Cryptography and Communications (2023) 15:775–793
https://doi.org/10.1007/s12095-023-00641-7

Complete characterization of some permutation polynomials of the form $x^r(1 + ax^{s_1(q-1)} + bx^{s_2(q-1)})$ over $\mathbb{F}_{q^2}$

Ferruh Özbudak[1] · Burcu Gülmez Temür[2]

Received: 29 May 2022 / Accepted: 15 March 2023 / Published online: 18 April 2023

Abstract
We completely characterize all permutation trinomials of the form $f(x) = x^3(1 + ax^{q-1} + bx^{2(q-1)})$ over $\mathbb{F}_{q^2}$, where $a, b \in \mathbb{F}_q^*$ and all permutation trinomials of the form $f(x) = x^3(1 + bx^{2(q-1)} + cx^{3(q-1)})$ over $\mathbb{F}_{q^2}$, where $b, c \in \mathbb{F}_q^*$ in both even and odd characteristic cases.

Keywords Permutation polynomials · Finite fields · Absolutely irreducible

Mathematics Subject Classification (2010) 11T06 · 11T71 · 12E10

1 Introduction

Let q be a power of a prime, $\mathbb{F}_q$ be a finite field with q elements and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. A polynomial is called a permutation polynomial if it induces a bijection on $\mathbb{F}_q$. Permutation polynomials over finite fields have been studied by many researchers for a rather long time. The main interest is to obtain permutation polynomials that look simple, having some additional properties which are required in some applications in some areas such as coding theory, crptography and combinatorial designs etc. In general permutation polynomials having such properties are hard to obtain.

To the best of our knowledge permutation polynomials were first studied by Dickson and Hermite (see, [11, 15]). For the interested readers, we believe that the books on finite fields (see, [28] and Chapter 8 in [30]) will be a good beginning to get into the topic, and moreover the survey papers (see, [17, 19, 32, 40]) will be very useful to go over many of the recent results on permutation polynomials. For some more results on permutation polynomials over finite fields we refer the interested reader to [5, 6, 13, 18, 26, 27] and the references therein.

✉ Burcu Gülmez Temür
burcu.temur@atilim.edu.tr

Ferruh Özbudak
ozbudak@metu.edu.tr

[1] Department of Mathematics and Institute of Applied Mathematics,
Middle East Technical University, Ankara, Turkey

[2] Department of Mathematics, Atılım University, Ankara, Turkey

In recent years there has been a great interest on determining permutation properties of polynomials of the form

$$f(x) = x^r(1 + ax^{s_1(q-1)} + bx^{s_2(q-1)}) \in \mathbb{F}_{q^2}[x], \tag{1}$$

where r, s_1, s_2 are positive integers and $a, b \in \mathbb{F}_{q^2}$ (see for instance [4, 7, 21, 22, 25, 31, 36]).

In this paper we work on some types of permutation trinomials of the form as in (1) over the finite field $\mathbb{F}_{q^2}$. We develop a method to characterize certain permutation polynomials completely. Our method starts with a clever choice of polar coordinate transformation as an important technical step. Then we use an algorithmic method to decide whether the resulting polynomial in two variables is irreducible or not. This algorithmic method allows us to obtain all permutation polynomials in our classes as follows: The ones which lead to factorizations are easy to decide whether they are permutations or not. The ones which are irreducible turn out not to be permutations by using the well known Hasse-Weil inequality. We apply our method to some classes of polynomials of the form $x^r(1 + ax^{s_1(q-1)} + bx^{s_2(q-1)})$ over $\mathbb{F}_{q^2}$. In particular, we obtain not only new permutation polynomials over $\mathbb{F}_{q^2}$ analogous to the ones in [18] and [42] but we also obtain a complete characterization.

The paper is organized as follows: In the preliminaries section we explain the ideas that we use throughout the paper in details. In [18] Hou determined all necessary and sufficient conditions for which the polynomial $g(x) = x(a + bx^{q-1} + x^{2(q-1)})$ permutes $\mathbb{F}_{q^2}$ for both even and odd characteristic finite fields. Inspired by this result, in Section 3, we study the permutation properties of the polynomial $f(x) = x^3(1+ax^{q-1}+bx^{2(q-1)})$ over $\mathbb{F}_{q^2}$, where $a, b \in \mathbb{F}_q^*$ and we find all necessary and sufficient conditions on a, b such that $f(x)$ is a permutation trinomial of $\mathbb{F}_{q^2}$ in both even and odd characteristic cases.

In Zha et al. [42] determined that the polynomials of the form $x^3 + x^{2q+1} + x^{3q} = x^3(1 + x^{2(q-1)} + x^{3(q-1)})$ are permutation polynomials over $\mathbb{F}_{q^2}$, where $q = 2^m$ iff m is odd (see [42, Theorem 4.1]). In Section 4 we completely classify all permutation trinomials of a more general form $f(x) = x^3 + bx^{2q+1} + cx^{3q} = x^3(1 + bx^{2(q-1)} + cx^{3(q-1)})$ over $\mathbb{F}_{q^2}$, where $b, c \in \mathbb{F}_q^*$ in both even and odd characteristic cases.

We explain our contributions in each section via Remarks 1, 2. Finally in Section 5 we compare the results of our paper with the existing permutation trinomials in the literature under the quasi-multiplicative equivalence.

2 Preliminaries

There is a well known criterion due to Wan and Lidl [38], Park and Lee [34], Akbary and Wang [3], Wang [39] and Zieve [43] which is very useful for deciding whether a polynomial of the form $f(x) = x^r h\left(x^{(q^n-1)/d}\right)$ permutes $\mathbb{F}_{q^n}$ or not, which is given in the following lemma.

Lemma 1 [3, 34, 38, 39, 43] *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* $\mu_d = \{a \in \mathbb{F}_{q^n}^* \mid a^d = 1\}$.

In all cases we study in this paper we plan to apply Lemma 1 over the finite field $\mathbb{F}_{q^2}$ with $d = q+1$, but instead of trying to find the conditions for which $f(x) = x^r h(x)^{q-1}$ permutes μ_{q+1} we use the following idea throughout the paper:

Let z be an arbitrary element in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. We define the map $\phi(x) = \dfrac{x+z}{x+z^q}$, for any $x \in \mathbb{F}_q$ with $\phi(\infty) = 1$. We first observe that ϕ is one to one from $\mathbb{F}_q \cup \{\infty\}$ to μ_{q+1} by the following discussion:
Assume that $\phi(x) = \phi(y)$ for some $x, y \in \mathbb{F}_q$, that is,

$$\frac{x+z}{x+z^q} = \frac{y+z}{y+z^q}$$

which implies that $(x-y)z^q = (x-y)z$. Whenever $x \neq y$ we obtain $z^q = z$ which gives a contradiction since $z \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Thus ϕ is one to one. Moreover ϕ is also onto since we have the same number of elements on both sides. Then one obtains that $\phi^{-1}(x) = \dfrac{xz^q - z}{1-x}$, for any $x \neq 1$ with $\phi^{-1}(1) = \infty$. In this setting, $f(x) = x^r h(x)^{q-1}$ is one to one on μ_{q+1} and thus permutes μ_{q+1} if and only if the map $\left(\phi^{-1} \circ f \circ \phi\right)$ is one to one on $\mathbb{F}_q \cup \{\infty\}$.

The situation can be easily followed in the diagram below:

$$\begin{tikzcd}
\mathbb{F}_q \cup \{\infty\} \arrow[r, "\phi^{-1} \circ f \circ \phi"] \arrow[d, "\phi"] & \mathbb{F}_q \cup \{\infty\} \\
\mu_{q+1} \arrow[r, "f"] & \mu_{q+1} \arrow[u, "\phi^{-1}"']
\end{tikzcd}$$

An important further technique we use is that we choose $z \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ suitably so that the computations become simpler.

3 Permutation trinomials of the form $x^3 + ax^{q+2} + bx^{2q+1}$ over $\mathbb{F}_{q^2}$, where $a, b \in \mathbb{F}_q^*$

In this section, aiming both necessity and sufficiency, we study the permutation properties of the polynomial $f(x) = x^3(1 + ax^{q-1} + bx^{2(q-1)})$ over $\mathbb{F}_{q^2}$, where $a, b \in \mathbb{F}_q^*$ (see Remark 1 below).
We first observe that,

$$f(x) = x^3(1 + ax^{q-1} + bx^{2(q-1)}) = x^3 h(x^{q-1}),$$

where $h(x) = 1 + ax + bx^2$ with $a, b \in \mathbb{F}_q^*$. As we plan to apply Lemma 1, we must first find out $a, b \in \mathbb{F}_q^*$ for which the polynomial $h(x) = 1 + ax + bx^2 \in \mathbb{F}_q[x]$ does not have any roots in μ_{q+1}. If $h(1) = 0$ or $h(-1) = 0$, then $h(x)$ has a root in μ_{q+1} trivially, therefore we characterize all such polynomials in the next proposition under the assumptions $h(1) \neq 0$ and $h(-1) \neq 0$.

Proposition 1 *Let $\mathbb{F}_q$ be a finite field and $h(x) = 1 + ax + bx^2 \in \mathbb{F}_q[x]$ where $a, b \in \mathbb{F}_q^*$. Assume that $h(1) = 1 + a + b \neq 0$, $h(-1) = 1 - a + b \neq 0$. Then $h(x)$ has no roots in μ_{q+1} if and only if one of the following conditions hold:*

i) $b \neq 1$,
ii) $b = 1$ *and*

$$\begin{cases} \operatorname{Tr}\left(\dfrac{1}{a}\right) = 0, \ \textit{if } char(\mathbb{F}_q) \textit{ is even}, \\[2ex] a^2 - 4 \textit{ is a nonzero square in } \mathbb{F}_q, \ \textit{if } char(\mathbb{F}_q) \textit{ is odd}. \end{cases}$$

Proof Let $x \in \mu_{q+1}$ such that $h(x) = 0$, that is, $x^q = 1/x$ and $1 + ax + bx^2 = 0$. Taking the q-th power of the equation $1 + ax + bx^2 = 0$ and inserting $x^q = 1/x$ we obtain

$$x^2 + ax + b = 0.$$

Hence there exists $x \in \mu_{q+1}$ such that $h(x) = 0$ if and only if the following system

$$\left.\begin{array}{r} bx^2 + ax + 1 = 0 \\ bx^2 + abx + b^2 = 0 \end{array}\right\} \tag{2}$$

holds. Subtracting the equations in the above system (2) we get:

$$a(1-b)x + 1 - b^2 = 0. \tag{3}$$

Assuming that $b \neq 1$ we get $x = \frac{-(1+b)}{a} \in \mathbb{F}_q \cap \mu_{q+1} = \{-1, 1\}$ but this gives a contradiction since $h(1) \neq 0$ and $h(-1) \neq 0$. Thus $h(x)$ has no roots in μ_{q+1} if $b \neq 1$. Now, assume that $b = 1$, then $h(x) = x^2 + ax + 1$. Assume that $x \in \mu_{q+1}$ is a root of $h(x)$, that is, $x^2 + ax + 1 = 0$. First, assume that $char(\mathbb{F}_q) = 2$, then we obtain

$$x^2 + ax = 1 \iff \frac{x^2}{a^2} + \frac{1}{a}x = \frac{1}{a^2} \iff y^2 + y = \frac{1}{a^2},$$

where $y = x/a$. If $\mathrm{Tr}\left(\frac{1}{a^2}\right) = \mathrm{Tr}\left(\frac{1}{a}\right) = 0$ then $x/a \in \mathbb{F}_q$ which implies that $x \in \mathbb{F}_q \cap \mu_{q+1} = \{-1, 1\}$ but this is not possible since $h(1) \neq 0$ and $h(-1) \neq 0$. Therefore $h(x)$ has no roots in μ_{q+1} iff $\mathrm{Tr}\left(\frac{1}{a}\right) = 0$ in the even characteristic case.

Next, assume that $char(\mathbb{F}_q)$ is odd. Then we have

$$0 = x^2 + ax + 1 = x^2 + ax + \frac{a^2}{4} + 1 - \frac{a^2}{4} \iff \left(x + \frac{a}{2}\right)^2 = \frac{a^2-4}{4}.$$

Thus, $h(x)$ has no roots in μ_{q+1} iff $a^2 - 4$ is a nonzero square in $\mathbb{F}_q$ in the odd characteristic case. □

Now, suppose that $h(x)$ has no roots in μ_{q+1}, then for any $x \in \mu_{q+1}$ we have the following

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

Let $g(x) = \dfrac{x^3 + ax^2 + bx}{bx^2 + ax + 1}$, $\phi(x) = \dfrac{x + z}{x + z^q}$ and thus $\phi^{-1}(x) = \dfrac{xz^q - z}{1 - x}$, where $z \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$.

We define $\Delta(z; x) := (x + z)^3 + a(x + z)^2(x + z^q) + b(x + z)(x + z^q)^2$. Then we have the following

$$(g \circ \phi)(x) = \frac{\Delta(z; x)}{\Delta(z^q; x)} = \frac{(x + z)^3 + a(x + z)^2(x + z^q) + b(x + z)(x + z^q)^2}{b(x + z)^2(x + z^q) + a(x + z)(x + z^q)^2 + (x + z^q)^3}$$

and thus

$$(\phi^{-1} \circ g \circ \phi)(x) = \frac{\dfrac{\Delta(z; x)}{\Delta(z^q; x)} z^q - z}{1 - \dfrac{\Delta(z; x)}{\Delta(z^q; x)}} = \frac{\Delta(z; x) z^q - z\Delta(z^q; x)}{\Delta(z^q; x) - \Delta(z; x)}.$$

Hereafter, in this section we deal with odd characteristic and even characteristic cases seperately.

First, assume that $\mathbb{F}_q$ is a finite field of odd characteristic and let $z^q = -z$, then we get the following

$$\Delta(z;x)z^q - z\Delta(z^q;x) = -2z\left((1+a+b)x^3 + (3-a-b)z^2x\right)$$

and

$$\Delta(z^q;x) - \Delta(z;x) = -2z\left((3+a-b)x^2 + (1+b-a)z^2\right).$$

Thus,

$$(\phi^{-1}\circ g\circ\phi)(x) = \frac{\Delta(z;x)z^q - z\Delta(z^q;x)}{\Delta(z^q;x)-\Delta(z;x)} = \frac{(1+a+b)x^3+(3-a-b)z^2x}{(3+a-b)x^2+(1+b-a)z^2}. \tag{4}$$

First, we deal with the case where $3+a-b=0$ in the following proposition.

Proposition 2 *Let $\mathbb{F}_q$ be a finite field of odd characteristic, where $gcd(3, q-1) = 1$. Let $h(x) = bx^2 + ax + 1$, with $a, b \in \mathbb{F}_q^*$. Assume that $h(x)$ has no roots in μ_{q+1}, that is, $h(x)$ satisfies the conditions in Proposition 1, and $3+a-b=0$. If $char(\mathbb{F}_q) \neq 3$ then there are no permutation polynomials of the form $f(x) = x^3h(x^{q-1})$ of $\mathbb{F}_{q^2}$. If $char(\mathbb{F}_q) = 3$ then $f(x) = x^3h(x^{q-1})$ is a permutation polynomial of $\mathbb{F}_{q^2}$ iff $a = b$ and $\frac{b}{b-1}$ is a square in $\mathbb{F}_q$.*

Proof In this case, after computing

$$\frac{(\phi^{-1}\circ g\circ\phi)(x) - (\phi^{-1}\circ g\circ\phi)(y)}{x-y}$$

using the equation in (4) and simplifying we obtain the following

$$\mathcal{C}(x,y) := x^2 + xy + y^2 + A, \text{ where } A = \frac{(3-b)}{b-1}z^2. \tag{5}$$

Note that, if $b-1=0$ then $3+a-b=0$ implies that $a=-2$ and thus f is not a permutation polynomial since $h(x)$ has a root (i.e., $h(1) = 1+a+b = 0$) in μ_{q+1}. Hence we assume that $b \neq 1$. We also have $A \neq 0$ otherwise $b = 3$ and this implies $a = 0$ but $a \in \mathbb{F}_q^*$.
First, assume that $\mathcal{C}(x,y)$ in (5) is not absolutely irreducible over the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$ and it can be decomposed in the form:

$$(x+\alpha y + lot)(\beta_1 x + \beta_2 y + lot) = \beta_1 x^2 + (\beta_2 + \beta_1\alpha)xy + \beta_2\alpha y^2 + lot \tag{6}$$

Later in this proof we determine exactly in which extensions of $\mathbb{F}_q$ α, β_1, β_2 lie. Here and throughout the paper we use "lot" as the abbreviated form of the so called "lower order terms". Comparing the coefficients of degree 2 terms in (6) with the ones in $\mathcal{C}(x,y)$ in (5) we obtain: $\beta_1 = 1$, $\beta_2 + \alpha = 1$ and $\beta_2\alpha = 1$ which implies that $\alpha(1-\alpha) = 1$. Now, substituting $\beta_1 = 1$, $\beta_2 = 1-\alpha$ and $\alpha(1-\alpha) = 1$ in (6) we get:

$$\begin{aligned} &(x+\alpha y+\alpha_1)(x+(1-\alpha)y+\alpha_2) \\ &= x^2+xy+y^2+(\alpha_2+\alpha_1)x+(\alpha\alpha_2+\alpha_1(1-\alpha))y+\alpha_1\alpha_2 \end{aligned} \tag{7}$$

Comparing the coefficients of degree 1 terms in (6) with the ones in $\mathcal{C}(x,y)$ in (5) we obtain: $\alpha_1+\alpha_2 = 0$ so we have $\alpha_2 = -\alpha_1$ and $\alpha\alpha_2+\alpha_1(1-\alpha) = 0$ which implies that $\alpha_1(1-2\alpha) = 0$. Note that $\alpha_1 \neq 0$ as $A = -\alpha_1^2$ and $A \neq 0$. Thus we must have $\alpha = 1/2$. Substituting $\alpha = 1/2$ in $\alpha(1-\alpha) = 1$ we obtain that $4 = 1$ which is only possible if $char(\mathbb{F}_q) = 3$. Therefore, $\mathcal{C}(x,y)$ is absolutely irreducible in the case where $char(\mathbb{F}_q) \neq 3$. Homogenizing $\mathcal{C}(x,y)$ in

(5) with $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$ we obtain a homogeneous polynomial of degree $d = 2$. Then by the Hasse-Weil bound (see [20, Theorem 5.28]) we have the following:

$c(d) = \frac{1}{2}d(d-1)^2 + 1$, note that $c(d) = 2$ as $d = 2$, hence

$$\mid N - q \mid \leq (d-1)(d-2)q^{1/2} + c(d) = 2,$$

where N is the number of affine $\mathbb{F}_q$-rational points of $\mathcal{C}(x, y)$. This implies that if $q - 2 > 2$ then $\mathcal{C}(x, y)$ in (5) has an affine $\mathbb{F}_q$-rational point off the line $x = y$ and thus $f(x)$ is not a permutation polynomial of $\mathbb{F}_{q^2}$.

Next, if $char(\mathbb{F}_q) = 3$ then $\alpha = 1/2$, $A = -\alpha_1^2 = \dfrac{-b}{b-1}z^2$ and by $3 + a - b = 0$ we have $a = b$. Assume that $x + \frac{1}{2}y + \alpha_1 = 0$ for some $x, y \in \mathbb{F}_q$. Taking its q-th power we obtain $x + \frac{1}{2}y + \alpha_1^q = 0$. Subtracting these two equations we get that $\alpha_1^q = \alpha_1$, thus $\alpha_1 \in \mathbb{F}_q$. On the other hand $\alpha_1^2 = \frac{b}{b-1}z^2$, where $z \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Thus, $\alpha_1 \notin \mathbb{F}_q$ iff $\frac{b}{b-1}$ is a square in $\mathbb{F}_q$. □

Next, assume that $3 + a - b \neq 0$. Note also that $1 + b + a \neq 0$, $1 + b - a \neq 0$ since $h(-1) \neq 0$, $h(1) \neq 0$. Then by (4) we have:

$$\frac{x^3 + \dfrac{(3-b-a)}{(1+b+a)}z^2 x}{x^2 + \dfrac{(1+b-a)}{(3-b+a)}z^2} = \frac{x^3 + Ax}{x^2 + B}, \tag{8}$$

where $A = z^2\dfrac{(3-b-a)}{1+b+a}$ and $B = z^2\dfrac{(1+b-a)}{3-b+a} \neq 0$ since $h(-1) = 1 + b - a \neq 0$. First, we consider the case where $-B$ is a square in $\mathbb{F}_q$. In this case there exists $x \in \mathbb{F}_q$ such that the denominator of the fraction in (8), that is, $x^2 + B$ becomes zero which implies that ∞ has at least three distinct preimages under the map $(\phi^{-1} \circ g \circ \phi)(x)$ and therefore $g(x)$ is not a permutation polynomial. Thus, from here on assume that $-B$ is not a square in $\mathbb{F}_q$, that is, $\dfrac{-(1+b-a)}{3-b+a}$ is a square in $\mathbb{F}_q$ since $z \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$.

Computing $\dfrac{\dfrac{x^3+Ax}{x^2+B} - \dfrac{y^3+Ay}{y^2+B}}{x-y}$ one gets the following

$$\mathcal{C}(x, y) := x^2y^2 + (B - A)xy + B(x^2 + y^2) + AB. \tag{9}$$

In this setting, $(\phi^{-1} \circ g \circ \phi)$ permutes $\mathbb{F}_q$ if and only $\mathcal{C}(x, y)$ defined in (9) is not zero for any $x, y \in \mathbb{F}_q$ with $x \neq y$. The following theorem completes the problem in the remaining case for finite fields of odd characteristic, where $3 + a - b \neq 0$.

Theorem 3 *Let $\mathbb{F}_q$ be a finite field of odd characteristic, where $gcd(3, q-1) = 1$. Let $h(x) = bx^2 + ax + 1$, with $a, b \in \mathbb{F}_q^*$. Assume that $3 + a - b \neq 0$. Then $f(x) = x^3h(x^{q-1})$ is a permutation polynomial of $\mathbb{F}_{q^2}$ iff one of the following conditions hold*

i $b = 1$, $a \neq \pm 2$ *and* $a^2 - 4$ *is a square in* $\mathbb{F}_q$,

ii $b \neq 1$, $b^2 + 3b - a^2 = 0$, $\dfrac{-(1+b-a)}{3+a-b}$ *is a square in* $\mathbb{F}_q$, $1 + a + b \neq 0$ *and* $1 + b - a \neq 0$.

Proof We need to check all decompositions of the bivariate polynomial $\mathcal{C}(x, y)$ in (9) 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 (9) is 4, the possibilities are: 3 + 1

decomposition and $2+2$ decomposition according to the degrees of the possible factors and finally the case where the bivariate polynomial $\mathcal{C}(x, y)$ in (9) is absolutely irreducible. We first fix a monomial ordering by taking $x \geq y$ without loss of generality.
We begin the discussion with $3+1$ decomposition. Let $\mathcal{C}(x, y)$ defined in (9) be decomposed in the following form

$$\begin{aligned} &(x+\alpha_1 y+lot)(\beta_1 x^3+\gamma_1 x^2 y+\delta_1 x y^2+\eta_1 y^3+lot) \\ =\ &\beta_1 x^4+(\gamma_1+\alpha_1\beta_1)x^3 y+(\delta_1+\alpha_1\gamma_1)x^2y^2+(\eta_1+\alpha_1\delta_1)xy^3+\alpha_1\eta_1 y^4+lot. \end{aligned} \tag{10}$$

By comparing the coefficients of the degree 4 terms in (10) with the ones in $\mathcal{C}(x, y)$ defined in (9), we obtain that: $\beta_1=0$, $\gamma_1=0$, $\delta_1=1$, $\alpha_1=0$ and $\eta_1=0$. Substituting these in (10) we have

$$(x+lot)(xy^2+lot),$$

that is, writing down the possible lower order terms, the decomposition is as follows:

$$\begin{aligned} &(x+\alpha)(xy^2+\alpha_2 x^2+\beta_2 xy+\gamma_2 y^2+lot) \\ =\ &x^2y^2+\alpha_2 x^3+\beta_2 x^2 y+(\gamma_2+\alpha)xy^2+lot. \end{aligned} \tag{11}$$

Now, by comparing the coefficients of the degree 3 terms in (11) with the ones in $\mathcal{C}(x, y)$ defined in (9), we observe that $\alpha_2=0$, $\beta_2=0$, $\gamma_2=-\alpha$. Thus we have

$$\begin{aligned} &(x+\alpha)(xy^2-\alpha y^2+\alpha_3 x+\beta_3 y+lot) \\ =\ &x^2y^2+\alpha_3 x^2+\beta_3 xy-\alpha^2 y^2+lot. \end{aligned} \tag{12}$$

By comparing the coefficients of the degree 2 terms in (12) with the ones in $\mathcal{C}(x, y)$ defined in (9), we observe that $\alpha_3=-\alpha^2=B$, $\beta_3=B-A$. That is, we have

$$\begin{aligned} &(x+\alpha)(xy^2-\alpha y^2+Bx+(B-A)y+\beta) \\ =\ &x^2y^2+(B-A)xy+B(x^2+y^2)+(\beta+\alpha B)x+\alpha(B-A)y+\alpha\beta. \end{aligned} \tag{13}$$

By comparing the coefficients of the degree 1 terms in (13) with the ones in $\mathcal{C}(x, y)$ defined in (9), we observe that $\beta=-\alpha B$ and $\alpha(B-A)=0$ which implies that $B=A$ since $\alpha\neq 0$ (as $-\alpha^2=B\neq 0$). Finally, comparing the constant term in (13) with the one in $\mathcal{C}(x, y)$ we get $\alpha\beta=AB$ and substituting $\beta=-\alpha B$ in $\alpha\beta=AB$, we obtain that $A=B=-\alpha^2$. Thus we have

$$(x+\alpha)(xy^2-\alpha y^2-\alpha^2 x+\alpha^3)=(x+\alpha)(x-\alpha)(y+\alpha)(y-\alpha), \tag{14}$$

so we end up with the 1+1+1+1 decomposition of $\mathcal{C}(x, y)$. Now, we have

$$A=B \implies z^2\frac{(3-b-a)}{1+b+a}=z^2\frac{(1+b-a)}{3-b+a}\text{, that is,}$$

$$(3-b-a)(3-b+a)=(1+b-a)(1+b+a)$$

which implies that $b=1$. Note that $-\alpha^2=B$, so $\alpha\notin\mathbb{F}_q$ since we have that $-B=z^2\dfrac{(a-2)}{a+2}$ is not a square in $\mathbb{F}_q$ (that is, $\dfrac{a-2}{a+2}$ is a square in $\mathbb{F}_q$) and thus none of the factors in the decomposition (14) can have a root in $\mathbb{F}_q$. Therefore, in this case, $f(x)$ is a permutation poynomial iff $b=1$, $a\neq\pm 2$ and $\dfrac{a-2}{a+2}$ is a square in $\mathbb{F}_q$, that is, a^2-4 is a square in $\mathbb{F}_q$.

Next, we deal with the possible 2+2 decompositions of $\mathcal{C}(x, y)$. Here, there are two possibilities: $\mathcal{C}(x, y)$ defined in (9) is either decomposed in the form

$$(x^2 + \alpha_1 xy + \beta_1 y^2 + lot)(\alpha_2 x^2 + \beta_2 xy + \gamma_2 y^2 + lot) \tag{15}$$

or

$$(xy + \alpha_1 x + \beta_1 y + lot)(xy + \alpha_2 x + \beta_2 y + lot). \tag{16}$$

First, assume that $\mathcal{C}(x, y)$ is decomposed in the form (15).

$$\begin{aligned}(x^2 + \alpha_1 xy + \beta_1 y^2 + lot)(\alpha_2 x^2 + \beta_2 xy + \gamma_2 y^2 + lot)\\ = \alpha_2 x^4 + (\beta_2 + \alpha_1\alpha_2)x^3 y + (\gamma_2 + \alpha_1\beta_2 + \alpha_2\beta_1)x^2 y^2\\ +(\alpha_1\gamma_2 + \beta_1\beta_2)xy^3 + \beta_1\gamma_2 y^4 + lot.\end{aligned} \tag{17}$$

After comparing the coefficients of degree 4 terms of (15) with the ones in $\mathcal{C}(x, y)$ defined in (9) we get: $\alpha_1 = 0, \alpha_2 = 0, \beta_1 = 0, \beta_2 = 0, \gamma_2 = 1$, so we end up with the following decomposition

$$\begin{aligned}(x^2 + \alpha_3 x + \beta_3 y + lot)(y^2 + \alpha_4 x + \beta_4 y + lot)\\ = x^2 y^2 + \alpha_4 x^3 + \beta_4 x^2 y + \alpha_3 xy^2 + \beta_3 y^3 + lot.\end{aligned} \tag{18}$$

Comparing the coefficients of degree 3 terms of (18) with the ones in $\mathcal{C}(x, y)$ defined in (9) we get: $\alpha_4 = 0, \beta_4 = 0, \alpha_3 = 0, \beta_3 = 0$. Thus we have

$$(x^2 + \eta)(y^2 + \zeta) = x^2 y^2 + \zeta x^2 + \eta y^2 + \eta\zeta. \tag{19}$$

Comparing the coefficients of (19) with the ones in $\mathcal{C}(x, y)$ defined in (9) we obtain that $B - A = 0$, that is, $A = B$ (implying $b = 1$) and $\eta = \zeta = B$. Now, if $x^2 + \eta = 0$ for some $x \in \mathbb{F}_q$ then we have $x^2 = -\eta = -B$, that is, $-B$ is a square in $\mathbb{F}_q$ which gives a contradiction. Thus $x^2 + \eta \neq 0$ and similarly $y^2 + \zeta \neq 0$ for any $x, y \in \mathbb{F}_q$. Therefore in this case, $f(x)$ is a permutation poynomial iff $b = 1, a \neq \pm 2$ and $\frac{a-2}{a+2}$ is a square in $\mathbb{F}_q$, that is, $a^2 - 4$ is a square in $\mathbb{F}_q$.

Next, assume that $\mathcal{C}(x, y)$ is decomposed in the form (16).

$$\begin{aligned}(xy + \alpha_1 x + \beta_1 y + lot)(xy + \alpha_2 x + \beta_2 y + lot)\\ = x^2 y^2 + (\alpha_1 + \alpha_2)x^2 y + (\beta_1 + \beta_2)xy^2 + lot.\end{aligned} \tag{20}$$

After comparing the coefficients of degree 3 terms of (16) with the ones in $\mathcal{C}(x, y)$ we obtain: $\alpha_2 = -\alpha_1$ and $\beta_2 = -\beta_1$ and so we end up with the following decomposition

$$\begin{aligned}(xy + \alpha_1 x + \beta_1 y + \alpha)(xy - \alpha_1 x - \beta_1 y + \beta)\\ = x^2 y^2 - \alpha_1^2 x^2 + (\beta + \alpha - 2\alpha_1\beta_1)xy - \beta_1^2 y^2 + lot.\end{aligned} \tag{21}$$

Comparing the coefficients of degree 2 terms in (21) with the ones in $\mathcal{C}(x, y)$ we obtain $-\alpha_1^2 = -\beta_1^2 = B$ and $\beta + \alpha - 2\alpha_1\beta_1 = B - A$. By $-\alpha_1^2 = -\beta_1^2 = B$ we deduce that $\alpha_1, \beta_1 \notin \mathbb{F}_q$ since we have that $-B$ is not a square in $\mathbb{F}_q$, which further implies that $\alpha_1^q = -\alpha_1$ and $\beta_1^q = -\beta_1$ (as $-\alpha_1^2 = -\beta_1^2 = B \in \mathbb{F}_q$). Thus, we have $\alpha_1^2 = \beta_1^2$ which implies that either $\alpha_1 = \beta_1$ or $\alpha_1 = -\beta_1$.

Now, assume that $\alpha_1 = \beta_1$, then substituting $\alpha_1 = \beta_1$ and $-\alpha_1^2 = -\beta_1^2 = B$ in $\beta + \alpha - 2\alpha_1\beta_1 = B - A$ we obtain $\beta = -(A + B + \alpha)$. Then the decomposition in (21) becomes the following:

$$\begin{aligned}&(xy+\alpha_1x+\alpha_1y+\alpha)(xy-\alpha_1x-\alpha_1y-(A+B+\alpha)) \\ &=x^2y^2-\alpha_1^2(x^2+y^2)+(B-A)xy-\alpha_1(A+B+2\alpha)(x+y)-\alpha(A+B+\alpha).\end{aligned}\tag{22}$$

Comparing the coefficients of degree 1 terms and the constant terms in (22) with the ones in $\mathcal{C}(x,y)$, we obtain $A+B+2\alpha=0$ as $\alpha_1\neq0$ and so $\alpha=\frac{-(A+B)}{2}$. Comparing the constant term in (22) with the one in $\mathcal{C}(x,y)$, we obtain $-\alpha(A+B+\alpha)=AB$. Substituting $\alpha=\frac{-(A+B)}{2}$ in $-\alpha(A+B+\alpha)=AB$ we obtain $AB=\frac{(A+B)^2}{4}$ which implies that $(A-B)^2=0$ then $A=B$ and so $b=1$.
Assume that there exists $x,y\in\mathbb{F}_q$ such that $xy+\alpha_1x+\alpha_1y+\alpha=0$. Taking its q-th power we get $xy-\alpha_1x-\alpha_1y+\alpha=0$. Subtracting these two equations we obtain $2\alpha_1(x+y)=0$ which implies that $x=-y$ since $\alpha_1\neq0$ (as $-\alpha_1^2=B\neq0$). Substituting $x=-y$ in the equation $xy+\alpha_1x+\alpha_1y+\alpha=0$ we get $-x^2+\alpha=-x^2-B=0$ which contradicts with the fact that $-B$ is not a square in $\mathbb{F}_q$. Thus, we conclude that none of the factors in the decomposition (22) can have roots in $\mathbb{F}_q$. Therefore, in this case, $f(x)$ is a permutation poynomial iff $b=1$, $a\neq\pm2$ and $\frac{a-2}{a+2}$ is a square in $\mathbb{F}_q$, that is, a^2-4 is a square in $\mathbb{F}_q$.

Finally, assume that $\alpha_1=-\beta_1$. Then by (21) we have the following decomposition:

$$(xy+\alpha_1x-\alpha_1y+\alpha)(xy-\alpha_1x+\alpha_1y-(A-3B+\alpha)).\tag{23}$$

Comparing the coefficients of degree 1 terms and the constant terms in (23) with the ones in $\mathcal{C}(x,y)$ we obtain $\alpha=\beta$, $AB=\alpha^2$ and $\alpha=\frac{3B-A}{2}$. Substituting $\alpha=\frac{3B-A}{2}$ in $AB=\alpha^2$ we get $(9B-A)(B-A)=0$ implying that either $A=B$ or $A=9B$.
If $A=B$ then $b=1$ and we obtain that $f(x)$ is a permutation poynomial iff $b=1$, $a\neq\pm2$ and $\frac{a-2}{a+2}$ is a square in $\mathbb{F}_q$, that is, a^2-4 is a square in $\mathbb{F}_q$. If $9B=A$ then we obtain $b^2+3b-a^2=0$.
Assume that there exists $x,y\in\mathbb{F}_q$ such that $xy+\alpha_1x-\alpha_1y+\alpha=0$. Taking its q-th power we get $xy-\alpha_1x+\alpha_1y+\alpha=0$. Subtracting these two equations we obtain $2\alpha_1(x-y)=0$ implying that $x=y$ since $\alpha_1\neq0$. Therefore, in this case $f(x)$ is a permutation poynomial iff $b^2+3b-a^2=0$, $\frac{-(1+b-a)}{3+a-b}$ is a square in $\mathbb{F}_q$, $1-a+b\neq0$, $1+a+b\neq0$ and $b\neq1$ (otherwise, if $b=1$, $b^2+3b-a^2=0$ implies that $a=\pm2$ which contradicts with $1-a+b\neq0$ or $1+a+b\neq0$).

As the last step, we deal with the absolutely irreducible case. Assume that $\mathcal{C}(x,y)$ defined in (9) is absolutely irreducible. Homogenizing $\mathcal{C}(x,y)$ in (9) with $x=\frac{X}{Z}$ and $y=\frac{Y}{Z}$ we obtain a homogeneous polynomial of degree $d=4$. Then by the Hasse-Weil bound (see [20, Theorem 5.28]) we have the following:
$c(d)=\frac{1}{2}d(d-1)^2+1$, note that $c(d)=19$ as $d=4$, hence

$$\mid N-q\mid\leq(d-1)(d-2)q^{1/2}+c(d)\leq6q^{1/2}+19,$$

where N is the number of affine $\mathbb{F}_q$-rational points of $\mathcal{C}(x,y)$. This implies that if $q-6q^{1/2}-19>4$ then $\mathcal{C}(x,y)$ has an affine $\mathbb{F}_q$-rational point off the line $x=y$. As q is a prime power, we note that $q-6q^{1/2}-19>4$ for any such q provided that $q\geq79$. As a result, we deduce that $f(x)$ is not a permutation polynomial of $\mathbb{F}_{q^2}$ if $\mathcal{C}(x,y)$ is absolutely irreducible and $q\geq79$. It remains to consider $q<79$. Now, since characteristic of $\mathbb{F}_q$ is odd and 3 does not

Table 1 List of all pairs of coefficients (a, b) of permutation polynomials of $\mathbb{F}_{81}$ of the form $f(x) = x^3h(x^{q-1})$, where $h(x) = bx^2 + ax + 1$, with $a, b \in \mathbb{F}_9^*$ and $x^2 + 2x + 2 \in \mathbb{F}_3[x]$ is the minimal polynomial of α obtained by Proposition 2

(a, b)	(α, α)	(α^3, α^3)	$(2, 2)$

divide $q - 1$ we need to consider only $q \in \{3, 5, 9, 11, 17, 23, 27, 29, 41, 47, 53, 59, 71\}$. Using MAGMA [29], we observe that there are no other permutation polynomials of the form $f(x)$ other than the ones obtained by Proposition 2 and Theorem 1. □

Next, assume that $\mathbb{F}_q$ is a finite field of even characteristic. Note that if $char(\mathbb{F}_q)$ is even then in order to have $\gcd(3, q - 1) = 1$, q must be of the form $q = 2^{2k+1}$, for some $k \in \mathbb{N}$. Let $z \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ satisfying $z^2 + z + 1 = 0$. Note that $z \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ satisfying $z^q + z = 1$. Then we get the following

$$\Delta(z; x)z^q - z\Delta(z^q; x) = (1 + a + b)x^3 + ax^2 + (a + 1)x + b + 1$$

and

$$\Delta(z^q; x) - \Delta(z; x) = (1 + a + b)x^2 + (1 + a + b)x + a + b.$$

Thus, we get

$$\begin{aligned}(\phi^{-1} \circ f \circ \phi)(x) &= \frac{\Delta(z; x)z^q - z\Delta(z^q; x)}{\Delta(z^q; x) - \Delta(z; x)} \\ &= \frac{(1 + a + b)x^3 + ax^2 + (a + 1)x + b + 1}{(1 + a + b)x^2 + (1 + a + b)x + a + b}.\end{aligned} \tag{24}$$

Let $A_2 = \dfrac{a}{1 + a + b}$, $A_1 = \dfrac{a + 1}{1 + a + b}$, $A_0 = \dfrac{b + 1}{1 + a + b}$ and $B_0 = \dfrac{a + b}{1 + a + b}$, so we have $B_0 = A_1 + A_0$.

Computing $\dfrac{\dfrac{x^3 + A_2x^2 + A_1x + A_0}{x^2 + x + B_0} - \dfrac{y^3 + A_2y^2 + A_1y + A_0}{y^2 + y + B_0}}{x - y}$ one gets the following

$$\mathcal{C}(x, y) := x^2y^2 + x^2y + xy^2 + B_0(x^2 + y^2) + xy + (A_2B_0 + A_0)(x + y) + A_1B_0 + A_0. \tag{25}$$

In this setting, $(\phi^{-1} \circ f \circ \phi)$ permutes $\mathbb{F}_q$ if and only $\mathcal{C}(x, y)$ defined in (25) is not zero for any $x, y \in \mathbb{F}_q$ with $x \neq y$. Our second main result in this section is given in the following theorem.

Theorem 4 *Let $\mathbb{F}_q$ be a finite field of even characteristic, where $q = 2^{2k+1}$, for some $k \in \mathbb{N}$. Let $h(x) = bx^2 + ax + 1$, with $a, b \in \mathbb{F}_q^*$. Then $f(x) = x^3h(x^{q-1})$ is a permutation polynomial of $\mathbb{F}_{q^2}$ iff one of the following conditions hold*

i) $b = 1$ *and* $\mathrm{Tr}\left(\dfrac{1}{a}\right) = 0$,

ii) $b \neq 1$, $1 + a + b \neq 0$ *and* $a^2 = b(1 + b)$.

Proof The proof can be done in an analogous way to Theorem 1 therefore we omit the proof in order not to repeat the similar long discussions on all possible decompositions. □

Example 1 In the following tables we explicitly give the coefficients over the finite field $\mathbb{F}_9$ of all permutation polynomials obtained from Proposition 2 and Theorem 1. Here, $\mathbb{F}_9$ is the smallest nontrivial finite field containing coefficients a, b which give rise to permutation polynomials of the form $f(x) = x^3h(x^{q-1})$ of $\mathbb{F}_{81}$, where $h(x) = bx^2 + ax + 1$. Let $x^2 + 2x + 2 \in \mathbb{F}_3[x]$ be the minimal polynomial of α, that is $\mathbb{F}_9^* =< \alpha >$. In Tables 1 and 2 below we list all pairs of coefficients (a, b) of permutation polynomials of $\mathbb{F}_{81}$ of the form $f(x) = x^3h(x^{q-1})$, where $h(x) = bx^2 + ax + 1$, with $a, b \in \mathbb{F}_9^*$ obtained by Proposition 2 and Theorem 1 respectively .

Example 2 In the following table we explicitly give the coefficients over the finite field $\mathbb{F}_8$ of all permutation polynomials obtained from Theorem 2. Here, $\mathbb{F}_8$ is the smallest nontrivial finite field containing coefficients a, b which give rise to permutation polynomials of the form $f(x) = x^3h(x^{q-1})$ of $\mathbb{F}_{64}$, where $h(x) = bx^2 + ax + 1$. Let $x^3 + x + 1 \in \mathbb{F}_2[x]$ be the minimal polynomial of α, that is $\mathbb{F}_8^* =< \alpha >$. In Table 3 below we list all pairs of coefficients (a, b) of permutation polynomials of $\mathbb{F}_{64}$ of the form $f(x) = x^3h(x^{q-1})$, where $h(x) = bx^2 + ax + 1$, with $a, b \in \mathbb{F}_8^*$ and $x^3 + x + 1 \in \mathbb{F}_2[x]$ is the minimal polynomial of α, obtained by Theorem 2.

Remark 1 In recent years, there have been many attempts to find new classes of permutation trinomials of the form $f(x) = x^r(1 + ax^{s_1(q-1)} + bx^{s_2(q-1)}) \in \mathbb{F}_{q^2}[x]$, where r, s_1, s_2 are positive integers and $a, b \in \mathbb{F}_{q^2}$. In Hou [18] determined all necessary and sufficient conditions for which the polynomial $g(x) = x(a + bx^{q-1} + x^{2(q-1)})$ permutes $\mathbb{F}_{q^2}$ for both even and odd characteristic finite fields. Inspired by this result, in this section, we studied on the permutation properties of the polynomial $f(x) = x^3(1 + ax^{q-1} + bx^{2(q-1)})$ over $\mathbb{F}_{q^2}$, where $a, b \in \mathbb{F}_q^*$ and we completely determined all necessary and sufficient conditions on a, b such that $f(x)$ is a permutation trinomial of $\mathbb{F}_{q^2}$ in both even and odd characteristic cases.

4 Permutation trinomials of the form $x^3 + bx^{2q+1} + cx^{3q}$ over $\mathbb{F}_{q^2}$, where $b, c \in \mathbb{F}_q^*$

In Zha et al. [42] determined that the polynomials of the form $x^3+x^{2q+1}+x^{3q}$ are permutation polynomials over $\mathbb{F}_{q^2}$, where $q = 2^m$ iff m is odd (see [42, Theorem 4.1]). Inspired by this result, in this section we study the permutation properties of the more general polynomial $f(x) = x^3 + bx^{2q+1} + cx^{3q}$ over $\mathbb{F}_{q^2}$, where $b, c \in \mathbb{F}_q^*$ in both odd and even characteristic cases (see Remark 2 below).

We first observe that,

$$f(x) = x^3 + bx^{2q+1} + cx^{3q} = x^3(1 + bx^{2q-2} + cx^{3q-3}) = x^3h(x^{q-1}),$$

Table 2 List of all pairs of coefficients (a, b) of permutation polynomials of $\mathbb{F}_{81}$ of the form $f(x) = x^3h(x^{q-1})$, where $h(x) = bx^2 + ax + 1$, with $a, b \in \mathbb{F}_9^*$ and $x^2 + 2x + 2 \in \mathbb{F}_3[x]$ is the minimal polynomial of α obtained by Theorem 1

(a, b)	$(\alpha^2, 1)$	(α^5, α)	$(\alpha^6, 1)$	(α^7, α^3)	$(1, 2)$

Table 3 List of all pairs of coefficients (a, b) of permutation polynomials of $\mathbb{F}_{64}$ of the form $f(x) = x^3h(x^{q-1})$, where $h(x) = bx^2 + ax + 1$, with $a, b \in \mathbb{F}_8^*$ and $x^3 + x + 1 \in \mathbb{F}_2[x]$ is the minimal polynomial of α, obtained by Theorem 2

(a, b)	(α, α^4)	,(α^2, α)	$(\alpha^3, 1)$	(α^4, α^2)	$(\alpha^5, 1)$	$(\alpha^6, 1)$

where $h(x) = 1 + bx^2 + cx^3$ with $b, c \in \mathbb{F}_q^*$. As we plan to apply Lemma 1, we must first find out $b, c \in \mathbb{F}_q^*$ for which the polynomial $h(x) = 1 + bx^2 + cx^3 \in \mathbb{F}_q^*[x]$ have roots in μ_{q+1}.

Proposition 5 *Let $h(x) = 1 + bx^2 + cx^3 \in \mathbb{F}_q[x]$ where $b, c \in \mathbb{F}_q^*$. Assume that $h(1) = 1 + b + c \neq 0$, $h(-1) = 1 + b - c \neq 0$. Then there exists $x \in \mu_{q+1}$ such that $h(x) = 0$ if and only if one the following conditions hold according to the characteristic of the finite field $\mathbb{F}_q$:*

(i) $b = 1 - c^2$ and $\mathrm{Tr}(1/c) = 1$ if char$(\mathbb{F}_q)$ is even.
(ii) $b = 1 - c^2$ and $c^2 - 4$ is a nonsquare in $\mathbb{F}_q$ if char$(\mathbb{F}_q)$ is odd.

Proof We first claim that if $h(x)$ has a root in μ_{q+1} then it must be in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Assume that there exists $x \in \mu_{q+1} \cap \mathbb{F}_q$ such that $h(x) = 0$, then we have $x = x^q = 1/x$ implying $x^2 = 1$, that is, $x = 1$ or $x = -1$ both of which contradict with the assumptions $h(1) \neq 0$ and $h(-1) \neq 0$. Now, let $x \in \mu_{q+1}$ such that $h(x) = 0$, that is, $x^q = 1/x$ and

$$1 + bx^2 + cx^3 = 0 \Leftrightarrow x^3 + \frac{b}{c}x^2 + \frac{1}{c} = 0.$$

Taking the q-th power of the equation $1 + bx^2 + cx^3 = 0$ and inserting $x^q = 1/x$ we obtain

$$1 + bx^{2q} + cx^{3q} = 1 + b\frac{1}{x^2} + c\frac{1}{x^3} = 0 \Leftrightarrow x^3 + bx + c = 0. \tag{26}$$

Hence, there exists $x \in \mu_{q+1}$ such that $h(x) = 0$ if and only if the following system

$$\left.\begin{aligned} x^3 + bx + c = 0 \\ x^3 + \frac{b}{c}x^2 + \frac{1}{c} = 0 \end{aligned}\right\} \tag{27}$$

holds. Subtracting the equations in the above system (27) we get:

$$\frac{b}{c}x^2 - bx + \frac{1}{c} - c = 0 \tag{28}$$

and then multiplying the equation in (28) by $\frac{c}{b}$ we have:

$$x^2 - cx + \frac{1}{b} - \frac{c^2}{b} = 0. \tag{29}$$

Letting $\delta = \frac{1 - c^2}{b}$, the equation in (29) becomes

$$x^2 - cx + \delta = 0. \tag{30}$$

Here, we note that $\delta \neq 0$, because otherwise the equation in (30) implies that either $x = 0$ or $x = c$, which contradicts with the claim as $0, c \in \mathbb{F}_q$. Note also that $\delta \in \mathbb{F}_q$. Taking the

q-th power of the equation in (30) and substituting $x^q = 1/x$, we obtain

$$\frac{1}{x^2} - \frac{c}{x} + \delta = 0 \Leftrightarrow \delta x^2 - cx + 1 = 0 \Leftrightarrow x^2 - \frac{c}{\delta}x + \frac{1}{\delta} = 0. \tag{31}$$

Now, subtracting the equations in (30) and (31) we have

$$-cx + \frac{c}{\delta}x + \delta - \frac{1}{\delta} = 0, \tag{32}$$

which is equivalent to

$$c\left(\frac{1}{\delta} - 1\right)x + \frac{\delta^2 - 1}{\delta} = 0 \Leftrightarrow c(1-\delta)x + (\delta^2 - 1) = 0. \tag{33}$$

If $\delta \neq 1$, then by the equation in (33) we get

$$cx - (\delta + 1) = 0 \Leftrightarrow x = \frac{\delta + 1}{c},$$

which contradicts with the claim, since $\dfrac{\delta+1}{c} = \dfrac{1 - c^2 + b}{bc} \in \mathbb{F}_q$. Thus, $\delta = 1$, that is, $b = 1 - c^2$, so the proof of the first condition in both cases is complete. First, assume that $char(\mathbb{F}_q) = 2$. Using the equation in (30) and that $\delta = 1$, we obtain

$$x^2 + cx = 1 \iff \frac{x^2}{c^2} + \frac{x}{c} = \frac{1}{c^2} \iff y^2 + y = \frac{1}{c^2} \tag{34}$$

where $y = x/c$. Note that, if $\mathrm{Tr}(1/c^2) = \mathrm{Tr}(1/c) = 0$ then $y = x/c \in \mathbb{F}_q$, so $x \in \mathbb{F}_q \cap \mu_{q+1} = \{1\}$ which is not possible by the assumption $h(1) \neq 0$, therefore $\mathrm{Tr}(1/c) = 1$. Next, assume that $char(\mathbb{F}_q)$ is odd. Using the equation in (30) and that $\delta = 1$, we obtain

$$x^2 - cx + 1 = x^2 - cx + \frac{c^2}{4} + 1 - \frac{c^2}{4} = 0 \Leftrightarrow x^2 - cx + \frac{c^2}{4} = \frac{c^2 - 4}{4},$$

which holds if and only if

$$\left(x - \frac{c}{2}\right)^2 = \frac{c^2 - 4}{4}. \tag{35}$$

Using the equation in (35) and the claim, we obtain that $\dfrac{c^2-4}{4}$ must be a nonsquare in $\mathbb{F}_q$, or equivalently $c^2 - 4$ must be a nonsquare in $\mathbb{F}_q$ and this completes the proof of the secod condition. □

Now, suppose that $h(x)$ has no roots in μ_{q+1}, then for any $x \in \mu_{q+1}$ we have:

$$x^3 h(x)^{q-1} = \frac{x^3(1 + bx^{2q} + cx^{3q})}{1 + bx^2 + cx^3} = \frac{x^3(1 + bx^{-2} + cx^{-3})}{1 + bx^2 + cx^3} = \frac{x^3 + bx + c}{cx^3 + bx^2 + 1}.$$

Let $g(x) = \dfrac{x^3 + bx + c}{cx^3 + bx^2 + 1}$, $\phi(x) = \dfrac{x + z}{x + z^q}$ and thus $\phi^{-1}(x) = \dfrac{xz^q - z}{1 - x}$, where $z \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Let $\mathbb{F}_q$ be a finite field of odd characteristic and $z^q = -z$, $z \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. We define $\Delta(z; x) := (x+z)^3 + b(x+z)(x+z^q)^2 + c(x+z^q)^3$ and so we obtain $\Delta(z^q; x) = c(x+z)^3 + b(x+z)^2(x+z^q) + (x+z^q)^3$. Then we have

$$(g \circ \phi)(x) = \frac{\Delta(z; x)}{\Delta(z^q; x)} = \frac{(x+z)^3 + b(x+z)(x+z^q)^2 + c(x+z^q)^3}{c(x+z)^3 + b(x+z)^2(x+z^q) + (x+z^q)^3}$$

and thus

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

where

$$\Delta(z;x)z^q - z\Delta(z^q;x) = -2z\left((1+b+c)x^3 + z^2(3-b+3c)x\right)$$

and

$$\Delta(z^q;x) - \Delta(z;x) = 2z\left((3c+b-3)x^2 + z^2(c-1-b)\right).$$

Thus,

$$(\phi^{-1} \circ g \circ \phi)(x) = \frac{\Delta(z;x)z^q - z\Delta(z^q;x)}{\Delta(z^q;x) - \Delta(z;x)} = -\frac{(1+b+c)x^3 + z^2(3+3c-b)x}{(3c+b-3)x^2 + z^2(c-1-b)}.$$

First we deal with the case where $3-b-3c=0$ in the following proposition.

Proposition 6 *Let $\mathbb{F}_q$ be finite field of odd characteristic, where $\gcd(3, q-1) = 1$. Let $h(x) = 1 + bx^2 + cx^3$ with $b, c \in \mathbb{F}_q^*$. Assume that $3-b-3c=0$. There are no permutation polynomials of the form $f(x) = x^3 h(x^{q-1})$ of $\mathbb{F}_{q^2}$ in this case.*

Proof The proof can be done in an analogous way to Proposition 2 therefore we omit the proof in order not to repeat the similar long discussions. □

Next, assume that $3-b-3c \neq 0$. Note also that $1+b-c \neq 0$, $1+b+c \neq 0$ since $h(-1) \neq 0$, $h(1) \neq 0$. Then we have:

$$\frac{x^3 + z^2 \dfrac{(3-b+3c)}{(1+b+c)x}}{x^2 + \dfrac{(1+b-c)}{(3-b-3c)} z^2} = \frac{x^3 + Ax}{x^2 + B}, \tag{36}$$

where $A = z^2 \dfrac{(3-b+3c)}{1+b+c}$ and $B = z^2 \dfrac{(1+b-c)}{3-b-3c}$. First, we consider the case where $-B$ is a square in $\mathbb{F}_q$. In this case there exists $x \in \mathbb{F}_q$ such that the denominator of the fraction in (36), that is $x^2 + B$, becomes zero which implies that ∞ has at least three distinct preimages under the map $(\phi^{-1} \circ f \circ \phi)(x)$ and therefore $f(x)$ is not a permutation polynomial. Thus, from here on assume that $-B$ is not a square in $\mathbb{F}_q$, that is, $\frac{(1+b-c)}{3c+b-3}$ is a square in $\mathbb{F}_q$ since $z \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Computing $\dfrac{\dfrac{x^3+Ax}{x^2+B} - \dfrac{y^3+Ay}{y^2+B}}{x-y}$ and simplifying one gets:

$$\mathcal{C}(x, y) := x^2y^2 + (B-A)xy + B(x^2+y^2) + AB. \tag{37}$$

That is, $(\phi^{-1} \circ g \circ \phi)$ permutes $\mathbb{F}_q$ if and only $\mathcal{C}(x, y)$ defined in (37) is not zero for any $x, y \in \mathbb{F}_q$ with $x \neq y$.

The following theorem completes the problem in the remaining case for finite fields of odd characteristic, where $3-b-3c \neq 0$.

Theorem 7 *Let $\mathbb{F}_q$ be a finite field of odd characteristic, where $gcd(3, q-1) = 1$. Let $h(x) = 1 + bx^2 + cx^3$ with $b, c \in \mathbb{F}_q^*$. Assume that $3-b-3c \neq 0$. Then $x^3 h(x^{q-1})$ is a permutation polynomial of $\mathbb{F}_{q^2}$ iff one of the following conditions hold:*

Table 4 List of all pairs of coefficients (b, c) of permutation polynomials of $\mathbb{F}_{25}$ of the form $f(x) = x^3h(x^{q-1})$, where $h(x) = 1 + bx^2 + cx^3$, with $b, c \in \mathbb{F}_5^*$, obtained by Theorem 3

(b, c)	$(2, 4)$	$(2, 1)$

(i) $b = 1 - c^2$ *and* $c^2 - 4$ *is a nonzero square in* $\mathbb{F}_q$,

(ii) $char(\mathbb{F}_q) \neq 3$, $b = -3$, $c \neq -2, 2$ *and* $\dfrac{4 - c^2}{3}$ *is a nonzero square in* $\mathbb{F}_q$.

Proof The proof can be done in an analogous way to Theorem 1 therefore we omit the proof in order not to repeat the similar long discussions on all possible decompositions. □

Now, let $\mathbb{F}_q$ be a finte field with even characteristic. The following theorem is the main result of this section in even characteristic case.

Theorem 8 *Let* $\mathbb{F}_q$ *be a finite field of even characteristic, where* $q = 2^{2k+1}, k \in \mathbb{N}$. *Let* $h(x) = 1 + bx^2 + cx^3$ *with* $b, c \in \mathbb{F}_q^*$. *Then* $x^3h(x^{q-1})$ *is a permutation polynomial of* $\mathbb{F}_{q^2}$ *iff one of the following conditions hold:*

(i) $b = 1 + c^2$ *and* $\mathrm{Tr}(1/c) = 0$,
(ii) $b = 1$ *and* $\mathrm{Tr}(1/c) = 1$.

Proof The proof can be done in an analogous way to Theorem 2 therefore we omit the proof in order not to repeat the similar long discussions on all possible decompositions. □

Example 3 In the following tables we explicitly give the coefficients over the finite fields $\mathbb{F}_5, \mathbb{F}_7, \mathbb{F}_9$ and $\mathbb{F}_{11}$ of all permutation polynomials obtained from Theorem 3. Here, $\mathbb{F}_5$ is the smallest nontrivial finite field containing coefficients b, c which give rise to permutation polynomials of the form $f(x) = x^3h(x^{q-1})$ of $\mathbb{F}_{25}$, where $h(x) = 1 + bx^2 + cx^3$ with $b, c \in \mathbb{F}_5^*$. In Tables 4, 5, 6 and 7 below we list all pairs of coefficients (b, c) of permutation polynomials of $\mathbb{F}_{q^2}$ of the form $f(x) = x^3h(x^{q-1})$, where $h(x) = 1 + bx^2 + cx^3$ with $b, c \in \mathbb{F}_q^*$, obtained by Theorem 3 for $q = 5, 7, 9, 11$ respectively. Note that, in Table 6, $x^2 + 2x + 2 \in \mathbb{F}_3[x]$ is the minimal polynomial of α, that is $\mathbb{F}_9^* =< \alpha >$.

Example 4 In the following table we explicitly give the coefficients over the finite field $\mathbb{F}_8$ of all permutation polynomials of $\mathbb{F}_{64}$ obtained from Theorem 2. Let $x^3 + x + 1 \in \mathbb{F}_2[x]$ be the minimal polynomial of α, that is $\mathbb{F}_8^* =< \alpha >$. In Table 8 below we list all pairs of coefficients (b, c) of permutation polynomials of $\mathbb{F}_{64}$ of the form $f(x) = x^3h(x^{q-1})$, where $h(x) = 1 + bx^2 + cx^3$, with $b, c \in \mathbb{F}_8^*$ obtained by Theorem 2.

Remark 2 In [42] Zha, Hu and Fan found out that the polynomials of the form $x^3+x^{2q+1}+x^{3q}$ are permutation polynomials over $\mathbb{F}_{q^2}$, where $q = 2^m$ iff m is odd (see [42, Theorem 4.1]).

Table 5 List of all pairs of coefficients (b, c) of permutation polynomials of $\mathbb{F}_{49}$ of the form $f(x) = x^3h(x^{q-1})$, where $h(x) = 1 + bx^2 + cx^3$, with $b, c \in \mathbb{F}_7^*$, obtained by Theorem 3

(b, c)	$(4, 6)$	$(4, 1)$

Table 6 List of all pairs of coefficients (b, c) of permutation polynomials of $\mathbb{F}_{81}$ of the form $f(x) = x^3h(x^{q-1})$, where $h(x) = 1 + bx^2 + cx^3$, with $b, c \in \mathbb{F}_9^*$, obtained by Theorem 7

(b, c)	$(2, \alpha^2)$	$(2, \alpha^6)$

In this section we worked on the more general polynomial $f(x) = x^3 + bx^{2q+1} + cx^{3q}$ over $\mathbb{F}_{q^2}$, where $b, c \in \mathbb{F}_q^*$ for both odd and even characteristic cases and we completely determined all necessary and sufficient conditions for $f(x)$ to be a permutation polynomial of $\mathbb{F}_{q^2}$.

5 A comparison with known permutation trinomials

Definition 1 [36] Two permutation polynomials $f(x), g(x) \in \mathbb{F}_q[x]$ are called quasi-multiplicative equivalent (abbreviated as QM equivalent), if there exists $d \in \mathbb{Z}, 1 \leq d \leq q-1$ with $\gcd(d, q-1) = 1$ and $f(x) = ag(cx^d)$, where $a, c \in \mathbb{F}_q^*$.

The above definition which was introduced by Wu, Yuan, Ding and Ma [41], is being used in the literature (see for instance [12, 33, 36]) in order to decide whether permutations which are proposed to be new are really new or not. In general it is nontrivial to determine the QM equivalence of two permutation polynomials theoretically.

In this section we prove that the classses of permutation trinomials obtained in this paper are not QM equivalent to 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 permuation trinomials found in this paper with known permutation trinomials over $\mathbb{F}_{q^2}$. We use the method in [36] for this purpose.

In order to determine whether the permutation polynomials $f(x) = x^3(1 + ax^{q-1} + bx^{2(q-1)})$ and $f(x) = x^3(1 + bx^{2q-2} + cx^{3q-3})$ over $\mathbb{F}_{q^2}$, where $a, b, c \in \mathbb{F}_q^*$ are QM equivalent to any permutation trinomial of the form $g(x) = a_1x^{k_1} + a_2x^{k_2} + a_3x^{k_3} \in \mathbb{F}_q[x]$ 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 $\{k_1, k_2, k_3 \bmod (q^2 - 1)\} = \{3k, (q + 2)k, (2q + 1)k\}$.
Step 2: Comparison of the coefficients of $b_2 f(b_1x^k)$ and $g(x)$.

In the above strategy, if Step 1 is not satisfied then $f(x)$ and $g(x)$ will not be QM equivalent, otherwise we will go on with Step 2 and compare the coefficients of $b_2 f(b_1x^k)$ and $g(x)$. In Step 1 we observe that in any permutation polynomial which is QM equivalent to our classes of permutation polynomials, at least one of the k_i's must be a multiple of 3. For this purpose we constructed Table 9 by collecting all known permutation trinomials of this form over finite fields of both even and odd characteristic.

Let $f(x) = x^3(1+ax^{q-1}+bx^{2(q-1)})$ which we considered in Section 3. First we compare $f(x)$ with the polynomial $g_1(x) = x^3 + x^{3.2^m} + x^{2^{m+2}-1} \in \mathbb{F}_{2^{2m}}[x]$ in [14, Theorem 3.5] in

Table 7 List of all pairs of coefficients (b, c) of permutation polynomials of $\mathbb{F}_{121}$ of the form $f(x) = x^3h(x^{q-1})$, where $h(x) = 1 + bx^2 + cx^3$, with $b, c \in \mathbb{F}_{11}^*$, obtained by Theorem 7

(b, c)	$(8, 5)$	$(8, 10)$	$(8, 6)$	$(8, 1)$	$(7, 4)$	$(7, 7)$	$(3, 8)$	$(2, 3)$

Table 8 List of all pairs of coefficients (b, c) of permutation polynomials of $\mathbb{F}_{64}$ of the form $f(x) = x^3h(x^{q-1})$, where $h(x) = 1 + bx^2 + cx^3$, with $b, c \in \mathbb{F}_8^*$, obtained by Theorem 8

(b, c)	(α, α^5)	(α^2, α^3)	$(1, \alpha)$	$(1, \alpha^2)$	$(1, \alpha^4)$	$(1, 1)$	(α^4, α^6)

Table 9. Note that $3 \mid q^2 - 1$, where $q = 2^m$. Let $(a_1, a_2, a_3) = (3, 3 + (q - 1), 3 + 2(q - 1))$ and $(b_1, b_2, b_3) = (3, 3q, 4q - 1)$. Note that $\{a_1, a_2, a_3\}$ is the set of the exponents of $f(x)$ and $\{b_1, b_2, b_3\}$ is the set of exponents of $g_1(x)$. Assume that there exists an integer k, $1 \le k \le q^2 - 1$ with $\gcd(k, q^2 - 1) = 1$ such that $\{ka_1 \pmod{q^2 - 1}, ka_2 \pmod{q^2 - 1}, ka_3 \pmod{q^2 - 1}\} = \{b_1, b_2, b_3\}$. As $3 \mid q^2 - 1$, $b_1 \equiv 0 \pmod 3$ and $b_2 \equiv 0 \pmod 3$ then it is necessary that there are at least two elements $a \in \{a_1, a_2, a_3\}$ such that $a \equiv 0 \pmod 3$. However $a_2 \not\equiv 0 \pmod 3$ and $a_3 \not\equiv 0 \pmod 3$. This proves that $f(x)$ can not be QM equivalent to $g_1(x)$. Let $g_i(x)$ be the corresponding polynomial in the i-th row of Table 9 for $i = 1, 2, 3, 4, 5$. The same argument we used above works for $g_i(x)$ for $1 \le i \le 3$ and hence $f(x)$ is not QM equivalent to $g_i(x)$ for $1 \le i \le 3$. Next we consider $g_i(x)$ for $i = 4, 5$. Note that $\gcd(3, q - 1) = 1$ for $f(x)$. Hence, if $char(\mathbb{F}_q) \ne 3$ then $3 \mid q^2 - 1$. The same argument we used above works for $g_i(x)$ for $i = 4, 5$ when $char(\mathbb{F}_q) \ne 3$. Assume that $char(\mathbb{F}_q) = 3$. Then $8 \mid q^2 - 1$. In this case $q - 1 \equiv 0$ or $2 \pmod 8$. Let (a_1, a_2, a_3) be the exponents as above and let $(b_1, b_2, b_3) = 3(q - 1, q - 1, 3)$ be the exponents of $g_i(x)$. Note that $a_j \not\equiv 0 \pmod 8$ for $1 \le j \le 3$. However $b_1 \equiv 0$ or $6 \pmod 8$. Hence it is impossible to choose $1 \le k \le q^2 - 1$ such that $\gcd(k, q^2 - 1) = 1$ and $ka_j \equiv b \pmod{q^2 - 1}$. This completes the proof of the fact that $f(x)$ can not be QM equivalent to any $g_i(x)$ in Table 9 for each $1 \le i \le 5$. Let $f(x) = x^3(1 + bx^{2q-2} + cx^{3q-3})$ that we considered in Section 4. Assume that $f(x)$ is QM equivalent to $g_1(x)$ in Table 9. This implies that there exists $\alpha, \beta \in \mathbb{F}_{q^2}$ and $1 \le k \le q^2 - 1$ with $\gcd(k, q^2 - 1) = 1$ such that $\alpha g_1(\beta x^k) = f(x)$. Consequently we obtain that either

$$\alpha\beta^3 = 1, \alpha\beta^{4q-1} = b, \alpha\beta^{3q} = c \tag{38}$$

or

$$\alpha\beta^3 = c, \alpha\beta^{3q} = 1, \alpha\beta^{4q-1} = b. \tag{39}$$

If (38) and (26) hold, then $b = c = 1$. This completes the proof of the fact that $f(x)$ in Section 4 is not QM equivalent to $g_1(x)$ if $(b, c) \ne (1, 1)$. The argument above also show that $f(x)$ in Section 4 is not QM equivalent to $g_i(x)$ with $1 \le i \le 3$ if $(b, c) \ne (1, 1)$.

Table 9 List of all known classes of permutation trinomials of the form $ax^{3r} + bx^s + cx^t$ over $\mathbb{F}_{q^2}$

i	$g_i(x)$	condition(s) on m	Reference
1	$x^3 + x^{3.2^m} + x^{2^{m+2}-1} \in \mathbb{F}_{2^{2m}}[x]$	m is odd	[14, Theorem 3.5]
2	$x^3 + x^{2^{m+1}+1} + x^{3.2^m} \in \mathbb{F}_{2^{2m}}[x]$	m is odd	[42, Theorem 4.1]
3	$x^3 + x^{2^m+2} + x^{3.2^m} \in \mathbb{F}_{2^{2m}}[x]$	m is odd	[42, Theorem 4.2]
4	$x^{3(q-1)} + bx^{q-1} + cx^3 \in \mathbb{F}_{2^{2m}}[x]$		[31, Theorem 4]
5	$x^{3(q-1)} + bx^{q-1} + cx^3 \in \mathbb{F}_{q^2}[x]$, q odd		[31, Theorem 8]

Similarly we observe that the polynomial $f(x)$ in Section 4 is not QM equivalent to $g_4(x)$ and $g_5(x)$. Thus the classes of permutation polynomials obtained in this paper are completely new except the case $(b, c) = (1, 1)$ for the polynomial $f(x) = x^3(1 + bx^{2q-2} + cx^{3q-3})$.

Acknowledgements The authors would like to thank the anonymous referees for their valuable comments and helpful suggestions which improved both the quality and presentation of this paper.

Author Contributions Ferruh Özbudak and Burcu Gülmez Temür contributed equally to this work.

Funding Not applicable.

Data Availability Not applicable.

Declarations

Conflicts of Interest Not applicable.

Ethical standard Not applicable.

Consent for publication Not applicable.

References

1. Aubry, Y., McGuire, G., Rodier, F.: A few more functions that are not APN infinitely often, Finite fields: theory and applications, Contemp. Math., 518, Amer. Math. Soc., Providence, RI, 23–31 (2010)
2. Bartoli, D., Quoos, L.: Permutation polynomials of the type $x^r g(x^s)$ over $\mathbb{F}_{q^{2n}}$. Des. Codes Cryptogr. **86**, 1589–1599 (2018)
3. Akbary, A., Wang, Q., On polynomials of the form $x^r f(x^{(q-1)/l})$, Int. J. Math. Math. Sci., Art. ID 23408, 7 pp. (2007)
4. Bartoli, D.: On a conjecture about a class of permutation trinomials. Finite Fields Appl. **52**, 30–50 (2018)
5. Giulietti, M.: Bartoli, D. Permutation polynomials, fractional polynomials, and algebraic curves, Finite Fields Appl. **51**, 1–16 (2018)
6. Bartoli, D., Timpanella, M.: A family of permutation trinomials over $\mathbb{F}_q^2$. Finite Fields Appl. **70**, 101718 (2021)
7. Bartoli, D., Timpanella, M.: On trinomials of type $x^{n+m}(1 + Ax^{m(q-1)} + Bx^{n(q-1)})$, n, m odd, over $\mathbb{F}_{q^2}$, $q = 2^{2s+1}$. Finite Fields Appl. **72** (2021)
8. Bartoli, D., Zhou, Y.: Exceptional scattered polynomials, J. Algebra **509**, 507–534 (2018)
9. Caullery, F., Schmidt, K.-U.: On the classification of hyperovals, Adv. Math. **283**, 195-203 (2015)
10. Caullery, F., Schmidt, K.-U., Zhou, Y.: Exceptional planar polynomials. Des. Codes Cryptogr. **78**(3), 605–613 (2016)
11. Dickson, L.E.: 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)
12. Gupta, R., Gahlyan, P., Sharma, R.K.: New classes of permutation trinomials over $\mathbb{F}_q^3$. Finite Fields Appl. **84**, 102110 (2022)
13. Gupta, R., Sharma, R.K.: Some new classes of permutation trinomials over finite fields with even characteristic. Finite Fields Appl. **41**, 89–96 (2016)
14. Gupta, R., Sharma, R.K.: Some new classes of permutation trinomials over finite fields with even characteristic. Finite Fields Appl. **41**, 89–96 (2016)
15. Hermite, Ch.: Sur les fonctions de sept lettres, C.R. Acad. Sci. Paris **57**, 750–757 (1863)
16. Hernando, F., McGuire, G.: Proof of a conjecture of Segre and Bartocci on monomial hyperovals in projective planes, Des. Codes Cryptogr. **65**(3) , 275–289 (2012)
17. Hou, X.: Permutation polynomials over finite fields - a survey of recent advances. Finite Fields Appl. **32**, 82–119 (2015)
18. Hou, X.: Determination of a type of permutation trinomials over finite fields II. Finite Fields Appl. **35**, 16–35 (2015)
19. Hou, X.: 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

20. Hou, X.: Lectures on finite fields, Graduate Studies in Mathematics, 190. American Mathematical Society, Providence, RI (2018)
21. Hou, X.: On the Tu-Zeng permutation trinomial of type $(1/4, 3/4)$. Discrete Math. **344**(3), 112241 (2021)
22. Hou, X., Tu, Z., Zeng, X.: Determination of a class of permutation trinomials in characteristic three. Finite Fields Appl. **61**, 1–27 (2020)
23. Janwa, H., Wilson, R.M.: Hyperplane sections of Fermat varieties in P^3 in char.2 and some applications to cyclic codes, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, San Juan, PR, Lecture Notes in Comput. Sci., **673**, 180–194, Springer, Berlin (1993)
24. Leducq, E.: Functions which are PN on infinitely many extensions of $\mathbb{F}_p$, p odd, Des. Codes Cryptogr. **75**(2), 281–299 (2015)
25. Li, N., Helleseth, T.: Several classes of permutation trinomials from Niho exponents. Cryptogr. Commun. **9**, 693–705 (2017)
26. Li, K., Qu, L., Chen, X.: New classes of permutation binomials and permutation trinomials over finite fields. Finite Fields Appl. **43**, 69–85 (2017)
27. Li, K., Qu, L., Wang, Q.: 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)
28. Lidl, R., Niederreiter, H.: Finite Fields. Encyclopedia of Mathematics and its Applications), Cambridge University Press, Cambridge (1997)
29. Bosma W., Cannon J., and Playoust C.: The Magma algebra system. I. The user language, J. Symbolic Comput. **24**, 1179–1260 (1997)
30. Mullen, G.L., Panario, D.: Handbook of Finite Fields, Discrete Mathematics and its Applications. Boca Raton), CRC Press, Boca Raton, FL (2013)
31. Özbudak, F., Gülmez Temür, B.: 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 $\mathbb{F}b, c \in^*$, Des. Codes Cryptogr., https://doi.org/10.1007/s10623-022-01052-0
32. Özbudak, F., Gülmez Temür, B.: A survey on permutation polynomials over finite fields, to appear in Foundational principles of error-correcting codes and related concepts, Springer Lecture Notes in Mathematics
33. Pang, T., Xu, Y., Li, N., Zeng, X.: Permutation polynomials of the form $x^d + L(x^s)$ over $\mathbb{F}_q^3$. Finite Fields Appl. **76**, 101906 (2021)
34. Park, Y.H., Lee, J.B.: Permutation polynomials and group permutation polynomials. Bull. Austral. Math. Soc. **63**, 67–74 (2001)
35. Rodier, F.: Borne sur le degré des polynômes presque parfaitement non-linéaires, Arithmetic, geometry, cryptography and coding theory, 169–181, Contemp. Math., 487, Amer. Math. Soc., Providence, RI, 2009
36. Tu, Z., Zeng, X., Li, C., Helleseth, T.: A class of new permutation trinomials. Finite Fields Appl. **50**, 178–195 (2018)
37. Tu, Z., Zeng, X., Jiang, Y., Li, Y.: Binomial permutations over finite fields with even characteristic. Des. Codes Cryptogr. **89**, 2869–2888 (2021)
38. Wan, D., Lidl, R.: Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure. Monatshefte Math. **112**, 149–163 (1991)
39. Wang, Q.: Cyclotomic mapping permutation polynomials over finite fields, Sequences, subsequences, and consequences, Lecture Notes in Comput. Sci., 4893, Springer, Berlin, 119–128, (2007)
40. Wang, Q.: Polynomials over finite fields: an index approach, in: Combinatorics and Finite Fields, Difference Sets, Polynomials, Pseudorandomness and Applications, De Gruyter, 319–348 (2019)
41. Wu, D., Yuan, P., Ding, C., Ma, Y.: Permutation trinomials over $\mathbb{F}_{2^m}$. Finite Fields Appl. **46**, 38–56 (2017)
42. Zha, Z., Hu, L., Fan, S.: Further results on permutation trinomials over finite fields with even characteristic. Finite Fields Appl. **45**, 43–52 (2017)
43. Zieve, M.E.: 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)
44. Zieve, M.E.: Planar functions and perfect nonlinear monomials over finite fields. Des. Codes Cryptogr. **75**(1), 71–80 (2015)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.