Constructing new permutation polynomials by the AGW Criterion

Qian Liu [1,2] *, Liwei Fang [1], Zhengbang Zha [3], Jing Zhang [2]
1. Key Laboratory of Information Security of Network Systems, College of Computer and Data Science, Fuzhou University, Fuzhou 350116, China
2. Key Laboratory of Computing and Stochastic Mathematics (Ministry of Education), School of Mathematics and Statistics, Hunan Normal University, Changsha 410081, China
3. College of Mathematics and System Sciences, Xinjiang University, Urumqi 830046, China

Abstract

In this paper, we propose several classes of permutation polynomials having the form $\sum_i (x^{2^m}+x+\delta)^{s_i}+ax$ for $i=1$ or $i=2$, where the exponent s_i satisfies $s_i \equiv 2^j \pmod{2^m+1}$ or $s_i \equiv 2^j \pmod{2^m-1}$ for some different integers j, $a \in \mathbb{F}_{2^m}^*$ and $\delta \in \mathbb{F}_{2^{2m}}$. More precisely, by applying the AGW criterion and determining the number of solutions to certain equations over $\mathbb{F}_{2^{2m}}$, several classes of permutation polynomials of the form $(x^{2^m}+x+\delta)^s+ax$ over $\mathbb{F}_{2^{2m}}$ are presented. In addition, we construct some classes of permutation polynomials of the form $(x^{2^m}+x+\delta)^{s_1}+(x^{2^m}+x+\delta)^{s_2}+ax$ over $\mathbb{F}_{2^{2m}}$. Our results generalize some known constructions of permutation polynomials. Finally, we demonstrate that the permutation polynomials proposed in this paper are not quasi-multiplicative equivalent to known ones.

Keywords: Finite field, Permutation polynomial, AGW criterion.

1 Introduction

Let $\mathbb{F}_q$ denote the finite field with q elements, where q is a power of a prime p. 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) if the mapping $x \mapsto f(x)$ from $\mathbb{F}_q$ into itself is bijective. Furthermore, we call $f(x)$ a *complete permutation polynomial* (CPP) if both $f(x)$ and $f(x)+x$ are permutations of $\mathbb{F}_q$. PPs have been widely employed in cryptography [5, 18, 37], combinatorial design theory [4], coding theory [9], and other areas of mathematics and engineering [8, 14, 16, 21, 24, 30]. In general, constructing PPs over finite fields has been a prominent research topic in recent decades.

In 2003, Helleseth and Zinoviev [7] utilized PPs of the form

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

to derive new Kloosterman sums identities over $\mathbb{F}_{2^n}$, where $\delta \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}_1^n(\delta)=1$, and $l=0$ or 1. This motivated Yuan and Ding [28, 31] to investigate the permutation behavior of polynomials having the form

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

*e-mail: lqmova@foxmail.com

over $\mathbb{F}_{p^n}$, where k, n, s are integers, $\delta \in \mathbb{F}_{p^n}$ and $L(x)$ is a linearized polynomial (see Definition 2.1) with coefficients in $\mathbb{F}_p$. Following these pioneering contributions, several families of PPs of the form (1) have been proposed in [3, 10, 12, 15, 23, 26, 27, 30, 34–36] for odd prime p. Meanwhile, for $p = 2$, a number of research works have been devoted to constructing PPs with the form

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

over $\mathbb{F}_{2^n}$, where $m \mid n$, $\delta \in \mathbb{F}_{2^n}$, k_i and s_i are positive integers and $L(x)$ is a linearized polynomial. The reader may refer to [11, 13, 32] for details. In the case $n = 2m$ with $i = 1$ and $k_1 = 1$, Yuan and Ding [29, 30] provided a unified treatment of some earlier constructions of PPs and derived some new special PPs by the AGW criterion. Subsequently, Tu et al. [19] constructed several classes of PPs over $\mathbb{F}_{2^{2m}}$, where $s \equiv 1 \pmod{2^m - 1}$ or $s \equiv 1 \pmod{2^m + 1}$. Inspired by [19, 20], Zha and Hu [34] investigated three classes of PPs with the form (2) for some exponents s satisfying $s(2^m - 1) \equiv 2^m - 1 \pmod{2^{2m} - 1}$ or $s(2^m + 1) \equiv 2^m + 1 \pmod{2^{2m} - 1}$. Later, Wang et al. [22] proposed four classes of PPs of the form $(x^{2^m} + x + \delta)^s + x$ over $\mathbb{F}_{2^{2m}}$, where $s(2^m + 1) \equiv 2^m + 1 \pmod{2^{2m} - 1}$. Several classes of PPs of the form $(x^{2^m} + x + \delta)^{i(2^m-1)+1} + x$ were constructed by Gupta and Sharma [6] for specific values of i. Recently, by applying the AGW criterion and determining the number of solutions to certain equations over finite fields, several classes of PPs with the form $(x^{p^m} - x + \delta)^{s_1} + (x^{p^m} - x + \delta)^{s_2} + x$ over $\mathbb{F}_{p^n}$ were proposed in [12], where m, n, s_1, s_2 are positive integers with $m \mid n$ and $\delta \in \mathbb{F}_{p^n}$. After that, several classes of CPPs with exponents of the form $s = i(2^m \pm 1) + 2^j$ were proposed in [26]. Subsequently, four classes of PPs were presented in [27] based on the AGW criterion. Later, several classes of PPs of the form $b(x^{2^m} + ax + \delta)^s + ax$ over $\mathbb{F}_{2^{2m}}$ were provided in [23]. Chen et al. [3] discovered further classes of PPs with the form (2) by identifying new suitable exponent s. To the best of our knowledge, there are only a few PPs of the form given in (2) with $n = 2m$, $i = 2$ and $k_1 = k_2 = 1$. Zeng et al. [33] firstly investigated eight classes of PPs with the form (2). Later, several classes of PPs were constructed in [12] by using the AGW criterion. Inspired by the works in [26, 27], Li and Cao [10] proposed four classes of PPs with the form (2). Most recently, by employing the linearized q-associate $L_{g_{t,\alpha}}$ of $g_{t,\alpha} = \frac{x^n-1}{x^t-\alpha}$ within the AGW criterion framework, the authors unified two series of results on explicit constructions of PPs appeared in recent literatures and obtained new findings on constructing PPs with the form $f(L_{g_{t,\alpha}}(x)) + k(L_{g_{t,\alpha}}(x)) \cdot L_h(x)$ over $\mathbb{F}_{q^n}$ in [17].

Following the previous works done in [3, 10, 19, 23, 26, 34], the purpose of this paper is to characterize more classes of PPs with the form

$$\sum_i (x^{2^m} + x + \delta)^{s_i} + L(x) \tag{3}$$

over $\mathbb{F}_{2^{2m}}$, where i and m are positive integers, $\delta \in \mathbb{F}_{2^{2m}}$ and $L(x) = ax$ with $a \in \mathbb{F}_{2^m}$. Our approach is based on the AGW criterion and determining the number of solutions to certain equations over $\mathbb{F}_{2^{2m}}$. In this paper, we first investigate the permutation behavior of polynomials of the form $(x^{2^m} + x + \delta)^s + ax$ over $\mathbb{F}_{2^{2m}}$ for the exponent s satisfying $s \equiv 2^j \pmod{2^m + 1}$ or $s \equiv 2^j \pmod{2^m - 1}$, where j is an integer, $a \in \mathbb{F}_{2^m}^*$ and $\delta \in \mathbb{F}_{2^{2m}}$. Furthermore, some classes of PPs with the form $(x^{2^m} + x + \delta)^{s_1} + (x^{2^m} + x + \delta)^{s_2} + ax$ are given over $\mathbb{F}_{2^{2m}}$, where the exponent $s_1 \equiv s_2 \pmod{2^m + 1}$, or $s_1 \equiv 2^j \pmod{2^m + 1}$ and $s_2 \equiv 2^k \pmod{2^m + 1}$ for some different integers j and k, $a \in \mathbb{F}_{2^m}^*$ and $\delta \in \mathbb{F}_{2^{2m}}$. Finally, we prove that the PPs constructed in this paper are quasi-multiplicative (QM) inequivalent to the known PPs.

The remainder of this paper is organized as follows. In Section 2, some necessary notations and related results are introduced. Several classes of PPs with the form (3) are proposed over $\mathbb{F}_{2^{2m}}$ for $i = 1$ in Section 3. Section 4 is devoted to constructing some new classes of PPs with the form (3) over $\mathbb{F}_{2^{2m}}$ for $i = 2$. In Section 5, we evaluate whether the PPs in this paper are QM equivalent to all known ones or not. Finally, we give some concluding remarks in Section 6.

2 Preliminaries

In this section, we introduce some basic notations and related results needed in this paper.

For two positive integers m and n with $m \mid n$, the trace function $\mathrm{Tr}_m^n(\cdot)$ from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ is defined by

$$\mathrm{Tr}_m^n(x) = x + x^{p^m} + x^{p^{2m}} + \cdots + x^{p^{(\frac{n}{m}-1)m}}.$$

Define a subset of $\mathbb{F}_{p^n}$ by

$$\mathcal{J} = \{\gamma^{p^m} - \gamma | \gamma \in \mathbb{F}_{p^n}\} = \{\alpha \in \mathbb{F}_{p^n} : \mathrm{Tr}_m^n(\alpha) = 0\}.$$

For each element $x \in \mathbb{F}_{p^{2m}}$, its conjugate is defined by $\bar{x} = x^{p^m}$. For $a, b \in \mathbb{F}_{p^{2m}}$, we have $a + \bar{a}$, $a\bar{a} \in \mathbb{F}_{p^m}$ and $\overline{a+b} = \bar{a} + \bar{b}$, $\overline{ab} = \bar{a}\bar{b}$.

First, we recall the definition of a q-polynomial from [14] as follows.

Definition 2.1. ([14]) *For a fixed prime power q, a polynomial of the form*

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

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

In the following, we introduce a useful lemma, which follows from the AGW criterion.

Lemma 2.1. ([1]) *For positive integers m, n with $m \mid n$, let $\varphi(x)$ be an $\mathbb{F}_{p^m}$-linear polynomial over $\mathbb{F}_{p^m}$, $h(x) \in \mathbb{F}_{q^n}[x]$ be any polynomial such that $h(x^{p^m} - x) \in \mathbb{F}_{p^m} \backslash \{0\}$ for all $x \in \mathbb{F}_{p^n}$, and let $g(x) \in \mathbb{F}_{p^n}[x]$ be any polynomial. Then $h(x^{p^m} - x)\varphi(x) + g(x^{p^m} - x)$ is a permutation of $\mathbb{F}_{p^n}$ if and only if the following two conditions hold*

(1) *$\varphi(x)$ induces a permutation polynomial of $\mathbb{F}_{p^m}$;*

(2) *$h(x)\varphi(x) + g(x)^{p^m} - g(x)$ permutes $\mathcal{J}$.*

The following result is immediately obtained by taking $g(x) = \sum_{j=1}^{t}(x+\delta)^{s_j}$, $h(x) = 1$ and $\varphi(x) = ax$, where $a \in \mathbb{F}_{2^m}^*$.

Lemma 2.2. *Let m and n be positive integers with $m \mid n$, and let $s_1, \cdots, s_t$ be nonnegative integers. For $a \in \mathbb{F}_{2^m}^*$ and $\delta \in \mathbb{F}_{2^n}$, the polynomial*

$$f(x) = \sum_{j=1}^{t}(x^{2^m} + x + \delta)^{s_j} + ax$$

permutes $\mathbb{F}_{2^n}$ if and only if

$$\sum_{j=1}^{t}\left((x+\delta)^{2^m s_j} + (x+\delta)^{s_j}\right) + ax$$

permutes $\mathcal{J}$.

Remark 1. If $\delta \in \mathbb{F}_{2^m}$, then $\mathrm{Tr}_m^{2m}(\delta) = \delta + \bar{\delta} = 0$. By applying Lemma 2.2, one can obtain that $f(x) = \sum_{j=1}^{t}(x^{2^m} + x + \delta)^{s_j} + ax$ permutes $\mathbb{F}_{2^{2m}}$ if and only if ax permutes $\mathbb{F}_{2^m}$, which is always true since $a \in \mathbb{F}_{2^m}^*$.

Next, we recall some useful lemmas needed in the subsequent section.

Lemma 2.3. ([14]) *For a positive integer m and $a, b \in \mathbb{F}_{2^m}$ with $a \neq 0$, the equation $x^2 + ax + b = 0$ has a solution in $\mathbb{F}_{2^m}$ if and only if $\mathrm{Tr}_1^m\left(\frac{b}{a^2}\right) = 0$.*

Lemma 2.4. ([2]) *For $a \in \mathbb{F}_{2^m}^*$, the cubic equation $x^3 + x + a = 0$ over $\mathbb{F}_{2^m}$ 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 polynomial $P_m(x)$ are 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 2.5. ([3]) *For $a \in \mathbb{F}_{2^m}$ and $b \in \mathbb{F}_{2^m}^*$, the cubic equation $x^3 + ax + b = 0$ has exactly one solution in $\mathbb{F}_{2^m}$ if and only if $\mathrm{Tr}_1^m\left(1 + \frac{a^3}{b^2}\right) \neq 0$.*

The following result is a direct consequence of Lemma 2.2.

Lemma 2.6. *For two positive integers m and s, let $a \in \mathbb{F}_{2^m}^*$ and $\delta \in \mathbb{F}_{2^{2m}}$, the polynomial $f(x) = (x^{2^m} + x + \delta)^s + ax$ is a PP over $\mathbb{F}_{2^{2m}}$ if and only if $g(x) = (x^{2^m} + x + \delta)^{2^m \cdot s} + ax$ permutes $\mathbb{F}_{2^{2m}}$.*

3 PPs with the form $(x^{2^m} + x + \delta)^s + ax$ over $\mathbb{F}_{2^{2m}}$

In this section, we construct several classes of PPs of the form $(x^{2^m}+x+\delta)^s+ax$ over $\mathbb{F}_{2^{2m}}$,where the exponent s satisfies $s \equiv 2^j \pmod{2^m+1}$ or $s \equiv 2^j \pmod{2^m-1}$ for some integers j, $a \in \mathbb{F}_{2^m}^*$ and $\delta \in \mathbb{F}_{2^{2m}}$. It is easy to see that $f(x) = (x^{2^m} + x + \delta)^s + ax$ is a PP of $\mathbb{F}_{2^{2m}}$ if $\mathrm{Tr}_m^{2m}(\delta) = 0$ from Remark 1. Therefore, we only consider the permutation behavior of $(x^{2^m} + x + \delta)^s + ax$ if $\mathrm{Tr}_m^{2m}(\delta) \neq 0$ in the sequel.

The following lemma concerning the number of solutions of a quintic equation would be useful in the sequel.

Lemma 3.1. *Let k be a positive integer. For $a \in \mathbb{F}_{2^m}^*$ and $\delta \in \mathbb{F}_{2^{2m}}$ such that $\mathrm{Tr}_m^{2m}(\delta) \neq 0$, let $c \in \mathbb{F}_{2^m}$ with $\mathrm{Tr}_1^m\left(\frac{c}{(\delta+\bar{\delta})^2}\right) = 0$. Then for any $d \in \mathbb{F}_{2^m}$, the equation*

$$x^5 + (\delta+\bar{\delta})^2x^3 + \left(d^4 + d^2(\delta+\bar{\delta})^2 + (\delta\bar{\delta})^2 + c^2\right)x + \frac{(\delta+\bar{\delta})^k}{a} = 0$$

has at most one solution in $\mathbb{F}_{2^m}$ if $\mathrm{Tr}_m^{2m}(\delta)^{k-5} = a$.

Proof. Let $\theta = \mathrm{Tr}_m^{2m}(\delta) = \delta + \bar{\delta}$, and define $b = d^4 + d^2(\delta+\bar{\delta})^2 + (\delta\bar{\delta})^2 + c^2 = (d^2 + \theta d + \delta\bar{\delta} + c)^2$. Since $\mathrm{Tr}_1^m\left(\frac{c}{(\delta+\bar{\delta})^2}\right) = 0$, one can verify that

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

Then we obtain $b \neq 0$ for any $d \in \mathbb{F}_{2^m}$, which follows from Lemma 2.3. Suppose that there are two solutions x and $x+t$ in $\mathbb{F}_{2^m}$ for some $t \in \mathbb{F}_{2^m}^*$, which leads to

$$\begin{cases} x^5 + \theta^2 x^3 + bx + \frac{\theta^k}{a} = 0, \\ (x+t)^5 + \theta^2 (x+t)^3 + b(x+t) + \frac{\theta^k}{a} = 0. \end{cases} \tag{4}$$

Adding the above two equations yields

$$x^4 + \theta^2 x^2 + (t^3 + \theta^2 t)x + t^4 + \theta^2 t^2 + b = 0. \tag{5}$$

We distinguish two cases.

Case I: $t^3 + \theta^2 t = 0$. Then $t = \theta$ and Eq. (5) becomes

$$(x+d)^4 + \theta^2 (x+d)^2 + (\delta\bar{\delta} + c)^2 = 0.$$

Note that $\mathrm{Tr}_1^m\left(\frac{\delta\bar{\delta}+c}{\theta^2}\right) = 1$, we have $x + d \notin \mathbb{F}_{2^m}$ by Lemma 2.3, which leads to a contradiction.

Case II: $t^3 + \theta^2 t \neq 0$. Substituting $x^4 + \theta^2 x^2 = (t^3 + \theta^2 t)x + t^4 + \theta^2 t^2 + b$ into the first equation of Eq. (4) gives

$$x^5 + \theta^2 x^3 + bx + \frac{\theta^k}{a} = (t^3 + \theta^2 t)x^2 + t(t^3 + \theta^2 t)x + \frac{\theta^k}{a} = 0,$$

which implies

$$x^2 = tx + \frac{\theta^k}{a(t^3 + \theta^2 t)}, \tag{6}$$

and hence

$$x^4 = t^2 x^2 + \frac{\theta^{2k}}{a^2(t^6 + \theta^4 t^2)} = t^3 x + \frac{t\theta^k}{a(t^2 + \theta^2)} + \frac{\theta^{2k}}{a^2(t^6 + \theta^4 t^2)}. \tag{7}$$

Plugging Eqs. (6) and (7) into Eq. (5), we obtain

$$d^4 + \theta^2 d^2 + (\delta\bar{\delta})^2 + \frac{t\theta^k}{a(t^2+\theta^2)} + \frac{\theta^{2k}}{a^2(t^6+\theta^4 t^2)} + \frac{\theta^{k+2}}{a(t^3+\theta^2 t)} + t^4 + \theta^2 t^2 + c^2 = 0. \tag{8}$$

It can be verified that

$$\begin{aligned} & \mathrm{Tr}_1^m\left(\frac{(\delta\bar{\delta})^2 + \frac{t\theta^k}{a(t^2+\theta^2)} + \frac{\theta^{2k}}{a^2(t^6+\theta^4 t^2)} + \frac{\theta^{k+2}}{a(t^3+\theta^2 t)} + t^4 + \theta^2 t^2 + c^2}{\theta^4}\right) \\ = \; & \mathrm{Tr}_1^m\left(\frac{(\delta\bar{\delta})^2}{\theta^4} + \frac{t\theta^{k-4}}{a(t^2+\theta^2)} + \frac{\theta^{2k-4}}{a^2(t^6+\theta^4 t^2)} + \frac{\theta^{k-2}}{a(t^3+\theta^2 t)} + \frac{t^4}{\theta^4} + \frac{t^2}{\theta^2} + \frac{c^2}{\theta^4}\right) \\ = \; & 1 + \mathrm{Tr}_1^m\left(\frac{t\theta^{k-4}}{a(t^2+\theta^2)}\right). \end{aligned}$$

If $\mathrm{Tr}_m^{2m}(\delta)^{k-5} = \theta^{k-5} = a$, we have $\mathrm{Tr}_1^m\left(\frac{t\theta^{k-4}}{a(t^2+\theta^2)}\right) = \mathrm{Tr}_1^m\left(\frac{1}{1+\frac{t}{\theta}} + \frac{1}{1+(\frac{t}{\theta})^2}\right) = 0$. By Lemma 2.3, Eq. (8) has no solution in $\mathbb{F}_{2^m}$, which contradicts the fact that $d^2 \in \mathbb{F}_{2^m}$.

Therefore, we conclude that there does not exist $t \in \mathbb{F}_{2^m}^*$ such that Eq. (4) holds. This completes the proof. □

3.1 $s \equiv 2^j \pmod{2^m+1}$

In this subsection, we will investigate several classes of PPs with the form $(x^{2^m}+x+\delta)^s+ax$ over $\mathbb{F}_{2^{2m}}$,where the exponent s satisfies $s \equiv 2^j \pmod{2^m+1}$ for some integers j, $a \in \mathbb{F}_{2^m}^*$ and $\delta \in \mathbb{F}_{2^{2m}}$.

Theorem 3.1. *Let m, i, j be three positive integers, and let $s_1 = i(2^m+1)+2^j$ and $s_2 = i(2^m+1)+2^{m+j}$. For any $\delta \in \mathbb{F}_{2^{2m}}$ and $a \in \mathbb{F}_{2^m}^*$, the polynomial $f(x) = (x^{2^m}+x+\delta)^{s_1}+ax$ permutes $\mathbb{F}_{2^{2m}}$ if and only if $g(x) = (x^{2^m}+x+\delta)^{s_2}+ax$ permutes $\mathbb{F}_{2^{2m}}$.*

Proof. From Lemma 2.2, $f(x)$ permutes $\mathbb{F}_{2^{2m}}$ if and only if $(x+\delta)^{i(2^m+1)+2^{j+m}}+(x+\delta)^{i(2^m+1)+2^j}+ax$ permutes $\mathbb{F}_{2^m}$.

Similarly, to prove that $g(x)$ is a permutation polynomial of $\mathbb{F}_{2^{2m}}$, we only need to prove that $(x+\delta)^{i(2^m+1)+2^j}+(x+\delta)^{i(2^m+1)+2^{j+m}}+ax$ permutes $\mathbb{F}_{2^m}$. This completes the proof. □

Theorem 3.2. *Let m be a positive integer, and let i and j be integers satisfying $0 \le i \le m-1$ and $0 \le j \le 2m-1$. For any $\delta \in \mathbb{F}_{2^{2m}}$ and $a \in \mathbb{F}_{2^m}^*$, consider the polynomial*

$$f(x) = (x^{2^m}+x+\delta)^{2^i(2^m+1)+2^j}+ax.$$

Then $f(x)$ permutes $\mathbb{F}_{2^{2m}}$ if and only if either $\mathrm{Tr}_m^{2m}(\delta)=0$, or $\mathrm{Tr}_m^{2m}(\delta)\neq 0$ and the equation

$$x^{2^{i+1}-1}+x^{2^i-1}+\frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j+2^{i+1}-1}}=0$$

has no nonzero solution in $\mathbb{F}_{2^m}$.

Proof. If $\mathrm{Tr}_m^{2m}(\delta)=0$, then $f(x)$ permutes $\mathbb{F}_{2^{2m}}$, which follows from Remark 1. Now we consider the case $\mathrm{Tr}_m^{2m}(\delta)\neq 0$. According to Lemma 2.2, it suffices to show that for each $d \in \mathbb{F}_{2^m}$, the equation

$$(x+\delta)^{2^i(1+2^m)+2^{m+j}}+(x+\delta)^{2^i(2^m+1)+2^j}+ax=d$$

has at most one solution in $\mathbb{F}_{2^m}$. The above equation can be simplified as

$$(x+\delta)^{2^i(1+2^m)}(\delta^{2^j}+\bar{\delta}^{2^j})+ax=\mathrm{Tr}_m^{2m}(\delta)^{2^j}(x^2+\mathrm{Tr}_m^{2m}(\delta)x+\delta\bar{\delta})^{2^i}+ax=d. \tag{9}$$

Dividing Eq. (9) by $\mathrm{Tr}_m^{2m}(\delta)^{2^j}$, we obtain that Eq. (9) has at most one solution if and only if the following linearized equation

$$x^{2^{i+1}}+\mathrm{Tr}_m^{2m}(\delta)^{2^i}x^{2^i}+\frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j}}x=0$$

has only the zero solution, or equivalently, the equation

$$x^{2^{i+1}-1}+x^{2^i-1}+\frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j+2^{i+1}-1}}=0 \tag{10}$$

has no nonzero solution in $\mathbb{F}_{2^m}$, obtained by replacing x with $\mathrm{Tr}_m^{2m}(\delta)x$ and dividing by x. This completes the proof. □

In Theorem 3.2, let $i=m-1$ and $i=m-2$, respectively, the following PPs over $\mathbb{F}_{2^{2m}}$ can be obtained correspondingly.

Corollary 3.1. *Let m be a positive integer, and let j be an integer satisfying $0 \le j \le 2m-1$. For any $\delta \in \mathbb{F}_{2^{2m}}$ and $a \in \mathbb{F}_{2^m}^*$, the polynomial*

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

permutes $\mathbb{F}_{2^{2m}}$ if and only if either $\mathrm{Tr}_m^{2m}(\delta) = 0$ or $\mathrm{Tr}_m^{2m}(\delta)^{2^j} = a$.

Proof. Since

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

by Theorem 3.2, we know that $f(x)$ permutes $\mathbb{F}_{2^{2m}}$ if $\mathrm{Tr}_m^{2m}(\delta) = 0$. Thus it remains to consider the case $\mathrm{Tr}_m^{2m}(\delta) \neq 0$ and the necessary and sufficient condition for determining that the equation

$$x^{2^m-1} + x^{2^{m-1}-1} + \frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j}} = 0$$

has no nonzero solution in $\mathbb{F}_{2^m}$.

For any $x \in \mathbb{F}_{2^m}^*$, squaring both sides of the above equation gives

$$\frac{1}{x} + \left(1 + \frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j}}\right)^2 = 0. \tag{11}$$

If $\mathrm{Tr}_m^{2m}(\delta)^{2^j} = a$, then Eq. (11) can be reduced to $\frac{1}{x} = 0$, which clearly has no solution in $\mathbb{F}_{2^m}$. If $\mathrm{Tr}_m^{2m}(\delta)^{2^j} \neq a$, then Eq. (11) admits the nonzero solution $x_0 = 1 + \frac{a^2}{\mathrm{Tr}_m^{2m}(\delta)^{2^{j+1}}+a^2}$, a contradiction.

Consequently, we deduce that $f(x)$ is a PP over $\mathbb{F}_{2^{2m}}$ if and only if either $\mathrm{Tr}_m^{2m}(\delta) = 0$ or $\mathrm{Tr}_m^{2m}(\delta)^{2^j} = a$. This completes the proof. □

Corollary 3.2. *Let m be a positive integer, and let j be an integer such that $0 \le j \le 2m-1$. For any $\delta \in \mathbb{F}_{2^{2m}}$ and $a \in \mathbb{F}_{2^m}^*$, the polynomial*

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

permutes $\mathbb{F}_{2^{2m}}$ if and only if either $\mathrm{Tr}_m^{2m}(\delta) = 0$, or $\mathrm{Tr}_m^{2m}(\delta) \neq 0$, $\mathrm{Tr}_1^m({c_1}^{-1}) = \mathrm{Tr}_1^m(1)$ and $P_m(c_1) \neq 0$, where $c_1 = \frac{a^2}{\mathrm{Tr}_m^{2m}(\delta)^{2^{j+1}-1}}$ and $P_m(x)$ is defined in Lemma 2.4.

Proof. Note that $2^{2m-2} + 2^{m-2} + 2^j = 2^{m-2}(2^m+1) + 2^j$. According to Theorem 3.2, we obtain that $f(x)$ is a PP over $\mathbb{F}_{2^{2m}}$ if $\mathrm{Tr}_m^{2m}(\delta) = 0$. Next, we only focus on the case $\mathrm{Tr}_m^{2m}(\delta) \neq 0$ and characterize the necessary and sufficient condition for the equation

$$x^{2^{m-1}-1} + x^{2^{m-2}-1} + \frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j+2^{m-1}-1}} = 0 \tag{12}$$

has no nonzero solution in $\mathbb{F}_{2^m}$.

For any $x \in \mathbb{F}_{2^m}^*$, raising both sides of Eq. (12) to the fourth power yields

$$x^{-2} + x^{-3} + \frac{a^4}{\mathrm{Tr}_m^{2m}(\delta)^{2^{j+2}-2}} = 0.$$

Multiplying by x^3 and replacing x by $\frac{\mathrm{Tr}_m^{2m}(\delta)^{2^{j+1}-1}}{a^2}x$, the above equation can be reduced to

$$\frac{\mathrm{Tr}_m^{2m}(\delta)^{2^{j+1}-1}}{a^2}(x^3+x+\frac{a^2}{\mathrm{Tr}_m^{2m}(\delta)^{2^{j+1}-1}})=0,$$

which is equivalent to

$$x^3+x+\frac{a^2}{\mathrm{Tr}_m^{2m}(\delta)^{2^{j+1}-1}}=0. \tag{13}$$

It can be checked that $f(x)$ is a PP over $\mathbb{F}_{2^{2m}}$ if Eq. (13) has no nonzero solution in $\mathbb{F}_{2^m}$ when $\mathrm{Tr}_m^{2m}(\delta)\neq 0$. Denote $c_1=\frac{a^2}{\mathrm{Tr}_m^{2m}(\delta)^{2^{j+1}-1}}$, we know that Eq. (13) has no solution in $\mathbb{F}_{2^m}$ if and only if $\mathrm{Tr}_1^m({c_1}^{-1})=\mathrm{Tr}_1^m(1)$ and $P_m(c_1)\neq 0$, which follows from Lemma 2.4. This completes the proof. □

Remark 2. If $j\in\{0,2m-1\}$ and $a=1$, then the PPs given in Corollary 3.2 are exactly proposed by [34]. Moreover, if $j\in\{0,m-1,m,2m-1,m-4,2m-4,m-3,2m-3\}$, then the PPs given in Corollary 3.2 are exactly proposed by [26].

Theorem 3.3. *Let m be a positive integer, and let i and j be integers satisfying $0\leq i\leq m-1$ and $0\leq j\leq 2m-1$. For any $d\in\mathbb{F}_{2^m}$, $\delta\in\mathbb{F}_{2^{2m}}$ and $a\in\mathbb{F}_{2^m}^*$, consider the polynomial*

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

Then $f(x)$ permutes $\mathbb{F}_{2^{2m}}$ if and only if either $\mathrm{Tr}_m^{2m}(\delta)=0$, or $\mathrm{Tr}_m^{2m}(\delta)\neq 0$ and the equation

$$(ax+d)(x^2+(\delta+\bar{\delta})x+\delta\bar{\delta})^{2^i}+\mathrm{Tr}_m^{2m}(\delta)^{2^j}=0$$

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

Proof. Based on Remark 1, $f(x)$ permutes $\mathbb{F}_{2^{2m}}$ if $\mathrm{Tr}_m^{2m}(\delta)=0$. We now consider the case $\mathrm{Tr}_m^{2m}(\delta)\neq 0$. Applying Lemma 2.2, it suffices to show that for any $d\in\mathbb{F}_{2^m}$, the equation

$$(x+\delta)^{2^{2m}+2^{m+j}-2^i(2^m+1)-1}+(x+\delta)^{2^{2m}-2^i(2^m+1)+2^j-1}+ax=d \tag{14}$$

has at most one solution in $\mathbb{F}_{2^m}$. Since the exponents are reduced modulo $2^{2m}-1$, Eq. (14) can be simplified as

$$\mathrm{Tr}_m^{2m}(\delta)^{2^j}(x+\delta)^{2^{2m}-2^i(2^m+1)-1}+ax=d.$$

For any $x\in\mathbb{F}_{2^m}$ and $\delta\notin\mathbb{F}_{2^m}$, we have $x+\delta\neq 0$. Multiplying by $(x+\delta)^{2^i(2^m+1)}$ yields

$$(ax+d)\left(x^2+(\delta+\bar{\delta})x+\delta\bar{\delta}\right)^{2^i}+\mathrm{Tr}_m^{2m}(\delta)^{2^j}=0. \tag{15}$$

Hence, $f(x)$ is a PP over $\mathbb{F}_{2^{2m}}$ if and only if Eq. (15) has at most one solution in $\mathbb{F}_{2^m}$ when $\mathrm{Tr}_m^{2m}(\delta)\neq 0$. This completes the proof. □

Let $i=0$ and $i=1$, respectively. According to Theorem 3.3, we have the following corollaries.

Corollary 3.3. *Let m be a positive integer, and let j be integer satisfying $0 \le j \le 2m-1$. For any $\delta \in \mathbb{F}_{2^{2m}}$ and $a \in \mathbb{F}_{2^m}^*$, the polynomial*

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

permutes $\mathbb{F}_{2^{2m}}$ if either $\mathrm{Tr}_m^{2m}(\delta) = 0$ or $\mathrm{Tr}_m^{2m}(\delta)^{2^j-3} = a$.

Proof. Note that

$$f(x) = (x^{2^m} + x + \delta)^{2^{2m}+2^j-2^m-2} + ax = (x^{2^m} + x + \delta)^{2^{2m}+2^j-2^0(2^m+1)-1} + ax,$$

we obtain that $f(x)$ is a PP over $\mathbb{F}_{2^{2m}}$ if $\mathrm{Tr}_m^{2m}(\delta) = 0$, which follows from Theorem 3.3. Next, assume that $\mathrm{Tr}_m^{2m}(\delta) \neq 0$, we need to show that for any $d \in \mathbb{F}_{2^m}$, the equation

$$\begin{aligned} & (ax+d)\left(x^2 + (\delta+\bar{\delta})x + \delta\bar{\delta}\right) + \mathrm{Tr}_m^{2m}(\delta)^{2^j} \\ = \;& ax^3 + (a\mathrm{Tr}_m^{2m}(\delta) + d)x^2 + (a\delta\bar{\delta} + d\mathrm{Tr}_m^{2m}(\delta))x + d\delta\bar{\delta} + \mathrm{Tr}_m^{2m}(\delta)^{2^j} = 0 \end{aligned}$$

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

Denote $\theta_1 = \mathrm{Tr}_m^{2m}(\delta)$. Dividing the above equation by a and replacing $\frac{d}{a}$ by d_1, we can get

$$x^3 + (\theta_1 + d_1)x^2 + (\delta\bar{\delta} + d_1\theta_1)x + d_1\delta\bar{\delta} + \frac{\theta_1^{2^j}}{a} = 0.$$

Replacing x by $\theta_1 + d_1 + x$ gives

$$x^3 + (d_1^2 + d_1\theta_1 + \theta_1^2 + \delta\bar{\delta})x + \left(d_1^2\theta_1 + d_1\theta_1^2 + \delta\bar{\delta}\theta_1 + \frac{\theta_1^{2^j}}{a}\right) = 0. \tag{16}$$

Thus it suffices to prove that Eq. (16) has at most one solution in $\mathbb{F}_{2^m}$ whenever $\mathrm{Tr}_m^{2m}(\delta) \neq 0$.

Define $u_1 = d_1^2 + d_1\theta_1 + \theta_1^2 + \delta\bar{\delta}$ and $v_1 = d_1^2\theta_1 + d_1\theta_1^2 + \delta\bar{\delta}\theta_1 + \frac{\theta_1^{2^j}}{a}$. Note that $v_1 = \theta_1 u_1$ if $\mathrm{Tr}_m^{2m}(\delta)^{2^j-3} = \theta_1^{2^j-3} = a$.

If $v_1 = 0$, then $x = 0$ is the unique solution of Eq. (16) in $\mathbb{F}_{2^m}$. If $v_1 \neq 0$, we know that $\mathrm{Tr}_1^m(1 + \frac{u_1^3}{v_1^2}) = \mathrm{Tr}_1^m(\frac{\delta\bar{\delta}}{\theta_1^2}) = \mathrm{Tr}_1^m\left(\frac{\delta(\theta_1+\delta)}{\theta_1^2}\right) = \frac{\delta+\bar{\delta}}{\theta_1} = 1 \neq 0$. By Lemma 2.5, Eq. (16) has a unique solution in $\mathbb{F}_{2^m}$.

Therefore, we deduce that $f(x)$ permutes $\mathbb{F}_{2^{2m}}$ if either $\mathrm{Tr}_m^{2m}(\delta) = 0$ or $\mathrm{Tr}_m^{2m}(\delta)^{2^j-3} = a$. This completes the proof. □

Example 1. Take $m = 4$ and $j = 3$. Let ω be a root of the primitive polynomial $x^4 + x + 1$ and set $a = \omega^{10}$. By calculation, it can be verified that there are 16 different $\delta \in \mathbb{F}_{2^8}$ satisfying that $\mathrm{Tr}_4^8(\delta) = 0$, and 80 different $\delta \in \mathbb{F}_{2^8}$ satisfying that $\mathrm{Tr}_4^8(\delta)^5 = \omega^{10}$, and these δ are exactly all the elements in $\mathbb{F}_{2^8}$ such that

$$f(x) = (x^{16} + x + \delta)^{-9} + \omega^{10}x$$

is a permutation of $\mathbb{F}_{2^8}$. Furthermore, one can verify that $f(x)$ cannot permute $\mathbb{F}_{2^8}$ if $\mathrm{Tr}_4^8(\delta) \neq 0$ and $\mathrm{Tr}_4^8(\delta)^5 \neq \omega^{10}$. In this example, all possible elements $\delta \in \mathbb{F}_{2^8}$ such that $f(x)$ is a permutation over $\mathbb{F}_{2^8}$ are covered by Corollary 3.3.

Remark 3. If $j = 2m$ and $a = 1$, then the PP given in Corollary 3.3 is exactly Theorem 3 in [19].

Corollary 3.4. *Let m be a positive integer, and let j be integer satisfying $0 \le j \le 2m-1$. For any $\delta \in \mathbb{F}_{2^{2m}}$ and $a \in \mathbb{F}_{2^m}^*$, the polynomial*

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

permutes $\mathbb{F}_{2^{2m}}$ if either $\mathrm{Tr}_m^{2m}(\delta) = 0$ or $\mathrm{Tr}_m^{2m}(\delta)^{2^j-5} = a$.

Proof. Observing that $2^{2m} + 2^j - 2^{m+1} - 3 = 2^{2m} + 2^j - 2^i(2^m+1) - 1$ with $i = 1$. According to Theorem 3.3, $f(x)$ permutes $\mathbb{F}_{2^{2m}}$ if and only if either $\mathrm{Tr}_m^{2m}(\delta) = 0$, or $\mathrm{Tr}_m^{2m}(\delta) \neq 0$ and the equation

$$\begin{aligned} & (ax+d)(x^2 + (\delta+\bar{\delta})x + \delta\bar{\delta})^2 + \mathrm{Tr}_m^{2m}(\delta)^{2^j} \\ = \;& ax^5 + dx^4 + a(\delta+\bar{\delta})^2x^3 + d(\delta+\bar{\delta})^2x^2 + a(\delta\bar{\delta})^2x + \mathrm{Tr}_m^{2m}(\delta)^{2^j} + d(\delta\bar{\delta})^2 = 0 \end{aligned} \tag{17}$$

has at most one solution in $\mathbb{F}_{2^m}$ for any $d \in \mathbb{F}_{2^m}$. We now focus on the case $\mathrm{Tr}_m^{2m}(\delta) \neq 0$.

Dividing Eq. (17) by a and setting $d_2 = \frac{d}{a}$ yields

$$x^5 + d_2x^4 + (\delta+\bar{\delta})^2x^3 + d_2(\delta+\bar{\delta})^2x^2 + (\delta\bar{\delta})^2x + \frac{\mathrm{Tr}_m^{2m}(\delta)^{2^j}}{a} + d_2(\delta\bar{\delta})^2 = 0,$$

then we obtain that Eq. (17) has at most one solution in $\mathbb{F}_{2^m}$ if the following equation

$$x^5 + (\delta+\bar{\delta})^2x^3 + (d_2^4 + d_2^2(\delta+\bar{\delta})^2 + (\delta\bar{\delta})^2)x + \frac{\mathrm{Tr}_m^{2m}(\delta)^{2^j}}{a} = 0 \tag{18}$$

has at most one solution in $\mathbb{F}_{2^m}$, obtained by replacing x with $d_2 + x$. Thus, Eq. (18) has at most one solution if $\mathrm{Tr}_m^{2m}(\delta)^{2^j-5} = a$, which follows from Lemma 3.1. This completes the proof. □

Example 2. Take $m = 4$ and $j = 3$. Let ω be a root of the primitive polynomial $x^4 + x^3 + 1$ and set $a = \omega^3$. Magma experiments show that there are 16 different $\delta \in \mathbb{F}_{2^8}$ satisfying that $\mathrm{Tr}_4^8(\delta) = 0$, and 48 different $\delta \in \mathbb{F}_{2^8}$ satisfying that $\mathrm{Tr}_4^8(\delta)^3 = \omega^3$, and these δ are exactly all the elements in $\mathbb{F}_{2^8}$ such that

$$g(x) = (x^{16} + x + \delta)^{-26} + \omega^3 x$$

is a permutation of $\mathbb{F}_{2^8}$. Furthermore, it can be checked that $g(x)$ cannot permute $\mathbb{F}_{2^8}$ if $\mathrm{Tr}_4^8(\delta) \neq 0$ and $\mathrm{Tr}_4^8(\delta)^3 \neq \omega^3$. The experimental results are consistent with our result in Corollary 3.4.

Remark 4. If $j = m+1$ and $a = 1$, then the PP given in Corollary 3.4 is exactly proposed by [27]. Moreover, if $a = 1$, then the PP given in Corollary 3.4 is exactly investigated in [23].

3.2 $s \equiv 2^j \pmod{2^m - 1}$

In this subsection, we will propose several classes of PPs with the form $(x^{2^m} + x + \delta)^s + ax$ over $\mathbb{F}_{2^{2m}}$,where the exponent s satisfies $s \equiv 2^j \pmod{2^m-1}$ for some integers j, $a \in \mathbb{F}_{2^m}^*$ and $\delta \in \mathbb{F}_{2^{2m}}$.

Theorem 3.4. *Let m be a positive integer, and let i and j be integers satisfying $0 \le i, j \le 2m-1$. For any $d \in \mathbb{F}_{2^m}$, $\delta \in \mathbb{F}_{2^{2m}}$ and $a \in \mathbb{F}_{2^m}^*$, consider the polynomial*

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

permutes $\mathbb{F}_{2^{2m}}$ if and only if either $\mathrm{Tr}_m^{2m}(\delta) = 0$, or $\mathrm{Tr}_m^{2m}(\delta) \neq 0$ and the equation

$$(x+\delta)^{2^i}(x+\bar{\delta})^{2^j-2^i} + (x+\delta)^{2^j-2^i}(x+\bar{\delta})^{2^i} + ax + d = 0$$

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

Proof. According to Remark 1, $f(x)$ permutes $\mathbb{F}_{2^{2m}}$ if $\mathrm{Tr}_m^{2m}(\delta) = 0$. Next, we only consider the case $\mathrm{Tr}_m^{2m}(\delta) \neq 0$. Based on Lemma 2.2, it suffices to prove that for any $d \in \mathbb{F}_{2^m}$, the equation

$$(x+\delta)^{2^{i+m}(2^m-1)+2^{j+m}} + (x+\delta)^{2^i(2^m-1)+2^j} + ax = d \tag{19}$$

has at most one solution in $\mathbb{F}_{2^m}$. Since $x \in \mathbb{F}_{2^m}$ and $\delta \notin \mathbb{F}_{2^m}$, we have $x+\delta \neq 0$ and $x+\bar{\delta} \neq 0$. Expanding Eq. (19) gives

$$(x+\delta)^{2^i}(x+\bar{\delta})^{2^j-2^i} + (x+\delta)^{2^j-2^i}(x+\bar{\delta})^{2^i} + ax + d = 0. \tag{20}$$

Thus, $f(x)$ is a PP over $\mathbb{F}_{2^{2m}}$ if and only if Eq. (20) has at most one solution in $\mathbb{F}_{2^m}$. This completes the proof. □

Next, according to Theorem 3.4, we derive the following corollaries by specifying i and j.

Corollary 3.5. *Let m be a positive integer. For any $\delta \in \mathbb{F}_{2^{2m}}$ and $a \in \mathbb{F}_{2^m}^*$, the polynomial*

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

permutes $\mathbb{F}_{2^{2m}}$ if $\mathrm{Tr}_m^{2m}(\delta) \in \{0, a\}$.

Proof. Recall

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

based on Theorem 3.4, we know that $f(x)$ permutes $\mathbb{F}_{2^{2m}}$ if and only if either $\mathrm{Tr}_m^{2m}(\delta) = 0$, or $\mathrm{Tr}_m^{2m}(\delta) \neq 0$ and the equation

$$(x+\delta)^4(x+\bar{\delta})^{-2} + (x+\delta)^{-2}(x+\bar{\delta})^4 + (ax+d) = 0 \tag{21}$$

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

Assume $\mathrm{Tr}_m^{2m}(\delta) \neq 0$, if $x \in \mathbb{F}_{2^m}$, then $x+\delta \neq 0$ and $x+\bar{\delta} \neq 0$. Multiplying Eq. (21) by $(x+\delta)^2(x+\bar{\delta})^2$ and denote $\theta_3 = \mathrm{Tr}_m^{2m}(\delta)$, Eq. (21) can be simplified as

$$ax^5 + (\theta_3^2 + d)x^4 + a\theta_3^2x^3 + (\theta_3^4 + d\theta_3^2)x^2 + a(\delta\bar{\delta})^2x + (\delta^6 + \bar{\delta}^6 + d(\delta\bar{\delta})^2) = 0.$$

Dividing the above equation by a and replacing $\frac{d}{a}$ by d_3 yields

$$x^5 + (\frac{\theta_3^2}{a} + d_3)x^4 + \theta_3^2x^3 + (\frac{\theta_3^4}{a} + d_3\theta_3^2)x^2 + (\delta\bar{\delta})^2x + (d_3(\delta\bar{\delta})^2 + \frac{\delta^6 + \bar{\delta}^6}{a}) = 0.$$

Replacing x by $x+\frac{\theta_3^2}{a}+d_3$, the above equation can be reduced to

$$x^5+\theta_3^2x^3+\left(d_3^4+d_3^2\theta_3^2+\frac{\theta_3^8}{a^4}+\frac{\theta_3^6}{a^2}+(\delta\bar{\delta})^2\right)x+\frac{\theta_3^6}{a}=0. \tag{22}$$

Note that $\mathrm{Tr}_1^m\left(\frac{\frac{\theta_3^4}{a^2}+\frac{\theta_3^3}{a}}{\theta_3^2}\right)=\mathrm{Tr}_1^m\left(\frac{\theta_3^2}{a^2}+\frac{\theta_3}{a}\right)=0$, based on Lemma 3.1, Eq. (22) has at most one solution in $\mathbb{F}_{2^m}$ if $\mathrm{Tr}_m^{2m}(\delta)=a$. This completes the proof. □

Example 3. Take $m=5$. Let ω be a root of the primitive polynomial x^5+x^2+1 and set $a=\omega^8$. Magma experiments show that there are 32 different $\delta\in\mathbb{F}_{2^{10}}$ satisfying that $\mathrm{Tr}_5^{10}(\delta)=0$, and 32 different $\delta\in\mathbb{F}_{2^{10}}$ satisfying that $\mathrm{Tr}_5^{10}(\delta)=\omega^8$, and these δ are exactly all the elements in $\mathbb{F}_{2^{10}}$ such that

$$f(x)=(x^{32}+x+\delta)^{126}+\omega^8x$$

is a permutation of $\mathbb{F}_{2^{10}}$. Furthermore, it can also be verified that $f(x)$ cannot permute $\mathbb{F}_{2^{10}}$ if $\mathrm{Tr}_5^{10}(\delta)\neq 0$ and $\mathrm{Tr}_5^{10}(\delta)\neq\omega^8$. The experimental results are consistent with our result in Corollary 3.5.

Remark 5. By Lemma 2.6, we conclude that $f(x)=(x^{2^m}+x+\delta)^{2^{2m+1}-2^{m+1}+2}+ax$ permutes $\mathbb{F}_{2^{2m}}$ if and only if $g(x)=(x^{2^m}+x+\delta)^{2^{m+2}-2}+ax$ permutes $\mathbb{F}_{2^{2m}}$. Note that the permutation behavior of $g(x)$ have been proved in [3], yet the sufficient conditions provided are incomplete. Moreover, the method to verify the permutation behavior of polynomials in this paper differs from that in [3].

Corollary 3.6. *Let m be a positive integer. For any $\delta\in\mathbb{F}_{2^{2m}}$ and $a\in\mathbb{F}_{2^m}^*$, the polynomial*

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

permutes $\mathbb{F}_{2^{2m}}$ if $\mathrm{Tr}_m^{2m}(\delta)\in\{0,a\}$.

Proof. Note that $3\cdot 2^m-1=2^i(2^m-1)+2^j$ with $i=0$ and $j=m+1$. Hence, based on Theorem 3.4, for any $d\in\mathbb{F}_{2^m}$, we need to prove that the equation

$$(x+\delta)(x+\bar{\delta})^{2^{m+1}-1}+(x+\delta)^{2^{m+1}-1}(x+\bar{\delta})+ax+d=0 \tag{23}$$

has at most one solution in $\mathbb{F}_{2^m}$ if $\mathrm{Tr}_m^{2m}(\delta)\neq 0$.

Since $x\in\mathbb{F}_{2^m}$ and $\mathrm{Tr}_m^{2m}(\delta)\neq 0$, we have $\delta\notin\mathbb{F}_{2^m}$, which implies that $x+\delta\neq 0$ and $x+\bar{\delta}\neq 0$. Multiplying Eq. (23) by $(x+\delta)(x+\bar{\delta})$ yields

$$ax^3+\left(d+a(\delta+\bar{\delta})\right)x^2+\left(d(\delta+\bar{\delta})+a\delta\bar{\delta}\right)x+\left((\delta+\bar{\delta})^4+d\delta\bar{\delta}\right)=0.$$

Replacing x by $x+\frac{d}{a}+\delta+\bar{\delta}$ and dividing by a, the above equation can be simplified as

$$\begin{aligned}&x^3+\left(\frac{d^2}{a^2}+(\delta+\bar{\delta})^2+\frac{d}{a}(\delta+\bar{\delta})+\delta\bar{\delta}\right)x\\&+\left(\frac{d^2}{a^2}(\delta+\bar{\delta})+\frac{d}{a}(\delta+\bar{\delta})^2+\delta^2\bar{\delta}+\delta\bar{\delta}^2+\frac{(\delta+\bar{\delta})^4}{a}\right)=0.\end{aligned} \tag{24}$$

Therefore, $f(x)$ permutes $\mathbb{F}_{2^{2m}}$ if Eq. (24) has at most one solution in $\mathbb{F}_{2^m}$ when $\mathrm{Tr}_m^{2m}(\delta)\neq 0$.

Define $u_2 = \frac{d^2}{a^2} + (\delta+\bar{\delta})^2 + \frac{d}{a}(\delta+\bar{\delta}) + \delta\bar{\delta}$ and $v_2 = \frac{d^2}{a^2}(\delta+\bar{\delta}) + \frac{d}{a}(\delta+\bar{\delta})^2 + \delta^2\bar{\delta} + \delta\bar{\delta}^2 + \frac{(\delta+\bar{\delta})^4}{a}$. Thus we can get $v_2 = (\delta+\bar{\delta})u_2$ if $\mathrm{Tr}_m^{2m}(\delta) = a$.

If $v_2 = 0$, Eq. (24) has the unique solution $x = 0$. If $v_2 \neq 0$, we have $\mathrm{Tr}_1^m\left(1 + \frac{u_2^3}{v_2^2}\right) = \mathrm{Tr}_1^m\left(\frac{\delta\bar{\delta}}{\delta^2+\delta^2}\right) = 1 \neq 0$. By Lemma 2.5, Eq. (24) has a unique solution in $\mathbb{F}_{2^m}$.

Consequently, we deduce that $f(x)$ permutes $\mathbb{F}_{2^{2m}}$ if $\mathrm{Tr}_m^{2m}(\delta) \in \{0, a\}$. This completes the proof. □

Example 4. Take $m = 3$. Let ω be a root of the primitive polynomial $x^3 + x + 1$ and set $a = \omega^6$. By calculation, it can be verified that there are 8 different $\delta \in \mathbb{F}_{2^6}$ satisfying that $\mathrm{Tr}_3^6(\delta) = 0$, and 8 different $\delta \in \mathbb{F}_{2^6}$ satisfying that $\mathrm{Tr}_3^6(\delta) = \omega^6$, and these δ are exactly all the elements in $\mathbb{F}_{2^6}$ such that

$$f(x) = (x^8 + x + \delta)^{23} + \omega^6 x$$

is a permutation of $\mathbb{F}_{2^8}$. Furthermore, one can check that $f(x)$ cannot permute $\mathbb{F}_{2^6}$ if $\mathrm{Tr}_3^6(\delta) \neq 0$ and $\mathrm{Tr}_3^6(\delta) \neq \omega^6$. The experimental results are covered by Corollary 3.6.

Remark 6. If $a = 1$, then the PP given in Corollary 3.6 is exactly proposed in [3].

Corollary 3.7. *Let m be a positive integer. For any $\delta \in \mathbb{F}_{2^{2m}}$, the polynomial*

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

permutes $\mathbb{F}_{2^{2m}}$ if $\mathrm{Tr}_m^{2m}(\delta) \in \{0, 1\}$.

Proof. Since

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

by Theorem 3.4, $f(x)$ is a PP over $\mathbb{F}_{2^{2m}}$ if $\mathrm{Tr}_m^{2m}(\delta) = 0$. Next, assume $\mathrm{Tr}_m^{2m}(\delta) \neq 0$, we only need to show that for $d \in \mathbb{F}_{2^m}$, the equation

$$(x+\delta)^{2^{m-1}}(x+\bar{\delta})^{2-2^{m-1}} + (x+\delta)^{2-2^{n-1}}(x+\bar{\delta})^{2^{m-1}} + ax + d = 0 \tag{25}$$

has at most one solution in $\mathbb{F}_{2^m}$. Squaring Eq. (25) gives

$$(x+\bar{\delta})(x+\bar{\delta})^{4-2^m} + (x+\delta)(x+\delta)^{4-2^m} + x^2 + d^2 = 0.$$

Since $x \in \mathbb{F}_{2^m}$ and $\delta \notin \mathbb{F}_{2^m}$, then we have $x + \delta \neq 0$ and $x + \bar{\delta} \neq 0$. Multiplying both sides of the above equation by $(x+\delta)(x+\bar{\delta})$ and setting $\theta_4 = \mathrm{Tr}_m^{2m}(\delta) = \delta + \bar{\delta}$ leads to

$$(\theta_4^2+1)x^4 + \theta_4 x^3 + (\theta_4^4 + \delta\bar{\delta} + d^2)x^2 + d^2\theta_4 x + \left(\theta_4^6 + \theta_4^2(\delta\bar{\delta})^2 + d^2\delta\bar{\delta}\right) = 0. \tag{26}$$

If $\mathrm{Tr}_m^{2m}(\delta) = 1$, then Eq. (26) becomes

$$x^3 + (1 + \delta\bar{\delta} + d^2)x^2 + d^2 x + (1 + (\delta\bar{\delta})^2 + d^2\delta\bar{\delta}) = 0. \tag{27}$$

Replacing x by $x + 1 + d^2 + \delta\bar{\delta}$ in Eq. (27) yields

$$x^3 + \left(1 + d^4 + d^2 + (\delta\bar{\delta})^2\right)x + \left(1 + d^4 + d^2 + (\delta\bar{\delta})^2\right) = 0. \tag{28}$$

If $1+d^4+d^2+(\delta\bar{\delta})^2=0$, then $x=0$ is the unique solution of Eq. (28). If $1+d^4+d^2+(\delta\bar{\delta})^2\neq 0$, then we can verify that

$$\mathrm{Tr}_1^m\left(1+(1+d^4+d^2+(\delta\bar{\delta})^2)\right)=\mathrm{Tr}_1^m(\delta\bar{\delta})=\mathrm{Tr}_1^m\left(\frac{\delta\bar{\delta}}{\delta+\bar{\delta}}\right)=\mathrm{Tr}_1^m\left(\frac{\delta(\delta+\bar{\delta}+\delta)}{(\delta+\bar{\delta})^2}\right)=\frac{\delta+\bar{\delta}}{\delta+\bar{\delta}}=1.$$

By Lemma 2.5, Eq. (28) has exactly one solution in $\mathbb{F}_{2^m}$.

Therefore, we know that $f(x)$ permutes $\mathbb{F}_{2^{2m}}$ if $\mathrm{Tr}_m^{2m}(\delta)\in\{0,1\}$. This completes the proof. □

Example 5. Take $m=6$. Magma experiments show that there are 64 different $\delta\in\mathbb{F}_{2^{12}}$ satisfying that $\mathrm{Tr}_6^{12}(\delta)=0$, and 64 different $\delta\in\mathbb{F}_{2^{12}}$ satisfying that $\mathrm{Tr}_6^{12}(\delta)=1$, and these δ are exactly all the elements in $\mathbb{F}_{2^{12}}$ such that

$$f(x)=(x^{64}+x+\delta)^{2018}+x$$

is a permutation of $\mathbb{F}_{2^{12}}$. Furthermore, it can also be checked that $f(x)$ cannot permute $\mathbb{F}_{2^{12}}$ if $\mathrm{Tr}_6^{12}(\delta)\neq 0$ and $\mathrm{Tr}_6^{12}(\delta)\neq 1$. In this example, the set of all $\delta\in\mathbb{F}_{2^{12}}$ such that $f(x)$ permutes $\mathbb{F}_{2^{12}}$ is given by Corollary 3.7.

Remark 7. In [17, Theorem 3.2], for $(\alpha,t,n)=(-1,1,2)$ and $L_{g_{t,\alpha}}(x)=x^q-x$, the authors prove that $f(L_{g_{t,\alpha}}(x))+k(L_{g_{t,\alpha}}(x))\cdot L_h(x)$ permutes $\mathbb{F}_{q^2}$. Here, for $L_{g_{t,\alpha}}(x)=x^{2^m}+x$, $f(x)=(x+\delta)^s$, $k(x)=1$ and $L_h(x)=ax$, we can get $f(x)$ permutes $\mathbb{F}_{2^{2m}}$ for some given j in this section. However, proving that $Q_{t,\alpha}(x)$ is a PP over $\mathbb{F}_q$ becomes challenging for all integers $0<j<2m$.

4 PPs with the form $(x^{2^m}+x+\delta)^{s_1}+(x^{2^m}+x+\delta)^{s_2}+ax$ over $\mathbb{F}_{2^{2m}}$

In this section, we investigate some classes of PPs with the form $(x^{2^m}+x+\delta)^{s_1}+(x^{2^m}+x+\delta)^{s_2}+ax$ over $\mathbb{F}_{2^{2m}}$, where the exponent $s_1\equiv s_2 \pmod{2^m+1}$, or $s_1\equiv 2^j \pmod{2^m+1}$ and $s_2\equiv 2^k \pmod{2^m+1}$ for some integers j and k, $a\in\mathbb{F}_{2^m}^*$ and $\delta\in\mathbb{F}_{2^{2m}}$. It is easy to see that $f(x)=(x^{2^m}+x+\delta)^{s_1}+(x^{2^m}+x+\delta)^{s_2}+ax$ is a PP of $\mathbb{F}_{2^{2m}}$ if $\mathrm{Tr}_m^{2m}(\delta)=0$ from Remark 1. Therefore, we only consider the permutation behavior of $(x^{2^m}+x+\delta)^{s_1}+(x^{2^m}+x+\delta)^{s_2}+ax$ if $\mathrm{Tr}_m^{2m}(\delta)\neq 0$ in the sequel.

4.1 $s_1\equiv s_2 \pmod{2^m+1}$

In this subsection, we will construct several classes of PPs with the form $(x^{2^m}+x+\delta)^{s_1}+(x^{2^m}+x+\delta)^{s_2}+ax$ over $\mathbb{F}_{2^{2m}}$, where the exponent $s_1\equiv s_2 \pmod{2^m+1}$, $a\in\mathbb{F}_{2^m}^*$ and $\delta\in\mathbb{F}_{2^{2m}}$.

Theorem 4.1. *Let m and k be two positive integers, and let i and j be integers satisfying $0\le i\le m-1$ and $0\le j\le 2m-1$. For any $\delta\in\mathbb{F}_{2^{2m}}$ and $a\in\mathbb{F}_{2^m}^*$, consider the polynomial*

$$f(x)=(x^{2^m}+x+\delta)^{2^i(2^m+1)+2^j}+(x^{2^m}+x+\delta)^{2^k(2^m+1)+2^j}+ax.$$

Then $f(x)$ permutes $\mathbb{F}_{2^{2m}}$ if and only if either $\mathrm{Tr}_m^{2m}(\delta)=0$, or $\mathrm{Tr}_m^{2m}(\delta)\neq 0$ and the equation

$$x^{2^{i+1}-1}+\mathrm{Tr}_m^{2m}(\delta)^{2^i}x^{2^i-1}+x^{2^{k+1}-1}+\mathrm{Tr}_m^{2m}(\delta)^{2^k}x^{2^k-1}+\frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j}}=0$$

has no nonzero solution in $\mathbb{F}_{2^m}$.

Proof. Based on Remark 1, $f(x)$ permutes $\mathbb{F}_{2^{2m}}$ if $\mathrm{Tr}_m^{2m}(\delta)=0$. Next, we only consider the case $\mathrm{Tr}_m^{2m}(\delta)\neq 0$. According to Lemma 2.2, to prove that $f(x)$ permutes $\mathbb{F}_{2^{2m}}$, it is sufficient to show that for any $d\in\mathbb{F}_{2^m}$, the equation

$$(x+\delta)^{2^i(1+2^m)+2^{m+j}}+(x+\delta)^{2^i(2^m+1)+2^j}+(x+\delta)^{2^k(1+2^m)+2^{m+j}}+(x+\delta)^{2^k(2^m+1)+2^j}+ax=d$$

has at most one solution in $\mathbb{F}_{2^m}$. The above equation is equivalent to

$$\mathrm{Tr}_m^{2m}(\delta)^{2^j}\left((x^2+\mathrm{Tr}_m^{2m}(\delta)x+\delta\bar{\delta})^{2^i}+(x^2+\mathrm{Tr}_m^{2m}(\delta)x+\delta\bar{\delta})^{2^k}\right)+ax+d=0. \tag{29}$$

For any $x\in\mathbb{F}_{2^m}$, dividing Eq. (29) by $\mathrm{Tr}_m^{2m}(\delta)^{2^j}$, we obtain that Eq. (29) has at most one solution if and only if the linearized part of the equation

$$x^{2^{i+1}}+\mathrm{Tr}_m^{2m}(\delta)^{2^i}x^{2^i}+x^{2^{k+1}}+\mathrm{Tr}_m^{2m}(\delta)^{2^k}x^{2^k}+\frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j}}x=0$$

has only the zero solution in $\mathbb{F}_{2^m}$, or equivalently, the equation

$$x^{2^{i+1}-1}+\mathrm{Tr}_m^{2m}(\delta)^{2^i}x^{2^i-1}+x^{2^{k+1}-1}+\mathrm{Tr}_m^{2m}(\delta)^{2^k}x^{2^k-1}+\frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j}}=0 \tag{30}$$

has no nonzero solution, obtained by replacing x with $\mathrm{Tr}_m^{2m}(\delta)x$. This completes the proof. □

Let $(i,k)\in\{(1,0),(0,m-1),(m-1,m-2)\}$, respectively, we obtain the following PPs over $\mathbb{F}_{2^{2m}}$ by Theorem 4.1.

Corollary 4.1. *Let m be a positive integer, and let j be an integer satisfying $0\leq j\leq 2m-1$. For any $\delta\in\mathbb{F}_{2^{2m}}$ and $a\in\mathbb{F}_{2^m}^*$, the polynomial*

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

permutes $\mathbb{F}_{2^{2m}}$ if and only if one of the following conditions is satisfied:

(1) $\mathrm{Tr}_m^{2m}(\delta)=0$;

(2) $\mathrm{Tr}_m^{2m}(\delta)=1$ *and* $1+a$ *is not a cube element in* $\mathbb{F}_{2^m}^*$;

(3) $\mathrm{Tr}_m^{2m}(\delta)\notin\mathbb{F}_2$, $\mathrm{Tr}_1^m({c_2}^{-1})=\mathrm{Tr}_1^m(1)$ *and* $P_m(c_2)\neq 0$, *where* $c_2=\frac{\mathrm{Tr}_m^{2m}(\delta)+\frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j}}}{(1+\mathrm{Tr}_m^{2m}(\delta))^3}$ *and* $P_m(x)$ *is defined in Lemma 2.4.*

Proof. Observing that $s_1=2^0(2^m+1)+2^j$ and $s_2=2^1(2^m+1)+2^j$. By Theorem 4.1, we obtain that $f(x)$ permutes $\mathbb{F}_{2^{2m}}$ if $\mathrm{Tr}_m^{2m}(\delta)=0$. Thus we only consider the case $\mathrm{Tr}_m^{2m}(\delta)\neq 0$ and determine a necessary and sufficient condition for the equation

$$x^3+(\mathrm{Tr}_m^{2m}(\delta)^2+1)x+\left(\mathrm{Tr}_m^{2m}(\delta)+\frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j}}\right)=0 \tag{31}$$

has no nonzero solution in $\mathbb{F}_{2^m}$. We distinguish the following two cases.

Case I: $\mathrm{Tr}_m^{2m}(\delta)=1$. Thus, Eq. (31) is reduced to $x^3+(1+a)=0$. Consequently, $f(x)$ is PP over $\mathbb{F}_{2^{2m}}$ if and only if $1+a$ is not a cube element in $\mathbb{F}_{2^m}^*$.

Case II: $\mathrm{Tr}_m^{2m}(\delta)\notin\mathbb{F}_2$. For any $x\in\mathbb{F}_{2^m}^*$, replacing x by $\left(1+\mathrm{Tr}_m^{2m}(\delta)\right)x$, then Eq. (31) can be simplified as

$$(1+\mathrm{Tr}_m^{2m}(\delta))^3x^3+(1+\mathrm{Tr}_m^{2m}(\delta))^3x+(\mathrm{Tr}_m^{2m}(\delta)+\frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j}})=0,$$

which can be reduced to

$$x^3+x+\frac{\mathrm{Tr}_m^{2m}(\delta)+\frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j}}}{(1+\mathrm{Tr}_m^{2m}(\delta))^3}=0. \tag{32}$$

Set $c_2=\frac{\mathrm{Tr}_m^{2m}(\delta)+\frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j}}}{\left(1+\mathrm{Tr}_m^{2m}(\delta)\right)^3}$. By Lemma 2.4, we obtain that Eq. (32) has no solution in $\mathbb{F}_{2^m}$ if and only if $\mathrm{Tr}_1^m(c_2^{-1})=\mathrm{Tr}_1^m(1)$ and $P_m(c_2)\neq 0$. This completes the proof. □

Remark 8. If $a=1$ and $j\in\{0,m\}$, then the PP given in Corollary 4.1 is exactly Proposition 5 in [10].

Corollary 4.2. *Let m be a positive integer, and let j be an integer satisfying $0\leq j\leq 2m-1$. For any $\delta\in\mathbb{F}_{2^{2m}}$ and $a\in\mathbb{F}_{2^m}^*$, the polynomial*

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

permutes $\mathbb{F}_{2^{2m}}$ if and only if one of the following conditions is satisfied:

(1) $\mathrm{Tr}_m^{2m}(\delta)=0$;

(2) $\mathrm{Tr}_m^{2m}(\delta)\neq 0$ *and* $1+\frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j}}+\mathrm{Tr}_m^{2m}(\delta)=0$, $\mathrm{Tr}_m^{2m}(\delta)$ *is not a cube element in* $\mathbb{F}_{2^m}^*$;

(3) $\mathrm{Tr}_m^{2m}(\delta)\neq 0$ *and* $1+\frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j}}+\mathrm{Tr}_m^{2m}(\delta)\neq 0$, $\mathrm{Tr}_1^m({c_3}^{-1})=\mathrm{Tr}_1^m(1)$ *and* $P_m(c_3)\neq 0$, *where* $c_3=\frac{\mathrm{Tr}_m^{2m}(\delta)}{\left(1+\frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j}}+\mathrm{Tr}_m^{2m}(\delta)\right)^3}$ *and $P_m(x)$ is defined in Lemma 2.4.*

Proof. Since

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

based on Theorem 4.1, $f(x)$ is a PP over $\mathbb{F}_{2^{2m}}$ if and only if either $\mathrm{Tr}_m^{2m}(\delta)=0$, or $\mathrm{Tr}_m^{2m}(\delta)\neq 0$ and the equation

$$1+\mathrm{Tr}_m^{2m}(\delta)^{2^{m-1}}x^{2^{m-1}-1}+x+\mathrm{Tr}_m^{2m}(\delta)+\frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j}}=0 \tag{33}$$

has no nonzero solution in $\mathbb{F}_{2^m}$. For any $x\in\mathbb{F}_{2^m}^*$, squaring Eq. (33) and multiplying by x yields

$$x^3+(1+\mathrm{Tr}_m^{2m}(\delta)+\frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j}})^2x+\mathrm{Tr}_m^{2m}(\delta)=0. \tag{34}$$

Next, we consider the following two cases.

Case I: $1+\frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j}}+\mathrm{Tr}_m^{2m}(\delta)=0$. Eq. (34) turns to $x^3+\mathrm{Tr}_m^{2m}(\delta)=0$. Consequently, $f(x)$ permutes $\mathbb{F}_{2^{2m}}$ if and only if $\mathrm{Tr}_m^{2m}(\delta)$ is not a cube element in $\mathbb{F}_{2^m}^*$.

Case II: $1+\frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j}}+\mathrm{Tr}_m^{2m}(\delta)\neq 0$. Replacing x by $\left(1+\frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j}}+\mathrm{Tr}_m^{2m}(\delta)\right)x$ and then dividing by $\left(1+\frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j}}+\mathrm{Tr}_m^{2m}(\delta)\right)^3$, Eq. (34) is reduced to

$$x^3+x+\frac{\mathrm{Tr}_m^{2m}(\delta)}{\left(1+\frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j}}+\mathrm{Tr}_m^{2m}(\delta)\right)^3}=0. \tag{35}$$

Set $c_3=\frac{\mathrm{Tr}_m^{2m}(\delta)}{\left(1+\frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j}}+\mathrm{Tr}_m^{2m}(\delta)\right)^3}$. By Lemma 2.4, Eq. (35) has no solution in $\mathbb{F}_{2^m}$ if and only if $\mathrm{Tr}_1^m(c_3^{-1})=\mathrm{Tr}_1^m(1)$ and $P_m(c_3)\neq 0$. This completes the proof. □

The proof of the following corollary is similar to Corollary 4.2 and is hence omitted.

Corollary 4.3. *Let m be a positive integer, and let j be integer satisfying $0 \le j \le 2m-1$. For any $\delta \in \mathbb{F}_{2^{2m}}$ and $a \in \mathbb{F}_{2^m}^*$, the polynomial*

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

permutes $\mathbb{F}_{2^{2m}}$ if and only if one of the following conditions is satisfied:

(1) $\mathrm{Tr}_m^{2m}(\delta) = 0$;

(2) $\mathrm{Tr}_m^{2m}(\delta) = 1$ *and* $(1+a)^4$ *is not a cube element in* $\mathbb{F}_{2^m}^*$;

(3) $\mathrm{Tr}_m^{2m}(\delta) \notin \mathbb{F}_2$, $\mathrm{Tr}_1^m({c_4}^{-1}) = \mathrm{Tr}_1^m(1)$ *and* $P_m(c_4) \neq 0$, *where* $c_4 = \frac{\mathrm{Tr}_m^{2m}(\delta)(1+\frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j}})^2}{\left(1+\mathrm{Tr}_m^{2m}(\delta)\right)^3}$ *and* $P_m(x)$ *is defined in Lemma 2.4.*

Example 6. Take $m=4$ and $j=1$. Let ω be a root of the primitive polynomial $x^4+x^3+x^2+x+1$ and set $a=\omega^2$, it is clear that $1+a$ is not a cube element. By calculation, it can be verified that there are 16 different $\delta \in \mathbb{F}_{2^8}$ satisfying that $\mathrm{Tr}_4^8(\delta)=0$, and 16 different $\delta \in \mathbb{F}_{2^8}$ satisfying that $\mathrm{Tr}_4^8(\delta)=1$, and 96 different $\delta \in \mathbb{F}_{2^8}$ satisfying that $\mathrm{Tr}_1^m({c_4}^{-1}) = \mathrm{Tr}_1^m(1)$, $P_m(c_4) \neq 0$. These δ are exactly all the elements in $\mathbb{F}_{2^8}$ such that

$$f(x) = (x^{16}+x+\delta)^{138} + (x^{16}+x+\delta)^{70} + \omega^2 x$$

is a permutation of $\mathbb{F}_{2^8}$. The experimental results are consistent with our result in Corollary 4.3.

4.2 $s_1 \equiv 2^j \pmod{2^m+1}$, $s_2 \equiv 2^k \pmod{2^m+1}$

In this subsection, we will study several classes of PPs with the form $(x^{2^m}+x+\delta)^{s_1} + (x^{2^m}+x+\delta)^{s_2} + ax$ over $\mathbb{F}_{2^{2m}}$, where the exponent $s_1 \equiv 2^j \pmod{2^m+1}$ and $s_2 \equiv 2^k \pmod{2^m+1}$ for some integers j and k, $a \in \mathbb{F}_{2^m}^*$ and $\delta \in \mathbb{F}_{2^{2m}}$.

Theorem 4.2. *Let m be a positive integer, and let i,j,k be integers satisfying $0 \le i \le m-1$ and $0 \le j,k \le 2m-1$. For any $\delta \in \mathbb{F}_{2^{2m}}$ and $a \in \mathbb{F}_{2^m}^*$, consider the polynomial*

$$f(x) = (x^{2^m}+x+\delta)^{2^i(2^m+1)+2^j} + (x^{2^m}+x+\delta)^{2^i(2^m+1)+2^k} + ax.$$

Then $f(x)$ permutes $\mathbb{F}_{2^{2m}}$ if and only if either $\mathrm{Tr}_m^{2m}(\delta)^{2^j} + \mathrm{Tr}_m^{2m}(\delta)^{2^k} = 0$, or $\mathrm{Tr}_m^{2m}(\delta)^{2^j} + \mathrm{Tr}_m^{2m}(\delta)^{2^k} \neq 0$ and the equation

$$x^{2^{i+1}-1} + x^{2^i-1} + \frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j+2^{i+1}-1} + \mathrm{Tr}_m^{2m}(\delta)^{2^k+2^{i+1}-1}} = 0$$

has no nonzero solution in $\mathbb{F}_{2^m}$.

Proof. By Lemma 2.2, to prove that $f(x)$ permutes $\mathbb{F}_{2^{2m}}$, it suffices to show that for any $d \in \mathbb{F}_{2^m}$, the equation

$$(x+\delta)^{2^i(1+2^m)+2^{m+j}} + (x+\delta)^{2^i(2^m+1)+2^j} + (x+\delta)^{2^i(1+2^m)+2^{m+k}} + (x+\delta)^{2^i(2^m+1)+2^k} + ax = d \tag{36}$$

has at most one solution in $\mathbb{F}_{2^m}$, or equivalently, the equation

$$(\mathrm{Tr}_m^{2m}(\delta)^{2^j} + \mathrm{Tr}_m^{2m}(\delta)^{2^k})(x^2 + \mathrm{Tr}_m^{2m}(\delta)x + \delta\bar{\delta})^{2^i} + ax + d = 0 \tag{37}$$

has at most one solution in $\mathbb{F}_{2^m}$. It is clear that $f(x)$ permutes $\mathbb{F}_{2^{2m}}$ if $\mathrm{Tr}_m^{2m}(\delta)^{2^j}+\mathrm{Tr}_m^{2m}(\delta)^{2^k}=0$, thus we only consider the case $\mathrm{Tr}_m^{2m}(\delta)^{2^j}+\mathrm{Tr}_m^{2m}(\delta)^{2^k}\neq 0$.

Dividing Eq. (37) by $\mathrm{Tr}_m^{2m}(\delta)^{2^j}+\mathrm{Tr}_m^{2m}(\delta)^{2^k}$, we obtain that Eq. (37) has at most one solution if and only if the linearized equation

$$x^{2^{i+1}}+\mathrm{Tr}_m^{2m}(\delta)^{2^i}x^{2^i}+\frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j}+\mathrm{Tr}_m^{2m}(\delta)^{2^k}}x=0 \tag{38}$$

has only the zero solution.

If $\mathrm{Tr}_m^{2m}(\delta)^{2^j}+\mathrm{Tr}_m^{2m}(\delta)^{2^k}\neq 0$, then we have $\mathrm{Tr}_m^{2m}(\delta)\neq 0$. For any $x\in\mathbb{F}_{2^m}^*$, replacing x by $\mathrm{Tr}_m^{2m}(\delta)x$ and dividing by $\mathrm{Tr}_m^{2m}(\delta)^{2^{i+1}}x$ gives

$$x^{2^{i+1}-1}+x^{2^i-1}+\frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j+2^{i+1}-1}+\mathrm{Tr}_m^{2m}(\delta)^{2^k+2^{i+1}-1}}=0. \tag{39}$$

Therefore, to prove that $f(x)$ permutes $\mathbb{F}_{2^{2m}}$, it is sufficient to show that Eq. (39) has no nonzero solution in $\mathbb{F}_{2^m}$. This completes the proof. □

In Theorem 4.2, let $i=0$, 1, $m-2$ and $m-1$, we have the following four corollaries.

Corollary 4.4. *Let m be a positive integer, and let j and k be integers satisfying $0\le j,k\le 2m-1$. For any $\delta\in\mathbb{F}_{2^{2m}}$ and $a\in\mathbb{F}_{2^m}^*$, the polynomial*

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

permutes $\mathbb{F}_{2^{2m}}$ if and only if $\mathrm{Tr}_m^{2m}(\delta)^{2^j+1}+\mathrm{Tr}_m^{2m}(\delta)^{2^k+1}\in\{0,a\}$.

Proof. It follows from Theorem 4.2 that $f(x)$ permutes $\mathbb{F}_{2^{2m}}$ if and only if $\mathrm{Tr}_m^{2m}(\delta)^{2^j}+\mathrm{Tr}_m^{2m}(\delta)^{2^k}=0$, or $\mathrm{Tr}_m^{2m}(\delta)^{2^j}+\mathrm{Tr}_m^{2m}(\delta)^{2^k}\neq 0$ and the equation

$$x+1+\frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j+1}+\mathrm{Tr}_m^{2m}(\delta)^{2^k+1}}=0 \tag{40}$$

has no nonzero solution.

If $\mathrm{Tr}_m^{2m}(\delta)^{2^j+1}+\mathrm{Tr}_m^{2m}(\delta)^{2^k+1}=a$, then $x=0$ is the unique solution of Eq. (40). Thus, $f(x)$ permutes $\mathbb{F}_{2^{2m}}$. If $\mathrm{Tr}_m^{2m}(\delta)^{2^j+1}+\mathrm{Tr}_m^{2m}(\delta)^{2^k+1}\neq a$, then we know that Eq. (40) has a nonzero solution $x=1+\frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j+1}+\mathrm{Tr}_m^{2m}(\delta)^{2^k+1}}$, which means that $f(x)$ is not a PP over $\mathbb{F}_{2^{2m}}$.

In summary, we conclude that $f(x)$ is a PP over $\mathbb{F}_{2^{2m}}$ if and only if $\mathrm{Tr}_m^{2m}(\delta)^{2^j+1}+\mathrm{Tr}_m^{2m}(\delta)^{2^k+1}\in\{0,a\}$. This completes the proof. □

The proof of the following corollaries is similar to Corollary 4.4 and is hence omitted.

Corollary 4.5. *Let m be a positive integer, and let j and k be integers satisfying $0\le j,k\le 2m-1$. For any $\delta\in\mathbb{F}_{2^{2m}}$ and $a\in\mathbb{F}_{2^m}^*$, the polynomial*

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

permutes $\mathbb{F}_{2^{2m}}$ if and only if $\mathrm{Tr}_m^{2m}(\delta)^{2^j}+\mathrm{Tr}_m^{2m}(\delta)^{2^k}=0$, or $\mathrm{Tr}_1^m({c_5}^{-1})=\mathrm{Tr}_1^m(1)$ and $P_m(c_5)\neq 0$, where $c_5=\frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j+3}+\mathrm{Tr}_m^{2m}(\delta)^{2^k+3}}$.

Remark 9. If $a=1$, $j\in\{0,m\}$ and $k\in\{m-1,2m-1\}$, then the PP given in Corollary 4.5 is exactly Proposition 7 in [10].

Corollary 4.6. *Let m be a positive integer, and let j and k be integers satisfying $0\le j,k\le 2m-1$. For any $\delta\in\mathbb{F}_{2^{2m}}$ and $a\in\mathbb{F}_{2^m}^*$, the polynomial*

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

permutes $\mathbb{F}_{2^{2m}}$ if and only if $\mathrm{Tr}_m^{2m}(\delta)^{2^j}+\mathrm{Tr}_m^{2m}(\delta)^{2^k}=0$ or $\mathrm{Tr}_1^m({c_6}^{-1})=\mathrm{Tr}_1^m(1)$ and $P_m(c_6)\neq 0$, where $c_6=\frac{a^2\mathrm{Tr}_m^{2m}(\delta)}{\mathrm{Tr}_m^{2m}(\delta)^{2^{j+1}}+\mathrm{Tr}_m^{2m}(\delta)^{2^{k+1}}}$ and $P_m(x)$ is defined in Lemma 2.4.

Remark 10. If $a=1$, $j\in\{0,m\}$ and $k\in\{m-2,2m-2\}$, then the PP given in Corollary 4.6 is exactly Proposition 6 in [10].

Corollary 4.7. *Let m be a positive integer, and let j and k be integers satisfying $0\le j,k\le 2m-1$. For any $\delta\in\mathbb{F}_{2^{2m}}$ and $a\in\mathbb{F}_{2^m}^*$, the polynomial*

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

permutes $\mathbb{F}_{2^{2m}}$ if and only if $\mathrm{Tr}_m^{2m}(\delta)^{2^j}+\mathrm{Tr}_m^{2m}(\delta)^{2^k}\in\{0,a\}$.

Theorem 4.3. *Let m be a positive integer, and let i,j,k be integers satisfying $0\le i\le m-1$ and $0\le j,k\le 2m-1$. For any $d\in\mathbb{F}_{2^m}$, $\delta\in\mathbb{F}_{2^{2m}}$ and $a\in\mathbb{F}_{2^m}^*$, consider the polynomial*

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

permutes $\mathbb{F}_{2^{2m}}$ if and only if either $\mathrm{Tr}_m^{2m}(\delta)^{2^j}+\mathrm{Tr}_m^{2m}(\delta)^{2^k}=0$, or $\mathrm{Tr}_m^{2m}(\delta)^{2^j}+\mathrm{Tr}_m^{2m}(\delta)^{2^k}\neq 0$ and the equation

$$(ax+d)(x^2+\mathrm{Tr}_m^{2m}(\delta)x+\delta\bar{\delta})^{2^i}+\mathrm{Tr}_m^{2m}(\delta)^{2^j}+\mathrm{Tr}_m^{2m}(\delta)^{2^k}=0$$

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

Proof. By Lemma 2.2, to prove that $f(x)$ permutes $\mathbb{F}_{2^{2m}}$, it suffices to show that for any $d\in\mathbb{F}_{2^m}$, the equation

$$\begin{aligned}&(x+\delta)^{2^{3m}-2^i(1+2^m)+2^{m+j}-2^m}+(x+\delta)^{2^{2m}-2^i(2^m+1)+2^j-1}\\+\;&(x+\delta)^{2^{3m}-2^i(1+2^m)+2^{m+k}-2^m}+(x+\delta)^{2^{2m}-2^i(2^m+1)+2^k-1}+ax=d\end{aligned}$$

has at most one solution in $\mathbb{F}_{2^m}$. A straightforward simplification gives

$$(\mathrm{Tr}_m^{2m}(\delta)^{2^j}+\mathrm{Tr}_m^{2m}(\delta)^{2^k})(x^2+\mathrm{Tr}_m^{2m}(\delta)x+\delta\bar{\delta})^{2^{2m}-2^i-1}+ax+d=0.$$

It is clear that $f(x)$ permutes $\mathbb{F}_{2^{2m}}$ if $\mathrm{Tr}_m^{2m}(\delta)^{2^j}+\mathrm{Tr}_m^{2m}(\delta)^{2^k}=0$. Next we consider the case $\mathrm{Tr}_m^{2m}(\delta)^{2^j}+\mathrm{Tr}_m^{2m}(\delta)^{2^k}\neq 0$. For any $x\in\mathbb{F}_{2^m}$, since $\mathrm{Tr}_m^{2m}(\delta)\neq 0$, we have $x+\delta\neq 0$ and $x+\bar{\delta}\neq 0$. Multiplying both sides of the above equation by $(x+\delta)^{2^i}(x+\bar{\delta})^{2^i}$, we derive

$$(ax+d)(x^2+\mathrm{Tr}_m^{2m}(\delta)x+\delta\bar{\delta})^{2^i}+\mathrm{Tr}_m^{2m}(\delta)^{2^j}+\mathrm{Tr}_m^{2m}(\delta)^{2^k}=0. \tag{41}$$

Consequently, $f(x)$ permutes $\mathbb{F}_{2^{2m}}$ if and only if Eq. (41) has at most one solution in $\mathbb{F}_{2^m}$ whenever $\mathrm{Tr}_m^{2m}(\delta)^{2^j}+\mathrm{Tr}_m^{2m}(\delta)^{2^k}\neq 0$. This completes the proof. □

Let $i = 0$ and 1, respectively, we derive the following two classes of PPs from Theorem 4.3 correspondingly. We only give the proof for Corollary 4.8, since Corollary 4.9 can be proved in the same way.

Corollary 4.8. *Let m be a positive integer, and let j and k be integers satisfying $0 \le j, k \le 2m-1$. For any $\delta \in \mathbb{F}_{2^{2m}}$ and $a \in \mathbb{F}_{2^m}^*$, the polynomial*

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

permutes $\mathbb{F}_{2^{2m}}$ if $\mathrm{Tr}_m^{2m}(\delta)^{2^j} + \mathrm{Tr}_m^{2m}(\delta)^{2^k} = 0$ or $\mathrm{Tr}_m^{2m}(\delta)^{2^j-3} + \mathrm{Tr}_m^{2m}(\delta)^{2^k-3} = a$.

Proof. Note that $s_1 = 2^{2m} - (2^m+1) + 2^j - 1$ and $s_2 = 2^{2m} - (2^m+1) + 2^j - 1$. By Theorem 4.3, we know that $f(x)$ permutes $\mathbb{F}_{2^{2m}}$ if either $\mathrm{Tr}_m^{2m}(\delta)^{2^j} + \mathrm{Tr}_m^{2m}(\delta)^{2^k} = 0$, or $\mathrm{Tr}_m^{2m}(\delta)^{2^j} + \mathrm{Tr}_m^{2m}(\delta)^{2^k} \neq 0$ and the equation

$$\mathrm{Tr}_m^{2m}(\delta)^{2^j} + \mathrm{Tr}_m^{2m}(\delta)^{2^k} + (ax+d)(x^2 + \mathrm{Tr}_m^{2m}(\delta)x + \delta\bar{\delta}) = 0.$$

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

Denote $\theta_1' = \delta + \bar{\delta} = \mathrm{Tr}_m^{2m}(\delta)$. Dividing the above equation by a and replacing d_1' by $\frac{d}{a}$, the equation can be rewritten as

$$x^3 + (\theta_1' + d_1')x^2 + (\delta\bar{\delta} + d_1'\theta_1')x + (d_1'\delta\bar{\delta} + \frac{\theta_1'^{2^j} + \theta_1'^{2^k}}{a}) = 0.$$

Replacing x by $x + \theta_1' + d_1'$ yields

$$x^3 + (\theta_1'^2 + d_1'^2 + \delta\bar{\delta} + \theta_1'd_1')x + (\frac{\theta_1'^{2^j} + \theta_1'^{2^k}}{a} + d_1'^2\theta_1' + \delta\bar{\delta}\theta_1' + \theta_1'^2d_1') = 0. \tag{42}$$

Therefore, $f(x)$ permutes $\mathbb{F}_{2^{2m}}$ if Eq. (42) has at most one solution in $\mathbb{F}_{2^{2m}}$ if $\mathrm{Tr}_m^{2m}(\delta)^{2^j} + \mathrm{Tr}_m^{2m}(\delta)^{2^k} \neq 0$.

Let $u_1' = \theta_1'^2 + d_1'^2 + \delta\bar{\delta} + \theta_1'd_1'$ and $v_1' = \frac{\theta_1'^{2^j} + \theta_1'^{2^k}}{a} + d_1'^2\theta_1' + \delta\bar{\delta}\theta_1' + \theta_1'^2d_1'$. It is clear that $v_1' = \theta_1'u_1'$ if $\mathrm{Tr}_m^{2m}(\delta)^{2^j-3} + \mathrm{Tr}_m^{2m}(\delta)^{2^k-3} = a$. If $v_1' = 0$, then $x = 0$ is the unique solution of Eq. (42). If $v_1' \neq 0$, we have $\mathrm{Tr}_1^m\left(1 + \frac{u_1'^3}{v_1'^2}\right) = \mathrm{Tr}_1^m\left(\frac{\delta\bar{\delta}}{\delta^2+\bar{\delta}^2}\right) = \mathrm{Tr}_1^m\left(\frac{\delta(\delta+\bar{\delta}+\delta)}{(\delta+\bar{\delta})^2}\right) = \frac{\delta+\bar{\delta}}{\delta+\bar{\delta}} = 1 \neq 0$. By Lemma 2.5, Eq. (42) has a unique solution. This completes the proof. □

Example 7. Take $m = 5$, $j = 2$ and $k = 1$. Let ω be a root of the primitive polynomial $x^5 + x^3 + x^2 + x + 1$ and set $a = \omega^{30}$. Magma experiments show that there are 64 different $\delta \in \mathbb{F}_{2^{10}}$ satisfying that $\mathrm{Tr}_5^{10}(\delta)^4 + \mathrm{Tr}_4^8(\delta)^2 = 0$, and 32 different $\delta \in \mathbb{F}_{2^8}$ satisfying that $\mathrm{Tr}_5^{10}(\delta) + \mathrm{Tr}_5^{10}(\delta)^{-1} = \omega^{30}$, and these δ are exactly all the elements in $\mathbb{F}_{2^{10}}$ such that

$$f(x) = (x^{32} + x + \delta)^{994} + (x^{32} + x + \delta)^{992} + \omega^{30}x$$

is a permutation of $\mathbb{F}_{2^{10}}$. Furthermore, it can also be verified that $f(x)$ cannot permute $\mathbb{F}_{2^8}$ if $\mathrm{Tr}_5^{10}(\delta)^4 + \mathrm{Tr}_5^{10}(\delta)^2 \neq 0$ and $\mathrm{Tr}_5^{10}(\delta) + \mathrm{Tr}_5^{10}(\delta)^{-1} \neq \omega^{30}$. The experimental results are consistent with our result in Corollary 4.8.

Corollary 4.9. *Let m be a positive integer, and let j and k be integers satisfying $0 \le j, k \le 2m-1$. For any $\delta \in \mathbb{F}_{2^{2m}}$ and $a \in \mathbb{F}_{2^m}^*$, the polynomial*

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

permutes $\mathbb{F}_{2^{2m}}$ if $\mathrm{Tr}_m^{2m}(\delta)^{2^j} + \mathrm{Tr}_m^{2m}(\delta)^{2^k} = 0$ or $\mathrm{Tr}_m^{2m}(\delta)^{2^j-5} + \mathrm{Tr}_m^{2m}(\delta)^{2^k-5} = a$.

Example 8. Take $m = 4$, $j = 2$ and $k = 1$. Let ω be a root of the primitive polynomial $x^4 + x^3 + 1$ and set $a = \omega^{10}$. Magma experiments show that there are 32 different $\delta \in \mathbb{F}_{2^8}$ satisfying that $\mathrm{Tr}_4^8(\delta)^4 + \mathrm{Tr}_4^8(\delta)^2 = 0$, and 48 different $\delta \in \mathbb{F}_{2^8}$ satisfying that $\mathrm{Tr}_4^8(\delta)^{-1} + \mathrm{Tr}_4^8(\delta)^{-3} = \omega^{10}$, and these δ are exactly all the elements in $\mathbb{F}_{2^8}$ such that

$$f(x) = (x^{16} + x + \delta)^{225} + (x^{16} + x + \delta)^{221} + \omega^{10}x$$

is a permutation of $\mathbb{F}_{2^8}$. Furthermore, one can verify that $f(x)$ cannot permute $\mathbb{F}_{2^8}$ if $\mathrm{Tr}_4^8(\delta)^4 + \mathrm{Tr}_4^8(\delta)^2 \neq 0$ and $\mathrm{Tr}_4^8(\delta)^{-1} + \mathrm{Tr}_4^8(\delta)^{-3} \neq \omega^{10}$. The experimental results confirm Corollary 4.9.

Remark 11. In [17, Theorem 3.2], for $(\alpha, t, n) = (-1, 1, 2)$ and $L_{g_{t,\alpha}}(x) = x^q - x$, the authors prove that $f(L_{g_{t,\alpha}}(x)) + k(L_{g_{t,\alpha}}(x)) \cdot L_h(x)$ permutes $\mathbb{F}_{q^2}$. Here, for $L_{g_{t,\alpha}}(x) = x^{2^m} + x$, $f(x) = (x+\delta)^{s_1} + (x+\delta)^{s_2}$, $k(x) = 1$ and $L_h(x) = ax$, we can get $f(x)$ permutes $\mathbb{F}_{2^{2m}}$ for some given i, j, k in this section. However, verifying that $Q_{t,\alpha}(x)$ is a PP over $\mathbb{F}_q$ becomes challenging for all integers $0 < j, k < 2m$.

5 QM equivalence

In this section, we verify that the PPs constructed in this paper are QM inequivalent to the known PPs.

Definition 5.1. ([25]) Two permutation polynomials $f(x)$ and $g(x)$ in $\mathbb{F}_{2^n}[x]$ are called quasi-multiplicative equivalent if there exists an integer $1 \le l \le 2^n - 1$ with $\gcd(l, 2^n - 1) = 1$ and $f(x) = e_1 g(e_2 x^l)$, where $e_1, e_2 \in \mathbb{F}_{2^n}^*$.

Clearly, two QM equivalent PPs have the same number of terms. It shows that $f(x) = \sum_{i=0}^{t} a_i x^{r_i}$ and $g(x) = \sum_{i=0}^{t} b_i x^{s_i}$ over $\mathbb{F}_{2^n}$ are QM equivalent if and only if the following two conditions hold:

(1) For two positive integers n and t, there exists an integer $1 \le l \le 2^n - 1$ with $\gcd(l, 2^n - 1) = 1$ such that

$$\{ls_0, ls_1, \cdots, ls_t\} \pmod{2^n-1} = \{r_0, r_1, \cdots, r_t\} \pmod{2^n-1}.$$

(2) There exists $e_1, e_2 \in \mathbb{F}_{2^n}^*$ such that the coefficients of $e_1 g(e_2 x^l)$ and $f(x)$ are equal.

Proposition 5.1. *Let m be a positive integer. For a fixed $\delta \in \mathbb{F}_{2^{2m}}$ and $a \in \mathbb{F}_{2^m}^*$, $f(x) = (x^{2^m} + x + \delta)^{2^{2m-1}+2^{m-1}+2^j} + ax$ is not QM equivalent to $g_1(x) = (x^{2^m} + x + \delta)^{2^i+2^m+1} + ax$ (No.29 in Table 1).*

Proof. Expanding $f(x)$ into the form $\sum_{i=0}^{t} a_i x^{r_i}$ and $g_1(x)$ as $\sum_{i=0}^{t} b_i x^{s_i}$ yields the following exponent sets

$$\begin{aligned}
r_i \in \{&1, 2^{m-1}, 2^j, 2^m, 2^{m-1}+2^j, 2^{2m-1}, 1+2^j, 2^m+2^j, 2^{m-1}+2^{2m-1},\\
&2^{2m-1}+2^j, 1+2^{m+j}, 2^m+2^{m+j}, 2^{m+j}, 2^{m-1}+2^{m+j}, 2^{2m-1}+2^{m+j}\},\\
s_i \in \{&1, 2, 2^j, 2^m, 1+2^j, 2+2^j, 2^{m+1}, 2^{m+j}, 1+2^{m+j},\\
&2^m+2^j, 2^m+2^{m+j}, 2^{m+1}+2^j, 2+2^{m+j}, 2^{m+1}+2^{m+j}\}.
\end{aligned}$$

A comparison shows that $f(x)$ and $g_1(x)$ do not have the same number of terms. Therefore, we conclude that $f(x)$ is not QM equivalent to $g_1(x)$. □

Remark 12. Through a lengthy verification, using similar arguments as Proposition 5.1, we can verify that the PPs in Section 3 are not QM equivalent to the known PPs listed in Table 1.

Proposition 5.2. *Let m be a positive integer. For a fixed $\delta \in \mathbb{F}_{2^{2m}}$ and $a \in \mathbb{F}_{2^m}^*$, $f(x) = (x^{2^m}+x+\delta)^{2^{m+1}+2+2^j} + (x^{2^m}+x+\delta)^{2^{m+1}+2+2^k} + ax$ is not QM equivalent to $g_2(x) = (x^{2^m}+x+\delta)^{3\cdot 2^m+2} + (x^{2^m}+x+\delta)^{2^{2m-1}+2^{m+1}+2} + x$ (No.12 in Table 2).*

Proof. The expansion of $f(x)$ into the form $\sum_{i=0}^{t} a_i x^{r_i}$ yields the set of exponents

$$\begin{aligned}
r_i \in \{&1, 2, 4, 2^{m+1}, 2^{m+2}, 2^j, 2^k, 2^{m+j}, 2^{m+k}, 2^{m+2}+2^{m+j}, 2^{m+2}+2^{m+k},\\
&2^{m+2}+2^j, 2^{m+2}+2^k, 4+2^{m+j}, 4+2^{m+k}, 4+2^j, 4+2^k, 2^{m+1}+2^{m+j},\\
&2^{m+1}+2^{m+k}, 2^{m+1}+2^j, 2^{m+1}+2^k, 2+2^{m+j}, 2+2^{m+k}, 2+2^j, 2+2^k\}.
\end{aligned}$$

Substituting $j = 0$ and $k = m-1$ into r_i, it can be verified that $2^j = 1$, thus $f(x)$ and $g_2(x)$ do not have the same number of terms. Therefore, $f(x)$ is not QM equivalent to $g_2(x)$. □

Remark 13. Through a lengthy verification, using similar arguments as Proposition 5.2, we can prove that PPs constructed in Section 4 are not QM equivalent to the known PPs listed in Table 2.

Table 1
Known PPs of the form $(x^{2^m}+x+\delta)^s + L(x)$ over $\mathbb{F}_{2^{2m}}$.

No.	Values of s	$L(x)$	Conditions	Refs.
1	$s(2^m-1) \equiv 0 \pmod{2^{2m}-1}$	x	all δ	[29]
2	all s	x	$\delta \in \mathbb{F}_{2^m}$	[30]
3	$2^{m+1}-1$	x	all δ	[19]
4	$\{2^{2m}-2^m-1,$ $2^m+2, 2^{2m-1}+2^{m-1}+1\}$	x	$\delta \in \mathbb{F}_{2^m}$ or $\mathrm{Tr}_m^{2m}(\delta)=1$	[19]
5	$2^{m+1}+3$	x	$\delta \in \mathbb{F}_{2^m}$, or $\delta \notin \mathbb{F}_{2^m}$ with $\mathrm{Tr}_1^{2m}(\delta) = \mathrm{Tr}_1^m(1)$ and $P_m(\frac{1}{\delta+\delta^2}) \neq 0$	[19]
6	$2^{2m-2}+3\cdot 2^{m-2}$	x	$m \not\equiv 0 \pmod 3$	[22]
7	$\{2^{2m+1}+2^{m-1}, 2^{2m}-2^m+1\}$	x	all δ	[22]
8	$\frac{2^{2m+1}+2^{m+1}-1}{3}$	x	m is even	[22]
9	$i(2^m-1)+1$	x	$5i \equiv 1 \pmod{2^m+1}$ or $5i \equiv 4 \pmod{2^m+1}$, $\delta \in \mathbb{F}_{2^{2m}}$	[6]

(continued on next page)

Table 1 (continued)

No.	Values of s	$L(x)$	Conditions	Refs.
10	$2^{2m-2}+2^{m-2}+1$	x	$\delta \in \mathbb{F}_{2^m}$, or $\delta \notin \mathbb{F}_{2^m}$ with $\mathrm{Tr}_1^{2m}(\delta)=\mathrm{Tr}_1^m(1)$ and $P_m(\frac{1}{\delta+\delta^*}) \neq 0$	[34]
11	$3\cdot 2^{2m-2}+2^{m-2}$	x	$m \not\equiv 0 \pmod 3$	[34]
12	$\frac{2^{2m}+2^m+1}{3}$	x	m is even	[34]
13	$2^{2m-1}+2^{m-1}$	$a_1x^{2^m}+a_2x$	See [26]	[26]
14	$\{i(2^m-1)+1, (i\cdot 2^m+1)(2^m-1)+1\}$	$a_1x^{2^m}+a_2x$	$\mathrm{Tr}_m^{2m}(\delta)\neq 0$, $a_1+a_2\in\mathbb{F}_{2^m}^*\backslash\{1\}$, and $\frac{a_1^{2^m+1}+a_2^{2^m+1}}{a_1+a_2}\in\mathbb{F}_{2^{\gcd(k,m)}}^*$	[26]
15	$\{i(2^m-1)+1, (i\cdot 2^m+1)(2^m-1)+1\}$	$a_1x^{2^m}+a_2x$	$\mathrm{Tr}_m^{2m}(\delta)\neq 0$, $a_1+a_2\in\mathbb{F}_{2^m}^*\backslash\{1\}$, and $\frac{a_1^{2^m+1}+a_2^{2^m+1}}{a_1+a_2}\in\mathbb{F}_{2^{\gcd(k,m)}}^*$	[26]
16	$\{2^{m+1}+3, 3\cdot 2^m+2\}$	$a_1x^{2^m}+a_2x$	See [26]	[26]
17	$\{3\cdot 2^{2m-2}+2^{m-2}, 2^{2m-2}+3\cdot 2^{m-2}\}$	$a_1x^{2^m}+a_2x$	See [26]	[26]
18	$\{2^{2m-2}+2^{m-2}+1, 2^{2m-2}+2^m+2^{m-2}\}$	$a_1x^{2^m}+a_2x$	See [26]	[26]
19	$\{5\cdot 2^{m-1}+2, 2^{2m-1}+2^{m+1}+2\}$	$a_1x^{2^m}+a_2x$	See [26]	[26]
20	$\{2^{2m-2}+3\cdot 2^{m-3}, 3\cdot 2^{2m-3}+2^{m-2}\}$	$a_1x^{2^m}+a_2x$	See [26]	[26]
21	$\{2^{2m-2}+5\cdot 2^{m-4}, 5\cdot 2^{2m-4}+2^{m-2}\}$	$a_1x^{2^m}+a_2x$	See [26]	[26]
22	$2^{m+1}+1$	x	$\mathrm{Tr}_m^{2m}(\delta)=0$ or $\mathrm{Tr}_m^{2m}(\delta)=1$	[27]
23	$3\cdot 2^m+2$	x	$\mathrm{Tr}_m^{2m}(\delta)=0$ or $\delta\notin\mathbb{F}_{2^m}$ with $\mathrm{Tr}_1^{2m}(\delta)=\mathrm{Tr}_1^m(1)$ and $P_m(\frac{1}{\mathrm{Tr}_m^{2m}(\delta)})\neq 0$	[27]
24	$2^{2m}-2$	x	$\mathrm{Tr}_m^{2m}(\delta)=0$ or $\mathrm{Tr}_m^{2m}(\delta)=1$	[27]
25	$2^{2m}-3$	x	$\mathrm{Tr}_m^{2m}(\delta)=0$ or $\mathrm{Tr}_m^{2m}(\delta)^3=1$	[27]
26	$2^{m+1}+1$	$a_1x^{2^m}+a_2x$	$a_1+a_2\in\mathbb{F}_{2^m}^*$, $a_1^{2^m}+a_2\notin\{0,\mathrm{Tr}_m^{2m}(\delta^2)\}$, $\mathrm{Tr}_m^{2m}(\delta)=0$	[10]
27	2^i	ax	all δ and $a\in\mathbb{F}_{2^m}^*$	[23]
28	2^i+2^m	ax	See [23]	[23]
29	2^i+2^m+1	ax	$a\in\mathbb{F}_{2^m}^*$, either $\mathrm{Tr}_m^{2m}(\delta)=0$ or $\mathrm{Tr}_m^{2m}(\delta)^{2^i+1}=a$	[23]
30	$2^i-2^{m+1}-2$	x	$i>0$, $\mathrm{Tr}_m^{2m}(\delta^{2^i})=0$ or $\mathrm{Tr}_m^{2m}(\delta^{2^i})=1$	[23]
31	6	ax	See [23]	[23]
32	$\frac{2^m(2^{m+1}+1)}{4}$	ax	See [23]	[23]
33	$\frac{2^m(2^{m+1}+3)}{4}$	ax	$a\in\mathbb{F}_{2^m}^*$, $m>2$, either $\mathrm{Tr}_m^{2m}(\delta)=0$ or $\mathrm{Tr}_m^{2m}(\delta)=a^4$	[23]
34	2^i+1	ax	$a\in\mathbb{F}_{2^m}^*$ and $0<i<2m$ and $\gcd(i,m)=1$, $\mathrm{Tr}_m^{2m}(\delta^{2^i})=0$ or $\mathrm{Tr}_m^{2m}(\delta^{2^i})=a$	[3]
35	$2^{m+1}+2^i+2$	ax	See [3]	[3]
36	$3\cdot 2^m-1$	x	$\mathrm{Tr}_m^{2m}(\delta)=1$	[3]
37	$2^{m+2}-2$	ax	$\mathrm{Tr}_m^{2m}(\delta)=a$ and $a\in\mathbb{F}_{2^m}^*$	[3]
38	$2^{2m}-2^m-3$	ax	$a\mathrm{Tr}_m^{2m}(\delta)^4=1$ and $a\in\mathbb{F}_{2^m}^*$	[3]
39	$2^{2m-1}+2^{m-1}+2^j$	ax	$a\in\mathbb{F}_{2^m}^*$, either $\mathrm{Tr}_m^{2m}(\delta)=0$ or $\mathrm{Tr}_m^{2m}(\delta)^{2^j}=a$	Corollary 3.1
40	$2^{2m-2}+2^{m-2}+2^j$	ax	$a\in\mathbb{F}_{2^m}^*$, either $\mathrm{Tr}_m^{2m}(\delta)=0$ or $\delta\notin\mathbb{F}_{2^m}$ with $\mathrm{Tr}_1^m({c_1}^{-1})=\mathrm{Tr}_1^m(1)$ and $P_m(c_1)\neq 0$ where $c_1=\frac{a^2}{\mathrm{Tr}_m^{2m}(\delta)^{2^{j+1}-1}}$	Corollary 3.2
41	$2^{2m}+2^j-2^m-2$	ax	$a\in\mathbb{F}_{2^m}^*$, $\mathrm{Tr}_m^{2m}(\delta)=0$ or $\mathrm{Tr}_m^{2m}(\delta)^{2^j-3}=a$	Corollary 3.3
42	$2^{2m}+2^j-2^{m+1}-3$	ax	$a\in\mathbb{F}_{2^m}^*$, $\mathrm{Tr}_m^{2m}(\delta)=0$ or $\mathrm{Tr}_m^{2m}(\delta)^{2^j-5}=a$	Corollary 3.4
43	$2^{2m+1}-2^{m+1}+2$	ax	$a\in\mathbb{F}_{2^m}^*$, $\mathrm{Tr}_m^{2m}(\delta)=0$ or $\mathrm{Tr}_m^{2m}(\delta)=a$	Corollary 3.5
44	$3\cdot 2^m-1$	ax	$a\in\mathbb{F}_{2^m}^*$, $\mathrm{Tr}_m^{2m}(\delta)=0$ or $\mathrm{Tr}_m^{2m}(\delta)=a$	Corollary 3.6
45	$2^{2m-1}-2^{m-1}+2$	x	$\mathrm{Tr}_m^{2m}(\delta)=0$ or $\mathrm{Tr}_m^{2m}(\delta)=1$	Corollary 3.7

6 Concluding remarks

In this paper, using AGW criterion and some techniques in solving equations over finite fields, several classes of PPs with the form $(x^{2^m}+x+\delta)^s+ax$ and $(x^{2^m}+x+\delta)^{s_1}+(x^{2^m}+x+\delta)^{s_2}+ax$ over $\mathbb{F}_{2^{2m}}$ are obtained. It is a continuation and generalization of previous results in [3, 10, 19, 23, 26, 34]. All known classes of PPs of the forms $(x^{2^m}+x+\delta)^s+L(x)$ and $(x^{2^m}+x+\delta)^{s_1}+(x^{2^m}+x+\delta)^{s_2}+L(x)$ over $\mathbb{F}_{2^{2m}}$ are summarized in Tables 1 and 2, respectively. Moreover, we prove that the PPs constructed in this paper are not QM equivalent to any known PPs.

Table 2
Known PPs of the form $(x^{2^m}+x+\delta)^{s_1}+(x^{2^m}+x+\delta)^{s_2}+L(x)$ over $\mathbb{F}_{2^{2m}}$.

No.	Values of $\{s_1,s_2\}$	$L(x)$	Conditions	Refs.
1	$\{2^m+1, 2^{m+1}-1\}$	x	all δ	[33]
2	$\{2-2^m, 3-2^{m+1}\}$	x	all δ	[33]
3	$\{s_1, 2^m s_1\}$	x	all δ	[12]
4	$\{\frac{i(2^{2m}-1)}{3}+1, \frac{i(2^{2m}-1)}{3}+2^m\}$	x	all δ	[12]
5	$\{2^{m+i}+2^j, 2^{m+i}+2^{m+j}\}$	x	all δ	[12]
6	$\{2^{\frac{jm}{2^i}}+2^{\frac{jm}{2^i}+\frac{km}{2}}, 2^{(\frac{j}{2^i}+\frac{1}{2})m}+2^{\frac{jm}{2^i}+\frac{(k+1)m}{2}}\}$	x	$2^i \mid jm$, m is even	[12]
7	$\{2^{\frac{im}{3}}+2^{\frac{km}{3}}, 2^{\frac{2im}{3}}+2^{\frac{(k+i)m}{3}}\}$	x	$i\in\{1,2\}$, $3\mid m$	[12]
8	$\{\frac{2^{2m}-1}{3}+2^{jm}, \frac{2(2^{2m}-1)}{3}+2^{jm}\}$	x	all δ	[12]
9	$s_1\in\{2^{m+1}+1, 2^m+2\}$, $s_2\in\{3\cdot 2^m+2, 2^{m+1}+3\}$	x	$\mathrm{Tr}_m^{2m}(\delta)=0$ or $\mathrm{Tr}_m^{2m}(\delta)\notin\mathbb{F}_2$ with $P_m(\frac{1}{\mathrm{Tr}_m^{2m}(\delta)+\mathrm{Tr}_m^{2m}(\delta^2)})\neq 0$ and $\mathrm{Tr}_1^m(1)=0$	[10]
10	$s_1\in\{3\cdot 2^{2m-2}+2^{m-2}, 2^{2m-2}+3\cdot 2^{m-2}\}$, $s_2\in\{2^{2m-2}+2^{m-2}+1, 2^{2m-2}+2^m+2^{m-2}\}$	x	$\mathrm{Tr}_m^{2m}(\delta)\in\mathbb{F}_2$ or $\mathrm{Tr}_m^{2m}(\delta)\notin\mathbb{F}_2$ with $\mathrm{Tr}_1^{2m}(\delta)=0$ and $P_m(\frac{1}{1+\mathrm{Tr}_m^{2m}(\delta)})\neq 0$	[10]
11	$s_1\in\{2^{m+1}+1, 2^m+2\}$, $s_2\in\{2^{2m-1}+2^{m+1}+2, 5\cdot 2^{m-1}+2\}$	x	$\mathrm{Tr}_m^{2m}(\delta)\in\mathbb{F}_2$ or $\mathrm{Tr}_m^{2m}(\delta)\notin\mathbb{F}_2$ with $\mathrm{Tr}_1^m(1+c_7^{-1})=0$ and $P_m(c_7)\neq 0$, where $c_7=\frac{\mathrm{Tr}_m^{2m}(\delta^2)+1}{(\mathrm{Tr}_m^{2m}(\delta))^{\frac{1}{2}}(\mathrm{Tr}_m^{2m}(\delta)+(\mathrm{Tr}_m^{2m}(\delta))^{\frac{1}{4}})^3}$	[10]
12	$s_1\in\{3\cdot 2^m+2, 2^{m+1}+3\}$, $s_2\in\{2^{2m-1}+2^{m+1}+2, 5\cdot 2^{m-1}+2\}$	x	$\mathrm{Tr}_m^{2m}(\delta)\in\mathbb{F}_2$ or $\mathrm{Tr}_m^{2m}(\delta)\notin\mathbb{F}_2$ with $\mathrm{Tr}_1^m(1+c_8^{-1})=0$ and $P_m(c_8)\neq 0$, where $c_8=\frac{1}{\mathrm{Tr}_m^{2m}(\delta^4)+(\mathrm{Tr}_m^{2m}(\delta))^{\frac{7}{2}}}$	[10]
13	$\{2^m+1+2^j, 2^{m+1}+2+2^j\}$	ax	$a\in\mathbb{F}_{2^m}^*$, $\mathrm{Tr}_m^{2m}(\delta)=0$ or $\mathrm{Tr}_m^{2m}(\delta)=1$ if $1+a$ is not a cube element in $\mathbb{F}_{2^m}^*$ or $\mathrm{Tr}_m^{2m}(\delta)\in\mathbb{F}_2$ or $\mathrm{Tr}_m^{2m}(\delta)\notin\mathbb{F}_2$ with $\mathrm{Tr}_1^m({c_2}^{-1})=\mathrm{Tr}_1^m(1)$ and $P_m(c_2)\neq 0$, where $c_2=\frac{\mathrm{Tr}_m^{2m}(\delta)+\frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j}}}{(1+\mathrm{Tr}_m^{2m}(\delta))^3}$	Corollary 4.1
14	$\{2^{2m-1}+2^{m-1}+2^j, 2^m+1+2^j\}$	ax	$a\in\mathbb{F}_{2^m}^*$, $\mathrm{Tr}_m^{2m}(\delta)=0$ or $\mathrm{Tr}_m^{2m}(\delta)\neq 0$, $1+\frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j}}+\mathrm{Tr}_m^{2m}(\delta)=0$ and $\mathrm{Tr}_m^{2m}(\delta)$ is not a cube element in $\mathbb{F}_{2^m}^*$ or $\mathrm{Tr}_m^{2m}(\delta)\neq 0$, $1+\frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j}}+\mathrm{Tr}_m^{2m}(\delta)\neq 0$, $\mathrm{Tr}_1^m({c_3}^{-1})=\mathrm{Tr}_1^m(1)$ and $P_m(c_3)\neq 0$ where $c_3=\frac{\mathrm{Tr}_m^{2m}(\delta)}{(1+\frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j}}+\mathrm{Tr}_m^{2m}(\delta))^3}$.	Corollary 4.2
15	$\{2^{2m-1}+2^{m-1}+2^j, 2^{2m-2}+2^{m-2}+2^j\}$	ax	$a\in\mathbb{F}_{2^m}^*$, $\mathrm{Tr}_m^{2m}(\delta)=0$ or $\mathrm{Tr}_m^{2m}(\delta)=1$ if $(1+a)^4$ is not a cube element in $\mathbb{F}_{2^m}^*$ or $\mathrm{Tr}_m^{2m}(\delta)\notin\mathbb{F}_2$, $\mathrm{Tr}_1^m({c_4}^{-1})=\mathrm{Tr}_1^m(1)$, $P_m(c_4)\neq 0$, where $c_4=\frac{\mathrm{Tr}_m^{2m}(\delta)(1+\frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j}})^2}{(1+\mathrm{Tr}_m^{2m}(\delta))^3}$.	Corollary 4.3
16	$\{2^m+1+2^j, 2^m+1+2^k\}$	ax	$a\in\mathbb{F}_{2^m}^*$, $\mathrm{Tr}_m^{2m}(\delta)^{2^j+1}+\mathrm{Tr}_m^{2m}(\delta)^{2^k+1}=\{0,a\}$	Corollary 4.4

(continued on next page)

Table 2 (continued)

No.	Values of $\{s_1, s_2\}$	$L(x)$	Conditions	Refs.
17	$\{2^{m+1}+2+2^j,\ 2^{m+1}+2+2^k\}$	ax	$a \in \mathbb{F}_{2^m}^*$, $\mathrm{Tr}_m^{2m}(\delta)^{2^j} + \mathrm{Tr}_m^{2m}(\delta)^{2^k} = 0$ or $\mathrm{Tr}_1^m({c_5}^{-1}) = \mathrm{Tr}_1^m(1)$ and $P_m(c_5) \neq 0$ where $c_5 = \frac{a}{\mathrm{Tr}_m^{2m}(\delta)^{2^j+3}+\mathrm{Tr}_m^{2m}(\delta)^{2^k+3}}$	Corollary 4.5
18	$\{2^{2m-2}+2^{m-2}+2^j,\ 2^{2m-2}+2^{m-2}+2^k\}$	ax	$a \in \mathbb{F}_{2^m}^*$, $\mathrm{Tr}_m^{2m}(\delta)^{2^j} + \mathrm{Tr}_m^{2m}(\delta)^{2^k} = 0$ or $\mathrm{Tr}_1^m({c_6}^{-1}) = \mathrm{Tr}_1^m(1)$ and $P_m(c_6) \neq 0$, where $c_6 = \frac{a^2\mathrm{Tr}_m^{2m}(\delta)}{\mathrm{Tr}_m^{2m}(\delta)^{2^j+1}+\mathrm{Tr}_m^{2m}(\delta)^{2^k+1}}$	Corollary 4.6
19	$\{2^{2m-1}+2^{m-1}+2^j,\ 2^{2m-1}+2^{m-1}+2^k\}$	ax	$a \in \mathbb{F}_{2^m}^*$, $\mathrm{Tr}_m^{2m}(\delta)^{2^j} + \mathrm{Tr}_m^{2m}(\delta)^{2^k} = \{0, a\}$	Corollary 4.7
20	$\{2^{2m}-2^m-2+2^j,\ 2^{2m}-2^m-2+2^k\}$	ax	$a \in \mathbb{F}_{2^m}^*$, $\mathrm{Tr}_m^{2m}(\delta)^{2^j} + \mathrm{Tr}_m^{2m}(\delta)^{2^k} = 0$ or $\mathrm{Tr}_m^{2m}(\delta)^{2^j-3} + \mathrm{Tr}_m^{2m}(\delta)^{2^k-3} = a$	Corollary 4.8
21	$\{2^{2m}-2^{m+1}-3+2^j,\ 2^{2m}-2^{m+1}-3+2^k\}$	ax	$a \in \mathbb{F}_{2^m}^*$, $\mathrm{Tr}_m^{2m}(\delta)^{2^j} + \mathrm{Tr}_m^{2m}(\delta)^{2^k} = 0$ or $\mathrm{Tr}_m^{2m}(\delta)^{2^j-5} + \mathrm{Tr}_m^{2m}(\delta)^{2^k-5} = a$	Corollary 4.9

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

Q. Liu was supported in part by the Natural Science Foundation of Fujian Province of China under Grant 2022J05134 and the Open Fund of Key Laboratory of Computing and Stochastic Mathematics (Ministry of Education) (Hunan Normal University) under Grant 202602. Z. Zha was supported in part by the Natural Science Foundation of Xinjiang Urgur Autonomous Region under Grant 2024D01C37, in part by the National Natural Science Foundation of China under Grant 12461103, and in part by the Tianchi Talent Project in Xinjiang Uygur Autonomous Region.

Data availability

No data was used for the research described in this article.

References

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

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

[3] C. Chen, H. Kan, Y. Li, J. Peng, L. Zheng, Several classes of permutation polynomials of the form $(x^{p^m} - x + \delta)^s + L(x)$, Adv. Math. Commun. 19 (2025) 319–336.

[4] C. Ding, J. Yuan, A family of skew Hadamard difference sets, J. Comb. Theory, Ser. A 113 (2006) 1526–1535.

[5] C. Ding, Z. Zhou, Binary cyclic codes from explicit polynomials over GF(2^m), Discrete Math. 324 (2014) 76–89.

[6] R. Gupta, R.K. Sharma, Further results on permutation polynomials of the form $(x^{p^m} - x + \delta)^s + L(x)$ over $\mathbb{F}_{p^{2m}}$, Finite Fields Appl. 50 (2018) 196–208.

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

[8] X. Hou, A survey of permutation binomials and trinomials over finite fields, Finite Fields Appl. 32 (2015) 82–119.

[9] Y. Laigle-Chapuy, Permutation polynomials and applications to coding theory, Finite Fields Appl. 13 (2007) 58–70.

[10] G. Li, X. Cao, Several classes of permutation polynomials over the finite field $\mathbb{F}_{p^{2m}}$, Finite Fields Appl. 89 (2023) 102197.

[11] G. Li, X. Cao, Several classes of permutation polynomials based on the AGW criterion over the finite field $\mathbb{F}_{2^{2m}}$, Finite Fields Appl. 95 (2024) 102378.

[12] L. Li, S. Wang, C. Li, Zeng X., 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] Z. Li, M. Wang, J. Wu, X. Zhu, Some new forms of permutation polynomials based on the AGW criterion, Finite Fields Appl. 61 (2020) 101584.

[14] R. Lidl, H. Niederreiter, Finite Fields, Cambridge University Press, Cambridge, 1997.

[15] Q. Liu, R. Jiang, J. Zou, Several classes of permutation polynomials over $\mathbb{F}_{p^{2m}}$ with odd characteristic based on the AGW criterion, Cryptogr. Commun. 17 (2025) 1569–1582.

[16] G.L. Mullen, Permutation polynomials over finite fields, in: Proc. Conf. Finite Fields and Their Applications, Lecture Notes in Pure and Applied Mathematics, vol. 141, Dekker, New York, 1993, pp. 131–151.

[17] L. Reis, Q. Wang, Constructing permutation polynomials from permutation polynomials of subfields, Finite Fields Appl. 96 (2024) 102415.

[18] J. Schwenk, K. Huber, Public key encryption and digital signatures based on permutation polynomials, Electron. Lett. 34 (1998) 759–760.

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

[20] Z. Tu, X. Zeng, C. Li, T. Helleseth, Permutation polynomials of the form $(x^{p^m} - x + \delta)^s + L(x)$, Finite Fields Appl. 34 (2015) 20–35.

[21] Q. Wang, A survey of compositional inverses of permutation polynomials over finite fields, Des. Codes Cryptogr. 93 (2025) 831–870.

[22] 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.

[23] D. Wu, 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.

[24] D. Wu, P. Yuan, The compositional inverses of the permutation polynomials from trace functions over finite fields, Des. Codes Cryptogr. 93 (2025) 3933–3953.

[25] D. Wu, P. Yuan, C. Ding, Y. Ma, Permutation trinomials over $\mathbb{F}_{2^m}$, Finite Fields Appl. 46 (2017) 38–56.

[26] X. Xu, F. Feng, 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.

[27] G. Xu, G. Luo, 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.

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

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

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

[31] 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.

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

[33] 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.

[34] Z. Zha, 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.

[35] Z. Zha, L. Hu, Z. Zhang, New results on permutation polynomials of the form $(x^{p^m}-x+\delta)^s+x^{p^m}+x$ over $\mathbb{F}_{p^{2m}}$, Cryptogr. Commun. 10 (2018) 567–578.

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

[37] L. Zheng, J. Peng, H. Kan, Y. Li, J. Luo, On constructions and properties of (n,m)-functions with maximal number of bent components, Des. Codes Cryptogr. 88 (2020) 2171–2186.