Università Degli Studi di
Modena e Reggio Emilia

Ph.D. in Mathematics

In agreement with:

Università degli Studi di Ferrara

Università degli Studi di Parma

XXXIV Cycle

Geometry over finite fields and its applications

Candidate: Vincenzo Pallozzi Lavorante

Advisor: Prof. Massimo Giulietti

Co-advisor: Prof. Arrigo Bonisoli

Ph.D. Coordinator: Prof. Christian Giatdinà

Ph.D. Thesis

Abstract

This PhD dissertation focuses on some particular problems in classical finite geometry and combinatorics. Two intertwined topics have been considered. The first one is the construction of hemysistems of the Hermitian surface and blocking sets arising from conics. The techniques used to obtain our contribution are based on the Natural Embedding Theorem (NET) of maximal algebraic curves on the Hermitian surface and the Weil theorem for the number of rational points of a cubic surface over a finite field. The second topic is the investigation of polynomials which permute a finite field. Again, the techniques will be of algebraic nature, involving the theory of plane curves over finite fields and Hasse-Weil type theorems.

Sommario

Questa tesi di dottorato si concentra su alcuni problemi di geometria finita classica e di combinatoria. Sono stati considerati due argomenti intrecciati. Il primo è la costruzione di hemisystems della superficie Hermitiana e di blocking sets su coniche irriducibili. Le tecniche utilizzate per ottenere il nostro contributo si basano sul Teorema di Immersione Naturale (NET) delle curve algebriche massimali sulla superficie Hermitiana e sul teorema di Weil per il numero di punti razionali di una superficie cubica su un campo finito. Il secondo argomento è lo studio dei polinomi che permutano un campo finito. Anche in questo caso, le tecniche saranno di natura algebrica, e coinvolgeranno la teoria delle curve piane su campi finiti e teoremi di tipo Hasse-Weil.

*

Contents

Introduction

The investigation of finite projective spaces has received increasing attention both for their links with such applied topics as coding theory and cryptography (which are becoming more and more relevant within ICT) and for their connections to other mathematical theories, say for example graph theory and group theory. In this thesis we focus our attention on notions and problems of geometry over finite fields. At the same time we constantly keep in mind possible applications (e.g. strongly regular graphs and permutation polynomials).

In the first chapter we present the preliminaries one needs to understand most of the original part. References are given for the proofs of the theorems, whenever necessary. To begin with, the basic concepts of algebraic curves defined over a finite field are explored. The original results of Chapters 4 and 5 strongly rely on this part. Algebraic curves over finite fields have been much studied in recent years because of their natural application to several areas of coding theory and cryptography. We then state the Natural Embedding Theorem (NET) for maximal curves. The NET provides a powerful method to understand the properties of a maximal curve when embedded in a Hermitian variety. We will use those ideas in Chapter 2 to construct new families of hemisystems of the Hermitian surface.
Showing the connections between plane algebraic curves and permutation polynomials (PPs) is the last objective of this part of the chapter. This relation has been proven useful to find conditions for a polynomial to be a PP, we will investigate those aspects in Chapters 4 and 5.

After that, we will set the backgrounds for finite classical polar spaces. This second part of Chapter 1 aims to introduce Chapters 2 and 3. The geometry of finite projective spaces and classical polar spaces is the main topic and it is divided into three subsections, each of them focusing on a precise aspect: collineations of projective spaces, classical polar spaces and geometrical point-line configurations.

Chapter 2 is about hemisystems of the Hermitian surface $\mathcal{H}_{3,q^2}$. Hemisystems are interesting configurations which are connected with important combinatorial objects such as strongly regular graphs, partial quadrangles and 4-class imprimitive cometric Q-antipodal association schemes that are not metric; see [15, 6, 13]. Finding hemisystems is a challenging problem. The first infinite family was constructed in 2005 by Cossidente and Penttila [15] who also found a new sporadic example in $\mathcal{H}_{3,25}$. Later on, Bamberg, Giudici and Royle [4, Section 4.1] constructed more sporadic examples for $q = 11, 17, 19, 23, 27$. Recently several new infinite families of hemisystems appeared in the literature. Bamberg, Lee, Momihara and Xiang [6] constructed a new infinite family of hemisystems on $\mathcal{H}_{3,q^2}$ for every $q \equiv -1 \pmod 4$ that generalize the previously known sporadic examples. Cossidente and Pavese [14] constructed, for every odd q, a hemisystem of $\mathcal{H}_{3,q^2}$ invariant under a subgroup of $\mathrm{PGU}(4, q)$ of order $(q + 1)q^2$. Our original contribution is the investigation of the possibility of constructing hemisystems of the Hermitian surface $\mathcal{H}_{3,q^2}$ by using the Natural Embedding Theorem previously mentioned. More precisely our goal is to extend the construction of Korchmáros et al. [34] to the case $p \equiv 1 \pmod 4$. Methods are of algebraic nature, involving number theory and group theory.

In Chapter 3, we focus on a combinatorial problem, related to point-line configurations with respect to an irreducible conic, viewed as a symmetric polar space. In a projective plane Π of odd order $n = m^2$, let C be an oval, and π a Baer-subplane, that is, a projective subplane of order m. We ask to compute, or estimate, the number $E_m(C) = E_m(C, \pi)$ of points in π which are external to C. The trivial bound is $E_m(C) \leq |\pi| = n + m + 1$ but the largest known example is for $E_m(C) = n$. The desarguesian case $\Pi = \mathrm{PG}(2, q^2)$ is worked out. Another statement of the problem can be given in terms of blocking sets. Given an irreducible conic defined over $\mathrm{PG}(2, q^2)$, consider the set of points which are either on the conic or external to the conic. The intersection between a Baer subplane and that set is a blocking set with respect to the tangent lines to the conic. Our goal is to characterize the order of this set.

The application of the theory of algebraic plane curves to PPs is the objective of the last two chapters. In particular, in Chapter 4, we use results also known as *Hasse-Weil type theorems for PPs* to give a non-existence result for permutation binomials. Moreover, we state an equivalence relation for binomials. The reason behind that is to give a contribution towards the systematic classification of permutation binomials. More precisely, there are in the literature numerous results concerning permutation binomials, which use neither the same approach to the problem nor the same notations.

The last chapter is devoted to the proof of a recent conjecture on permutation quadrinomials from Niho exponents in characteristic 2.
Recently Zheng et al. [50] characterized the coefficients of $f(\mathtt{X}) = \mathtt{X}+a_1\mathtt{X}^{s_1(2m-1)+1}+a_2\mathtt{X}^{s_2(2m-1)+1}+a_3\mathtt{X}^{s_3(2m-1)+1}$ over $\mathbb{F}_{2^{2m}}$ that lead $f(\mathtt{X})$ 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 their sufficient conditions were also necessary. We will give a positive answer to that question for most cases.

Chapter 1

Preliminaries

1.1 Curves and permutation polynomials

1.1.1 Basic properties of finite fields

Given a finite field $|\mathrm{F}| < \infty$ of characteristic $p \neq 0$ we we will write $p = \mathrm{char}\mathrm{F}$. We recall the following results.

Theorem 1.1. *Let $p = \mathrm{char}\mathrm{F}$. Then p is a prime number and $\mathbb{Z}_p$ is a subfield of F, where $\mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z}$ is the field of integers modulo p.*

Proof. Define a ring homomorphism

$$\begin{aligned} f\colon \mathbb{Z} &\longrightarrow \mathrm{F}, \\ n &\longmapsto n1_{\mathrm{F}} \end{aligned}$$

By the first isomorphism theorem we have the field embedding $\mathbb{Z}/\ker f \hookrightarrow \mathrm{F}$. Thus $\ker f$ is a prime ideal of $\mathbb{Z}$, namely $p\mathbb{Z}$, where p is the characteristic of the field. Therefore we have p prime and $\mathbb{Z}_p \leq \mathrm{F}$. □

Given two finite fields E, F such that $\mathrm{E} \leq \mathrm{F}$ we denote with $[\mathrm{F} : \mathrm{E}]$ the dimension of F as a vector space over E, that is $\dim_E \mathrm{F}$, and we say that F/E is a *field extension.* Since the field F is finite and $\mathbb{Z}_p \leq \mathrm{F}$, we have that $[\mathrm{F} : \mathbb{Z}_p] < \infty$. Let $n = [\mathrm{F} : \mathbb{Z}_p]$, then there is a group isomorphism $\mathrm{F} \simeq \mathbb{Z}_p^n$.

Theorem 1.2 ([30, Theorem 1.2])**.** *Let F be a finite field and $p = \mathrm{char}\mathrm{F}$. Then $|\mathrm{F}| = p^n$, for some integer $n \in \mathbb{Z}_+$.*

We now investigate whether or not, given a prime number p and an integer $n > 0$, there exists a field F with $|\mathrm{F}| = p^n$. Given a field extension K/F, we say that an element $\alpha \in \mathrm{K}$ is *algebraic* over F if it is a root of a polynomial $f(\mathtt{X}) \in \mathrm{F}[\mathtt{X}]$. An element $\alpha \in \mathrm{K}$ which is not algebraic over F is said to be *transcendental* over F. A finite set $A \subset \mathrm{K}$ is algebraically independent over F if the map v_A is injective, where

$$v_A \colon \mathrm{F}[\mathtt{X}_1, \dots, \mathtt{X}_r] \longrightarrow \mathrm{F}[a_1, \dots, a_r], \quad f \longmapsto f(a_1, \dots, a_r).$$

Definition 1.3. Let K/F be a field extension. We say that K has a finite transcendence degree $n \geq 0$ over F, and we write $\mathrm{trdeg}_F K = n$, if n is the maximum number of algebraically independent elements of K over F. Furthermore, we say that K is *finitely generated* over F.

Definition 1.4. Let F be a field; a field K containing F is said to be an *algebraic closure* of F if and only if every elements in K is algebraic over F and every polynomial with coefficients in K splits completely over K.

There is only one algebraic closure up to isomorphism. We denote by $\overline{\mathrm{F}}$ the algebraic closure of F and we say that F is *algebraically closed* if $\mathrm{F} = \overline{\mathrm{F}}$. The *splitting field* of a polynomial f with coefficients in F is the field generated by the roots of f in the algebraic closure of F.

Theorem 1.5 ([30, Theorem 1.2]). *Let p be a prime and n a positive integer. The splitting field of $\mathtt{X}^{p^n} - \mathtt{X} \in \mathbb{Z}_p[\mathtt{X}]$ has precisely p^n elements.*

Theorem 1.6 ([30, Theorem 1.2]). *Given a prime p and an integer $n > 0$, all finite fields of order p^n are isomorphic.*

We will denote the finite field with $q = p^n$ elements by $\mathbb{F}_q$. Consequently, we have a $\mathbb{Z}_p$-vector space isomorphism $\mathbb{F}_q \simeq \mathbb{F}_p^n$. Note that $\mathbb{F}_p = \mathbb{Z}_p$.

Let $q = p^n$, for p prime and n a positive integer. We will denote with $\mathbb{F}_q^*$ the multiplicative group of $\mathbb{F}_q$.

Theorem 1.7 ([30, Theorem 1.3]). *The multiplicative group $(\mathbb{F}_q^*, \cdot)$ is cyclic.*

A generator of $\mathbb{F}_q^*$ is called a *primitive element* of $\mathbb{F}_q$. For every positive integer d, define the map ψ_d:

$$\begin{aligned} \psi_d \colon \mathbb{F}_q^* &\longrightarrow \mathbb{F}_q^*, \\ a &\longmapsto a^d \end{aligned}$$

The next three results are straightforward consequences of Theorem 1.7.

Proposition 1.8. *The map ψ_d is a group homomorphism, with* $\ker \psi_d = \langle \alpha^{\frac{q-1}{e}} \rangle$, *where α is a primitive element of $\mathbb{F}_q$ and $e := \gcd(q-1, d)$.*

The last proposition leads to the following.

Theorem 1.9 ([18, Teorema 1.11]). *Let d be a positive integer, such that $d < q$ and let $e = \gcd(q-1, d)$. The following hold:*

- *The set of d-th roots of unity in $\mathbb{F}_q$ is a cyclic group of order e.*
- *The number of non zero d-th powers in $\mathbb{F}_q$ is $\frac{q-1}{e}$.*
- *If $\alpha \in \mathbb{F}_q^*$ has a d-th root in $\mathbb{F}_q$, then α has exactly e different d-th roots in $\mathbb{F}_q$.*

Corollary 1.10. *When q is odd, there are exactly half of the non-zero elements of $\mathbb{F}_q$ that are squares, whereas if q is even, every element in $\mathbb{F}_q$ is a square.*

Theorem 1.11 ([30, Theorem 1.6]). *Let p be a prime. For each integer $n \geq 0$, $\overline{\mathbb{F}}_p$ has a unique subfield of order p^n.*

Let K/F be a field extension. The *Galois group* of the extension K/F is

$$\mathrm{Aut}(\mathrm{K}/\mathrm{F}) = \{\phi \in \mathrm{Aut}(\mathrm{K}) : \phi(a) = a \text{ for all } a \in \mathrm{F}\}.$$

Furthermore, the extension K/F is *Galois* if

$$\{a \in \mathrm{K} : \phi(a) = a \text{ for all } \phi \in \mathrm{Aut}(\mathrm{K}/\mathrm{F})\} = \mathrm{F}.$$

Theorem 1.12 ([30, Theorem 1.8]). *The extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois and* $\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \varphi \rangle$, *where*

$$\begin{aligned} \varphi \colon \mathbb{F}_{p^n} &\longrightarrow \mathbb{F}_{p^n}, \\ a &\longmapsto a^p. \end{aligned}$$

More generally, if $m \mid n$, the extension $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$ is Galois and $\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) = \langle \varphi^m \rangle$.

We say that the automorphism $\varphi^m \in \mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m})$ is the *Frobenius map* of $\mathbb{F}_{p^n}$ over $\mathbb{F}_{p^m}$. Note that the map

$$\Phi \colon \overline{\mathbb{F}}_q \longrightarrow \overline{\mathbb{F}}_q, \quad x \longmapsto x^q$$

is the Frobenius homomorphism φ^h, if $q = p^h$.

When q is a prime power and n is a positive integer we define the *trace* and the *norm* of $a \in \mathbb{F}_{q^n}$ from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ by

$$\mathrm{Tr}_{\frac{q^n}{q}}(a) = \sum_{\phi \in \mathrm{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q)} \phi(a) = \sum_{i=0}^{n-1} a^{q^i},$$

and

$$\mathrm{N}_{\frac{q^n}{q}}(a) = \prod_{\phi \in \mathrm{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q)} \phi(a) = a^{\frac{q^n-1}{q-1}}.$$

1.1.2 Affine and projective varieties

Let K be an algebraically closed field and let $\mathbb{A}^n(\mathrm{K}) = \{(a_1, \dots, a_n) | a_i \in \mathrm{K}\}$ denote the *affine n-dimensional space* over K.

Definition 1.13. Let I be an ideal of $\mathrm{K}[X_1, \dots, X_n]$. We say that

$$\mathbf{V}(I) := \{P \in \mathbb{A}^n(\mathrm{K}) | F(P) = 0 \text{ for all } F \in I\}$$

is the *affine (algebraic) set* associated to I. Furthermore if $V = \mathbf{V}(I)$ is an affine set, the ideal

$$\mathbf{I}(V) := \{F \in \mathrm{K}[\mathtt{X}_1, \dots, \mathtt{X}_n] | F(P) = 0 \text{ for all } P \in V\}$$

is said to be the ideal of V.

Definition 1.14. An affine set V is said to be *reducible* if $V = V_1 \cup V_2$, with V_1, V_2 affine sets different from V. V is *irreducible* if it is not reducible. An irreducible affine set is an *affine variety.*

Definition 1.15. Let $\mathrm{PG}(n, \mathrm{K})$ be the n-dimensional projective space defined over the field K, that is the set of $(x_0, \dots, x_n) \in \mathbb{A}^{n+1}(\mathrm{K})$ such that at least one x_i is non-zero, modulo the following equivalence relation: $(x_0, \dots, x_n) \sim (y_0, \dots, y_n)$ if there exists $\lambda \in \mathrm{K}^*$ such that $x_i = \lambda y_i$ for all $i = 0, \dots, n$.

We will denote the set $\{(\lambda a_0, \dots, \lambda a_n) | \lambda \in \mathrm{K}^*\}$ by $(a_0 : \cdots : a_n)$, the elements of this set are the *homogeneous coordinates* in $\mathrm{PG}(n, \mathrm{K})$.

Definition 1.16. Let $F \in \mathrm{K}[\mathtt{X}_0, \dots, \mathtt{X}_n]$ and let I be an ideal of $\mathrm{K}[\mathtt{X}_0, \dots, \mathtt{X}_n]$.

(a) F is said to be homogeneous of degree d if $F(\lambda \mathtt{X}_0, \dots, \lambda \mathtt{X}_n) = \lambda^d F(\mathtt{X}_0, \dots, \mathtt{X}_n)$, for all $\lambda \in \mathrm{K}$.

(b) I is said to be homogeneous if it is generated by homogeneous polynomials.

Definition 1.17. Let $I \subset \mathrm{K}[\mathtt{X}_0, \ldots, \mathtt{X}_n]$ be an homogeneous ideal. Then

$$\mathbf{V}(I) := \{P \in \mathrm{PG}(n, \mathrm{K}) | F(P) = 0 \text{ for all } F \in I\}$$

is the *projective* (*algebraic*) *set* associated to I. Furthermore, if $V = \mathbf{V}(I)$ is a projective set, the homogeneous ideal

$$\mathbf{I}(V) := \{F \in \mathrm{K}[\mathtt{X}_0, \ldots, \mathtt{X}_n] | F \text{ homogeneous, } F(P) = 0 \text{ for all } P \in V\}$$

is said the *ideal of* V.

Definition 1.18. A projective set V is said to be *reducible* if $V = V_1 \cup V_2$ with V_1, $V_2 \in \mathrm{PG}(n, \mathrm{K})$ projective sets different from V. Otherwise V is *irreducible.* An irreducible projective set is a *projective variety.*

Proposition 1.19. *V is a projective variety if and only if $\mathbf{I}(V)$ is a prime ideal.*

Definition 1.20. Let $V \subset \mathrm{PG}(n, \mathrm{K})$ be a projective variety, the quotient ring

$$\mathrm{K}[V] := \mathrm{K}[\mathtt{X}_0, \ldots, \mathtt{X}_n]/\mathbf{I}(V)$$

is the *ring of homogeneous coordinates* on V. The quotient field of $\mathrm{K}[V]$ is denoted by

$$\mathrm{K}(V) := \left\{ \frac{F + \mathbf{I}(V)}{G + \mathbf{I}(V)} \middle| F, G \text{ homogeneous polynomials, } \deg F = \deg G,\ G \notin \mathbf{I}(V) \right\}$$

and it is said to be the *field of rational functions* on V.

Definition 1.21. A rational function $\alpha \in \mathrm{K}(V)$ is said to be *regular* at $P \in V$ if there are F, $G \in \mathrm{K}[\mathtt{X}_0, \ldots \mathtt{X}_n]$ homogeneous such that $\alpha = \frac{F+\mathbf{I}(V)}{G+\mathbf{I}(V)}$ with $G(P) \neq 0$.

Assume without loss of generality that $X_0 \notin \mathbf{I}(V)$ and denote $\bar{x}_i := \frac{X_i+\mathbf{I}(V)}{X_0+\mathbf{I}(V)}$, for $i \in \{1, \ldots, n\}$. This means that, any $\alpha \in \mathrm{K}(V)$ can be written

$$\alpha = \frac{f(\bar{x}_1, \ldots, \bar{x}_n)}{g(\bar{x}_1, \ldots, \bar{x}_n)},$$

for $f, g \in \mathrm{K}[\mathtt{X}_1, \ldots, \mathtt{X}_n]$.

Next we define the dimension of a variety which will lead to the notion of projective curve.

Definition 1.22. Let V be a projective variety. The dimension of V is

$$\dim V := \mathrm{degtr}_{\mathrm{K}}\mathrm{K}(V),$$

that is the transcendence degree of the field extension $\mathrm{K}(V)/\mathrm{K}$.

Sometimes is more convenient to use the non-homogeneous coordinates. For the sake of simplicity, we will explain how to move from an affine equation to a projective equation (and vice-versa) only for projective varieties of dimension 1 in the projective plane. However, one can easily generalize to higher dimensions.

Definition 1.23. Let $\mathcal{C} : F(X_0, X_1, X_2) = 0$ be a projective variety of dimension 1, different from the line $X_0 = 0$. The equation

$$F_*(X, Y) := F(1, X, Y) = 0 \tag{1.1.1}$$

is the *affine equation* of $\mathcal{C}$. Moreover, F_* is called the *dehomogenization* of F with respect to X_0. Vice-versa, when $F(\mathtt{X}, \mathtt{Y})$ is a polynomial of degree d, the *homogenization* of F is

$$F^*(X_0, X_1, X_2) := X_0^d F\left(\frac{X_1}{X_0}, \frac{X_2}{X_0}\right). \tag{1.1.2}$$

Theorem 1.24 ([18, Teorema 3.5])**.** *The homogenization induces a bijection between the polynomials in* $\mathrm{K}[\mathtt{X}, \mathtt{Y}]$ *of degree* d *and the homogeneous polynomials in* $\mathrm{K}[\mathtt{X}_0, \mathtt{X}_1, \mathtt{X}_2]$ *of degree* d *not divided by* $\mathtt{X}_0$*. Equivalently, it induces a bijection between plane projective varieties of dimension* 1 *(different from* $X_0 = 0$*) and their affine part.*

Definition 1.25. Let V be an affine variety. The dimension of V is the dimension of V as a projective variety.

Definition 1.26. Let $P = (a_1, \dots, a_n)$ be a point of an affine variety V and let $\mathbf{I}(V) = \langle F_1, \dots, F_r\rangle$. The tangent space to V at P is the affine subspace

$$T_P(V) := \bigcap_{j=1}^{r} (\mathrm{d}_P F_j = 0), \tag{1.1.3}$$

if $\mathrm{d}_P(F) := \frac{\partial F}{\partial \mathtt{X}_1}(P)(\mathtt{X}_1 - a_1) + \cdots + \frac{\partial F}{\partial \mathtt{X}_n}(P)(\mathtt{X}_n - a_n)$.

Proposition 1.27 ([19, Corollario 1.22])**.** *Let* s *be the dimension of* V*. The dimension of the tangent space equals* s *at each point of* V*, except for a finite affine proper subset.*

Definition 1.28. Let $P \in V$, V an affine variety. P is said to be *singular* if

$$\dim T_P(V) > \dim V.$$

Otherwise, P is *simple*. Moreover, when V is a projective variety, $P \in V$ is singular (simple) if and only if it is singular (simple) for the affine part with respect to the dehomogenization above.

Theorem 1.29. *The following bijection holds:*

$$\begin{array}{ccc} \left\{\begin{matrix} \textit{Projective variety} \\ \textit{over } \mathrm{K} \end{matrix}\right\} & \overset{\sim}{\rightarrow} & \left\{\begin{matrix} \textit{Field extension} \\ \textit{finitely generated over } \mathrm{K} \end{matrix}\right\} \\ V & \longmapsto & \mathrm{K}(V) \end{array} \tag{1.1.4}$$

In this correspondence we have $\dim V = \mathrm{trdeg}_{\mathrm{K}}\mathrm{K}(V)$.

Definition 1.30. Let $\mathcal{X} \subset \mathrm{PG}(n, \mathrm{K})$ be a projective variety. A *rational map* from $\mathcal{X}$ to $\mathrm{PG}(m, \mathrm{K})$ is an element

$$\phi := (\alpha_0 : \cdots : \alpha_m) \in \mathrm{PG}(m, \mathrm{K}(\mathcal{X})).$$

We will write $\phi\colon \mathcal{X} \longrightarrow \mathrm{PG}(m, \mathrm{K})$.

Definition 1.31. A rational map

$$\phi\colon \mathcal{X} \longrightarrow \mathrm{PG}(m, \mathrm{K}), \quad \phi = (\alpha_0 : \cdots : \alpha_m)$$

is said to be regular at a point $P \in \mathcal{X}$ if there exists $\lambda \in \mathrm{K}(\mathcal{X})$ such that

(*i*) every $\lambda\alpha_i$ is regular at P;

(*ii*) $(\lambda\alpha_j)(P) \neq 0$, for some $j \in \{1, \ldots, m\}$.

Definition 1.32. Let $\mathcal{X} \subset \mathrm{PG}(n, \mathrm{K})$ and $\mathcal{Y} \subset \mathrm{PG}(m, \mathrm{K})$ be two projective varieties, a *rational map from* $\mathcal{X}$ *to* $\mathcal{Y}$, in symbol $\phi\colon \mathcal{X} \to \mathcal{Y}$, is a rational map of $\phi\colon \mathcal{X} \to \mathrm{PG}(m, \mathrm{K})$ such that for each point $P \in \mathcal{X}$ at which ϕ is regular we have $\phi(P) \in \mathcal{Y}$. Moreover we say that ϕ is *birational* if there is a rational map ψ with $\phi \circ \psi = Id(\mathcal{Y})$ and $\psi \circ \phi = Id(\mathcal{X})$.

From the definition we note that a rational map may not be defined at every point of $\mathcal{X}$.

Definition 1.33. A rational map

$$\phi\colon \mathcal{X} \to \mathcal{Y}, \quad \phi = (\alpha_0 : \cdots : \alpha_m)$$

which is regular at every point $P \in \mathcal{X}$ is said to be a *morphism* of $\mathcal{X}$ in $\mathcal{Y}$. A birational morphism is called an *isomorphism.*

1.1.3 Algebraic curves

Definition 1.34. An (*algebraic*) *projective curve* $\mathcal{C}$ is a projective variety of dimension 1.

Definition 1.35. Let $\mathcal{C}$ be an algebraic curve and $P \in \mathcal{C}$. The *local ring* of $\mathcal{C}$ at P is

$$\mathrm{K}[\mathcal{C}]_P := \{\alpha \in \mathrm{K}(\mathcal{C}) : \alpha \text{ is regular at } P\}$$

More generally, a *local ring* is a commutative ring R satisfying the following equivalent conditions:

1. The set of non-invertible elements of R is an ideal;
2. There exists one and only one maximal ideal of R.

Furthermore, we say that R is *Noetherian* if every ideal is finitely generated. Noetherian ring are of great interest in algebraic geometry, see e.g. [2].

Proposition 1.36 ([17, Sec. 3.2, Theorem 1])**.** *$\mathrm{K}[\mathcal{C}]_P$ is a Noetherian local domain, with maximal ideal*

$$M_P := \{\alpha \in \mathrm{K}[V]_P : \alpha(P) = 0\}.$$

Moreover, if $P \in \mathcal{C}$ is simple, then M_P is principal.

Definition 1.37. We say that an integral domain O (which is not a field) is a *discrete valuation ring* (DVR) if O is a Noetherian and local ring and its maximal ideal is a principal ideal.

Definition 1.38. Let $P \in \mathcal{C}$ be a simple point of a projective curve $\mathcal{C}$. A *local parameter* t of $\mathcal{C}$ at P is a generator of M_P.

Our next objective is to associate a valuation map to every simple point of a curve. Taking this into account, from now on, $\mathcal{C}$ will be a *non-singular*, projective curve $\mathcal{C}$ defined over K. That is, every point $P \in \mathcal{C}$ is a simple point.

Proposition 1.39. *Let $\mathcal{C}$ be a projective curve and $t \in M_P$ be a local parameter of $\mathcal{C}$ at P. For every $\alpha \in \mathrm{K}[\mathcal{C}]_P$, $\alpha \neq 0$, there exists a unique $m \in \mathbb{Z}$ and a unique $u \in \mathrm{K}[\mathcal{C}]_P \setminus M_P$ such that $\alpha = ut^m$. Also, the integer m does not depend on the choice of t.*

Definition 1.40. Let $P \in \mathcal{C}$ and $\alpha \in \mathrm{K}(\mathcal{C})$, $\alpha \neq 0$. The *valuation* $v_P(\alpha)$ of α at P is the integer m such that $\alpha = ut^m$ for $u \in \mathrm{K}[\mathcal{C}]_P \setminus M_P$ and t be a local parameter of $\mathcal{C}$ at P.

Note that

$$\mathrm{K}[\mathcal{C}]_P = \{\alpha \in \mathrm{K}(\mathcal{C}) : v_P(\alpha) \geq 0\} \text{ and } M_P = \{\alpha \in \mathrm{K}(\mathcal{C}) : v_P(\alpha) > 0\}.$$

The valuation map of a DVR satisfies the properties of linearity and sub-additivity. Moreover, $v_P(\alpha) = 0$ if and only if $\alpha \in \mathrm{K} \setminus \{0\}$.

Definition 1.41. A point $P \in \mathcal{C}$ is said to be a *zero* of multiplicity m for $\alpha \in \mathrm{K}(\mathcal{C})$ if $v_P(\alpha) = m > 0$. A point $P \in \mathcal{C}$ is said to be a *pole* of multiplicity $-m$ for $\alpha \in \mathrm{K}(\mathcal{C})$ if $v_P(\alpha) = m < 0$.

Given two curves $\mathcal{C}$ and $\mathcal{D}$ and a non constant rational map $\phi \colon \mathcal{C} \to \mathcal{D}$, ϕ induces an immersion of fields $\phi^* \colon K(\mathcal{D}) \to K(\mathcal{C})$, which is called the *pull-back* of ϕ.

When dealing with algebraic curves we will write $\mathrm{Gal}(\mathcal{C}/\mathcal{D})$ for the automorphism group $\mathrm{Gal}(\mathrm{K}(\mathcal{C})/\mathrm{K}(\mathcal{D}))$ of the automorphisms of $\mathrm{K}(\mathcal{C})$ which fix $\mathrm{K}(\mathcal{D})$ elementwise, that is

$$\mathrm{Gal}(\mathcal{C}/\mathcal{D}) = \{\sigma \colon \mathrm{K}(\mathcal{C}) \to \mathrm{K}(\mathcal{C}) | \sigma \text{ automorphism}, \sigma(z) = z \text{ if } z \in \mathrm{K}(\mathcal{D})\}.$$

Definition 1.42. Let $\mathcal{C}$ and $\mathcal{D}$ be two projective curves. A non constant rational map $\phi \colon \mathcal{C} \to \mathcal{D}$ is *Galois* if the field extension $\mathrm{K}(\mathcal{C})/\mathrm{K}(\mathcal{D})$ is Galois.

Remark 1.43. Note that if $\mathcal{C}$ and $\mathcal{D}$ are two non-singular curves, there exists a bijection between the points of $\mathcal{D}$ and the orbits of points in $\mathcal{C}$ under the action of $\mathrm{Gal}(\mathcal{C}/\mathcal{D})$.

Definition 1.44. We say that $\mathcal{D}$ is a *quotient curve* of $\mathcal{C}$, or $\mathcal{D}$ is Galois-covered by $\mathcal{C}$, if there is a Galois map $\phi \colon \mathcal{C} \to \mathcal{D}$.

One may ask whether there is a quotient curve for each finite subgroup of $\mathrm{Aut}(\mathrm{K}(\mathcal{C}))$, the group of automorphism of $\mathrm{K}(\mathcal{C})$ fixing K elementwise. The following theorem answers that question.

Theorem 1.45 ([19, Teorema 5.16]). *Let G be a finite automorphism group of* $\mathrm{K}(\mathcal{C})$. *Then the fixed field*

$$\mathrm{F}_G = \{\alpha \in \mathrm{K}(\mathcal{C}) | \sigma(\alpha) = \alpha \textit{ for all } \sigma \in G\}$$

is such that $\mathrm{K}(\mathcal{C})/\mathrm{F}_G$ *is Galois and* $G = \mathrm{Gal}(\mathrm{K}(\mathcal{C})/\mathrm{F}_G)$. *Moreover* F_G *is an extension of* K *with* $\mathrm{trdeg}_{\mathrm{K}}\mathrm{F}_G = 1$.

Definition 1.46. The algebraic curve over K which corresponds to F_G, for an automorphism group G of $\mathcal{C}$ (with respect to (1.1.4)) will be denoted by ${}^{\mathcal{C}}\!/_{G}$.

Corollary 1.47. *The map $G \mapsto {}^{\mathcal{C}}\!/_{G}$ defines a bijection between the finite subgroups of* $\mathrm{Aut}(\mathrm{K}(\mathcal{C}))$ *and the quotient curves of $\mathcal{C}$.*

Note that the G acts on the point of $\mathcal{C}$ and the point of $\mathcal{D} := {}^{\mathcal{C}}\!/_{G}$ are in bijection with the orbit of such action. When the base field is finite, we recall that an action is *transitive* on $\mathcal{C}$ if there is only one G-orbit, that is there exists $x \in \mathcal{C}$ such that $x^G = \mathcal{C}$. If the action is transitive and $|G| = |\mathcal{C}|$, then the action is *sharply transitive.* Furthermore, we say that the G-action on $\mathcal{C}$ is *faithful* if any two distinct elements of G give two distinct permutations of $\mathcal{C}$.

1.1.4 Plane curves over finite fields

In this section let $\mathrm{K} = \overline{\mathbb{F}}_q$ define the algebraic closure of the finite field $\mathbb{F}_q$ with q elements. For every integer r the projective space $\mathrm{PG}(n, \overline{\mathbb{F}}_q)$ contains the finite projective space $\mathrm{PG}(n, q^i) := \mathrm{PG}(n, \mathbb{F}_{q^i})$ for $i \geq 1$.
For the sake of simplicity, we give the definition of genus only for a non-singular plane curve. We refer the reader to [23] for a deeper approach.

Definition 1.48. Let $\mathcal{C} : F(X_0, X_1, X_2) = 0$ be a projective and non-singular plane curve defined over K. The genus of $\mathcal{C}$ is defined to be:

$$g := \frac{(\deg F - 1)(\deg F - 2)}{2}.$$

From now on, for a plane curve we mean a projective and *non-singular* plane curve defined over $\overline{\mathbb{F}}_q$.

Definition 1.49. A plane curve $\mathcal{C} : F(X_0, X_1, X_2) = 0$ is defined over $\mathbb{F}_q$ if there is a non-zero constant $c \in \mathrm{K}$ such that $cF(\mathtt{X}_0, \mathtt{X}_1, \mathtt{X}_2) \in \mathbb{F}_q[\mathtt{X}_0, \mathtt{X}_1, \mathtt{X}_2]$. We say that $\mathcal{C}$ is

$\mathbb{F}_q$-rational, if $\mathcal{C}$ is an (irreducible) plane curve defined over $\mathbb{F}_q$.

Note that the finite field $\mathbb{F}_{q^n}$ is made by all the elements that are fixed by Φ^n.

Lemma 1.50. *A plane curve $\mathcal{C}$ is $\mathbb{F}_q$-rational if and only if for every $P = (a_0 : a_1 : a_2) \in \mathcal{C}$, we have $\Phi(P) := (a_0^q : a_1^q : a_2^q) \in \mathcal{C}$.*

Lemma 1.50 holds also for $\mathbb{F}_q^n$, in fact, say

$$\Phi^n \colon \mathcal{C} \longrightarrow \mathcal{C}, \quad (a_0 : a_1 : a_2) \longmapsto (\Phi^n(a_0) : \Phi^n(a_1) : \Phi^n(a_2)),$$

$\mathcal{C}$ is defined over $\mathbb{F}_q^n$ if and only if for every $P \in \mathcal{C}$ we have $\Phi^n(P) \in \mathcal{C}$.

The Frobenius homomorphism can be extended to the field of rational functions on $\mathcal{C}$ by using

$$\sum_{i,j} a_{ij} \bar{x}_1^i \bar{x}_2^j \longmapsto \sum_{i,j} a_{ij}^q \bar{x}_1^i \bar{x}_2^j, \tag{1.1.5}$$

and

$$\Phi \colon \mathrm{K}(\mathcal{C}) \longrightarrow \mathrm{K}(\mathcal{C}), \quad \frac{f(\bar{x}_1, \bar{x}_2)}{g(\bar{x}_1, \bar{x}_2)} \longmapsto \frac{\Phi(f(\bar{x}_1, \bar{x}_2))}{\Phi(g(\bar{x}_1, \bar{x}_2))}. \tag{1.1.6}$$

Definition 1.51. Let $\mathcal{C}$ be a curve, $P \in \mathcal{C}$ and $\alpha \in \mathrm{K}(\mathcal{C})$ be a rational function.

(a) P is said to be $\mathbb{F}_{q^n}$-rational if $\Phi^n(P) = P$. The set of $\mathbb{F}_{q^n}$-rational points is denoted by $\mathcal{C}(\mathbb{F}_{q^n})$.

(b) α is said to be $\mathbb{F}_{q^n}$-rational if $\Phi^n(\alpha) = \alpha$. The set of all the $\mathbb{F}_{q^n}$-rational functions is denoted by $\mathbb{F}_{q^n}(\mathcal{C})$.

Remark 1.52. Since every projective curve is birationally isomorphic to a plane curve, what it has been said for plane curves extends to any curves. In particular, a curve $\mathcal{C}$ is $\mathbb{F}_q$-rational if and only if it is birationally equivalent to an $\mathbb{F}_q$-rational plane curve, by an $\mathbb{F}_q$-rational map, which is a rational map defined by $\mathbb{F}_q$-rational functions, see for example [19, Corollario 1.68].

The Hasse-Weil bound

The purpose of this section is to investigate the number of $\mathbb{F}_q$-rational points of a (non-singular and irreducible) curve defined over $\mathbb{F}_q$. The key result is surely the *Hasse-Weil's bound* which provides a lower and upper bound for that number.

Definition 1.53. Let $\mathcal{C} : F = 0$ be an irreducible curve over $\mathbb{F}_q$. We say that $\mathcal{C}$ is *absolutely irreducible* over $\mathbb{F}_q$ if F is irreducible in $\mathrm{K} = \overline{\mathbb{F}}_q$.

Theorem 1.54 (Hasse-Weil). *Let $\mathcal{C}$ be a projective absolutely irreducible non-singular curve of genus g defined over $\mathbb{F}_q$. Then*

$$\mathcal{C}(\mathbb{F}_q^n) = q^n + 1 - \sum_{i=1}^{2g} \alpha_i^n, \tag{1.1.7}$$

where $\alpha_i \in \mathbb{C}$ and $|\alpha_i| = \sqrt{q}$.

As a corollary, one gets the famous Hasse-Weil bound.

Theorem 1.55 (Hasse-Weil bound). *Let $\mathcal{C}$ be a projective absolutely irreducible non-singular curve of genus g defined over $\mathbb{F}_q$. Then*

$$q + 1 - 2g\sqrt{q} \leq |\mathcal{C}(\mathbb{F}_q)| \leq q + 1 + 2g\sqrt{q}. \tag{1.1.8}$$

If $\mathcal{C}$ is a non-singular plane curve, then equation (1.1.8) *reads*

$$q + 1 - (d-1)(d-2)\sqrt{q} \leq |\mathcal{C}(\mathbb{F}_q)| \leq q + 1 + (d-1)(d-2)\sqrt{q}. \tag{HW}$$

Definition 1.56. A curve $\mathcal{C}$ is said to be $\mathbb{F}_q$-maximal if it attains the upper bound of the Hasse-Weil bound; i.e.,

$$|\mathcal{C}(\mathbb{F}_q)| = q + 1 + 2g\sqrt{q},$$

where g is the genus of the curve.

When the curve $\mathcal{C}$ is singular, one can not easily deal with the Hasse-Weil bound. The reason is that when a point $P \in \mathcal{C}$ is singular, there may be more than one generator for the maximal ideal M_P of the local ring $\mathrm{K}[\mathcal{C}]_P$ and one needs to use a different approach to overcome this problem, namely the function field setting. We refer the reader to [47] for a very deep and accurate description of this approach.

If a curve $\mathcal{C}$ is $\mathbb{F}_{q^2}$-maximal and N_n is the number of his $\mathbb{F}_{q^{2n}}$-rational points, then

$$N_n = q^{2n} + 1 + (-1)^{n-1} 2gq^n, \qquad \text{for all } n \geq 1. \tag{1.1.9}$$

We conclude this section stating an important theorem concerning coverings of maximal curves [33].

Theorem 1.57 ([23, Theorem 9.17], Kleiman-Serre). *Let $\mathcal{D}$ be an $\mathbb{F}_{q^2}$-rational curve covered by an $\mathbb{F}_{q^2}$-maximal curve $\mathcal{C}$, by an $\mathbb{F}_{q^2}$-rational map. Then, $\mathcal{D}$ is an $\mathbb{F}_{q^2}$-*

maximal curve.

We last introduce the notion of a *divisor* of a (non-singular) curve $\mathcal{C}$.

Definition 1.58. The *divisor group* $\mathrm{Div}(\mathcal{C})$ of a non-singular curve $\mathcal{C}$ is defined as the free abelian group generated by the points of $\mathcal{C}$. An element $D \in \mathrm{Div}(\mathcal{C})$ is a *divisor* on $\mathcal{C}$. Equivalently, a divisor $D \in \mathrm{Div}(\mathcal{C})$ is a formal sum

$$D := \sum_{P\in\mathcal{C}} n_P P \;\text{ with } n_P \in \mathbb{Z},$$

and $n_P \neq 0$ for as much as finitely many points P. The *support* of D is the set

$$\mathrm{supp} D := \{P \in \mathcal{C} |\; n_P \neq 0\}.$$

Addition and subtraction of divisors are defined by summing their coefficients. The identity is the zero divisor, namely the divisor with $n_P = 0$ for all $P \in \mathcal{C}$. Given a divisor $D \in \mathrm{Div}(\mathcal{C})$, we define the *valuation* of D at a point $P \in \mathcal{C}$ as

$$v_P(D) := n_P.$$

Definition 1.59. We give a partial ordering to the set $\mathrm{Div}(\mathcal{C})$ by the following relation:

$$D_1 \leq D_2 \iff v_P(D_1) \leq v_P(D_2) \text{ for all } P \in \mathcal{C}.$$

A divisor $D \geq 0$ is said to be *effective.* The *degree* of a divisor D is defined as

$$\deg D := \sum_{P\in\mathcal{C}} v_P(D),$$

which gives rise to a group homomorphism $\deg\colon \mathrm{Div}(\mathcal{C}) \to \mathbb{Z}$.

The next definition shows that an important class of divisors arises from rational functions. Recall that any non-zero rational function $\alpha \in \mathrm{K}(\mathcal{C})$ has at most a finite number of *zeros* and *poles.*

Definition 1.60. Let $0 \neq \alpha \in \mathrm{K}(\mathcal{C})$. Then the *principal divisor* of α is

$$(\alpha) := \sum_{P\in\mathcal{C}} v_P(\alpha)P.$$

Moreover, if $\mathbf{Z}$ is the set of zeros and $\mathbf{N}$ the set of poles of α, we define

$$(\alpha)_0 := \sum_{P\in\mathbf{Z}} v_P(\alpha)P, \text{ the \textit{divisor of the zeros} of } \alpha,$$
$$(\alpha)_\infty := \sum_{P\in\mathbf{N}} -v_P(\alpha)P, \text{ the \textit{divisor of the poles} of } \alpha.$$

The following identity holds: $(\alpha) = (\alpha)_0 - (\alpha)_\infty$.

Also, recall that we have the following characterization:

$$x \in \mathrm{K}^* \iff (x) = 0.$$

Definition 1.61. Two divisors D and $D' \in \mathrm{Div}(\mathcal{C})$ are linearly equivalent if they differs for a principal divisor, that is, there exists an element $\alpha \in \mathrm{K}(\mathcal{C})$ such that

$$D = D' + (\alpha).$$

Being linearly equivalent is an equivalence relation, which will be denoted by $D \equiv D'$.

Divisors are very useful when we want to describe intersection between projective curves. In fact, from Bézout theorem, any two plane curves $\mathcal{C}$ and $\mathcal{D}$ intersect in exactly $\deg \mathcal{C} \cdot \deg \mathcal{D}$ points (counted with multiplicity). Thus, we get the following definition, which is given in a more general background.

Definition 1.62. Given an irreducible variety $\mathcal{X}$ and a hyperplane Π, the intersection divisor $\mathcal{I}(\mathcal{X}, \Pi)$ on $\mathcal{X}$ is defined to be the divisor with support the set of the intersection points of $\mathcal{X}$ and Π. More precisely, any point that appears in $\mathcal{I}(\mathcal{X}, \Pi)$ has degree equal to its intersection multiplicity.

1.1.5 Permutation polynomials

We introduce the notion of polynomial function with respect to the algebra of functions with value over a finite field. This part follows [30, Section 2.3]. For any two sets A and B, by $\mathcal{F}(A, B)$ we denote the set of all functions from A to B.

We aim to investigate the $\mathbb{F}_q$-algebra $\mathcal{F}(\mathbb{F}_q^n, \mathbb{F}_q)$, for every $n > 0$. When the field is finite, every function can be represented by a polynomial function, and vice-versa. More precisely, let $\mathbb{F}_q[\mathtt{X}_1, \ldots, \mathtt{X}_n]$ be the polynomial ring in $\mathtt{X}_1, \ldots, \mathtt{X}_n$ over $\mathbb{F}_q$. Each element $f(\mathtt{X}_1,\dots,\mathtt{X}_n) \in \mathbb{F}_q[\mathtt{X}_1,\dots,\mathtt{X}_n]$ induces a function

$$\begin{aligned} \bar{f}\colon \mathbb{F}_q^n &\longrightarrow \mathbb{F}_q \\ (a_1,\dots,a_n) &\longmapsto f(a_1,\dots,a_n). \end{aligned}$$

We want to investigate the map $\overline{(\,)}\colon f \mapsto \bar{f}$. Clearly it is an $\mathbb{F}_q$-algebra homomorphism. Now define for each element $(a_1,\dots,a_n) \in \mathbb{F}_q^n$ the polynomial:

$$\Lambda_{(a_1,\dots,a_n)} = \prod_{i=1}^{n} \prod_{b\in\mathbb{F}_q\setminus\{a_i\}} \frac{\mathtt{X}_i - b}{a_i - b} \tag{1.1.10}$$

The set $\{\Lambda_{(a_1,\dots,a_n)} : (a_1,\dots,a_n) \in \mathbb{F}_q^n\}$ is a basis of $\mathcal{F}(\mathbb{F}_q^n,\mathbb{F}_q)$ (see [30, Section 2.3]). Consequently, the map $\overline{(\,)}\colon \mathbb{F}_q[\mathtt{X}_1,\dots,\mathtt{X}_n] \to \mathcal{F}(\mathbb{F}_q^n,\mathbb{F}_q)$ is onto.

Theorem 1.63 ([30, Theorem 2.15])**.** *The homomorphism* $\overline{(\,)}\colon \mathbb{F}_q[\mathtt{X}_1,\dots,\mathtt{X}_n] \to \mathcal{F}(\mathbb{F}_q^n,\mathbb{F}_q)$ *induces an* $\mathbb{F}_q$*-algebra isomorphism*

$$\mathbb{F}_q[\mathtt{X}_1,\dots,\mathtt{X}_n]\big/(\mathtt{X}_1^q - \mathtt{X}_1,\dots,\mathtt{X}_n^q - \mathtt{X}_n) \simeq \mathcal{F}(\mathbb{F}_q^n,\mathbb{F}_q), \tag{1.1.11}$$

where $(\mathtt{X}_1^q-\mathtt{X}_1,\dots,\mathtt{X}_n^q-\mathtt{X}_n)$ *is the ideal of* $\mathbb{F}_q[\mathtt{X}_1,\dots,\mathtt{X}_n]$ *generated by* $\mathtt{X}_1^q-\mathtt{X}_1,\dots,\mathtt{X}_n^q-\mathtt{X}_n$.

Note that since we are making the quotient by $\mathtt{X}_i^q - \mathtt{X}_i$, not only can we represent each function from $\mathbb{F}_q^n$ to $\mathbb{F}_q$ by using a polynomial, but also the order of every $\mathtt{X}_i$ in the representative polynomial is at most $q-1$.

Corollary 1.64. *Every function* $f\colon \mathbb{F}_q \to \mathbb{F}_q$ *is uniquely represented by a polynomial of degree at most* $q-1$ *in* $\mathbb{F}_q[\mathtt{X}]$.

Definition 1.65. A polynomial $f \in \mathbb{F}_q[\mathtt{X}]$ is called a *permutation polynomial* of $\mathbb{F}_q$ if the function $a \mapsto f(a)$ is a permutation of $\mathbb{F}_q$.

By Corollary 1.64, the number of permutation polynomials of $\mathbb{F}_q$ is $q!$. In principle, constructing permutation polynomials is simple, and it can be done by using Lagrange interpolation. However, a main question concerning permutation polynomials over $\mathbb{F}_q$ is how to recognize them. Below we will see some useful criteria to address this problem. For a survey of the most recent advances on permutation polynomials the reader is invited to see [30, 27, 8].

Theorem 1.66 (Hermite's criterion, [30, Theorem 2.20])**.** *A polynomial* $f \in \mathbb{F}_q[\mathtt{X}]$ *is a permutation polynomial of* $\mathbb{F}_q$ *if and only if the following two conditions are both* *satisfied.*

(i) f *has exactly one root in* $\mathbb{F}_q$.

(ii) *For each integer* $1 \leq s \leq q-2$, $f^s \equiv f_s \pmod{\mathtt{X}^q - \mathtt{X}}$ *for some* $f_s \in \mathbb{F}_q[\mathtt{X}]$ *with* $\deg f_s \leq q-2$.

The proof of the Hermite's criterion makes use of the following Lemma, which is of its own interest.

Lemma 1.67 ([30, Lemma 2.21])**.** *Let* $a_0, \ldots, a_{q-1} \in \mathbb{F}_q$. *Then the following two conditions are equivalent.*

(i) $a_0, \ldots, a_{q-1}$ *are distinct in* $\mathbb{F}_q$.

(ii) *The following holds:*

$$\sum_{j=0}^{q-1} a_j^s = \begin{cases} 0, & \text{if } 0 \leq s \leq q-2, \\ -1, & \text{if } s = q-1. \end{cases}$$

An equivalent statement for the Hermite's criterion is the following, which is more useful in the applications.

Theorem 1.68 ([30, Corollary 2.22])**.** *Let* $f \in \mathbb{F}_q[\mathtt{X}]$, *then* f *is a permutation polynomial if and only if the following holds*

$$\sum_{x \in \mathbb{F}_q} f(\mathtt{X})^s = \begin{cases} 0, & \text{if } 0 \leq s \leq q-2 \\ -1, & \text{if } s = q-1. \end{cases} \tag{H}$$

However, computing the summation (H), that is a power sum for f, may be challenging. This is the reason why in the next section we will describe a different approach, connected to the theory of algebraic curves defined over a finite field.

A lot of efforts have been made to find a way to construct permutation polynomials. The following is referred in [27] as the Akbary–Ghioca–Wang (AGW) criterion.

Theorem 1.69 (The AGW criterion, [27, Theorem 2.1])**.** *Let* A, S *and* $\bar{S}$ *be finite sets such that* $|S| = |\bar{S}|$, *and let* $f\colon A \mapsto A$, $\bar{f}\colon S \mapsto \bar{S}$, $\lambda\colon A \mapsto S$ *and* $\bar{\lambda}\colon A \mapsto \bar{S}$ *be a mapping such that* λ *and* $\bar{\lambda}$ *are onto and* $\bar{\lambda} \circ f = \bar{f} \circ \lambda$. *Then, the following statements are equivalent.*

(i) f *is a permutation of* A.

(*ii*) *$\bar{f}$ is a bijection and f is one-to-one on $\lambda^{-1}(s)$ for all $s \in S$.*

The AGW criterion has been thought as a generalization of a result by Zieve [52], which provides a powerful method to recognize permutation polynomials. This approach involves the set of $(q+1)$-th roots of unity μ_{q+1}.

Theorem 1.70 ([52, Lemma 2.1]). *Let $h(\mathtt{X}) \in \mathbb{F}_{q^2}[\mathtt{X}]$. Then $f(\mathtt{X}) = \mathtt{X}^r h(\mathtt{X}^{q-1})$ is a permutation polynomial if and only if the following conditions are satisfied:*

(*i*) $\gcd(r, q-1) = 1$*;*

(*ii*) $\mathtt{X}^r h(\mathtt{X})^{q-1}$ *permutes* μ_{q+1}*.*

The main advantage of using Theorem 1.70 is that one can simplify by a lot the form of f, working only out the case $\mathtt{X}^{q+1} = 1$, which may simplify the computations. As a demonstration of that, a lot of results on permutation polynomials comes from it, see for example [24, 26, 42].

Connection to algebraic curves

Given a permutation polynomial $f \in \mathbb{F}_q[\mathtt{X}]$ we can associate to f the curve $\mathcal{C}_f$ defined by

$$\mathcal{C}_f \colon \frac{f(X) - f(Y)}{X - Y} = 0$$

Investigating the $\mathbb{F}_q$-rational points of $\mathcal{C}_f$ is certainly a way to recognize whether the polynomial f is a permutation polynomial or not. In fact, if $a \neq b$ are two distinct elements of $\mathbb{F}_q$ such that $f(a) = f(b)$, then the $\mathbb{F}_q$-rational point (a, b) belongs to $\mathcal{C}_f$ and does not lie on the line $X - Y = 0$. On the other hand, if (a, b) is an $\mathbb{F}_q$-rational point of $\mathcal{C}_f$ not lying on $X - Y = 0$, then $f(a) = f(b)$ and so $f(\mathtt{X})$ is not a permutation polynomial.

Proposition 1.71 ([8, Proposition 5.1]). *Let $f(\mathtt{X}) \in \mathbb{F}_q[\mathtt{X}]$ and $\mathcal{C}_f$ be the associated plane curve. Then f is a permutation polynomial if and only if there are no (affine) $\mathbb{F}_q$-rational points of $\mathcal{C}_f$ off the line $X - Y = 0$.*

Taking this into account, the Hasse-Weil bound gives a strong technique to work out this problem. Unfortunately, the Hasse-Weil bound works only for irreducible curves (over $\overline{\mathbb{F}}_q$).

To show that $\mathcal{C}_f$ has a suitable $\mathbb{F}_q$ rational point we do not need to prove that the curve $\mathcal{C}_f$ is absolutely irreducible over $\mathbb{F}_q$, but we just need to show that $\mathcal{C}_f$ has an absolutely irreducible components defined over $\mathbb{F}_q$. More precisely, if $f(\mathtt{X}) \in \mathbb{F}_q[\mathtt{X}]$ is such that the numerator of $\mathcal{C}_f$ contains an absolutely irreducible factor in $\mathbb{F}_q[\mathtt{X}]$

(other than $X - Y$), then, by the Hasse-Weil bound, $f(\mathtt{X})$ is not a PP of $\mathbb{F}_q$ (when q is large enough with respect to the degree of f). On the other hand, if we assume that the numerator of $\mathcal{C}_f$ does not contain any absolutely irreducible factor in $\mathbb{F}_q[\mathtt{X}]$, other than possibly $X - Y = 0$, we get nontrivial conditions on the coefficients of $f(\mathtt{X})$, which sometimes lead to new PPs ([24, 28]). The Hasse-Weil bound is a powerful tool for PPs when the size of the field (q) is large compared with the degree of the polynomial function (d); the condition usually takes the form $q \geq Cd^4$ for some constant $C > 0$.

Proposition 1.72 ([8, Proposition 5.3])**.** *Let $f(\mathtt{X}) \in \mathbb{F}_q[\mathtt{X}]$, $q \geq 7$, be a permutation polynomial. Then $\mathcal{C}_f$ does not contain any absolutely irreducible component defined over $\mathbb{F}_q$ of degree d smaller than $\sqrt[4]{q} + 2$ and different from $X - Y = 0$.*

1.2 Finite projective and polar spaces

This section aims to introduce basic notions of finite projective spaces and finite classical polar spaces. Particular regard is given to their automorphism group. We will follow outline and notation of [44, Chapter 2].

1.2.1 Collineations of finite projective spaces

Let $q = p^h$ a prime power and consider the vector space $\mathrm{V}(n+1, q)$ of dimension $n+1$ defined over $\mathbb{F}_q$. Any element $v \in V$ is represented as a column vector. This means that $v^T = [v_0, \dots, v_n]$. In this section we denote by PG(V) the projective space defined over V. As common we will call *point*, *line*, *plane* and *hyperplane* a 0, 1, 2 and $n-1$-dimensional subspace of $\mathrm{PG}(n, q)$. Moreover, for a vector $v \in \mathrm{V}$ and an automorphism $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$, we denote by $v^\sigma := [v_0^\sigma, \dots, v_n^\sigma]$. Similarly for a point $P \in \mathrm{PG(V)}$ we denote by P^θ the image of a map θ on P.

Definition 1.73. Let V_1 and V_2 be two vector spaces of the same dimension. A *collineation* between $\mathrm{PG}(V_1)$ and $\mathrm{PG}(V_2)$ is a bijection which sends points to points, lines to lines and preserves the incidence between lines.

Given a bijection $\theta\colon \mathrm{PG}(V_1) \to \mathrm{PG}(V_2)$, then θ is a collineation if $\Pi \subset \Pi'$ implies $\Pi^\theta \subset \Pi'^\theta$, for any two subspaces $\Pi, \Pi' \subset \mathrm{PG}(V_1)$.

Let $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$ and let $A \in \mathrm{GL}(n+1, q)$ be an invertible $(n+1) \times (n+1)$ matrix over $\mathbb{F}_q$.

Definition 1.74. A *semilinear isomorphism* of $\mathrm{V}(n+1,q)$ is a map

$$\begin{aligned}\gamma_{\sigma,A}\colon \mathrm{V}(n+1,q) &\longrightarrow \mathrm{V}(n+1,q),\\ v &\longmapsto Av^{\sigma}\end{aligned}$$

By $\Gamma\mathrm{L}(n+1,q)$ we denote the group of all semilinear isomorphisms of $\mathrm{V}(n+1,q)$.

Any $\gamma \in \Gamma\mathrm{L}(n+1,q)$ defines a bijection on the points of $\mathrm{PG}(n,q)$, which is also a collineation. More precisely we will say that $\gamma \in \Gamma\mathrm{L}(n+1,q)$ is a *projective semilinear map*. A projective semilinear map with $\sigma = Id$ is a *projectivity*.

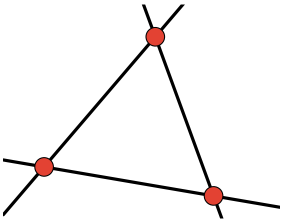
Definition 1.75. The set of all the projective linear (semilinear) maps of $\mathrm{PG}(n,q)$ is a group called *projective linear* (*semilinear*) *group* and denoted by $\mathrm{PGL}(n+1,q)$ ($\mathrm{P\Gamma L}(n+1,q)$).

Theorem 1.76 (Fundamental Theorem of Projective Geometry, [18, Teorema 1.25])**.** *Let V_1 and V_2 be two vector spaces of the same dimension over $\mathbb{F}_q$. Every collineation between $\mathrm{PG}(V_1)$ and $\mathrm{PG}(V_2)$ is induced by a semilinear map $\gamma_{\sigma,A}$.*

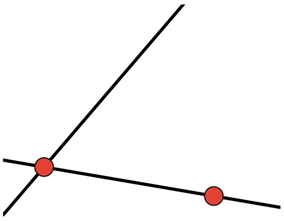
In line with Chapter 1 we will use homogeneous coordinates $P^T = (X_0 : \dots : X_n)$ to describe a point of $\mathrm{PG}(n,q)$. Any hyperplane $\Pi \subset \mathrm{PG}(n,q)$ can be written as $P^T u = 0$ for a vector $u^T = [u_0, \dots, u_{n+1}] \in \mathrm{V}(n+1,q)$. Moreover, let $\gamma_{\sigma,A}$ be a projective semilinear map, then a point $P \in \mathrm{PG}(n,q)$ belongs to $\Pi^{\gamma_{\sigma,A}}$ if and only if $(AP^{\sigma})^T(A^{-T}u^{\sigma}) = P^T u = 0$, which means that $\Pi^{\gamma_{\sigma,A}}$ is represented by the vector $A^{-T}u^{\sigma}$.

The last part of this section is devoted to the canonical forms of transformation in the plane. We refer the reader to [40] for more details. The transformations of the projective plane may be classified (up to projectivities) according to the five types of invariant figures.

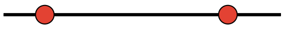
In particular the collineations in case 4 and 5 belong to the class of collineations fixing an hyperplane.



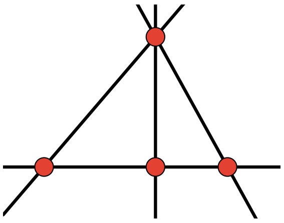
Case 1: collineations fixing a triangle.



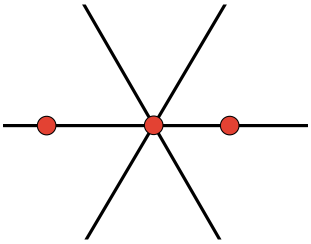
Case 2: collineation fixing two points and two lines.



Case 3: collineations fixing a lineal element.



case 4 (*homology*): collineation fixing a line and a point off the line;



Case 5 (*elation*): collineation fixing a line and a point of the line.

Definition 1.77. A collineation of $\mathrm{PG}(2,q)$ is called a *central collineation* or *perspectivity* if there exists a line Π (called the *axis* of the collineation) and a point z (called the *center* of the collineation) such that each point of Π is a fixed point and each line through z is a fixed line.

We will say that a (z,Π)-perspectivity is an *elation* or a *homology* according as $z \in \Pi$ or $z \notin \Pi$. A homology of the plane can be written in canonical form as $(X_0 : X_1 : X_2) \mapsto (\alpha X_0 : X_1 : X_2)$, where α is different from 0 and 1. When $\alpha = -1$ we will refer to them as *reflection*. An elation of the projective plane can be written in canonical form as $(X_0 : X_1 : X_2) \mapsto (X_0 : X_1 + X_2 : X_2)$. Finally, a perspectivity π is *skew* if the points in which intersects sides of a triangle and their images under π do not colline.

1.2.2 Finite classical polar spaces

The *dual* of $\mathrm{V}(n+1,q)$ is the set of linear functionals

$$\mathrm{V}^*(n+1,q) := \{f \colon \mathrm{V}(n+1,q) \longrightarrow \mathbb{F}_q \mid f \text{ is linear}\}.$$

From a basis $\mathcal{B} = \{e_0,\dots,e_n\}$ of $\mathrm{V}(n+1,q)$ we can construct a basis for $\mathrm{V}^*(n+1,q)$, that is $\mathcal{B}^* = \{e_0^*,\dots,e_n^*\}$, for $e_i^*(e_j) := \delta_{i,j}$ (Kronecker's delta).

Definition 1.78. Let U be a subspace of $\mathrm{V}(n+1,q)$. The *annihilator* of U is

$$U^* := \{f \in \mathrm{V}^*(n+1,q) \mid f(u) = 0, \text{ for all } u \in U\},$$

and it is a $(n+1-\dim(U))$-subspace of $\mathrm{V}^*(n+1,q)$.

The correspondence $U \mapsto U^*$ is a bijection between the subspaces of $\mathrm{V}(n+1,q)$ and those of $\mathrm{V}^*(n+1,q)$. In particular, $U \subset W$ if and only if $W^* \subset U^*$. Let $\mathrm{PG}(V^*)$ or, equivalently, $\mathrm{PG}(n,q)^*$ denote the dual space of $\mathrm{PG}(V)$.

Theorem 1.79 ([44, Proposition 2.5])**.** $\mathrm{PG}(n,q)$ *is isomorphic to* $\mathrm{PG}(n,q)^*$.

Definition 1.80. A collineation between $\mathrm{PG}(n,q)$ and its dual is called a *reciprocity* of $\mathrm{PG}(n,q)$.

Recall that any collineation is induced by a semilinear transformation $\gamma_{\sigma,A} : \mathrm{V}(n+1,q) \to \mathrm{V}^*(n+1,q)$. A reciprocity ρ induced by $\gamma_{\sigma,A}$ maps the point P to the hyperplane AP^σ and maps the hyperplane u to the point $A^{-T}u^\sigma$, where $A^{-T} := (A^{-1})^T$.

Now applying a reciprocity ρ twice one has:

$$P^{\rho^2} = (P^\rho)^\rho = (AP^\sigma)^\rho = A^{-T}A^\sigma P^{\sigma^2},$$

therefore ρ^2 is a map induced by $A^{-T}A^\sigma \in \mathrm{GL}(n+1, q)$ and $\sigma^2 \in \mathrm{Aut}(\mathbb{F}_q)$.

Definition 1.81. A reciprocity ρ of order 2 is called a *polarity* of $\mathrm{PG}(n, q)$. Moreover, if P is a point e H a hyperplane of $\mathrm{PG}(n, q)$, we say that P^ρ is the *polar* of P and H^ρ is the *pole* of H.

Note that for $P, Q \in \mathrm{PG}(n, q)$ the following holds:

$$P \in Q^\rho \iff Q \in P^\rho.$$

Two such points are called *conjugate points.*

Definition 1.82. Let ρ be a polarity of $\mathrm{PG}(n, q)$. A point $P \in \mathrm{PG}(n, q)$ is *totally isotropic* w.r.t. ρ if $P \in P^\rho$.

The notion of conjugates and totally isotropic points is extended to subspaces of any dimension. A totally isotropic subspace has dimension at most $\left\lfloor \frac{n-1}{2} \right\rfloor$.

For every reciprocity ρ of $\mathrm{PG}(n, q)$ induced by a semilinear transformation $\gamma_{\sigma,A}$ we define

$$\beta\colon \mathrm{V}(n+1, q) \times \mathrm{V}(n+1, q) \longrightarrow \mathbb{F}_q, \quad (u, v) \longmapsto u^T\gamma_{\sigma,A}(v) = u^T A v^\sigma. \tag{1.2.1}$$

which is a *σ-sesquilinear form*, that is a map such that

(i) $\beta(u + v, w) = \beta(u, w) + \beta(v, w)$;

(ii) $\beta(u, v + w) = \beta(u, v) + \beta(u, w)$;

(iii) $\beta(au, bv) = a\sigma(b)\beta(u, v)$.

A σ-sesquilinear form is *non-degenerate* if $\beta(u, v) = 0$ for all $v \in \mathrm{V}(n+1, q)$ implies that $u = 0$, and $\beta(u, v) = 0$ for all $u \in \mathrm{V}(n+1, q)$ implies that $v = 0$. Moreover, a σ-sesquilinear form is *reflexive* if $\beta(u, v) = 0$ if and only if $\beta(v, u) = 0$, for all $u, v \in \mathrm{V}(n+1, q)$.

Theorem 1.83 ([44, Lemma 2.6])**.** *Any reciprocity of* $\mathrm{PG}(n, q)$ *arises from a non-degenerate σ-sesquilinear form of* $\mathrm{V}(n+1, q)$ *and vice-versa. In this correspondence, non-degenerate reflexive sesquilinear forms correspond to polarities.*

Theorem 1.83 justifies the following definition.

Definition 1.84. Let β be a (non-degenerate) reflexive sesquilinear form on the vector space $\mathrm{V}(n+1,q)$. In $\mathrm{PG}(n,q)$, the set of totally isotropic subspaces w.r.t. β is called a (non-degenerate) *finite classical polar space.*

From now on we will consider q odd.
When q is square, given a matrix $A=(a_{ij})$, by $A^{\sqrt{q}}$ we denote the matrix $A^{\sqrt{q}} = (a_{ij}^{\sqrt{q}})$. There are three types of polarity:

1. Orthogonal polarity : $\sigma = Id$ and $M^T = M$ (β is a symmetric form);

2. Symplectic polarity: $\sigma = Id$ and $M^T = -M$;

3. Hermitian polarity: $\sigma \neq Id$ and $M^T = M^{\sqrt{q}}$ (β is a Hermitian form).

Two sesquilinear forms β and β' are *equivalent* if there is $\gamma_{\sigma,A} \in \Gamma\mathrm{L}(n,q)$ such that $\beta(\gamma_{\sigma,A}(u), \gamma_{\sigma,A}(v)) = \beta'(u,v)$, for all $u, v \in \mathrm{V}(n+1,q)$.

Let β be a symmetric form. Upon equivalences, the following are the classes of the set of the totally isotropic points (w.r.t. β) and their canonical forms.

1. The *elliptic quadric* $\mathcal{Q}^-(2m+1,q)$, $m \geq 1$ of $\mathrm{PG}(2m+1,q)$:

$$X_1X_2 + \cdots + X_{2m-1}X_{2m} + f(X_{2m+1}, X_{2m+2}) = 0,$$

   where f is a homogeneous irreducible polynomial of degree two over $\mathbb{F}_q$.

2. The *hyperbolic quadric* $\mathcal{Q}^+(2m+1,q)$, $m \geq 1$ of $\mathrm{PG}(2m+1,q)$:

$$X_1X_2 + \cdots + X_{2m-1}X_{2m} + X_{2m+1}X_{2m+2} = 0;$$

3. The *parabolic quadric* $\mathcal{Q}(2m,q)$, $m \geq 1$ of $\mathrm{PG}(2m,q)$:

$$X_1X_2 + \cdots + X_{2m-1}X_{2m} + X_{2m+1}^2 = 0.$$

If β is a Hermitian form of $\mathrm{V}(n+1,q^2)$, up to projectivities, the set of all the totally isotropic points is the *Hermitian variety*, that is given by

$$\mathcal{H}_{n,q^2} : X_0^{q+1} + \cdots + X_n^{q+1} = 0$$

1.2.3 The Natural Embedding Theorem

In this section we state the *Natural Embedding Theorem*, a crucial theorem in the theory of maximal curves [35]. The NET gives an important link between maximal curves and the Hermitian variety.

Theorem 1.85 (Natural Embedding Theorem, [23, Theorem 10.22])**.** *The followings hold.*

- *If $\mathcal{C}$ is $\mathbb{F}_{q^2}$-maximal, then it is $\mathbb{F}_{q^2}$-isomorphic to a curve $\mathcal{D}$ in $\mathrm{PG}(r, \mathrm{K})$, such that $\mathcal{D}$ has degree $q+1$ and lies on a non-degenerate Hermitian variety defined over $\mathbb{F}_{q^2}$ of $\mathrm{PG}(r, \mathrm{K})$. Furthermore, $\mathrm{Aut}_{\mathbb{F}_{q^2}}(\mathcal{C})$ is isomorphic to a subgroup of the projective unitary group $\mathrm{PGU}(r+1, q^2)$.*

- *If $\mathcal{C}$ is $\mathbb{F}_{q^2}$-birational to a curve $\mathcal{D}$ embedded in $\mathrm{PG}(r, \mathrm{K})$ such that $\mathcal{D}$ has degree $q+1$ and lies on a non-degenerate Hermitian variety defined over $\mathbb{F}_{q^2}$ of $\mathrm{PG}(r, \mathrm{K})$, then $\mathcal{C}$ is $\mathbb{F}_{q^2}$-maximal and $\mathcal{C}$ is $\mathbb{F}_{q^2}$-isomorphic to $\mathcal{D}$.*

The following is a corollary to the NET, which will be used in the next part of this thesis to construct new hemisystems arising from maximal curves embedded in the Hermitian surface $\mathcal{H}_{3,q^2}$.

Theorem 1.86 (Corollary to the NET, [34, Result 3.1])**.** *Any algebraic curve $\mathcal{C}$ defined over $\mathbb{F}_{q^2}$ of degree $q+1$ and contained in the non degenerate Hermitian surface $\mathcal{H}_{3,q^2}$ is an $\mathbb{F}_{q^2}$-maximal curve. Furthermore*

- *The intersection divisor $D = \mathcal{I}(\mathcal{H}_{3,q^2}, \Pi_P)$ cut out on $\mathcal{C}$ by the tangent hyperplane Π_P to $\mathcal{H}_{3,q^2}$ at P is*

$$D = \begin{cases} (q+1)P, & \text{for } P \in \mathcal{C}(\mathbb{F}_{q^2}) \\ qP + \Phi(P), & \text{for } P \in \mathcal{C} \setminus \mathcal{C}(\mathbb{F}_{q^2}). \end{cases}$$

- *The tangent line to $\mathcal{C}$ at a point $P \in \mathcal{C}(\mathbb{F}_{q^2})$ is also a tangent line to $\mathcal{H}_{3,q^2}$ at P, and it has no further common point with $\mathcal{H}_{3,q^2}$.*

1.2.4 Configurations of point-line sets

This subsection is devoted to introduce some considerable configurations of points and lines within either a finite projective space or a finite classical polar space.

m-ovoids and m-regular systems

Definition 1.87. A *generator* of a polar space $\mathcal{P}$ is a maximal dimension totally isotropic subspace of $\mathcal{P}$.

Any two generators have the same dimension and this common vector space dimension is called the *rank* of $\mathcal{P}$.

Definition 1.88. A set of points $\mathcal{O}$ of $\mathcal{P}$ is an m-ovoid if each generator of $\mathcal{P}$ meets $\mathcal{O}$ in m points.

We are interested in m-ovoids of $\mathcal{P}$, when $\mathcal{P}$ is the polar space of elliptic quadrics $\mathcal{Q}^-(5,q)$. The following theorem is due to Segre [45].

Theorem 1.89. *Let $\mathcal{O}$ be a non trivial m-ovoid of $\mathcal{Q}^-(5,q)$. Then q is odd and $m=(q+1)/2$.*

The Klein map gives a bijective correspondence between lines of $\mathrm{PG}(3,q^2)$ and points of $\mathcal{Q}^+(5,q^2)$. In this setting the lines of a Hermitian surface $\mathcal{H}(3,q^2)$ of $\mathrm{PG}(3,q^2)$ are mapped bijectively to the points of an elliptic quadric $\mathcal{Q}^-(5,q)$ contained in a subgeometry $\Sigma \simeq \mathrm{PG}(5,q)$ such that $\Sigma \cap \mathcal{Q}^+(5,q^2) = \mathcal{Q}^-(5,q)$. Moreover the $q+1$ generators of $\mathcal{H}(3,q^2)$ through a point are mapped to the points of a line of $\mathcal{Q}^-(5,q)$. Therefore there is a bijective correspondence between points of $\mathcal{H}(3,q^2)$ and lines of $\mathcal{Q}^-(5,q)$. Hence it follows that a pointset $\mathcal{O}$ of $\mathcal{Q}^-(5,q)$ having the property that every line of $\mathcal{Q}^-(5,q)$ has m points in common with $\mathcal{O}$, i.e., an m-ovoid of $\mathcal{Q}^-(5,q)$, is equivalent to a lineset $\mathcal{L}$ of $\mathcal{H}(3,q^2)$ such that through each point of $\mathcal{H}(3,q^2)$ there pass m lines of $\mathcal{L}$.

Definition 1.90. A set of lines $\mathcal{L}$ of a polar space $\mathcal{P}$ is an *m-regular system* if through each point of $\mathcal{P}$ there pass m lines of $\mathcal{L}$.

From Theorem 1.89 the only possible case for an m-regular system of $\mathcal{H}_{3,q^2}$ is $m=(q+1)/2$. We will call the latter set of lines a *hemisystem* of the Hermitian surface.

More precisely, a line of $\mathrm{PG}(3,q^2)$ entirely contained in $\mathcal{H}_{3,q^2}$ is a generator of $\mathcal{H}_{3,q^2}$. The total number of generators of $\mathcal{H}_{3,q^2}$ is $(q^3+1)(q+1)$ and through any point $P \in \mathcal{H}_{3,q^2}$ there exists exactly $q+1$ generators and they are the intersection of $\mathcal{H}_{3,q^2}$ with its tangent plane at P. Thus a hemisystem of $\mathcal{H}_{3,q^2}$ consists of $\frac{1}{2}(q^3+1)(q+1)$ generators of $\mathcal{H}_{3,q^2}$, exactly $\frac{1}{2}(q+1)$ for each point of $\mathcal{H}_{3,q^2}$.

Blocking sets

For a given nonempty subset $\mathcal{L}$ of the lineset of $\mathrm{PG}(2,q)$, a *blocking set* w.r.t. $\mathcal{L}$ (or simply, an $\mathcal{L}$-blocking set) is a subset B of the pointset of $\mathrm{PG}(2,q)$ such that every line of $\mathcal{L}$ contains at least one point of B. An $\mathcal{L}$-blocking set is said to be *minimal* if no proper subset of it blocks all the lines of $\mathcal{L}$.

Blocking sets of $\mathrm{PG}(2,q)$ with respect to considerable sets of lines have been studied by several authors. The first step in this regard has been to determine the cardinality of a blocking set and, if possible, to describe all the blocking sets of that size.

In Chapter 3 we will study a particular blocking set involving an irreducible conic in $\mathrm{PG}(2,q^2)$. More precisely, given an irreducible conic $\mathcal{C}$ defined over $\mathrm{PG}(2,q^2)$ and given a Baer subplane $\mathcal{B} \subset \mathrm{PG}(2,q^2)$, we will investigate the cardinality of the blocking set $\mathcal{B} \cap (E_q(\mathcal{C}) \cup \mathcal{C})$, where $E_q(\mathcal{C})$ is the set of external points to $\mathcal{C}$. The set $\mathcal{B} \cap (E_q(\mathcal{C}) \cup \mathcal{C})$ is a blocking set w.r.t. the tangent lines to $\mathcal{C}$.

Chapter 2

Hemisystems from maximal curves

In Chapter 1, we have seen that the Hermitian surface $\mathcal{H}_{3,q^2}$ of $\mathrm{PG}(3,q^2)$ is the set of all totally isotropic points of a non-degenerate unitary polarity of $\mathrm{PG}(3,q^2)$.

The approach introduced in [34] relies on the Fuhrmann-Torres curve over $\mathrm{PG}(3,q^2)$ naturally embedded in $\mathcal{H}_{3,q^2}$. Their construction provided a hemisystem of $\mathcal{H}_{3,q^2}$ whenever $q=p$ is a prime of the form $p=1+4a^2$ for an even integer a. In this thesis we investigate the analog construction for $p=1+4a^2$ with an odd integer a, and show that it produces a hemisystem, as well, for every such p. We mention that a prime number p of the form $p=1+4a^2$ with an integer a is called a Landau number. If Landau's conjecture is true, that is there exist infinitely many Landau numbers, then an infinite family of hemisystems is obtained.

Our main result is stated in the following theorem.

Theorem 2.1 ([43, Theorem 1.1])**.** *Let p be a prime number where $p=1+4a^2$ for some integer a. Then there exists a hemisystem in the Hermitian surface $\mathcal{H}_{3,q^2}$ of $\mathrm{PG}(3,p^2)$ which is left invariant by a subgroup of $\mathrm{PGU}(4,p)$ isomorphic to $\mathrm{PSL}(2,p)\times C_{\frac{p+1}{2}}$, the cyclic group of order $\frac{p+1}{2}$.*

2.1 Hemisystems and maximal curves

In Chapter 1 we have seen that the canonical form of $\mathcal{H}_{3,q^2}$ is

$$X_0^{q+1}+X_1^{q+1}+X_2^{q+1}+X_3^{q+1}=0.$$

The group of projectivities preserving $\mathcal{H}_{3,q^2}$ is isomorphic to the projective unitary group $\mathrm{PGU}(4,q)$ and it acts on the points $\mathcal{H}_{3,q^2}$ as a 2-transitive permutation group [23]. The number of points of $\mathcal{H}_{3,q^2}$ is $(q^2+1)(q^3+1)$. A hemisystem of $\mathcal{H}_{3,q^2}$ consists of $\frac{1}{2}(q^3+1)(q+1)$ generators of $\mathcal{H}_{3,q^2}$, exactly $\frac{1}{2}(q+1)$ of them through each point of $\mathcal{H}_{3,q^2}$. Up to a change of the projective frame in $\mathrm{PG}(3,q^2)$, the equation of $\mathcal{H}_{3,q^2}$ may also be written in the form

$$\mathcal{H}_{3,q^2}\colon X_1^{q+1}+2X_2^{q+1}-X_3^qX_0-X_3X_0^q=0.$$

Our aim is to use the Natural Embedding Theorem to construct new families of hemisystems on $\mathcal{H}_{3,q^2}$. In $\mathrm{PG}(2,\overline{\mathbb{F}}_q)$ with homogeneous coordinates $(X:Y:Z)$, the Fuhrmann-Torres curve is the plane curve $\mathcal{F}^+$ of genus $\frac{1}{4}(q-1)^2$ with equation

$$\mathcal{F}^+\colon Y^q-YZ^{q-1}=X^{\frac{q+1}{2}}Z^{\frac{q-1}{2}}.$$

The morphism

$$\varphi\colon \mathcal{F}^+\to \mathrm{PG}(3,\overline{\mathbb{F}}_q),\quad (X:Y:Z)\mapsto (Z^2:XZ:YZ:Y^2)$$

defines an embedding (called natural embedding) of $\mathcal{F}^+$ which is a $q+1$ degree curve $\mathcal{X}^+$ whose points (including those defined over $\overline{\mathbb{F}}_q$) are contained in $\mathcal{H}_{3,q^2}$. In particular, $\mathcal{F}^+$ is an $\mathbb{F}_{q^2}$-maximal curve. The twin Fuhrmann-Torres curve is defined by the equation

$$\mathcal{F}^-\colon Y^q-YZ^{q-1}=-X^{\frac{q+1}{2}}Z^{\frac{q-1}{2}}.$$

and the above claims remain valid with respect to the same morphism. For more details see [16].

Some useful properties of the Fuhrmann-Torres curve, also valid for any $\mathbb{F}_{q^2}$-maximal curve $\mathcal{X}$ naturally embedded in $\mathcal{H}_{3,q^2}$, can be found in [34, Sections 2,3,4].

In particular, $\mathcal{X}^+$ is a $q+1$ degree curve lying in the Hermitian surface $\mathcal{H}_{3,q^2}$. Furthermore $\mathcal{X}^+(\mathbb{F}_{q^2})$ is partitioned in Ω and $\mathcal{X}^+(\mathbb{F}_{q^2})\setminus\Omega=\Delta^+$, where Ω is the set cut out on $\mathcal{X}^+$ by the plane $\pi\colon X_1=0$. Note that $|\Omega|=q+1$ and $|\Delta^+|=\frac{1}{2}(q^3-q)$.

Equivalently Ω is the intersection in π of the conic $\mathcal{C}$ with equation $X_0X_3-X_2^2=0$ and the Hermitian curve $\mathcal{H}(2,q^2)$ with equation $X_0^qX_3+X_0X_3^q-2X_2^{q+1}=0$. Moreover, the above properties hold true for when $^+$ is replaced by $^-$ and $\mathcal{X}^-$ is the natural embedding of the plane curve $\mathcal{F}^-$. The curves $\mathcal{X}^+$ and $\mathcal{X}^-$ are isomorphic over $\mathbb{F}_{q^2}$ and Ω is the set of common points of $\mathcal{X}^+$ and $\mathcal{X}^-$.

We use classical terminology regarding maximal curves. In particular, a (*real*) *chord* of $\mathcal{X}$ is a line in $\mathrm{PG}(3,q^2)$ which meets $\mathcal{X}(\mathbb{F}_{q^2})$ in at least two distinct point, whereas an *imaginary chord* of $\mathcal{X}$ is a line in $\mathrm{PG}(3,q^2)$ joining a point $P \in \mathcal{X}(\mathbb{F}_{q^4}) \setminus \mathcal{X}(\mathbb{F}_{q^2})$ to its conjugate, that is, its Frobenius image.

The key point of the construction below is the following corollary to the NET.

Lemma 2.2 ([34, Lemma 3.4]). *Let $\mathcal{C}$ be an $\mathbb{F}_{q^2}$-maximal curve naturally embedded in the Hermitian surface $\mathcal{H}_{3,q^2}$. Then*

(i) No two distinct points in $\mathcal{C}(\mathbb{F}_{q^2})$ are conjugate under the unitary polarity associated with $\mathcal{H}_{3,q^2}$.

(ii) Any imaginary chord of $\mathcal{C}$ is a generator of $\mathcal{H}_{3,q^2}$ which is disjoint from $\mathcal{C}$.

(iii) For any point $P \in \mathcal{H}_{3,q^2}$ in $\mathrm{PG}(3,q^2)$, if $P \notin \mathcal{C}(\mathbb{F}_{q^2})$ and Π_P is the tangent plane to $\mathcal{H}_{3,q^2}$ at P, then $\Pi_P \cap \mathcal{C}$ consists of $q+1$ pairwise distinct points which are in $\mathcal{C}(\mathbb{F}_{q^4})$.

2.2 The Fuhrmann-Torres construction

From now on let q be a prime $p \equiv 1 \pmod 4$ and let $\mathcal{X}$ be an $\mathbb{F}_{q^2}$-maximal curve. Denote by N_{q^2} the number of $\mathbb{F}_{q^2}$-rational points of $\mathcal{X}$.

Let $\mathcal{H}$ denote the set of all imaginary chords of $\mathcal{X}$. Furthermore, for a point $P \in \mathrm{PG}(3,q^2)$ lying in $\mathcal{H}_{3,q^2} \setminus \mathcal{X}(\mathbb{F}_{q^2})$, let $n_P(\mathcal{X})$ denote the number of generators of $\mathcal{H}_{3,q^2}$ through P which contain an $\mathbb{F}_{q^2}$-rational point of $\mathcal{X}$.

Definition 2.3. A set $\mathcal{M}$ of generators of $\mathcal{H}_{3,q^2}$ is an *half-hemisystem* on $\mathcal{X}$ if the following properties hold:

(A) Each $\mathbb{F}_{q^2}$-rational points of $\mathcal{X}$ is incident with exactly $\frac{1}{2}(q+1)$ generators in $\mathcal{M}$.

(B) For any point $P \in \mathcal{H}_{3,q^2} \setminus \mathcal{X}(\mathbb{F}_{q^2})$ lying in $\mathrm{PG}(3,q^2)$, $\mathcal{M}$ has as many as $\frac{1}{2}n_P(\mathcal{X})$ generators through P which contain an $\mathbb{F}_{q^2}$-rational point of $\mathcal{X}$.

Note that $\mathcal{M}$ consists of $\frac{1}{2}(q+1)N_{q^2}$ generators and $\mathcal{H}$ of $\frac{1}{2}(q^2+q)(q^2-q-2g(\mathcal{X}))$ generators of $\mathcal{H}_{3,q^2}$. Therefore $\mathcal{M} \cup \mathcal{H}$ has exactly $\frac{1}{2}(q^3+1)(q+1)$ generators of $\mathcal{H}_{3,q^2}$.

Result 2.4 ([34, Proposition 4.1]). *$\mathcal{M} \cup \mathcal{H}$ is a hemisystem of $\mathcal{H}_{3,q^2}$.*

Let $\mathfrak{G}$ be a subgroup of $\mathrm{Aut}(\mathcal{X})$ and $o_1, \ldots, o_r$ be the $\mathfrak{G}$-orbits on $\mathcal{X}(\mathbb{F}_{q^2})$. Let $\mathcal{G}$ be the set of all generators meeting $\mathcal{X}^+$. Moreover, for $1 \leq j \leq r$, let $\mathcal{G}_j$ denote the set of all generators of $\mathcal{H}_{3,q^2}$ meeting o_j. Note that $\mathfrak{G}$ leaves each $\mathcal{G}_j$ invariant.

Result 2.5 ([34, Proposition 4.2]). *With the above notation, assume that the subgroup $\mathfrak{G}$ fulfills the hypothesis:*

(C) $\mathfrak{G}$ has a subgroup $\mathfrak{h}$ of index 2 such that $\mathfrak{G}$ and $\mathfrak{h}$ have the same orbits $o_1, \ldots, o_r$ on $\mathcal{X}(\mathbb{F}_{q^2})$.

(D) For any $1 \leq j \leq r$, $\mathfrak{G}$ acts transitively on $\mathcal{G}_j$ while $\mathfrak{h}$ has two orbits on $\mathcal{G}_j$.

Let $P \notin \mathcal{X}(\mathbb{F}_{q^2})$ be a point lying on a generator in $\mathcal{G}$, if

(E) there is an element in $\mathfrak{G}_P$ not in $\mathfrak{h}_P$,

then P satisfies (B).

From [34, Lemma 5.1] $\mathcal{G}$ is also the set of all generators meeting $\mathcal{X}^-$. In particular, $\mathcal{G}$ splits into two subset

$$\mathcal{G} = \mathcal{G}_1 \cup \mathcal{G}_2, \tag{2.2.1}$$

where $\mathcal{G}_2$ is the set of the $(q+1)^2$ generators meeting Ω, while $\mathcal{G}_1$ is the set of the $\frac{1}{2}(q^3-q)(q+1)$ generators meeting both Δ^+ and Δ^-. Thus, the following characterization of $\mathcal{G}$ is very useful.

Result 2.6 ([34, Lemma 5.3]). *The generator set $\mathcal{G}_1$ consists of all the lines $g_{u,v,s,t}$ spanned by the points $P_{u,v} = (1 : u : v : v^2) \in \Delta^+$ and $Q_{s,t} = (1 : s : t : t^2) \in \Delta^-$ such that*

$$\mathcal{F}\colon\, F(v,t) = (v+t)^{q+1} - 2(vt + (vt)^q) = 0$$

and

$$u^{\frac{q+1}{2}} = v^q - v, \quad -s^{\frac{q+1}{2}} = t^q - t, \quad u^q s = (t - v^q)^2.$$

Result 2.7 ([34, Lemma 5.4]). $\mathrm{Aut}(\mathcal{F})$ *contains a subgroup* $\Psi \cong \mathrm{PGL}(2,q)$ *that acts faithfully on the set $\mathcal{F}(\mathbb{F}_{q^2}) \setminus \mathcal{F}(\mathbb{F}_q)$ as a sharply transitive permutation group.*

2.3 Automorphisms preserving $\mathcal{G}$ and $\mathcal{X}^+$

In this subsection we recall the main results about the group-theoretic properties involving, $\mathcal{X}^+$, $\mathcal{X}^-$ and $\mathcal{G}$; see [34, Section 5]. The authors showed that Ψ contains a subgroup Γ which acts sharply transitively on $\mathcal{G}_1$. Furthermore, Γ has a unique index 2 subgroup Φ such that

$$\Phi \cong PSL(2,q) \times C_{\frac{q+1}{2}}.$$

In particular, Φ has two orbits on $\mathcal{G}_1$, namely $\mathcal{M}_1$ and $\mathcal{M}_2$.

In terms of subgroups of $\mathrm{PGU}(4,q)$ we have the following characterization.

Result 2.8 ([34, Lemma 5.7]). *The group* $\mathrm{PGU}(4,q)$ *has a subgroup* $\mathfrak{G}$ *with the following properties:*

(i) $\mathfrak{G}$ *is an automorphism group of* $\mathcal{X}^+$ *and* $\mathcal{X}^-$*;*

(ii) $\mathfrak{G}$ *preserves the point-sets* Δ^+, Δ^-, Ω *and* $\mathcal{G}_1$*;*

(iii) $\mathfrak{G}$ *acts faithfully on* Δ^+, Δ^- *and* $\mathcal{G}_1$*;*

(iv) the collineation group induced by $\mathfrak{G}$ *on* π *is* $\mathfrak{G}/Z(\mathfrak{G}) \cong \mathrm{PGL}(2,q)$ *with* $Z(\mathfrak{G}) \cong C_{\frac{q+1}{2}}$*;*

(v) the permutation representation of $\mathfrak{G}$ *on* $\mathcal{G}_1$ *is* Γ*; in particular* $\mathfrak{G} \cong \Gamma$*;*

(vi) $\mathfrak{G}/Z(\mathfrak{G})$ *acts on* Ω *as* $\mathrm{PGL}(2,q)$ *in its* 3*-transitive permutation representation.*

Furthermore, $\mathfrak{G}$ *has an index* 2 *subgroup* $\mathfrak{h}$ *isomorphic to* $\mathrm{PSL}(2,q) \times C_{\frac{q+1}{2}}$.

With the above notation, in the isomorphism $\mathfrak{G} \cong \Gamma$, $\mathfrak{h}$ and Φ correspond.

Result 2.9 ([34, Lemma 5.9]). *The elements of order* 2 *in* $\mathfrak{h}$ *are skew perspectivities, while those in* $\mathfrak{G} \setminus \mathfrak{h}$ *are homologies. Furthermore, the linear collineation* $\mathfrak{w}$*, defined by*

$$\mathbf{W} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

interchanges $\mathcal{X}^+$ *with* $\mathcal{X}^-$ *and the linear group generated by* $\mathfrak{G}$ *and* $\mathfrak{w}$ *is the direct product* $\mathfrak{G} \times \langle \mathfrak{w} \rangle$.

Result 2.10 ([34, Lemma 5.11]). *]* $\mathfrak{G}$ *acts transitively on* $\mathcal{G}_2$ *while* $\mathfrak{h}$ *has two orbits on* $\mathcal{G}_2$.

From the result of this section, the following theorem follows

Theorem 2.11 ([34, Theorem 5.13]). *] Conditions* (C) *and* (D) *are fulfilled for* $\mathcal{X} = \mathcal{X}^+$*, with* $\Gamma = \mathfrak{G}$ *and* $\Phi = \mathfrak{h}$.

More precisely, $\mathcal{G} = \mathcal{G}_1 \cup \mathcal{G}_2$ with $\mathcal{G}_1 = \mathcal{M}_1 \cup \mathcal{M}'_1$ and $\mathcal{G}_2 = \mathcal{M}_2 \cup \mathcal{M}'_2$, where $\mathcal{G}_1$ and $\mathcal{G}_2$ are the $\mathfrak{G}$-orbits on $\mathcal{G}$ whereas $\mathcal{M}_1$, $\mathcal{M}'_1$, $\mathcal{M}_2$, $\mathcal{M}'_2$ are the $\mathfrak{h}$-orbits on $\mathcal{G}_1$ and $\mathcal{G}_2$ respectively. This notation fits with [34, Section 5].

2.4 Points satisfying Condition (E)

The plane $\pi\colon X_1 = 0$ can be seen as the projective plane $\mathrm{PG}(2, q^2)$, with homogeneous coordinates $(X_0 : X_2 : X_3)$. Then $\mathcal{C}$ is the conic of equation $X_0X_3 - X_2^2 = 0$ and Ω is the set of points of $\mathcal{C}$ lying in the (canonical Baer) subplane $\mathrm{PG}(2, q)$.

The points in $\mathrm{PG}(2, q^2) \setminus \mathrm{PG}(2, q)$ are of three types with respect to the lines of $\mathrm{PG}(2, q)$, i.e.

(I) points of a unique line disjoint from Ω which meets $\mathcal{C}$ in two distinct points both in $\mathrm{PG}(2, q^2) \setminus \mathrm{PG}(2, q)$;

(II) points of a unique line meeting Ω in two distinct points;

(III) points of a unique line which is tangent to $\mathcal{C}$ with tangency point of Ω.

Points of type (I) - (II) and points in $\mathrm{PG}(2, q)$ satisfy condition (B), as can be readily seen in the next result.

Result 2.12 ([34, Theorem 6.1])**.** *] If the projection of $P \in \mathcal{H}_{3,q^2}$ on π is a point P' of type* (I) - (II) *or $P' \in \mathrm{PG}(2, q)$, then condition* (E) *is fulfilled for $\mathcal{X} = \mathcal{X}^+$, $\Gamma = \mathfrak{G}$ and $\Phi = \mathfrak{h}$.*

2.5 Condition (B) for case (III) and $p \equiv 5 \pmod 8$

Condition (B) is not always satisfied in Case (III), that is, for points P whose projection from $X_\infty = (0, 1, 0, 0)$ on π is a point P' lying on a tangent l to $\mathcal{C}$. Our goal is to show that [34, Theorem 7.1], proven for $p \equiv 1 \pmod 8$, remains true for

$$p \equiv 5 \pmod 8,$$

extending their results to the case $p \equiv 1 \pmod 4$.

For this reason, from now on, we assume q be a prime $p \equiv 5 \pmod 8$.

Theorem 2.13. *Condition (B) for Case (III) is satisfied if and only if the number N_q of $\mathbb{F}_q$-rational points of the elliptic curve with affine equation $Y^2 = X^3 - X$ equals* *either* $q-1$, *or* $q+3$.

We need few steps before to prove Theorem 2.13. To begin with, we have to prove the following theorem.

Theorem 2.14. *Let* n_q *be the number of* $\xi \in \mathbb{F}_q$ *for which* $f(\xi) = \xi^4 - 48\xi^2 + 64$ *is a square in* $\mathbb{F}_q$. *Condition* (*B*) *for Case* (*III*) *is satisfied if and only if* n_q *equals either* $\frac{1}{2}(q+1)$ *or* $\frac{1}{2}(q-3)$.

The proof of Theorem 2.14 is carried out by a series of lemmas.

Since $q \equiv 5 \pmod 8$, 2 is not a square in $\mathbb{F}_q$. Therefore the proof is carried out differently.

Let h and $-h$ be the square roots of 2 in $\mathbb{F}_{q^2}$. In particular we have that $h^q + h = 0$ and $(\pm h)^{q+1} = -2$. Moreover h is a non-square in $\mathbb{F}_{q^2}$.

Moreover $h^{(q-1)/2} = \alpha$, with $\alpha^2 = -1$. Thus, $\alpha \notin \square_q$ and $(1+\alpha)(1-\alpha) = 2 \notin \square_q$.

Since $\mathfrak{G}$ is transitive on Ω, the point $O = (1:0:0:0)$ may be assumed to be the tangency point of l. Then l has equation $X_1 = 0, X_3 = 0$, and $P = (a_0 : a_1 : a_2 : 0)$ with $a_1 \neq 0$ and $a_1^{q+1} + 2a_2^{q+1} = 0$. If $a_0 = 0$ then $P = (0 : d : 1 : 0)$ with $d^{q+1} + 2 = 0$ and his projection to $\pi\colon X_1 = 0$ is $P' = (0:1:0)$, which is a point in $\mathrm{PG}(2,q)$. By Result 2.12 the case $a_0 = 0$ can be dismissed and $a_0 = 1$ may be assumed.

Therefore, after the dehomogenization with respect to X_0, consider the affine coordinates (X, Y, Z) for a point in $\mathrm{PG}(3, q^2)$.
We may limit ourselves to a point $P = (a, b, 0)$ such that $a^{q+1} + 2b^{q+1} = 0$. The latter equation holds for $a = \pm h^2$ and $b = h$. Then we may chose

$$P = (2\varepsilon, h, 0), \qquad \text{where } \varepsilon \in \{-1, 1\}$$

and we can carry out the case $\varepsilon = 1$ and $\varepsilon = -1$ simultaneously.

2.5.1 Case of $\mathcal{G}_1$

We keep up our notation $P_{u,v} = (u, v, v^2)$ for a point in Δ^+. The following lemmas are analogous to those in [34, section 7.1].

Lemma 2.15. *Let* $v \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. *Then there exists* $u \in \mathbb{F}_{q^2}$ *such that the line joining*

P at $P_{u,v}$ is a generator of $\mathcal{H}_{3,q^2}$ if and only if

$$(v^2+2hv)^{\frac{q+1}{2}} = 2\varepsilon(v^q - v). \tag{2.5.1}$$

If (2.5.1) *holds, then u is uniquely determined by v.*

Proof. The line $l = PP_{u,v}$ is a generator if and only if $P_{u,v}$ lies on the tangent plane to $\mathcal{H}_{3,q^2}$ at P. This implies

$$u = \frac{v^2+2hv}{2\varepsilon}. \tag{2.5.2}$$

and since $P_{u,v} \in \Delta^+$ then $u^{\frac{q+1}{2}} = v^q - v$ and l is a generator. The converse follows from the proof of [34, Lemma 7.4]. □

Lemma 2.5.1 can be extended to $Q_{s,t} \in \Delta^-$ provided that u, v are replaced by s, t and Equations (2.5.1), (2.5.2) by

$$(t^2+2ht)^{\frac{q+1}{2}} = -2\varepsilon(t^q - t) \tag{2.5.3}$$

and

$$s = \frac{t^2+2ht}{2\varepsilon}. \tag{2.5.4}$$

Furthermore $P, P_{u,v}$ and $Q_{s,t}$ are collinear if and only if

$$\begin{cases} 2\varepsilon(t^2-v^2) = t^2u - v^2s, \\ vt - h(v+t) = 0. \end{cases} \tag{2.5.5}$$

Thereefore, the following lemma holds.

Lemma 2.16. *Let $v, t \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ with $F(v,t) = 0$. If the line through $P_{u,v} \in \Delta^+$ and $Q_{s,t} \in \Delta^-$ is a generator through P, then*

$$vt - h(v+t) = 0 \tag{2.5.6}$$

holds.

We now count the number of generator in $\mathcal{G}_1$ which pass through P.

Lemma 2.17. *Equation* (2.5.1) *has exactly $\frac{1}{2}(q+1)$ solution in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$.*

Proof. Let $r = vh^{-1}$. We obtain:

$$(r^2+2r)^{\frac{q+1}{2}} = \varepsilon h(r^q + r).$$

Hence,

$$(r^2+2r)^{\frac{q^2-1}{2}} = -1$$

and then $r^2 + 2r$ is a non-square of $\mathbb{F}_{q^2}$. Thus, there exists $z \in \mathbb{F}_{q^2}{}^*$ such that $r^2 + 2r = hz^2$. Now the system is

$$\begin{cases} hz^2 = r^2 + 2r \\ \alpha h z^{q+1} = \varepsilon h(r^q + r) \end{cases} \tag{2.5.7}$$

where $\alpha = h^{(q-1)/2}$. Let $\lambda = zr^{-1}$, so that

$$\begin{cases} h\lambda^2 r = r + 2, \\ \alpha(\lambda r)^{q+1} = \varepsilon(r^q + r). \end{cases} \tag{2.5.8}$$

Since $r = 2/(h\lambda^2 - 1)$ we obtain

$$4\alpha\lambda^{q+1} - 2\varepsilon(h\lambda^2 - 1) - 2\varepsilon(h\lambda^2 - 1)^q = 0. \tag{2.5.9}$$

Now if $\lambda = \lambda_1 + h\lambda_2$, with λ_1, $\lambda_2 \in \mathbb{F}_q$, Equation (2.5.9) reads

$$\alpha\lambda_1^2 - 2\alpha\lambda_2^2 - 4\varepsilon\lambda_1\lambda_2 + 4\varepsilon = 0. \tag{2.5.10}$$

Since the determinant of the matrix of the quadratic form associated to (2.5.10) is -8ε, that quadratic form is the equation of an irreducible conic of $\mathrm{PG}(2, q)$. Thus, we have exactly $q+1$ solutions λ of (2.5.9): if λ is a solution, then $-\lambda$ is too, hence we have $\frac{q+1}{2}$ values for both r and v.

Every solution v of (2.5.1) is in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. In fact, if $(hr)^q = hr$ then $r^q = -r$ and $\lambda r = 0$, which contradicts the first equation of (2.5.8). □

Let $\alpha = h^{\frac{q-1}{2}}$. Note that α is a non-square of $\mathbb{F}_q$.

Lemma 2.18. *For every solution $v = v_1 + hv_2$ of* (2.5.1),

$$\varepsilon v_2 + \frac{\alpha}{2}(v_1 v_2 + v_1) \notin \square_q.$$

Proof. Consider System (2.5.7) and let $z = z_1 + hz_2$ and $r = r_1 + hr_2$. Then

$$\begin{cases} z_1^2 + 2z_2^2 = 2r_1r_2 + 2r_2 \\ \alpha z_1^2 - 2\alpha z_2^2 = 2\varepsilon r_1. \end{cases} \tag{2.5.11}$$

Summing the two equations we have:

$$\alpha z_1^2 = \alpha r_2(r_1 + 1) + \varepsilon r_1.$$

Since $\alpha^2 = -1$ and $q \equiv 5 \pmod 8$, it follows $\alpha \notin \square_q$ and then

$$\alpha r_2(r_1 + 1) + \varepsilon r_1$$

is a non-square of $\mathbb{F}_q$. With $v_2 = r_1$ and $v_1 = 2r_2$ we obtain

$$\varepsilon v_2 + \frac{\alpha}{2}(v_1v_2 + v_1) \notin \square_q.$$

□

Our next step is to characterize the generators of $\mathcal{G}_1$ through P.

To begin with, we need some notions of number theory, which would allow us to simplify the notation we will use. Note that $(2 + h)^{\frac{q+1}{2}} = \lambda h$, where,

$$\lambda = (2 + h)^{\frac{q+1}{2}} h^{-1} = [(1 + h)h]^{\frac{q+1}{2}} h^{-1} = (1 + h)^{\frac{q+1}{2}} h^{\frac{q-1}{2}}. \tag{2.5.12}$$

Since

$$\lambda^2 = (1 + h)^{q+1} 2^{\frac{q-1}{2}} = (1 + h)(1 - h)(-1) = 1,$$

we have $\lambda = \pm1$. Applying the Frobenius map to (2.5.12) gives

$$\lambda = (1 - h)^{\frac{q+1}{2}} (-h)^{\frac{q-1}{2}}.$$

Hence λ is independent of the choice of h as a square root of 2.

Proposition 2.19. *We have*

$$\lambda = \begin{cases} 1, & q \equiv 13 \pmod{16} \\ -1, & q \equiv 5 \pmod{16} \end{cases}$$

Proof. See Appendix A. □

Let

$$\chi := \begin{cases} -1, \text{ if either } \varepsilon = 1 \text{ and } q \equiv 13 \pmod{16} \text{ or } \varepsilon = -1 \text{ and } q \equiv 5 \pmod{16} \\ 1, \text{ if either } \varepsilon = 1 \text{ and } q \equiv 5 \pmod{16} \text{ or } \varepsilon = -1 \text{ and } q \equiv 13 \pmod{16} \end{cases}$$

Furthermore,

$$v_0 := -2(h - 2\chi), \quad u_0 := \frac{4}{\varepsilon}(2 - h\chi)$$

and

$$t_0 := -2(h + 2\chi), \quad s_0 := \frac{4}{\varepsilon}(2 + h\chi)$$

Since $h = \varepsilon(2 + \chi h)^{\frac{q+1}{2}}$,

$$v_0^q - v_0 = 4h = u_0^{\frac{q+1}{2}} \tag{2.5.13}$$

and

$$u_0^q s_0 = 16(2 - h\chi)^2 = (t_0 - v_0^q)^2.$$

Furthermore,

$$(v_0 + t_0)^{q+1} = -32 = 2(t_0 v_0 + (t_0 v_0)^q)$$

Therefore, $F(v_0, t_0) = 0$. Thus, from Result 2.6, the line trough P_{u_0,v_0} and Q_{s_0,t_0} is a generator $g_0 \in \mathcal{G}_1$. Moreover the following hold:

$$u_0 = \frac{v_0^2 + 2hv_0}{2\varepsilon}, \quad s_0 = \frac{t_0^2 + 2ht_0}{2\varepsilon}$$

showing that g_0 pass through P.

We show how each generator g passing through P can be obtained from g_0. If $g = P_{u,v}Q_{s,t}$ is a line through P, then, by Lemma 2.16, $F(v,t) = 0$ and $vt = h(v+t)$. Now for α, β, γ and $\delta \in \mathbb{F}_q$, with $\alpha\delta - \beta\gamma \neq 0$, write

$$v = \frac{\alpha v_0 + \beta}{\gamma v_0 + \delta}, \quad t = \frac{\alpha t_0 + \beta}{\gamma t_0 + \delta}.$$

From $v_0 t_0 = -8$ and $v_0 + t_0 = -4h$, we may write Equation (2.5.6) as

$$\begin{aligned} 8\alpha\gamma &= 2\alpha\beta + \beta\delta, \\ \beta^2 &= 8(\alpha^2 - \alpha\delta - \beta\gamma). \end{aligned} \tag{2.5.14}$$

Our aim is to show that these equations hold if and only if α, β, γ and δ depend on a unique parameter $\xi \in \mathbb{F}_q \cup \{\infty\}$. To begin with, let $\delta \neq 0$. Then $\alpha \neq 0$. The first equation in (2.5.14) forces

$$\gamma = \frac{(2\alpha+1)\beta}{8\alpha}.$$

Together with the other equation, we have

$$8\alpha^3 - 3\alpha\beta^2 - 8\alpha^2 - \beta^2 = 0.$$

Let $\xi = \beta\alpha^{-1}$. This implies $\alpha^2(8\alpha - 3\alpha\xi^2 - 8 - \xi^2) = 0$. Therefore

$$\alpha = \frac{\xi^2+8}{8-\xi^2},$$

and the assertion follows for $\delta \neq 0$. For $\delta = 0$ we may assume $\beta = 1$. If $\alpha \neq 0$ then $\gamma = 1/4$ and $8\alpha^2 = -1$, which is impossible as -1 is a square in $\mathbb{F}_q$ while 8 is not. When $\delta = \alpha = 0$ and $\beta = 1$, then $\gamma = \frac{-1}{8}$.

Therefore,

$$v = v_\xi = \frac{(\xi^2+8)v_0 + (\xi^2+8)\xi}{\frac{\xi}{8}(-\xi^2+24)v_0 + 8 - 3\xi^2}, \quad v_\infty = \frac{1}{-\frac{1}{8}v_0} = -2(h+2\chi). \tag{2.5.15}$$

Let A_ξ and A_∞ be two matrices in $GL(2, \mathrm{K})$ representing the fractional linear maps v_ξ and v_∞. Thus,

$$\det(A_\xi) = \frac{(\xi^2+8)(\xi^4 - 48\xi^2 + 64)}{8}, \quad \det(A_\infty) = (8)^{-1}. \tag{2.5.16}$$

These equations remains true for t_0 and t:

$$t = t_\xi = \frac{(\xi^2+8)t_0 + (\xi^2+8)\xi}{\frac{\xi}{8}(-\xi^2+24)t_0 + 8 - 3\xi^2}, \quad t_\infty = \frac{1}{-\frac{1}{8}t_0} = -2(h - 2\mathcal{X}). \tag{2.5.17}$$

Next, we show that Lemma 2.18 imposes a condition on ξ in (2.5.15).

Lemma 2.20. *$\xi^2 + 8$ is a square in $\mathbb{F}_q$.*

Proof. To use Lemma 2.18 we rewrite $\varepsilon v_2 + \frac{\alpha}{2}(v_1 v_2 + v_1)$ in terms of ξ. This requires a certain amount of straightforward and tedious computations that we omit. From (2.5.15), we have

$$v = \frac{4(\xi^2+8)}{\chi 16 - \chi 2\xi^2 + h(8 - \chi 8\xi + \xi^2)} \tag{2.5.18}$$

and

$$v_1 = \frac{-4(\chi 16 - \chi 2\xi^2)(8+\xi^2)}{k}, \quad v_2 = \frac{-4(8+\xi^2)(8-\chi 8\xi + \xi^2)}{k} \tag{2.5.19}$$

where $k = 128 + \chi 256\xi - 224\xi^2 + \chi 32\xi^3 + 2\xi^4$.
Then,

$$\varepsilon v_2 + \frac{\alpha}{2}(v_1 v_2 + v_1) = \frac{2(1-\chi\varepsilon\alpha)(8+\xi^2)((-16+16\alpha)+(8+32\alpha)\xi+(6+10\alpha)\xi^2+\xi^3)^2}{(64-128\xi-112\xi^2-16\xi^3+\xi^4)^2} \tag{2.5.20}$$

Note that $(1+\alpha)(1-\alpha) = 2$ and that $1+\alpha \in \square_q$ if and only if $q \equiv 13 \pmod{16}$. In fact,

$$1+\alpha = \pm h^{\frac{q+3}{4}} \in \square_q \iff h^{\frac{(q-1)(q+3)}{8}} = 1$$

and in this case $1-\alpha$ is a non-square in $\mathbb{F}_q$.

Since $\chi\epsilon = 1$ when $q \equiv 5 \pmod{16}$ and $\chi\epsilon = -1$ when $q \equiv 13 \pmod{16}$, we get that $1 - \chi\epsilon\alpha$ is always a square in $\mathbb{F}_q$. Hence $\xi^2 + 8 \in \square_q$. □

To state a corollary of Lemmas 2.17, 2.18 and 2.20, the partition of $\mathbb{F}_q \cup \{\infty\}$ into two subsets $\Sigma_1 \cup \{\infty\}$ and Σ_2 is useful, where $x \in \Sigma_1 \cup \{\infty\}$ or $x \in \Sigma_2$ according as $x^2 + 8 \in \square_q$ or not.

Proposition 2.21. *Let $P = (2\varepsilon, h, 0) \in \mathcal{H}_{3,q^2}$ with $h^2 = 2$. Then the generators in $\mathcal{G}_1$ through the point P which meet $\mathcal{X}^+$ are as many as $n_P = \frac{1}{2}(q+1)$. They are precisely the lines g_ξ joining P to $P_{u,v} = (u, v, v^2)$ with u, v as in equation* (2.5.2) *and* (2.5.15)*, where ξ ranges over the set $\Sigma_1 \cup \{\infty\}$.*

2.5.2 Case of $\mathcal{G}_2$

This case requires much less effort. The tangent plane π_P at $P = (2\epsilon : h : 0)$ meets π in the line r of equation $2h^qY + Z = 0$. Since $\mathcal{C}$ has equation $Z = Y^2$ in π, the only common points of r and $\mathcal{C}$ are $(0:0:0)$ and $Q = (0 : 2h : 8)$, with $Q \notin \Omega$ as $h \notin \mathbb{F}_q$. Then we have the following result.

Proposition 2.22. *Let $P = (2\varepsilon, h, 0) \in \mathcal{H}_{3,q^2}$, with $h^2 = 2$. Then there is a unique generator through the point P which meets Ω, namely the line l through P and the origin $O = (0:0:0)$.*

From now on, we denote with ℓ^+ and ℓ^- the two generators through P when $\varepsilon = 1$ and $\varepsilon = -1$ respectively.

2.5.3 Choice of $\mathcal{M}_1$ and $\mathcal{M}_2$

In this last subsection, we are going to choose $\mathcal{M}_1$ and $\mathcal{M}_2$ such that Condition (B) is fulfilled.

We have two different generators g_0's, one for $\varepsilon = 1$, the other for $\varepsilon = -1$:

$$g_0^+ \text{ passing through } P^+(2 : h : 0)$$

and

$$g_0^- \text{ passing through } P^-(-2 : h : 0)$$

Lemma 2.23. *The generators g_0^+ and g_0^- are in different orbits of Φ.*

Proof. The linear collineation associated to the matrix $\mathbf{W}$ interchanges the two generators. □

Let r (resp. r') be the number of generators in $\mathcal{M}_1$ (resp. $\mathcal{M}_1'$) through the point P^+ that meet Δ^+. Note that

$$r + r' = \frac{1}{2}(q+1). \tag{2.5.21}$$

Similarly,

Lemma 2.24. *The generators ℓ^+ and ℓ^- are in different orbits of Φ.*

Proof. We use the same arguments of [34, Lemma 7.14]. Indeed, we replace $(\sqrt{-2}b, b, 0)$ and $(-\sqrt{-2}b, b, 0)$ with P^+ and P^- and the proof follows. □

We are ready to choose $\mathcal{M}_1$ and $\mathcal{M}_2$.

- $\mathcal{M}_1$ is the Φ-orbit containing g_0^+.
- $\mathcal{M}_2$ is the Φ-orbit containing ℓ^+ for $r < r'$ and ℓ^- for $r > r'$.

Remark 2.25. As in [34, Proposition 7.15], r' is obtained counting the squares in the value set of the polynomial $f(\xi)$, defined in Theorem 2.14. More precisely, we obtain that the number of $\xi \in \mathbb{F}_q$ for which $f(\xi) \in \square_q$ equals $2r' - 1$.

Therefore we have the following proposition.

Proposition 2.26. *Condition* (B) *for case* (III) *holds if and only if*

$$r = \frac{1}{4}(q-1), \ \textit{and } r' = \frac{1}{4}(q+3)$$

or

$$r = \frac{1}{4}(q+3), \ \textit{and } r' = \frac{1}{4}(q-1)$$

Proof. Note that $n_P = \frac{1}{2}(q+3)$ and that condition (B) holds if and only if half of them is in $\mathcal{M}_1 \cup \mathcal{M}_2$. The choices of r and r' are readily seen. □

Thus, Theorem 2.14 follows.

Since the properties of the plane curve $\mathcal{C}_4$

$$Y^2 = X^4 - 24\omega X^2 + 16\omega^2, \text{ with } \omega = 2$$

depend only on $q \equiv 1 \pmod 4$, we also get the proof of Theorem 2.13, that is Condition (B) in case (III) is satisfied if and only if the curve $\mathcal{C}_3$

$$Y^2 = X^3 - X$$

has $q-1$ or $q+3$ points. For the details, see [34] at the end of Section 7.

2.6 Proof of Theorem 2.1

We are in the position to work out the case $q = p$ when $p \equiv_4 1$. We write $p = \pi\bar{\pi}$, with $\pi \in \mathbb{Z}[i]$. Here, π can be chosen such that $\pi = \alpha_1 + i\alpha_2$ and $\alpha_1 = 1$. From [46, Section 2.2.2], $N_p(\mathcal{C}_3) = q + 1 - 2\alpha_1$. This implies that condition (B) in case (III) is satisfied if and only if

$$p = 1 + 4a^2 \quad \text{and} \quad N_p(\mathcal{C}_3) = q - 1.$$

Therefore, Theorem 2.1 is a corollary of Theorem 2.11, Result 2.12 and Theorem 2.14.

2.7 Some applications

In the last section of this chapter we will focus on some applications connected to hemisystems.

Strongly regular graphs

A *strongly regular graph* with parameters (v, k, λ, μ) is a graph with v vertices, each vertex lies on k edges, any two adjacent vertices have λ common neighbors and any two non-adjacent vertices have μ common neighbors. A strongly regular graph Γ with parameters $((q^3+1)(q+1-m), (q^2+1)(q-m), q-1-m, q^2+1-m(q+1))$ may arise from any m-regular system $\mathcal{S}$ on the Hermitian surface $\mathcal{H}_{3,q^2}$, q odd, where the vertices of Γ are the lines lying on the surface but not contained in $\mathcal{S}$, and two vertices are adjacent if the lines are incident. Thus, every hemisystem gives rise to a strongly regular graph with the following parameters: $v = \frac{1}{2}(q^3+1)(q+1)$, $k = \frac{1}{2}(q^2+1)(q-1)$, $\lambda = \frac{1}{2}(q-3)$, $\mu = \frac{1}{2}(q-1)^2$. The spectrum of Γ can be hence computed. The first eigenvalue is k, of multiplicity 1, and the other two (the restricted eigenvalues) are:

$$\theta_1 = \tfrac{1}{2}\left[(\lambda-\mu) + \sqrt{(\lambda-\mu)^2 + 4(k-\mu)}\right] = q-1,$$

$$\theta_2 = \tfrac{1}{2}\left[(\lambda-\mu) - \sqrt{(\lambda-\mu)^2 + 4(k-\mu)}\right] = \tfrac{1}{2}(-q^2+q-2),$$

of multiplicity

$$m_1 = \tfrac{1}{2}\left[(v-1) - \tfrac{2k+(v-1)(\lambda-\mu)}{\sqrt{(\lambda-\mu)^2+4(k-\mu)}}\right] = \tfrac{1}{2}(q^4 - q^3 + 2q^2 - q + 1),$$

$$m_2 = \tfrac{1}{2}\left[(v-1) + \tfrac{2k+(v-1)(\lambda-\mu)}{\sqrt{(\lambda-\mu)^2+4(k-\mu)}}\right] = (q^2+1)(q-1) = 2k,$$

respectively. See [44, Section 1.4].

The hemisystems on the Hermitian surface $\mathcal{H}_{3,p^2}$, for $p = 1+4a^2$, constructed in this chapter produce a strongly regular graph Γ with the above parameters for $q = p$. We point out that, in the smallest case $p = 5$, the graph Γ has parameters $(378, 52, 1, 8)$ and spectrum $52, 4^{273}, -11^{104}$. A comparison of Γ with the Cossidente-Penttila strongly regular graph ([15]) with the same parameters, shows that they are cospectral. It is an open question whether these two strongly regular graphs are isomorphic.

Two-weight codes from strongly regular graphs

An $[n,k]$-linear code C over the finite field $\mathbb{F}_q$ is a k-dimensional subspace of ${\mathbb{F}_q}^n$. Vectors in C are called *codewords*, and the weight $w(v)$ of $v \in C$ is the number of non-zero entries in v. A *two-weight code* is an $[n,k]$-linear code C such that $|\{w : \exists v \in C \setminus \{\underline{0}\} \;\; w(v) = w\}| = 2$

For a subset Ω of $\mathbb{F}_q^k$, with $\Omega = -\Omega$ and $0 \notin \Omega$, define $G(\Omega)$ to be the graph whose vertices are the vectors of $\mathbb{F}_q^k$, and two vertices are adjacent if and only if their difference is in Ω. Moreover, let Σ denote the set of points in $\mathrm{PG}(k-1,q)$ that correspond to the vectors in Ω, i.e. $\Sigma = \{\langle \mathbf{v} \rangle : \mathbf{v} \in \Omega\}$. An useful result connecting two-weight linear codes and strongly regular graphs is found in [11] which relies on projective (n,k,h_1,h_2)-sets, i.e. a proper, non-empty set Σ of n points of the projective space $\mathrm{PG}(k-1,q)$ such that every hyperplane meets Σ in either h_1 or h_2 points.

Result 2.27 ([11, Theorems 3.1 and 3.2]). *Let Ω and Σ be defined as above. If $\Sigma = \{\langle \mathbf{v_i} \rangle : i = 1,\dots,n\}$ is a proper subset of $\mathrm{PG}(k-1,q)$ that spans $\mathrm{PG}(k-1,q)$, then the following are equivalent:*

(i) $G(\Omega)$ is a strongly regular graph;

(ii) Σ is a projective $(n,k,n-w_1,n-w_2)$-set for some w_1 and w_2;

(iii) the linear code $C = \{(\mathbf{x}\cdot\mathbf{v_1}, \mathbf{x}\cdot\mathbf{v_2}, \dots, \mathbf{x}\cdot\mathbf{v_n}) : \mathbf{x} \in \mathbb{F}_q^k\}$ (here $\mathbf{x}\cdot\mathbf{v}$ is the classical scalar product) is an $[n,k]$-linear two-weight code with weights w_1 and w_2.

Since an m-regular system on the Hermitian surface provides an m-ovoid $\mathcal{O}$ on the elliptic quadric $\mathcal{Q}^-(5,q)$, the hemisystems constructed in the previous sections give rise to a projective set.. Moreover, see [5, Theorem 11], an m-ovoid on the elliptic quadric $\mathcal{Q}^-(5,q)$ is a projective $(m(q^{r+1}+1), 6, m(q^r+1), m(q^r+1)-q^r)$-set and it produces a strongly regular graph with parameters:

$$(q^6, m(q-1)(q^3+1), m(q-1)(3+m(q-1))-q^2, m(q-1)(m(q-1)+1)).$$

Since $m = \frac{1}{2}(q+1)$ we get a strongly regular graph with parameters $(q^6, \frac{1}{2}(q^3+1)(q^2-1), \frac{1}{4}(q^4-5), \frac{1}{4}(q^4-1))$, and the $\frac{1}{2}(q+1)$-ovoid $\mathcal{O}$ is a projective $(\frac{1}{2}(q^3+1)(q+1), 6, \frac{1}{2}(q^2+1)(q+1), \frac{1}{2}(q^3-q^2+q+1))$-set, which gives a $[\frac{1}{2}(q^3+1)(q+1), 6]$-linear two-weight code with weights $w_1 = \frac{1}{2}q^2(q^2-1)$ and $w_2 = \frac{1}{2}q^2(q^2+1)$.

Chapter 3

Blocking sets and conics

Combinatorial problems in finite projective planes often ask to count the number of points in the intersection of two algebraic subsets. A typical problem of this kind, posed in [1], is the following. The points of a projective plane $\mathrm{PG}(2,q)$ fall into three classes with respect to an (absolutely) irreducible conic, namely the points lying on two tangent lines (*external*), on no tangent line (*internal*) and the point s on the conic. Let $\mathcal{C}$ and $\mathcal{D}$ be two distinct irreducible conics. The points of $\mathcal{D}$ fall into one of three subsets, namely those points $E_{\mathcal{C}}(\mathcal{D})$ of $\mathcal{D}$ that are external to $\mathcal{C}$, those points $I_{\mathcal{C}}(\mathcal{D})$ that are internal, and $\mathcal{C}\cap\mathcal{D}$. This gives rise to the functions $\varepsilon_{\mathcal{C}}(\mathcal{D}) = |E_{\mathcal{C}}(\mathcal{D})|$ and $\iota_{\mathcal{C}}(\mathcal{D}) = |I_{\mathcal{C}}(\mathcal{D})|$ defined over the set of all conics $\mathcal{D}$ distinct from $\mathcal{C}$. The combinatorial problem is to compute, or estimate the value sets of $\varepsilon = \varepsilon_{\mathcal{C}}(\mathcal{D})$ (or equivalently of $\iota = \iota_{\mathcal{C}}(\mathcal{D})$). A solution is given in [1]: either $\varepsilon = 0, q-1, q, q+1$, or $\frac{1}{2}(q-1)-(\sqrt{q}-3) \leq \varepsilon \leq \frac{1}{2}(q-1)-(\sqrt{q}+3)$. Let $\mathrm{PG}(2,q)$ be the projective plane defined over a finite field $\mathbb{F}_q$ of odd order, canonically embedded in the projective plane $\mathrm{PG}(2,q^2)$ over the quadratic extension $\mathbb{F}_{q^2}$ of $\mathbb{F}_q$. Let $\mathcal{C}$ be an (absolutely) irreducible conic of $\mathrm{PG}(2,q^2)$ with homogeneous equation $F(X_0,X_1,X_2)=0$ where $F \in \mathbb{F}_{q^2}[\mathtt{X}_0,\mathtt{X}_1,\mathtt{X}_2]$ is an irreducible quadratic form. Then the number of points of $\mathcal{C}$ lying in $\mathrm{PG}(2,q)$ is at most 4 unless $\mathcal{C}$ is a conic defined over $\mathbb{F}_q$, that is, $F \in \mathbb{F}_q[\mathtt{X}_0,\mathtt{X}_1,\mathtt{X}_2]$, in which case that number equals $q+1$. In this chapter we are interested in the number $E_q(\mathcal{C})$ of external points to $\mathcal{C}$ which lie in $\mathrm{PG}(2,q)$. Since conics defined over $\mathbb{F}_{q^2}$ are not equivalent over $\mathbb{F}_q$ in general, $E_q(\mathcal{C})$ viewed as a function of $\mathcal{C}$ is not expected to be constant when $\mathcal{C}$ runs over all conics of $\mathrm{PG}(2,q^2)$. Our goal is to determine the relative value set.

The main results are stated in the following theorems.

Theorem 3.1. *Let $\mathcal{C}$ be a conic in the desarguesian plane* $\mathrm{PG}(2,q^2)$ *with at least one rational point in* $\mathrm{PG}(2,q)$ *and* $q \geq 5$*. Then*

$$E_q(\mathcal{C}) = q^2 \text{ if and only if } \mathcal{C} \text{ is defined over } \mathbb{F}_q.$$

Theorem 3.2 ([41, Theorem 1.2])**.** *In the desarguesian plane* $\mathrm{PG}(2,q^2)$ *let $\mathcal{C}$ be a conic not defined over $\mathbb{F}_q$ with at least one $\mathbb{F}_q$-rational point. Then:*

- *For $q=3$, $E_q(\mathcal{C}) \in \{3,4,5,6,7,8,9\}$;*
- *for $q=5$, $E_q(\mathcal{C}) \in \{11,12,14,15,16,17,19,20,21,22,25\}$;*
- *for $q>5$, we have*
$$E_q(\mathcal{C}) = \frac{1}{2}(q^2 + (\alpha-1)q - n_0),$$
where $n_0 \in \{0,1,2,3\}$ and $\alpha \in \{1,2,3,4,5,7\}$, and $\alpha - n_0$ is even.

Remark 3.3. When $q=3$ all the values occur, that is 7 possibilities.
When $q=5$ the only values missing are $\{16,22\}$, that is 2 out of 11.
When $q>5$ we have 13 possibilities.

3.1 External points

Our notation and terminology are standard; see [12, 20, 21, 22]. In particular, for a point $(X_0 : X_1 : X_2)$ of $\mathrm{PG}(2,q^2)$ we also use the shorter notation $X = (X_0 : X_1 : X_2)$. Let

$$F(X_0,X_1,X_2) = \sum_{0\leq i,j\leq 2} a_{ij}X_iX_j.$$

where $a_{ij} \in \mathbb{F}_{q^2}$, and $\det(a_{ij}) \neq 0$. Then $\mathcal{C}$ has equation $X^t\mathcal{A}X = 0$, for

$$\mathcal{A} = \begin{pmatrix} a_{00} & \frac{a_{01}}{2} & \frac{a_{02}}{2} \\ \frac{a_{01}}{2} & a_{11} & \frac{a_{12}}{2} \\ \frac{a_{02}}{2} & \frac{a_{12}}{2} & a_{22} \end{pmatrix}$$

For any two distinct points P and Q in $\mathrm{PG}(2,q^2)$, the line PQ meets $\mathcal{C}$ in $\mathrm{PG}(2,q^2)$ or in a quadratic extension $\mathrm{PG}(2,q^4)$ of $\mathrm{PG}(2,q^2)$, and their common points arise from the roots (ξ,ϑ) of the homogeneous Joachimsthal equation

$$\xi^2 P^t\mathcal{A}P + 2\xi\vartheta P^t\mathcal{A}Q + \vartheta^2 Q^t\mathcal{A}Q = 0.$$

More precisely, if (ξ_1, ϑ_1) and (ξ_2, ϑ_2) are the (non necessarily distinct) non-$\mathbb{F}_q$-proportional solutions of the Joachimsthal equation, then the common points are $U_i = \xi_i P + \vartheta_i Q$ for $i = 1, 2$. Joachimsthal equation is useful to distinguish between external and internal points of $\mathcal{C}$.

Lemma 3.4 ([12, Theorem 7.51])**.** *If P runs over the set of all external points to $\mathcal{C}$ then the values $P^t \mathcal{A} P$ are all squares or all non-squares. For an external point P, if $P^t \mathcal{A} P$ is a square then $Q^t \mathcal{A} Q$ is a non-square for every internal point Q to $\mathcal{C}$.*

Therefore, in terms of the equation $X^t \mathcal{A} X = \vartheta^2$ with $\vartheta \in \mathbb{F}_{q^2} \setminus \{0\}$, the problem of determining $E_q(\mathcal{C})$ asks to find its homogeneous solutions $X = (X_0 : X_1 : X_2)$, with $X_i \in \mathbb{F}_q$.

3.2 The maximal case

We start the discussion with a conic $\mathcal{C}$ defined over $\mathbb{F}_q$. Write the equation of $\mathcal{C}$ as

$$\mathcal{C}\colon aX^2 + bXY + cY^2 + dXZ + eYZ + fZ^2 = 0,$$

with $a, b, c, d, e, f \in \mathbb{F}_q$.

Lemma 3.5. *Let $\mathcal{C}$ be a conic defined over $\mathbb{F}_q$ with matrix $\mathcal{A}$. For every point $P \in \mathrm{PG}(2, q)$ we have $P^t \mathcal{A} P \in \Box_{q^2}$.*

Proof. $P^t \mathcal{A} P$ is an element of $\mathbb{F}_q$ and so a square of $\mathbb{F}_{q^2}$. □

Theorem 3.6. *Let $\mathcal{C}$ be a conic defined over $\mathbb{F}_q$. The number $E_q(\mathcal{C})$ of external points to $\mathcal{C}$ in $\mathrm{PG}(2, q^2)$ which lie in $\mathrm{PG}(2, q)$ is q^2.*

Proof. Any irreducible conic defined over $\mathbb{F}_q$ has $q+1$ points over $\mathbb{F}_q$. From Lemma 3.5 the remaining points of $\mathrm{PG}(2, q)$ are either all external or all internal to the conic $\mathcal{C}$. Let t_P be the $\mathbb{F}_q$-rational tangent to $\mathcal{C}$ at an $\mathbb{F}_q$-rational point P. Now any other point of t_P defined over $\mathbb{F}_q$ is an external point to $\mathcal{C}$ (note that this set is non-empty as t_P is defined over $\mathbb{F}_q$). In particular, this means that any point of $\mathrm{PG}(2, q)$ is either on the conic or is external to the conic. Since $|\mathrm{PG}(2, q)| = q^2 + q + 1$ points, this implies that there are other q^2 external points. □

3.3 Conics with at least one point in $\mathrm{PG}(2,q)$.

Up to a change of the reference system, we may assume that $\mathcal{C}$ contains the point $(0:1:0)$. Then $\mathcal{C}$ has equation

$$\mathcal{C}\colon aX^2+bXY+cXZ+dYZ+eZ^2=0 \tag{3.3.1}$$

with $a,b,c,d,e\in\mathbb{F}_{q^2}$ where either $b\neq 0$ or $d\neq 0$. From now on we may assume $b\neq 0$. In case $b=0$ we can apply the collineation $(X:Y:Z)\mapsto(Z:Y:X)$ which swaps b and d.

Lemma 3.7. *If P runs over the set of all external points to $\mathcal{C}$ then the values $P^t\mathcal{A}P$ are all squares or all non-squares according as $-bcd+ad^2+b^2e$ is a square or a non-square in $\mathbb{F}_{q^2}$.*

Proof. Since the tangent line to $\mathcal{C}$ at $Q=(0:1:0)$ has equation $bX+dZ=0$, the point $P=(-d/b:0:1)$ of t_Q is external to $\mathcal{C}$. We have $P^T\mathcal{A}P=(-bcd+ad^2+b^2e)$. Now, Lemma 3.7 follows from Lemma 3.4 . □

Remark 3.8. Without loss of generality we can always suppose $-bcd+ad^2+b^2e\in\square_{q^2}$. Indeed, if $-bcd+ad^2+b^2e=\alpha\gamma^2$, with $\alpha\notin\square_{q^2}$, we only need to multiply by α the equation of $\mathcal{C}$.

Equation $X^t\mathcal{A}X=\vartheta^2$ with $\vartheta\in\mathbb{F}_{q^2}$ can be rewritten over $\mathbb{F}_q$ as $\mathbb{F}_{q^2}$ is a finite extension of $\mathbb{F}_q$, that is, the elements of $\mathbb{F}_{q^2}$ are of the form $z=z_1+\epsilon z_2$ with $z_1,z_2\in\mathbb{F}_q$ where $\epsilon\in\mathbb{F}_{q^2}$ is a root of an irreducible polynomial $p(X)=X^2-\omega$ over $\mathbb{F}_q$. Since the other root of $p(X)$ is ϵ^q, we have $\epsilon+\epsilon^q=0$. Thus, $X^t\mathcal{A}X=\vartheta^2$ reads over $\mathbb{F}_q$:

$$\begin{cases} a_1X^2+b_1XY+c_1XZ+d_1YZ+e_1Z^2=t_1^2+\omega t_2^2\\ a_2X^2+b_2XY+c_2XZ+d_2YZ+e_2Z^2=2t_1t_2\end{cases} \tag{3.3.2}$$

where $a=a_1+\epsilon a_2$, $b=b_1+\epsilon b_2$, $c=c_1+\epsilon c_2$, $d=d_1+\epsilon d_2$, $e=e_1+\epsilon e_2$, $\vartheta=t_1+\epsilon t_2$ and $\omega=\epsilon^2$. Since we have $b\neq 0$ or $d\neq 0$, we can assume $d_2\neq 0$ or $b_2\neq 0$ without loss of generality. From the second equation then

$$Y=\frac{-e_2Z^2+2t_1t_2-c_2XZ-a_2X^2}{d_2Z+b_2X}. \tag{3.3.3}$$

Note that we lose the point $(0:1:0)$. Substituting Y by the expression on the right hand side gives

$$2t_1t_2(b_1X+d_1Z)-(t_1^2+\omega t_2^2)(b_2X+d_2Z)+AX^3+BX^2Z+CXZ^2+DZ^3=0, \quad (3.3.4)$$

where $A=-a_2b_1+a_1b_2$, $B=b_2c_1-b_1c_2-a_2d_1+a_1d_2$, $C=-c_2d_1+c_1d_2+b_2e_1-b_1e_2$, $D=d_2e_1-d_1e_2$ and $\omega=\epsilon^2$ is a non-square of $\mathbb{F}_q$. Note that Equation (3.3.4) is equivalent to:

$$(2t_1t_2-(a_2X^2+c_2XZ+e_2Z^2))(b_1X+d_1Z)+(a_1X^2+c_1XZ+e_1Z^2-t_1^2-\omega t_2^2)(b_2X+d_2Z)=0.$$

Remark 3.9. The number of solutions $(X:Y:Z)$ of System (3.3.2) can be obtained (but it is not necessarily equal) by counting the points over $\mathbb{F}_q$ lying on the cubic surface $\mathcal{S}\colon F(t_1,t_2,X,Z)=0$ of PG$(3,q)$ with homogeneous equation (3.3.4). Here PG$(3,q)$ stands for the projective space over $\mathbb{F}_q$ with homogeneous coordinates (t_1,t_2,X,Z).

Remark 3.10. Note that the conic $\mathcal{C}$ of equation (3.3.1) is defined over $\mathbb{F}_q$ if and only if the following hold:

$$a_1b_2=a_2b_1, \quad c_1b_2=c_2b_1, \quad d_1b_2=d_2b_1, \quad e_1b_2=e_2b_1.$$

Lemma 3.11. *With the notation above, if $(A,B,C,D)=(0,0,0,0)$ then $\mathcal{C}$ is a singular conic.*

Proof. The determinant of the matrix associated to the polynomial (3.3.4) defining $\mathcal{C}$ is

$$\frac{1}{4}(-a_1-a_2\epsilon+(b_1+b_2\epsilon)(c_1+c_2\epsilon-(b_1+b_2\epsilon)(e_1+e_2\epsilon))),$$

where we write every element z of $\mathbb{F}_{q^2}$ as $z=z_1+\epsilon z_2$ with $z_1,z_2\in\mathbb{F}_q$ where $\epsilon\in\mathbb{F}_{q^2}$ is a root of an irreducible polynomial $p(X)=X^2+\beta$ over $\mathbb{F}_q$. Since $d=1$ and $D=0$ we have that $e_2=0$. Furthermore, $A=0$, $C=0$ and $B=0$ imply respectively:

$$a_1=\frac{a_2b_1}{b_2}, \quad c_2=b_2e_1 \text{ and } a_2=b_2c_1-b_1c_2. \quad (3.3.5)$$

Then $\det(\mathcal{A})=0$. □

Remark 3.12. Since by hypothesis the conic $\mathcal{C}$ is non-singular, we cannot have $(A,B,C,D)=(0,0,0,0)$.

Lemma 3.13. *The cubic surface $\mathcal{S}$, defined by the equation* (3.3.4)*, is irreducible if and only if $b_1d_2 - b_2d_1 \neq 0$.*

Proof. Note that we can write the equation of $\mathcal{S}$ as

$$H(t_1, t_2, X, Z) + G(X, Z) = 0,$$

with F of degree 1 in X and Z. Hence the only possibility for $\mathcal{S}$ to be reducible is the following one:

$$(k_1X + k_2Z)(H_1(t_1, t_2) + G_1(X, Z)) = 0, \tag{3.3.6}$$

where $H_1(t_1, t_2) + G_1(X, Z)$ may be reducible itself.
Consider now $b_1d_2 - b_2d_1 = 0$. Then the plane $\pi : b_1X + d_1Z = 0$ is a component of the cubic surface $\mathcal{S}$. Indeed, using (3.3.4), we have

$$(b_1X+d_1Z)(b_2t_1^2-2b_1t_1t_2+b_2\omega t_2^2+(b_1a_2-a_1b_2)X^2+(b_1c_2-b_2c_1)XZ+(b_1e_2-b_2e_1)Z^2) = 0.$$

Hence $\mathcal{S}$ is reducible.
On the other hand, if $\mathcal{S}$ is reducible, using Equation (3.3.6) and the identity principle of polynomials, we have

$$\begin{cases} k_1X + k_2Z = h(b_1X + d_1Z) \\ k_1X + k_2Z = j(b_2X + d_2Z) \end{cases}$$

which implies $h(b_1X + d_1Z) = j(b_2X + d_2Z)$, for some $h, j \in \overline{\mathbb{F}}_q^*$ and so $b_1d_2 = b_2d_1$. □

3.3.1 Irreducible case

For a survey on cubic surfaces see [38]. In this section we suppose $\mathcal{S}$ irreducible. In particular we know that $b_1d_2 - b_2d_1 \neq 0$ or equivalently $\frac{d}{b} \notin \mathbb{F}_q$.

Remark 3.14. In this case we can set $d = 1$. Indeed, we can divide the equation (3.3.1) by d, since we have $d \neq 0$ and $b \neq 0$. This also implies $b_2 \neq 0$.

We want to find a bound for the number of rational points of $\mathcal{S}$. If $\mathcal{S}$ is a smooth surface we have the following theorem, see [38, Theorem 27.1 and Table 1 §31].

Theorem 3.15 (Weil)**.** *Let $\mathcal{S}$ be a smooth cubic surface defined over a finite field*

$\mathbb{F}_q$. Then

$$|\mathcal{S}(\mathbb{F}_q)| = q^2 + \alpha q + 1,$$

with $\alpha \in \{-2, -1, 0, 1, 2, 3, 4, 5, 7\}$.

The missing case is when $\mathcal{S}$ is singular. We start our investigation from the possible singularities of $\mathcal{S}$.

Theorem 3.16. *Let $\mathcal{S}$ be the cubic surface defined by equation* (3.3.4)*. Then $\mathcal{S}$ has at most one singular point P. In this case P is a double point and is defined over $\mathbb{F}_q$.*

Proof. Let $\mathcal{S}\colon F(t_1, t_2, X, Z) = 0$. The condition $\frac{\partial F}{\partial t_1} = \frac{\partial F}{\partial t_2} = 0$ implies

$$t_1^2 - \epsilon^2 t_2^2 = 0 \text{ or } X = Z = 0.$$

This means that $t_1 = t_2 = 0$, as $\epsilon \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, or $X = Z = 0$. When $X = Z = 0$ together with $\frac{\partial F}{\partial X} = \frac{\partial F}{\partial Z} = 0$ imply

$$\begin{cases} 2t_1t_2b_1 - b_2(t_1^2 + \omega t_2^2) = 0 \\ 2t_1t_2 = 0 \end{cases} \tag{3.3.7}$$

Hence $t_1 = t_2 = 0$. We need to study

$$\begin{cases} \dfrac{\partial F}{\partial X} = 3AX^2 + 2BXZ + CZ^2 = 0 \\ \dfrac{\partial F}{\partial Z} = BX^2 + 2CXZ + 3DZ^2 = 0 \end{cases} \tag{3.3.8}$$

If $A \neq 0$ then $Z = 0$ implies $X = 0$, so we can have only solutions of the form $(0 : 0 : \beta : 1)$. The system becomes

$$\begin{cases} \dfrac{\partial F}{\partial X} = 3AX^2 + 2BX + C = 0 \\ \dfrac{\partial F}{\partial Z} = BX^2 + 2CX + 3D = 0 \end{cases} \tag{3.3.9}$$

Note that System (3.3.9) has either one or two solutions (counted with multiplicity). The second case is only possible if either the two equations are proportional, namely

$$3A = kB, \quad B = kC \text{ and } C = 3kD,$$

or

$$B = C = D = 0.$$

In any cases we have a double root ($\frac{-1}{k}$ and 0). Hence we can just have one singular point, say $P = (0 : 0 : \beta : 1)$. Note that this still remains true when the characteristic of the field is 3 and $B = C = 0$. Furthermore, β needs to be an element of $\mathbb{F}_q$, otherwise $P' = (0 : 0 : \beta^q : 1)$ would be another singular point different from P.
Suppose now $A = 0$. System (3.3.8) becomes

$$\begin{cases} \dfrac{\partial F}{\partial X} = 2BXZ + CZ^2 = 0 \\ \dfrac{\partial F}{\partial Z} = BX^2 + 2CXZ + 3DZ^2 = 0 \end{cases}$$

If $Z = 0$ and $B \neq 0$ then we have no solutions. If $Z = 0$ and $B = 0$ we have only the solution $(0 : 0 : 1 : 0)$. If $Z \neq 0$ we can suppose $Z = 1$:

$$\begin{cases} \dfrac{\partial F}{\partial X} = 2BX + C = 0 \\ \dfrac{\partial F}{\partial Z} = BX^2 + 2CX + 3D = 0 \end{cases}$$

Note that B needs to be different from 0. Indeed, if $B = 0$ then we have $C = 0$ and $D = 0$. Hence we can have at most one solution which is defined over $\mathbb{F}_q$.
Finally, observe that $P = (0 : 0 : X : Z)$ cannot be a triple point for $\mathcal{S}$. Since both d_2 and b_2 cannot be zero, the condition $\frac{\partial^2 F}{\partial t_1^2}(P) = \frac{\partial^2 F}{\partial t_2^2}(P) = 0$ implies $-2(b_2X) = -2\omega(b_2X)$ and then $\omega = 1$, which is a contradiction as ω is a non-square of $\mathbb{F}_q$. □

We are going to study the tangent cone at a singular point P to investigate the number of points of $\mathcal{S}$. See [9]. Remember that the tangent cone $T_P(\mathcal{S})$ is the set of all tangent lines at a singular point P of $\mathcal{S}$. When $\mathcal{S}$ is a cubic surface we have four possibilities for the tangent cone $T_P(\mathcal{S})$:

- a quadric cone;
- a line (the intersection of two planes defined over $\mathbb{F}_{q^2}$.);
- a couple of distinct planes;
- a repeated plane.

Theorem 3.17. *With the notation above, the tangent cone $T_P(\mathcal{S})$ at $P = (0 : 0 : 1 : 0)$ or $P = (0 : 0 : \beta : 1)$ is a quadric cone with the exception of $\beta = -1, 0$. In these cases it is a couple of planes either defined over $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ or over $\mathbb{F}_q$. In particular* *there are* $q+1$*,* 1*,* $2q+1$ *tangent lines through* P*, respectively.*

Proof. The point $P=(0:0:1:0)$ is singular if and only if $A,B=0$ (and so $C\neq 0$ by hypothesis). In this case the associated matrix of $T_P(\mathcal{S})$ is

$$\mathcal{T}=\begin{pmatrix}-b_2 & b_1 & 0 & 0\\ b_1 & -b_2\omega & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & C\end{pmatrix}$$

It follows that $T_P(\mathcal{S})$ is a quadric cone.
When $P=(0:0:\beta:1)$ the tangent cone has the following associated matrix:

$$\mathcal{T}=\begin{pmatrix}-b_2\beta & b_1\beta+1 & 0 & 0\\ b_1\beta+1 & -b_2\beta\omega & 0 & 0\\ 0 & 0 & B+3A\beta & C+B\beta\\ 0 & 0 & C+B\beta & 3D+C\beta\end{pmatrix}=\begin{pmatrix}\mathcal{T}_1 & 0\\ 0 & \mathcal{T}_2\end{pmatrix}.$$

Note that β satisfies $3D+C\beta=-(B\beta^2+C\beta)$ and $C+B\beta=-(3A\beta^2+B\beta)$. This implies that $|\mathcal{T}|=0$. Indeed,

$$|\mathcal{T}_2|=-(B\beta+3A\beta^2)(B\beta+C)+(B\beta+3A\beta^2)(B\beta+C)=0.$$

Furthermore the rank of $\mathcal{T}$ is 3 except when

1. $B=C=D=0$. In this case we have $\beta=0$.
2. $B\neq 0$ and $\beta=\frac{-B}{3A}$. This case occurs when System (3.3.9) is reduced to the single equation $X^2+2X+1=0$. Thus, $\beta=-1$.

In both situations the rank of $\mathcal{T}$ equals 2. □

We want to study the maximum number of lines through $P=(0:0:\beta:1)$ entirely contained in $\mathcal{S}$. We apply to $\mathcal{S}$ the invertible projectivity defined by

$$(t_1:t_2:X:Z)\mapsto(t_1:t_2:X-\beta Z:Z),$$

so that

$$\mathcal{S}'\colon Z(2(1+b_1\beta)t_1t_2-(b_2\beta)(t_1^2+\omega t_2^2)+(3A\beta+B)X^2)+X(2b1t_1t_2-b_2(t_1^2+\omega t_2^2)+AX^2)=0$$

and $P' = (0:0:0:1)$. This means that we need to study the system

$$\begin{cases} \phi_2(t_1,t_2,X) := 2(1+b_1\beta)t_1t_2 - (b_2\beta)(t_1^2+\omega t_2^2) + (3A\beta+B)X^2 = 0 \\ \phi_3(t_1,t_2,X) := X(2b_1t_1t_2 - b_2(t_1^2+\omega t_2^2) + AX^2) = 0 \end{cases} \tag{3.3.10}$$

In fact, each point satisfying System (3.3.10) corresponds to a line through P' contained in $\mathcal{S}'$.

Theorem 3.18. *With the notation above, if α is the number of lines through the singular point P', then $\alpha \in \{0,2,4\}$.*

Proof. The homogeneous polynomial ϕ_2 cannot be a factor of ϕ_3. Thus, we have at most 6 points of intersection. According whether $\phi_2(t_1,t_2,0)$ is irreducible or not over $\mathbb{F}_q$ we lose or have two intersections and for every solution $(t_1:t_2:1)$ we have also the solution $(-t_1:-t_2:1)$. This implies that $\alpha \neq 1$. Now note that we have at most two solutions with $X=1$. They are given precisely by t_1 and t_2 satisfying $t_1t_2 = c_1$, where $c_1 \in \mathbb{F}_q \setminus \{0\}$ depends on A, B and β. □

Remark 3.19. Note that when ϕ_2 is reducible ($\beta = 0$ or $\beta = -1$) we have $\alpha = 0$ when we deal with two complex planes. In particular for $\beta = 0$ this cannot happen and hence $\alpha = 4$.

We are ready to state the main theorem.

Theorem 3.20. *Let $\mathcal{S}$ be the irreducible cubic surface defined by Equation* (3.3.4) *with a singular point, say $P = (0:0:\beta:1)$, and let $\beta_1 = (1+b_1\beta)^2 - b_2^2\beta^2\omega$. The following are the only possibilities for $\mathcal{S}_q = |\mathcal{S}(\mathbb{F}_q)|$.*

$$\mathcal{S}_q = \begin{cases} q^2+\alpha q+1, & \text{if } \beta \neq 0,-1 \\ q^2+3q+1, & \text{if } \beta = 0 \\ q^2+q+1, & \text{if } \beta_1 \notin \square_q, \beta = -1 \\ q^2+(\alpha-1)q+1, & \text{if } \beta_1 \in \square_q, \beta = -1 \end{cases}$$

where $\alpha \in \{0,2,4\}$ if $\beta_1 \notin \square_q$ and $\alpha \in \{2,4\}$ if $\beta_1 \in \square_q$.

Proof. This proof relies on the above results. In particular, since P is a double point, every line passing through P, not in $T_P(\mathcal{S})$, meets $\mathcal{S}$ in exactly one point (different from P). Thus, we need to subtract from q^2+q+1 the number of lines contained in $T_P(\mathcal{S})$ through P and add q whenever one of these lines lie on $\mathcal{S}$. □

We will use the following notation.

> $\mathcal{S}_q$ is the number of points defined over $\mathrm{PG}(3,q)$ of $\mathcal{S}$; moreover we set n_0 and n_∞ to be the number of the ones with $t_1 = t_2 = 0$ and $X = Z = 0$ respectively.

Lemma 3.21. *With the above notation, let* $\mathcal{C}$ *be a conic defined by Equation* (3.3.1). *Then*

$$E_q(\mathcal{C}) = \frac{1}{2}(\mathcal{S}_q - n_0 - n_\infty)$$

Proof. The points of $\mathcal{C}$ can be obtained putting $\vartheta = 0$ in the system (3.3.2) whereas $E_q(\mathcal{C})$ is obtained counting the points of $\mathcal{S}(\mathbb{F}_q)$ with $\vartheta \neq 0$. This means that every point of $\mathcal{S}(\mathbb{F}_q)$ with $t_1 = t_2 = 0$ is an $\mathbb{F}_q$-rational point of $\mathcal{C}$. Furthermore, we need to subtract the points with $X = Z = 0$, since they correspond to $(0 : 1 : 0)$ which is on the conic. Note that for fixed X, Y, Z we have either 0 or 2 solution for (t_1, t_2) defined over $\mathbb{F}_q$. The discriminant of the quadratic equation (3.3.4) in t_1 (or t_2) is actually different from 0. This because ω is not a square in $\mathbb{F}_q$. Thus, for every point $(X : Y : Z)$ of $\mathcal{C}(\mathbb{F}_q)$, we have two points $(t_1 : t_2 : X : Z)$ of $\mathcal{S}(\mathbb{F}_q)$ so, after we subtracted the values of n_0 and n_∞, we need to divide by two. □

Lemma 3.22. *With the above notation, we have* $n_\infty = q + 1$ *and* $n_0 \in \{0, 1, 2, 3\}$.

Proof. The points of $\mathcal{S}(\mathbb{F}_q)$ with $t_1 = 0$ and $t_2 = 0$ can be obtained as follows:

- $A = 0$. In this case we have at least the point $(0 : 0 : 1 : 0)$ and at most other two points, $(0 : 0 : \beta : 1)$, with β solution of

$$BX^2 + CX + D = 0.$$

- $A \neq 0$. The points are $(0 : 0 : \lambda : 1)$, with λ that runs over the solution set of

$$AX^3 + BX^2 + CX + D = 0,$$

  that are at most three.

The computation of n_∞ follows easily. Indeed, the number of points $(t_1 : t_2 : 0 : 0)$, for $t_1, t_2 \in \mathbb{F}_q$, is $q + 1$. □

Now we are ready to establish the possible values for $E_q(C)$. The values of $\mathcal{S}_q$ come from Theorems 3.15 and 3.20 , for $\mathcal{S}$ non-singular and singular respectively.

Corollary 3.23. *Let $\mathcal{S}_q = |\mathcal{S}(\mathbb{F}_q)|$. With the notations above:*

$$E_q(\mathcal{C}) = \frac{1}{2}(\mathcal{S}_q - n_0 - q - 1).$$

Corollary 3.24. *With the notation above, the possible values for $E_q(\mathcal{C})$, when $\mathcal{S}$ is non-singular are the following*

- $E_q(\mathcal{C}) = \frac{1}{2}(q^2 + (\alpha - 1)q - n_0)$, *with* $n_0 = 0, 2$ *and* $\alpha \in \{-2, 0, 2, 4\}$
- $E_q(\mathcal{C}) = \frac{1}{2}(q^2 + (\alpha - 1)q - n_0)$, *with* $n_0 = 1, 3$ *and* $\alpha \in \{-1, 1, 3, 5, 7\}$

Proof. We just need to study the parity of $q^2+(\alpha-1)q-n_0$ to establish the possible values for n_0 and α. □

3.3.2 Reducible case

Throughout this section we will suppose $b \neq 0$ and $\frac{d}{b} \in \mathbb{F}_q$ or equivalently $b_1 d_2 = d_1 b_2$. The case $d \neq 0$ is analogous.
Thus, from the proof of Lemma 3.13 we know that $\mathcal{S}$ splits as

$$\mathcal{S} = \Pi \cup \mathcal{Q},$$

where Π is the plane defined by $b_1 X + d_1 Z = 0$ (or $b_2 X + d_2 Z = 0$) and $\mathcal{Q}$ is a is a possibly degenerate quadric surface of $\mathrm{PG}(3, q)$ in t_1, t_2, X, Z.
The equation of $\mathcal{S}$ is

$$(b_1X+d_1Z)(b_2t_1^2-2b_1t_1t_2+b_2\omega t_2^2+(b_1a_2-a_1b_2)X^2+(b_1c_2-b_2c_1)XZ+(b_1e_2-b_2e_1)Z^2)$$

We study the two factors separately. Remember that $\mathcal{C}$ is defined by equation (3.3.1).

Lemma 3.25. *The line of* $\mathrm{PG}(2, q)$ *defined by $b_1 X + d_1 Z = 0$ is the tangent line to $\mathcal{C}$ at the point* $(0 : 1 : 0)$*. In particular, it contains exactly q external points to $\mathcal{C}$.*

Proof. By a straightforward computation

$$\frac{d}{b} = \frac{d_1 b_1 - \omega d_2 b_2}{b_1^2 - \omega b_2^2} = \frac{1}{b_2 b_1} \frac{b_1^2 d_2 b_1 - \omega b_2^2 d_1 b_2}{b_1^2 - \omega b_2^2} = \frac{d_1 b_2}{b_1 b_2} = \frac{d_1}{b_1}.$$

This means that the lines $bX + dZ = 0$ and $b_1 X + d_1 Z = 0$ are actually the same. In particular this is the tangent line to $\mathcal{C}$ at $(0 : 1 : 0)$. □

Remark 3.26. Lemma 3.25 implies that the plane Π is contributing with exactly q solutions to System (3.3.2), see Remark 3.8.

From now on we focus on the quadric surface $\mathcal{Q}$, defined by

$$b_2t_1^2-2b_1t_1t_2+b_2\omega t_2^2+(b_1a_2-a_1b_2)X^2+(b_1c_2-b_2c_1)XZ+(b_1e_2-b_2e_1)Z^2=0 \quad (3.3.11)$$

First, note that if $b_1a_2-a_1b_2=0$, $b_1c_2-b_2c_1=0$ and $b_1e_2-b_2e_1=0$ then the conic $\mathcal{C}$ is defined over $\mathbb{F}_q$, so we can skip it now (see Section 3.2).
One associate matrix of $\mathcal{Q}$ is

$$M=\begin{pmatrix} b_2 & -b_1 & 0 & 0 \\ -b_1 & b_2\omega & 0 & 0 \\ 0 & 0 & a' & \frac{c'}{2} \\ 0 & 0 & \frac{c'}{2} & e' \end{pmatrix},$$

where $a'=b_1a_2-a_1b_2$, $c'=b_1c_2-b_2c_1$ and $e'=b_1e_2-b_2e_1$. As mentioned above, we can assume that at least one of a',c' and e' is non-zero.

Lemma 3.27. *Let $\delta':=c'^2-4a'e'$ and $\delta=b_2^2\omega-b_1^2$.*

- *if $\delta'=0$ then $\mathcal{Q}$ is a quadric cone with vertex* $v=\begin{cases}(0:0:-c':2a'), & \text{if } a'\neq 0,\\ (0:0:1:0), & \text{if } a'=0\end{cases}$.
- *if $\delta'\neq 0$ then $\mathcal{Q}$ is a non-singular elliptic or hyperbolic quadric;*

Proof. The determinant of M is $\Delta=-\frac{1}{4}\delta\delta'=\frac{1}{4}(b_2^2\omega-b_1^2)(4a'e'-c'^2)$. Since $\omega$is a non-square of $\mathbb{F}_q$ and $b\neq 0$, we have $\Delta=0$ only when $\delta'=0$. The proof follows from the classification of quadric surfaces. See for example [21, pg. 14]. □

Lemma 3.28. *We have*

$$E_q(\mathcal{C})=\frac{1}{2}\big(|\mathcal{Q}|-|\mathcal{Q}_0|-|\Pi\cap\mathcal{Q}|+|\mathcal{Q}_0\cap\Pi|\big)+q,$$

where $\mathcal{Q}_0=\{(t_1,t_2,X,Z)\in\mathcal{Q}|t_1=t_2=0\}$.

Proof. We have already seen that Π gives its contribution of q points to $E_q(\mathcal{C})$. The remaining points that contribute to $E_q(\mathcal{C})$ are those on $\mathcal{Q}$ not in Π nor $\mathcal{Q}_0$ (as the points of $\mathcal{Q}_0$ correspond to points of $\mathcal{C}$), so the equation follows easily. □

From the previous lemma, we need to understand better the mutual position between Π, $\mathcal{Q}$, and $\mathcal{Q}_0$ to achieve our goal.

Lemma 3.29. Π *meets* $\mathcal{Q}_0$ *if and only if* $\kappa = 0$, *where*

$$\kappa := a'd_1^2 - c'd_1b_1 + e'b_1^2,$$

in which case $|\Pi \cap \mathcal{Q}_0| = 1$. *Furthermore, when* $\delta' = 0$, $\Pi \cap \mathcal{Q}_0$ *is the vertex of the quadric cone* $\mathcal{Q}$, *if* $a' \neq 0$, *and the empty set, if* $a' = 0$.

Proof. The plane Π meets $\mathcal{Q}_0$ only at one point, that is $(0 : 0 : -d_1 : b_1)$. Note that $\delta' = 0$ and $a' = 0$ imply $c' = 0$. Thus, κ needs to be different from zero otherwise we have $e' = 0$ too. The claim follows from standard computation. □

Corollary 3.30. *We have*

$$|\mathcal{Q}_0 \cap \Pi| = \begin{cases} 0, & \text{if } \kappa \neq 0 \\ 1, & \text{if } \kappa = 0 \end{cases}$$

Lemma 3.31.

$$|\mathcal{Q}_0| = \begin{cases} 0, & \text{if } \delta' \notin \square_q \\ 1, & \text{if } \delta' = 0 \\ 2, & \text{if } \delta' \in \square_q \end{cases}$$

Proof. This result follows from standard theory. See [21, Table 15.5] for more details. □

We are ready to describe the situation for every type of $\mathcal{Q}$.

Theorem 3.32. *Let* $\mathcal{S} = \Pi \cup \mathcal{Q}$, *with* $\mathcal{Q}$ *quadric cone* $(\delta' = 0)$. *Then*

$$E_q(\mathcal{C}) = \begin{cases} \frac{1}{2}(q^2 - q) + q, & \text{if } \kappa = 0, \delta \in \square_q \\ \frac{1}{2}(q^2 + q) + q, & \text{if } \kappa = 0, \delta \notin \square_q \\ \frac{1}{2}(q^2 - 1) + q, & \text{if } \kappa \neq 0 \end{cases}, \quad \delta = b_2^2\omega - b_1^2.$$

Proof. If $\delta' = 0$,

- $\kappa = 0$. This means that Π is a plane either meeting $\mathcal{Q}$ only at the vertex v or through two generators of $\mathcal{Q}$. More precisely, it depends on whether

$\delta = b_2^2\omega - b_1^2$ is in $\Box_q$ or not (note that δ cannot be equal to zero). Thus, we have

$$|\Pi \cap \mathcal{Q}| = \begin{cases} 2q+1, \text{ if } \delta \in \Box_q \\ \quad\; 1, \text{ if } \delta \notin \Box_q \end{cases}$$

- $\kappa \neq 0$. This implies that Π intersects $\mathcal{Q}$ in a non-singular conic with $q+1$ points, not containing v and $\mathcal{Q}_0 = \{v\}$, where v is the vertex of $\mathcal{Q}$.

Finally, the contribution of Π to $E_q(\mathcal{C})$ is q, as we have already seen. □

Lemma 3.33. *Let $\mathcal{S} = \Pi \cup \mathcal{Q}$. If $\delta' \neq 0$,*

$$|\Pi \cap \mathcal{Q}| = \begin{cases} 1, & \kappa = 0, \delta \notin \Box_q \\ 2q+1, & \kappa = 0, \delta \in \Box_q \\ q+1, & \kappa \neq 0 \end{cases}$$

Proof. Note that a point $P = (t_1 : t_2 : X, -\frac{b_1}{d_1}X) \in \Pi \cap \mathcal{Q}$ if and only if

$$F_1(t_1, t_2) + X^2\kappa = 0,$$

where $F_1(t_1, t_2) = b_2t_1^2 + b_2\omega t_2^2 - 2t_1t_2b_1$. Thus, if $\kappa \neq 0$ there are the $q+1$ points of a non-singular conic. On the other hand, if $\kappa = 0$ the number of solutions depend on whether $\delta \in \Box_q$ or not. The claim follows by [21, Par. 15.3]. □

Theorem 3.34. *Let $\mathcal{S} = \Pi \cup \mathcal{Q}$, with $\mathcal{Q}$ a non-singular quadric surface. Then*

- *if $\kappa \neq 0$ and $\delta' \in \Box_q$ then*

$$E_q(\mathcal{C}) = \begin{cases} \frac{1}{2}(q^2 - q - 2) + q, & \delta \notin \Box_q, \\ \frac{1}{2}(q^2 + q - 2) + q, & \delta \in \Box_q; \end{cases}$$

- *if $\kappa \neq 0$ and $\delta' \notin \Box_q$ then*

$$E_q(\mathcal{C}) = \begin{cases} \frac{1}{2}(q^2 - q) + q, & \delta \in \Box_q, \\ \frac{1}{2}(q^2 + q) + q, & \delta \notin \Box_q; \end{cases}$$

- *if $\kappa = 0$ (and $\delta' \in \Box_q$), then $E_q(\mathcal{C}) = \frac{1}{2}(q^2 - 1) + q$.*

Proof. The claims follows from Lemmas 3.28 and 3.33 and from [21, Tables 15.6 and 15.7] for the number of points of quadrics over $\mathbb{F}_q$. $\square$

3.4 Proof of Theorems 1.1 and 1.2

We are now able to prove our main theorems. More precisely Theorem 3.1 follows from Theorems 3.15, 3.32, 3.34 and the next result.

Theorem 3.35 ([48])**.** *In* Theorem 3.15 *the bounds are best possible, except that when* $q = 2, 3$ *or* 5 *the upper bound can be improved to* $\alpha \leq 5$.

The proof of Theorem 3.2 requires one last step. For further details about the next Theorem, see [3].

Theorem 3.36. *Let* $\mathcal{C}$ *be an oval of a projective plane of order* q^2, *say* Π_{q^2}, *with* q *being odd. Let* $\mathcal{B}$ *denote a blocking set of* Π_{q^2} *and* $\mathcal{E}$ *denote the set of points lying on a tangent to* $\mathcal{C}$.

If $\mathcal{C} \cap \mathcal{B} = k$, *then* $|\mathcal{E} \cap \mathcal{B}| \geq \frac{q^2+1-k}{2}$.

Proof. Each line of the plane, hence also the tangents to $\mathcal{C}$, meets $\mathcal{B}$. If t is a tangent to $\mathcal{C}$ at $P \in \mathcal{C}$, then $t \setminus \{P\} \subseteq \mathcal{E}$ and hence $t \cap \mathcal{B} \subseteq (\mathcal{E} \cap \mathcal{B}) \cup \{P\}$. Thus $\mathcal{E} \cap \mathcal{B}$ has a point of each of the tangents to the points of $\mathcal{C} \setminus \mathcal{B}$. Since each point not in $\mathcal{C}$ is incident with either 0 or 2 tangents to $\mathcal{C}$, then $|\mathcal{E} \cap \mathcal{B}| \geq \frac{q^2+1-k}{2}$. $\square$

Corollary 3.37. *Let* $\mathcal{C}$ *be an irreducible conic of* $\mathrm{PG}(2, q^2)$, q *odd, and let* $\mathcal{B}$ *denote a Baer subplane. Also, denote by* $\mathcal{E}$ *the set of external points to* $\mathcal{C}$.

Then $|\mathcal{E} \cap \mathcal{B}| \geq \frac{q^2-3}{2}$.

Corollary 3.37 shows that when $q > 3$ then in Theorem 3.24 we can exclude the cases $\alpha = -2, -1, 0$. Taking this into account, the proof of Theorem 3.2 is a direct consequence of Theorem 3.24, 3.20, 3.32 and 3.34.

3.5 Example

Let $\mathcal{C}_1$ be a conic of equation

$$ax^2 + bxy + dyz = 0,$$

with $\frac{b}{d} \notin \mathbb{F}_q$ and $\frac{a}{d} \in \mathbb{F}_q$. This means that we can rewrite the equation as

$$a'x^2 + b'xy + yz = 0,$$

where $a' \in \mathbb{F}_q$ and $b' \in \mathbb{F}_{q^2} \setminus \{\mathbb{F}_q\}$. Thus, we have $2(-bcd + ad^2 + b^2e) = a'$ which is always a square in $\mathbb{F}_{q^2}$. We conclude that the System (3.3.2) counts the number of external points to $\mathcal{C}_1$.
Lemma 3.22 can be refined. Indeed, we have $a_1'b_2'X^3 = 0$ admits only the root $(0 : 0 : 0 : 1)$. This implies that $n_0 = 1$ and $C_q = 2$.

From Theorem 3.23, since $\mathcal{S}$ is singular with $\delta' = 0$, we have just one possibility for σ_q:

$$\sigma_q = \frac{1}{2}(q^2 + 2q - 1).$$

Using the Computational Algebra System Magma [10], we found the following values for (q, E_q): $(3, 7)$, $(5, 17)$, $(7, 31)$, $(9, 49)$.

Chapter 4

Permutation binomials

In this chapter we are interested in investigating permutation binomials (PBs) over $\mathbb{F}_{q^2}$, where $p = \operatorname{char} \mathbb{F}_q$. A permutation binomial (PB) of $\mathbb{F}_q$ is a PP of the form $a\mathtt{X}^m + b\mathtt{X}^n$, where $a, b \in \mathbb{F}_q^*$, $m \not\equiv 0$, $n \not\equiv 0$ and $m \not\equiv n \pmod{q-1}$. Permutation binomials are an active topic that has attracted much attention. We refer the reader to [28] for a survey on PBs and to [27] for a survey on PPs. Permutation binomials are complex objects; in general, one can not expect a simple criterion on the parameters q, m, n, a, b for $a\mathtt{X}^m + b\mathtt{X}^n$ to be a PB of $\mathbb{F}_q$. In this chapter, we focus on PBs of $\mathbb{F}_{q^e}$ of the form

$$f_{q,e,n,d,a}(\mathtt{X}) = \mathtt{X}^n(\mathtt{X}^{d(q-1)} + a) \in \mathbb{F}_{q^e}[\mathtt{X}], \tag{4.0.1}$$

where $n, d \in \mathbb{Z}^+$, $n \not\equiv 0$, $d(q-1) \not\equiv 0$, $n + d(q-1) \not\equiv 0 \pmod{q^e - 1}$, and $a \in \mathbb{F}_{q^e}^*$. Here is an overview of current knowledge on such PBs.

Result 4.1 ([51, Corollary 5.3]). *Assume $e = 2$ and $a^{q+1} = 1$. Then $f_{q,2,n,d,a} = \mathtt{X}^n(\mathtt{X}^{d(q-1)} + a)$ is a PB of $\mathbb{F}_{q^2}$ if and only if $\gcd(n, q-1) = 1$, $\gcd(n-d, q+1) = 1$ and $(-a)^{(q+1)/\gcd(q+1,d)} \neq 1$.*

Result 4.2 ([26, Theorem A]). *Assume $e = 2$, $n = 1$, $d = 2$ and $a^{q+1} \neq 1$. Then $f_{q,2,1,2,a} = \mathtt{X}(\mathtt{X}^{2(q-1)} + a)$ is a PB of $\mathbb{F}_{q^2}$ if and only if q is odd and $(-a)^{(q+1)/2} = 3$.*

Result 4.3 ([29, Theorem 1.1]). *Assume $e = 2$, $n = 1$, $d > 2$, $a^{q+1} \neq 1$, and q is large relative to d. Then $f_{q,2,1,d,a} = \mathtt{X}(\mathtt{X}^{d(q-1)} + a)$ is not a PB of $\mathbb{F}_{q^2}$.*

Result 4.4 ([36, 37]). *Assume $e = 2$, $n = 3$, $d = 2$ and $a^{q+1} \neq 1$. Then $f_{q,2,3,2,a} = \mathtt{X}^3(\mathtt{X}^{2(q-1)} + a)$ is a PB of $\mathbb{F}_{q^2}$ if and only if q is odd, $q \equiv -1 \pmod 3$ and $(-a)^{(q+1)/2} = 1/3$.*

Result 4.5 ([49, Theorem 1]). *Assume $e = 2$, $q = 2^{2m}$ and $d = 3$. Then $f_{q,2,n,3,a} = \mathtt{X}^n(\mathtt{X}^{3(q-1)} + a)$ is a PB of $\mathbb{F}_{q^2}$ if and only if* $\gcd(n, q-1) = 1$, *$n \equiv 3 \pmod{q+1}$ and $a^{q+1} \neq 1$.*

(Note: in the original statement of Result 4.5 in [49], it is assumed that $m \geq 2$. However, the result also holds for $m = 1$; see Example 4.16.)

Result 4.6 ([24, Theorem 4.2]). *Assume $e = 2$ and $d = 1$. Then $f_{q,2,n,1,a} = \mathtt{X}^n(\mathtt{X}^{q-1} + a)$ is a PB of $\mathbb{F}_{q^2}$ if and only if* $\gcd(n, q-1) = 1$, *$n \equiv 1 \pmod{q+1}$ and $a^{q+1} \neq 1$.*

Result 4.7 ([39]). *Assume $e \geq 2$, $d = 1$ and $n < q^e - q$. For the special cases $(q, e) = (q, 2), (q, 3), (q, 4), (p, 5), (p, 6)$, where p is a prime, the following statement is true: if $f_{q,e,n,1,a} = \mathtt{X}^n(\mathtt{X}^{q-1} + a)$ is a PB of $\mathbb{F}_{q^e}$, then $f_{q,e,n,1,a} \equiv \mathtt{X}^{nq^h} + a\mathtt{X}^n \pmod{\mathtt{X}^{q^e} - \mathtt{X}}$ for some integer $h > 0$. It is conjectured that the statement is true for all q.*

(Note: in Result 4.7, when $q = 2$, $f_{2,e,n,1,a} = \mathtt{X}^n(\mathtt{X} + a)$ is never a PB of $\mathbb{F}_{2^e}$, so the statement is vacuously true.)

Through these results, we begin to understand the roles played by the parameters in the PBs of the form (4.0.1). At the same time, as more results on PBs gather, one feels a need for a properly defined notion of *equivalence* of PBs that allows us to categorize existing results and channel future efforts to PBs that are new under equivalence. Section 4.1 is included for this purpose. We define the equivalence among all PBs (not just those of the form (4.0.1)). We show that every PB can be brought to a canonical form which is uniquely determined by a triple of invariants. In particular, we see that the PB in Result 4.4 is equivalent to a PB in Result 4.2 and the PB in Result 4.5 is equivalent to a PB in Result 4.6.

Regarding Result 4.5, if we assume $e = 2$, $q = 2^{2m+1}$, $d = 3$ and $a^{q+1} \neq 1$, [49] conjectured that $f_{q,2,n,3,a} = \mathtt{X}^n(\mathtt{X}^{3(q-1)} + a)$ is not a PB of $\mathbb{F}_{q^2}$ and provided strong evidence for this conjecture. Note that in this case, $d \mid q + 1$. As we will see in Section 4.1, when the PB in (4.0.1) is brought to its canonical form, we always have $d \mid (q^e - 1)/(q - 1)$.

Let us further focus on the case $e = 2$, and we assume $d \mid q + 1$ by the above comment. In this case, if $a^{q+1} = 1$ or $d = 1$, all PBs are given by Results 4.1 and 4.6. Therefore, we assume $e = 2$, $2 \leq d \mid q + 1$ and $a^{q+1} \neq 1$. Under these assumptions and up to equivalence, the PBs in Result 4.2 form the only known class that contains infinitely many q's. This leads to the following question.

Question 4.8. *Fix integers $n \geq 1$ and $d \geq 2$. If there are infinitely many pairs (q, a) such that $d \mid q+1$, $a \in \mathbb{F}_{q^2}^*$, $a^{q+1} \neq 1$, and $f(\mathtt{X}) = f_{q,2,n,d,a}(\mathtt{X}) = \mathtt{X}^n(\mathtt{X}^{d(q-1)} + a)$ is a PB of $\mathbb{F}_{q^2}$, can we conclude that when q is sufficiently large, f is equivalent to a PB in* Result 4.2*?*

In this chapter, we prove two nonexistence results that support an affirmative answer to the above question.

Theorem 4.9 ([31, Theorem 1.9])**.** *Let $q = 2^m$, $n \geq 1$ and $a \in \mathbb{F}_{q^2}^*$ be such that $q \geq (2\max\{n, 6-n\})^4$ and $a^{q+1} \neq 1$. Then $f(\mathtt{X}) = f_{q,2,n,3,a}(\mathtt{X}) = \mathtt{X}^n(\mathtt{X}^{3(q-1)} + a)$ is not a PB of $\mathbb{F}_{q^2}$.*

Theorem 4.9 proves the conjecture of [49] when q is large relative to n.

Theorem 4.10 ([31, Theorem 1.10])**.** *Let $n \geq 1$, $d \geq 2$ and $a \in \mathbb{F}_{q^2}^*$ be such that $d \mid q+1$, $q \geq (2\max\{n, 2d-n\})^4$. Then $f(\mathtt{X}) = f_{q,2,n,d,a}(\mathtt{X}) = \mathtt{X}^n(\mathtt{X}^{d(q-1)} + a)$ is not a PB of $\mathbb{F}_{q^2}$ if one of the following conditions is satisfied.*

(i) $d - n > 1$ *and* $\gcd(d, n+1)$ *is a power of* 2.

(ii) $d + 2 \leq n < 2d$ *and* $\gcd(d, n-1)$ *is a power of* 2.

(iii) $n \geq 2d$*,* $\gcd(d, n-1)$ *is a power of* 2*, and* $\gcd(n-d, q-1) = 1$.

Remark 4.11. In Theorem 4.10, one can replace the assumption that $d \mid q+1$ with $\gcd(n, d) = 1$. If the f in Theorem 4.10 is a PB of $\mathbb{F}_{q^2}$, then $d \mid q+1$ implies $\gcd(n, d) = 1$. However, as we will see in Section 4.3, the proof of Theorem 4.10 only uses $\gcd(n, d) = 1$. Moreover, the assumption that $\gcd(n, d) = 1$ causes no loss of generality. If $f_{q,2,n,d,a}$ is a PB of $\mathbb{F}_{q^2}$ with $\gcd(n, d) = \delta$, then $\gcd(\delta, q^2-1) = 1$. Let $\delta' \in \mathbb{Z}^+$ be such that $\delta\delta' \equiv 1 \pmod{q^2-1}$. Then

$$f_{q,2,n,d,a}(\mathtt{X}^{\delta'}) \equiv f_{q,2,n/\delta,d/\delta,a}(\mathtt{X}) \pmod{\mathtt{X}^{q^2} - \mathtt{X}},$$

where $\gcd(n/\delta, d/\delta) = 1$.

Result 4.3 is a special case of Theorem 4.10 (i) with $n = 1$. Although the conditions in Theorem 4.10 are rather restrictive, they do cover many parameters that were not investigated previously. For example, (i) is satisfied for all $d > n+1$ with $\gcd(d, n+1) = 1$.

Theorems 4.9 and 4.10 are proved in Sections 4.2 and 4.3, respectively. The method is similar to that in [29]. Here we recall the basic strategy.

Let

$$f(\mathtt{X}) = f_{q,2,n,d,a}(\mathtt{X}) = \mathtt{X}^n(\mathtt{X}^{d(q-1)} + a) \in \mathbb{F}_{q^2}[\mathtt{X}], \tag{4.0.2}$$

where $n \geq 1$, $2 \leq d \mid q+1$ and $a \in \mathbb{F}_{q^2}^*$. From Theorem 1.70 we have to study $\mathtt{X}^n(\mathtt{X}^d + a)^{q-1}$ on the set μ_{q+1}. Assume that $f(\mathtt{X})$ in (4.0.2) is a PB of $\mathbb{F}_{q^2}$. Then for $x \in \mu_{q+1}$,

$$x^n(x^d + a)^{q-1} = \frac{x^n(x^{dq} + a^q)}{x^d + a} = \frac{x^n(a^q x^d + 1)}{x^d(x^d + a)} = G(x),$$

where

$$G(\mathtt{X}) = \frac{a^q\mathtt{X}^n + \mathtt{X}^{n-d}}{\mathtt{X}^d + a}. \tag{4.0.3}$$

Write

$$G(\mathtt{X}) = \frac{P(\mathtt{X})}{Q(\mathtt{X})},$$

where

$$\begin{cases} P(\mathtt{X}) = a^q\mathtt{X}^n + \mathtt{X}^{n-d}, \\ Q(\mathtt{X}) = \mathtt{X}^d + a, \end{cases} \qquad \text{if } n \geq d,$$

$$\begin{cases} P(\mathtt{X}) = a^q\mathtt{X}^d + 1, \\ Q(\mathtt{X}) = \mathtt{X}^{2d-n} + a\mathtt{X}^{d-n}, \end{cases} \qquad \text{if } n < d.$$

We assume that $a^{q+1} \neq 1$, which implies that $\gcd(P, Q) = 1$. Thus

$$\deg G = \begin{cases} n & \text{if } n \geq d, \\ 2d - n & \text{if } n < d. \end{cases}$$

Let

$$N(G) = \frac{P(\mathtt{X})Q(\mathtt{Y}) - P(\mathtt{Y})Q(\mathtt{X})}{\mathtt{X} - \mathtt{Y}} \in \mathbb{F}_{q^2}[\mathtt{X}, \mathtt{Y}], \tag{4.0.4}$$

which is the numerator of $(G(\mathtt{X}) - G(\mathtt{Y}))/(\mathtt{X} - \mathtt{Y})$. We have

$$\deg N(G) \leq \begin{cases} n + d - 1 & \text{if } n \geq d, \\ 3d - n - 1 & \text{if } n < d. \end{cases}$$

Theorem 4.12. *Assume that $f(\mathtt{X})$ in* (4.0.2) *is a PB of $\mathbb{F}_{q^2}$, where $q \geq (2\max\{n, 2d-n\})^4$. Then $N(G)$ in* (4.0.4) *is reducible in $\overline{\mathbb{F}}_q[\mathtt{X}, \mathtt{Y}]$, where $\overline{\mathbb{F}}_q$ is the algebraic closure of $\mathbb{F}_q$.*

Proof. We only give a sketch of the proof; the omitted details are given in [29, §3].

There exist $l_1, l_2 \in \mathbb{F}_{q^2}(\mathtt{X})$ of degree one such that $H := l_1 \circ G \circ l_2$ permutes $\mathbb{F}_q$. Since $\deg H = \deg G < q$, by [29, Lemma 3.2], $H \in \mathbb{F}_q(\mathtt{X})$. Let $A(\mathtt{X}, \mathtt{Y}) = N(H) \in \mathbb{F}_q[\mathtt{X}, \mathtt{Y}]$, the numerator of $(H(\mathtt{X}) - H(\mathtt{Y}))/(\mathtt{X} - \mathtt{Y})$. Assume to the contrary that $N(G)$ is irreducible over $\overline{\mathbb{F}}_q$. Then by [29, Lemma 3.1], $A(\mathtt{X}, \mathtt{Y})$ is also irreducible over $\overline{\mathbb{F}}_q$. We have

$$\delta := \deg A(\mathtt{X}, \mathtt{Y}) \le 2 \deg H - 2 = 2 \deg G - 2.$$

By the Hasse-Weil bound, the number of zeros of $A(\mathtt{X}, \mathtt{Y})$ in the projective plane $\mathrm{PG}(2, q)$ is at least

$$q - (\delta - 1)(\delta - 2)q^{1/2}.$$

Excluding the zeros at infinity of $\mathrm{PG}(2, q)$ and on the diagonal $\{(x, x) : x \in \mathbb{F}_q\}$ of the affine plane $\mathbb{F}_q^2$, we have

$$|\{(x, y) \in \mathbb{F}_q^2 : x \ne y,\ A(x, y) = 0\}| \ge q - (\delta - 1)(\delta - 2)q^{1/2} - 2\delta.$$

The right side is positive since $q \ge \delta^4$. Hence there exist $(x, y) \in \mathbb{F}_q^2$ with $x \ne y$ such that $A(x, y) = 0$. Then $H(x) = H(y)$, which is a contradiction. □

4.1 Canonical forms of permutation binomials

For our purpose, a binomial over $\mathbb{F}_q$ is a polynomial of the

$$f(\mathtt{X}) = a\mathtt{X}^m + b\mathtt{X}^n \in \mathbb{F}_q[\mathtt{X}],$$

where $a, b \in \mathbb{F}_q^*$, $m, n > 0$, $m \not\equiv 0$, $n \not\equiv 0$ and $m \not\equiv n \pmod{q-1}$. We treat $f(\mathtt{X})$ as a function from $\mathbb{F}_q$ to $\mathbb{F}_q$, that is, we identify $f(\mathtt{X})$ with its image in the quotient ring $\mathbb{F}_q[\mathtt{X}]/\langle \mathtt{X}^q - \mathtt{X}\rangle$. Let $\mathcal{B}_q$ denote the set of all such binomials. Two members $f, g \in \mathcal{B}_q$ are considered *equivalent*, denoted as $f \sim g$, if one can be obtained from the other through a combination of the following transformations of $\mathcal{B}_q$:

$$\begin{aligned} &\alpha_u : \mathcal{B}_q \to \mathcal{B}_q,\ f(\mathtt{X}) \mapsto uf(\mathtt{X}), \quad u \in \mathbb{F}_q^*, \\ &\beta : \mathcal{B}_q \to \mathcal{B}_q,\ f(\mathtt{X}) \mapsto f(\mathtt{X})^p, \quad p = \mathrm{char}\,\mathbb{F}_q, \\ &\gamma_{v,s} : \mathcal{B}_q \to \mathcal{B}_q,\ f(\mathtt{X}) \mapsto f(v\mathtt{X}^s), \quad v \in \mathbb{F}_q^*,\ s \in \mathbb{Z}^+, \gcd(s, q-1) = 1. \end{aligned} \tag{4.1.1}$$

If $f, g \in \mathcal{B}_q$ are equivalent, then f permutes $\mathbb{F}_q$ if and only if g does. It is clear that $\gamma_{v,s}$ commutes with α_u and β, and $\beta \circ \alpha_u = \alpha_{u^p} \circ \beta$. Therefore, for $f, g \in \mathcal{B}_q$, $f \sim g$ if and only if

$$g(\mathtt{X}) = uf(v\mathtt{X}^s)^{p^i} \tag{4.1.2}$$

for some $u, v \in \mathbb{F}_q^*$, $i \geq 0$ and $s > 0$ with $\gcd(s, q-1) = 1$.

For $d \mid q-1$, define

$$N_d = \{1 \leq n \leq q-1 : n = n^*\}, \tag{4.1.3}$$

where

$$\begin{aligned} n^* = \min\bigl\{1 \leq n' \leq q-1 : \ & n' \equiv tn \pmod{q-1} \text{ for some } t \in \mathbb{Z}_{q-1}^\times \\ & \text{with } t \equiv 1 \pmod{(q-1)/d} \text{ or} \\ & n' \equiv tn - d \pmod{q-1} \text{ for some } t \in \mathbb{Z}_{q-1}^\times \\ & \text{with } t \equiv -1 \pmod{(q-1)/d}\bigr\}. \end{aligned}$$

(Here $\mathbb{Z}_{q-1}^\times$ denotes the multiplicative group of $\mathbb{Z}_{q-1}$.) Let $\theta : \mathbb{Z}_{q-1}^\times \to \mathbb{Z}_{(q-1)/d}^\times$ be the natural homomorphism (which is onto). Then $G := \theta^{-1}(\{\pm 1\})$ acts on $\mathbb{Z}_{q-1}$ as follows: For $t \in G$ and $n \in \mathbb{Z}_{q-1}$,

$$t(n) = \begin{cases} tn & \text{if } \theta(t) = 1, \\ tn - d & \text{if } \theta(t) = -1. \end{cases}$$

Write $\mathbb{Z}_{q-1} = \{1, 2, \dots, q-1\}$. Then for $n \in \mathbb{Z}_{q-1}$, n^* is the least element in the G-orbit of n. Therefore N_d is the set of least elements of the G-orbits in $\mathbb{Z}_{q-1}$.

Example 4.13. Let $q = 2^4$ and $d = 3$. We have $\theta : \mathbb{Z}_{15}^\times \to \mathbb{Z}_5^\times$, $\theta^{-1}(1) = \{1, 11\}$, $\theta^{-1}(-1) = \{-1, 4\}$ and $G = \{1, 11, -1, 4\}$. The G-orbits of $\mathbb{Z}_{15}$ are $\{1, 11\}$, $\{2, 7, 10, 5\}$, $\{3, 9\}$, $\{4, 14, 8, 13\}$, $\{6\}$, $\{15\}$. Hence $N_d = \{1, 2, 3, 4, 6, 15\}$.

For $d \mid q-1$ and $n \in N_d$, let

$$\begin{aligned} G_{d,n} = & \text{the subgroup of } \mathbb{Z}_d^\times \text{ generated by} \\ & \begin{cases} \{p, -1\} & \text{if } d \equiv -2n \pmod{(q-1)/d} \text{ and } \gcd(n, q-1) = 1, \\ \{p\} & \text{otherwise,} \end{cases} \end{aligned} \tag{4.1.4}$$

Let $G_{d,n}$ act on $\mathbb{F}_q^*/(\mathbb{F}_q^*)^d$, where $(\mathbb{F}_q^*)^d = \{x^d : x \in \mathbb{F}_q^*\}$, as follows:

$$\begin{aligned} G_{d,n} \times \mathbb{F}_q^*/(\mathbb{F}_q^*)^d & \longrightarrow \mathbb{F}_q^*/(\mathbb{F}_q^*)^d \\ (s, a(\mathbb{F}_q^*)^d) & \longmapsto a^s(\mathbb{F}_q^*)^d, \quad a \in \mathbb{F}_q^*. \end{aligned}$$

Let $A_{d,n} \subset \mathbb{F}_q^*$ be such that $\{a(\mathbb{F}_q^*)^d : a \in A_{d,n}\}$ is a system of representatives of the $G_{d,n}$-orbits in $\mathbb{F}_q^*/(\mathbb{F}_q^*)^d$. Equivalently, let $G_{d,n}$ act on $\mathbb{Z}_d$ through multiplication and let ξ be a primitive element of $\mathbb{F}_q$. Then $A_{d,n} = \{\xi^e : e \in E_{d,n}\}$, where $E_{d,n}$ is a system of representatives of the $G_{d,n}$-orbits in $\mathbb{Z}_d$.

We now are ready to state and prove the main result of this section.

Theorem 4.14. *Assume that $f \in \mathcal{B}_q$ permutes $\mathbb{F}_q$. Then there is a unique triple (d, n, a), where $d \mid q-1$, $n \in N_d$ and $a \in A_{d,n}$, such that*

$$f(\mathtt{X}) \sim \mathtt{X}^n(\mathtt{X}^d + a). \tag{4.1.5}$$

We call the right side of (4.1.5) *the* canonical form *of f.*

Proof. Existence of (d, n, a)

Write $f(\mathtt{X}) = a_0\mathtt{X}^{m_0} + b_0\mathtt{X}^{n_0}$, where $a_0, b_0 \in \mathbb{F}_q^*$ and $m_0 > n_0$. Let $d = \gcd(m_0 - n_0, q-1)$. Let $r \in \mathbb{Z}^+$ be such that

$$r\frac{m_0 - n_0}{d} \equiv 1 \pmod{\frac{q-1}{d}}.$$

Since $\gcd(r, (q-1)/d) = 1$, there exists integer $k \geq 0$ such that $s := r + k(q-1)/d$ is relatively prime to $q-1$. (To see this, use Dirichlet's theorem on primes in arithmetic progression or the following simple argument: Let $p_1, \dots, p_l$ be the prime divisors of $q-1$ that do not divide r and let $k = p_1 \cdots p_l$.) Then

$$f(\mathtt{X}) \sim f(\mathtt{X}^s) = \mathtt{X}^{sn_0}(a_0\mathtt{X}^{s(m_0-n_0)} + b_0) = \mathtt{X}^{n_1}(a_0\mathtt{X}^d + b_0),$$

where $n_1 = sn_0$. We now assume $f(\mathtt{X}) = \mathtt{X}^{n_1}(a_0\mathtt{X}^d + b_0)$.

Let $n = n_1^* \in N_d$. We claim that

$$f(\mathtt{X}) \sim \mathtt{X}^n(a_1\mathtt{X}^d + b_1) \tag{4.1.6}$$

for some $a_1, b_1 \in \mathbb{F}_q^*$. To prove this claim, we consider two cases.

Case 1. Assume that $n \equiv tn_1 \pmod{q-1}$ for some $t \in \mathbb{Z}_{q-1}^\times$ with $t \equiv 1 \pmod{(q-1)/d}$. Then

$$f(\mathtt{X}) \sim f(\mathtt{X}^t) = \mathtt{X}^{tn_1}(a_0\mathtt{X}^{td} + b_0) = \mathtt{X}^n(a_0\mathtt{X}^d + b_0).$$

Case 2. Assume that $n \equiv tn_1 - d \pmod{q-1}$ for some $t \in \mathbb{Z}_{q-1}^\times$ with $t \equiv -1 \pmod{(q-1)/d}$. Then

$$f(\mathtt{X}) \sim f(\mathtt{X}^t) \ = \mathtt{X}^{tn_1}(a_0\mathtt{X}^{td} + b_0) = a_0\mathtt{X}^{tn_1+td} + b_0\mathtt{X}^{tn_1}$$

$$= a_0\mathtt{X}^n + b_0\mathtt{X}^{n+d} = \mathtt{X}^n(b_0\mathtt{X}^d + a_0).$$

Hence (4.1.6) is proved.

By (4.1.6), we may assume

$$f(\mathtt{X}) = \mathtt{X}^n(\mathtt{X}^d + c),$$

where $c \in \mathbb{F}_q^*$. To prove that $f(\mathtt{X}) \sim \mathtt{X}^n(\mathtt{X}^d + a)$ for some $a \in A_{d,n}$, again, we consider two cases.

Case 1. Assume that $d \not\equiv -2n \pmod{(q-1)/d}$ or $\gcd(n, q-1) \neq 1$. By (4.1.4), $G_{d,n} = \langle p \rangle < \mathbb{Z}_d^\times$. Then by the definition of $A_{d,n}$, there exist $i \in \mathbb{N}$, $a \in A_{d,n}$ and $b \in \mathbb{F}_q^*$ such that $c^{p^i} = ab^d$. Write $b = b_1^{p^i}$, where $b_1 \in \mathbb{F}_q^*$. Let $s \in \mathbb{Z}^+$ be such that $sp^i \equiv 1 \pmod{q-1}$. Then

$$\begin{aligned} f(\mathtt{X}) &\sim f(b_1\mathtt{X}^s)^{p^i} = (b_1\mathtt{X}^s)^{np^i}((b_1\mathtt{X}^s)^{dp^i} + c^{p^i}) \\ &\sim \mathtt{X}^n(b_1^{dp^i}\mathtt{X}^d + c^{p^i}) = \mathtt{X}^n(b^d\mathtt{X}^d + c^{p^i}) \\ &\sim \mathtt{X}^n(\mathtt{X}^d + c^{p^i}b^{-d}) = \mathtt{X}^n(\mathtt{X}^d + a). \end{aligned}$$

Case 2. Assume that $d \equiv -2n \pmod{(q-1)/d}$ and $\gcd(n, q-1) = 1$. Then $G_{d,n} = \langle p, -1 \rangle < \mathbb{Z}_d^\times$. So there exist $i \in \mathbb{N}$, $a \in A_{d,n}$ and $b \in \mathbb{F}_q^*$ such that either $c^{p^i} = ab^d$ or $c^{-p^i} = ab^d$. In the former case, the proof is identical to Case 1. In the latter case, write $b = b_1^{p^i}$, where $b_1 \in \mathbb{F}_q^*$. Let $k \in \mathbb{Z}^+$ be such that $kn \equiv 1 \pmod{q-1}$, and let $s = 1 + kd$. Then

$$\begin{aligned} sn = n + nkd &\equiv n + d \pmod{q-1} \\ &\equiv -n \pmod{(q-1)/d}. \end{aligned}$$

Hence $s \equiv -1 \pmod{(q-1)/d}$. It follows that $\gcd(s, (q-1)/d) = 1$. We also have $\gcd(s, d) = \gcd(1 + kd, d) = 1$. Therefore $\gcd(s, q-1) = 1$. We have

$$f(\mathtt{X}) \sim f(\mathtt{X}^s) = \mathtt{X}^{sn}(\mathtt{X}^{sd} + c) = \mathtt{X}^{sn+sd} + c\mathtt{X}^{sn}.$$

In the above,

$$sn = n + nkd \equiv n + d \pmod{q-1}$$

and

$$sd = (1 + kd)d \equiv (1 + k(-2n))d \equiv -d \pmod{q-1}.$$

Hence

$$f(\mathtt{X}) \sim \mathtt{X}^n + c\mathtt{X}^{n+d} \sim \mathtt{X}^n(\mathtt{X}^d + c^{-1}),$$

where $(c^{-1})^{p^i} = ab^d$. It follows from Case 1 that

$$\mathtt{X}^n(\mathtt{X}^d + c^{-1}) \sim \mathtt{X}^n(\mathtt{X}^d + a).$$

Uniqueness of (d, n, a)

Assume that

$$f(\mathtt{X}) = \mathtt{X}^n(\mathtt{X}^d + a) \sim \mathtt{X}^{n_1}(\mathtt{X}^{d_1} + a_1), \tag{4.1.7}$$

where $d \mid q-1$, $n \in N_d$, $a \in A_{d,n}$, $d_1 \mid q-1$, $n_1 \in N_{d_1}$, $a_1 \in A_{d_1,n_1}$.

In general, for $b\mathtt{X}^m + c\mathtt{X}^l \in \mathcal{B}_q$, $\gcd(m-l, q-1)$ is invariant under equivalence. Therefore, in (4.1.7), we have $d = d_1$.

By (4.1.7),

$$\mathtt{X}^{n_1}(\mathtt{X}^d + a_1) = uf(v\mathtt{X}^s)^{p^i} \tag{4.1.8}$$

for some $u, v \in \mathbb{F}_q^*$, $i \geq 0$ and $s > 0$ with $\gcd(s, q-1) = 1$. Expanding (4.1.8) gives

$$\mathtt{X}^{n_1+d} + a_1\mathtt{X}^{n_1} = \alpha\mathtt{X}^{t(n+d)} + \beta\mathtt{X}^{tn},$$

where $t = sp^i$ and $\alpha, \beta \in \mathbb{F}_q^*$. It follows that

$$\begin{cases} n_1 + d \equiv t(n+d) \pmod{q-1}, \\ n_1 \equiv tn \pmod{q-1}, \end{cases} \tag{4.1.9}$$

or

$$\begin{cases} n_1 + d \equiv tn \pmod{q-1}, \\ n_1 \equiv t(n+d) \pmod{q-1}. \end{cases} \tag{4.1.10}$$

Note that (4.1.9) is equivalent to

$$\begin{cases} t \equiv 1 \pmod{(q-1)/d}, \\ n_1 \equiv tn \pmod{q-1}, \end{cases} \tag{4.1.11}$$

and (4.1.10) is equivalent to

$$\begin{cases} t \equiv -1 \pmod{(q-1)/d}, \\ n_1 \equiv tn - d \pmod{q-1}. \end{cases} \tag{4.1.12}$$

Since $n \in N_d$, it follows from (4.1.11), (4.1.12) and the definition of N_d ((4.1.3)) that $n \le n_1$. By symmetry, $n_1 \le n$, whence $n = n_1$.

Now (4.1.8) becomes

$$\begin{aligned} \mathtt{X}^{n+d} + a_1\mathtt{X}^n &= u\big[(v\mathtt{X}^s)^{n+d} + a(v\mathtt{X}^s)^n\big]^{p^i} \\ &= uv^{p^i(n+d)}\mathtt{X}^{sp^i(n+d)} + ua^{p^i}v^{p^in}\mathtt{X}^{sp^in}. \end{aligned}$$

Let $t = sp^i$. Then there are two possibilities.

Case 1. (4.1.11) holds with $n = n_1$ and

$$(uv^{p^i(n+d)},\, ua^{p^i}v^{p^in}) = (1, a_1). \tag{4.1.13}$$

Case 2. (4.1.12) holds with $n = n_1$ and

$$(ua^{p^i}v^{p^in},\, uv^{p^i(n+d)}) = (1, a_1). \tag{4.1.14}$$

It suffices to show that in both cases, a and a_1 are in the same $G_{d,n}$-orbit. Which implies $a = a_1$.

First, assume Case 1. We have

$$a_1 = \frac{ua^{p^i}v^{p^in}}{uv^{p^i(n+d)}} = a^{p^i}v^{-p^id},$$

which is in the $G_{d,n}$-orbit of a.

Next, assume Case 2. (4.1.12) with $n = n_1$ gives

$$\begin{cases} t \equiv -1 \pmod{(q-1)/d}, \\ n \equiv tn - d \pmod{q-1}. \end{cases}$$

It follows that $n \equiv tn - d \equiv -n - d \pmod{(q-1)/d}$, i.e., $d \equiv -2n \pmod{(q-1)/d}$. Since $f(\mathtt{X})$ permutes $\mathbb{F}_q$, we have $\gcd(n, d) = 1$. From $n \equiv tn - d \pmod{q-1}$, we have $(t-1)n-d \equiv 0 \pmod{q-1}$, whence $d \mid t-1$ and

$$\frac{t-1}{d}n - 1 \equiv 0 \pmod{\frac{q-1}{d}}.$$

In particular, $\gcd(n,(q-1)/d) = 1$. Combining this with $\gcd(n,d) = 1$, we have $\gcd(n,q-1) = 1$. Therefore $G_{d,n} = \langle p, -1 \rangle$. Now by (4.1.14),

$$a_1 = \frac{uv^{p^i(n+d)}}{ua^{p^i}v^{p^i n}} = a^{-p^i}v^{p^i d},$$

which is in the $G_{d,n}$-orbit of a. □

Example 4.15. Assume that $n, d \in \mathbb{Z}^+$ are such that $d \mid q+1$, $n < 2d$, $\gcd(n, q^2 - 1) = 1$ and $\gcd(2d-n, q-1) = 1$, and let $a \in \mathbb{F}_{q^2}^*$. Since $\gcd(dq-n+d, q-1) = \gcd(2d-n, q-1) = 1$ and $\gcd(dq-n+d, q+1) = \gcd(n, q+1) = 1$, we have $\gcd(dq-n+d, q^2-1) = 1$. Then in $\mathcal{B}_q$,

$$\begin{aligned}
\mathtt{X}^n(\mathtt{X}^{d(q-1)} + a) &= \mathtt{X}^{dq+n-d} + a\mathtt{X}^n \\
&\sim \mathtt{X}^{(dq-n+d)(dq+n-d)} + a\mathtt{X}^{(dq-n+d)n} && (\mathtt{X} \mapsto \mathtt{X}^{dq-n+d}) \\
&= \mathtt{X}^{d^2q^2-(n-d)^2} + a\mathtt{X}^{(dq-n+d)n} \\
&= \mathtt{X}^{d^2-(n-d)^2} + a\mathtt{X}^{(dq-n+d)n} \\
&= \mathtt{X}^{n(2d-n)} + a\mathtt{X}^{(dq-n+d)n} \\
&\sim \mathtt{X}^{2d-n} + a\mathtt{X}^{dq-n+d} && (\mathtt{X}^n \mapsto \mathtt{X}) \\
&= \mathtt{X}^{2d-n}(1 + a\mathtt{X}^{d(q-1)}) \\
&\sim \mathtt{X}^{2d-n}(\mathtt{X}^{d(q-1)} + a^{-1}).
\end{aligned}$$

In particular, when $n = 1$, $d = 2$, q is odd and $q \not\equiv 1 \pmod 3$, we have

$$\mathtt{X}(\mathtt{X}^{2(q-1)} + a) \sim \mathtt{X}^3(\mathtt{X}^{2(q-1)} + a^{-1}).$$

This shows that the PB in Result 4.4 is equivalent to a PB in Result 4.2.

Example 4.16. We show that the PB in Result 4.5 is equivalent to a PB in Result 4.6. Let $e = 2$, $q = 2^{2m}$, $n \in \mathbb{Z}^+$, $d = 3$, $a \in \mathbb{F}_{q^2}^*$, and consider $f = f_{q,2,n,3,a} = \mathtt{X}^n(\mathtt{X}^{3(q-1)} + a)$.

Let $s=(q+2)/3+k(q+1)$, where

$$k=\begin{cases}0 & \text{if } m\equiv 0,1 \pmod 3,\\ 1 & \text{if } m\equiv -1 \pmod 3.\end{cases}$$

We claim that $\gcd(s,q^2-1)=1$. Clearly, $\gcd(s,q+1)=1$. We have

$$\begin{aligned}\gcd(s,q-1)&=\gcd\Bigl(\frac{q+2}{3}+2k,\ q-1\Bigr)\\ &=\frac{1}{3}\gcd(q+2+6k,\ 3q-3)\\ &=\frac{1}{3}\gcd(q+2+6k,\ 3(-2-6k)-3)\\ &=\frac{1}{3}\gcd(q+2+6k,\ 9(2k+1)).\end{aligned}$$

In the above, $9(2k+1)$ equals 3^2 or 3^3, and

$$\begin{aligned}q+2+6k&=(3-1)^{2m}+2+6k\\ &\equiv 1-2m\cdot 3+2+6k \pmod{3^2}\\ &=3+6(k-m)\\ &\not\equiv 0 \pmod{3^2}.\end{aligned}$$

So $\gcd(s,q-1)=1$ and the claim is proved.

Now we have

$$f(\mathtt{X})\sim f(\mathtt{X}^s)=\mathtt{X}^{sn}(\mathtt{X}^{s\cdot 3(q-1)}+a)=\mathtt{X}^{sn}(\mathtt{X}^{q-1}+a).$$

By Result 4.6, $\mathtt{X}^{sn}(\mathtt{X}^{q-1}+a)$ permutes $\mathbb{F}_{q^2}$ if and only if

$$\gcd(sn,q-1)=1,\quad sn\equiv 1 \pmod{q+1},\quad \text{and } a^{q+1}\neq 1,$$

i.e.,

$$\gcd(n,q-1)=1,\quad n\equiv 3 \pmod{q+1},\quad \text{and } a^{q+1}\neq 1,$$

which are precisely the conditions in Result 4.5.

4.2 Proof of Theorem 4.9

Theorem 4.9. *Let $q = 2^m$, $n \geq 1$ and $a \in \mathbb{F}_{q^2}^*$ be such that $q \geq (2\max\{n, 6-n\})^4$ and $a^{q+1} \neq 1$. Then $f(\mathtt{X}) = f_{q,2,n,3,a}(\mathtt{X}) = \mathtt{X}^n(\mathtt{X}^{3(q-1)} + a)$ is not a PB of $\mathbb{F}_{q^2}$.*

Assume to the contrary that f is a PB of $\mathbb{F}_{q^2}$. If m is even, by Result 4.5, $n \geq q+4$, which is a contradiction. So m is odd, and $3 \mid q+1$. By (4.0.3),

$$G(\mathtt{X}) = \frac{a^q\mathtt{X}^n + \mathtt{X}^{n-3}}{\mathtt{X}^3 + a}. \tag{4.2.1}$$

Let

$$N(\mathtt{X}, \mathtt{Y}) := N(G) \text{ be the numerator of } \frac{G(\mathtt{X}) + G(\mathtt{Y})}{\mathtt{X} + \mathtt{Y}}.$$

By Theorem 4.12, $N(\mathtt{X}, \mathtt{Y})$ is reducible over $\overline{\mathbb{F}}_q$. However, we will show that $N(\mathtt{X}, \mathtt{Y})$ is irreducible over $\overline{\mathbb{F}}_q$, hence creating a contradiction. We consider two cases, $n \geq 3$ and $n \leq 2$, separately.

4.2.1 Case 1. $n \geq 3$

Since $\gcd(n, 3(q-1)) = 1$ (Theorem 1.70), we have $n > 3$. We have

$$\begin{aligned} N(\mathtt{X}, \mathtt{Y}) &= \frac{1}{\mathtt{X}+\mathtt{Y}}\Big[(a^q\mathtt{X}^n + \mathtt{X}^{n-3})(\mathtt{Y}^3 + a) + (a^q\mathtt{Y}^n + \mathtt{Y}^{n-3})(\mathtt{X}^3 + a)\Big] \\ &= a\frac{\mathtt{X}^{n-3} + \mathtt{Y}^{n-3}}{\mathtt{X}+\mathtt{Y}} + \left[a^{q+1}\frac{\mathtt{X}^n + \mathtt{Y}^n}{\mathtt{X}+\mathtt{Y}} + \mathtt{X}^3\mathtt{Y}^3\frac{\mathtt{X}^{n-6} + \mathtt{Y}^{n-6}}{\mathtt{X}+\mathtt{Y}}\right] \\ &\quad + a^q\mathtt{X}^3\mathtt{Y}^3\frac{\mathtt{X}^{n-3} + \mathtt{Y}^{n-3}}{\mathtt{X}+\mathtt{Y}}. \end{aligned}$$

The homogenization of $N(\mathtt{X}, \mathtt{Y})$ is

$$\begin{aligned} N^*(\mathtt{X}, \mathtt{Y}, \mathtt{Z}) &= a\frac{\mathtt{X}^{n-3} + \mathtt{Y}^{n-3}}{\mathtt{X}+\mathtt{Y}}\mathtt{Z}^6 + \left[a^{q+1}\frac{\mathtt{X}^n + \mathtt{Y}^n}{\mathtt{X}+\mathtt{Y}} + \mathtt{X}^3\mathtt{Y}^3\frac{\mathtt{X}^{n-6} + \mathtt{Y}^{n-6}}{\mathtt{X}+\mathtt{Y}}\right]\mathtt{Z}^3 \\ &\quad + a^q\mathtt{X}^3\mathtt{Y}^3\frac{\mathtt{X}^{n-3} + \mathtt{Y}^{n-3}}{\mathtt{X}+\mathtt{Y}} \\ &= Q(\mathtt{Z}^3), \end{aligned}$$

where

$$\begin{aligned} Q(\mathtt{Z}) &= a\frac{\mathtt{X}^{n-3} + \mathtt{Y}^{n-3}}{\mathtt{X}+\mathtt{Y}}\mathtt{Z}^2 + \left[a^{q+1}\frac{\mathtt{X}^n + \mathtt{Y}^n}{\mathtt{X}+\mathtt{Y}} + \mathtt{X}^3\mathtt{Y}^3\frac{\mathtt{X}^{n-6} + \mathtt{Y}^{n-6}}{\mathtt{X}+\mathtt{Y}}\right]\mathtt{Z} \\ &\quad + a^q\mathtt{X}^3\mathtt{Y}^3\frac{\mathtt{X}^{n-3} + \mathtt{Y}^{n-3}}{\mathtt{X}+\mathtt{Y}}. \end{aligned}$$

It suffices to show that $N^*(\mathtt{X},\mathtt{Y},\mathtt{Z})$ is irreducible over $\overline{\mathbb{F}}_q$. We first show that $N^*(\mathtt{X},\mathtt{Y},\mathtt{Z})$, as a polynomial in $\mathtt{Z}$ over $\overline{\mathbb{F}}_q[\mathtt{X},\mathtt{Y}]$, is primitive, i.e., the gcd of its coefficients is 1; that is,

$$\gcd\Bigl(\frac{\mathtt{X}^{n-3}+\mathtt{Y}^{n-3}}{\mathtt{X}+\mathtt{Y}},\ a^{q+1}\frac{\mathtt{X}^{n}+\mathtt{Y}^{n}}{\mathtt{X}+\mathtt{Y}}+\mathtt{X}^3\mathtt{Y}^3\frac{\mathtt{X}^{n-6}+\mathtt{Y}^{n-6}}{\mathtt{X}+\mathtt{Y}}\Bigr)=1. \tag{4.2.2}$$

Since the polynomials in (4.2.2) are homogeneous, it suffices to prove (4.2.2) with $\mathtt{Y}=1$, i.e.,

$$\gcd\Bigl(\frac{\mathtt{X}^{n-3}+1}{\mathtt{X}+1},\ a^{q+1}\frac{\mathtt{X}^{n}+1}{\mathtt{X}+1}+\mathtt{X}^3\frac{\mathtt{X}^{n-6}+1}{\mathtt{X}+1}\Bigr)=1. \tag{4.2.3}$$

Let $\zeta\in\overline{\mathbb{F}}_q$ be a root of $(\mathtt{X}^{n-3}+1)/(\mathtt{X}+1)$. If $\zeta\neq 1$, then $\zeta^{n-3}+1=0$. Thus

$$\begin{aligned}
&\Bigl(a^{q+1}\frac{\mathtt{X}^{n}+1}{\mathtt{X}+1}+\mathtt{X}^3\frac{\mathtt{X}^{n-6}+1}{\mathtt{X}+1}\Bigr)\Big|_{\mathtt{X}=1}\\
=&\frac{1}{\zeta+1}\bigl(a^{q+1}(\zeta^n+1)+\zeta^3(\zeta^{n-6}+1)\bigr)\\
=&\frac{1}{\zeta+1}\bigl(a^{q+1}(\zeta^3+1)+1+\zeta^3\bigr)\\
=&\frac{1}{\zeta+1}(a^{q+1}+1)(\zeta^3+1)\neq 0.
\end{aligned}$$

(Note: $\zeta^3\neq 1$ since $\zeta^{n-3}=1$ and $\gcd(n,3(q-1))=1$.) If $\zeta=1$, then n must be odd, in which case,

$$\Bigl(a^{q+1}\frac{\mathtt{X}^{n}+1}{\mathtt{X}+1}+\mathtt{X}^3\frac{\mathtt{X}^{n-6}+1}{\mathtt{X}+1}\Bigr)\Big|_{\mathtt{X}=1}=a^{q+1}n+n-6=n(a^{q+1}+1)\neq 0.$$

This proves (4.2.3) and hence (4.2.2).

With (4.2.2), to prove that $N^*(\mathtt{X},\mathtt{Y},\mathtt{Z})$ is irreducible in $\overline{\mathbb{F}}_q[\mathtt{X},\mathtt{Y},\mathtt{Z}]$, it suffices to show that it is irreducible in $\overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y})[\mathtt{Z}]$. Let w be a root of $N^*(\mathtt{X},\mathtt{Y},\mathtt{Z})\in\overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y})[\mathtt{Z}]$ and let $z=w^3$. Then z is a root of $Q(\mathtt{Z})$. It suffices to show that $[\overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y},z):\overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y})]=2$ and $[\overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y},w):\overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y},z)]=3$.

$$\begin{tikzcd}
\overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y},w) \arrow[d, dash, "3"] \\
\overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y},z) \arrow[d, dash, "2"] \\
\overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y})
\end{tikzcd}$$

Proof that $[\overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y},z):\overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y})]=2$

Assume to the contrary that $Q(\mathtt{Z})$ is reducible over $\overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y})$. Then there exists $A/B\in\overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y})$ ($A,B\in\overline{\mathbb{F}}_q[\mathtt{X},\mathtt{Y}]$, $\gcd(A,B)=1$) such that

$$\frac{a^{q+1}\mathtt{X}^3\mathtt{Y}^3\Big(\dfrac{\mathtt{X}^{n-3}+\mathtt{Y}^{n-3}}{\mathtt{X}+\mathtt{Y}}\Big)^2}{\Big(a^{q+1}\dfrac{\mathtt{X}^n+\mathtt{Y}^n}{\mathtt{X}+\mathtt{Y}}+\mathtt{X}^3\mathtt{Y}^3\dfrac{\mathtt{X}^{n-6}+\mathtt{Y}^{n-6}}{\mathtt{X}+\mathtt{Y}}\Big)^2}=\Big(\frac{A}{B}\Big)^2+\frac{A}{B}=\frac{A(A+B)}{B^2}. \tag{4.2.4}$$

In Equation (4.2.4), the numerator and the denominator on the left side are relatively prime (by (4.2.2)), so

$$B=a^{q+1}\frac{\mathtt{X}^n+\mathtt{Y}^n}{\mathtt{X}+\mathtt{Y}}+\mathtt{X}^3\mathtt{Y}^3\frac{\mathtt{X}^{n-6}+\mathtt{Y}^{n-6}}{\mathtt{X}+\mathtt{Y}} \tag{4.2.5}$$

and

$$A(A+B)=a^{q+1}\mathtt{X}^3\mathtt{Y}^3\Big(\frac{\mathtt{X}^{n-3}+\mathtt{Y}^{n-3}}{\mathtt{X}+\mathtt{Y}}\Big)^2.$$

Since $\gcd(A,A+B)=1$, we may assume that

$$\begin{cases}A=\mathtt{X}^3U^2,\\ A+B=\mathtt{Y}^3V^2,\end{cases} \tag{4.2.6}$$

for some $U,V\in\overline{\mathbb{F}}_q[\mathtt{X},\mathtt{Y}]$ with $UV=(\mathtt{X}^{n-3}+\mathtt{Y}^{n-3})/(\mathtt{X}+\mathtt{Y})$. Therefore,

$$B=\mathtt{X}^3U^2+\mathtt{Y}^3V^2. \tag{4.2.7}$$

By (4.2.7), the coefficient of $\mathtt{X}\mathtt{Y}^{n-2}$ in B is 0. However, by (4.2.5), the coefficient of $\mathtt{X}\mathtt{Y}^{n-2}$ in B is either a^{q+1} or $a^{q+1}+1$. We have a contradiction.

Proof that $[\overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y},w):\overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y},z)]=3$

Assume the contrary. Then z is a third power in $\overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y},z)$, that is, there exists $A,B\in\overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y})$ such that

$$z=(A+Bz)^3,$$

i.e.,

$$(A+B\mathtt{Z})^3-\mathtt{Z}\equiv 0 \pmod{Q(\mathtt{Z})}. \tag{4.2.8}$$

Setting $\mathtt{Y}=1$ in (4.2.8) gives

$$(A_1+B_1\mathtt{Z})^3-\mathtt{Z}\equiv 0 \pmod{Q_1(\mathtt{Z})}, \tag{4.2.9}$$

where $A_1(\mathtt{X})=A(\mathtt{X},1)$, $B_1(\mathtt{X})=B(\mathtt{X},1)$ and

$$\begin{aligned}&Q_1(\mathtt{Z})=Q(\mathtt{Z})|_{\mathtt{Y}=1}=\\ &a\frac{\mathtt{X}^{n-3}+1}{\mathtt{X}+1}\mathtt{Z}^2+\left[a^{q+1}\frac{\mathtt{X}^n+1}{\mathtt{X}+1}+\mathtt{X}^3\frac{\mathtt{X}^{n-6}+1}{\mathtt{X}+1}\right]\mathtt{Z}+a^q\mathtt{X}^3\frac{\mathtt{X}^{n-3}+1}{\mathtt{X}+1}.\end{aligned}$$

We find that

$$(A_1+B_1\mathtt{Z})^3-\mathtt{Z}\equiv\frac{f_0(\mathtt{X})}{a^2(\mathtt{X}^3+\mathtt{X}^n)}+\frac{f_1(\mathtt{X})}{a^2(\mathtt{X}^3+\mathtt{X}^n)^2}\mathtt{Z} \pmod{Q_1(\mathtt{Z})},$$

where

$$\begin{aligned}f_0(\mathtt{X})=&a^2A_1^3\mathtt{X}^3+a^{1+q}A_1B_1^2\mathtt{X}^6+a^{1+2q}B_1^3\mathtt{X}^6+a^qB_1^3\mathtt{X}^9+a^2A_1^3\mathtt{X}^n\\ &+a^{1+q}A_1B_1^2\mathtt{X}^{3+n}+a^qB_1^3\mathtt{X}^{3+n}+a^{1+2q}B_1^3\mathtt{X}^{6+n},\\ f_1(\mathtt{X})=&a^2\mathtt{X}^6+a^2A_1^2B_1\mathtt{X}^6+a^{2+q}A_1B_1^2\mathtt{X}^6+a^{2+2q}B_1^3\mathtt{X}^6+aA_1B_1^2\mathtt{X}^9\\ &+a^{1+q}B_1^3\mathtt{X}^9+B_1^3\mathtt{X}^{12}+a^2\mathtt{X}^{2n}+a^2A_1^2B_1\mathtt{X}^{2n}+aA_1B_1^2\mathtt{X}^{2n}+B_1^3\mathtt{X}^{2n}\\ &+aA_1B_1^2\mathtt{X}^{3+n}+a^{2+q}A_1B_1^2\mathtt{X}^{3+n}+aA_1B_1^2\mathtt{X}^{6+n}+a^{2+q}A_1B_1^2\mathtt{X}^{6+n}\\ &+a^{2+q}A_1B_1^2\mathtt{X}^{3+2n}+a^{1+q}B_1^3\mathtt{X}^{3+2n}+a^{2+2q}B_1^3\mathtt{X}^{6+2n}.\end{aligned}$$

In particular, $f_0(\mathtt{X})=0$. From (4.2.9), $B_1\neq 0$. Then $f_0(\mathtt{X})=0$ implies $A_1\neq 0$. Let $C=B_1/A_1$. Then $f_0(\mathtt{X})=0$ becomes

$$(a^2+a^{1+q}\mathtt{X}^3C^2)(1+\mathtt{X}^{n-3})=a^q\mathtt{X}^3(a^{1+q}+\mathtt{X}^3+\mathtt{X}^{n-3}+a^{1+q}\mathtt{X}^n)C^3. \tag{4.2.10}$$

In Equation (4.2.10),

$$\begin{aligned}&\gcd(1+\mathtt{X}^{n-3},\ a^{1+q}+\mathtt{X}^3+\mathtt{X}^{n-3}+a^{1+q}\mathtt{X}^n)\\ =&\gcd(1+\mathtt{X}^{n-3},\ a^{1+q}+\mathtt{X}^3+1+a^{1+q}\mathtt{X}^3)\\ =&\gcd(1+\mathtt{X}^{n-3},\ (a^{1+q}+1)(1+\mathtt{X}^3))\\ =&1+\mathtt{X}.\end{aligned}$$

Let $C=D/E$, where $D,E\in\overline{\mathbb{F}}_q[\mathtt{X}]$, E is monic and $\gcd(D,E)=1$. Then (4.2.10) becomes

$$(a^2E^3+a^{1+q}\mathtt{X}^3D^2E)\frac{1+\mathtt{X}^{n-3}}{1+\mathtt{X}}=a^q\mathtt{X}^3D^3\,\frac{a^{1+q}+\mathtt{X}^3+\mathtt{X}^{n-3}+a^{1+q}\mathtt{X}^n}{1+\mathtt{X}}. \tag{4.2.11}$$

It follows that

$$\frac{1+\mathtt{X}^{n-3}}{1+\mathtt{X}}\;\Big|\;D\quad\text{and}\quad D\;\Big|\;\frac{1+\mathtt{X}^{n-3}}{1+\mathtt{X}}. \tag{4.2.12}$$

(4.2.11) and (4.2.12) force $D\in\overline{\mathbb{F}}_q^*$ and $n=4$. So

$$a^2E^3+a^{1+q}D^2\mathtt{X}^3E=a^qD^3\mathtt{X}^3(a^{1+q}(1+\mathtt{X})^3+\mathtt{X}(1+\mathtt{X})).$$

Then $\mathtt{X}\mid E$, say $E=\mathtt{X}E_1$. Thus

$$a^2E_1^3+a^{1+q}D^2\mathtt{X}E_1=a^qD^3(1+\mathtt{X})(a^{1+q}\mathtt{X}^2+\mathtt{X}+a^{1+q}). \tag{4.2.13}$$

It follows that $\deg E_1=1$, say $E_1=\mathtt{X}+\epsilon$, $\epsilon\in\overline{\mathbb{F}}_q$. Comparing the coefficients of $\mathtt{X}^3$ and $\mathtt{X}^0$ in Equation (4.2.13) gives

$$\begin{aligned}a^2&=a^{1+2q}D^3,\\a^2\epsilon^3&=a^{1+2q}D^3.\end{aligned}$$

Hence $\epsilon^3=1$. Then $(a^{1+q}\mathtt{X}^2+\mathtt{X}+a^{1+q})|_{\mathtt{X}=\epsilon}=a^{1+q}(1+\epsilon^2)+\epsilon\neq 0$ since $a^{1+q}\neq 1$. It follows from (4.2.13) that $E_1\mid 1+\mathtt{X}$, that is, $E_1=\mathtt{X}+1$. Now (4.2.13) becomes

$$a^2(\mathtt{X}+1)^2+a^{1+q}D^2\mathtt{X}=a^qD^3(a^{1+q}\mathtt{X}^2+\mathtt{X}+a^{1+q}).$$

Comparing the coefficients of $\mathtt{X}$ in the last equation gives $a^{1+q}D^2=a^qD^3$, i.e., $D=a$. But then (4.2.14) gives $a^{1+q}=1$, which is a contradiction.

4.2.2 Case 2. $n\le 2$

When $n=1$, the absolute irreducibility of $N(\mathtt{X},\mathtt{Y})$ follows from [29, §3]. So we assume $n=2$. The arguments are similar to those in Case 1. We have

$$G(\mathtt{X})=\frac{a^q\mathtt{X}^3+1}{\mathtt{X}(\mathtt{X}^3+a)}, \tag{4.2.14}$$

$$N(\mathtt{X},\mathtt{Y})=a^q\mathtt{X}^3\mathtt{Y}^3+a^{q+1}\mathtt{X}\mathtt{Y}(\mathtt{X}+\mathtt{Y})+(\mathtt{X}+\mathtt{Y})^3+a, \tag{4.2.15}$$

and

$$Q(\mathtt{Z}) = a\mathtt{Z}^2 + (a^{q+1}\mathtt{XY}(\mathtt{X}+\mathtt{Y}) + (\mathtt{X}+\mathtt{Y})^3)\mathtt{Z} + a^q\mathtt{X}^3\mathtt{Y}^3. \tag{4.2.16}$$

When proving $[\overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y},z) : \overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y})] = 2$, Equations (4.2.4), (4.2.5) and (4.2.6) are replaced by

$$\frac{a^{q+1}\mathtt{X}^3\mathtt{Y}^3}{(a^{q+1}\mathtt{XY}(\mathtt{X}+\mathtt{Y}) + (\mathtt{X}+\mathtt{Y})^3)^2} = \frac{A(A+B)}{B^2},$$

$$B = a^{q+1}\mathtt{XY}(\mathtt{X}+\mathtt{Y}) + (\mathtt{X}+\mathtt{Y})^3, \tag{4.2.17}$$

and

$$\begin{cases} A = u\mathtt{X}^3, \\ A + B = v\mathtt{Y}^3, \end{cases} \qquad u, v \in \overline{\mathbb{F}}_q^*.$$

Then $B = u\mathtt{X}^3 + v\mathtt{Y}^3$, which contradicts (4.2.17) since $a^{1+q} \neq 1$.

When proving $[\overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y},w) : \overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y},z)] = 3$, Equation (4.2.10) is replaced by

$$\begin{aligned} f_0(\mathtt{X}) = {} & a^2A_1^3 + a^{1+q}A_1B_1^2\mathtt{X}^3 + a^qB_1^3\mathtt{X}^3 + a^qB_1^3\mathtt{X}^4 + a^{1+2q}B_1^3\mathtt{X}^4 + a^qB_1^3\mathtt{X}^5 \\ & + a^{1+2q}B_1^3\mathtt{X}^5 + a^qB_1^3\mathtt{X}^6. \end{aligned}$$

Setting $E = A_1/B_1$, the equation $f_0(\mathtt{X}) = 0$ becomes

$$a^2E^3 + a^{1+q}\mathtt{X}^3E + a^q\mathtt{X}^3(1+\mathtt{X})(1 + a^{1+q}\mathtt{X} + \mathtt{X}^2) = 0.$$

It follows that $E \in \overline{\mathbb{F}}_q[\mathtt{X}]$ and $\mathtt{X} \mid E$. Write $E = \mathtt{X}E_1$. Then

$$a^2E_1^3 + a^{1+q}\mathtt{X}E_1 + a^q(1+\mathtt{X})(1 + a^{1+q}\mathtt{X} + \mathtt{X}^2) = 0. \tag{4.2.18}$$

Thus $\deg E_1 = 1$, say $E_1 = e(\mathtt{X}+\epsilon)$, $e \in \overline{\mathbb{F}}_q^*$, $\epsilon \in \overline{\mathbb{F}}_q$. Comparing the coefficients of $\mathtt{X}^3$ and $\mathtt{X}^0$ in Equation (4.2.18) gives

$$\begin{aligned} a^2e^3 + a^q &= 0, \\ a^2e^3\epsilon^3 + a^q &= 0. \end{aligned}$$

Hence $\epsilon^3 = 1$. Then $(1 + a^{1+q}\mathtt{X} + \mathtt{X}^2)|_{\mathtt{X}=\epsilon} \neq 0$. It follows form (4.2.18) that $E_1 \mid 1 + \mathtt{X}$, whence $E_1 = e(\mathtt{X}+1)$. Then (4.2.18) becomes

$$a^2e^3(\mathtt{X}+1)^2 + a^{1+q}e\mathtt{X} + a^q(1 + a^{1+q}\mathtt{X} + \mathtt{X}^2) = 0.$$

Comparing the coefficients of $\mathtt{X}$ in the last equation gives $e = a^q$. But then (4.2.19) gives $a^{1+q} = 1$, which is a contradiction.

4.3 Proof of Theorem 4.10

Theorem 4.10. *Let $n \geq 1$, $d \geq 2$ and $a \in \mathbb{F}_{q^2}^*$ be such that $d \mid q+1$, $q \geq (2\max\{n, 2d-n\})^4$. Then $f(\mathtt{X}) = f_{q,2,n,d,a}(\mathtt{X}) = \mathtt{X}^n(\mathtt{X}^{d(q-1)} + a)$ is not a PB of $\mathbb{F}_{q^2}$ if one of the following conditions is satisfied.*

(i) $d-n > 1$ and $\gcd(d, n+1)$ is a power of 2.

(ii) $d+2 \leq n < 2d$ and $\gcd(d, n-1)$ is a power of 2.

(iii) $n \geq 2d$, $\gcd(d, n-1)$ is a power of 2, and $\gcd(n-d, q-1) = 1$.

Assume to the contrary that $f(\mathtt{X})$ is a PB of $\mathbb{F}_{q^2}$. Recall that

$$G(\mathtt{X}) = \frac{a^q\mathtt{X}^n + \mathtt{X}^{n-d}}{\mathtt{X}^d + a}.$$

Let

$$N(\mathtt{X},\mathtt{Y}) = \text{the numerator of } \frac{G(\mathtt{X}) - G(\mathtt{Y})}{\mathtt{X}-\mathtt{Y}}$$

and

$$N^*(\mathtt{X},\mathtt{Y},\mathtt{Z}) = \text{the homogenization of } N(\mathtt{X},\mathtt{Y}).$$

Our objective is to show that $N^*(\mathtt{X},\mathtt{Y},\mathtt{Z})$ is irreducible over $\overline{\mathbb{F}}_q$ under the conditions in Theorem 4.10. We consider two cases: the case $d-n > 1$, which corresponds to (i) in Theorem 4.10, and the case $n-d > 1$, which corresponds to (ii) and (iii) in Theorem 4.10.

4.3.1 The Case $d - n > 1$

We have

$$G(\mathtt{X}) = \frac{a^q\mathtt{X}^d + 1}{\mathtt{X}^{d-n}(\mathtt{X}^d + a)},$$

$$\begin{aligned} N(\mathtt{X},\mathtt{Y}) = &-a\frac{\mathtt{X}^{d-n} - \mathtt{Y}^{d-n}}{\mathtt{X}-\mathtt{Y}} + \left[a^{q+1}\mathtt{X}^{d-n}\mathtt{Y}^{d-n}\frac{\mathtt{X}^n - \mathtt{Y}^n}{\mathtt{X}-\mathtt{Y}} - \frac{\mathtt{X}^{2d-n} - \mathtt{Y}^{2d-n}}{\mathtt{X}-\mathtt{Y}}\right] \\ &- a^q\mathtt{X}^d\mathtt{Y}^d\frac{\mathtt{X}^{d-n} - \mathtt{Y}^{d-n}}{\mathtt{X}-\mathtt{Y}}, \end{aligned}$$

$$N^*(\mathtt{X},\mathtt{Y},\mathtt{Z}) = Q(\mathtt{Z}^d),$$

where

$$\begin{aligned} Q(\mathtt{Z}) = &-a\frac{\mathtt{X}^{d-n}-\mathtt{Y}^{d-n}}{\mathtt{X}-\mathtt{Y}}\mathtt{Z}^2 + \Big[a^{q+1}\mathtt{X}^{d-n}\mathtt{Y}^{d-n}\frac{\mathtt{X}^n-\mathtt{Y}^n}{\mathtt{X}-\mathtt{Y}} - \frac{\mathtt{X}^{2d-n}-\mathtt{Y}^{2d-n}}{\mathtt{X}-\mathtt{Y}}\Big]\mathtt{Z} \\ &- a^q\mathtt{X}^d\mathtt{Y}^d\frac{\mathtt{X}^{d-n}-\mathtt{Y}^{d-n}}{\mathtt{X}-\mathtt{Y}}. \end{aligned}$$

We claim that

$$\gcd\Big(\frac{\mathtt{X}^{d-n}-\mathtt{Y}^{d-n}}{\mathtt{X}-\mathtt{Y}},\ a^{q+1}\mathtt{X}^{d-n}\mathtt{Y}^{d-n}\frac{\mathtt{X}^n-\mathtt{Y}^n}{\mathtt{X}-\mathtt{Y}} - \frac{\mathtt{X}^{2d-n}-\mathtt{Y}^{2d-n}}{\mathtt{X}-\mathtt{Y}}\Big) = 1. \tag{4.3.1}$$

Since the polynomials in (4.3.1) are homogeneous, it suffices to prove (4.3.1) with $\mathtt{Y}=1$, i.e.,

$$\gcd\Big(\frac{\mathtt{X}^{d-n}-1}{\mathtt{X}-1},\ a^{q+1}\mathtt{X}^{d-n}\frac{\mathtt{X}^n-1}{\mathtt{X}-1} - \frac{\mathtt{X}^{2d-n}-1}{\mathtt{X}-1}\Big) = 1. \tag{4.3.2}$$

Let ζ be a root of $(\mathtt{X}^{d-n}-1)/(\mathtt{X}-1)$. If $\zeta \neq 1$, then $\zeta^{d-n}=1$. It follows that

$$\begin{aligned} &\Big(a^{q+1}\mathtt{X}^{d-n}\frac{\mathtt{X}^n-1}{\mathtt{X}-1} - \frac{\mathtt{X}^{2d-n}-1}{\mathtt{X}-1}\Big)\Big|_{\mathtt{X}=\zeta} \\ &= \frac{1}{\zeta-1}\big(a^{q+1}(\zeta^n-1) - (\zeta^n-1)\big) = \frac{1}{\zeta-1}(a^{q+1}-1)(\zeta^n-1) \neq 0. \end{aligned}$$

(Note: $\zeta^n \neq 1$ since $\zeta^{d-n}=1$ and $\gcd(n,d)=1$.) If $\zeta = 1$, then $d-n \equiv 0 \pmod{p}$, where $p = \operatorname{char}\mathbb{F}_q$, whence

$$\Big(a^{q+1}\mathtt{X}^{d-n}\frac{\mathtt{X}^n-1}{\mathtt{X}-1} - \frac{\mathtt{X}^{2d-n}-1}{\mathtt{X}-1}\Big)\Big|_{\mathtt{X}=1} = a^{q+1}n - (2d-n) = (a^{q+1}-1)n \neq 0.$$

This proves (4.3.2) and hence (4.3.1). By (4.3.1), $N^*(\mathtt{X},\mathtt{Y},\mathtt{Z})$ is a primitive polynomial in $\mathtt{Z}$ over $\overline{\mathbb{F}}_q[\mathtt{X},\mathtt{Y}]$, i.e., the gcd of its coefficients in $\overline{\mathbb{F}}_q[\mathtt{X},\mathtt{Y}]$ is 1. Thus, to prove that $N^*(\mathtt{X},\mathtt{Y},\mathtt{Z})$ is irreducible in $\overline{\mathbb{F}}_q[\mathtt{X},\mathtt{Y},\mathtt{Z}]$, it suffices to show that it is irreducible in $\overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y})[\mathtt{Z}]$. Let w be a root of $N^*(\mathtt{X},\mathtt{Y},\mathtt{Z})$ for $\mathtt{Z}$ and let $z = w^d$. Then z is a root of $Q(\mathtt{Z})$, and it suffices to show that $[\overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y},z) : \overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y})] = 2$ and $[\overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y},w) : \overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y},z)] = d$.

$$\begin{tikzcd}
\overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y},w) \arrow[d, dash, "d"] \\
\overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y},z) \arrow[d, dash, "2"] \\
\overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y})
\end{tikzcd}$$

Proof that $[\overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y},z):\overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y})]=2$

Assume to the contrary that $Q(\mathtt{Z})$ is reducible over $\overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y})$.

First assume that q is odd. The discriminant of Q is

$$D=\Big[a^{q+1}\mathtt{X}^{d-n}\mathtt{Y}^{d-n}\frac{\mathtt{X}^n-\mathtt{Y}^n}{\mathtt{X}-\mathtt{Y}}-\frac{\mathtt{X}^{2d-n}-\mathtt{Y}^{2d-n}}{\mathtt{X}-\mathtt{Y}}\Big]^2-4a^{q+1}\mathtt{X}^d\mathtt{Y}^d\Big(\frac{\mathtt{X}^{d-n}-\mathtt{Y}^{d-n}}{\mathtt{X}-\mathtt{Y}}\Big)^2.$$

By assumption, $D=\Delta^2$ for some $\Delta\in\overline{\mathbb{F}}_q[\mathtt{X},\mathtt{Y}]$. Then

$$\begin{aligned}
&4a^{q+1}\mathtt{X}^d\mathtt{Y}^d\Big(\frac{\mathtt{X}^{d-n}-\mathtt{Y}^{d-n}}{\mathtt{X}-\mathtt{Y}}\Big)^2=\\
&\Big[a^{q+1}\mathtt{X}^{d-n}\mathtt{Y}^{d-n}\frac{\mathtt{X}^n-\mathtt{Y}^n}{\mathtt{X}-\mathtt{Y}}-\frac{\mathtt{X}^{2d-n}-\mathtt{Y}^{2d-n}}{\mathtt{X}-\mathtt{Y}}+\Delta\Big]\\
&\cdot\Big[a^{q+1}\mathtt{X}^{d-n}\mathtt{Y}^{d-n}\frac{\mathtt{X}^n-\mathtt{Y}^n}{\mathtt{X}-\mathtt{Y}}-\frac{\mathtt{X}^{2d-n}-\mathtt{Y}^{2d-n}}{\mathtt{X}-\mathtt{Y}}-\Delta\Big].
\end{aligned}$$

Let δ be the gcd of the two factors on the right side of (4.3.3). Then

$$\delta\ \Big|\ \Big(a^{q+1}\mathtt{X}^{d-n}\mathtt{Y}^{d-n}\frac{\mathtt{X}^n-\mathtt{Y}^n}{\mathtt{X}-\mathtt{Y}}-\frac{\mathtt{X}^{2d-n}-\mathtt{Y}^{2d-n}}{\mathtt{X}-\mathtt{Y}}\Big)$$

and

$$\delta\ \Big|\ \frac{\mathtt{X}^{d-n}-\mathtt{Y}^{d-n}}{\mathtt{X}-\mathtt{Y}}.$$

It follows from (4.3.1) that $\delta=1$.

Now from (4.3.3), we have

$$\begin{cases}
a^{q+1}\mathtt{X}^{d-n}\mathtt{Y}^{d-n}\dfrac{\mathtt{X}^n-\mathtt{Y}^n}{\mathtt{X}-\mathtt{Y}}-\dfrac{\mathtt{X}^{2d-n}-\mathtt{Y}^{2d-n}}{\mathtt{X}-\mathtt{Y}}+\Delta=\mathtt{X}^dU,\\
a^{q+1}\mathtt{X}^{d-n}\mathtt{Y}^{d-n}\dfrac{\mathtt{X}^n-\mathtt{Y}^n}{\mathtt{X}-\mathtt{Y}}-\dfrac{\mathtt{X}^{2d-n}-\mathtt{Y}^{2d-n}}{\mathtt{X}-\mathtt{Y}}-\Delta=\mathtt{Y}^dV,
\end{cases}$$

for some $U, V \in \overline{\mathbb{F}}_q[\mathtt{X}, \mathtt{Y}]$. It follows that

$$2a^{q+1}\mathtt{X}^{d-n}\mathtt{Y}^{d-n}\frac{\mathtt{X}^n - \mathtt{Y}^n}{\mathtt{X} - \mathtt{Y}} - 2\frac{\mathtt{X}^{2d-n} - \mathtt{Y}^{2d-n}}{\mathtt{X} - \mathtt{Y}} = \mathtt{X}^d U + \mathtt{Y}^d V. \tag{4.3.3}$$

The coefficient of $\mathtt{X}^{d-1}\mathtt{Y}^{d-n}$ on the left side of (4.3.3) is $2(a^{q+1} - 1) \neq 0$, while the coefficient of the same term on the right side of (4.3.3) is 0. This is a contradiction.

Next, assume that q is even. Since $Q(\mathtt{Z})$ is assumed to be reducible over $\overline{\mathbb{F}}_q(\mathtt{X}, \mathtt{Y})$, we have

$$\frac{a^{q+1}\mathtt{X}^d\mathtt{Y}^d\Big(\dfrac{\mathtt{X}^{d-n} + \mathtt{Y}^{d-n}}{\mathtt{X} + \mathtt{Y}}\Big)^2}{\Big[a^{q+1}\mathtt{X}^{d-n}\mathtt{Y}^{d-n}\dfrac{\mathtt{X}^n + \mathtt{Y}^n}{\mathtt{X} + \mathtt{Y}} + \dfrac{\mathtt{X}^{2d-n} + \mathtt{Y}^{2d-n}}{\mathtt{X} + \mathtt{Y}}\Big]^2} = \Big(\frac{A}{B}\Big)^2 + \frac{A}{B} = \frac{A(A+B)}{B^2},$$

where $A, B \in \overline{\mathbb{F}}_q[\mathtt{X}, \mathtt{Y}]$, $\gcd(A, B) = 1$. By (4.3.1), the numerator and the denominator on the left side are relatively prime. Therefore we may assume

$$B = a^{q+1}\mathtt{X}^{d-n}\mathtt{Y}^{d-n}\frac{\mathtt{X}^n + \mathtt{Y}^n}{\mathtt{X} + \mathtt{Y}} + \frac{\mathtt{X}^{2d-n} + \mathtt{Y}^{2d-n}}{\mathtt{X} + \mathtt{Y}}, \tag{4.3.4}$$

$$A(A+B) = a^{q+1}\mathtt{X}^d\mathtt{Y}^d\Big(\frac{\mathtt{X}^{d-n} + \mathtt{Y}^{d-n}}{\mathtt{X} + \mathtt{Y}}\Big)^2.$$

Since $\gcd(A, A+B) = 1$, we have

$$\begin{cases} A = \mathtt{X}^d U^2, \\ A + B = \mathtt{Y}^d V^2, \end{cases}$$

where $U, V \in \overline{\mathbb{F}}_q[\mathtt{X}, \mathtt{Y}]$, $UV = (\mathtt{X}^{d-n} + \mathtt{Y}^{d-n})/(\mathtt{X} + \mathtt{Y})$. Then

$$B = \mathtt{X}^d U^2 + \mathtt{Y}^d V^2. \tag{4.3.5}$$

The coefficient of $\mathtt{X}^{d-1}\mathtt{Y}^{d-n}$ in (4.3.4) is $a^{q+1} + 1 \neq 0$. However, the coefficient of $\mathtt{X}^{d-1}\mathtt{Y}^{d-n}$ in (4.3.5) is 0, which is a contradiction.

Proof that $[\overline{\mathbb{F}}_q(\mathtt{X}, \mathtt{Y}, w) : \overline{\mathbb{F}}_q(\mathtt{X}, \mathtt{Y}, z)] = d$

To prove this claim, it suffices to show that for each prime divisor t of d, z is not a t-th power in $\overline{\mathbb{F}}_q(\mathtt{X}, \mathtt{Y}, z)$. In (4.3.1), divide $Q(\mathtt{Z})$ by its leading coefficient and set

$\mathtt{Y}=1$, the result is

$$Q_1(\mathtt{Z})=\mathtt{Z}^2-\frac{a^{q+1}\mathtt{X}^{d-n}\frac{\mathtt{X}^n-1}{\mathtt{X}-1}-\frac{\mathtt{X}^{2d-n}-1}{\mathtt{X}-1}}{a\frac{\mathtt{X}^{d-n}-1}{\mathtt{X}-1}}\mathtt{Z}+a^{q-1}\mathtt{X}^d, \tag{4.3.6}$$

which is irreducible in $\overline{\mathbb{F}}_q(\mathtt{X})[\mathtt{Z}]$. Let z_1 be a root of $Q_1(\mathtt{Z})$. By [29, §3.3, Claim II′], it suffices to show that for each prime divisor t of d, z_1 is not a t-th power in $\overline{\mathbb{F}}_q(\mathtt{X},z_1)$.

Let $\overline{(\ )}$ denote the nonidentity automorphism in $\mathrm{Aut}(\overline{\mathbb{F}}_q(\mathtt{X},z_1)/\overline{\mathbb{F}}_q(\mathtt{X}))$. We have

$$z_1\bar{z}_1=a^{q-1}\mathtt{X}^d, \tag{4.3.7}$$

$$z_1+\bar{z}_1=\frac{a^{q+1}\mathtt{X}^{d-n}\frac{\mathtt{X}^n-1}{\mathtt{X}-1}-\frac{\mathtt{X}^{2d-n}-1}{\mathtt{X}-1}}{a\frac{\mathtt{X}^{d-n}-1}{\mathtt{X}-1}}. \tag{4.3.8}$$

Let $d-n=p^md'$, where $p=\mathrm{char}\,\mathbb{F}_q$, $p\nmid d'$. Let $\zeta\in\overline{\mathbb{F}}_q$ be a primitive d'th root of unity. Let $\mathfrak{p}$ be the place of the rational function field $\overline{\mathbb{F}}_q(\mathtt{X})$ which is the zero of $\mathtt{X}-\zeta$, and let $\mathfrak{P}$ be a place of $\overline{\mathbb{F}}_q(\mathtt{X},z_1)$ such that $\mathfrak{P}\mid\mathfrak{p}$. Then $\mathfrak{P}$ is unramified over $\mathfrak{p}$ ([47, III 7.3 (b) and 7.8 (b)]). From (4.3.7) and (4.3.8), we have

$$\nu_{\mathfrak{p}}(z_1\bar{z}_1)=0, \tag{4.3.9}$$

$$\nu_{\mathfrak{p}}(z_1+\bar{z}_1)=\begin{cases}-p^m & \text{if } d'>1,\\ -p^m+1 & \text{if } d'=1,\end{cases} \tag{4.3.10}$$

where $\nu_{\mathfrak{p}}$ is the valuation of $\overline{\mathbb{F}}_q(\mathtt{X})$ at $\mathfrak{p}$. Equation (4.3.10) is derived as follows. First, note that in (4.3.8),

$$\nu_{\mathfrak{p}}\Bigl(\frac{\mathtt{X}^{d-n}-1}{\mathtt{X}-1}\Bigr)=\begin{cases}p^m & \text{if } d'>1,\\ p^m-1 & \text{if } d'=1.\end{cases} \tag{4.3.11}$$

Next, write

$$a^{q+1}\mathtt{X}^{d-n}\frac{\mathtt{X}^n-1}{\mathtt{X}-1}-\frac{\mathtt{X}^{2d-n}-1}{\mathtt{X}-1}=(a^{q+1}\mathtt{X}^{d-n}-1)\frac{\mathtt{X}^n-1}{\mathtt{X}-1}-\mathtt{X}^n\frac{\mathtt{X}^{2(d-n)}-1}{\mathtt{X}-1}. \tag{4.3.12}$$

If $d' > 1$, the value of (4.3.12) at $\mathtt{X} = \zeta$ is

$$(a^{q+1}-1)\frac{\zeta^n-1}{\zeta-1} \neq 0.$$

If $d' = 1$, we have $m > 0$ (since $d-n > 1$), whence $d-n \equiv 0 \pmod{p}$. Then $n \not\equiv 0$ since $\gcd(n,d) = 1$. Therefore, the value of (4.3.12) at $\mathtt{X} = \zeta$ $(=1)$ is

$$(a^{q+1}-1)n - 2(d-n) = (a^{q+1}-1)n \neq 0.$$

Hence we always have

$$\nu_{\mathfrak{p}}\Big(a^{q+1}\mathtt{X}^{d-n}\frac{\mathtt{X}^n-1}{\mathtt{X}-1} - \frac{\mathtt{X}^{2d-n}-1}{\mathtt{X}-1}\Big) = 0. \tag{4.3.13}$$

Combining (4.3.8), (4.3.11) and (4.3.13) gives (4.3.10).

Write (4.3.9) and (4.3.10) as

$$\nu_{\mathfrak{P}}(z_1) + \nu_{\mathfrak{P}}(\bar{z}_1) = 0,$$

$$\nu_{\mathfrak{P}}(z_1+\bar{z}_1) = \begin{cases} -p^m & \text{if } d' > 1,\\ -p^m+1 & \text{if } d' = 1,\end{cases}$$

where $\nu_{\mathfrak{P}}$ is the valuation of $\overline{\mathbb{F}}_q(\mathtt{X}, z_1)$ at $\mathfrak{P}$. It follows that

$$\{\nu_{\mathfrak{P}}(z_1), \nu_{\mathfrak{P}}(\bar{z}_1)\} = \begin{cases} \{\pm p^m\} & \text{if } d' > 1,\\ \{\pm(p^m-1)\} & \text{if } d' = 1.\end{cases} \tag{4.3.14}$$

Assume to the contrary that z_1 is a t-th power in $\overline{\mathbb{F}}_q(\mathtt{X}, z_1)$. Then $t \mid \nu_{\mathfrak{P}}(z_1)$. If $d' > 1$, the by (4.3.14), $t \mid p^m$, whence $t \mid d-n$. This is impossible since $t \mid d$ and $\gcd(n,d) = 1$. Therefore, $d' = 1$ and $d-n = p^m$. By (4.3.14), $t \mid p^m - 1 = d-n-1$. Since $t \mid \gcd(d, d-n-1) = \gcd(d, n+1)$ and $\gcd(d, n+1)$ is a power of 2, we have $t = 2$. It follows that p is odd.

Recall that $Q_1(z_1) = 0$, where $Q_1(\mathtt{Z})$ is given in (4.3.6). Using (4.3.12) and $d-n = p^m$, the equation $Q_1(z_1) = 0$ can be written as

$$u^2 = \delta,$$

where

$$u = z_1 - \gamma,$$

$$\gamma = \frac{1}{2}\frac{(a^{q+1}\mathtt{X}^{p^m} - 1)\dfrac{\mathtt{X}^n - 1}{\mathtt{X} - 1} - \mathtt{X}^n(\mathtt{X}+1)^{p^m}(\mathtt{X}-1)^{p^m-1}}{a(\mathtt{X}-1)^{p^m-1}},$$

and

$$\delta = \gamma^2 - a^{q-1}\mathtt{X}^{p^m+n}.$$

By assumption, there exist $\alpha, \beta \in \overline{\mathbb{F}}_q(\mathtt{X})$ such that

$$(\alpha u + \beta)^2 = u + \gamma,$$

i.e.,

$$\alpha^2\delta + \beta^2 + 2\alpha\beta u = u + \gamma.$$

Since u is of degree 2 over $\overline{\mathbb{F}}_q(\mathtt{X})$, we have

$$\begin{cases} \alpha^2\delta + \beta^2 = \gamma, \\ 2\alpha\beta = 1. \end{cases}$$

Letting $\tau = \alpha/\beta$, we have

$$1 + \delta\tau^2 - 2\gamma\tau = 0 \tag{4.3.15}$$

and

$$\tau = 2\alpha^2. \tag{4.3.16}$$

Fortunately, (4.3.15) has an explicit solution

$$\tau = \frac{1}{\delta}(\gamma \pm a^{(q-1)/2}\mathtt{X}^{(p^m+n)/2}) = \frac{1}{\gamma \mp a^{(q-1)/2}\mathtt{X}^{(p^m+n)/2}}. \tag{4.3.17}$$

In Equation (4.3.17),

$$\begin{aligned} &\gamma \mp a^{(q-1)/2}\mathtt{X}^{(p^m+n)/2} = \\ &\frac{1}{2a(\mathtt{X}-1)^{p^m-1}}\Big[(a^{q+1}\mathtt{X}^{p^m} - 1)\frac{\mathtt{X}^n - 1}{\mathtt{X}-1} - \mathtt{X}^n(\mathtt{X}+1)^{p^m}(\mathtt{X}-1)^{p^m-1} \\ &\qquad \mp 2a^{(q+1)/2}\mathtt{X}^{(p^m+n)/2}(\mathtt{X}-1)^{p^m-1}\Big]. \end{aligned}$$

Since τ is square in $\overline{\mathbb{F}}_q(\mathtt{X})$ (by (4.3.16)),

$$h := (1 - a^{q+1}\mathtt{X}^{p^m})\frac{\mathtt{X}^n - 1}{\mathtt{X}-1} + \mathtt{X}^n(\mathtt{X}+1)^{p^m}(\mathtt{X}-1)^{p^m-1} + 2\epsilon\mathtt{X}^{(p^m+n)/2}(\mathtt{X}-1)^{p^m-1},$$

where $\epsilon = \pm a^{(q+1)/2}$, is a square in $\overline{\mathbb{F}}_q(\mathtt{X})$, say $h = g^2$, where $g \in \overline{\mathbb{F}}_q[\mathtt{X}]$ is monic of degree $p^m + (n-1)/2$. Note that

$$\begin{aligned} h =& \frac{\mathtt{X}^n - 1}{\mathtt{X}-1} + (\mathtt{X}^n + \mathtt{X}^{p^m+n})\frac{\mathtt{X}^{p^m}-1}{\mathtt{X}-1} - a^{q+1}\mathtt{X}^{p^m}\frac{\mathtt{X}^n-1}{\mathtt{X}-1} + 2\epsilon\mathtt{X}^{(p^m+n)/2}\frac{\mathtt{X}^{p^m}-1}{\mathtt{X}-1} \\ =& (1 + \cdots + \mathtt{X}^{2p^m+n-1}) \\ & - a^{q+1}(\mathtt{X}^{p^m} + \cdots + \mathtt{X}^{p^m+n-1}) \\ & + 2\epsilon(\mathtt{X}^{(p^m+n)/2} + \cdots + \mathtt{X}^{(3p^m+n)/2-1}), \end{aligned}$$

which is self-reciprocal. Hence $g^* = \pm g$, where g^* is the reciprocal polynomial of g. (In fact, $g^* = g$, but we do not need to be precise.) Let

$$\begin{aligned} H &= (\mathtt{X}-1)h \\ &= (1 - a^{q+1}\mathtt{X}^{p^m})(\mathtt{X}^n - 1) + \mathtt{X}^n(\mathtt{X}+1)^{p^m}(\mathtt{X}-1)^{p^m} + 2\epsilon\mathtt{X}^{(p^m+n)/2}(\mathtt{X}-1)^{p^m}. \end{aligned}$$

Then

$$H' = (1 - a^{q+1}\mathtt{X}^{p^m})n\mathtt{X}^{n-1} + n\mathtt{X}^{n-1}(\mathtt{X}+1)^{p^m}(\mathtt{X}-1)^{p^m} + \epsilon n\mathtt{X}^{(p^m+n)/2-1}(\mathtt{X}-1)^{p^m}.$$

(When computing H', we used the assumption that $m > 0$.) Let

$$\begin{aligned} K = H - n^{-1}\mathtt{X}H' &= -(1 - a^{q+1}\mathtt{X}^{p^m}) + \epsilon\mathtt{X}^{(p^m+n)/2}(\mathtt{X}-1)^{p^m} \\ &= -1 + a^{q+1}\mathtt{X}^{p^m} - \epsilon\mathtt{X}^{(p^m+n)/2} + \epsilon\mathtt{X}^{(p^m+n)/2+p^m}. \end{aligned}$$

The reciprocal of K is

$$K^* = \epsilon - \epsilon\mathtt{X}^{p^m} + a^{q+1}\mathtt{X}^{(p^m+n)/2} - \mathtt{X}^{(p^m+n)/2+p^m}.$$

Since $g \mid K$ and g is self-reciprocal, we also have $g = \pm g^* \mid K^*$. Thus g divides

$$K + \epsilon K^* = -1 + \epsilon^2 + (-\epsilon + \epsilon a^{q+1})\mathtt{X}^{(p^m+n)/2} = (a^{q+1} - 1)(1 + \epsilon\mathtt{X}^{(p^m+n)/2}).$$

This is a contradiction since

$$\frac{p^m + n}{2} < p^m + \frac{n-1}{2} = \deg g.$$

4.3.2 The Case $n - d > 1$

In this case,

$$G(\mathtt{X})=\frac{a^q\mathtt{X}^n+\mathtt{X}^{n-d}}{\mathtt{X}^d+a},$$

$$\begin{aligned}N(\mathtt{X},\mathtt{Y})=&\,a\frac{\mathtt{X}^{n-d}-\mathtt{Y}^{n-d}}{\mathtt{X}-\mathtt{Y}}+\Big[a^{q+1}\frac{\mathtt{X}^n-\mathtt{Y}^n}{\mathtt{X}-\mathtt{Y}}+\mathtt{X}^d\mathtt{Y}^d\frac{\mathtt{X}^{n-2d}-\mathtt{Y}^{n-2d}}{\mathtt{X}-\mathtt{Y}}\Big]\\&+a^q\mathtt{X}^d\mathtt{Y}^d\frac{\mathtt{X}^{n-d}-\mathtt{Y}^{n-d}}{\mathtt{X}-\mathtt{Y}},\end{aligned}$$

$$N^*(\mathtt{X},\mathtt{Y},\mathtt{Z})=Q(\mathtt{Z}^d),$$

where

$$\begin{aligned}Q(\mathtt{Z})=&\,a\frac{\mathtt{X}^{n-d}-\mathtt{Y}^{n-d}}{\mathtt{X}-\mathtt{Y}}\mathtt{Z}^2+\Big[a^{q+1}\frac{\mathtt{X}^n-\mathtt{Y}^n}{\mathtt{X}-\mathtt{Y}}+\mathtt{X}^d\mathtt{Y}^d\frac{\mathtt{X}^{n-2d}-\mathtt{Y}^{n-2d}}{\mathtt{X}-\mathtt{Y}}\Big]\mathtt{Z}\\&+a^q\mathtt{X}^d\mathtt{Y}^d\frac{\mathtt{X}^{n-d}-\mathtt{Y}^{n-d}}{\mathtt{X}-\mathtt{Y}}.\end{aligned}$$

We claim that

$$\gcd\Big(\frac{\mathtt{X}^{n-d}-\mathtt{Y}^{n-d}}{\mathtt{X}-\mathtt{Y}},\ a^{q+1}\frac{\mathtt{X}^n-\mathtt{Y}^n}{\mathtt{X}-\mathtt{Y}}+\mathtt{X}^d\mathtt{Y}^d\frac{\mathtt{X}^{n-2d}-\mathtt{Y}^{n-2d}}{\mathtt{X}-\mathtt{Y}}\Big)=1, \tag{4.3.18}$$

equivalently,

$$\gcd\Big(\frac{\mathtt{X}^{n-d}-1}{\mathtt{X}-1},\ a^{q+1}\frac{\mathtt{X}^n-1}{\mathtt{X}-1}+\mathtt{X}^d\frac{\mathtt{X}^{n-2d}-1}{\mathtt{X}-1}\Big)=1. \tag{4.3.19}$$

Let ζ be a root of $(\mathtt{X}^{n-d}-1)/(\mathtt{X}-1)$. If $\zeta\neq 1$, then

$$\begin{aligned}\Big(a^{q+1}\frac{\mathtt{X}^n-1}{\mathtt{X}-1}+\mathtt{X}^d\frac{\mathtt{X}^{n-2d}-1}{\mathtt{X}-1}\Big)\Big|_{\mathtt{X}=\zeta}&=\frac{1}{\zeta-1}\big(a^{q+1}(\zeta^n-1)+\zeta^d(\zeta^{n-2d}-1)\big)\\&=\frac{1}{\zeta-1}(a^{q+1}-1)(\zeta^n-1)\neq 0.\end{aligned}$$

If $\zeta=1$, then $n-d\equiv 0 \pmod p$, and

$$\Big(a^{q+1}\frac{\mathtt{X}^n-1}{\mathtt{X}-1}+\mathtt{X}^d\frac{\mathtt{X}^{n-2d}-1}{\mathtt{X}-1}\Big)\Big|_{\mathtt{X}=1}=a^{q+1}n+n-2d=n(a^{q+1}-1)\neq 0.$$

So (4.3.19) and (4.3.18) hold. Therefore $Q(\mathtt{Z})$ is a primitive polynomial over $\overline{\mathbb{F}}_q[\mathtt{X},\mathtt{Y}]$.

Let

$$\begin{aligned} Q_1(\mathtt{Z}) &= \Big[\Big(a\frac{\mathtt{X}^{n-d}-\mathtt{Y}^{n-d}}{\mathtt{X}-\mathtt{Y}}\Big)^{-1}Q(\mathtt{Z})\Big]\Big|_{\mathtt{Y}=1} \\ &= \mathtt{Z}^2+\frac{a^{q+1}\dfrac{\mathtt{X}^n-1}{\mathtt{X}-1}+\mathtt{X}^d\dfrac{\mathtt{X}^{n-2d}-1}{\mathtt{X}-1}}{a\dfrac{\mathtt{X}^{n-d}-1}{\mathtt{X}-1}}\mathtt{Z}+a^{q-1}\mathtt{X}^d \in \overline{\mathbb{F}}_q(\mathtt{X})[\mathtt{Z}]. \end{aligned} \tag{4.3.20}$$

Following the arguments in Section 4.3.1, we only have to prove the following two claims:

Claim 1. $Q(\mathtt{Z})$ is irreducible in $\overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y})[\mathtt{Z}]$.

Claim 2. Let z be a root of $Q_1(\mathtt{Z})$ and t be a prime divisor of d. Then z is not a t-th power in $\overline{\mathbb{F}}_q(\mathtt{X},z)$.

Proof of Claim 1

Assume to the contrary that $Q(\mathtt{Z})$ is reducible in $\overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y})[\mathtt{Z}]$.

First, assume that q is odd. The discriminant of $Q(\mathtt{Z})$ is

$$D=\Big[\frac{a^{q+1}(\mathtt{X}^n-\mathtt{Y}^n)}{\mathtt{X}-\mathtt{Y}}+\frac{\mathtt{X}^d\mathtt{Y}^d(\mathtt{X}^{n-2d}-\mathtt{Y}^{n-2d})}{\mathtt{X}-\mathtt{Y}}\Big]^2-\frac{4a^{q+1}\mathtt{X}^d\mathtt{Y}^d(\mathtt{X}^{n-d}-\mathtt{Y}^{n-d})^2}{(\mathtt{X}-\mathtt{Y})^2}.$$

By assumption, $D=\Delta^2$ for some $\Delta\in\overline{\mathbb{F}}_q[\mathtt{X},\mathtt{Y}]$. Then

$$\begin{aligned} \frac{4a^{q+1}\mathtt{X}^d\mathtt{Y}^d\left(\mathtt{X}^{n-d}-\mathtt{Y}^{n-d}\right)^2}{(\mathtt{X}-\mathtt{Y})^2} &= \Big(a^{q+1}\frac{\mathtt{X}^n-\mathtt{Y}^n}{\mathtt{X}-\mathtt{Y}}+\mathtt{X}^d\mathtt{Y}^d\frac{\mathtt{X}^{n-2d}-\mathtt{Y}^{n-2d}}{\mathtt{X}-\mathtt{Y}}+\Delta\Big) \\ &\quad\cdot\Big(a^{q+1}\frac{\mathtt{X}^n-\mathtt{Y}^n}{\mathtt{X}-\mathtt{Y}}+\mathtt{X}^d\mathtt{Y}^d\frac{\mathtt{X}^{n-2d}-\mathtt{Y}^{n-2d}}{\mathtt{X}-\mathtt{Y}}-\Delta\Big). \end{aligned}$$

The two factors on the right side are relatively prime. (This follows from (4.3.18).) Therefore, we may assume

$$\begin{cases} a^{q+1}\dfrac{\mathtt{X}^n-\mathtt{Y}^n}{\mathtt{X}-\mathtt{Y}}+\mathtt{X}^d\mathtt{Y}^d\dfrac{\mathtt{X}^{n-2d}-\mathtt{Y}^{n-2d}}{\mathtt{X}-\mathtt{Y}}+\Delta=2a^{(q+1)/2}\mathtt{X}^dU^2, \\ a^{q+1}\dfrac{\mathtt{X}^n-\mathtt{Y}^n}{\mathtt{X}-\mathtt{Y}}+\mathtt{X}^d\mathtt{Y}^d\dfrac{\mathtt{X}^{n-2d}-\mathtt{Y}^{n-2d}}{\mathtt{X}-\mathtt{Y}}-\Delta=2a^{(q+1)/2}\mathtt{Y}^dV^2, \end{cases} \tag{4.3.21}$$

for some $U, V \in \overline{\mathbb{F}}_q[\mathtt{X}, \mathtt{Y}]$ with

$$UV = \frac{\mathtt{X}^{n-d} - \mathtt{Y}^{n-d}}{\mathtt{X} - \mathtt{Y}}. \tag{4.3.22}$$

Then

$$\frac{a^{q+1}\left(\mathtt{X}^n - \mathtt{Y}^n\right)}{\mathtt{X} - \mathtt{Y}} + \frac{\mathtt{X}^d\mathtt{Y}^d\left(\mathtt{X}^{n-2d} - \mathtt{Y}^{n-2d}\right)}{\mathtt{X} - \mathtt{Y}} = a^{(q+1)/2}(\mathtt{X}^d U^2 + \mathtt{Y}^d V^2). \tag{4.3.23}$$

Let L denote the left side of (4.3.23). We have

$$\begin{aligned} L = {} & a^{q+1}(\mathtt{Y}^{n-1} + \mathtt{X}\mathtt{Y}^{n-2} + \cdots + \mathtt{X}^{n-1}) \\ & + \begin{cases} \mathtt{X}^d\mathtt{Y}^{n-d-1} + \mathtt{X}^{d+1}\mathtt{Y}^{n-d-2} + \cdots + \mathtt{X}^{n-d-1}\mathtt{Y}^d & \text{if } n \geq 2d, \\ -\mathtt{X}^{n-d}\mathtt{Y}^{d-1} - \mathtt{X}^{n-d+1}\mathtt{Y}^{d-2} - \cdots - \mathtt{X}^{d-1}\mathtt{Y}^{n-d} & \text{if } d+2 \leq n < 2d. \end{cases} \end{aligned}$$

If $d + 2 \leq n < 2d$, the coefficient of $\mathtt{X}^{d-1}\mathtt{Y}^{n-d}$ in L is $a^{q+1} - 1 \neq 0$, while the coefficient of $\mathtt{X}^{d-1}\mathtt{Y}^{n-d}$ on the right side of (4.3.23) is 0, which is a contradiction. Hence Theorem 4.10 (iii) holds. In particular, $\gcd(n - d, q - 1) = 1$.

Since

$$\Delta(\mathtt{Y}, \mathtt{X})^2 = D(\mathtt{Y}, \mathtt{X}) = D(\mathtt{X}, \mathtt{Y}) = \Delta(\mathtt{X}, \mathtt{Y})^2.$$

we have $\Delta(\mathtt{Y}, \mathtt{X}) = \pm\Delta(\mathtt{X}, \mathtt{Y})$. If $\Delta(\mathtt{Y}, \mathtt{X}) = \Delta(\mathtt{X}, \mathtt{Y})$, then by (4.3.21), $\mathtt{X}^d U(\mathtt{X}, \mathtt{Y})^2 = \mathtt{Y}^d U(\mathtt{Y}, \mathtt{X})^2$. Then $\mathtt{Y} \mid U(\mathtt{X}, \mathtt{Y})$, which is a contradiction to (4.3.22). Hence $\Delta(\mathtt{Y}, \mathtt{X}) = -\Delta(\mathtt{X}, \mathtt{Y})$, and by (4.3.21),

$$U(\mathtt{Y}, \mathtt{X})^2 = V(\mathtt{X}, \mathtt{Y})^2. \tag{4.3.24}$$

By (4.3.24) and (4.3.22), we have

$$U(\mathtt{X}, \mathtt{Y})^2 = \alpha \prod_{i=1}^{(n-d-1)/2} (\mathtt{X} - \epsilon_i\mathtt{Y})^2, \tag{4.3.25}$$

$$V(\mathtt{X}, \mathtt{Y})^2 = \alpha^{-1} \prod_{i=1}^{(n-d-1)/2} (\mathtt{X} - \epsilon_i^{-1}\mathtt{Y})^2, \tag{4.3.26}$$

where $\alpha, \beta \in \overline{\mathbb{F}}_q$ and $\epsilon_i \in \overline{\mathbb{F}}_q^*$ are such that

$$\frac{\mathtt{X}^{n-d} - \mathtt{Y}^{n-d}}{\mathtt{X} - \mathtt{Y}} = \prod_{i=1}^{(n-d-1)/2} \left[(\mathtt{X} - \epsilon_i\mathtt{Y})(\mathtt{X} - \epsilon_i^{-1}\mathtt{Y})\right].$$

We have

$$\begin{aligned} \alpha &= U(1,0)^2 && \text{(by (4.3.25))} \\ &= V(0,1)^2 && \text{(by (4.3.24))} \\ &= \alpha^{-1} \prod_{i=1}^{(n-d-1)/2} \epsilon_i^{-2} && \text{(by (4.3.26)).} \end{aligned}$$

It follows that

$$\alpha^2 = \prod_{i=1}^{(n-d-1)/2} \epsilon_i^{-2}. \tag{4.3.27}$$

On the other hand, comparing the coefficients of $\mathtt{X}^{n-1}$ in (4.3.23) gives $a^{q+1} = a^{(q+1)/2} \cdot \alpha$, i.e., $\alpha = a^{(q+1)/2}$. Since the ϵ_i's are roots of $\mathtt{X}^{n-d} - 1$, we have

$$a^{(q+1)(n-d)} = \alpha^{2(n-d)} = 1 \qquad \text{(by (4.3.27)).}$$

This, combined with $a^{(q+1)(q-1)} = 1$ and $\gcd(n-d, q-1) = 1$, implies that $a^{q+1} = 1$, which is a contradiction.

Next, assume that q is even. Since $Q(\mathtt{Z})$ is assumed to be reducible over $\overline{\mathbb{F}}_q(\mathtt{X},\mathtt{Y})$, there are $A, B \in \overline{\mathbb{F}}_q[\mathtt{X},\mathtt{Y}]$, relatively prime, such that

$$\frac{a^{q+1}\mathtt{X}^d\mathtt{Y}^d\Big(\dfrac{\mathtt{X}^{n-d}+\mathtt{Y}^{n-d}}{\mathtt{X}+\mathtt{Y}}\Big)^2}{\Big(a^{q+1}\dfrac{\mathtt{X}^n+\mathtt{Y}^n}{\mathtt{X}+\mathtt{Y}} + \mathtt{X}^d\mathtt{Y}^d\dfrac{\mathtt{X}^{n-2d}+\mathtt{Y}^{n-2d}}{\mathtt{X}+\mathtt{Y}}\Big)^2} = \Big(\frac{A}{B}\Big)^2 + \frac{A}{B} = \frac{A(A+B)}{B^2}.$$

The numerator and the denominator on the left side are relatively prime (by (4.3.18)). Thus

$$B = a^{q+1}\frac{\mathtt{X}^n+\mathtt{Y}^n}{\mathtt{X}+\mathtt{Y}} + \mathtt{X}^d\mathtt{Y}^d\frac{\mathtt{X}^{n-2d}+\mathtt{Y}^{n-2d}}{\mathtt{X}+\mathtt{Y}} \tag{4.3.28}$$

and

$$A(A+B) = a^{q+1}\mathtt{X}^d\mathtt{Y}^d\Big(\frac{\mathtt{X}^{n-d}+\mathtt{Y}^{n-d}}{\mathtt{X}+\mathtt{Y}}\Big)^2.$$

We may assume that

$$\begin{cases} A = \mathtt{X}^d U^2, \\ A+B = \mathtt{Y}^d V^2, \end{cases}$$

for some $U, V \in \overline{\mathbb{F}}_q[\mathtt{X},\mathtt{Y}]$ such that $UV = (\mathtt{X}^{n-d}+\mathtt{Y}^{n-d})/(\mathtt{X}+\mathtt{Y})$. Then

$$B = \mathtt{X}^d U^2 + \mathtt{Y}^d V^2. \tag{4.3.29}$$

By (4.3.28),

$$
\begin{aligned}
B = & a^{q+1}(\mathtt{Y}^{n-1} + \mathtt{X}\mathtt{Y}^{n-2} + \cdots + \mathtt{X}^{n-1}) \\
& + \begin{cases} \mathtt{X}^d\mathtt{Y}^{n-d-1} + \mathtt{X}^{d+1}\mathtt{Y}^{n-d-2} \cdots + \mathtt{X}^{n-d-1}\mathtt{Y}^d & \text{if } n \geq 2d, \\ \mathtt{X}^{n-d}\mathtt{Y}^{d-1} + \mathtt{X}^{n-d+1}\mathtt{Y}^{d-2} + \cdots + \mathtt{X}^{d-1}\mathtt{Y}^{n-d} & \text{if } d+2 \leq n < 2d. \end{cases}
\end{aligned}
$$

Since we assume $d > 1$ and $n - d > 1$, the coefficient of $\mathtt{X}\mathtt{Y}^{n-2}$ in (4.3.28) is $a^{q+1} \neq 0$. (Even if we allowed $d = 1$ or $n - d = 1$, the coefficient of $\mathtt{X}\mathtt{Y}^{n-2}$ in (4.3.28) would be $a^{q+1} + 1$, which is still nonzero.) However, the coefficient of $\mathtt{X}\mathtt{Y}^{n-2}$ in (4.3.29) is 0, which is a contradiction.

Proof of Claim 2

Recall that $Q_1(\mathtt{Z})$ is given in (4.3.20). Let z be a root of $Q_1(Z)$ and t be a prime divisor of d. Assume to the contrary that z is a t-th power in $\overline{\mathbb{F}}_q(\mathtt{X}, z)$. Let $\overline{(\ )}$ be the nonidentity automorphism in $\mathrm{Aut}(\overline{\mathbb{F}}_q(\mathtt{X}, z)/\overline{\mathbb{F}}_q(\mathtt{X}))$. Then

$$
z\bar{z} = a^{q-1}\mathtt{X}^d, \tag{4.3.30}
$$

$$
\begin{aligned}
z + \bar{z} &= -\frac{a^{q+1}\dfrac{\mathtt{X}^n - 1}{\mathtt{X} - 1} + \mathtt{X}^d\dfrac{\mathtt{X}^{n-2d} - 1}{\mathtt{X} - 1}}{a\dfrac{\mathtt{X}^{n-d} - 1}{\mathtt{X} - 1}} \\
&= -\frac{(a^{q+1} - 1)\dfrac{\mathtt{X}^d - 1}{\mathtt{X} - 1} + (a^{q+1}\mathtt{X}^d + 1)\dfrac{\mathtt{X}^{n-d} - 1}{\mathtt{X} - 1}}{a\dfrac{\mathtt{X}^{n-d} - 1}{\mathtt{X} - 1}}.
\end{aligned} \tag{4.3.31}
$$

Write $n - d = p^m d'$, where $p \nmid d'$, and let ζ be a primitive d'th root of unity. Let $\mathfrak{p}$ be the place of the rational function field $\overline{\mathbb{F}}_q(\mathtt{X})$ which is the zero of $\mathtt{X} - \zeta$, and let $\mathfrak{P}$ be a place of $\overline{\mathbb{F}}_q(\mathtt{X}, z)$ such that $\mathfrak{P} \mid \mathfrak{p}$. Then $\mathfrak{P}$ is unramified over $\mathfrak{p}$ ([47, III 7.3 (b) and 7.8 (b)]). From (4.3.30) and (4.3.31), we have

$$
\nu_{\mathfrak{p}}(z\bar{z}) = 0, \tag{4.3.32}
$$

$$
\nu_{\mathfrak{p}}(z + \bar{z}) = \begin{cases} -p^m & \text{if } d' > 1, \\ -p^m + 1 & \text{if } d' = 1, \end{cases} \tag{4.3.33}
$$

(The proof of (4.3.33) is similar to that of (4.3.10) and uses the assumption $n-d>1$ in the case $d'=1$.) Therefore,

$$\nu_{\mathfrak{P}}(z)+\nu_{\mathfrak{P}}(\bar{z})=0,$$

$$\nu_{\mathfrak{P}}(z+\bar{z})=\begin{cases}-p^m & \text{if } d'>1,\\ -p^m+1 & \text{if } d'=1,\end{cases}$$

and it follows that

$$\{\nu_{\mathfrak{P}}(z),\nu_{\mathfrak{P}}(\bar{z})\}=\begin{cases}\{\pm p^m\} & \text{if } d'>1,\\ \{\pm(p^m-1)\} & \text{if } d'=1.\end{cases}$$

Since z is a t-th power in $\overline{\mathbb{F}}_q(\mathtt{X},z)$, we have $t\mid\nu_{\mathfrak{P}}(z)$. If $d'>1$, then $t=p$. It follows from $t\mid d$ and $t\mid n-d$ that $\gcd(n,d)\neq 1$, which is a contradiction. So we must have $d'=1$ and $n-d=p^m$, $m>0$. Then $t\mid p^m-1=n-d-1$. Since $t\mid\gcd(n-d-1,d)=\gcd(n-1,d)$, where $\gcd(n-1,d)$ is a power of 2 (by assumption), we have $t=2$. Consequently, p is odd. The equation $Q_1(z)=0$ can be written as

$$u^2=\delta,$$

where

$$u=z-\gamma,$$

$$\gamma=-\frac{1}{2}\frac{(a^{q+1}-1)\dfrac{\mathtt{X}^d-1}{\mathtt{X}-1}+(a^{q+1}\mathtt{X}^d+1)(\mathtt{X}-1)^{p^m-1}}{a(\mathtt{X}-1)^{p^m-1}},$$

and

$$\delta=\gamma^2-a^{q-1}\mathtt{X}^d.$$

By assumption, there exist $\alpha,\beta\in\overline{\mathbb{F}}_q(\mathtt{X})$ such that

$$(\alpha u+\beta)^2=u+\gamma,$$

i.e.,

$$\alpha^2\delta+\beta^2+2\alpha\beta u=u+\gamma.$$

So

$$\begin{cases}\alpha^2\delta+\beta^2=\gamma,\\ 2\alpha\beta=1.\end{cases}$$

Letting $\tau = \alpha/\beta$, we have

$$1 + \delta\tau^2 - 2\gamma\tau = 0 \tag{4.3.34}$$

and

$$\tau = 2\alpha^2. \tag{4.3.35}$$

Equation (4.3.34) has an explicit solution

$$\tau = \frac{1}{\delta}(\gamma \pm a^{(q-1)/2}\mathtt{X}^{d/2}) = \frac{1}{\gamma \mp a^{(q-1)/2}\mathtt{X}^{d/2}} = \frac{-2a(\mathtt{X}-1)^{p^m-1}}{h(\mathtt{X})},$$

where

$$h(\mathtt{X}) = (a^{q+1}-1)\frac{\mathtt{X}^d-1}{\mathtt{X}-1} + (a^{q+1}\mathtt{X}^d+1)(\mathtt{X}-1)^{p^m-1} + 2\epsilon\mathtt{X}^{d/2}(\mathtt{X}-1)^{p^m-1}$$

and $\epsilon = \pm a^{(q+1)/2}$. By (4.3.35), $h(\mathtt{X})$ is a square in $\overline{\mathbb{F}}_q[\mathtt{X}]$, say $h = g^2$ for some $g \in \overline{\mathbb{F}}_q[\mathtt{X}]$ with $\deg g = (d+p^m-1)/2$. Note that

$$\begin{aligned} h(\mathtt{X}) &= a^{q+1}\Big(\frac{\mathtt{X}^d-1}{\mathtt{X}-1} + \mathtt{X}^d\frac{\mathtt{X}^{p^m}-1}{\mathtt{X}-1}\Big) + \Big(\frac{\mathtt{X}^{p^m}-1}{\mathtt{X}-1} - \frac{\mathtt{X}^d-1}{\mathtt{X}-1}\Big) + 2\epsilon\mathtt{X}^{d/2}\frac{\mathtt{X}^{p^m}-1}{\mathtt{X}-1} \\ &= a^{q+1}(1+\cdots+\mathtt{X}^{p^m+d-1}) + (\mathtt{X}^d+\cdots+\mathtt{X}^{p^m-1}) + 2\epsilon(\mathtt{X}^{d/2}+\cdots+\mathtt{X}^{p^m+d/2-1}), \end{aligned}$$

which is self-reciprocal. It follows that $g^* = \pm g$, where g^* is the reciprocal polynomial of g. Let

$$H = (\mathtt{X}-1)h = (a^{q+1}-1)(\mathtt{X}^d-1) + (a^{q+1}\mathtt{X}^d+1)(\mathtt{X}-1)^{p^m} + 2\epsilon\mathtt{X}^{d/2}(\mathtt{X}-1)^{p^m}.$$

Then

$$H' = (a^{q+1}-1)d\mathtt{X}^{d-1} + a^{q+1}d\mathtt{X}^{d-1}(\mathtt{X}-1)^{p^m} + \epsilon d\mathtt{X}^{d/2-1}(\mathtt{X}-1)^{p^m}.$$

Let

$$K = -H + d^{-1}\mathtt{X}H' = a^{q+1} - \mathtt{X}^{p^m} + \epsilon\mathtt{X}^{d/2} - \epsilon\mathtt{X}^{p^m+d/2}.$$

The reciprocal of K is

$$K^* = -\epsilon + \epsilon\mathtt{X}^{p^m} - \mathtt{X}^{d/2} + a^{q+1}\mathtt{X}^{p^m+d/2}.$$

Since $g \mid K$, we have $g = \pm g^* \mid K^*$. Hence g divides

$$\epsilon K + K^* = (a^{q+1}-1)(\epsilon + \mathtt{X}^{d/2}).$$

This is a contradiction since

$$\frac{d}{2} < \frac{d + p^m - 1}{2} = \deg g.$$

The proof of Theorem 4.10 is now complete.

4.4 Final Remarks

Theorem 4.10 leaves ample room for improvement, by which we mean nonexistence results of PB under conditions that are weaker than or not covered by (i) – (iii) in Theorem 4.10. While some improvements may be obtained by fine tuning the techniques demonstrated in the present chapter, breakthroughs may require new methods or substantially new elements in the current approach.

The cases $d - n = \pm 1$ appear to be special. These are the two cases not covered by Theorem 4.10 and there are indeed infinite classes of PBs in these two cases with $e = 2$ (Results 4.2 and 4.4). A natural question is this: When $d - n = \pm 1$ and $e > 2$, are there infinite classes of PBs of the form $f_{q,e,n,d,a}(\mathtt{X}) = \mathtt{X}^n(\mathtt{X}^{d(q-1)} + a)$ of $\mathbb{F}_{q^e}$?

Chapter 5

Permutation quadrinomials in characteristic 2

Permutation trinomials with Niho exponents of the form $f(\mathtt{X}) = \mathtt{X} + a_1\mathtt{X}^{s_1(2^m-1)+1} + a_2\mathtt{X}^{s_2(2m-1)+1} + a_3\mathtt{X}^{s_3(2m-1)+1} \in \mathbb{F}_{q^2}[\mathtt{X}]$, have attracted much interest in recent years. See for example [7, 25]. The parameters s_1, s_2 should be read modulo $q+1$, for $q = 2^m$, since they are multiplied by $q-1$ and the exponent is taken modulo q^2-1. 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 has been done in that direction. See [28, 26].

However, the situation for permutation quadrinomials is different. Recently, Tu et al. investigated the case of $(s_1, s_2, s_3) = (-1, 1, 2)$ under some restrictive conditions [49]. In [50] 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 k is a positive integers and $(s_1, s_2, s_3) = (\frac{1}{4}, 1, \frac{3}{4})$. The fractional number on the exponent, say $1/h$ should be read as the inverse of h modulo $q-1$, which is well defined since $\gcd(h, q-1) = 1$. In the last case they suggested that the sufficient conditions of [50, Theorem 1.4] were also necessary (for $m > 5$).

In this chapter we aim to answer that question. We will use the connections between algebraic curves and permutation polynomials (see Subsection 1.1.5) to prove necessary conditions for a polynomial to be a PP. In particular we investigate all the cases given in [50, Theorem 1.4], showing in most cases that those conditions are also necessary.

5.1 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 $\theta_1 = 1 + a_1^{q+1} + a_2^{q+1} + a_3^{q+1}$, $\theta_2 = a_1^q + a_3 a_2^q$, $\theta_3 = a_3 + a_2 a_1^q$, $\theta_4 = a_1^{q+1} + a_3^{q+1}$ and $\theta_4' = \theta_1 + \theta_4 = 1 + a_2^{q+1}$. Note that

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

We now summarize the previous results we need in this chapter. See [50, B.] for more details.

Theorem 5.1 ([50, Theorems 1.1, 1.3 and 1.4]). *The following hold.*

1. *Let $n = 2m$ and $k < m$ be two positive integers such that $\gcd(2^k - 1, 2^m + 1) = 1$. Let $(s_1, s_2, s_3) = (\frac{-1}{2^k-1}, 1, \frac{2^k}{2^k-1})$. Denote $d = ord_2(\gcd(m,k))$. Let $a_1, a_2, a_3 \in \mathbb{F}_{q^2}$. 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*

$$\theta_1 \neq 0, \quad \left(\frac{\theta_2}{\theta_1}\right)^{2^k} = \frac{\theta_3}{\theta_1} \quad \textit{and} \quad \mathrm{Tr}_{\frac{2^m}{2^d}}\left(\frac{\theta_4}{\theta_1}\right) = 0$$

2. *Let $n = 2m$ and $k < m$ be two positive integers such that $\gcd(2^k + 1, 2^m + 1) = 1$. Let $(s_1, s_2, s_3) = (\frac{1}{2^k+1}, 1, \frac{2^k}{2^k+1})$. Denote $d = ord_2(\gcd(m,k))$. Let $a_1, a_2, a_3 \in \mathbb{F}_{q^2}$. 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*

$$\theta_1 \neq 0, \quad \left(\frac{\theta_2}{\theta_1}\right)^{2^k} = \frac{\theta_3^{2^k}}{\theta_1} \quad \textit{and} \quad \mathrm{Tr}_{\frac{2^m}{2^d}}\left(\frac{\theta_4}{\theta_1}\right) = 0$$

3. *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*

$$\theta_1 \neq 0, \quad \theta_2 = 0 \quad \textit{and} \quad a_3 \in \mu_{q+1}, \quad a_3 \notin \{x^3 | x \in \mu_{q+1}\} \tag{5.1.1}$$

or

$$\theta_1 \neq 0, \theta_2 \neq 0, \theta_4 = 0, \theta_3 = \theta_2^{2q-1} \textit{ and } x^3 + x + \frac{\theta_1^2}{\theta_2^{q+1}} = 0 \textit{ has no solutions over } \mathbb{F}_q. \tag{5.1.2}$$

The aim of this chapter is to answer the question left open by the authors in [50, Theorem 1.4] and prove that Condition (5.1.1) and (5.1.2) are also necessary. When $m \geq 9$ we managed to show that Condition (5.1.1) is indeed necessary, whereas we found Condition (5.1.2) harder to invert. However, if we limit ourselves to case $\theta_4 = 0$, we obtain that Condition (5.1.2) is also necessary.

The main result is stated in the following theorem.

Theorem 5.2 ([42, Theorem 2.2])**.** *Let $m \geq 9$ be an integer and $q = 2^m$. With the notation above, if the polynomial*

$$f(\mathtt{X}) = \mathtt{X} + a_1\mathtt{X}^{s_1(q-1)+1} + a_2\mathtt{X}^{s_2(q-1)+1} + a_3\mathtt{X}^{s_3(q-1)+1}$$

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

- *if $\theta_2 = 0$ then either $\theta_1 = 0$ and m is odd, or $\theta_1 \neq 0$ and $a_3 \in \mu_{q+1} \setminus \Gamma$, where $\Gamma = \{x^3 | x \in \mu_{q+1}\}$;*
- *if $\theta_2 \neq 0$ and $\theta_4 = 0$, then $\theta_1 \neq 0$, $\theta_3 = \theta_2^{2q-1}$ and*

$$x^3 + x + \frac{\theta_1^2}{\theta_2^{q+1}} = 0 \tag{5.1.3}$$

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

The only case still open is when $\theta_2 \neq 0$ and $\theta_4 \neq 0$. However, computer-aided investigations seem to confirm that the conjecture is still true.

5.2 Algebraic curves and necessary conditions

In this section we use the methods presented in the first chapter to investigate the necessary conditions for f being a PP. From Theorem 1.70 we know that $f(\mathtt{X}) = \mathtt{X}h(\mathtt{X}^{q-1})$ permutes $\mathbb{F}_{q^2}$ if and only $g(x) = xh(x)^{q-1}$ permutes the set μ_{q+1} of the $(q+1)$-roots of unity in $\mathbb{F}_{q^2}$. In [50] the authors showed that this is equivalent to prove that the rational function

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

permutes μ_{q+1}. Let $\mathcal{C}$ be the plane curve associated to $p(x)$, with equation:

$$\begin{aligned} F(X,Y) =& \frac{(a_1Y + a_2Y^4 + a_3Y^3 + 1)\,(X^3{a_1}^q + {a_2}^q + {a_3}^qX + X^4)}{X+Y} + \\ &+ \frac{(a_1X + a_2X^4 + a_3X^3 + 1)\,(Y^3{a_1}^q + {a_2}^q + Y{a_3}^q + Y^4)}{X+Y} = 0. \end{aligned}$$

$\mathcal{C}$ 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 $X \neq Y$.

Choose an element $e \in \mathbb{F}_{q^2}$ such that $e^q = e + 1$. Every $x \in \mu_{q+1}$ different from 1 can be written as $x = \frac{X+e}{X+e+1}$, where X runs over $\mathbb{F}_q$. Following this idea we consider the rational transformation:

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

Let $\mathcal{X}$ be the curve defined by $H(X, Y) = (X+e+1)^3(Y+e+1)^3F(\phi(X, Y))$, then the following hold.

Lemma 5.3. *The curve $\mathcal{X}$ is $\mathbb{F}_q$-rational and $\mathbb{F}_{q^2}$-birationally equivalent to $\mathcal{C}$.*

Proof. By direct checking, $\mathcal{X}$ is $\mathbb{F}_q$-rational. Consider the rational transformation defined by

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

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

Since $\mathcal{C}$ and $\mathcal{X}$ are isomorphic, we can study the properties of $\mathcal{C}$ to obtain information on $\mathcal{X}$.

Proposition 5.4. *Let $q \geq 512$. If $f(\mathtt{X}) \in \mathbb{F}_{q^2}[\mathtt{X}]$ 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 $\mathcal{X}$ is absolutely irreducible over $\mathbb{F}_q$. Since $\mathcal{X}$ has degree at most 6, the Hasse-Weil bound implies that $\mathcal{X}$ has at least an affine rational point (a, b) with $a \neq b$ whenever

$$q + 1 - 20\sqrt{q} - 12 \geq 0, \tag{5.2.1}$$

where 12 is the maximum number of points belonging either to the line $x = y$ or to the infinity line. Equation (5.2.1) is satisfied for every integer greatest than 421. Thus, if $q = 2^m \geq 512$, $\mathcal{X}$ 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 $f(\mathtt{X})$ being a PP of $\mathbb{F}_{q^2}$. □

Proposition 5.4 allows us to focus on $\mathcal{C}$ to obtain necessary conditions on $f(\mathtt{X})$. 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 when $\mathcal{C}$ is either 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. Along with this view, the curve $\mathcal{C}$ becomes

$$\begin{aligned}\mathcal{C}\colon \theta_3^q + \theta_3 X^3Y^3 + \theta_4 xY(X+Y) + \theta_4'(X+Y)^3 + \\ + \theta_2(XY + (X+Y)^2) + \theta_2^q(X^2Y^2 + XY(X+Y)^2) = 0.\end{aligned} \tag{5.2.2}$$

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

$$\mathcal{D}\colon \theta_3^q + \theta_4' u^3 + \theta_4 uv + \theta_3 v^3 + \theta_2(u^2+v) + \theta_2^q v(u^2+v) = 0, \tag{5.2.3}$$

which is the quotient curve $\mathcal{C}/G$. In the next sections we will study $\mathcal{D}$ to find information about $\mathcal{C}$.

5.3 Case $\theta_2 = 0$

We first consider the case $\theta_1 = 0$.

Proposition 5.5. *Let $\theta_2 = 0$. If $\theta_1 = 0$ then the equation of $\mathcal{C}$ is*

$$\mathcal{C}\colon X^3 + Y^3 = 0.$$

Proof. Since $\theta_1 = \theta_2 = 0$ and $\theta_2^{q+1} = \theta_3^{q+1}$, the equation of $\mathcal{D}$ is

$$u(u^2+v) = 0$$

so $\mathcal{C}$ has equation

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

which is exactly the claim. □

Corollary 5.6. *If $\theta_1 = \theta_2 = 0$ then f is a PP if and only if m is an odd integer.*

Proof. f is a PP of $\mathbb{F}_{q^2}$ if and only if the set $\mathcal{C} \cap \mu_{q+1}^2$ is either empty or it has solutions lying on $X+Y=0$. Since the equation of $\mathcal{C}$ is $X^3+Y^3=0$, f is a PP is and only if there are no elements $z \in \mathbb{F}_{q^2}$ satisfying $z^3=1$ and $z^{q+1}=1$, which is equivalent to m be odd (and hence $3|q+1$). □

Now we work out the case $\theta_1 \neq 0$. In the following remark, we recall some properties from [50].

Remark 5.7. When $\theta_2 = 0$ and $\theta_1 \neq 0$ the following hold

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

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

$$F(X,Y) = a_3^q + a_3X^3Y^3 + a_3^{q+1}XY(X+Y) + (X+Y)^3$$

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

$$G(u,v) = a_3^q + u^3 + a_3^{q+1}uv + a_3v^3.$$

Proposition 5.8. *The curve $\mathcal{D}$ defined by Equation* (5.2.3) *is absolutely irreducible if and only if $a_3 \notin U$.*

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 solution 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 $a_3 \notin U$. □

Remark 5.9. 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 5.10. *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, we obtain the following equation for $\mathcal{C}'$,

$$(a_{00} + a_{10}X + a_{20}X^2 + a_{30}X^3 + a_{01}Y + a_{11}XY + a_{21}X^2Y + a_{02}Y^2 + a_{12}XY^2 + a_{03}Y^3)$$
$$(a_{00} + a_{01}X + a_{02}X^2 + a_{03}X^3 + a_{10}Y + a_{11}XY + a_{12}X^2Y + a_{20}Y^2 + a_{21}XY^2 + a_{30}Y^3) = 0 \tag{5.3.1}$$

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, by a straightforward computation, the only possible equation for $\mathcal{C}'$ is

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

This means that we need to require $a_3^{q+1} + 1 = 0$, that is $a_3 \in U$. □

Corollary 5.11. *Let $a_3 \notin U$. The curve $\mathcal{C}$ is absolutely irreducible.*

Proof. Proposition 5.8 implies that for $a_3 \notin U$ the curve $\mathcal{D}$ is absolutely irreducible. The proof follows from Remark 5.9 together with Proposition 5.10. □

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

Lemma 5.12. *Let $q = 2^m$ and let a_3 be a cube in U. Then the equation $x^3 = a_3$ admits exactly 3 solutions over $\mathbb{F}_{q^2}$.*

Proof. From [20, 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 5.13. *Let $\mathcal{D}$ be the curve with equation* (5.2.3)*. Let a_3 be an element of U and $\mathcal{D}\colon G(u,v)=0$. Then $G(u,v)$ is irreducible over $\mathbb{F}_{q^2}$ if and only if $a_3 \in \Gamma$, where $\Gamma = \{$non-cubes in $U\}$. Moreover, if $a_3 \in U \setminus \Gamma$, $\mathcal{D}$ is the union of three (absolutely irreducible) linear components over $\mathbb{F}_{q^2}$.*

Proof. From Proposition 5.8 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 5.12 $\mathcal{D}$ has exactly three singular (double) points defined over $\mathbb{F}_{q^2}$ if and only if $a_3 \in \mu_{q+1} \setminus \Gamma$. Moreover, in that case, $\mathcal{D}$ is the union of three (non-concurrent) lines passing through these points. □

Corollary 5.14. *When $a_3 \in U \setminus \Gamma$, $\mathcal{D}$ decomposes as follows:*

$$\mathcal{D}\colon (u+\alpha_1 v+\alpha_1^{-1})(u+\alpha_2 v+\alpha_2^{-1})(u+\alpha_3 v+\alpha_3^{-1})=0$$

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

$$F(X,Y) = a_3^q + a_3X^3Y^3 + a_3^{q+1}XY(X+Y) + (X+Y)^3$$

Proposition 5.15. *Let $a_3 \in U \setminus \Gamma$. 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 5.14 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 5.16. *Let $a_3 \in U \setminus \Gamma$. Then the set $\mathcal{C} \cap \mu_{q+1}^2$ is non-empty.*

Proof. The claim follows since $a_3 \in U$ (and hence α_i). □

5.4 $\theta_2 \neq 0$ and $\theta_4 = 0$

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

$$\theta_2^{q+1} + \theta_3^{q+1} = 0. \tag{5.4.1}$$

The equation of $\mathcal{C}$ becomes

$$\mathcal{C}\colon \theta_3^q + \theta_3 X^3 Y^3 + \theta_1 (X+Y)^3 + \theta_2 (XY + (X+Y)^2) + \theta_2^q (X^2Y^2 + XY(X+Y)^2) = 0, \tag{5.4.2}$$

while $\mathcal{D}$ has equation

$$\mathcal{D}\colon \theta_3^q + \theta_1 u^3 + \theta_3 v^3 + \theta_2 (u^2+v) + \theta_2^q v(u^2+v) = 0.$$

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

Proposition 5.17. *$\mathcal{C}$ 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 form an orbit under $\mathfrak{G}$. The union of two such cubics has equation $F'(X,Y) = 0$, where $F'(X,Y)$ is defined as

$$\begin{aligned}&(a_{00} + a_{10}X + a_{20}X^2 + a_{30}X^3 + a_{01}Y + a_{11}XY + a_{21}X^2Y + a_{02}Y^2 + a_{12}XY^2 + a_{03}Y^3)\\ &(a_{00} + a_{01}X + a_{02}X^2 + a_{03}X^3 + a_{10}Y + a_{11}XY + a_{12}X^2Y + a_{20}Y^2 + a_{21}XY^2 + a_{30}Y^3) = 0.\end{aligned} \tag{5.4.3}$$

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 $\mathcal{C}$). We proceed as follows: first, we show that when $\theta_1 = 0$ the polynomial $f(x)$ is not a PP. After that, we work out the case $\theta_1 \neq 0$ and we factorize $\mathcal{D}$ under precise conditions.

Proposition 5.18. *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

$$u^2 v \theta_2^q + v^2 \theta_2^q + \theta_3^q + \theta_2 u^2 + \theta_2 v + \theta_3 v^3 = 0$$

and the partial derivatives system is made by the single equation

$$\frac{\partial h}{\partial v} = \theta_2 + \theta_2^q u^2 + \theta_3 v^2 = 0$$

which implies

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

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

$$v^2 \theta_2^{2q} + \theta_2^q \theta_3^q + \theta_2^2 + \theta_2 \theta_3 v^2 = 0. \tag{5.4.4}$$

Therefore, if $\theta_3 \neq \theta_2^{2q-1}$, equation (5.4.4), together with equation (5.4.1), 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:

$$v^3 \theta_2^{2q-1} + \theta_2^{2-q} + v\theta_2^q \left(u^2 + v\right) + \theta_2 \left(u^2 + v\right) = 0 \tag{5.4.5}$$

Note that the resultant between $h(x)$ and the derivative with respect to v is 0. This means that they share a common factor. Indeed, we have the following factorization for (5.4.5):

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

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

Proposition 5.19. *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

$$\begin{cases} \theta_1 u^2 = 0 \\ \theta_2 + \theta_2^q u^2 + \theta_3 v^2 = 0 \end{cases} \tag{5.4.6}$$

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

Propositions 5.18 and 5.19 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

$$(\theta_2 + \alpha\theta_2^q)U^2 + (\theta_2^q + \alpha\theta_3)V^2 + \theta_1 U^3 + \theta_2^q U^2 V + \theta_3 V^3 = 0. \tag{5.4.7}$$

Proposition 5.20. *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 5.21. *Let $\theta_2 \neq 0$ and $\theta_4 = 0$. If $\theta_1 = 0$ then $\mathcal{C} \cap \mu_{q+1}^2$ is non-empty, whereas if $\theta_1 \neq 0$ and $\theta_2^{2q-1} \neq \theta_3$ then $\mathcal{C}$ is absolutely irreducible over $\mathbb{F}_{q^2}$*

Proof. The proof is obtained summing up previous propositions. More precisely, if $\theta_1 = 0$ and $\theta_2^{2q-1} = \theta_3$, from Proposition 5.18, we have

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

This means that $(1/\theta_2^{q-1}, 1) \in \mathcal{C} \cap \mu_{q+1}^2$. On the other hand, if $\theta_2^{2q-1} \neq \theta_3$, the proof follows from Proposition 5.19 and 5.20. □

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

$$\theta_1 + z + \frac{1}{\theta_2^{q+1}} z^3 = 0 \tag{5.4.8}$$

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 (5.4.8) are in $\mathbb{F}_q$. The claim is obtained by standard theory, see for example [20, Pg. 20]. □

Proposition 5.23. *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 $\mathbb{F}_{q^2}$. In particular, $\mathcal{C} \cap \mu_{q+1}^2$ is a non-empty set.*

Proof. Every solution of Equation (5.4.8) in $\mathbb{F}_{q^2}$ gives a linear component of $\Phi(\mathcal{D})$ (and $\mathcal{D}$). From Lemma 5.22, 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 (5.4.8). Going back to the curve $\mathcal{D}$ we obtain the following decomposition:

$$\mathcal{D}\colon (z_1u + \theta_2^q v + \theta_2^q \alpha)(z_2u + \theta_2^q v + \theta_2^q \alpha)(z_3u + \theta_2^q v + \theta_2^q \alpha) = 0$$

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 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 (5.4.8) 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, the point $(\frac{\theta_2+z_1}{\theta_2^q+z_1}, 1) \in \mathcal{C} \cap \mu_{q+1}^2$. □

Corollary 5.24. *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 a PP of $\mathbb{F}_{q^2}$.*

5.5 Proof of main Theorem 5.2

If $\theta_2 = 0$, the proof is obtained summing up the results of Corollary 5.6 (for $\theta_1 = 0$) and those of Corollary 5.11 and Corollary 5.16 (for $\theta_1 \neq 0$). When $\theta_2 \neq 0$ and $\theta_4 = 0$, the proof follows from Corollary 5.24, since the equation

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

is equivalent to the equation (5.1.3) after substituting $z = \theta_2^{q+1}x$.

Appendix A

We provide a proof of Proposition 2.19. Since our proof relies on cyclotomic fields from algebraic number theory, we present it in the form of an appendix.

Proof of Proposition 2.19. Let $\mathbb{Q}(\zeta_m)$ be the m-th cyclotomic field of mth roots of unity with $\zeta_m = e^{2\pi i/m} \in \mathbb{C}$. In particular, the cyclotomic field $\mathbb{Q}(\zeta_{16})$ contains $\sqrt{2}$ as an integer. Let $\mathfrak{b}$ be a prime ideal of $\mathbb{Q}(\zeta_{16})$ such that $\mathfrak{b}$ contains p (i.e. $\mathfrak{b} \mid p$). The extension $\mathfrak{b} \mid \langle p \rangle$ is unramified and $\mathbb{Z}[\zeta_{16}]/\mathfrak{b} \cong \mathbb{F}_{p^4}$; see [32, Proposition 13.2.5] and [30, Section 4.5]. Note that $h = \pm\sqrt{2} \pmod{\mathfrak{b}}$. We may assume $h \equiv \sqrt{2} \pmod{\mathfrak{b}}$. We do the computation for $q \equiv 13 \pmod{16}$, the proof for the other cases being analogous.

$$\begin{aligned}
(1+h)^{\frac{q+1}{2}} h^{\frac{q-1}{2}} &\equiv (1+\sqrt{2})^{\frac{q+1}{2}} (\sqrt{2})^{\frac{q-1}{2}} \pmod{\mathfrak{b}} \\
&= (\sqrt{2}+2)^{\frac{q+1}{2}} \frac{1}{\sqrt{2}} \\
&= (\zeta_8 + \zeta_8^{-1} + 2)^{\frac{q+1}{2}} \frac{1}{\sqrt{2}} \\
&= (\zeta_{16} + \zeta_{16}^{-1})^{q+1} \frac{1}{\sqrt{2}} \\
&\equiv (\zeta_{16} + \zeta_{16}^{-1})(\zeta_{16}^{13} + \zeta_{16}^{-13}) \frac{1}{\sqrt{2}} \pmod{\mathfrak{b}} \\
&\equiv (\zeta_{16} + \zeta_{16}^{-1})(\zeta_{16}^{-3} + \zeta_{16}^{3}) \frac{1}{\sqrt{2}} \pmod{\mathfrak{b}} \\
&= (\zeta_{16}^{4} + \zeta_{16}^{-2} + \zeta_{16}^{2} + \zeta_{16}^{-4}) \frac{1}{\sqrt{2}} \\
&= (\zeta_8 + \zeta_8^{-1}) \frac{1}{\sqrt{2}} = 1
\end{aligned}$$

□

Bibliography

[1] V. Abatangelo, J. C. Fisher, G. Korchmáros, and B. Larato, "On the mutual position of two irreducible conics in $\mathrm{PG}(2, q)$, q odd," *Advances in Geometry*, vol. 11, no. 4, pp. 603–614, 2011.

[2] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra.* CRC Press, 2018.

[3] S. Ball and Z. Weiner, "An introduction to finite geometry," 2011, preprint.

[4] J. Bamberg, M. Giudici, and G. F. Royle, "Hemisystems of small flock generalized quadrangles," *Designs, codes and cryptography*, vol. 67, no. 1, pp. 137–157, 2013.

[5] J. Bamberg, S. Kelly, M. Law, and T. Penttila, "Tight sets and m-ovoids of finite polar spaces," *Journal of Combinatorial Theory, Series A*, vol. 114, no. 7, pp. 1293–1314, 2007.

[6] J. Bamberg, M. Lee, K. Momihara, and Q. Xiang, "A new infinite family of hemisystems of the hermitian surface," *Combinatorica*, vol. 38, no. 1, pp. 43–66, 2018.

[7] D. Bartoli, "On a conjecture about a class of permutation trinomials," *Finite Fields and Their Applications*, vol. 52, pp. 30–50, 2018.

[8] ——, "Hasse - weil type theorems and relevant classes of polynomial functions," in *Surveys in Combinatorics 2021*, ser. London Mathematical Society Lecture Note Series, K. K. Dabrowski, M. Gadouleau, N. Georgiou, M. Johnson, G. B. Mertzios, and D. Paulusma, Eds. Cambridge University Press, 2021, p. 43–102.

[9] M. Bonini, M. Sala, and L. Vicino, "Rational points on cubic surfaces and ag codes from the norm-trace curve," *arXiv preprint arXiv:2102.05478*, 2021.

[10] W. Bosma, J. Cannon, and C. Playoust, “The Magma algebra system. I. The user language,” *J. Symbolic Comput.*, vol. 24, no. 3-4, pp. 235–265, 1997, computational algebra and number theory (London, 1993). [Online]. Available: http://dx.doi.org/10.1006/jsco.1996.0125

[11] R. Calderbank and W. M. Kantor, “The geometry of two-weight codes,” *Bulletin of the London Mathematical Society*, vol. 18, no. 2, pp. 97–122, 1986.

[12] R. Casse, *Projective geometry: an introduction.* OUP Oxford, 2006.

[13] A. Cossidente, “Combinatorial structures in finite classical polar spaces,” *Surveys in combinatorics*, vol. 440, pp. 204–237, 2017.

[14] A. Cossidente and F. Pavese, “Intriguing sets of quadrics in pg (5, q),” *Advances in Geometry*, vol. 17, no. 3, pp. 339–345, 2017.

[15] A. Cossidente and T. Penttila, “Hemisystems on the hermitian surface,” *Journal of the London Mathematical Society*, vol. 72, no. 3, pp. 731–741, 2005.

[16] R. Fuhrmann and F. Torres, “The genus of curves over finite fields with many rational points,” *manuscripta mathematica*, vol. 89, no. 1, pp. 103–106, 1996.

[17] W. Fulton, “Algebraic curves,” 2008. [Online]. Available: http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf

[18] M. Giulietti, “Codici e crittografia,” 2013. [Online]. Available: https://www.dmi.unipg.it/~giuliet/CC.pdf

[19] ——, “Geometria superiore,” 2011. [Online]. Available: https://www.dmi.unipg.it/~giuliet/GS.pdf

[20] J. W. P. Hirschfeld, *Projective geometry over finite fields.* Clarendon Press, 1979.

[21] ——, *Finite projective spaces of three dimensions.* Oxford University Press, 1985.

[22] J. W. P. Hirschfeld, J. A. Thas *et al.*, *General Galois geometries.* Springer, 1991.

[23] J. Hirschfeld, G. Korchmáros, and F. Torres, *Algebraic curves over a finite field.* Princeton Series in Applied Mathematics, Princeton University Press, 2013.

[24] X. D. Hou, "Permutation polynomials of the form $x^r(a + x^{2(q-1)})$ — a nonexistence result," 2016. [Online]. Available: https://arxiv.org/abs/1609.03662

[25] ——, "Determination of a type of permutation trinomials over finite fields," *Acta Arithmetica*, vol. 3, no. 166, pp. 253–278, 2014.

[26] ——, "Determination of a type of permutation trinomials over finite fields, ii," *Finite Fields Appl.*, vol. 35, pp. 16 – 35, 2015.

[27] ——, "Permutation polynomials over finite fields — a survey of recent advances," *Finite Fields Appl.*, vol. 32, pp. 82 – 119, 2015.

[28] ——, "A survey of permutation binomials and trinomials over finite fields," *Proceedings of the 11th International Conference on Finite Fields and Their Applications*, vol. 632, pp. 177 – 191, 2015.

[29] ——, *Applications of the Hasse-Weil bound to permutation polynomials*, 2018, vol. 54.

[30] ——, *Lectures on Finite Fields.* AMS & Graduate studies in mathematics, 2018, vol. 190.

[31] X. D. Hou and V. Pallozzi Lavorante, "New results on permutation binomials over finite fields," 2021. [Online]. Available: https://arxiv.org/abs/2111.06533

[32] I. Kenneth and R. Michael, "A classical introduction to modern number theory," *The Mathematical Gazette*, vol. 76, no. 476, pp. 316–317, 1992.

[33] S. L. Kleiman, *Algebraic cycles and the Weil conjectures.* North-Holland, Amsterdam, 1968, pp. 359–386.

[34] G. Korchmáros, G. P. Nagy, and P. Speziali, "Hemisystems of the hermitian surface," *Journal of Combinatorial Theory, Series A*, vol. 165, pp. 408–439, 2019.

[35] G. Korchmáros and F. Torres, "Embedding of a maximal curve in a hermitian variety," *Compositio Mathematica*, vol. 128, no. 1, pp. 95–113, 2001.

[36] S. D. Lappano, "Some results concerning permutation polynomials over finite fields," Ph.D. dissertation, University of South Florida, 2016.

[37] ——, "A family of permutation trinomials over $\mathbb{F}_{q^2}$," 2020, private communication.

[38] Y. I. Manin, *Cubic forms: algebra, geometry, arithmetic.* Elsevier, 1986.

[39] A. M. Masuda, I. Rubio, and J. Santiago, "Permutation binomials of index $q^{e-1} + \cdots + q + 1$ over $\mathbf{F}_{q^e}$," 2020. [Online]. Available: https://arxiv.org/abs/2009.10851

[40] H. H. Mitchell, "Determination of the ordinary and modular ternary linear groups," *Transactions of the American Mathematical Society*, vol. 12, no. 2, pp. 207–242, 1911.

[41] V. Pallozzi Lavorante, "External points to a conic from a baer subplane," 2021, submitted. [Online]. Available: https://arxiv.org/abs/2104.12434

[42] ——, "On permutation quadrinomials from niho exponents in characteristic 2," 2021, preprint. [Online]. Available: https://arxiv.org/abs/2112.07006

[43] V. Pallozzi Lavorante and V. Smaldore, "New hemisystems of the hermitian surface," 2021, submitted. [Online]. Available: https://arxiv.org/abs/2105.09656

[44] F. Pavese, "Finite classical polar spaces and their geometry," 2021. [Online]. Available: https://corsidibasepoliba.cloud.ba.infn.it/geometria-pavese/wp-content/uploads/sites/58/2021/09/naples.pdf

[45] B. Segre, "Forme e geometrie hermitiane, con particolare riguardo al caso finito," *Annali di Matematica Pura ed Applicata*, vol. 70, no. 1, pp. 1–201, 1965.

[46] J.-P. Serre, *Lectures on $N_X(p)$.* CRC Press, 2016.

[47] H. Stichtenoth, *Algebraic function fields and codes.* Springer Science & Business Media, 2009, vol. 254.

[48] P. Swinnerton-Dyer, "Cubic surfaces over finite fields," *Cambridge University Press*, vol. 149, no. 3, pp. 385–388, 2010.

[49] Z. Tu, X. Zeng, Y. Jiang, and Y. Li, "Binomial permutations over finite fields with even characteristic," *Designs, Codes and Cryptography*, vol. 89, no. 12, pp. 2869–2888, 2021.

[50] L. Zheng, B. Liu, H. Kan, J. Peng, and D. Tang, "More classes of permutation quadrinomials from niho exponents in characteristic two," *Finite Fields and Their Applications*, vol. 78, p. 101962, 2022.

[51] M. Zieve, “Permutation polynomials on $\mathbf{F}_q$ induced from rédei function bijections on subgroups of $\mathbf{F}_q^*$,” 2013. [Online]. Available: https://arxiv.org/abs/1310.0776

[52] ——, “On some permutation polynomials over f_q of the form $x^r h(x^{(q-1)/d})$,” *Proc.Amer.Math.Soc.*, vol. 137, pp. 2209–2216, 2009.