CLASSIFICATION OF SOME QUADRINOMIALS OVER FINITE FIELDS OF ODD CHARACTERISTIC★

FERRUH ÖZBUDAK AND BURCU GÜLMEZ TEMÜR

ABSTRACT. In this paper, we completely determine all necessary and sufficient conditions such that the polynomial $f(x) = x^3+ax^{q+2}+bx^{2q+1}+cx^{3q}$, where $a, b, c \in \mathbb{F}_q^*$, is a permutation quadrinomial of $\mathbb{F}_{q^2}$ over any finite field of odd characteristic. This quadrinomial has been studied first in [25] by Tu, Zeng and Helleseth, later in [24] Tu, Liu and Zeng revisited these quadrinomials and they proposed a more comprehensive characterization of the coefficients that results with new permutation quadrinomials, where $char(\mathbb{F}_q) = 2$ and finally, in [16], Li, Qu, Li and Chen proved that the sufficient condition given in [24] is also necessary and thus completed the solution in even characteristic case. In [6] Gupta studied the permutation properties of the polynomial $x^3+ax^{q+2}+bx^{2q+1}+cx^{3q}$, where $char(\mathbb{F}_q) = 3, 5$ and $a, b, c \in \mathbb{F}_q^*$ and proposed some new classes of permutation quadrinomials of $\mathbb{F}_{q^2}$.

In particular, in this paper we classify all permutation polynomials of $\mathbb{F}_{q^2}$ of the form $f(x) = x^3+ax^{q+2}+bx^{2q+1}+cx^{3q}$, where $a, b, c \in \mathbb{F}_q^*$, over all finite fields of odd characteristic and obtain several new classes of such permutation quadrinomials.

1. INTRODUCTION

Let $\mathbb{F}_q$ be a finite field with q elements, where q is a power of a prime. A polynomial $g(x) \in \mathbb{F}_q[x]$ is called a *permutation polynomial* over $\mathbb{F}_q$ whenever the associated function $g : a \mapsto g(a)$ is a permutation of $\mathbb{F}_q$. There is a huge interest in permutation polynomials with a few terms because of their simple algebraic structures and extraordinary properties. Permutation polynomials have also a great importance since they have many applications in areas such as cryptography, coding theory and combinatorial designs. As far as we know, the studies on permutation polynomials dates back to researches done by Dickson and Hermite (see, [5, 9]). For the interested reader, we believe that the books on finite fields (see, [18] and Chapter 8 in [20]) will be very helpful to get into the topic and moreover the survey papers (see, [10, 12, 22, 28]) will be useful as they contain many of the recent results on permutation polynomials over finite fields. We refer the interested reader to [3, 4, 8, 11, 15, 17, 21] and the references therein for more results on permutation polynomials over finite fields.

In the literature there are only a few results on permutation quadrinomials. In [25] Tu, Zeng and Helleseth constructed new permutation quadrinomials of the form

$$x^{3q} + ax^{2q+1} + bx^{q+2} + cx^3 \in \mathbb{F}_{q^2}[x] \tag{1.1}$$

over $\mathbb{F}_{q^2}$, where $char(\mathbb{F}_q) = 2$ (see [25, Theorem 1]). In [24] Tu, Liu and Zeng revisited the quadrinomials as in (1.1) and they proposed a more comprehensive characterization of the coefficients that results with new permutation quadrinomials (see [24, Theorem 1]). Finally, in [16], Li, Qu, Li and Chen proved that the sufficient condition given in [24] is also necessary and thus completed the solution in even characteristic case. Later, in [6] Gupta studied the permutation properties of the polynomial $x^3 + ax^{q+2} + bx^{2q+1} + cx^{3q}$, where $char(\mathbb{F}_q) = 3, 5$

★ PUBLISHED BY FINITE FIELDS AND THEIR APPLICATIONS, HTTPS://DOI.ORG/10.1016/J.FFA.2022.102158

and $a,b,c \in \mathbb{F}_q^*$ and proposed some new classes of permutation quadrinomials of $\mathbb{F}_{q^2}$ (see [6, Theorems 3.2, 3.4, 4.2]) and then in [7] with some additional assumptions on the coefficients, the author proposed some new necessary and sufficient conditions on the coefficients that end up with permutation quadrinomials over finite fields with $char(\mathbb{F}_q) = 3, 5$ (see [7, Theorems 3.1, 3.2, 3.3, 4.1]).

In this paper, our aim is to determine all necessary and sufficient conditions such that the polynomial $f(x) = x^3 + ax^{q+2} + bx^{2q+1} + cx^{3q}$, where $a,b,c \in \mathbb{F}_q^*$, is a permutation quadrinomial of $\mathbb{F}_{q^2}$ over any finite field of odd characteristic. We build up a method to characterize permutation quadrinomials of this form completely. A significant step of our method is a smart choice of a polar coordinate transformation and thereafter we use an algorithmic technique to decide whether the resulting polynomial in two variables is irreducible or not. This algorithmic technique ensure us to obtain all permutation quadrinomials in our classes (see Theorem 3.3 and Theorem 3.4) as follows: If the corresponding polynomial in two variables can be factorized into absolutely irreducible components it is usually not so hard to determine whether the quadrinomial is a permutation polynomial or not and if the corresponding polynomial in two variables is absolutely irreducible, by using the well known Hasse-Weil inequality, it turns out that the quadrinomial is not a permutation polynomial. In particular, we obtain not only new classes of permutation quadrinomials over $\mathbb{F}_{q^2}$ but we also obtain a complete characterization over finite fields of odd characteristic.

The paper is organized as follows: In the preliminaries section we point out the main ideas that we use throughout the paper in details. In Section 3, we obtain our main results over finite fields of odd characteristic in Theorem 3.3 and Theorem 3.4 which completes the classification over finite fields of odd characteristic.

2. Preliminaries

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, there is a well known criterion due to Wan and Lidl [26], Park and Lee [23], Akbary and Wang [1], Wang [27] and Zieve [29] which is given in the following lemma.

Lemma 2.1. [26, 23, 1, 27, 29] *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 2.1 over the finite field $\mathbb{F}_{q^2}$ with $d = q+1$, but rather than finding the conditions for which $f(x) = x^r h(x)^{q-1}$ permutes μ_{q+1} we will use the following idea throughout the paper:

Let z be an arbitrary element in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Let $\varphi : \mathbb{F}_q \cup \{\infty\} \longrightarrow \mu_{q+1}$ be the map defined as $\varphi(x) = \dfrac{x+z}{x+z^q}$, for any $x \in \mathbb{F}_q$ with $\varphi(\infty) = 1$. It is easy to observe that φ is one to one from $\mathbb{F}_q \cup \{\infty\}$ to μ_{q+1} and thus onto since cardinalities are the same on both sides. Then we find out that $\varphi^{-1}(x) = \dfrac{xz^q - z}{1-x}$, for any $x \neq 1$ with $\varphi^{-1}(1) = \infty$. In this framework, we have that $f(x) = x^r h(x)^{q-1}$ is one to one on μ_{q+1} and therefore permutes μ_{q+1} if and only if the map $(\varphi^{-1} \circ f \circ \varphi)$ is one to one on $\mathbb{F}_q \cup \{\infty\}$. We note that a similar idea has been used in a number of studies before, see for instance [2, 3, 13].

The situation explained above can be easily followed in the diagram below:

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

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

3. Permutation quadrinomials of the form $f(x) = x^3 + ax^{q+2} + bx^{2q+1} + cx^{3q}$ of $\mathbb{F}_{q^2}$, where $a, b, c \in \mathbb{F}_q^*$ and $char(\mathbb{F}_q)$ is odd

Let $\mathbb{F}_q$ be a finite field of odd characteristic. We first observe that $f(x) = x^3 + ax^{q+2} + bx^{2q+1} + cx^{3q}$ can be written in the form $f(x) = x^3 h(x^{q-1})$, where $h(x) = 1 + ax + bx^2 + cx^3 \in \mathbb{F}_q[x]$ with $a, b, c \in \mathbb{F}_q^*$. In order to be able to apply Lemma 2.1 we first need to find out the conditions for which $h(x)$ has no roots in μ_{q+1}. Note that, 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 3.1. *Let $\mathbb{F}_q$ be a finite field of odd characteristic. Let $h(x) = 1 + ax + bx^2 + cx^3 \in \mathbb{F}_q[x]$ with $a, b, c \in \mathbb{F}_q^*$. Assume that $h(1) = 1 + a + b + c \neq 0$ and $h(-1) = 1 - a + b - c \neq 0$. Then $h(x)$ has a root in μ_{q+1} if and only if the following conditions hold:*

$b - ac \neq 0$, $1 - c^2 = b - ac$ and $(a - bc)^2 - 4(b - ac)^2$ is nonzero, nonsquare in $\mathbb{F}_q$.

Proof. Let $x \in \mu_{q+1}$, that is $x^q = 1/x$, such that $h(x) = 0$, that is

$$cx^3 + bx^2 + ax + 1 = 0 \tag{3.1}$$

Taking the q-th power of the equation in (3.1) we obtain the following

$$cx^{3q} + bx^{2q} + ax^q + 1 = 0 \implies \frac{c}{x^3} + \frac{b}{x^2} + \frac{a}{x} + 1 = 0,$$

that is,

$$x^3 + ax^2 + bx + c = 0. \tag{3.2}$$

Multiplying the equation in (3.1) by $1/c$ and subtracting the equation in (3.2) we get

$$\left(\frac{b}{c} - a\right) x^2 + \left(\frac{a}{c} - b\right) x + \frac{1}{c} - c = 0$$

which implies that

$$(b - ca)x^2 + (a - cb)x + 1 - c^2 = 0. \tag{3.3}$$

First, if $b - ca = 0$, that is, if $b = ca$ then substituting $b = ca$ in (3.3) we get:

$$(a - ac^2)x + 1 - c^2 = 0 \implies (1 - c^2)(ax + 1) = 0, \tag{3.4}$$

which implies that either $1 - c^2 = 0$, that is, $c = \pm 1$ or $x = -1/a$, but $x = -1/a \in \mu_{q+1} \cap \mathbb{F}_q = \{-1, 1\}$ which is not possible by the assumptions $h(1) = 1 + a + b + c \neq 0$, $h(-1) = 1 - a + b - c \neq 0$, thus $c = \pm 1$. If $c = 1$, then $b - ca = 0$ implies $b = a$, but then $h(-1) = 1 - a + b - c = 0$ which contradicts with the assumption $h(-1) \neq 0$. Similarly, if $c = -1$, then $b - ca = 0$ implies $b = -a$, but then $h(1) = 1 + a + b + c = 0$ which contradicts

with the assumption $h(1) \neq 0$.

Next, assume that $b - ac \neq 0$, then multiplying (3.3) by $\dfrac{1}{b-ac}$ we obtain

$$x^2 + \frac{(a-bc)}{b-ac}x + \frac{1-c^2}{b-ac} = 0. \tag{3.5}$$

Let $A = \frac{a-bc}{b-ac}, B = \frac{1-c^2}{b-ac}$, then by (3.5) we have $x^2 + Ax + B = 0$. Note that $B \neq 0$, because otherwise $c = \pm 1$ which implies $A = \pm 1$ and so we have $x^2 \pm x = 0$ which implies $x = \pm 1$ which is not possible by the assumptions $h(1) \neq 0$ and $h(-1) \neq 0$. Taking the q-th power of the equation $x^2 + Ax + B = 0$, we obtain

$$x^{2q} + Ax^q + B = 0 \iff \frac{1}{x^2} + A\frac{1}{x} + B = 0 \iff Bx^2 + Ax + 1 = 0,$$

that is,

$$x^2 + \frac{A}{B}x + \frac{1}{B} = 0. \tag{3.6}$$

Subtracting the equations in (3.5) and (3.6) we obtain

$$\left(A - \frac{A}{B}\right)x = B - \frac{1}{B}. \tag{3.7}$$

Here note that, $A \neq 0$, because otherwise $a = bc$ and (3.7) implies $B = -1$, as a result we get $b = -1, a = -c$ which contradict with the assumption $h(1) \neq 0$. Moreover, we observe that if $B \neq 1$, then the equation in (3.7) implies $x = \frac{B^2-1}{AB-A} \in \mu_{q+1} \cap \mathbb{F}_q = \{-1, 1\}$ which contradicts with the assumptions $h(1) \neq 0$ and $h(-1) \neq 0$. Thus $B = 1$, that is, $1 - c^2 = b - ac$. Substituting $B = 1$ in (3.5) we obtain

$$x^2 + Ax + 1 = 0 \implies \left(x + \frac{A}{2}\right)^2 = \frac{A^2 - 4}{4}. \tag{3.8}$$

Thus, $A^2 - 4$ must be nonzero and nonsquare in $\mathbb{F}_q$, that is, $(a - bc)^2 - 4(b - ac)^2$ must be nonzero and nonsquare in $\mathbb{F}_q$. Otherwise, as $A \in \mathbb{F}_q$ we have $x \in \mu_{q+1} \cap \mathbb{F}_q = \{-1, 1\}$ which contradicts with the assumptions $h(1) \neq 0$ and $h(-1) \neq 0$. This completes the proof. □

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

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

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

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

$$(f \circ \varphi)(x) = \frac{\Delta(z, x)}{\Delta(z^q, x)} = \frac{(x + z)^3 + a(x + z)^2(x + z^q) + b(x + z)(x + z^q)^2 + c(x + z^q)^3}{c(x + z)^3 + b(x + z)^2(x + z^q) + a(x + z)(x + z^q)^2 + (x + z^q)^3}$$

and thus

$$(\varphi^{-1} \circ f \circ \varphi)(x) = \frac{\frac{\Delta(z, x)}{\Delta(z^q, x)}z^q - z}{1 - \frac{\Delta(z, x)}{\Delta(z^q, x)}} = \frac{\Delta(z, x)z^q - z\Delta(z^q, x)}{\Delta(z^q, x) - \Delta(z, x)}.$$

Let $z^q = -z$, then we get the following

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

and

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

Thus,

$$(\varphi^{-1}\circ f\circ\varphi)(x) = \frac{\Delta(z,x)z^q - z\Delta(z^q,x)}{\Delta(z^q,x)-\Delta(z,x)} = \frac{(1+a+b+c)x^3+(3+3c-a-b)z^2x}{(3-3c+a-b)x^2+(1-c+b-a)z^2}. \tag{3.9}$$

First, we deal with the case where $3-3c+a-b=0$ in the following theorem. We first need to prove the following lemma in this case.

Lemma 3.2. *Let p be an odd prime, with $p \neq 3$. Let $q = p^s$, $s \geq 1$ and assume that $gcd(3, q-1) = 1$. Then s is odd and -3 is a nonsquare in $\mathbb{F}_q$.*

Proof. First, assume that $p \equiv 1 (\mathrm{mod}\, 3)$. Then $p^s \equiv 1 (\mathrm{mod}\, 3)$ and hence 3 divides $q-1$ which contradicts the assumption that $gcd(3, q-1) = 1$. Therefore, $p \equiv 2 (\mathrm{mod}\, 3)$. Then, $p^s \equiv (-1)^s (\mathrm{mod}\ 3)$ and hence s is odd. Moreover, as s is odd and $-3 \in \mathbb{F}_p$, -3 is a nonsquare in $\mathbb{F}_q$ if and only if -3 is a nonsquare in $\mathbb{F}_p$. Note that 3 and p are distinct odd primes. Using the Law of Quadratic Reciprocity (see for instance, [18, Theorem 5.17]) we have

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{\frac{(3-1)(p-1)}{4}}. \tag{3.10}$$

Here, for an integer x with $x \not\equiv 0 \,(\mathrm{mod}\ p)$, recall that the Legendre symbol (see for instance, [18]) is defined as

$$\left(\frac{x}{p}\right) = \begin{cases} -1, & \text{if } x \text{ is not a square mod } p, \\ 0, & \text{if } x \text{ is a square mod } p. \end{cases}$$

Moreover, it is well known that (see for instance, [18]),

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \text{ and } \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right). \tag{3.11}$$

Combining (3.10) and (3.11) we conclude that

$$\left(\frac{-3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)(-1)^{\frac{(p-1)(3-1)}{4}} = \left(\frac{2}{3}\right) = -1, \tag{3.12}$$

where we use the fact that $p \equiv 2 (\mathrm{mod}\, 3)$. This completes the proof. □

Theorem 3.3. *Let $\mathbb{F}_q$ be a finite field of odd characteristic, where $gcd(3, q-1) = 1$. Let $h(x) = cx^3 + bx^2 + ax + 1$, with $a, b, c \in \mathbb{F}_q^*$. Assume that $3-3c+a-b=0$. If $char(\mathbb{F}_q) \neq 3$ then $f(x) = x^3h(x^{q-1})$ is a permutation polynomial of $\mathbb{F}_{q^2}$ if and only if $a = 3c$ and $b = 3$. If $char(\mathbb{F}_q) = 3$ then $f(x) = x^3h(x^{q-1})$ is a permutation polynomial of $\mathbb{F}_{q^2}$ if and only if $\frac{a}{2-c+a}$ is a square in $\mathbb{F}_q$.*

Proof. Assume that $3-3c+a-b=0$, then by (3.9) we have

$$(\varphi^{-1}\circ f\circ\varphi)(x) = \frac{\Delta(z,x)z^q - z\Delta(z^q,x)}{\Delta(z^q,x)-\Delta(z,x)} = \frac{(1+a+b+c)x^3+(3+3c-a-b)z^2x}{(1-c+b-a)z^2}, \tag{3.13}$$

that is,

$$\frac{x^3+\frac{(3+3c-a-b)z^2x}{1+a+b+c}}{(1-c+b-a)z^2}. \tag{3.14}$$

Let $A=\frac{3+3c-a-b}{1+a+b+c}z^2$, then we get $A=\frac{3c-a}{2-c+a}z^2$ by substituting $b=3-3c+a$. Computing $\frac{(x^3+Ax)-(y^3+Ay)}{x-y}$ we obtain

$$C(x,y):=x^2+xy+y^2+A. \tag{3.15}$$

Note that $2-c+a\neq 0$ since otherwise $a=c-2$ and $b=3-3c+a$ which implies $h(1)=1+a+b+c=0$, thus $f(x)$ is not a permutation polynomial as $h(x)$ has a root in μ_{q+1}. Hence, we assume that $2-c+a\neq 0$.
First, assume that $C(x,y)$ is not absolutely irreducible and it can be decomposed in the following form

$$(x+\alpha y+lot)(\beta_1 x+\beta_2 y+lot)=\beta_1 x^2+(\beta_2+\beta_1\alpha)xy+\beta_2\alpha y^2+lot \tag{3.16}$$

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 (3.16) with the ones in $C(x,y)$ in (3.15) we get: $\beta_1=1,\beta_2+\alpha=1,\beta_2\alpha=1$ which imply that $\beta_2=1-\alpha$ and $\alpha(1-\alpha)=1$. So we have

$$\begin{aligned}&(x+\alpha y+\alpha_1)(x+(1-\alpha)y+\alpha_2)\\ &=x^2+xy+y^2+(\alpha_2+\alpha_1)x+(\alpha\alpha_2+\alpha_1(1-\alpha))y+\alpha_1\alpha_2.\end{aligned} \tag{3.17}$$

Comparing the coefficients of degree 1 terms with the ones in $C(x,y)$ in (3.15) we obtain: $\alpha_1+\alpha_2=0$, that is, $\alpha_2=-\alpha_1$ and $\alpha\alpha_2+\alpha_1(1-\alpha)=0$ which imply that $\alpha_1(1-2\alpha)=0$, that is, either $\alpha=1/2$ or $\alpha_1=0$ which implies that $A=0$ as $A=-\alpha_1^2$. First, if $\alpha=1/2$ then substituting $\alpha=1/2$ in $\alpha(1-\alpha)=1$ we obtain $4=1$ which is only possible if $char(\mathbb{F}_q)=3$. Now, if $char(\mathbb{F}_q)=3$ then by $b=3-3c+a$ we get that $a=b$. Assume that the first factor in (3.17) is 0, that is, $x+\frac{1}{2}y+\alpha_1=0$, for some $x,y\in\mathbb{F}_q$. Taking its q-th power we get $x+\frac{1}{2}y+\alpha_1^q=0$. Subtracting these two equations we obtain $\alpha_1^q=\alpha_1$ which implies that $\alpha_1\in\mathbb{F}_q$. On the other hand, $A=-\alpha_1^2=\frac{(3c-a)}{2-c+a}z^2$ (note that, $A=\frac{-a}{2-c+a}z^2$ if $char(\mathbb{F}_q)=3$), where $z\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q$. Thus $\alpha_1\notin\mathbb{F}_q$ if and only if $\frac{a}{2-c+a}$ is a square in $\mathbb{F}_q$. Moreover, since $b=a$, if $1-c^2=b-ac=a-ac=a(1-c)$ then we either have $a=1+c$ (which contradicts with the fact that $2-c+a\neq 0$) or $c=1$ (which implies $b-ac=0$) and thus in both cases, by Proposition 3.1 $h(x)$ does not have any roots in μ_{q+1}. Therefore, if $char(\mathbb{F}_q)=3$ then $f(x)$ is a permutation polynomial if and only if $\frac{a}{2-c+a}$ is a square in $\mathbb{F}_q$.
Next, if $\alpha_1=0$, that is, if $A=0$ then we have $a=3c$, $b=3$ and thus in this case $char(\mathbb{F}_q)\neq 3$, otherwise $a=0$, $b=0$ which is not the case since $a,b\in\mathbb{F}_q^*$. Assume that the factor $x+\alpha y=0$ in (3.17) for some $x,y\in\mathbb{F}_q$. Taking its q-th power we get $x+\alpha^q y=0$. Subtracting these two equations we have $(\alpha^q-\alpha)y=0$, thus either $y=0$ and so $x=0$ or $\alpha^q-\alpha=0$ which implies $\alpha\in\mathbb{F}_q$. Moreover we have $\alpha(1-\alpha)=1$, that is, $\left(\alpha-\frac{1}{2}\right)^2=-\frac{3}{4}$ and thus $\alpha\notin\mathbb{F}_q$ if and only if -3 is not a square in $\mathbb{F}_q$. By Lemma 3.2, -3 is not a square in $\mathbb{F}_q$. Hence, $\alpha\notin\mathbb{F}_q$. Moreover, if $c\neq\pm 1$ then we have $1-c^2=b-ac=3-3c^2$ which implies $3=1$ which is not possible since $char(\mathbb{F}_q)$ is odd and if $c=\pm 1$ then $b-ac=3-3c^2=0$ and thus in both cases, by Proposition 3.1 $h(x)$ does not have any roots in μ_{q+1}. Therefore, $f(x)$ is a permutation polynomial of $\mathbb{F}_{q^2}$ if and only if $char(\mathbb{F}_q)\neq 3$, $a=3c$ and $b=3$.

Now, we deal with the case where $C(x,y)$ is absolutely irreducible. Homogenizing $C(x,y)$ in (3.15) 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 [14, 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 $C(x,y)$. This implies that if $q-2>2$ then $C(x,y)$ in (3.15) has an affine $\mathbb{F}_q$-rational point off the line $x=y$ and thus $f(x)$ is not a permutation polynomial of $\mathbb{F}_{q^2}$. □

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

Theorem 3.4. *Assume that $\mathbb{F}_q$ is a finite field of odd characteristic, where $gcd(3,q-1)=1$. Let $h(x)=1+ax+bx^2+cx^3$, with $a,b,c\in\mathbb{F}_q^*$. Assume that $3-3c+a-b\neq 0$. Then $f(x)=x^3h(x^{q-1})$ is a permutation polynomial of $\mathbb{F}_{q^2}$ if and only if one of the following conditions hold*

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

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

Proof. Assume that $3-3c+a-b\neq 0$, then using (3.9) we have

$$\frac{x^3+\dfrac{(3+3c-a-b)}{1+a+b+c}z^2x}{x^2+\dfrac{(1-c+b-a)}{3-3c+a-b}z^2}. \tag{3.18}$$

Let $A=\dfrac{(3+3c-a-b)}{1+a+b+c}z^2$ and $B=\dfrac{(1-c-a+b)}{3-3c+a-b}z^2$. Note that $B\neq 0$ as $h(-1)=1-c-a+b\neq 0$. 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 (3.18), that is, x^2+B becomes zero which implies that ∞ has at least three distinct preimages under the map $(\varphi^{-1}\circ f\circ\varphi)(x)$ 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, $\dfrac{-(1-c+b-a)}{3-3c-b+a}$ is a square in $\mathbb{F}_q$ since $z\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q$. Computing

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

we obtain

$$C(x,y):=x^2y^2+(B-A)xy+B(x^2+y^2)+AB. \tag{3.19}$$

In this setting, $(\varphi^{-1}\circ f\circ\varphi)$ permutes $\mathbb{F}_q$ if and only $C(x,y)$ defined in (3.19) is not zero for any $x,y\in\mathbb{F}_q$ with $x\neq y$. We need to check all decompositions of the bivariate polynomial $C(x,y)$ in (3.19) into absolutely irreducible factors in $\overline{\mathbb{F}}_q$, where $\overline{\mathbb{F}}_q$ stands for an algebraic closure of the finite field $\mathbb{F}_q$. Since the degree of the bivariate polynomial in (3.19) is 4, the possibilities are: $3+1$ decomposition, $2+2$ decomposition and $1+1+1+1$ decomposition according to the degrees of the possible factors and finally the case where the bivariate polynomial $C(x,y)$ in (3.19) is absolutely irreducible. We first observe that $C(x,y)$ is fixed by the automorphism $(x,y)\mapsto(y,x)$ and $C(x,y)$ is also fixed by the Frobenius automorphism $(\,)\mapsto(\,)^q$ applied

to the coefficients of $C(x,y)$ and thus these automorphisms both act on the components of $C(x,y)$. The only possible factorizations for $C(x,y)$ into absolutely irreducible factors which may give rise to permutation polynomials are the following:

(i) Two factors of degree 2 which are switched by the Frobenius automorphism and are either fixed or switched by the automorphism $(x,y)\mapsto(y,x)$,
(ii) Four factors of degree one in the following form: $(x+\alpha)(x+\alpha^q)(y+\alpha)(y+\alpha^q)$.

since all other factorizations contain at least one absolutely irreducible factor which is fixed by the Frobenius automorphism and thus the corresponding polynomial is not a permutation polynomial.
We first fix a monomial ordering by taking $x\geq y$ without loss of generality.
We begin the discussion with the possible $2+2$ decompositions. Here, there are two possibilities: $C(x,y)$ defined in (3.19) is either decomposed in the form

$$(x^2+\alpha_1xy+\beta_1y^2+lot)(\alpha_2x^2+\beta_2xy+\gamma_2y^2+lot) \tag{3.20}$$

or

$$(xy+\alpha_1x+\beta_1y+lot)(xy+\alpha_2x+\beta_2y+lot). \tag{3.21}$$

First, assume that $C(x,y)$ is decomposed in the form (3.20):

$$\begin{aligned}&(x^2+\alpha_1xy+\beta_1y^2+lot)(\alpha_2x^2+\beta_2xy+\gamma_2y^2+lot)\\&=\alpha_2x^4+(\beta_2+\alpha_1\alpha_2)x^3y+(\gamma_2+\alpha_1\beta_2+\alpha_2\beta_1)x^2y^2\\&\qquad+(\alpha_1\gamma_2+\beta_1\beta_2)xy^3+\beta_1\gamma_2y^4+lot.\end{aligned} \tag{3.22}$$

After comparing the coefficients of degree 4 terms of (3.20) with the ones in $C(x,y)$ defined in (3.19) 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

$$\begin{aligned}&(x^2+\alpha_3x+\beta_3y+lot)(y^2+\alpha_4x+\beta_4y+lot)\\&=x^2y^2+\alpha_4x^3+\beta_4x^2y+\alpha_3xy^2+\beta_3y^3+lot.\end{aligned} \tag{3.23}$$

Comparing the coefficients of degree 3 terms of (3.23) with the ones in $C(x,y)$ defined in (3.19) we get: $\alpha_4=0,\beta_4=0,\alpha_3=0,\beta_3=0$. Thus we have

$$(x^2+\eta)(y^2+\zeta)=x^2y^2+\zeta x^2+\eta y^2+\eta\zeta. \tag{3.24}$$

Comparing the coefficients of (3.24) with the ones in $C(x,y)$ defined in (3.19) we obtain that $B-A=0$, that is, $A=B$ (implying $b=1-c^2+ac$) 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 $x^2+\eta\neq0$ and similarly $y^2+\zeta\neq0$ for any $x,y\in\mathbb{F}_q$. Therefore, in this case $f(x)$ is a permutation poynomial if and only if $c\neq\pm1$, $b=1-c^2+ac$ and $(a-c)^2-4$ is a square in $\mathbb{F}_q$.
Next, assume that $C(x,y)$ is decomposed in the form (3.21):

$$\begin{aligned}&(xy+\alpha_1x+\beta_1y+lot)(xy+\alpha_2x+\beta_2y+lot)\\&=x^2y^2+(\alpha_1+\alpha_2)x^2y+(\beta_1+\beta_2)xy^2+lot.\end{aligned} \tag{3.25}$$

After comparing the coefficients of degree 3 terms of (3.21) with the ones in $C(x,y)$ we obtain: $\alpha_2=-\alpha_1$ and $\beta_2=-\beta_1$ and so we end up with the following decomposition

$$\begin{aligned}&(xy+\alpha_1x+\beta_1y+\alpha)(xy-\alpha_1x-\beta_1y+\beta)\\&=x^2y^2-\alpha_1^2x^2+(\beta+\alpha-2\alpha_1\beta_1)xy-\beta_1^2y^2+lot.\end{aligned} \tag{3.26}$$

Comparing the coefficients of degree 2 terms in (3.26) with the ones in $C(x,y)$ 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 (3.26) becomes the following:

$$(xy + \alpha_1 x + \alpha_1 y + \alpha)(xy - \alpha_1 x - \alpha_1 y - (A + B + \alpha)) \tag{3.27}$$

$$= x^2y^2 - \alpha_1^2(x^2 + y^2) + (B - A)xy - \alpha_1(A + B + 2\alpha)(x + y) - \alpha(A + B + \alpha).$$

Comparing the coefficients of degree 1 terms in (3.27) with the ones in $C(x,y)$, we obtain $A + B + 2\alpha = 0$ as $\alpha_1 \neq 0$ and so $\alpha = \dfrac{-(A+B)}{2} \in \mathbb{F}_q$. Comparing the constant term in (3.27) with the one in $C(x,y)$, we obtain $-\alpha(A+B+\alpha) = AB$. Substituting $\alpha = \dfrac{-(A+B)}{2}$ in $-\alpha(A + B + \alpha) = AB$ we obtain $AB = \dfrac{(A+B)^2}{4}$ which implies that $(A - B)^2 = 0$ then $A = B$ and so $b = 1 - c^2 + ac$.

Assume that there exists $x, y \in \mathbb{F}_q$ such that $xy + \alpha_1 x + \alpha_1 y + \alpha = 0$. Taking its q-th power we get $xy - \alpha_1 x - \alpha_1 y + \alpha = 0$. Subtracting these two equations we obtain $2\alpha_1(x + y) = 0$ which implies that $x = -y$ since $\alpha_1 \neq 0$ (as $-\alpha_1^2 = B \neq 0$). Substituting $x = -y$ in the equation $xy + \alpha_1 x + \alpha_1 y + \alpha = 0$ we get $-x^2 + \alpha = -x^2 - B = 0$ which contradicts with the assumption that $-B$ is not a square in $\mathbb{F}_q$. Thus, we conclude that none of the factors in the decomposition (3.27) can have roots in $\mathbb{F}_q$. Therefore, in this case, $f(x)$ is a permutation poynomial if and only if $c \neq \pm 1$, $b = 1 - c^2 + ac$ and $(a - c)^2 - 4$ is a square in $\mathbb{F}_q$.

Finally, assume that $\alpha_1 = -\beta_1$. Then by (3.26) we have the following decomposition:

$$(xy + \alpha_1 x - \alpha_1 y + \alpha)(xy - \alpha_1 x + \alpha_1 y - (A - 3B + \alpha)). \tag{3.28}$$

Comparing the coefficients of degree 1 terms and the constant terms in (3.28) with the ones in $C(x,y)$ we obtain $\alpha = \beta$, $AB = \alpha^2$ and $\alpha = \dfrac{3B - A}{2}$. Substituting $\alpha = \dfrac{3B - A}{2}$ in $AB = \alpha^2$ we get $(9B - A)(B - A) = 0$ implying that either $A = B$ or $A = 9B$.

If $A = B$ then $b = 1 - c^2 + ac$. Assume that the first factor in (3.28) is 0, that is, $xy + \alpha_1 x - \alpha_1 y + \alpha = 0$ for some $x, y \in \mathbb{F}_q$. Taking its q-th power we get $xy + \alpha_1^q x - \alpha_1^q y + \alpha = xy - \alpha_1 x + \alpha_1 y + \alpha = 0$, as $\alpha_1^q = -\alpha_1$. Subtracting these two equations we get $2\alpha_1(x - y) = 0$ which implies that $x = y$ since $\alpha_1 \neq 0$. Thus, we obtain that in this case, $f(x)$ is a permutation poynomial if and only if $c \neq \pm 1$, $b = 1 - c^2 + ac$ and $(a - c)^2 - 4$ is a square in $\mathbb{F}_q$. Finally, if $9B = A$ then we obtain $3b - 3ac - a^2 + b^2 = 0$. Assume that there exists $x, y \in \mathbb{F}_q$ such that $xy + \alpha_1 x - \alpha_1 y + \alpha = 0$. Taking its q-th power we get $xy - \alpha_1 x + \alpha_1 y + \alpha = 0$. Subtracting these two equations we obtain $2\alpha_1(x - y) = 0$ implying that $x = y$ since $\alpha_1 \neq 0$. Therefore, in this case $f(x)$ is a permutation poynomial if and only if $3b - 3ac - a^2 + b^2 = 0$ and $\dfrac{-(1 - c + b - a)}{3 - 3c + a - b}$ is a square in $\mathbb{F}_q$.

As the next step, we deal with the decomposition of $C(x,y)$ in the following form:

$$(x + \alpha)(x + \alpha^q)(y + \alpha)(y + \alpha^q) \tag{3.29}$$

By comparing the coefficients of the terms in (3.29) with the coefficients of $C(x,y)$ (3.19) we obtain the following: $\alpha^q=-\alpha$ and $A=B=-\alpha^2$. Now, we have

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

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

which implies that $1-b-c^2+ac=0$, that is, $b=1-c^2+ac$. Substituting $b=1-c^2+ac$ in $-B=-\frac{1-c+b-a}{3-3c-b+a}$ we get $-\frac{(1-c)(2-a+c)}{(1-c)(2+a-c)}=-\frac{(2-a+c)}{2+a-c}$. Here, note that $c\neq 1$ since then $b=1-c^2+ac$ implies $b=a$ and so $3-3c+a-b=0$ which contradicts with the assumption that $3-3c+a-b\neq 0$. As $-B$ is not a square in $\mathbb{F}_q$ we have

$$-\frac{(2-a+c)}{2+a-c}=-\frac{(2-a+c)}{(2+a-c)}\frac{(2+a-c)}{(2+a-c)}=-\frac{4-(a-c)^2}{(2+a-c)^2} \tag{3.30}$$

is a square in $\mathbb{F}_q$, that is, $(a-c)^2-4$ is square in $\mathbb{F}_q$. Now, $b=1-c^2+ac$ implies that $b-ac=1-c^2$ and $(a-bc)^2-4(b-ac)^2=(1-c^2)^2((a-c)^2-4)$ is a square in $\mathbb{F}_q$ since $(a-c)^2-4$ is square in $\mathbb{F}_q$, thus $h(x)$ has no roots in μ_{q+1} by Proposition 3.1. Note that $-\alpha^2=B$, so $\alpha\notin\mathbb{F}_q$ since we have that $-B$ is not a square in $\mathbb{F}_q$ and thus none of the factors in the decomposition (3.29) can have a root in $\mathbb{F}_q$. Thus, $f(x)$ is a permutation polynomial of $\mathbb{F}_{q^2}$ iff $c\neq\pm 1$, $b=1-c^2+ac$ and $(a-c)^2-4$ is a square in $\mathbb{F}_q$.

As the last step, we deal with the absolutely irreducible case. Assume that $C(x,y)$ defined in (3.19) is absolutely irreducible. Homogenizing $C(x,y)$ in (3.19) 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 [14, 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

$$\mid N-q\mid\leq (d-1)(d-2)q^{1/2}+c(d)\leq 6q^{1/2}+19,$$

where N is the number of affine $\mathbb{F}_q$-rational points of $C(x,y)$. This implies that if $q-6q^{1/2}-19>4$ then $C(x,y)$ 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 $q\geq 79$. 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 $q\geq 79$. It remains to consider $q<79$. Now, since characteristic of $\mathbb{F}_q$ is odd and 3 does not 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 [19] we observed that there are no other permutation polynomials of the form $f(x)$ other than the ones obtained by Theorem 3.3 and Theorem 3.4. □

Acknowledgements

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 $x^r f(x^{(q-1)/l})$, Int. J. Math. Sci., Art. ID 23408 (2007).
[2] Bartoli, D., On a conjecture about a class of permutation trinomials, Finite Fields Appl. 52, 30-50 (2018).
[3] Bartoli, D., Giulietti, M., Permutation polynomials, fractional polynomials, and algebraic curves, Finite Fields Appl. 51, 1-16 (2018).
[4] Bartoli, D., Timpanella, M., A family of permutation trinomials over $\mathbb{F}_{q^2}$, Finite Fields Appl. 70, 101781 (2021).
[5] 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).

[6] Gupta, R., Several new permutation quadrinomials over finite fields of odd characteristic. Des. Codes Cryptogr. 88, 223-239 (2020).
[7] Gupta, R., More results about a class of quadrinomials over finite fields of odd characteristic. Comm. Algebra 50, no. 1, 324–333 (2022).
[8] Gupta, R., Sharma, R.K., Some new classes of permutation trinomials over finite fields with even characteristic. Finite Fields Appl. 41, 89-96 (2016).
[9] Hermite, Ch., Sur les fonctions de sept lettres, C.R. Acad. Sci. Paris 57, 750-757 (1863).
[10] Hou, X., Permutation polynomials over finite fields - a survey of recent advances, Finite Fields Appl. 32, 82-119 (2015).
[11] Hou, X., Determination of a type of permutation trinomials over finite fields, Finite Fields Appl. 35, 16-35 (2015).
[12] 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.
[13] Hou, X., Applications of the Hasse-Weil bound to permutation polynomials, Finite Fields Appl. 54, 113-132 (2018).
[14] Hou, X., Lectures on finite fields, Graduate Studies in Mathematics, 190, American Mathematical Society, Providence, RI (2018)
[15] Li, K., Qu, L., Chen, X., New classes of permutation binomials and permutation trinomials over finite fields. Finite Fields Appl. 43, 69-85 (2017).
[16] Li, K., Qu, L., Li, C., Chen, H., On a conjecture about a class of permutation quadrinomials. Finite Fields Appl. 66: 101690 (2020).
[17] 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).
[18] Lidl, R. and Niederreiter, H., Finite Fields (Encyclopedia of Mathematics and its Applications), Cambridge University Press, Cambridge (1997).
[19] Bosma W., Cannon J., and Playoust C., The Magma algebra system. I. The user language, J. Symbolic Comput. 24, 1179-1260 (1997).
[20] Mullen, G.L. and Panario, D., Handbook of Finite Fields, Discrete Mathematics and its Applications (Boca Raton), CRC Press, Boca Raton, FL (2013).
[21] 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 $b, c \in \mathbb{F}_q^*$, Des. Codes Cryptogr., DOI: 10.1007/s10623-022-01052-0.
[22] 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.
[23] Park, Y.H. and Lee, J. B., Permutation polynomials and group permutation polynomials, Bull. Austral. Math. Soc. 63, 67-74 (2001).
[24] Tu, Z., Liu, X., Zeng, X., A revisit to a class of permutation quadrinomials. Finite Fields Appl. 59, 57-85 (2019).
[25] Tu, Z., Zeng, X., Helleseth, T., New permutation quadrinomials over $\mathbb{F}_{2^{2m}}$. Finite Fields Appl. 50, 304-318 (2018).
[26] 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).
[27] Wang, Q., Cyclotomic mapping permutation polynomials over finite fields, Sequences, subsequences, and consequences, Lecture Notes in Comput. Sci., 4893, Springer, Berlin, 119?128, (2007).
[28] 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).
[29] 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).
[30] Zieve, M.E., Planar functions and perfect nonlinear monomials over finite fields, Des. Codes Cryptogr. 75(1), 71-80 (2015).

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

Email address: ozbudak@metu.edu.tr

Department of Mathematics, Atilim University, 06830 İncek, Ankara, Turkey

Email address: burcu.temur@atilim.edu.tr