Turkish Journal of Mathematics

Volume 48 | Number 4 Article 11

7-3-2024

On a class of permutation trinomials over finite fields

BURCU GÜLMEZ TEMÜR

BUKET ÖZKAYA

Turkish Journal of Mathematics

http://journals.tubitak.gov.tr/math/

Research Article

Turk J Math
(2024) 48: 778 – 792
© TÜBİTAK
doi:10.55730/1300-0098.3540

On a class of permutation trinomials over finite fields

Burcu GÜLMEZ TEMÜR[1], **Buket ÖZKAYA**[2,*]
[1]Department of Mathematics, Atılım University, Ankara, Turkiye
[2]Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkiye

Received: 18.06.2023 • **Accepted/Published Online:** 06.05.2024 • **Final Version:** 03.07.2024

Abstract: In this paper, we study the permutation properties of the class of trinomials of the form $f(x) = x^{4q+1} + \lambda_1 x^{q+4} + \lambda_2 x^{2q+3} \in \mathbb{F}_{q^2}[x]$, where $\lambda_1, \lambda_2 \in \mathbb{F}_q$ and they are not simultaneously zero. We find all necessary and sufficient conditions on λ_1 and λ_2 such that $f(x)$ permutes $\mathbb{F}_{q^2}$, where q is odd and $q = 2^{2k+1}, k \in \mathbb{N}$.

Key words: Permutation polynomials, finite fields, Hasse-Weil bound, cryptography

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 $\mathbb{F}_q$ whenever the associated function $g : a \mapsto g(a)$ is a permutation of $\mathbb{F}_q$. Permutation polynomials have many applications in areas such as cryptography, coding theory, and combinatorial designs. The studies on permutation polynomials goes back to work done by Dickson and Hermite (see, [6, 9]). There are several books on finite fields such as [19] and Chapter 8 in [20], which are very helpful for the interested reader to get into the topic. Moreover, the survey papers (see, [10, 12, 27]) are also useful as they consist of many of the recent results on permutation polynomials over finite fields. We refer the interested reader to [3, 4, 8, 11, 17, 18, 21] and the references therein for more results on permutation polynomials over finite fields.

There has been a great interest in permutation polynomials with a few terms because of their simple algebraic structures and extraordinary properties. In this paper, our aim is to determine the permutation properties of the class of trinomials of the form $f(x) = x^{4q+1} + \lambda_1 x^{q+4} + \lambda_2 x^{2q+3} \in \mathbb{F}_{q^2}[x]$, where $\lambda_1, \lambda_2 \in \mathbb{F}_q$ which are not simultaneously zero.

The paper is organized as follows: In Section 2, we introduce the basic tools that we use throughout the paper. We note that the polynomial $f(x) = x^{4q+1} + \lambda_1 x^{q+4} + \lambda_2 x^{2q+3}$ can be written as $f(x) = x^5 h(x^{q-1})$, where $h(x) = \lambda_1 x + \lambda_2 x^2 + x^4$. In Section 3, we determine the necessary and sufficient conditions for which $h(x)$ has no roots in μ_{q+1}, where $\mu_{q+1} = \{a \in \mathbb{F}_{q^2}^* \mid a^{q+1} = 1\}$. In Sections 4 and 5, we determine all necessary and sufficient conditions for $f(x)$ to be a PP of $\mathbb{F}_{q^2}$ in even characteristic with q of the form $q = 2^{2k+1}, k \in \mathbb{N}$, and in odd characteristic, respectively.

*Correspondence: ozkayab@metu.edu.tr
2010 *AMS Mathematics Subject Classification:* 11T06, 11T71, 12E10

2. Preliminaries

There is a well known criterion due to Wan and Lidl [25], Park and Lee [22], Akbary and Wang [1], Wang [26] and Zieve [28], which is widely used in order to determine 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. It is given in the following lemma.

Lemma 1 *[1, 22, 25, 26, 28] 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 this paper, we plan to apply Lemma 1 over the finite field $\mathbb{F}_{q^2}$ with $d = q+1$, but 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 $\Phi : \mathbb{F}_q \cup \{\infty\} \longrightarrow \mu_{q+1}$ be the map defined by $\Phi(x) = \dfrac{x+z}{x+z^q}$, where $\Phi(\infty) = 1$. It is somewhat easy 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.

One can find out 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 $\left(\Phi^{-1} \circ g \circ \Phi\right)$ is one to one on $\mathbb{F}_q \cup \{\infty\}$. An analogous idea has been used in a few more studies before, see for instance [2, 3, 13, 21].

This situation can be easily followed in the diagram below:

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

Moreover, our suitable choice of $z \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ results in simpler computations.

3. Roots of $h(x)$ in μ_{q+1}

Assuming the notation above, we define $g(x) := x^5 h(x)^{q-1}$, where $h(x) = \lambda_1 x + \lambda_2 x^2 + x^4$, in order to apply Lemma 1. Before studying when $g(x)$ permutes μ_{q+1}, we have to make sure that $g(x)$ has no roots in μ_{q+1}. As $0 \notin \mu_{q+1}$, we have to consider the roots of $h(x)$. First, note that $\mu_{q+1} \cap \mathbb{F}_q = \{-1, 1\}$. So, $h(1) = \lambda_1 + \lambda_2 + 1$ and $h(-1) = -\lambda_1 + \lambda_2 + 1$ must be nonzero. Next, the following lemma characterizes when $h(x)$ has roots in $\mu_{q+1} \setminus \{1, -1\}$.

Lemma 2 *[7, 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

$m(x) = (x-\theta)(x-\theta^q) = x^2 - (\theta+\theta^q)x + \theta^{q+1} = x^2 + Ax + 1$ 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 $1 = \theta_1\theta_2 = \theta_1^{q+1}$. □

In the following proposition, we determine the conditions for which $h(x)$ does not have any roots in μ_{q+1}. Throughout the paper, the trace function denoted by Tr stands for the absolute trace from $\mathbb{F}_q$ onto $\mathbb{F}_2$.

Proposition 1 *Let $h(x) = \lambda_1 x + \lambda_2 x^2 + x^4 \in \mathbb{F}_q[x]$. Assume that $h(1) = \lambda_1 + \lambda_2 + 1 \neq 0$ and $h(-1) = -\lambda_1 + \lambda_2 + 1 \neq 0$. The polynomial $h(x)$ has no roots in μ_{q+1} if and only if one of the following conditions holds:*

i) $\lambda_2 \neq 1 - \lambda_1^2$ or $\lambda_1^2 - 4$ is a square in $\mathbb{F}_q$, where $\mathbb{F}_q$ is of odd characteristic,

ii) $\lambda_2 \neq 1 - \lambda_1^2$ or $\mathrm{Tr}\left(\frac{1}{\lambda_1}\right) = 0$ when $\lambda_1 \neq 0$, where $\mathbb{F}_q$ is of even characteristic.

Proof Assuming $h(x) = \lambda_1 x + \lambda_2 x^2 + x^4 = (x^2 + Ax + 1)(x^2 + ax + b)$ and solving for A, a, b, we obtain $A = -\lambda_1$, $a = \lambda_1$, $b = 0$ and $-a^2 + 1 = \lambda_2$. Hence, by using Lemma 2 above, we conclude that $h(x)$ has a root in $\mu_{q+1} \setminus \{1, -1\}$ if and only if $\lambda_2 = 1 - \lambda_1^2$ and $x^2 - \lambda_1 x + 1$ is irreducible. In odd characteristic, this is equivalent to say that $h(x)$ has no roots in $\mu_{q+1} \setminus \{1, -1\}$ if and only if $\lambda_2 \neq 1 - \lambda_1^2$ or $\lambda_1^2 - 4$ is a square in $\mathbb{F}_q$ (i.e. $x^2 - \lambda_1 x + 1$ is reducible). In even characteristic, $h(x)$ has no roots in $\mu_{q+1} \setminus \{1, -1\}$ if and only if $\lambda_2 \neq 1 - \lambda_1^2$ or $\mathrm{Tr}\left(\frac{1}{\lambda_1}\right) = 0$, where $\lambda_1 \neq 0$ (see for instance Theorem 2.25 in [19]). □

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

$$\begin{aligned} g(x) = x^5 h(x)^{q-1} &= \frac{x^5(\lambda_1 x^q + \lambda_2 x^{2q} + x^{4q})}{\lambda_1 x + \lambda_2 x^2 + x^4} \\ &= \frac{x^5\left(\lambda_1 \frac{1}{x} + \lambda_2 \frac{1}{x^2} + \frac{1}{x^4}\right)}{\lambda_1 x + \lambda_2 x^2 + x^4} \\ &= \frac{\lambda_1 x^3 + \lambda_2 x^2 + 1}{x^3 + \lambda_2 x + \lambda_1}. \end{aligned}$$

Computing $g \circ \Phi$, we get

$$\begin{aligned} (g \circ \Phi)(x) &= \frac{\lambda_1\left(\frac{x+z}{x+z^q}\right)^3 + \lambda_2\left(\frac{x+z}{x+z^q}\right)^2 + 1}{\left(\frac{x+z}{x+z^q}\right)^3 + \lambda_2\left(\frac{x+z}{x+z^q}\right) + \lambda_1} \\ &= \frac{\lambda_1(x+z)^3 + \lambda_2(x+z)^2(x+z^q) + (x+z^q)^3}{(x+z)^3 + \lambda_2(x+z)(x+z^q)^2 + \lambda_1(x+z^q)^3} \\ &= \frac{\Delta(z,x)}{\Delta(z^q,x)}. \end{aligned}$$

Then

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

Computing the numerator, we get

$$\begin{aligned} N=z^q\Delta(z,x)-z\Delta(z^q,x) &= z^q\lambda_1(x+z)^3+z^q\lambda_2(x+z)^2(x+z^q)+z^q(x+z^q)^3 \\ &- z(x+z)^3-z\lambda_2(x+z)(x+z^q)^2-z\lambda_1(x+z^q)^3. \end{aligned} \tag{2}$$

Similarly, computing the denominator, we obtain

$$\begin{aligned} D=\Delta(z^q,x)-\Delta(z,x) &= (x+z)^3+\lambda_2(x+z)(x+z^q)^2+\lambda_1(x+z^q)^3 \\ &- \lambda_1(x+z)^3-\lambda_2(x+z)^2(x+z^q)-(x+z^q)^3. \end{aligned} \tag{3}$$

4. PPs over finite fields of even characteristic

In this section, we study the permutation properties of the polynomial $f(x)=x^5h(x^{q-1})$ over $\mathbb{F}_{q^2}$, where $h(x)=\lambda_1x+\lambda_2x^2+x^4\in\mathbb{F}_q[x]$ and $\mathbb{F}_q$ is a finite field of even characteristic with $q=2^{2k+1},k\in\mathbb{N}$. We plan to apply Lemma 1 to obtain our results. Note that, according to Lemma 1 (i), we first need to have $5\nmid q-1$. By an inductive argument, one can easily show that $5\mid 2^n-1$ if and only if $n=4k,k\in\mathbb{N}$. Hence, $5\nmid q-1$ under our assumption that q is of the form $q=2^{2k+1},k\in\mathbb{N}$. We also note that when $\lambda_1=\lambda_2=0$, then it is well-known that the monomial $f(x)=x^{4q+1}$ permutes $\mathbb{F}_{q^2}$ if and only if $\gcd(q^2-1,4q+1)=1$ (e.g. see [19, Theorem 7.8]). Hence, we are interested in the case when λ_1 or λ_2 is not zero. The following theorem is our first main result.

Theorem 1 *Let $q=2^{2k+1}$, $k\in\mathbb{N}$. Assume that $h(1)=\lambda_1+\lambda_2+1\neq 0$. Then, $f(x)=x^5h(x^{q-1})$ is a permutation polynomial of $\mathbb{F}_{q^2}$ if and only if $\mathrm{Tr}\left(\frac{\lambda_2}{\lambda_1+\lambda_2+1}\right)\neq 0$ when $\lambda_2\neq 0$ and exactly one of the following conditions holds:*

i) $\lambda_1^2+\lambda_2+1=0$,

ii) $\lambda_2=1$.

Proof Let $z^q=z+1$ and so $z^2=z+1$. Substituting $z^q=z+1$ in the numerator in (2), we obtain

$$N=(\lambda_1+\lambda_2+1)x^3+(\lambda_2+1)x^2+(\lambda_1+\lambda_2)x+\lambda_1+1$$

and similarly substituting $z^q=z+1$ in the denominator in (3), we obtain

$$D=(\lambda_1+\lambda_2+1)(x^2+x)+\lambda_2.$$

Here, note that $\lambda_1+\lambda_2+1=h(1)\neq 0$. So we can write

$$\frac{N}{D}=\frac{x^3+A_2x^2+A_1x+A_0}{x^2+x+B_0},$$

where $A_2 = \dfrac{\lambda_2+1}{\lambda_1+\lambda_2+1}, A_1 = \dfrac{\lambda_1+\lambda_2}{\lambda_1+\lambda_2+1}, A_0 = \dfrac{\lambda_1+1}{\lambda_1+\lambda_2+1}, B_0 = \dfrac{\lambda_2}{\lambda_1+\lambda_2+1}$. Here, x^2+x+B_0 must be nonzero if N and D are coprime, so in that case, we need to assume that $\mathrm{Tr}(B_0) \neq 0$ (see for instance Theorem 2.25 in [19]). If N and D are not coprime, then

$$N = (x^2+x+B_0)(x+d) = x^3+(d+1)x^2+(B_0+d)x+B_0d.$$

By comparing the coefficients, we obtain $d = \dfrac{\lambda_1}{\lambda_1+\lambda_2+1}$ and $A_0 = B_0d \implies \lambda_1^2+\lambda_2+1 = 0$.

Case 1: $\lambda_1^2+\lambda_2+1 = 0$:

If $\lambda_1 = 1$, then $\lambda_2 = 0$, which contradicts $h(1) \neq 0$. Similarly, if $\lambda_1 = 0$, then $\lambda_2 = 1$, which again contradicts $h(1) \neq 0$. If $\lambda_1 \neq 0$ and $\lambda_1 \neq 1$, then we have

$$\mathrm{Tr}(B_0) = \mathrm{Tr}\left(\frac{1-\lambda_1^2}{\lambda_1-\lambda_1^2}\right) = \mathrm{Tr}\left(\frac{(1-\lambda_1)(1+\lambda_1)}{\lambda_1(1-\lambda_1)}\right) = \mathrm{Tr}\left(\frac{1+\lambda_1}{\lambda_1}\right) = \mathrm{Tr}\left(\frac{1}{\lambda_1}\right) + \mathrm{Tr}(1).$$

Note that $\mathrm{Tr}(1) = 1$ when $q = 2^{2k+1}$. Hence, the condition $\mathrm{Tr}(B_0) = 1$ gives $\mathrm{Tr}\left(\dfrac{1}{\lambda_1}\right) = 0$, satisfying Proposition 1. Note that we have $\dfrac{N}{D} = x+d$, where $d = \dfrac{\lambda_1}{\lambda_1+\lambda_2+1} \neq 0$, which always permutes $\mathbb{F}_q$, and the proof of (i) ends here.

Case 2: $\lambda_1^2+\lambda_2+1 \neq 0$:

In this case, N and D are coprime and we assume that $\mathrm{Tr}(B_0) \neq 0$.

Computing

$$\frac{\dfrac{x^3+A_2x^2+A_1x+A_0}{x^2+x+B_0} - \dfrac{y^3+A_2y^2+A_1y+A_0}{y^2+y+B_0}}{x-y}$$

we obtain

$$C(x,y) = x^2y^2+xy^2+x^2y+xy+B_0(x^2+y^2)+(A_2B_0+A_0)(x+y)+A_1B_0+A_0 \tag{4}$$

First, assume that $C(x,y)$ in (4) is decomposed in the following form

$$(x+\alpha)(x+\alpha^q)(y+\alpha)(y+\alpha^q).$$

Computing this product and comparing the coefficients of it with the corresponding ones in $C(x,y)$, we get: $\alpha+\alpha^q = 1, \alpha^{q+1} = B_0, (\alpha+\alpha^q)\alpha^{q+1} = A_2B_0+A_0$, which implies that $B_0 = A_2B_0+A_0$. Computing $B_0 = A_2B_0+A_0$, we obtain that $\lambda_1^2+\lambda_2+1 = 0$, which yields a contradiction.

Next, assume that $C(x,y)$ in (4) is decomposed in the following form:

$$(x^2+\alpha_1xy+\beta_1y^2+lot)(\alpha_2x^2+\beta_2xy+\gamma_2y^2+lot).$$

Here and throughout the paper, we use "lot" as the abbreviated form of the so called "lower order terms". Computing this product and comparing the coefficients of it with the corresponding ones in $C(x,y)$, we get: $\alpha_2 = 0, \beta_2 = 0, \alpha_1 = 0, \beta_1 = 0, \gamma_2 = 1$, so we have

$$(x^2+\alpha_3x+\beta_3y+lot)(y^2+\alpha_4x+\beta_4y+lot).$$

Comparing the coefficients of it with the corresponding ones in $C(x,y)$ once more, we get: $\alpha_3=1, \alpha_4=0, \beta_3=0, \beta_4=1$, so we arrive at

$$(x^2+x+\eta)(y^2+y+\xi),$$

which implies that $B_0=\eta=\xi$, $\eta=\xi=A_2B_0+A_0$, so we have $A_2B_0+A_0=B_0$ ending in the contradiction $\lambda_1^2+\lambda_2+1=0$ once more.

Finally, assume that $C(x,y)$ in (4) is decomposed in the following form:

$$(xy+\alpha_1x+\beta_1y+lot)(xy+\alpha_2x+\beta_2y+lot).$$

Computing this product and comparing the coefficients of it with the corresponding ones in $C(x,y)$, we get: $\alpha_1+\alpha_2=1$, that is, $\alpha_2=\alpha_1+1$ and $\beta_1+\beta_2=1$, that is, $\beta_2=\beta_1+1$. Substituting these in the above decomposition, we get

$$(xy+\alpha_1x+\beta_1y+\alpha)(xy+(\alpha_1+1)x+(\beta_1+1)y+\beta).$$

Comparing the coefficients of it with the corresponding ones in $C(x,y)$ once more, we get: $\beta+\alpha_1+\beta_1+\alpha=1$, $\alpha_1(\alpha_1+1)=\beta_1(\beta_1+1)=B_0$, $\alpha_1\beta+\alpha(\alpha_1+1)=\beta_1\beta+\alpha(\beta_1+1)=A_2B_0+A_0$ and $\alpha\beta=A_1B_0+A_0$. Here, $\alpha_1\beta+\alpha(\alpha_1+1)=\beta_1\beta+\alpha(\beta_1+1)$ implies that $(\beta+\alpha)(\alpha_1+\beta_1)=0$ and so we have either $\beta=\alpha$ or $\alpha_1=\beta_1$.

Let us first assume that $\beta=\alpha$. Then we obtain $\alpha_1+\beta_1=1$, $\alpha=A_2B_0+A_0=\beta$, $\alpha^2=A_1B_0+A_0$ and thus $(A_2B_0+A_0)^2=A_1B_0+A_0$, which implies that either $\lambda_2=0$ or $\lambda_1^2\lambda_2+\lambda_1^2+\lambda_2^2+1=0$. If $\lambda_2=0$, then $B_0=0$, which contradicts our assumption $\mathrm{Tr}(B_0)\neq 0$. Now let $\lambda_1^2\lambda_2+\lambda_1^2+\lambda_2^2+1=(\lambda_1^2+\lambda_2+1)(\lambda_2+1)=0$, which implies $\lambda_2=1$. Note that, in this case, $\mathrm{Tr}(B_0)=\mathrm{Tr}\left(\frac{\lambda_2}{\lambda_1+\lambda_2+1}\right)=\mathrm{Tr}\left(\frac{1}{\lambda_1}\right)\neq 0$ but $\lambda_1^2+\lambda_2+1\neq 0$, therefore Proposition 1 is satisfied. Now, assume that the factor $xy+\alpha_1x+\beta_1y+\alpha=0$ for some $x,y\in\mathbb{F}_q$. Taking the q-th power of this equation, we get $xy+\alpha_1^qx+\beta_1^qy+\alpha=0$ and adding these two equations we obtain $(\alpha_1+\alpha_1^q)x+(\beta_1+\beta_1^q)y=0$ which implies that $x=y$ since $\beta_1+\beta_1^q=\alpha_1+1+\alpha_1^q+1=\alpha_1+\alpha_1^q$. The proof of (ii) ends here.

Next, assume that $\alpha_1=\beta_1$, then we have $\beta=\alpha+1$ and $\alpha(\alpha+1)=A_1B_0+A_0$. By comparing the coefficients of this decomposition with the corresponding ones in $C(x,y)$ once more, together with further calculations, we obtain $B_0=\alpha^2+\alpha$. However, this implies $A_1=1$, which is a contradiction with $h(1)\neq 0$.

Finally, assume that $C(x,y)$ in (4) is absolutely irreducible. Homogenizing $C(x,y)$ 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 $Z\neq 0$ respectively. 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 (10) that $\widetilde{C}(X, Y, 0) = X^2Y^2$. This implies $V_0 = |\{(1:0:0), (0:1:0)\}| = 2$. Using [14, Theorem 5.28], we get

$$|V - q| \leq (d-1)(d-2)q^{1/2} + c(d) = 6q^{1/2} + 19, \tag{5}$$

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

$$V = N + 2. \tag{6}$$

Combining (5) and (6), we conclude that

$$|N - q| = |(V - q) - 2| \leq |V - q| + 2 \leq 6q^{1/2} + 21.$$

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 $q - 6q^{1/2} - 21 > 4$, then $C(x, y)$ has an affine point off the line $x = y$. As q is a prime power, we note that $q - 6q^{1/2} - 21 > 4$ for any such q, provided that $q \geq 78$. 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 $q \geq 78$. It remains to consider $q < 78$. Now, since characteristic of $\mathbb{F}_q$ is even and k is odd, we need to consider only $q \in \{2, 8, 32\}$. Using MAGMA [5], we observe that there are no other permutation polynomials of the form $f(x)$ other than the ones obtained by Theorem 1. □

5. PPs over finite fields of odd characteristics

In this section, we deal with the permutation properties of the polynomial $f(x) = x^5h(x^{q-1})$ over $\mathbb{F}_{q^2}$, where $h(x) = \lambda_1 x + \lambda_2 x^2 + x^4$, where $\lambda_1, \lambda_2 \in \mathbb{F}_q$ are not simultaneously zero and $\mathbb{F}_q$ is a finite field of odd characteristic such that $5 \nmid q - 1$. Our plan is to apply Lemma 1 again and the following theorem is our second main result.

Theorem 2 *Let $\mathbb{F}_q$ be a finite field of odd characteristic such that $5 \nmid q-1$. Let $h(x) = \lambda_1 x + \lambda_2 x^2 + x^4$, where $\lambda_1, \lambda_2 \in \mathbb{F}_q$ are not simultaneously zero and assume that $h(1) = \lambda_1 + \lambda_2 + 1 \neq 0$ and $h(-1) = -\lambda_1 + \lambda_2 + 1 \neq 0$. Then, $f(x) = x^5h(x^{q-1})$ is a permutation polynomial of $\mathbb{F}_{q^2}$ if and only if any one of the following conditions hold:*

i) $\lambda_1 = 0, \lambda_2 = 3$ *and* -3 *is a nonsquare in* $\mathbb{F}_q$,

ii) $\lambda_2 = 0$ *and* $\mathbb{F}_q$ *is of characteristic three,*

iii) $\lambda_1^2 + \lambda_2 - 1 = 0$ *and* $\lambda_1^2 - 4$ *is a square in* $\mathbb{F}_q$,

iv) $\lambda_2 = 0$ *and* -3 *is a square in* $\mathbb{F}_q$.

v) $\lambda_2 = -3$ *and* $-3(\lambda_1^2 - 4)$ *is a square in* $\mathbb{F}_q$.

Proof When q is odd, we set $z^q = -z$ and rewrite (2) and (3) as follows:

$$\begin{aligned} N &= -\lambda_1 z(x+z)^3 - \lambda_2 z(x+z)^2(x-z) - z(x-z)^3 - z(x+z)^3 - \lambda_2 z(x+z)(x-z)^2 \\ &\quad -\lambda_1 z(x-z)^3 \\ &= -2z\left((\lambda_1+\lambda_2+1)x^3 + (3\lambda_1-\lambda_2+3)xz^2\right), \end{aligned}$$

$$\begin{aligned} D &= (x+z)^3 + \lambda_2(x+z)(x-z)^2 + \lambda_1(x-z)^3 - \lambda_1(x+z)^3 - \lambda_2(x+z)^2(x-z) - (x-z)^3 \\ &= -2z\left((3\lambda_1+\lambda_2-3)x^2 + (\lambda_1-\lambda_2-1)z^2\right). \end{aligned}$$

First, assume that $3\lambda_1+\lambda_2-3=0$. Then computing $\dfrac{N}{D}$, we obtain

$$\frac{N}{D} = (\lambda_1+\lambda_2+1)\left(\frac{x^3 + \dfrac{3\lambda_1-\lambda_2+3}{\lambda_1+\lambda_2+1}z^2x}{(\lambda_1-\lambda_2-1)z^2}\right)$$

Note that $\lambda_1+\lambda_2+1 = h(1) \neq 0$, so we can ignore the prefactor $(\lambda_1+\lambda_2+1)$ in $\dfrac{N}{D}$ above and $\lambda_1-\lambda_2-1 = -h(-1) \neq 0$, so the denominator of $\dfrac{N}{D}$ is nonzero. We let $A = \dfrac{3\lambda_1-\lambda_2+3}{\lambda_1+\lambda_2+1}z^2$ and by substituting $\lambda_2 = 3-3\lambda_1$ in A, we obtain

$$A = \frac{6\lambda_1}{-2\lambda_1+4}z^2 = \frac{3\lambda_1}{-\lambda_1+2}z^2.$$

Observe that $-\lambda_1+2 \neq 0$ since otherwise $\lambda_1 = 2$ would imply $\lambda_2 = -3$, which contradicts $h(1) = \lambda_1+\lambda_2+1 \neq 0$.

Computing

$$\frac{\left(x^3+Ax\right) - \left(y^3+Ay\right)}{x-y}$$

we get

$$C(x,y) = x^2+xy+y^2+A. \tag{7}$$

Assume that $C(x,y)$ is not absolutely irreducible and it decomposes as:

$$(x+\alpha_1 y+\alpha_2)(\beta_1 x+\beta_2 y+\beta_3).$$

Comparing the coefficients of the above product with $C(x,y)$, we obtain $\beta_1 = 1, \beta_2+\alpha_1 = 1, \beta_3 = -\alpha_2$ and $\alpha_1(1-\alpha_1) = 1$, so we have

$$(x+\alpha_1 y+\alpha_2)(x+(1-\alpha_1)y-\alpha_2) = x^2+xy+y^2+(\alpha_2-2\alpha_1\alpha_2)y-\alpha_2^2.$$

Now comparing the coefficient of y with the one in $C(x,y)$, we obtain $\alpha_2(1-2\alpha_1) = 0$, which implies that $\alpha_2 = 0$ or $\alpha_1 = \dfrac{1}{2}$. First, if $\alpha_2 = 0$, then $A = -\alpha_2^2 = 0$, which implies $\lambda_1 = 0$ and so $\lambda_2 = 3$, since

$3\lambda_1+\lambda_2-3=0$. In this case, we have $C(x,y)=(x+\alpha_1 y)(x+(1-\alpha_1)y)$. Therefore, either the coefficients of both factors should not be in $\mathbb{F}_q$ (i.e., $\alpha_1\notin\mathbb{F}_q$) or both factors must be equal to $x-y$. For the case $\alpha_1\notin\mathbb{F}_q$, we require the polynomial x^2-x+1 satisfied by α_1 (since we have $\alpha_1(1-\alpha_1)=1$) to be irreducible over $\mathbb{F}_q$. Note that the roots are of the form $\frac{1\pm\sqrt{-3}}{2}$, hence we need -3 to be a nonsquare in $\mathbb{F}_q$. Note also that, in this case $3=\lambda_2\neq 1-\lambda_1^2=1$ as q is odd and hence Proposition 1 is already satisfied; moreover, $h(1)=\lambda_1+\lambda_2+1=0+3+1=4=h(-1)=-\lambda_1+\lambda_2+1\neq 0$ since $char(\mathbb{F}_q)$ is odd, that is, in this case $h(x)$ has no roots in μ_{q+1}. In the case $x+\alpha_1 y=x+(1-\alpha_1)y=x-y$, we get $\alpha_1=1-\alpha_1=-1$, which implies that $\alpha_1=\frac{1}{2}$. Substituting $\alpha_1=\frac{1}{2}$ in $\alpha_1(1-\alpha_1)=1$, we obtain that $4=1$, which is only possible for $char(\mathbb{F}_q)=3$ but then $\lambda_1=\lambda_2=0$, which contradicts with our assumption that λ_1,λ_2 are not simultaneously zero.

Next, if $\alpha_1=\frac{1}{2}$, then $\alpha_1(1-\alpha_1)=1$ implies $4=1$, forcing the characteristic to be 3. Note that in characteristic 3, we have $A=0$ and both factors become $x+\frac{1}{2}y=x-y$. In this case, $3\lambda_1+\lambda_2-3=0$ implies $\lambda_2=0$ and we obtain item (ii). Note that $0=\lambda_2=1-\lambda_1^2$ would imply $\lambda_1=\pm 1$, but then $h(1)=h(-1)=0$, contradicting with our assumptions. Therefore, $\lambda_2\neq 1-\lambda_1^2$ and Proposition 1 is again satisfied. The proofs of items (i) and (ii) are completed.

Now, assume that $C(x,y)$ in (7) is absolutely irreducible. In this paper, we use [14, Theorem 5.28], which constitutes a bound obtained from the Hasse-Weil bound. Let $\widetilde{C}(X,Y,Z)\in\mathbb{F}_q[X,Y,Z]$ be the homogeneous polynomial of degree $d=2$ defined as

$$\widetilde{C}(X,Y,Z)=Z^2C\left(\frac{X}{Z},\frac{Y}{Z}\right).$$

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 $\mathbb{P}^2(\mathbb{F}_q)$ denote the projective space consisting of projective coordinates $(X:Y:Z)$ and $V=|\{(X:Y:Z)\in\mathbb{P}^2(\mathbb{F}_q) \mid \widetilde{C}(X,Y,Z)=0\}|$ 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 $Z\neq 0$, respectively. 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 is obvious that $N=V_1$ and $V=V_0+V_1=V_0+N$. Moreover, it follows from (7) that $\widetilde{C}(X,Y,0)=X^2+XY+Y^2$. This implies $V_0=0$. Thus, we have $V=V_0+V_1=0+N=N$. Using [14, Theorem 5.28], we get

$$|V-q|=|N-q|\leq(d-1)(d-2)q^{1/2}+c(d)=c(d)=2, \tag{8}$$

where $c(d)=\frac{1}{2}d(d-1)^2+1=2$ as $d=2$. Note that

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

as $C(x,x)$ is a polynomial of degree 2 in $\mathbb{F}_q[x]$. Therefore, if $q-2>2$, then $C(x,y)$ has an affine point off the line $x=y$. 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 $q > 4$. It remains to consider only when $q = 3$. Using MAGMA [5], we observe that $f(x)$ is not a permutation of $\mathbb{F}_9$ for any $\lambda_1, \lambda_2 \in \mathbb{F}_3$.

Next, we assume that $3\lambda_1 + \lambda_2 - 3 \neq 0$, then we have

$$\frac{N}{D} = \left(\frac{\lambda_1 + \lambda_2 + 1}{3\lambda_1 + \lambda_2 - 3}\right)\left(\frac{x^3 + \dfrac{(3\lambda_1 - \lambda_2 + 3)}{(\lambda_1 + \lambda_2 + 1)}z^2x}{x^2 + \dfrac{(\lambda_1 - \lambda_2 - 1)}{(3\lambda_1 + \lambda_2 - 3)}z^2}\right).$$

We observe that, since $h(1) = \lambda_1 + \lambda_2 + 1 \neq 0$ and $3\lambda_1 + \lambda_2 - 3 \neq 0$, the prefactor $\left(\dfrac{\lambda_1 + \lambda_2 + 1}{3\lambda_1 + \lambda_2 - 3}\right)$ in $\dfrac{N}{D}$ is nonzero and does not have a pole, we can ignore it. Thus, we just deal with the following fraction:

$$\frac{x^3 + \dfrac{(3\lambda_1 - \lambda_2 + 3)}{(\lambda_1 + \lambda_2 + 1)}z^2x}{x^2 + \dfrac{(\lambda_1 - \lambda_2 - 1)}{(3\lambda_1 + \lambda_2 - 3)}z^2}. \tag{9}$$

Now, let $A = \dfrac{(3\lambda_1 - \lambda_2 + 3)}{(\lambda_1 + \lambda_2 + 1)}z^2$ and $B = \dfrac{(\lambda_1 - \lambda_2 - 1)}{(3\lambda_1 + \lambda_2 - 3)}z^2$. Note that $B \neq 0$ since $h(-1) = -\lambda_1 + \lambda_2 + 1 \neq 0$ and $z \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. In order to guarantee that the polynomial $x^2 + B$ in the denominator of (9) does not have any zeroes in $\mathbb{F}_q$ (and hence (9) does not have any poles), we have to assume that $-B$ is not a square in $\mathbb{F}_q$, that is, $\left(\dfrac{-\lambda_1 + \lambda_2 + 1}{3\lambda_1 + \lambda_2 - 3}\right)$ is a square in $\mathbb{F}_q$. Computing

$$\frac{\dfrac{x^3 + Ax}{x^2 + B} - \dfrac{y^3 + Ay}{y^2 + B}}{x - y}$$

we obtain

$$C(x, y) = x^2y^2 + B(x^2 + y^2) + (B - A)xy + AB. \tag{10}$$

Assume first that $C(x, y)$ is decomposed as

$$(x + \alpha)(x + \alpha^q)(y + \alpha)(y + \alpha^q).$$

Comparing the coefficients with $C(x, y)$, we get $\alpha^q = -\alpha, \alpha^{q+1} = -\alpha^2 = B = A$. Now we have

$$\begin{aligned} A = B \quad &\iff \quad \frac{(3\lambda_1 - \lambda_2 + 3)}{(\lambda_1 + \lambda_2 + 1)}z^2 = \frac{(\lambda_1 - \lambda_2 - 1)}{(3\lambda_1 + \lambda_2 - 3)}z^2 \\ &\iff \quad 8\lambda_1^2 + 8\lambda_2 - 8 = 0 \\ &\iff \quad \lambda_1^2 + \lambda_2 - 1 = 0. \end{aligned}$$

So, by Proposition 1, for $h(x)$ not to have any roots in μ_{q+1}, $\lambda_1^2 - 4$ must be a square in $\mathbb{F}_q$. Note that, by substituting $\lambda_2 = 1 - \lambda_1^2$ in $\dfrac{-\lambda_1 + \lambda_2 + 1}{3\lambda_1 + \lambda_2 - 3}$, we get the following:

$$\frac{-\lambda_1 + \lambda_2 + 1}{3\lambda_1 + \lambda_2 - 3} = \frac{\lambda_1^2 + \lambda_1 - 2}{\lambda_1^2 - 3\lambda_1 + 2} = \frac{(\lambda_1 + 2)(\lambda_1 - 1)}{(\lambda_1 - 2)(\lambda_1 - 1)} = \frac{\lambda_1 + 2}{\lambda_1 - 2} = \frac{\lambda_1^2 - 4}{(\lambda_1 - 2)^2}. \tag{11}$$

Here, note that $\lambda_1 \neq 1$, since otherwise we have $\lambda_1 = 1$, $\lambda_2 = 1-\lambda_1^2 = 0$ which contradicts with the assumption $h(-1) = -\lambda_1 + \lambda_2 + 1 \neq 0$. Similarly, $\lambda_1 \neq 2$, since otherwise we have $\lambda_1 = 2$, $\lambda_2 = 1 - \lambda_1^2 = -3$ which contradicts with the assumption $h(1) = \lambda_1 + \lambda_2 + 1 \neq 0$. Hence, by (11), we obtain that $\dfrac{-\lambda_1 + \lambda_2 + 1}{3\lambda_1 + \lambda_2 - 3}$ is a square in $\mathbb{F}_q$ if and only if $\lambda_1^2 - 4$ is a square in $\mathbb{F}_q$. This proves item (iii).

Next, assume that $C(x,y)$ is decomposed as

$$(x^2 + \alpha_1 xy + \beta_1 y^2 + lot)(\alpha_2 x^2 + \beta_2 xy + \gamma_2 y^2 + lot).$$

Comparing the coefficients of degree 4 terms with those of $C(x,y)$, we obtain that $\alpha_2 = 0, \beta_2 = 0, \gamma_2 = 1, \alpha_1 = 0, \beta_1 = 0$. So we have

$$(x^2 + \alpha_3 x + \beta_3 y + lot)(y^2 + \alpha_4 x + \beta_4 y + lot).$$

Comparing the coefficients of degree 3 terms with those of $C(x,y)$, we obtain that $\alpha_4 = 0, \beta_4 = 0, \alpha_3 = 0, \beta_3 = 0$. So we have

$$(x^2 + \eta)(y^2 + \xi) = x^2y^2 + \xi x^2 + \eta y^2 + \eta\xi.$$

Comparing the coefficients of degree 2 terms and the constant term with those of $C(x,y)$, we obtain that $\xi = \eta = B$ and $B - A = 0$ which implies that $\lambda_1^2 + \lambda_2 - 1 = 0$. Now, if $x^2 + \eta = 0$ for some $x \in \mathbb{F}_q$, then $x^2 = -\eta = -B$, that is, $-B$ is a square in $\mathbb{F}_q$, which gives a contradiction since we already assumed that $-B$ is not a square in $\mathbb{F}_q$ (which is the case if and only if $\left(\dfrac{-\lambda_1 + \lambda_2 + 1}{3\lambda_1 + \lambda_2 - 3}\right)$ is a square in $\mathbb{F}_q$). Therefore, $f(x) = x^5 h(x^{q-1})$ is a permutation polynomial of $\mathbb{F}_{q^2}$ if and only if $\left(\dfrac{-\lambda_1 + \lambda_2 + 1}{3\lambda_1 + \lambda_2 - 3}\right)$ is a square in $\mathbb{F}_q$ (recall that this is the case if and only if $\lambda_1^2 - 4$ is a square in $\mathbb{F}_q$) and $\lambda_1^2 + \lambda_2 - 1 = 0$; hence, we obtain the same result with the previous one.

Now, assume that $C(x,y)$ is decomposed as

$$(xy + \alpha_1 x + \beta_1 y + lot)(xy + \alpha_2 x + \beta_2 y + lot).$$

Comparing the coefficients of degree 3 terms with those of $C(x,y)$, we obtain that $\alpha_1 + \alpha_2 = 0 \implies \alpha_2 = -\alpha_1$ and $\beta_1 + \beta_2 = 0 \implies \beta_2 = -\beta_1$. So we have

$$(xy + \alpha_1 x + \beta_1 y + \alpha)(xy - \alpha_1 x - \beta_1 y + \beta).$$

Comparing the coefficients of degree 2 terms with those of $C(x,y)$, we obtain that $-\alpha_1^2 = B = -\beta_1^2$, $\beta + \alpha - 2\alpha_1\beta_1 = B - A$ and $\alpha = \beta$. Thus, we have $\alpha_1^2 = \beta_1^2$, which implies that either $\alpha_1 = \beta_1$ or $\alpha_1 = -\beta_1$. Furthermore, using $-\alpha_1^2 = -\beta_1^2 = B$, we deduce that $\alpha_1, \beta_1 \notin \mathbb{F}_q$ since $-B$ is not a square in $\mathbb{F}_q$, which further imply that $\alpha_1^q = -\alpha_1$ and $\beta_1^q = -\beta_1$. We deal with the cases where $\alpha_1 = \beta_1$ and $\alpha_1 = -\beta_1$ separately.

First, assume that $\alpha_1 = \beta_1$. Then $\beta - 2\alpha_1^2 + \alpha = 2\alpha + 2B = B - A$ implies that $\alpha = -\dfrac{A+B}{2}$ and we get $\alpha\beta = \alpha^2 = AB = \dfrac{(A+B)^2}{4} \iff (A-B)^2 = 0 \iff A = B$ again, which yields $\lambda_1^2 + \lambda_2 - 1 = 0$ giving the same result as above. Now assume that $xy + \alpha_1 x + \alpha_1 y + \alpha = 0$ for some $x, y \in \mathbb{F}_q$. By taking the q-th

power of this equation, we get $xy-\alpha_1 x-\alpha_1 y+\alpha=0$ (since $\alpha_1^q=-\alpha_1$ and $\beta_1^q=-\beta_1$). By subtracting the second equation from the first one, we obtain $2\alpha_1(x+y)=0$, which implies $x=-y$. Then, by substituting $y=-x$ in the equation $xy+\alpha_1 x+\alpha_1 y+\alpha=0$ and in $xy-\alpha_1 x-\alpha_1 y+\alpha=0$, we get $-x^2+\alpha=-x^2-B=0$, which gives a contradiction since $-B$ is not a square in $\mathbb{F}_q$. Hence, none of the factors of the decomposition have any roots in $\mathbb{F}_q$ in this case.

Next, assume that $\alpha_1=-\beta_1$. Then we have

$$(xy+\alpha_1 x-\alpha_1 y+\alpha)(xy-\alpha_1 x+\alpha_1 y+\alpha).$$

Again by comparing the coefficients with those of $C(x,y)$, we obtain that $\beta+2\alpha_1^2+\alpha=2\alpha-2B=B-A \implies \alpha=\dfrac{3B-A}{2}$. We get $\alpha\beta=\alpha^2=AB=\dfrac{(3B-A)^2}{4} \iff (9B-A)(B-A)=0 \iff A=B$ or $A=9B$. We have already discussed the case $A=B$. So assume that $A=9B$, which implies that

$$\frac{(3\lambda_1-\lambda_2+3)}{(\lambda_1+\lambda_2+1)}z^2=9\frac{(\lambda_1-\lambda_2-1)}{(3\lambda_1+\lambda_2-3)}z^2 \iff \lambda_2(\lambda_2+3)=0 \iff \lambda_2=0 \text{ or } \lambda_2=-3.$$

Note that in characteristic 3, $A=9B=0$ already implies $\lambda_2=0$, which was already shown in the second item. Now suppose that there exists $x,y\in\mathbb{F}_q$ such that $xy+\alpha_1 x-\alpha_1 y+\alpha=0$. By taking the q-th power of this equation, we get $xy-\alpha_1 x+\alpha_1 y+\alpha=0$. By subtracting the second equation from the first one, we obtain $2\alpha_1(x-y)=0$, which implies $x=y$. Thus, in this case $f(x)=x^5h(x^{q-1})$ is a permutation polynomial of $\mathbb{F}_{q^2}$ if and only if $\lambda_2=0$ or -3 and $\dfrac{-\lambda_1+\lambda_2+1}{3\lambda_1+\lambda_2-3}$ is a square in $\mathbb{F}_q$ or $\lambda_2=0$ and $\mathbb{F}_q$ is of characteristic three. Note that, if $\lambda_2=0$, then

$$\left(\frac{-\lambda_1+\lambda_2+1}{3\lambda_1+\lambda_2-3}\right)=\left(\frac{-\lambda_1+1}{3\lambda_1-3}\right)=-\frac{1}{3}$$

is a square in $\mathbb{F}_q$. Like above, $0=\lambda_2=1-\lambda_1^2$ would imply $\lambda_1=\pm1$, which contradicts $h(1)\neq0, h(-1)\neq0$. Therefore, $\lambda_2\neq1-\lambda_1^2$ and Proposition 1 is again satisfied.

Similarly, if $\lambda_2=-3$, then

$$\left(\frac{-\lambda_1+\lambda_2+1}{3\lambda_1+\lambda_2-3}\right)=\left(\frac{-\lambda_1-2}{3\lambda_1-6}\right)=-\frac{1}{3}\frac{\lambda_1+2}{\lambda_1-2}=-\frac{1}{3}\frac{\lambda_1^2-4}{(\lambda_1-2)^2}$$

is a square in $\mathbb{F}_q$ and Proposition 1 is satisfied. The proof of the last two items ends here.

Finally, assume that $C(x,y)$ in (10) is absolutely irreducible. Homogenizing $C(x,y)$ 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 $Z\neq 0$ respectively. 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 (10) that $\widetilde{C}(X,Y,0)=X^2Y^2$. This implies $V_0=|\{(1:0:0),(0:1:0)\}|=2$. Using [14, Theorem 5.28], we get

$$|V-q|\leq (d-1)(d-2)q^{1/2}+c(d)=6q^{1/2}+19, \tag{12}$$

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

$$V=N+2. \tag{13}$$

Combining (12) and (13), we conclude that

$$|N-q|=|(V-q)-2|\leq |V-q|+2\leq 6q^{1/2}+21.$$

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 $q-6q^{1/2}-21>4$, then $C(x,y)$ has an affine point off the line $x=y$. As q is a prime power, we note that $q-6q^{1/2}-21>4$ for any such q, provided that $q\geq 78$. 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 $q\geq 78$. It remains to consider $q<78$. Now, since characteristic of $\mathbb{F}_q$ is odd and 5 must be relatively prime with $q-1$, we need to consider only $q\in\{3,5,7,9,13,17,19,23,25,27,29,37,43,47,49,53,59,67,73\}$. Using MAGMA [5], we observe that there are no other permutation polynomials of the form $f(x)$ other than the ones obtained by Theorem 2. □

Remark 1 *When $\lambda_1\neq 0$ and $\lambda_2\neq 0$, the polynomial $f(x)$ we have studied in this paper is quasimultiplicative equivalent to another class of permutation polynomials given by $g(x)=x(1+ax^{q(q-1)}+bx^{2(q-1)})\in\mathbb{F}_{q^2}[x]$ with $a,b\in\mathbb{F}_{q^2}^*$, whose complete characterization in any characteristic could only be achieved in a total of six different papers [2, 4, 15, 16, 23, 24]. Namely, $g(x)$ is introduced in [24], where the sufficient conditions for $g(x)$ to be a permutation polynomial are given in even characteristic. In [2] and [15], these conditions are shown to be also necessary. Then, a complete characterization in characteristic three is given in [16]. After that, in characteristic bigger than three, the sufficient conditions are given in [23] and those conditions are proven to be necessary in [4]. In this paper, we have provided much simpler and shorter proofs in any characteristic by taking λ_1,λ_2 from $\mathbb{F}_q$. Moreover, the equivalence is given by $f(x)=b^{-1}g(x^{2q+3})$, which requires $b\neq 0$, and therefore this class does not cover many of our conditions given for $\lambda_1=0$ or $\lambda_2=0$ as $a,b\in\mathbb{F}_{q^2}^*$.*

Acknowledgment

We would like to thank the anonymous referees for their valuable suggestions and comments which improved our paper.

References

[1] Akbary A, Wang Q. On polynomials of the form $x^r f(x^{(q-1)/l})$. International Journal of Mathematics and Mathematical Sciences 2007; Article 23408. https://doi.org/10.1155/2007/23408

[2] Bartoli D. On a conjecture about a class of permutation trinomials. Finite Fields and Their Applications 2018; 52: 30-50. https://doi.org/10.1016/j.ffa.2018.03.003

[3] Bartoli D, Giulietti M. Permutation polynomials, fractional polynomials, and algebraic curves. Finite Fields and Their Applications 2018; 51: 1-16. https://doi.org/10.1016/j.ffa.2018.01.001

[4] Bartoli D, Timpanella M. A family of permutation trinomials over $\mathbb{F}_{q^2}$. Finite Fields and Their Applications 2021; 70: Article 101781. https://doi.org/10.1016/j.ffa.2020.101781

[5] Bosma W, Cannon J, Playoust C. The Magma algebra system. I. The user language. Journal of Symbolic Computation 1997; 24: 1179-1260. https://doi.org/10.1006/jsco.1996.0125

[6] Dickson LE. The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group. Annals of Mathematics 1896; 11: 65-120. https://doi.org/10.2307/1967224

[7] Grassl M, Özbudak F, Özkaya B, Gülmez Temür B. Complete characterization of a class of permutation trinomial in characteristic five. Cryptography and Communications 2024; 16: 825-841. https://doi.org/10.1007/s12095-024-00705-2

[8] Gupta R, Sharma RK. Some new classes of permutation trinomials over finite fields with even characteristic. Finite Fields and Their Applications 2016; 41: 89-96. https://doi.org/10.1016/j.ffa.2016.05.004

[9] Hermite C. Sur les fonctions de sept lettres. Comptes rendus de l'Academie des Sciences Paris 1863; 57: 750-757. (in French)

[10] Hou X. Permutation polynomials over finite fields - a survey of recent advances. Finite Fields and Their Applications 2015; 32: 82-119. https://doi.org/10.1016/j.ffa.2014.10.001

[11] Hou X. Determination of a type of permutation trinomials over finite fields II. Finite Fields and Their Applications 2015; 35: 16-35. https://doi.org/10.1016/j.ffa.2015.03.002

[12] Hou X. A survey of permutation binomials and trinomials over finite fields. (English summary). In: Topics in Finite Fields. Contemporary Mathematics 632, American Mathematical Society, Providence, RI, 2015, pp. 177-191.

[13] Hou X. Applications of the Hasse-Weil bound to permutation polynomials. Finite Fields and Their Applications 2018; 54: 113-132. https://doi.org/10.1016/j.ffa.2018.08.005

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

[15] Hou X. On a class of permutation trinomials in characteristic 2. Cryptography and Communications 2019; 11: 1199-1210. https://doi.org/10.1007/s12095-018-0342-1

[16] Hou X, Tu Z, Zeng X. Determination of a class of permutation trinomials in characteristic three. Finite Fields and Their Applications 2020; 61: Article 101596. https://doi.org/10.1016/j.ffa.2019.101596

[17] Li K, Qu L, Chen X. New classes of permutation binomials and permutation trinomials over finite fields. Finite Fields and Their Applications 2017; 43: 69-85. https://doi.org/10.1016/j.ffa.2016.09.002

[18] Li K, Qu L, Wang Q. New constructions of permutation polynomials of the form $x^r h(x^{q-1})$ over $\mathbb{F}_{q^2}$. Designs, Codes and Cryptography 2018; 86: 2379-2405. https://doi.org/10.1007/s10623-017-0452-3

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

[20] Mullen GL, Panario D. Handbook of Finite Fields. Discrete Mathematics and its Applications. Boca Raton, FL, USA: CRC Press, 2013.

[21] Özbudak F, Gülmez Temür B. Classification of permutation polynomials of the form $x^3g(x^{q-1})$ of $\mathbb{F}_{q^2}$ where $g(x) = x^3 + bx + c$ and $b, c \in \mathbb{F}_q^*$. Designs, Codes and Cryptography 2022; 90: 1537-1556. https://doi.org/10.1007/s10623-022-01052-0

[22] Park YH, Lee JB. Permutation polynomials and group permutation polynomials. Bulletin of the Australian Mathematical Society 2001; 63: 67-74. https://doi.org/10.1017/S0004972700019110

[23] Tu Z, Zeng X. A class of permutation trinomials over finite fields of odd characteristic. Cryptography and Communications 2019; 11: 563-583. https://doi.org/10.1007/s12095-018-0307-4

[24] Tu Z, Zeng X, Li C, Helleseth T. A class of new permutation trinomials. Finite Fields and Their Applications 2018; 50: 178-195. https://doi.org/10.1016/j.ffa.2017.11.009

[25] Wan D, Lidl R. Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure. Monatshefte für Mathematik 1991; 112: 149-163. https://doi.org/10.1007/BF01525801

[26] Wang Q. Cyclotomic mapping permutation polynomials over finite fields. Sequences, subsequences, and consequences. Lecture Notes in Computer Science 2007; 4893: 119-128. https://doi.org/10.1007/978-3-540-77404-4_11

[27] Wang Q. Polynomials over finite fields: an index approach. In: Combinatorics and Finite Fields, Difference Sets, Polynomials, Pseudorandomness and Applications. Berlin, Germany: De Gruyter, 2019, pp. 319-348. https://doi.org/10.1515/9783110642094-015

[28] Zieve ME. On some permutation polynomials over $\mathbb{F}_q$ of the form $x^r h(x^{(q-1)/d})$. Proceedings of the American Mathematical Society 2009; 137: 2209-2216. https://doi.org/10.48550/arXiv.0707.1110