delta)^2(x + b)^3 + (\bar{\delta} - \delta)Tr_m^{2m}(\delta)^2(x + b)^2 + 2\delta\bar{\delta}Tr_m^{2m}(\delta)^2(x + b) + \delta^2\bar{\delta}^2(\bar{\delta} - \delta) = d. \quad (15)$$

By subtracting Eq. (14) from Eq. (15), we get

$$3b^5 + Tr_m^{2m}(\delta)^2(b^3 + 3xb^2 + 3x^2b) + (\bar{\delta} - \delta)Tr_m^{2m}(\delta)^2(2bx + b^2) + 2b\delta\bar{\delta}Tr_m^{2m}(\delta)^2 = 0. \quad (16)$$

Since $b \neq 0$, the above equation leads to

$$3b^4 + Tr_m^{2m}(\delta)^2(b^2 + 3xb + 3x^2) + (\bar{\delta} - \delta)Tr_m^{2m}(\delta)^2(2x + b) + 2\delta\bar{\delta}Tr_m^{2m}(\delta)^2 = 0.$$

Note that $Tr_m^{2m}(\delta) \neq 0$. Therefore the above equation can be rewritten as

$$\begin{aligned} 3x^2 + (3b + 2(\bar{\delta} - \delta))x + \frac{3b^4}{Tr_m^{2m}(\delta)^2} + b^2 + b(\bar{\delta} - \delta) + 2\delta\bar{\delta} &= 0 \\ \implies x^2 + (b - (\bar{\delta} - \delta))x + \frac{b^4}{Tr_m^{2m}(\delta)^2} + 2b^2 + 2b(\bar{\delta} - \delta) + 4\delta\bar{\delta} &= 0. \end{aligned}$$

Let $A = b - (\bar{\delta} - \delta)$ and $B = \frac{b^4}{Tr_m^{2m}(\delta)^2} + 2b^2 + 2b(\bar{\delta} - \delta) + 4\delta\bar{\delta}$. Then the discriminant of the polynomial on the left hand side of the above equation is

$$\begin{aligned} A^2 + B &= (b - (\bar{\delta} - \delta))^2 + \frac{b^4}{Tr_m^{2m}(\delta)^2} + 2b^2 + 2b(\bar{\delta} - \delta) + 4\delta\bar{\delta} \\ &= b^2 + (\bar{\delta} - \delta)^2 - 2b(\bar{\delta} - \delta) + \frac{b^4}{Tr_m^{2m}(\delta)^2} + 2b^2 + 2b(\bar{\delta} - \delta) + 4\delta\bar{\delta} \\ &= 3b^2 + (\delta + \bar{\delta})^2 + \frac{b^4}{Tr_m^{2m}(\delta)^2} \\ &= \frac{3b^2(\delta + \bar{\delta})^2 + (\delta + \bar{\delta})^4 + b^4}{Tr_m^{2m}(\delta)^2} \\ &= \frac{(b^2 - (\delta + \bar{\delta})^2)^2}{Tr_m^{2m}(\delta)^2}. \end{aligned}$$

Thus $x = \frac{-A \pm \sqrt{A^2 + B}}{2}$. Note that $\bar{A} = -A$ and $\sqrt{A^2 + B} \in \mathbb{F}_q$. Since $x \in J$, we must have

$$\frac{-A \pm \sqrt{A^2 + B}}{2} + \frac{-A \pm \sqrt{A^2 + B}}{2} = \frac{-A \pm \sqrt{A^2 + B}}{2} + \frac{A \pm \sqrt{A^2 + B}}{2} = 0,$$

which implies $\sqrt{A^2 + B} = 0$, i.e., $b^2 = Tr_m^{2m}(\delta)^2$. It follows that $b \in J \cap \mathbb{F}_q$ and hence $b = 0$, a contradiction. This completes the proof. $\square$

Theorem 3.5. For a positive integer m and $\delta \in \mathbb{F}_{5^{2m}}$, the polynomial

$$f(x) = (x^{5^m} - x + \delta)^{2.5^m+4} + ax^{5^m} + ax$$

for $a \in \mathbb{F}_{5^m}^*$ is a permutation polynomial of $\mathbb{F}_{5^{2m}}$ if and only if $Tr_m^{2m}(\delta) \neq 0$.

Proof. From lemma 2.3, the polynomial $f(x)$ permutes $\mathbb{F}_{5^{2m}}$ if and only if for each $d \in J$, the equation

$$(x + \delta)^{5^m(2.5^m+4)} - (x + \delta)^{2.5^m+4} + ax^{5^m} + ax = d \quad (17)$$

has at most one solution in J . Since $x + x^{3^m} = 0$ for $x \in J$, the left-hand side of equation (17) can be simplified as

$$\begin{aligned} &(x + \delta)^{5^m(2.5^m+4)} - (x + \delta)^{2.5^m+4} + ax^{5^m} + ax \\ &= (x + \delta)^2(-x + \bar{\delta})^4 - (-x + \bar{\delta})^2(x + \delta)^4 \\ &= (x + \delta)^2(-x + \bar{\delta})^2(-2x(\delta + \bar{\delta}) + \bar{\delta}^2 - \delta^2) \\ &= Tr_m^{2m}(\delta)(x + \delta)^2(-x + \bar{\delta})^2(-2x + \bar{\delta} - \delta) \\ &= Tr_m^{2m}(\delta)(x^2 + \delta^2 + 2x\delta)(x^2 + \bar{\delta}^2 - 2x\bar{\delta})(-2x + \bar{\delta} - \delta) \\ &= Tr_m^{2m}(\delta)(x^4 + 2(\delta - \bar{\delta})x^3 + (\delta^2 + \bar{\delta}^2 - 4\delta\bar{\delta})x^2 + 2\delta\bar{\delta}(\bar{\delta} - \delta)x + \delta^2\bar{\delta}^2)(-2x + \bar{\delta} - \delta). \end{aligned}$$

If $Tr_m^{2m}(\delta) = 0$, then Eq. (17) reduces to $0 = d$, which clearly has more than one solution if $d = 0$. Therefore $f(x)$ is not a permutation polynomial if $Tr_m^{2m}(\delta) = 0$.

Next, we assume $Tr_m^{2m}(\delta) \neq 0$. It is enough to show that the equation

$$-2x^5 + Tr_m^{2m}(\delta)^2 x^3 + (\bar{\delta} - \delta)Tr_m^{2m}(\delta)^2 x^2 + 2\delta\bar{\delta}Tr_m^{2m}(\delta)^2 x + \delta^2\bar{\delta}^2(\bar{\delta} - \delta) = \frac{d}{Tr_m^{2m}(\delta)} \quad (18)$$

has unique solution in J . Suppose on the contrary that Eq. (18) has two solutions x and $x + b$, where $0 \neq b \in J$. Then we have

$$-2(x+b)^5 + Tr_m^{2m}(\delta)^2(x+b)^3 + (\bar{\delta} - \delta)Tr_m^{2m}(\delta)^2(x+b)^2 + 2\delta\bar{\delta}Tr_m^{2m}(\delta)^2(x+b) + \delta^2\bar{\delta}^2(\bar{\delta} - \delta) = \frac{d}{Tr_m^{2m}(\delta)}. \quad (19)$$

By subtracting Eq. (18) from Eq. (19), we get

$$3b^5 + Tr_m^{2m}(\delta)^2(b^3 + 3xb^2 + 3x^2b) + (\bar{\delta} - \delta)Tr_m^{2m}(\delta)^2(2bx + b^2) + 2b\delta\bar{\delta}Tr_m^{2m}(\delta)^2 = 0,$$

which is same as Eq. (16). By following the same arguments as in the proof of Theorem 3.4, we get a contradiction. $\square$

Theorem 3.6. For a positive integer m and $\delta \in \mathbb{F}_{5^{2m}}$, the polynomial

$$f(x) = (x^{5^m} - x + \delta)^{2.5^m+3} + (x^{5^m} - x + \delta)^{2.5^m+4} + ax^{5^m} + ax$$

for $a \in \mathbb{F}_{5^m}^*$ is a permutation polynomial of $\mathbb{F}_{5^{2m}}$ if and only if $Tr_m^{2m}(\delta) + 1 \neq 0$.

Proof. From lemma 2.3, the polynomial $f(x)$ permutes $\mathbb{F}_{5^{2m}}$ if and only if for each $d \in J$, the equation

$$(x + \delta)^{5^m(2.5^m+3)} - (x + \delta)^{2.5^m+3} + (x + \delta)^{5^m(2.5^m+4)} - (x + \delta)^{2.5^m+4} = d \quad (20)$$

has at most one solution in J . Since $x + x^{5^m} = 0$ for $x \in J$, the left-hand side of equation (20) can be simplified as

$$\begin{aligned} & (x + \delta)^{5^m(2.5^m+3)} - (x + \delta)^{2.5^m+3} + (x + \delta)^{5^m(2.5^m+4)} - (x + \delta)^{2.5^m+4} + ax^{5^m} + ax \\ &= (x + \delta)^2(-x + \bar{\delta})^3 - (-x + \bar{\delta})^2(x + \delta)^3 + (x + \delta)^2(-x + \bar{\delta})^4 - (-x + \bar{\delta})^2(x + \delta)^4 \\ &= (x + \delta)^2(-x + \bar{\delta})^2(-2x(\delta + \bar{\delta} + 1) + (\bar{\delta} - \delta) + \delta^2 - \delta^2) \\ &= (Tr_m^{2m}(\delta) + 1)(x + \delta)^2(-x + \bar{\delta})^2(-2x + \bar{\delta} - \delta) \\ &= (Tr_m^{2m}(\delta) + 1)((x^2 + \delta^2 + 2x\delta)(x^2 + \bar{\delta}^2 - 2x\bar{\delta})(-2x + \bar{\delta} - \delta)) \\ &= (Tr_m^{2m}(\delta) + 1)(x^4 + 2(\delta - \bar{\delta})x^3 + (\delta^2 + \bar{\delta}^2 - 4\delta\bar{\delta})x^2 + 2\delta\bar{\delta}(\bar{\delta} - \delta)x + \delta^2\bar{\delta}^2)(-2x + \bar{\delta} - \delta). \end{aligned}$$

If $Tr_m^{2m}(\delta) + 1 = 0$, then Eq. (20) reduces to $0 = d$, which clearly has more than one solution if $d = 0$. Therefore $f(x)$ is not a permutation polynomial if $Tr_m^{2m}(\delta) + 1 = 0$.

Next, we assume $Tr_m^{2m}(\delta) + 1 \neq 0$. It is enough to show that the equation

$$-2x^5 + Tr_m^{2m}(\delta)^2 x^3 + (\bar{\delta} - \delta)Tr_m^{2m}(\delta)^2 x^2 + 2\delta\bar{\delta}Tr_m^{2m}(\delta)^2 x + \delta^2\bar{\delta}^2(\bar{\delta} - \delta) = \frac{d}{Tr_m^{2m}(\delta) + 1} \quad (21)$$

has unique solution in J . Suppose on the contrary that Eq. (18) has two solutions x and $x + b$, where $0 \neq b \in J$. Then we have

$$\begin{aligned} & -2(x+b)^5 + Tr_m^{2m}(\delta)^2(x+b)^3 + (\bar{\delta} - \delta)Tr_m^{2m}(\delta)^2(x+b)^2 + 2\delta\bar{\delta}Tr_m^{2m}(\delta)^2(x+b) \\ & \quad + \delta^2\bar{\delta}^2(\bar{\delta} - \delta) = \frac{d}{Tr_m^{2m}(\delta) + 1}. \end{aligned} \quad (22)$$

By subtracting Eq. (21) from Eq. (22), we get

$$3b^5 + Tr_m^{2m}(\delta)^2(b^3 + 3xb^2 + 3x^2b) + (\bar{\delta} - \delta)Tr_m^{2m}(\delta)^2(2bx + b^2) + 2b\delta\bar{\delta}Tr_m^{2m}(\delta)^2 = 0,$$

which is same as Eq. (16). By following the same arguments as in the proof of Theorem 3.4, we get a contradiction. $\square$

4. Conclusion

In this paper, for $p = 3$ or $p = 5$, we present three classes of permutation polynomials of the form $(x^{p^m} - x + \delta)^s + L(x)$ and three classes of permutation polynomials of the form $(x^{p^m} - x + \delta)^{s_1} + (x^{p^m} - x + \delta)^{s_2} + L(x)$ over the finite field $\mathbb{F}_{p^{2m}}$ are given, where $L(x) = ax^{p^m} + ax$ and $a \in \mathbb{F}_{p^m}^*$. We also proved that the conditions on δ are necessary and sufficient. In the Table 1 and Table 2, we list all the known classes (to the best of authors' knowledge) of permutation polynomials of the form $(x^{p^m} - x + \delta)^s + ax^{p^m} + bx$ and $(x^{p^m} - x + \delta)^{s_1} + (x^{p^m} - x + \delta)^{s_2} + ax^{p^m} + bx$, respectively.

Table 1. Known permutation polynomials of the form $(x^{p^m} - x + \delta)^s + ax^{p^m} + bx$ over $\mathbb{F}_{p^{2m}}$, where p is odd.

i	Values of s	Conditions on p, a, b, δ	Reference
1	$3^{2m-1} + 2 \cdot 3^{m-1}$	$p = 3, a = b = 1$, all δ	[19, Theorem 4.1]
2	$\frac{3^{2m}+1}{2}, \frac{3^{2m}+2 \cdot 3^{m-1}}{2}$, $3^{2m} - 3^m + 1$ or $2 \cdot 3^{2m-1} + 3^{m-1}$	$p = 3, a = b = 1$, all δ	[19, Theorem 4.2]
3	$\frac{p^{2m}+1}{2}$	p odd, $a = b = 1, Tr_m^{2m}(\delta) \neq 0$	[29, Theorem 1]
4	$\frac{p^{2m}+1}{2}$	p odd, $a = b = 1$, all δ	[9, Theorem 2] and [26, Theorem 4.1]
5	$\frac{p^{2m}-1}{2} + p^{2m}$	p odd, $a = b = 1$, all δ	[9, Theorem 6]
6	$\frac{p^{2m}-1}{2} + p^{2m}$	p odd, $a = b = -1$, all δ	[9, Theorem 7]
7	$2 \cdot 3^m - 1$	$p = 3, a = b = 1$, all δ	[18, Theorem 1]
8	$i(p^m + 1) + 1$ where $0 < i < p^m - 1$ $\gcd(1 + 2i, p^m - 1) = 1$	p odd, $a = b = 1, Tr_m^{2m}(\delta) = 0$	[18, Theorem 5]
9	$\frac{p^{2m}-1}{2} + 1$	p odd, $a = b \in \mathbb{F}_{p^m}^*, Tr_m^{2m}(\delta) = 0$	[28, Theorem 3.3]
10	$\frac{p^{2m}-1}{d} + 1$, $p^m \equiv 1 \pmod{d}$, $\gcd(\frac{p^{2m}-1}{d} + 1, d) = 1$ $d > 1$	p odd, $a = b \in \mathbb{F}_{p^m}^*, Tr_m^{2m}(\delta) = 0$	[28, Theorem 4.11]
11	$\frac{p^m+1}{2}, p^m \equiv 1 \pmod{4}$	p odd, $a = b = 1, Tr_m^{2m}(\delta) = 0$	[31, Theorem 1]
12	$\frac{3^{2m}-1+1}{2}$	$p = 3, a = b = 1, Tr_m^{2m}(\delta) \neq 0$	[31, Theorem 2]
13	$t(p^m - 1) + 1$, $0 < t \leq p^m$	p odd, $a = b = 1, Tr_m^{2m}(\delta) = 0$	[22, Theorem 3.2]
14	$i(p^m + 1)$ where $i \in \mathbb{N}$	p odd, $a, b \in \mathbb{F}_{p^{2m}}^*$ with $a + b \in \mathbb{F}_{p^m}^*$, $b \neq a^{p^m}$, all δ	[10, Proposition 5]
15	s is even	p odd, $a, b \in \mathbb{F}_{p^{2m}}^*$ with $a + b \in \mathbb{F}_{p^m}^*$, $b \neq a^{p^m}, Tr_m^{2m}(\delta) = 0$	[10, Proposition 5]
16	$2p^m$	p odd, $a, b \in \mathbb{F}_{p^{2m}}^*$ with $a + b \in \mathbb{F}_{p^m}^*$, $2Tr_m^{2m}(\delta) + b - a^{p^m} \neq 0$	[10, Proposition 6]
17	$3^{2m-1} + 2 \cdot 3^{m-1}$	$p = 3, a, b \in \mathbb{F}_{3^{2m}}^*$ with $a + b \in \mathbb{F}_{3^m}^*$, $b - a^{3^m} + 1$ is a square in $\mathbb{F}_{3^m}^*$, all δ	[10, Proposition 6]
18	$p^i + p^j$ where $i, j < 2m$	p odd, $a, b \in \mathbb{F}_{p^{2m}}^*$ with $a + b \in \mathbb{F}_{p^m}^*$, $b \neq a^{p^m}, Tr_m^{2m}(\delta) = 0$ or $Tr_m^{2m}(\delta) \neq 0$ with $\frac{b - a^{p^m}}{Tr_m^{2m}(\delta)^{p^i + p^j - 1}} \notin \{\alpha^{p^i - 1} + \alpha^{p^j - 1} \mid \alpha \in J\}$ where $J = \{\gamma^{p^m} - \gamma \mid \gamma \in \mathbb{F}_{p^{2m}}\}$	[10, Proposition 7]

19	$p^{m+1} + 1$	p odd, $a, b \in \mathbb{F}_{p^{2m}}^*$ with $a + b \in \mathbb{F}_{p^m}^*$, $b \neq a^{p^m}$, $Tr_m^{2m}(\delta) = 0$ or $\frac{(Tr_m^{2m}(\delta))^p - b + a^{p^m}}{Tr_m^{2m}(\delta)}$ is $(p-1)$ -th power in $\mathbb{F}_{p^m}^*$	[15, Theorem 10]
20	$2p^i$, $0 < i < 2m$	p odd, $b = a^{p^m}$, $a + b \neq 0$ and $Tr_m^{2m}(\delta) \neq 0$	[2, Theorem 3.11]
21	$\frac{p^{2m+3}}{2}$	p odd, $b = a^{p^m}$, $a + b \neq 0$ and $Tr_m^{2m}(\delta) \neq 0$	[2, Theorem 3.13]
22	$p^i + 1$, $0 < i < 2m$	p odd, $b = a^{p^m}$, $\gcd(2(p^i - 1), p^{2m} - 1) = 4$, $p^m - 1 \equiv 0 \pmod{4}$ $a + b \neq 0$ and $Tr_m^{2m}(\delta) \neq 0$	[2, Theorem 3.14]
23	$p^m + p^i$, $i \mid m$	p odd, $b = a^{p^m}$, $a + b \neq 0$ and $Tr_m^{2m}(\delta) \neq 0$	[2, Theorem 3.15]
24	$s \geq 0$ with $\gcd(s, p^m - 1) = 1$	p odd, $b = a^{p^m}$, $a + b \neq 0$ and $Tr_m^{2m}(\delta) = 0$; or all $\delta \in \mathbb{F}_{p^n}$ if s is a power of p .	[2, Theorem 3.17]
25	$p^m + 2$	$p = 3$, $b = a^{p^m}$, $a + b \neq 0$, all δ	[2, Theorem 3.18]
26	$i(p^m + 1) + 1$, $0 < i < p^m - 1$	p odd, $b = a^{p^m}$, $a + b \neq 0$, $Tr_m^{2m}(\delta) = 0$ $\gcd(1 + 2i, p^m - 1) = 1$	[2, Theorem 3.18]
27	$p^{m+1} + 1$	p odd, $b = a^{p^m}$, $a + b \neq 0$, $Tr_m^{2m}(\delta) \neq 0$	[8, Proposition 2]
28	$2p^m$	p odd, $a = b = 1$, $Tr_m^{2m}(\delta) \neq 0$	[8, Proposition 3]
29	$i(p^m - 1) + 1$	p odd, $a + b \neq 0$ and $Tr_m^{2m}(\delta) = 0$, and $(-1)^{i+1}Tr_m^{2m}(a + b) + b^{p^m+1} - a^{p^m+1} \neq 0$	[23, Proposition 9]
30	$p^m + 2$	$p = 3$, $a + b \neq 0$ and $(Tr_m^{2m}(\delta))^2 + b - a^{p^m}$ is a square in $\mathbb{F}_{p^m}$	[23, Proposition 13]
31	$2 \cdot p^m + 1$	$p = 3$, $a + b \neq 0$ and $(Tr_m^{2m}(\delta))^2 - b + a^{p^m}$ is a square in $\mathbb{F}_{p^m}$	[23, Proposition 13]
32	$2 \cdot p^{2m-1} + p^{m-1}$	$p = 3$, $a + b \neq 0$ and $Tr_m^{2m}(\delta) = 0$ $a^{p^m} \neq b$	[23, Proposition 13]
33	$2 \cdot p^{2m-1} + p^{m-1}$	$p = 3$, $a + b \neq 0$ and $Tr_m^{2m}(\delta) \neq 0$ $a^{p^m} - b$ is a square in $\mathbb{F}_{p^m}$	[23, Proposition 13]
34	$2 \cdot 3^m + 1$	$p = 3$, $a = b \in \mathbb{F}_{3^m}^*$, all δ	This paper
35	$2 \cdot 5^m + 3$	$p = 5$, $a = b \in \mathbb{F}_{5^m}^*$, all δ	This paper
36	$2 \cdot 5^m + 4$	$p = 5$, $a = b \in \mathbb{F}_{5^m}^*$, $Tr_m^{2m}(\delta) \neq 0$	This paper

Table 2. Known permutation polynomials of the form $(x^{p^m} - x + \delta)^{s_1} + (x^{p^m} - x + \delta)^{s_2} + ax^{p^m} + bx$ over $\mathbb{F}_{p^{2m}}$, where p is odd.

i	s_1 and s_2	Conditions on p, a, b, δ	Reference
1	$s_1 = 2 \cdot 3^{m+k} + 3^l$; $s_2 = 2 \cdot 3^{m+k} + 3^{m+l}$ k, l are non negative integers and $\gcd(k, 2m) = 1$	$p = 3, a, b \in \mathbb{F}_{3^{2m}}^*$ with $a + b \in \mathbb{F}_{3^m}^*$, $b - a^{3^m}$ is a square in $\mathbb{F}_{3^m}^*$, all δ	[10, Proposition 6]
2	$s_1 = 3^m + 4; s_2 = 5$	$p = 3, a, b \in \mathbb{F}_{3^{2m}}^*$ with $a + b \in \mathbb{F}_{3^m}^*$, $b - a^{3^m} \neq 0, b - a^{3^m} + (Tr_m^{2m}(\delta))^4$ is an square element in $\mathbb{F}_{3^m}^*$	[10, Proposition 6]
3	$s_1 = 3^m + 2$; $s_2 = 2 \cdot 3^{im}, i \in \{0, 1\}$	$p = 3, a, b \in \mathbb{F}_{3^{2m}}^*, a + b \in \mathbb{F}_{3^m}^*$, $[(Tr_m^{2m}(\delta)) - (i - 1)]^2 + b - a^{3^m}$ is a square in $\mathbb{F}_{3^m}^*$	[10, Proposition 6]
4	$s_1 = \frac{i(p^{2m}-1)}{p^2-1} + 1, m$ is even; $s_2 = \frac{i(p^{2m}-1)}{p^2-1} + p^m, m$ is even	p odd, $a, b \in \mathbb{F}_{p^{2m}}^*$ with $a + b \in \mathbb{F}_{p^m}^*$ $b \neq a^{p^m}$, all δ	[15, Theorem 11]
5	$s_1 = 2 \cdot p^m$, $s_2 = p^{m+1} + 1$	p odd, $a, b \in \mathbb{F}_{p^{2m}}^*$ with $a + b \in \mathbb{F}_{p^m}^*$, $(b - a^{p^m}) \neq 0, Tr_m^{2m}(\delta) = 0$ or $\frac{(Tr_m^{2m}(\delta))^{p-b+a^{p^m}} - 2Tr_m^{2m}(\delta)}{Tr_m^{2m}(\delta)}$ is $(p - 1)$ -th power in $\mathbb{F}_{p^m}^*$	[15, Theorem 12]
6	$s_1 = 2 \cdot 3^m$; $s_2 = 3^{2m-1} + 2 \cdot 3^{m-1}$	$p = 3, a, b \in \mathbb{F}_{3^{2m}}^*$ and $a + b \in \mathbb{F}_{3^m}^*$ $b - a^{3^m} \neq -1$ and $Tr_m^{2m}(\delta) = 0$ or $2Tr_m^{2m}(\delta) - a^{3^m} + b + 1$ is a square elements in $\mathbb{F}_{3^m}^*$	[15, Theorem 13]
7	$s_1 = 3^{2m-1} + 2 \cdot 3^{m-1}$, $s_2 = 2 \cdot 3^{2m-1} + 3^{m-1}$	$p = 3, a, b \in \mathbb{F}_{3^{2m}}^*$ with $a + b \in \mathbb{F}_{3^m}^*$, $b - a^{3^m} \neq 0$, all δ	[15, Theorem 14]
8	$s_1 = 3^{2m} + 3^m + 1$ $s_2 = 3^{m+1} + 1$	$p = 3, a = b \in \mathbb{F}_{3^m}^*$, $Tr_m^{2m}(\delta) \neq 1$	This paper
9	$s_1 = 3^m + 3$, $s_2 = 2 \cdot 3^m + 1$	$p = 3, a = b \in \mathbb{F}_{3^m}^*$, $Tr_m^{2m}(\delta) \neq 1$	This paper
10	$s_1 = 2 \cdot 5^m + 3$, $s_2 = 2 \cdot 5^m + 4$	$p = 5, a = b \in \mathbb{F}_{5^m}^*$, $Tr_m^{2m}(\delta) + 1 \neq 0$	This paper

Acknowledgment

The authors thank the anonymous referees and the editor for their comments and suggestions. The first author is supported by the University Grants Commission(UGC), India, under the grant number 1089/(CSIR-UGC NET DEC. 2016).

References

- [1] A. Akbary, D. Ghioca, and Q. Wang, [On constructing permutations of finite fields](#), Finite Fields Appl. 17(1) (2011) 51–67.

- [2] C. Chen, H. Kan, Y. Li, J. Peng, and L. Zheng, [Several classes of permutation polynomials of the form \$\(x^{p^m} - x + \delta\)^s + L\(x\)\$](#) , *Adv. Math. Commun.* 19(1) (2025) 319–336.
- [3] C. Ding and T. Helleseeth, [Optimal ternary cyclic codes from monomials](#), *IEEE Trans. Inform. Theory* 59(9) (2013) 5898–5904.
- [4] C. Ding and J. Yuan, [A family of skew Hadamard difference sets](#), *J. Combin. Theory Ser. A* 113(7) (2006) 1526–1535.
- [5] R. Gupta and R. K. Sharma, [Further results on permutation polynomials of the form \$\(x^{p^m} - x + \delta\)^s + x\$ over \$\mathbb{F}_{p^{2m}}\$](#) , *Finite Fields Appl.* 50 (2018) 196–208.
- [6] T. Helleseeth and V. Zinoviev, [New Kloosterman sums identities over \$\mathbb{F}_{2^m}\$ for all \$m\$](#) , *Finite Fields Appl.* 9(2) (2003) 187–193.
- [7] Y. Laigle-Chapuy, [Permutation polynomials and applications to coding theory](#), *Finite Fields Appl.* 13(1) (2007) 58–70.
- [8] G. Li and X. Cao, [Several classes of permutation polynomials over the finite field \$\mathbb{F}_{p^{2m}}\$](#) , *Finite Fields Appl.* 89 (2023) 102197.
- [9] N. Li, T. Helleseeth, and X. Tang, [Further results on a class of permutation polynomials over finite fields](#), *Finite Fields Appl.* 22 (2013) 16–23.
- [10] L. Li, C. Li, C. Li, and X. Zeng, [New classes of complete permutation polynomials](#), *Finite Fields Appl.* 55 (2019) 177–201.
- [11] K. Li, L. Qu, and Y. Zhou, [A link between two classes of permutation polynomials](#), *Finite Fields Appl.* 63 (2020) 101641.
- [12] L. Li, S. Wang, C. Li, and X. Zeng, [Permutation polynomials \$\(x^{p^m} - x + \delta\)^{s_1} + \(x^{p^m} - x + \delta\)^{s_2} + x\$ over \$\mathbb{F}_{p^n}\$](#) , *Finite Fields Appl.* 51 (2018) 31–61.
- [13] R. Lidl and W. B. Müller, [Permutation Polynomials in RSA-Cryptosystems](#), in: D. Chaum, ed., *Advances in Cryptology*, Springer, Boston, MA (1984).
- [14] R. Lidl and H. Niederreiter, [Finite fields](#), 2nd ed., Cambridge University Press, Cambridge (1996).
- [15] Q. Liu, J. Xie, X. Liu, and J. Zou, [Further results on permutation polynomials and complete permutation polynomials over finite fields](#), *AIMS Math.* 6(12) (2021) 13503–13514.
- [16] J. Schwenk and K. Huber, [Public key encryption and digital signatures based on permutation polynomials](#), *Electron. Lett.* 34(8) (1998) 759–760.
- [17] Z. Tu, X. Zeng, and Y. Jiang, [Two classes of permutation polynomials having the form \$\(x^{2^m} + x + \delta\)^s + x\$](#) , *Finite Fields Appl.* 31 (2015) 12–24.
- [18] Z. Tu, X. Zeng, C. Li, and T. Helleseeth, [Permutation polynomials of the form \$\(x^{p^m} - x + \delta\)^s + L\(x\)\$ over the finite field \$\mathbb{F}_{p^{2m}}\$ of odd characteristic](#), *Finite Fields Appl.* 34 (2015) 20–35.
- [19] L. Wang, B. Wu, and Z. Liu, [Further results on permutation polynomials of the form \$\(x^{p^m} - x + \delta\)^s + L\(x\)\$ over \$\mathbb{F}_{p^{2m}}\$](#) , *Finite Fields Appl.* 44 (2017) 92–112.
- [20] D. Wu and P. Yuan, [Some classes of permutation polynomials of the form \$b\(x^q + ax + \delta\)^{1+i\(q^2-1\)/d} + c\(x^q + ax + \delta\)^{1+j\(q^2-1\)/d} + L\(x\)\$ over \$\mathbb{F}_{q^2}\$](#) , *Appl. Algebra Engrg. Comm. Comput.* 33 (2022) 135–149.
- [21] D. Wu and P. Yuan, [Some new results on permutation polynomials of the form \$b\(x^q + ax + \delta\)^s - ax\$ over \$\mathbb{F}_{q^2}\$](#) , *Finite Fields Appl.* 93 (2024) 102329.
- [22] G. Xu, X. Cao, and S. Xu, [Further results on permutation polynomials of the form \$\(x^{p^m} - x + \delta\)^s + L\(x\)\$ over \$\mathbb{F}_{p^{2m}}\$](#) , *J. Algebra Appl.* 15(5) (2016) 1650098.
- [23] X. Xu, X. Feng, and X. Zeng, [Complete permutation polynomials with the form \$\(x^{p^m} - x + \delta\)^s + ax^{p^m} + bx\$ over \$\mathbb{F}_{p^n}\$](#) , *Finite Fields Appl.* 57 (2019) 309–343.
- [24] G. Xu, G. Luo, and X. Cao, [Several classes of permutation polynomials of the form \$\(x^{p^m} - x + \delta\)^s + x\$ over \$\mathbb{F}_{p^{2m}}\$](#) , *Finite Fields Appl.* 79 (2022) 102001.
- [25] J. Yuan and C. Ding, [Four classes of permutation polynomials of \$\mathbb{F}_{2^m}\$](#) , *Finite Fields Appl.* 13(4) (2007) 869–876.
- [26] P. Yuan and C. Ding, [Further results on permutation polynomials over finite fields](#), *Finite Fields Appl.* 27 (2014) 88–103.
- [27] J. Yuan, C. Ding, H. Wang, and J. Pieprzyk, [Permutation polynomials of the form \$\(x^{p^m} - x + \delta\)^s + L\(x\)\$](#) , *Finite Fields Appl.* 14(2) (2008) 482–493.
- [28] P. Yuan and Y. Zheng, [Permutation polynomials from piecewise functions](#), *Finite Fields Appl.* 35 (2015) 215–230.

- [29] Z. Zha and L. Hu, [Two classes of permutation polynomials over finite fields](#), *Finite Fields Appl.* 18(4) (2012) 781–790.
- [30] Z. Zha and L. Hu, [Some classes of permutation polynomials of the form \$\(x^{p^m} - x + \delta\)^s + x\$ over \$\mathbb{F}_{p^{2m}}\$](#) , *Finite Fields Appl.* 40 (2016) 150–162.
- [31] D. Zheng and Z. Chen, [More classes of permutation polynomials of the form \$\(x^{p^m} - x + \delta\)^s + L\(x\)\$](#) , *Appl. Algebra Engrg. Comm. Comput.* 28 (2017) 215–223.
- [32] D. Zheng, M. Yuan, and L. Yu, [Two types of permutation polynomials with special forms](#), *Finite Fields Appl.* 56 (2019) 1–16.