Several classes of permutation polynomials of the form $(x^{p^m} - x + \delta)^s + x$ over $\mathbb{F}_{p^{2m}}$

Guangkui Xu[a], Gaojun Luo[b], Xiwang Cao[c,d]

[a] School of Finance and Mathematics, Huainan Normal University, Huainan 232038, China
[b] School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, Singapore 637371, Singapore
[c] Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China
[d] Key Laboratory of Mathematical Modeling and High Performance Computing of Air Vechicles (NUAA), MIIT, Nanjing 210016, China

Abstract

In this paper, we give a further study on the permutation behavior of polynomials of a special form by considering the number of solutions of certain equations over finite fields. First, four classes of permutation polynomials of the form $(x^{2^m} + x + \delta)^s + x$ over $\mathbb{F}_{2^{2m}}$ are presented. Notably, some necessary and sufficient conditions for this kind of polynomials to permute $\mathbb{F}_{2^{2m}}$ are provided. Second, we present several classes of permutation polynomials of the form $(x^{p^m} - x + \delta)^s + x$ over $\mathbb{F}_{p^{2m}}$ of odd characteristic, some of which can provide complete permutation polynomials of this form over $\mathbb{F}_{3^{2m}}$.

Keywords: Finite field, Permutation polynomial, Complete permutation polynomial, Trace function
2000 MSC: 05A05; 11T06; 11T55

1. Introduction

Let q be a power of a prime p, and $\mathbb{F}_q$ be the finite field containing q elements. Let $\mathbb{F}_q^*$ denote the multiplicative group of $\mathbb{F}_q$. A polynomial $f(x) \in \mathbb{F}_q[x]$ is called a *permutation polynomial* (PP) of $\mathbb{F}_q$ if the function $f : c \mapsto f(c)$ from $\mathbb{F}_q$ to $\mathbb{F}_q$ induces a permutation. A permutation polynomial $f(x) \in \mathbb{F}_q[x]$ is a *complete permutation polynomial* (CPP) over $\mathbb{F}_q$ if $f(x) + x$ permutes $\mathbb{F}_q$ as well. Permutation polynomials over finite fields have been widely studied in recent years due to their significant applications in cryptography, coding theory, and combinatorial design theory. In general, finding new permutation polynomials of finite fields is not an easy task. For more introduction to permutations polynomials, we refer to [8, Chapter 7] and [10, Chapter 8]. The most recent survey paper on permutation polynomials is [5].

Email address: xuguangkuiy@163.com, gjluo1990@163.com, xwcao@nuaa.edu.cn (Guangkui Xu[a], Gaojun Luo[b], Xiwang Cao[c,d])

To derive new Kloosterman sums identities over $\mathbb{F}_{2^n}$, Helleseth and Zinoviev [3] first studied an important class of permutation polynomials of the form

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

where $s = 1$ or 2 and $\delta \in \mathbb{F}_{2^n}$. Motivated by Helleseth and Zinoviev's work, Yuan and Ding [14, 15] investigated the permutation behavior of polynomials of the form

$$(x^{p^k} - x + \delta)^s + L(x) \tag{1}$$

over $\mathbb{F}_{p^n}$, where k, s are integers, $\delta \in \mathbb{F}_{2^n}$ and $L(x)$ is a linearized polynomial. Subsequently, a number of research works have been devoted to the construction of permutation polynomials with the form as in (1). For more details, the reader is referred to [2, 6, 7, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 23, 24]. After these work, there are two extensions of permutation polynomials with the form as in (1): (i) Zeng, Tian and Tu [21] presented several classes of permutation polynomials of the form

$$(\mathrm{Tr}_m^n(x) + \delta)^s + L(x) \tag{2}$$

over $\mathbb{F}_{2^n}$, where $m \mid n$, $L(x) = x$ or $\mathrm{Tr}_m^n(x) + x$, and $\mathrm{Tr}_m^n(x)$ is the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$; (ii) permutation polynomials of the form

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

over $\mathbb{F}_{p^n}$ were investigated in [9, 22].

In this paper, we first further discuss the permutation behavior of polynomials of the form $(x^{2^m} + x + \delta)^s + x$ over $\mathbb{F}_{2^{2m}}$. In particular, based on the technique used in [9], four classes of permutation polynomials of the form $(x^{2^m} + x + \delta)^s + x$ are given over $\mathbb{F}_{2^{2m}}$ for $s = 2^{m+1} + 1, 3 \cdot 2^m + 2, 2^{2m} - 2$ or $2^{2m} - 3$. The second objective of this paper is to construct permutation polynomials of the form $(x^{p^m} - x + \delta)^s$ over the finite field $\mathbb{F}_{p^{2m}}$ of odd characteristic. Some complete permutation polynomials of such form over $\mathbb{F}_{3^{2m}}$ are also presented. Determining the number of solutions to special equations with degree 3, 4 or 5 over finite fields plays a vital role in our constructions.

The paper is organized as follows. In Section 2, we introduce notation and some related results. In Section 3, we present several classes of permutation polynomials over $\mathbb{F}_{2^n}$ by using a lemma given by [9, Lemma 2]. In Section 4, we obtain some permutation polynomials and complete permutation polynomials with the form as in (1) over finite fields of odd characteristic.

2. Preliminaries

In this section, we introduce the basic notation and give related results of the number of solutions to some equations over finite fields . For any positive integer m dividing n, the trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$, denoted by $\mathrm{Tr}_m^n(\cdot)$, is defined as

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

Define a subset of $\mathbb{F}_{p^n}$ by $\mathcal{J} = \{x^{p^m} - x \mid x \in \mathbb{F}_{p^n}\}$. It is clear that $\mathrm{Tr}_m^n(\beta) = 0$ for any $\beta \in \mathcal{J}$.

To investigate the permutation behavior of some polynomials of the form $(x^{p^m} - x + \delta)^s + x$ over $\mathbb{F}_{p^{2m}}$, we need the following lemma, which is a direct consequence of Lemma 2 in [9].

Lemma 2.1. *For a positive integer m and a fixed $\delta \in \mathbb{F}_{p^{2m}}$, the polynomial*

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

permutes $\mathbb{F}_{p^{2m}}$ if and only if $(x+\delta)^{p^m s} - (x+\delta)^s + x$ permutes $\mathcal{J}$.

In what follows, a series of auxiliary results of the number of solutions to some equations over finite fields are described, which play a key role in later proofs.

Lemma 2.2. *[8] For a positive integer m, the quadratic equation $x^2 + ax + b = 0$, $a, b \in \mathbb{F}_{2^m}$, $a \neq 0$, has solutions in $\mathbb{F}_{2^m}$ if and only if $\mathrm{Tr}_1^m(\frac{b}{a^2}) = 0$.*

Lemma 2.3. *(see [1, Theorem 2].) For $a \in \mathbb{F}_{2^m}^*$, the cubic equation $x^3 + x + a = 0$ has*

1) *a unique solution in $\mathbb{F}_{2^m}$ if and only if $\mathrm{Tr}_1^m(a^{-1}) \neq \mathrm{Tr}_1^m(1)$;*

2) *three distinct solutions in $\mathbb{F}_{2^m}$ if and only if $P_m(a) = 0$, where the polynomials $P_m(x)$ are recursively defined by the equations $P_1(x) = P_2(x) = x, P_k(x) = P_{k-1}(x) + x^{2^{k-3}} P_{k-2}(x)$ for $k \geq 3$;*

3) *no solution in $\mathbb{F}_{2^m}$, otherwise.*

Lemma 2.4. *[12, Lemma 4] For $q = p^m$ odd, $a, b \in \mathbb{F}_{p^m}$, the quadratic equation $x^2 + ax + b = 0$ has solutions in $\mathbb{F}_q$ if and only if the discriminant $\Delta = b^2 - 4a$ is either 0 or a square.*

The next lemma is about the solutions of the cubic equation over finite fields of odd characteristic, which is a corollary of Theorem 1.8.8 in [4].

Lemma 2.5. *[4] For $q = p^m$ odd, $a_0 \in \mathbb{F}_q^*, a_1, a_2, a_3 \in \mathbb{F}_q$, if*

$$\Delta = a_1^2 a_2^2 - 4a_0 a_2^3 - 4a_1^3 a_3 - 27a_0^2 a_3^2 + 18a_0 a_1 a_2 a_3 \neq 0,$$

then the cubic equation $a_0 x^3 + a_1 x^2 + a_2 x + a_3 = 0$ has exactly one solution in $\mathbb{F}_q$ if and only if the discriminant Δ is a nonsquare.

For each $a \in \mathbb{F}_{p^{2m}}$, the conjugate of a is defined by $\overline{a} = a^{p^m}$. For $a, b \in \mathbb{F}_{p^{2m}}$, it is easy to verify that $a + \overline{a}, a\overline{a} \in \mathbb{F}_{p^m}$ and $\overline{a+b} = \overline{a} + \overline{b}, \overline{ab} = \overline{a}\,\overline{b}$.

Lemma 2.6. *[12, Lemma 2] Let m be a positive integer. Let $N(a, b)$ denote the number of solutions of the equation*

$$x^{p^m} - ax + b = 0 \tag{3}$$

in $\mathbb{F}_{p^{2m}}$, where $a, b \in \mathbb{F}_{p^{2m}}$ and $a \neq 0$. Then

$$N(a,b) = \begin{cases} 1, & \text{if } \overline{a}a \neq 1; \\ 0, & \text{if } \overline{a}a = 1 \text{ and } \overline{a}b + \overline{b} \neq 0; \\ p^m, & \text{if } \overline{a}a = 1 \text{ and } \overline{a}b + \overline{b} = 0. \end{cases}$$

Moreover, the unique solution of (3) is $\frac{\overline{a}b+\overline{b}}{a\overline{a}-1}$ when $\overline{a}a \neq 1$.

Lemma 2.7. *[12, Lemma 5] For an odd prime p and $a, b \in \mathbb{F}_{p^m}$, the equation $x^p - ax + b = 0$ has a unique solution in $\mathbb{F}_{p^m}$ if and only if $a = 0$ or a is not a $(p-1)$-th power in $\mathbb{F}_{p^m}$.*

3. Four classes of permutation polynomials over $\mathbb{F}_{2^{2m}}$

In this section, we present four classes of permutation polynomials of the form

$$(x^{2^m} + x + \delta)^s + x \tag{4}$$

over $\mathbb{F}_{2^{2m}}$.

By Lemma 2.1, an immediate result is obtained as follows.

Theorem 3.1. *Let m be a positive integer and $n = 2m$. Let $s_1 = \frac{(2^n-1)l}{2^m-1} + 1$ and $s_2 = \frac{(2^n-1)l}{2^m-1} + 2^m$ for an integer l. For a $\delta \in \mathbb{F}_{2^{2m}}$, $f(x) = (x^{2^m} + x + \delta)^{s_1} + x$ permutes $\mathbb{F}_{2^n}$ if and only if $g(x) = (x^{2^m} + x + \delta)^{s_2} + x$ permutes $\mathbb{F}_{2^n}$.*

Proof: From Lemma 2.1, $f(x)$ permutes $\mathbb{F}_{2^n}$ if and only if $(x+\delta)^{2^m s_1} + (x+\delta)^{s_1} + x$ permutes $\mathbb{F}_{2^m}$. It is clear that

$$(x+\delta)^{2^m s_1} + (x+\delta)^{s_1} + x = (x+\delta)^{s_2} + (x+\delta)^{2^m s_2} + x.$$

The conclusion follows from Lemma 2.1. ∎

We now give the necessary and sufficient conditions for the first two classes of polynomials over $\mathbb{F}_{2^{2m}}$ to be permutation polynomials depend on Lemma 2.1 and Theorem 3.1.

Theorem 3.2. *Let $n = 2m$ and $\delta \in \mathbb{F}_{2^n}$. The polynomial*

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

permutes $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}_m^n(\delta) = 0$, or $\mathrm{Tr}_m^n(\delta) = 1$.

Proof: Note that $2^{m+1} + 1 = \frac{(2^n-1)}{2^m-1} + 2^m$. The sufficiency follows from Theorem 3 in [11] and Theorem 3.1. We now prove the necessity. If $f(x)$ permutes $\mathbb{F}_{2^n}$, by Lemma 2.1, then the polynomial $(x+\delta)^{2^m(2^{m+1}+1)} + (x+\delta)^{2^{m+1}+1} + x$ permutes $\mathbb{F}_{2^m}$, i.e., the equation

$$\begin{aligned} &(x+\delta)^{2^m(2^{m+1}+1)} + (x+\delta)^{2^{m+1}+1} + x \\ &= (\delta + \delta^{2^m})x^2 + ((\delta + \delta^{2^m})^2 + 1)x + \delta^{2^{m+1}}(\delta + \delta^{2^m}) = \gamma \end{aligned} \tag{5}$$

has a unique in $\mathbb{F}_{2^m}$ for any $\gamma \in \mathbb{F}_{2^m}$. Suppose on the contrary that $\mathrm{Tr}_m^n(\delta) \notin \mathbb{F}_2$. Then $\delta + \delta^{2^m} \neq 0$ and $(\delta + \delta^{2^m})^2 + 1 \neq 0$. Let $\gamma = \delta^{2^{m+1}}(\delta + \delta^{2^m})$. It is clear that Eq. (5) has two solutions $\{0, \frac{(\delta+\delta^{2^m})^2+1}{\delta+\delta^{2^m}}\}$ for $\gamma = \delta^{2^{m+1}}(\delta + \delta^{2^m})$. This is contrary to our assumption that $(x+\delta)^{2^m(2^{m+1}+1)} + (x+\delta)^{2^{m+1}+1} + x$ permutes $\mathbb{F}_{2^m}$.

This completes the proof. ∎

Theorem 3.3. *Let $n = 2m$ and $\delta \in \mathbb{F}_{2^n}$. The polynomial*

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

permutes $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}_m^n(\delta) = 0$, or $\delta \notin \mathbb{F}_{2^m}$ with $\mathrm{Tr}_1^n(\delta) = \mathrm{Tr}_1^m(1)$ and $P_m\left(\frac{1}{\mathrm{Tr}_m^n(\delta)}\right) \neq 0$.

Proof: Note that $3 \cdot 2^m + 2 = \frac{2\cdot(2^n-1)}{2^m-1} + 2^m$. The sufficiency follows from Theorem 2 in [11] and Theorem 3.1. We only prove the necessity.

If $f(x)$ permutes $\mathbb{F}_{2^n}$, by Lemma 2.1 again, then the equation

$$(x+\delta)^{2^m(3\cdot 2^m+2)} + (x+\delta)^{3\cdot 2^m+2} + x = \gamma \tag{6}$$

has a unique solution in $\mathbb{F}_{2^m}$ for any $\gamma \in \mathbb{F}_{2^m}$. From Eq. (6), we have

$$\begin{aligned}
&(x+\delta)^{2^m(3\cdot 2^m+2)} + (x+\delta)^{3\cdot 2^m+2} + x \\
&= (x+\delta)^3(x+\delta^{2^m})^2 + (x+\delta^{2^m})^3(x+\delta)^2 + x \\
&= (\delta+\delta^{2^m})x^4 + (\delta+\delta^{2^m})^3x^2 + x + \delta^{2^{m+1}+2}(\delta+\delta^{2^m}) = \gamma.
\end{aligned} \tag{7}$$

Suppose on the contrary that $\delta \notin \mathbb{F}_{2^m}$ with $\mathrm{Tr}_1^n(\delta) \neq \mathrm{Tr}_1^m(1)$ or $P_m\left(\frac{1}{\mathrm{Tr}_m^n(\delta)}\right) = 0$.

Note that $\delta+\delta^{2^m} \neq 0$. Multiplying both sides of Eq. (7) by $\frac{1}{\delta+\delta^{2^m}}$ yields the following affine equation

$$x^4 + (\delta+\delta^{2^m})^2x^2 + \frac{1}{\delta+\delta^{2^m}}x + \delta^{2^{m+1}+2} + \frac{\gamma}{\delta+\delta^{2^m}} = 0. \tag{8}$$

The linear part of Eq. (8) is

$$x^4 + (\delta+\delta^{2^m})^2x^2 + \frac{1}{\delta+\delta^{2^m}}x = 0. \tag{9}$$

Clearly, $x = 0$ is a solution of Eq. (9) and its nonzero solutions also satisfy

$$x^3 + (\delta+\delta^{2^m})^2x + \frac{1}{\delta+\delta^{2^m}} = 0. \tag{10}$$

Set $x = (\delta+\delta^{2^m})y$. Then Eq. (10) can be written as

$$y^3 + y + a = 0, \tag{11}$$

where $a = \frac{1}{(\delta+\delta^{2^m})^4}$. Therefore, Eq. (8) has at most one solution in $\mathbb{F}_{2^m}$ if Eq. (11) has no solution in $\mathbb{F}_{2^m}$.

If $\mathrm{Tr}_1^n(\delta) \neq \mathrm{Tr}_1^m(1)$ or $P_m\left(\frac{1}{\mathrm{Tr}_m^n(\delta)}\right) = 0$, by Lemma 2.3, we know that Eq. (11) has a unique solution or three distinct solutions in $\mathbb{F}_{2^m}$, which implies that Eq. (6) has no solutions or at least two distinct solutions in $\mathbb{F}_{2^m}$ for $\gamma \in \mathbb{F}_{2^m}$. This obtains a contradiction. ∎

In [3, 14, 15, 20], the authors investigated the permutation behavior of the polynomials of the form

$$f(x) = \left(\frac{1}{x^{p^k} - x + \delta}\right)^s + x$$

over $\mathbb{F}_{p^n}$. In what follows, we consider the permutation behavior of the polynomials of the form

$$f(x) = (\frac{1}{x^{p^m} - x + \delta})^s + x$$

over $\mathbb{F}_{p^{2m}}$ for $s = 1$ or 2. Note that $2^{2m} - 2 = \frac{(2^m-2)(2^{2m}-1)}{2^m-1} + 2^m$ and $2^{2m} - 2^m - 1 = \frac{(2^m-2)(2^{2m}-1)}{2^m-1} + 1$. By Theorem 2 in [11] and Theorem 3.1, we obtain the following class of permutation polynomials for $s = 1$ and $p = 2$.

Theorem 3.4. *Let $n = 2m$ and $\delta \in \mathbb{F}_{2^n}$. If $\mathrm{Tr}_m^n(\delta) = 0$, or $\mathrm{Tr}_m^n(\delta) = 1$, then the polynomial*

$$f(x) = (x^{2^m} + x + \delta)^{2^n-2} + x$$

permutes $\mathbb{F}_{2^n}$.

For $s = 2$ and $p = 2$, we need the following lemma about the number of solutions of quintic equations.

Lemma 3.1. *Let m be a positive integer and $n = 2m$, and let $\delta \in \mathbb{F}_{2^n}$.*

1) *If m is even and $(\mathrm{Tr}_m^n(\delta))^3 = 1$, then the quintic equation*

$$x^5 + (\delta + \delta^{2^m})^2 x^3 + (\gamma^4 + \gamma^2(\delta + \delta^{2^m})^2 + (\delta \cdot \delta^{2^m})^2)x + (\delta + \delta^{2^m})^2 = 0 \qquad (12)$$

has at most one solution in $\mathbb{F}_{2^m}$ for any $\gamma \in \mathbb{F}_{2^m}$.

2) *If m is odd and $\mathrm{Tr}_m^n(\delta) = 1$, then the quintic equation*

$$x^5 + x^3 + (\gamma^4 + \gamma^2 + (\delta \cdot \delta^{2^m})^2)x + 1 = 0 \qquad (13)$$

has at most one solution in $\mathbb{F}_{2^m}$ for any $\gamma \in \mathbb{F}_{2^m}$.

Proof: We only give the proof of 1) since the other can be proved by a similar manner. For simplicity, denote $\omega = \mathrm{Tr}_m^n(\delta) = \delta + \delta^{2^m}$ and $a = \gamma^4 + \gamma^2(\delta + \delta^{2^m})^2 + (\delta \cdot \delta^{2^m})^2 = (\gamma^2 + \gamma\omega + (\delta \cdot \delta^{2^m}))^2$. It can be verified that

$$\mathrm{Tr}_1^m\left(\frac{\delta \cdot \delta^{2^m}}{\omega^2}\right) = \mathrm{Tr}_1^m\left(\frac{\delta(\omega + \delta)}{\omega^2}\right) = \mathrm{Tr}_1^m\left(\frac{\delta}{\omega} + \left(\frac{\delta}{\omega}\right)^2\right) = \frac{\delta}{\omega} + \left(\frac{\delta}{\omega}\right)^{2^m} = \frac{\delta + \delta^{2^m}}{\omega} = 1.$$

This implies that $a \neq 0$ for any $\gamma \in \mathbb{F}_{2^m}$ by Lemma 2.2. Suppose on the contrary that Eq. (12) has two solutions x and $x + t$ in $\mathbb{F}_{2^m}$, where $t \in \mathbb{F}_{2^m}^*$. Then we have

$$\begin{cases} x^5 + \omega^2 x^3 + ax + \omega^2 = 0 \\ (x + t)^5 + \omega^2(x + t)^3 + a(x + t) + \omega^2 = 0. \end{cases} \qquad (14)$$

Adding the above two equations gives

$$x^4 + \omega^2 x^2 + (t^3 + \omega^2 t)x + t^4 + \omega^2 t^2 + a = 0. \qquad (15)$$

We consider the following two cases.

Case I: ($t^3 + \omega^2 t = 0$). In this case, $t = \omega$, Eq. (15) becomes

$$(x+\gamma)^4 + \omega^2(x+\gamma)^2 + (\delta \cdot \delta^{2^m})^2 = 0.$$

Since $\mathrm{Tr}_1^m\left(\frac{\delta \cdot \delta^{2^m}}{\omega^2}\right) = 1$, $x + \gamma \notin \mathbb{F}_{2^m}$ by Lemma 2.2. This contradicts $x + \gamma \in \mathbb{F}_{2^m}$.

Case II: ($t^3 + \omega^2 t \neq 0$). From Eq. (15), we have $x^4 + \omega^2 x^2 = (t^3 + \omega^2 t)x + t^4 + \omega^2 t^2 + a$. Plugging it into the first equation of Eqs. (14), we obtain

$$\begin{aligned}
&x^5 + \omega^2 x^3 + ax + \omega^2 \\
&= x(x^4 + \omega^2 x^2) + ax + \omega^2 \\
&= x((t^3 + \omega^2 t)x + t^4 + \omega^2 t^2 + a) + ax + \omega^2 \\
&= (t^3 + \omega^2 t)x^2 + t(t^3 + \omega^2 t)x + \omega^2 = 0.
\end{aligned}$$

Dividing the above equation by $t^3 + \omega^2 t$ gives

$$x^2 = tx + \frac{\omega^2}{t^3 + \omega^2 t}. \tag{16}$$

Further, we have

$$\begin{aligned}
x^4 &= t^2 x^2 + \frac{\omega^4}{t^6 + \omega^4 t^2} \\
&= t^2\left(tx + \frac{\omega^2}{t^3 + \omega^2 t}\right)^2 + \frac{\omega^4}{t^6 + \omega^4 t^2} \\
&= t^3 x + \frac{t\omega^2}{t^2 + \omega^2} + \frac{\omega^4}{t^6 + \omega^4 t^2}.
\end{aligned} \tag{17}$$

Plugging Eqs. (16) and (17) into Eq. (15), we obtain

$$\begin{aligned}
&\frac{t\omega^2}{t^2 + \omega^2} + \frac{\omega^4}{t^6 + \omega^4 t^2} + \frac{\omega^4}{t^3 + \omega^2 t} + t^4 + \omega^2 t^2 + a \\
&= \gamma^4 + \omega^2\gamma^2 + (\delta \cdot \delta^{2^m})^2 + \frac{t\omega^2}{t^2 + \omega^2} + \frac{\omega^4}{t^6 + \omega^4 t^2} + \frac{\omega^4}{t^3 + \omega^2 t} + t^4 + \omega^2 t^2 = 0.
\end{aligned} \tag{18}$$

By our assumption that $\omega^3 = 1$, it can be verified that

$$\begin{aligned}
&\mathrm{Tr}_1^m\left(\frac{(\delta \cdot \delta^{2^m})^2 + \frac{t\omega^2}{t^2+\omega^2} + \frac{\omega^4}{t^6+\omega^4 t^2} + \frac{\omega^4}{t^3+\omega^2 t} + t^4 + \omega^2 t^2}{\omega^4}\right) \\
&= \mathrm{Tr}_1^m\left(\frac{(\delta \cdot \delta^{2^m})^2}{\omega^4} + \frac{t\omega}{t^2 + \omega^2} + \frac{1}{t^6 + \omega^4 t^2} + \frac{1}{t^3 + \omega^2 t} + \frac{t^4}{\omega^4} + \frac{t^2}{\omega^2}\right) \\
&= \mathrm{Tr}_1^m\left(\frac{\delta \cdot \delta^{2^m}}{\omega^2}\right) + \mathrm{Tr}_1^m\left(\frac{t\omega}{t^2 + \omega^2}\right) \\
&= 1 + \mathrm{Tr}_1^m\left(\frac{1}{1 + \frac{t}{\omega}} + \frac{1}{1 + (\frac{t}{\omega})^2}\right) = 1.
\end{aligned}$$

It follows from Lemma 2.2 and Eq.(18) that $\gamma^2 \notin \mathbb{F}_{2^m}$. This contradicts $\gamma^2 \in \mathbb{F}_{2^m}$. The proof is completed. ∎

Theorem 3.5. *Let $n = 2m$ and $\delta \in \mathbb{F}_{2^n}$. The polynomial*

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

1) *is a permutation polynomial over $\mathbb{F}_{2^n}$ if $\mathrm{Tr}_m^n(\delta) = 0$, or $(\mathrm{Tr}_m^n(\delta))^3 = 1$ when m is even;*

2) *is a permutation polynomial over $\mathbb{F}_{2^n}$ if $\mathrm{Tr}_m^n(\delta) = 0$, or $\mathrm{Tr}_m^n(\delta) = 1$ when m is odd.*

Proof: We only give the proof for even m since the other case can be proved similarly. According to Lemma 2.1, it suffices to prove the equation

$$(x + \delta)^{2^m(2^n-3)} + (x + \delta)^{2^n-3} + x = \gamma \tag{19}$$

has at most one solution in $\mathbb{F}_{2^m}$ for any $\gamma \in \mathbb{F}_{2^m}$.

When $\mathrm{Tr}_m^n(\delta) = 0$, it is clear that

$$(x + \delta)^{2^m(2^n-3)} + (x + \delta)^{2^n-3} + x = (x + \delta)^{2^n-3} + (x + \delta)^{2^n-3} + x = x = \gamma$$

has a unique solution $x = \gamma$ in $\mathbb{F}_{2^m}$.

When $(\mathrm{Tr}_m^n(\delta))^3 = 1$, then $\delta \notin \mathbb{F}_{2^m}$, which implies that $x + \delta \neq 0$. In this case, Eq. (19) becomes

$$\begin{aligned}&(x + \delta)^{2^m(2^n-3)} + (x + \delta)^{2^n-3} + x\\ &= (x + \delta^{2^m})^{-2} + (x + \delta)^{-2} + x = \gamma.\end{aligned} \tag{20}$$

Multiplying both sides of Eq. (20) by $(x + \delta^{2^m})^2(x + \delta)^2$, we obtain

$$x^5 + \gamma x^4 + (\delta + \delta^{2^m})^2 x^3 + \gamma(\delta + \delta^{2^m})^2 x^2 + (\delta \cdot \delta^{2^m})^2)x + \gamma(\delta \cdot \delta^{2^m})^2)(\delta + \delta^{2^m})^2 = 0. \tag{21}$$

We replace x with $x + \gamma$ in Eq. (20) and obtain

$$x^5 + (\delta + \delta^{2^m})^2 x^3 + (\gamma^4 + \gamma^2(\delta + \delta^{2^m})^2 + (\delta \cdot \delta^{2^m})^2)x + (\delta + \delta^{2^m})^2 = 0. \tag{22}$$

Then the number of solutions of Eq. (20) is equal to the number of solutions obtained from Eq. (22). The conclusion then follows from Lemma 3.1. ∎

4. Permutation polynomials and complete permutation polynomials of the form $(x^{p^m} - x + \delta)^s + x$ over the finite field $\mathbb{F}_{p^{2m}}$ of odd characteristic

4.1. Permutation polynomials of the form $(x^{p^m} - x + \delta)^s + x$ over the finite field $\mathbb{F}_{p^{2m}}$

In this section, several classes of permutation polynomials of the form

$$f(x) = (x^{p^m} - x + \delta)^s + x \tag{23}$$

over $\mathbb{F}_{p^n}$ are presented, where $n = 2m$. The main proofs in this section depend on the idea of some proofs in [11, 12]. In order to simplify the proof, we first give some analysis.

Let's assume that $\mathrm{Tr}_m^n(\delta) \neq 0$. This implies that $\overline{x} - x + \delta \neq 0$ for any $x \in \mathbb{F}_{p^n}$. Let $\theta = \overline{\gamma} - \gamma + \delta$. It is clear that $\theta \neq 0$ and $\overline{\theta} + \theta = \overline{\delta} + \delta = \mathrm{Tr}_m^n(\delta)$. To demonstrate that $f(x)$ permutes $\mathbb{F}_{p^n}$, it suffices to prove that the equation

$$(\overline{x} - x + \delta)^s = -x + \gamma \tag{24}$$

has at most one solution in $\mathbb{F}_{p^n}$ for any $\gamma \in \mathbb{F}_{p^n}$.

Analysis I: ($s = \frac{(p^n-1)l}{p^m-1} + p^m$.) Note that $\frac{(p^n-1)l}{p^m-1} + p^m = (l+1)p^m + l$. Raising both sides of Eq. (24) to the power $p^m - 1$ leads to $(x - \overline{x} + \overline{\delta})^{p^m-1} = (x-\gamma)^{p^m-1}$. Then there exists some $w \in \mathbb{F}_{p^m}^*$ such that

$$x - \overline{x} + \overline{\delta} = w(x - \gamma) \tag{25}$$

which is equivalent to the equation

$$\overline{x} - (1-w)x - (\overline{\delta} + w\gamma) = 0. \tag{26}$$

Raising Eq. (25) to the power p^m, we obtain $\overline{x} - x + \delta = w(\overline{x} - \overline{\gamma})$. Substituting it into Eq. (24) yields

$$w^{2l+1}\left((\overline{x} - \overline{\gamma})(x-\gamma)\right)^l = -1. \tag{27}$$

To show that $f(x)$ permutes $\mathbb{F}_{p^n}$, we need to prove that there is at most one $w \in \mathbb{F}_{p^m}^*$ such that Eqs. (26) and (27) have a unique common solution. Below we distinguish two cases $\overline{\theta} = \theta$ and $\overline{\theta} \neq \theta$. It can be verified that $(1-w)\overline{(1-w)} = (1-w)^2 = 1$ if and only if $w = 2$.

When $w = 2$, in the case of $\overline{\theta} = \theta$, i.e., $\delta - 2\gamma = \overline{\delta} - 2\overline{\gamma}$, we have $(1-w)(-(\overline{\delta} + w\gamma)) + \overline{(-(\overline{\delta} + w\gamma))} = \overline{\delta} - 2\overline{\gamma} - (\delta - 2\gamma) = 0$. By Lemma 2.6, Eq. (26) has p^m solutions. In the case of $\overline{\theta} \neq \theta$, i.e., $\delta - 2\gamma \neq \overline{\delta} - 2\overline{\gamma}$, we have $(1-w)(-(\overline{\delta} + w\gamma)) + \overline{(-(\overline{\delta} + w\gamma))} = \overline{\delta} - 2\overline{\gamma} - (\delta - 2\gamma) \neq 0$. By Lemma 2.6, Eq. (26) has no solution.

When $w \neq 2$, by Lemma 2.6 again, Eq. (26) has a unique solution

$$x_w = \frac{(1-w)(-(\overline{\delta} + w\gamma)) + \overline{(-(\overline{\delta} + w\gamma))}}{w(w-2)}.$$

Furthermore, we have

$$x_w - \gamma = \frac{w\overline{\theta} - (\overline{\delta} + \delta)}{w(w-2)}. \tag{28}$$

Analysis II: ($s = \frac{(p^n-1)l}{p^m-1} + 1$.) Note that $\frac{(p^n-1)l}{p^m-1} + 1 = l(p^m + l) + 1$. Raising both sides of Eq. (24) to the power $p^m - 1$ leads to $(\overline{x} - x + \delta)^{p^m-1} = (x-\gamma)^{p^m-1}$. Then there exists some $w \in \mathbb{F}_{p^m}^*$ such that

$$\overline{x} - x + \delta = w(x - \gamma) \tag{29}$$

which is equivalent to the equation

$$\overline{x} - (1+w)x + (\delta + w\gamma) = 0. \tag{30}$$

Substituting $\overline{x} - x + \delta = w(x-\gamma)$ into Eq. (24), we can also obtain Eq. (27).

For $s = \frac{(p^n-1)l}{p^m-1} + 1$, to show that $f(x)$ permutes $\mathbb{F}_{p^n}$, we need to prove that there is at most one $w \in \mathbb{F}_{p^m}^*$ such that Eqs. (29) and (27) have a unique common solution. It can be verified that $(1+w)\overline{(1+w)} = (1+w)^2 = 1$ if and only if $w = -2$.

When $w = -2$, in the case of $\overline{\theta} = \theta$, i.e., $\delta - 2\gamma = \overline{\delta} - 2\overline{\gamma}$, we have $(1+w)(\delta + w\gamma) + \overline{(\delta + w\gamma)} = \overline{\delta} - 2\overline{\gamma} - (\delta - 2\gamma) = 0$. By Lemma 2.6, Eq. (29) has p^m solutions. In the case of $\overline{\theta} \neq \theta$, i.e., $\delta - 2\gamma \neq \overline{\delta} - 2\overline{\gamma}$, we have $(1+w)(\delta + w\gamma) + \overline{(\delta + w\gamma)} \neq 0$. By Lemma 2.6, Eq. (29) has no solutions.

When $w \neq -2$, by Lemma 2.6 again, Eq. (29) has a unique solution

$$x_w = \frac{(1+w)(\delta + w\gamma) + \overline{(\delta + w\gamma)}}{w(w+2)}.$$

Furthermore, we have

$$x_w - \gamma = \frac{w\theta + (\overline{\delta} + \delta)}{w(w+2)}. \tag{31}$$

Based on the above analysis, we present several classes of permutation polynomials.

Theorem 4.1. *Let $n = 2m$ and $\delta \in \mathbb{F}_{p^n}$. If $\mathrm{Tr}_m^n(\delta) = 1$ or $\mathrm{Tr}_m^n(\delta) = -1$, then the polynomial*

$$f(x) = (x^{p^m} - x + \delta)^{p^n-2} + x$$

is a permutation polynomial over $\mathbb{F}_{p^n}$.

Proof: Note that $\mathrm{Tr}_m^n(\delta) = 1$ or $\mathrm{Tr}_m^n(\delta) = -1$, and $p^n - 2 = \frac{(p^{2m}-1)(p^m-2)}{p^m-1} + p^m$, i.e., $l = p^m - 2$. Then Eq. (27) becomes

$$w(\overline{x} - \overline{\gamma})(x - \gamma) = -1. \tag{32}$$

By Analysis I, we now show that there is at most one $w \in \mathbb{F}_{p^m}^*$ such that Eqs. (26) and (32) have a unique common solution. We distinguish two cases $\overline{\theta} = \theta$ and $\overline{\theta} \neq \theta$.

Case I: ($\overline{\theta} = \theta$). In this case, $\overline{\theta} = \theta$ implies that $\delta - 2\gamma = \overline{\delta} - 2\overline{\gamma}$ and $\theta^2 = \frac{1}{4}$ due to $\overline{\theta} + \theta = \overline{\delta} + \delta = \pm 1$.

When $p = 3$, it is clear that $\theta^2 = 1$. In the case of $w = 2$, let x be a common solution of Eqs. (26) and (27) and denote $y = x - \gamma$. From Eq. (26) and Eq. (32), we have $\overline{y} + y = \overline{\theta} = \theta$ and $\overline{y} \cdot y = 1$, respectively. This implies that y satisfies the equation $y^2 - \theta y + 1 = y^2 + 2\theta y + \theta^2 = (y+\theta)^2 = 0$ because $\theta^2 = 1$. It follows that this equation has a unique solution $y = -\theta$. That is to say, Eqs. (26) and (32) have a unique common solution $x = \gamma - \theta$. For the case of $w \neq 2$, substituting Eq. (28) into Eq. (32), we obtain

$$w^3 + (\theta^2 - 1)w^2 + (1 - (\overline{\theta} + \theta)(\overline{\delta} + \delta))w + (\overline{\delta} + \delta)^2 = 0.$$

Note that $\theta^2 = 1$ and $\overline{\theta} + \theta = \overline{\delta} + \delta = \pm 1$. It follows that $w^3 = 2$, and thus, $w = 2$, which contradicts $w \neq 2$. Therefore, when $p = 3$, Eqs. (26) and (32) have a unique common solution $x = \gamma - \theta$.

When $p > 3$, in the case of $w = 2$, denote $y = x - \gamma$, similar as the argument in the case of $p = 3$, we know that y satisfies the equation $y^2 - \theta y - \frac{1}{2} = 0$. Note that $\theta^2 = \frac{1}{4}$. It can be verified that the discriminant $\Delta = \theta^2 - 4 \cdot (-\frac{1}{2}) = \frac{9}{4}$ is a square. By Lemma 2.6, we have $\{y, \overline{y}\} = \{\frac{\theta+\frac{3}{2}}{2}, \frac{\theta-\frac{3}{2}}{2}\}$, which implies that $\overline{\frac{\theta-\frac{3}{2}}{2}} = \frac{\overline{\theta}-\frac{3}{2}}{2} = \frac{\theta-\frac{3}{2}}{2} = \frac{\theta+\frac{3}{2}}{2}$ because $\overline{\theta} = \theta$. Then we obtain $-\frac{3}{2} = \frac{3}{2}$, which is a contradiction. Thus, Eqs. (26) and (32) have no common solutions if $w = 2$. In the case of $w \neq 2$, substituting Eq. (28) into Eq. (32), we have

$$w^3 - \frac{15}{4}w^2 + 3w + 1 = 0$$

because $\overline{\delta} + \delta = \pm 1$. This equation can be written as

$$(w - 2)^2(w + \frac{1}{4}) = 0.$$

Since $w \neq 2$, $w = -\frac{1}{4}$. Therefore, when $p > 3$, Eqs. (26) and (32) have a common solution x_w only if $w = -\frac{1}{4}$.

Case II: ($\overline{\theta} \neq \theta$). For $w = 2$, as discussed above, Eq. (26) has no solutions. For $w \neq 2$, we substitute Eq. (28) into Eq. (32) and obtain

$$w^3 + (\overline{\theta}\theta - 4)w^2 + 3w + 1 = 0. \tag{33}$$

due to $\delta + \overline{\delta} = \pm 1$.

When $p = 3$, Eq. (33) becomes

$$w^3 + (\overline{\theta}\theta - 1)w^2 + 1 = 0. \tag{34}$$

Replacing w by $\frac{1}{w}$ in the above equation and multiplying both sides by w^3, we obtain

$$w^3 + (\overline{\theta}\theta - 1)w + 1 = 0.$$

We observe that $\overline{\theta}\theta - 1 \neq 0$. Otherwise, $\overline{\theta}\theta = 1$. This together with our assumption $\overline{\theta} + \theta = \pm 1$ implies that $\theta = \pm 1$, which contradicts $\overline{\theta} \neq \theta$. Furthermore, we claim that $-(\overline{\theta}\theta - 1) = (\theta \pm 1)^2$ is not a square in $\mathbb{F}_{p^m}$. Otherwise, if $(\theta \pm 1)^2 = a^2$ for some $a \in \mathbb{F}_{p^m}^*$, then $\overline{\theta} = \theta$, which contradicts $\overline{\theta} \neq \theta$. Thus, by Lemma 2.7, Eq. (34) has a unique solution w_0 in $\mathbb{F}_{3^m}$.

When $p > 3$, we can calculate the discriminant of Eq. (33)

$$\begin{aligned}\Delta &= 9(\overline{\theta}\theta - 4)^2 - 4(\overline{\theta}\theta - 4)^3 - 4 \times 27 - 27 + 18 \times 3(\overline{\theta}\theta - 4) \\ &= -4(\overline{\theta}\theta)^3 + 57(\overline{\theta}\theta)^2 - 210(\overline{\theta}\theta) + 49.\end{aligned}$$

Similar as above, we can prove that $1 - 4\overline{\theta}\theta = 4(\theta \pm \frac{1}{2})^2 \neq 0$ and $1 - 4\overline{\theta}\theta$ is not a square in $\mathbb{F}_{p^m}$ because $\overline{\theta} + \theta = \pm 1$ and $\overline{\theta} \neq \theta$. If $p = 7$, then $\Delta = -4(\overline{\theta}\theta)^3 + (\overline{\theta}\theta)^2 = (\overline{\theta}\theta)^2(1 - 4\overline{\theta}\theta)$ is not a square in $\mathbb{F}_{7^m}$. It follows from Lemma 2.5 that Eq. (34) has a unique solution

w_0 in $\mathbb{F}_{7^m}$. If $p \neq 7$, then $\Delta = -4(\overline{\theta}\theta)^3 + 57(\overline{\theta}\theta)^2 - 210(\overline{\theta}\theta) + 49 = (\overline{\theta}\theta - 7)^2(1 - 4\overline{\theta}\theta)$. In the case of $\overline{\theta}\theta = 7$, i.e., $\Delta = 0$, Eq. (34) becomes

$$w^3 + 3w^2 + 3w + 1 = (w + 1)^3 = 0,$$

and thus, Eq. (34) has a unique $w_0 = -1$. In the case of $\overline{\theta}\theta \neq 7$, i.e., $\Delta = (\overline{\theta}\theta - 7)^2(1 - 4\overline{\theta}\theta) \neq 0$. It is clear that $(\overline{\theta}\theta - 7)^2$ is a square in $\mathbb{F}_{p^m}$. Hence, $\Delta = (\overline{\theta}\theta - 7)^2(1 - 4\overline{\theta}\theta)$ is not a square in $\mathbb{F}_{p^m}$. By Lemma 2.5 again, Eq. (34) has a unique solution w_0 in $\mathbb{F}_{p^m}$.

To summarize, we conclude that Eqs. (26) and (32) have a unique common solution x_{w_0} when $\overline{\theta} \neq \theta$.

∎

Combining Analysis II and a way similar to that in the proof of Theorem 4.1, we give a class of permutation polynomials with exponent $s = (p^m - 2)(p^m + 1) + 1 = p^n - p^m - 1$.

Theorem 4.2. *Let $n = 2m$ and $\delta \in \mathbb{F}_{p^n}$. Assume that $p - 1$ is a square in $\mathbb{F}_{p^m}$. For an odd prime p, if $(\mathrm{Tr}_m^n(\delta))^2 = p - 1$, then the polynomial*

$$f(x) = (x^{p^m} - x + \delta)^{p^n - p^m - 1} + x \tag{35}$$

is a permutation polynomial over $\mathbb{F}_{p^n}$.

Remark 4.1. *Tu et al. [12, Theorem 3] investigated the permutation behavior of the polynomials of the form (35) for $p = 3$, which can be generalized to any odd prime p by Theorem 4.2.*

Theorem 4.3. *Let $n = 2m$ and $\delta \in \mathbb{F}_{p^n}$. Assume that $p - 2$ is a square in $\mathbb{F}_{p^m}$. For an odd prime p, if $(\mathrm{Tr}_m^n(\delta))^2 = p - 2$ and $\gcd(p^{m-i} + 2, p^m - 1) = 1$, then the polynomial*

$$f(x) = (x^{p^m} - x + \delta)^{p^i(p^m+1)+p^m} + x$$

is a permutation polynomial over $\mathbb{F}_{p^n}$, where $1 \leq i \leq m - 1$.

Proof: Note that $(\mathrm{Tr}_m^n(\delta))^2 = p - 2$ and $s = p^i(p^m + 1) + p^m$, i.e., $l = p^i$. Eq. (27) becomes

$$w^{2p^i+1}((\overline{x} - \overline{\gamma})(x - \gamma))^{p^i} = -1.$$

Raising both sides of this equation to the power p^{m-i} and obtain

$$w^{2+p^{m-i}}((\overline{x} - \overline{\gamma})(x - \gamma)) = -1. \tag{36}$$

By Analysis I, we need to show that there is at most one $w \in \mathbb{F}_{p^m}^*$ such that Eqs. (26) and (36) have a unique common solution. We distinguish two cases $\overline{\theta} = \theta$ and $\overline{\theta} \neq \theta$.

Case I: ($\overline{\theta} = \theta$). In this case, $\overline{\theta} = \theta$ implies that $\theta^2 = \frac{p-2}{4} = -\frac{1}{2}$ because $(\overline{\theta} + \theta)^2 = (\overline{\delta} + \delta)^2 = p - 2$.

In the case of $w = 2$, let x be a common solution of Eqs. (26) and (36) and denote $y = x - \gamma$. From Eq. (26) and Eq. (36), we have $\overline{y} + y = \overline{\theta} = \theta$ and $\overline{y} \cdot y = -\frac{1}{8}$,

respectively. Thus, y satisfies the equation $y^2 - \theta y - \frac{1}{8} = y^2 - \theta y + \frac{\theta^2}{4} = (y - \frac{\theta}{2})^2 = 0$ because $\theta^2 = -\frac{1}{2}$. It follows that $y = \frac{\theta}{2}$. Hence, Eqs. (26) and (36) have a unique common solution $x = \frac{\theta}{2} + \gamma$. For the case of $w \neq 2$, substituting Eq. (28) into Eq. (36), we obtain

$$\theta\overline{\theta}w^{p^{m-i}+2} - (\theta + \overline{\theta})(\delta + \overline{\delta})w^{p^{m-i}+1} + (\delta + \overline{\delta})^2 w^{p^{m-i}} + w^2 - 4w + 4 = 0. \tag{37}$$

Note that $\theta^2 = -\frac{1}{2}$ and $\overline{\theta} + \theta = \overline{\delta} + \delta = p - 2$. Then (37) becomes

$$\begin{aligned} & w^{p^{m-i}+2} - 4w^{p^{m-i}+1} + 4w^{p^{m-i}} - 2w^2 + 8w - 8 \\ &= w^{p^{m-i}}(w-2)^2 - 2(w-2)^2 \\ &= (w-2)^{p^{m-i}+2} = 0. \end{aligned}$$

It follows that $w = 2$, which contradicts $w \neq 2$. Therefore, when $\overline{\theta} = \theta$, Eqs. (26) and (36) have a unique common solution $x = \frac{\theta}{2} + \gamma$.

Case II: ($\overline{\theta} \neq \theta$). For $w = 2$, as discussed in Analysis I, Eq. (26) has no solutions. For $w \neq 2$, similarly as in Case (I), we now consider the number of solutions of Eq. (37) in $\mathbb{F}_{p^m}$. From the condition that $(\overline{\theta} + \theta)^2 = (\overline{\delta} + \delta)^2 = p - 2$, Eq. (37) can be written as

$$\theta\overline{\theta}w^{p^{m-i}+2} + 2w^{p^{m-i}+1} - 2w^{p^{m-i}} + w^2 - 4w + 4 = 0. \tag{38}$$

Replacing w by $\frac{1}{w}$ and multiplying $\frac{1}{w^{p^{m-i}+2}}$, we obtain

$$4w^{p^{m-i}+2} - 4w^{p^{m-i}+1} + w^{p^{m-i}} - 2w^2 + 2w + \theta\overline{\theta} = 0.$$

Replacing w by $w - \frac{p-1}{2}$ in the above equation, we get

$$4w^{p^{m-i}+2} + \frac{1}{2} + \theta\overline{\theta} = 0. \tag{39}$$

It is clear that the number of solutions of Eq. (38) is equal to the number of solutions obtained from Eq. (39). Since $\gcd(p^{m-i}+2, p^m - 1) = 1$, Eq. (39) has a unique solution in $\mathbb{F}_{p^m}$. Thus, Eq. (38) has a unique solution w_0 in $\mathbb{F}_{p^m}$.

To summarize, we conclude that Eqs. (26) and (36) have a unique common solution x_{w_0} when $\overline{\theta} \neq \theta$. ∎

Remark 4.2. *Let η and η_0 be the quadratic characters of $\mathbb{F}_{p^m}^*$ and $\mathbb{F}_p^*$, respectively. It is well known that $\eta(y) = 1$ for each $y \in \mathbb{F}_p^*$ if m is even and $\eta(y) = \eta_0(y) = 1$ for each $y \in \mathbb{F}_p^*$ if m is odd. Clearly, $p-1$ and $p-2$ are always squares in $\mathbb{F}_{p^m}^*$ if m is even. Note that $\eta_0(-1) = 1$ if $p \equiv 1 (\bmod 4)$ and $\eta_0(-2) = 1$ if $p \equiv 1 (\bmod 8)$ or $p \equiv 3 (\bmod 8)$ when m is odd. Hence, odd prime p needs to satisfy $p \equiv 1 (\bmod 4)$ in Theorem 4.2 and $p \equiv 1 (\bmod 8)$ or $p \equiv 3 (\bmod 8)$ in Theorem 4.3 when m is odd,respectively.*

Similarly, combining Analysis II and a way similar to that in the proof of Theorem 4.3, we obtain a class of permutation polynomials with exponent $s = p^i(p^m + 1) + 1 = p^{m+i} + p^i + 1$.

Theorem 4.4. *Let $n = 2m$ and $\delta \in \mathbb{F}_{p^n}$. Assume that 2 is a square in $\mathbb{F}_{p^m}$. For an odd prime p, if $(\mathrm{Tr}_m^n(\delta))^2 = 2$ and $\gcd(p^{m-i}+2, p^m-1) = 1$, then the polynomial*

$$f(x) = (x^{p^m} - x + \delta)^{p^i(p^m+1)+1} + x$$

is a permutation of $\mathbb{F}_{p^n}$, where $1 \le i \le m-1$.

Remark 4.3. *For odd m, p needs to satisfy $p \equiv \pm 1 \pmod 8$ in Theorem 4.4 because $\eta_0(2) = 1$ if $p \equiv \pm 1 \pmod 8$. In addition, odd prime p also needs to satisfy $p \not\equiv 1 \pmod 3$ in Theorems 4.3 and 4.4. Otherwise, $p^{m-i}+2$ and $p^m - 1$ have a common divisor 3.*

The next theorem is about a class of permutation polynomials over the finite field $\mathbb{F}_{3^{2m}}$.

Theorem 4.5. *Let $n = 2m$ and $\delta \in \mathbb{F}_{3^n}$. If $(\mathrm{Tr}_m^n(\delta))^2 + 2 = 0$ or $(\mathrm{Tr}_m^n(\delta))^2 + 2$ is a square in $\mathbb{F}_{3^m}$, then the polynomial*

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

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

Proof: To prove $f(x)$ permutes $\mathbb{F}_{3^n}$, it suffices to prove the equation

$$(\overline{x} - x + \delta)^{2\cdot 3^m+1} = -x + \gamma \tag{40}$$

has at most one solution in $\mathbb{F}_{3^n}$ for any $\gamma \in \mathbb{F}_{3^n}$. Let θ be defined as before. We only give the proof of the case of $\theta = 0$ since the case of $\theta \neq 0$ can be proven by a proof similar to that of Theorem 2 in [12] and Analysis I.

In the case of $\theta = 0$, it can be verified that $\mathrm{Tr}_m^n(\delta) = 0$, which implies that m is even. In fact, if $\theta = 0$ and m is odd, then $(\mathrm{Tr}_m^n(\delta))^2 + 2 = 2$ is a nonsquare in $\mathbb{F}_{3^m}$ since $\eta(2) = \eta_0(2) = -1$. This contradicts our condition that $(\mathrm{Tr}_m^n(\delta))^2 + 2$ is a square in $\mathbb{F}_{3^m}$. We now prove that Eq. (40) has at most one solution in $\mathbb{F}_{3^n}$. It is clear that $x = \gamma$ is a solution of Eq. (40) when $\theta = 0$. Suppose that $\gamma + t$ is also a solution of Eq. (40) for some $t \in \mathbb{F}_{3^n}^*$. Then we have$(\overline{\gamma} + \bar{t} - \gamma - t + \delta)^{2\cdot 3^m+1} = -\gamma - t + \gamma$, i.e.,

$$(\bar{t} - t)^{2\cdot 3^m+1} = (t - \bar{t})^2(\bar{t} - t) = -t \tag{41}$$

because $\theta = \overline{\gamma} - \gamma + \delta = 0$. We raise Eq. (41) by 3^m and obtain

$$(\bar{t} - t)^2(t - \bar{t}) = (t - \bar{t})^2(\bar{t} - t) = \bar{t}. \tag{42}$$

From Eqs. (41) and (43), we have $t = -\bar{t}$. Placing this into Eq. (41) yields $\bar{t}^3 = t$, i.e., $t^{3^{m+1}-1} = 1$ because $t \neq 0$. Note that $\gcd(3^{m+1}-1, 3^{2m}-1) = \gcd(3^{m+1}-1, 3^{m-1}-1) = \gcd(8, 3^{m-1}-1) = 2$ since m is even. It follows that $t^2 = 1$, which implies that $t = \pm 1$. This contradicts $\bar{t} = -t$. Thus, Eq. (40) has a unique solution $x = \gamma$ in $\mathbb{F}_{3^n}$ when $\theta = 0$. ∎

Finally, based on Lemma 2.1, we present the other two classes of permutation polynomials of the form $(x^{p^m} - x + \delta)^s + x$ over $\mathbb{F}_{p^{2m}}$.

Theorem 4.6. *Let $n = 2m$ and $\delta \in \mathbb{F}_{p^n}$. The polynomial*

$$f(x) = (x^{p^m} - x + \delta)^2 + x$$

is a permutation polynomial over $\mathbb{F}_{p^n}$ if and only if $\mathrm{Tr}_m^n(\delta) \neq \frac{1}{2}$.
Proof: By Lemma 2.1, the proof is similar to that of proposition 1 in [9] and is omitted. ∎

Theorem 4.7. *Let $n = 2m$ and $\delta \in \mathbb{F}_{p^n}$. If $\mathrm{Tr}_m^n(\delta) = 0$ or $\frac{\mathrm{Tr}_m^n(\delta)+1}{\mathrm{Tr}_m^n(\delta)}$ is a $(p-1)$-th power in $\mathbb{F}_{p^m}$, then the polynomial*

$$f(x) = (x^{p^m} - x + \delta)^{p^m+p} + x$$

is a permutation polynomial over $\mathbb{F}_{p^n}$.
Proof: By Lemma 2.1, the proof is similar to that of proposition 2 in [9] and is omitted. ∎

4.2. Complete permutation polynomials of the form $(x^{3^m} - x + \delta)^s + x$ over $\mathbb{F}_{3^{2m}}$

In this subsection, we provide several classes of complete permutation polynomials of the form $(x^{3^m} - x + \delta)^s + x$ over $\mathbb{F}_{3^{2m}}$. Let

$$g(x) = (x^{3^m} - x + \delta)^s + x. \tag{43}$$

We observe that

$$(g((-x)^{3^m}))^{3^m} = (x^{3^m} - x + \delta)^{3^m \cdot s} - x = (x^{3^m} - x + \delta)^{3^m \cdot s} + x + x.$$

Denote $f(x) = (x^{3^m} - x + \delta)^{3^m \cdot s} + x$. Clearly, $f(x) + x$ permutes $\mathbb{F}_{3^n}$ if and only if $g(x)$ permutes $\mathbb{F}_{3^n}$. Let A denote the set of all elements δ in $\mathbb{F}_{3^n}$ such that $g(x)$ permutes $\mathbb{F}_{3^n}$ and B the set of all elements δ in $\mathbb{F}_{3^n}$ such that $f(x)$ permutes $\mathbb{F}_{3^n}$. Then we have the following result.

Theorem 4.8. *Let $n = 2m$ and $\delta \in \mathbb{F}_{3^n}$. Let $g(x)$, A and B be defined as before. If $\delta \in A \cap B$, then the polynomial $f(x) = (x^{3^m} - x + \delta)^{s \cdot 3^m} + x$ is a complete permutation polynomial over $\mathbb{F}_{3^n}$.*

Combining Theorem 4.8 and earlier works in [9, 12, 24], we present the following four classes of complete permutation polynomials over $\mathbb{F}_{3^n}$.

Corollary 1. *Let $n = 2m$ and $\delta \in \mathbb{F}_{3^n}$. Let*

$$A = \{(\mathrm{Tr}_m^n(\delta))^2 + 1 = 0 \text{ or } (\mathrm{Tr}_m^n(\delta))^2 + 1 \text{ is a square in } \mathbb{F}_{3^m} | \delta \in \mathbb{F}_{3^n}\}$$

and

$$B = \{(\mathrm{Tr}_m^n(\delta))^2 + 2 = 0 \text{ or } (\mathrm{Tr}_m^n(\delta))^2 + 2 \text{ is a square in } \mathbb{F}_{3^m} | \delta \in \mathbb{F}_{3^n}\}.$$

If $\delta \in A \cap B$, then the polynomial $f(x) = (x^{3^m} - x + \delta)^{2 \cdot 3^m + 1} + x$ is a complete permutation polynomial over $\mathbb{F}_{3^n}$.
Proof: Let $g(x) = (x^{3^m} - x + \delta)^{3^m+2} + x$. By Theorem 2 in [12], $g(x)$ permutes $\mathbb{F}_{3^n}$ if $\delta \in A$. On the other hand, $f(x)$ permutes $\mathbb{F}_{3^n}$ if $\delta \in B$ by Theorem 4.5. It can be verified that $(g((-x)^{3^m}))^{3^m} = (x^{3^m} - x + \delta)^{2 \cdot 3^m + 1} - x = f(x) + x$. The conclusion follows from Theorem 4.8. ∎

Corollary 2. *Let $n = 2m$ and $\delta \in \mathbb{F}_{3^n}$. If $\mathrm{Tr}_m^n(\delta) \notin \mathbb{F}_3^*$, then the polynomial $f(x) = (x^{3^m} - x + \delta)^2 + x$ is a complete permutation polynomial over $\mathbb{F}_{3^n}$.*
Proof: Let $g(x) = (x^{3^m} - x + \delta)^{2\cdot 3^m} + x$. By Proposition 1 in [9], $g(x)$ permutes $\mathbb{F}_{3^n}$ if $\mathrm{Tr}_m^n(\delta) \neq 1$. It follows from Theorem 4.6 that $f(x)$ permutes $\mathbb{F}_{3^n}$ if $\mathrm{Tr}_m^n(\delta) \neq 2$. Note that $(g((-x)^{3^m}))^{3^m} = (x^{3^m} - x + \delta)^2 - x = f(x) + x$. The conclusion follows from Theorem 4.8. ∎

Corollary 3. *Let $n = 2m$ and $\delta \in \mathbb{F}_{3^n}$. Let*

$$A = \{\mathrm{Tr}_m^n(\delta) = 0 \text{ or } \frac{\mathrm{Tr}_m^n(\delta) - 1}{\mathrm{Tr}_m^n(\delta)} \text{ is a square in } \mathbb{F}_{3^m} | \delta \in \mathbb{F}_{3^n}\}$$

and

$$B = \{\mathrm{Tr}_m^n(\delta) = 0 \text{ or } \frac{\mathrm{Tr}_m^n(\delta) + 1}{\mathrm{Tr}_m^n(\delta)} \text{ is a square in } \mathbb{F}_{3^m} | \delta \in \mathbb{F}_{3^n}\}.$$

If $\delta \in A \cap B$, then the polynomial $f(x) = (x^{3^m} - x + \delta)^{3^m+3} + x$ is a complete permutation polynomial over $\mathbb{F}_{3^n}$.
Proof: Let $g(x) = (x^{3^m} - x + \delta)^{3^{m+1}+1} + x$. By Proposition 2 in [9], $g(x)$ permutes $\mathbb{F}_{3^n}$ if $\delta \in A$. On the other hand, $f(x)$ permutes $\mathbb{F}_{3^n}$ if $\delta \in B$ by Theorem 4.7. It can be verified that $(g((-x)^{3^m}))^{3^m} = (x^{3^m} - x + \delta)^{3^m+3} - x = f(x) + x$. The conclusion follows from Theorem 4.8. ∎

The last class of complete permutation polynomials can be obtained from Theorem 2.3 [24] and Proposition 3 [9].

Corollary 4. *Let $n = 2m$ and $\delta \in \mathbb{F}_{3^n}$. If $\mathrm{Tr}_m^n(\delta) \neq 0$, then the polynomial $f(x) = (x^{3^m} - x + \delta)^{2\cdot 3^{2m-1}+3^{m-1}} + x$ is a complete permutation polynomial over $\mathbb{F}_{3^n}$.*

Remark 4.4. *It should be noted that permutation polynomials in Theorems 4.1 and 4.2 can not provide more complete permutation polynomials by Theorem 4.8 when $p = 3$. In fact, let $f(x) = (x^{3^m} - x + \delta)^{3^n-2} + x$ and $g(x) = (x^{3^m} - x + \delta)^{3^n-3^m-1} + x$, it is clear that $A \cap B = \emptyset$, where A and B are defined as before. So do Theorem 4.3 and Theorem 4.4.*

5. Concluding remarks

The main objective of this paper is to give a further study on constructions of permutation polynomials of the form $(x^{p^m} - x + \delta)^s$ over $\mathbb{F}_{p^{2m}}$. Notably, we derive some necessary and sufficient conditions for this kind of polynomials over $\mathbb{F}_{2^{2m}}$ to be permutation polynomials. To the best of our knowledge, there are only a few permutation polynomials of the form $(x^{p^m} - x + \delta)^s$ over $\mathbb{F}_{p^n}$ for infinitely many odd primes p. We succeed in constructing six classes of such permutation polynomials. All the known classes of permutation polynomials of the form $(x^{p^m} - x + \delta)^s$ over $\mathbb{F}_{p^n}$ for infinitely many odd primes p are summarized in Table 1. We also construct some complete permutation polynomials of such form over $\mathbb{F}_{3^{2m}}$. According to our experimental data, some of sufficient conditions for such polynomials to be permutation polynomials are also necessary. It would be nice if the necessity of these conditions could be proved.

Table 1: Known PPs of the form $(x^{p^m} - x + \delta)^s + x$ over $\mathbb{F}_{p^{2m}}$ for infinitely many odd primes p.

No.	Values of p, m and s	Conditions on δ	Reference
1	$s(p^m - 1) \equiv 0 \pmod{p^{2m-1}}$	all δ	[16]
2	all p, m and s is even	$\mathrm{Tr}_m^{2m}(\delta) = 0$	[17]
3	$s = \frac{p^{2m}-1}{d} + 1$, $d \in \{2, 3, 4, 6\}$, and the details of the parameters p and m are mentioned in [18]	$\mathrm{Tr}_m^{2m}(\delta) = 0$	[18]
4	$p^m \equiv 2 \pmod 3$, $s = \frac{p^{2m}-1}{3} + 1$ and $-\frac{1}{2}$ is a cube of $\mathbb{F}_{p^{2m}}^*$	$\mathrm{Tr}_m^{2m}(\delta) = 0$	[7]
5	$p \neq 7$, $p^m \equiv 1 \pmod 3$, $s = \frac{p^{2m}-1}{3} + 1$, $\frac{\alpha(2\epsilon^2-1)^2}{2\epsilon-1}$ is not a cube in $\mathbb{F}_{p^{2m}}^*$, where α is a primitive element of $\mathbb{F}_{p^{2m}}^*$ and $\epsilon = \alpha^{\frac{p^{2m}-1}{3}}$	$\mathrm{Tr}_m^{2m}(\delta) = 0$	[7]
6	$s = i(p^m - 1) + 1$, $0 < i \leq p^m$ and i is even if $p = 3$	$\mathrm{Tr}_m^{2m}(\delta) = 0$	[12]
7	$s = 2p^m$	$2\mathrm{Tr}_m^{2m}(\delta) + 1 \neq 0$	[9]
8	$s = p^{m+1} + 1$	$\mathrm{Tr}_m^{2m}(\delta) = 0$ or $\frac{\mathrm{Tr}_m^{2m}(\delta)-1}{\mathrm{Tr}_m^{2m}(\delta)}$ is a $(p-1)$-th power in $\mathbb{F}_{p^m}$	[9]
9	$s = p^{2m} - 2$	$(\mathrm{Tr}_m^{2m}(\delta))^2 = 1$	Thm. 4.1
10	$s = p^{2m} - p^m - 1$	$(\mathrm{Tr}_m^{2m}(\delta))^2 = -1$	Thm. 4.2
11	$s = p^i(p^m + 1) + p^m$, $\gcd(p^{m-i} + 2, p^m - 1) = 1$, $1 \leq i \leq m - 1$	$(\mathrm{Tr}_m^{2m}(\delta))^2 = 2$	Thm. 4.3
12	$s = p^i(p^m + 1) + 1$, $\gcd(p^{m-i} + 2, p^m - 1) = 1$, $1 \leq i \leq m - 1$	$(\mathrm{Tr}_m^{2m}(\delta))^2 = -2$	Thm. 4.4
13	$s = 2$	$\mathrm{Tr}_m^{2m}(\delta) \neq \frac{1}{2}$	Thm. 4.6
14	$s = p^m + p$	$\mathrm{Tr}_m^{2m}(\delta) = 0$ or $\frac{\mathrm{Tr}_m^{2m}(\delta)+1}{\mathrm{Tr}_m^{2m}(\delta)}$ is a $(p-1)$-th power in $\mathbb{F}_{p^m}$	Thm. 4.7

6. Acknowledgments

G. Xu was supported by the National Natural Science Foundation of China (Grant No. 62172183), the Natural Science Foundation for the Higher Education Institutions of Anhui Province of China under Grant KJ2020A0643 and Program for Innovative Research Team in Huainan Normal University (XJTD202008). G. Luo was supported by Nanyang Technological University Research Grant No. 04INS000047C230GRT01. X. Cao was supported by the National Natural Science Foundation of China (Grant No. 12171241).

References

[1] E. R. Berlekamp, H. Rumsey, G. Solomon, On the solution of algebraic equations over finite fields, Inf. Control. 10 (6) (1967) 553-564.

[2] X. Cao, L. Hu, New methods for generating permutation polynomials over finite fields, Finite Fields Appl. 17 (2011) 493-503.

[3] T. Helleseth, V. Zinoviev, New Kloosterman sums identities over $\mathbb{F}_{2^m}$ for all m, Finite Fields Appl. 9(2) (2003) 187-193.

[4] J. W. P. Hirschfeld, Projective spaces over finite fields, Clarendon Press, Oxford, 1979.

[5] X. Hou, Permutation polynomials over finite fields-A survey of recent advances, Finite Fields Appl. 32 (2015) 82-119.

[6] K. Li, L. Qu, X. Chen, New classes of permutation binomials and permutation trinomials over finite fields, Finite Fields Appl. 43 (2016) 69-85.

[7] N. Li, T. Helleseth, X. Tang, Further results on a class of permutation polynomials over finite fields, Finite Fields Appl. 22 (2013) 16-23.

[8] R. Lidl, H. Niederreiter, Finite Fields, second ed., Encycl. Math. Appl., vol.20, Cambridge University Press, Cambridge, 1997.

[9] L. Li, S. Wang, C. Li, N. Li, 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.

[10] G. L. Mullen, D. Panario (Eds.), Handbook of Finite Fields, CRC Press, Boca Raton, 2013.

[11] Z. Tu, X. Zeng, Y. Jiang, Two classes of permutation polynomials of the form $(x^{2^m} + x + \delta)^s + x$, Finite Fields Appl. 31 (2015) 12-24.

[12] Z. Tu, X. Zeng, C. Li, T. Helleseth, 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.

[13] L. Wang, B. Wu, 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.

[14] J. Yuan, C. Ding, Four classes of permutation polynomials of $\mathbb{F}_{2^m}$, Finite Fields Appl. 13 (2007) 869-876.

[15] J. Yuan, C. Ding, H. Wang, J. Pieprzyk, Permutation polynomials of the form $(x^p - x + \delta)^s + L(x)$, Finite Fields Appl. 14 (2008) 482-493.

[16] P. Yuan, C. Ding, Permutation polynomials over finite fields from a powerful lemma, Finite Fields Appl. 17 (2011) 560-574.

[17] P. Yuan, C. Ding, Further results on permutation polynomials over finite fields, Finite Fields Appl. 27 (2014) 88-103.

[18] P. Yuan, Y. Zheng, Permutation polynomials from piecewise functions, Finite Fields Appl. 35 (2015) 215-230.

[19] D. Zheng, Z. Chen, More classes of permutation polynomials of the form $(x^{p^m} - x + \delta)^s + L(x)$, Appl. Algebra Eng. Commun. Comput. 28(3) (2017) 215-223.

[20] X. Zeng, X. Zhu, L. Hu, Two new permutation polynomials with the form $(x^{2^k} + x + \delta)^s + x$ over $\mathbb{F}_{2^n}$, Appl. Algebra Eng. Commun. Comput. 21 (2010) 145-150.

[21] X. Zeng, S. Tian, Z. Tu, Permutation polynomials from trace functions over finite fields, Finite Fields Appl. 35 (2015) 36-51.

[22] X. Zeng, X. Zhu, N. Li, X. Liu, Permutation polynomials over $\mathbb{F}_{2^n}$ of the form $(x^{2^i} + x + \delta)^{s_1} + (x^{2^i} + x + \delta)^{s_2} + x$, Finite Fields Appl. 47 (2017) 256-268.

[23] Z. Zha, L. Hu, Two classes of permutation polynomials over finite fields, Finite Fields Appl. 18 (2012) 781-790.

[24] Z. Zha, L. Hu, Some classes of permutation polynomials of the form $(x^{p^m} - x + \delta)^s + L(x)$ over $\mathbb{F}_{p^{2m}}$, Finite Fields Appl. 40 (2016) 150-162.