Two new classes of permutation trinomials over $\mathbb{F}_{q^3}$ with odd characteristic

Xi Xie, Nian Li, Linjie Xu, Xiangyong Zeng and Xiaohu Tang *

Abstract: Let q be an odd prime power and $\mathbb{F}_{q^3}$ be the finite field with q^3 elements. In this paper, we propose two classes of permutation trinomials of $\mathbb{F}_{q^3}$ for an arbitrary odd characteristic based on the multivariate method and some subtle manipulation of solving equations with low degrees over finite fields. Moreover, we demonstrate that these two classes of permutation trinomials are QM inequivalent to all known permutation polynomials over $\mathbb{F}_{q^3}$. To the best of our knowledge, this paper is the first to study the construction of nonlinearized permutation trinomials of $\mathbb{F}_{q^3}$ with at least one coefficient lying in $\mathbb{F}_{q^3}\backslash\mathbb{F}_q$.

Keywords: Finite fields, permutation polynomials, trinomials.

1 Introduction

For a prime power q, let $\mathbb{F}_q$ denote the finite field with q elements and $\mathbb{F}_q^*$ 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 associated polynomial mapping $f : c \to f(c)$ from $\mathbb{F}_q$ to itself is a bijection. Permutation polynomials over finite fields have important applications in a wide range of areas such as coding theory [5], combinational designs [7] and cryptography [8].

Permutation polynomials were first studied by Hermite [11] for the case of finite prime fields and by Dickson [4] for arbitrary finite fields. Permutation polynomials with few terms, especially binomials and trinomials, attract people's interest due to their simple algebraic form

*X. Xie, N. Li, X. Zeng and X. Tang are with the Hubei Key Laboratory of Applied Mathematics, Faculty of Mathematics and Statistics, Hubei University, Wuhan, 430062, China. L. Xu is with the WuHan Marine Communication Research Institute, Wuhan, 430000, China. X. Tang is also with the Information Security and National Computing Grid Laboratory, Southwest Jiaotong University, Chengdu, 610031, China. Email: xi.xie@aliyun.com, nian.li@hubu.edu.cn, linjiexu@126.com, xzeng@hubu.edu.cn, xhutang@swjtu.edu.cn

and additional extraordinary properties [12]. So far a number of permutation binomials and trinomials have been found in the literatures [1, 10, 13, 14, 21, 24, 26–28]. However, most of them were constructed over the finite field $\mathbb{F}_{q^2}$, and only very few permutation trinomials over $\mathbb{F}_{q^3}$ are known. For the permutation trinomials of $\mathbb{F}_{q^3}$ in characteristic 2 and those in odd characteristic, the reader is referred to [2, 9, 15, 18, 20, 26] and [1, 3, 6, 16, 25, 27, 28] respectively.

In this paper, we study the construction of nonlinearized permutation trinomials over $\mathbb{F}_{q^3}$ with the form

$$f(x) = ax^{e_1} + bx^{e_2} + cx, \tag{1}$$

where $a, b, c \in \mathbb{F}_{q^3}^*$ and e_1, e_2 are distinct integers with $1 < e_1, e_2 < q^3 - 1$. The objective of this paper is to find new pairs (e_1, e_2) and coefficients $a, b, c \in \mathbb{F}_{q^3}^*$ such that $f(x)$ defined by (1) is a permutation polynomial over $\mathbb{F}_{q^3}$ for an arbitrary odd characteristic. By virtue of some techniques in dealing with equations over finite fields, we present two new classes of permutation trinomials with the form (1). Compared with the known results in this direction, we demonstrate that the presented two classes of permutation trinomials are QM inequivalent to all known permutation polynomials over $\mathbb{F}_{q^3}$. It is worthy noting that the two classes of permutation trinomials proposed in this paper are the first instances that at least one coefficient of the nonlinearized permutation trinomials over $\mathbb{F}_{q^3}$ belongs to $\mathbb{F}_{q^3} \backslash \mathbb{F}_q$.

The rest of this paper is organized as follows. Section 2 proposes two classes of permutation trinomials. Section 3 investigates the QM equivalence between the permutation polynomials in this paper and the previously known permutation trinomials. Section 4 concludes this study.

2 Two new classes of permutation trinomials of the form (1)

In this section, we present two classes of permutation trinomials with the form (1) over the finite field $\mathbb{F}_{q^3}$. Throughout this paper, let q be an odd prime power, $d \,|\, q^3 - 1$ and $\mu_d = \{x \in \mathbb{F}_{q^3} : x^d = 1\}$ be the set of d-th roots of unity in $\mathbb{F}_{q^3}$. The trace function from $\mathbb{F}_{q^3}$ to its subfield $\mathbb{F}_q$ is defined by $\mathrm{Tr}_{q^3/q}(x) = x + x^q + x^{q^2}$. For a function $f(x)$ over $\mathbb{F}_{q^3}$, we denote the image set of $f(x)$ by $\mathrm{Im}(f)$.

2.1 The first class of permutation trinomials of the form (1)

In this subsection, we consider the permutation property of

$$f_1(x) = ax^{q(q^2-q+1)} + bx^{q^2-q+1} + 2x,\ a, b \in \mathbb{F}_{q^3}^* \tag{2}$$

over $\mathbb{F}_{q^3}$. To prove the permutation property of $f_1(x)$, we need the following basic facts:

(1) $\mathbb{F}_{q^3} = \{0\} \bigcup \{x^{q+1} : x \in \mathbb{F}_{q^3}^*\} \bigcup \{\varepsilon x^{q+1} : x \in \mathbb{F}_{q^3}^*\}$,

(2) each $x \in \mathbb{F}_{q^3}^*$ can be expressed as $x = yz\epsilon$,

where ε is a non-square in $\mathbb{F}_{q^3}$, $y \in \mathbb{F}_q^*$, $z \in \mu_{q^2+q+1}$, $\epsilon \in \{1, \sigma, \sigma^2\}$ and $\sigma \in \mathbb{F}_{q^3}^*$ is a fixed non-cubic element. The first fact is due to $\gcd(q+1, q^3-1) = 2$ and the second one depends on the value of $\gcd(q-1, q^2+q+1)$ which can also be readily verified.

Our first result is stated as follows.

Theorem 1. *Let q be an odd prime power and $a, b \in \mathbb{F}_{q^3}^*$. Then*

$$f_1(x) = ax^{q(q^2-q+1)} + bx^{q^2-q+1} + 2x$$

is a permutation polynomial of $\mathbb{F}_{q^3}$ if one of the following conditions is satisfied:

(1) $ab = 1$ and $a^{q^2+q+1} \neq -1$;

(2) $ab \in \mathbb{F}_q^* \backslash \{1\}$ and $a^{q^2+q+1} + 2ab + b^{q^2+q+1} = 0$.

Proof. (1) According to the first basic fact given as above, to prove that $f_1(x)$ permutes $\mathbb{F}_{q^3}$, it suffices to prove that the image sets of $f_1(0)$, $f_1(x^{q+1})$ and $f_1(\varepsilon x^{q+1})$ form the whole field $\mathbb{F}_{q^3}$, where ε is a non-square element in $\mathbb{F}_{q^3}$. Observe that $f_1(0) = 0$ and

$$\begin{aligned} f_1(x^{q+1}) &= ax^{2q} + bx^2 + 2x^{q+1} = a\big(x^q + bx\big)^2, \\ f_1(\varepsilon x^{q+1}) &= a\varepsilon^{q^3-q^2+q}x^{2q} + b\varepsilon^{q^2-q+1}x^2 + 2\varepsilon x^{q+1} = a\varepsilon^{q^3-q^2+q}\big(x^q + b\varepsilon^{q^2-q}x\big)^2. \end{aligned}$$

Since $ab = 1$ and $a^{q^2+q+1} \neq -1$, we have $b^{q^2+q+1} \neq -1$. This implies that both $x^q + bx$ and $x^q + b\varepsilon^{q^2-q}x$ are permutation polynomials over $\mathbb{F}_{q^3}$, which indicates that one of the image sets of $f_1(x^{q+1})$ and $f_1(\varepsilon x^{q+1})$ is the set of all squares in $\mathbb{F}_{q^3}^*$ and the other is the set of all non-squares in $\mathbb{F}_{q^3}^*$. This proves (1).

(2) Let $a = y_1z_1\epsilon_1$ and $b = y_2z_2\epsilon_2$ with $y_1, y_2 \in \mathbb{F}_q^*$, $z_1, z_2 \in \mu_{q^2+q+1}$ and $\epsilon_1, \epsilon_2 \in \{1, \sigma, \sigma^2\}$, where $\sigma \in \mathbb{F}_{q^3}^*$ is a fixed non-cubic element. Since $ab = y_1y_2z_1z_2\epsilon_1\epsilon_2 \in \mathbb{F}_q^*$, we have $z_1z_2\epsilon_1\epsilon_2 \in \mathbb{F}_q^*$, which implies

$$(z_1z_2\epsilon_1\epsilon_2)^{q^2+q+1} = (z_1z_2\epsilon_1\epsilon_2)^3 = (\epsilon_1\epsilon_2)^{q^2+q+1}. \tag{3}$$

If $\gcd(q-1, q^2+q+1) = 3$, then both $z_1z_2 \in \mu_{q^2+q+1}$ and $z_1z_2\epsilon_1\epsilon_2 \in \mathbb{F}_q^*$ are cubic elements, which implies $\epsilon_1\epsilon_2$ is a cubic element. Together with the fact $\epsilon_1 = \epsilon_2 = 1$ when $\gcd(q-1, q^2+q+1) = 1$, without loss of generality, we can assume that $\epsilon_1 = \epsilon$ and $\epsilon_2 = \epsilon^2$ with $\epsilon \in \{1, \sigma\}$. Substituting $\epsilon_1 = \epsilon$ and $\epsilon_2 = \epsilon^2$ into (3) gives

$$\Big(\frac{z_1z_2\epsilon^3}{\epsilon^{q^2+q+1}}\Big)^3 = 1.$$

Setting $\lambda = \frac{z_1 z_2 \epsilon^3}{\epsilon^{q^2+q+1}}$ implies $\lambda \in \mathbb{F}_q^*$ and $\lambda^3 = 1$. Then z_2 can also be written as $z_2 = \frac{\epsilon^{q^2+q+1}\lambda}{z_1 \epsilon^3}$. Plugging $a = y_1 z_1 \epsilon_1$ and $b = y_2 z_2 \epsilon_2$ into the condition $a^{q^2+q+1} + 2ab + b^{q^2+q+1} = 0$ leads to

$$\epsilon^{q^2+q+1} y_1^3 + 2\epsilon^{q^2+q+1} \lambda y_1 y_2 + \epsilon^{2(q^2+q+1)} y_2^3 = 0,$$

that is

$$y_1^3 + 2\lambda y_1 y_2 + \epsilon^{q^2+q+1} y_2^3 = 0.$$

Since y_1, $y_2 \in \mathbb{F}_q^*$, we can assume $y_1 = \beta y_2$ for some $\beta \in \mathbb{F}_q^*$. Then the above equation becomes

$$\beta^3 y_2^3 + 2\lambda\beta y_2^2 + \epsilon^{q^2+q+1} y_2^3 = 0.$$

It can be seen that $\epsilon^{q^2+q+1} + \beta^3 \neq 0$ due to $y_2 \neq 0$. Further, from the above equation we can derive $y_2 = -\frac{2\lambda\beta}{\epsilon^{q^2+q+1}+\beta^3}$, and then $y_1 = -\frac{2\lambda\beta^2}{\epsilon^{q^2+q+1}+\beta^3}$. Subsequently,

$$a = -\frac{2\lambda\beta^2}{\epsilon^{q^2+q+1} + \beta^3} z_1 \epsilon,\ b = -\frac{2\lambda^2 \beta \epsilon^{q^2+q+1}}{(\epsilon^{q^2+q+1} + \beta^3) z_1 \epsilon}. \tag{4}$$

Substituting (4) into $f_1(x)$, it then turns into

$$f_1(x) = -2(\epsilon^{q^2+q+1} + \beta^3)^{-1}\big(\beta^2\epsilon(\lambda z_1) x^{q(q^2-q+1)} + \beta\epsilon^{q^2+q}(\lambda z_1)^{-1} x^{q^2-q+1} - (\epsilon^{q^2+q+1} + \beta^3)x\big).$$

Since $(\lambda z_1)^{q^2+q+1} = \lambda^3 = 1$ due to $\lambda \in \mathbb{F}_q^*$, $\lambda^3 = 1$ and $z_1 \in \mu_{q^2+q+1}$, we know $\lambda z_1 \in \mu_{q^2+q+1}$. Hence, there exists an $\alpha \in \mathbb{F}_{q^3}^*$ such that $\lambda z_1 = \alpha^{q^2-q}$. Substituting x with αx, $f_1(x)$ becomes

$$f_1(x) = -2\alpha(\epsilon^{q^2+q+1} + \beta^3)^{-1}\big(\beta^2\epsilon x^{q(q^2-q+1)} + \beta\epsilon^{q^2+q} x^{q^2-q+1} - (\epsilon^{q^2+q+1} + \beta^3)x\big).$$

Therefore, to prove that $f_1(x)$ permutes $\mathbb{F}_{q^3}$, it suffices to prove that

$$\beta^2\epsilon x^{q(q^2-q+1)} + \beta\epsilon^{q^2+q} x^{q^2-q+1} - (\epsilon^{q^2+q+1} + \beta^3)x = d \tag{5}$$

has at most one solution in $\mathbb{F}_{q^3}$ for any $d \in \mathbb{F}_{q^3}$.

Case I. $d = 0$. For this case, (5) can be written as

$$x^{q(q^2-q+1)}(\epsilon^{q^2+q} x^{q^2-q} - \beta^2)(\beta x^{q^2-q} - \epsilon) = 0.$$

We claim that neither $\epsilon^{q^2+q} x^{q^2-q} - \beta^2$ nor $\beta x^{q^2-q} - \epsilon$ is 0. Otherwise, $\epsilon^{q^2+q} x^{q^2-q} - \beta^2 = 0$ implies $(\beta^2/\epsilon^{q^2+q})^{q^2+q+1} = 1$ and $\beta x^{q^2-q} - \epsilon = 0$ implies $(\epsilon/\beta)^{q^2+q+1} = 1$. In either case we can deduce $\epsilon^{q^2+q+1} = \beta^3$ due to $\beta \in \mathbb{F}_q^*$ and $\epsilon^{q^2+q+1} + \beta^3 \neq 0$. Using the values of a and b given in (4), a calculation gives $ab = \frac{4\beta^3\epsilon^{q^2+q+1}}{(\epsilon^{q^2+q+1}+\beta^3)^2} = 1$, which contradicts with $ab \neq 1$. Therefore, (5) has only the zero solution in $\mathbb{F}_{q^3}$.

Case II. $d \neq 0$. Obviously, in this case $x = 0$ is not a solution of (5). Let $y = x^q$, $z = y^q$, $d_1 = d^q$, $d_2 = d_1^q$, then from (5), we obtain the system of equations

$$\begin{cases} \beta^2\epsilon\dfrac{xy}{z} + \beta\epsilon^{q^2+q}\dfrac{xz}{y} - (\epsilon^{q^2+q+1} + \beta^3)x = d, & (6) \\ \beta^2\epsilon^q\dfrac{yz}{x} + \beta\epsilon^{q^2+1}\dfrac{xy}{z} - (\epsilon^{q^2+q+1} + \beta^3)y = d_1, & (7) \\ \beta^2\epsilon^{q^2}\dfrac{xz}{y} + \beta\epsilon^{q+1}\dfrac{yz}{x} - (\epsilon^{q^2+q+1} + \beta^3)z = d_2. & (8) \end{cases}$$

Eliminating the terms $\frac{xy}{z}$ and $\frac{yz}{x}$ from (6), (7) and (8) results in

$$\epsilon^{q^2}\beta(\epsilon^{q^2+q+1} + \beta^3)\frac{xz}{y} - (\epsilon^{q^2+q+1} + \beta^3)(\epsilon^{q^2+1}x - \beta\epsilon y + \beta^2 z) = \epsilon^{q^2+1}d - \beta\epsilon d_1 + \beta^2 d_2.$$

Note that $\epsilon^{q^2}\frac{x}{y} - \beta \neq 0$ from the fact $\epsilon^{q^2+q+1} \neq \beta^3$. Then we can obtain that

$$z = \frac{\epsilon^{q^2+1}x - \beta\epsilon y + \Delta}{\beta(\epsilon^{q^2}\frac{x}{y} - \beta)} \tag{9}$$

with

$$\Delta = \frac{\epsilon^{q^2+1}d - \beta\epsilon d_1 + \beta^2 d_2}{\epsilon^{q^2+q+1} + \beta^3}. \tag{10}$$

Rewriting (8) as

$$\frac{yz}{x}(\beta^2\frac{x}{y} - \epsilon^{q+1})(\epsilon^{q^2}\frac{x}{y} - \beta) = d_2$$

and substituting (9) into the above equation leads to

$$\frac{y}{x}(\epsilon^{q^2+1}x - \beta\epsilon y + \Delta)(\beta^2\frac{x}{y} - \epsilon^{q+1}) = \beta d_2,$$

which gives

$$\epsilon^{q^2+1}x - \beta\epsilon y + \Delta = \frac{\beta d_2 x}{\beta^2 x - \epsilon^{q+1}y} \tag{11}$$

and

$$\epsilon(\epsilon^{q^2}x - \beta y)(\beta^2 x - \epsilon^{q+1}y) = (\beta d_2 - \Delta\beta^2)x + \Delta\epsilon^{q+1}y. \tag{12}$$

Further, using the value of z given in (9) and combining with (11) and (12), one obtains

$$\frac{y}{z} = \frac{\beta(\epsilon^{q^2}x - \beta y)}{\epsilon^{q^2+1}x - \beta\epsilon y + \Delta} = \frac{(\epsilon^{q^2}x - \beta y)(\beta^2 x - \epsilon^{q+1}y)}{d_2 x} = \frac{(\beta d_2 - \Delta\beta^2)x + \Delta\epsilon^{q+1}y}{\epsilon d_2 x}. \tag{13}$$

This together with (6), i.e.,

$$\frac{xz}{y}(\beta^2\frac{y}{z} - \epsilon^{q^2+q})(\epsilon\frac{y}{z} - \beta) = d$$

one gets

$$-\Delta\big(\big((\beta^3 - \epsilon^{q^2+q+1})d_2 - \Delta\beta^4\big)x + \Delta\beta^2\epsilon^{q+1}y\big)(\beta^2 x - \epsilon^{q+1}y) = dd_2\big((\beta d_2 - \Delta\beta^2)x + \Delta\epsilon^{q+1}y\big). \tag{14}$$

Note that $\epsilon^{q^2+q}x^{q^2-q}-\beta^2\neq 0$, i.e., $\epsilon^{q^2+q}z\neq\beta^2 y$ as we claimed in Case I. Taking q^2-th power on both sides of it gives $\beta^2x-\epsilon^{q+1}y\neq 0$. Then substituting (12) into (14) and dividing $\beta^2x-\epsilon^{q+1}y$ on both sides of it, one obtains

$$-\Delta\big(((\beta^3-\epsilon^{q^2+q+1})d_2-\Delta\beta^4)x+\Delta\beta^2\epsilon^{q+1}y\big)=\epsilon dd_2(\epsilon^{q^2}x-\beta y),$$

i.e.,

$$(\epsilon^{q^2+1}dd_2+\Delta((\beta^3-\epsilon^{q^2+q+1})d_2-\Delta\beta^4))x=(\beta\epsilon dd_2-\Delta^2\beta^2\epsilon^{q+1})y. \tag{15}$$

Case II-1. $\beta\epsilon dd_2-\Delta^2\beta^2\epsilon^{q+1}=0$. If this case happens, then $dd_2=\Delta^2\beta\epsilon^q$ and (15) holds only when

$$\epsilon^{q^2+1}dd_2+\Delta((\beta^3-\epsilon^{q^2+q+1})d_2-\Delta\beta^4)=0$$

due to $x\neq 0$. Substituting $dd_2=\Delta^2\beta\epsilon^q$ into the above equation, we can obtain that

$$\Delta(\beta\epsilon^{q^2+q+1}\Delta+(\beta^3-\epsilon^{q^2+q+1})d_2-\Delta\beta^4)=0$$

i.e.,

$$\Delta(\epsilon^{q^2+q+1}-\beta^3)(\beta\Delta-d_2)=0. \tag{16}$$

Then, by (10), one gets

$$(\epsilon^{q^2+1}d-\beta\epsilon d_1+\beta^2d_2)(\beta\epsilon^{q^2+1}d-\beta^2\epsilon d_1-\epsilon^{q^2+q+1}d_2)=0. \tag{17}$$

Recall that $d_1=d^q$ and $d_2=d_1^q$. Thus the polynomial $\epsilon^{q^2+1}d-\beta\epsilon d_1+\beta^2d_2$, i.e.,

$$\epsilon^{q^2+1}d-\beta\epsilon d^q+\beta^2d^{q^2}$$

with respect to d is a linearized polynomial over $\mathbb{F}_{q^3}$ and it permutes $\mathbb{F}_{q^3}$ if and only if the determinant of the matrix

$$\begin{pmatrix}\epsilon^{q^2+1} & -\beta\epsilon & \beta^2\\ \beta^2 & \epsilon^{q+1} & -\beta\epsilon^q\\ -\beta\epsilon^{q^2} & \beta^2 & \epsilon^{q^2+q}\end{pmatrix}$$

is nonzero. A direct calculation gives the determinant of the above matrix is $(\epsilon^{q^2+q+1}+\beta^3)^2\neq 0$, which means $\epsilon^{q^2+1}d-\beta\epsilon d_1+\beta^2d_2$ is a permutation polynomial of $\mathbb{F}_{q^3}$. Hence $\epsilon^{q^2+1}d-\beta\epsilon d_1+\beta^2d_2\neq 0$ since $d\neq 0$. Similarly, we can derive $\beta\epsilon^{q^2+1}d-\beta^2\epsilon d_1-\epsilon^{q^2+q+1}d_2\neq 0$. This contradicts with (17), which implies (15) has no solution in $\mathbb{F}_{q^3}$.

Case II-2. $\beta\epsilon dd_2-\Delta^2\beta^2\epsilon^{q+1}\neq 0$. In this case (15) gives $y=\theta x$ with

$$\theta=\frac{\epsilon^{q^2+1}dd_2+\Delta((\beta^3-\epsilon^{q^2+q+1})d_2-\Delta\beta^4)}{\beta\epsilon dd_2-\Delta^2\beta^2\epsilon^{q+1}}. \tag{18}$$

Using the relation $y = \theta x$, (12) becomes

$$\epsilon(\epsilon^{q^2} - \beta\theta)(\beta^2 - \epsilon^{q+1}\theta)x^2 = \big(\beta d_2 - (\beta^2 - \epsilon^{q+1}\theta)\Delta\big)x. \tag{19}$$

Next we show that neither $\epsilon^{q^2} - \beta\theta$ nor $\beta^2 - \epsilon^{q+1}\theta$ is 0. If $\epsilon^{q^2} - \beta\theta = 0$, then $\theta = \epsilon^{q^2}/\beta$ can be simplified to

$$\Delta(\epsilon^{q^2+q+1} - \beta^3)(\beta\Delta - d_2) = 0$$

by (18), which is exactly (16) and it cannot hold as we proved before. If $\beta^2 - \epsilon^{q+1}\theta = 0$, then (19) holds only when

$$\beta d_2 - (\beta^2 - \epsilon^{q+1}\theta)\Delta = 0 = \beta d_2$$

due to $x \neq 0$. This is impossible since $\beta \neq 0$ and $d_2 \neq 0$. Hence, by (19), we can get

$$x = \frac{(\beta d_2 - \Delta\beta^2) + \Delta\epsilon^{q+1}\theta}{\epsilon(\epsilon^{q^2} - \beta\theta)(\beta^2 - \epsilon^{q+1}\theta)}. \tag{20}$$

Combining the above cases, we can conclude that the solution of (5) is zero when $d = 0$ and is given by (20) when $d \neq 0$. This completes the proof. □

2.2 The second class of permutation trinomials of the form (1)

In this subsection, we investigate the permutation property of

$$f_2(x) = x^{q^2-q+1} + ax^{q^2} + bx,\ a, b \in \mathbb{F}_{q^3}^* \tag{21}$$

over $\mathbb{F}_{q^3}$.

Lemma 1. ([19,22,29]) *Let n and d be positive integers such that $d|(p^n - 1)$, where p is a prime. Let $h(x) \in \mathbb{F}_{p^n}[x]$. Then $f(x) = xh\big(x^{\frac{p^n-1}{d}}\big)$ is a permutation polynomial over $\mathbb{F}_{p^n}$ if and only if $g(x) = xh(x)^{\frac{p^n-1}{d}}$ permutes the set of d-th roots of unity in $\mathbb{F}_{p^n}$.*

According to Lemma 1, to prove that $f_2(x)$ permutes $\mathbb{F}_{q^3}$, it suffices to prove that

$$g(x) = x(ax^{q+1} + x^q + b)^{q-1}$$

permutes μ_{q^2+q+1}. Then we can do this by the following two steps.

Step 1. Prove that $ax^{q+1} + x^q + b \neq 0$ for any $x \in \mu_{q^2+q+1}$. Suppose that $ax^{q+1} + x^q + b = 0$ for some $x \in \mu_{q^2+q+1}$, then we have $ax + 1 \neq 0$ since $x \neq 0$ and $b \neq 0$, and consequently,

$$x^q = -\frac{b}{ax+1},\ x^{q^2} = -\frac{b^q(ax+1)}{-a^q b + ax + 1}.$$

The fact $x^{q^2+q+1}=1$ implies $b^{q+1}x=-a^qb+ax+1$. Hence, we only need to verify that

$$(a-b^{q+1})x=a^qb-1 \tag{22}$$

does not hold for any $x\in\mu_{q^2+q+1}$ satisfying $ax^{q+1}+x^q+b=0$.

Step 2. Prove that $g(x_1)\neq g(x_2)$ for any distinct x_1, $x_2\in\mu_{q^2+q+1}$. Suppose that there are distinct x_1, $x_2\in\mu_{q^2+q+1}$ such that $g(x_1)=g(x_2)$ holds, then

$$x_1\big(ax_1^{q+1}+x_1^q+b\big)^{q-1}=x_2\big(ax_2^{q+1}+x_2^q+b\big)^{q-1},$$

i.e.,

$$\left(\frac{ax_1^{q+1}+x_1^q+b}{ax_2^{q+1}+x_2^q+b}\right)^{q-1}=\frac{x_2}{x_1}.$$

Since $\frac{x_2}{x_1}\in\mu_{q^2+q+1}\backslash\{1\}$, we assume $\frac{x_2}{x_1}=\omega^{q-1}$ and $\omega\notin\mathbb{F}_q$. Then the above equation yields

$$ax_1^{q+1}+x_1^q+b=\xi\omega(ax_2^{q+1}+x_2^q+b)$$

for some $\xi\in\mathbb{F}_q^*$. Combining with $x_2=x_1\omega^{q-1}$, one gets

$$\theta_1x_1^{q+1}+\theta_2x_1^q+\theta_3=0, \tag{23}$$

where

$$\theta_1=a(1-\xi\omega)^{q^2},\ \theta_2=1-\xi\omega^{q^2-q+1}\text{ and }\theta_3=b(1-\xi\omega). \tag{24}$$

It can be seen that $\theta_3=b(1-\xi\omega)\neq0$ from $\omega\notin\mathbb{F}_q$. Then from (23), we can obtain that

$$x_1^q=-\frac{\theta_3}{\theta_1x_1+\theta_2},\ x_1^{q^2}=-\frac{\theta_3^q(\theta_1x_1+\theta_2)}{-\theta_1^q\theta_3+\theta_2^q(\theta_1x_1+\theta_2)}.$$

The fact $x_1^{q^2+q+1}=1$ implies

$$\theta_3^{q+1}x_1=-\theta_1^q\theta_3+\theta_2^q(\theta_1x_1+\theta_2),$$

that is,

$$(\theta_3^{q+1}-\theta_1\theta_2^q)x_1=(\theta_2^{q+1}-\theta_1^q\theta_3). \tag{25}$$

Case I. $\theta_3^{q+1}-\theta_1\theta_2^q=0$. If $\theta_3^{q+1}-\theta_1\theta_2^q=0$, from (25) we know that $\theta_2^{q+1}-\theta_1^q\theta_3=0$. This together with (24) gives

$$\begin{cases}\theta_3^{q+1}-\theta_1\theta_2^q=b^{q+1}(1-\xi\omega)^{q+1}-a(1-\xi\omega)^{q^2}(1-\xi\omega^{q^3-q^2+q})=0,\\ \theta_2^{q+1}-\theta_1^q\theta_3=(1-\xi\omega^{q^2-q+1})^{q+1}-a^qb(1-\xi\omega)^2=0,\end{cases}$$

which can be simplified as

$$\begin{cases} (b^{q+1}-a)(1+\xi^2\omega^{q+1}) = \xi(b^{q+1}(\omega+\omega^q) - a(\omega^{q^2}+\omega^{q^3-q^2+q})), & (26) \\ (1-a^qb)(1+\xi^2\omega^2) = \xi(\omega^{q^2-q+1}+\omega^{q^3-q^2+q} - 2a^qb\omega). & (27) \end{cases}$$

Thus, in order to obtain a contradiction, we have to show that (26) and (27) cannot hold simultaneously for any $\omega \in \mathbb{F}_{q^3}\backslash\mathbb{F}_q$ and $\xi \in \mathbb{F}_q^*$ with given a and b.

Case II. $\theta_3^{q+1} - \theta_1\theta_2^q \neq 0$. For this case, from (25) we have

$$x_1 = \frac{\theta_2^{q+1} - \theta_1^q\theta_3}{\theta_3^{q+1} - \theta_1\theta_2^q}.$$

Substituting it into (23) and dividing θ_3^{q+1} on both sides lead to

$$\theta_1^{q^2+q+1} + \theta_2^{q^2+q+1} + \theta_3^{q^2+q+1} = \theta_1\theta_2^q\theta_3^{q^2} + \theta_1^q\theta_2^{q^2}\theta_3 + \theta_1^{q^2}\theta_2\theta_3^q.$$

Then by (24) and a straightforward computation, one obtains

$$\begin{aligned} &\big(a^{q^2+q+1} + b^{q^2+q+1} - \mathrm{Tr}_{q^3/q}(a^qb) + 1\big)\omega^{1+q+q^2}\xi^3 - \big[\,\mathrm{Tr}_{q^3/q}\big((a^{q^2+q+1} + b^{q^2+q+1} \\ &- 2ab^{q^2})\omega^{q+1}\big) + \mathrm{Tr}_{q^3/q}\big((1-a^qb)\,\omega^2\big)\,\big]\xi^2 + \big[\,\mathrm{Tr}_{q^3/q}\big((a^{q^2+q+1} + b^{q^2+q+1} - 2a^qb)\omega\big) \\ &+ \mathrm{Tr}_{q^3/q}\big((1-a^{q^2}b^q)\omega^{q^2-q+1}\big)\big]\xi - \big(a^{q^2+q+1} + b^{q^2+q+1} - \mathrm{Tr}_{q^3/q}(a^qb) + 1\big) = 0. \end{aligned} \quad (28)$$

Hence, to prove $g(x_1) \neq g(x_2)$, we need to show that (28) has no solution on ξ for any $\omega \in \mathbb{F}_{q^3}\backslash\mathbb{F}_q$ with given a and b.

Our second main result is stated as follows.

Theorem 2. *Let q be an odd prime power and a, $b \in \mathbb{F}_{q^3}^*$. Then*

$$f_2(x) = x^{q^2-q+1} + ax^{q^2} + bx$$

is a permutation polynomial over $\mathbb{F}_{q^3}$ if one of the following conditions is satisfied:

(1) $a^qb = 1$ and $a^{q^2+q+1} \neq 1$;

(2) $a^qb \in \mathbb{F}_q^*\backslash\{1\}$ and $a^{q^2+q+1} - 2a^qb + b^{q^2+q+1} = 0$.

Proof. We can prove this result by employing the above strategy.

(1) Step 1. If $a^qb = 1$, then (22) is reduced to $(a - b^{q+1})x = 0$ which leads to $a - b^{q+1} = 0$ due to $x \neq 0$. Since $a^qb = 1$, one has

$$a - b^{q+1} = a - \frac{1}{a^{q+q^2}} = \frac{a^{q^2+q+1} - 1}{a^{q+q^2}} \neq 0$$

since $a^{q^2+q+1} \neq 1$. This implies (22) does not hold and then $ax^{q+1} + x^q + b \neq 0$ for any $x \in \mu_{q^2+q+1}$.

Step 2. In Case I, when $a^q b = 1$, (27) becomes

$$0 = \xi(\omega^{q^2-q+1} + \omega^{q^3-q^2+q} - 2\omega) = \xi\omega^{q^3-q^2-q}(\omega^{q^2} - \omega^q)^2,$$

which contradicts to the fact $\omega \notin \mathbb{F}_q$. In Case II, the condition $a^q b = 1$ implies $a^q b = a^{q^2} b^q = ab^{q^2} = 1$, then

$$a^{q^2+q+1} + b^{q^2+q+1} - 2 = \frac{a^{2(q^2+q+1)} - 2a^{q^2+q+1} + 1}{a^{q^2+q+1}} = \frac{(a^{q^2+q+1} - 1)^2}{a^{q^2+q+1}} \in \mathbb{F}_q^*$$

due to $a^{q^2+q+1} \neq 1$ and (28) turns into

$$\begin{aligned} &\big(a^{q^2+q+1} + b^{q^2+q+1} - 2\big)\omega^{1+q+q^2}\xi^3 - \mathrm{Tr}_{q^3/q}\left((a^{q^2+q+1} + b^{q^2+q+1} - 2)\omega^{q+1}\right)\xi^2 \\ &+ \mathrm{Tr}_{q^3/q}\left((a^{q^2+q+1} + b^{q^2+q+1} - 2)\omega\right)\xi - \big(a^{q^2+q+1} + b^{q^2+q+1} - 2\big) = 0. \end{aligned} \tag{29}$$

Dividing both sides of (29) by $a^{q^2+q+1} + b^{q^2+q+1} - 2$ gives

$$\omega^{1+q+q^2}\xi^3 - \mathrm{Tr}_{q^3/q}\left(\omega^{q+1}\right)\xi^2 + \mathrm{Tr}_{q^3/q}(\omega)\xi - 1 = 0.$$

It can be verified that $1/\omega$, $1/\omega^q$ and $1/\omega^{q^2}$ are three distinct solutions of the above equation. Note that $1/\omega^{q^i} \notin \mathbb{F}_q$ for $i = 0, 1, 2$ due to $\omega \notin \mathbb{F}_q$. Therefore, this equation has no solution in $\mathbb{F}_q$, and then the desired result follows.

(2) For simplicity, denote $\tau = a^q b$ and $c = b^{q^2+q+1}$, then in this case we have $\tau \in \mathbb{F}_q^* \backslash \{1\}$, $c \in \mathbb{F}_q^*$ and $a^q = \tau/b$. Further, from the condition $a^{q^2+q+1} - 2a^q b + b^{q^2+q+1} = 0$, we can obtain

$$\tau^3 - 2\tau c + c^2 = 0. \tag{30}$$

Step 1. If (22) holds, then $a - b^{q+1} \neq 0$ since $a^q b - 1 \neq 0$, and then (22) gives $x = \frac{\tau-1}{a-b^{q+1}}$. Since $\tau \in \mathbb{F}_q^*$ and $a^q = \tau/b$, one has $a = \tau/b^{q^2}$ and

$$x = \frac{\tau - 1}{\tau/b^{q^2} - b^{q+1}} = \frac{\tau - 1}{\tau - c} b^{q^2}.$$

Plugging it into $ax^{q+1} + x^q + b = 0$ and multiplying both sides by $(\tau - c)^2/b$ gives

$$\tau(\tau - 1)^2 + (\tau - 1)(\tau - c) + (\tau - c)^2 = 0$$

due to $\frac{\tau-1}{\tau-c} \in \mathbb{F}_q^*$ and $ab^{q^2} = a^q b = \tau$. That is

$$\tau^3 - 3\tau c + c^2 + c = 0. \tag{31}$$

By (31) and (30), one gets $-\tau c + c = 0$, i.e., $\tau = 1$, a contradiction. Thus $ax^{q+1} + x^q + b \neq 0$ for any $x \in \mu_{q^2+q+1}$.

Step 2. In Case I, multiplying b^{q^2} on both sides of (26) and substituting $\tau = a^q b$, $c = b^{q^2+q+1}$ into (26) and (27), we can obtain

$$\begin{cases} (c-\tau)(1+\xi^2\omega^{q+1}) = \xi(c(\omega+\omega^q) - \tau(\omega^{q^2} + \omega^{q^3-q^2+q})), & (32) \\ (1-\tau)(1+\xi^2\omega^2) = \xi(\omega^{q^2-q+1} + \omega^{q^3-q^2+q} - 2\tau\omega) & (33) \end{cases}$$

since $ab^{q^2} = a^q b = \tau$. Taking q-th power on both sides of (32) (resp. (33)) and subtracting the resulting equation from (32) (resp. (33)) gives

$$\begin{cases} (c-\tau)(\omega^{q+1} - \omega^{q^2+q})\xi^2 = \xi(c(\omega - \omega^{q^2}) - \tau(\omega^{q^2} + \omega^{q^3-q^2+q} - \omega - \omega^{q^2+q-1})), \\ (1-\tau)(\omega^2 - \omega^{2q})\xi^2 = \xi(\omega^{q^2-q+1} - \omega^{q^2+q-1} - 2\tau(\omega - \omega^q)) \end{cases}$$

since τ, c, $\xi \in \mathbb{F}_q$. Note that $\omega - \omega^q \neq 0$ and $\omega - \omega^{q^2} \neq 0$ due to $\omega \notin \mathbb{F}_q$. Then the above equations can be reduced to

$$\begin{cases} (c-\tau)\omega^q\xi = c + \tau(1 - \omega^{-q^2+q-1}(\omega + \omega^{q^2})), & (34) \\ (1-\tau)(\omega+\omega^q)\xi = \omega^{q^2-q-1}(\omega+\omega^q) - 2\tau. & (35) \end{cases}$$

Taking q-th power on both sides of (34) (resp. (35)) and subtracting the resulting equation from (34) (resp. (35)), one can similarly obtain that

$$\begin{cases} (c-\tau)\xi = -\tau(\omega^{-1} + \omega^{-q} + \omega^{-q^2}), \\ (1-\tau)\xi = -(\omega^{-1} + \omega^{-q} + \omega^{-q^2}). \end{cases}$$

This indicates $(c-\tau)/\tau = 1-\tau$, i.e., $\tau - c = \tau(\tau-1)$. Then, by (30), we have

$$\tau^3 - 2\tau c + c^2 = \tau^3 - \tau^2 + (\tau - c)^2 = \tau^2(\tau-1) + \tau^2(\tau-1)^2 = \tau^3(\tau-1) = 0$$

which leads to $\tau = 0$ or 1, a contradiction. Hence (26) and (27) cannot hold simultaneously.

In Case II, using $a^{q^2+q+1} - 2a^q b + b^{q^2+q+1} = 0$ and $\tau = a^q b \in \mathbb{F}_q^*$, (28) turns into

$$(1-\tau)\omega^{1+q+q^2}\xi^3 - (1-\tau)\mathrm{Tr}_{q^3/q}(\omega^2)\xi^2 + (1-\tau)\mathrm{Tr}_{q^3/q}(\omega^{q^2-q+1})\xi - (1-\tau) = 0.$$

Since $\tau \neq 1$, the above equation is equivalent to

$$\omega^{1+q+q^2}\xi^3 - \mathrm{Tr}_{q^3/q}\left(\omega^2\right)\xi^2 + \mathrm{Tr}_{q^3/q}(\omega^{q^2-q+1})\xi - 1 = 0. \quad (36)$$

It can be verified that $\frac{1}{\omega^{q^2+q-1}}$, $\frac{1}{\omega^{q^2-q+1}}$ and $\frac{1}{\omega^{q^3-q^2+q}}$ are three solutions of (36). Note that $\frac{1}{\omega^{(q^2+q-1)q^i}} \notin \mathbb{F}_q$ for $i = 0, 1, 2$. Otherwise we have $\frac{1}{\omega^{q^2+q-1}} = \frac{1}{\omega^{q^2-q+1}}$, i.e.,

$$\omega^{2q} - \omega^2 = (\omega^q - \omega)(\omega^q + \omega) = 0,$$

which leads to $\omega^q + \omega = 0$ due to $\omega \notin \mathbb{F}_q$. Further, we have $\omega^{q^2} = (-\omega)^q = \omega$ and consequently $\omega = \omega^q$, a contradiction to $\omega \notin \mathbb{F}_q$. Therefore, (36) has no solution in $\mathbb{F}_q$. □

Table 1: Known nonlinearized permutation trinomials over $\mathbb{F}_{q^3}$ with coefficients in $\{1, -1\}$

No.	PPs	$q = p^m$	References
1	$x^{\frac{q^2+1}{2}} + x^q - x$	$p = 3$, $m \not\equiv 2 (\mathrm{mod}\, 3)$	[6, Theorem 3.2]
2	$x^{\frac{q^2+1}{2}} - x^q - x$	$p = 3$, $m \not\equiv 2 (\mathrm{mod}\, 3)$	[6, Theorem 3.4]
3	$x^{\frac{q^2+1}{2}} - x^q + x$	$p = 3$, $m \not\equiv 1 (\mathrm{mod}\, 3)$	[6, Theorem 3.6]
4	$x^{\frac{q^2+q^4}{2}} - x^{\frac{q^2+1}{2}} + x$	$p = 3$, $m \not\equiv 2 (\mathrm{mod} 3)$	[28, Table 4]
5	$2x^{\frac{q+q^3}{2}} + x^q + x$	$q \equiv 3 (\mathrm{mod}\, 4)$, m odd	[3, Table 1]
6	$2x^{\frac{q^2+1}{2}} + x^{q^2} + x$	$q \equiv 3 (\mathrm{mod}\, 4)$, m odd	[3, Table 2]
7	$x^{\frac{q^3+q}{2}} + x^{\frac{q^2+1}{2}} - x$	p odd	[16, Theorem 4.1]
8	$x^{q^2+q-1} - x^{q^2-q+1} + x$	$p = 3$, $m \not\equiv 1 (\mathrm{mod}\, 3)$	[27, Theorem 3.1]
9	$-x^{q^2+q-1} + x^{q^2} + x$	$p = 3$, $m \not\equiv 1 (\mathrm{mod}\, 3)$	[27, Theorem 3.2]
10	$x^{q^2+q-1} + x^q - x$	$p = 3$, $m \not\equiv 1 (\mathrm{mod}\, 3)$	[27, Theorem 3.3]
11	$x^{q^2+q-1} - x^{q^3-q^2+q} + x$	$p = 3$, $m \not\equiv 2 (\mathrm{mod}\, 3)$	[27, Theorem 3.4]
12	$-x^{q^2+q-1} + x^q + x$	$p = 3$, $m \not\equiv 2 (\mathrm{mod}\, 3)$	[27, Theorem 3.5]
13	$x^{q^2+q-1} + x^{q^2} - x$	$p = 3$, $m \not\equiv 2 (\mathrm{mod}\, 3)$	[27, Theorem 3.6]

3 QM equivalence

In this section, we compare our permutation polynomials with those in the previous works. Two permutation polynomials $f(x)$ and $g(x)$ in $\mathbb{F}_{p^n}[x]$ are called quasi-multiplicative (QM, for short) equivalent [24] if there exists an integer $1 \leq e \leq p^n - 1$ with $\gcd(e, p^n - 1) = 1$ and $f(x) = \alpha g(\gamma x^e)$, where p is a prime, n is a positive integer and $\alpha, \gamma \in \mathbb{F}_{p^n}^*$. Observe that two QM equivalent permutation polynomials have the same number of terms. Thus, we only need to compare our results with the known permutation trinomials over $\mathbb{F}_{q^3}$ with odd characteristic in Tables 1 and 2 as well as the linearized permutation trinomials of the form $ax^{q^2} + bx^q + cx \in \mathbb{F}_{q^3}[x]$ in [6], [28, Tables 2 and 3] and [3, Tables 1 and 2].

Observe that the monomial x is a term of all the known permutation trinomials over $\mathbb{F}_{q^3}$. Thus we only need to consider the QM equivalence between polynomials $g_i(x) = a_i x^{s_i} + b_i x^{t_i} + c_i x \in \mathbb{F}_{q^3}[x]$ for $i = 1, 2$, where $1 \leq s_i, t_i \leq p^n - 1$. For convenience, denote $E_{\mathrm{mod}\, q^3-1} = \{e (\mathrm{mod}\, q^3 - 1) | e \in E\}$. According to the definition of QM equivalence, $g_1(x)$ is QM equivalent to $g_2(x)$ if and only if the following two conditions are satisfied:

Table 2: Known nonlinearized permutation trinomials over $\mathbb{F}_{q^3}$ with coefficients in $\mathbb{F}_q^*$

No.	PPs	$q = p^m$	References
1	$x^{q^2+q-1} + Ax^{q^2-q+1} + Bx$	$p > 3$	[1, Theorem 3.1]
2	$x^{q^2+q-1} + Ax^{q^3-q^2+q} + Bx$	$p > 3$	[1, Theorem 3.3]
3	$x^{q^2+q-1} + Ax^{q^2} - Bx$	$q \equiv 1 (\mathrm{mod} 3)$, $p > 3$	[1, Theorem 3.4]
4	$x^{q^2+q-1} + Ax^{q} - Bx$	$p > 3$	[1, Theorem 3.5]
5	$x^{q^2-q+1} + Ax^{q^3-q^2+q} + Bx$	p odd	[25, Theorem 3.3]
6	$x^{q^2+q-1} + Ax^{q^2} + Bx$	p odd	[25, Theorem 3.4]
7	$x^{q^2+q-1} + Ax^{q} + Bx$	p odd	[25, Theorem 3.5]

- where $A, B \in \mathbb{F}_q^*$, as specified in references.

(C1) There exists $e \in \{1, s_1, t_1\}$ with $\gcd(e, q^3 - 1) = 1$ such that

$$\{s_1,\, t_1,\, 1\} = \left\{es_2,\, et_2,\, e\right\}_{\mathrm{mod}\, q^3-1}.$$

(C2) For any e in (C1), there exist $\alpha, \gamma \in \mathbb{F}_{p^n}^*$ such that $g_1(x)$ and $\alpha g_2\left(\gamma x^e\right)$'s corresponding coefficients equal each other.

First, according to (C1), through a series of easy computations, it can be verified that

1) $f_1(x)$ and $f_2(x)$ are QM inequivalent to each other;
2) $f_1(x)$ and $f_2(x)$ are QM inequivalent to all known linearized permutation trinomials;
3) $f_1(x)$ is QM inequivalent to Nos. 1-4, 7-13 in Table 1 and Nos. 1-4, 6-7 in Table 2;
4) $f_2(x)$ is QM inequivalent to Nos. 1-6, 8-13 in Table 1 and Nos. 1-7 in Table 2.

Next, we show the inequivalence between $f_1(x)$ and No. 5, $f_1(x)$ and No. 6 in Table 1, $f_1(x)$ and No. 5 in Table 2 as well as $f_2(x)$ and No. 7 in Table 1 by using (C2). Here we only give the proof for the case $f_1(x)$ is QM inequivalent to No. 5 in Table 1 since the other cases can be proved in the same manner.

Let $f_1(x)$ be given by Theorem 1 and $g(x)$ be the No. 5 in Table 1. If $f_1(x)$ is QM equivalent to $g(x)$, then both (C1) and (C2) hold. A direct calculation indicates that $e = q^2 - q + 1$ is the unique integer satisfying (C1). Then (C2) implies that there exist $\alpha, \gamma \in \mathbb{F}_{p^n}^*$ such that

$$f_1(x) = \alpha g\big(\gamma x^{q^2-q+1}\big) = 2\alpha\gamma^{\frac{q^3+q}{2}} x + \alpha\gamma^q x^{q^3-q^2+q} + \alpha\gamma x^{q^2-q+1}$$

i.e., $a = \alpha\gamma^q$, $b = \alpha\gamma$, $2 = 2\alpha\gamma^{\frac{q^3+q}{2}}$, which leads to

$$ab = \alpha^2\gamma^{q+1} = (\alpha\gamma^{\frac{q^3+q}{2}})^2 = 1,\ a^{q^2+q+1} = (\alpha\gamma)^{q^2+q+1} = (\alpha\gamma^{\frac{q^3+q}{2}})^{q^2+q+1} = 1.$$

Thus $f_1(x)$ is QM equivalent to $g(x)$ only when both $ab = 1$ and $a^{q^2+q+1} = 1$. This indicates that No. 5 in Table 1 is a very special case of Theorem 1 and each $f_1(x)$ in Theorem 1 with $(ab, a^{q^2+q+1}) \neq (1, 1)$ is QM inequivalent to No. 5 in Table 1.

Combining above discussions, we can conclude that the proposed two classes of permutation trinomials are QM inequivalent to all known permutation polynomials over $\mathbb{F}_{q^3}$.

4 Conclusion

In this paper, two classes of permutation trinomials over $\mathbb{F}_{q^3}$ with odd characteristic were obtained based on the multivariate method and some techniques in solving equations with low degrees over finite fields, and it was shown that they are QM inequivalent to all known permutation trinomials over $\mathbb{F}_{q^3}$. To our knowledge, our work is the first contribution to the study of nonlinearized permutation trinomials of $\mathbb{F}_{q^3}$ with at least one coefficient in $\mathbb{F}_{q^3} \backslash \mathbb{F}_q$. Our experiments indicate that the sufficient conditions in both Theorem 1 and Theorem 2 are also necessary. However, it seems hard to confirm it in general. The reader is cordially invited to attack this problem.

Acknowledgments

This work was supported by the National Key Research and Development Program of China (No. 2021YFA1000600), the National Natural Science Foundation of China (No. 62072162) and the Natural Science Foundation of Hubei Province of China (No. 2021CFA079).

References

[1] D. Bartoli, Permutation trinomials over $\mathbb{F}_{q^3}$, Finite Fields Appl. 61 (2020) 101597.

[2] A. Blokhuis, R.S. Coulter, M. Henderson, C.M. O'Keefe, Permutations amongst the Dembowski-Ostrom polynomials, in: Finite Fields and Applications, Augsburg, 1999, Springer, Berlin, 2001, pp. 37-42.

[3] X. Cao, L. Hu, New methods for generating permutation polynomials over finite fields, Finite Fields Appl. 17 (6) (2011) 493-503.

[4] L.E. Dickson, The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, Ann. Math. 11 (1986) 65-120.

[5] C. Ding, T. Helleseth, Optimal ternary cyclic codes from monomials, IEEE Trans. Inf. Theory 59 (9) (2013) 5898-5904.

[6] C. Ding, Q. Xiang, J. Yuan, P. Yuan, Explicit classes of permutation polynomials of $\mathbb{F}_{3^{3m}}$, Sci. China Ser. A 52 (2009) 639-647.

[7] C. Ding, J. Yuan, A family of skew Hadamard difference sets, J. Comb. Theory, Ser. A 113 (7) (2006) 1526-1535.

[8] H. Dobbertin, Almost perfect nonlinear power functions on GF(2^n): The Welch case, IEEE Trans. Inf. Theory 45(4) (1999) 1271-1275.

[9] X. Gong, G. Gao, W. Liu, On permutation polynomials of the form $x^{1+2^k} + L(x)$, Int. J. Comput. Math., 93 (10) (2016) 1715-1722.

[10] R. Gupta, R.K. Sharma, Some new classes of permutation trinomials over finite fields with even characteristic, Finite Fields Appl. 41 (2016) 89-96.

[11] Ch. Hermite, Sur les fonctions de sept lettres, C. R. Acad. Sci. Paris 57 (1863) 750-757.

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

[13] X. Hou, A survey of permutation binomials and trinomials over finite fields, in: G. Kyureghyan, G.L. Mullen, A. Pott (Eds.), Topics in Finite Fields, Proceedings of the 11th International Conference on Finite Fields and Their Applications, vol. 632, AMS, 2015, pp. 177-191.

[14] K. Li, L. Qu, X. Chen, New classes of permutation binomials and permutation trinomials over finite fields, Finite Fields Appl. 43 (2017) 69-85.

[15] K. Li, L. Qu, X. Chen, C. Li, Permutation polynomials of the form $cx + \mathrm{Tr}_{q^l/q}(x^a)$ and permutation trinomials over finite fields with even characteristic, Cryptogr. Commun. 10 (67) (2018) 531-554.

[16] J. Ma, T. Zhang, T. Feng, G. Ge, Some new results on permutation polynomials over finite fields, Des. Codes Cryptogr. 83 (2) (2017) 425-443.

[17] S. Mesnager, L. Qu, On two-to-one mappings over finite fields, IEEE Trans. Inf. Theory 65(12) (2019) 7884-7895.

[18] T. Pang, Y. Xu, N. Li, X. Zeng, Permutation polynomials of the form $x^d + L(x^s)$ over $\mathbb{F}_{q^3}$, Finite Fields Appl. 76 (2021) 101906.

[19] Y.H. Park, J.B. Lee, Permutation polynomials and group permutation polynomials, Bull. Aus. Math. Soc. 63 (1) (2001) 67-74.

[20] Z. Tu, X. Zeng, L. H, T. Helleseth, Several classes of complete permutation polynomials, Finite Fields Appl. 25 (2014) 182-193.

[21] Z. Tu, X. Zeng, C. Li, T. Helleseth, A class of new permutation trinomials, Finite Fields Appl. 50 (2018) 178-195.

[22] Q. Wang, Cyclotomic mapping permutation polynomials over finite fields. In: Golomb, S.W., Gong, G., Helleseth, T., Song, H.-Y. (eds.) Sequences, Subsequences, and Consequences, Lect. Notes Comput. Sci., vol. 4893, pp. 119-128. Springer, Berlin (2007).

[23] D. Wan, R. Lidl, Permutation polynomials of the form $x^r f(x^{\frac{q-1}{d}})$ and their group structure, Monatshefte Math. 112 (1991) 149-163.

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

[25] Y. Wang, W. Zhang, D. Bartoli, Q. Wang, Permutation polynomials and complete permutation polynomials over $\mathbb{F}_{q^3}$, arXiv.1806.05712, 2018.

[26] Y. Wang, W. Zhang, Z. Zha, Six new classes of permutation trinomials over $\mathbb{F}_{2^n}$, SIAM J. Discrete Math. 32 (3) (2018) 1946-1961.

[27] Y. Wang, Z. Zha, W. Zhang, Six new classes of permutation trinomials over $\mathbb{F}_{3^{3k}}$, Appl. Algebra Eng. Commun. Comput. 29 (6) (2018) 479-499.

[28] P. Yuan, More explicit classes of permutation polynomials of $\mathbb{F}_{3^{3m}}$, Finite Fields Appl. 16 (2) (2010) 88-95.

[29] M. E. Zieve, On some permutation polynomials over $\mathbb{F}_q$ of the form $x^r h(x^{(q-1)/d}$, Proc. Amer. Math. Soc. 137 (2009) 2209-2216.