Hacettepe Journal of Mathematics & Statistics

Hacet. J. Math. Stat.
Volume 54 (3) (2025), 797 – 806
DOI : 10.15672/hujms.1443686

Research Article

On some permutation trinomials in characteristic three

Burcu Gülmez Temür*[1], Buket Özkaya[2]

[1] *Department of Mathematics, Atılım University, Ankara, Turkey*
[2] *Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey*

Abstract

In this paper, we determine the permutation properties of the polynomial $x^3+x^{q+2}-x^{4q-1}$ over the finite field $\mathbb{F}_{q^2}$ in characteristic three. Moreover, we consider the trinomials of the form $x^{4q-1}+x^{2q+1}\pm x^3$. In particular, we first show that $x^3+x^{q+2}-x^{4q-1}$ permutes $\mathbb{F}_{q^2}$ with $q=3^m$ if and only if m is odd. This enables us to show that the sufficient condition in [34, Theorem 4] is also necessary. Next, we prove that $x^{4q-1}+x^{2q+1}-x^3$ permutes $\mathbb{F}_{q^2}$ with $q=3^m$ if and only if $m\not\equiv 0 \pmod 4$. Consequently, we prove that the sufficient condition in [20, Theorem 3.2] is also necessary. Finally, we investigate the trinomial $x^{4q-1}+x^{2q+1}+x^3$ and show that it is never a permutation polynomial of $\mathbb{F}_{q^2}$ in any characteristic. All the polynomials considered in this work are not quasi-multiplicative equivalent to any known class of permutation trinomials.

Mathematics Subject Classification (2020). 11T06, 11T71, 12E10

Keywords. permutation polynomials, finite fields, absolutely irreducible

1. Introduction

Let $\mathbb{F}_q$ be a finite field with q elements, where q is a prime power. A polynomial $g(x)\in\mathbb{F}_q[x]$ is called a *permutation polynomial (PP)* over $\mathbb{F}_q$ if $g(x)$ is bijective on $\mathbb{F}_q$. Recently, there has been a great interest in permutation polynomials with a few terms, such as binomials or trinomials due to their simple algebraic structure and extraordinary properties. Permutation polynomials are also important because of their applications in areas such as cryptography, coding theory and combinatorial designs. To our knowledge, the studies on permutation polynomials goes back to work done by Dickson and Hermite (see, [9, 12]). In order to get into the topic, the books on finite fields (see, [23] and [24, Chapter 8]) could be very helpful for the interested reader. Furthermore, the survey papers (see, [13, 16, 33]) could also be very useful as they consist of many of the recent results on permutation polynomials over finite fields. We refer the interested reader also to [3,4,11,14,19,21,25] and the references therein for more results on permutation polynomials over finite fields.

In [34, Theorem 4], Wang, Wu, Yue and Zheng studied the trinomial $g(x)=x^{q^2-q+1}-x^{3q-2}+x$ over $\mathbb{F}_{q^2}$ where $q=3^m$ and they showed that if m is odd then $g(x)$ permutes

*Corresponding Author.
Email addresses: burcu.temur@atilim.edu.tr (B. Gülmez Temür), ozkayab@metu.edu.tr (B. Özkaya)
Received: 27.02.2024; Accepted: 11.06.2024

$\mathbb{F}_{q^2}$. In this paper, we first consider $f(x) = x^3 + x^{q+2} - x^{4q-1}$ in characteristic three, where $f(x) = g(x^{q+2})$ (i.e., $f(x)$ is quasi-multiplicative equivalent to $g(x)$) and prove that $f(x)$ is a permutation polynomial of $\mathbb{F}_{q^2}$ if and only if m is odd. Since the polynomial $f(x)$ is quasi-multiplicative equivalent to the polynomial given in Theorem 4 in [34], Theorem 3.2 shows that the condition m being odd is in fact necessary and sufficient.

In [20, Theorem 3.2], Li, Qu, Li and Fu studied the polynomial $h(x) = x - x^{2q-1} + x^{q^2-2q+2}$ over $\mathbb{F}_{q^2}$ where $q = 3^m$ and they showed that if $m \not\equiv 0 \pmod 4$ then $h(x)$ is a permutation polynomial of $\mathbb{F}_{q^2}$. Instead, we consider $f(x) = x^{4q-1} + x^{2q+1} - x^3$ in characteristic three, where $f(x) = h(x^{2q+1})$ (i.e., $f(x)$ is quasi-multiplicative equivalent to $h(x)$ and this polynomial leads to a very much easier proof) and prove that $f(x)$ is a permutation polynomial of $\mathbb{F}_{q^2}$ if and only if $m \not\equiv 0 \pmod 4$. Since the polynomial $f(x)$ is quasi-multiplicative equivalent to the polynomial given in Theorem 3.2 in [20], Theorem 4.1 shows that the condition $m \not\equiv 0 \pmod 4$ is in fact necessary and sufficient. Finally, we consider the trinomial $x^{4q-1}+x^{2q+1}+x^3$ and prove that it is not a permutation polynomial of $\mathbb{F}_{q^2}$ in any characteristic. None of these polynomials are quasi-multiplicative equivalent to any other known class of permutation polynomials.

The paper is organized as follows. Section 2 provides the required background used in the rest of the paper. Section 3 is devoted to the trinomial $x^3 + x^{q+2} - x^{4q-1}$ over $\mathbb{F}_{q^2}$ where $q = 3^m$. In section 4 we study the trinomials of the form $x^{4q-1} + x^{2q+1} \pm x^3$ over $\mathbb{F}_{q^2}$. Finally, in section 5 we investigate the relation of these trinomials with the existing ones and we show that they are not quasi-multiplicative equivalent to any other known class of permutation trinomials.

2. Preliminaries

To determine whether a polynomial which is given in the form $f(x) = x^r h\left(x^{(q^n-1)/d}\right)$ permutes $\mathbb{F}_{q^n}$ or not, mostly a well known criterion due to Wan and Lidl [31], Park and Lee [28], Akbary and Wang [1], Wang [32] and Zieve [35] is being used, which is given in the following lemma.

Lemma 2.1. *[1, 28, 31, 32, 35] Let $h(x) \in \mathbb{F}_{q^n}[x]$ and d, r be positive integers with d dividing $q^n - 1$. Then $f(x) = x^r h\left(x^{(q^n-1)/d}\right)$ permutes $\mathbb{F}_{q^n}$ if and only if the following conditions hold:*

(i) $\gcd(r, (q^n-1)/d) = 1$,
(ii) $x^r h(x)^{(q^n-1)/d}$ *permutes* μ_d, *where* $\mu_d = \{\theta \in \mathbb{F}_{q^n}^* \mid \theta^d = 1\}$.

In this paper, we plan to apply Lemma 2.1 over the finite field $\mathbb{F}_{q^2}$ with $d = q + 1$ and $r = 3$. Condition (i) of Lemma 2.1 holds as long as $\gcd(r, (q^n - 1)/d) = \gcd(3, q - 1) = 1$. Instead of finding the conditions for which $g(x) = x^r h(x)^{q-1}$ permutes μ_{q+1}, we will use the following idea throughout the paper:

Let $z \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ be an arbitrary element. For any $x \in \mathbb{F}_q$, let $\phi\colon \mathbb{F}_q \cup \{\infty\} \longrightarrow \mu_{q+1}$ be the map defined by $\phi(x) = \dfrac{x+z}{x+z^q}$, where $\phi(\infty) = 1$. It is not so hard to observe that ϕ is one to one from $\mathbb{F}_q \cup \{\infty\}$ to μ_{q+1} and thus onto since the number of elements on both sides are equal. Then we obtain that $\phi^{-1}(x) = \dfrac{xz^q - z}{1 - x}$, for any $x \neq 1$ with $\phi^{-1}(1) = \infty$. In this setting, we have $g(x) = x^r h(x)^{q-1}$ is one to one on μ_{q+1} and therefore permutes μ_{q+1} if and only if the map $(\phi^{-1} \circ g \circ \phi)$ is one to one on $\mathbb{F}_q \cup \{\infty\}$. In Theorem 3.2 and Theorem 4.1, we will always have $g(1) = 1$ when $h(1) \neq 0$. Then ∞ is a fixed-point of the map $(\phi^{-1} \circ g \circ \phi)$, and it suffices to investigate its action on $\mathbb{F}_q$. We note that an analogous idea has been used in a few more studies before, see for instance [3, 25–27].

This situation can be easily followed in the diagram below:

$$\begin{array}{ccc} \mathbb{F}_q \cup \{\infty\} & \xrightarrow{\phi^{-1}\circ g\circ \phi} & \mathbb{F}_q \cup \{\infty\} \\ \downarrow \phi & & \uparrow \phi^{-1} \\ \mu_{q+1} & \xrightarrow{\quad g \quad} & \mu_{q+1} \end{array} \tag{2.1}$$

Moreover, we will make a suitable choice of the element $z \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ that results in simpler computations.

The following definition will be needed in Sections 3, 4 and 5.

Definition 2.2. [30] Two permutation polynomials $f(x), g(x) \in \mathbb{F}_q[x]$ are said to be quasi-multiplicative (QM) equivalent, if there exists $d \in \mathbb{Z}$, $1 \leq d \leq q-1$ with $\gcd(d, q-1) = 1$ and $f(x) = ag(cx^d) \pmod{x^q - x}$, where $a, c \in \mathbb{F}_q^*$. If $c = 1$, then $f(x), g(x) \in \mathbb{F}_q[x]$ are called multiplicative equivalent.

The notion of QM equivalence defined above can be rephrased in algebraic terms as follows: $f(x), g(x) \in \mathbb{F}_q[x]$ are said to be QM equivalent, if there exists $h_1(x) = ax, h_2(x) = cx^d \in \mathbb{F}_q[x]$ such that $f(x) = (h_1 \circ g \circ h_2)(x) \pmod{x^q - x}$, where $d \in \mathbb{Z}$, $1 \leq d \leq q-1$ with $\gcd(d, q-1) = 1$ and $a, c \in \mathbb{F}_q^*$.

3. Permutation Trinomials of the form $x^3 + x^{q+2} - x^{4q-1}$ over $\mathbb{F}_{q^2}$, where $q = 3^m$

Wang, Wu, Yue and Zheng considered polynomials of the form $x^{q^2-q+1} - x^{3q-2} + x$ in characteristic three (see, [34, Theorem 4]). Inspired by their results, we take $f(x) = x^3 + x^{q+2} - x^{4q-1}$ and we determine all the necessary and sufficient conditions so that $f(x)$ permutes $\mathbb{F}_{q^2}$.

Observe that $f(x) = x^3 h(x^{q-1})$, where $h(x) = -x^4 + x + 1$. We will apply Lemma 2.1, therefore we first note that $\gcd(3, q-1) = 1$ when $q = 3^m$. Then, we need to determine the roots of $h(x)$ in μ_{q+1}. Note that $\mu_{q+1} \cap \mathbb{F}_q = \{1, -1\}$ and we already have $h(1) = h(-1) = 1 \neq 0$. Next, we will use the method in [10] to investigate whether $h(x)$ has roots in $\mu_{q+1} \setminus \{1, -1\}$ or not. For this, we need the following Lemma.

Lemma 3.1. *[10, Lemma 2] The polynomial $h(x)$ has a root in $\mu_{q+1} \setminus \{1, -1\}$ if and only if there exists $A \in \mathbb{F}_q$ such that $m(x) = x^2 + Ax + 1$ is irreducible over $\mathbb{F}_q$ and $m(x)$ divides $h(x)$.*

Proof. The set $\mu_{q+1} \setminus \{1, -1\}$ contains exactly the elements $\theta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ with $\theta^{q+1} = 1$.

Let $\theta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ be such that $h(\theta) = 0$ and $\theta^{q+1} = 1$. As $h(x)$ is a polynomial over $\mathbb{F}_q$, θ^q is another root of $h(x)$. Then $m(x) = (x-\theta)(x-\theta^q) = x^2 - (\theta + \theta^q) + \theta^{q+1} = x^2 + Ax + 1$ divides $h(x)$. Moreover $m(x)$ is the minimal polynomial of θ over $\mathbb{F}_q$ and hence irreducible.

For the converse, assume that an irreducible polynomial $m(x) = x^2 + Ax + 1$ divides $h(x)$. The roots θ_1 and θ_2 of $m(x) = (x-\theta_1)(x-\theta_2)$ are roots of $h(x)$ as well. As $m(x)$ is irreducible, the roots lie in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and they are conjugates, i.e., $\theta_2 = \theta_1^q$. From the constant coefficient of $m(x)$ we find $1 = \theta_1\theta_2 = \theta_1^{q+1}$. □

One can easily verify that if $h(x)$ decomposes as $h(x) = -x^4 + x + 1 = (x^2 + Ax + 1)(-x^2 + ax + b)$, then by comparing the corresponding coefficients we obtain a contradiction from the equalities $a - A = 0$, $A + a = 1$ and $Aa = 0$. Hence, $h(x)$ has no roots in μ_{q+1}.

Now, for any $x \in \mu_{q+1}$ (that is, $x^{q+1} = 1$ which implies that $x^q = 1/x$), we have the following:

$$x^3 h(x)^{q-1} = x^3 \frac{h(x)^q}{h(x)} = \frac{x^3(1 + x^q - x^{4q})}{1 + x - x^4} = \frac{x^3\left(1 + \frac{1}{x} - \frac{1}{x^4}\right)}{1 + x - x^4} = \frac{x^4 + x^3 - 1}{-x^5 + x^2 + x}.$$

Now, let $g(x) = \dfrac{x^4+x^3-1}{-x^5+x^2+x}$, $\phi(x) = \dfrac{x+z}{x+z^q}$ and thus $\phi^{-1}(x) = \dfrac{xz^q-z}{1-x}$, where $z \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Then we have

$$\begin{aligned}(g\circ\phi)(x) &= \frac{\left(\frac{x+z}{x+z^q}\right)^4+\left(\frac{x+z}{x+z^q}\right)^3-1}{-\left(\frac{x+z}{x+z^q}\right)^5+\left(\frac{x+z}{x+z^q}\right)^2+\left(\frac{x+z}{x+z^q}\right)} \\ &= \frac{(x+z)^4(x+z^q)+(x+z)^3(x+z^q)^2-(x+z^q)^5}{-(x+z)^5+(x+z)^2(x+z^q)^3+(x+z)(x+z^q)^4} \qquad (3.1)\end{aligned}$$

Here, we observe that if we define the numerator of (3.1) as $\Delta(z,x)$, that is,

$$\Delta(z,x) := (x+z)^4(x+z^q)+(x+z)^3(x+z^q)^2-(x+z^q)^5,$$

then the denominator of (3.1) of (3.1) is

$$\Delta(z^q,x) = -(x+z)^5+(x+z)^2(x+z^q)^3+(x+z)(x+z^q)^4,$$

since $z \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, that is, we can write $(g\circ\phi)(x) = \dfrac{\Delta(z,x)}{\Delta(z^q,x)}$. Then

$$(\phi^{-1}\circ g\circ\phi)(x) = \phi^{-1}\left(\frac{\Delta(z,x)}{\Delta(z^q,x)}\right) = \frac{z^q\Delta(z,x)-z\Delta(z^q,x)}{\Delta(z^q,x)-\Delta(z,x)}. \qquad (3.2)$$

Here, let us define the numerator of (3.2) as $N := z^q\Delta(z,x)-z\Delta(z^q,x)$ and the denominator of (3.2) as $D := \Delta(z^q,x)-\Delta(z,x)$. Choosing $z^q = -z$, that is, z is the square root of a nonsquare in $\mathbb{F}_q$ and computing N, D by substituting $z^q = -z$ we obtain that

$$N = z^5\left(\frac{1}{z^4}x^5+\frac{2}{z^2}x^3+2x\right) \text{ and } D = z^5.$$

Thus,

$$(\phi^{-1}\circ g\circ\phi) = \frac{1}{z^4}x^5+\frac{2}{z^2}x^3+2x. \qquad (3.3)$$

The following theorem is our first main result.

Theorem 3.2. *Let $q = 3^m$, $m \in \mathbb{N}$. The polynomial $f(x) = x^3+x^{q+2}-x^{4q-1}$ permutes $\mathbb{F}_{q^2}$ if and only if m is odd.*

Proof. Note that, by Lemma 2.1 we have to prove that $g(x) = x^3h(x)^{q-1}$ permutes the set μ_{q+1}. Here, we apply the idea we explained in the preliminaries section and hence show that $(\phi^{-1}\circ g\circ\phi)$ permutes $\mathbb{F}_q$. For this purpose, using (3.3), we consider the curve obtained by computing

$$\begin{aligned}\frac{(\phi^{-1}\circ g\circ\phi)(x)-(\phi^{-1}\circ g\circ\phi)(y)}{x-y} &= \frac{\left(\frac{1}{z^4}x^5+\frac{2}{z^2}x^3+2x\right)-\left(\frac{1}{z^4}y^5+\frac{2}{z^2}y^3+2y\right)}{x-y} \\ = \frac{1}{z^4}(x^4+y^4)+\frac{1}{z^4}(x^3y+x^2y^2+xy^3)+\frac{2}{z^2}(x^2+xy+y^2)+2. \qquad (3.4)\end{aligned}$$

Here, since $z \neq 0$ (as $z \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$), multiplying (3.4) by z^4 we can instead consider

$$C(x,y) = x^4+y^4+x^3y+x^2y^2+xy^3+A(x^2+xy+y^2)+B, \qquad (3.5)$$

where $A = -z^2$ and $B = -z^4$. Note that, we have $B = -A^2$.

First, we deal with the absolutely irreducible case. A curve defined over a finite field $\mathbb{F}_q$ is absolutely irreducible if it is irreducible over every algebraic extension of $\mathbb{F}_q$. Note that the underlying idea here is first of all estimating the number of $\mathbb{F}_q$-rational points of the curve $C(x,y)$ in (3.5) above. For this purpose, one can use Hasse-Weil type bounds. In this

paper, we use [17, Theorem 5.28], which involves a bound obtained from the Hasse-Weil bound.

Assume that $C(x,y)$ is absolutely irreducible. Homogenizing $C(x,y)$ in (3.5) with $x=\frac{X}{Z}$ and $y=\frac{Y}{Z}$ we obtain a homogeneous polynomial of degree $d=4$. Let $\widetilde{C}(X,Y,Z)\in \mathbb{F}_q[X,Y,Z]$ be the homogeneous polynomial defined as

$$\widetilde{C}(X,Y,Z)=Z^4C\left(\frac{X}{Z},\frac{Y}{Z}\right).$$

Let $\mathbb{P}^2(\mathbb{F}_q)$ denote the projective space consisting of projective coordinates $(X:Y:Z)$. Let $N=|\{(x,y)\in\mathbb{F}_q\times\mathbb{F}_q \mid C(x,y)=0\}|$ be the number of affine $\mathbb{F}_q$-rational points of C. Let $V=|\{(X:Y:Z)\in\mathbb{P}^2(\mathbb{F}_q) \mid \widetilde{C}(X,Y,Z)=0\}|$ be the number of projective $\mathbb{F}_q$-rational points of $\widetilde{C}$. Let V_0 and V_1 be the number of projective $\mathbb{F}_q$-rational points of $\widetilde{C}$ corresponding to the cases $Z=0$ and $Z\neq 0$. Namely,

$$V_0=|\{(X:Y:0)\in\mathbb{P}^2(\mathbb{F}_q) \mid \widetilde{C}(X,Y,0)=0\}|$$
$$\text{and}\qquad V_1=|\{(X:Y:1)\in\mathbb{P}^2(\mathbb{F}_q) \mid \widetilde{C}(X,Y,1)=0\}|.$$

It follows from the definitions that $N=V_1$ and $V=V_0+V_1$. Moreover it follows from (3.5) that $\widetilde{C}(X,Y,0)=X^4+Y^4+X^3Y+X^2Y^2+XY^3$. Note that, when $X=0$ or $Y=0$, $\widetilde{C}(X,Y,0)\neq 0$. On the other hand, when $X=1$ we have

$$\widetilde{C}(1,Y,0)=Y^4+Y^3+Y^2+Y+1=\frac{Y^5-1}{Y-1}.$$

This implies that we have $V_0=0$ or $V_0=4$. The latter case happens whenever $\mathbb{F}_q$ contains 5'th roots of unity. Thus, V can be at most $N+4$. Using [17, Theorem 5.28] we get

$$|V-q|\leq (d-1)(d-2)q^{1/2}+c(d)=6q^{1/2}+19, \tag{3.6}$$

where $c(d)=\frac{1}{2}d(d-1)^2+1$ and $d=4$. The arguments above imply that

$$|N-q|\leq|(V-q)-4|\leq|V-q|+4\leq(d-1)(d-2)q^{1/2}+c(d)+4=6q^{1/2}+23.$$

Note that

$$|\{(x,y)\in\mathbb{F}_q^2 \mid C(x,y)=0 \text{ and } x=y\}|\leq 4$$

as $C(x,x)$ is a polynomial of degree 4 in $\mathbb{F}_q[x]$. Therefore, if $q-6q^{1/2}-23>4$, then $C(x,y)$ has an affine point off the line $x=y$. As q is a prime power, we note that $q-6q^{1/2}-23>4$ for any such q provided that $q\geq 82$. As a result, we deduce that $f(x)$ is not a permutation polynomial of $\mathbb{F}_{q^2}$ if $C(x,y)$ is absolutely irreducible and $q\geq 82$. It remains to consider $q<82$. Now, since characteristic of $\mathbb{F}_q$ is 3, we need to consider only $q\in\{3,9,27,81\}$. Using MAGMA [5] we observe that $f(x)$ permutes $\mathbb{F}_{3^2}$ and $\mathbb{F}_{27^2}$ but not $\mathbb{F}_{9^2}$ and $\mathbb{F}_{81^2}$.

Next, we must check all decompositions of the bivariate polynomial $C(x,y)$ in (3.5) into absolutely irreducible factors in $\overline{\mathbb{F}}_q$, where $\overline{\mathbb{F}}_q$ stands for an algebraic closure of the finite field $\mathbb{F}_q$. Since the degree of the bivariate polynomial in (3.5) is 4, the possibilities are: $3+1$ decomposition, $2+2$ decomposition, $2+1+1$ decomposition and $1+1+1+1$ decomposition according to the degrees of the possible factors.

First assume that $C(x,y)$ is decomposed in the following form:

$$(x^3+\alpha_1x^2y+\alpha_2xy^2+\alpha_3y^3+\alpha_4x^2+\alpha_5xy+\alpha_6y^2+\alpha_7x+\alpha_8y+\alpha_9)(x+\beta_1y+\beta_2). \tag{3.7}$$

The idea here is to compute the above product and compare the coefficients of it with the corresponding coefficients in $C(x,y)$. In order to apply this idea, we use the notion of Gröbner bases (see for instance [7]) using the computer algebra program MAGMA [5]. Namely, we subtract the product in (3.7) from the bivariate polynomial $C(x,y)$ given in (3.5) and then we compute a Gröbner basis of the ideal generated by the coefficients of this difference. By this computation we obtain $A=0$, $B=0$ which gives a contradiction

since $A = -z^2, B = -z^4$ and $z \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and thus $z \neq 0$. Thus, $C(x, y)$ can not be decomposed in this form. Note that, we obtain exactly the same contradiction in the following decompositions of $C(x, y)$:

(i) $(x^2 + \alpha_1 xy + \alpha_2 y^2 + \alpha_3 x + \alpha_4 y + \alpha_5)(x + \beta_1 y + \beta_2)(x + \gamma_1 y + \gamma_2)$,
(ii) $(x + \alpha_1 y + \alpha_2)(x + \beta_1 y + \beta_2)(x + \gamma_1 y + \gamma_2)(x + \delta_1 y + \delta_2)$.

Now, assume that $C(x, y)$ is decomposed in the following form:

$$(x^2 + \alpha_1 xy + \alpha_2 y^2 + \alpha_3 x + \alpha_4 y + \alpha_5)(x^2 + \beta_1 xy + \beta_2 y^2 + \beta_3 x + \beta_4 y + \beta_5). \tag{3.8}$$

We again compute a Gröbner basis of the ideal generated by the coefficients of the difference between the above product and $C(x, y)$ given in (3.5) and obtain $\alpha_3 = \alpha_4 = \beta_3 = \beta_4 = 0$, $\alpha_2 = \beta_2 = 1$ and the following equalities:

$$\begin{aligned} \alpha_1 + \beta_1 &= 1, && (3.9)\\ \alpha_1\beta_1 &= -1, && (3.10)\\ \alpha_5 + \beta_5 &= A, && (3.11)\\ \alpha_1\beta_5 + \alpha_5\beta_1 &= A, && (3.12)\\ \alpha_5\beta_5 &= B. && (3.13) \end{aligned}$$

Combining (3.9) and (3.10) we obtain that α_1 and β_1 are the roots of $x^2 - x - 1$ and thus $\alpha_1, \beta_1 \in \mathbb{F}_9$.

Suppose that $x^2 + \alpha_1 xy + y^2 + \alpha_5 = 0$, for some $x, y \in \mathbb{F}_q$, then together with its q-th power we get the following system of equations

$$\begin{aligned} x^2 + \alpha_1 xy + y^2 + \alpha_5 &= 0,\\ x^2 + \alpha_1^q xy + y^2 + +\alpha_5^q &= 0. \end{aligned}$$

Computing the difference of the equations in the above system we get

$$(\alpha_1 - \alpha_1^q)xy + (\alpha_5 - \alpha_5^q) = 0. \tag{3.14}$$

Now, if $\alpha_1 \in \mathbb{F}_q$, then $\alpha_5 \in \mathbb{F}_q$ by (3.14) and so each pair $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ becomes a solution. Hence $\alpha_1 \notin \mathbb{F}_q$. But we already know that $\alpha_1 \in \mathbb{F}_9$ therefore $\alpha_1 \notin \mathbb{F}_q$ if and only if m is odd.

Next, if $\alpha_5 \in \mathbb{F}_q$, then the solutions of (3.14) are either on the line $x = 0$ or $y = 0$, therefore we need $\alpha_5 \notin \mathbb{F}_q$. Substituting $\beta_5 = \frac{B}{\alpha_5}$ (by (3.13)) in (3.11) yields $\alpha_5^2 - A\alpha_5 + B = 0$. Note that $A, B \in \mathbb{F}_q$, where $B = -A^2$. The discriminant of $x^2 - Ax + B$ is $A^2 - 4B = -5B = B$. Hence $\alpha_5 \notin \mathbb{F}_q$ if and only if $B = -z^4$ is a nonsquare in $\mathbb{F}_q$. Since we have $z^2 \in \mathbb{F}_q$ as $A \in \mathbb{F}_q$, clearly z^4 is a square in $\mathbb{F}_q$. Therefore, $\alpha_5 \notin \mathbb{F}_q$ if and only if -1 is a nonsquare in $\mathbb{F}_q$, which occurs if and only if m is odd.

Similarly, if $x^2 + \beta_1 xy + y^2 + \beta_5 = 0$, then we require $\beta_1, \beta_5 \notin \mathbb{F}_q$ which happens if and only if m is odd. □

Remark 3.3. Since the polynomial $f(x)$ is QM equivalent to the polynomial given in Theorem 4 in [34], Theorem 3.2 above shows that the condition m being odd is in fact necessary and sufficient.

4. Permutation Trinomials of the form $x^{4q-1} + x^{2q+1} \pm x^3$ over $\mathbb{F}_{q^2}$

Li, Qu, Li and Fu [20] studied the polynomial $g(x) = x - x^{2q-1} + x^{3-2q}$ over $\mathbb{F}_{q^2}$ where $q = 3^m$ and they showed that $g(x)$ is a permutation polynomial of $\mathbb{F}_{q^2}$ if $m \not\equiv 0 \pmod 4$. Instead of studying this polynomial directly, we first consider $f(x) = x^{4q-1} + x^{2q+1} - x^3$ in characteristic three, where $f(x)$ is QM equivalent to $g(x)$ by $f(x) = g(x^{2q+1})$.

It is easy to observe that $f(x) = x^3 h(x^{q-1})$, where $h(x) = x^4 + x^2 - 1$. Note that $\gcd(3, q-1) = 1$ in characteristic three. We will apply Lemma 2.1, therefore we first need to determine the roots of $h(x)$ in μ_{q+1}. First, note that $h(1) = h(-1) = 1 \neq 0$. Next, we

will use Lemma 3.1 to ensure that $h(x)$ has no roots in $\mu_{q+1} \setminus \{1, -1\}$. One can easily verify that $h(x) = x^4 + x^2 - 1 = (x^2 + Ax + 1)(x^2 + ax + b)$ yields $b = -1$, $Aa = 1$ and $A = a = 0$, which is clearly a contradiction. Hence, $h(x)$ has no roots in μ_{q+1}.

Now, for any $x \in \mu_{q+1}$, we have:

$$x^3 h(x)^{q-1} = x^3 \frac{h(x)^q}{h(x)} = x^3 \frac{(x^4 + x^2 - 1)^q}{x^4 + x^2 - 1} = \frac{x^3(\frac{1}{x^4} + \frac{1}{x^2} - 1)}{x^4 + x^2 - 1} = \frac{-x^4 + x^2 + 1}{x^5 + x^3 - x}.$$

Let $g(x) = \dfrac{-x^4 + x^2 + 1}{x^5 + x^3 - x}$, $\phi(x) = \dfrac{x + z}{x + z^q}$ and $\phi^{-1}(x) = \dfrac{xz^q - z}{1 - x}$, where z is an arbitrary element in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Then we obtain the following:

$$(\phi^{-1} \circ g \circ \phi)(x) = \frac{z^q \Delta(z, x) - z\Delta(z^q, x)}{\Delta(z^q, x) - \Delta(z, x)}, \tag{4.1}$$

where $\Delta(z, x) = -(x + z)^4(x + z^q) + (x + z)^2(x + z^q)^3 + (x + z^q)^5$ and thus $\Delta(z^q, x) = (x + z)^5 + (x + z)^3(x + z^q)^2 - (x + z)(x + z^q)^4$.

Now let $z^q = -z$. Then the numerator in equation (4.1) is $N(x) = x^5$ and the denominator is $D(x) = -z^4$. Recall that $q = 3^m$ and it is a well-known fact that the monomial x^5 permutes $\mathbb{F}_q$ if and only if $\gcd(5, q - 1) = 1$. One can easily show that $5 \mid 3^m - 1$ if and only if $m \equiv 0 \pmod 4$. Therefore, we obtain the following theorem.

Theorem 4.1. *Let $\mathbb{F}_q$ be a finite field of characteristic three such that $q = 3^m$ and let $h(x) = x^4 + x^2 - 1$. Then $f(x) = x^3 h(x^{q-1})$ is a permutation polynomial of $\mathbb{F}_{q^2}$ if and only if $m \not\equiv 0 \pmod 4$.*

Remark 4.2. Since the polynomial $f(x)$ is QM equivalent to the polynomial given in Theorem 3.2 in [20], Theorem 4.1 above shows that the condition $m \not\equiv 0 \pmod 4$ is in fact necessary and sufficient.

Now we make a slight change by taking $h(x) = x^4 + x^2 + 1$ and we consider $f(x) = x^3 h(x^{q-1})$. We need the following lemma.

Lemma 4.3. *Let p be an odd prime, with $p \neq 3$. Let $q = p^s$, $s \geq 1$ and assume that $\gcd(3, q - 1) = 1$. Then s is odd and -3 is a nonsquare in $\mathbb{F}_q$.*

Proof. First let $p \equiv 1 (\mathrm{mod}\, 3)$. Then $p^s \equiv 1 (\mathrm{mod}\, 3)$ and hence 3 divides $q - 1$ which contradicts $\gcd(3, q - 1) = 1$. Therefore, $p \equiv 2 \pmod 3$. Then, $p^s \equiv (-1)^s \pmod 3$ and hence s is odd. Moreover, as s is odd and $-3 \in \mathbb{F}_p$, -3 is a nonsquare in $\mathbb{F}_q$ if and only if -3 is a nonsquare in $\mathbb{F}_p$. Note that 3 and p are distinct odd primes. Using the Law of Quadratic Reciprocity (see for instance, [23, Theorem 5.17]) we have

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{\frac{(3-1)(p-1)}{4}}. \tag{4.2}$$

Here, for an integer x with $x \not\equiv 0 \pmod p$, recall that the Legendre symbol (see for instance, [23]) is defined as

$$\left(\frac{x}{p}\right) = \begin{cases} -1, & \text{if } x \text{ is not a square mod } p, \\ 1, & \text{if } x \text{ is a square mod } p. \end{cases}$$

Moreover, it is well known that (see for instance, [23]),

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \text{ and } \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right). \tag{4.3}$$

Combining (4.2) and (4.3) we conclude that

$$\left(\frac{-3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)(-1)^{\frac{(p-1)(3-1)}{4}} = \left(\frac{2}{3}\right) = -1, \tag{4.4}$$

where we use the fact that $p \equiv 2 \pmod 3$. This completes the proof. □

Now given that $h(x) = x^4+x^2+1$, it can be verified that $h(x) = (x^2+x+1)(x^2-x+1)$. First, let q be odd with $\gcd(3, q-1) = 1$. Then, $h(x)$ has no roots in μ_{q+1} if and only if $h(x)$ splits into linear factors over $\mathbb{F}_q$, that is, -3 must be a square in $\mathbb{F}_q$. If $char(\mathbb{F}_q) \neq 3$, then -3 is never a square in $\mathbb{F}_q$ by Lemma 4.3, as $\gcd(3, q-1) = 1$. If $char(\mathbb{F}_q) = 3$, then $h(1) = h(-1) = 0$. Hence, this $h(x)$ has always roots in μ_{q+1} in odd characteristic. When q is even, we have $h(x) = (x^2+x+1)^2$. Note that the condition $\gcd(3, q-1) = 1$ forces q to be an odd power of 2. But then x^2+x+1 becomes irreducible over $\mathbb{F}_q$ and Lemma 3.1 implies that $h(x)$ has a root in $\mu_{q+1} \setminus \{1, -1\}$. When we combine all these observations, we obtain the following nonexistence result.

Theorem 4.4. *Let $\mathbb{F}_q$ be any finite field and let $h(x) = x^4+x^2+1$. Then $f(x) = x^3h(x^{q-1})$ is never a permutation polynomial of $\mathbb{F}_{q^2}$.*

5. Comparison with existing permutation polynomials

In this section, we show that the permutation trinomials considered in this paper are not QM equivalent to the known classes. We first observe that two QM equivalent permutations must have exactly the same number of terms. Therefore, we only need to compare the permutation polynomials found in this paper with known permutation trinomials over $\mathbb{F}_{q^2}$. We use the method in [30] for this purpose.

In order to determine whether the permutation trinomial $f(x) = x^3 + x^{q+2} - x^{4q-1}$ is QM equivalent to any permutation trinomial of the form $g(x) = a_1x^{s_1} + a_2x^{s_2} + a_3x^{s_3}$, we will use the following strategy:
Step 1: Determining whether there exists an integer k, $1 \leq k \leq q^2-1$, such that $\gcd(k, q^2-1) = 1$ and $\{ks_1, ks_2, ks_3\} \equiv \{3, q+2, 4q-1\} \bmod (q^2-1)$.
Step 2: Comparison of the coefficients of $f(x)$ and $b_2g(b_1x^k)$.
In the above strategy, if Step 1 is not satisfied, then $f(x)$ and $g(x)$ are not QM equivalent. Otherwise, we continue with Step 2 and compare the coefficients of $f(x)$ and $b_2g(b_1x^k)$.

The same procedure is repeated for $x^{4q-1} + x^{2q+1} - x^3$. Relying on [**?**, 13], we consider the trinomials given in Table 1 below. We applied the method in [30] described above using MAGMA [5] and we have verified that the trinomials considered in this paper are not QM equivalent to any of them. To the best of our knowledge, the list in Table 1 below is complete.

In this paper, we completely characterized the permutation properties of the trinomials $x^3+x^{q+2}-x^{4q-1}$ and $x^{4q-1}+x^{2q+1}\pm x^3$ over the finite field $\mathbb{F}_{q^2}$ in characteristic three. We would like to note that for $q > 3$, one obtains higher degree curves from $(\phi^{-1} \circ g \circ \phi)(x)$ and therefore the computations are more involved. We invite the interested reader to study the permutation properties of these trinomials in other odd characteristics when $q > 3$.

Acknowledgment. We would like to thank Ferruh Özbudak for his valuable suggestions and comments.

References

[1] A. Akbary and Q. Wang, *On polynomials of the form $x^r f(x^{(q-1)/l})$*, Int. J. Math. Math. Sci., Art. ID 23408, 2007.
[2] T. Bai and Y. Xia, *A new class of permutation trinomials constructed from Niho exponents*, Cryptogr. Commun. **10**, 1023-1036, 2018.
[3] D. Bartoli and M. Giulietti, *Permutation polynomials, fractional polynomials, and algebraic curves*, Finite Fields Appl. **51**, 1-16, 2018.
[4] D. Bartoli and M. Timpanella, *A family of permutation trinomials over $\mathbb{F}_{q^2}$*, Finite Fields Appl. **70**, 101781, 2021.

$g(x)$	q	Conditions	Reference
$ax + bx^q + x^{2q-1}$	odd		[15]
$ax^{q^2-q+1} + a^q x^q + (a^{q+1} + 1)x$	any		[18]
$a^q x^{kq(q-1)+1} + ax^{k(q-1)+1} + cx$	any	$\gcd(k, q+1) = 1$	[22]
$ax^{s_1(q-1)+1} + bx^{s_2(q-1)+1} + cx$	any	$(s_1, s_2) \in \{(-1, 2), (-1, 1), (1, 2)\}$	[22]
$x + x^{3q-2} - x^{q^2-q+1}$	3^m		[20]
$x^{\ell q+\ell+1} + x^{(\ell+3)q+\ell-2} - x^{(\ell-1)q+\ell+2}$	3^m	$\gcd(2\ell + 1, q - 1) = 1$	[20]
$x^{\ell q+\ell+5} + x^{(\ell+5)q+\ell} - x^{(\ell-1)q+\ell+6}$	3^m	$\gcd(2\ell + 5, q - 1) = 1$	[20]
$x^{\ell q+\ell+1} + x^{(\ell+4)q+\ell-3} - x^{(\ell-2)q+\ell+3}$	3^m	$\gcd(2\ell + 1, q - 1) = 1$	[20]
$x^{4q-3} + x^{q^2-2q+2} - x$	3^m	$m \not\equiv 0 \pmod 6$	[8]
$x^{k(q-1)+1} + x^{-k(q-1)+1} - x$	3^m		[34]
$x^{4q-3} - x^{q^2-2q+2} + x$	3^m	$m \equiv 0 \pmod 4$	[34]
$x^{s(q-1)+1} - x^{t(q-1)+1} + x$	3^m	$(s, t) \in \{(\frac{3q+4}{7}, \frac{4q+10}{7}), (\frac{2q+3}{7}, \frac{5q+11}{7}), (\frac{4q+5}{7}, \frac{3q+9}{7})\}$	[34]
$ax^{q(q-1)+1} + bx^{2(q-1)+1} + x$	odd		[29]
$x + ax^{s(q-1)+1} + ax^{t(q-1)+1}$	odd	$s = \frac{q-1}{2}, t = \frac{q+3}{2}$	[6]
$x^r(1 + x^{2(q-1)} + cx^{\frac{q+3}{2}(q-1)}$	any	$\gcd(r, q-1) = \gcd(r-2, q+1) = 1$	[6]
$x^{(p-1)q+1} + x^{pq} - x^{q+(p-1)}$	$3^m, 5^m$		[2]
$x^{(q+1)\ell}(x^{(p-1)q+1} + x^{pq} - x^{q+(p-1)})$	$3^m, 5^m$	$\gcd(2\ell + p, q - 1) = 1$	[2]
$x^{3q} + bx^{q+2} + cx^3$	any	$\gcd(3, q - 1) = 1$	[25]

Table 1. The known permutation trinomials of $\mathbb{F}_{q^2}$.

[5] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24**, 1179-1260, 1997.

[6] X. Cao, X. Hou, J. Mi and S. Xu, *More permutation polynomials with Niho exponents which permute* $\mathbb{F}_{q^2}$, Finite Fields Appl. **62**, 101626, 2020.

[7] D. Cox, D. Little and D. O'Shea, *Ideals, Varieties, and Algorithms, An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Undergraduate Texts in Mathematics, Springer, Cham, 2015.

[8] H. Deng and D. Zheng, *More classes of permutation trinomials with Niho exponents*, Cryptogr. Commun. **11**, 227-236, 2019.

[9] 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**, 65-120, 1896.

[10] M. Grassl, F. Özbudak, B. Özkaya and B. Gülmez Temür, *Complete Characterization of a Class of Permutation Trinomial in Characteristic Five*, to appear in Cryptogr. Commun., DOI: |https://doi.org/10.1007/s12095-024-00705-2.

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

[12] C. Hermite, *Sur les fonctions de sept lettres*, C.R. Acad. Sci. Paris **57**, 750-757, 1863.

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

[14] X. Hou, *Determination of a type of permutation trinomials over finite fields*, Acta Arith. **166** (3), 253-278, 2014.

[15] X. Hou, *Determination of a type of permutation trinomials over finite fields, II*, Finite Fields Appl. **35**, 16-35, 2015.

[16] X. Hou, *A survey of permutation binomials and trinomials over finite fields (English summary)*, Topics in finite fields, 177-191, Contemp. Math. **632**, Amer. Math. Soc., Providence, RI, 2015.

[17] X. Hou, *Lectures on finite fields*, Graduate Studies in Mathematics, **190**, American Mathematical Society, Providence, RI, 2018.

[18] L. Li, C. Li, C. Li and X. Zeng, *New classes of complete permutation polynomials*, Finite Fields Appl. **55**, 177-201, 2019.

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

[20] K. Li, L. Qu, C. Li and S. Fu, *New Permutation Trinomials Constructed from Fractional Polynomials*, Acta Arith. **183**, 101-116, 2018.

[21] K. Li, L. Qu and Q. Wang, *New constructions of permutation polynomials of the form* $x^r h(x^{q-1})$ *over* $\mathbb{F}_{q^2}$, Des. Codes Cryptogr. **86**, 2379-2405, 2018.

[22] L. Li, Q. Wang, Y. Xu and X. Zeng, *Several classes of complete permutation polynomials with Niho exponents*, Finite Fields Appl. **72**, 101831, 2021.

[23] R. Lidl and H. Niederreiter, *Finite Fields*, (Encyclopedia of Mathematics and its Applications), Cambridge University Press, Cambridge, 1997.

[24] G. L. Mullen and D. Panario, *Handbook of Finite Fields,* Discrete Mathematics and its Applications (Boca Raton), CRC Press, Boca Raton, FL, 2013.

[25] F. Özbudak and B. Gülmez Temür, *Classification of permutation polynomials of the form* $x^3 g(x^{q-1})$ *of* $\mathbb{F}_{q^2}$ *where* $g(x) = x^3 + bx + c$ *and* $b, c \in \mathbb{F}_q^*$, Des. Codes Cryptogr. **90**, 1537-1556, 2022.

[26] F. Özbudak and B. Gülmez Temür, *Complete characterization of some permutation polynomials of the form* $x^r(1 + ax^{s_1(q-1)} + bx^{s_2(q-1)})$ *over* $\mathbb{F}_{q^2}$, Cryptogr. Commun. **15**, 775-793, 2023.

[27] F. Özbudak and B. Gülmez Temür, *Classification of some quadrinomials over finite fields of odd characteristic*, Finite Fields Appl. **87**, 102158, 2023.

[28] Y. H. Park and J. B. Lee, *Permutation polynomials and group permutation polynomials*, Bull. Austral. Math. Soc. **63**, 67-74, 2001.

[29] Z. Tu and X. Zeng, *A class of permutation trinomials over finite fields of odd characteristic*, Cryptogr. Commun. **11**, 563-583, 2019.

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

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

[32] Q. Wang, *Cyclotomic mapping permutation polynomials over finite fields*, Sequences, subsequences, and consequences, Lecture Notes in Comput. Sci. **4893**, Springer, Berlin, 119-128, 2007.

[33] Q. Wang, *Polynomials over finite fields: an index approach*, Combinatorics and Finite Fields, Difference Sets, Polynomials, Pseudorandomness and Applications, De Gruyter, 319-348, 2019.

[34] L. Wang, B. Wu, X. Yue and Y. Zheng, *Further results on permutation trinomials with Niho exponents*, Cryptogr. Commun. **11**, 1057-1068, 2019.

[35] 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**, 2209-2216, 2009.