# COMPLETE CHARACTERIZATION OF A CLASS OF PERMUTATION TRINOMIALS IN CHARACTERISTIC FIVE★

MARKUS GRASSL, FERRUH ÖZBUDAK, BUKET ÖZKAYA, AND BURCU GÜLMEZ TEMÜR

ABSTRACT. In this paper, we address an open problem posed by Bai and Xia in [2]. We study polynomials of the form $f(x) = x^{4q+1} + \lambda_1 x^{5q} + \lambda_2 x^{q+4}$ over the finite field $\mathbb{F}_{5^k}$, which are not quasi-multiplicative equivalent to any of the known permutation polynomials in the literature. We find necessary and sufficient conditions on $\lambda_1, \lambda_2 \in \mathbb{F}_{5^k}$ so that $f(x)$ is a permutation monomial, binomial, or trinomial of $\mathbb{F}_{5^{2k}}$.

## 1. INTRODUCTION

Let $\mathbb{F}_q$ be a finite field with $q$ elements, where $q$ is a prime power. A polynomial $g(x) \in \mathbb{F}_q[x]$ is called a *permutation polynomial (PP)* over $\mathbb{F}_q$ if $g(x)$ is a bijection of $\mathbb{F}_q$. Due to their simple algebraic structure and extraordinary properties, there has been a great interest in permutation polynomials with a few terms, such as binomials or trinomials. Permutation polynomials are also very important in terms of their applications in areas such as cryptography, coding theory and combinatorial designs. As far as we know, the studies on permutation polynomials go back to the work done by Dickson and Hermite (see, [13, 17]). As an introduction, the books on finite fields (see, [28] and [29, Chapter 8]) could be very helpful for the interested reader to get into the topic. Furthermore, the survey papers (see, [19, 21, 31, 39]) could also be useful as they consist of many of the recent results on permutation polynomials over finite fields. We refer the interested reader to [6, 7, 15, 20, 25, 26, 30] and the references therein for more results on permutation polynomials over finite fields.

In [2], Bai and Xia proved that the polynomial $g(x) = x^{(p-1)q+1} + x^{pq} - x^{q+p-1}$ over the finite field $\mathbb{F}_{q^2}$, where $p = 3$ or 5 and $q = p^k$ with $k$ being a positive integer, is a permutation trinomial for $\mathbb{F}_{q^2}$ if and only if $k$ is even. Later, in [14] Gupta and Rai investigated the trinomial $f(x) = x^{4q+1} + \alpha x^{5q} + x^{q+4}$ over the finite field $\mathbb{F}_{5^{2k}}$, where $\alpha \in \mathbb{F}_{5^k}^*$ with $k$ being a positive integer. They proved that the trinomial $f(x)$ permutes $\mathbb{F}_{5^{2k}}$ if and only if $\alpha = -1$ and $k$ is even. In this paper, our aim is to determine the permutation properties of the more general trinomial $f(x) = x^{(p-1)q+1} + \lambda_1 x^{pq} + \lambda_2 x^{q+p-1} \in \mathbb{F}_q[x]$ over $\mathbb{F}_{q^2}$, where $\mathbb{F}_q$ is of characteristic 5. Our results include the ones in [2, 14]. Note that while proving our main result (see Theorem 4.1) in the absolutely irreducible case, we use a bound (see [23, Theorem 5.28]) which is derived from the well-known Hasse-Weil bound for function fields. For the characterization of some planar functions and related structures, like exceptional polynomials and APN permutations, the theory of algebraic curves over finite fields and in particular, Hasse-Weil type inequalities become a very useful instrument. In recent years, there have been very interesting studies on these topics through the Hasse-Weil approach (see for instance, [4], [8], [11], [18], [34] and the references therein).

The paper is organized as follows. Section 2 contains background material that is used in the rest of the paper. Section 3 and 4 contain our main results, where we prove necessary and

★ PUBLISHED BY CRYPTOGRAPHY AND COMMUNICATIONS DISCRETE STRUCTURES, BOOLEAN FUNCTIONS AND SEQUENCES , HTTPS://DOI.ORG/10.1007/S12095-024-00705-2

sufficient conditions on $\lambda_1, \lambda_2 \in \mathbb{F}_{5^k}$ so that $f(x)$ permutes $\mathbb{F}_{5^{2k}}$. Finally, Section 5 investigates the quasi-multiplicative equivalence of the polynomial $f(x)$ with the existing permutation trinomials in odd or arbitrary characteristic.

## 2. Preliminaries

In order to determine whether a polynomial that can be written in the form $f(x) = x^r h\left(x^{(q^n-1)/d}\right)$ permutes $\mathbb{F}_{q^n}$ or not, mostly a well known criterion due to Wan and Lidl [37], Park and Lee [32], Akbary and Wang [1], Wang [38] and Zieve [42] is being used, which is given in the following lemma.

**Lemma 2.1.** [37, 32, 1, 38, 42] *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* $\mu_d$, *where* $\mu_d = \{\theta \in \mathbb{F}_{q^n}^* \mid \theta^d = 1\}$.

In this paper, we plan to apply Lemma 2.1 over the finite field $\mathbb{F}_{q^2}$ with $d = q+1$ and $r = 5$, using

$$h(x) = \lambda_1 x^5 + x^4 + \lambda_2 x, \qquad \text{with } \lambda_1, \lambda_2 \in \mathbb{F}_q. \tag{2.1}$$

Condition (i) of Lemma 2.1 holds as $\gcd(r, (q^n-1)/d) = \gcd(r, q-1) = \gcd(5, 5^k - 1) = 1$. Instead of finding the conditions for which $g(x) = x^r h(x)^{q-1}$ permutes $\mu_{q+1}$, we will use the following idea throughout the paper:

Let $z \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ be an arbitrary element. For any $x \in \mathbb{F}_q$, let $\Phi\colon \mathbb{F}_q \cup \{\infty\} \longrightarrow \mu_{q+1}$ be the map defined by $\Phi(x) = \dfrac{x+z}{x+z^q}$, where $\Phi(\infty) = 1$. It is not so hard to observe that $\Phi$ is one to one from $\mathbb{F}_q \cup \{\infty\}$ to $\mu_{q+1}$ and thus onto since the number of elements on both sides are equal. Then we obtain that $\Phi^{-1}(x) = \dfrac{xz^q - z}{1-x}$, for any $x \neq 1$ with $\Phi^{-1}(1) = \infty$. In this setting, we have $g(x) = x^r h(x)^{q-1}$ is one to one on $\mu_{q+1}$ and therefore permutes $\mu_{q+1}$ if and only if the map $(\Phi^{-1} \circ g \circ \Phi)$ is one to one on $\mathbb{F}_q \cup \{\infty\}$. In our situation, $g(1) = (\lambda_1 + \lambda_2 + 1)^{q-1} = 1$ when $h(1) \neq 0$. Then $\infty$ is a fixed-point of the map $(\Phi^{-1} \circ g \circ \Phi)$, and it suffices to investigate its action on $\mathbb{F}_q$. We note that an analogous idea has been used in a few more studies before, see for instance [3, 6, 22].

This situation can be easily summarized in the diagram below:

$$\begin{array}{ccc} \mathbb{F}_q \cup \{\infty\} & \xrightarrow{\Phi^{-1} \circ g \circ \Phi} & \mathbb{F}_q \cup \{\infty\} \\ \big\downarrow{\scriptstyle \Phi} & & \big\uparrow{\scriptstyle \Phi^{-1}} \\ \mu_{q+1} & \xrightarrow{\quad g \quad} & \mu_{q+1} \end{array} \tag{2.2}$$

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

## 3. The trinomial $h(x)$ of degree 5 in arbitrary characteristic

As a preliminary step to apply Lemma 2.1, we investigate for which $\lambda_1, \lambda_2 \in \mathbb{F}_q$ the polynomial $h(x) = \lambda_1 x^5 + x^4 + \lambda_2 x \in \mathbb{F}_q[x]$ does not have any roots in $\mu_{q+1}$ without restrictions on the characteristic.

If $h(1) = 0$ or $h(-1) = 0$, then $h(x)$ has a root in $\mu_{q+1}$ trivially. Therefore we characterize all such polynomials in the next proposition under the assumptions $h(1) \neq 0$ and $h(-1) \neq 0$. For this we first need to prove some lemmas.

**Lemma 3.1.** *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 $\mathbb{F}_q$, $\theta^q$ is another root of $h(x)$. Then $m(x) = (x - \theta)(x - \theta^q) = x^2 - (\theta + \theta^q) + \theta^{q+1} = x^2 + Ax + 1$ divides $h(x)$. Moreover $m(x)$ is the minimal polynomial of $\theta$ 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 $\theta_1$ and $\theta_2$ 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 $1 = \theta_1\theta_2 = \theta_1^{q+1}$. □

**Lemma 3.2.** *The polynomial $h(x) = \lambda_1 x^5 + x^4 + \lambda_2 x \in \mathbb{F}_q[x]$ is divisible by $m(x) = x^2 + Ax + 1$ with $A \in \mathbb{F}_q$ if and only if $\lambda_2 \neq 0$ and*

$$s(\lambda_1, \lambda_2) = \lambda_1^3 - \lambda_1^2\lambda_2 - \lambda_1\lambda_2^2 + \lambda_2^3 - \lambda_2 = 0. \tag{3.1}$$

*Proof.* Let $h_1(x) = \lambda_1 x^4 + x^3 + \lambda_2$ such that $h(x) = xh_1(x)$. If $h(x)$ is divisible by $m(x)$, then $m(x)$ must be a factor of $h_1(x)$. If we divide $h_1(x)$ by $m(x) = x^2 + Ax + 1$, the remainder is

$$\left(-A^3\lambda_1 + A^2 + 2A\lambda_1 - 1\right) x - A^2\lambda_1 + A + \lambda_1 + \lambda_2 = c_1 x + c_0. \tag{3.2}$$

The polynomial $h_1(x)$ is divisible by $m(x)$ if and only if both $c_0$ and $c_1$ are zero. Direct calculation shows that

$$\begin{aligned} s(\lambda_1, \lambda_2) = {} & \left(-A^2\lambda_1^2 + A^2\lambda_1\lambda_2 - A\lambda_2 + \lambda_1^2 + 3\lambda_1\lambda_2 + \lambda_2^2\right) c_0 \\ & + \left(A\lambda_1^2 - A\lambda_1\lambda_2 + \lambda_2\right) c_1. \end{aligned} \tag{3.3}$$

Hence $s(\lambda_1, \lambda_2)$ vanishes when $h_1(x)$ is divisible by $m(x)$. When $\lambda_2 = 0$, condition (3.1) reduces to $\lambda_1^3 = 0$. Then $h_1(x) = x^3$, which contradicts divisibility by $m(x)$.

For the converse, assume that $\lambda_2 \neq 0$ and define

$$h_{1,1}(x) = x^2 + \frac{\lambda_1^2 - \lambda_2^2}{\lambda_2} x + 1 \tag{3.4}$$

$$\text{and} \qquad h_{1,2}(x) = \lambda_1 x^2 + (-\lambda_1^2 + \lambda_2^2)x + \lambda_2. \tag{3.5}$$

Direct calculation shows that

$$h_1(x) - h_{1,1}(x)h_{1,2}(x) = \left(\frac{(\lambda_1 + \lambda_2)x^2 - x^3}{\lambda_2}\right) s(\lambda_1, \lambda_2). \tag{3.6}$$

Hence the condition in (3.1) implies that the polynomial $h_{1,1}(x)$ in (3.4) is a factor of $h(x)$. □

Combining Lemma 3.1 and Lemma 3.2, we obtain the following characterization of the roots of $h(x)$ in $\mu_{q+1} \setminus \{1, -1\}$.

**Proposition 3.3.** *The polynomial $h(x) = \lambda_1 x^5 + x^4 + \lambda_2 x \in \mathbb{F}_q[x]$ has a root in $\mu_{q+1} \setminus \{1, -1\}$ if and only if all the following conditions hold:*

(i) $\lambda_2 \neq 0$,
(ii) $s(\lambda_1, \lambda_2) = \lambda_1^3 - \lambda_1^2\lambda_2 - \lambda_1\lambda_2^2 + \lambda_2^3 - \lambda_2 = 0$,

(iii) (a) $\lambda_1/\lambda_2 - 3$ *is not a square in* $\mathbb{F}_q$ *when* $q$ *is odd,*
(b) $\lambda_1 \neq \lambda_2$ *and* $\mathrm{Tr}\left(\frac{\lambda_2}{\lambda_1^2 - \lambda_2^2}\right) = 1$ *when* $q$ *is even.*

*Proof.* By Lemma 3.2, conditions (i) and (ii) are equivalent to $h(x)$ having a factor $m(x) = x^2 + Ax + 1$. From the proof of Lemma 3.2 it follows that $m(x) = h_{1,1}(x)$ given in (3.4). If $m(x)$ was a multiple of $h_{1,2}(x)$, then $\lambda_1 = \lambda_2$, which by (ii) implies $-\lambda_2 = 0$, contradicting (i). In order to apply Lemma 3.1, we have to investigate when $h_{1,1}(x)$ is irreducible. For odd characteristic, this is the case if and only if the discriminant $D$ of $h_{1,1}(x)$ is not a square in $\mathbb{F}_q$. Direct calculation yields

$$D = \lambda_1/\lambda_2 - 3 + \left(\frac{\lambda_1 + \lambda_2}{\lambda_2^2}\right) s(\lambda_1, \lambda_2) = \lambda_1/\lambda_2 - 3. \tag{3.7}$$

For the last equality, we have used condition (ii). In even characteristic, $m(x) = x^2 + Ax + 1$ is irreducible if and only if $A \neq 0$ and $\mathrm{Tr}(1/A) = 1$. Applying this criterion to $m(x) = h_{1,1}(x)$ yields the conditions in case (b) of (iii). We are left to investigate whether the second factor $h_{1,2}(x)$ in (3.5) has a root in $\mu_{q+1} \setminus \{1, -1\}$. If that is the case, we get $\lambda_1 = \lambda_2$. Then $s(\lambda_2, \lambda_2) = -\lambda_2 = 0$, a contradiction to condition (i). □

Note that necessity of condition (ii) was shown in [14, Lemma 3.1] for the polynomial $h_1(x)$ of degree four in the case of characteristic five.

## 4. PPs over finite fields of characteristic five

With this preparation, we study the action of $g(x) = x^5 h(x)^{q-1}$ on the set $\mu_{q+1}$, using the idea of diagram (2.2). Assuming that $h(x)$ has no roots in $\mu_{q+1}$ and using the relation $x^{q+1} = 1$ for $x \in \mu_{q+1}$, we have

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

Let $z$ be an arbitrary element in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and let $\Phi(x) = \frac{x+z}{x+z^q}$ and $\Phi^{-1}(x) = \frac{xz^q - z}{1-x}$, for any $x \neq 1$. We obtain

$$(g \circ \Phi)(x) = \frac{\lambda_2(x+z)^4(x+z^q) + (x+z)(x+z^q)^4 + \lambda_1(x+z^q)^5}{\lambda_1(x+z)^5 + (x+z)^4(x+z^q) + \lambda_2(x+z)(x+z^q)^4} \tag{4.1}$$

Let $\Delta(z, x) = \lambda_2(x+z)^4(x+z^q) + (x+z)(x+z^q)^4 + \lambda_1(x+z^q)^5$, then we have

$$\Delta(z^q, x) = \lambda_2(x+z^q)^4(x+z) + (x+z^q)(x+z)^4 + \lambda_1(x+z)^5.$$

Then we get

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

Choosing $z^q = -z$, i.e., $z$ is the square root of a non-square in $\mathbb{F}_q$, we get that the denominator is

$$\Delta(z^q, x) - \Delta(z, x) = (-\lambda_2 + 1)(zx^4 + z^3x^2) + (2\lambda_1 + 2\lambda_2 - 2)z^5. \tag{4.2}$$

Similarly, computing the numerator we get

$$\Delta(z,x)z^q - z\Delta(z^q,x) = -2z(\lambda_1+\lambda_2+1)x^5 + (\lambda_2+1)z^3x^3 + (\lambda_2+1)z^5x. \tag{4.3}$$

The following theorem is our main result.

**Theorem 4.1.** *Let $\mathbb{F}_q$ be a finite field, where $q = 5^k$. Let $h(x) = \lambda_1 x^5 + x^4 + \lambda_2 x$ with $\lambda_1, \lambda_2 \in \mathbb{F}_q$ and assume that $h(1) = \lambda_1 + \lambda_2 + 1 \neq 0$, $h(-1) = -\lambda_1 - \lambda_2 + 1 \neq 0$. Then $f(x) = x^5 h(x^{q-1}) = \lambda_1 x^{5q} + x^{4q+1} + \lambda_2 x^{q+4}$ is a permutation polynomial of $\mathbb{F}_{q^2}$ if and only if one of the following holds:*

(i) $\lambda_1 = 0$, $\lambda_2 \neq \pm 1$ *and $k$ is even,*
(ii) $\lambda_1 = 1$, $\lambda_2 = -1$ *and $k$ is even,*
(iii) $\lambda_1 = -1$, $\lambda_2 = 1$ *and $k$ is even,*
(iv) $(\lambda_1, \lambda_2) = (2,1)$ *or* $(\lambda_1, \lambda_2) = (3,-1)$ *for $q = 5$.*

*Proof.* By Lemma 2.1, we have to show that $g(x) = x^5 h(x)^{q-1}$ permutes the set $\mu_{q+1}$. We apply the idea shown in diagram (2.2) and hence show that $(\Phi^{-1} \circ g \circ \Phi)$ permutes $\mathbb{F}_q$. For this, we consider the curve defined by

$$\mathcal{C}(x,y) = \frac{(\Phi^{-1} \circ g \circ \Phi)(x) - (\Phi^{-1} \circ g \circ \Phi)(y)}{x - y} \tag{4.4}$$

and show that is has no rational points off the line $x = y$ over $\mathbb{F}_q$.

We first assume that $-\lambda_2 + 1 \neq 0$, that is, $\lambda_2 \neq 1$ and consider the map $(\Phi^{-1} \circ g \circ \Phi)(x)$ which is given by

$$2\frac{\lambda_1+\lambda_2+1}{\lambda_2-1}\left(\frac{x^5 + \dfrac{2\lambda_2+2}{\lambda_1+\lambda_2+1}z^2x^3 + \dfrac{2\lambda_2+2}{\lambda_1+\lambda_2+1}z^4x}{x^4 + z^2x^2 + \dfrac{3\lambda_1+3\lambda_2+2}{\lambda_2-1}z^4}\right). \tag{4.5}$$

We investigate whether this map in injective on $\mathbb{F}_q$. Recall that $h(x)$ may not have any root in $\mu_{q+1}$. In particular, $h(1) = \lambda_1 + \lambda_2 + 1 \neq 0$, i.e., the prefactor in (4.5) is non-zero. Moreover, we have assumed $\lambda_2 \neq 1$, i.e., the prefactor does not have a pole, and we can ignore it.

The denominator of the expression in brackets in (4.5) is the quartic polynomial

$$x^4 + z^2x^2 + \frac{3\lambda_1+3\lambda_2+2}{\lambda_2-1}z^4, \tag{4.6}$$

and we investigate when it has a root in $\mathbb{F}_q$. First note that the constant coefficient is non-zero, since $h(-1) = -\lambda_1 - \lambda_2 + 1 \neq 0$. Using the substitution $t = x^2$, we obtain a quadratic polynomial for $t$ with discriminant

$$D_1 = \frac{3\lambda_1 - \lambda_2 + 1}{\lambda_2 - 1}z^4. \tag{4.7}$$

When $D_1$ is not a square in $\mathbb{F}_q$, then there is no solution for $t$ in $\mathbb{F}_q$, and hence (4.5) has no pole in $\mathbb{F}_q$. Note that $z^4$ is a square in $\mathbb{F}_q$, and hence it is sufficient that $\dfrac{3\lambda_1 - \lambda_2 + 1}{\lambda_2 - 1}$ is a non-square in $\mathbb{F}_q$.

Next assume that $D_1$ is a square in $\mathbb{F}_q$, i.e., $D_1 = \delta^2 z^4$ for some $\delta \in \mathbb{F}_q$. Then (4.6) factors as

$$\Big(x^2 - 2(1+\delta)z^2\Big)\Big(x^2 - 2(1-\delta)z^2\Big). \tag{4.8}$$

Hence, (4.6) has a root in $\mathbb{F}_q$ when $D_1$ is a square in $\mathbb{F}_q$ and additionally $2(1+\delta)z^2$ or $2(1-\delta)z^2$ is a square in $\mathbb{F}_q$. As $z^2$ is a non-square in $\mathbb{F}_q$, the second part is equivalent to $2(1+\delta)$ or $2(1-\delta)$ being a non-square.

First consider the special case that $D_1 = 0$, i.e., $\lambda_2 = 3\lambda_1 + 1$. Then (4.8) has a root in $\mathbb{F}_q$ if and only if $2z^2$ is a square in $\mathbb{F}_q$, which is equivalent to $q = 5^k$ with $k$ odd. The roots are $\pm\sqrt{2}z$. For these values of $x$, the numerator of (4.5) is nonzero, i.e., (4.5) has a pole. That implies that we do not get a permutation polynomial when $\lambda_2 = 3\lambda_1 + 1 \neq 1$ and $q = 5^k$, $k$ odd.

When $D_1$ is a non-zero square, we have roots of (4.6) with

$$x^2 = 2(1 \pm \delta)z^2. \tag{4.9}$$

Recall that the constant coefficient of (4.6) is non-zero, and hence $x \neq 0$. In order to obtain a permutation polynomial, (4.5) must not have a pole in $\mathbb{F}_q$, i.e., it is necessary that the numerator of (4.5) vanishes as well for the roots (4.9) that lie in $\mathbb{F}_q$. We fix one root $x$ and compute for the fixed choice of the sign in the factor $1 \pm \delta$:

$$\begin{aligned} 0 &= x^5 + \frac{2\lambda_2+2}{\lambda_1+\lambda_2+1}z^2x^3 + \frac{2\lambda_2+2}{\lambda_1+\lambda_2+1}z^4x \\ &= x\left(x^4 + \frac{2\lambda_2+2}{\lambda_1+\lambda_2+1}z^2x^2 + \frac{2\lambda_2+2}{\lambda_1+\lambda_2+1}z^4\right) \\ &= x\left(4(1\pm\delta)^2z^4 + \frac{2\lambda_2+2}{\lambda_1+\lambda_2+1}2(1\pm\delta)z^4 + \frac{2\lambda_2+2}{\lambda_1+\lambda_2+1}z^4\right) \\ &= xz^4\left(4(1\pm\delta)^2 + \big(4(1\pm\delta)+2\big)\frac{\lambda_2+1}{\lambda_1+\lambda_2+1}\right). \end{aligned} \tag{4.10}$$

Using that both $x$ and $z$ are non-zero, this reduces to the condition

$$\left(4(1\pm\delta)^2 + \big(4(1\pm\delta)+2\big)\frac{\lambda_2+1}{\lambda_1+\lambda_2+1}\right) = 0. \tag{4.11}$$

From (4.7) we get the condition

$$\delta^2 = \frac{3\lambda_1 - \lambda_2 + 1}{\lambda_2 - 1}. \tag{4.12}$$

For either choice of the sign in the factor $1 \pm \delta$, combining (4.11) and (4.12) implies that $\lambda_1 = 0$ or $s(\lambda_1, \lambda_2) = 0$. This can be shown computing an elimination ideal in Magma. These cases are treated below, yielding reduced equations for $\mathcal{C}(x, y)$ in (4.22) and (4.27).

In summary, excluding the last two cases, (4.5) does not have a pole if and only if one of the following conditions holds:

(i) $\dfrac{3\lambda_1 - \lambda_2 + 1}{\lambda_2 - 1}$ is a non-square in $\mathbb{F}_q$, (4.13)

(ii) $\lambda_2 = 3\lambda_1 + 1$ and $q = 5^k$, $k$ even, (4.14)

(iii) $\dfrac{3\lambda_1 - \lambda_2 + 1}{\lambda_2 - 1} = \delta^2$ with $\delta \in \mathbb{F}_q$

and $2(1+\delta), 2(1-\delta)$ are both squares in $\mathbb{F}_q$. (4.15)

In the calculations with the possible factorizations of the curve (4.17) below, we check every possible outcome in terms of these conditions and we verify that they all satisfy one of the conditions above. Therefore, we do not add these conditions in the statement of the theorem.

Returning to the curve (4.4), consider the normalized denominator and numerator in (4.2) and (4.3) to obtain

$$\frac{\dfrac{x^5+A_1x^3+A_0x}{x^4+B_1x^2+B_0}-\dfrac{y^5+A_1y^3+A_0y}{y^4+B_1y^2+B_0}}{x-y}. \tag{4.16}$$

Simplifying this expression and considering the numerator, we obtain the following curve defined by a polynomial

$$\begin{aligned}\mathcal{C}(x,y) := {} & x^4y^4+B_1(x^4y^2+x^2y^4)+B_0(x^4+y^4)+(B_1-A_1)x^3y^3\\ & +(B_0-A_0)(x^3y+xy^3)+(B_0+A_1B_1-A_0)x^2y^2\\ & +A_1B_0(x^2+y^2)+(A_1B_0-A_0B_1)xy+A_0B_0,\end{aligned} \tag{4.17}$$

where we have used

$$\begin{aligned}A_0 &= \frac{-(\lambda_2+1)}{2(\lambda_1+\lambda_2+1)}z^4, \qquad A_1 = \frac{-(\lambda_2+1)}{2(\lambda_1+\lambda_2+1)}z^2,\\ B_0 &= \frac{(2\lambda_1+2\lambda_2-2)}{-\lambda_2+1}z^4, \qquad B_1 = z^2.\end{aligned} \tag{4.18}$$

Recall that we have chosen $z \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ such that $z^2 \in \mathbb{F}_q$.

First assume that the curve in (4.17) is absolutely irreducible. Note that the underlying idea here is first of all estimating the number of $\mathbb{F}_q$-rational points of the curve $\mathcal{C}(x,y)$ in (4.17). For this purpose, one can use Hasse-Weil type bounds (see for instance [33, Theorem 5.2.3] for the Hasse-Weil bound given in terms of algebraic function fields, [24] for the Lang-Weil bound). In this paper we use [23, Theorem 5.28] which involves a bound obtained from the Hasse-Weil bound. Let $\widetilde{\mathcal{C}}(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ be the homogeneous polynomial defined as

$$\widetilde{\mathcal{C}}(X,Y,Z) = Z^8\mathcal{C}\left(\frac{X}{Z},\frac{Y}{Z}\right).$$

Homogenization of $\mathcal{C}(x,y)$ in (4.17) by substituting $\left(\dfrac{X}{Z},\dfrac{Y}{Z}\right)$ yields a homogeneous polynomial of degree $d=8$. Let $\mathbb{P}^2(\mathbb{F}_q)$ denote the projective space consisting of projective coordinates $(X:Y:Z)$. Let $N = |\{(x,y) \in \mathbb{F}_q \times \mathbb{F}_q \mid \mathcal{C}(x,y)=0\}|$ be the number of affine $\mathbb{F}_q$-rational points of $\mathcal{C}$. Let $V = |\{(X:Y:Z) \in \mathbb{P}^2(\mathbb{F}_q) \mid \widetilde{\mathcal{C}}(X,Y,Z)=0\}|$ be the number of projective $\mathbb{F}_q$-rational points of $\widetilde{\mathcal{C}}$. Let $V_0$ and $V_1$ be the numbers of projective $\mathbb{F}_q$-rational points of $\widetilde{\mathcal{C}}$ corresponding to the cases $z=0$ and $z\neq 0$ respectively. Namely,

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

It follows from the definitions that $N=V_1$ and $V=V_0+V_1$. Moreover it follows from (4.17) that $\widetilde{\mathcal{C}}(X,Y,0)=X^4Y^4$. This implies $V_0 = |\{(1:0:0),(0:1:0)\}| = 2$. Using [23, Theorem 5.28] we get

$$|V-q| \leq (d-1)(d-2)q^{1/2}+c(d) = 42q^{1/2}+197, \tag{4.19}$$

where $c(d) = \frac{1}{2}d(d-1)^2 + 1$ and $d = 8$. The arguments above imply that

$$V = N + 2. \tag{4.20}$$

Combining (4.19) and (4.20) we conclude that

$$|N - q| = |(V - q) - 2| \leq |V - q| + 2 \leq 42q^{1/2} + 199.$$

Note that

$$|\{(x, y) \in \mathbb{F}_q^2 \mid \mathcal{C}(x, y) = 0 \text{ and } x = y\}| \leq 8$$

as $\mathcal{C}(x, x)$ is a polynomial of degree 8 in $\mathbb{F}_q[x]$. Therefore, if $q - 42q^{1/2} - 199 > 8$, then $\mathcal{C}(x, y)$ has an affine point off the line $x = y$. We note that $q - 42q^{1/2} - 199 > 8$ for any $q = 5^k$ with $k \geq 5$. 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 $q \geq 5^k$. In characteristic 5, it remains to consider $q \in \{5, 25, 125, 625\}$. Using MAGMA [9], we obtained the following:

(1) Over $\mathbb{F}_5$, $f(x)$ permutes $\mathbb{F}_{25}$ when $(\lambda_1, \lambda_2) = (2, 1)$ and $(\lambda_1, \lambda_2) = (3, -1)$.
(2) Over $\mathbb{F}_{25}$, $f(x)$ permutes $\mathbb{F}_{625}$ when $(\lambda_1, \lambda_2) = (-1, 1)$, $(\lambda_1, \lambda_2) = (1, -1)$ and $(\lambda_1, \lambda_2) = (0, \zeta)$ where $\zeta \in \mathbb{F}_{25} \setminus \{1, -1\}$.
(3) Over $\mathbb{F}_{125}$, $f(x)$ is not a PP of $\mathbb{F}_{5^6}$ for any $(\lambda_1, \lambda_2) \in \mathbb{F}_{125}^2 \setminus \{(0, 0)\}$.
(4) Over $\mathbb{F}_{625}$, the situation is similar to $\mathbb{F}_{25}$, with $\zeta \in \mathbb{F}_{625} \setminus \{1, -1\}$.

Hence, except the first item corresponding to item (iv) of Theorem 4.1 where $\mathcal{C}(x, y)$ is absolutely irreducible, all the remaining cases are covered by items (i)–(iii) of Theorem 4.1.

In order to obtain a permutation polynomial for $q \geq 5^5$, the polynomial $\mathcal{C}(x, y)$ in (4.17) has to be reducible. We consider all possible non-trivial factorizations of $\mathcal{C}(x, y)$, noting the symmetry which keeps $\mathcal{C}(x, y)$ fixed when we interchange $x$ and $y$. Without loss of generality, we fix a monomial ordering by taking $x > y$ and start with all factorizations of the leading monomials $x^4y^4$ which are symmetric with respect to interchanging $x$ and $y$. There are 22 possibilities listed in A.2. Each factor has the form

$$p_m(x, y) = m(x, y) + \sum_{m' < m} c_i m'(x, y),$$

where $m(x, y)$ is the leading monomial from the factorization of $x^4y^4$. For each of the monomials $m'(x, y)$ with $m' < m$ and for each of the factors $p_m(x, y)$ we use a different variable $c_i$ as coefficient.

We use the notion of Gröbner bases (see for instance [12]) in order to solve for the coefficients with the help of the computer algebra program MAGMA [9]. Namely, we subtract the products of the generic factors $p_m(x, y)$ from $\mathcal{C}(x, y)$ in (4.17) and compute a Gröbner basis of the ideal generated by the coefficients of this difference. The elimination ideal with respect to $\lambda_1$ and $\lambda_2$ provides necessary conditions on $\lambda_1$ and $\lambda_2$ for the particular factorization to exist. More details can be found in A.2. A similar approach has, for example, been used in [5]. We obtain the following necessary conditions:

(a) $\lambda_1 = 0$, or
(b) $\lambda_1 = 1$ and $\lambda_2 = -1$, or
(c) $\lambda_1^3 - \lambda_1^2\lambda_2 - \lambda_1\lambda_2^2 + \lambda_2^3 - \lambda_2 = 0$.

For each of these cases, we recompute the equation for the curve $\mathcal{C}(x, y)$ in (4.16).

First, assume that $\lambda_1 = 0$. In this case, (4.4) yields

$$2\frac{\lambda_2+1}{\lambda_2-1}\left(\frac{x^2y^2+2z^2(x+y)^2+z^4}{x^2y^2+2z^2(x^2+y^2)-z^4}\right), \tag{4.21}$$

and from the numerator we get the equation

$$\mathcal{C}(x,y) = x^2y^2+2z^2(x+y)^2+z^4. \tag{4.22}$$

The equation factors as

$$\mathcal{C}(x,y) = \left(xy+2\alpha z(x-y)-z^2\right)\left(xy-2\alpha z(x-y)-z^2\right) \tag{4.23}$$

where $\alpha^2 = 2$. For $q = 5^k$ and $k$ odd, $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and $\alpha^q = -\alpha$. Then $(\alpha z)^q = \alpha z$, i.e., $\mathcal{C}(x,y)$ factors over $\mathbb{F}_q$. For $y = -x$, equation (4.21) reduces to

$$2\frac{\lambda_2+1}{\lambda_2-1}\left(\frac{x^2-2z^2}{x^2+2z^2}\right).$$

This implies that the curve has the $\mathbb{F}_q$-rational point $(\alpha z, -\alpha z)$ off the line $x = y$, and we do not get a permutation polynomial for $k$ odd.

For $k$ even, $\alpha \in \mathbb{F}_q$. Then the two factors in (4.23) are conjugates over $\mathbb{F}_{q^2}[x,y]$. Any $\mathbb{F}_q$-rational point is hence a root of both factors, and also of their difference which equals $\alpha z(x-y)$. Hence the curve has no $\mathbb{F}_q$-rational points off the line $x = y$, we get a permutation polynomial when $k$ is even. This completes the proof of item (i) in Theorem 4.1.

Next, for case (b) assume that $\lambda_1 = 1$ and $\lambda_2 = -1$. Then (4.4) yields

$$\frac{x^4y^4+z^2(x^4y^2+x^3y^3+x^2y^4)-z^4(x^4+x^3y+x^2y^2+xy^3+y^4)}{(x^2-2z^2)^2(y^2-2z^2)^2}, \tag{4.24}$$

and from the numerator we get the equation

$$\begin{aligned}\mathcal{C}(x,y) = {} & x^4y^4+z^2(x^4y^2+x^3y^3+x^2y^4) \\ & -z^4(x^4+x^3y+x^2y^2+xy^3+y^4).\end{aligned} \tag{4.25}$$

The equation factors as

$$\begin{aligned}\mathcal{C}(x,y) = {} & \left(x^2y^2+2\alpha z(x^2y+xy^2)+z^2(2x^2+xy+2y^2)\right) \\ & \left(x^2y^2-2\alpha z(x^2y+xy^2)+z^2(2x^2+xy+2y^2)\right),\end{aligned} \tag{4.26}$$

where $\alpha^2 = 2$. Eq. (4.24) must not have a pole. Condition (4.14) requires that $q = 5^k$ with $k$ even, and hence $\alpha \in \mathbb{F}_q$. Then the two factors in (4.26) are conjugates over $\mathbb{F}_{q^2}[x,y]$. Any $\mathbb{F}_q$-rational point is hence a root of both factors. Computing the prime decomposition of the zero-dimensional ideal generated by the two factors we find that the only solutions are $(0,0) \in \mathbb{F}_q^2$ and $(\alpha z, -\alpha z), (-\alpha z, \alpha z) \in \mathbb{F}_{q^2}^2 \setminus \mathbb{F}_q^2$. As the curve has no $\mathbb{F}_q$-rational points off the line $x = y$, we get a permutation polynomial when $k$ is even. This completes the proof of item (ii) of Theorem 4.1.

For case (c), assume $s(\lambda_1,\lambda_2) = \lambda_1^3-\lambda_1^2\lambda_2-\lambda_1\lambda_2^2+\lambda_2^3-\lambda_2 = 0$. As the case $\lambda_1 = 0$ is covered in case (a), we can assume $\lambda_1 \neq 0$. Then the equation for the curve is

$$\begin{aligned}\mathcal{C}(x,y) = {} & (\lambda_1+\lambda_2+1)x^2y^2-z^2(\lambda_1^2+2\lambda_1-\lambda_2^2+2\lambda_2-2)(x^2+y^2) \\ & +z^2(\lambda_1-\lambda_2-1)xy+z^4(-\lambda_1^2+2\lambda_1+\lambda_2^2+2\lambda_2+1).\end{aligned} \tag{4.27}$$

Using similar techniques as described in A, we find that $\lambda_1 = 0$ for all possible non-trivial factorizations of this polynomial of degree 4. As this contradicts our assumption, there are no permutation polynomials in this case. Note, however, that case (c) is not excluded by

Proposition 3.3. The condition $s(\lambda_1, \lambda_2) = 0$ is only necessary for $h(x)$ to have a root in $\mu_{q+1} \setminus \{1, -1\}$, i.e., that one does not obtain a permutation polynomial.

Going back to (4.2) and (4.3), we now consider the case when $\lambda_2 = 1$. Recall that

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

Again choosing $z \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ with $z^q = -z$ we get that the denominator is

$$\Delta(z^q; x) - \Delta(z; x) = 2\lambda_1 z^5.$$

Similarly, computing the numerator we get

$$\Delta(z;x)z^q - z\Delta(z^q;x) = -2z(\lambda_1 + 2)x^5 + 2z^3x^3 + 2z^5x.$$

In this case

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

is a polynomial in $\mathbb{F}_{q^2}[x, y]$, and hence has no poles. After simplifying we obtain the following curve

$$\mathcal{C}(x,y) = x^4 + x^3y + xy^3 + y^4 + x^2y^2 + A(x^2 + xy + y^2) + B, \tag{4.28}$$

where $A = \dfrac{-z^2}{\lambda_1 + 2}$, $B = \dfrac{-z^4}{\lambda_1 + 2}$. The degree of the curve in (4.28) is smaller than the degree of the curve in (4.17). Therefore the case of $\mathcal{C}(x, y)$ being absolutely irreducible has already been covered above.

Hence, assume that $\mathcal{C}(x, y)$ in (4.28) is not absolutely irreducible and it is decomposed as follows:

$$(x^2 + \alpha_1 xy + \alpha_2 y^2 + \alpha_3 x + \alpha_4 y + \alpha_5)(\beta_1 x^2 + \beta_2 xy + \beta_3 y^2 + \beta_4 x + \beta_5 y + \beta_6).$$

Comparing the coefficients of this decomposition and $\mathcal{C}(x, y)$ in (4.28) we first obtain that $\beta_1 = 1$, $\beta_2 = 3$, $\beta_3 = 1$, $\alpha_1 = 3$, $\alpha_2 = 1$, $\beta_4 = -\alpha_3$, $\beta_5 = -\alpha_4$, $\beta_6 = \alpha_5$. Moreover, we get that $\beta_6^2 = B$ and $\beta_6 = 2A$. Thus $B = (2A)^2$ which implies that

$$\frac{4z^4}{(\lambda_1 + 2)^2} = \frac{-z^4}{\lambda_1 + 2}, \tag{4.29}$$

and so $\lambda_1 = -1$.

Now assume that $\lambda_1 = -1$ and $\lambda_2 = 1$. Then the curve has the equation

$$\mathcal{C}(x,y) = x^4 + x^3y + x^2y^2 - z^2(x^2 + xy + y^2) + xy^3 + y^4 - z^4. \tag{4.30}$$

The equation factors as

$$\mathcal{C}(x,y) = \left((x-y)^2 + \alpha z(x+y) - 2z^2\right)\left((x-y)^2 - \alpha z(x+y) - 2z^2\right), \tag{4.31}$$

where $\alpha^2 = 2$. As before, $\alpha z \in \mathbb{F}_q$ for $q = 5^k$ and $k$ odd. For $y = -x$, we get

$$\mathcal{C}(x,-x) = (x + 2\alpha z)^2(x - 2\alpha z)^2. \tag{4.32}$$

This implies that the curve has the $\mathbb{F}_q$-rational point $(2\alpha z, -2\alpha z)$ off the line $x = y$ and we do not get a permutation polynomial for $k$ odd.

For $k$ even, $\alpha \in \mathbb{F}_q$ and the two factors in (4.31) are conjugates over $\mathbb{F}_{q^2}[x, y]$. Any $\mathbb{F}_q$-rational point is hence a root of both factors. Computing the prime decomposition of the zero-dimensional ideal generated by the two factors we find that the only solutions are

$(\alpha z, -\alpha z), (-\alpha z, \alpha z) \in \mathbb{F}_{q^2}^2 \setminus \mathbb{F}_q^2$. As the curve has no $\mathbb{F}_q$-rational points, we get a permutation polynomial when $k$ is even.

For all the other decompositions of $\mathcal{C}(x, y)$ in (4.28), we obtain a contradiction after computing its Gröbner basis by MAGMA. This completes the proof of item (iii) of Theorem 4.1.

In all items in the statement of Theorem 4.1, the values of $\lambda_1$ and $\lambda_2$ do not satisfy at least one of the conditions of Proposition 3.3 and thus $h(x)$ does not have any roots in $\mu_{q+1}$. □

**Remark 4.2.** Items (ii) and (iii) in Theorem 4.1 have already been obtained in [2] and [14], respectively.

## 5. Comparison with existing permutation trinomials

**Definition 5.1.** [36] Two permutation polynomials $f(x), g(x) \in \mathbb{F}_q[x]$ are said to be quasi-multiplicative (QM) equivalent, if there exists $d \in \mathbb{Z}$, $1 \leq d \leq q-1$ with $\gcd(d, q-1) = 1$ and $f(x) = ag(cx^d) \pmod{x^q - x}$ , where $a, c \in \mathbb{F}_q^*$. If $c = 1$, then $f(x), g(x) \in \mathbb{F}_q[x]$ are called multiplicative equivalent.

In this section, we show that the permutation trinomial considered in this paper is not QM equivalent to some known classes. We first observe that two QM equivalent permutations must have exactly the same number of terms. Therefore, we only need to compare the permutation trinomials found in this paper with known permutation trinomials over $\mathbb{F}_{q^2}$ where $q = 5^k$. We use the method in [36] for this purpose. In order to determine whether the permutation polynomial $f(x) = x^{4q+1} + \lambda_1 x^{5q} + \lambda_2 x^{q+4} \in \mathbb{F}_q[x]$ is QM equivalent to any permutation trinomial of the form $g(x) = a_1 x^{s_1} + a_2 x^{s_2} + a_3 x^{s_3} \in \mathbb{F}_q[x]$, 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 $\{ks_1, ks_2, ks_3\} \equiv \{4q + 1, 5q, q + 4\} \bmod (q^2 - 1)$.
Step 2: Comparison of the coefficients of $f(x)$ and $b_2 g(b_1 x^k)$.
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 $f(x)$ and $b_2 g(b_1 x^k)$.

In [2], Bai and Xia characterized the multiplicative equivalence of $f(x)$ when $(\lambda_1, \lambda_2) = (1, 4)$ and their result can be modified to the more general setting that we consider in this paper. The proof of the following is very similar to Proposition 1 in [2], therefore it is omitted.

**Proposition 5.2.** *In characteristic* 5*, the polynomial* $f(x) = x^{4q+1} + \lambda_1 x^{5q} + \lambda_2 x^{q+4} \in \mathbb{F}_q[x]$ *with* $q = 5^k$ *is multiplicative equivalent to the following permutation trinomials of* $\mathbb{F}_{q^2}$*:*

- $f_1(x) = \lambda_1 x + x^{(4 \cdot 5^{k-1}+1)(q-1)+1} + \lambda_2 x^{(5^{k-1}+1)(q-1)+1}$,
- $f_2(x) = x + \lambda_1 x^{\frac{2q+1}{3}(q-1)+1} + \lambda_2 x^q$,
- $f_3(x) = \lambda_2 x + x^q + \lambda_1 x^{\frac{q+5}{3}(q-1)+1}$.

Bai and Xia presented a list of known polynomials in Table 3 in [2] to which $f(x)$ is not multiplicative equivalent. Therefore we omit the polynomials listed in Table 3 in [2] and we consider the polynomials given in Table 1 below. We applied the method in [36] above using MAGMA and we have verified that $f(x)$ is not QM equivalent to any of them. To the best of our knowledge, the list in Table 1 below is complete.

We now consider case (i) in Theorem 4.1, where $\lambda_1 = 0$ and we have the binomial $f(x) = x^{4q+1} + \lambda_2 x^{q+4}$. Observe that $f(x)$ is QM equivalent to the linearized polynomial $g(x) =$

| $g(x)$ | $q$ | Conditions | Reference |
|---|---|---|---|
| $ax + bx^{q+2} + x^{2q+3}$ | any | $a, b \in \mathbb{F}_{q^2}$ | [16] |
| $a^q x^{kq(q-1)+1} + ax^{k(q-1)+1} + cx$ | any | $\gcd(k, q+1) = 1$, $a \in \mathbb{F}_{q^2}^*$, $c \in \mathbb{F}_q$ | [27] |
| $ax^{-(q-1)+1} + bx^{(q-1)+1} + cx$ | any | $a, b, c \in \mathbb{F}_{q^2}^*$ | [27] |
| $x + ax^{q(q-1)+1} + bx^{2(q-1)+1}$ | odd | $a, b \in \mathbb{F}_{q^2}^*$ | [7, 35] |
| $x - x^{\frac{q+3}{2}(q-1)+1} + x^{q(q-1)+1}$ | $5^k$ | $k$ odd | [40] |
| $x^q - x^{\frac{q+1}{2}(q-1)+1} + x^{2(q-1)+1}$ | $5^k$ | $k$ odd | [40] |
| $x^q - x^{\frac{q+1}{2}(q-1)+1} + x^{\frac{q-1}{2}(q-1)+1}$ | $5^k$ | $k$ odd | [40] |
| $x^q - x^{q(q-1)+1} + x^{\frac{q+1}{2}(q-1)+1}$ | $5^k$ | $k$ even | [40] |
| $x + x^{\frac{q+3}{2}(q-1)+1} - x^{q(q-1)+1}$ | $5^k$ | $k$ even | [40] |
| $x^r + \lambda_1 x^{s(q-1)+r} + \lambda_2 x^{2s(q-1)+r}$ | odd | $\gcd(r, q-1) = 1$ $\gcd(r-2s, q+1) = 1$ | [10] |
| $x + \lambda_1 x^{\frac{q+3}{2}(q-1)+1} + \lambda_2 x^{q(q-1)+1}$ | $5^k$ | $\lambda_1, \lambda_2 \in \{(-1,-1), (1,1), (1,-1)\}$ | [10] |
| $x^{3(q-1)+3} + bx^{(q-1)+3} + cx^3$ | any | $\gcd(3, q-1) = 1$ | [30] |
| $cx - x^s + x^{qs}$ | odd | $s = \frac{3q^2+2q-1}{4}$ or $s = \frac{(q+1)^2}{4}$ | [41] |

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

$x^q + bx \in \mathbb{F}_{q^2}[x]$, where $f(x) = g(x^{q+4}) \bmod (x^{q^2} - x)$ with $b = \lambda_2 \in \mathbb{F}_q$. Since $g(x)$ is linearized, Theorem 7.9 in [28] tells that $g(x) = x^q + bx$ permutes $\mathbb{F}_{q^2}$ if and only if $g(x)$ only has the root 0 in $\mathbb{F}_{q^2}$. This happens if and only if $(-b)^{q+1} \neq 1$. Indeed, if $g(\omega) = 0$, for some $\omega \in \mathbb{F}_{q^2}^*$, then $-b = \omega^{q-1}$ and therefore $(-b)^{q+1} = 1$. Conversely, if $(-b)^{q+1} = 1$, then $-b = \gamma^{k(q-1)}$, for some $k \in \mathbb{Z}$ and some primitive element $\gamma \in \mathbb{F}_{q^2}^*$. In that case, $g(\gamma^k) = 0$. Hence, $g(x)$ permutes $\mathbb{F}_{q^2}$ if and only if $(-b)^{q+1} \neq 1$. In our case where $b = \lambda_2 \in \mathbb{F}_q$, this corresponds to $(-\lambda_2)^{q+1} = (-\lambda_2)^2 = \lambda_2^2 \neq 1$ (i.e. $\lambda_2 \neq \pm 1$).

**Remark 5.3.** Note that this QM equivalence holds in any characteristic $p$ since $f(x) = x^{(p-1)q+1} + \lambda_2 x^{q+p-1} = g(x^{q+p-1}) \bmod (x^{q^2} - x)$ with $g(x) = x^q + \lambda_2 x$.

## DECLARATIONS

**Ethics approval and consent to participate.** Not applicable.

**Consent for publication.** Not applicable.

**Availability of data and materials.** The data used to support the findings of this study is available from the authors upon reasonable request.

**Competing interests.** Not applicable.

**Funding.** Markus Grassl received research support from Fundacja na rzecz Nauki Polskiej, MAB/2018/5.

**Authors' contributions.** Markus Grassl, Ferruh Özbudak, Buket Özkaya and Burcu Gülmez Temür contributed equally to this work.

## Acknowledgments

We would like to thank the anonymous referees for their valuable suggestions and comments which improved our paper. The 'International Centre for Theory of Quantum Technologies' project (contract no. MAB/2018/5) is carried out within the International Research Agendas Programme of the Foundation for Polish Science co-financed by the European Union from the funds of the Smart Growth Operational Programme, axis IV: Increasing the research potential (Measure 4.3).

## Appendix A. Factorizations of $\mathcal{C}(x, y)$

A.1. **Overview.** We consider all factorizations of $\mathcal{C}(x, y)$ given in (4.17). Out of 108 non-trivial factorizations of the leading monomial $x^4y^4$, it is sufficient to consider the 22 cases that are invariant with respect to interchanging $x$ and $y$. We did not impose that symmetry on the factors themselves, but used different coefficients $c_i$ for all factors. For each of the 22 cases listed below, we consider the coefficients with respect to $x$ and $y$ of the difference of $\mathcal{C}(x, y)$ in (4.17) and the product of the factors. Those generate an ideal in the polynomial ring with variables $A_0, A_1, B_0, B_1$ and $c_i$. From the substitutions (4.18) we obtain additional polynomial relations between $A_0, A_1, B_0, B_1$ and $\lambda_1, \lambda_2$. We treat $z$ as a variable, too. In the derivation of the equations, we made the following assumptions: $\lambda_2 \neq 1$, $\lambda_1 + \lambda_2 + 1 \neq 0$, $\lambda_1 + \lambda_2 - 1 \neq 0$, and $z \neq 0$. Those can be accounted for by considering the saturation of the ideal by the corresponding polynomials, i.e., computing ideal quotients.

While computer algebra systems like MAGMA [9] provide implementations of all the required algorithms, the computations can be simplified a lot in our case. As we are only interested in the solutions of the system of polynomial equations, we can replace any non-square-free polynomial by its square-free part. Moreover, if a polynomial in the basis of an intermediate result splits, we can treat each factor separately. We first use so-called grevlex order, and in the final step an elimination order to obtain the conditions on $\lambda_1$ and $\lambda_2$. The whole computation took less than 3 hours, with cases 7 and 19 taking about 45% and 25% of the total time, respectively. The calculations did no use more than 1 GB of memory.

When the final Gröbner basis contains the constant 1, then we have no solution to the original equations or those equations imply that some of the expressions that are assumed to be zero vanish. We summarize those cases by just stating that we obtain a contradiction.

A.2. **The 22 cases.**

1. $(x^2+c_{10}xy^4+c_9xy^3+c_8xy^2+c_7xy+c_6x+c_5y^4+c_4y^3+c_3y^2+c_2y+c_1)(y+c_{11})(x+c_{16}y^4+c_{15}y^3+c_{14}y^2+c_{13}y+c_{12})(y^2+c_{18}y+c_{17})(xy+c_{24}x+c_{23}y^4+c_{22}y^3+c_{21}y^2+c_{20}y+c_{19})$
   In this case, we obtain a contradiction.
2. $(y+c_1)(x+c_6y^4+c_5y^3+c_4y^2+c_3y+c_2)(y^3+c_9y^2+c_8y+c_7)(x^3+c_{24}x^2y^4+c_{23}x^2y^3+c_{22}x^2y^2+c_{21}x^2y+c_{20}x^2+c_{19}xy^4+c_{18}xy^3+c_{17}xy^2+c_{16}xy+c_{15}x+c_{14}y^4+c_{13}y^3+c_{12}y^2+c_{11}y+c_{10})$
   Here, we again get a contradiction.
3. $(y+c_1)(x+c_6y^4+c_5y^3+c_4y^2+c_3y+c_2)(x^2y^2+c_{18}x^2y+c_{17}x^2+c_{16}xy^4+c_{15}xy^3+c_{14}xy^2+c_{13}xy+c_{12}x+c_{11}y^4+c_{10}y^3+c_9y^2+c_8y+c_7)(xy+c_{24}x+c_{23}y^4+c_{22}y^3+c_{21}y^2+c_{20}y+c_{19})$
   In this case, we obtain two possibilities: either $\lambda_1 = 0$ or $\lambda_1^3-\lambda_1^2\lambda_2-\lambda_1\lambda_2^2+\lambda_2^3-\lambda_2 = 0$.
4. $(y+c_1)(x+c_6y^4+c_5y^3+c_4y^2+c_3y+c_2)(xy+c_{12}x+c_{11}y^4+c_{10}y^3+c_9y^2+c_8y+c_7)(xy+c_{18}x+c_{17}y^4+c_{16}y^3+c_{15}y^2+c_{14}y+c_{13})(xy+c_{24}x+c_{23}y^4+c_{22}y^3+c_{21}y^2+c_{20}y+c_{19})$
   Here we get $\lambda_1 = 0$.

5. $(y+c_1)(x+c_6y^4+c_5y^3+c_4y^2+c_3y+c_2)(xy^2+c_{13}xy+c_{12}x+c_{11}y^4+c_{10}y^3+c_9y^2+c_8y+c_7)(x^2y+c_{24}x^2+c_{23}xy^4+c_{22}xy^3+c_{21}xy^2+c_{20}xy+c_{19}x+c_{18}y^4+c_{17}y^3+c_{16}y^2+c_{15}y+c_{14})$
   We again have $\lambda_1 = 0$.
6. $(x^3y^3+c_{18}x^3y^2+c_{17}x^3y+c_{16}x^3+c_{15}x^2y^4+c_{14}x^2y^3+c_{13}x^2y^2+c_{12}x^2y+c_{11}x^2+c_{10}xy^4+c_9xy^3+c_8xy^2+c_7xy+c_6x+c_5y^4+c_4y^3+c_3y^2+c_2y+c_1)(y+c_{19})(x+c_{24}y^4+c_{23}y^3+c_{22}y^2+c_{21}y+c_{20})$
   We have either $\lambda_1 = 0$ or $\lambda_1^3-\lambda_1^2\lambda_2-\lambda_1\lambda_2^2+\lambda_2^3-\lambda_2=0$.
7. $(x^2+c_{10}xy^4+c_9xy^3+c_8xy^2+c_7xy+c_6x+c_5y^4+c_4y^3+c_3y^2+c_2y+c_1)(y+c_{11})(y+c_{12})(x+c_{17}y^4+c_{16}y^3+c_{15}y^2+c_{14}y+c_{13})(x+c_{22}y^4+c_{21}y^3+c_{20}y^2+c_{19}y+c_{18})(y^2+c_{24}y+c_{23})$
   In this case, we get a contradiction.
8. $(y+c_1)(y+c_2)(x+c_7y^4+c_6y^3+c_5y^2+c_4y+c_3)(x+c_{12}y^4+c_{11}y^3+c_{10}y^2+c_9y+c_8)(xy+c_{18}x+c_{17}y^4+c_{16}y^3+c_{15}y^2+c_{14}y+c_{13})(xy+c_{24}x+c_{23}y^4+c_{22}y^3+c_{21}y^2+c_{20}y+c_{19})$
   We have $\lambda_1 = 0$.
9. $(y+c_1)(y+c_2)(x+c_7y^4+c_6y^3+c_5y^2+c_4y+c_3)(x+c_{12}y^4+c_{11}y^3+c_{10}y^2+c_9y+c_8)(x^2y^2+c_{24}x^2y+c_{23}x^2+c_{22}xy^4+c_{21}xy^3+c_{20}xy^2+c_{19}xy+c_{18}x+c_{17}y^4+c_{16}y^3+c_{15}y^2+c_{14}y+c_{13})$
   Here, $\lambda_1 = 0$ or $\lambda_1^3-\lambda_1^2\lambda_2-\lambda_1\lambda_2^2+\lambda_2^3-\lambda_2=0$.
10. $(y+c_1)(y+c_2)(y+c_3)(x+c_8y^4+c_7y^3+c_6y^2+c_5y+c_4)(x+c_{13}y^4+c_{12}y^3+c_{11}y^2+c_{10}y+c_9)(x+c_{18}y^4+c_{17}y^3+c_{16}y^2+c_{15}y+c_{14})(xy+c_{24}x+c_{23}y^4+c_{22}y^3+c_{21}y^2+c_{20}y+c_{19})$
    Here, we get a contradiction.
11. $(y+c_1)(y+c_2)(y+c_3)(y+c_4)(x+c_9y^4+c_8y^3+c_7y^2+c_6y+c_5)(x+c_{14}y^4+c_{13}y^3+c_{12}y^2+c_{11}y+c_{10})(x+c_{19}y^4+c_{18}y^3+c_{17}y^2+c_{16}y+c_{15})(x+c_{24}y^4+c_{23}y^3+c_{22}y^2+c_{21}y+c_{20})$
    We again get a contradiction.
12. $(x^2+c_{10}xy^4+c_9xy^3+c_8xy^2+c_7xy+c_6x+c_5y^4+c_4y^3+c_3y^2+c_2y+c_1)(y^2+c_{12}y+c_{11})(xy+c_{18}x+c_{17}y^4+c_{16}y^3+c_{15}y^2+c_{14}y+c_{13})(xy+c_{24}x+c_{23}y^4+c_{22}y^3+c_{21}y^2+c_{20}y+c_{19})$
    In this case we obtain $\lambda_1 = 0$.
13. $(x^2+c_{10}xy^4+c_9xy^3+c_8xy^2+c_7xy+c_6x+c_5y^4+c_4y^3+c_3y^2+c_2y+c_1)(x^2y^2+c_{22}x^2y+c_{21}x^2+c_{20}xy^4+c_{19}xy^3+c_{18}xy^2+c_{17}xy+c_{16}x+c_{15}y^4+c_{14}y^3+c_{13}y^2+c_{12}y+c_{11})(y^2+c_{24}y+c_{23})$
    In this case we obtain that either $\lambda_1 = 0$ or $\lambda_1^3-\lambda_1^2\lambda_2-\lambda_1\lambda_2^2+\lambda_2^3-\lambda_2=0$.
14. $(x^2+c_{10}xy^4+c_9xy^3+c_8xy^2+c_7xy+c_6x+c_5y^4+c_4y^3+c_3y^2+c_2y+c_1)(x_2+c_{20}xy^4+c_{19}xy^3+c_{18}xy^2+c_{17}xy+c_{16}x+c_{15}y^4+c_{14}y^3+c_{13}y^2+c_{12}y+c_{11})(y^2+c_{22}y+c_{21})(y^2+c_{24}y+c_{23})$
    We obtain a contradiction in this case.
15. $(y^3+c_3y^2+c_2y+c_1)(x^3+c_{18}x^2y^4+c_{17}x^2y^3+c_{16}x^2y^2+c_{15}x^2y+c_{14}x^2+c_{13}xy^4+c_{12}xy^3+c_{11}xy^2+c_{10}xy+c_9x4c_8y^4+c_7y^3+c_6y^2+c_5y+c_4)(xy+c_{24}x+c_{23}y^4+c_{22}y^3+c_{21}y^2+c_{20}y+c_{19})$
    We obtain a contradiction.
16. $(y^4+c_4y^3+c_3y^2+c_2y+c_1)(x^4+c_{24}x^3y^4+c_{23}x^3y^3+c_{22}x^3y^2+c_{21}x^3y+c_{20}x^3+c_{19}x^2y^4+c_{18}x^2y^3+c_{17}x^2y^2+c_{16}x^2y+c_{15}x^2+c_{14}xy^4+c_{13}xy^3+c_{12}xy^2+c_{11}xy+c_{10}x+c_9y^4+c_8y^3+c_7y^2+c_6y+c_5)$
    We again get a contradiction.
17. $(xy^2+c_7xy+c_6x+c_5y^4+c_4y^3+c_3y^2+c_2y+c_1)(x^2y+c_{18}x^2+c_{17}xy^4+c_{16}xy^3+c_{15}xy^2+c_{14}xy+c_{13}x+c_{12}y^4+c_{11}y^3+c_{10}y^2+c_9y+c_8)(xy+c_{24}x+c_{23}y^4+c_{22}y^3+c_{21}y^2+c_{20}y+c_{19})$
    In this case we obtain $\lambda_1 = 0$.
18. $(x^3y^3+c_{18}x^3y^2+c_{17}x^3y+c_{16}x^3+c_{15}x^2y^4+c_{14}x^2y^3+c_{13}x^2y^2+c_{12}x^2y+c_{11}x^2+c_{10}xy^4+c_9xy^3+c_8xy^2+c_7xy+c_6x+c_5y^4+c_4y^3+c_3y^2+c_2y+c_1)(xy+c_{24}y^4+c_{23}y^4+c_{22}y^3+c_{21}y^2+c_{20}y+c_{19})$
    Here we have $\lambda_1 = 0$ or $\lambda_1^3-\lambda_1^2\lambda_2-\lambda_1\lambda_2^2+\lambda_2^3-\lambda_2=0$.
19. $(x^2y^2+c_{12}x^2y+c_{11}x^2+c_{10}xy^4+c_9xy^3+c_8xy^2+c_7xy+c_6x+c_5y^4+c_4y^3+c_3y^2+c_2y+c_1)(xy+c_{18}x+c_{17}y^4+c_{16}y^3+c_{15}y^2+c_{14}y+c_{13})(xy+c_{24}x+c_{23}y^4+c_{22}y^3+c_{21}y^2+c_{20}y+c_{19})$
    We get $\lambda_1 = 0$ or $\lambda_1^3-\lambda_1^2\lambda_2-\lambda_1\lambda_2^2+\lambda_2^3-\lambda_2=0$.

20. $(xy+c_6x+c_5y^4+c_4y^3+c_3y^2+c_2y+c_1)(xy+c_{12}x+c_{11}y^4+c_{10}y^3+c_9y^2+c_8y+c_7)(xy+c_{18}x+c_{17}y^4+c_{16}y^3+c_{15}y^2+c_{14}y+c_{13})(xy+c_{24}x+c_{23}y^4+c_{22}y^3+c_{21}y^2+c_{20}y+c_{19})$
    In this case we obtain $\lambda_1 = 0$.
21. $(xy^3+c_8xy^2+c_7xy+c_6x+c_5y^4+c_4y^3+c_3y^2+c_2y+c_1)(x^3y+c_{24}x^3+c_{23}x^2y^4+c_{22}x^2y^3+c_{21}x^2y^2+c_{20}x^2y+c_{19}x^2+c_{18}xy^4+c_{17}xy^3+c_{16}xy^2+c_{15}xy+c_{14}x+c_{13}y^4+c_{12}y^3+c_{11}y^2+c_{10}y+c_9)$
    We again get $\lambda_1 = 0$.
22. $(x^2y^2+c_{12}x^2y+c_{11}x^2+c_{10}xy^4+c_9xy^3+c_8xy^2+c_7xy+c_6x+c_5y^4+c_4y^3+c_3y^2+c_2y+c_1)(x^2y^2+c_{24}x^2y+c_{23}x^2+c_{22}xy^4+c_{21}xy^3+c_{20}xy^2+c_{19}xy+c_{18}x+c_{17}y^4+c_{16}y^3+c_{15}y^2+c_{14}y+c_{13})$
    In this case we obtain that either $\lambda_1 = 0$ or $\lambda_1^3-\lambda_1^2\lambda_2-\lambda_1\lambda_2^2+\lambda_2^3-\lambda_2 = 0$, or $\lambda_1 = 1, \lambda_2 = -1$. Note that the last one is the same as the result of Bai and Xia [2].

## 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] Bai T., Xia Y., A new class of permutation trinomials constructed from Niho exponents, Cryptogr. Commun. 10, 1023–1036 (2018).
[3] Bartoli, D., On a conjecture about a class of permutation trinomials, Finite Fields Appl. 52, 30–50 (2018).
[4] Bartoli, D., Hasse-Weil type theorems and relevant classes of polynomial functions, in K. Dabrowski, M. Gadouleau, N. Georgiou, M. Johnson, G. Mertzios, D. Paulusma (Eds.), Surveys in Combinatorics 2021 (London Mathematical Society Lecture Note Series, 43–102), Cambridge University Press (2021).
[5] Bartoli, D., Bonini, M., A short note on polynomials $f(X) = X + AX^{1+q^2(q-1)/4} + BX^{1+3q^2(q-1)/4} \in \mathbb{F}_{q^2}[X]$, $q$ even, J. Alg. Appl. 22, no. 07, 2350144 (2023).
[6] Bartoli, D., Giulietti, M., Permutation polynomials, fractional polynomials, and algebraic curves, Finite Fields Appl. 51, 1–16 (2018).
[7] Bartoli, D., Timpanella, M., A family of permutation trinomials over $\mathbb{F}_{q^2}$, Finite Fields Appl. 70, 101781 (2021).
[8] Bartoli, D., Timpanella, M., On a conjecture on APN permutations, Cryptogr. Commun. 14, 925–931 (2022).
[9] Bosma W., Cannon J., and Playoust C., The Magma algebra system. I. The user language, J. Symbolic Comput. 24, 1179–1260 (1997).
[10] Cao, X., Hou, X., Mi, J., Xu, S., More permutation polynomials with Niho exponents which permute $\mathbb{F}_{q^2}$, Finite Fields Appl. 62, 101626 (2020).
[11] Caullery, F., Schmidt, K.-U., Zhou, Y., Exceptional planar polynomials, Des. Codes Cryptogr. 78, 605–613 (2016).
[12] Cox, D., Little, D., O'Shea, D., Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra, Undergraduate Texts in Mathematics, Springer, Cham (2015).
[13] 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).
[14] Gupta, R., Rai, A., A note on a class of permutation trinomials, Journal of Algebra and Its Applications, Vol. 22, No. 08, 2350163 (2023).
[15] Gupta, R., Sharma, R. K., Some new classes of permutation trinomials over finite fields with even characteristic, Finite Fields Appl. 41, 89–96 (2016).
[16] Gupta, R., Sharma, R. K., Determination of a type of permutation binomials and trinomials, Appl. Algebra Engrg. Comm. Comput. 31, 65–86 (2020).
[17] Hermite, Ch., Sur les fonctions de sept lettres, C.R. Acad. Sci. Paris 57, 750–757 (1863).
[18] Hernando, F., McGuire, G., Monserrat, F., On the classification of exceptional planar functions over $\mathbb{F}_p$, Geom. Dedicata 173, 1–35 (2014).
[19] Hou, X., Permutation polynomials over finite fields – a survey of recent advances, Finite Fields Appl. 32, 82–119 (2015).
[20] Hou, X., Determination of a type of permutation trinomials over finite fields, Finite Fields Appl. 35, 16–35 (2015).

[21] 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).
[22] Hou, X., Applications of the Hasse-Weil bound to permutation polynomials, Finite Fields Appl. 54, 113–132 (2018).
[23] Hou, X., Lectures on finite fields, Graduate Studies in Mathematics, 190, American Mathematical Society, Providence, RI (2018)
[24] Lang, S., Weil, A., Number of points of varieties in finite fields, Am. J. Math. 76, 819–827 (1954).
[25] Li, K., Qu, L., Chen, X., New classes of permutation binomials and permutation trinomials over finite fields, Finite Fields Appl. 43, 69–85 (2017).
[26] 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).
[27] Li, L., Wang, Q., Xu, Y., Zeng, X., Several classes of complete permutation polynomials with Niho exponents, Finite Fields Appl. 72, 101831 (2021).
[28] Lidl, R. and Niederreiter, H., Finite Fields (Encyclopedia of Mathematics and its Applications), Cambridge University Press, Cambridge (1997).
[29] Mullen, G. L. and Panario, D., Handbook of Finite Fields, Discrete Mathematics and its Applications (Boca Raton), CRC Press, Boca Raton, FL (2013).
[30] 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. 90, 1537–1556 (2022).
[31] 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.
[32] Park, Y. H. and Lee, J. B., Permutation polynomials and group permutation polynomials, Bull. Austral. Math. Soc. 63, 67–74 (2001).
[33] Stichtenoth, H., Algebraic Function Fields and Codes (2nd edition), Graduate Texts in Mathematics, 254, Springer, Berlin (2009).
[34] Schmidt, K.-U., Zhou, Y., Planar functions over fields of characteristic two, J. Algebraic Combin. 40, 503–526 (2014).
[35] Tu, Z., Zeng, X., A class of permutation trinomials over finite fields of odd characteristic, Cryptogr. Commun. 11, 563–583 (2019).
[36] Tu, Z., Zeng, X., Li, C. and Helleseth, T., A class of new permutation trinomials. Finite Fields Appl. 50, 178–195 (2018).
[37] 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).
[38] Wang, Q., Cyclotomic mapping permutation polynomials over finite fields, Sequences, subsequences, and consequences, Lecture Notes in Comput. Sci., 4893, Springer, Berlin, 119–128, (2007).
[39] 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).
[40] Wu, G., Li, N., Several classes of permutation trinomials over $\mathbb{F}_{5^n}$, Cryptogr. Commun. 11, 313–324 (2019).
[41] Zheng, D., Yuan, Y., Yu, L., Two types of permutation polynomials with special forms, Finite Fields Appl. 56, 1–16 (2019).
[42] 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).

International Centre for Theory of Quantum Technologies, University of Gdansk, Poland
*Email address*: markus.grassl@ug.edu.pl

FENS, Sabanci University, Ístanbul, Turkey
*Email address*: ferruh.ozbudak@sabanciuniv.edu

Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey
*Email address*: ozkayab@metu.edu.tr

Department of Mathematics, Atilim University, Ankara, Turkey
*Email address*: burcu.temur@atilim.edu.tr