Finite Fields and Their Applications 96 (2024) 102418

Contents lists available at ScienceDirect

Finite Fields and Their Applications

journal homepage: www.elsevier.com/locate/ffa

On permutation quadrinomials from Niho exponents in characteristic two

Vincenzo Pallozzi Lavorante

Department of Mathematics and Statistics, University of South Florida, Tampa, FL 33620, USA

A R T I C L E I N F O

Article history:
Received 1 June 2023
Received in revised form 8 January 2024
Accepted 13 March 2024
Available online 26 March 2024
Communicated by Gary L. Mullen

MSC:
11T06
11T55
14H05

Keywords:
Permutation quadrinomials
Hasse-Weil
Niho exponents

A B S T R A C T

Recently Zheng et al. [18] characterized the coefficients of $f(x) = x + a_1 x^{s_1(2^m-1)+1} + a_2 x^{s_2(2^m-1)+1} + a_3 x^{s_3(2^m-1)+1}$ over $\mathbb{F}_{2^{2m}}$ that lead $f(x)$ to be a permutation of $\mathbb{F}_{2^{2m}}$ for $(s_1, s_2, s_3) = (\frac{1}{4}, 1, \frac{3}{4})$. They left open the question whether those conditions were also necessary. In this paper, we give a positive answer to that question, solving their conjecture.

1. Introduction

Let $q = p^m$ be a prime power. Let $\mathbb{F}_q$ denote the finite fields of q elements. A polynomial $f \in \mathbb{F}_q[x]$ is called a permutation polynomial (PP) of $\mathbb{F}_q$ if the induced mapping $x \mapsto f(x)$ is a bijection of $\mathbb{F}_q$. Several authors in recent history have focused on permutation polynomials and their applications. For example, PPs have been widely used in

E-mail address: vincenzop@usf.edu.

https://doi.org/10.1016/j.ffa.2024.102418
1071-5797/

coding theory and cryptography, and we refer the reader to [9,10] for a survey on the latest advances. Recently, PPs taking simple forms and few terms have attracted much interest and have been deeply investigated. In [19,17] the authors provided a powerful method to construct PPs using the set of $q+1$-th roots of unity. Along this view, several new families of PPs have been constructed and we refer the reader to [6,15,14,13,12] for more details.

Another way to look at the PPs is based on algebraic curves over finite fields. In [11], it was shown how to use the theory of algebraic curves to determine whether a polynomial is a permutation polynomial or not.

Permutation trinomials with Niho exponents of the form $f(x) = x + a_1 x^{s_1(2^m-1)+1} + a_2 x^{s_2(2^m-1)+1} \in \mathbb{F}_{q^2}[x]$, have attracted much interest in recent years. See for example [2, 8,5]. The parameters s_1, s_2 should be read modulo $q+1$. Given (s_1, s_2), finding conditions on a_1, a_2 that are sufficient and necessary for f to be a permutation polynomial of $\mathbb{F}_{q^2}$ is a hard question and some progress have been done in that direction. See [7,8,1].

However, the situation for permutation quadrinomials is different. Let $f(x) = x + a_1 x^{s_1(2^m-1)} + a_2 x^{s_2(2^m-1)} + a_3 x^{s_3(2^m-1)}$. Recently, Tu et al. investigated the case of $(s_1, s_2, s_3) = (-1, 1, 2)$ under some restrictive conditions [16]. In [18] the authors provided more classes of permutation quadrinomials from Niho exponents in characteristic two for $(s_1, s_2, s_3) = (\frac{-1}{2^k-1}, 1, \frac{2^k}{2^k-1})$, $(s_1, s_2, s_3) = (\frac{1}{2^k+1}, 1, \frac{2^k}{2^k+1})$, where m and k are positive integers and $(s_1, s_2, s_3) = (\frac{1}{4}, 1, \frac{3}{4})$. Their work focuses on finding sufficient conditions for the polynomials to be permutation polynomials and it is based on arithmetic over finite fields. Proving whether these conditions are necessary can be challenging. In fact, they also suggested that the conditions given were necessary for m big enough, but they have not found efficient techniques to show those facts.

Very recently the problem of characterizing permutation quadrinomials was also address by Ding and Zieve in [4], where the authors determined a very large class of permutation quadrinomials by using novel geometric techniques (even when the Weil bounds do not provide useful information). In particular they were able to solve two out of the three conjectures presented in [18, Th 1.1 and 1.3].

In this paper, we aim to answer the conjecture left open, that is investigating whether the conditions in [18, Theorem 1.4] are also necessary. We will use the Hasse-Weil type theorems to prove necessary conditions for a polynomial to be a permutation polynomial. In particular we will give a complete answer to the question, see Theorem 2.2.

2. Setting and known results

Let $q = 2^m$ be a prime power and $\mathbb{F}_{q^2}$ be the finite field of q^2 elements. Let $a_1, a_2, a_3 \in \mathbb{F}_{q^2}$ and denote $\theta_1 = 1+a_1^{q+1}+a_2^{q+1}+a_3^{q+1}$, $\theta_2 = a_1^q+a_3a_2^q$, $\theta_3 = a_3+a_2a_1^q$, $\theta_4 = a_1^{q+1}+a_3^{q+1}$ and $\theta_4' = \theta_1 + \theta_4 = 1 + a_2^{q+1}$. Note that

$$\theta_2^{q+1} + \theta_3^{q+1} = \theta_4\theta_4'.$$

For the sake of completeness, we now summarize the main previous result we will use in this paper. See [18] for more details.

Theorem 2.1 *([18, Theorem 1.4]). Let $n = 2m$ be a positive integer. Let $(s_1, s_2, s_3) = (\frac{1}{4}, 1, \frac{3}{4})$ and $a_1, a_2, a_3 \in \mathbb{F}_{q^2}$. Then $f(\mathtt{X}) = \mathtt{X} + a_1\mathtt{X}^{s_1(q-1)+1} + a_2\mathtt{X}^{s_2(q-1)+1} + a_3\mathtt{X}^{s_3(q-1)+1}$ is a PP of $\mathbb{F}_{q^2}$ if either*

$$\theta_4 \neq 0, \quad \theta_2 = 0 \quad \text{and} \quad a_3 \in \mu_{q+1}, \quad a_3 \notin \{x^3 | x \in \mu_{q+1}\} \tag{2.1}$$

or

$$\theta_1 \neq 0, \theta_2 \neq 0, \theta_4 = 0, \theta_3 = \theta_2^{2q-1} \text{ and } x^3 + x + \frac{\theta_1^2}{\theta_2^{q+1}} = 0 \text{ has no solutions over } \mathbb{F}_q. \tag{2.2}$$

The aim of this paper is to answer the question left open by the authors in [18, Theorem 1.4] and prove that conditions (2.1) and (2.2) are also necessary.

The main result is stated in the following theorem.

Theorem 2.2. *Let $m \geq 9$ be an integer and $q = 2^m$. With the notation above, if the polynomial*

$$f(x) = x + a_1 x^{s_1(q-1)+1} + a_2 x^{s_2(q-1)+1} + a_3 x^{s_3(q-1)+1} \tag{2.3}$$

is a PP of $\mathbb{F}_{q^2}$ then

- *if $\theta_2 = 0$ then $\theta_4 \neq 0$, $a_3 \in \mu_{q+1}$, $a_3 \notin \{x^3 | x \in \mu_{q+1}\}$;*
- *if $\theta_2 \neq 0$, then $\theta_4 = 0$, $\theta_1 \neq 0$, $\theta_3 = \theta_2^{2q-1}$ and*

$$x^3 + x + \frac{\theta_1^2}{\theta_2^{q+1}} = 0 \tag{2.4}$$

has no solutions in $\mathbb{F}_q$.

Corollary 2.3. Conditions (2.1) *and* (2.2) *of* Theorem 2.1 *are also necessary.*

3. Algebraic curves and necessary conditions

It is well known that polynomials of the form $f(x) = xh(x^{q-1})$ permute $\mathbb{F}_{q^2}$ if and only if $g(x) = xh(x)^{q-1}$ permutes the set μ_{q+1} of the $(q+1)$-roots of unity in $\mathbb{F}_{q^2}$. See [19, Theorem 1.2]. For $f(x)$ in Equation (2.3) this means to prove that the rational function

$$p(x) = \frac{x^4 + a_1^q x^3 + a_3^q x + a_2^q}{a_2 x^4 + a_3 x^3 + a_1 x + 1}$$

permutes μ_{q+1}, see [18, Section 5] for more details.

Let $\mathcal{C}$ be the plane curve associated to $p(x)$, with equation $F(X,Y) = (p(X) - p(Y))/(X-Y) = 0$, that is

$$\begin{aligned} F(X,Y) =& \frac{\left(a_1 Y + a_2 Y^4 + a_3 Y^3 + 1\right)\left(X^3 a_1{}^q + a_2{}^q + a_3{}^q X + X^4\right)}{X+Y} + \\ &+ \frac{\left(a_1 X + a_2 X^4 + a_3 X^3 + 1\right)\left(Y^3 a_1{}^q + a_2{}^q + Y a_3{}^q + Y^4\right)}{X+Y} = 0, \end{aligned} \tag{3.1}$$

or equivalently

$$\begin{aligned} F(X,Y) =& \theta_3^q + \theta_3 X^3 Y^3 + \theta_4 XY(X+Y) + \theta_4'(X+Y)^3 + \\ &+ \theta_2(XY + (X+Y)^2) + \theta_2^q(X^2Y^2 + XY(X+Y)^2) = 0. \end{aligned} \tag{3.2}$$

$\mathcal{C}$ is a curve defined over $\mathbb{F}_{q^2}$ and $p(x)$ permutes μ_{q+1} if and only if there are no points $(X,Y) \in \mathcal{C} \cap \mu_{q+1}^2$ such that $X \neq Y$. Since understanding whether or not $\mathcal{C}$ has points in the set μ_{q+1} is not always an easy task to do, we will consider also the following idea. Choose an element $e \in \mathbb{F}_{q^2}$ such that $e^q = e+1$. Every $x \in \mu_{q+1}^2$ different from 1 can be written as $x = \frac{X+e}{X+e+1}$, where X runs over $\mathbb{F}_q$. Then $p(x)$ permutes μ_{q+1} if and only if $p(\phi(x))\colon \mathbb{F}_q \cup \{\infty\} \to \mu_{q+1}$, where $\phi(x) = \frac{x+e}{x+e+1}$, $\phi(\infty) = 1$, is a bijection. This is equivalent to ask that $H(x) = p(\phi(x))_{|\mathbb{F}_q}\colon \mathbb{F}_q \to \mu_{q+1} \setminus \{(a_1+a_2+a_3+1)^{q-1}\}$ is a bijection. Let $\mathcal{H}$ be the affine curve defined by $(H(X) - H(Y))/(X-Y) = 0$. It is easily checked that $\mathcal{H}$ is defined over $\mathbb{F}_q$ and therefore $H(x)$ is a bijection if and only if $\mathcal{H}$ has no $\mathbb{F}_q$-rational points off the line $X = Y$.

Moreover, an equation for $\mathcal{H}$ is given by $H(X,Y) = (X+e+1)^3(Y+e+1)^3 F(\phi(X), \phi(Y))$ and $\mathcal{H}$ is $\mathbb{F}_{q^2}$-birationally equivalent to $\mathcal{C}$: let

$$\psi(X,Y) = \Big(\frac{X(e+1)+e}{X+1}, \frac{Y(e+1)+e}{Y+1}\Big),$$

then $(1+X)^3(1+Y)^3 H(\psi(X,Y)) = F(X,Y)$ and the two curves are $\mathbb{F}_{q^2}$-birationally equivalent.

Proposition 3.1. *Let $q \geq 512$. If $f(x) \in \mathbb{F}_{q^2}[x]$ is a PP then $\mathcal{C}$ is not absolutely irreducible over $\mathbb{F}_{q^2}$.*

Proof. If $\mathcal{C}$ is absolutely irreducible over $\mathbb{F}_{q^2}$ then $\mathcal{H}$ is absolutely irreducible over $\mathbb{F}_q$. Since $\mathcal{H}$ has degree at most 6, the Hasse-Weil bound implies that $\mathcal{H}$ has at least an affine rational point (a,b) with $a \neq b$ whenever

$$q + 1 - 20\sqrt{q} - 12 \geq 0, \tag{3.3}$$

where 12 is the maximum number of points belonging either to the line $X = Y$ or to the infinity line. Equation (3.3) is satisfied for every integer greatest than 421. Thus, if

$q = 2^m \geq 512$, $\mathcal{H}$ has an $\mathbb{F}_q$-rational point (a, b), with $a \neq b$. Consequently, we obtain a point $\left(\frac{a+e}{a+e+1}, \frac{b+e}{b+e+1}\right) = (a', b') \in \mu_{q+1}^2$ such that

$$a' \neq b' \quad \text{and} \quad p(a') = p(b'),$$

which is in contrast with $f(x)$ being a PP of $\mathbb{F}_{q^2}$. □

Proposition 3.1 allows us to focus on $\mathcal{C}$ to obtain necessary conditions on $f(x)$. However we will see that proving the absolutely irreducibility of $\mathcal{C}$ is not always possible. Thus, in some cases, we will exhibit explicitly points belonging to $\mathcal{C} \cap \mu_{q+1}^2$, off the line $X+Y=0$.

Understanding whether $\mathcal{C}$ is reducible or not may be difficult. For this reason, one can ask for a transformation that sends $\mathcal{C}$ to a lower degree curve easier to study. In particular, the group $\mathfrak{G}$ generated by $(X, Y) \mapsto (Y, X)$ is a subgroup of $\mathrm{Aut}(\mathcal{C})$, the automorphism group of $\mathcal{C}$. Furthermore, let $u = X+Y$, $v = XY$ and $G(u, v) = F(X, Y)$. Let $\mathcal{D}$ be the curve defined by $G(u, v) = 0$, that is

$$\mathcal{D}\colon \theta_3^q + \theta_4' u^3 + \theta_4 uv + \theta_3 v^3 + \theta_2(u^2 + v) + \theta_2^q v(u^2 + v) = 0, \tag{3.4}$$

which is the quotient curve $\mathcal{C}/\mathfrak{G}$. When convenient, we will study the connection between $\mathcal{C}$ and $\mathcal{D}$ to derive information on the irreducibility of $\mathcal{C}$.

The paper is organized as follows: Sections 4 and 5 are dedicated to the cases $\theta_2 = 0$ and $\theta_4 = 0$ respectively, strongly using the connection between $\mathcal{C}$ and $\mathcal{D}$. Section 6 will be devoted to the case $\theta_2 \neq 0$ and $\theta_4 \neq 0$ and we will focus on the factorization of $\mathcal{H}$ showing that there must always be an absolutely irreducible component defined over $\mathbb{F}_q$ in that case.

4. Case $\theta_2 = 0$

We note that if $\theta_1 = 0$ then $\theta_4 \neq 0$ and $a_3 \in \mu_{q+1}$. In fact since $a_1 = a_3^q a_2$ and $a_1^q = a_2^q a_3$, then

$$\theta_4 = a_1^{q+1} + a_3^{q+1} = a_3^{q+1}(1 + a_2^{q+1}) = a_3^{q+1}\theta_4,$$

and $\theta_3 = a_3\theta_4$ which justifies $\theta_4 \neq 0$ and $a_3 \in \mu_{q+1}$, otherwise f is trivially not a PP (see for example [13, Result 1.2]). When this happens the equation of $\mathcal{D}$ is exactly

$$G(u, v) = a_3^q + u^3 + uv + a_3 v^3.$$

The latter equation needs to be studied also when $\theta_1 \neq 0$, this is why we will see both cases together at the end of this section. See Remark 4.5.

Let $\theta_1 \neq 0$. By the same passages as above, we have

$$\theta_4 = a_3^{q+1}\theta_4', \quad \theta_3 = a_3\theta_4' \quad \text{and} \quad \theta_4' \neq 0.$$

If $\theta_4 = 0$, then $a_3 = 0, a_1 = 0$ and the binomial f in equation (2.3) is not a PP (see for example [13, Result 1.2]).

Therefore $\mathcal{C}$ becomes $F(X, Y) = 0$ with

$$F(X, Y) = a_3^q + a_3 X^3 Y^3 + a_3^{q+1} XY(X + Y) + (X + Y)^3$$

and $\mathcal{D}$ becomes $G(u, v) = 0$ with

$$G(u, v) = a_3^q + u^3 + a_3^{q+1} uv + a_3 v^3.$$

Proposition 4.1. *The curve $\mathcal{D}$ defined by the equation (3.4) is absolutely irreducible if and only if $a_3 \notin \mu_{q+1}$.*

Proof. If $a_3 = 0$ then $G(u, v)$ is not absolutely irreducible. Let $a_3 \neq 0$. Note that every singular point of $\mathcal{D}$ is a double point. In fact, we have $\partial_{uv} G \neq 0$ and $\partial_{vu} G \neq 0$. The system of partial derivatives is

$$\begin{cases} u^2 + a_3^{q+1} v = 0 \\ a_3^q u + v^2 = 0 \end{cases}$$

and it implies that a point $P = (u, v)$ is singular if and only if $P = (a_3^{q+2/3}, a_3^{q+1/3})$ and $P \in \mathcal{D}$ (note that the cubic roots of a_3 are not uniquely determined). More precisely $G(P) = 0$ implies that

$$a_3^q + a_3^{3q+2} = 0$$

which proves that $\mathcal{D}$ is singular if and only if $a_3^{q+1} = 1$. Furthermore, since the equation $v^3 = a_3^{3q+1}$ admits 3 solutions in the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_{q^2}$, we have three double points and the cubic is the union of three non concurrent lines. This means that $\mathcal{D}$ is absolutely irreducible if and only if it is non-singular, namely $a_3 \notin \mu_{q+1}$. □

Remark 4.2. Since $\mathfrak{G}$ is an automorphism group of $\mathcal{C}$, there is only one situation in which $\mathcal{C}$ is reducible whereas $\mathcal{D}$ is not: when $\mathcal{C}$ is the product of two cubics, which form an orbit under $\mathfrak{G}$. In fact, in that case, $\mathcal{D}$ is a cubic curve, which may be irreducible.

Proposition 4.3. *The curve $\mathcal{C}$ is the union of two cubic curves only if $a_3 \in \mu_{q+1}$.*

Proof. Since the action of $\mathfrak{G}$ is exchanging the x with the y, the only possible factorization of $\mathcal{C}$ is

$$\begin{aligned} &(a_{00} + a_{10}X + a_{20}X^2 + a_{30}X^3 + a_{01}Y + a_{11}XY + a_{21}X^2Y + a_{02}Y^2 + a_{12}XY^2 + a_{03}Y^3) \\ &(a_{00} + a_{01}X + a_{02}X^2 + a_{03}X^3 + a_{10}Y + a_{11}XY + a_{12}X^2Y + a_{20}Y^2 + a_{21}XY^2 + a_{30}Y^3) \\ &\quad = 0 \end{aligned} \tag{4.1}$$

Note that the equation of $\mathcal{C}$ is

$$a_3^q + X^3 + (a_3^{q+1} + 1)X^2Y + (a_3^{q+1} + 1)XY^2 + Y^3 + a_3X^3Y^3 = 0.$$

Thus, comparing the coefficients, we see that the only possibility for Equation (4.1) is

$$a_{00}^2 + a_{00}a_{30}X^3 + a_{00}a_{30}Y^3 + a_{30}^2X^3Y^3 = 0.$$

However, this is admissible if and only if $a_3^{q+1} + 1 = 0$, that is $a_3 \in \mu_{q+1}$. □

Corollary 4.4. *Let $a_3 \notin \mu_{q+1}$. The curve $\mathcal{C}$ is absolutely irreducible.*

Proof. Proposition 4.1 implies that for $a_3 \notin \mu_{q+1}$ the curve $\mathcal{D}$ is absolutely irreducible. The proof follows from Remark 4.2 together with Proposition 4.3. □

We consider now the case when $\mathcal{D}$ is not absolutely irreducible. In this case we have

$$G(u, v) = a_3^q + u^3 + uv + a_3v^3,$$

since $a_3 \in \mu_{q+1}$.

Remark 4.5. Note that this is the same equation obtained for $\theta_1 = 0$, hence what follows also applies for $\theta_1 = 0$.

Lemma 4.6. *Let $q = 2^m$ and let a_3 be a cube in μ_{q+1}. Then the equation $x^3 = a_3$ admits exactly 3 solutions over $\mathbb{F}_{q^2}$.*

Proof. From [5, pg. 4] the equation $x^3 = a_3$ has 3 solutions if $3 \mid q^2 - 1$ and $a_3^{\frac{q^2-1}{3}} = 1$. Since $q^2 \equiv 1 \pmod 3$ and $a_3^{\frac{q+1}{3}} = 1$ the claim follows. □

Proposition 4.7. *Let $\mathcal{D}$ be the curve with equation (3.4). Let a_3 be an element of μ_{q+1} and $\mathcal{D}\colon G(u, v) = 0$. Then $G(u, v)$ is irreducible over $\mathbb{F}_{q^2}$ if and only if $a_3 \notin \{x^3 | x \in \mu_{q+1}\}$. Moreover, if $a_3 \in \{x^3 | x \in \mu_{q+1}\}$, then $\mathcal{D}$ is the union of three (absolutely irreducible) linear components over $\mathbb{F}_{q^2}$.*

Proof. From Proposition 4.1 we know that the singular points of $\mathcal{D}$ are $P_i = (a_3^q\alpha_i^2, a_3^q\alpha_i)$, for $i = 1, 2, 3$, where α_i are the solutions in $\overline{\mathbb{F}}_q$ of $x^3 = a_3$. From Lemma 4.6 $\mathcal{D}$ has exactly three singular (double) points defined over $\mathbb{F}_{q^2}$ if and only if a_3 is a cube in μ_{q+1}. Moreover, in that case, $\mathcal{D}$ is the union of three (non-concurrent) lines passing through these points. □

Corollary 4.8. *If a_3 is a cube in μ_{q+1}, then $\mathcal{D}$ decomposes as follows:*

$$\mathcal{D}\colon (u + \alpha_1v + \alpha_1^{-1})(u + \alpha_2v + \alpha_2^{-1})(u + \alpha_3v + \alpha_3^{-1}) = 0.$$

Proof. We just note that $\alpha_1\alpha_2^2 + \alpha_1^2\alpha_2 = a_3$. The claim follows since the line $l_i\colon u + \alpha_i v + \alpha_i^{-1} = 0$ is the one passing through $P_j = (a_3^q\alpha_j^2, a_3^q\alpha_j)$, with $j \neq i$. □

After that, our next goal is to understand what happens when we go back to the curve $\mathcal{C} : F(X,Y) = 0$, with

$$F(X,Y) = a_3^q + a_3X^3Y^3 + XY(X+Y) + (X+Y)^3.$$

Proposition 4.9. *Let a_3 be a cube in μ_{q+1}. Then the curve $\mathcal{C}$ splits into linear (absolutely irreducible) components over $\mathbb{F}_{q^2}$. More precisely,*

$$\mathcal{C}\colon \Pi_{i=1}^3(X + \alpha_i^{-1})(Y + \alpha_i^{-1}) = 0,$$

where $\alpha_i^3 = a_3$ for $i = 1, 2, 3$.

Proof. The proof is a consequence of Corollary 4.8 and $u = X+Y$, $v = XY$. As a matter of fact, the quadric

$$X + Y + \alpha_i XY + \alpha_i^{-1} = 0$$

splits as

$$(X + \alpha_i^{-1})(Y + \alpha_i^{-1}) = 0$$

for every $i = 1, 2, 3$. □

Corollary 4.10. *Let a_3 be a cube in μ_{q+1}. Then the set $\mathcal{C} \cap \mu_{q+1}^2$ is non-empty and f is not a PP of $\mathbb{F}_{q^2}$.*

Proof. The claim follows since a_3 is a cube in μ_{q+1} (and hence $\alpha_i \in \mu_{q+1}$). □

5. $\theta_2 \neq 0$ and $\theta_4 = 0$

Now we suppose that $\theta_2 \neq 0$ and $\theta_4 = 0$. Recall that in this case

$$\theta_2^{q+1} + \theta_3^{q+1} = 0. \tag{5.1}$$

The equation of $\mathcal{C}$ becomes

$$\mathcal{C}\colon \theta_3^q + \theta_3X^3Y^3 + \theta_1(X+Y)^3 + \theta_2(XY + (X+Y)^2) + \theta_2^q(X^2Y^2 + XY(X+Y)^2) = 0, \tag{5.2}$$

while $\mathcal{D}$ has equation

$$\mathcal{D}\colon \theta_3^q + \theta_1u^3 + \theta_3v^3 + \theta_2(u^2 + v) + \theta_2^qv(u^2 + v) = 0.$$

Similarly to the first case, we want to understand the relation between the irreducibility of $\mathcal{D}$ and $\mathcal{C}$.

Proposition 5.1. *$\mathcal{C}$ is absolutely irreducible if and only if $\mathcal{D}$ is absolutely irreducible.*

Proof. As we have already pointed out, the only case to be checked is when $\mathcal{C}$ is the product of two cubics, which belong to the same orbit under $\mathfrak{G}$. The union of two such cubics has equation $F'(X,Y)=0$, where $F'(X,Y)$ is defined as

$$\begin{aligned}&(a_{00}+a_{10}X+a_{20}X^2+a_{30}X^3+a_{01}Y+a_{11}XY+a_{21}X^2Y+a_{02}Y^2+a_{12}XY^2+a_{03}Y^3)\\&(a_{00}+a_{01}X+a_{02}X^2+a_{03}X^3+a_{10}Y+a_{11}XY+a_{12}X^2Y+a_{20}Y^2+a_{21}XY^2+a_{30}Y^3)\\&\quad=0.\end{aligned}\tag{5.3}$$

By straightforward computations, we obtain

$$\begin{cases}\theta_3^q=a_{00}^2\\ \theta_2=a_{01}^2+a_{10}^2\\ a_{00}a_{01}+a_{00}a_{10}=0\end{cases}$$

Since $\theta_3^{q+1}=\theta_2^{q+1}\neq 0$, this implies $a_{00}\neq 0$ and hence $a_{10}=a_{01}$, which contradicts the assumption $\theta_2\neq 0$. □

The next propositions allow us to obtain information about the factorization of $\mathcal{D}$ (and so $\mathcal{C}$).

Proposition 5.2. *Let $\theta_1=0$. The followings hold:*

1. *if $\theta_3=\theta_2^{2q-1}$ then the curve $\mathcal{D}$ splits as*

$$\mathcal{D}\colon (\theta_2+\theta_2^q v)(\theta_2^{1-q}+u^2+\theta_2^{q-1}v^2)=0;$$

2. *if $\theta_3\neq\theta_2^{2q-1}$ then the curve $\mathcal{D}$ has exactly one singular point $P=(0,\alpha)$, where α is the (unique) solution of $\alpha^2=\frac{\theta_2}{\theta_3}$.*

Proof. The equation of $\mathcal{D}$ becomes

$$G(u,v)=u^2v\theta_2^q+v^2\theta_2^q+\theta_3^q+\theta_2u^2+\theta_2v+\theta_3v^3=0$$

and the partial derivatives system is made by the single equation

$$\frac{\partial G}{\partial v}=\theta_2+\theta_2^q u^2+\theta_3v^2=0$$

which implies

$$u^2 = \frac{\theta_3 v^2 + \theta_2}{\theta_2^q}.$$

Going back to the equation of $\mathcal{D}$, we obtain

$$v^2\theta_2^{2q} + \theta_2^q\theta_3^q + \theta_2^2 + \theta_2\theta_3 v^2 = 0. \tag{5.4}$$

Therefore, if $\theta_3 \neq \theta_2^{2q-1}$, equation (5.4), together with equation (5.1), implies

$$v^2 = \frac{\theta_2^{q-1}\theta_3^q + \theta_2}{\theta_2^{2q-1} + \theta_3} = \frac{\theta_2}{\theta_3}$$

which means that $u = 0$ and $\mathcal{D}$ has only one singular double point $P = (0, \alpha)$, where $\alpha^2 = \frac{\theta_2}{\theta_3}$.

On the other hand, if $\theta_3 = \theta_2^{2q-1}$, the equation of $\mathcal{D}$ becomes:

$$v^3\theta_2^{2q-1} + \theta_2^{2-q} + v\theta_2^q\left(u^2 + v\right) + \theta_2\left(u^2 + v\right) = 0 \tag{5.5}$$

Note that the resultant between the equation (5.5) and the derivative with respect to v is 0. This means that they share a common factor. Indeed, we have the following factorization for (5.5):

$$\begin{aligned} v^3\theta_2^{2q-1} + \theta_2^{2-q} + v\theta_2^q\left(u^2 + v\right) + \theta_2\left(u^2 + v\right) = \\ (\theta_2 + \theta_2^q v)(\theta_2^{1-q} + u^2 + \theta_2^{q-1}v^2) = 0 \end{aligned}$$

where the second factor equals $\theta_2^{-q}\frac{\partial G}{\partial v}$. □

Proposition 5.3. *Let $\theta_1 \neq 0$. The curve $\mathcal{D}$ has exactly one singular point $P = (0, \alpha)$, where α is the (unique) solution of $\alpha^2 = \frac{\theta_2}{\theta_3}$.*

Proof. The system of partial derivatives is

$$\begin{cases} \theta_1 u^2 = 0 \\ \theta_2 + \theta_2^q u^2 + \theta_3 v^2 = 0 \end{cases} \tag{5.6}$$

This means that there is only one singular point $P = (0, \alpha)$ where $\alpha^2 = \frac{\theta_2}{\theta_3}$. □

Propositions 5.2 and 5.3 lead us to study what kind of singular point $P = (0, \alpha)$ is. We can treat both cases together. Applying a birational transformation which sends P to the origin, namely

$$\Phi : (u, v) \mapsto (U, V + \alpha),$$

the equation for $\Phi(\mathcal{D})$ is

$$(\theta_2 + \alpha\theta_2^q)U^2 + (\theta_2^q + \alpha\theta_3)V^2 + \theta_1 U^3 + \theta_2^q U^2 V + \theta_3 V^3 = 0. \tag{5.7}$$

Proposition 5.4. *The curve $\mathcal{D}$ is absolutely irreducible if and only if $\theta_3 \neq \theta_2^{2q-1}$.*

Proof. The only case in which $\mathcal{D}$ is absolutely irreducible is when the origin O is an ordinary double point of $\Phi(\mathcal{D})$. However, when $\theta_3 = \theta_2^{2q-1}$ the equation becomes

$$\theta_1 U^3 + \theta_2^q U^2 V + \theta_3 V^3 = 0$$

and O is a triple point. On the other hand, when $\theta_3 \neq \theta_2^{2q-1}$ the equation is

$$(U + V)(V\frac{\theta_2^q + \alpha\theta_3}{\theta_2 + \alpha\theta_2^q} + U) + \theta_1 U^3 + \theta_2^q U^2 V + \theta_3 V^3 = 0$$

and P is an ordinary double point. □

Corollary 5.5. *Let $\theta_2 \neq 0$ and $\theta_4 = 0$. If $\theta_1 = 0$ then $\mathcal{C} \cap \mu_{q+1}^2$ is non-empty and disjoint from the line $X = Y$, whereas if $\theta_1 \neq 0$ and $\theta_2^{2q-1} \neq \theta_3$ then $\mathcal{C}$ is absolutely irreducible over $\mathbb{F}_{q^2}$ (over $\mathbb{F}_q$) if $\theta_2 \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ ($\theta_2 \in \mathbb{F}_q$).*

Proof. The proof is obtained by summing up the previous propositions. More precisely, if $\theta_1 = 0$ and $\theta_2^{2q-1} = \theta_3$, from Proposition 5.2, we have

$$\mathcal{C}\colon (\theta_2 + \theta_2^q XY)(\theta_2^{1-q} + (X + Y)^2 + \theta_2^{q-1} X^2 Y^2) = 0.$$

Let $\alpha \in \mu_{q+1} \setminus \{\frac{1}{\theta_2^{q-1}}\}$, then $(1/(\alpha\theta_2^{q-1}), \alpha) \in \mathcal{C} \cap \mu_{q+1}^2$, off the line $X = Y$. On the other hand, if $\theta_2^{2q-1} \neq \theta_3$, the proof follows from Proposition 5.3 and 5.4. □

We now want to further investigate the remaining case $\theta_3 = \theta_2^{2q-1}$ and $\theta_1 \neq 0$. The equation for $\Phi(\mathcal{D})$ is

$$\theta_1 U^3 + \theta_2^q U^2 V + \theta_2^{-1+2q} V^3 = 0.$$

Let $Z = \frac{V}{U}$ and $z = \theta_2^q Z$. Then every solution of

$$\theta_1 + z + \frac{1}{\theta_2^{q+1}} z^3 = 0$$

gives a linear component of $\Phi(\mathcal{D})$.

Lemma 5.6. *Let $\theta_1, \theta_2 \neq 0$ and z_1, z_2, z_3 be the solutions of*

$$\theta_1 + z + \frac{1}{\theta_2^{q+1}} z^3 = 0 \tag{5.8}$$

in the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_{q^2}$. Only one of the following conditions holds.

- *$z_i \in \mathbb{F}_q$ for $i = 1, 2, 3$.*
- *There exists j such that $z_j \in \mathbb{F}_q$ and $z_i \in \mathbb{F}_{q^2}$ for $i \neq j$.*
- *$z_i \notin \mathbb{F}_{q^2}$ for $i = 1, 2, 3$.*

Proof. Note that the coefficients of Equation (5.8) are in $\mathbb{F}_q$. The claim is obtained by standard theory, see for example [5, Pg. 20]. □

Proposition 5.7. *Let $\theta_3 = \theta_2^{2q-1}$. If $\theta_1 + z + \frac{1}{\theta_2^{q+1}} z^3 = 0$ has at least one solution in $\mathbb{F}_q$ then the curve $\mathcal{C}$ splits as the union of three absolutely irreducible conics defined over $\mathbb{F}_{q^2}$ (over $\mathbb{F}_q$) if $\theta_2 \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ ($\theta_2 \in \mathbb{F}_q$). In particular, $\mathcal{C} \cap \mu_{q+1}^2$ is a non-empty set disjoint from the line $X = Y$.*

Proof. Every solution of Equation (5.8) in $\mathbb{F}_{q^2}$ gives a linear component of $\Phi(\mathcal{D})$ (and $\mathcal{D}$). From Lemma 5.6, without loss of generality, we can suppose that $z_1 \in \mathbb{F}_q$ and $z_2, z_3 \in \mathbb{F}_{q^2}$ are the solutions of Equation (5.8). Going back to the curve $\mathcal{D}$ we obtain the following decomposition:

$$\mathcal{D}\colon (z_1 u + \theta_2^q v + \theta_2^q \alpha)(z_2 u + \theta_2^q v + \theta_2^q \alpha)(z_3 u + \theta_2^q v + \theta_2^q \alpha) = 0$$

This means that the equation of the curve $\mathcal{C}$ becomes

$$\mathcal{C}\colon (z_1(X+Y) + \theta_2^q XY + \theta_2)(z_2(X+Y) + \theta_2^q XY + \theta_2)(z_3(X+Y) + \theta_2^q XY + \theta_2) = 0$$

In fact $\alpha^2 = \frac{\theta_2}{\theta_2^{2q-1}}$ implies $\alpha\theta_2^q = \frac{\theta_2^q}{\theta_2^{q-1}} = \theta_2$. We now claim that the above conics are absolutely irreducible over $\mathbb{F}_{q^2}$. A conic is absolutely irreducible if and only if it does not have a singular point. Consider the conic corresponding to z_1, the partial derivatives system is

$$\begin{cases} \theta_2^q Y + z_1 = 0 \\ \theta_2^q X + z_1 = 0 \end{cases}$$

which means that a singular point has coordinate $X = Y = \frac{z_1}{\theta_2^q}$. Such a point belongs to $\mathcal{C}$ if and only if

$$z_1^2 + \theta_2^{q+1} = 0.$$

However, if $z_1^2 = \theta_2^{q+1}$, from equation (5.8) we obtain

$$\theta_1 + z_1 + z_1 = \theta_1 = 0$$

and this is in contrast with $\theta_1 \neq 0$. Similarly, it can be proven that also the other conics are absolutely irreducible. Finally, let $\alpha \in \mu_{q+1} \setminus \{\frac{1}{\theta_2^{q-1}}\}$, then the point $(\frac{\theta_2 + z_1\alpha}{\theta_2^q\alpha + z_1}, \alpha) \in \mathcal{C} \cap \mu_{q+1}^2$, off the line $X = Y$. □

Corollary 5.8. *Let $\theta_2 \neq 0$ and $\theta_4 = 0$. If either $\theta_1 = 0$ or $\theta_3 \neq \theta_2^{2q-1}$ or $\theta_1 + z + \frac{1}{\theta_2^{q+1}} z^3 = 0$ has solutions z defined over $\mathbb{F}_q$, then f is not a PP of $\mathbb{F}_{q^2}$.*

6. $\theta_2 \neq 0$ and $\theta_4 \neq 0$

We just need to prove that in this case the polynomial $f(\mathrm{X})$ is never a PP. We will do that again by using the connection between permutation polynomials and algebraic curves. This part is inspired by the work done in [1]. In Section 3 we showed that the polynomial $f(x)$ in Theorem 2.2 is a PP if and only if $\mathcal{H}$ has no $\mathbb{F}_q$-rational points off the line $X = Y$. In our case the curve $\mathcal{H}$ has degree at most 6. By Proposition 3.1, for q large enough such a curve has no $\mathbb{F}_q$-rational points off the line $X = Y$ if only if it splits into absolutely irreducible components not defined over $\mathbb{F}_q$ which have no $\mathbb{F}_q$-rational points off the line $X = Y$. We will show that for $\theta_2 \neq 0$ and $\theta_4 \neq 0$ this is never the case.

For this last section, our method requires a computer to assist us in computing resultants between polynomials and in factorizing polynomials of low degrees over small fields. The elementary MAGMA [3] programs used for our purposes are presented in the Appendix. However, we point out that our results are valid for general q's of type 2^m, and do not rely on computer searches.

Let $k \in \mathbb{F}_q$ be an element of absolute trace (over $\mathbb{F}_2$) equal to 1. Then we can choose $i \in \mathbb{F}_{q^2}$ such that $i^2 = i + k$ and in particular $i^q = i + 1$.

Let $\theta_2 = C + iD$, $\theta_3 = E + iF$, for $C, D, E, F \in \mathbb{F}_q$. By direct computations the curve $\mathcal{H}$ has equation $L(X, Y) = 0$, for:

$$\begin{aligned} L(X,Y) =& \gamma_{3,3}X^3Y^3 + \gamma_{3,2}X^3Y^2 + \gamma_{2,3}X^2Y^3 + \gamma_{3,1}X^3Y + \gamma_{1,3}XY^3 + \gamma_{3,0}X^3 + \gamma_{0,3}Y^3 \\ &+ \gamma_{2,2}X^2Y^2 + \gamma_{2,1}X^2Y + \gamma_{1,2}XY^2 + \gamma_{2,0}X^2 + \gamma_{1,1}XY + \gamma_{0,2}Y^2 + \gamma_{1,0}X + \gamma_{0,1}Y + \gamma_{0,0}, \end{aligned} \tag{6.1}$$

with

$$\begin{aligned} \gamma_{3,3} &= D + F, \\ \gamma_{3,2} &= C + D + E + F + \theta_4, \\ \gamma_{3,1} &= C + Dk + D + E + Fk + F + \theta_4, \\ \gamma_{3,0} &= Ck + C + Ek + E + F + k\theta_4 + \theta_4 + \theta_1, \\ \gamma_{2,3} &= C + D + E + F + \theta_4, \end{aligned}$$

$$\gamma_{1,3} = C + Dk + D + E + Fk + F + \theta_4,$$
$$\gamma_{0,3} = Ck + C + Ek + E + F + k\theta_4 + \theta_4 + \theta_1,$$
$$\gamma_{2,2} = C + Dk + D + E + Fk + F,$$
$$\gamma_{2,1} = Ck + C + Ek + E + F + k\theta_4 + \theta_1,$$
$$\gamma_{1,2} = Ck + C + Ek + E + F + k\theta_4 + \theta_1,$$
$$\gamma_{2,0} = C + Dk^2 + Dk + E + Fk^2 + Fk + F + k\theta_4,$$
$$\gamma_{0,2} = C + Dk^2 + Dk + E + Fk^2 + Fk + F + k\theta_4,$$
$$\gamma_{1,1} = C + Dk^2 + Dk + E + Fk^2 + Fk + F,$$
$$\gamma_{1,0} = Ck^2 + Ck + Dk^2 + Ek^2 + Ek + E + Fk^2 + F + k^2\theta_4,$$
$$\gamma_{0,1} = Ck^2 + Ck + Dk^2 + Fk^2 + F + k^2\theta_4 + Ek^2 + Ek + E,$$
$$\gamma_{0,0} = Ck^2 + Dk^3 + Fk^3 + Fk + F + Ek^2 + E.$$

In the following we will show that if $\theta_4 \neq 0$ and $\theta_2 \neq 0$ then $\mathcal{H}$ never splits into components none of them is defined over $\mathbb{F}_q$.

6.1. Case $\gamma_{3,3} \neq 0$

In this case $\mathcal{H}$ has degree 6. We observe that the morphism $(x, y) \mapsto (y, x)$ fixes $\mathcal{H}$ and therefore it acts on its components. Also, since $\mathcal{H}$ is defined over $\mathbb{F}_q$, then the Frobenius $\phi_q(x) = x^q$ acts on its components either. This implies that if there is a line as a component, then there must be 6 lines. If not, $\mathcal{H}$ splits as either 3 absolutely irreducible conics or 2 absolutely irreducible cubics.

1. $\mathcal{H}$ splits into 6 lines. In this case the factorization of $L(X, Y)$ in Equation (6.1) must be

$$(D + F)(X + a)(X + b)(X + c)(Y + a)(Y + b)(Y + c) \tag{6.2}$$

for some a, b, c in $\overline{\mathbb{F}}_q$, since the homogeneous part of degree 6 is $(D + F)x^3y^3$. Now we get

$$C + Dk + Dab + Dac + Dbc + D + E + Fk + Fab + Fac + Fbc + F + \theta_4 = 0$$
$$C + Da + Db + Dc + D + E + Fa + F\ b + Fc + F + \theta_4 = 0$$

which implies $k + ab + ac + a + bc + b + c = 0$ since $D + F \neq 0$. Last condition implies:

$$Ca^2 + Cb^2 + C + Dk^2 + Dka^2 + Dkb^2 + Dk + Da^4 + Da^2b^2 + Da^2 + Db^4 + Db^2 + D +$$
$$Ea^2 + Eb^2 + E + Fk^2 + Fka^2 + Fkb^2 + Fk + Fa^4 + Fa^2b^2 + Fa^2 + Fb^4 + Fb^2 + F = 0$$

$$Ca^2 + Cb^2 + C + Dk^2 + Dka^2 + Dkb^2 + Dk + Da^4 + Da^2b^2 + Db^4 + Ea^2 + Eb^2 + E +$$
$$Fk^2 + Fka^2 + Fkb^2 + Fk + Fa^4 + Fa^2b^2 + Fa^2 + Fb^4 + Fb^2 + F = 0$$

which implies in particular: $Da^2 + Db^2 + D = 0$. Now let $D \neq 0$. Then $a^2 + b^2 + 1 = 0$, which implies $k = b^2 + b + 1$ and $a = b + 1$. Thus, substituting in the equation (6.2) the values $a = b + 1$ and computing the resultant for $k = b^2 + b + 1$, we get the following equations

$$C + Db^2 + Db + Dc^2 + D + E + Fb^2 + Fb + Fc^2 + F = 0,$$
$$C + Db^2 + Db + Dc^2 + E + Fb^2 + Fb + Fc^2 + F = 0,$$

which implies $D = 0$ a contradiction.
On the other hand, if $D = 0$, we obtain

$$C + E + Fa + Fb + Fc + F + \theta_4 = 0$$
$$C + E + Fk + Fab + Fac + Fbc + F + \theta_4 = 0$$

which implies:

$$k + ab + ac + a + bc + b + c = 0.$$

Substituting k we get

$$C + E + Fa + Fb + Fc + F + \theta_4 = 0,$$

and by eliminating E we obtain

$$Fa^2 + Fab + Fac + Fb^2 + Fbc + Fc^2 + \theta_4 + \theta_1 = 0,$$
$$Fa^2 + Fab + Fac + Fb^2 + Fbc + Fc^2 + \theta_4 = 0$$

which implies $\theta_1 = 0$. The details of the latter computations can be found in the Appendix A.1, case $D = 0$. By definition we know that $\theta_2^{q+1} + \theta_3^{q+1} = \theta_4(\theta_4 + \theta_1)$. Since $D = 0$ and $\theta_1 = 0$, the latter becomes $C^2 + E^2 + EF + F^2k + \theta_4^2 = 0$. By direct computations we get

$$E + Fk + Fa^2 + Fb^2 + Fc^2 + F = 0,$$

which implies $C = 0$ or $F = 0$. In both cases we have a contradiction.

2. $\mathcal{H}$ splits into 3 absolutely irreducible conics. This case is only possible when the three conics belong to the same orbit under the Frobenius ϕ_q. More precisely, the equations of the curve must be of the form

$$(D + F)(XY + a(X + Y) + b)(XY + a^q(X + Y) + b^q)(XY + a^{q^2}(X + Y) + b^{q^2}) = 0$$

for $a, b \in \mathbb{F}_{q^3}$. First we suppose that both a, $b \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$. In this case, $\{1, a, a^2\}$ and $\{1, b, b^2\}$ are linearly independent over $\mathbb{F}_q$. Also, we know that $a^3 = c_1 a + c_2$ and $b^3 = d_1 b + d_2$, for some $c_1, c_2, d_1, d_2 \in \mathbb{F}_q$. First, we derive y from the equation of the first conic and then we plug it in the equation of our curve. After that, we isolate the coefficients of a and a^2. By direct computations we obtain:

$$C + D + E + F + \theta_4 = 0, \text{ or } \theta_4 = 0$$

which implies $C + D + E + F + \theta_4 = 0$. It follows $k = c_1$ and

$$DE + DF + Dc_2\theta_4 + D\theta_4 + EF + F^2 + Fc_2\theta_4 + F\theta_4 + \theta_4^2 = 0 \tag{6.3}$$

Repeating for b we obtain

$$\begin{aligned} &Dk + Fk + \theta_4 = 0 \\ &D^2 + DF + D^2 d_1 + F^2 d_1 + \theta_4^2 = 0 \\ &D^2 d_2 + DE + DF + EF + F^2 d_2 + F^2 + F\theta_4 + \theta_4^2 = 0 \end{aligned} \tag{6.4}$$

The first two equations in (6.4) imply that $Da^2b + D + Fa^2b + a\theta_4 + b\theta_4 = 0$. From the latter equation together with the third equation in (6.4) and Equation (6.3) we derive that either $Da + E + F + \theta_4 = 0$ or $(DE + DF + D\theta_4 + EF + F^2 + F\theta_4)a + D\theta_4 = 0$, which leads to $D = 0$ and one of the following: either $a = 0$ or $E + F + \theta_4 = 0$ or $F = 0$. However, since $D = 0$ and $D + C + E + F + \theta_4 = 0$, the latter two conditions are both non-admissible (we would have either $D + F = 0$ or $\theta_2 = 0$). Hence $a = 0$, a contradiction. When either $a \in \mathbb{F}_q$ or $b \in \mathbb{F}_q$ we derive easily a contradiction by direct checking (see the Appendix for all the computations).

3. $\mathcal{H}$ splits into 2 absolutely irreducible cubics defined over $\mathbb{F}_{q^2}$. The leading homogeneous part of $L(X, Y)$ is $(D + F)X^3Y^3$, so the homogeneous part of the cubics is either X^3, Y^3 or X^2Y, XY^2. Since the Frobenius ϕ_q switches the two cubics, this implies that they must be defined over $\mathbb{F}_q$.

6.2. Case $\gamma_{3,3} = 0$

If $\theta_4 \neq C + E$, $\mathcal{H}$ has degree 5. In this case we note that the line $X + Y = 0$ cannot be a component of $\mathcal{H}$. In fact, by direct computations, $X = Y$ implies $C + E = F = 0$ and $E = 0$ which in particular means $\theta_2 = 0$. Now, since the leading homogeneous part is $(C + E + \theta_4)(X^3Y^2 + X^2Y^3)$, the point $P = (1 : 1 : 0)$ is a simple $\mathbb{F}_q$-rational point. Then there must be an absolutely irreducible component through P distinct from the line $X + Y = 0$.

Let $\theta_4 = C + E$. Note that $\theta_2^{q+1} + \theta_3^{q+1} = \theta_4(\theta_1 + \theta_4)$, we obtain

$$CD + C\theta_1 + D^2k + EF + E\theta_1 + F^2k = 0,$$

and, since $D + F = 0$,

$$F + \theta_1 = 0 \text{ or } C + E = 0$$

which implies $F = \theta_1$. In this case the homogeneous part of $L(x, y)$ is $(C + E)x^2y^2$.

Since now the degree of $\mathcal{H}$ is 4 we need to deal only with two cases: 4 lines or 2 absolutely irreducible conics.

1. $\mathcal{H}$ splits as the union of 4 lines. The factorization of $L(x, y)$ must be

$$(C + E)(X + a)(X + b)(Y + a)(Y + b) = 0 \tag{6.5}$$

for some $a, b \in \overline{\mathbb{F}}_q$. Then

$$a + b + 1 = 0$$

which implies $F = 0$. It follows that

$$k + b^2 + b + 1 = 0$$

which leads to $C = 0$. But this is a contradiction since $C = D = 0$ implies $\theta_2 = 0$.

2. $\mathcal{H}$ splits as the union of two absolutely irreducible conics. Since those conics are switched by ϕ_q, we have only two possibilities, according whether they are switched by $(x, y) \mapsto (y, x)$ or not, that is either

$$XY + (a+ib)X + (a+(i+1)b)Y + c = 0, \text{ and } XY + (a+(i+1)b)X + (a+ib)Y + c = 0,$$

for some $a, b, c \in \mathbb{F}_q$, or

$$X(a + bi) + Y(a + bi) + c + di + XY = 0, \text{ and}$$
$$X(a + b(i + 1)) + Y(a + b(i + 1)) + c + d(i + 1) + XY = 0,$$

for some $a, b, c, d \in \mathbb{F}_q$.
In the first case we get $b + 1 = 0$ which leads to $F = 0$ and then $a^2 + a + 1 = 0$. It follows

$$Ck + Cc + Ek + Ec + E = 0$$

which implies either $C = 0$ or $E = 0$. Since $C = 0$ is again a contradiction this means that $E = 0$ and $c = k$. However when $F = \theta_1 = D = E = 0$, the equation of our curve $\mathcal{C}$ (see Equations (3.1) and (3.2)) becomes

$$C(X + 1)(Y + 1)(X^2 + XY + Y^2) = 0,$$

for $\theta_2 = \theta_4 = C$, which has points $(X, Y) \in \mu_{q+1}^2$ off the line $X = Y$.
In the second case, by direct computation, we obtain $b = 1$ and after substituting,

$$Cd + C + Ed + E + F = 0,$$

which implies

$$Ck + Ca + Cc + Ek + Ea + Ec + E + Fa + F = 0.$$

Again, by direct computation, one finds

$$Ca^2 + Ca + C + Ea^2 + Ea + E + F = 0.$$

Now we distinguish two cases. If $F \neq 0$, then

$$k = (C^3 - C^2F - CF^2 - F^3 - C^2E - CFE - F^2E)/(F^2(C + E)),$$

and by replacing k in the equation of our curve $\mathcal{H}$, we obtain the following factorization of $L(X, Y)$:

$$(FX + C)(FY + C)L'(X, Y),$$

(for the equation of $L'(X, Y)$ see the Appendix) which leads to a contradiction, for the conics being irreducible. If $F = 0$, by direct computations, we obtain $b = 1$, $d = 1$, $a^2 + a + 1 = 0$ and

$$Ck^2 + Ck + Cc^2 + Cc + Ek^2 + Ek + Ec^2 + Ec + E = 0,$$

which implies $C = 0$, a contradiction again since $\theta_2 \neq 0$.

7. Proof of main Theorem 2.2

If $\theta_2 = 0$, the proof is obtained by Corollary 4.4 and Corollary 4.10. When $\theta_2 \neq 0$ and $\theta_4 = 0$, the proof follows from Corollary 5.8, since the equation

$$\theta_1 + z + \frac{1}{\theta_2^{q+1}} z^3 = 0$$

is equivalent to the equation (2.4) after substituting $z = \theta_2^{q+1} x$. When $\theta_2 \neq 0$ and $\theta_4 \neq 0$, the proof is obtained in Section 6.

Data availability

No data was used for the research described in the article.

Acknowledgment

This work was supported by the National Science Foundation under Grant N° 2127742.

Appendix A

In [1], the author provided a very useful mini-program to compute resultant of polynomials over finite fields. In what follows we will use the same Magma procedure to investigate the solutions of a system of polynomial equations. For the sake of completeness, we now recall the main functions we use in this paper "FindCoefficients2" and "Substitution". See [1, Appendix] for more details.

```
K<x,y,C,D,E,F,i,j,m,k,a,b,c,d,e,f,g,t4,t1,aq,bq,aq2,bq2> := PolynomialRing(GF(2),23);

FindCoefficients2 := function(pol,var1,var2)
T := Terms(pol);
Coeff := {};
MAX1 := Degree(pol,var1);
MAX2 := Degree(pol,var2);
for i in [0..MAX1] do
for j in [0..MAX2] do
c := K!0;
for t in T do
if IsDivisibleBy(t,var1^i*var2^j) eq true and
IsDivisibleBy(t,var1^i*var2^(j+1)) eq false  and
IsDivisibleBy(t,var1^(i+1)*var2^j) eq false  then
c := c+ K! (t/(var1^i*var2^j));
end if;
end for;
if c ne 0 then
Coeff := Coeff join {c};
i,j,c;
end if;
end for;
end for;
return Coeff;
end function;

Substitution := function (pol, m, p)
e := 0;
New := K! pol;
while e eq 0 do
N := K!0;
T := Terms(New);
i:= 0;
for t in T do
if IsDivisibleBy(t,m) eq true then
Q := K! (t/m);
i := 1;
N := K!(N + Q* p);
else
N := K!(N + t);
end if;
end for;
```

```
if i eq 0 then
return New;
else
New := K!N;
end if;
end while;
end function;

t2:=C+i*D;
t2q:=C+(i+1)*D;
t3:=E+i*F;
t3q:=E+(i+1)*F;
eq1:=Substitution(t2*t2q+t3*t3q+t4*(t4+t1),i^2,i+k);
X:=(x+i)/(x+i+1);
Y:=(y+i)/(y+i+1);
Gxy:=t3q + t3*X^3*Y^3 +
t4*X*Y*(X + Y) +
(t1 + t4)*(X + Y)^3 +
t2*(X*Y + (X + Y)^2) +
t2q*X*Y*(X*Y + (X + Y)^2);
Curve:=(x+i+1)^3*(y+i+1)^3*Gxy;
Curve:=Substitution(Curve,i^2,i+k);
```

A.1. $\gamma_{3,3} \neq 0$

$\mathcal{H}$ splits as 6 lines.

Case $D \neq 0$.

```
PROD := (x+a)*(x+b)*(x+c)*(y+a)*(y+b)*(y+c);
CC := FindCoefficients2(Curve+ (D+F)*PROD,x,y);
{Factorization(pol) : pol in CC | pol ne 0};
///C + D*a + D*b + D*c + D + E + F*a + F*b + F*c + F + t4+C + D*k + D*a*b + D*a*c + D*b*c + D + E +
   F*k + F*a*b + F*a*c + F*b*c + F + t4=0
/// C + D*k + D*a*b + D*a*c + D*b*c + D + E + F*k + F*a*b + F*a*c + F*b*c + F + t4=0
p2 := k+ a*b + a*c + a + b*c + b + c;
CC2 := {Resultant(pol,p2,c) : pol in CC};
{Factorization(pol) : pol in CC2 | pol ne 0};
///D*a^2 + D*b^2 + D=0
p3:=a + b + 1;
CC3 := {Resultant(pol,p3,a) : pol in CC2};
{Factorization(pol) : pol in CC3 | pol ne 0};
///k=b^2+b+1
PROD := (x+b+1)*(x+b)*(x+c)*(y+b+1)*(y+b)*(y+c);
CC := FindCoefficients2(Curve+ (D+F)*PROD,x,y);
CC := {Resultant(pol,k+b^2+b+1,k) : pol in CC};
{Factorization(pol) : pol in CC | pol ne 0};
///D=0 ###
```

Case $D = 0$.

```
PROD := (x+a)*(x+b)*(x+c)*(y+a)*(y+b)*(y+c);
CC := FindCoefficients2(Curve+ (D+F)*PROD,x,y);
CC:={Resultant(pol,D,D) : pol in CC};
{Factorization(pol) : pol in CC | pol ne 0};
p2 := k + a*b + a*c + a + b*c + b + c;
CC2 := {Resultant(pol,p2,k) : pol in CC};
{Factorization(pol) : pol in CC2 | pol ne 0};
```

```
p3:=C + E + F*a + F*b + F*c + F + t4;
CC3 := {Resultant(pol,p3,E) : pol in CC2};
{Factorization(pol) : pol in CC3 | pol ne 0};
///t1=0
eq1_2:=Substitution(eq1,t1,0);
eq1_2:=Substitution(eq1_2,D,0);
CC := FindCoefficients2(Curve+ (D+F)*PROD,x,y);
CC:={Resultant(pol,D,D) : pol in CC};
CC:={Resultant(pol,t1,t1) : pol in CC};
p1:=eq1;
CC1:={Resultant(pol,p1,C) : pol in CC};
{Factorization(pol) : pol in CC1 | pol ne 0};
p2 :=E + F*k + F*a^2 + F*b^2 + F*c^2 + F;
CC2 := {Resultant(pol,p2,a) : pol in CC};
{Factorization(pol) : pol in CC2 | pol ne 0};
/// C=0 or F=0 ###
```

$\mathcal{H}$ splits as 3 absolutely irreducible conics. Case $\alpha, \beta \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$.

```
Curve1:=K!((x+a)^3*Evaluate(Curve, [x,(b+a*x)/(x+(a)),C,D,E,F,i,j,m,k,
a,b,c,d,e,f,g,t4,t1,aq,bq,aq2,bq2]));
CC := FindCoefficients2(Curve1,x,y);
CC:={Resultant(pol,eq1,t1) : pol in CC};
CC:={Substitution(pol,a^3,m*a+g) : pol in CC};
CC:={Substitution(pol,b^3,i*b+j) : pol in CC};
{Factorization(pol) : pol in CC | pol ne 0};
pa1:=C^2 + C*D + C*k*t4 + C*a^2*t4 + C*a*t4 + C*t4 + D^2*k + D*m*a*t4 + D*k*a*t4 +
D*a^2*t4 + D*a*t4 + D*g*t4 + E^2 + E*F + E*k*t4 + E*a^2*t4 + E*a*t4 + E*t4 +
F^2*k + F*m*a*t4 + F*k*a*t4 + F*a^2*t4 +  F*a*t4 + F*g*t4 + F*t4 + k*t4^2 + a^2*t4^2 + a*t4^2;
Coefficients(pa1,a);
p1:=C + D + E + F + t4;
CC1:={Resultant(pol,p1,C) : pol in CC};
{Factorization(pol) : pol in CC1 | pol ne 0};
pa2:=D*k + E + F*k + F + m*a*t4 + k*a*t4 + k*t4 + g*t4;
Coefficients(pa2,a);
p2:=k +m;
CC2 := {Resultant(pol,p2,m) : pol in CC1};
{Factorization(pol) : pol in CC2 | pol ne 0};
pb1:=D*i*b + D*j + D*k^3 + D*k^2*b + D*k^2 + D*k*b^2 + D*k*b + D*b + E + F*i*b + F*j +
F*k^3 + F*k^2*b + F*k^2 + F*k*b^2 + F*k*b + F*k + F + k^2*t4 + b^2*t4 + b*t4;
Coefficients(pb1,b);
p3:= D*k + F*k + t4;
CC3:={Resultant(pol,p3,k) : pol in CC2};
{Factorization(pol) : pol in CC3 | pol ne 0};
pb2:=D^2*i*b + D^2*j + D^2*b + D*E + D*F*b + D*F + E*F + F^2*i*b +
F^2*j + F^2 + F*t4 + b*t4^2 + t4^2;
Coefficients(pb2,b);
p4:= D^2 + D*F + D^2*i + F^2*i + t4^2;
CC4:={Resultant(pol,p4,i) : pol in CC3};
{Factorization(pol) : pol in CC4 | pol ne 0};
p5:=D*a^2*b + D + F*a^2*b + a*t4 + b*t4;
CC5:={Resultant(pol,p5,b) : pol in CC4};
{Factorization(pol) : pol in CC5 | pol ne 0};
CC6:={Substitution(pol,a^3,k*a+g) : pol in CC5};
CC6:={Resultant(pol,D*k+ F*k + t4,k) : pol in CC6};
{Factorization(pol) : pol in CC6 | pol ne 0};
p7:=D*E + D*F + D*g*t4 + D*t4 + E*F + F^2 + F*g*t4 + F*t4 + t4^2;
CC7:={Resultant(pol,p7,g) : pol in CC6};
{Factorization(pol) : pol in CC7 | pol ne 0};
p8:=D^2*j + D*E + D*F + E*F + F^2*j + F^2 + F*t4 + t4^2;
CC8:={Resultant(pol,p8,j) : pol in CC7};
{Factorization(pol) : pol in CC8 | pol ne 0};
p9:=D;
```

```
CC9:={Resultant(pol,p9,D) : pol in CC8};
{Factorization(pol) : pol in CC9 | pol ne 0};
///a=0 ###
```

Case $\alpha \in \mathbb{F}_q$ or $\beta \in \mathbb{F}_q$.

```
PROD1:= (x*y+a*(x+y)+b)*(x*y+a*(x+y)+bq)*(x*y+a*(x+y)+bq2);
PROD2:= (x*y+a*(x+y)+b)*(x*y+aq*(x+y)+b)*(x*y+aq2*(x+y)+b);
CC := FindCoefficients2(Curve+(D+F)*PROD1,x,y);
CC:={Resultant(pol,eq1,t1) : pol in CC};
{Factorization(pol) : pol in CC | pol ne 0};
/// t4=0 (by sum of the two equations starting by C^2+CD+..) ###
CC := FindCoefficients2(Curve+(D+F)*PROD2,x,y);
CC:={Resultant(pol,eq1,t1) : pol in CC};
{Factorization(pol) : pol in CC | pol ne 0};
/// t4=0 (by sum of the two equations starting by C^2+CD+..) ###
```

A.2. $\gamma_{3,3} = 0$

In this case we recall that $D + F = 0$ and $\theta_4 = C + E$, implying $\theta_1 = F$.

```
Curve2:=Substitution(Curve,D,F);
Curve2:=Substitution(Curve2,t4,C+E);
Curve2:=Substitution(Curve2,t1,F);
```

$\mathcal{H}$ splits as 4 lines.

```
PROD := (x+a)*(x+b)*(y+a)*(y+b);
CC := FindCoefficients2(Curve2+ (C+E)*PROD,x,y);
{Factorization(pol) : pol in CC | pol ne 0};
p2 := a + b + 1;
CC2 := {Resultant(pol,p2,a) : pol in CC};
{Factorization(pol) : pol in CC2 | pol ne 0};
p3:=F;
CC3 := {Resultant(pol,p3,F) : pol in CC2};
{Factorization(pol) : pol in CC3 | pol ne 0};
p4:=k + b^2 + b + 1;
CC4 := {Resultant(pol,p4,k) : pol in CC3};
{Factorization(pol) : pol in CC4 | pol ne 0};
/// C=0 ###
```

$\mathcal{H}$ splits as the union of two absolutely irreducible conics.

Case 1: $(x, y) \mapsto (y, x)$ switches the two conics.

```
PROD := (x*y+(a+i*b)*x+(a+(i+1)*b)*y+c)*(x*y+(a+(i+1)*b)*x+(a+i*b)*y+c);
PROD := Substitution(PROD,i^2,i+k);
CC := FindCoefficients2(Curve2+(C+E)*PROD,x,y);
{Factorization(pol) : pol in CC | pol ne 0};
p2 :=  b + 1;
CC2 := {Resultant(pol,p2,b) : pol in CC};
{Factorization(pol) : pol in CC2 | pol ne 0};
p3:=F;
CC3 := {Resultant(pol,p3,F) : pol in CC2};
{Factorization(pol) : pol in CC3 | pol ne 0};
p4:=a^2+a+1;
CC4 := {Resultant(pol,p4,a) : pol in CC3};
```

```
{Factorization(pol) : pol in CC4 | pol ne 0};
p5:=C*k + C*c + E*k + E*c + E;
CC5:={Resultant(pol,p5,k) : pol in CC4};
{Factorization(pol) : pol in CC5 | pol ne 0};
/// E=0 ###
```

Case 2: $(x, y) \mapsto (y, x)$ fixes the two conics.

Case $F \neq 0$.

```
PROD := (x*y+(a+i*b)*x+(a+i*b)*y+(c+i*d))*(x*y+(a+(i+1)*b)*x+(a+(i+1)*b)*y+(c+(i+1)*d));
PROD := Substitution(PROD,i^2,i+k);
CC := FindCoefficients2(Curve2+(C+E)*PROD,x,y);
{Factorization(pol) : pol in CC | pol ne 0};
p2 :=  b + 1;
CC2 := {Resultant(pol,p2,b) : pol in CC};
{Factorization(pol) : pol in CC2 | pol ne 0};
p3:=C*d + C + E*d + E + F;
CC3 := {Resultant(pol,p3,d) : pol in CC2};
{Factorization(pol) : pol in CC3 | pol ne 0};
p4:=C*k + C*a + C*c + E*k + E*a + E*c + E + F*a + F;
CC4 := {Resultant(pol,p4,c) : pol in CC3};
{Factorization(pol) : pol in CC4 | pol ne 0};
p5:=C*a^2 + C*a + C + E*a^2 + E*a + E + F;
CC5:={Resultant(pol,p5,a) : pol in CC4};
{Factorization(pol) : pol in CC5 | pol ne 0};
/// k:=-(C^3 - C^2*F - C*F^2 - F^3 -  C^2*E - C*F*E - F^2*E)/(F^2*(C + E));
Factorization(K!(F^4*Evaluate(Curve2,
[x,y,C,D,E,F,i,j,m,(C^3 + C^2*F + C*F^2 + F^3 +  C^2*E + C*F*E + F^2*E)/(F^2*(C + E)),
a,b,c,d,e,f,g,t4,t1,aq,bq,aq2,bq2])));
```

Case $F = 0$

```
Curve3:=Substitution(Curve2,F,0);
PROD := (x*y+(a+i*b)*x+(a+i*b)*y+(c+i*d))*(x*y+(a+(i+1)*b)*x+(a+(i+1)*b)*y+(c+(i+1)*d));
PROD := Substitution(PROD,i^2,i+k);
CC := FindCoefficients2(Curve3+(C+E)*PROD,x,y);
{Factorization(pol) : pol in CC | pol ne 0};
p2 :=  b + 1;
CC2 := {Resultant(pol,p2,b) : pol in CC};
{Factorization(pol) : pol in CC2 | pol ne 0};
p3:=d+1;
CC3 := {Resultant(pol,p3,d) : pol in CC2};
{Factorization(pol) : pol in CC3 | pol ne 0};
p4:=a^2+a+1;
CC4 := {Resultant(pol,p4,a) : pol in CC3};
{Factorization(pol) : pol in CC4 | pol ne 0};
p5:=C*k^2 + C*k + C*c^2 + C*c + E*k^2 + E*k + E*c^2 + E*c + E;
CC5:={Resultant(pol,p5,c) : pol in CC4};
{Factorization(pol) : pol in CC5 | pol ne 0};
/// C=0 ###
```

References

[1] D. Bartoli, On a conjecture about a class of permutation trinomials, Finite Fields Appl. 52 (2018) 30–50.

[2] D. Bartoli, Hasse - Weil type theorems and relevant classes of polynomial functions, in: K.K. Dabrowski, M. Gadouleau, N. Georgiou, M. Johnson, G.B. Mertzios, D. Paulusma (Eds.), Surveys in Combinatorics 2021, in: London Mathematical Society Lecture Note Series, Cambridge University Press, 2021, pp. 43–102.

[3] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language, in: Computational Algebra and Number Theory, London, 1993, J. Symb. Comput. 24 (3–4) (1997) 235–265.
[4] Z. Ding, M.E. Zieve, Determination of a class of permutation quadrinomials, arXiv preprint, arXiv: 2203.04216, 2022.
[5] J.W.P. Hirschfeld, Projective Geometry over Finite Fields, Clarendon Press, 1979.
[6] X.-d. Hou, Permutation polynomials of the form $x^r(a + x^{2(q-1)})$ — a nonexistence result, arXiv preprint, arXiv:1609.03662, 2016.
[7] X.-d. Hou, Determination of a type of permutation trinomials over finite fields, Acta Arith. 3 (166) (2014) 253–278.
[8] X.-d. Hou, Determination of a type of permutation trinomials over finite fields, II, Finite Fields Appl. 35 (2015) 16–35.
[9] X.-d. Hou, Permutation polynomials over finite fields — a survey of recent advances, Finite Fields Appl. 32 (2015) 82–119.
[10] X.-d. Hou, A survey of permutation binomials and trinomials over finite fields, in: Proceedings of the 11th International Conference on Finite Fields and Their Applications, vol. 632, 2015, pp. 177–191.
[11] X.-d. Hou, Applications of the Hasse-Weil bound to permutation polynomials, Finite Fields Appl. 54 (2018) 113–132.
[12] X.-d. Hou, V. Pallozzi Lavorante, A general construction of permutation polynomials of $\mathbb{F}_{q^2}$, Finite Fields Appl. 89 (2023) 102193.
[13] X.-d. Hou, V. Pallozzi Lavorante, New results on permutation binomials of finite fields, Finite Fields Appl. 88 (2023) 102179.
[14] S.D. Lappano, Some Results Concerning Permutation Polynomials over Finite Fields, PhD thesis, University of South Florida, 2016.
[15] S.D. Lappano, A family of permutation trinomials over $\mathbb{F}_{q^2}$, private communication, 2020.
[16] Z. Tu, X. Zeng, Y. Jiang, Y. Li, Binomial permutations over finite fields with even characteristic, Des. Codes Cryptogr. 89 (12) (2021) 2869–2888.
[17] Q. Wang, Cyclotomic mapping permutation polynomials over finite fields, Seq. Subseq. Conseq. 4893 (2007) 119–128.
[18] L. Zheng, B. Liu, H. Kan, J. Peng, D. Tang, More classes of permutation quadrinomials from Niho exponents in characteristic two, Finite Fields Appl. 78 (2022) 101962.
[19] M. Zieve, On some permutation polynomials over f_q of the form $x^r h(x^{(q-1)/d})$, Proc. Am. Math. Soc. 137 (2009) 2209–2216.