UNIVERSIDADE FEDERAL DE MINAS GERAIS
Instituto de Ciências Exatas
Programa de Pós-graduação em Matemática

José Alves Oliveira

SOME TOPICS ON FINITE FIELDS

Belo Horizonte
2022

José Alves Oliveira

SOME TOPICS ON FINITE FIELDS

Tese apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de Minas Gerais, como requisito parcial à obtenção do título de Doutor em Matemática.

Orientador: Fabio Enrique Brochero Martínez

Belo Horizonte
2022

Oliveira, José Alves

048s Some topics on finite fields [manuscrito] / José Alves Oliveira — 2022.
140 f. il.

Orientador: Fabio Enrique Brochero Martínez.
Tese (doutorado) - Universidade Federal de Minas Gerais, Instituto de Ciências Exatas, Departamento de Matemática
Referências: f. 134-140.

1. Matemática – Teses. 2. Corpos finitos (Álgebra) -Teses. 3. Hipersuperfícies – Teses. 4. Somas de Gauss – Teses. 5 Curvas algébricas – Teses. I. Brochero Martínez, Fabio Enrique. II. Universidade Federal de Minas Gerais, Instituto de Ciências Exatas, Departamento de Matemática. III. Título.

CDU 51 (043)

Ficha catalográfica elaborada pela bibliotecária Belkiz Inez Rezende Costa
CRB 6/1510 – Insituto de Ciências Exatas da UFMG.

UNIVERSIDADE FEDERAL DE MINAS GERAIS

COLEGIADO DO CURSO DE PÓS-GRADUAÇÃO EM MATEMÁTICA

FOLHA DE APROVAÇÃO

Some Topics on Finite Fields

José Alves Oliveira

Tese defendida e aprovada pela banca examinadora constituída por:

Prof. Fabio Enrique Brochero Martinez
UFMG

Prof. Cícero Carvalho
UFU

Prof. Claudio Qureshi
UdelaR - Uruguai

Prof. Daniel Panario
Carleton University - Canadá

Prof. Herivelto Borges
USP

Prof. Lucas da Silva Reis
UFMG

Belo Horizonte, 26 de janeiro de 2022.

Documento assinado eletronicamente por **Herivelto Marins Borges Filho**, **Usuário Externo**, em 26/01/2022, às 12:25, conforme horário oficial de Brasília, com fundamento no art. 5° do Decreto n° 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Daniel Nelson Panario**, **Usuário Externo**, em 26/01/2022, às 13:08, conforme horário oficial de Brasília, com fundamento no art. 5° do Decreto n° 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Fabio Enrique Brochero Martinez**, **Professor do Magistério Superior**, em 26/01/2022, às 13:33, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Claudio Michael Qureshi Valdez**, **Usuário Externo**, em 26/01/2022, às 14:01, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Cícero Fernandes de Carvalho**, **Usuário Externo**, em 26/01/2022, às 14:42, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Lucas da Silva Reis**, **Professor do Magistério Superior**, em 26/01/2022, às 15:10, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.ufmg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1214969** e o código CRC **A434B3A1**.

Agradecimentos

Agradeço primeiramente a Deus.

Aos meus pais, Cleber e Magdália, e ao meu irmão, Guilherme, por todo apoio, carinho e incetivo que tem me dado desde que me mudei para Belo Horizonte e me tornei estudante da UFMG.

À minha namorada Tata, por todo amor, carinho, compreensão e companheirismo e por me sempre me fazer acreditar que tudo daria certo.

Á todos os membros da minha família, que sempre me apoiaram em todas as minhas escolhas.

À todos meus amigos conterrâneos Claudienses, que estão sempre presentes em diversas situações, mesmo tendo cada um tomado um caminho distinto.

Ao meu orientador e também amigo, Fabio, por toda paciência durante os dois últimos anos e por todos os ensinamentos que tem me passado. Tenho aprendido muito contigo nesses últimos anos.

Aos meus colaboradores, Dani, Fabio, Herivelto e Lucas.

À todos meus amigos da graduação, mestrado e doutorado em matemática, pela amizade e pelo companheirismo durante todos os momentos de dificuldade.

À todos amigos com quem morei junto em BH, pelos momentos que dividimos juntos e por todo o apoio.

À toda equipe do PICME, por todo apoio, dicas e por todo suporte que tem me durante os últimos anos.

Ao programa de Pós-Graduação da Matemática, pela oportunidade.

Aos participantes da banca, Cícero, Claudio, Daniel, Herivelto, Lucas e Fabio, por todas as sugestões e dicas apresentadas.

Às secretárias da pós-graduação, Kelli e Andréa, por sempre estarem dispostas a sanar minhas dúvidas e resolver meus contratempos.

À todos os professores com os quais tive aula durante toda a vida, por todos ensinamentos.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

Resumo

Neste trabalho, nós estudamos alguns problemas teóricos na teoria de corpos finitos e que são de interesse para várias aplicações, bem como em teoria de códigos, criptografia e áreas relacionadas. Em particular, nós estudamos o número de pontos racionais sobre hipersuperfícies e apresentamos cotas para tais números e fórmulas explícitas nos casos em que certas condições são satisfeitas. Para algumas dessas hipersuperfícies, nós também apresentamos condições para a maximalidade e minimalidade do número de pontos com respeito à cota de Weil. Outro tópico de interesse nessa tese é a interação de polinômios sobre corpos. Por exemplo, nós estudamos o grafo funcional associado à iteração de polinômios sobre corpos finitos. Nós também estudamos o número de soluções da equação $R^{(n)}(x) = \alpha$ sobre $\overline{\mathbb{F}}_q$ para uma função racional R. O último tópico dessa tese contém o estudo de códigos com métrica de posto que são construídos com polinômios linearizados sobre $\mathbb{F}_q$, os chamados códigos Gabidulin retorcidos.

Palavras-chave: Corpos Finitos, hipersuperfícies, Fermat hipersuperfícies, Artin-Schreier hipersuperfícies, curvas elípticas, somas de caracteres, somas de Gauss, somas de Jacobi, puridade de somas de Gauss e somas de Jacobi, pontos racionais, curvas maximais, corpos perfeitos, funções racionais, funções iteradas, grafos funcionais, dinâmica sobre corpos finitos, dinâmica de funções polinomiais, polinômios linearizados, código com métrica de posto.

Abstract

In this work, we study some theoretical problems in the theory of finite fields that are of interest for a number of applications, such as in coding theory, cryptography and related areas. In particular, we study the number of rational points on hypersurfaces and present bounds for such numbers and explicit formulas in the cases where certain conditions are satisfied. For some of these hypersurfaces, we also provide conditions for the maximality and minimality of the number of rational points with respect to Weil's bound. Another topic of interest in this thesis is the iteration of maps over fields. For example, we study the functional graph associated to the iteration of polynomial maps over finite fields. We also study the number of solutions of the equation $R^{(n)}(x) = \alpha$ over $\overline{\mathbb{F}}_q$ for a rational function R. The last topic in the thesis contains a study of code rank metric codes arising from linearized polynomials over $\mathbb{F}_q$, the so called twisted Gabidulin codes.

Keywords: Finite fields, hypersurfaces, Fermat hypersurfaces, Artin-Schreier hypersurfaces, elliptic curves, character sums, Gauss sums, Jacobi sums, purity of Gauss and Jacobi sums, rational points, maximal curves, perfect fields, rational functions, iterated maps, functional graphs, dynamics over finite fields, dynamics of polynomial maps, linearized polynomails, rank metric codes.

List of Figures

List of Symbols

$\mathbb{F}_q$	a finite fields with q elements;
$\overline{\mathbb{F}}_q$	the algebraic closure of $\mathbb{F}_q$;
$\mathbb{F}_q^*$	the non-null elements of $\mathbb{F}_q$;
$\mathbb{F}_p$	a finite fields with p (prime) elements ;
μ_m	the set of m-roots of the unity of $\overline{\mathbb{F}}_q$;
$\mathbb{K}$	a field;
ψ	the canonical additive character of $\mathbb{F}_q$;
χ_d	an multiplicative character of $\mathbb{F}_q^*$ of order d;
$\mathrm{Tr}_{q^n/q}(x)$	the trace function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$;
$\mathrm{N}_{q^n/q}(x)$	the norm function from $\mathbb{F}_{q^n}^*$ to $\mathbb{F}_q^*$;
$\mathbb{Z}_d$	the ring of residues modulo d;
$\mathbb{Z}_d^*$	the set of units of $\mathbb{Z}_d$;
$\mathrm{ord}_d(a)$	the order of a in the multiplicative group $\mathbb{Z}_d^*$;
$\mathbb{1}_A$	the indicator function of the event A;
$\mu(d)$	the Möbius function;
$\mathbb{C}$	the complex numbers field;
i	the imaginary unity of $\mathbb{C}$;

Table of contents

Introduction

The study of finite fields goes back to Fermat (1601-1665), Euler (1707-1783), Lagrange (1736-1813) and Legendre (1752-1833), that contribute to the structure of special finite fields, the so called prime finite fields. The general theory of finite fields was done by Gauss (1777-1855) and Galois (1811-1832), but the interest for the study of the finite fields theory only increased in the last 50 years because of its many applications in combinatorics, finite geometry, coding theory, cryptography, number theory, among others.

In the last few decades, the theory developed and led to the emergence of many interesting problems. In this thesis, we approach some problems in contemporary topics of finite fields. Among other matters, this thesis compiles the original work contained in the following papers:

(i) [63] Oliveira, José Alves. On diagonal equations over finite fields. Finite Fields and their Applications, v. 76, p. 101927, 2021.

(ii) [62] Oliveira, José Alves. Equivalence, group of automorphism and invariants of a family of rank metric codes arising from linearized polynomials. Linear Algebra and its Applications, v. 630, p. 274-292, 2021.

(iii) [65] Oliveira, José Alves. Rational points on cubic, quartic and sextic curves over finite fields. Journal of Number Theory, v. 224, p. 191-216, 2021.

(iv) [64] Oliveira, José Alves. On maximal and minimal hypersurfaces of Fermat type, arXiv:2110.07452, 2021. Submitted.

(v) [66] Oliveira, José Alves; Oliveira, Daniela; Reis, Lucas. On iterations of rational functions over perfect fields, arXiv:2008.02619, 2020. Submitted.

(vi) On the number of rational points on Artin-Schreier hypersurfaces. Collaboration with Fabio Brochero and Herivelto Borges, in final stage of preparation.

(vii) Dynamics of polynomial maps over finite fields. Collaboration with Fabio Brochero, in final stage of preparation.

The content of the thesis is presented in 8 chapters. In Chapter 1 we provide background results that are used throughout the text. The remaining 7 chapters are divided in 3 parts.

Part I: In this part, we study the number of rational points on some suitable families of hypersurfaces.

- Chapter 2: We use character sums to give the number of rational points on suitable curves of low degree over $\mathbb{F}_q$ in terms of the number of rational points on elliptic curves. In the case where q is a prime number, we give a way to compute these numbers. As a consequence of these results, one can readily characterize maximal and minimal curves given by equations of the forms $ax^3+by^3+cz^3=0$ and $ax^4+by^4+cz^4=0$.
- Chapter 3: We study the number of rational points on the affine Fermat hypersurfaces given by equations of the form $a_1x_1^{d_1}+\cdots+a_sx_s^{d_s}=b$ with $x_i\in\mathbb{F}_{p^{t_i}}$, where $a_i,b\in\mathbb{F}_q$ and $t_i|n$ for all $i=1,\ldots,s$. In our main results, we employ results on quadratic forms to give an explicit formula for the number of rational points on Fermat hypersurfaces with restricted solution sets satisfying certain natural restrictions on the exponents. As a consequence, we present conditions for the existence of rational points. In the case $t_1=\cdots=t_s=n$, we provide results with the exact number of rational points, generalizing previous results of Wolfmann and Cao, Chou and Gu.
- Chapter 4: We study the number of rational points on the affine hypersurface $\mathcal{X}$ given by $a_1x_1^{d_1}+\cdots+a_sx_s^{d_s}=b$, where $b\in\mathbb{F}_q$. A classic well-known result from Weil yields a bound for such number of points. In the case $d_1=\cdots=d_s$, we present necessary and sufficient conditions for the number of solutions of a diagonal equation being maximal and minimal with respect to Weil's bound. The second part of the chapter presents necessary and sufficient conditions for the maximality and minimality of $\mathcal{X}$ with respect to Weil's bound in the case $b\neq 0$ and arbitrary exponents $d_1,\ldots,d_s$. In particular, we completely characterize maximal and minimal Fermat curves. We also discuss further questions concerning equations and present some open problems.
- Chapter 5: We determine the number $\mathbb{F}_{q^k}$-rational points of affine hypersurfaces given by the equation $y^q-y=a_1x_1^{d_1}+\cdots+a_sx_s^{d_s}+b$ in terms of Gauss sums and provide necessary and sufficient conditions for Weil's bound to be attained. Moreover, we present an improvement of Weil's bound in terms of a constant depending on $d_1,\ldots,d_s$. We also prove that if the exponents d_i satisfy some natural conditions, then explicit formulas for the number of $\mathbb{F}_{q^k}$-rational points can be obtained.

Part II: This part comprises results concerning the iteration of maps over finite fields and its dynamics.

- Chapter 6: In this chapter, we study the digraph associated to the map $x\mapsto x^nh(x^{\frac{q-1}{m}})$, where $h(x)\in\mathbb{F}_q[x]$. We completely determine the associated functional graph of maps that satisfy a certain condition of regularity. In particular, we provide the functional graphs associated to monomial maps. As

a consequence of our results, the number of connected components, length of the cycles and number of fixed points of these class of maps are provided.

- Chapter 7: Let $\mathbb{K}$ be a perfect field of characteristic $p \geq 0$ and let $R \in \mathbb{K}(x)$ be a rational function. This chapter studies the number $\Delta_{\alpha,R}(n)$ of distinct solutions of $R^{(n)}(x) = \alpha$ over the algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$, where $\alpha \in \overline{\mathbb{K}}$ and $R^{(n)}$ is the n-fold composition of R with itself. With the exception of some pairs (α, R), we prove that $\Delta_{\alpha,R}(n) = c_{\alpha,R} \cdot d^n + O_{\alpha,R}(1)$ for some $0 < c_{\alpha,R} \leq 1 < d$. The number d is readily obtained from R and we provide estimates on $c_{\alpha,R}$. Moreover we prove that the exceptional pairs (α, R) satisfy $\Delta_{\alpha,R}(n) \leq 2$ for every $n \geq 0$, and we fully describe them. We also discuss further questions and propose some problems in the case where $\mathbb{K}$ is finite.

Part III: This part contains a study of a class of rank metric codes that arise from linearized polynomials.

- Chapter 8: Maximum Rank metric codes (MRD for short) are subsets of $\mathrm{M}_{m\times n}(\mathbb{F}_q)$ whose number of elements attains the Singleton-like bound. The first MRD codes known were found by Delsarte (1978) and Gabidulin (1985). Sheekey (2016) presented a new class of MRD codes over $\mathbb{F}_q$ called twisted Gabidulin codes and also proposed a generalization of the twisted Gabidulin codes to the codes $\mathcal{H}_{k,s}(L_1, L_2)$. The equivalence and duality of twisted Gabidulin codes were discussed by Lunardon, Trombetti, and Zhou (2018). A new class of MRD codes in $\mathrm{M}_{2n\times 2n}(\mathbb{F}_q)$ was found by Trombetti and Zhou (2018). In this chapter, we characterize the equivalence of the class of codes proposed by Sheekey, generalizing the results known for twisted Gabidulin codes and Trombetti-Zhou codes. In the second part of the chapter, we restrict ourselves to the case $L_1(x) = x$, where we present its right nucleus, middle nucleus, Delsarte dual and adjoint codes. In the last section, we present the automorphism group of $\mathcal{H}_{k,s}(x, L(x))$ and compute its cardinality. In particular, we obtain the number of elements in the automorphism group of some twisted Gabidulin codes.

CHAPTER 1

Preliminaries

In this chapter, we introduce the main definitions, notations and basic results from finite fields and related areas that are used along the text. Most of them are presented without a proof. Nevertheless, a detailed introduction to the theory of finite fields containing the proof for such results can be found in [50].

1.1 Introduction to finite fields

We start by presenting one of the most important example of finite field, which is $\mathbb{Z}/(p)$, the residue class modulo a prime p. It is direct to prove that the cardinality of any finite field is a power of a prime p, usually denoted by q, where p is the characteristic of the field. On the other hand, there exists, up to isomorphism, a unique finite field with q elements. This finite field is denoted by $\mathbb{F}_q$. In particular, $\mathbb{F}_p$ is isomorphic to $\mathbb{Z}/(p)$. The extension of degree n of $\mathbb{F}_q$ is denoted by $\mathbb{F}_{q^n}$ and $\overline{\mathbb{F}}_q$ denotes the closure of $\mathbb{F}_q$. We use $\mathbb{F}_q^*$ to denote the nonzero elements of $\mathbb{F}_q$. The following result is very useful and it is used throughout the text.

Lemma 1.1. *[50, Theorem 2.8] For every finite field $\mathbb{F}_q$, the multiplicative group $\mathbb{F}_q^*$ is cyclic.*

1.2 Characters

In this section, we provide some definitions, basic and well-known facts. Let G be a finite abelian group. A *character* of G is a homomorphism from G into the multiplicative group of complex numbers of absolute value 1. Characters of $\mathbb{F}_q$ and $\mathbb{F}_q^*$ are called additive and multiplicative characters, respectively. Along this thesis, χ_0 denotes the trivial multiplicative

character defined by $\chi_0(a) = 1$ for all $a \in \mathbb{F}_q^*$. The order of a multiplicative character of χ is the least positive integer d for which $\chi^d = \chi_0$.

Throughout the thesis, unless otherwise stated, for a divisor d of $q-1$, χ_d denotes a multiplicative character of $\mathbb{F}_q^*$ of order d and ψ is the canonical additive character of $\mathbb{F}_q$. As costumary, we extend the definition of a multiplicative character of $\mathbb{F}_q^*$, by defining $\chi(0) = 0$.

1.2.1 Character sums

In this section, we present some results on Gauss and Jacobi sums, that are defined as follows.

Definition 1.2. *Let $\lambda_1, \ldots, \lambda_s$ be a multiplicative characters of $\mathbb{F}_q^*$.*

(a) The Gauss sum of λ_1 over $\mathbb{F}_q$ is the sum

$$G(\lambda_1) = \sum_{x \in \mathbb{F}_q^*} \psi(x)\lambda_1(x).$$

(b) Let $b \in \mathbb{F}_q$. The Jacobi sum of $\lambda_1, \ldots, \lambda_s$ is defined as

$$J_b(\lambda_1, \ldots, \lambda_s) = \sum_{\substack{b_1+\cdots+b_s=b \\ (b_1,\ldots,b_s)\in\mathbb{F}_q^s}} \lambda_1(b_1)\cdots\lambda_s(b_s);$$

One can verify that

$$J_b(\lambda_1, \ldots, \lambda_s) = \lambda_1(b)\ldots\lambda_s(b)J_1(\lambda_1, \ldots, \lambda_s)$$

for all $b \in \mathbb{F}_q^*$, fact that will be extensively used in the paper. Throughout the paper, we set $J(\lambda_1, \ldots, \lambda_s) = J_1(\lambda_1, \ldots, \lambda_s)$.

Lemma 1.3 ([50, Theorem 5.4])**.** *Let χ be a nontrivial multiplicative character of $\mathbb{F}_q^*$. Then*

$$\sum_{c \in \mathbb{F}_q} \psi(c) = \sum_{c \in \mathbb{F}_q} \chi(c) = 0.$$

Lemma 1.4 ([50, Equation 5.4, p. 189])**.** *Let d be a divisor of $q-1$. If $c \in \mathbb{F}_q$, then*

$$\sum_{j=0}^{d-1} \chi_d^j(c) = \begin{cases} 1, & \text{if } \chi_d(c) = 0 \\ d, & \text{if } \chi_d(c) = 1 \\ 0, & \text{otherwise.} \end{cases}$$

Along this thesis, for a complex number ω, we denote by $\overline{\omega}$ the complex conjugate of ω.

Lemma 1.5 ([50, Theorem 5.30])**.** *Let d be a divisor of $q-1$ and $a \in \mathbb{F}_q^*$. Then*

$$\sum_{x \in \mathbb{F}_q} \psi(ax^d) = \sum_{j=1}^{d-1} \overline{\chi_d}^j(a)G(\chi_d^j).$$

Lemma 1.6. *[50, Theorems 5.11 and 5.12] Let χ_0 denote the trivial multiplicative character of $\mathbb{F}_q^*$. If $\chi \neq \chi_0$, then*

(a) $|G(\chi)| = \sqrt{q}$;

(b) $G(\chi)G(\overline{\chi}) = \chi(-1)q$;

(c) $G(\chi_0) = -1$.

Throughout the paper, we use $\mathrm{i} \in \mathbb{C}$ to denote the imaginary unity.

Theorem 1.7 ([50, Theorem 5.15])**.** *Let χ_2 be the quadratic character of $\mathbb{F}_q^*$. Then*

$$G(\chi_2) = \begin{cases} (-1)^{n+1}q^{1/2}, & \text{if } p \equiv 1 \pmod 4; \\ (-1)^{n+1}\mathrm{i}^n q^{1/2}, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Theorem 1.8. *[50, Theorem 5.16 (Stickelberger's Theorem)] Let χ_d be a nontrivial multiplicative character of $\mathbb{F}_{q^2}^*$ of order d dividing $q+1$. Then*

$$G(\chi_d) = \begin{cases} q, & \text{if } d \text{ odd or } \frac{q+1}{d} \text{ even;} \\ -q, & \text{if } d \text{ even and } \frac{q+1}{d} \text{ odd.} \end{cases}$$

Theorem 1.9. *[50, Theorem 5.21] If $\lambda_1, \ldots, \lambda_s$ are nontrivial multiplicative characters of $\mathbb{F}_q^*$, then*

$$J(\lambda_1, \ldots, \lambda_s) = \begin{cases} \frac{G(\lambda_1)\cdots G(\lambda_s)}{G(\lambda_1,\ldots,\lambda_s)}, & \text{if } \lambda_1 \cdots \lambda_s \text{ is nontrivial;} \\ -q^{-1}G(\lambda_1)\ldots G(\lambda_s), & \text{if } \lambda_1 \cdots \lambda_s \text{ is trivial.} \end{cases}$$

As a consequence of Hasse-Davenport Relation, we have the following result.

Theorem 1.10. *[50, Theorem 5.26] Let $\eta_1, \ldots, \eta_s$ be multiplicative characters of $\mathbb{F}_q^*$, not all of which are trivial. Suppose $\eta_1, \ldots, \eta_s$ are lifted to characters $\lambda_1, \ldots, \lambda_s$ of $\mathbb{F}_{q^n}^*$. Then*

$$J(\lambda_1, \ldots, \lambda_s) = (-1)^{(n-1)(s-1)}J(\eta_1, \ldots, \eta_s)^n$$

Proposition 1.11. *[50, Theorems 5.20 and 5.22] Let $\lambda_1, \ldots, \lambda_k$ be nontrivial multiplicative characters of $\mathbb{F}_q^*$. Then*

$$|J_b(\lambda_1, \ldots, \lambda_k)| = \begin{cases} q^{\frac{k-1}{2}}, & \text{if } b \neq 0 \text{ and } \lambda_1 \cdots \lambda_k \text{ is nontrivial;} \\ q^{\frac{k-2}{2}}, & \text{if } b \neq 0 \text{ and } \lambda_1 \cdots \lambda_k \text{ is trivial;} \\ (q-1)q^{\frac{k-2}{2}}, & \text{if } b = 0 \text{ and } \lambda_1 \cdots \lambda_k \text{ is trivial;} \\ 0, & \text{if } b = 0 \text{ and } \lambda_1 \cdots \lambda_k \text{ is nontrivial.} \end{cases}$$

1.2.2 Some important definitions

In order to make notation simpler, we introduce the following notion, which is used along all this thesis.

Definition 1.12. *Let r be a positive integer. We say that an integer d is (p,r)-admissible if $d|(p^r+1)$ and there exists no $r' < r$ such that $d|(p^{r'}+1)$.*

This notion was introduced by us in [63] in the study of diagonal equations and appears as a natural condition for the maximality and minimality of the number of solutions of these equations. It turned out that this condition is closely related to the purity of Gauss and Jacobi sums. For more details on this, see Theorem 1.16 and Chapters 3, 4 and 5.

Definition 1.13. *We define*

$$\Omega = \{z \in \mathbb{C} : \text{ there exists an integer } n \text{ such that } z^n \in \mathbb{R}\}.$$

Definition 1.14. *A Gauss sum $G(\lambda_1)$ (or a Jacobi sum $J_b(\lambda_1,\ldots,\lambda_s)$) is said to be pure if some non-zero integral power of it is real.*

Let $\chi, \lambda_1, \ldots, \lambda_s$ be nontrivial multiplicative characters and $b \in \mathbb{F}_q$. We note that $G(\chi)$ is a pure Gauss sum if and only if $G(\chi) \in \Omega$. Also, $J_b(\lambda_1,\ldots,\lambda_s)$ is a pure Jacobi sum if and only if $J_b(\lambda_1,\ldots,\lambda_s) \in \Omega$. The concept of purity of Gauss and Jacobi sums is well-known and widespread. The purity of Jacobi sums have been extensively studied [3, 23, 67].

Lemma 1.15. *$(\Omega, \times)$ is a group.*

Along of this text, we will use relations between (p,r)-admissibility and purity in order to prove our results. In particular, the following result will be very important in the proof of some results in the thesis.

Theorem 1.16 ([23, Theorem 1])**.** *Let $q = p^n$. Given a divisor $d > 2$ of $q-1$ and a multiplicative character χ_d of $\mathbb{F}_q^*$ with order d, the following are equivalent.*

(i) *there exist an integer r such that d is (p,r)-admissible;*

(ii) *$G(\chi_d^j)$ is pure for all $j \in \mathbb{Z}$;*

(iii) *there exist r such that $d \mid (p^r+1)$, and for minimal such $r > 0$ and $u = \frac{p^r+1}{d}(d-1)$, it follows that*

$$G(\chi_d^j) = -(-1)^{n(uj+1)/2r} q^{1/2}$$

for all $j \not\equiv 0 \pmod{d}$.

The following result is a direct consequence of Theorems 5.16, 5.21 and 5.26 of Lidl and Niederreiter [50].

Lemma 1.17. *Let $q = p^n$ and let r be a divisor of n. Let m and k be positive integers that are (p, r)-admissible. For two integers ℓ_1, ℓ_2, it follows that*

$$J\big(\chi_k^{\ell_1}, \chi_m^{\ell_2}\big) = \begin{cases} -\varepsilon\sqrt{q}, & \text{if } \chi_k^{\ell_1}\chi_m^{\ell_2} \text{ is nontrivial;} \\ -1, & \text{otherwise,} \end{cases}$$

where $\varepsilon = (-1)^{n/2r}$.

Proof. The case where $\chi_k^{\ell_1}\chi_m^{\ell_2}$ is trivial is direct. Assume that $\chi_k^{\ell_1}\chi_m^{\ell_2}$ is nontrivial. Since $k|(p^r+1)$ and $k|(p^n-1)$, it follows that $\mathrm{ord}_k(p) = 2r|n$, where $\mathrm{ord}_k(p)$ denotes the the multiplicative order of p in $\mathbb{Z}/(k)$. Let η_k and η_m be multiplicative characters of order k and m over $\mathbb{F}_{p^{2r}}$ such that η_k and η_m are lifted to χ_k and χ_m. By Theorem 1.10, we have that

$$J\big(\chi_k^{\ell_1}, \chi_m^{\ell_2}\big) = (-1)^{\frac{n}{2r}-1} J(\eta_k^{\ell_1}, \eta_m^{\ell_2})^{\frac{n}{2r}}.$$

By Theorem 1.9,

$$J\big(\eta_k^{\ell_1}, \eta_m^{\ell_2}\big) = \frac{G(\eta_k^{\ell_1})G(\eta_m^{\ell_1})}{G(\eta_k^{\ell_1}\eta_m^{\ell_2})}.$$

Now, let $D = \mathrm{lcm}(k, m)$ and $d = \gcd(k, m)$ and let η_D be a multiplicative of order D over $\mathbb{F}_{p^{2r}}$ such that $\eta_k = \eta_D^{m/d}$ and $\eta_m = \eta_D^{k/d}$. Then the order of $\eta_k^{\ell_1}$ is $k/\gcd(k, \ell_1)$, the order of $\eta_m^{\ell_2}$ is $m/\gcd(m, \ell_2)$ and the order of $\eta_k^{\ell_1}\eta_m^{\ell_2}$ is $D/\gcd(D, \frac{\ell_1 m + \ell_2 k}{d})$. By Stickelberger's Theorem (Theorem 1.8),

$$J\big(\eta_k^{\ell_1}, \eta_m^{\ell_2}\big) = (-1)^{\frac{p^r+1}{D}\left(\frac{D}{k}\gcd(k,\ell_1)+\frac{D}{m}\gcd(m,\ell_2)+\gcd(D,\frac{\ell_1 m+\ell_2 k}{d})\right)} p^r.$$

Since p is odd along all the thesis, one can verify that

$$\frac{p^r+1}{D}\left(\frac{D}{k}\gcd(k,\ell_1) + \frac{D}{m}\gcd(m,\ell_2) + \gcd(D, \frac{\ell_1 m + \ell_2 k}{d})\right)$$

is even. Therefore, $J\big(\eta_k^{\ell_1}, \eta_m^{\ell_2}\big) = p^r$ and so

$$J\big(\chi_k^{\ell_1}, \chi_m^{\ell_2}\big) = (-1)^{\frac{n}{2r}-1} p^{\frac{n}{2}},$$

which completes the proof. ■

1.3 Algebraic geometry over finite fields

As usual, in this text, $\mathbb{A}^s$ is the affine s-dimensional space $\overline{\mathbb{F}}_q^s$ and $\mathbb{P}^s$ is the projective s-dimensional space over $\overline{\mathbb{F}}_q$. A subset $\mathcal{V} \subset \mathbb{P}^s$ is a *projective variety* defined over $\overline{\mathbb{F}}_q$ (or projective $\overline{\mathbb{F}}_q$-variety) if it is the set of common zeros in $\mathbb{P}^r$ of homogeneous polynomials $F_1, \ldots, F_m \in \overline{\mathbb{F}}_q[X_0, \ldots, X_s]$. In the same way, an *affine variety* of $\mathbb{A}^s$ defined over $\overline{\mathbb{F}}_q$ (or affine $\overline{\mathbb{F}}_q$-variety) is the set of common zeros in $\mathbb{A}^s$ of polynomials $F_1, \ldots, F_m \in \overline{\mathbb{F}}_q[X_1, \ldots, X_s]$. A *hypersurface* (affine or projective) is a variety defined as the set of zeros of a single polynomial F. In the case where $s = 2$, the hypersurface is called a *curve*.

A variety $\mathcal{V}$ is *irreducible* if it cannot be expressed as a finite union of proper $\overline{\mathbb{F}}_q$-subvarieties of $\mathcal{V}$. A variety $\mathcal{V}$ is *absolutely irreducible* if it is $\overline{\mathbb{F}}_q$-irreducible as a $\overline{\mathbb{F}}_q$-variety. Any $\overline{\mathbb{F}}_q$-variety $\mathcal{V}$ can be expressed as a union $\mathcal{V} = \mathcal{V}_1 \cup \cdots \cup \mathcal{V}_s$ of irreducible (or absolutely irreducible) $\overline{\mathbb{F}}_q$-varieties, unique up to reordering, called the irreducible (absolutely irreducible) $\overline{\mathbb{F}}_q$-components of $\mathcal{V}$.

Let $\mathbb{P}^s(\mathbb{F}_q)$ be the s-dimensional projective space over $\mathbb{F}_q$ and $\mathbb{A}^s(\mathbb{F}_q)$ the s-dimensional $\mathbb{F}_q$-vector space $\mathbb{F}_q^s$. For a projective variety $\mathcal{V} \subset \mathbb{P}^s$ or an affine variety $\mathcal{V} \subset \mathbb{A}^s$, $\mathcal{V}(\mathbb{F}_q)$ denotes the set of $\mathbb{F}_q$-rational points of $\mathcal{V}$, namely $\mathcal{V}(\mathbb{F}_q) := \mathcal{V} \cap \mathbb{P}^s(\mathbb{F}_q)$ in the projective case and $\mathcal{V}(\mathbb{F}_q) := \mathcal{V} \cap \mathbb{A}^s(\mathbb{F}_q)$ in the affine case. For more details on algebraic geometry, we recommend [40, 57, 83].

Along this thesis, we study the number of points on affine and projective varieties defined over $\mathbb{F}_q$ that are zeros of certain polynomials F (see Sections 2.1, 2.2 and 2.3).

Part I

Rational points on hypersurfaces

CHAPTER 2

Rational points on curves of low degree

For a curve $\mathcal{C} \subset \mathbb{P}^2$, we let $N_n(\mathcal{C}) = |\mathcal{C}(\mathbb{F}_{q^n})|$, the number of $\mathbb{F}_{q^n}$-rational points on $\mathcal{C}$. For an irreducible non-singular curve $\mathcal{C}$ over $\mathbb{F}_q$, the well-known result [57, Theorem 3.3] states that there exist complex numbers $\omega_1, \ldots, \omega_{2g}$ such that the number of rational points on a curve $\mathcal{C}$ over $\mathbb{F}_{q^n}$ satisfies

$$N_n(\mathcal{C}) = q^n + 1 - \sum_{i=1}^{2g} \omega_i^n,$$

where g denotes the genus of $\mathcal{C}$ and $|\omega_i| = \sqrt{q}$ for all $i = 1, \ldots, 2g$. This result is usually referred as Riemann Hypothesis for algebraic curves. As a direct consequence of this statement, we have the well-known Hasse-Weil bound, given by

$$|N_n(\mathcal{C}) - q^n - 1| \leq 2g\sqrt{q^n}. \tag{2.1}$$

In general, it is difficult to compute the number of rational points $N_n(\mathcal{C})$. Many authors have studied the so called maximal curves, that are curves whose number of rational points attains the upper Hasse-Weil bound. The number of points on some special curves was studied in [17, 27, 39, 40, 42, 48, 81]. Aubry and Perret [6] proved the following result.

Theorem 2.1. *[6, Corollary 2.4] The number of $\mathbb{F}_{q^n}$-rational points on an irreducible curve $\mathcal{C}$ over $\mathbb{F}_q$ is given by*

$$N_n(\mathcal{C}) = q^n + 1 - \sum_{i=1}^{2g} \omega_i^n - \sum_{i=1}^{\Delta_{\mathcal{C}}} \beta_i^n,$$

where $\Delta_{\mathcal{C}}$ is a constant depending on $\mathcal{C}$ and ω_i, β_i are complex numbers. Furthermore, $|\omega_i| = \sqrt{q}$, for all $1 \leq i \leq 2g$, and $|\beta_i| = 1$, for all $1 \leq i \leq \Delta_{\mathcal{C}}$. In addition, $\Delta_{\mathcal{C}} \leq \pi - g$, where π is the arithmetic genus of $\mathcal{C}$.

The numbers β_i in Theorem 2.1 are related to the singularities of the curve $\mathcal{C}$. If $\mathcal{C}$ is a non-singular curve, for example, $\Delta_{\mathcal{C}} = 0$ and then Theorem 2.1 is the well-celebrated

Riemann Hypothesis for algebraic curves. Let q be an odd prime power. After a linear change of variables, an elliptic curve over $\mathbb{F}_q$ is a curve given by equations of the form

$$y^2 = ax^3 + bx^2 + cx + d,$$

with $18abcd - 4b^3d + b^2c^2 - 4ac^3 - 27a^2d^2 \neq 0$, where $a \neq 0, b, c, d$ are elements of $\mathbb{F}_q$. Results involving points on elliptic curves can be found in [49, 82, 88]. Since the elliptic curve $\mathcal{C} : y^2 = ax^3 + bx^2 + cx + d$ is a non-singular curve of genus 1, Theorem 2.1 states that there is a complex number $\omega_q(a, b, c, d)$ satisfying

$$N_n(\mathcal{C}) = q^n + 1 - \omega_q(a, b, c, d)^n - \overline{\omega_q(a, b, c, d)}^n,$$

where $|\omega_q(a, b, c, d)| = \sqrt{q}$. In Section 2.2, we show a way to calculate $\omega_q(a, b, c, d)$ computationally faster than direct computation.

In this chapter, we use sums of characters to give the number of rational points on suitable curves of degree $3, 4$ and 6 over $\mathbb{F}_q$ in terms of the complex numbers $\omega_q(a, b, c, d)$. There is a connection between character sums and number of rational points on curves, but there exists few articles in literature exploring this relation. The connection between character sums and elliptic curves have already been studied by Williams [107]. We use techniques similar to those used by Williams in addition to character properties, relating different ways to count the number of points on the same curve in order to get the exact number of points. In this chapter, we are interested in affine curves with equation $y^i = f(x)$, where $i = 2, 3$ or 4 and $f(x)$ has suitable form.

Throughout the chapter, $\mathbb{F}_q$ is a finite field with $q = p^k$ elements. For n a positive integer and m a divisor of $q^n - 1$, let χ_m denote a multiplicative character of order m on $\mathbb{F}_{q^n}^*$. To reduce the notation, we leave implicit the dependence on n. It is convenient to extend the domain of the definition of χ_m from $\mathbb{F}_{q^n}^*$ to $\mathbb{F}_{q^n}$ by setting $\chi_m(0) = 1$ if $m = 1$ and $\chi_m(0) = 0$ if $m \geq 2$. Some of the main results of the chapter are summarized below.

Theorem 2.2. *Let $a, b \in \mathbb{F}_q^*$. The number of rational points on the curve $\mathcal{C} : y^3 = ax^6 + b$ over $\mathbb{F}_{q^n}$ satisfies*

$$N_n(\mathcal{C}) = q^n + 1 - \omega_1^n - \overline{\omega_1}^n - \omega_2^n - \overline{\omega_2}^n - \omega_3^n - \overline{\omega_3}^n - \omega_4^n - \overline{\omega_4}^n - \chi_3(a) - \chi_3^2(a),$$

where $\omega_1 := \omega_q(a^{-1}, 0, 0, -ba^{-1})$, $\omega_2 := \omega_q(b^{-1}, 0, 0, -ab^{-1})$, $\omega_3 := \omega_q(1, 0, 0, -4ab)$ and $\omega_4 := \omega_q(-4ab, 0, 0, 1)$.

In what follows, the letter i denotes a positive integer. The following result gives a relation between the number of points on two suitable curves.

Theorem 2.3. *Let A, B, C, a, b, c be elements in $\mathbb{F}_q$ and $\alpha_1, \alpha_2 \in \mathbb{F}_{q^2}$ be the roots of the polynomial $f(x) = ax^2 + bx + c$. Let $\mathcal{C}_1 : y^i = (Ax^2 + Bx + C)(ax^2 + bx + c)^{i-1}$, $\mathcal{C}_2 : y^i(ax^2 + bx + c) = Ax^2 + Bx + C$ and $\mathcal{C} : z^2 = (B - by^i)^2 - 4(A - ay^i)(C - cy^i)$ be curves over $\overline{\mathbb{F}}_q$. The numbers of $\mathbb{F}_{q^n}$-rational points on the curves $\mathcal{C}_1, \mathcal{C}_2$ and $\mathcal{C}$ satisfy*

$$N_n(\mathcal{C}_1) = N_n(\mathcal{C}) - \sum_{j=1}^{k-1} \chi_k^j\left(\tfrac{A}{a}\right) - \delta + \gamma$$

and

$$N_n(\mathcal{C}_2) = N_n(\mathcal{C}) + 1 - \sum_{j=1}^{k-1} \chi_k^j\left(\tfrac{A}{a}\right) - \delta,$$

where $\gamma := |\{\alpha_1, \alpha_2\} \cap \mathbb{F}_{q^n}|$ *and* δ *is given by*

$$\delta := \begin{cases} 1 + \chi_2(b^2 - 4ac), & \text{if } i = 1; \\ 1 + \chi_2(4Ac + 4Ca - 2Bb), & \text{if } i = 2 \text{ and } b^2 - 4ac = 0; \\ 1, & \text{otherwise.} \end{cases}$$

Theorem 2.4. *For* $a, b, c \in \mathbb{F}_q$*, with* $a \neq 0$*, let* $\mathcal{C} : y^4 = ax^4 + bx^2 + c$ *be a curve over* $\mathbb{F}_q$*, with* $q \equiv 1 \pmod 4$*. The number of rational points on* $\mathcal{C}$ *over* $\mathbb{F}_{q^n}$ *satisfies*

$$N_n(\mathcal{C}) = \begin{cases} q^n + 1 - \omega_1^n - \overline{\omega_1}^n - \omega_2^n - \overline{\omega_2}^n - \omega_3^n - \overline{\omega_3}^n, & \text{if } b^2 - 4ac \neq 0 \text{ and } c \neq 0; \\ q^n + 1 - \omega_1^n - \overline{\omega_1}^n - \chi_2(b), & \text{if } b^2 - 4ac \neq 0 \text{ and } c = 0; \\ q^n + 1 - \chi_2(-b/2) + q^n \cdot \chi_2(a), & \text{if } b^2 - 4ac = 0 \text{ and } c \neq 0; \\ q^n + 1 - \chi_2(b) + q^n \cdot \chi_2(a), & \text{if } b^2 - 4ac = 0 \text{ and } c = 0, \end{cases}$$

where $\omega_1 := \omega_q(a^{-1}, 0, d_1, 0)$*,* $d_1 := \frac{b^2 - 4ac}{4a^2}$*,* $\omega_2 := \omega_q(c^{-1}, 0, d_2, 0)$*,* $d_2 := \frac{b^2 - 4ac}{4c^2}$ *and* $\omega_3 := \omega_q(a, b, c, 0)$*.*

In order to prove these main results, we compute the number of points on many other curves. For all the curves, we give explicitly the complex numbers from Theorem 2.1, as we can see in Theorems 2.2 and 2.4.

As a direct consequence of the results presented throughout this section, one can readily obtain results on the maximality and minimality of curves with equations of the form

$$ax^n + by^n + cz^n = 0$$

in the cases $n = 3$ and $n = 4$, where a, b, c are elements in a prime field $\mathbb{F}_p$, generalizing the conditions presented by Garcia and Tafazolian [32] in these cases. The case where $a = b = c = 1$, the well-known Fermat curve, was discussed in [32]. More generally, the techniques presented here give a new way to state when an irreducible curve attains the upper bound given in Theorem 2.1.

The reason why we can not generalize this results to curves given by equations of the form $y^i = f(x)$ of any degree is due to the fact that we do not know how to relate any sum of characters with elliptic curves. For low degree, there is a natural way relate this two objects, as we will see in the next sections.

2.1 Preparation

In this section, we recall some general results involving rational points on curves over finite fields.

Remark 2.5. *The algebraic curves theory is developed in the projective space, then points at infinity may be on the curve. For example, the point* $(x_0, y_0, z_0) = (0, 1, 0)$ *is on the homogenization of the elliptic curve* $y^2 = x^3 + 1$ *.Therefore, Theorem 2.1 is considering those points at infinity. In the results that we present in this chapter, we follow that convention, considering those rational points.*

Definition 2.6. *Let* $a \neq 0, b, c, d$ *be elements in* $\mathbb{F}_q$*. The curve* $\mathcal{C} : y^2 = ax^3 + bx^2 + cx + d$ *is called elliptic curve over* $\mathbb{F}_q$ *if the roots of the polynomial* $f(x) := ax^3 + bx^2 + cx + d$ *are distinct.*

As a direct consequence from Riemann Hypothesis for algebraic curves, we have the following result.

Theorem 2.7. *Let* $\mathcal{C} : y^2 = ax^3 + bx^2 + cx + d$ *be an elliptic curve over a finite field* $\mathbb{F}_q$*. There exists a complex number* ω*, with* $|\omega| = \sqrt{q}$*, that satisfies*

$$N_n(\mathcal{C}) = q^n + 1 - \omega^n - \overline{\omega}^n.$$

The number ω *is unique up to conjugation. As* ω *depends on* a, b, c, d *and* q*, we denote* ω *by* $\omega_q(a, b, c, d)$*.*

Since $\omega_q(a, b, c, d)$ is unique up to conjugation, we let

$$\omega_q : \mathbb{F}_q^* \times \mathbb{F}_q^3 \longrightarrow \{z \in \mathbb{C} : |z| = \sqrt{q}, \Im(z) \geq 0\} \tag{2.2}$$

be the function defined by $(a, b, c, d) \mapsto \omega_q(a, b, c, d)$, where $\Im(z)$ denotes the imaginary part of z. In Section 2.2, we present a way to determine $\omega_q(a, b, c, d)$ computationally fast.

Remark 2.8. *By definition of* ω_q *and Theorem 2.7, we have* $\omega_{q^n}(a, b, c, d) = \omega_q(a, b, c, d)^n$ *for all* $a, b, c, d \in \mathbb{F}_q$ *and for all positive integer* n*.*

2.2 Rational points on elliptic curves

From now, we consider q odd.

Lemma 2.9. *[50, Theorem 5.48] If* $a, b, c \in \mathbb{F}_q$*, with* $a \neq 0$ *and* $\Delta := b^2 - 4ac$*, then*

$$\sum_{x \in \mathbb{F}_{q^n}} \chi_2(ax^2 + bx + c) = \begin{cases} -\chi_2(a), & \text{if } \Delta \neq 0; \\ (q^n - 1)\chi_2(a), & \text{if } \Delta = 0. \end{cases}$$

Remark 2.10. *The discriminant of a cubic polynomial* $f(x) = ax^3 + bx^2 + cx + d$ *is given by*

$$\Delta = 18abcd - 4b^3d + b^2c^2 - 4ac^3 - 27a^2d^2, \tag{2.3}$$

where $\Delta \neq 0$ *if and only if the roots of* $f(x)$ *are distinct. In addition, every root of* $f(x)$ *is an element of* $\mathbb{F}_q$ *if* $\Delta = 0$*.*

From here, let $\Delta(a,b,c,d)$ denote the discriminant of the polynomial $f(x) = ax^3 + bx^2 + cx + d$.

Lemma 2.11. *Let $a,b,c,d \in \mathbb{F}_q$, with $a \neq 0$. If $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_{q^6}$ are the roots of the polynomial $f(x) := ax^3 + bx^2 + cx + d$, then*

$$\sum_{x\in\mathbb{F}_{q^n}} \chi_2\big(f(x)\big) = \begin{cases} -\omega_q(a,b,c,d)^n - \overline{\omega_q(a,b,c,d)}^n, & \text{if } \Delta \neq 0; \\ -\chi_2(a)\chi_2(\alpha_1 - \alpha_2), & \text{if } f(x) = a(x-\alpha_1)^2(x-\alpha_2); \\ 0, & \text{if } f(x) = a(x-\alpha_1)^3, \end{cases}$$

where $\Delta := \Delta(a,b,c,d)$ as defined in Equation (2.3) and the complex number $\omega_q(a,b,c,d)$ is defined as in Theorem 2.7.

Proof. Let $\mathcal{C}$ be the curve $y^2 = ax^3 + cx^2 + cx + d$. We observe that

$$N_n(\mathcal{C}) = 1 + \sum_{x\in\mathbb{F}_{q^n}} \big[1 + \chi_2(ax^3 + bx^2 + cx + d)\big].$$

By Theorem 2.7, if $\Delta \neq 0$, we have

$$N_n(\mathcal{C}) = 1 + \sum_{x\in\mathbb{F}_{q^n}} \big[1 + \chi_2(ax^3 + bx^2 + cx + d)\big] = q^n + 1 - \omega_q(a,b,c,d)^n - \overline{\omega_q(a,b,c,d)}^n,$$

Since $\sum_{x\in\mathbb{F}_{q^n}} 1 = q^n$, the result follows. If $\Delta = 0$, then there exists a root $\alpha \in \mathbb{F}_q$ of the polynomial ax^3+bx^2+cx+d with multiplicity ≥ 2. Hence, $ax^3+bx^2+cx+d = a(x-\alpha)^2(x-\beta)$, with $\alpha, \beta \in \mathbb{F}_q$. Thus, from the relation

$$\chi_2(ax^3 + bx^2 + cx + d) = \chi_2\left((x-\alpha)^2\right)\chi_2\big(a(x-\beta)\big) = \begin{cases} \chi_2\big(a(x-\beta)\big), & \text{if } x \neq \alpha; \\ 0, & \text{if } x = \alpha, \end{cases}$$

and Lemma 1.3, we have

$$\begin{aligned} \sum_{x\in\mathbb{F}_{q^n}} \chi_2(ax^3 + bx^2 + cx + d) &= \sum_{x\in\mathbb{F}_{q^n}\setminus\{\alpha\}} \chi_2\big(a(x-\alpha)^2(x-\beta)\big) \\ &= \sum_{x\in\mathbb{F}_{q^n}\setminus\{\alpha\}} \chi_2(ax - a\beta) \\ &= -\chi_2(a\alpha - a\beta). \end{aligned}$$

This completes the proof. ∎

Since we use Lemma 2.11 in most results in this chapter, it is convenient to introduce the following notation. We define the function $\Delta' : \mathbb{F}_q^4 \to \{1,2,3\}$ by letting

$$\Delta'(a,b,c,d) = \begin{cases} 1, & \text{if } \alpha_i \neq \alpha_j \text{ for all } 1 \leq i < j \leq 3; \\ 2, & \text{if } \alpha_i = \alpha_j \neq \alpha_k \text{ for some } \{i,j,k\} = \{1,2,3\}; \\ 3, & \text{if } \alpha_1 = \alpha_2 = \alpha_3, \end{cases}$$

where $\alpha_1, \alpha_2, \alpha_3$ are the roots of the polynomial $f(x) := ax^3 + bx^2 + cx + d$. From this definition, it follows that $\Delta(a,b,c,d) \neq 0$ if and only if $\Delta'(a,b,c,d) = 1$. We also define the function $\alpha : \{(a,b,c,d) \in \mathbb{F}_q^4 : \Delta'(a,b,c,d) = 2\} \to \mathbb{F}_q$ by

$$\alpha(a,b,c,d) = a\alpha_1 - a\alpha_2,$$

where $f(x) = a(x-\alpha_1)^2(x-\alpha_2)$.

Lemma 2.12. *[50, Lemma 7.3] Let m be a positive integer. We have*

$$\sum_{a \in \mathbb{F}_q} a^m = \begin{cases} 0, & \text{if } (q-1) \nmid m \text{ or } m = 0; \\ -1, & \text{if } (q-1) \mid m \text{ and } m \neq 0, \end{cases}$$

where $0^0 := 1$.

Remark 2.13. *It is known that $\chi_2(a) = (-1)^n \in \mathbb{C}$ if and only if $a^{\frac{q-1}{2}} = (-1)^n \in \mathbb{F}_q$. Indeed, by definition, $\chi_2(b) = -1$ if and only if b is not a square in $\mathbb{F}_q^*$, so $b = \theta^i$, where θ is a generator of the group $\mathbb{F}_q^*$ and i is odd. It follows that $b^{\frac{q-1}{2}} = (\theta^{\frac{q-1}{2}})^i = (-1)^i = -1$. In similar way, we have that $\chi_2(b) = -1$ if and only if $b^{\frac{q-1}{2}} = 1$.*

The following lemma characterizes, modulo p, the *trace of Frobenius*

$$\tau_q(a,b,c,d) := \omega_q(a,b,c,d) + \overline{\omega_q(a,b,c,d)}$$

of an elliptic curve given by equation $y^2 = ax^3 + bx^2 + cx + d$ over $\mathbb{F}_p$. Since we are interested in odd characteristic, we may suppose $b = 0$. This lemma allows us to calculate the number of points on elliptic curves whose coefficients are in a prime field $\mathbb{F}_p$. Along the proof of the following result, we use $\lfloor a \rfloor$ and $\lceil a \rceil$ to denote the floor and ceiling of a real number a.

Lemma 2.14. *Let $\mathcal{C} : y^2 = Ax^3 + Bx + C$ be an elliptic curve over $\mathbb{F}_{p^n}$, where p is an odd prime. The trace of Frobenius of $\mathcal{C}$ satisfies the relation*

$$\tau_{p^n}(A,0,B,C) \equiv \sum_{l=\lceil \frac{p^n-1}{6} \rceil}^{\lfloor \frac{p^n-1}{4} \rfloor} \binom{\frac{p^n-1}{2}}{2l} \binom{2l}{\frac{p^n-1-2l}{2}} A^{\frac{p^n-1}{2}-l} B^{3l-\frac{p^n-1}{2}} C^{\frac{p^n-1}{2}-2l} \pmod{p}.$$

Proof. We observe that

$$1 + \chi_2(Ax^3 + Bx + C) = \begin{cases} 0, & \text{if } Ax^3 + Bx + C \text{ is not a square in } \mathbb{F}_{p^n}; \\ 2, & \text{if } Ax^3 + Bx + C \text{ is a square in } \mathbb{F}_{p^n}. \end{cases}$$

Therefore, we have

$$N_1(\mathcal{C}) = 1 + \sum_{x \in \mathbb{F}_{p^n}} [1 + \chi_2(Ax^3 + Bx + C)] = p^n + 1 + \sum_{x \in \mathbb{F}_{p^n}} \chi_2(Ax^3 + Bx + C).$$

By Remark 2.13,

$$\begin{aligned}\sum_{x\in\mathbb{F}_{p^n}}\chi_2(Ax^3+Bx+C) &\equiv \sum_{x\in\mathbb{F}_{p^n}}(Ax^3+Bx+C)^{\frac{p^n-1}{2}}\\ &\equiv \sum_{x\in\mathbb{F}_{p^n}}\sum_{i=0}^{\frac{p^n-1}{2}}\binom{\frac{p^n-1}{2}}{i}(Ax^3+Bx)^i C^{\frac{p^n-1}{2}-i}\\ &\equiv \sum_{x\in\mathbb{F}_{p^n}}\sum_{i=0}^{\frac{p^n-1}{2}}\binom{\frac{p^n-1}{2}}{i}C^{\frac{p^n-1}{2}-i}\sum_{j=0}^{i}\binom{i}{j}A^jB^{i-j}x^{2j+i}\\ &\equiv \sum_{i=0}^{\frac{p^n-1}{2}}\sum_{j=0}^{i}\binom{\frac{p^n-1}{2}}{i}\binom{i}{j}A^jB^{i-j}C^{\frac{p^n-1}{2}-i}\sum_{x\in\mathbb{F}_p}x^{2j+i} \pmod p.\end{aligned}$$

By Lemma 2.12, the sum $\sum_{x\in\mathbb{F}_{p^n}}x^{2j+i}$ is nonzero only if $2j+i\equiv 0 \pmod{p^n-1}$ and $2j+i\neq 0$, and in these cases, the sum is -1. In addition, since

$$2j+i \le 2\cdot\frac{p^n-1}{2}+\frac{p^n-1}{2}=\frac{3(p^n-1)}{2}<2(p^n-1),$$

it follows that

$$\begin{aligned}N_1(\mathcal{C})-p^n-1 &\equiv \sum_{i=0}^{\frac{p^n-1}{2}}\sum_{j=0}^{i}\binom{\frac{p^n-1}{2}}{i}\binom{i}{j}A^jB^{i-j}C^{\frac{p^n-1}{2}-i}\sum_{x\in\mathbb{F}_{p^n}}x^{2j+i}\\ &\equiv -\sum_{l=\lceil\frac{p^n-1}{6}\rceil}^{\lfloor\frac{p^n-1}{4}\rfloor}\binom{\frac{p^n-1}{2}}{2l}\binom{2l}{\frac{p^n-1-2l}{2}}A^{\frac{p^n-1-2l}{2}}B^{2l-\frac{p^n-1-2l}{2}}C^{\frac{p^n-1}{2}-2l}\\ &\equiv -\sum_{l=\lceil\frac{p^n-1}{6}\rceil}^{\lfloor\frac{p^n-1}{4}\rfloor}\binom{\frac{p^n-1}{2}}{2l}\binom{2l}{\frac{p^n-1-2l}{2}}A^{\frac{p^n-1-2l}{2}}B^{3l-\frac{p^n-1}{2}}C^{\frac{p^n-1}{2}-2l} \pmod p.\end{aligned}$$

Since $N_1(\mathcal{C})=p^n+1-\tau_{p^n}(A,0,B,C)$, the result follows. ■

In Lemma 2.14 there is an abuse of language when we write

$$\sum_{x\in\mathbb{F}_p}\chi_2(Ax^3+Bx+C)\equiv\sum_{x\in\mathbb{F}_p}(Ax^3+Bx+C)^{\frac{p-1}{2}}$$

since the left summation is over $\mathbb{C}$ and the right summation is over $\mathbb{F}_p$. In fact, we do it many times throughout this chapter.

Since $|\tau(A,0,B,C)|=|\omega_p(A,0,B,C)+\overline{\omega_p(A,0,B,C)}|\le\lfloor 2\sqrt{p}\rfloor$ (by Theorem 2.7), we can use Lemma 2.14 to compute the complex number $\omega_p(A,0,B,C)$ in the case where $p\ge 17$, as in the following example.

Example 2.15. *Let $\mathcal{J}: y^2=x^3+2$ be an elliptic curve over $\mathbb{F}_{19}$. From Lemma 2.14,*

$$\omega_{19}(1,0,0,2)+\overline{\omega_{19}(1,0,0,2)}\equiv\sum_{l=3}^{4}\binom{9}{2l}\binom{2l}{9-l}0^{3l-9}2^{9-2l}\equiv 7 \pmod{19}.$$

Since $|\omega_{19}(1,0,0,2)+\overline{\omega_{19}(1,0,0,2)}| \leq \lfloor 2\sqrt{19} \rfloor = 8$, *we have* $\omega_{19}(1,0,0,2)+\overline{\omega_{19}(1,0,0,2)} = 7$. *Thus, using that* $|\omega_{19}(1,0,0,2)| = \sqrt{19}$, *we must have*

$$\omega_{19}(1,0,0,2) = \frac{7}{2} + \mathrm{i}\sqrt{19 - \frac{7^2}{2^2}} = \frac{7}{2} + \mathrm{i}\sqrt{\frac{27}{4}}.$$

In addition, the number of rational points of $\mathcal{J}$ *over* $\mathbb{F}_{19^n}$ *is given by*

$$N_n(\mathcal{J}) = 19^n + 1 - \left(\frac{7}{2} + \mathrm{i}\sqrt{\frac{27}{4}}\right)^n - \left(\frac{7}{2} - \mathrm{i}\sqrt{\frac{27}{4}}\right)^n.$$

We will use this technique in the examples of this chapter in order to compute the number of rational points on suitable curves. In [95], the author presents congruences similar to congruence in Lemma 2.14. In fact, some values of ω_q are well-known in the case where p is a prime number, e.g. see Theorem 6.2.9 and Theorem 6.2.10 in [11].

2.3 Rational points on curves of the form $y^2 = f(x)$

Throughout this section, for an event A, let

$$\mathbb{1}_A := \begin{cases} 1, & \text{if } A \text{ occurs;} \\ 0, & \text{if } A \text{ does not occur} \end{cases}$$

be the indicator function of the event A. In Algebraic Geometry, a hyperelliptic curve of genus $g \geq 1$ is an algebraic curve given by equation

$$y^2 + h(x)y = f(x),$$

where $f(x)$ is a polynomial of degree $2g+1$ or $2g+2$ with distinct roots and $h(x)$ is a polynomial of degree at most $g+1$. When the characteristic of the field is not 2, we can take $h(x) = 0$ (make the change of variables, by taking $y = z - \frac{1}{2}h(x)$ and $x = w$). Hyperelliptic curves are useful in cryptography (for example, see [15]). In Ulas [101] and Nelson, Solymosi, Tom and Wong [60], the authors present results concerning the number of rational points on hyperelliptic curves. In this section, we present the number of rational points on curves of the form $y^2 = f(x)$, where $f(x) \in \mathbb{F}_q[x]$ is a suitable polynomial of degree 4 or 6. In particular, we give the number of points on most hyperelliptic curves of genus 1 when q is odd.

Remark 2.16. *Let* $\Lambda_1, \Lambda_2 \subset \mathbb{F}_q$ *be two sets with the same number of elements. Let* f *be a bijective map from* Λ_1 *to* Λ_2 *and* $g : \Lambda_2 \to \mathbb{F}_q$ *an arbitrary function. Then*

$$\sum_{x \in \Lambda_1} \chi_k\big(g(f(x))\big) = \sum_{z \in \Lambda_2} \chi_k\big(g(z)\big).$$

Lemma 2.17. *If $a, b, c, d \in \mathbb{F}_q$, with $a \neq 0$ and $d \neq 0$, then*

$$\sum_{x \in \mathbb{F}_{q^n}} \chi_2(ax^3+bx^2+cx+d)\chi_2(x) = \begin{cases} -\omega_q(d,c,b,a)^n - \overline{\omega_q(d,c,b,a)}^n - \chi_2(a), & \text{if } \Delta' = 1; \\ -\chi_2(\alpha) - \chi_2(a), & \text{if } \Delta' = 2; \\ -\chi_2(a), & \text{if } \Delta' = 3, \end{cases}$$

where $\Delta' := \Delta'(a,b,c,d)$, $\alpha := \alpha(a,b,c,d)$ and $\omega_q(d,c,b,a)$ is defined as in Theorem 2.7.

Proof. Using the fact that $\chi_2(0) = 0$, we have

$$\begin{aligned} \sum_{x \in \mathbb{F}_{q^n}} \chi_2(ax^3+bx^2+cx+d)\chi_2(x) &= \sum_{x \in \mathbb{F}_{q^n}^*} \chi_2(ax^3+bx^2+cx+d)\chi_2(x^{-3}) \\ &= \sum_{x \in \mathbb{F}_{q^n}^*} \chi_2(a+bx^{-1}+cx^{-2}+dx^{-3}) \\ &= \sum_{z \in \mathbb{F}_{q^n}^*} \chi_2(a+bz+cz^2+dz^3). \end{aligned}$$

By Lemma 2.11,

$$\sum_{z \in \mathbb{F}_{q^n}^*} \chi_2(a+bz+cz^2+dz^3) = \begin{cases} -\omega_q(d,c,b,a)^n - \overline{\omega_q(d,c,b,a)}^n - \chi_2(a), & \text{if } \Delta' = 1; \\ -\chi_2(\alpha) - \chi_2(a), & \text{if } \Delta' = 2; \\ -\chi_2(a), & \text{if } \Delta' = 3, \end{cases}$$

where $\Delta' := \Delta'(a,b,c,d)$ and $\alpha := \alpha(a,b,c,d)$. ■

Theorem 2.18. *For $a, b, c, d, e \in \mathbb{F}_q$, with $a \neq 0$, let $\mathcal{C} : y^2 = (ax^3+bx^2+cx+d)(x+e)$ be a curve over $\overline{\mathbb{F}}_q$. The number of rational points on $\mathcal{C}$ over $\mathbb{F}_{q^n}$ satisfies*

$$N_n(\mathcal{C}) = \begin{cases} q^n+1-\omega_q(d',c',b',a')^n - \overline{\omega_q(d',c',b',a')}^n - \chi_2(a'), & \text{if } d' \neq 0 \text{ and } \Delta' = 1; \\ q^n+1-\chi_2(\alpha)-\chi_2(a'), & \text{if } d' \neq 0 \text{ and } \Delta' = 2, \\ q^n+1-\chi_2(a'), & \text{if } d' \neq 0 \text{ and } \Delta' = 3; \\ q^n+1-\chi_2(a')-\chi_2(c'), & \text{if } d' = 0 \text{ and } (b')^2 \neq 4a'c'; \\ q^n+1+(q^n-1)\chi_2(a')-\chi_2(c'), & \text{if } d' = 0 \text{ and } (b')^2 = 4a'c'; \end{cases}$$

where $a' = a$, $b' = b-3ae$, $c' = 3ae^2-2eb+c$, $d' = be^2-ae^3+d-ec$, $\Delta' := \Delta'(a',b',c',d')$ and $\alpha := \alpha(a',b',c',d')$.

Proof. We have

$$\begin{aligned} N_n(\mathcal{C}) &= 1 + \sum_{x \in \mathbb{F}_{q^n}} \left[1+\chi_2(ax^3+bx^2+cx+d)\chi_2(x+e)\right] \\ &= q^n+1+\sum_{z \in \mathbb{F}_{q^n}} \chi_2(a(z-e)^3+b(z-e)^2+c(z-e)+d)\chi_2(z) \\ &= q^n+1+\sum_{z \in \mathbb{F}_{q^n}} \chi_2(a(z^3-3z^2e+3ze^2-e^3)+b(z^2-2ze+e^2)+c(z-e)+d)\chi_2(z) \\ &= q^n+1+\sum_{z \in \mathbb{F}_{q^n}} \chi_2(az^3+(b-3ae)z^2+(3ae^2-2eb+c)z+be^2-ae^3+d-ec)\chi_2(z). \end{aligned}$$

Hence, the result follows from Lemma 2.17 in the case $be^2 - ae^3 + d - ec \neq 0$. Otherwise,

$$\begin{aligned} N_n(\mathcal{C}) &= q^n + 1 + \sum_{z \in \mathbb{F}_{q^n}^*} \chi_2(az^3 + (b-3ae)z^2 + (3ae^2 - 2eb + c)z)\chi_2(\tfrac{1}{z}) \\ &= q^n + 1 + \sum_{z \in \mathbb{F}_{q^n}^*} \chi_2(az^2 + (b-3ae)z + (3ae^2 - 2eb + c)). \end{aligned}$$

In this case, the result follows from Lemma 2.9. ■

Example 2.19. *Let $\mathcal{J} : y^2 = (x^3 + x^2 - x + 1)(x + 1)$ be a curve over $\mathbb{F}_{73}$. In order to calculate $\omega_{73}(2, 0, -2, 1)$, we use Lemma 2.14 as in Example 2.15. We note that*

$$\omega_{73}(2,0,-2,1) + \overline{\omega_{73}(2,0,-2,1)} \equiv \sum_{l=12}^{18} \binom{36}{2l} \binom{2l}{36-l} 2^{36-l}(-2)^{3l-36}1^{36-2l} \equiv 16 \pmod{73},$$

then $\omega_{73}(2, 0, -2, 1) = 8 + 3\mathrm{i}$. Since $\Delta'(2, 0, -2, 1) = 1$, Theorem 2.18 states that the number of rational points on $\mathcal{J}$ over $\mathbb{F}_{73^n}$ is given by

$$N_n(\mathcal{J}) = 73^n - (8 + 3\mathrm{i})^n - (8 - 3\mathrm{i})^n .$$

Theorem 2.20. *For $a, b, c, d \in \mathbb{F}_q$, with $a \neq 0$, let $\mathcal{C} : y^2 = ax^6 + bx^4 + cx^2 + d$ be a curve over $\mathbb{F}_q$. The number of rational points on $\mathcal{C}$ over $\mathbb{F}_{q^n}$ is given by*

$$N_n(\mathcal{C}) = \begin{cases} q^n + 1 - \omega_1^n - \overline{\omega_1}^n - \omega_2^n - \overline{\omega_2}^n - \chi_2(a), & \text{if } d \neq 0 \text{ and } \Delta' = 1; \\ q^n + 1 - \chi_2(\alpha_1) - \chi_2(\alpha_2) - \chi_2(a), & \text{if } d \neq 0 \text{ and } \Delta' = 2; \\ q^n + 1 - \chi_2(a), & \text{if } d \neq 0 \text{ and } \Delta' = 3; \\ q^n + 1 - \omega_1^n - \overline{\omega_1}^n - \chi_2(a) - \chi_2(c), & \text{if } d = 0 \neq c \text{ and } b^2 - 4ac \neq 0; \\ q^n + 1 - \chi_2(\alpha_1) + (q^n - 1)\chi_2(a) - \chi_2(c), & \text{if } d = 0 \text{ and } b^2 - 4ac = 0; \\ q^n + 1 - \chi_2(\alpha_1) - \chi_2(a) - \chi_2(c), & \text{if } c = d = 0 \text{ and } b^2 - 4ac \neq 0, \end{cases}$$

where $\omega_1 := \omega_q(a, b, c, d)$, $\omega_2 := \omega_q(d, c, b, a), \alpha_1 := \alpha(a, b, c, d), \alpha_2 := \alpha(d, c, b, a)$ and $\Delta' := \Delta'(a, b, c, d)$.

Proof. The number of rational points on $\mathcal{C}$ is given by

$$\begin{aligned} N_n(\mathcal{C}) &= 1 + \sum_{x \in \mathbb{F}_{q^n}} \left[1 + \chi_2(ax^6 + bx^4 + cx^2 + d)\right] \\ &= 1 + \sum_{x \in \mathbb{F}_{q^n}} \left[1 + \chi_2(ax^3 + bx^2 + cx + d)\right] \left[1 + \chi_2(x)\right] \\ &= q^n + 1 + \sum_{x \in \mathbb{F}_{q^n}} \left[\chi_2(ax^3 + bx^2 + cx + d) + \chi_2(x) + \chi_2(ax^3 + bx^2 + cx + d)\chi_2(x)\right] . \end{aligned}$$

The result follows from Lemmas 2.11, 1.3 and 2.17 in the case $d \neq 0$. Otherwise,

$$\begin{aligned} N_n(\mathcal{C}) &= q^n + 1 + \sum_{x \in \mathbb{F}_{q^n}} \chi_2(ax^3 + bx^2 + cx) + \sum_{x \in \mathbb{F}_{q^n}^*} \chi_2(ax^3 + bx^2 + cx)\chi_2(\tfrac{1}{x}) \\ &= q^n + 1 + \sum_{x \in \mathbb{F}_{q^n}} \chi_2(ax^3 + bx^2 + cx) + \sum_{x \in \mathbb{F}_{q^n}^*} \chi_2(ax^2 + bx + c). \end{aligned}$$

Hence, the result follows from Lemma 2.9 and Lemma 2.11. ■

Example 2.21. *Let $\mathcal{J} : y^2 = 2x^6 + 1$ be a curve over $\mathbb{F}_{29}$. In order to calculate $\omega_{29}(2,0,0,1)$ and $\omega_{29}(1,0,0,2)$, we use Lemma 2.14 as in Example 2.15. We note that*

$$\omega_{29}(2,0,0,1) + \overline{\omega_{29}(2,0,0,1)} \equiv \sum_{l=5}^{7} \binom{14}{2l}\binom{2l}{14-l} 2^{14-l}0^{3l-14}1^{14-2l} \equiv 0 \pmod{29}$$

and

$$\omega_{29}(1,0,0,2) + \overline{\omega_{29}(1,0,0,2)} \equiv \sum_{l=5}^{7} \binom{14}{2l}\binom{2l}{14-l} 1^{14-l}0^{3l-14}2^{14-2l} \equiv 0 \pmod{29},$$

then $\omega_{29}(2,0,0,1) = \omega_{29}(1,0,0,2) = \mathrm{i}\sqrt{29}$. Since 2 is not square residue in $\mathbb{F}_{29}$ and $\Delta'(2,0,0,1) = 1$, Theorem 2.20 states that the number of rational points on $\mathcal{J}$ over $\mathbb{F}_{29^n}$ is given by

$$N_n(\mathcal{J}) = \begin{cases} 29^n + 4\cdot 29^{2k+1}, & \text{if } n = 4k+2 \text{ for an integer } k; \\ 29^n - 4\cdot 29^{2k}, & \text{if } n = 4k \text{ for an integer } k; \\ 29^n + 2, & \text{if } n \text{ is odd.} \end{cases}$$

Theorem 2.22. *For $a, b, c \in \mathbb{F}_q$, with $a \neq 0$, let $\mathcal{C} : y^2 = ax^4 + bx^2 + c$ be a curve over $\overline{\mathbb{F}}_q$. The number of rational points on $\mathcal{C}$ over $\mathbb{F}_{q^n}$ is given by*

$$N_n(\mathcal{C}) = \begin{cases} q^n + 1 - \omega_q(a,b,c,0)^n - \overline{\omega_q(a,b,c,0)}^n - \chi_2(a), & \text{if } b^2 - 4ac \neq 0, \text{ with } c \neq 0; \\ q^n + 1 - \chi_2(b) - \chi_2(a), & \text{if } b^2 - 4ac \neq 0, \text{ with } c = 0; \\ q^n + 1 - \chi_2(-b/2) + (q^n - 1)\chi_2(a), & \text{if } b^2 - 4ac = 0, \text{ with } c \neq 0; \\ q^n + 1 + (q^n - 1)\chi_2(a), & \text{if } b^2 - 4ac = 0, \text{ with } c = 0. \end{cases}$$

Proof. As in the last theorem,

$$N_n(\mathcal{C}) = q^n + 1 + \sum_{x \in \mathbb{F}_{q^n}} \left[\chi_2(ax^2 + bx + c) + \chi_2(x) + \chi_2(ax^3 + bx^2 + cx)\right].$$

By Lemmas 2.9, 1.3 and 2.11, the result follows. ■

Lemma 2.23. *Let i be a divisor of $q^n - 1$ and $A, B, C, a, b, c \in \mathbb{F}_q$, with $A \neq 0$ and $a \neq 0$. If $\alpha_1, \alpha_2 \in \mathbb{F}_{q^2}$ are the roots of the polynomial $f(x) = ax^2 + bx + c$ and the polynomials $f(x)$ and $g(x) = Ax^2 + Bx + C$ have no common roots, then*

$$\sum_{\substack{x \in \mathbb{F}_{q^n} \\ x \notin \{\alpha_1, \alpha_2\}}} \left[1 + \chi_k\left(\tfrac{Ax^2+Bx+C}{ax^2+bx+c}\right) + \cdots + \chi_k^{k-1}\left(\tfrac{Ax^2+Bx+C}{ax^2+bx+c}\right)\right] = N_n(\mathcal{C}) - \delta - \left[1 + \cdots + \chi_k^{k-1}\left(\tfrac{A}{a}\right)\right],$$

where $\mathcal{C}$ is a curve given by the equation $z^2 = (B - by^k)^2 - 4(A - ay^k)(C - cy^k)$ and δ is a constant referent to points at infinity given by

$$\delta := \begin{cases} 1 + \chi_2(b^2 - 4ac), & \text{if } k = 1; \\ 1 + \chi_2(4Ac + 4Ca - 2Bb), & \text{if } k = 2 \text{ and } b^2 - 4ac = 0; \\ 1, & \text{otherwise.} \end{cases}$$

Proof. We observe that the summation

$$\sum_{\substack{x\in\mathbb{F}_{q^n}\\ x\notin\{\alpha_1,\alpha_2\}}}\left[1+\chi_k\left(\tfrac{Ax^2+Bx+C}{ax^2+bx+c}\right)+\cdots+\chi_k^{k-1}\left(\tfrac{Ax^2+Bx+C}{ax^2+bx+c}\right)\right]$$

count the number of rational points on the curve $\mathcal{C}' : y^k(ax^2+bx+c) = Ax^2+Bx+C$ over $\mathbb{F}_{q^n}$. Let $y_0^k \in \mathbb{F}_{q^n}$, if there exists $x_0 \in \mathbb{F}_{q^n}$ such that (x_0, y_0) is on the curve, then it is given by one of the following

$$\frac{by^k - B \pm M}{2(A-ay^k)},$$

where $M^2 = (B-by^k)^2-4(A-ay^k)(C-cy^k)$. Therefore, fixing $y_0^k \in \mathbb{F}_{q^n}$, there exists $x_0 \in \mathbb{F}_{q^n}$ such that (x_0, y_0) is on the curve $\mathcal{C}'$ only if $(B-by_0^k)^2-4(A-ay_0^k)(C-cy_0^k)$ is a square in $\mathbb{F}_{q^n}$ or if $y_0^k = Aa^{-1}$. Let $\mathcal{C}$ be the curve given by equation $z^2 = (B-by^k)^2-4(A-ay^k)(C-cy^k)$. In the case where Aa^{-1} is a k-th power in $\mathbb{F}_{q^n}$ and $Aa^{-1}b \neq B$, there are i rational points of the form $\left(\frac{cA-Ca}{Ba-bA}, \gamma\right)$ on the curve $\mathcal{C}'$, where γ is a k-th primitive root of Aa^{-1}. Since there are $2k$ rational points in $\mathcal{C}$ where $y^k = Aa^{-1}$ (namely $\left(\pm\frac{Ba-bA}{a}, \gamma\right)$), the result is proved in this case. In the case where $Aa^{-1}b = B$, there are no rational points with $y^k = Aa^{-1}$ on the curve $\mathcal{C}'$ and only k on $\mathcal{C}$, then, in the same way, the result follows. ■

Remark 2.24. *Let $b, c, A, B, C \in \mathbb{F}_q$, with $A \neq 0$, $b \neq 0$ and $A(\frac{-c}{b})^2 + B(\frac{-c}{b}) + C \neq 0$. For k a divisor of $q^n - 1$, in the same way of the proof of Lemma 2.23, we have*

$$\sum_{\substack{x\in\mathbb{F}_{q^n}\\ x\neq -c/b}}\left[1+\chi_k\left(\tfrac{Ax^2+Bx+C}{bx+c}\right)+\cdots+\chi_k^{k-1}\left(\tfrac{Ax^2+Bx+C}{bx+c}\right)\right] = \begin{cases} N_n(\mathcal{C})-2, & \text{if } k=1;\\ N_n(\mathcal{C})-1, & \text{otherwise.}\end{cases}$$

where $\mathcal{C}$ is a curve given by the equation $z^2 = (B-by^k)^2 - 4A(C-cy^k)$.

Proof of Theorem 2.3. By Lemma 2.23,

$$\begin{aligned} N_n(\mathcal{C}_1) &= 1 + \sum_{x\in\mathbb{F}_{q^n}}\left[1+\cdots+\chi_k^{k-1}\big((Ax^2+Bx+C)(ax^2+bx+c)^{k-1}\big)\right]\\ &= 1 + |\{\alpha_1,\alpha_2\}\cap\mathbb{F}_{q^n}| + \sum_{x\in\mathbb{F}_{q^n}\setminus\{\alpha_1,\alpha_2\}}\left[1+\cdots+\chi_k^{k-1}\left(\frac{Ax^2+Bx+C}{ax^2+bx+c}\right)\right]\\ &= 1 + |\{\alpha_1,\alpha_2\}\cap\mathbb{F}_{q^n}| + N_n(\mathcal{C}) - \left[1+\chi_k\left(\tfrac{A}{a}\right)+\cdots+\chi_k^{k-1}\left(\tfrac{A}{a}\right)\right] - \delta, \end{aligned}$$

where $\mathcal{C}$ is the curve given by the equation $z^2 = (B-by^k)^2 - 4(A-ay^k)(C-cy^k)$. In the same way,

$$\begin{aligned} N_n(\mathcal{C}_2) &= 2 + \sum_{x\in\mathbb{F}_{q^n}\setminus\{\alpha_1,\alpha_2\}}\left[1+\chi_k\left(\frac{Ax^2+Bx+C}{ax^2+bx+c}\right)+\cdots+\chi_k^{k-1}\left(\frac{Ax^2+Bx+C}{ax^2+bx+c}\right)\right]\\ &= 2 + N_n(\mathcal{C}) - \left[1+\chi_k\left(\tfrac{A}{a}\right)+\cdots+\chi_k^{k-1}\left(\tfrac{A}{a}\right)\right] - \delta. \end{aligned}$$

■

We have the necessary tools to compute $N_n(\mathcal{C})$ in some cases, as we will see in the following results.

Corollary 2.25. *Let A, B, C, a, b, c be elements in $\mathbb{F}_q$ that satisfy the hypothesis of the Lemma 2.23. Assuming $b^2 - 4ac \neq 0$ and $B^2 - 4AC \neq 0$, the number of rational points on the curve $\mathcal{C} : y^2(ax^2 + bx + c) = Ax^2 + Bx + C$ over $\mathbb{F}_{q^n}$ is given by*

$$N_n(\mathcal{C}) = \begin{cases} q^n + 1 - \omega_q(a', b', c', 0)^n - \overline{\omega_q(a', b', c', 0)}^n - \chi_2(a') - \chi_2\left(\frac{A}{a}\right), & \text{if } \Delta \neq 0; \\ q^n + 1 - \chi_2(\alpha) + (q^n - 1)\chi_2(a') - \chi_2\left(\frac{A}{a}\right), & \text{if } \Delta = 0, \end{cases}$$

where $a' := b^2 - 4ac$, $b' := 4Ac + 4Ca - 2Bb$, $c' := B^2 - 4AC$, $\Delta := \Delta(a', b', c', 0)$ and $\alpha = \alpha(a', b', c', 0)$.

Proof. It follows from Theorems 2.3 and 2.22. ■

Corollary 2.26. *Let A, B, C, a, b, c be elements in $\mathbb{F}_q$ that satisfy the hypothesis of the Lemma 2.23. Assuming $b^2 - 4ac \neq 0$ and $B^2 - 4AC \neq 0$, the number of rational points on the curve $\mathcal{C} : y^2 = (ax^2 + bx + c)(Ax^2 + Bx + C)$ over $\mathbb{F}_{q^n}$ is given by*

$$N_n(\mathcal{C}) = \begin{cases} q^n + 2 \cdot \mathbb{1}_{\{\alpha_1 \in \mathbb{F}_{q^n}\}} - \omega_q(a', b', c', 0)^n - \overline{\omega_q(a', b', c', 0)}^n - \chi_2(a') - \chi_2\left(\frac{A}{a}\right), & \text{if } \Delta \neq 0; \\ q^n + 2 \cdot \mathbb{1}_{\{\alpha_1 \in \mathbb{F}_{q^n}\}} - \chi_2(\alpha) + (q^n - 1)\chi_2(a'), & \text{if } \Delta = 0, \end{cases}$$

where $a' := b^2 - 4ac$, $b' := 4Ac + 4Ca - 2Bb$, $c' := B^2 - 4AC$, $\Delta := \Delta(a', b', c', 0)$ and $\alpha = \alpha(a', b', c', 0)$.

Proof. It follows from Theorems 2.3 and 2.22. ■

The previous result generalizes the sums of quadratic characters studied by Williams in [107], where the author computes the sum

$$\sum_{x \in \mathbb{F}_p} \chi_2\left((ax^2 + bx + c)(Ax^2 + Bx + C)\right)$$

over a prime field $\mathbb{F}_p$.

Example 2.27. *Let $\mathcal{J} : y^2 = (x^2 + 3x + 2)(x^2 - 2x - 5)$ be a curve over $\mathbb{F}_{67}$. In order to calculate $\omega_{67}(1, 0, 24, 0)$, we use Lemma 2.14 as in Example 2.15. We note that*

$$\omega_{67}(1, 0, 24, 0) + \overline{\omega_{67}(1, 0, 24, 0)} \equiv \sum_{l=11}^{16} \binom{33}{2l} \binom{2l}{33 - l} 1^{33-l} (24)^{3l-33} 0^{33-2l} \equiv 0 \pmod{67},$$

then $\omega_{67}(1, 0, 24, 0) = \mathrm{i}\sqrt{67}$. Since $\Delta(1, 0, 24, 0) = -55296 \neq 0$, Corollary 2.26 states that the number of rational points on $\mathcal{J}$ over $\mathbb{F}_{67^n}$ is given by

$$N_n(\mathcal{J}) = \begin{cases} 67^n - 2\left(\mathrm{i}\sqrt{67}\right)^n, & \text{if } n \text{ is even}; \\ 67^n, & \text{if } n \text{ is odd}. \end{cases}$$

In Theorem 2.18 and Corollary 2.26, we give the number of rational points on $y^2 = f(x)$, where $f(x)$ is a polynomial of degree 4 that is reducible over $\mathbb{F}_q$. In Theorem 2.22 we give this number in the case where $f(x) = ax^4 + bx^2 + c$. Hence, we presented the number of rational points on most hyperelliptic curves of degree 4 over finite fields of odd characteristic. The remaining case is the curve given by the equation $y^2 = ax^4 + bx^2 + cx + d$, with $c \neq 0$, where $f(x) = ax^4 + bx^2 + cx + d$ is an irreducible polynomial over $\mathbb{F}_q$. In fact, we do not know how to calculate the number of rational points in this specific case.

2.4 Rational points on curves of the form $y^3 = f(x)$

In this section, we assume $q \equiv 1 \pmod 3$. The case $q \not\equiv 1 \pmod 3$ is not interesting, since the function $y \mapsto y^3$ permutes the elements of $\mathbb{F}_q$.

Theorem 2.28. *Let $a, A, B, C \in \mathbb{F}_q$ with $A \neq 0$. Let $\mathcal{C}_1 : y^3 = (x+a)(Ax^2+Bx+C)$ and $\mathcal{C}_2 : y^3 = (x+a)^2(Ax^2+Bx+C)^2$ be curves over $\overline{\mathbb{F}}_q$. If $Aa^2 - Ba + C \neq 0$, then the number of rational points on $\mathcal{C}_1$ and $\mathcal{C}_2$ over $\mathbb{F}_{q^n}$ satisfies*

$$N_n(\mathcal{C}_1) = N_n(\mathcal{C}_2) + \chi_3(A) + \chi_3^2(A) = q^n + 1 - \omega_q(a', 0, 0, c')^n - \overline{\omega_q(a', 0, 0, c')}^n,$$

where $a' := 4Aa^2 + 4C - 4Ba$ and $c' := B^2 - 4AC$.

Proof. Since the number of rational points on the $\mathcal{C}_1 : y^3 = (x+a)(Ax^2+Bx+C)$ is equal to the number of rational points on the curve $\mathcal{C}' : y^3 = (x+a)^4(Ax^2+Bx+C)$, except 3 possible points at infinity, the value $N_n(\mathcal{C}_1)$ follows from Theorem 2.3 and Lemma 2.11. In order to calculate $N_n(\mathcal{C}_2)$, we note that

$$\begin{aligned}
N_n(\mathcal{C}_2) &= 1 + \sum_{x \in \mathbb{F}_{q^n}} \left[1 + \chi_3\left((x+a)^2(Ax^2+Bx+C)^2\right) + \chi_3^2\left((x+a)^2(Ax^2+Bx+C)^2\right)\right] \\
&= 1 + \sum_{x \in \mathbb{F}_{q^n}} \left[1 + \chi_3^2\left((x+a)^4(Ax^2+Bx+C)^4\right) + \chi_3\left((x+a)(Ax^2+Bx+C)\right)\right] \\
&= 1 + \sum_{x \in \mathbb{F}_{q^n}} \left[1 + \chi_3^2\left((x+a)(Ax^2+Bx+C)\right) + \chi_3\left((x+a)(Ax^2+Bx+C)\right)\right] \\
&= N_n(\mathcal{C}_1) - \chi_3(A) - \chi_3^2(A).
\end{aligned}$$

■

Example 2.29. *Let $\mathcal{J}_1 : y^3 = (x+3)(-x^2+2x+2)$ be a curve over $\mathbb{F}_{37}$. In order to calculate $\omega_{37}(-52, 0, 0, 12)$, we use Lemma 2.14 as in Example 2.15. We note that*

$$\omega_{37}(-52,0,0,12) + \overline{\omega_{37}(-52,0,0,12)} \equiv \sum_{l=6}^{9} \binom{18}{2l}\binom{2l}{18-l}(-52)^{18-l}0^{3l-18}12^{18-2l} \equiv 27 \pmod{37},$$

then $\omega_{37}(-52, 0, 0, 12) = -5 + \mathrm{i}\sqrt{12}$. Theorem 2.28 states that the number of rational points on $\mathcal{J}_1$ over $\mathbb{F}_{37^n}$ is given by

$$N_n(\mathcal{J}_1) = 37^n + 1 - \left(-5 + \mathrm{i}\sqrt{12}\right)^n - \left(-5 - \mathrm{i}\sqrt{12}\right)^n.$$

In addition, the number of rational points on the curve $\mathcal{J}_2 : y^3 = (x+3)^2(-x^2+2x+2)^2$ *over* $\mathbb{F}_{37^n}$ *is given by*

$$N_n(\mathcal{J}_2) = 37^n - 1 - \left(-5 + \mathrm{i}\sqrt{12}\right)^n - \left(-5 - \mathrm{i}\sqrt{12}\right)^n.$$

Theorem 2.30. *Let* $a, b \in \mathbb{F}_q^*$. *The number of rational points on* $\mathcal{C} : y^3 = ax^3 + b$ *over* $\mathbb{F}_{q^n}$ *satisfies*

$$N_n(\mathcal{C}) = q^n + 1 - \omega_q(a^{-1}, 0, 0, (b/2a)^2)^n - \overline{\omega_q(a^{-1}, 0, 0, (b/2a)^2)}^n.$$

Proof. We have

$$\begin{aligned} N_n(\mathcal{C}) &= 1 + \chi_3(a) + \chi_3^2(a) + \sum_{x \in \mathbb{F}_{q^n}} \left[1 + \chi_3(ax+b) + \chi_3^2(ax+b)\right]\left[1 + \chi_3(x) + \chi_3^2(x)\right] \\ &= 1 + \chi_3(a) + \chi_3^2(a) + S_1 + S_2, \end{aligned}$$

where

$$\begin{aligned} S_1 :&= \sum_{x \in \mathbb{F}_{q^n}} \left[1 + \chi_3(ax^2+bx) + \chi_3^2(ax^2+bx)\right] \\ &= \sum_{z \in \mathbb{F}_{q^n}} \left[1 + \chi_3\left(a\left(z - \tfrac{b}{2a}\right)^2 + b\left(z - \tfrac{b}{2a}\right)\right) + \chi_3^2\left(a\left(z - \tfrac{b}{2a}\right)^2 + b\left(z - \tfrac{b}{2a}\right)\right)\right] \\ &= \sum_{z \in \mathbb{F}_{q^n}} \left[1 + \chi_3\left(az^2 - \tfrac{b^2}{4a}\right) + \chi_3^2\left(az^2 - \tfrac{b^2}{4a}\right)\right] \end{aligned}$$

and

$$\begin{aligned} S_2 :&= \sum_{x \in \mathbb{F}_{q^n}^*} \left[\chi_3(ax+b)\chi_3^2(x) + \chi_3^2(ax+b)\chi_3^4(x)\right] \\ &= \sum_{x \in \mathbb{F}_{q^n}^*} \left[\chi_3(a + b\tfrac{1}{x}) + \chi_3^2(a + b\tfrac{1}{x})\right] \\ &= \sum_{z \in \mathbb{F}_{q^n}^*} \left[\chi_3(a+bz) + \chi_3^2(a+bz)\right] \\ &= -\chi_3(a) - \chi_3^2(a). \end{aligned}$$

Since S_1 count the number of rational points in the curve with equation $z^2 = \frac{y^3}{a} + \frac{b^2}{4a^2}$, the result follows from Lemma 2.11. ■

Proof of Theorem 2.2. We note that

$$\begin{aligned} N_n(\mathcal{C}) &= 1 + \sum_{x \in \mathbb{F}_{q^n}} \left[1 + \chi_3(ax^2+b) + \chi_3^2(ax^2+b)\right]\left[1 + \chi_3(x) + \chi_3^2(x)\right] \\ &= 1 + S_1 + S_2 + S_3, \end{aligned}$$

where

$$\begin{aligned} S_1 &:= \sum_{x \in \mathbb{F}_{q^n}} \left[1 + \chi_3(ax^2+b) + \chi_3^2(ax^2+b) + \chi_3(x) + \chi_3^2(x)\right] \\ &= \sum_{x \in \mathbb{F}_{q^n}} \left[1 + \chi_3(ax^2+b) + \chi_3^2(ax^2+b)\right] \\ &= \sum_{w \in \mathbb{F}_{q^n}} \left[1 + \chi_2(a^{-1}w^3 - ba^{-1})\right], \end{aligned}$$

$$\begin{aligned} S_2 &:= \sum_{x\in\mathbb{F}_{q^n}} \left[\chi_3(ax^2+b)\chi_3(x) + \chi_3^2(ax^2+b)\chi_3^2(x)\right] \\ &= \sum_{x\in\mathbb{F}_{q^n}^*} \left[\chi_3\left(\frac{ax^2+b}{x^2}\right) + \chi_3^2\left(\frac{ax^2+b}{x^2}\right)\right] \\ &= \sum_{z\in\mathbb{F}_{q^n}^*} \left[\chi_3(a+bz^2) + \chi_3^2(a+bz^2)\right] \\ &= \sum_{w\in\mathbb{F}_{q^n}} \chi_2(b^{-1}w^3 - ab^{-1}) - \chi_3(a) - \chi_3^2(a) \end{aligned}$$

and

$$\begin{aligned} S_3 &:= \sum_{x\in\mathbb{F}_{q^n}} \left[\chi_3(ax^2+b)\chi_3^2(x) + \chi_3^2(ax^2+b)\chi_3(x)\right] \\ &= \sum_{x\in\mathbb{F}_{q^n}^*} \left[\chi_3\left(\frac{ax^2+b}{x}\right) + \chi_3^2\left(\frac{ax^2+b}{x}\right)\right]. \end{aligned}$$

By Lemma 2.11,

$$S_1 = q^n - \omega_1^n - \overline{\omega_1}^n,$$

where $\omega_1 := \omega_q(a^{-1}, 0, 0, -ba^{-1})$ and

$$S_2 = -\omega_2^n - \overline{\omega_2}^n - \chi_3(a) - \chi_3^2(a),$$

where $\omega_2 := \omega_q(b^{-1}, 0, 0, -ab^{-1})$. By Remark 2.24 and Theorem 2.20,

$$S_3 = -\omega_3^n - \overline{\omega_3}^n - \omega_4^n - \overline{\omega_4}^n,$$

where $\omega_3 := \omega_q(1, 0, 0, -4ab)$ and $\omega_4 := \omega_q(-4ab, 0, 0, 1)$. ■

Example 2.31. *Let $\mathcal{J} : y^3 = x^6 + 1$ be a curve over $\mathbb{F}_{103}$. We use Lemma 2.14 as in Example 2.15 to calculate the complex numbers ω_i in Theorem 2.2. We have*

$\omega_{103}(1,0,0,-1) = -10+\mathrm{i}\sqrt{3}$, $\omega_{103}(1,0,0,-4) = \frac{7+\mathrm{i}\sqrt{363}}{2}$ *and* $\omega_{103}(-4,0,0,1) = \frac{-13+\mathrm{i}\sqrt{243}}{2}$.

Then, by Theorem 2.2,

$$N_n(\mathcal{J}) = 103^n - 1 - 2\cdot\omega_1^n - 2\cdot\overline{\omega_1}^n - \omega_2^n - \overline{\omega_2}^n - \omega_3^n - \overline{\omega_3}^n,$$

where $\omega_1 := -10 + \mathrm{i}\sqrt{3}$, $\omega_2 := \frac{7+\mathrm{i}\sqrt{363}}{2}$ *and* $\omega_3 := \frac{-13+\mathrm{i}\sqrt{243}}{2}$.

2.5 Rational points on curves of the form $y^4 = f(x)$

In this section, we compute the number of rational points on curves of the form $y^4 = ax^4 + bx^2 + c$. The case $q \equiv 3 \pmod 4$ must be considered separately, since every square is a fourth power, as we show in the following lemma.

Lemma 2.32. *Let $\mathbb{F}_q$ be a finite field with $q \equiv 3 \pmod 4$ elements and k a positive integer. An element $\alpha \in \mathbb{F}_q$ is a square if and only if it is a 2^k power.*

Proof. Since $\gcd(2^{k-1}, \frac{q-1}{2}) = 1$, there are integers a, b such that $2^{k-1} \cdot a + \frac{q-1}{2} \cdot b = 1$. Then

$$\alpha^2 = \alpha^{2^k \cdot a + (q-1)\cdot b} = (\alpha^a)^{2^k}$$

for all $\alpha \in \mathbb{F}_q$. Conversely,

$$\alpha^{2^k} = \alpha^{2^{2k-1}a + 2^{k-1}(q-1)b} = \left(\alpha^{2^{2k-2}a}\right)^2,$$

which completes the proof. ■

Therefore, in the case $q \equiv 3 \pmod 4$, the number of rational points on $\mathcal{L} : y^4 = ax^4 + bx^2 + c$ is the same as the number of rational points on $y^2 = ax^4 + bx^2 + c$ except points at infinity. We have already presented the number of points on $y^2 = ax^4 + bx^2 + c$ in Theorem 2.22. In order to compute $N_n(\mathcal{L})$ for any positive integer n in the case where the a, b, c are elements in a prime field, we have to compute the number of points in these curves in the case $q \equiv 1 \pmod 4$.

Lemma 2.33. *Let $a, b, c \in \mathbb{F}_q$, with $a \neq 0$ and $q \equiv 1 \pmod 4$. For $f(x) := ax^2 + bx + c$, we have*

$$\sum_{x \in \mathbb{F}_{q^n}} \left[\chi_4(f(x)) + \chi_4^3(f(x))\right] = \begin{cases} -\omega_q(a^{-1}, 0, d, 0)^n - \overline{\omega_q(a^{-1}, 0, d, 0)}^n, & \text{if } b^2 - 4ac \neq 0; \\ 0, & \text{if } b^2 - 4ac = 0, \end{cases}$$

where $d := \frac{b^2 - 4ac}{4a^2}$.

Proof. We observe that

$$\begin{aligned} &1 + \sum_{x \in \mathbb{F}_{q^n}} \left[1 + \chi_4(ax^2 + bx + c) + \chi_4^2(ax^2 + bx + c) + \chi_4^3(ax^2 + bx + c)\right] \\ &= 1 + \sum_{z \in \mathbb{F}_{q^n}} \left[1 + \chi_4\big(az^2 - \tfrac{b^2 - 4ac}{4a}\big) + \chi_4^2\big(az^2 - \tfrac{b^2 - 4ac}{4a}\big) + \chi_4^3\big(az^2 - \tfrac{b^2 - 4ac}{4a}\big)\right] \end{aligned}$$

calculate the number of rational points on the curve $\mathcal{C} : z^2 = \frac{y^4}{a} + \frac{b^2 - 4ac}{4a^2}$. Therefore, letting $L := \sum_{x \in \mathbb{F}_{q^n}} \left[\chi_4(f(x)) + \chi_4^3(f(x))\right]$, by Theorem 2.22, we have

$$L = -\sum_{x \in \mathbb{F}_{q^n}} \chi_4^2(ax^2 + bx + c) + \begin{cases} -\omega_q(a^{-1}, 0, d, 0)^n - \overline{\omega_q(a^{-1}, 0, d, 0)}^n - \chi_2(a), & \text{if } b^2 - 4ac \neq 0; \\ (q^n - 1)\chi_2(a), & \text{if } b^2 - 4ac = 0, \end{cases}$$

where $d := \frac{b^2 - 4ac}{4a^2}$. The result follows from Lemma 2.9. ■

Proof of Theorem 2.4. We have

$$\begin{aligned} N_n(\mathcal{C}) &= \delta + \sum_{x \in \mathbb{F}_{q^n}} \left[1 + \chi_4(ax^2 + bx + c) + \chi_4^2(ax^2 + bx + c) + \chi_4^3(ax^2 + bx + c)\right]\left[1 + \chi_4^2(x)\right] \\ &= \delta + S_1 + S_2, \end{aligned}$$

where $\delta := 1 + \chi_4(a) + \chi_4^2(a) + \chi_4^3(a)$.

$$S_1 := \sum_{x \in \mathbb{F}_{q^n}} 1 + \chi_4(ax^2+bx+c) + \chi_4^2(ax^2+bx+c) + \chi_4^3(ax^2+bx+c)$$

and

$$S_2 := \sum_{x \in \mathbb{F}_{q^n}^*} \big[1 + \chi_4(ax^2+bx+c) + \chi_4^2(ax^2+bx+c) + \chi_4^3(ax^2+bx+c)\big]\chi_4^2(x).$$

By Remark 2.16,

$$\begin{aligned} S_2 &= \sum_{x \in \mathbb{F}_{q^n}^*} \left[\chi_4^2(x) + \chi_4\left(\frac{ax^2+bx+c}{x^2}\right) + \chi_4^2(ax^3+bx^2+cx) + \chi_4^3\left(\frac{ax^2+bx+c}{x^2}\right)\right] \\ &= \sum_{x \in \mathbb{F}_{q^n}^*} \chi_4^2(ax^3+bx^2+cx) + \sum_{z \in \mathbb{F}_q^*} \big[\chi_4(a+bz+cz^2) + \chi_4^3(a+bz+cz^2)\big]. \end{aligned}$$

Using Lemmas 2.9 and 2.33 in S_1 and Lemmas 1.3, 2.11 and 2.33 in S_2, the result follows. ■

Example 2.34. *Let $\mathcal{J} : y^4 = x^4 + 4x^2 - 1$ be a curve over $\mathbb{F}_{41}$. We use Lemma 2.14 as in Example 2.15 to calculate the complex numbers ω_i in Theorem 2.4. We have*

$$\omega_{41}(1,0,5,0) = \omega_{41}(-1,0,5,0) = \omega_{41}(1,4,-1,0) = -5 + 4\mathrm{i}.$$

Then, by Theorem 2.4, the number of rational points on $\mathcal{J}$ over $\mathbb{F}_{41^n}$ is given by

$$N_n(\mathcal{J}) = 41^n + 1 - 3 \cdot (-5+4\mathrm{i})^n - 3 \cdot (-5-4\mathrm{i})^n.$$

In the following result, we use that the number of rational points on $\mathcal{L} : y^4 = ax^4 + bx^2 + c$ is essentially the number of points on $\mathcal{L}' : y^2 = ax^4 + bx^2 + c$, as we have seen in Lemma 2.32.

Corollary 2.35. *For $a, b, c \in \mathbb{F}_p$, where $p \equiv 3 \pmod 4$ is a prime number and $a \neq 0$. The number of rational points on the curve $\mathcal{C} : y^4 = ax^4 + bx^2 + c$ over $\mathbb{F}_{p^n}$ satisfies*

$$N_n(\mathcal{C}) = \begin{cases} p^n + 1 - 2(i\sqrt{p})^n - 2(-i\sqrt{p})^n - \omega^n - \overline{\omega}^n, & \text{if } b^2 - 4ac \neq 0 \text{ and } c \neq 0; \\ p^n + 1 - (i\sqrt{p})^n - (-i\sqrt{p})^n - \chi_2(b), & \text{if } b^2 - 4ac \neq 0 \text{ and } c = 0; \\ p^n + 1 - \chi_2(-b/2) + p^n \cdot \chi_2(a), & \text{if } b^2 - 4ac = 0 \text{ and } c \neq 0; \\ p^n + 1 - \chi_2(b) + p^n \cdot \chi_2(a), & \text{if } b^2 - 4ac = 0 \text{ and } c = 0, \end{cases}$$

where $\omega := \omega_p(a,b,c,0)$.

Proof. By Theorem 2.4 and Remark 2.8,

$$N_{2n}(\mathcal{C}) = \begin{cases} p^{2n} + 1 - \omega_1^{2n} - \overline{\omega_1}^{2n} - \omega_2^n - \overline{\omega_2}^{2n} - \omega_3^{2n} - \overline{\omega_3}^{2n}, & \text{if } b^2 - 4ac \neq 0 \text{ and } c \neq 0; \\ p^{2n} + 1 - \omega_1^{2n} - \overline{\omega_1}^{2n} - \chi_2(b), & \text{if } b^2 - 4ac \neq 0 \text{ and } c = 0; \\ p^{2n} + 1 - \chi_2(-b/2) + p^{2n} \cdot \chi_2(a), & \text{if } b^2 - 4ac = 0 \text{ and } c \neq 0; \\ p^{2n} + 1 - \chi_2(b) + p^{2n} \cdot \chi_2(a), & \text{if } b^2 - 4ac = 0 \text{ and } c = 0, \end{cases}$$

where $\omega_1 := \omega_p(a^{-1}, 0, d_1, 0)$, $d_1 := \frac{b^2-4ac}{4a^2}$, $\omega_2 := \omega_p(c^{-1}, 0, d_2, 0)$, $d_2 := \frac{b^2-4ac}{4c^2}$ and $\omega_3 := \omega_p(a, b, c, 0)$. Lemma 2.14 states that

$$\omega_1 + \overline{\omega_1} \equiv \omega_2 + \overline{\omega_2} \equiv 0 \pmod{p}.$$

Since $|\omega_1 + \overline{\omega_1}| \leq 2\sqrt{p}$ and $|\omega_2 + \overline{\omega_2}| \leq 2\sqrt{p}$, we must have

$$\Re(\omega_1) = \Re(\omega_2) = 0$$

for $p > 4$. A straightforward calculation shows that

$$\Re(\omega_3(a^{-1}, 0, d_1, 0)1) = \Re(\omega_3(c^{-1}, 0, d_2, 0)) = 0.$$

In addition, since there are $1 + \chi_2(a)$ points at infinity on $\mathcal{C}$ (by Lemma 2.32, each element $a \in \mathbb{F}_p$ has exactly 0 or 2 fourth roots), by Theorem 2.22, we have

$$N_{2n-1}(\mathcal{C}) = \begin{cases} p^{2n-1} + 1 - \omega_3^{2n-1} - \overline{\omega_3}^{2n-1}, & \text{if } b^2 - 4ac \neq 0, \text{ with } c \neq 0; \\ p^{2n-1} + 1 - \chi_2(b), & \text{if } b^2 - 4ac \neq 0, \text{ with } c = 0; \\ p^{2n-1} + 1 - \chi_2(-b/2) + p^{2n-1} \cdot \chi_2(a), & \text{if } b^2 - 4ac = 0, \text{ with } c \neq 0; \\ p^{2n-1} + 1 + p^{2n-1} \cdot \chi_2(a), & \text{if } b^2 - 4ac = 0, \text{ with } c = 0 \end{cases}$$

for all positive integer n. The result follows by gathering the expressions for N_{2n} and N_{2n-1}. ■

The results provided in this chapter can be readily used to characterize the maximality and minimality of the Fermat curve

$$ax^n + by^n + cz^n = 0,$$

where $a, b, c \in \mathbb{F}_p^*$ and $n \in \{3, 4\}$. For more details on how this can be done, see Section 7 of [65]. In this thesis we will study a more general version of this problem. In Chapter 4 we provide necessary and sufficient conditions in which hypersurfaces of Fermat type are maximal or minimal.

CHAPTER 3

Hypersurfaces of Fermat type

Throughout this chapter, $\mathbb{F}_q$ denotes a finite field with $q = p^n$ elements. For $\vec{a} = (a_1, \ldots, a_s) \in \mathbb{F}_q^s$, $\vec{d} = (d_1, \ldots, d_s) \in \mathbb{Z}_+^s$, $\vec{t} = (t_1, \ldots, t_s) \in \mathbb{Z}_+^s$ and $b \in \mathbb{F}_q$, let $N_s(\vec{a}, \vec{d}, \vec{t}, q, b)$ be the number of $\mathbb{F}_q$-rational points on the affine hypersurface defined over $\mathbb{F}_q$ given by

$$a_1 x_1^{d_1} + \cdots + a_s x_s^{d_s} = b \tag{3.1}$$

where $x_i \in \mathbb{F}_{p^{t_i}}$. The Equation (3.1) is also called diagonal equation in the literature. In this thesis, we prefer using the algebraic geometry notation so that all the chapters have the same notation. Along the chapter, by Fermat type hypersurface we mean the affine hypersurface defined by Equation (3.1). We sometimes call them Fermat hypersurface for short. We set $N_s(\vec{a}, \vec{d}, q, b) = N_s(\vec{a}, \vec{d}, \vec{t}, q, b)$, where $\vec{t} = (n, \ldots, n)$. Weil [105] and Hua and Vandiver [43] independently showed that $N_s(\vec{a}, \vec{d}, q, b)$ can be expressed in terms of character sums. In particular, Weil's result implies that

$$|N_s(\vec{a}, \vec{d}, q, 0) - q^{s-1}| \leq I(d_1, \ldots, d_s)(q-1)q^{(s-2)/2} \tag{3.2}$$

where $I(d_1, \ldots, d_s)$ is the number of s-tuples $(y_1, \ldots, y_s) \in \mathbb{Z}^s$, with $1 \leq y_i \leq d_i - 1$ for all $i = 1, \ldots, s$, such that

$$\frac{y_1}{d_1} + \cdots + \frac{y_s}{d_s} \equiv 0 \pmod 1. \tag{3.3}$$

The study of solutions of diagonal equations played an essential role in the statement of Weil's conjectures for algebraic varieties and in the development of the algebraic geometry. A formula for $I(d_1, \ldots, d_s)$ can be found in Lidl and Niederreiter [50, p. 293]. A simpler formula is established in Lemma 9 of [89]. Some properties of $I(d_1, \ldots, d_s)$ have been explored by several authors [12, 93] and the possible values of $N_s(\vec{a}, \vec{d}, q, 0)$ in the case where $I(d_1, \ldots, d_s) \in \{1, 2\}$ was studied by Sun and Yuan [94]. A Fermat hypersurface (with $b = 0$) is called *maximal* (or *minimal*) if its number of $\mathbb{F}_q$-rational points attains the bound (3.2) and the maximality or minimality are set accordingly to $N_s(\vec{a}, \vec{d}, q, 0)$

attaining the upper or lower bound, respectively. The number of $\mathbb{F}_q$-rational points of Fermat hypersurfaces, with $s = 3$, $d_1 = d_2 = d_3$ and $b = 0$, is closely related to the number of $\mathbb{F}_q$-rational points on projective curves given by the equation $ax^m + by^m = c$ (see Section 3.6 for more details). Maximality and minimality have been extensively studied in the context of curves [33, 97, 98]. For instance, maximal and minimal Fermat type curves of the form $x^m + y^m = 1$ were studied by Tafazolian [96].

The number of $\mathbb{F}_q$-rational points on Fermat hypersurfaces with $t_1 = \cdots = t_s = n$ has been extensively studied in the last few decades [8, 9, 12, 41, 94, 110]. In many cases, the authors present a formula for the number of $\mathbb{F}_q$-rational points on Fermat hypersurfaces whose exponents satisfy certain natural restrictions. The case where q is a square provides families of Fermat hypersurfaces whose number of points can be obtained by means of simple parameters. For instance, in the case where $q = p^n$ for an even integer n, Wolfmann [109] presented an explicit formula for $N_s(\vec{a}, \vec{d}, q, b)$ in the case where $d = d_1 = \cdots = d_s$ and there exists a divisor r of n such that d divides $p^r + 1$. Still in the case where n is even, Cao, Chou and Gu [13] obtained a formula for $N_s(\vec{a}, \vec{d}, q, b)$ in terms of $I(d_1, \ldots, d_s)$ in the case where there exists a divisor r of n such that d_i divides $p^r + 1$ and $a_i \in \mathbb{F}_{p^r}$ for all $i = 1, \ldots, s$. For more results concerning Fermat hypersurfaces, see Section 7.3 in [59] and the references therein.

In [78], the author studies a class of suitable generalized diagonal equations with restricted solutions sets. The problem of counting the number of $\mathbb{F}_q$-rational points with variables in different subfields of finite fields has been studied theoretically in great generality by Wan [102, 103]. In his works, it is proved the rationality of the associated partial zeta function. Although the zeta function have been studied by Wan, none explicit formula is known. Inspired by Weil's approach on the counting of $\mathbb{F}_q$-rational points on Fermat hypersurfaces and the results obtained recently in [78, 102, 103], one goal of this chapter is to present a study on the number of $\mathbb{F}_q$-rational points on Fermat hypersurfaces over $\mathbb{F}_q$ where each variable is restricted to a subfield of $\mathbb{F}_q$. It turned out that the number of $\mathbb{F}_q$-rational points on these hypersurfaces can be computed similarly to the way that is done in the traditional Fermat hypersurfaces' case. In order to do that, we employ some well-known results on quadratic forms over finite dimensional vector spaces over a finite field.

In this chapter, we also obtain an explicit formula for $N_s(\vec{a}, \vec{d}, q, b)$ in a setting more general than that presented in [109] and [13]. In Theorem 3.7, we present the number of $\mathbb{F}_q$-rational points on Equation (3.1) in the case where $b = 0$, $q = p^n$ and, for each $i = 1, \ldots, s$, there exists a divisor r_i of n such that $d_i | (p^{r_i} + 1)$. Most notably, Theorem 3.9 provides the number of $\mathbb{F}_q$-rational points Equation (3.1) in the case where $b \neq 0$, $q = p^n$ and there exists a divisor r of t such that $d_i | (p^r + 1)$ for all $i = 1, \ldots, s$.

The chapter is organized as follows. In Section 3.1 we state our main results and provide some important remarks. Section 3.2 provides preliminary results which will be used to prove some of our results. In Section 3.3 we prove our counting results in the

general case. The case $d_1 = \cdots = d_s = 2$ is settled in Section 3.4. We focus on the case where $t_1 = \cdots = t_s = n$ in Section 3.5. In Section 3.6, we present bounds on the number of $\mathbb{F}_q$-rational point on Fermat curves. Finally, in Section **??** we provide some final considerations and open problems.

3.1 Main results

In this section we state the main results of this chapter. Throughout the chapter, $q = p^n$ for some positive integer n and an odd prime p and α is a primitive element of $\mathbb{F}_q$. If $d_i = 1$ for some $i \in \{1, \ldots, s\}$, then the number of $\mathbb{F}_q$-rational points on Equation (3.1) over $\mathbb{F}_q$ is q^{s-1}, then along the chapter we assume that $d_i > 1$ for all $i = 1, \ldots, s$. We let $\vec{a}$ denote a vector $(a_1, \ldots, a_s) \in \mathbb{F}_q^s$, where $a_i \neq 0$ for all $i = 1, \ldots, s$. For d a divisor of $q-1$, let χ_d be a multiplicative character of $\mathbb{F}_q^*$ of order d. As usual, we extend χ_d to $\mathbb{F}_q$ by setting $\chi_d(0) = 0$. The following definitions will be extensively used in our main results.

Definition 3.1. *For $\vec{a} = (a_1, \ldots, a_s) \in \mathbb{F}_q^s$, $\vec{d} = (d_1, \ldots, d_s)$ and $\vec{t} = (t_1, \ldots, t_s)$, let $N_s(\vec{a}, \vec{d}, \vec{t}, q, b)$ be the number of $\mathbb{F}_q$-rational points on the Fermat hypersurface given by*

$$a_1 x_1^{d_1} + \cdots + a_s x_s^{d_s} = b \tag{3.4}$$

where $x_i \in \mathbb{F}_{p^{t_i}}$.

For t a divisor of n, let Tr_{p^n/p^t} denote the trace function from $\mathbb{F}_{p^n}$ into $\mathbb{F}_{p^t}$. Throughout the following results, let $\vec{t} = (2t_1, \ldots, 2t_s)$ and $\vec{a} \in \mathbb{F}_q^s$, where $2t_i | n$ for all $i = 1, \ldots, s$. Since we are interested in the number of $\mathbb{F}_q$-rational points given by the hypersurface defined by Equation (3.1), by a simple change of variables, we may assume without loss of generality that d_i is a divisor of $p^{2t_i} - 1$ for all $i = 1, \ldots, s$.

Throughout the chapter, when we assume d_i is (p, r_i)-admissible, we mean d_i is (p, r_i)-admissible for all $i = 1, \ldots, s$. This hypothesis is extremely important and it will be used frequently in our results. More comments about the importance of this hypothesis can be found in Section **??**.

Definition 3.2. *Let $a \in \mathbb{F}_q$ and let d, t, r be positive integers such that $r|t$, $2t|n$ and d is a (p, r)-admissible. We set $m = \frac{p^{2t}-1}{d}$, $u = \frac{p^r+1}{d}$ and $\varepsilon = (-1)^{t/r}$. Let $T(x) = \mathrm{Tr}_{q/p^{2t}}(x)$.*

(a) For $c \in \mathbb{F}_q$, let

$$\Delta(a, d, t, r, c) = \begin{cases} p^t, & \text{if } T(ca) = 0; \\ \varepsilon(1-d), & \text{if } T(ca)^m = \varepsilon^u; \\ \varepsilon, & \text{if } T(ca)^m \notin \{0, \varepsilon^u\}. \end{cases}$$

(b) Let $\Lambda(a, t) = \{c \in \mathbb{F}_q : T(ca) = 0\}$.

We start with the following important result.

Theorem 3.3. *Assume that d_i is (p, r_i)-admissible. Then*

$$N_s(\vec{a}, \vec{d}, \vec{t}, q, 0) = p^{t_1+\cdots+t_s-n} \sum_{c\in\mathbb{F}_q} \prod_{i=1}^{s} \Delta(a_i, d_i, t_i, r_i, c),$$

where $\Delta(a_i, d_i, t_i, r_i, c)$ is as in Definition 3.2.

As a direct consequence of Theorem 3.3, if $t_1+\cdots+t_s > n$, then we have that $p^{t_1+\cdots+t_s-n}$ divides $N_s(\vec{a}, \vec{d}, \vec{t}, q, 0)$. Then $N_s(\vec{a}, \vec{d}, \vec{t}, q, 0) > 0$ implies that $N_s(\vec{a}, \vec{d}, \vec{t}, q, 0) \geq p^{t_1+\cdots+t_s-n}$.

Corollary 3.4. *Let $b \in \mathbb{F}_q^*$ and suppose $d_1 = \cdots = d_s = d$. Assume that d is (p, r)-admissible. Then*

$$N_s(\vec{a}, \vec{d}, \vec{t}, q, b) = \frac{p^{t_1+\cdots+t_s-n}}{p^{2r}-1} \sum_{c\in\mathbb{F}_q} (\Delta(-b, d, r, r, c)p^r - 1) \prod_{i=1}^{s} \Delta(a_i, d, t_i, r, c),$$

where $\Delta(-b, d, r, r, c)$ and $\Delta(a_i, d, t_i, r, c)$ are as in Definition 3.2.

Some results in the literature (for example Theorem 1 of [109] and Theorem 2.9 of [13]) can be obtained by a direct employment of Theorem 3.3 and Corollary 3.4, which means that the results of this chapter are far more general than the known results. The case where $d_1 = \cdots = d_s = 2$ and n is even is covered by Corollary 3.4. More about the case where $d_1 = \cdots = d_s = 2$ is discussed in Section 3.4.

Corollary 3.5. *Assume that d_i is (p, r_i)-admissible. Then*

$$\left| \frac{N_s(\vec{a}, \vec{d}, \vec{t}, q, 0)}{p^{t_1+\cdots+t_s-n}} - |\Lambda| p^{t_1+\cdots+t_s} \right| \leq \sum_{c\in\mathbb{F}_q\setminus\Lambda} \prod_{i\in\nu(c)} p^{t_i} \prod_{i\notin\nu(c)} (d_i - 1),$$

where $\Lambda = \cap_{i=1}^{s} \Lambda(a_i, t_i)$ and $\nu(c) = \{i \in \{1, \ldots, s\} : c \in \Lambda(a_i, t_i)\}$. In particular, if $\Lambda(a_i, t_i) \cap \Lambda(a_j, t_j) = \{0\}$ for all $1 \leq i < j \leq s$ and

$$\prod_{i=1}^{s}(d_i - 1)\left(\sum_{i=1}^{s} \left(\frac{1}{p^{t_i}(d_i - 1)} - \frac{1}{p^{2t_i}} \right) + 1 + \frac{s-1}{q} \right) < p^{t_1+\cdots+t_s-n},$$

then there exists one $\mathbb{F}_q$-rational point on the Fermat hypersurface if $b = 0$.

One can obtain bounds for the case $b \neq 0$ and $d_1 = \cdots = d_s$ from Corollary 3.4. In particular, tight bounds can be obtained in case where $s = 2$, as we will see in Section 3.6.

In the case where $t_1 = \cdots = t_s = n$ in Equation(3.1), the number of $\mathbb{F}_q$-rational points on Fermat hypersurfaces can be more deeply studied. In the following results, we present the number of $\mathbb{F}_q$-rational points on Fermat hypersurfaces in this case and also present necessary and sufficient conditions in which Weil's bound is attained in the case $d_1 = \cdots = d_s$. In particular, we employ Theorem 3.3 to obtain Theorem 3.7. Throughout the following results, we assume that $d_1, \ldots, d_2$ are integers, not all equal to 2. The following definition will be important throughout the chapter.

Definition 3.6. *For d a divisor of $q-1$ and $a, b \in \mathbb{F}_q^*$, we set*

$$\theta_d(a,b) = \begin{cases} 1, & \text{if } \chi_d(a) = \chi_d(b); \\ 0, & \text{otherwise.} \end{cases}$$

Let α be a primitive element of $\mathbb{F}_q^*$. Our main results for $t_1 = \cdots = t_s = n$ can be summarized as follows.

Theorem 3.7. *Let $\vec{a} \in \mathbb{F}_q^s$. Assume that d_i is (p, r_i)-admissible. For each $i = 1, \ldots, s$, let $\lambda_i = \alpha^{(p^{n/2}+1)/2}$ if $d_i | (p^{n/2}+1)$ and let $\lambda_i = 1$ otherwise. Then*

$$N_s(\vec{a}, \vec{d}, q, 0) = q^{s-1} + q^{\frac{s-2}{2}} \sum_{j=1}^{q-1} \prod_{i=1}^{s} \varepsilon_i (1-d_i)^{\Delta_{i,j}},$$

where $\varepsilon_i = (-1)^{n/2r_i}$ and $\Delta_{i,j} = \theta_{d_i}(a_i, \lambda_i \alpha^j)$.

The following results are generalizations of Theorem 1 in Wolfmann [109] and Theorem 2.9 in Cao, Chou and Gu [13].

Corollary 3.8. *Let $\vec{a} \in \mathbb{F}_q^s$. If d_i is (p, r)-admissible for all $i = 1, \ldots, s$, then*

$$N_s(\vec{a}, \vec{d}, q, 0) = q^{s-1} + \varepsilon^s q^{\frac{s-2}{2}} (\sqrt{q} + \varepsilon) \sum_{j=1}^{\sqrt{q}-\varepsilon} \prod_{i=1}^{s} (1-d_i)^{\delta_{i,j}},$$

where $\delta_{i,j} = \theta_{d_i}(a_i, \alpha^j)$ and $\varepsilon = (-1)^{n/2r}$.

For the case $b \neq 0$, we have the following result, which is one of the most important of this chapter.

Theorem 3.9. *Let $\vec{a} \in \mathbb{F}_q^s$. If d_i is (p, r)-admissible, then*

$$N_s(\vec{a}, \vec{d}, q, b) = q^{s-1} - \varepsilon^{s+1} q^{\frac{s-2}{2}} \left(\sqrt{q} \prod_{i=1}^{s} (1-d_i)^{\nu_i(b)} - \sum_{j=1}^{\sqrt{q}-\varepsilon} \prod_{i=1}^{s} (1-d_i)^{\delta_{i,j}} \right) \tag{3.5}$$

for $b \neq 0$, where $\delta_{i,j} = \theta_{d_i}(a_i, \alpha^j)$, $\nu_i(b) = \theta_{d_i}(a_i, b)$ and $\varepsilon = (-1)^{n/2r}$.

Theorems 3.7 and 3.9 were already known (see Theorem 2.9 in [13]) in the particular case where $a_1, \ldots, a_s \in \mathbb{F}_{p^r}^*$, which yields a setting where the bound (3.2) is attained. In Theorem 4.1, we present necessary and sufficient conditions for which the bound (3.2) is attained. In the special case where $s = 2$, we have the following result for the $\mathbb{F}_q$-rational number of points on Fermat curves.

Corollary 3.10. *Let $a, b \in \mathbb{F}_q^*$ and $c \in \mathbb{F}_q$. Let m and k be divisors of $q-1$ and let $N(c)$ be the number of $\mathbb{F}_q$-rational points on the affine Fermat curve given by equation $ax^k + by^m = c$. If m and k are (p, r)-admissible, then*

$$N(0) = q - (q-1)(1-l)^{\theta_l(a,b)} + 1 - C(k,m)$$

and

$$N(c) = q - \varepsilon\sqrt{q}(1-k)^{\theta_k(a,c)}(1-m)^{\theta_m(b,c)} - \varepsilon(\sqrt{q}-\varepsilon)(1-l)^{\theta_l(a,b)} + 1 - C(k,m)$$

for $c \neq 0$, *where* $l = \gcd(m,k)$, $\varepsilon = (-1)^{t/r}$ *and* $C(k,m) := (1-k)^{\theta_k(a,b)}$ *if* $k = m$ *and* $C(k,m) := 0$ *otherwise.*

3.2 On the number of solutions of $\mathrm{Tr}_{p^n/p}(ax^d) = \lambda$

In this section we provide tools from quadratic forms over finite fields which will be used throughout the chapter. We use the ideas from Wolfmann [108] in order to generalize his results. The following result is well known (see [50]).

Lemma 3.11. *Let* Φ *be a quadratic form on a* k *dimensional vector space* E *over* $\mathbb{F}_q$, Ψ *the associated symmetric bilinear form and* κ *the dimension of the kernel of* Ψ. *For* $\lambda \in \mathbb{F}_q$, *let* S_λ *be the number of solutions in* E *of* $\Phi(x) = \lambda$. *If* $k = 2t$ *and* $\kappa = 2v$, *then there exists* $D \in \{-1, 0, 1\}$ *such that*

$$S_\lambda = \begin{cases} q^{2t-1} + Dq^{t+v-1}(q-1), & \text{if } \lambda = 0; \\ q^{2t-1} - Dq^{t+v-1}, & \text{if } \lambda \neq 0. \end{cases}$$

The following result can be obtained from Lemma 2 in [108].

Proposition 3.12. *Let* $q = p^n$ *and let* t *and* r *be integers such that* $2t|n$ *and* $r|t$. *For each* $a \in \mathbb{F}_q$, *the map* Φ_a *from* $\mathbb{F}_{p^{2t}}$ *into* $\mathbb{F}_p$ *defined by* $\Phi_a(x) = \mathrm{Tr}_{q/p}(ax^{p^r+1})$ *is a quadratic form. Let* $\hat{a} = \mathrm{Tr}_{q/p^{2t}}(a)$ *and* $m = \frac{p^{2t}-1}{p^r+1}$. *If* v *and* D *are integers as defined in Lemma 3.11, then*

1. *If* $\hat{a} = 0$, *then* $v = t$ *and* $D = 1$;
2. *If* $\hat{a}^m = (-1)^{t/r}$, *then* $v = r$ *and* $D = (-1)^{t/r-1}$;
3. *If* $\hat{a}^m \notin \{0, (-1)^{t/r}\}$, *then* $v = 0$ *and* $D = (-1)^{t/r}$.

Theorem 3.13. *Let* $q = p^n$ *and let* $d|(p^{2t}-1)$ *such that* d *is* (p,r)*-admissible. Let* $a \in \mathbb{F}_q^*$, $\lambda \in \mathbb{F}_p$ *and let* N_λ *denote the number of solutions of* $\mathrm{Tr}_{q/p}\left(ax^d\right) = \lambda$ *over* $\mathbb{F}_{p^{2t}}$. *Set* $\hat{a} = \mathrm{Tr}_{q/p^{2t}}(a)$, $k = \frac{p^{2t}-1}{d}$, $\varepsilon = (-1)^{t/r}$ *and* $u = \frac{p^r+1}{d}$. *Then*

(a) If $\hat{a} = 0$, *then*

$$N_\lambda = \begin{cases} p^{2t}, & \text{if } \lambda = 0; \\ 0, & \text{if } \lambda \neq 0. \end{cases}$$

(b) If $\hat{a}^k \notin \{0, \varepsilon^u\}$, *then*

$$N_\lambda = \begin{cases} p^{2t-1} + \varepsilon p^{t-1}(p-1), & \text{if } \lambda = 0; \\ p^{2t-1} - \varepsilon p^{t-1}, & \text{if } \lambda \neq 0. \end{cases}$$

(c) If $\hat{a}^k = \varepsilon^u$, *then*

$$N_\lambda = \begin{cases} p^{2t-1} - \varepsilon p^{t-1}(d-1)(p-1), & \text{if } \lambda = 0; \\ p^{2t-1} + \varepsilon p^{t-1}(d-1), & \text{if } \lambda \neq 0. \end{cases}$$

Proof. Let α be a primitive element of $\mathbb{F}^*_{p^{2t}}$ and let M_ℓ denote the number of elements $x \in \mathbb{F}_{p^{2t}}$ such that

$$\mathrm{Tr}_{q/p}\left(a\alpha^{\ell d} x^{p^r+1}\right) = \lambda.$$

By using the same arguments used in page 2057 of [108], it follows that

$$N_\lambda = \frac{d}{p^r+1} \sum_{\ell=0}^{\frac{p^r+1}{d}-1} M_\ell. \tag{3.6}$$

For $\ell = 0, \ldots, \frac{p^r+1}{d} - 1$, we set $\hat{a}_\ell = \mathrm{Tr}_{q/p^{2t}}(a\alpha^{\ell d})$ and observe that $\mathrm{Tr}_{q/p^{2t}}(a\alpha^{\ell d}) = \alpha^{\ell d}\,\mathrm{Tr}_{q/p^{2t}}(a) = \alpha^{\ell d}\hat{a}$, so that $\hat{a}_\ell = 0$ if and only if $\mathrm{Tr}_{q/p^{2t}}(a) = 0$. In this case, Proposition 3.12 and Equation (3.6) implies that $N_0 = q^{2t}$ and $N_\lambda = 0$ if $\lambda \neq 0$. Let $m = \frac{p^{2t}-1}{p^r+1}$ and $\varepsilon = (-1)^{t/r}$. We split the remaining part of the proof into two cases:

- If there exists no $j \in \{0, \ldots, \frac{p^r+1}{d} - 1\}$ such that $\hat{a}_j^m = (-1)^{t/r}$, then Proposition 3.12 and Equation (3.6) entail that

$$N_\lambda = \begin{cases} p^{2t-1} + \varepsilon p^{t-1}(p-1), & \text{if } \lambda = 0; \\ p^{2t-1} - \varepsilon p^{t-1}, & \text{if } \lambda \neq 0. \end{cases}$$

- If there exists some $j \in \{0, \ldots, \frac{p^r+1}{d} - 1\}$ such that $\hat{a}_j^m = (-1)^{t/r}$, then it is easy to verify that $\hat{a}_i^m \neq (-1)^{t/r}$ for all $i \in \{0, \ldots, \frac{p^r+1}{d} - 1\} \backslash \{j\}$, so that a straightforward computation using Proposition 3.12 and Equation (3.6) shows that

$$N_\lambda = \begin{cases} p^{2t-1} - \varepsilon p^{t-1}(d-1)(p-1), & \text{if } \lambda = 0; \\ p^{2t-1} + \varepsilon p^{t-1}(d-1), & \text{if } \lambda \neq 0. \end{cases}$$

Our assertion follows from observing that there exists $j \in \{0, \ldots, \frac{p^r+1}{d} - 1\}$ such that $\hat{a}_j^m = (-1)^{t/r}$ if and only if $\hat{a}^{(p^{2t}-1)/d} = \varepsilon^{(p^r+1)/d}$. ■

3.3 Counting results in the general case

In this section, we prove our counting results. To prove Theorem 3.3, we will follow the main ideas of Wolfmann [109]. We let $a \in \mathbb{F}_q$ and $\psi_a(x) = \exp\left((2\pi\mathrm{i})\,\mathrm{Tr}_{q/p}(ax)/p\right)$, an additive character. We have the following known results.

Lemma 3.14. *Let* $\vec{a} = (a_1, \ldots, a_s) \in \mathbb{F}_q^s$ *and* $\vec{d} = (d_1, \ldots, d_s) \in \mathbb{Z}_+^s$ *such that* $d_i | (q-1)$ *for all* $i = 1, \ldots, s$. *Then*

$$N_s(\vec{a}, \vec{d}, \vec{t}, q, b) = q^{-1} \sum_{c \in \mathbb{F}_q} \psi_c(-b) \prod_{i=1}^{s} S_i(c),$$

where $S_i(c) := \sum_{x \in \mathbb{F}_{p^{2t_i}}} \psi_{ca_i}\left(x^{d_i}\right)$.

Proof. It follows from an argument similar to the proof of Proposition 1 of [109]. ■

Lemma 3.15. *Let $q = p^n$, $c \in \mathbb{F}_q$, and $\vec{a}, \vec{d}$ and $S_i(c)$ as defined in Lemma 3.14. Suppose d_i is (p, r_i)-admissible. Let $\varepsilon_i = (-1)^{t_i/r_i}$, $\epsilon_i = \varepsilon_i^{(p^{r_i}+1)/d_i}$ and $\hat{a}_i = \mathrm{Tr}_{q/p^{2t_i}}(ca_i)$. Then, for each $i = 1, \ldots, s$, we have that*

(a) If $\hat{a}_i = 0$, then $S_i(c) = p^{2t_i}$;

(b) If $\hat{a}_i^{(p^{2t_i}-1)/d_i} = \epsilon_i$, then $S_i(c) = -\varepsilon_i(d_i - 1)p^{t_i}$;

(c) If $\hat{a}_i^{(p^{2t_i}-1)/d_i} \notin \{0, \epsilon_i\}$, then $S_i(c) = \varepsilon_i\, p^{t_i}$.

Proof. We observe that

$$S_i(c) = \sum_{\lambda \in \mathbb{F}_p} \exp\left(\frac{2\pi \mathrm{i}\lambda}{p}\right) N_\lambda, \tag{3.7}$$

where N_λ is as in Lemma 3.13. Our result follows directly from Equation (3.7) and Theorem 3.13. ■

From Lemmas 3.14 and 3.15, we are able to prove Theorem 3.3.

3.3.1 Proof of Theorem 3.3

Since $b = 0$, it follows from Lemma 3.14 that

$$N_s(\vec{a}, \vec{d}, \vec{t}, q, 0) = q^{-1} \sum_{c \in \mathbb{F}_q} \prod_{i=1}^{s} S_i(c).$$

Let $\varepsilon_i = (-1)^{t_i/r_i}$, $m_i = \frac{p^{2t_i}-1}{d_i}$ and $u_i = \frac{p^{r_i}+1}{d_i}$. Let $T_i(x) = \mathrm{Tr}_{q/p^{2t_i}}(x)$. By Lemma 3.15, it follows that $S_i(c) = p^{t_i}\Delta(a_i, d_i, t_i, r_i, c)$. This completes the proof of our assertion. ■

Definition 3.16. *For $f \in \mathbb{F}_q[x_1, \ldots, x_s]$ and $\vec{t} = (t_1, \ldots, t_s)$ with $t_i | n$ for all $i = 1, \ldots, s$, let*

$$V_{\vec{t}}(f(x_1, \ldots, x_s) = 0) = \{(x_1, \ldots, x_s) \in \mathbb{F}_{p^{t_1}} \times \cdots \times \mathbb{F}_{p^{t_s}} : f(x_1, \ldots, x_s) = 0\},$$

the set of zeros of f. For $i \in \{1, \ldots, s\}$, let

$$V_{\vec{t}, x_i}(f(x_1, \ldots, x_s) = 0) = \{(x_1, \ldots, x_s) \in \mathbb{F}_{p^{t_1}} \times \cdots \times \mathbb{F}_{p^{t_s}} : f(x_1, \ldots, x_s) = 0 \text{ and } x_i \neq 0\}.$$

3.3.2 Proof of Corollary 3.4

Let $b \in \mathbb{F}_q^*$, $\vec{t_0} = (2t_1, \ldots, 2t_s, 2r)$ and $\vec{t} = (2t_1, \ldots, 2t_s)$. For indeterminates $x_1, \ldots, x_s, y$, let

$$\psi : V_{\vec{t_0}, y}(a_1x_1^d + \cdots + a_sx_s^d = by^d) \to V_{\vec{t}}(a_1x_1^d + \cdots + a_sx_s^d = b)$$

be the function defined by

$$(x_1, \ldots, x_s, y) \mapsto (x_1/y, \ldots, x_s/y).$$

Since $r|t_i$ for all $i = 1, \ldots, s$, it follows that ψ is well-defined. It is direct to verify that ψ is a $(p^{2r}-1)$-to-one function and then

$$|V_{\vec{t_0},y}(a_1x_1^d + \cdots + a_sx_s^d = by^d)| = (p^{2r}-1)|V_{\vec{t}}(a_1x_1^d + \cdots + a_sx_s^d = b)|. \tag{3.8}$$

We observe that $V_{\vec{t_0},y}(a_1x_1^d + \cdots + a_sx_s^d = by^d)$ is equal to

$$V_{\vec{t_0}}(a_1x_1^d + \cdots + a_sx_s^d = by^d) \backslash V_{\vec{t_0}}(a_1x_1^d + \cdots + a_sx_s^d = 0^d b),$$

so that

$$|V_{\vec{t_0},y}(a_1x_1^d + \cdots + a_sx_s^d = by^d)| = |V_{\vec{t_0}}(a_1x_1^d + \cdots + a_sx_s^d = by^d)| - |V_{\vec{t}}(a_1x_1^d + \cdots + a_sx_s^d = 0)|. \tag{3.9}$$

Let $\vec{a_0} = (a_1, \ldots, a_s, b)$ and $\vec{d_0} = (d, \ldots, d) \in \mathbb{Z}^{s+1}$. Since $N_s(\vec{a}, \vec{d}, \vec{t}, q, b) = |V_{\vec{t}}(a_1x_1^d + \cdots + a_sx_s^d = b)|$, $N_s(\vec{a}, \vec{d}, \vec{t}, q, 0) = |V_{\vec{t}}(a_1x_1^d + \cdots + a_sx_s^d = 0)|$ and $N_{s+1}(\vec{a_0}, \vec{d_0}, \vec{t_0}, q, 0) = |V_{\vec{t_0}}(a_1x_1^d + \cdots + a_sx_s^d = by^d)|$, our result follows from Equations (3.8) and (3.9) and Theorem 3.3. ■

3.3.3 Proof of Corollary 3.5

Let $\Lambda = \cap_{i=1}^{s} \Lambda(a_i, t_i)$. By Theorem 3.3, we have that

$$\begin{aligned} N_s(\vec{a}, \vec{d}, \vec{t}, q, 0)p^{n-t_1-\cdots-t_s} &= \sum_{c\in\mathbb{F}_q} \prod_{i=1}^{s} \Delta(a_i, d_i, t_i, r_i, c) \\ &= \sum_{c\in\Lambda} \prod_{i=1}^{s} \Delta(a_i, d_i, t_i, r_i, c) + \sum_{c\in\mathbb{F}_q\backslash\Lambda} \prod_{i=1}^{s} \Delta(a_i, d_i, t_i, r_i, c) \\ &= |\Lambda|p^{t_1+\cdots+t_s} + \sum_{c\in\mathbb{F}_q\backslash\Lambda} \prod_{i=1}^{s} \Delta(a_i, d_i, t_i, r_i, c), \end{aligned}$$

and then

$$\left| N_s(\vec{a}, \vec{d}, \vec{t}, q, 0)p^{n-t_1-\cdots-t_s} - |\Lambda|p^{t_1+\cdots+t_s} \right| \leq \sum_{c\in\mathbb{F}_q\backslash\Lambda} \prod_{i=1}^{s} \Delta(a_i, d_i, t_i, r_i, c). \tag{3.10}$$

By the definition of $\Delta(a_i, d_i, t_i, r_i, c)$, it follows that

$$|\Delta(a_i, d_i, t_i, r_i, c)| \leq \begin{cases} p^{t_i}, & \text{if } c \in \Lambda(a_i, t_i); \\ d_i - 1, & \text{if } c \notin \Lambda(a_i, t_i) \end{cases}$$

and therefore the Triangle Inequality on Equation (3.10) implies that

$$\left| \frac{N_s(\vec{a}, \vec{d}, \vec{t}, q, 0)}{p^{t_1+\cdots+t_s-n}} - |\Lambda|p^{t_1+\cdots+t_s} \right| \leq \sum_{c\in\mathbb{F}_q\backslash\Lambda} \prod_{i\in\nu(c)} p^{t_i} \prod_{i\notin\nu(c)} (d_i - 1), \tag{3.11}$$

where $\nu(c) = \{i \in \{1, \ldots, s\} : c \in \Lambda(a_i, t_i)\}$. This completes the first part of our result. Assume that $\Lambda(a_i, t_i) \cap \Lambda(a_j, t_j) = \{0\}$ for all $1 \leq i < j \leq s$. In this case, we have that

$$\sum_{c \in \mathbb{F}_q \setminus \Lambda} \prod_{i \in \nu(c)} p^{t_i} \prod_{i \notin \nu(c)} (d_i - 1) \leq \sum_{j=1}^{s} \left(|\Lambda(a_j, t_j)| \cdot p^{t_j} \prod_{i \neq j} (d_i - 1) \right) + \left(q - 1 - \sum_{j=1}^{s} (|\Lambda(a_j, t_j)| - 1) \right) \prod_{i=1}^{s} (d_i - 1).$$

Since $|\Lambda(a_j, t_j)| = q/p^{2t_i}$, it follows that

$$\sum_{c \in \mathbb{F}_q \setminus \Lambda} \prod_{i \in \nu(c)} p^{t_i} \prod_{i \notin \nu(c)} (d_i - 1) \leq q \prod_{i=1}^{s} (d_i - 1) \left(\sum_{i=1}^{s} \left(\frac{1}{p^{t_i}(d_i - 1)} - \frac{1}{p^{2t_i}} \right) + 1 + \frac{s-1}{q} \right) \quad (3.12)$$

Therefore, Equations (3.11) and (3.12) imply that

$$\frac{N_s(\vec{a}, \vec{d}, \vec{t}, q, 0)}{p^{t_1 + \cdots + t_s - n}} \geq p^{t_1 + \cdots + t_s} - q \prod_{i=1}^{s} (d_i - 1) \left(\sum_{i=1}^{s} \left(\frac{1}{p^{t_i}(d_i - 1)} - \frac{1}{p^{2t_i}} \right) + 1 + \frac{s-1}{q} \right),$$

which is bigger than zero whenever

$$\prod_{i=1}^{s} (d_i - 1) \left(\sum_{i=1}^{s} \left(\frac{1}{p^{t_i}(d_i - 1)} - \frac{1}{p^{2t_i}} \right) + 1 + \frac{s-1}{q} \right) < p^{t_1 + \cdots + t_s - n}.$$

This completes the proof of the Corollary. ■

3.4 The case $d_1 = \cdots = d_s = 2$

In the case where $d_1 = \cdots = d_s = 2$, we can compute the number of $\mathbb{F}_q$-rational points on Fermat hypersfaces over arbitrary finite fields, as we will see in this section. The following result will be useful to compute the number of solutions of Equation (3.1) in this case.

Lemma 3.17. *For $t|n$, $a \in \mathbb{F}_q^*$ and $\lambda \in \mathbb{F}_p$, let N_λ denote the number of solutions of $\mathrm{Tr}_{q/p}\left(ax^2\right) = \lambda$ over $\mathbb{F}_{p^t}$ and let $\hat{a} = \mathrm{Tr}_{q/p^t}(a)$. Assume that $\hat{a} \neq 0$. Then*

$$N_\lambda = \begin{cases} p^{t-1} + \chi_2(\hat{a}) p^{t/2-1}, & \text{if } t \text{ is even and } p \equiv 1 \pmod 4; \\ p^{t-1} + \mathrm{i}^t \chi_2(\hat{a}) p^{t/2-1}, & \text{if } t \text{ is even and } p \equiv 3 \pmod 4; \\ p^{t-1} + \chi_2(-\lambda\hat{a}) p^{(t-1)/2}, & \text{if } t \text{ is odd and } p \equiv 1 \pmod 4, \\ p^{t-1} + \mathrm{i}^{t+1} \chi_2(-\lambda\hat{a}) p^{(t-1)/2}, & \text{if } t \text{ is odd and } p \equiv 3 \pmod 4, \end{cases}$$

if $\lambda \neq 0$ and

$$N_0 = \begin{cases} p^{t-1} - (p-1)\chi_2(\hat{a}) p^{t/2-1}, & \text{if } t \text{ is even and } p \equiv 1 \pmod 4; \\ p^{t-1} - (p-1)\mathrm{i}^t \chi_2(\hat{a}) p^{t/2-1}, & \text{if } t \text{ is even and } p \equiv 3 \pmod 4, \\ p^{t-1}, & \text{if } t \text{ is odd,} \end{cases}$$

where χ_2 denotes the quadratic multiplicative character of $\mathbb{F}_{p^t}$.

Proof. Let $\psi(x) = \exp\left((2\pi i)\operatorname{Tr}_{p^t/p}(x)/p\right)$, the canonical additive character, let $\delta \in \mathbb{F}_{p^t}$ be an element such that $\operatorname{Tr}_{p^t/p}(\delta) = \lambda$ and let $\hat{a} = \operatorname{Tr}_{q/p^t}(a)$. We observe that if $c \in \mathbb{F}_{p^t}$, then $\operatorname{Tr}_{q/p}\left(ac^2\right) = \operatorname{Tr}_{p^t/p}\left(\operatorname{Tr}_{q/p^t}(a)c^2\right) = \operatorname{Tr}_{p^t/p}\left(\hat{a}c^2\right)$ so that $\operatorname{Tr}_{q/p}\left(ac^2\right) = \lambda$ if and only if $\psi(\hat{a}c^2 - \delta) = 1$. Therefore,

$$\begin{aligned} pN_\lambda &= \sum_{c\in\mathbb{F}_{p^t}} \left[1 + \cdots + \psi(\hat{a}c^2 - \delta)^{p-1}\right] \\ &= \sum_{c\in\mathbb{F}_{p^t}} \left[1 + \cdots + \psi(\hat{a}c - \delta)^{p-1}\right] [1 + \chi_2(c)] \\ &= p^t + \sum_{\ell=1}^{p-1} \psi(-\delta)^\ell \chi_2(\ell^{-1}\hat{a}^{-1}) \sum_{z\in\mathbb{F}_{p^t}} \psi(z)\chi_2(z) \\ &= p^t + \sum_{\ell=1}^{p-1} \psi(-\delta)^\ell \chi_2(\ell^{-1}\hat{a}^{-1}) G(\chi_2), \end{aligned}$$

where $G(\chi_2)$ is the Gauss sum of χ_2 over $\mathbb{F}_{p^t}$. Now, we split the proof into two cases:

- If $\lambda = 0$, then

$$\sum_{\ell=1}^{p-1} \psi(-\delta)^\ell \chi_2(\ell^{-1}\hat{a}^{-1}) = \sum_{\ell=1}^{p-1} \chi_2(\ell^{-1}\hat{a}^{-1}) = \begin{cases} (p-1)\chi_2(\hat{a}), & \text{if } t \text{ is even;} \\ 0, & \text{if } t \text{ is odd.} \end{cases}$$

- If $\lambda \neq 0$, then

$$\begin{aligned} \sum_{\ell=1}^{p-1} \psi(-\delta)^\ell \chi_2(\ell^{-1}\hat{a}^{-1}) &= \chi_2\left(\tfrac{1}{\hat{a}}\right) \sum_{\ell\in\mathbb{F}_p^*} \psi(-\delta)^\ell \overline{\chi}_2(\ell) = \chi_2(\tfrac{1}{\hat{a}}) \sum_{\ell\in\mathbb{F}_p^*} \psi(-\delta\ell)\overline{\chi}_2(\ell) \\ &= \chi_2\left(\tfrac{-\lambda}{\hat{a}}\right) \sum_{x\in\mathbb{F}_p^*} \psi(x)\overline{\chi}_2(x) = \chi_2\left(\tfrac{-\lambda}{\hat{a}}\right) \sum_{x\in\mathbb{F}_p^*} \psi(x)\chi_2(x) \\ &= \begin{cases} -\chi_2\left(\hat{a}\right), & \text{if } t \text{ is even;} \\ \chi_2\left(-\lambda\hat{a}\right) G_p(\chi_2), & \text{if } t \text{ is odd,} \end{cases} \end{aligned}$$

  where $G_p(\chi_2)$ is the Gauss sum of χ_2 over $\mathbb{F}_p$. Our result follows directly by using Theorem 1.7 in the values of $G(\chi_2)$ and $G_p(\chi_2)$.

■

Proposition 3.18. *For $c, a_1, \ldots, a_s \in \mathbb{F}_q$, let $\hat{a}_j = \operatorname{Tr}_{q/p^{t_j}}(ca_j)$ and $S_j(c) := \sum_{x\in\mathbb{F}_{p^{t_j}}} \psi_{ca_j}\left(x^2\right)$. If $\hat{a}_j = 0$, then $S_j(c) = p^{t_j}$. If $\hat{a}_j \neq 0$, then*

$$S_j(c) = \begin{cases} -\chi_2^{(j)}(\hat{a}_j)p^{t_j/2}, & \text{if } t_j \text{ is even and } p \equiv 1 \pmod 4; \\ -\mathrm{i}^{t_j}\chi_2^{(j)}(\hat{a}_j)p^{t_j/2}, & \text{if } t_j \text{ is even and } p \equiv 3 \pmod 4; \\ \chi_2^{(j)}(\hat{a}_j)p^{t_j/2}, & \text{if } t_j \text{ is odd and } p \equiv 1 \pmod 4; \\ \mathrm{i}^{t_j}\chi_2^{(j)}(\hat{a}_j)p^{t_j/2}, & \text{if } t_j \text{ is odd and } p \equiv 3 \pmod 4, \end{cases}$$

where $\chi_2^{(j)}$ denotes the quadratic character in $\mathbb{F}_{p^{t_j}}$.

Proof. For a fixed $j \in \{1, \ldots, s\}$, we observe that

$$S_j(c) = \sum_{\lambda \in \mathbb{F}_p} \exp\left(\frac{2\pi \mathrm{i}\lambda}{p}\right) N_\lambda, \tag{3.13}$$

where N_λ is denote the number of solutions of $\mathrm{Tr}_{q/p}\left(ax^2\right) = \lambda$ over $\mathbb{F}_{p^{t_j}}$. Assume that t_j is odd. If $p \equiv 1 \pmod 4$, then Equation (3.13) and Lemma 3.17 imply that

$$\sum_{\lambda \in \mathbb{F}_p} e^{\frac{2\pi \mathrm{i}\lambda}{p}} N_\lambda = \chi_2^{(j)}(\hat{a}_j) p^{\frac{t_j-1}{2}} \sum_{\lambda \in \mathbb{F}_p^*} e^{\frac{2\pi \mathrm{i}\lambda}{p}} \chi_2^{(j)}(\lambda) = \chi_2^{(j)}(\hat{a}_j) p^{\frac{t_j-1}{2}} G_p(\chi_2).$$

If $p \equiv 3 \pmod 4$, then Equation (3.13) and Lemma 3.17 imply that

$$\sum_{\lambda \in \mathbb{F}_p} e^{\frac{2\pi \mathrm{i}\lambda}{p}} N_\lambda = -\mathrm{i}^{t_j+1} \chi_2^{(j)}(\hat{a}_j) p^{\frac{t_j-1}{2}} \sum_{\lambda \in \mathbb{F}_p^*} e^{\frac{2\pi \mathrm{i}\lambda}{p}} \chi_2^{(j)}(\lambda) = -\mathrm{i}^{t_j+1} \chi_2^{(j)}(\hat{a}_j) p^{\frac{t_j-1}{2}} G_p(\chi_2).$$

By Theorem 1.7, we have that

$$G_p(\chi_2) = \begin{cases} p^{1/2}, & \text{if } p \equiv 1 \pmod 4; \\ \mathrm{i}p^{1/2}, & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

from where our result follows. The case where t_j is even follows directly from Lemma 3.17. ■

The following result is a straightforward application of Lemma 3.14 and Proposition 3.18

Theorem 3.19. *Let $a_1, \ldots, a_s, b \in \mathbb{F}_q$, where $q = p^n$. The number of $\mathbb{F}_q$-rational points on the Fermat hypersurface defined by the equation*

$$a_1 x_1^2 + \cdots + a_s x_s^2 = b$$

with $x_j \in \mathbb{F}_{p^{t_j}}$ is given by

$$p^{\frac{t_1+\cdots+t_s}{2}-n} \sum_{c \in \mathbb{F}_q} \psi_c(-b) \prod_{j=1}^{s} \Gamma_j(c),$$

where $\chi_2^{(j)}$ denotes the quadratic character in $\mathbb{F}_{p^{t_j}}$ and

$$\Gamma_j(c) = \begin{cases} p^{t_j}, & \text{if } \mathrm{Tr}_{q/p^{t_j}}(ca_j) = 0; \\ (-1)^{t_j+1} \chi_2^{(j)}\big(\mathrm{Tr}_{q/p^{t_j}}(ca_j)\big), & \text{if } \mathrm{Tr}_{q/p^{t_j}}(ca_j) \neq 0 \text{ and } p \equiv 1 \pmod 4; \\ (-1)^{t_j+1} \mathrm{i}^{t_j} \chi_2^{(j)}\big(\mathrm{Tr}_{q/p^{t_j}}(ca_j)\big), & \text{if } \mathrm{Tr}_{q/p^{t_j}}(ca_j) \neq 0 \text{ and } p \equiv 3 \pmod 4. \end{cases}$$

Theorem 3.19 generalizes Theorems 6.26 and 6.27 of [50].

3.5 On the number of $\mathbb{F}_q$-rational points in the case where $\vec{t} = (n, \ldots, n)$

In this section, we study deeper the case where $\vec{t} = (n, \ldots, n)$ with n even. At first, we employ Theorem 3.3 to give a more explicit formula for $N_s(\vec{a}, \vec{d}, q, 0)$.

3.5.1 Proof of Theorem 3.7

By Theorem 3.3,

$$N_s(\vec{a},\vec{d},q,0) = q^{s-1} + q^{-1}\sum_{c\in\mathbb{F}_q^*}\prod_{i=1}^{s}\Delta(a_i,d_i,r_i,c),$$

where

$$\Delta(a_i,d_i,r_i,c) = \begin{cases} \varepsilon_i(1-d_i), & \text{if } \chi_{d_i}(ca_i) = \varepsilon_i^{u_i}; \\ \varepsilon_i, & \text{if } \chi_{d_i}(ca_i) \neq \varepsilon_i^{u_i}; \end{cases}$$

for $u_i = \frac{p^{r_i}+1}{d_i}$ and $\varepsilon_i = (-1)^{n/2r_i}$. Since d_i is (p,r_i)-admissible, it follows that $\epsilon_i = -1$ if and only if $d_i|(p^{n/2}+1)$ and $(p^{r_i}+1)/d_i$ is odd. Furthermore, if $d_i|(p^{n/2}+1)$, then $\left(\alpha^{(p^{n/2}+1)/2}\right)^{(q-1)/d_i} = \epsilon_i$. Altogether, we have shown that

$$\Delta(a_i,d_i,r_i,c^{-1}) = \varepsilon_i(1-d_i)^{\theta_{d_i}(a_i,\lambda_i c)}\sqrt{q},$$

where $\lambda_i = \alpha^{(p^{n/2}+1)/2}$ if $d_i|(p^{n/2}+1)$ and $\lambda_i = 1$ otherwise. Therefore,

$$N_s(\vec{a},\vec{d},q,0) = q^{s-1} + q^{\frac{s-2}{2}}\sum_{j=1}^{q-1}\prod_{i=1}^{s}\varepsilon_i(1-d_i)^{\Delta_{i,j}},$$

where $\varepsilon_i = (-1)^{n/2r_i}$ and $\Delta_{i,j} = \theta_{d_i}(a_i,\lambda_i\alpha^j)$. ■

Remark 3.20. *Assume that $d > 2$. From Theorem 3.7, it can be verified that*

$$\left|N_s(\vec{a},\vec{d},q,0) - q^{s-1}\right| \leq q^{\frac{s-2}{2}}\left|\sum_{m=1}^{q-1}\prod_{d_i|m}(1-d_i)\right|,$$

for $\vec{a}$ and $\vec{d}$ satisfying the hypothesis of Theorem 3.7.

Example 3.21. *Let $q = p^n$ for an even positive integer n and let $d = (d_1,\ldots,d_s) \in \mathbb{F}_q^s$ be a s-tuple satisfying the hypothesis of Theorem 3.7 and such that $d_1,\ldots,d_k$ are divisors of $\sqrt{q}-1$ and $d_{k+1},\ldots,d_s$ are divisors of $\sqrt{q}+1$. Let $\lambda = \alpha^{(\sqrt{q}+1)/2}$. By Theorem 3.7, the number of $\mathbb{F}_q$-rational points on the Fermat hypersface*

$$x^{d_1} + \cdots + x^{d_k} + \lambda x^{d_{k+1}} + \cdots + \lambda x^{d_s} = 0$$

attains the bound in Remark 3.20.

3.5.2 Proof of Corollary 3.8

By Theorem 3.7, it follows that

$$N_s(\vec{a},\vec{d},q,0) = q^{s-1} + q^{\frac{s-2}{2}}\varepsilon^s\sum_{j=1}^{q-1}\prod_{i=1}^{s}(1-d_i)^{\Delta_{i,j}},$$

where $\varepsilon = (-1)^{n/2r}$, $\Delta_{i,j} = \theta_{d_i}(a_i, \lambda_i\alpha^j)$ and $\lambda_i = \alpha^{(p^{n/2}+1)/2}$ if $d_i|(p^{n/2}+1)$ and $\lambda_i = 1$ otherwise. We observe that $(p^r+1)|(p^{n/2}+1)$ if and only if $n/2r$ is odd. If $n/2r$ is odd, then $\lambda_i = 1$ for all $i = 1, \ldots, s$. If $n/2r$ is even, then $\lambda_i = \alpha^{(p^{n/2}+1)/2}$ for all $i = 1, \ldots, s$ and so $\Delta_{i,j} = \theta_{d_i}(a_i, \alpha^{(p^{n/2}+1)/2+j}) = \Delta_{i,(p^{n/2}+1)/2+j}$. In both cases, we have that

$$N_s(\vec{a}, \vec{d}, q, 0) = q^{s-1} + q^{\frac{s-2}{2}}\varepsilon^s \sum_{j=1}^{q-1}\prod_{i=1}^{s}(1-d_i)^{\Delta_{i,j}} = q^{s-1} + q^{\frac{s-2}{2}}\varepsilon^s \sum_{j=1}^{q-1}\prod_{i=1}^{s}(1-d_i)^{\delta_{i,j}}, \quad (3.14)$$

where $\delta_{i,j} := \theta_{d_i}(a_i, \alpha^j)$. We observe that $d_i|(p^r+1)$ implies that $d_i|(\sqrt{q}-\varepsilon)$. Therefore $\delta_{i,j} = \delta_{i,k}$ if $j \equiv k \pmod{\sqrt{q}-\varepsilon}$ and then the assertion of our result follows from Equation (3.14). ■

3.5.3 Preliminary Results

The first step in order to prove Theorem 3.9 is the following result.

Proposition 3.22. *If d_1 and d_2 are (p,r)-admissible, then*

$$N_2(\vec{a}, \vec{d}, q, 0) = q - (q-1)(1-l)^{\theta_l(a_1,a_2)}$$

and

$$N_2(\vec{a}, \vec{d}, q, c) = q - \varepsilon\sqrt{q}(1-d_1)^{\theta_{d_1}(a_1,c)}(1-d_2)^{\theta_{d_2}(a_2,c)} - \varepsilon(\sqrt{q}-\varepsilon)(1-l)^{\theta_l(a_1,a_2)}$$

for $c \neq 0$, where $l := \gcd(d_1, d_2)$ and $\varepsilon = (-1)^{n/2r}$.

Proof. For $c \in \mathbb{F}_q$, let

$$\mathcal{C}_c = \{(x,y) \in \mathbb{F}_q^2 : a_1x_1^{d_1} + a_2x_2^{d_2} = c\}$$

be the set of solutions of $a_1x_1^{d_1} + a_2x_2^{d_2} = c$. Assume $c = 0$. A pair $(x_1, x_2) = (\alpha^i, \alpha^j)$ is a solution of $a_1x_1^{d_1} + a_2x_2^{d_2} = 0$ if and only if $\alpha^{id_1-jd_2} = -\frac{a_2}{a_1}$ and it is easy to verify that this occurs if and only if $\theta_l(a_1,a_2) = 1$. If $\theta_l(a_1,a_2) = 0$, then $(x_1,x_2) = (0,0)$ is the unique solution of $a_1x^{d_1} + a_2y^{d_2} = 0$. Otherwise, there exists an integer k such that $-\frac{a_2}{a_1} = \alpha^{lk}$ and then

$$\mathcal{C}_0 = \bigcup_{\lambda=0}^{l-1}\left\{(\alpha^i, \alpha^j) : \alpha^{i\frac{d_1}{l}+j\frac{d_2}{l}} = \alpha^{\lambda\frac{q-1}{l}}\alpha^k\right\}\bigcup\{(0,0)\},$$

where the sets in the union are disjoint. Let $A_\lambda = \{(\alpha^i, \alpha^j) : \alpha^{i\frac{d_1}{l}+j\frac{d_2}{l}} = \alpha^{\lambda\frac{q-1}{l}}\alpha^k\}$. We note that

$$|A_\lambda| = |\{(i,j) \in \mathbb{Z}_{(q-1)} : i\tfrac{d_1}{l} + j\tfrac{d_2}{l} \equiv \lambda\tfrac{q-1}{l} + k \pmod{q-1}\}|.$$

Let (i_0, j_0) be integers such that $i_0\frac{d_1}{l} + j_0\frac{d_2}{l} = 1$. For $u \in \mathbb{Z}_{(q-1)}$, let

$$B_u := \{(i,j) \in \mathbb{Z}_{(q-1)} : i\tfrac{d_1}{l} + j\tfrac{d_2}{l} \equiv u \pmod{q-1}\}. \quad (3.15)$$

For $u, v \in \mathbb{Z}_{(q-1)}$, it is easy to verify that the function $\varphi : B_u \to B_v$ defined by $\varphi : (i,j) \mapsto (i + i_0(v-u), j + j_0(v-u))$ is a bijective function from B_u to B_v and so $|B_u| = |B_v|$. Since u and v are arbitrarily taken and $\sum_u |B_u| = (q-1)^2$, it follows that $|B_u| = q-1$ for all $u \in \mathbb{Z}_{(q-1)}$. In particular, $|A_\lambda| = |B_{\lambda(q-1)/l+k}| = q-1$ and so $|C_0| = l(q-1)+1$, proving the first part of our result for the case $\theta_l(a_1, a_2) = 1$.

Assume $c \neq 0$ and let B_0 the set as defined in Equation 3.15. We have that

$$\begin{aligned}
|\mathcal{C}_c| &= \sum_{b_1+b_2=1} \left[1 + \cdots + \chi_{d_1}^{d_1-1}\left(\tfrac{cb_1}{a_1}\right)\right]\left[1 + \cdots + \chi_{d_2}^{d_2-1}\left(\tfrac{cb_2}{a_2}\right)\right] \\
&= q + \sum_{b_1+b_2=1} \sum_{1 \le \ell_i \le d_i - 1} \chi_{d_1}^{\ell_1}\left(\tfrac{cb_1}{a_1}\right)\chi_{d_2}^{\ell_2}\left(\tfrac{cb_2}{a_2}\right) \\
&= q + \sum_{\substack{1 \le \ell_i \le d_i - 1 \\ (\ell_1,\ell_2) \notin B_0}} \sum_{b_1+b_2=1} \chi_{d_1}^{\ell_1}\left(\tfrac{cb_1}{a_1}\right)\chi_{d_2}^{\ell_2}\left(\tfrac{cb_2}{a_2}\right) + \sum_{\substack{1 \le \ell_i \le d_i - 1 \\ (\ell_1,\ell_2) \in B_0}} \sum_{b_1+b_2=1} \chi_{d_1}^{\ell_1}\left(\tfrac{cb_1}{a_1}\right)\chi_{d_2}^{\ell_2}\left(\tfrac{cb_2}{a_2}\right) \\
&= q - \varepsilon\sqrt{q} \sum_{\substack{1 \le \ell_i \le d_i - 1 \\ (\ell_1,\ell_2) \notin B_0}} \chi_{d_1}^{\ell_2}\left(\tfrac{c}{a_1}\right)\chi_{d_2}^{\ell_2}\left(\tfrac{c}{a_2}\right) - \sum_{\substack{1 \le \ell_i \le d_i - 1 \\ (\ell_1,\ell_2) \in B_0}} \chi_{d_1}^{\ell_1}\left(\tfrac{c}{a_1}\right)\chi_{d_2}^{\ell_2}\left(\tfrac{c}{a_2}\right).
\end{aligned}$$

The last equality follows from Lemma 1.17 and entails that

$$\begin{aligned}
|\mathcal{C}_c| &= q - \varepsilon\sqrt{q} \sum_{1 \le \ell_i \le d_i - 1} \chi_{d_1}^{\ell_2}\left(\tfrac{c}{a_1}\right)\chi_{d_2}^{\ell_2}\left(\tfrac{c}{a_2}\right) + (\varepsilon\sqrt{q} - 1) \sum_{\substack{1 \le \ell_i \le d_i - 1 \\ (\ell_1,\ell_2) \in B_0}} \chi_{d_1}^{\ell_1}\left(\tfrac{c}{a_1}\right)\chi_{d_2}^{\ell_2}\left(\tfrac{c}{a_2}\right) \\
&= q - \varepsilon\sqrt{q}(1-d_1)^{\theta_{d_1}(a_1,c)}(1-d_2)^{\theta_{d_2}(a_2,c)} + (\varepsilon\sqrt{q} - 1) \sum_{(\ell_1,\ell_2) \in \Lambda} \chi_{d_1}^{\ell_1}\left(\tfrac{c}{a_1}\right)\chi_{d_2}^{\ell_2}\left(\tfrac{c}{a_2}\right),
\end{aligned} \tag{3.16}$$

where $\Lambda := B_0 \cap \{(\ell_1, \ell_2) : 1 \le \ell_i \le d_i - 1 \text{ for } i = 1, 2\}$. A direct computation shows that

$$\Lambda = \{(\tfrac{md_1}{l}, \tfrac{-md_2}{l}) : 1 \le m \le l-1\}$$

and therefore

$$\sum_{(\ell_1,\ell_2) \in \Lambda} \chi_{d_1}^{\ell_1}\left(\tfrac{c}{a_1}\right)\chi_{d_2}^{\ell_2}\left(\tfrac{c}{a_2}\right) = \sum_{m=1}^{d-1} \chi_l^m\left(\tfrac{a_2}{a_1}\right) = \begin{cases} l-1, & \text{if } \theta_l(a_1,a_2) = 1; \\ -1, & \text{if } \theta_l(a_1,a_2) = 0. \end{cases} \tag{3.17}$$

Our result follows from Equations (3.16) and (3.17). ■

For $f \in \mathbb{F}_q[x_1, \ldots, x_s]$, we set $N(f(x_1, \ldots, x_s) = 0) = |V_{\vec{t}}(f(x_1, \ldots, x_s) = 0)|$ and $N^*_{x_i}(f(x_1, \ldots, x_s) = 0) = |V_{\vec{t}, x_i}(f(x_1, \ldots, x_s) = 0)|$ where $t = (n, \ldots, n)$ and V and V_{x_i} are as in Definition 3.16. The following definitions will be useful in the proof of our results.

The following result is straightforward.

Lemma 3.23. *Let $a, b \in \mathbb{F}_q$ and let α be a primitive element of $\mathbb{F}_q$. Let d_1 and d_2 be divisors of $q-1$. Then*

$$d_2^{-1} \cdot N_y^*\left(ax^{d_1} + \alpha^j y^{d_2} = b\right) = \sum_{i=1}^{(q-1)/d_2} N\left(ax^{d_1} = b - \alpha^{j+id_2}\right)$$

The following lemma will be important in the proof of Theorem 3.9.

Lemma 3.24. *Let $\varepsilon \in \{\pm 1\}$ and $d, d_1, \ldots, d_s$ be integers such that $d|(\sqrt{q}-\varepsilon)$ and $d_i|(\sqrt{q}-\varepsilon)$ for all $i = 1, \ldots, s$.*

(a) For $b \in \mathbb{F}_q^*$, we have the following relation:

$$\sum_{j=1}^{\sqrt{q}-\varepsilon} (1-d)^{\theta_d(\alpha^j, b)} = 0.$$

(b) Let $M_s(\vec{a}, \vec{d}, q, \alpha^j)$ denote the right-hand expression in Equation (3.5) of Theorem 3.9. Then

$$\sum_{j=1}^{\sqrt{q}-\varepsilon} M_s(\vec{a}, \vec{d}, q, \alpha^j) = q^{s-1}(\sqrt{q}-\varepsilon) - \varepsilon^s q^{\frac{s-2}{2}} \sum_{j=1}^{\sqrt{q}-\varepsilon} \prod_{i=1}^{s} (1-d_i)^{\delta_{i,j}}.$$

Proof. We observe that

$$-(1-d)^{\theta_d(\alpha^j, b)} = \chi_d\left(\frac{\alpha^j}{b}\right) + \cdots + \chi_d^{d-1}\left(\frac{\alpha^j}{b}\right).$$

Therefore, for $b \in \mathbb{F}_q^*$, it follows that

$$-\sum_{j=1}^{\sqrt{q}-\varepsilon} (1-d)^{\theta_d(\alpha^j, b)} = \sum_{j=1}^{\sqrt{q}-\varepsilon} \left[\chi_d\left(\frac{\alpha^j}{b}\right) + \cdots + \chi_d^{d-1}\left(\frac{\alpha^j}{b}\right)\right] = 0,$$

which proves item (a). Let $S = \sum_{j=1}^{\sqrt{q}-\varepsilon} \prod_{i=1}^{s} (1-d_i)^{\delta_{i,j}}$. For an integer $s \geq 2$, it follows that

$$\begin{aligned}
\sum_{j=1}^{\sqrt{q}-\varepsilon} M_s(\vec{a}, \vec{d}, q, \alpha^j) &= (\sqrt{q}-\varepsilon)\big(q^{s-1} + \varepsilon^{s+1} q^{\frac{s-2}{2}} S\big) - \varepsilon^{s+1} q^{\frac{s-1}{2}} \sum_{j=1}^{\sqrt{q}-\varepsilon} \prod_{i=1}^{s} (1-d_i)^{\nu_i(\alpha^j)} \\
&= (\sqrt{q}-\varepsilon)\big(q^{s-1} + \varepsilon^{s+1} q^{\frac{s-2}{2}} S\big) - \varepsilon^{s+1} q^{\frac{s-1}{2}} \sum_{j=1}^{\sqrt{q}-\varepsilon} \prod_{i=1}^{s} (1-d_i)^{\delta_{i,j}} \\
&= q^{s-1}(\sqrt{q}-\varepsilon) - \varepsilon^s q^{\frac{s-2}{2}} S,
\end{aligned}$$

proving item (b). ∎

From the previous results we are able to prove the main result of the section.

3.5.4 Proof of Theorem 3.9

We proceed by induction on s. We make an abuse of language using $\vec{a}$ and $\vec{d}$ for all $k \leq s$; meaning that, for each k, we use only the first k entries of $\vec{a}$ and $\vec{d}$. The base case of the induction is $s = 2$, which we prove as follows.

3.5.4.1 The case $s = 2$

By Proposition 3.22, we only need to show that

$$(1-l)^{\theta_l(a_1,a_2)} = -(\sqrt{q}-\varepsilon)^{-1}\sum_{j=1}^{\sqrt{q}-\varepsilon}(1-d_1)^{\theta_{d_1}(a_1,\alpha^j)}(1-d_2)^{\theta_{d_2}(a_2,\alpha^j)}, \tag{3.18}$$

where $l = \gcd(d_1, d_2)$. By the Inclusion and Exclusion Principle, the sum in Equation (3.18) is equal to

$$\begin{aligned}&(1-d_1)(1-d_2)u + \sum_{i=1}^{2}(1-d_i)(\tfrac{\sqrt{q}-\varepsilon}{d_i} - u) + \Big(\sqrt{q}-\varepsilon - (\tfrac{\sqrt{q}-\varepsilon}{d_1} - u) - (\tfrac{\sqrt{q}-\varepsilon}{d_2} - u) - u\Big)\\ &= d_1d_2u - (\sqrt{q}-\varepsilon),\end{aligned}$$

where $u := |\{1 \le j \le \sqrt{q}-\varepsilon : \theta_{d_1}(a_1,\alpha^j) = \theta_{d_2}(a_2,\alpha^j) = 1\}|$. We split the proof for Equation (3.18) into two cases:

- The case $\theta_l(a_1, a_2) = 0$. Since $\chi_l(a_1) \neq \chi_l(a_2)$, it follows that there exists no j such that $\chi_{d_1}(a_1) = \chi_{d_1}(\alpha^j)$ and $\chi_{d_2}(a_2) = \chi_{d_2}(\alpha^j)$ and then $u = 0$. In this case, $d_1d_2u - (\sqrt{q}-\varepsilon) = -(\sqrt{q}-\varepsilon)$.

- The case $\theta_l(a_1, a_2) = 1$. Let j_1 and j_2 be integers such that $a_1 = \alpha^{j_1}$ and $a_2 = \alpha^{j_2}$. Since $\chi_l(a_1) = \chi_l(a_2)$, it follows that $j_1 \equiv j_2 \pmod{l}$ and this relation entails that

  $$\{1 \le j \le \sqrt{q}-\varepsilon : \theta_{d_i}(a_i,\alpha^j) = 1 \text{ for } i = 1,2\} = \Big\{k\,\mathrm{lcm}(d_1,d_2) : 1 \le k \le \tfrac{\sqrt{q}-\varepsilon}{\mathrm{lcm}(d_1,d_2)}\Big\}$$

  and then $u = \frac{\sqrt{q}-\varepsilon}{\mathrm{lcm}(d_1,d_2)}$. In this case, $d_1d_2u - (\sqrt{q}-\varepsilon) = (\sqrt{q}-\varepsilon)(l-1)$.

Altogether, we have shown that $d_1d_2u - (\sqrt{q}-\varepsilon) = -(\sqrt{q}-\varepsilon)(1-l)^{\theta_l(a_1,a_2)}$ and then

$$(\sqrt{q}-\varepsilon)^{-1}\sum_{j=1}^{\sqrt{q}-\varepsilon}(1-d_1)^{\theta_{d_1}(a_1,\alpha^j)}(1-d_2)^{\theta_{d_2}(a_2,\alpha^j)} = -(1-l)^{\theta_l(a_1,a_2)},$$

therefore our result follows for the case $s = 2$.

3.5.4.2 Induction Hypothesis

Suppose that the result holds for $N_s(\vec{a}, \vec{d}, q, b)$ with $s \le k$ and $b \in \mathbb{F}_q^*$. We observe that

$$\begin{aligned}N_{k+1}(\vec{a},\vec{d},q,b) &= \sum_{c\in\mathbb{F}_q} N(a_1x_1^{d_1} + \cdots + a_kx_k^{d_k} = c)N(b - a_{k+1}x_{k+1}^{d_{k+1}} = c)\\ &= \sum_{c\in\mathbb{F}_q} N_k(\vec{a},\vec{d},q,c)N(b - a_{k+1}x_{k+1}^{d_{k+1}} = c).\end{aligned}$$

Along the proof, we denote $N_k(\vec{a},\vec{d},q,c)$ by M_c. Let $\tilde{\theta}=\theta_{d_{k+1}}(a_{k+1},b)$ and $C_0=(1-(1-d_{k+1})^{\tilde{\theta}})M_0$. Since $M_{\alpha^i}=M_{\alpha^j}$ if $i\equiv j \pmod{\sqrt{q}-\varepsilon}$, it follows that

$$\begin{aligned}N_{k+1}(\vec{a},\vec{d},q,b)&=N(b=a_{k+1}x_{k+1}^{d_{k+1}})M_0+\sum_{j=1}^{\sqrt{q}-\varepsilon}M_{\alpha^j}\sum_{i\equiv j}N(b-a_{k+1}x_{k+1}^{d_{k+1}}=\alpha^i)\\&=(1-(1-d_{k+1})^{\tilde{\theta}})M_0+\sum_{j=1}^{\sqrt{q}-\varepsilon}M_{\alpha^j}\sum_{i\equiv j}N(b-a_{k+1}x_{k+1}^{d_{k+1}}=\alpha^i)\qquad(3.19)\\&=C_0+\sum_{j=1}^{\sqrt{q}-\varepsilon}\left(\frac{M_{\alpha^j}}{\sqrt{q}-\varepsilon}\right)N_y^*(b-a_{k+1}x_{k+1}^{d_{k+1}}=\alpha^j y^{\sqrt{q}-\varepsilon}),\end{aligned}$$

where the last equality follows from Lemma 3.23 and $N_y^*(b-a_{k+1}x_{k+1}^{d_{k+1}}=\alpha^j y^{\sqrt{q}-\varepsilon})$ is as in Definition 3.16. Let $M_j^*=N_y^*(b-a_{k+1}x_{k+1}^{d_{k+1}}=\alpha^j y^{\sqrt{q}-\varepsilon})$ for $1\le j\le\sqrt{q}-\varepsilon$. Let B be a positive integer such that $b=\alpha^B$, where $B=(\sqrt{q}-\varepsilon)\ell+m$ for some non-negative integer ℓ and some $m<\sqrt{q}-\varepsilon$. Proposition 3.22 entails that

$$M_j^*=\begin{cases}q-1+(1-\varepsilon\sqrt{q})(1-d_{k+1})^{\tilde{\theta}}-\varepsilon(\sqrt{q}-\varepsilon)(1-d_{k+1})^{\theta_{d_{k+1}}(\alpha^j,b)},\ \text{if } j\neq m;\\ q-1+(\varepsilon\sqrt{q}-1)(\sqrt{q}-1)(1-d_{k+1})^{\tilde{\theta}}-\varepsilon(\sqrt{q}-\varepsilon)(1-d_{k+1})^{\theta_{d_{k+1}}(\alpha^j,b)},\ \text{if } j=m.\end{cases}$$

Let $\theta_j=\theta_{d_{k+1}}(\alpha^j,b)$ for $1\le j\le\sqrt{q}-\varepsilon$. Then from Equation (3.19) it follows that

$$N_{k+1}(\vec{a},\vec{d},q,b)=C_0+\sum_{j=1}^{\sqrt{q}-\varepsilon}\frac{M_{\alpha^j}(q-1+(1-\varepsilon\sqrt{q})(1-d_{k+1})^{\tilde{\theta}}-\varepsilon(\sqrt{q}-\varepsilon)(1-d_{k+1})^{\theta_j})}{\sqrt{q}-\varepsilon}+\varepsilon\sqrt{q}(1-d_{k+1})^{\tilde{\theta}}M_b.$$

Set $S_j=\prod_{i=1}^k(1-d_i)^{\nu_i(\alpha^j)}$ and $S=\sum_{j=1}^{\sqrt{q}-\varepsilon}\prod_{i=1}^k(1-d_i)^{\delta_{i,j}}$. By the induction hypothesis and Lemma 3.24, the last equality becomes

$$N_{k+1}(\vec{a},\vec{d},q,b)=C_0+C_1+\varepsilon^k q^{\frac{k-1}{2}}\sum_{j=1}^{\sqrt{q}-\varepsilon}S_j(1-d_{k+1})^{\theta_j}+C_2.\qquad(3.20)$$

where $C_1:=\dfrac{\left(q^{k-1}(\sqrt{q}-\varepsilon)-\varepsilon^k q^{\frac{k-2}{2}}S\right)\left(q-1+(1-\varepsilon\sqrt{q})(1-d_{k+1})^{\tilde{\theta}}\right)}{\sqrt{q}-\varepsilon}$ and $C_2:=\varepsilon\sqrt{q}(1-d_{k+1})^{\tilde{\theta}}M_b$. We recall that the values of M_b and M_0 are known (by the induction hypothesis and Corollary 3.8) and so a straightforward computation shows that C_0+C_2 equals

$$q^{k-1}+\varepsilon^k q^{\frac{k-2}{2}}(\sqrt{q}+\varepsilon)S-(1-d_{k+1})^{\tilde{\theta}}\left((1-\varepsilon\sqrt{q})q^{k-1}+\varepsilon^{k+1}q^{\frac{k-2}{2}}S+\varepsilon^k q^{\frac{k}{2}}\prod_{i=1}^k(1-d_i)^{\nu_i(b)}\right).\qquad(3.21)$$

By Equations (3.20) and (3.21), it follows that

$$\begin{aligned}N_{k+1}(\vec{a},\vec{d},q,b)&=q^k-\varepsilon^k q^{\frac{k-1}{2}}\left(\sqrt{q}(1-d_{k+1})^{\tilde{\theta}}\prod_{i=1}^k(1-d_i)^{\nu_i(b)}-\sum_{j=1}^{\sqrt{q}-\varepsilon}S_j(1-d_{k+1})^{\theta_j}\right)\\&=q^k-\varepsilon^k q^{\frac{k-1}{2}}\left(\sqrt{q}\prod_{i=1}^{k+1}(1-d_i)^{\nu_i(b)}-\sum_{j=1}^{\sqrt{q}-\varepsilon}\prod_{i=1}^{k+1}(1-d_i)^{\delta_{i,j}}\right),\end{aligned}$$

which proves the result for $s=k+1$. ■

Let $\mathcal{F}(k,m)$ be the projective Fermat type curve given by the affine equation $ax^k+by^m=c$. As a direct consequence of Theorem 3.9, we have the number of points on $\mathcal{F}(k,m)$ in the case

where k and m are (p,r)-admissible. In fact, Corollary 3.10 follows easily from Theorem 3.9 by taking account the points at the infinity. From Example 6.3.3 in [91], it follows that the genus g of $\mathcal{F}(k,m)$ is given by

$$g = \frac{(k-1)(m-1)+1-\gcd(k,m)}{2}.$$

Corollary 3.10 provides conditions in which the number of $\mathbb{F}_q$-rational points on $\mathcal{F}(k,m)$ attains the Hasse-Weil bound. In fact, the characterization of maximal and minimal varieties is a problem of interest in the last few decades because of its applications in coding theory. In Chapter 4, we will study this problem for Fermat hypersurfaces. Before doing that, we will study Fermat hypersurfaces whose number of $\mathbb{F}_q$-rational points attaining Weil's bound in the affine space.

3.6 Further consequences for the case $s = 2$

As presented in Chapter 2, for a curve $\mathcal{C}$ over $\mathbb{F}_q$, we denote by $M_n(\mathcal{C})$ the number of rational points of $\mathcal{C}$ over $\mathbb{F}_{q^n}$. For an irreducible non-singular curve $\mathcal{C}$ over $\mathbb{F}_q$, the well-known Riemann Hypothesis [57, Theorem 3.3] states that the number of rational points on a curve $\mathcal{C}$ over $\mathbb{F}_{q^n}$ satisfies

$$M_n(\mathcal{C}) = q^n + 1 - \sum_{i=1}^{2g} \omega_i^n,$$

where g denotes the genus of $\mathcal{C}$ and $|\omega_i| = \sqrt{q}$ for all i. The well-known Hasse-Weil bound for the number of $\mathbb{F}_q$-rational points on an irreducible non-singular curve of genus g states that

$$|M_n(\mathcal{C}) - q^n - 1| \leq 2g\sqrt{q^n}. \tag{3.22}$$

The curve $\mathcal{C}$ is called maximal over $\mathbb{F}_{q^2}$ if its number of points attains the Hasse-Weil upper bound, that is,

$$M_2(\mathcal{C}) = q^2 + 1 + 2gq,$$

where g is the genus of $\mathcal{C}$. Similarly, a curve is called minimal over $\mathbb{F}_{q^2}$ if it attains the Hasse-Weil lower bound. There exist many families of maximal curves in the literature. In particular, a curve $\mathcal{J}$ with affine equation $x_1^d + x_2^d = 1$ yields examples of maximal and minimal curves (see Theorem 4.2). We observe that $M_n(\mathcal{J}) = N_2(\vec{a},\vec{d},\vec{t},p^n,b) + c_0$ if $t_1 = t_2 = n$, where c_0 is the number of points at infinity on $\mathcal{J}$. Our aim in this section is to present a bound such as (3.22) in the case the points on $\mathcal{C}$ has restricted solutions sets, replacing $M_n(\mathcal{C})$ by $N_2(\vec{a},\vec{d},\vec{t},p^n,b)$.

Corollary 3.25. *Let $q = p^n$, $\vec{a} = (1,1)$, $\vec{d} = (d,d)$ and $\vec{t} = (t_1,t_2)$. Assume that d is (p,r)-admissible. Then the number N of points on the affine curve $x^d + y^d + 1 = 0$ with $x \in \mathbb{F}_{q^{2t_1}}$ and $y \in \mathbb{F}_{q^{2t_2}}$ satisfies*

$$\left|N - |\Lambda| p^{2t_1+2t_2-n}\right| \leq (d-1)^2 p^{t_1+t_2} + (d-1)(p^{t_1}+p^{t_2}),$$

where $\Lambda := \Lambda(1,t_1) \cap \Lambda(1,t_2)$.

Proof. Since $\Lambda(1,t_i) \subset \Lambda(1,r)$ for $i = 1,2$, the result follows directly by Corollary 3.4. ■

From here, we pose the following problem.

Problem 3.26. *Can we obtain a bound similar to Hasse-Weil's bound for the number of $\mathbb{F}_q$-rational points on affine curves with with restricted coordinates?*

Another way that could be used to build interesting bounds on $N_2(\vec{a}, \vec{d}, \vec{t}, q, b)$ (or $N_s(\vec{a}, \vec{d}, \vec{t}, q, b)$ in general) is by proving that the associated zeta function has total degree bounded by a polynomial in $\vec{t} = (t_1, ..., t_n)$. The partial zeta function is studied in [103]. In this paper, the author conjectures the following result.

Conjecture 3.27. *[103] Let $T = \operatorname{lcm}(t_1, \ldots, t_s)$. There exist two positive constants c_1 and c_2 depending only on $a_1, \ldots, a_s, b, d_1, \ldots, d_s$ and s such that the total degree of the partial zeta function associated to $N_s(\vec{a}, \vec{d}, \vec{t}, q, b)$ is uniformly bounded by $c_1 T^{c_2}$ for all positive integers $\{t_1, \ldots, t_s\}$.*

CHAPTER 4

On maximal and minimal hypersurfaces of Fermat type

Let $\mathbb{F}_q$ be a finite field with $q = p^n$ elements, where p is a prime and n is a positive integer. Let $(a_1, \ldots, a_s) \in \mathbb{F}_q^s$, $(d_1, \ldots, d_s) \in \mathbb{Z}_+^s$ and $b \in \mathbb{F}_q$, and let $\mathcal{X} \subset \mathbb{A}^s$ be an irreducible Fermat hypersurface defined over $\mathbb{F}_q$ given by

$$\mathcal{X} : a_1 x_1^{d_1} + \cdots + a_s x_s^{d_s} = b. \tag{4.1}$$

If $|\mathcal{X}(\mathbb{F}_q)|$ denotes the number of $\mathbb{F}_q$-rational points on $\mathcal{X}$ and $b \in \mathbb{F}_q^*$, then the famous Weil bound [105] states that

$$\left||\mathcal{X}(\mathbb{F}_q)| - q^{s-1}\right| \leq q^{(s-2)/2}\left[\sqrt{q}\prod_{i=1}^{s}(d_i - 1) - (\sqrt{q} - 1)I(d_1, \ldots, d_s)\right], \tag{4.2}$$

where $I(d_1, \ldots, d_s)$ is the number of s-tuples $(y_1, \ldots, y_s) \in \mathbb{Z}^s$, with $1 \leq y_i \leq d_i - 1$ for all $i = 1, \ldots, s$, such that

$$\frac{y_1}{d_1} + \cdots + \frac{y_s}{d_s} \equiv 0 \pmod 1. \tag{4.3}$$

If $b = 0$, then Weil's bound implies that

$$\left||\mathcal{X}(\mathbb{F}_q)| - q^{s-1}\right| \leq I(d_1, \ldots, d_s)(q-1)q^{(s-2)/2}. \tag{4.4}$$

If the number of $\mathbb{F}_q$-rational points on $\mathcal{X}$ attains the upper (lower) Weil's bound, then it is called a maximal (minimal) hypersurface. In general, maximal hypersurfaces are of great interest due to their wide use for applications in coding theory [5, 90]. Indeed, the problem of studying the number of points on $\mathcal{X}$ has been tackled by many authors. Although the exact number of points on $\mathcal{X}$ has been studied in many papers [12, 13, 109], the complete characterization of the maximality and minimality of it with respect to Weil's bound has not been provided. The particular case where $\mathcal{X}$ is a curve has been studied by some authors [33, 97]. For example, maximal and minimal Fermat type curves of the form $x^n + y^m = 1$ were studied in [96] and [97].

The aim of this chapter is to provide necessary and sufficient conditions in which a Fermat hypersurface is maximal or minimal. For $d_1 = \cdots = d_s$, we study the number of $\mathbb{F}_q$-rational points in order to find those Fermat hypersurfaces whose number of rational points attains Weil's

bound. In Theorem 4.1 we provide necessary and sufficient conditions on $a_1, \ldots, a_s$ and q in which Fermat hypersurfaces are maximal or minimal. In particular, we prove that a maximal (or minimal) Fermat hypersurfaces must satisfy the hypothesis of Theorem 3.9. Our approach for this problem relies in the use of Lemma 4.6, which is a important result on Jacobi sums proved by Shioda and Katsura [87]. As a direct consequence of Theorem 4.1 we obtain a complete characterization of maximal and minimal affine curves given by $ax^d + by^d = c$. It turns out that the maximal and minimal hypersurfaces given by Equation (4.1) satisfy a natural condition, which is being covered by a Hermitian type hypersurface defined over $\mathbb{F}_q$ given by

$$\mathcal{H}_r : x_1^{p^r+1} + \cdots + x_s^{p^r+1} = 1,$$

where r is a positive integer. The aproach used to prove Theorem 4.1 seems not to be applicable in the general situation where $d_1, \ldots, d_s$ are distintic, so that we could not characterize the maximality and minimality in the general setting. Our second goal in this chapter is to provide tools that allow us to study the maximality and minimality of $\mathcal{X}$ in the case $b \neq 0$ for distinct $d_1, \ldots, d_s$. Along Section 4.3 we provide a new approach to tackle this problem. The main ingredients we use are the celebrated Hasse-Davenport Relation and a purity result for Jacobi sums. In Theorem 4.3 we provide necessary and sufficient conditions in which the number of $\mathbb{F}_q$-rational points on $\mathcal{X}$ attains the bound (4.2). In particular, we will prove that the condition of being covered by the Hermitian curve remains being necessary in this more general setting. Throughout the chapter, $s \geq 2$ is an integer, $d_1, \ldots, d_s$ are non-negative integers ≥ 2 dividing $q-1$ and $a_1, \ldots, a_s, b$ are elements in $\mathbb{F}_q$.

The main results of this chapter are summarized as follows.

Theorem 4.1. *Assume that $d_1 = \cdots = d_s = d > 2$, $(s, b) \neq (2, 0)$, $(s, d, b) \neq (4, 3, 0)$ and $(s, d) \neq (3, 3)$ if $b \neq 0$. The maximality and minimality of χ are set as follows.*

1. *If $b = 0$, then bound (4.4) is attained if and only if*
   - *d is (p, r)-admissible;*
   - *$\chi_d(a_1) = \cdots = \chi_d(a_s)$.*
2. *If $b \neq 0$, then bound (4.2) is attained if and only if*
   - *d is (p, r)-admissible;*
   - *$n/2r$ is even;*
   - *$\chi_d(a_1) = \cdots = \chi_d(a_s) = \chi_d(b)$.*

Suppose Weil's bound is attained. If $b = 0$, then χ is minimal if and only if $n/2r$ is even and s is odd. If $b \neq 0$, then χ is minimal if and only if s is even.

The case $(s, b) = (2, 0)$ is commented in Remark 4.7. The cases $(s, d, b) = (4, 3, 0)$ and $(s, d) \neq (3, 3)$ with $b \neq 0$ are not included in Theorem 4.1 because of a technical obstruction in Lemma 4.6. For these cases, it still not known if the result is true. The number of $\mathbb{F}_q$-rational points on Fermat hypersfaces of degree $d = 2$ is well-known (see Theorems 6.26 and 6.27 in [50]).

As a direct consequence of Theorem 4.1, we have a characterization for maximal and minimal Fermat curves.

Corollary 4.2. *For $a, b, c \in \mathbb{F}_q$ and d a divisor of $q-1$, let $\mathcal{C}$ be the curve $ax^d + by^d = c$ over $\mathbb{F}_q$. Then*

1. *$\mathcal{C}$ is maximal over $\mathbb{F}_q$ if and only if the following hold:*
   - *n is even;*
   - *d divides $\sqrt{q}+1$;*
   - *$\chi_d(a) = \chi_d(b) = \chi_d(c)$.*
2. *$\mathcal{C}$ is minimal over $\mathbb{F}_q$ if and only if the following hold:*
   - *$4|n$ and there exists a divisor r of $n/4$ such that d divides $p^r + 1$;*
   - *$\chi_d(a) = \chi_d(b) = \chi_d(c)$.*

Theorem 4.2 generalizes the main result of Tafazolian [96] and also generalizes Theorem 4.4 of Garcia and Tafazolian [33], where the authors study maximal curves of the form $x^d + y^d = 1$. In particular, Theorem 4.2 implies that $\mathcal{C}$ is maximal (or minimal) only if it is covered by a Hermitian curve.

Now, we focus on the case $b \neq 0$.

Theorem 4.3. *Assume that $b \in \mathbb{F}_q^*$, $s \neq 3$ and suppose that $\gcd(d_1, \ldots, d_s) > 2$ if $s > 3$. Then the number of $\mathbb{F}_q$-rational points on $\mathcal{X}$ attains the bound (4.2) if and only if*

- *each d_i is (p, r)-admissible;*
- *$\frac{n}{2r}$ is even;*
- *$\chi_{d_i}(a_i) = \chi_{d_i}(b)$ for all $i = 1, \ldots, s$.*

Furthermore, $\mathcal{X}$ is maximal if s is odd and minimal otherwise.

It is worth mentioning that a hypersurface is maximal (or minimal) if and only the inverses of all roots of the associated L-function are equal to $-q^{\frac{s-1}{2}}$ and $-q^{\frac{s-2}{2}}$ (or $q^{\frac{s-1}{2}}$ and $q^{\frac{s-2}{2}}$). In particular, in the cases where the conditions of Theorem 4.3 are satisfied, the Zeta function associated to $\mathcal{X}$ is provided. Furthermore, our result generalizes many results in the literature, such as the main results of [96, 97] and Theorem 4.4 of [33]. As we will see in Section 4.3, the hypothesis imposed here are important in our approach and are difficult to ride out. For example, a characterization for maximal and minimal Fermat hypersurfaces in case where $b = 0$ remains being an open problem. More results concerning the number of points on these type of hypersurfaces can be found in [59], [63] and in the references therein.

4.1 Preparation

In this section we provide some preliminary results that will be important along the chapter. A formula for $I(d_1, \ldots, d_s) = 0$ is presented in the following result.

Lemma 4.4. *Let $d_1, \dots, d_s$ be positive integers and let $D = \operatorname{lcm}(d_1, \dots, d_s)$. Then*

$$I(d_1, \dots, d_s) = \tfrac{(-1)^s}{D} \sum_{m=1}^{D} \prod_{d_i \mid m} (1 - d_i). \tag{4.5}$$

Proof. A well-known formula for $I(d_1, \dots, d_s)$ (see p.293 of [50]) is the following:

$$I(d_1, \dots, d_s) = (-1)^s + (-1)^s \sum_{r=1}^{s} (-1)^r \sum_{1 \le i_1 < \cdots < i_r \le s} \frac{d_{i_1} \dots d_{i_r}}{\operatorname{lcm}(d_{i_1}, \dots, d_{i_r})}. \tag{4.6}$$

Let $i_1, \dots, i_r$ be integers such that $1 \le i_1 < \cdots < i_r \le s$. The product $d_{i_1} \cdots d_{i_r}$ appears in an expansion of a product in (4.5) whenever $d_{i_j} | m$ for all $j = 1, \dots, r$, which occurs $\frac{D}{\operatorname{lcm}(d_{i_1}, \dots, d_{i_r})}$ times, since $1 \le m \le D$. Therefore the expressions in (4.5) and (4.6) coincide, proving our result. ■

Sufficient and necessary conditions in which $I(d_1, \dots, d_s) = 0$ were studied by Sun and Wan [93], where the authors state the following result.

Lemma 4.5. *[72, Main Result] Let $s > 2$ be an integer and let $d_1, \dots, d_s$ be positive integers. Then $I(\vec{d}) = 0$ if and only if one of the following holds:*

- *for some d_i, $\gcd(d_i, d_1 \cdots d_s / d_i) = 1$*
- *if $d_{i_1}, \dots, d_{i_t}$ $(1 \le i_1 < \cdots < i_t \le s)$ is the set of all even integers among $\{d_1, \dots, d_s\}$, then $2 \nmid t$, $d_{i_1}/2, \dots, d_{i_t}/2$ are pairwise coprime, and d_{i_j} is coprime to any odd number in $\{d_1, \dots, d_s\}$ $(j = 1, \dots, t)$.*

In order to characterize the maximality and minimality of Fermat hypersurfaces, we recall the following way to compute their number of $\mathbb{F}_q$-rational points:

$$\begin{aligned} |\mathcal{X}(\mathbb{F}_q)| &= \sum_{b_1 + \cdots + b_s = b} \prod_{i=1}^{s} \left[1 + \chi_{d_i}(a_i^{-1} b_i) + \cdots + \chi_{d_i}^{d_i - 1}(a_i^{-1} b_i) \right] \\ &= q^{s-1} + \sum_{0 < \ell_i < d_i} \chi_{d_1}^{\ell_1}(a_1^{-1}) \dots \chi_{d_s}^{\ell_s}(a_s^{-1}) J_b(\chi_{d_1}^{\ell_1}, \dots, \chi_{d_s}^{\ell_s}). \end{aligned} \tag{4.7}$$

In order to prove our results, we need the following result.

Lemma 4.6. *[87, Proposition 3.5 and Remark 3.8] Let $s \ge 2$ be an integer, $d \ge 3$ be a divisor of $q - 1$ and let*

$$\mathcal{U}_s(d) = \{(\ell_1, \dots, \ell_s) \in [1, d-1]^s : \ell_1 + \cdots + \ell_s \not\equiv 0 \pmod{d}\}.$$

If $s = 3$, assume that $d > 3$. If the Jacobi sum $J(\chi_d^{\ell_1}, \dots, \chi_d^{\ell_s})$ is pure for all s-tuples $(\ell_1, \dots, \ell_s) \in \mathcal{U}_s(d)$, then d is (p, r)-admissible for some positive integer r.

4.2 The case $d_1 = \cdots = d_s$

The aim of this section is to provide a proof for Theorem 4.1.

Proof of Theorem 4.1: Let $\mathcal{U}_s(d)$ be as defined in Lemma 4.6. Suppose that $b = 0$, $s \geq 3$ and assume that the bound (4.4) is attained. By Equation (4.7) and Proposition 1.11, we have that

$$|\mathcal{X}(\mathbb{F}_q)| = q^{s-1} + \sum_{\substack{0<\ell_i<d \\ (\ell_1,\ldots,\ell_s)\in\mathcal{U}_s^c(d)}} \chi_d^{\ell_1}(a_1^{-1})\ldots\chi_d^{\ell_s}(a_s^{-1})J_0(\chi_d^{\ell_1},\ldots,\chi_d^{\ell_s}), \tag{4.8}$$

where $\mathcal{U}_s^c(d) := \{(\ell_1,\ldots,\ell_s) \in [1,d-1]^s : \ell_1+\cdots+\ell_s \equiv 0 \pmod d\}$. Moreover, if $(\ell_1,\ldots,\ell_s) \in \mathcal{U}_s^c(d)$, then

$$\begin{aligned} J_0(\chi_d^{\ell_1},\ldots,\chi_d^{\ell_s}) &= \sum_{b_1+\cdots+b_s=0} \chi_d^{\ell_1}(b_1)\ldots\chi_d^{\ell_s}(b_s) \\ &= (q-1)\sum_{b_1+\cdots+b_{s-1}=1} \chi_d^{\ell_1}(b_1)\ldots\chi_d^{\ell_{s-1}}(b_{s-1}) \\ &= (q-1)J(\chi_d^{\ell_1},\ldots,\chi_d^{\ell_{s-1}}). \end{aligned} \tag{4.9}$$

We recall that $|\mathcal{U}_s^c(d)| = I(d,\ldots,d)$ and that we are assuming that the bound (4.4) is attained. Furthermore, by Lemma 4.5, $I(d,\ldots,d) = 0$ if and only if $d = 2$ and s is odd. Therefore, since we are under the assumption $d > 2$, it follows from Equations (4.8) and (4.9) that

$$\chi_d^{\ell_1}(a_1^{-1})\ldots\chi_d^{\ell_s}(a_s^{-1})J(\chi_d^{\ell_1},\ldots,\chi_d^{\ell_{s-1}}) \in \{\pm q^{(s-2)/2}\}$$

for all $(\ell_1,\ldots,\ell_s) \in \mathcal{U}_s^c(d)$ or, equivalently, for all $(\ell_1,\ldots,\ell_{s-1}) \in \mathcal{U}_{s-1}(d)$. In particular, $J(\chi_d^{\ell_1},\ldots,\chi_d^{\ell_{s-1}})$ is pure for all $(\ell_1,\ldots,\ell_{s-1}) \in \mathcal{U}_{s-1}(d)$ and so, by Lemma 4.6, d is (p,r)-admissible for some positive integer r. Then $2r$ is the order of p in the multiplicative group $\mathbb{Z}_d^\times$. Since $q \equiv 1 \pmod d$, with $q = p^n$, it follows that $2r|n$. In particular, n is even. Therefore we are under the hypothesis of Theorem 3.9 and so

$$|\mathcal{X}(\mathbb{F}_q)| = q^{s-1} + \varepsilon^s q^{\frac{s-2}{2}}(\sqrt{q}+\varepsilon)\sum_{j=1}^{\sqrt{q}-\varepsilon}\prod_{i=1}^{s}(1-d)^{\delta_{i,j}},$$

where $\varepsilon = (-1)^{n/2r}$. It is direct to verify that $|(-1)^s(\sqrt{q}-\varepsilon)^{-1}\sum_{j=1}^{\sqrt{q}-\varepsilon}\prod_{i=1}^{s}(1-d)^{\delta_{i,j}}| = |I(d,\ldots,d)|$ if and only if $\chi_d(a_1) = \cdots = \chi_d(a_s)$, proving our result. Moreover,

$$(-1)^s(\sqrt{q}-\varepsilon)^{-1}\sum_{j=1}^{\sqrt{q}-\varepsilon}\prod_{i=1}^{s}(1-d)^{\delta_{i,j}} = -I(d,\ldots,d)$$

if and only if $\varepsilon = 1$ and s is odd, which occurs if and only if $n/2r$ is even and s is odd. The converse follows from Theorem 3.9.

The case $b \neq 0$ can be obtained similarly to the case $b = 0$. ■

Theorem 4.1 does not consider the case where $s = 2$ and $b = 0$. For $s = 2$ only the upper bound can be attained, as it is shown in the following remark.

Remark 4.7. *If $s = 2$ and $b = 0$, then $I(d,d) = d-1$ and*

$$J_q(\chi_d^{\ell_1},\chi_d^{\ell_2},0) = \sum_{b_1\in\mathbb{F}_q}\chi_d(b_1^{\ell_1}(-b_1)^{\ell_2}) = \begin{cases} 0, & \text{if } d \nmid (\ell_1+\ell_2); \\ (q-1)\chi_d((-1)^{\ell_2}), & \text{if } d \mid (\ell_1+\ell_2). \end{cases}$$

Furthermore, $d \mid (\ell_1 + \ell_2)$ *if and only if* $\ell_1 = d - \ell_2$ *with* $\ell_2 = 1, \ldots, d-1$. *Therefore, by Equation* (4.8) *we have that*

$$\begin{aligned} |\mathcal{X}(\mathbb{F}_q)| &= q + \sum_{\ell_2=1}^{d-1} \chi_d^{-\ell_2}(a_1^{-1})\chi_d^{\ell_2}(a_2^{-1})(q-1)\chi_d((-1)^{\ell_2}) \\ &= q + (q-1)\sum_{\ell_2=1}^{d-1} \chi_d^{-\ell_2}(a_1^{-1})\chi_d^{\ell_2}(-a_2^{-1}) \end{aligned}$$

and then the bound (4.4) *is attained if and only if* $\chi_d(-a_1a_2^{-1}) = 1$. *Therefore the bound in Theorem 4.1 is attained only if* $\chi_d(a_1) = \chi_d(-a_2)$ *and, in this case, the upper bound is attained.*

4.3 The case $b \neq 0$ and distinct $d_1, \ldots, d_s$

In this section we provide the proof of Theorem 4.3. Our strategy is to prove a result similar to Lemma 4.6. In order to do so, the following definitions will be useful.

Definition 4.8. *Let* $\vec{d} = (d_1, \ldots, d_s) \in \mathbb{Z}$ *with* $d_i \geq 2$ *for all* $i = 1, \ldots, s$. *We set*

1. $\mathcal{B}(\vec{d}) = \{(\ell_1, \ldots, \ell_s) \in \mathbb{Z}^s : 0 < \ell_i < d_i \text{ for all } i = 1, \ldots, s\}$;
2. $\mathcal{U}(\vec{d}) = \{(\ell_1, \ldots, \ell_s) \in \mathcal{B}(\vec{d}) : \frac{y_1}{d_1} + \cdots + \frac{y_s}{d_s} \not\equiv 0 \pmod 1\}$;
3. $\mathcal{U}^c(\vec{d}) = \{(\ell_1, \ldots, \ell_s) \in \mathcal{B}(\vec{d}) : \frac{y_1}{d_1} + \cdots + \frac{y_s}{d_s} \equiv 0 \pmod 1\}$.

For $b \in \mathbb{F}_q^*$, Equation (4.7) implies that

$$|\mathcal{X}(\mathbb{F}_q)| = q^{s-1} + \sum_{(\ell_1,\ldots,\ell_s)\in\mathcal{B}(\vec{d})} \chi_{d_1}^{\ell_1}\big(\tfrac{b}{a_1}\big)\cdots\chi_{d_s}^{\ell_s}\big(\tfrac{b}{a_s}\big)J\big(\chi_{d_1}^{\ell_1}, \ldots, \chi_{d_s}^{\ell_s}\big). \tag{4.10}$$

Proposition 1.11 states that

$$\big|J\big(\chi_{d_1}^{\ell_1}, \ldots, \chi_{d_s}^{\ell_s}\big)\big| = \begin{cases} q^{\frac{s-1}{2}}, & \text{if } (\ell_1, \ldots, \ell_s) \in \mathcal{U}(\vec{d}); \\ q^{\frac{s-2}{2}}, & \text{if } (\ell_1, \ldots, \ell_s) \in \mathcal{U}^c(\vec{d}). \end{cases}$$

From here, we have the following direct result.

Lemma 4.9. *If* $|\mathcal{X}(\mathbb{F}_q)|$ *attains the bound* (4.2), *then* $J\big(\chi_{d_1}^{\ell_1}, \ldots, \chi_{d_s}^{\ell_s}\big)$ *is pure for all* $(\ell_1, \ldots, \ell_s) \in \mathcal{B}(\vec{d})$.

In what follows, we use this fact to obtain necessary conditions for which bound (4.2) is attained. The following lemma is a consequence of the well-known Hasse-Davenport Relation and will be used in the main results of this section.

Lemma 4.10. *Let* k *be a positive integer and let* λ *and* χ *be multiplicative characters of* $\mathbb{F}_q^*$ *such that* λ *has order* $m \geq 1$. *Then*

$$\frac{\prod_{j=0}^{m-1} G\big(\lambda^{kj}\chi\big)}{G\big(\chi^{m/d}\big)^d} \in \Omega,$$

where $d = \gcd(m, k)$ *and* Ω *is defined as in Definition 1.13.*

Proof. We observe λ^k has order $\frac{m}{d}$. If χ also has order $\frac{m}{d}$, then item (b) of Lemma 1.6 entails that

$$\frac{\prod_{j=0}^{m-1} G(\lambda^{kj}\chi)}{G(\chi^{m/d})^d} = \frac{\prod_{j=0}^{m-1} G(\lambda^{kj})}{(-1)^d} = \begin{cases} q^{\frac{m-1}{2}} \prod_{j=1}^{\frac{m-1}{2}} \lambda^j(-1), & \text{if } m \text{ is odd;} \\ G(\lambda^{m/2}) q^{\frac{m-2}{2}} \prod_{j=1}^{\frac{m-2}{2}} \lambda^j(-1), & \text{if } m \text{ is even.} \end{cases} \tag{4.11}$$

The assertion follows from Equation (4.11) and Theorem 1.7. If $d = m$, then

$$\prod_{j=0}^{m-1} G(\lambda^{kj}\chi) = \prod_{j=0}^{m-1} G(\chi) = G(\chi)^d,$$

which proves the assertion. Now, we assume that the order of χ is not $\frac{m}{d}$ and $d \neq m$. It follows from Theorem 1.7 and Corollary 5.29 of [50] that

$$\frac{\prod_{j=0}^{m/d-1} G(\lambda^{kj}\chi)}{G(\chi^{m/d})} \in \Omega,$$

and therefore our result follows by using that λ^k has order $\frac{m}{d}$. ■

The following proposition is the key step of the proof of our main results.

Proposition 4.11. *Let $s \neq 3$ be an integer and suppose $\gcd(d_1, \ldots, d_s) > 2$ if $s > 3$. If $J(\chi_{d_1}^{\ell_1}, \ldots, \chi_{d_s}^{\ell_s})$ is pure for all $(\ell_1, \ldots, \ell_s) \in \mathcal{B}(\vec{d})$, then $G(\chi_{d_j}^{\ell})$ is pure for all $\ell \in \mathbb{Z}$ and $j = 1, \ldots, s$.*

Proof. We will prove that $G(\chi_{d_1}^{\ell})$ is pure for all $\ell \in \mathbb{Z}$. If $\ell \equiv 0 \pmod{d_1}$, then the result follows directly by item (c) of Lemma 1.6. Assume that $\ell \not\equiv 0 \pmod{d_1}$. Since $\gcd(d_1, \ldots, d_s) > 2$ and $s \neq 3$, it follows from Lemma 4.5 that there exists a $(s-2)$-tuple $(m_3, \ldots, m_s) \in \mathbb{Z}^{s-2}$, with $1 \leq m_i \leq d_i - 1$ for all $i = 3, \ldots, s$, such that

$$\frac{m_3}{d_3} + \cdots + \frac{m_s}{d_s} \equiv 0 \pmod{1}.$$

Then, by Theorem 1.9 and Lemmas 1.6 and 1.15, we have that

$$\frac{G(\chi_{d_1}^{\ell_1})^2 G(\chi_2^{\ell_2})^2}{G(\chi_{d_1}^{\ell_1}\chi_{d_2}^{\ell_2})^2} = \frac{J(\chi_{d_1}^{\ell_1}, \chi_{d_2}^{\ell_2}, \chi_{d_3}^{m_3}, \ldots, \chi_{d_s}^{m_s}) J(\chi_{d_1}^{\ell_1}, \chi_{d_2}^{\ell_2}, \chi_{d_3}^{-m_3}, \ldots, \chi_{d_s}^{-m_s})}{q^{\frac{s-2}{2}} \chi_{d_3}(-1) \cdots \chi_{d_s}(-1)} \in \Omega \tag{4.12}$$

for all $1 \leq \ell_1 < d_1$ and $1 \leq \ell_2 < d_2$. By Lemmas 1.6, 1.15 and 4.10 and Theorem 1.7 we have that

$$\prod_{\ell_2=1}^{d_2-1} \frac{G(\chi_{d_1}^{\ell_1})^2 G(\chi_2^{\ell_2})^2}{G(\chi_{d_1}^{\ell_1}\chi_{d_2}^{\ell_2})^2} = \lambda \frac{G(\chi_{d_1}^{\ell_1})^{2d_2}}{G(\chi_{d_1}^{\ell_1 d_2})^2}$$

where $\lambda \in \Omega$. In particular, it follows from Lemma 4.10 that

$$\frac{G(\chi_{d_1}^{\ell_1})^{d_2}}{G(\chi_{d_1}^{\ell_1 d_2})} \in \Omega \tag{4.13}$$

for all $1 \leq \ell_1 < d_1$. Now we fix an integer $\ell \in \{1, \ldots, d_1 - 1\}$ in order to prove that $G(\chi_{d-1}^{\ell})$ is pure. We split the proof into two cases:

- There exists an integer $u \geq 1$ such that $\ell d_2^u \equiv 0 \pmod{d_1}$. In this case, we employ Equation (4.13), Lemma 1.15 and item (c) of Lemma 1.6 and obtain

$$-G(\chi_{d_1}^{\ell}) = \prod_{j=0}^{u-1} \frac{G\left(\chi_{d_1}^{\ell d_2^j}\right)^{d_2^{-j}}}{G\left(\chi_{d_1}^{\ell d_2^{j+1}}\right)^{d_2^{-(j+1)}}} \in \Omega.$$

- There exist integer $u > 0$ and $v > u$ such that $\ell d_2^v \equiv \ell d_2^u \pmod{d_1}$. We employ Equation (4.13) and Lemma 1.15 in order to obtain

$$G\left(\chi_{d_1}^{\ell d_2^u}\right)^{d_2^{-u}-d_2^{-v}} = \frac{G\left(\chi_{d_1}^{\ell d_2^u}\right)^{d_2^{-u}}}{G\left(\chi_{d_1}^{\ell d_2^v}\right)^{d_2^{-v}}} = \prod_{j=u}^{v-1} \frac{G\left(\chi_{d_1}^{\ell d_2^j}\right)^{d_2^{-j}}}{G\left(\chi_{d_1}^{\ell d_2^{j+1}}\right)^{d_2^{-(j+1)}}} \in \Omega. \tag{4.14}$$

  Furthermore, Equation (4.13) and Lemma 1.15 entail that

$$\frac{G\left(\chi_{d_1}^{\ell}\right)}{G\left(\chi_{d_1}^{\ell d_2^u}\right)^{d_2^{-(u)}}} = \prod_{j=0}^{u-1} \frac{G\left(\chi_{d_1}^{\ell d_2^j}\right)^{d_2^{-j}}}{G\left(\chi_{d_1}^{\ell d_2^{j+1}}\right)^{d_2^{-(j+1)}}} \in \Omega. \tag{4.15}$$

  Lemma 1.15 and Equations (4.14) and (4.15) imply that $G\left(\chi_{d_1}^{\ell}\right) \in \Omega$.

The cases where $i = 2, \ldots, s$ follow similarly. ■

The following theorem is one of the most important results of the section.

Theorem 4.12. *Let $s \neq 3$ be an integer and suppose $\gcd(d_1, \ldots, d_s) > 2$ if $s > 3$. If $J\left(\chi_{d_1}^{\ell_1}, \ldots, \chi_{d_s}^{\ell_s}\right)$ is pure for all $(\ell_1, \ldots, \ell_s) \in \mathcal{B}(\vec{d})$, then each d_i is (p, r)-admissible.*

Proof. By Theorem 1.16 and Proposition 4.11, it follows that for each $i = 1, \ldots, s$ there exists an positive integer r_i such that d_i is (p, r_i)-admissible. Since $\gcd(d_1, \ldots, d_s) > 2$ and $s \neq 3$, it follows from Lemma 4.5 that there exists a $(s-2)$-tuple $(m_3, \ldots, m_s) \in \mathbb{Z}^{s-2}$, with $1 \leq m_i \leq d_i - 1$ for all $i = 3, \ldots, s$, such that

$$\frac{m_3}{d_3} + \cdots + \frac{m_s}{d_s} \equiv 0 \pmod{1}.$$

By Theorem 1.9, we have that

$$\frac{G\left(\chi_{d_1}^{\ell_1}\right)G\left(\chi_{d_2}^{\ell_2}\right)G\left(\chi_{d_3}^{m_3}\right)\ldots G\left(\chi_{d_s}^{m_s}\right)}{G\left(\chi_{d_1}^{\ell_1}\chi_{d_2}^{\ell_2}\right)} = J\left(\chi_{d_1}^{\ell_1}, \chi_{d_2}^{\ell_2}, \chi_{d_2}^{m_3}, \ldots, \chi_{d_s}^{m_s}\right) \in \Omega$$

for all $1 \leq \ell_1 < d_1$ and $1 \leq \ell_2 < d_2$ and then, by Lemma 1.15 and Proposition 4.11, it follows that

$$G\left(\chi_{d_1}^{\ell_1}\chi_{d_2}^{\ell_2}\right) \in \Omega \tag{4.16}$$

for all $1 \leq \ell_1 < d_1$ and $1 \leq \ell_2 < d_2$. We set $D = \operatorname{lcm}(d_1, d_2)$. Let ℓ_1 and ℓ_2 be integers such that

$$\left(\tfrac{q-1}{d_1}\right)\ell_1 + \left(\tfrac{q-1}{d_2}\right)\ell_2 = \gcd\left(\tfrac{q-1}{d_1}, \tfrac{q-1}{d_2}\right) = \tfrac{q-1}{D}.$$

Claim: $G\left(\chi_{d_1}^{t\ell_1}\chi_{d_2}^{t\ell_2}\right) = G\left(\chi_D^t\right)$ is pure for all $t \in \mathbb{Z}$.

Proof of the claim: If $t \equiv 0 \pmod{d_1}$ or $t \equiv 0 \pmod{d_2}$, then the claim follows from Proposition 4.11. Assume that $t \not\equiv 0 \pmod{d_1}$ or $t \not\equiv 0 \pmod{d_2}$. In this case, Equation (4.16) states that $G\left(\chi_D^t\right)$ is pure, which completes the proof of the claim.

We observe that the claim and Theorem 1.16 imply that there exists an integer r such that D is (p,r)-admissible. In particular, it follows that $r_1 = r_2 = r$. By using the same arguments, we prove that $r_1 = \cdots = r_s$ and our result follows. ■

With the results obtained in this section, we are able to complete the proof of our result.

4.3.1 Proof of Theorem 4.3

Assume that the bound (4.2) is attained, then Lemma 4.9 and Theorem 4.12 state that each d_i is (p,r)-admissible. In particular, since $d_i|(p^n-1)$, we have that $2r|n$. Therefore, we are under the hypothesis of Theorem 3.9, which states that the bound (4.2) is attained if and only if

$$\prod_{i=1}^{s}(d_i-1)^{\nu_i(b)} = \prod_{i=1}^{s}(d_i-1), \tag{4.17}$$

where $\nu_i(b) = \theta_{d_i}(a_i,b)$. Therefore, by definition of $\theta_{d_i}(a_i,b)$ and Equation (4.17), we have that $\chi_{d_i}(a_i) = \chi_{d_i}(b)$ for all $i = 1,\ldots,s$.

For the converse, assume that d_i is (p,r)-admissible (and then n is even) and suppose that $\chi_{d_i}(a_i) = \chi_{d_i}(b)$ for all $i = 1,\ldots,s$. Since $\chi_{d_i}(a_i) = \chi_{d_i}(b)$, there exists $c_i \in \mathbb{F}_q$ such that $\frac{a_i}{b} = c_i^{d_i}$. Therefore, we can make a change of variables by replacing $c_i x_i$ by y_i in Equation (4.1) so that $|\mathcal{X}(\mathbb{F}_q)|$ equals the number of solutions of the equation

$$y_1^{d_1} + \cdots + y_s^{d_s} = 1.$$

Hence, by Theorem 3.9, we have that

$$\begin{aligned}
|\mathcal{X}(\mathbb{F}_q)| &= q^{s-1} - \varepsilon^{s+1} q^{\frac{s-2}{2}} \left(\sqrt{q} \prod_{i=1}^{s}(1-d_i) - \sum_{j=1}^{\sqrt{q}-\varepsilon} \prod_{i=1}^{s}(1-d_i)^{\delta_{i,j}} \right) \\
&= q^{s-1} - \varepsilon^{s+1} q^{\frac{s-2}{2}} \left(\sqrt{q} \prod_{i=1}^{s}(1-d_i) - \frac{\sqrt{q}-\varepsilon}{\sqrt{q}-\varepsilon} \sum_{m=0}^{\sqrt{q}-\varepsilon} \prod_{d_i|m}(1-d_i) \right) \\
&= q^{s-1} - \varepsilon^{s+1} q^{\frac{s-2}{2}} (-1)^s \left(\sqrt{q} \prod_{i=1}^{s}(d_i-1) - (\sqrt{q}-\varepsilon) I(d_1,\ldots,d_s) \right),
\end{aligned} \tag{4.18}$$

where the last equality follows from Lemma 4.4. From here, we observe that it is necessary and sufficient that $(-1)^{\frac{n}{2r}} = \varepsilon = 1$, which it is equivalent to $\frac{n}{2r}$ being even. Therefore the maximality and minimality depend only on the sign $(-1)^{s+1}$, which completes the proof. ■

CHAPTER 5

On the number of rational points on Artin-Schreier hypersurfaces

Let $\mathbb{F}_{q^k}$ be the finite field with q^k elements, and let $\mathcal{X} \subseteq \mathbb{A}^{s+1}$ be an irreducible Artin-Schreier hypersurface defined over $\mathbb{F}_{q^k}$ given by

$$\mathcal{X} : y^q - y = a_1 x_1^{d_1} + \cdots + a_s x_s^{d_s} + b, \quad d_i > 1. \tag{5.1}$$

If N denotes the number of points of $\mathcal{X}$ in $\mathbb{A}^{s+1}\left(\mathbb{F}_{q^k}\right)$, then the famous Weil's bound yields

$$|N - q^{sk}| \leq (q-1)(d_1 - 1)\cdots(d_s - 1)q^{sk/2}. \tag{5.2}$$

The hypersurface $\mathcal{X}$ is called $\mathbb{F}_{q^k}$-maximal ($\mathbb{F}_{q^k}$-minimal) if N attains the upper (lower) bound in (5.2). While particular examples of Artin-Schreier hypersurfaces attaining (5.2) can be readily constructed, a complete characterization of such hypersurfaces has not been provided previously. This and other related problems, such as determining the exact number of $\mathbb{F}_{q^k}$-rational points or improving Weil's bound under certain conditions, are compelling problems that have a number of applications [37], [109]. In this chapter, we address all the above questions. In particular, we provide an improvement for Weil's bound. The extent of the improvement will depend on certain data, but, at a minimum, bound (5.2) will be replaced by the sharp bound

$$|N - q^{sk}| \leq q^{1/2}(d_1 - 1)\cdots(d_s - 1)q^{sk/2}. \tag{5.3}$$

provided $\mathrm{Tr}_{q^k/q}(b) \neq 0$.

Equations of type (5.1) have been extensively studied in the case $s = 1$. For instance, in [109], Wolfmann considered the Artin-Schreier curves $\mathcal{X} : y^q - y = ax^s + b$ defined over $\mathbb{F}_{q^k}$. His results provide the number of $\mathbb{F}_{q^k}$-rational points of $\mathcal{X}$ in the following scenario:

(i) $k = 2t$

(ii) There exists a divisor r of t such that $q^r \equiv -1 \bmod s$.

In [16], Cosgun, Özbudak, and Saygi studied the number of $\mathbb{F}_{q^k}$-rational points on the curves $\mathcal{X} : y^{q^n} - y = \gamma x^{q^h+1} - b$. Several additional results regarding the number of rational points on Artin-Schreier curves were proved by Coulter [18], [19]. It is worth noting that despite the strength the aforementioned results, they do not lead to the proof of the $\mathbb{F}_{q^{2n}}$-maximality of the curve of type (5.1) given by

$$\mathcal{Y}_n : y^{q^2} - y = x^{\frac{q^n+1}{q+1}}, \tag{5.4}$$

where $n \geq 3$ is odd. The $\mathbb{F}_{q^6}$-maximality of $\mathcal{Y}_3$ was first proved by Garcia and Stichtenoth as a generalization of an example provided by Serre [30]. In [1], Abdón, Bezerra and Quoos proved the $\mathbb{F}_{q^{2n}}$-maximality of $\mathcal{Y}_n$ for all odd $n \geq 3$, and later in 2010, Garcia and Stichtenoth provided an alternative proof of this general result [31]. In these three papers, the proofs use techniques that are specific to curves and do not seem to extend to higher dimensional versions of $\mathcal{Y}_n$, such as

$$\mathcal{Y}_{n,s} : y^{q^2} - y = a_1 x_1^{\frac{q^n+1}{q+1}} + \cdots + a_s x_s^{\frac{q^n+1}{q+1}}. \tag{5.5}$$

Note that the important role played by $\mathcal{Y}_n$ in the context of maximal curves (see [22], [21], [24], [28], [29], [35]) brings additional interest to the hypersurfaces given by (5.5).

Among other matters, this chapter will characterize all hypersurfaces of type (5.1) that attain Weil's bound. It turns out that if $\mathcal{X} : y^q - y = a_1 x_1^{d_1} + \cdots + a_s x_s^{d_s} + b$ is defined over $\mathbb{F}_{q^k}$ and attains Weil's bound, then $\mathrm{Tr}_{q^k/q}(b) = 0$ (Theorem 5.8). An immediate consequence of this will be a proof for the $\mathbb{F}_{q^{2n}}$-maximality of the hypersurface $\mathcal{Y}_{n,s}$ for $a_1 = \cdots = a_s = 1$. In particular, the result yields a new proof for the maximality of the curve $\mathcal{Y}_n$ in (5.4).

Furthermore, under certain arithmetic conditions on $\mathbb{F}_{q^k}$ and $d_1, \ldots, d_s$, we provide the exact number of $\mathbb{F}_{q^k}$-rationals points of $\mathcal{X}$ (Corollaries 5.7 and 5.10), subsuming all such results provided for curves in [16] and [109].

Notation

The following notation is used throughout this chapter.

- $\mathbb{F}_{q^k}$ is a finite field with $q^k = p^{nk}$ elements
- For any divisor t of nk, Tr_{q^k/p^t} denotes the trace function from $\mathbb{F}_{q^k}$ to $\mathbb{F}_{p^t}$
- For divisors d of $q^k - 1$, χ_d denotes a multiplicative character of order d of $\mathbb{F}_{q^k}^*$
- $d_1, \ldots, d_s$ are integers greater than 1, and divisors of $q^k - 1$
- $a_1, \ldots, a_s$, and b are elements in $\mathbb{F}_{q^k}$
- γ denotes a generator of the multiplicative group $\mathbb{F}_q^*$
- For an positive integer k, $v_k = \frac{q^k-1}{q-1}$
- $v = \frac{q-1}{p-1}$ and $\gamma_1, \ldots, \gamma_v \in \mathbb{F}_q^*$ denote coset representatives of $\mathbb{F}_q^*/\mathbb{F}_p^*$.

5.1 Main Results

In this section, we present our main results, along with a few comments. Note that the equations $y^q - y = \sum_{i=1}^{s} a_i x^{d_i}$ and $y^q - y = \sum_{i=1}^{s} a_i x^{\gcd(d_i, q^k-1)}$ have the same number of $\mathbb{F}_{q^k}$-solutions. Hereafter, we will assume that $d_i \mid (q^k - 1)$ for $i = 1, \ldots, s$. The problem of bounding the number of $\mathbb{F}_q$-rational points on a hypersurface goes back to Weil (1950). In one of his most famous paper [105], he presented a simple bounds (bounds (4.2) and (4.4) presented in Section 4) for the number of points on a Fermat hypersurface in terms of a constant depending on the exponents of the monomials in the equation of the Fermat hypersurface. In this chapter, we generalize the definition of this constant in order to provide a bound for the number of $\mathbb{F}_q$-rational points on Artin-Schreier hypersurfaces.

Definition 5.1. *For $\vec{d} = (d_1, \ldots, d_s)$ and an positive integer k, we let $\Gamma_k(\vec{d})$ be the set of tuples $(j_1, \ldots, j_s) \in \mathbb{Z}^s$, with $1 \leq j_i < d_i$ for $i = 1, \ldots, s$, such that*

$$\left(\frac{q^k - 1}{q - 1}\right)\left(\frac{j_1}{d_1} + \cdots + \frac{j_s}{d_s}\right) \equiv 0 \pmod 1.$$

The cardinality of $\Gamma_k(\vec{d})$ is denoted by $I_k(\vec{d})$.

It is noteworthy that $I_1(\vec{d})$ coincides with the constant $I(d_1, \ldots, d_s)$ defined for Fermat hypersurfaces in Weil's paper [105]. One of the efforts of this chapter is to present the number of $\mathbb{F}_q$-rational points on Artin-Schreier hypersurfaces in terms of Gauss sums, which allow us to improve Weil's bound. This improvement will naturally depend of the constant $I_k(\vec{d})$ and it is stated as follows.

Theorem 5.2. *Let $N(b)$ denote the number of $\mathbb{F}_{q^k}$-rational points on the affine hypersurface given by $y^q - y = a_1 x_1^{d_1} + \cdots + a_s x_s^{d_s} + b$. Then*

$$\left|N(b) - q^{sk}\right| \leq \begin{cases} q^{\frac{sk}{2}}(q-1)I_k(\vec{d}), & \text{if } \operatorname{Tr}_{q^k/q}(b) = 0 \\ q^{\frac{sk+1}{2}}\prod_{i=1}^{s}(d_i - 1) - q^{\frac{sk}{2}}\left(q^{\frac{1}{2}} - 1\right) I_k(\vec{d}), & \text{if } \operatorname{Tr}_{q^k/q}(b) \neq 0 \end{cases} \tag{5.6}$$

The extent of the improvement depend on the exponents $d_1, \ldots, d_s$, q and k. One can readily verify that $0 \leq I_k(\vec{d}) \leq \prod_{i=1}^{s}(d_i - 1)$, but is hard to give a precise estimate for $I_k(\vec{d})$. The case where $k = 1$, for example, is extensively studied in Chapter 6 of [50]. Along this chapter, we will present necessary and sufficient conditions in which such bounds are attained (see Section 5.3). As a consequence of this characterization of $I_k(\vec{d})$, we obtain the following result.

Corollary 5.3. *If some $d_\alpha \in \{d_1, \ldots, d_s\}$ is coprime to each element of $\{v_k, d_1, \ldots, d_s\} \setminus \{d_\alpha\}$, then the number of $\mathbb{F}_{q^k}$-rational points on the affine hypersurface given by*

$$y^q - y = a_1 x_1^{d_1} + \cdots + a_s x_s^{d_s}$$

is equal to q^{sk}.

On the other hand, we will see that the case where $I_k(\vec{d})$ is maximal yields cases where Weil's bound is attained. Indeed, one of our aims in this chapter is to characterize the maximal and minimial Artin-Schreier hypersurfaces. Before doing so, we provide a family of hypersurfaces

whose number of $\mathbb{F}_q$-rational points can be explicty given. This family of hypersurfaces satisfy a very natural condition on the exponents, which is being (p, r_i)-admissible (see Chapter 1).

Note that if an integer d is (p, r)-admissible, then $2r$ is the order of p in $(\mathbb{Z}/d\mathbb{Z})^\times$. In addition, $d \mid (q^k - 1)$ implies $2r \mid nk$. Along the chapter, the following definition will be important.

Definition 5.4. *For $c \in \mathbb{F}_{q^k}$, we define the integer*

$$\Delta(c) = \begin{cases} -1, & \text{if } \mathrm{Tr}_{q^k/p}(c) \neq 0 \\ p-1, & \text{if } \mathrm{Tr}_{q^k/p}(c) = 0. \end{cases}$$

The following result provides a formula for the number of rational points on Artin-Schreier hypersurfaces.

Theorem 5.5. *Let $d_1, \ldots, d_s$ be integers not all equal to 2, and let $N(b)$ denote the number of $\mathbb{F}_{q^k}$-rational points on the affine hypersurface given by*

$$\mathcal{X} : y^q - y = a_1 x_1^{d_1} + \cdots + a_s x_s^{d_s} + b. \tag{5.7}$$

Assume that d_i is (p, r_i)-admissible, and let $u_i = \frac{p^{r_i}+1}{d_i}(d_i - 1)$. Then

$$N(b) = q^{sk} + q^{\frac{sk}{2}} \sum_{j=1}^{v} \Delta(\gamma_j b) \prod_{i=1}^{s} \varepsilon_i (1 - d_i)^{\delta_{i,j}}, \tag{5.8}$$

where $\varepsilon_i = (-1)^{\frac{nk}{2r_i}}$, and

$$\delta_{i,j} = \begin{cases} 1, & \text{if } \chi_{d_i}(\gamma_j a_i) = \varepsilon_i^{u_i} \\ 0, & \text{if } \chi_{d_i}(\gamma_j a_i) \neq \varepsilon_i^{u_i}. \end{cases}$$

Theorem 5.5 does not apply for $d_1 = \cdots = d_s = 2$, but the number of $\mathbb{F}_{q^k}$-rational points in this case will be determined in Section 5.7. Note that if $\mathrm{Tr}_{q^k/q}(b) = 0$, then (5.8) reads as follows

$$N(b) = q^{sk} + (p-1) q^{\frac{sk}{2}} \sum_{j=1}^{v} \prod_{i=1}^{s} \varepsilon_i (1 - d_i)^{\delta_{i,j}}. \tag{5.9}$$

In particular, this yields the following result, which also provides a new proof for the maximality of the curve $\mathcal{Y}_n$ in (5.4).

Corollary 5.6. *If $k \geq 3$ odd, then the hypersurface given by*

$$\mathcal{Y}_{k,s} : y^{q^2} - y = x_1^{\frac{q^k+1}{q+1}} + \cdots + x_s^{\frac{q^k+1}{q+1}} \tag{5.10}$$

is $\mathbb{F}_{q^{2k}}$-maximal.

More generally, considering cases in Theorem 5.5 for which $\delta_{i,j}$ does not depend on j, we have the following.

Corollary 5.7. *With the same notation as in Theorem 5.5, if $d_i \mid \left(\frac{q^k-1}{q-1}\right)$ for $i = 1, \ldots, s$, then*

$$N(b) = \begin{cases} q^{sk} - q^{\frac{sk}{2}} \prod_{i=1}^{s} \varepsilon_i (1 - d_i)^{\delta_i} & \text{if } \mathrm{Tr}_{q^k/q}(b) \neq 0 \\ q^{sk} + (q-1) q^{\frac{sk}{2}} \prod_{i=1}^{s} \varepsilon_i (1 - d_i)^{\delta_i} & \text{if } \mathrm{Tr}_{q^k/q}(b) = 0, \end{cases} \tag{5.11}$$

where $\delta_i = \delta_{i,j}$.

Note that if $\mathrm{Tr}_{q^k/q}(b) = 0$, then Corollary 5.7 gives sufficient conditions for having hypersurfaces attaining Weil's bound, and new examples thereof. The following result shows that such conditions are necessary.

Theorem 5.8. *Let $N(b)$ denote the number of $\mathbb{F}_{q^k}$-rational points on the affine hypersurface given by $y^q - y = a_1 x_1^{d_1} + \cdots + a_s x_s^{d_s} + b$. Then Weil's bound (5.2) is attained if and only if $\mathrm{Tr}_{q^k/q}(b) = 0$ and the following hold for $i = 1, \ldots, s$:*

(i) *d_i are (p, r_i)-admissible divisors of $\frac{q^k-1}{q-1}$*

(ii) *$\chi_{d_i}(a_i) = (-1)^{\frac{nku_i}{2r_i}}$, where $u_i = \frac{p^{r_i}+1}{d_i}(d_i - 1)$.*

Theorem 5.8 provided the number of $\mathbb{F}_q$-rational points of a wide class of Artin-Schreier hypersurfaces in the case where $\mathrm{Tr}_{q^k/q}(b) = 0$. Now, we turn our attention to the case $\mathrm{Tr}_{q^k/q}(b) \neq 0$.

Theorem 5.9. *With the same notation and hypothesis as in Theorem 5.5, let $D = \mathrm{lcm}(d_1, \ldots, d_s)$, $v_k = \frac{q^k-1}{q-1}$, and $\Gamma = \Gamma_k(\vec{d})$. Assume that $b' = \mathrm{Tr}_{q^k/q}(b) \neq 0$ and $a_1 = \cdots = a_s = a$. If $M = \frac{D}{\gcd(D, v_k)}$ is (p, r)-admissible and $u = \frac{p^r+1}{M}(M-1)$, then*

$$N(b) = q^{sk} - q^{\frac{sk}{2}}\theta \sum_{\vec{j}\in\Gamma} \left[\left(1 - \varepsilon^{1+u\sum_{i=1}^{s} j_i} q^{\frac{1}{2}} \right) \prod_{i=1}^{s} \varepsilon_i^{u_i j_i} \right] - q^{\frac{sk+1}{2}} \varepsilon\theta(-1)^s \prod_{i=1}^{s} (1 - d_i)^{\delta_{i,j}},$$

where $\varepsilon_i = (-1)^{\frac{nk}{2r_i}}$, $\varepsilon = (-1)^{\frac{n}{2r}}$, $\theta = (-1)^s \prod_{i=1}^{s} \varepsilon_i$, and

$$\delta_i = \begin{cases} 1, & \text{if } \chi_{d_i}(b'a^{-1}) = \varepsilon^u \varepsilon_i^{u_i} \\ 0, & \text{if } \chi_{d_i}(b'a^{-1}) \neq \varepsilon^u \varepsilon_i^{u_i}. \end{cases}$$

Note that if r be an integer such that $\frac{n}{2r}$ is even, and $b \in \mathbb{F}_{q^k}$ is such that $\mathrm{Tr}_{q^k/q}(b) = 1$, then the number of $\mathbb{F}_{q^k}$-rational points of

$$y^q - y = x_1^{\frac{p^r+1}{2}} + \cdots + x_s^{\frac{p^r+1}{2}} + b$$

attains bound (5.6). More generally, the following holds.

Corollary 5.10. *The bound in Theorem 5.2 is attained if the following hold.*

(i) *$a_1 = \cdots = a_s = a$*

(ii) *$\chi_{d_i}(b'a^{-1}) = 1$*

(iii) *d_i are (p, r_i)-admissible*

(iv) *$M = \frac{D}{\gcd(D, v_k)}$ is (p, r)-admissible*

(v) *$I_k(\vec{d}) \neq 0$*

(vi) *$\frac{n}{2r}$ and $\frac{p^{r_i}+1}{d_i}$ are even integers.*

5.2 First results

In this section, we provide expressions for the number of $\mathbb{F}_q$-rational points on a Artin-Schreier in terms of character sums. These results play an important role in the proof of our main results.

Proposition 5.11. *The number of $\mathbb{F}_{q^k}$-rational points on $y^q - y = a_1x_1^{d_1} + \cdots + a_sx_s^{d_s} + b$ is given by*

$$q^{sk} + \sum_{c\in\mathbb{F}_q^*} \psi(cb) \sum_{j_1=1}^{d_1-1} \cdots \sum_{j_s=1}^{d_s-1} \prod_{i=1}^{s} \overline{\chi_{d_i}}^{j_i}(ca_i)G(\chi_{d_i}^{j_i}),$$

where $G(\chi)$ denotes the Gauss sum of χ.

Proof. Let N be the number of points of $y^q - y = a_1x_1^{d_1} + \cdots + a_sx_s^{d_s} + b$ in $\mathbb{A}^{s+1}\left(\mathbb{F}_{q^k}\right)$. Let $\vec{x} = (x_1, \ldots, x_s)$. By the orthogonality relations of characters, we have

$$\begin{aligned} N &= \sum_{\vec{x}\in\mathbb{F}_{q^k}^s} \sum_{c\in\mathbb{F}_q} \psi(c(a_1x_1^{d_1} + \cdots + a_sx_s^{d_s} + b)) \\ &= q^{sk} + \sum_{c\in\mathbb{F}_q^*} \sum_{\vec{x}\in\mathbb{F}_{q^k}^s} \psi(c(a_1x_1^{d_1} + \cdots + a_sx_s^{d_s} + b)) \\ &= q^{sk} + \sum_{c\in\mathbb{F}_q^*} \psi(cb) \sum_{x_1\in\mathbb{F}_{q^k}} \psi(ca_1x_1^{d_1}) \cdots \sum_{x_s\in\mathbb{F}_{q^k}} \psi(ca_sx_s^{d_s}). \end{aligned}$$

It follows from Lemma 1.5 that

$$N = q^{sk} + \sum_{c\in\mathbb{F}_q^*} \psi(cb) \sum_{j_1=1}^{d_1-1} \cdots \sum_{j_s=1}^{d_s-1} \overline{\chi_{d_1}}^{j_1}(ca_1) \cdots \overline{\chi_{d_s}}^{j_s}(ca_s) \prod_{i=1}^{s} G(\chi_{d_i}^{j_i}),$$

which completes the proof. ∎

As a direct consequence of Proposition 5.11, we have the following result.

Corollary 5.12. *If $b' = \mathrm{Tr}_{q^k/q}(b) \neq 0$, then the number of $\mathbb{F}_{q^k}$-rational points on $y^q - y = a_1x_1^{d_1} + \cdots + a_sx_s^{d_s} + b$ is given by*

$$q^{sk} + \sum_{j_1=1}^{d_1-1} \cdots \sum_{j_s=1}^{d_s-1} G_q(\overline{\chi_{d_1}}^{j_1} \ldots \overline{\chi_{d_s}}^{j_s}) \prod_{i=1}^{s} \chi_{d_i}^{j_i}(b'a_i^{-1})G(\chi_{d_i}^{j_i}),$$

where $G(\chi)$ denotes the Gauss sum of χ over $\mathbb{F}_{q^k}$, and $G_q(\overline{\chi_{d_1}}^{j_1} \ldots \overline{\chi_{d_s}}^{j_s})$ the Gauss sum of $\overline{\chi_{d_1}}^{j_1} \ldots \overline{\chi_{d_s}}^{j_s}$ over $\mathbb{F}_q$.

At this point, we are able to present an improvement of Weil's bound, that is stated in Theorem 5.2.

Proof of Theorem 5.2. Let Γ and B be as in the proof of Theorem 5.9. Assume that $\mathrm{Tr}_{q^k/q}(b) = 0$. By Proposition 5.11 and Lemma 1.3, it follows that

$$N(b) = q^{sk} + \sum_{\vec{j}\in\Gamma} \prod_{i=1}^{s} \left(\overline{\chi_{d_i}}^{j_i}(a_i)G(\chi_{d_i}^{j_i})\right) \sum_{c\in\mathbb{F}_q^*} \overline{\chi_{d_1}^{j_1} \cdots \chi_{d_s}^{j_s}}(c).$$

We recall that $|\chi_{d_i}^{j_i}(b'a_i^{-1})| = 1$ for all j_i and observe that $\vec{j} \in \Gamma$ implies $\sum_{c\in\mathbb{F}_q^*} \overline{\chi_{d_1}^{j_1} \cdots \chi_{d_s}^{j_s}}(c) = 0$. Therefore, Theorem 1.6 yields

$$|N(b) - q^{sk}| \leq (q-1) \sum_{\vec{j}\in\Gamma} \prod_{i=1}^{s} |\overline{\chi_{d_i}}^{j_i}(a_i)| |G(\chi_{d_i}^{j_i})| \leq (q-1) q^{\frac{sk}{2}} I_k(\vec{d}).$$

Now, we assume that $\mathrm{Tr}_{q^k/q}(b) \neq 0$. From Corollary 5.12, we have that

$$\left|N(b) - q^{sk}\right| = \sum_{j_1=1}^{d_1-1} \cdots \sum_{j_s=1}^{d_s-1} G_q(\overline{\chi_{d_1}}^{j_1} \cdots \overline{\chi_{d_s}}^{j_s}) \prod_{i=1}^{s} \chi_{d_i}^{j_i}(b'a_i^{-1}) G(\chi_{d_i}^{j_i})$$

If $\vec{j} \in \Gamma$, then $G_q(\overline{\chi_{d_1}}^{j_1} \cdots \overline{\chi_{d_s}}^{j_s}) = -1$. If $\vec{j} \in B\backslash\Gamma$, then Theorem 1.6 yields

$$|G_q(\overline{\chi_{d_1}}^{j_1} \cdots \overline{\chi_{d_s}}^{j_s})| = q^{\frac{1}{2}}.$$

Furthermore, $|\chi_{d_i}^{j_i}(b'a_i^{-1})| = 1$ for all j_i. Therefore, it follows from Theorem 1.6 that

$$\begin{aligned}
\left|N(b) - q^{sk}\right| &\leq \sum_{j_1=1}^{d_1-1} \cdots \sum_{j_s=1}^{d_s-1} |G_q(\overline{\chi_{d_1}}^{j_1} \cdots \overline{\chi_{d_s}}^{j_s})| \prod_{i=1}^{s} |\chi_{d_i}^{j_i}(b'a_i^{-1})| |G(\chi_{d_i}^{j_i})| \\
&\leq \sum_{j_1=1}^{d_1-1} \cdots \sum_{j_s=1}^{d_s-1} |G_q(\overline{\chi_{d_1}}^{j_1} \cdots \overline{\chi_{d_s}}^{j_s})| \prod_{i=1}^{s} q^{\frac{k}{2}} \\
&\leq \sum_{\vec{j}\in\Gamma} q^{\frac{sk}{2}} + \sum_{\vec{j}\in B\backslash\Gamma} q^{\frac{sk+1}{2}} \\
&\leq \sum_{\vec{j}\in\Gamma} q^{\frac{sk}{2}} \left(1 - q^{\frac{1}{2}}\right) + \sum_{\vec{j}\in B} q^{\frac{sk+1}{2}} \\
&\leq q^{\frac{sk+1}{2}} \prod_{i=1}^{s} (d_i - 1) - q^{\frac{sk}{2}} \left(q^{\frac{1}{2}} - 1\right) I_k(\vec{d}),
\end{aligned}$$

which completes the proof. ■

5.3 On bounds for $I_k(\vec{d})$

In this section, we study when the constant $I_k(\vec{d})$ attains its the upper and lower bounds. For the upper bound ($\prod_{i=1}^{s}(d_i - 1)$), we have the followin result.

Proposition 5.13. *For the exponents $d_1, \ldots, d_s > 1$, let $\mathcal{I} = \{i : d_i > 2\}$. Then $I_k(\vec{d}) = \prod_{i=1}^{s}(d_i - 1)$ if and only if $(s - |\mathcal{I}|)v_k$ is even and d_i divides v_k for all $i \in \mathcal{I}$.*

Proof. Suppose $I_k(\vec{d}) = \prod_{i=1}^{s}(d_i - 1)$, that is, $v_k \sum_{i=1}^{s} \frac{j_i}{d_i} \equiv 0 \pmod 1$ for all $(j_1, \ldots, j_s) \in B$. In particular,

$$v_k \sum_{i=1}^{s} \frac{1}{d_i} \equiv 0 \pmod 1 \quad \text{and } v_k \left(\frac{1}{d_\alpha} + \sum_{i=1}^{s} \frac{1}{d_i}\right) \equiv 0 \pmod 1,$$

for all $\alpha \in \mathcal{I}$. It then follows that $\frac{v_k}{d_\alpha} \equiv 0 \pmod 1$, that is, d_α divides v_k for all $\alpha \in \mathcal{I}$. In addition, the latter condition implies $v_k \cdot \frac{s-|\mathcal{I}|}{2} \equiv 0 \pmod 1$, and then $(s - |\mathcal{I}|)v_k$ is even. The converse is clear. ■

Now we characterize the conditions in which $I_k(\vec{d})$ attains the lower bound (namely, when $I_k(\vec{d}) = 0$).

Proposition 5.14. *$I_k(\vec{d}) = 0$ if and only if one of the following holds:*

- *for some d_i, $\gcd(d_i, v_k d_1 \cdots d_s/d_i) = 1$*
- *if $d_{i_1}, \ldots, d_{i_t}$ $(1 \le i_1 < \cdots < i_t \le s)$ is the set of all even integers among $\{d_1, \ldots, d_s\}$, then $2 \nmid t$, $d_{i_1}/2, \ldots, d_{i_t}/2$ are pairwise coprime, and d_{i_j} is coprime to v_k and to any odd number in $\{d_1, \ldots, d_s\}$ $(j = 1, \ldots, t)$.*

Proof. We observe that the number of solutions $(j_1, \ldots, j_s)$ with $1 \le j_i < d_i$ of the equation

$$v_k \left(\frac{j_1}{d_1} + \cdots + \frac{j_s}{d_s} \right) \equiv 0 \pmod 1,$$

which equals the number of solutions $\vec{j} = (j_1, \ldots, j_s)$ with $1 \le j_i < d_i$ of the equation

$$\frac{j_1}{e_1} + \cdots + \frac{j_s}{e_s} \equiv 0 \pmod 1, \tag{5.12}$$

where $e_i = d_i / \gcd(d_i, v_k)$. Let S denote the set of solutions $\vec{j}$ of Equation (5.12) and let $B = \{i = 1, \ldots, s : \gcd(d_i, v_k) > 1\}$. For $A \subset B$, let

$$S_A = \{\vec{j} \in S : j_i \equiv 0 \pmod{e_i} \text{ if and only if } i \in A\}.$$

We can stratify the set S of solutions of Equation (5.12) as follows:

$$S = \bigcup_{A \subset B} S_A.$$

One can easily verify that

$$|S_A| = \prod_{i \in A} \left(\tfrac{d_i}{e_i} - 1\right) \prod_{\substack{i=1,\ldots,s \\ i \notin A}} \left(\tfrac{d_i}{e_i}\right) I_{k,A}(\vec{e}),$$

where $\vec{e} = (e_1, \ldots, e_s)$, and $I_{k,A}(\vec{e})$ denotes the number of solutions $\vec{j} = (j_1, \ldots, j_s)$, with $j_i = 0$ for all $i \in A$ and $1 \le j_i < e_i$ for $i \notin A$, of the equation

$$\frac{j_1}{e_1} + \cdots + \frac{j_s}{e_s} \equiv 0 \pmod 1.$$

Therefore,

$$|S| = \sum_{A \subset B} \sum_{i \in A} \left(\tfrac{d_i}{e_i} - 1\right) \sum_{\substack{i=1,\ldots,s \\ i \notin A}} \left(\tfrac{d_i}{e_i}\right) I_{k,A}(\vec{e}). \tag{5.13}$$

In sum, we have shown that $I_k(\vec{d}) = 0$ if and only if $I_{k,A}(\vec{e}) = 0$ for all $A \subset B$.

Suppose $I_k(\vec{d}) = 0$. Since $I_{k,\varnothing}(\vec{e}) = 0$, Lemma 4.5 states that one (or both) of the followings condition holds:

1. for some e_i, $\gcd(e_i, e_1 \cdots e_s/e_i) = 1$
2. if $e_{i_1}, \ldots, e_{i_t}$ $(1 \le i_1 < \cdots < i_t \le s)$ is the set of all even integers among $\{e_1, \ldots, e_s\}$, then $2 \nmid t$, $e_{i_1}/2, \ldots, e_{i_t}/2$ are pairwise prime, and e_{i_ℓ} is prime to any odd number in the set $\{e_1, \ldots, e_s\}$ $(\ell = 1, \ldots, t)$.

Assume that conditions (1) and (2) hold simultaneously and let $C_1 = \{i = 1, \ldots, s : \gcd(e_i, e_1 \cdots e_s/e_i) = 1\}$ and $C_2 = \{i_1, \ldots, i_t\}$. If $B \cap C_2 = \varnothing$, then e_{i_ℓ} is coprime to v_k for each $\ell = 1, \ldots, t$, which implies that the second condition the statement of our result holds. Otherwise, assume without loss of generality that $e_{i_1} \in B \cap C_2$ and et $A = B \cap C_1 \cup \{e_{i_1}\}$. Since $I_{k,A}(\vec{e}) = 0$, it follows from Lemma 4.5 that there exists an integer $u \in \{1, \ldots, s\}$ such that $\gcd(d_u, d_1 \cdots d_s/d_u) = 1$ and $u \notin B$, which implies $\gcd(d_u, v_k d_1 \cdots d_s/d_u) = 1$.

The cases where only one of the two conditions holds follow similarly. The converse follows directly by employing Lemma 4.5 in Equation (5.13). ■

Corollary 5.3 follows as a direct consequence of Theorem 5.2 and Proposition 5.14.

5.4 Expressions for the number N

In this section, we provide expressions for the number of $\mathbb{F}_q$-rational points on Artin-Schreier hypersurfaces that satisfy some hypothesis on the exponents, namely, each d_i is (p, r_i)-admissible.

5.4.1 Proof of Theorem 5.5

From Proposition 5.11, we have that

$$N(b) = q^{sk} + \sum_{c \in \mathbb{F}_q^*} \psi(cb) \sum_{j_1=1}^{d_1-1} \cdots \sum_{j_s=1}^{d_s-1} \prod_{i=1}^{s} \overline{\chi_{d_i}}^{j_i}(ca_i) G(\chi_{d_i}^{j_i}).$$

Since $\gamma_1, \ldots, \gamma_v$ are coset representatives of $\mathbb{F}_q^*/\mathbb{F}_p^*$, it follows that

$$N = q^{sk} + \sum_{j=1}^{v} \sum_{\ell=1}^{p-1} \psi^\ell(\gamma_j b) \sum_{j_1=1}^{d_1-1} \cdots \sum_{j_s=1}^{d_s-1} \prod_{i=1}^{s} \overline{\chi_{d_i}}^{j_i}(\ell \gamma_j a_i) G(\chi_{d_i}^{j_i}).$$

Let $u_i = \frac{p^{r_i}+1}{d_i}(d_i - 1)$. From Theorems 1.7 and 1.16,

$$N(b) = q^{sk} + q^{\frac{sk}{2}} \sum_{j=1}^{v} \sum_{\ell=1}^{p-1} \psi^\ell(\gamma_j b) \sum_{j_1=1}^{d_1-1} \cdots \sum_{j_s=1}^{d_s-1} \prod_{i=1}^{s} \left[-\overline{\chi_{d_i}}^{j_i}(\ell \gamma_j a_i) \varepsilon_i (-1)^{\frac{nku_i j_i}{2r_i}} \right],$$

where $\varepsilon_i = (-1)^{\frac{nk}{2r_i}}$. Let us recall that $2r_i$ is the order of p in $(\mathbb{Z}/d\mathbb{Z})^\times$. Since $d_i | (q^k - 1)$, it follows that $(p^{2r_i} - 1) | (q^k - 1)$, and then $(p^{r_i} + 1) | \left(\frac{q^k-1}{p^{r_i}-1}\right)$. In particular, $d_i | \left(\frac{q^k-1}{p-1}\right)$, which implies that $\chi_{d_i}(\ell) = 1$ for all $\ell \in \mathbb{F}_p$. Therefore,

$$\begin{aligned} N(b) &= q^{sk} + q^{\frac{sk}{2}} \sum_{j=1}^{v} \left[\prod_{i=1}^{s} \varepsilon_i \sum_{j_i=1}^{d_i-1} - \left(\overline{\chi_{d_i}}(\gamma_j a_i)(-1)^{\frac{nku_i}{2r_i}} \right)^{j_i} \right] \sum_{\ell=1}^{p-1} \psi^\ell(\gamma_j b) \\ &= q^{sk} + q^{\frac{sk}{2}} \sum_{j=1}^{v} \left[\prod_{i=1}^{s} \varepsilon_i \sum_{j_i=1}^{d_i-1} - (\overline{\chi_{d_i}}(\gamma_j a_i) \varepsilon_i^{u_i})^{j_i} \right] \sum_{\ell=1}^{p-1} \psi^\ell(\gamma_j b). \end{aligned}$$

Let ψ_p be the canonical additive character of $\mathbb{F}_p$. From Lemma 1.3,

$$\sum_{\ell=1}^{p-1} \psi^\ell(\gamma_j b) = \sum_{\ell=1}^{p-1} \psi_p(\ell \operatorname{Tr}_{q^k/p}(\gamma_j b)) = \begin{cases} -1, & \text{if } \operatorname{Tr}_{q^k/p}(\gamma_j b) \neq 0 \\ p-1, & \text{if } \operatorname{Tr}_{q^k/p}(\gamma_j b) = 0, \end{cases}$$

and Lemma 1.4 gives

$$\sum_{j_i=1}^{d_i-1} -(\overline{\chi_{d_i}}(\gamma_j a_i)\varepsilon_i^{u_i})^{j_i} = \begin{cases} 1, & \text{if } \chi_{d_i}(\gamma_j a_i) \neq \varepsilon_i^{u_i} \\ 1-d, & \text{if } \chi_{d_i}(\gamma_j a_i) = \varepsilon_i^{u_i}. \end{cases}$$

Therefore,

$$N(b) = q^{sk} + q^{\frac{sk}{2}} \sum_{j=1}^{v} \left[\prod_{i=1}^{s} \varepsilon_i (1-d_i)^{\delta_{i,j}} \right] \Delta(\gamma_j b),$$

where

$$\delta_{i,j} = \begin{cases} 1, & \text{if } \chi_{d_i}(\gamma_j a_i) = \varepsilon_i^{u_i} \\ 0, & \text{if } \chi_{d_i}(\gamma_j a_i) \neq \varepsilon_i^{u_i}, \end{cases}$$

and this completes the proof. ■

We observe that the hypothesis of (p, r_i)-admissibility was essential in our approach. Under this hypothesis, we can present a proof for the maximality of some particular families of hypersurfaces.

5.4.2 Proof of Corollary 5.6

Throughout this proof, for a divisor d of $q^{2k}-1$, we let χ_d be a multiplicative character of $\mathbb{F}_{q^{2k}}$ of order d. Let $d = \frac{q^k+1}{q+1}$. We note that d is (p,r)-admissible for a divisor r of nk such that $\frac{nk}{r}$ is odd. Therefore, Theorem 5.5 implies that the number N of $\mathbb{F}_{q^{2k}}$-rational points on $\mathcal{Y}_{k,s}$ is given by

$$N = q^{2sk} + (p-1)q^{sk} \sum_{j=1}^{v} \varepsilon (1-d_i)^{s\delta_j}$$

where $\varepsilon = (-1)^{\frac{2nk}{2r}}$, $v = \frac{q^2-1}{p-1}$ and

$$\delta_j = \begin{cases} 1, & \text{if } \chi_{d_i}(\gamma_j) = \varepsilon_i^{u_i} \\ 0, & \text{if } \chi_{d_i}(\gamma_j) \neq \varepsilon_i^{u_i}. \end{cases}$$

Since $\frac{nk}{r}$ is odd, $d \mid \frac{q^k-1}{q-1}$ and $\gamma_j \in \mathbb{F}_q$ for all $j = 1, \ldots, v$, it follows that $\varepsilon = 1$ and $\delta_j = 1$ for all $j = 1, \ldots, v$. Then

$$N = q^{2sk} + (q^2-1)(d-1)^s q^{sk},$$

which proves that $\mathcal{Y}_{k,s}$ is maximal. ■

Lemma 5.15. *Let $b \in \mathbb{F}_{q^k}^*$ be such that $\mathrm{Tr}_{q^k/q}(b) \neq 0$, and let*

$$\Lambda = \{j \in \{1, \ldots, v\} : \mathrm{Tr}_{q^k/p}(\gamma_j b) \neq 0\}.$$

Then

$$|\Lambda| = \frac{q - q/p}{p-1}.$$

Proof. For $c \in \mathbb{F}_p$, let $\Lambda_c = \{j \in \{1, \ldots, v\} : \mathrm{Tr}_{q^k/p}(c\gamma_j b) \neq 0\}$. Since $c \in \mathbb{F}_p^*$, we have that $\mathrm{Tr}_{q^k/p}(c\gamma_j b) \neq 0$ if and only if $\mathrm{Tr}_{q^k/p}(\gamma_j b) \neq 0$, and then $|\Lambda| = |\Lambda_c|$. We recall that $\mathrm{Tr}_{q^k/p}(c\gamma_j b) = \mathrm{Tr}_{q/p}(c\gamma_j \mathrm{Tr}_{q^k/q}(b))$. Since

$$\bigcup_{c \in \mathbb{F}_p^*} \bigcup_{j=1}^{v} \{c\gamma_j\} = \mathbb{F}_q^*,$$

it follows that

$$\bigcup_{c\in\mathbb{F}_p^*} |\Lambda_c| = |\{w \in \mathbb{F}_q : \mathrm{Tr}_{q/p}(w\,\mathrm{Tr}_{q^k/q}(b))\}| = q - q/p.$$

After observing that $|\Lambda_c| = |\Lambda_1| = |\Lambda|$ for all $c \in \mathbb{F}_p^*$, the result follows. ■

Now, assuming that $d_i \mid \left(\frac{q^k-1}{q-1}\right)$, we are able to prove Corollary 5.7, which yields families of Artin-schreier hypersurfaces whose number of $\mathbb{F}_q$-rational points does not depend on the basis field $\mathbb{F}_q$.

5.4.3 Proof of Corollary 5.7

Let β be a primitive element of $\mathbb{F}_{q^k}$ and $\gamma = \beta^{\frac{q^k-1}{q-1}}$. Assume that $\mathrm{Tr}_{q^k/q}(b) \neq 0$. Since $d_i \left| \left(\frac{q^k-1}{q-1}\right)\right.$, it follows that

$$\chi_{d_i}(\gamma_j) = \chi_{d_i}\left(\beta^{j\frac{q^k-1}{q-1}}\right) = 1$$

for all positive integer j. Therefore, Theorem 5.5 implies that

$$N(b) = q^{sk} + q^{\frac{sk}{2}}\left[(p-1)\,(v - |\Lambda|) - |\Lambda|\right]\prod_{i=1}^{s}\varepsilon_i(1-d_i)^{\delta_i},$$

where $\Lambda = \{j \in \{1\ldots,v\} : \mathrm{Tr}_{q^k/p}(\gamma_j b) \neq 0\}$, $\varepsilon_i = (-1)^{\frac{nk}{2r_i}}$, and

$$\delta_i = \begin{cases} 1, & \text{if } \chi_{d_i}(a_i) = \varepsilon_i^{u_i} \\ 0, & \text{if } \chi_{d_i}(a_i) \neq \varepsilon_i^{u_i}. \end{cases}$$

Now, the result follows directly from Lemma 5.15. The case $\mathrm{Tr}_{q^k/q}(b) = 0$ is obtained similarly. ■

5.5 The Weil bound

In this section, we establish necessary and sufficient conditions for Artin-Schreier hypersurfaces $\mathcal{X} \subseteq \mathbb{A}^{s+1}\left(\mathbb{F}_{q^k}\right)$ given by (5.1) to be maximal or minimal and present an improvement of Weil's bound when $\mathrm{Tr}_{q^k/q}(b) \neq 0$. We recall from Definition 1.13 that

$$\Omega = \{z \in \mathbb{C} : \text{ there exists an integer } n \text{ such that } z^n \in \mathbb{R}\}.$$

For χ a nontrivial multiplicative character, we note that $G(\chi)$ is a pure Gauss sum if and only if $G(\chi) = z \in \Omega$.

Lemma 5.16. *Let $d_1,\ldots,d_s$ be divisors of q^k-1. If $G(\chi_{d_1}^{j_1})\cdots G(\chi_{d_s}^{j_s}) \in \Omega$ for all $1 \leq j_1 \leq (d_1-1),\ldots,1 \leq j_s \leq (d_s-1)$, then $G(\chi_{d_i}^{j_i})$ is pure for all $j_i \in \mathbb{Z}$, $i = 1,\ldots,s$.*

Proof. Let $g(j_1,\ldots,j_s) = G(\chi_{d_1}^{j_1})\cdots G(\chi_{d_s}^{j_s})$. Fixing an integer $j_i \in \{1,\ldots,d_i-1\}$, note that

$$g(1,\ldots,1,j_i,1,\ldots,1), g(-1,\ldots,-1,j_i,-1,\ldots,-1) \in \Omega.$$

From Theorem 1.6, it follows that

$$G(\chi_{d_i}^{j_i})^2 q^{k(s-1)} \prod_{\substack{l=1 \\ l\neq i}}^{s} \chi_{d_l}(-1) = g(1,\ldots,j_i,\ldots,1)g(-1,\ldots,j_i,\ldots,-1) \in \Omega,$$

which implies $G(\chi_{d_i}^{j_i}) \in \Omega$, that is, $G(\chi_{d_i}^{j_i})$ is pure. ■

5.5.1 Proof of Theorem 5.8

Let us assume that Weil's bound is attained. Then by Proposition 5.11 we have that

$$\sum_{j_1=1}^{d_1-1} \cdots \sum_{j_s=1}^{d_s-1} \prod_{i=1}^{s} \overline{\chi_{d_i}}^{j_i}(ca_i) G(\chi_{d_i}^{j_i}) \in \left\{ q^{\frac{sk}{2}}, -q^{\frac{sk}{2}} \right\}$$

for $c \in \mathbb{F}_q^*$ and $j_i = 1,\ldots,d_i-1$. In particular, by Lemma 5.16, if $i \in \{1,\ldots,s\}$ is an integer such that $d_i \neq 2$, then $G(\chi_{d_i}^{j_i})$ is pure for $j_i = 1,\ldots,d_i-1$, with $i = 1,\ldots,s$. Therefore, by Theorem 1.16, it follows that there exists an integer r_i such that $d_i|(p^{r_i}+1)$. Accordingly, being under the hypotheses of Theorem 5.5,

$$N(b) = q^{sk} + q^{\frac{sk}{2}} \sum_{j=1}^{v} \Delta(\gamma_j b) \prod_{i=1}^{s} \varepsilon_i (1-d_i)^{\delta_{i,j}}.$$

Since Weil's bound is attained, we have that $\Delta(\gamma_j b) = p-1$ and $\chi_{d_i}(\gamma_j a_i) = \varepsilon_i^{u_i}$ for $j = 1,\ldots,v$ and $i = 1,\ldots,s$. It can be readily verified that these conditions are equivalent to the following:

- $\mathrm{Tr}_{q^k/q}(b) = 0$
- $d_i \left| \left(\frac{q^k-1}{q-1} \right) \right.$
- $\chi_{d_i}(a_i) = \varepsilon_i^{u_i}$,

where $u_i = \frac{p^{r_i}+1}{d_i}(d_i-1)$, and $i = 1,\ldots,s$. The converse is straightforward. ■

5.6 The nonzero trace case

In this section, we focus on a special case where $\mathrm{Tr}_{q^k/q}(b) \neq 0$ and some suitable conditions are satisfied. In particular, these conditions are closely related to the maximality and minimality of the hypersurface, as we will se in Corollary 5.10.

5.6.1 Proof of Theorem 5.9

From Corollary 5.12, we have

$$N(b) = q^{sk} + \sum_{j_1=1}^{d_1-1} \cdots \sum_{j_s=1}^{d_s-1} G_q(\overline{\chi_{d_1}}^{j_1} \ldots \overline{\chi_{d_s}}^{j_s}) \prod_{i=1}^{s} \chi_{d_i}^{j_i}(b'a^{-1}) G(\chi_{d_i}^{j_i}).$$

Let $u_i = \frac{p^{r_i}+1}{d_i}(d_i-1)$ and

$$B = \{(j_1,\ldots,j_s) \in \mathbb{Z}^s : 1 \leq j_i < d_i \text{ for } i = 1,\ldots,s\}.$$

From Theorems 1.7 and 1.16, it follows that

$$N(b) = q^{sk} + q^{\frac{sk}{2}} \sum_{\vec{j} \in B} G_q(\overline{\chi_{d_1}}^{j_1} \cdots \overline{\chi_{d_s}}^{j_s}) \prod_{i=1}^{s} \left[-\chi_{d_i}^{j_i}(b'a^{-1}) \varepsilon_i (-1)^{\frac{nku_ij_i}{2r_i}} \right],$$

where $\varepsilon_i = (-1)^{\frac{nk}{2r_i}}$, $\vec{j} = (j_1, \ldots, j_s)$. Set $S(\vec{j}) = \prod_{i=1}^{s} \left[-\chi_{d_i}^{j_i}(b'a^{-1}) \varepsilon_i (-1)^{\frac{nku_ij_i}{2r_i}} \right]$, and let $\Gamma = \Gamma_k(\vec{d})$. Observe that $\vec{j} \in \Gamma$ if and only if $\overline{\chi_{d_1}}^{j_1} \cdots \overline{\chi_{d_s}}^{j_s}$ is the trivial multiplicative character over $\mathbb{F}_q^*$. Therefore,

$$\begin{aligned} N(b) &= q^{sk} + q^{\frac{sk}{2}} \sum_{\vec{j} \in B} G_q(\overline{\chi_{d_1}}^{j_1} \cdots \overline{\chi_{d_s}}^{j_s}) S(\vec{j}) \\ &= q^{sk} + q^{\frac{sk}{2}} \sum_{\vec{j} \in \Gamma} G_q(\overline{\chi_{d_1}}^{j_1} \cdots \overline{\chi_{d_s}}^{j_s}) S(\vec{j}) + q^{\frac{sk}{2}} \sum_{\vec{j} \in B \setminus \Gamma} G_q(\overline{\chi_{d_1}}^{j_1} \cdots \overline{\chi_{d_s}}^{j_s}) S(\vec{j}) \\ &= q^{sk} - q^{\frac{sk}{2}} \sum_{\vec{j} \in \Gamma} S(\vec{j}) + q^{\frac{sk}{2}} \sum_{\vec{j} \in B \setminus \Gamma} G_q(\overline{\chi_{d_1}}^{j_1} \cdots \overline{\chi_{d_s}}^{j_s}) S(\vec{j}). \end{aligned}$$

Since $M = \frac{D}{\gcd(D, v_k)}$ is (p, r)-admissible, it follows from Theorems 1.7 and 1.16 that

$$N(b) = q^{sk} - q^{\frac{sk}{2}} \sum_{\vec{j} \in \Gamma} S(\vec{j}) - q^{\frac{sk+1}{2}} \sum_{\vec{j} \in B \setminus \Gamma} S(\vec{j}) \varepsilon^{1 + \sum_{i=1}^{s} uj_i},$$

where $\varepsilon = (-1)^{\frac{n}{2r}}$, and then

$$N(b) = q^{sk} - q^{\frac{sk}{2}} \sum_{\vec{j} \in \Gamma} \left(1 - \varepsilon^{1 + \sum_{i=1}^{s} uj_i} q^{\frac{1}{2}} \right) S(\vec{j}) - q^{\frac{sk+1}{2}} \sum_{\vec{j} \in B} S(\vec{j}) \varepsilon^{1 + \sum_{i=1}^{s} uj_i}.$$

Since $\vec{j} \in \Gamma$ implies that $\overline{\chi_{d_1}}^{j_1} \cdots \overline{\chi_{d_s}}^{j_s}$ is the trivial multiplicative character over $\mathbb{F}_q^*$, if follows from the definition of $S(\vec{j})$ that

$$N(b) = q^{sk} - q^{\frac{sk}{2}} \theta \sum_{\vec{j} \in \Gamma} \left(1 - \varepsilon^{1 + \sum_{i=1}^{s} uj_i} q^{\frac{1}{2}} \right) (-1)^{\sum_{i=1}^{s} \frac{nku_ij_i}{2r_i}} - q^{\frac{sk+1}{2}} \sum_{\vec{j} \in B} S(\vec{j}) \varepsilon^{1 + \sum_{i=1}^{s} uj_i},$$

where $\theta = (-1)^s \prod_{i=1}^{s} \varepsilon_i$. By the same arguments used in the proof of Theorem 5.5, we obtain that

$$N(b) = q^{sk} - q^{\frac{sk}{2}} \theta \sum_{\vec{j} \in \Gamma} \left(1 - \varepsilon^{1 + \sum_{i=1}^{s} uj_i} q^{\frac{1}{2}} \right) (-1)^{\sum_{i=1}^{s} \frac{nku_ij_i}{2r_i}} - q^{\frac{sk+1}{2}} \varepsilon \prod_{i=1}^{s} \varepsilon_i (1 - d_i)^{\delta_{i,j}},$$

where $\varepsilon_i = (-1)^{\frac{nk}{2r_i}}$ and

$$\delta_{i,j} = \begin{cases} 1, & \text{if } \chi_{d_i}(b'a^{-1}) = \varepsilon^u \varepsilon_i^{u_i} \\ 0, & \text{if } \chi_{d_i}(b'a^{-1}) \neq \varepsilon^u \varepsilon_i^{u_i}, \end{cases}$$

which completes the proof of our assertion. ■

From Theorem 5.9, we obtain some sufficient conditions for a Artin-Schreier being maximal or minimal with respect to the bound presented in Theorem 5.2.

5.6.2 Proof of Corollary 5.10

By Theorem 5.9, it follows that

$$N(b) = q^{sk} - q^{\frac{sk}{2}}\theta \sum_{\vec{j}\in\Gamma} \left(1 - q^{\frac{1}{2}}\right) - q^{\frac{sk+1}{2}}\theta(-1)^s \prod_{i=1}^{s}(1-d_i),$$

where $\varepsilon_i = (-1)^{\frac{nk}{2r_i}}$ and $\theta = (-1)^s \prod_{i=1}^{s} \varepsilon_i$. Therefore,

$$N(b) = q^{sk} - \theta q^{\frac{sk}{2}} \left[- \left(q^{\frac{1}{2}} - 1\right) I_k(\vec{d}) + q^{\frac{1}{2}} \prod_{i=1}^{s}(d_i - 1) \right],$$

which proves our assertion. ■

We believe that the conditions presented in Corollary 5.10 are also necessary for a Artin-Schreier hypersurface to attain the Theorem 5.2 bound, but a proof for this remains being an open problem.

5.7 The case $d_1 = \cdots = d_s = 2$

In this section, we determine the number of $\mathbb{F}_q$-rational points on the hypersurface given by (5.1) in the case where $d_1 = \cdots = d_s = 2$. Let us recall that i denotes the imaginary unity and the integer n is such that $q = p^n$.

Theorem 5.17. *Let $N(b)$ denote the number of $\mathbb{F}_{q^k}$-rational points on the hypersurface $y^q - y = a_1x_1^2 + \cdots + a_sx_s^2 + b$. Let $\epsilon = \mathrm{i}$ if $p \equiv 3 \pmod 4$, and $\epsilon = 1$ otherwise. If either s or k is even, then*

$$N(b) = \begin{cases} q^{sk} + (-1)^{s(nk+1)}\epsilon^{snk} q^{\frac{sk}{2}} \chi_2(a_1 \dots a_s)(q-1), & \text{if } \mathrm{Tr}_{q^k/q}(b) = 0 \\ q^{sk} - (-1)^{s(nk+1)}\epsilon^{snk} q^{\frac{sk}{2}} \chi_2(a_1 \dots a_s), & \text{if } \mathrm{Tr}_{q^k/q}(b) \neq 0. \end{cases}$$

If both s and k are odd, then

$$N(b) = \begin{cases} q^{sk}, & \text{if } \mathrm{Tr}_{q^k/q}(b) = 0 \\ q^{sk} + (-1)^{s(nk+1)+n+1}\epsilon^{snk+n} q^{k\frac{s+1}{2}} \chi_2(a_1 \dots a_s \,\mathrm{Tr}_{q^k/q}(b)), & \text{if } \mathrm{Tr}_{q^k/q}(b) \neq 0. \end{cases}$$

Proof. Proposition 5.11 and Theorem 1.7 entail

$$\begin{aligned} N(b) &= q^{sk} + \sum_{c\in\mathbb{F}_q^*} \psi(cb) \prod_{i=1}^{s} \chi_2(ca_i) G(\chi_2) \\ &= q^{sk} + (-1)^{s(nk+1)}\epsilon^{snk} q^{\frac{sk}{2}} \sum_{c\in\mathbb{F}_q^*} \psi(cb)\chi_2^s(c)\chi_2(a_1 \dots a_s) \\ &= q^{sk} + (-1)^{s(nk+1)}\epsilon^{snk} q^{\frac{sk}{2}} \chi_2(a_1 \dots a_s) \sum_{c\in\mathbb{F}_q^*} \psi(cb)\chi_2^s(c). \end{aligned}$$

If either s or k is even, then χ_2^s is the trivial character over $\mathbb{F}_q$, and then

$$\begin{aligned} N(b) &= q^{sk} + (-1)^{s(nk+1)}\epsilon^{snk} q^{\frac{sk}{2}} \chi_2(a_1 \dots a_s) \sum_{c\in\mathbb{F}_q^*} \psi(cb) \\ &= \begin{cases} q^{sk} + (-1)^{s(nk+1)}\epsilon^{snk} q^{\frac{sk}{2}} \chi_2(a_1 \dots a_s)(q-1), & \text{if } \mathrm{Tr}_{q^k/q}(b) = 0 \\ q^{sk} - (-1)^{s(nk+1)}\epsilon^{snk} q^{\frac{sk}{2}} \chi_2(a_1 \dots a_s), & \text{if } \mathrm{Tr}_{q^k/q}(b) \neq 0. \end{cases} \end{aligned}$$

Let us assume that s and k are both odd, so that χ_2^s is the quadratic character over $\mathbb{F}_q$. In this case,

$$\begin{aligned} N(b) &= q^{sk} + (-1)^{s(nk+1)}\epsilon^{snk} q^{\frac{sk}{2}} \chi_2(a_1 \dots a_s) \sum_{c \in \mathbb{F}_q^*} \psi(cb)\chi_2^s(c) \\ &= \begin{cases} q^{sk}, & \text{if } \operatorname{Tr}_{q^k/q}(b) = 0 \\ q^{sk} + (-1)^{s(nk+1)}\epsilon^{snk} q^{\frac{sk}{2}} \chi_2(a_1 \dots a_s \operatorname{Tr}_{q^k/q}(b)) G_q(\chi_2), & \text{if } \operatorname{Tr}_{q^k/q}(b) \neq 0, \end{cases} \end{aligned}$$

where $G_q(\chi_2)$ is the Gauss sum of χ_2 over $\mathbb{F}_q$. The result now follows from Theorem 1.7.

■

Part II

Dynamics of maps over fields

CHAPTER 6

Dynamics of polynomial maps over finite fields

The iteration of polynomial maps over finite fields have attracted interest of many authors in the last few decades (for example see [36, 38, 66, 79]). The interest for these problems has increased mainly because of their applications in cryptography, for example see [45, 106]. The iteration of a polynomial map over a finite field yields a dynamical system, that can be related to its functional graph, which is formally defined as follows. Let $\mathbb{F}_q$ be a finite field with q elements and let $f \in \mathbb{F}_q[x]$. The functional graph associated to the pair $(f, \mathbb{F}_q)$ is the directed graph $\mathcal{G}(f/\mathbb{F}_q)$ with vertex set $V = \mathbb{F}_q$ and directed edges $A = \{(a, f(a)) : a \in \mathbb{F}_q\}$.

While the iteration of polynomial maps has been widely studied, a complete characterization of their functional graphs has not been provided. Even though, many particular results in this direction are known. For example, the functional graphs and related questions are known for the following classes of polynomials:

(i) $f(x) = x^2$ over prime fields [80];

(ii) $f(x) = x^n$ over prime fields [14];

(iii) Chebyshev polynomials [34] and [74];

(iv) Linearized polynomials [69].

Some other functions and problems concerning the dynamics of maps over finite structures has been of interest [71, 73, 75, 100]. For a survey of the results in the literature, see [55]. The chapter's goal is to provide the functional graph associated to a class of polynomials in a general setting. For a polynomial $f(x) = x^n h(x^{\frac{q-1}{m}})$ with index m, we study the dynamics of the map $a \mapsto f(a)$ in order to present its functional graph $\mathcal{G}(f/\mathbb{F}_q)$. Throughout the chapter, we write

$$\mathcal{G}(f/\mathbb{F}_q) = \mathcal{G}^{(0)}_{f/\mathbb{F}_q} \oplus \mathcal{G}^{(1)}_{f/\mathbb{F}_q},$$

where $\mathcal{G}^{(0)}_{f/\mathbb{F}_q}$ denotes the connected component of $\mathcal{G}(f/\mathbb{F}_q)$ containing $0 \in \mathbb{F}_q$. The aim of the chapter is to present explicitly the two functional graphs $\mathcal{G}^{(0)}_{f/\mathbb{F}_q}$ and $\mathcal{G}^{(1)}_{f/\mathbb{F}_q}$ under a natural condition. The condition imposed along the chapter guarantees that all the trees attached to

cyclic points of $\mathcal{G}^{(1)}_{f/\mathbb{F}_q}$ are isomorphic. Our main results are essentially presented in two theorems: Theorem 6.4 provides the component $\mathcal{G}^{(0)}_{f/\mathbb{F}_q}$ that contains the vertex 0 and Theorem 6.7 provides the functional graph $\mathcal{G}^{(1)}_{f/\mathbb{F}_q}$ that contains all vertices that are not connected to the vertex 0. For a polynomial $f(x) = x^n h(x^{\frac{q-1}{m}})$, the associated polynomial $\psi_f(x) = x^n h(x)^{\frac{q-1}{m}}$ will play an important role in the proof of our main results. In particular, the dynamics of the polynomial f over $\mathbb{F}_q$ is established in terms of the dynamics of the map ψ_f over the set $\mu_m \subset \mathbb{F}_q$ of m-th roots of the unity. For more details, see Section 6.3.

This chapter is organized as follows. In Section 6.1 we present the terminology used along the chapter and provide our main results. Section 6.2 presents preliminary results that will be used throughout the chapter. The proof of our main results is provided in Section 6.3.

6.1 Terminology and main results

In this section we fix the notation used in the chapter, present our main results and provide some major comments. We use the same terminology as in [73, 75, 76]. Let α be a generator of the multiplicative group $\mathbb{F}_q^*$. Along the chapter, we will make an abuse of terminology by saying that the graphs are equal if they are isomorphic. By rooted tree, we mean a directed rooted tree, where all the edges point towards the root. Also, we use the letter $\mathcal{T}$ to denote a rooted tree. The tree with a single vertex is denoted by $\bullet$. We use $\mathrm{Cyc}(k, \mathcal{T})$ to denote a directed graph composed by a cycle of length k, where every node of the cycle is the root of a tree isomorphic to $\mathcal{T}$. The cycle $\mathrm{Cyc}(k, \bullet)$ is also denoted by $\mathrm{Cyc}(k)$. We use $\oplus$ to denote the disjoint union of graphs, and, for a graph $\mathcal{G}$, $k \times \mathcal{G}$ denotes the graph $\oplus_{i=1}^{k} \mathcal{G}$. If $\mathcal{G} = \oplus_{i=1}^{s} \mathcal{T}_i$, where $\mathcal{T}_1, \ldots, \mathcal{T}_s$ are rooted trees, then $\langle \mathcal{G} \rangle$ represents the rooted tree whose children are roots of rooted trees isomorphic to $\mathcal{T}_1, \ldots, \mathcal{T}_s$.

We recall that the connected components of a functional graph related to the iteration of a function over a finite set consists of cycles where each vertex of the cyclic is the root of a rooted tree. In this chapter, we study a class of polynomial maps whose functional associated graph has a regularity in the trees attached to each vertex in a cycle. In order to describe such trees, we present the well-known notation of elementary trees.

Definition 6.1. *For a non increasing sequence of positive integers $V = (v_1, v_2, \ldots, v_D)$, the rooted tree $\mathcal{T}_V$ is defined recursively as follows:*

$$\begin{cases} \mathcal{T}_V^0 = \bullet, \\ \mathcal{T}_V^k = \left\langle v_k \times \mathcal{T}_V^{k-1} \oplus \bigoplus_{i=1}^{k-1} (v_i - v_{i+1}) \times \mathcal{T}_V^{i-1} \right\rangle \quad \text{for } 1 \le k \le D-1, \\ \mathcal{T}_V = \left\langle (v_D - 1) \times \mathcal{T}_V^{D-1} \oplus \bigoplus_{i=1}^{D-1} (v_i - v_{i+1}) \times \mathcal{T}_V^{i-1} \right\rangle \text{ and} \\ \mathcal{T}_V^k = \left\langle v_k \times \mathcal{T}_V^{k-1} \oplus \bigoplus_{i=1}^{k-1} (v_i - v_{i+1}) \times \mathcal{T}_V^{i-1} \right\rangle \quad \text{for } k \ge D, \end{cases}$$

where $v_i = 1$ for all $i \ge D+1$.

The graph $\mathcal{T}_V$ is called *elementary tree*. Elementary trees play an important role in the study of functional graphs over finite fields, for example see [34, 69, 73, 75, 76]. Along this text, elementary trees will appear in our main statements. Indeed all the trees attached to nonzero vertices in cycles in the functional graphs arising from the maps we study are elementary trees. For more details about this, see Lemmas 6.13 and 6.15.

Throughout the chapter, we use μ_m to denote the m-th roots of the unity in $\overline{\mathbb{F}}_q$. For a positive integer d, let

$$\mu(d) = \begin{cases} 1, & \text{if } d \text{ is square-free with an even number of prime factors;} \\ -1, & \text{if } d \text{ is square-free with an odd number of prime factors;} \\ 0, & \text{if } d \text{ has a squared prime factor.} \end{cases}$$

be the Möbius function.

In order to present our main results, we will follow the notation used in [76] denoting by $\gcd_n(v)$ the iterated gcd of v relative to n, that is, $\gcd_n(v) = (v_1, \ldots, v_s)$, where

$$v_i = \frac{\gcd(n^i, v)}{\gcd(n^{i-1}, v)} \text{ for } i \geq 1$$

and s is the least positive integer such that $v_s = 1$. This notion was introduced in [73], where it was called ν-series. An important property of $\gcd_n(v) = (v_1, \ldots, v_s)$ is that $v_1 \cdots v_j = \gcd(n^j, v)$. This property will be used in the proof of our results. Any polynomial $f \in \mathbb{F}_q[x]$ satisfying $f(0) = 0$ can be written uniquely as $f(x) = x^n h(x^{\frac{q-1}{m}})$, where $h(0) \neq 0$ and m is minimal. The number m is called the *index* of the polynomial f. The index of polynomials play an important role in the study of polynomials over finite fields, for more details see [104]. Along the chapter, $f(x) = x^n h(x^{\frac{q-1}{m}}) \in \mathbb{F}_q[x]$ is a polynomial with index m. We now present a notion that will be used to guarantee certain regularity on the functional graph of f.

Definition 6.2. *A polynomial $f(x) = x^n h(x^{\frac{q-1}{m}}) \in \mathbb{F}_q[x]$ with index m is said to be m-nice over $\mathbb{F}_q$ if the map $x \mapsto \psi_f(x) = x^n h(x)^{\frac{q-1}{m}}$ is an injective map from $\mu_m \backslash \psi_f^{(-1)}(0)$ to μ_m.*

It is worth mentioning that $(\psi_f \circ x^{\frac{q-1}{m}})(a) = (x^{\frac{q-1}{m}} \circ f)(a)$ for all $a \in \mathbb{F}_q$. This fact is used along the proofs of our results. The fact that the composition of the maps ψ_f and f commutes over $\mathbb{F}_q$ play an important role in the study of permutation polynomials, for example see [2]. In this chapter, we present the dynamics of f over $\mathbb{F}_q$ in terms of the dynamics of ψ_f over μ_m, that is usually a smaller set. In what follows, we present an example of polynomial that satisfy the notion of being nice.

Example 6.3. *Let $g(x) = x^{15} h(x^{36}) \in \mathbb{F}_{181}[x]$, where $h(x) = 98x^4 + 68x^3 + 68x^2 - 6x - 31$. Then $\psi_g(x) = x^{15} h(x)^{36}$. By straightforward computations, one can show that $\mu_5 = \{1, 42, 59, 125, 135\}$ and 2 is a primitive element of $\mathbb{F}_{181}$. Furthermore,*

$$\psi_g(59) = 42,\ \psi_g(42) = 0,\ \psi_g(125) = 125,\ \psi_g(1) = 135 \text{ and } \psi_g(135) = 1.$$

Therefore, $g(x)$ is 5-nice over $\mathbb{F}_{181}$.

Throughout the chapter, we let $\frac{q-1}{m} = \nu\omega$ where ω is the greatest divisor of $\frac{q-1}{m}$ that is relatively prime with n. Now we are able to present one of our main results. The following theorem provides the functional graph $\mathcal{G}^{(0)}_{f/\mathbb{F}_q}$ of m-nice polynomials.

Theorem 6.4. *Assume that $f(x) = x^n h(x^{\frac{q-1}{m}})$ is m-nice over $\mathbb{F}_q$ and let $d_j = \gcd(\nu, n^j)$ for each positive integer j. For each $i = 1, \ldots, m+1$, let $r_i = |\{\xi \in \mu_m : \psi_f^{(i)}(\xi) = 0\}|$. Then $\mathcal{G}^{(0)}_{f/\mathbb{F}_q} = \mathrm{Cyc}(1, T)$, where*

$$T = \left\langle \bigoplus_{i=0}^{m-1} \left(\tfrac{(q-1)r_{i+1}}{md_i} - \tfrac{(q-1)r_{i+2}}{md_{i+1}} \right) \times \mathcal{T}^i_{\gcd_n(\nu)} \right\rangle.$$

We present now an example.

Example 6.5. *Let $g(x) \in \mathbb{F}_{181}[x]$ be defined as in Example 6.3 and let notation be as in Theorem 6.4. Our goal is to apply Theorem 6.4 for the polynomial $g(x)$. Since $n = 15, m = 5$ and $\frac{q-1}{m} = 36$, we have that $\omega = 4$, $\nu = 9$ and $\gcd_n(\nu) = (3, 3, 1)$. From Example 6.3, it follows that $r_1 = r_2 = 1$ and $r_i = 0$ for $i \geq 2$. Furthermore, $d_1 = \gcd(9, 15) = 3$ and $d_i = \gcd(9, 15^i) = 9$ for $i \geq 2$. Therefore, Theorem 6.4 states that $\mathcal{G}^{(0)}_{g/\mathbb{F}_{181}} = \mathrm{Cyc}(1, T)$, where*

$$T = \left\langle 24 \times \mathcal{T}^0_{(3,3,1)} \oplus 12 \times \mathcal{T}^1_{(3,3,1)} \right\rangle.$$

Figure 6.1 shows this functional graph.

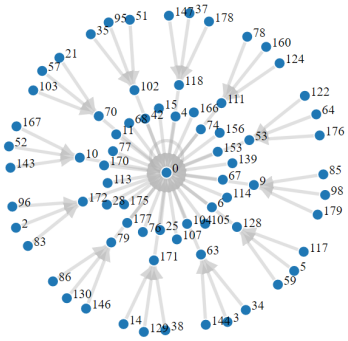

Figure 6.1: The connected component of $\mathcal{G}(g/\mathbb{F}_{181})$ that contains the element $0 \in \mathbb{F}_{181}$.

We now focus in the components of $\mathcal{G}(f/\mathbb{F}_q)$ that do not contain the element $0 \in \mathbb{F}_q$. In order to present this graph, the following definition will be used.

Definition 6.6. *For a polynomial $f(x) \in \mathbb{F}_q[x]$ with index m, we define*

$$\psi_f^{-\infty}(0) = \{\gamma \in \mu_m : \psi_f^{(i)}(\gamma) = 0 \text{ for a positive integer } i\}.$$

We note that if $f(x) = x^n h(x^{\frac{q-1}{m}})$ and $h(x)$ has no roots in μ_m, then $\psi_f^{-\infty}(0)$ is the empty set. Let ω' be the greatest divisor of $q-1$ that is relatively prime with n. In the following theorem, we determine the graph $\mathcal{G}^{(1)}_{f/\mathbb{F}_q}$ under the hypothesis that $f(x)$ is m-nice.

Theorem 6.7. *Assume that $f(x) = x^n h(x^{\frac{q-1}{m}})$ is m-nice over $\mathbb{F}_q$ and let $S_1, \ldots, S_t \subset \mu_m$ be sets such that $\mu_m \backslash \psi_f^{-\infty}(0) = S_1 \cup \cdots \cup S_t$ and $\mathcal{G}(\psi_f/S_i) = \mathrm{Cyc}(k_i)$. For each $i = 1, \ldots, t$, let $\xi_i \in S_i$ and ℓ_i, r_i integers such that $\xi_i = \alpha^{\frac{q-1}{m} r_i}$ and $\alpha^{\ell_i} = \prod_{j=0}^{k_i-1} h\big(\psi_f^{(j)}(\xi_i)\big)^{n^{k_i-j-1}}$. Then*

$$\mathcal{G}^{(1)}_{f/\mathbb{F}_q} = \bigoplus_{\substack{i=1,\ldots,t \\ u \mid \mathrm{ord}_{w'(n^{k_i}-1)}(n^{k_i})}} \left(\frac{\sum_{d|u} \mu(\frac{u}{d}) \tau_i(d)}{u} \times \mathrm{Cyc}\left(k_i u, \mathcal{T}_{\gcd_n(\nu)}\right) \right),$$

where

$$\tau_i(d) := \begin{cases} \gcd\left(\frac{q-1}{m}, n^{dk_i} - 1\right), & \text{if } \gcd\left(q-1, (n^{dk_i}-1)m\right) \mid \left(\ell_i\left(\frac{n^{dk_i}-1}{n^{k_i}-1}\right) + r_i(n^{dk_i}-1)\right); \\ 0, & \text{otherwise.} \end{cases}$$

We present now an example.

Example 6.8. *Let $g(x) \in \mathbb{F}_{181}[x]$ be defined as in Example 6.3 and let notation be as in Theorem 6.7. Our goal is to apply Theorem 6.7 for the polynomial $g(x)$. From Example 6.3, we can choose $S_1 = \{125\}$ and $S_2 = \{1, 135\}$, so that $k_1 = 1$ and $k_2 = 2$. Furthermore, $w' = 4$, $\mathrm{ord}_{4(15-1)}(15) = 2$, $\mathrm{ord}_{4(15^2-1)}(15^2) = 4$, $\ell_1 = 18$, $\ell_2 = 75$, $r_1 = 3$ and $r_2 = 0$, which implies that*

$$\tau_1(1) = 2,\ \tau_1(2) = 4,\ \tau_2(1) = 0,\ \tau_2(2) = 0 \text{ and } \tau_2(4) = 4.$$

Therefore, Theorem 6.7 states that

$$\mathcal{G}^{(1)}_{g/\mathbb{F}_{181}} = 2 \times \mathrm{Cyc}(1, \mathcal{T}_{(3,3,1)}) \oplus \mathrm{Cyc}(2, \mathcal{T}_{(3,3,1)}) \oplus \mathrm{Cyc}(8, \mathcal{T}_{(3,3,1)}).$$

Figure 6.2 shows this functional graph.

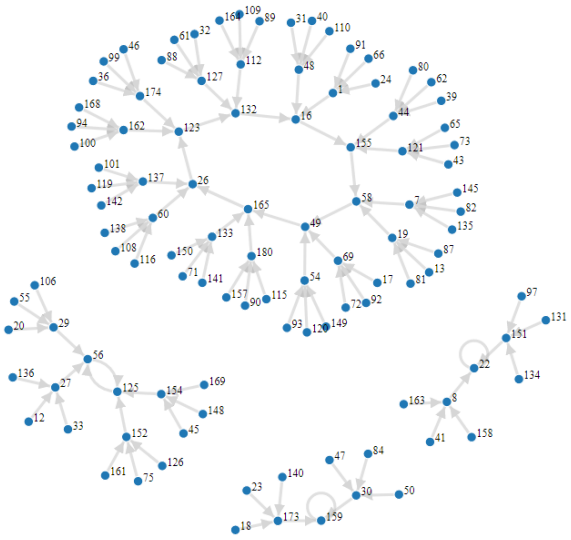

Figure 6.2: The conneted components of $\mathcal{G}(g/\mathbb{F}_{181})$ that does not contain the element $0 \in \mathbb{F}_{181}$.

In the case where $m = 1$ and $h(x) = a$, $f(x) = ax^n$ for all $x \in \mathbb{F}_q$. Furthermore, $f(x) = ax^n$ is 1-nice, which implies that Theorems 6.7 holds. In this case, Theorems 6.7 implies the following result.

Corollary 6.9. *Let $f(x) = ax^n$. Then*

$$\mathcal{G}(f/\mathbb{F}_q) = \mathrm{Cyc}(1) \oplus \bigoplus_{u \mid \mathrm{ord}_{w'(n-1)}(n)} \left(\frac{\sum_{d|u} \mu(\frac{u}{d}) \tau(d)}{u} \times \mathrm{Cyc}\left(u, \mathcal{T}_{\gcd_n(\nu)}\right) \right),$$

where $\alpha^\ell = a$ and

$$\tau(d) := \begin{cases} \gcd\left(q-1, n^d-1\right), & \text{if } \gcd\left(q-1, (n^d-1)\right) \mid l\left(\frac{n^d-1}{n-1}\right); \\ 0, & \text{otherwise.} \end{cases}$$

Corollary 6.9 generalizes some results obtained in [14, 73, 76]. Theorems 6.7 can be also employed for general classes of polynomial, as we see in the next result.

Corollary 6.10. *Let $f(x) = x^n h(x^{q-1})$, where $h \in \mathbb{F}_q[x]$ is a self-reciprocal polynomial of degree $n-1$ that has no roots in $\mu_{q+1} \subset \mathbb{F}_{q^2}$. For each $i = 1, \ldots, q+1$, let ℓ_r be an integer such that $\alpha^{\ell_r} = h(\alpha^{(q-1)r})$. Then*

$$\mathcal{G}(f/\mathbb{F}_{q^2}) = \mathrm{Cyc}(1) \oplus \bigoplus_{\substack{r=1,\ldots,q+1 \\ u \mid \mathrm{ord}_{w'(n-1)}(n)}} \left(\frac{\sum_{d \mid u} \mu(\frac{u}{d}) \tau_r(d)}{u} \times \mathrm{Cyc}\left(u, \mathcal{T}_{\gcd_n(\nu)}\right) \right),$$

where

$$\tau_r(d) := \begin{cases} \gcd\left(\frac{q-1}{m}, n^d - 1\right), & \text{if } \gcd\left(q-1, (n^d-1)m\right) \mid \left(r(n^d-1)\right); \\ 0, & \text{otherwise.} \end{cases}$$

We note that, in particular, Theorems 6.4 and 6.7 gives the number of connected components, the length of the cycles and the number of fixed points of m-nice polynomials. In the case where this condition is not satisfied, the functional graph of the polynomial is more chaotic, what makes it difficult to use the same approach used here. In the following example we present a polynomial that is not nice and its associated functional graph.

Example 6.11. *Let $g(x) = x^6 h(x^{24}) \in \mathbb{F}_{97}[x]$, where $h(x) = x - 1$. Then $\psi_g(x) = x^6(x-1)^{24}$. One can show that $\mu_5 = \{1, 22, 75, 96\}$. Furthermore,*

$$\psi_g(22) = \psi_g(75) = 22, \ \psi_g(96) = 96 \text{ and } \psi_g(1) = 0.$$

Therefore, $g(x)$ is not 4-nice over $\mathbb{F}_{97}$. In this case, the trees attached to cyclic vertices of $\mathcal{G}(g/\mathbb{F}_{97})$ have no regularity. Figure 6.3 shows this functional graph.

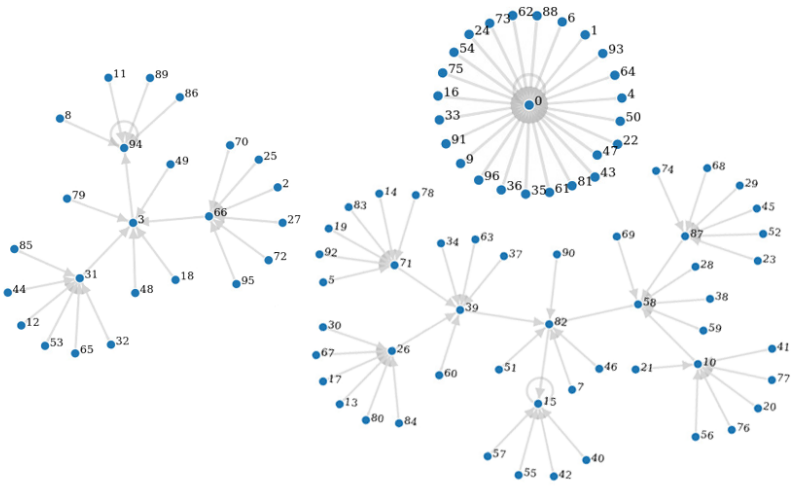

Figure 6.3: The functional graph $\mathcal{G}(g/\mathbb{F}_{97})$.

6.2 Preparation

In this section, we provide preliminary notations and results that will be important in the proof of our main results. Let b and c be vertices in a directed graph. If a vertex b is reachable from c, then c is a predecessor of b and b is a successor of c. If a vertex b is reachable from c by a directed path containing $k+1$ vertices, then we say that c is a k-distant predecessor of b. The following notions and results are the tools we need to prove Theorems 6.4 and 6.7.

Definition 6.12. *Let $\mathcal{G}$ be a directed graph, $V = (v_1, v_2, \ldots, v_D)$ be a non increasing sequence of positive integers and let $v_i = v_D$ for all $i \geq D$. We say that $\mathcal{G}$ is V-regular if for each positive integer k, the number of k-distant predecessors of a vertex of $\mathcal{G}$ is either 0 or $v_1 \cdots v_k$.*

Lemma 6.13. *Let $V = (v_1, v_2, \ldots, v_D)$ be a non increasing sequence of positive integers. If $\mathcal{T}$ is a V-regular rooted tree with depth k, then $\mathcal{T}$ is isomorphic to $\mathcal{T}_V^k$.*

Proof. For $i \geq D+1$, let $v_i = v_D$. We proceed by induction on k. The case $k = 0$ follows directly. Suppose that the result is true for an integer $k \geq 1$ and $\mathcal{T}$ is a V-regular rooted tree with depth $k+1$. Let T be the rooted tree obtained from $\mathcal{T}$ by deleting the vertices with depth $k+1$. By induction hypothesis, T is isomorphic to $\mathcal{T}_V^k$.

Let $z_1, \ldots, z_{v_{k+1}}$ be the vertices of $\mathcal{T}$ with depth 1 that have at least one descendant with depth $k+1$ and let $z'_1, \ldots, z'_{v_{k+1}}$ be the equivalent vertices in T. For $i = 1, \ldots, v_{k+1}$, let $\mathcal{T}_{z_i}$ be the rooted tree obtained from $\mathcal{T}$ containing all descendants of z_i and let T_{z_i} be the rooted tree obtained from T containing all descendants of z'_i. Since $\mathcal{T}$ is V-regular, each $\mathcal{T}_{z_i}$ is isomorphic to $\mathcal{T}_V^k$. Therefore, $\mathcal{T}$ can be recovered from T by replacing each T_{z_i} by $\mathcal{T}_V^k$. The tree obtained from these steps is isomorphic to the rooted tree $\mathcal{T}_V^{k+1}$, which completes the proof of our assertion. ■

Definition 6.14. *For a vertex b of a directed graph $\mathcal{G}$, the graph $R_b(\mathcal{G})$ is the subgraph of $\mathcal{G}$ containing all predecessors of b (including b).*

Lemma 6.15. *Let $V = (v_1, v_2, \ldots, v_D)$ be a non increasing sequence of positive integers such that $v_D = 1$, let $\mathcal{G}$ be a V-regular directed graph with depth at least D, b be a vertex of $\mathcal{G}$. Assume that $R_b(\mathcal{G})$ contains a cycle. Let G be the graph obtained from $R_b(\mathcal{G})$ by deleting the vertices $c \neq b$ that are in the cycle. Then G is isomorphic to $\mathcal{T}_V$.*

Proof. It follows similarly to the proof of Lemma 6.13. ■

If $f(x) = x^n h(x^{\frac{q-1}{m}})$ is a polynomial with index m and k is a positive integer, then one can readily prove that

$$f^{(k)}(x) = x^{n^k} \prod_{i=0}^{k-1} h\left(\psi_f^{(i)}\left(x^{\frac{q-1}{m}}\right)\right)^{n^{k-i-1}}. \tag{6.1}$$

This formula will be important in the proofs of the main results.

Lemma 6.16. *Let k be a positive integer and $b \in \mathbb{F}_q^*$. Assume that $f(x) = x^n h(x^{\frac{q-1}{m}})$ is m-nice. If $x \in \mathbb{F}_q$ is a solution of the equation $f^{(k)}(x) = b$, then $x^{\frac{q-1}{m}} = \psi_f^{(-k)}\left(b^{\frac{q-1}{m}}\right)$.*

Proof. We proceed by induction on k. Let $k = 1$ and let $x \in \mathbb{F}_q$ be a solution of the equation $f(x) = b$. Then $f(x)^{\frac{q-1}{m}} = x^{\frac{q-1}{m}n} h(x^{\frac{q-1}{m}})^{\frac{q-1}{m}} = b^{\frac{q-1}{m}}$. Since $f(x)$ is m-nice, it follows that $x^{\frac{q-1}{m}} = \psi_f^{(-1)}\left(b^{\frac{q-1}{m}}\right)$. Suppose that the result follows for an integer $k \geq 1$ and let $x \in \mathbb{F}_q$ be a solution of the equation $f^{(k+1)}(x) = b$. By induction hypothesis, $f(x)^{\frac{q-1}{m}} = \psi_f^{(-k)}\left(b^{\frac{q-1}{m}}\right)$. Therefore, $x^{\frac{q-1}{m}n} h(x^{\frac{q-1}{m}})^{\frac{q-1}{m}} = \psi_f^{(-k)}\left(b^{\frac{q-1}{m}}\right)$, which implies that $x^{\frac{q-1}{m}} = \psi_f^{(-(k+1))}\left(b^{\frac{q-1}{m}}\right)$, since $f(x)$ is m-nice. ■

Proposition 6.17. *Let $a \in \mathbb{F}_q^*$. If $f(x)$ is m-nice, then $R_a\left(\mathcal{G}\left(f/\mathbb{F}_q\right)\right)$ is $\gcd_n(\nu)$-regular.*

Proof. Let b be a vertex of $R_a\left(\mathcal{G}\left(f/\mathbb{F}_q\right)\right)$ and k be a positive integer. The number of k-distant predecessors of b is equal to the number of solutions of the equation

$$f^{(k)}(x) = b \tag{6.2}$$

over $\mathbb{F}_q$. By Lemma 6.16, a solution $x \in \mathbb{F}_q$ of Equation (6.2) must satisfy the relation $x^{\frac{q-1}{m}} = \psi_f^{(-k)}\left(b^{\frac{q-1}{m}}\right) =: \xi \in \mu_m$. Let α be a primitive element of $\mathbb{F}_q$ and let t be an integer such that $\xi = \alpha^{\frac{q-1}{m}t}$. Then the equality $x^{\frac{q-1}{m}} = \alpha^{\frac{q-1}{m}t}$ implies $x = \alpha^{t+m\ell}$ for some $l = 1, \ldots, \frac{q-1}{m}$. Now, Equations (6.1) and (6.2) states that

$$\alpha^{(t+m\ell)n^k} c = b, \tag{6.3}$$

where $c = \prod_{i=0}^{k-1} h\left(\psi_f^{(i)}(\xi)\right)^{n^{k-i-1}}$ and $l = 1, \ldots, \frac{q-1}{m}$. In order to complete the proof, we will prove the following statement.

Claim. The number of integers $\ell = 1, \ldots, \frac{q-1}{m}$ satisfying Equation (6.3) is equal to either 0 or $\gcd\left(n^k, \frac{q-1}{m}\right)$.

Proof of the claim. Let u be an integer such that $b/c = \alpha^u$. We want to compute the number of integers $\ell = 1, \ldots, \frac{q-1}{m}$ such that $\alpha^{(t+m\ell)n^k} = \alpha^u$, that is

$$(t + m\ell)n^k \equiv u \pmod{q-1}. \tag{6.4}$$

Assume that this equation has at least one solution. Then $\gcd(mn^k, q-1)$ must divide $u - tn^k$. In this case, Equation (6.4) becomes

$$\frac{n^k}{\gcd(n^k,s)}\ell \equiv \frac{u-tn^k}{\gcd(mn^k,q-1)} \pmod{\frac{q-1}{m\gcd(n^k,s)}},$$

where $s = \frac{q-1}{m}$. Now, since $\frac{n^k}{\gcd(n^k,s)}$ is relatively prime to $\frac{q-1}{m\gcd(n^k,s)}$, there exists exactly one solution ℓ to the above equation in the interval $\left[1, \frac{q-1}{m\gcd(n^k,s)}\right]$. Therefore, Equation (6.4) has $\gcd(n^k, s)$ solutions, which proves our claim.

By the Claim, the number of k-distant predecessors of b is either 0 or $\gcd(n^k, s)$, which is the product of the k first terms of $\gcd_n(\nu)$. Since $b \in \mathbb{F}_q^*$ and k were taken arbitrarily, the proof of our assertion is complete.

■

We recall a classic result from Number Theory that will be used in the proof of Theorem 6.7.

Theorem 6.18. *[44, Möbius Inversion Formula] Let $G(u) = \sum_{d|u} g(d)$. Then $g(u) = \sum_{d|u} \mu(u/d)G(d)$.*

Now we are able to prove the main results of the chapter.

6.3 Functional graph of polynomial maps

In this section, we provide the proof of our main results. We start by proving Theorem 6.4.

6.3.1 Proof of Theorem 6.4

Let $\{0, w_1, \ldots, w_{r_1(q-1)/m}\}$ denote the set of children of 0 in $\mathcal{G}(f/\mathbb{F}_q)$, that consists of the solutions of the equation

$$x^n h(x^{\frac{q-1}{m}}) = 0$$

over $\mathbb{F}_q$. For each $j = 1, \ldots, \frac{q-1}{m} r_1$, let $T_j = R_{w_j}(\mathcal{G}(f/\mathbb{F}_q))$. Since $f(0) = 0$, the vertex 0 is the single vertex of the cyclic part of this component and then each T_j is a tree. Therefore, $\mathcal{G}^{(0)}_{f/\mathbb{F}_q} = \mathrm{Cyc}(1, T)$, where

$$T = \left\langle \bigoplus_{j=1}^{r_1(q-1)/m} T_j \right\rangle. \tag{6.5}$$

By Proposition 6.17 and Lemma 6.13, each T_j is isomorphic to $\mathcal{T}^{i_j}_{\gcd_n(\nu)}$, where i_j is the depth of T_j. Therefore, we only need to determine the cardinality of each set

$$A_i = \big\{ j \in \{1, \ldots, r_1(q-1)/m\} : T_j \text{ is isomorphic to } \mathcal{T}^i_{\gcd_n(\nu)} \big\}.$$

In order to do so, we define the set

$$B_i = \{ j \in \{1, \ldots, r_1(q-1)/m\} : T_j \text{ has a vertex with depth } i \}.$$

We observe that $|A_i| = |B_i| - |B_{i+1}|$. Let $z_1, \ldots, z_{r_1}$ be the elements in μ_m that are solutions of the equation $h(x) = 0$. By Lemma 6.16, any vertex x of T_j with depth i is a solution of the equation

$$x^{\frac{q-1}{m}} = \psi_f^{(-i)}\big(w_j^{\frac{q-1}{m}}\big).$$

On the other hand, since $f(x)$ is m-nice, any solution of the above equation must be a vertex with depth i of T_j for some $j = 1, \ldots, r_1(q-1)/m$. Therefore, we are interested in the number of solutions of the equations

$$x^{\frac{q-1}{m}} = \psi_f^{(-i)}\big(z_\ell\big), \tag{6.6}$$

where $\ell = 1, \ldots, r_1$. Taking $x^{\frac{q-1}{m}} = \xi \in \mu_m$, Equation (6.6) becomes

$$\xi = \psi_f^{(-i)}\big(z_\ell\big),$$

that has a solution (for some ℓ) for r_{i+1} distinct values $\xi \in \mu_m$. Therefore, the number of solutions of Equation (6.6) is equal to $r_{i+1} \times \frac{q-1}{m}$. Since T_j is $\gcd_n(\nu)$-regular, the number of i-distant predecessors of w_j in T_j equals either 0 or $d_i = \gcd(n^i, \nu)$. Therefore,

$$|B_i| = \frac{r_{i+1}(q-1)}{m d_i}.$$

Now it follows from Equation (6.5) that

$$T = \left\langle \bigoplus_{i=0}^{\infty} \left(\tfrac{(q-1)r_{i+1}}{m d_i} - \tfrac{(q-1)r_{i+2}}{m d_{i+1}} \right) \times \mathcal{T}^i_{\gcd_n(\nu)} \right\rangle.$$

Since there exist at most m elements in μ_m, the depth of sum of these tree is at most $m-1$, and therefore we may assume without loss of generality that $i \leq m-1$, which completes the proof of our assertion. ■

We are now able to prove the main result of the chapter.

6.3.2 Proof of Theorem 6.7

We recall that each connected component of $\mathcal{G}^{(1)}_{f/\mathbb{F}_q}$ is composed by a cycle and each vertex of this cycle is a non-null element of $\mathbb{F}_q$ that is the root of a tree. By Lemma 6.15 and Proposition 6.17, each one of such trees is isomorphic to $\mathcal{T}_{\gcd_n(\nu)}$. Therefore, it only remains to determine what are the cycles in $\mathcal{G}^{(1)}_{f/\mathbb{F}_q}$. Our goal now is to determine how many cycles there exist with length ℓ.

By Lemma 6.16, we have that the length of a cycle is closely related to the dynamics of ψ_f over μ_m. Indeed, if $f^{(\ell)}(a) = a$ for a positive integer ℓ, then $a^{\frac{q-1}{m}} = \psi_f^{(-\ell)}(a^{\frac{q-1}{m}})$, which implies that $\psi_f^{(\ell)}(a^{\frac{q-1}{m}}) = a^{\frac{q-1}{m}}$, since f is m-nice. In this case, if $a^{\frac{q-1}{m}} \in S_i$, then $k_i \mid \ell$. Furthermore, any vertex b in the same cycle of a satisfies $b^{\frac{q-1}{m}} \in S_i$. In particular, that means that the cycles whose dynamics are related to two different sets S_i and S_j are not connected. Therefore, we may determine each one of this cycles separately. For a positive integer u and a fixed $i \in \{1, \ldots, t\}$, let

$$A_i(u) = \{a \in \mathbb{F}_q : a^{\frac{q-1}{m}} = \xi_i, f^{(uk_i)}(a) = a\}$$

and

$$B_i(d) = \{a \in \mathbb{F}_q : a^{\frac{q-1}{m}} = \xi_i, d \text{ is the least positive integer such that } f^{(dk_i)}(a) = a\}.$$

In order to determine how many cycles (with vertices a such that $a^{\frac{q-1}{m}} = \xi_i$)) there exist with length dk_i, we need to determine $|B_i(u)|$. We note that an element $a \in A_i(u)$ is a vertex in a cycle whose length s divides u, then $|A_i(u)| = \sum_{d|u} |B_i(d)|$. The Möbius inversion formula (Theorem 6.18) implies that

$$|B_i(u)| = \sum_{d|u} \mu(u/d)|A_i(d)|. \tag{6.7}$$

We now compute the value $|A_i(d)|$. In order to do so, let $a \in A_i(d)$. Since $a^{\frac{q-1}{m}} = \xi_i$ and $f^{(dk_i)}(a) = a$, it follows that $a = \alpha^{sm+r_i}$ for some integer $s \in \{1, \ldots, \frac{q-1}{m}\}$ and then Equation (6.1) states that

$$\left(\alpha^{sm+r_i}\right)^{n^{dk_i}} \prod_{j=0}^{dk_i-1} h\left(\psi_f^{(j)}(\xi)\right)^{n^{dk_i-j-1}} = \alpha^{sm+r_i}.$$

Since $\alpha^{\ell_i} = \prod_{j=0}^{k_i-1} h\big(\psi_f^{(j)}(\xi_i)\big)^{n^{k_i-j-1}}$, the previous equations becomes

$$\left(\alpha^{sm+r_i}\right)^{n^{dk_i}} \alpha^{\ell_i(1+n^{k_i}+\cdots+n^{(d-1)k_i})} = \alpha^{sm+r_i}.$$

Looking at the exponents in this equation and doing some algebraic manipulations, it follows that

$$\frac{n^{dk_i}-1}{n^{k_i}-1}\Big((sm+r_i)(n^{k_i}-1)+\ell_i\Big) \equiv 0 \pmod{q-1}. \tag{6.8}$$

By using the same arguments used along the proof of Proposition 6.17, one can prove that that number of solutions $s \in \{1, \ldots, \frac{q-1}{m}\}$ of the previous equations equals

$$\tau_i(d) := \begin{cases} \gcd\left(\frac{q-1}{m}, n^{dk_i}-1\right), & \text{if } \gcd\left(q-1, (n^{dk_i}-1)m\right) \mid \left(\ell_i\left(\frac{n^{dk_i}-1}{n^{k_i}-1}\right) + r_i(n^{dk_i}-1)\right); \\ 0, & \text{otherwise.} \end{cases}$$

On the other hand, each solution $s \in \{1, \ldots, \frac{q-1}{m}\}$ of Equation (6.8) yields an element in $A_i(d)$ and, therefore,

$$|A_i(d)| = \tau_i(d). \tag{6.9}$$

By Equations (6.7) and (6.9), it follows that

$$|B_i(u)| = \sum_{d|u} \mu(u/d)\tau_i(d).$$

Now we prove that if u is an integer for which there exist a cycle in $\mathcal{G}^{(1)}_{f/\mathbb{F}_q}$ with length uk_i, then $u \mid \mathrm{ord}_{w'(n^{k_i}-1)}(n^{k_i})$. In order to do so, we observe that if $a = \alpha^{sm+r_i}$ is an element in a cycle of length uk_i, then Equation (6.8) implies that u is the least integer such that

$$\frac{n^{uk_i}-1}{n^{k_i}-1}\Big((sm+r_i)(n^{k_i}-1)+\ell_i\Big) \equiv 0 \pmod{q-1},$$

which implies that $u = \mathrm{ord}_{d(n^{k_i}-1)}(n^{k_i})$, where d is a divisor of $q-1$ coprime to n. In particular, $d \mid w'$ so that $\mathrm{ord}_{d(n^{k_i}-1)}(n^{k_i}) \mid \mathrm{ord}_{w'(n^{k_i}-1)}(n^{k_i})$, which completes the proof of our theorem. ■

We notice that the conditions of being m-nice was essential in the proof of Theorems 6.4 and 6.7. A very good question here is if we can obtain similar results for some family of polynomials that does not satisfy that condition.

CHAPTER 7

On iterations of rational functions over perfect fields

For a field $\mathbb{K}$ and a rational function $R \in \mathbb{K}(x)$, we set $R^{(0)}(x) = x$ and, for $n \geq 1$, $R^{(n)}(x) = R^{(n-1)}(R(x))$. The rational function $R^{(n)}(x) \in \mathbb{K}(x)$ is the n-th iterate of R. When $R = f$ is a polynomial, the compositions $f^{(n)}(x)$ are also polynomials. The iterates of polynomials have been extensively studied in the past few years [4, 7, 46, 47, 61]; in many of the cases, the authors explore the *stable polynomials*. These are the polynomials $f \in \mathbb{K}[x]$ in which all the iterates $f^{(n)}(x), n \geq 1$ are irreducible over $\mathbb{K}$. When $\mathbb{K}$ is finite, the concept of stability is naturally extended to a set $\{f_1, \ldots, f_r\}$ of polynomials [38]. Still in the finite field case, further arithmetic properties of the polynomial iterates $f^{(n)}$ are studied in [36]. The authors explore the number of distinct roots, the number of irreducible factors over $\mathbb{K}$ and the largest degree of an irreducible factor of $f^{(n)}$ over $\mathbb{K}$. In particular they prove that, under some mild conditions on f, those three functions grow (roughly) at least linearly with respect to n.

Some results of [36] were recently improved and extended to iterates $f(g^{(n)}(x))$ in [79]. Most notably, in [79] it is proved that up to some exceptional pairs (f, g), the number Δ_n of distinct roots of $f(g^{(n)}(x))$ actually grows exponentially. More precisely, the inequality $c_1 d^n \leq \Delta_n \leq c_2 d^n$ holds for every sufficiently large n, where $c_1, c_2 > 0$ and $d > 1$ do not depend on n. However, only the constant d is explicitly given there, making the estimate imprecise. The exceptional pairs (f, g) are fully described and it is direct to verify that, for such pairs, the numbers $\{\Delta_n\}_{n\geq 0}$ are uniformly bounded by a constant. For more details, see Section 2 of [79]. Many other arithmetic aspects of the iterates $f(g^{(n)}(x))$ are also studied in [79], mainly motivated by Question 18.9 in [10]; this question includes a more general setting, allowing g to be a rational function.

In the context of rational functions, the iterates $f(R^{(n)}(x))$ have not been much explored, but we can naturally extend questions and definitions from the polynomial setting. For instance, if $R_n := R^{(n)}(x) = g_n/h_n$ with g_n, h_n relatively prime polynomials, we define the polynomial $f_R^{(n)} = h_n^{\deg(f)} f(R_n)$. So we may consider the notion of R-stability, meaning that f is R-stable if all the polynomials $f_R^{(n)}(x)$ are irreducible for every $n \geq 0$. The R-stability of polynomials was recently explored for a special class of rational functions R when $\mathbb{K}$ is finite [70].

The aim of this chapter is to refine the main result in [79], extending it to a more general

setting. We consider $\mathbb{K}$ a perfect field, $R \in \mathbb{K}(x)$ a rational function of positive degree and study the number $\Delta_{\alpha,R}(n)$ of distinct solutions of $R^{(n)}(x) = \alpha$ over the algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$. Our main results, Theorems 7.2 and 7.3, not only recovers the exponential bound in [79] but also provides a more precise estimate on $\Delta_{\alpha,R}(n)$. We prove that, with the exception of some pairs (α, R), the equality $\Delta_{\alpha,R}(n) = c_{\alpha,R} \cdot d^n + O_{\alpha,R}(1)$ holds for some $0 < c_{\alpha,R} \leq 1 < d$. The parameter d is easily obtained from R and there is an implicit formula for $c_{\alpha,R}$; in particular, we provide estimates on $c_{\alpha,R}$ by means of simple parameters. Similarly to the polynomial case [79], the exceptional pairs (α, R) satisfy $\Delta_{\alpha,R}(n) \leq 2$ for every $n \geq 0$, and are fully described. However, in contrast to the polynomial setting, we have many more pathological situations; for more details, see Theorem 7.3. We also discuss the growth of some arithmetic functions related to the factorization of $f_R^{(n)}(x)$ when $\mathbb{K}$ is finite, extending some minor results and open problems from [79].

The main idea behind the proof of Theorems 7.2 and 7.3 is to provide an implicit formula for $\Delta_{\alpha,R}(n)$, considering the number $r_{\beta,R}$ of solutions of $R(x) = \beta$ with β ranging over the elements in $\overline{\mathbb{K}}$ such that $R^{(i)}(\beta) = \alpha$ for some $i \geq 0$. With the exclusion of some exceptional R's, we prove that $\Delta_{\alpha,R}(n) = c_{\alpha,R} d^n + O_{\alpha,R}(1)$ for some $0 \leq c_{\alpha,R} \leq 1 < d$, where $c_{\alpha,R}$ depends on the numbers $r_{\beta,R}$. We then estimate $c_{\alpha,R}$ by means of parameters such as the degree of the extension $\mathbb{K}(\alpha)/\mathbb{K}$ and the degree of the Wronskian associated to R. This allows us to describe the pairs (α, R) in which $c_{\alpha,R}$ vanishes. Along with the exceptional R's, the latter fully describes the pathological cases.

The chapter is organized as follows. In Section 7.1 we state our main results and provide some important remarks. Section 7.2 provides background material and important preliminary results. In Section 7.3 we prove our main results. Finally, in Section 7.4 we extend some open problems and minor results from [79].

7.1 Main results

In this section we state our main results. Before doing so, we need to introduce some basic definitions. Throughout this chapter, $\mathbb{K}$ denotes a perfect field of characteristic $p \geq 0$ and $\overline{\mathbb{K}}$ denotes its algebraic closure. It is worth mentioning the finite fields are perfect. In fact, the most studied fields are perfect, so that this chapter studies a wide class of objects. By a rational function $R \in \mathbb{K}(x)$ we mean a quotient $\frac{g}{h}$, where $g, h \in \mathbb{K}[x]$ are relatively prime polynomials. For simplicity, we sometimes assume that h is monic. The degree of R is $\max\{\deg(g), \deg(h)\}$. Since $\mathbb{K}$ is perfect, if $p > 0$, the Frobenius map $a \mapsto a^p$ is an automorphism of $\mathbb{K}$. We have the following definition.

Definition 7.1. *Let $\mathbb{K}$ be a perfect field of characteristic $p \geq 0$ and let $R = g/h \in \mathbb{K}(x)$ be a rational function of degree $D \geq 1$. If $p > 0$, the p-reduction of R is the unique rational function $\tilde{R} \in \mathbb{K}(x)$ such that $R = \tilde{R}^{p^h}$, $h \geq 0$ and $\tilde{R}$ is not of the form R_0^p with $R_0 \in \mathbb{K}(x)$. For convention, if $p = 0$, the p-reduction of R equals R itself. For each $\alpha \in \overline{\mathbb{K}}$, we set $R^{-\infty}(\alpha) = \cup_{n \geq 0}\{\beta \in \overline{\mathbb{K}} \mid R^{(n)}(\beta) = \alpha\}$, the reversed R-orbit of α. Also, $\alpha \in \overline{\mathbb{K}}$ is R-critical if*

$$\sup_{n \geq 0} \Delta_{\alpha,R}(n) < +\infty,$$

where $\Delta_{\alpha,R}(n)$ denotes the number of distinct solutions of $R^{(n)}(x) = \alpha$ over $\overline{\mathbb{K}}$.

Our main results can be stated as follows.

Theorem 7.2. *Let $\mathbb{K}$ be a perfect field of characteristic $p \geq 0$ and let $R = G/H \in \mathbb{K}(x)$ be a rational function whose p-reduction $\tilde{R} = g/h$ has degree $d > 1$. Let $d' \geq 0$ be the degree of $W = g'h - gh'$, where f' denotes the formal derivative of f. Suppose that $\alpha \in \overline{\mathbb{K}}$ is not R-critical and set $e = [\mathbb{K}(\alpha) : \mathbb{K}]$. Then there exists $0 < c_{\alpha,R} \leq 1$ such that*

$$\Delta_{\alpha,R}(n) = c_{\alpha,R} d^n + O_{\alpha,R}(1).$$

The constant $c_{\alpha,R}$ can be implicitly computed from the set $R^{-\infty}(\alpha)$ and we have the following estimates:

1. *If α is not R-periodic, then $c_{\alpha,R} \geq \frac{1}{d^2} - \frac{1}{d^3}$. Moreover,*
   (a) *$c_{\alpha,R} \geq 1 - \frac{d'}{de} \geq \frac{1}{d}$ if $e > 1$;*
   (b) *$c_{\alpha,R} \geq 1 - \frac{\min\{d-1,d'\}}{d} - \frac{d'-\min\{d-1,d'\}}{d^2} \geq \frac{1}{d^2}$ if $e = 1$ and $R^{-\infty}(\alpha)$ does not contain an element $\gamma \in \mathbb{K}$ with $\deg(G - \gamma H) < \deg(R)$.*
2. *If α is R-periodic of period N, then $c_{\alpha,R} \geq \frac{1}{4d^2}$. Moreover,*
   (a) *$c_{\alpha,R} \geq 1 - \frac{d'}{e(d-1)} \geq \frac{1}{3}$ if $e > 2$;*
   (b) *$c_{\alpha,R} \geq \frac{1}{d^2} - \frac{1}{d^3}$ if $e = 2$.*

Theorem 7.3. *Let $\mathbb{K}$ be a perfect field of characteristic $p \geq 0$ and let $R = g/h \in \mathbb{K}(x)$ be a rational function of degree D whose p-reduction has degree $d \geq 1$. Fix $\alpha \in \overline{\mathbb{K}}$ and set $e = [\mathbb{K}(\alpha) : \mathbb{K}]$. Then α is R-critical if and only if one of the following holds:*

1. *$d = 1$, that is, $R(x) = \frac{ax^D+b}{cx^D+d}$ with $ad - bc \neq 0$ and $D = 1$ if $p = 0$ or $D = p^h, h \geq 0$, otherwise.*
2. *$d > 1, \alpha \in \mathbb{K}$ is not R-periodic and*
   (a) *$R(x) = \alpha + \frac{\lambda}{h(x)}$ for some $\lambda \in \mathbb{K}^*$ and some $h \in \mathbb{K}[x]$ of degree D;*
   (b) *$R(x) = \beta + \frac{\lambda}{(x-\beta)^D - \frac{\lambda}{\beta-\alpha}}$ for some $\beta, \lambda \in \mathbb{K}$ with $\beta \neq \alpha$ and $\lambda \neq 0$.*
3. *$d > 1$, $\alpha \in \overline{\mathbb{K}}$ is R-periodic of period N and*
   (a) *$e = 2, N = 1$ and $R(x) = \frac{\overline{\alpha}(x-\alpha)^D - \alpha(x-\overline{\alpha})^D}{(x-\alpha)^D - (x-\overline{\alpha})^D}$, where $\overline{\alpha} \neq \alpha$ is the conjugate root of the minimal polynomial of α over $\mathbb{K}$.*
   (b) *$e = N = 2$ and $R(x) = \frac{\alpha(x-\alpha)^D - \overline{\alpha}(x-\overline{\alpha})^D}{(x-\alpha)^D - (x-\overline{\alpha})^D}$, where $\overline{\alpha} \neq \alpha$ is the conjugate root of the minimal polynomial of α over $\mathbb{K}$.*
   (c) *$e = 1, d = 2, N = 3$ and $R(x) = \frac{y_1(x-y_1)^D - (y_1+y_2)(x-y_2)^D}{(x-y_1)^D - 2(x-y_2)^D}$, where $y_1 \neq y_2$ are elements of $\mathbb{K}$ and $\alpha \in \{y_1, y_2, \frac{y_1+y_2}{2}\}$.*
   (d) *$e = 1, N = 2$ and $R(x) = \frac{\alpha(x-\alpha)^A - \beta\lambda(x-\beta)^B}{(x-\alpha)^A - \lambda(x-\beta)^B}$, where $\beta \in \mathbb{K} \setminus \{\alpha\}, \lambda \in \mathbb{K}^*$ and A, B are positive integers with $\max\{A, B\} = D$.*

(e) $e = 1, N = d = 2 \neq p$ *and* $R(x) = \beta + \frac{(\alpha-\beta)^{D+1}}{(2x-\alpha-\beta)^D+(\alpha-\beta)^D}$ *for some* $\beta \in \mathbb{K} \setminus \{\alpha\}$.

(f) $e = 1$, $N = d = 2 \neq p$ *and* $R(x) = \beta + \frac{2(\alpha-\beta)^{D+1}}{(x-\alpha)^D+(\alpha-\beta)^D}$ *for some* $\beta \in \mathbb{K} \setminus \{\alpha\}$.

(g) $e = N = 1$ *and* $R(x) = \alpha + \frac{(x-\alpha)^A}{h(x)}$ *for some* $h \in \mathbb{K}[x]$ *and some integer* $A \geq 1$ *with* $h(\alpha) \neq 0$ *and* $\max\{A, \deg(h)\} = D$.

(h) $e = N = 1$ *and* $R(x) = \frac{\beta(x-\beta)^A(x-\alpha)^{D-A}-\alpha\lambda}{(x-\beta)^A(x-\alpha)^{D-A}-\lambda}$, *where* $\beta \in \mathbb{K} \setminus \{\alpha\}, \lambda \in \mathbb{K}^*$ *and* $1 \leq A < D$.

(i) $e = N = 1, d = 2 \neq p$ *and* $R(x) = \frac{\alpha+\beta}{2} + \frac{(\alpha-\beta)^{D+1}}{4(2x-\alpha-\beta)^D-2(\alpha-\beta)^D}$ *for some* $\beta \in \mathbb{K} \setminus \{\alpha\}$.

In particular, if α *is* R*-critical, the inequality* $\Delta_{\alpha,R}(n) \leq 2$ *holds for every* $n \geq 0$ *and the reversed* R*-orbit of* α, $R^{-\infty}(\alpha)$, *is finite if and only if one of the following holds:*

1. $d \neq 1$;
2. $d = 1$ *and* α *is* R*-periodic;*
3. $d = 1$ *and* $R(x) = \frac{ax^D+b}{cx^D+d}$ *with* $c \neq 0$, *and* $\frac{a}{c} \in R^{-\infty}(\alpha)$.

Theorems 7.2 and 7.3 entail that the arithmetic function $\Delta_{\alpha,R}(n)$ is either uniformly bounded by a constant or grows exponentially. Figure 7.1 shows the dynamics of the iteration of R in the cases where the reversed R-orbit of α is finite. The cases are presented in the order that they appear in Theorem 7.3.

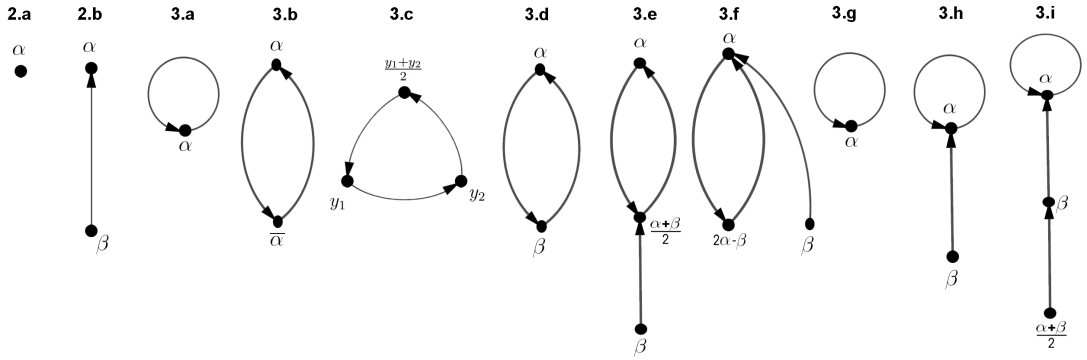

Figure 7.1: Cases where the reversed R-orbit of α is finite.

The following corollary is a straightforward application of Theorems 7.2 and 7.3 to the case where R is a polynomial.

Corollary 7.4. *Let* $\mathbb{K}$ *be a perfect field of characteristic* $p \geq 0$, $\alpha \in \overline{\mathbb{K}}$ *with* $[\mathbb{K}(\alpha) : \mathbb{K}] = e$ *and let* $f \in \mathbb{K}[x]$ *be a* D*-degree polynomial whose* p*-reduction* F *has degree* $d > 1$. *Furthermore, assume that* f *is not of the form* $a(x-\alpha)^D + \alpha$ *for some* $a \in \mathbb{K}$ *and set* $d' = \deg(F') \leq d-1$. *Then there exists a constant* $0 < c_{\alpha,f} \leq 1$ *such that*

$$\Delta_{\alpha,f}(n) = c_{\alpha,f} d^n + O_{\alpha,f}(1).$$

Moreover, $c_{\alpha,f} \geq \frac{1}{4d^2}$ *if* α *is* f*-periodic and* $c_{\alpha,f} \geq 1 - \frac{d'}{d} \geq \frac{1}{d}$, *otherwise.*

7.2 Preparation

In this section we provide some definitions and important preliminary results. Throughout this section, unless otherwise stated, $R \in \mathbb{K}(x)$ stands for a rational function of degree D whose p-reduction has degree $d \geq 1$.

Definition 7.5. *Let $R = f/g \in \mathbb{K}(x)$ be a rational function of degree $D \geq 1$ and $\alpha \in \overline{\mathbb{K}}$.*

(i) $r_{\alpha,R} \geq 0$ is the number of distinct roots of $g - \alpha h$ over $\overline{\mathbb{K}}$;

(ii) α is R-trivial if the polynomial $g - \alpha h$ has degree at most $D - 1$.

(iii) α is R-periodic if there exists an integer $N \geq 1$ such that $R^{(N)}(\alpha) = \alpha$. If α is R-periodic, the smallest integer with this property is the period of α.

Definition 7.6. *For a rational function $R \in \mathbb{K}(x)$ of degree D whose p-reduction has degree $d \geq 1$, let σ_R be the unique automorphism of $\overline{\mathbb{K}}$ satisfying $\sigma_R(a^{D/d}) = a$ for every $a \in \overline{\mathbb{K}}$.*

Remark 7.7. *We observe that σ_R is the identity map if $d = D$. If $d \neq D$, then $\mathbb{K}$ has characteristic $p > 0$ and σ_R is just the inverse of a power of the Frobenius automorphism $a \mapsto a^p$. Furthermore, for $y, \alpha \in \overline{\mathbb{K}}$, we have that $R(y) = \alpha$ if and only if $\tilde{R}(y) = \sigma_R(\alpha)$, where $\tilde{R}$ is the p-reduction of R.*

The following result is straightforward.

Lemma 7.8. *Let $R = f/g \in \mathbb{K}(x)$ be a rational function and let $\tilde{R}$ be its p-reduction, $d = \deg(\tilde{R})$. Then for every $\alpha \in \overline{\mathbb{K}}$, we have that $r_{\alpha,R} = r_{\sigma_R(\alpha),\tilde{R}}$. In particular, $r_{\alpha,R} \leq d$ for every $\alpha \in \overline{\mathbb{K}}$.*

Definition 7.9. *Let $R \in \mathbb{K}(x)$ and $\alpha \in \overline{\mathbb{K}}$. For each $n \geq 0$, set $R^{[-n]}(\alpha) = \{\beta \in \overline{\mathbb{K}} \mid R^{(n)}(\beta) = \alpha\}$ and let $R^{[-n]}(\alpha)^*$ be the set of elements $\beta \in R^{[-n]}(\alpha)$ such that no element $R^{(i)}(\beta)$ with $0 \leq i \leq n-1$ is R-periodic. Moreover, we set $\Delta_{\alpha,R}(n) = \#R^{[-n]}(\alpha)$ and $\Delta_{\alpha,R}(n)^* = \#R^{[-n]}(\alpha)^*$.*

In the proof of our main results, an implicit formula for $\Delta_{\alpha,R}(m)^*$ is required. In this context, the following definition is crucial.

Definition 7.10. *Let $R \in \mathbb{K}(x)$ be a rational function whose p-reduction has degree $d > 1$. For each $\alpha \in \overline{\mathbb{K}}$ and each integer $j \geq 2$, set*

$$n_{\alpha,j}(R) = \sum_{\gamma \in R^{[1-j]}(\alpha)^*} (d - r_{\gamma,R}) \geq 0.$$

For convention, we set $n_{\alpha,1}(R) = d - r_{\alpha,R} + 1$ if α is R-periodic and $n_{\alpha,1}(R) = d - r_{\alpha,R}$, otherwise.

We obtain the following result.

Proposition 7.11. *Let $R \in \mathbb{K}(x)$ be a rational function whose p-reduction has degree $d > 1$. Then for every $m \geq 1$ and every $\alpha \in \overline{\mathbb{K}}$, we have that*

$$\Delta_{\alpha,R}(m)^* = d^m - \sum_{j=1}^{m} n_{\alpha,j}(R) \cdot d^{m-j} = d^m \left(1 - \sum_{j=1}^{m} n_{\alpha,j}(R) d^{-j}\right).$$

Proof. We proceed by induction on m. The case $m = 1$ follows directly by the definition of $n_{\alpha,1}(R)$. Suppose that the result holds for an integer $m \geq 1$. We observe that the elements of $R^{[-m-1]}(\alpha)^*$ comprise the roots of $R(x) = \gamma$ with $\gamma \in R^{[-m]}(\alpha)$. The latter implies that

$$\Delta_{\alpha,R}(m+1)^* = d\Delta_{\alpha,R}(m)^* - \sum_{\gamma \in R^{[-m]}(\alpha)^*} (d - r_{\gamma,R}) = d\Delta_{\alpha,R}(m)^* - n_{\alpha,m+1}(R),$$

from where the result follows. ■

In the following proposition we provide estimates on the numbers $n_{\alpha,j}(R)$.

Proposition 7.12. *Let $R \in \mathbb{K}(x)$ be a rational function whose p-reduction $\tilde{R} = g/h$ has degree $d > 1$. For each $\alpha \in \overline{\mathbb{K}}$ set $\kappa_{\alpha,R} = \sum_{j \geq 1} n_{\alpha,j}(R)$, and let $\delta_{\alpha,R} = 1$ or 0, according to whether α is R-periodic or not, respectively. If $d' = \deg(g'h - gh')$, the following hold:*

(i) for distinct elements $\alpha_1, \ldots, \alpha_\ell \in \overline{\mathbb{K}}$, we have that

$$\sum_{i=1}^{\ell} \kappa_{\alpha_i,R} \leq \varepsilon + \sum_{i=1}^{\ell} \delta_{\alpha_i,R},$$

where $\varepsilon = d'$ if no set $R^{-\infty}(\alpha_i)$ contains an R-trivial element and $\varepsilon = 2d - 1$, otherwise;

(ii) $\kappa_{\alpha,R} \leq \frac{d'}{e} + \delta_{\alpha,R}$ if $[\mathbb{K}(\alpha) : \mathbb{K}] = e > 1$.

Proof. From Lemma 7.8, it follows that $r_{\gamma,R} \leq d$. For each $\gamma \in \overline{\mathbb{K}}$, let T_γ be the degree of $g - \sigma_R(\gamma)h$. We observe that the inequality $T_\gamma < d$ holds for at most one element $\gamma \in \overline{\mathbb{K}}$ and, in this case, we necessarily have that $\gamma \in \mathbb{K}$.

Since $\tilde{R}$ has degree d, Remark 7.7 entails that $d - r_{\gamma,R} > 0$ if and only if $g - \sigma_R(\gamma)h$ has $(T_\gamma - r_{\gamma,R})$ common roots with the polynomial $g' - \sigma_R(\gamma)h'$, multiplicities counted. In particular, $g - \sigma_R(\gamma)h$ has $(T_\gamma - r_{\gamma,R})$ common roots with the Wronskian $W = g'h - gh'$, multiplicities counted. From construction, the polynomials g and h are relatively prime and their formal derivatives cannot vanish simultaneously. In particular, W does not vanish and a detailed account on the possible degrees of g and h entails that $d' = \deg(W) \leq 2d - 2$.

We prove items (i) and (ii) separately.

(i) We observe that the sets $R^{[1-j]}(\alpha_i)^*$ with $j \geq 1$ and $1 \leq i \leq \ell$ are pairwise disjoint. Therefore, from the previous remarks we obtain that

$$\sum_{i=1}^{\ell} \sum_{j \geq 1} \sum_{\gamma \in R^{[1-j]}(\alpha_i)^*} (T_\gamma - r_{\gamma,R}) \leq d'. \tag{7.1}$$

If no set $R^{-\infty}(\alpha_i)$ contains an R-trivial element, it follows that $T_\gamma = d$ for every $\gamma \in R^{-\infty}(\alpha_i)$. In this case, Equation (7.1) implies that

$$\sum_{i=1}^{\ell} (\kappa_{\alpha_i,R} - \delta_{\alpha_i,R}) = \sum_{i=1}^{\ell} \sum_{j \geq 1} \sum_{\gamma \in R^{[1-j]}(\alpha_i)^*} (d - r_{\gamma,R}) \leq d'.$$

Suppose that $R^{-\infty}(\alpha_i)$ contains an R-trivial element $\lambda \in \mathbb{K}$ for some $1 \leq i \leq \ell$. We have that $g(x) = \lambda h(x) + h_0(x)$, where $\deg(h_0) = s$ with $0 \leq s < d$. Therefore, $T_\lambda = s$ and a

simple calculation yields $d' = \deg(W) \leq d + s - 1$. Since there exists at most one R-trivial element, we have that

$$\sum_{i=1}^{\ell} (\kappa_{\alpha_i,R} - \delta_{\alpha,i,R}) = (d-s) + \sum_{i=1}^{\ell} \sum_{j\geq 1} \sum_{\gamma \in R^{[1-j]}(\alpha_i)^*} (T_\gamma - r_{\gamma,R})$$
$$\leq d - s + d' \leq 2d - 1.$$

(ii) Fix $\alpha \in \overline{\mathbb{K}}$ with $[\mathbb{K}(\alpha) : \mathbb{K}] = e > 1$, hence $\alpha \notin \mathbb{K}$. Let F be the minimal polynomial of α over $\mathbb{K}$ and let $\mathbb{L} \subseteq \overline{\mathbb{K}}$ be the splitting field of F. Since $\mathbb{K}$ is a perfect field, the roots $\alpha := \alpha_1, \ldots, \alpha_e \in \overline{\mathbb{K}}$ of F are all distinct and the extension $\mathbb{L}/\mathbb{K}$ is Galois. Since the Galois group of an irreducible polynomial acts transitively on its roots, for each $1 \leq i \leq e$ there exists a $\mathbb{K}$-automorphism $\tau_i :\to L$ such that $\tau_i(\alpha) = \alpha_i$. Since $R \in \mathbb{K}(x)$, by extending these automorphisms to $\overline{\mathbb{K}}$ we conclude that $\kappa_{\alpha_i,R} = \kappa_{\alpha,R}$ and $\delta_{\alpha_i,R} = \delta_{\alpha,R}$ for every $1 \leq i \leq e$. Since $e > 1$, no element α_i lies in $\mathbb{K}$. Therefore, the sets $R^{-\infty}(\alpha_i)$ do not contain R-trivial elements. Applying item (i) for the elements $\alpha_1, \ldots, \alpha_e$, we obtain that

$$e \cdot \kappa_{\alpha,R} = \sum_{i=1}^{e} \kappa_{\alpha_i,R} \leq d' + \sum_{i=1}^{e} \delta_{\alpha_i,R} = d' + e \cdot \delta_{\alpha,R},$$

from where the result follows.

■

7.3 Proof of the main results

Before proceeding to the proof of Theorems 7.2 and 7.3, we introduce a useful definition.

Definition 7.13. *Let $R \in \mathbb{K}(x)$ be a rational function of degree D whose p-reduction has degree $d > 1$. For each $\alpha \in \overline{\mathbb{K}}$ and $j \geq 1$, let $n_{\alpha,j}(R)$ be as in Definition 7.10. If α is not R-periodic, we set*

$$c_{\alpha,R} = 1 - \sum_{j\geq 1} n_{\alpha,j}(R) d^{-j}.$$

If α is R-periodic and $\alpha_1, \ldots, \alpha_N = \alpha$ are the distinct R-periodic elements in the R-orbit of α, we set

$$c_{\alpha,R} = \frac{1}{d^N - 1} \sum_{i=1}^{N} d^i \left(1 - \sum_{j\geq 1} n_{\alpha_i,j}(R) d^{-j} \right).$$

Proposition 7.12 entails that the sum $\sum_{j\geq 1} n_{\alpha,j}(R) d^{-j}$ contains only finitely many nonzero terms; this fact is frequently used. We obtain the following estimate.

Proposition 7.14. *Let $R \in \mathbb{K}(x)$ be a rational function whose p-reduction Q has degree $d > 1$. For every $\alpha \in \mathbb{K}$, we have that*

$$\Delta_{\alpha,R}(n) = c_{\alpha,R} \cdot d^n + L_{\alpha,R}(n),$$

where $L_{\alpha,R}(n) = O_{\alpha,R}(1)$ and, in fact, $L_{\alpha,R}(n) = 0$ if α is not periodic and n is sufficiently large.

Proof. If α is not R-periodic we observe that, for every $n \geq 1$, we have that $\Delta_{\alpha,R}(n) = \Delta_{\alpha,R}(n)^*$. Proposition 7.11 implies that the equality

$$\Delta_{\alpha,R}(n) = c_{\alpha,R} \cdot d^n,$$

holds for sufficiently large n. Suppose that α is R-periodic and let $\alpha_1, \ldots, \alpha_N = \alpha$ be the distinct R-periodic elements in the R-orbit of α. By stratifying the elements $\beta \in R^{[-n]}(\alpha)$ according to how many integers $1 \leq i \leq n$ satisfy $R^{(i)}(\beta) = \alpha$, we obtain that

$$R^{[-n]}(\alpha) = \{\alpha_u\} \cup \bigcup_{i=1}^{N} \bigcup_{\substack{1 \leq m \leq n \\ N \mid n+i-m}} R^{[-m]}(\alpha_i)^*,$$

where $1 \leq u \leq N$ and $u \equiv -n \pmod{N}$. It follows from the definition that the sets $R^{[-m]}(\alpha_i)^*$ are pairwise distinct and none of them contains α_u, hence

$$\Delta_{\alpha,R}(n) = 1 + \sum_{i=1}^{N} \sum_{\substack{1 \leq m \leq n \\ N \mid n+i-m}} \Delta_{\alpha_i,R}(m)^*.$$

Let M be sufficiently large such that $\sum_{j \geq 1} n_{\alpha_i,j}(R) d^{-j} = \sum_{j=1}^{M} n_{\alpha_i,j}(R) d^{-j}$ for every $1 \leq i \leq N$. Fix an integer $t > M$, let $n > t$ be sufficiently large with $n \equiv t \pmod{N}$ and set $q = \frac{n-t}{N}$. Therefore, for a constant $C = C_t$, we have that

$$\Delta_{\alpha,R}(n) - C = \sum_{i=1}^{N} \sum_{\substack{t < m \leq n \\ N \mid n+i-m}} \Delta_{\alpha_i,R}(m)^* = \sum_{i=1}^{N} \sum_{s=1}^{q} \Delta_{\alpha_i,R}(n - Ns + i)^*.$$

Since $n - Ns + i \geq t > M$ for every $1 \leq s \leq q$ and every $1 \leq i \leq N$, Proposition 7.11 entails that $\Delta_{\alpha_i,R}(n - Ns + i)^* = d^{n-Ns+i} \cdot \theta_i$ with

$$\theta_i = 1 - \sum_{j \geq 1} n_{\alpha_i,j}(R) d^{-j}.$$

We conclude that

$$\Delta_{\alpha,R}(n) - C = \sum_{i=1}^{N} \sum_{s=1}^{q} d^{n-Ns+i} \theta_i = d^n \cdot \ell \cdot \sum_{i=1}^{N} d^i \theta_i,$$

where $\ell = \sum_{s=1}^{q} d^{-Ns} = \frac{1}{d^N - 1} + O_N(d^{-n})$. By the definition, $c_{\alpha,R} = \frac{1}{d^N-1} \sum_{i=1}^{N} d^i \theta_i$, so that $\Delta_{\alpha,R}(n) = c_{\alpha,R} \cdot d^n + C_{\alpha,R,t}$. By taking $t = M + i$ with $1 \leq i \leq N$, the error $C_{\alpha,R,t}$ is uniformly bounded by a constant $C_{\alpha,R}$. ■

Here we summarize the next steps in the proof of our main results. Proposition 7.14 implies that, for $d > 1$, $\alpha \in \overline{\mathbb{K}}$ is R-critical if and only if $c_{\alpha,R} = 0$. By employing the bounds from Proposition 7.12, we estimate the constant $c_{\alpha,R}$ and detect the possible distributions of the numbers $\{n_{\beta,j}\}_{\beta \in R^{-\infty}(\alpha)}$ in which $c_{\alpha,R} = 0$. We then characterize the pairs (α, R) that yield one of these distributions. Along with the generic critical case where $d = 1$, the latter fully describes the R-critical elements.

7.3.1 Proof of Theorem 7.2

We consider the cases where α is R-periodic or not R-periodic separately.

7.3.1.1 The case where α is not R-periodic

Recall that $c_{\alpha,R} = 1 - \sum_{j\geq 1} n_{\alpha,j}(R)d^{-j}$. If $[\mathbb{K}(\alpha):\mathbb{K}] = e > 1$, Proposition 7.12 entails that

$$c_{\alpha,R} = 1 - \sum_{j\geq 1} n_{\alpha,j}(R)d^{-j} \geq 1 - d^{-1}\sum_{j\geq 1} n_{\alpha,j}(R) \geq 1 - \frac{d'}{de} \geq \frac{1}{d},$$

where in the last inequality we used the fact that $e \geq 2$ and $d' \leq 2d-2$. Suppose that $e = 1$, that is, $\alpha \in \mathbb{K}$. We observe that $0 \leq n_{\alpha,1}(R) \leq d$ and Proposition 7.12 implies that $\sum_{j\geq 1} n_{\alpha,j}(R) \leq 2d-1$. We obtain the following trivial configurations:

- $n_{\alpha,1}(R) = d$;
- $n_{\alpha,1}(R) = d-1$ and $n_{\alpha,2}(R) = d$.

In both cases, it follows that $c_{\alpha,R} = 0$ and then α is R-critical. Suppose that α does not satisfy none of the cases described above. If $R^{-\infty}(\alpha)$ contains an R-trivial element, it follows that

$$c_{\alpha,R} = 1 - \sum_{j\geq 1} n_{\alpha,j}(R)d^{-j} \geq 1 - (d-1)\cdot d^{-1} - (d-1)\cdot d^{-2} - 1\cdot d^{-3} = \frac{1}{d^2} - \frac{1}{d^3}.$$

Otherwise, Proposition 7.12 entails that $\sum_{j\geq 1} n_{\alpha,j}(R) \leq d' \leq 2d-2$ and so

$$c_{\alpha,R} = 1 - \sum_{j\geq 1} n_{\alpha,j}(R)d^{-j} \geq 1 - \min\{d-1,d'\}\cdot d^{-1} - (d' - \min\{d-1,d'\})\cdot d^{-2} \geq \frac{1}{d^2}.$$

We combine all the previous bounds and obtain that $c_{\alpha,R} \geq \frac{1}{d^2} - \frac{1}{d^3}$ if α is neither R-periodic nor R-critical. This proves Theorem 7.2 for the non periodic case.

7.3.1.2 The case where α is R-periodic

Let $\alpha_1,\ldots,\alpha_N = \alpha$ be the distinct R-periodic elements in the R-orbit of α and, for each $1 \leq i \leq N$, set $\theta_i = 1 - \sum_{j\geq 1} n_{\alpha_i,j}(R)d^{-j}$. It follows from the definition that $c_{\alpha,R} = \frac{1}{d^N-1}\sum_{i=1}^{N} d^i\theta_i$. Moreover, $R^{-\infty}(\alpha_i) = R^{-\infty}(\alpha)$ for every $1 \leq i \leq N$. Proposition 7.11 entails that each θ_i is nonnegative, hence $c_{\alpha,R} > 0$ unless all the elements θ_i vanish. Proposition 7.12 provides the bound

$$\sum_{i=1}^{N}\sum_{j\geq 1} n_{\alpha_i,j}(R) \leq \varepsilon + N, \tag{7.2}$$

where $\varepsilon = d'$ if no set $R^{-\infty}(\alpha)$ contains an R-trivial element and $\varepsilon = 2d-1$, otherwise. Set $e = [\mathbb{K}(\alpha):\mathbb{K}]$. We split the proof into cases.

(i) Suppose that $e > 1$. It is direct to verify that $\mathbb{K}(\alpha_i) = \mathbb{K}(\alpha)$ for every $1 \leq i \leq N$ and so $[\mathbb{K}(\alpha_i):\mathbb{K}] = e$. In particular, no set $R^{-\infty}(\alpha_i)$ contains an R-trivial element. Since each α_i is R-periodic, $n_{\alpha_i,1}(R) \geq 1$ for every $1 \leq i \leq N$. In particular, Proposition 7.12 implies that $1 \leq \sum_{j\geq 1} n_{\alpha_i,j}(R) \leq d'/e + 1$. For $e > 2$, it follows that

$$\begin{aligned} c_{\alpha,R} &\geq \frac{1}{d^N-1}\sum_{i=1}^{N} d^i\left(1 - d^{-1}\sum_{j\geq 1} n_{\alpha_i,j}(R)\right) \\ &\geq \frac{1}{d^N-1}\sum_{i=1}^{N} d^i\left(1 - \frac{d'}{de} - \frac{1}{d}\right) = 1 - \frac{d'}{(d-1)e} \geq \frac{1}{3}, \end{aligned}$$

since $e > 2$ and $d' \leq 2(d-1)$. If $e = 2 < N$, Equation (7.2) implies that

$$c_{\alpha,R} = \frac{1}{d^N - 1} \sum_{i=1}^{N} d^i \left(1 - \sum_{j \geq 1} n_{\alpha_i,j}(R) d^{-i}\right)$$
$$\geq \frac{1}{d^N - 1} \sum_{i=1}^{N-2} d^i \left(1 - \frac{1}{d}\right) = \frac{d^{N-2} - 1}{d^N - 1} \geq \frac{1}{d^2} - \frac{1}{d^3}.$$

It remains to consider the cases where $e = 2$ and $N = 1, 2$. Equation (7.2) and the bound $\sum_{j \geq 1} n_{\alpha_i,j}(R) \leq d'/e + 1 \leq d$ yield the following trivial configurations:

- $e = 2, N = 1$ and $n_{\alpha,1}(R) = d$;
- $e = 2, N = 2$ and $n_{\alpha_1,1}(R) = n_{\alpha_2,1}(R) = d$.

In both cases, it follows that $c_{\alpha,R} = 0$ and so α is R-critical. Suppose that α does not satisfy none of the cases described above. For $N = 1$, the inequality $n_{\alpha,1}(R) < d$ implies that

$$c_{\alpha,R} = \frac{d\theta_1}{d-1} \geq \frac{d\left(1 - (d-1) \cdot d^{-1} - 1 \cdot d^{-2}\right)}{d-1} = \frac{1}{d} \geq \frac{1}{d^2} - \frac{1}{d^3}.$$

For $N = 2$, recall that we are under the condition $(n_{\alpha_1,1}(R), n_{\alpha_2,1}(R)) \neq (d, d)$. In particular, from the argument employed in the case $N = 1$, the inequality $\theta_i \geq \frac{d-1}{d^2}$ holds for at least one index $i \in \{1, 2\}$. Therefore,

$$c_{\alpha,R} = \frac{d\theta_1 + d^2\theta_2}{d^2 - 1} \geq \frac{d \cdot \frac{d-1}{d^2} + d^2 \cdot 0}{d^2 - 1} = \frac{1}{d(d+1)} \geq \frac{1}{d^2} - \frac{1}{d^3}.$$

(ii) Suppose that $e = 1$. Since $R^{-\infty}(\alpha)$ can contain an R-trivial element, Equation (7.2) implies that

$$\sum_{i=1}^{N} \sum_{j \geq 1} n_{\alpha_i,j}(R) \leq 2d - 1 + N. \tag{7.3}$$

We recall that $n_{\alpha_i,1}(R) \geq 1$. For $N \geq 3$, it follows that

$$c_{\alpha,R} \geq \frac{1}{d^N - 1} \sum_{i=1}^{N} d^i \left(1 - d^{-1} \sum_{j \geq 1} n_{\alpha_i,j}(R)\right)$$
$$\geq \frac{1}{d^N - 1} \left(\sum_{i=1}^{N-2} d^i \left(1 - d^{-1}\right) - d^{N-2} d^{-1}\right) = \frac{d^{N-2}(d-1) - d}{d(d^N - 1)} > \frac{1}{4d^2},$$

provided that $d > 2$ if $N = 3$. If $(d, N) = (2, 3)$, Equation (7.2) yields the trivial configuration $n_{\alpha_1,1}(R) = n_{\alpha_2,1}(R) = n_{\alpha_3,1}(R) = 2$, in which $c_{\alpha,R} = 0$ and so α is R-critical. If $(d, N) = (2, 3)$ and α is not R-critical, then $n_{\alpha_i,1}(R) = 1$ for at least one index $i \in \{1, 2, 3\}$. In particular, $\theta_i \geq (1 - 2^{-1} - 2^{-2}) = \frac{1}{4}$ for at least one index $i \in \{1, 2, 3\}$ and so

$$c_{\alpha,R} = \frac{2\theta_1 + 4\theta_2 + 8\theta_3}{7} \geq \frac{2 \cdot \frac{1}{4} + 4 \cdot 0 + 8 \cdot 0}{7} = \frac{1}{14} > \frac{1}{4 \cdot 2^2}.$$

For $N = 2$, Equation (7.3) yields the following trivial configurations:

- $e = 1, n_{\alpha_1,1}(R) = n_{\alpha_2,1}(R) = d$;
- $e = 1, d = 2$, $n_{\alpha_2,1}(R) = 2$, $n_{\alpha_1,1}(R) = 1$ and $n_{\alpha_1,2}(R) = 2$;

- $e = 1, d = 2$, $n_{\alpha_2,1}(R) = 1$, $n_{\alpha_2,2}(R) = 2$ and $n_{\alpha_1,1}(R) = 2$.

In these cases, it follows that $c_{\alpha,R} = 0$ and so α is R-critical. Suppose that α does not satisfy none of the cases described above. For $d > 2$, we employ the same argument used in the case $e = N = 2$ and obtain that

$$c_{\alpha,R} \geq \frac{d(1-(d-1)d^{-1}-2d^{-2})}{d^2-1} = \frac{d-2}{d(d^2-1)} > \frac{1}{4d^2}.$$

For $d = 2$ we have that $\theta_i \geq (1 - 2^{-1} - 2^{-2} - 2^{-3}) = \frac{1}{8}$ for at least one index $i \in \{1, 2\}$, hence

$$c_{\alpha,R} = \frac{2\theta_1 + 4\theta_2}{3} \geq \frac{2 \cdot \frac{1}{8} + 4 \cdot 0}{3} = \frac{1}{12} > \frac{1}{4 \cdot 2^2}.$$

For $N = 1$, Equation (7.3) yields the following trivial configurations:

- $e = 1, n_{\alpha,1}(R) = d$;
- $e = 1, n_{\alpha,1}(R) = d - 1$ and $n_{\alpha,2}(R) = d$.

In both cases, it follows that $c_{\alpha,R} = 0$ and so α is R-critical. If α does not satisfy any of the cases described above, then either $n_{\alpha,1}(R) < d$ or $n_{\alpha,1}(R) = d$ and $n_{\alpha,2}(R) < d$. In particular, Equation (7.3) implies that

$$c_{\alpha,R} = \frac{d\theta_1}{d-1} \geq \frac{d(1-d^{-1}(d-1)-d^{-2}(d-1)-2d^{-3})}{d-1} = \frac{d-2}{d^2(d-1)} > \frac{1}{4d^2},$$

whenever $d > 2$. For $d = 2$, Equation (7.3) yields the trivial configuration $n_{\alpha,1}(R) = n_{\alpha,2}(R) = 1$ and $n_{\alpha,3}(R) = 2$, in which $c_{\alpha,R} = 0$ and so α is R-critical. If α is not R-critical, then

$$c_{\alpha,R} = 2\theta_1 \geq 2(1 - 2^{-1} - 2^{-2} - 2^{-3} - 2^{-4}) = \frac{1}{8} > \frac{1}{4 \cdot 2^2}.$$

We combine all the previous bounds and obtain that if α is R-periodic and not R-critical, then $c_{\alpha,R} \geq \frac{1}{4d^2}$. This completes the proof of Theorem 7.2.

7.3.2 Proof of Theorem 7.3

Let $R = g/h$ be a rational function of degree D whose p-reduction has degree $d \geq 1$. If $d = 1$ it is direct to verify that $R(x) = \frac{ax^D+b}{cx^D+d}$ with $ad - bc \neq 0$ and either $D = 1$ or $\mathbb{K}$ has characteristic $p > 0$ and D is a power of p. Hence for every $n \geq 0$ we have that $R^{(n)}(x) = \frac{a_n x^{D^n}+b_n}{c_n x^{D^n}+d_n}$, where $a_n, b_n, c_n, d_n \in \mathbb{K}$ with $a_n d_n - b_n c_n \neq 0$. Since $\mathbb{K}$ is perfect it follows that for every $\alpha \in \overline{\mathbb{K}}$ and every $n \geq 0$, the equation $R^{(n)}(x) = \alpha$ has at most 1 solution in $\overline{\mathbb{K}}$. Hence every $\alpha \in \overline{\mathbb{K}}$ is R-critical and $R^{-\infty}(\alpha)$ is finite if and only if α is R-periodic or $c \neq 0$ and $R^{-\infty}(\alpha)$ contains the R-trivial element $\beta = \frac{a}{c}$.

For $d > 1$, Proposition 7.14 entails that α is R-critical if and only if $c_{\alpha,R} = 0$. From the proof of Theorem 7.2, we list the possible numerical configurations that yields $c_{\alpha,R} = 0$. As follows, we present them in the order that they appear.

I. α is not R-periodic and

(a) $n_{\alpha,1}(R) = d$;

(b) $n_{\alpha,1}(R) = d-1$ and $n_{\alpha,2}(R) = d$.

II. $\alpha = \alpha_N$ is R-periodic with period N and

(a) $e = 2$, $N = 1$ and $n_{\alpha_1,1}(R) = d$;

(b) $e = 2$, $N = 2$ and $n_{\alpha_1,1}(R) = n_{\alpha_2,1}(R) = d$;

(c) $e = 1$, $N = 3$, $d = 2$ and $n_{\alpha_1,1} = n_{\alpha_2,1} = n_{\alpha_3,1} = 2$;

(d) $e = 1$, $N = 2$ and $n_{\alpha_1,1}(R) = n_{\alpha_2,1}(R) = d$;

(e) $e = 1$, $N = 2$, $d = 2$, $n_{\alpha_2,1}(R) = 2$, $n_{\alpha_1,1}(R) = 1$ and $n_{\alpha_1,2}(R) = 2$;

(f) $e = 1$, $N = 2$, $d = 2$, $n_{\alpha_2,1}(R) = 1$, $n_{\alpha_2,2}(R) = 2$ and $n_{\alpha_1,1}(R) = 2$;

(g) $e = 1$, $N = 1$ and $n_{\alpha,1}(R) = d$;

(h) $e = 1$, $N = 1$ and $n_{\alpha,1}(R) = d-1$ and $n_{\alpha,2}(R) = d$;

(i) $e = 1$, $N = 1$, $d = 2$, $n_{\alpha,1} = n_{\alpha,2} = 1$ and $n_{\alpha,3} = 2$.

Remark 7.15. *If $\beta \in \overline{\mathbb{K}}$ is not an R-periodic element, then $n_{\beta,1}(R) = d$ if and only if β is the R-critical element and* $\deg(g - \beta h) = 0$. *In this case, $\beta \in \mathbb{K}$ and there exists $\lambda \in \mathbb{K}^*$ such that $g(x) = \beta h(x) + \lambda$.*

We characterize the pairs (α, R) satisfying the numerical conditions above and explicitly exhibit the set $R^{-\infty}(\alpha)$ in the corresponding case. In order to simplify calculations, we frequently use the fact that $\frac{g}{h} = \frac{ag}{ah}$ for every $a \in \overline{\mathbb{K}}^*$.

I. (a) Since $r_{\alpha,R} = d - n_{\alpha,1}(R) = 0$ and α is not R-periodic, it follows that $g(x) - \alpha h(x) = \lambda$ for some $\lambda \in \mathbb{K}^*$. Therefore, $R(x) = \alpha + \frac{\lambda}{h(x)}$ for some $h \in \mathbb{K}[x]$ of degree D. In this case, $R^{-\infty}(\alpha) = \{\alpha\}$.

(b) Since $r_{\alpha,R} = d - n_{\alpha,1}(R) = 1$ and $n_{\alpha,2}(R) = d$, Remark 7.15 entails that

$$\begin{cases} g(x) - \alpha h(x) = (x-\beta)^D; \\ g(x) - \beta h(x) = \lambda, \end{cases}$$

for some $\beta \in \mathbb{K} \setminus \{\alpha\}$ and some $\lambda \in \mathbb{K}^*$. By solving this system of equations, we obtain that $R(x) = \beta + \frac{\lambda}{(x-\beta)^D - \frac{\lambda}{\beta-\alpha}}$. In this case, $R^{-\infty}(\alpha) = \{\alpha, \beta\}$.

II. (a) Since $e = 2$, α is not an R-critical element. Since $r_{\alpha,R} = d + 1 - n_{\alpha,1} = 1$ and $N = 1$, we obtain that $g(x) - \alpha h(x) = (x-\alpha)^D$. If τ is the unique non trivial $\mathbb{K}$-automorphism of $\mathbb{K}(\alpha)$, it follows that $g(x) - \overline{\alpha} h(x) = (x - \overline{\alpha})^D$ with $\overline{\alpha} = \tau(\alpha)$. We conclude that $R(x) = \frac{\overline{\alpha}(x-\alpha)^D - \alpha(x-\overline{\alpha})^D}{(x-\alpha)^D - (x-\overline{\alpha})^D}$ and $R^{-\infty}(\alpha) = \{\alpha\}$.

(b) Since $e = 2$, α is not an R-critical element. Since $N = 2$ and $r_{\alpha_i,R} = n_{\alpha_i,1} - d + 1 = 1$ for $i = 1, 2$, we obtain that $g(x) - \alpha_1 h(x) = (x-\alpha_2)^D$ and $g(x) - \alpha_2 h(x) = \lambda(x-\alpha_1)^D$ for some $\lambda \in \overline{\mathbb{K}}$. Arguing similarly to item II-(a), we necessarily have that $(\alpha_1, \alpha_2) = (\overline{\alpha}, \alpha)$ and $\lambda = 1$. The latter implies that $R(x) = \frac{\alpha(x-\alpha)^D - \overline{\alpha}(x-\overline{\alpha})^D}{(x-\alpha)^D - (x-\overline{\alpha})^D}$ and so $R^{-\infty}(\alpha) = \{\alpha, \overline{\alpha}\}$.

(c) Let $\tilde{R} = \tilde{g}/\tilde{h}$ be the p-reduction of R. We observe that $r_{\alpha_i,R} = 2 + 1 - n_{\alpha_i,1}(R) = 1$ for $i \in \{1,2,3\}$. Following the proof of item (i) in Proposition 7.12, the latter entails that one of the elements α_i is R-critical and

$$\begin{cases} \tilde{g}(x) - \sigma_R(y_1)\tilde{h}(x) = (x-y_2)^2; \\ \tilde{g}(x) - \sigma_R(y_2)\tilde{h}(x) = \gamma(x-y_3)^2; \\ \tilde{g}(x) - \sigma_R(y_3)\tilde{h}(x) = \lambda(x-y_1), \end{cases}$$

where $\gamma, \lambda \in \mathbb{K}^*$ and $\{y_1, y_2, y_3\}$ is a permutation of $\{\alpha_1, \alpha_2, \alpha_3\}$. The system above implies that $2y_1 = y_2 + y_3$, $\gamma = \frac{\sigma_R(y_2)-\sigma_R(y_3)}{\sigma_R(y_1)-\sigma_R(y_3)}$ and $\lambda = (\sigma_R(y_2) - \sigma_R(y_3))(2y_2 - 2y_3)$. If $\mathbb{K}$ has characteristic 2 we have that $y_2 = y_3$, a contradiction. Hence $\mathbb{K}$ does not have characteristic 2 and so $y_1 = \frac{y_2+y_3}{2}, \gamma = 2$. We return to the initial equations, and after some calculations we obtain that

$$\tilde{R}(x) = \frac{\sigma_R(y_2)(x-y_2)^2 - \sigma_R(y_2+y_3)(x-y_3)^2}{(x-y_2)^2 - 2(x-y_3)^2}.$$

Since $R = \tilde{R}^{D/2}$ and either $D/2 = 1$ or $\mathbb{K}$ has characteristic $p > 0$ and $D/2 = p^h$, it follows from the definition of σ_R that

$$R(x) = \frac{y_2(x-y_2)^D - (y_2+y_3)(x-y_3)^D}{(x-y_2)^D - 2(x-y_3)^D}.$$

Moreover, $\alpha \in \{y_2, y_3, \frac{y_2+y_3}{2}\} = R^{-\infty}(\alpha)$.

(d) Similarly to the case II-(b) we have that if $(\alpha_1, \alpha_2) = (\beta, \alpha)$, then $g(x) - \beta h(x) = (x-\alpha)^A$ and $g(x) - \alpha h(x) = \lambda(x-\beta)^B$ for some $\lambda \in \mathbb{K}^*$ and some integers $A, B \geq 1$ with $\max\{A, B\} = D$. The latter implies that $R(x) = \frac{\alpha(x-\alpha)^A - \beta\lambda(x-\beta)^B}{(x-\alpha)^A - \lambda(x-\beta)^B}$ and so $R^{-\infty}(\alpha) = \{\alpha, \beta\}$.

(e) Set $\eta = \alpha_1$. Since $r_{\alpha,R} = d + 1 - n_{\alpha,1}(R) = 1$ and $r_{\eta,R} = d + 1 - n_{\alpha_2,1}(R) = 2$, there exists an element β that is not R-periodic with $R(\beta) = \eta$. Moreover, we have that $r_{\beta,R} = 0$ and then

$$\begin{cases} \tilde{g}(x) - \sigma_R(\alpha)\tilde{h}(x) = (x-\eta)^2; \\ \tilde{g}(x) - \sigma_R(\eta)\tilde{h}(x) = \gamma(x-\alpha)(x-\beta); \\ \tilde{g}(x) - \sigma_R(\beta)\tilde{h}(x) = \lambda, \end{cases}$$

for some $\lambda, \gamma \in \mathbb{K}^*$, where $\tilde{R} = \tilde{g}/\tilde{h}$ is the p-reduction of R. These equations imply that $2\sigma_R(\eta) = \sigma_R(\alpha) + \sigma_R(\beta)$, $\gamma = \frac{\sigma_R(\beta)-\sigma_r(\eta)}{\sigma_R(\beta)-\sigma_R(\alpha)}$ and $\eta^2 + \lambda\frac{\sigma_R(\eta)-\sigma_R(\alpha)}{\sigma_R(\beta)-\sigma_R(\eta)} = \alpha\beta$. If $\mathbb{K}$ has characteristic 2 the latter entails that $\alpha = \beta$, a contradiction. Hence $\mathbb{K}$ does not have characteristic 2 and so $\eta = \frac{\alpha+\beta}{2}$, $\gamma = \frac{1}{2}$ and $\lambda = -\frac{(\alpha-\beta)^2}{4}$. We return to the initial equations, and after some calculations we obtain that

$$\tilde{R}(x) = \sigma_R(\beta) + \frac{(\alpha-\beta)^2(\sigma_R(\alpha) - \sigma_R(\beta))}{(2x-\alpha-\beta)^2 + (\alpha-\beta)^2}.$$

Since $R = \tilde{R}^{D/2}$ and either $D/2 = 1$ or $\mathbb{K}$ has characteristic $p > 0$ and $D/2 = p^h$, it follows from the definition of σ_R that

$$R(x) = \beta + \frac{(\alpha-\beta)^{D+1}}{(2x-\alpha-\beta)^D + (\alpha-\beta)^D}.$$

In this case, $R^{-\infty}(\alpha) = \{\alpha, \beta, \frac{\alpha+\beta}{2}\}$.

(f) This case is entirely similar to item II-(e). We conclude that $\mathbb{K}$ does not have characteristic 2 and
$$R(x) = \beta + \frac{2(\alpha-\beta)^{D+1}}{(x-\alpha)^D + (\alpha-\beta)^D}.$$
Moreover, $R^{-\infty}(\alpha) = \{\alpha, \beta, 2\alpha - \beta\}$.

(g) Since $r_{\alpha,R} = d + 1 - n_{\alpha,1}(R) = 1$ and $N = 1$, it follows that $g(x) - \alpha h(x) = (x-\alpha)^A$ for some $1 \leq A \leq D$. We conclude that $R(x) = \alpha + \frac{(x-\alpha)^A}{h(x)}$ for some $h \in \mathbb{K}[x]$ with $h(\alpha) \neq 0$ and $\max\{\deg(h), A\} = D$. Moreover, $R^{-\infty}(\alpha) = \{\alpha\}$.

(h) Since $r_{\alpha,R} = d + 1 - n_{\alpha,1}(R) = 2$ and $n_{\alpha,2}(R) = d$, there exists $\beta \in \mathbb{K} \setminus \{\alpha\}$ such that $R(\beta) = \alpha$ and $r_{\beta,R} = 0$. Therefore, $g(x) - \alpha h(x) = (x-\beta)^A(x-\alpha)^{D-A}$ and $g(x) - \beta h(x) = \lambda$ for some $\lambda \in \mathbb{K}^*$ and some integer $1 \leq A < D$. The latter implies that $R(x) = \frac{\beta(x-\beta)^A(x-\alpha)^{D-A} - \alpha\lambda}{(x-\beta)^A(x-\alpha)^{D-A} - \lambda}$. Moreover, $R^{-\infty}(\alpha) = \{\alpha, \beta\}$.

(i) This case is entirely similar to item II-(e). We conclude that $\mathbb{K}$ does not have characteristic 2 and
$$R(x) = \frac{\alpha+\beta}{2} + \frac{(\alpha-\beta)^{D+1}}{4(2x-\alpha-\beta)^D - 2(\alpha-\beta)^D}.$$
Moreover, $R^{-\infty}(\alpha) = \{\alpha, \beta, \frac{\alpha+\beta}{2}\}$.

In particular, if α is R-critical, then $\Delta_{\alpha,R}(n) \leq 2$ for every $n \geq 0$. Moreover, for $d > 1$, we have verified that the set $R^{-\infty}(\alpha)$ is finite. The proof of Theorem 7.3 is complete.

7.4 Further results in the finite field setting

Throughout this section, $\mathbb{F}_q$ denotes the finite field of q elements, where q is a prime power. Let $\mathcal{M}_q$ be the set of monic polynomials $f \in \mathbb{F}_q[x]$ of positive degree, without any root in $\mathbb{F}_q$.

Definition 7.16. *Given a rational function $R = g/h \in \mathbb{F}_q(x)$ of degree $D \geq 1$ and $f \in \mathcal{M}_q$, we set $f_R = h^{\deg(f)} \cdot f\left(\frac{g}{h}\right)$. For each $n \geq 0$, the n-th R-transform of f is the polynomial $f_R^{(n)}$ defined by $f_R^{(0)} = f$ and $f_R^{(n)} = (f_R^{(n-1)})_R$ if $n \geq 1$. Moreover, let*
$$f_R^{(n)}(x) = p_{1,n}(x)^{e_{1,n}} \dots p_{N_n,n}(x)^{e_{N_n,n}},$$
be the irreducible factorization of $f_R^{(n)}$ in $\mathbb{F}_q[x]$. We define the following arithmetic functions

(a) $\delta_{f,R}(n) = \deg(p_{1,n}(x) \cdots p_{N_n,n}(x))$ is the degree of the squarefree part of $f_R^{(n)}$;

(b) $M_{f,R}(n) = \max\limits_{1 \leq i \leq N_n} \deg(p_{i,n}(x))$ is the largest degree of an irreducible factor of $f_R^{(n)}$ over $\mathbb{F}_q$;

(c) $N_{f,R}(n) = N_n$ is the number of distinct irreducible factors of $f_R^{(n)}$ over $\mathbb{F}_q$;

(d) $A_{f,R}(n) = \frac{\Delta_{f,R}(n)}{N_{f,R}(n)}$ is the average degree of the distinct irreducible factors of $f_R^{(n)}$ over $\mathbb{F}_q$.

The above naturally extends Definition 1.2 in [79], where $R = g$ is a polynomial. In [79] the author explores the growth (linear, polynomial, exponential) of the functions above, among some others. Our aim here is to discuss the growth of these arithmetic functions in the context of rational functions. For functions $\mathcal{F}, \mathcal{G} : \mathbb{N} \to \mathbb{R}_{>0}$, we write $\mathcal{F} \gg \mathcal{G}$ if there exists $c > 0$ such that $c \cdot \mathcal{F}(n) \geq \mathcal{G}(n)$ for every n sufficiently large. We also write $\mathcal{F} \approx \mathcal{G}$ if $\mathcal{F} \gg \mathcal{G}$ and $\mathcal{G} \gg \mathcal{F}$. We have the following result.

Lemma 7.17. *Given a rational function $R = g/h \in \mathbb{F}_q(x)$ of degree $D \geq 1$. Then for every $f \in \mathcal{M}_q$, the polynomials $f_R^{(n)}$ and $f_{R^{(n)}}$ have the same roots. In particular, if $\alpha_1, \ldots, \alpha_s \in \overline{\mathbb{F}}_q$ are the distinct roots of f, we have that*

$$\delta_{f,R}(n) = \sum_{i=1}^{s} \Delta_{\alpha_i,R}(n).$$

Proof. It suffices to prove the first statement. We proceed by induction on n. The cases $n = 0, 1$ follow directly by the definition. Suppose that the result holds for some $n \geq 1$ and let $N = n + 1$. We observe that, for every $k \geq 0$ and every $F \in \mathcal{M}_q$, the roots of $F_{R^{(k)}}$ comprise the solutions of the equations $R^{(k)}(x) = \alpha$ with α running over the roots of F. In particular, if $\beta \in \overline{\mathbb{F}}_q$ is a root of $f_{R^{(N)}}$, then $R(\beta)$ is a root of $f_{R^{(n)}}$. From induction hypothesis, $R(\beta)$ is a root of $f_R^{(n)}$, hence β is a root of $(f_R^{(n)})_R = f_R^{(N)}$. This proves that every root of $f_{R^{(N)}}$ is also a root of $f_R^{(n)}$. The converse follows in a similar way, proving the result. ■

Combining Lemma 7.17 with Theorems 7.2 and 7.3, we obtain the following result.

Corollary 7.18. *Let $R \in \mathbb{F}_q(x)$ be a rational function whose p-reduction has degree $d > 1$. If $f \in \mathcal{M}_q$ has at least one root α that is not R-critical, then there exists a constant $0 < c_{f,R} \leq \deg(f)$ such that*

$$\delta_{f,R}(n) = c_{f,R} \cdot d^n + O_{f,R}(1).$$

In this case, $M_{f,R}(n) \gg n$. In particular, any $f \in \mathcal{M}_q$ having at least one root in the set $\overline{\mathbb{F}}_q \setminus \mathbb{F}_{q^2}$ satisfies the above.

Proof. Pick n large such that $\delta_{f,R} > 0$. Let $m_n = M_{f,R}(n)$, hence the roots of f_n^R all lie in the set $\bigcup_{1 \leq j \leq m_n} \mathbb{F}_{q^j}$. Therefore,

$$\delta_{f,R}(n) \leq \sum_{j=1}^{m_n} q^j < q^{m_n+1},$$

and so $m_n \geq \frac{\log \delta_{f,R}(n)}{\log q} - 1 \gg n$ since $\delta_{f,R} \gg d^n$ and $d > 1$. Moreover, from Theorem 7.3, we have that any R-critical element lies in $\mathbb{F}_{q^2}$ if the p-reduction of R has degree $d > 1$. ■

Corollary 7.18 entails that under mild conditions on (f, R), the arithmetic function $M_{f,R}(n)$ grows at least linearly with respect to n. When $R = g$ is a polynomial, we recover Lemma 4.4 in [79]. According to [79], this lower bound is optimal on the growth type. More precisely, if $f \in \mathbb{F}_q[x]$ has positive degree, for infinitely many polynomials g we have that $M_{f,g}(n), A_{f,g}(n) \approx n$. The family of polynomials g taken there comprise linearized polynomials $\sum_{i=0}^{t} a_i x^{q^i}$. For more details, see Proposition 5.18 in [79]. As follows, we prove that this bound is also optimal for rational functions that are not polynomials. Our main idea is to conjugate a polynomial with a Möbius map in a way that the resulting rational function is not a polynomial. We need the following technical lemmas.

Lemma 7.19 ([92])**.** *For $[A] \in \mathrm{PGL}(2, q)$ with $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $\alpha \in \overline{\mathbb{F}}_q \setminus \mathbb{F}_q$ and $f \in \mathbb{F}_q[x]$ of degree $k \geq 1$, set $[A] \circ f(x) = (bx + d)^k f\left(\frac{ax+c}{bx+d}\right)$ and $[A] * \alpha = \frac{d\alpha - c}{-b\alpha + a}$. Then for $f \in \mathcal{M}_q$, the polynomial $[A] \circ f$ has degree k and, if $\alpha \in \overline{\mathbb{F}}_q \setminus \mathbb{F}_q$, we have that $f(\alpha) = 0 \iff ([A] \circ f)([A] * \alpha) = 0$.*

Lemma 7.20. *For* $[A] \in \mathrm{PGL}(2,q)$ *with* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *and* $R \in \overline{\mathbb{F}}_q(x) \setminus \mathbb{F}_q$, *set* $[A] \bullet R = \frac{aR+c}{bR+d}$. *This defines an action of* $\mathrm{PGL}(2,q)$ *on the set* $\overline{\mathbb{F}}_q(x) \setminus \mathbb{F}_q$. *If* $g \in \mathbb{F}_q[x]$ *has degree* $k \geq 1$ *and* $g^A(x) := [A] \bullet (g([A^{-1}] \bullet x)) \in \mathbb{F}_q(x)$, *then for every* $n \geq 1$ *and every* $f \in \mathcal{M}_q$, *we have that*

$$\mathcal{F}_{f,g^A}(n) = \mathcal{F}_{[A]\circ f,g}(n),$$

where $\mathcal{F}$ *is any of the four arithmetic functions in Definition 7.16. Moreover, for* $b = 0$, $g^A \in \mathbb{F}_q(x) \setminus \mathbb{F}_q[x]$ *is a rational function of degree* k.

Proof. It is direct to verify that, for every $[A], [B] \in \mathrm{PGL}(2,q)$ and every $g \in \overline{\mathbb{F}}_q[x] \setminus \overline{\mathbb{F}}_q$, we have that $[A] \bullet g \in \overline{\mathbb{F}}_q(x) \setminus \mathbb{F}_q$ and $[A] \bullet ([B] \bullet g) = [AB] \bullet g$. In particular, $\mathrm{PGL}(2,q)$ acts on $\overline{\mathbb{F}}_q(x) \setminus \mathbb{F}_q$ via the compositions $[A] \bullet g$. Pick $f \in \mathcal{M}_q$, let $n \geq 0$ be an integer and let Γ_1, Γ_2 be the set of distinct roots of $f_{g^A}^{(n)}$ and $([A] \circ f)_g^{(n)}$, respectively. Since $f \in \mathcal{M}_q$, we have that $\Gamma_1 \cap \mathbb{F}_q = \emptyset$. We observe that the n-fold composition $(g^A)^{(n)}$ equals $(g^{(n)})^A$. Moreover, $[A] * \alpha = [A]^{-1} \bullet \alpha$ for every $\alpha \in \overline{\mathbb{F}}_q \setminus \mathbb{F}_q$. In particular, Lemmas 7.17 and 7.19 imply that

$$\Gamma_1 = \{[A] \bullet \beta \,|\, \beta \in \Gamma_2\} \subseteq \overline{\mathbb{F}}_q \setminus \mathbb{F}_q.$$

Lemma 7.19 entails that the minimal polynomials of γ and $[A] \bullet \gamma$ over $\mathbb{F}_q$ have the same degree for every $\gamma \in \overline{\mathbb{F}}_q \setminus \mathbb{F}_q$. Moreover, the map $y \mapsto y^q$ commutes with the map $y \mapsto [A] \bullet y$. From these observations, we conclude that $\mathcal{F}_{f,g}(n) = \mathcal{F}_{[A]\circ f,g^A}(n)$, where $\mathcal{F}$ is any of the four arithmetic functions defined in Definition 7.16.

It follows from the definition that $g^A(x) = \frac{ag([A]^{-1} \bullet x)+c}{bg([A]^{-1} \bullet x)+d} = \frac{a \cdot [A^{-1}] \circ g(x) + c(a-bx)^k}{b \cdot [A^{-1}] \circ g(x) + d(a-bx)^k}$. In particular, if $b = 0$, the rational function $g^A \in \mathbb{F}_q(x)$ is not a polynomial and has degree k. ■

Combining Lemma 7.20 with Theorem 2.6 of [79], we obtain the following result.

Theorem 7.21. *For each* $f \in \mathcal{M}_q$, *the following hold:*

(i) there exist infinitely many rational functions $R \in \mathbb{F}_q(x) \setminus \mathbb{F}_q[x]$ *such that* $M_{f,R}(n) \approx n$;

(ii) for each integer $t \geq 0$, *there exist infinitely many rational functions* $R \in \mathbb{F}_q(x) \setminus \mathbb{F}_q[x]$ *such that* $N_{f,R}(n) \approx n^t$ *and* $M_{f,R}(n) \approx \deg(R)^n$.

From Proposition 5.18 of [79], we can also extend item (i) of the previous theorem to the function $A_{f,R}(n)$.

Part III

Rank metric codes

CHAPTER 8

Rank metric codes arising from linearized polynomials

For a field $\mathbb{K}$, let $\mathrm{M}_{m\times n}(\mathbb{K})$ be the set of $m \times n$ matrices over $\mathbb{K}$. A *rank metric code* $\mathcal{C}$ is a subset of $\mathrm{M}_{m\times n}(\mathbb{K})$ equipped with the distance function $d(A, B) = rank(A - B)$. The rank metric codes were introduced by Delsarte in [20]. The *minimun distance* of $\mathcal{C}$ is given by $d(\mathcal{C}) = \min_{A,B\in\mathcal{C},A\neq B}\{d(A, B)\}$. The particular case where $\mathbb{K}$ is a finite field has been studied over the last few decades, since there exist many interesting properties involving these codes. Let $\mathbb{F}_q$ denote a finite field with $q = p^\lambda$ elements, where p is a prime number and λ is a positive integer. A code $\mathcal{C} \subset \mathrm{M}_{m\times n}(\mathbb{F}_q)$ that attains the Singleton-like bound

$$|\mathcal{C}| \leq q^{\max\{m,n\}(\min\{m,n\}-d(\mathcal{C})+1)}$$

is called *maximum rank distance code* (MRD code for short). The first MRD codes over $\mathbb{F}_q$ have been constructed by Delsarte [20] and Gabidulin [25]. Currently, these codes are often called *generalized Gabidulin codes*. A matrix $A \in \mathrm{M}_{n\times n}(\mathbb{F}_q)$ can be represented by a polynomial in

$$\mathcal{L}_{n,q}[x] := \left\{ \sum_{i=0}^{\ell} a_i x^{q^i} : \text{ integer } \ell \geq 0 \text{ and } a_i \in \mathbb{F}_{q^n} \right\},$$

the set of linearized polynomials over $\mathbb{F}_{q^n}$. We note that $(\mathcal{L}_{n,q}[x], \circ)$ equipped with composition is an algebra. In this chapter, we will use the language of linearized polynomials over $\mathbb{F}_q$ (see definition in Section 8.1) in order to prove our main results. Throughout the chapter, we also use the bijection between $\mathrm{M}_{n\times n}(\mathbb{F}_q)$ and $\mathscr{L}_{n,q}[x] := \mathcal{L}_{n,q}[x]/(x^{q^n} - x)$. Using the language of linearized polynomials, the *generalized Gabidulin code* $\mathcal{G}_{k,s}$ can be seen as the set

$$\{a_0 x + a_1 x^{q^s} + \cdots + a_{k-1} x^{q^{s(k-1)}} : a_i \in \mathbb{F}_{q^n}\},$$

where s is relatively prime to n. The number of elements in $\mathcal{G}_{k,s}$ is q^{nk} and each polynomial in it has at most q^{k-1} roots, which means that its minimum distance is $d = n - k + 1$. Therefore, $\mathcal{G}_{k,s}$ is an MRD code.

In the last few years, many authors have presented important contributions to the general theory of MRD codes (e.g see [20, 25, 26, 52, 58, 77]). Sheekey [84] proposed the study of the

generalized twisted Gabidulin codes

$$\mathcal{H}_{k,s}(L_1, L_2) = \{L_1(a_0)x + a_1x^{q^s} + \cdots + L_2(a_0)x^{q^{sk}} : a_i \in \mathbb{F}_{q^n}\},$$

where L_1 and L_2 are linearized polynomials over $\mathbb{F}_{q^n}$ and s is an integer relatively prime to n. Let $\mathrm{N}_{q^n/q}(a) = a^{\frac{q^n-1}{q-1}}$ be the norm function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ and let $\mathbb{F}_{q^n}^* = \mathbb{F}_{q^n}\backslash\{0\}$. By Proposition 8.3, $\mathcal{H}_{k,s}(L_1(x), L_2(x))$ is an MRD code if $\mathrm{N}_{q^n/q}(L_1(a)) \neq (-1)^{nk}\,\mathrm{N}_{q^n/q}(L_2(a))$ for all $a \in \mathbb{F}_{q^n}^*$. These codes have been used by many authors in order to present new classes of MRD codes. Some of the known MRD codes are the following (see survey in [85]):

Name	$L_1(x)$	$L_2(x)$	Conditions	Reference
TG	x	ηx^{q^h}	$\mathrm{N}_{q^n/q}(\eta) \neq (-1)^{nk}$ and $s = 1$	[84]
GTG	x	ηx^{q^h}	$\mathrm{N}_{q^n/q}(\eta) \neq (-1)^{nk}$	[53, 84]
AGTG	x	ηx^{p^h}	$\mathrm{N}_{q^n/p}(\eta) \neq (-1)^{nk}$	[68]
TZ	$x + x^{q^{n/2}}$	$\frac{\eta(x - x^{q^{n/2}})}{\theta}$	n even, $\mathrm{N}_{q^n/q}(\eta)$ is not a quadratic residue in $\mathbb{F}_q$ and $\theta \in \mathbb{F}_{q^n}\backslash\mathbb{F}_{q^{n/2}}$ and $\theta^2 \in \mathbb{F}_{q^{n/2}}$	[99]

Table 8.1: TG=Twisted Gabidulin, GTG=Generalized Twisted Gabidulin, AGTG=Additive Generalized Twisted Gabidulin, TZ = Trombetti-Zhou

In a recent work, Sheekey [86] studied a new construction for MRD codes by using skew polynomial rings and obtained the following result.

Theorem 8.1. *[86, Theorem 7] Let L be a finite field, σ an automorphism of L with fixed field K, and ρ an automorphism of L over some field $K' \leq K$. Let $R = L[x;\sigma]$, let F be an irreducible polynomial in $K[y]$ of degree s, $E_F = \frac{K[y]}{(F(y))}$ and $R_F = \frac{R}{RF(x^n)}$. Then the set*

$$S_{n,s,k}(\eta, \rho, F) := \{a + RF(x^n) : \deg(a) \leq ks, a_{ks} = \eta a_0^\rho\}$$

defines a K'-linear MRD code in $R_F \simeq \mathrm{M}_{n\times n}(E_F)$ with minimum distance $n - k + 1$ for any $\eta \in$ such that $\mathrm{N}_{L/K'}(\eta)\,\mathrm{N}_{K/K'}((-1)^{sk(n-1)}F_0^k) \neq 1$.

We say that two codes $\mathcal{C}$ and $\mathcal{C}'$ are equivalent if there exist $\psi \in \mathscr{L}_{n,q}[x]$, two bijective linearized polynomials $\phi_1, \phi_2 \in \mathscr{L}_{n,q}[x]$ and $\varphi \in \mathrm{Aut}(\mathbb{F}_{q^n})$ such that

$$\mathcal{C}' = \{\phi_1 \circ f^\varphi \circ \phi_2 + \psi : f \in \mathcal{C}\},$$

where $f^\varphi = \sum_{i=0}^{\ell} \varphi(a_i)x^{q^i}$ for $f = \sum_{i=0}^{\ell} a_i x^{q^i}$. When $\mathcal{C}$ and $\mathcal{C}'$ are both additive, it is not difficult to show that we can suppose $\psi = 0$. It is always a difficult task to show that a new family of MRD codes is inequivalent to another family already known. Lunardon, Trombetti and Zhou [53] characterized the equivalence of generalized twisted Gabidulin codes and presented their Delsarte dual and adjoint codes. In Section 8.2 we fully characterize the equivalence between codes of the form $\mathcal{H}_{k,s}(L_1, L_2)$, generalizing the results obtained in [53, 99] for the codes in the Table 8.1.

In Section 8.3 we restrict ourselves to the codes of the form $\mathcal{H}_k(x, L(x))$, where we fully describe their nuclei, Delsarte dual codes and adjoint codes (see definitions in Section 8.1). Most of the codes in Table 8.1 (namely TG, GTG, AGTG) are covered by our results.

Lastly, in Section 8.4 we characterize the automorphism group of $\mathcal{H}_k(x, L(x))$ and compute its number of elements. In particular, the automorphism groups of TG, GTG, AGTG codes are obtained for k satisfying $2 < k < n - 2$.

8.1 Background

In this section we introduce concepts that will be useful throughout this chapter. For an integer $m \geq 0$ and $a_0, \ldots, a_m \in \mathbb{F}_{q^n}$ with $a_m \neq 0$, a polynomial of the form

$$a_0 x + a_1 x^q + \cdots a_m x^{q^m}$$

is called a linearized polynomial over $\mathbb{F}_{q^n}$ and its q-degree is m . Since $a^{q^n} = a$ for all $a \in \mathbb{F}_{q^n}$, we can consider only polynomials with q-degree smaller than n. To this end we will use the elements in $\mathscr{L}_{n,q}[x]$. The following result is an immediate consequence of the Lagrange interpolation formula for polynomials over $\mathbb{F}_{q^n}$.

Lemma 8.2. *Let $L(x) \in \mathscr{L}_{n,q}[x]$. If $L(a) = 0$ for all $a \in \mathbb{F}_{q^n}$, then $L(x) \equiv 0$.*

The following result, proved by Sheekey, present a family of MRD codes.

Proposition 8.3. *Let L_1 and L_2 be linearized polynomials over $\mathbb{F}_{q^n}$ and $k \leq n-1$. If $\mathrm{N}_{q^n/q}(L_1(a)) \neq (-1)^{kn} \mathrm{N}_{q^n/q}(L_2(a))$ for all $a \in \mathbb{F}_{q^n}^*$, then $\mathcal{H}_{k,1}(L_1, L_2)$ is an MRD code.*

There exist several invariants for rank metric codes that can be used to decide when two codes are equivalent to another already known. Next, we present some of these invariants. The left and right invariant of MRD-codes were introduced in [54]. We define the middle nucleus $\mathcal{N}_m$ and right nucleus $\mathcal{N}_r$ for a rank metric code $\mathcal{C}$ as

$$\mathcal{N}_m(\mathcal{C}) = \{g(x) \in \mathscr{L}_{n,q}[x] : f \circ g \in \mathcal{C} \text{ for all } f \in \mathcal{C}\}$$

and

$$\mathcal{N}_r(\mathcal{C}) = \{g(x) \in \mathscr{L}_{n,q}[x] : g \circ f \in \mathcal{C} \text{ for all } f \in \mathcal{C}\}.$$

Middle and right nucleus were already known as left and right idealizers and have originally been introduced to study automorphism and equivalence of Gabidulin codes in [51]. The nuclei of TG and GTG codes can be found in [53]. In [99] the authors present the nuclei of the TZ codes. Let $\mathrm{Tr}_{q^n/q}(x) = x + x^q + \cdots + x^{q^{n-1}}$ be the trace function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$. The *adjoint* of a linearized polynomial $f = \sum_{i=0}^{n-1} a_i x^{q^{si}}$ is given by

$$\hat{f} = \sum_{i=0}^{n-1} a_i^{q^{s(n-i)}} x^{q^{s(n-i)}}$$

and the *adjoint code* of a rank metric code $\mathcal{C}$ is $\widehat{\mathcal{C}} = \{\hat{f} : f \in \mathcal{C}\}$. For the codes which we are interested in this chapter, it is easy to verify that the following result holds.

Proposition 8.4. *The adjoint code of $\mathcal{H}_{k,s}(L_1, L_2)$ is equivalent to $\mathcal{H}_{n-k,s}(L_2^{q^{n-sk}}, L_1)$.*

Another useful invariant is the dual of a code. The *Delsarte dual code* of a code $\mathcal{C}$ is given by

$$\mathcal{C}^\perp = \{g(x) \in \mathscr{L}_{n,q}[x] : b(f, g) = 0 \text{ for all } f \in \mathcal{C}\},$$

where $b(f, g) = \sum_{i=0}^{n-1} \mathrm{Tr}_{q^n/q}(a_i b_i)$ for $f(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$ and $g(x) = \sum_{i=0}^{n-1} b_i x^{q^i}$.

It is not difficult to show that two additive codes $\mathcal{C}$ and $\mathcal{C}'$ are equivalent if and only if the codes $\mathcal{C}^\perp$ and $\mathcal{C}'^\perp$ are equivalent. Delsarte [20] proved the following result.

Lemma 8.5. *Let $\mathcal{C}$ be a $\mathbb{F}_q$-linear code. Then $\mathcal{C}$ is an MRD code if and only if its Delsarte dual $\mathcal{C}^\perp$ is an MRD code.*

An important relation between these invariants are the adjoint and Delsarte dual operation, given by

$$\mathcal{N}_r(\mathcal{C}^\perp) = \widehat{\mathcal{N}_r(\mathcal{C})} = \mathcal{N}_m(\widehat{\mathcal{C}})$$

and

$$\mathcal{N}_m(\mathcal{C}^\perp) = \widehat{\mathcal{N}_m(\mathcal{C})} = \mathcal{N}_r(\widehat{\mathcal{C}}).$$

These relations were stated in Proposition 4.2 of [54].

8.2 Equivalence

We say that a code is additive if the sum of two of its elements is also an element of the code. For $L_1, L_2 \in \mathscr{L}_{n,q}[x]$, it is direct to verify that $\mathcal{H}_{k,s}(L_1, L_2)$ is an additive code. Hence, the equivalence between the codes $\mathcal{H}_{k,s}(L_1, L_2)$ and $\mathcal{H}_{k,r}(M_1, M_2)$ is given by the existence of two bijective linearized polynomials $\phi_1, \phi_2 \in \mathscr{L}_{n,q}[x]$ and $\varphi \in \mathrm{Aut}(\mathbb{F}_{q^n})$ such that

$$\mathcal{H}_{k,r}(M_1, M_2) = \{\phi_1 \circ f^\varphi \circ \phi_2 : f \in \mathcal{H}_{k,s}(L_1, L_2)\}.$$

In this case, we say that $(\phi_1, \phi_2, \varphi)$ is an equivalence map between $\mathcal{H}_{k,s}(L_1, L_2)$ and $\mathcal{H}_{k,r}(M_1, M_2)$. It is well-known that $\mathrm{Aut}(\mathbb{F}_{q^n})$ is a cyclic group generated by σ, where $\sigma(c) := c^p$ is the *Frobenius automorphism* of $\mathbb{F}_{q^n}$ fixing $\mathbb{F}_p$ and p is the characteristic of $\mathbb{F}_{q^n}$. Hereafter, φ denotes an element in $\mathrm{Aut}(\mathbb{F}_{q^n})$ and $\rho = p^\nu$ is the integer such that $\varphi(c) = c^\rho$ for all $c \in \mathbb{F}_{q^n}$. Throughout this chapter, r, s and k are positive integers such that $k \leq n-1$ and $\gcd(r, n) = \gcd(s, n) = 1$. From now on, L_1, L_2, M_1, M_2, L, M will denote linearized polynomials in $\mathscr{L}_{n,q}[x]\backslash\{0\}$. The main result of this section presents conditions on r, s, L_1, L_2, M_1 and M_2 for which the codes $\mathcal{H}_{k,s}(L_1, L_2)$ and $\mathcal{H}_{k,r}(M_1, M_2)$ are equivalent and provides the equivalence maps. In order to describe these conditions, it will be useful to introduce the following definition.

Definition 8.6. *Let $\mathbb{Z}_n$ denote the ring of integers modulo n and, for an integer a, let $\overline{a}$ denote the class of a in $\mathbb{Z}_n$. For integers r, s, k, n with $2 \leq k \leq n-2$, we define*

$$\Gamma_{r,s,k,n} = \{\overline{tr - is} \in \mathbb{Z}_n : \ 1 \leq i \leq k-1 \text{ and } k+1 \leq t \leq n-1\}.$$

Remark 8.7. *For integers r, s, k, n, we have that $|\Gamma_{r,s,k,n}| = |\Gamma_{n-r,s,k,n}|$. In order to verify this statement, we observe that the function $\zeta : \Gamma_{r,s,k,n} \to \Gamma_{n-r,s,k,n}$ defined by*

$$\overline{tr - is} \mapsto \overline{(-t+n+k)(n-r) - is}$$

is one-to-one.

In order to prove the main result of this section, we present the following technical result.

Lemma 8.8. *Let r, s, k and $n \geq 4$ be positive integers such that $\gcd(n, r) = \gcd(n, s) = 1$, $2 \leq k \leq n-2$ and $1 \leq r, s < n$. For a integer a, let $\overline{a}$ denote the class of a in $\mathbb{Z}_n$. Then the*

following hold:

$$\Gamma_{r,s,k,n} = \begin{cases} \mathbb{Z}_n\backslash\{\overline{-s}, \overline{0}, \overline{s}\}, \text{ if } r = s; \\ \mathbb{Z}_n\backslash\{\overline{-s(k-1)}, \overline{-sk}, \overline{-s(k+1)}\}, \text{ if } r = n-s; \\ \mathbb{Z}_n\backslash\{\overline{-s}, \overline{-s+r}, \overline{-s+2r}\}, \text{ if } k = 2; \\ \mathbb{Z}_n\backslash\{\overline{-r}, \overline{-r+s}, \overline{-r+2s}\}, \text{ if } k+1 = n-1. \end{cases}$$

Furthermore, if $k \notin \{2, n-2\}$ *and* $r \notin \{s, n-s\}$*, then*

$$\Gamma_{r,s,k,n} = \begin{cases} \mathbb{Z}_n\backslash\{\overline{-2r}\}, \text{ if } k = 4 \text{ and } \overline{s} = \overline{2r}; \\ \mathbb{Z}_n\backslash\{\overline{6r}\}, \text{ if } k = 4 \text{ and } \overline{s} = \overline{-2r}; \\ \mathbb{Z}_n\backslash\{\overline{-r}, \overline{-2r}\}, \text{ if } k = 3 \text{ and } \overline{s} = \overline{2r}; \\ \mathbb{Z}_n\backslash\{\overline{5r}, \overline{4r}\}, \text{ if } k = 3 \text{ and } \overline{s} = \overline{-2r}; \\ \mathbb{Z}_n\backslash\{\overline{-3r}\}, \text{ if } k = 3 \text{ and } \overline{s} = \overline{3r}; \\ \mathbb{Z}_n\backslash\{\overline{6r}\}, \text{ if } k = 3 \text{ and } \overline{s} = \overline{-3r}; \\ \mathbb{Z}_n\backslash\{\overline{-2s}\}, \text{ if } k+1 = n-3 \text{ and } \overline{r} = \overline{2s}; \\ \mathbb{Z}_n\backslash\{\overline{6s}\}, \text{ if } k+1 = n-3 \text{ and } \overline{r} = \overline{-2s}; \\ \mathbb{Z}_n\backslash\{\overline{-s}, \overline{-2s}\}, \text{ if } k+1 = n-2 \text{ and } \overline{r} = \overline{2s}; \\ \mathbb{Z}_n\backslash\{\overline{5s}, \overline{4s}\}, \text{ if } k+1 = n-2 \text{ and } \overline{r} = \overline{-2s}; \\ \mathbb{Z}_n\backslash\{\overline{-3s}\}, \text{ if } k+1 = n-2 \text{ and } \overline{r} = \overline{3s}; \\ \mathbb{Z}_n\backslash\{\overline{6s}\}, \text{ if } k+1 = n-2 \text{ and } \overline{r} = \overline{-3s}; \\ \mathbb{Z}_n, \text{ otherwise.} \end{cases}$$

Proof. Initially, we prove the last case of our assertion. Suppose $k \geq \frac{n}{2}$. Since $\gcd(s, n) = 1$, there exists a positive integer $z < n$ such that $\overline{sz} = \overline{r}$ and, for this element, it follows that $|\Gamma_{r,s,k,n}| = |\Gamma_{z,1,k,n}|$. Therefore, we only need to prove the result for $\Gamma_{z,1,k,n}$.

We can also assume that $z < \frac{n}{2}$ replacing z by $n - z$ if it is necessary and then using Remark 8.7. We note that for each ℓ satisfying $k + 2 \leq \ell \leq n - 1$, we have that

$$S_\ell := \{\overline{(\ell-1)z}, \overline{(\ell-1)z+1}, \ldots, \overline{\ell z-1}\} \subset \Gamma_{z,1,k,n}$$

since $k - 1 \geq z$. We also have that

$$S_{k+1} := \{\overline{(k+1)z-k+1}, \overline{(k+1)z-k+2}, \ldots, \overline{(k+1)z-1}\} \subset \Gamma_{z,1,k,n}.$$

Then

$$\left(\bigcup_{\ell=k+1}^{n-1} S_\ell\right) \subset \Gamma_{z,1,k,n}. \tag{8.1}$$

Furthermore,

$$\left|\bigcup_{\ell=k+1}^{n-1} S_\ell\right| = \min\{n, (n-2-k)z + (k-1)\}. \tag{8.2}$$

We have that $\min\{n, (n-2-k)z + (k-1)\} < n$ only if one of the following holds:

- $k + 1 = n - 1$;

- $z = 1$;
- $(n-k, z) \in \{(3,2), (3,3), (4,2)\}$.

The last case of our lemma is the case where none of these conditions are satisfied, so that $\min\{n, (n-2-k)z + (k-1)\} = n$. Therefore, Equations (8.1) and (8.2) entail that $\Gamma_{z,1,k,n} = \mathbb{Z}_n$. The last case is obtained in a similar way for $k \leq \frac{n}{2}$ by changing the role of r and s. The first cases of our lemma can be obtained by straightforward computations. ■

In the following result, let r and s be integers satisfying $0 \leq r < n$ and $0 \leq s < n$.

Definition 8.9. *A pair (L_1, L_2) satisfies the condition (H) if there exists no $\gamma \in \mathbb{F}_{q^n}^*$ and integer $\ell \geq 0$ such that $L_1(c) = \gamma L_2(c)^{q^\ell}$ for all $c \in \mathbb{F}_{q^n}$.*

Theorem 8.10. *Suppose $n \geq 4$. Let $(\phi_1, \phi_2, \varphi)$ be an equivalence map between $\mathcal{H}_{k,s}(L_1, L_2)$ and $\mathcal{H}_{k,r}(M_1, M_2)$. If $2 < k < n-2$, then the following hold:*

1. *either $r = s$ or $r = n - s$;*
2. *if $r = s$, then there exist elements $\alpha, \beta \in \mathbb{F}_{q^n}$ and an integer l satisfying $0 \leq l \leq n-1$ such that $\phi_1(x) = \alpha x^{q^l}$ and $\phi_2(x) = \beta x^{q^{n-l}}$;*
3. *if $r = n - s$, then there exist elements $\alpha, \beta \in \mathbb{F}_{q^n}$ and an integer l satisfying $0 \leq l \leq n-1$ such that $\phi_1(x) = \alpha x^{q^{n(s-k)+l}}$ and $\phi_2(x) = \beta x^{q^{n-l}}$.*

Furthermore, if (L_1, L_2) and (M_1, M_2) satisfy the condition (H), then (1), (2) and (3) hold for $k = 2$ and $k = n-2$.

Proof. For all $y \in \mathbb{F}_{q^n}$ and integers i satisfying $1 \leq i \leq k-1$, we have that $\phi_1 \circ y^\rho x^{q^{si}} \circ \phi_2 \in \mathcal{H}_{k,r}(M_1, M_2)$. If $\phi_1(x) = \sum_{m=0}^{n-1} a_m x^{q^m}$ and $\phi_2(x) = \sum_{j=0}^{n-1} b_j x^{q^j}$, then

$$\phi_1 \circ y^\rho x^{q^{si}} \circ \phi_2 = \phi_1 \left(y^\rho \sum_{j=0}^{n-1} b_j^{q^{si}} x^{q^{j+si}} \right)$$

and therefore

$$\phi_1 \circ y^\rho x^{q^{si}} \circ \phi_2 = \sum_{m=0}^{n-1} a_m y^{\rho q^m} \sum_{j=0}^{n-1} b_j^{q^{si+m}} x^{q^{j+si+m}} = \sum_{t=0}^{n-1} \left[\sum_{si+j+m=tr} a_m y^{\rho q^m} b_j^{q^{si+m}} \right] x^{q^{tr}}.$$

Hereafter, we consider the indexes of a_j and b_j modulo n, which means that $a_m := a_j$ and $b_m := b_j$ for every $m \equiv j \pmod{n}$. Since $\phi_1 \circ y^\rho x^{q^{si}} \circ \phi_2 \in \mathcal{H}_{k,r}(M_1, M_2)$, we must have

$$T_{i,t}(y^\rho) := \sum_{si+j+m=tr} a_m y^{\rho q^m} b_j^{q^{si+m}} = 0 \tag{8.3}$$

for all $k+1 \leq t \leq n-1$, $y \in \mathbb{F}_{q^n}$ and $1 \leq i \leq k-1$. We can rewrite $T_{i,t}(y^\rho)$ as

$$\sum_{m=0}^{n-1} a_m \, b_{tr-m-si}^{q^{si+m}} \, y^{\rho q^m}.$$

We note that $T_{i,t}(x) \in \mathscr{L}_{n,q}[x]$, then the Equation (8.3) and Lemma 8.2 together imply that

$$a_m b_{tr-m-si} = 0 \tag{8.4}$$

for all $0 \leq m \leq n-1$, $k+1 \leq t \leq n-1$ and $1 \leq i \leq k-1$. We suppose $r = s$. By Equation (8.4) and Lemma 8.8, if $a_l \neq 0$ for some integer l, then $b_j = 0$ for every $j \notin \{n-s-l, n-l, n+s-l\}$. Using this argument with l running over all integers $l = 0, \ldots, n-1$, it follows that there exists a non-negative integer $l \leq n-1$ for which one of the following holds:

1. $a_j = 0$ for every $j \neq l$ and $b_j = 0$ for every $j \notin \{n-s-l, n-l, n+s-l\}$;
2. $b_j = 0$ for every $j \neq l$ and $a_j = 0$ for every $j \notin \{n-s-l, n-l, n+s-l\}$;
3. $a_j = 0$ for every $j \notin \{l, l+s\}$ and $b_j = 0$ for every $j \notin \{n-s-l, n-l\}$.

Since ϕ_1 and ϕ_2 can be switched, we may assume without loss of generality that (a) or (c) holds. Let us compute the image of $L_1(c)x + L_2(c)x^{q^{sk}}$ under the equivalence map $(\phi_1, \phi_2, \varphi)$. In the case (a), we have that $\phi_1 \circ (L_1(c)^\rho x + L_2(c)^\rho x^{q^{sk}}) \circ \phi_2$ equals

$$a_l\Big(L_1(c)^{\rho q^l}(b^{q^l}_{n-s-l}x^{q^{n-s}} + b^{q^l}_{n-l}x + b^{q^l}_{n+s-l}x^{q^{n+s}}) + L_2(c)^{\rho q^l}(b^{q^l}_{n-s-l}x^{q^{sk-s}} + b^{q^l}_{n-l}x^{q^{sk}} + b^{q^l}_{n+s-l}x^{q^{sk+s}})\Big).$$

Since $\phi_1 \circ (L_1(c)^\rho x + L_2(c)^\rho x^{q^{sk}}) \circ \phi_2 \in \mathcal{H}_{k,r}(M_1, M_2)$ (and under the condition (H) in the case $k = 2$ and $k = n-2$), it follows that $b_{n-s-l} = 0$ and $b_{n+s-l} = 0$. Then our result is shown in this case.

In the case (c), we have that $\phi_1 \circ (L_1(c)^\rho x + L_2(c)^\rho x^{q^{sk}}) \circ \phi_2$ equals

$$\begin{aligned} &a_l\Big(L_1(c)^{\rho q^l}(b^{q^l}_{n-s-l}x^{q^{n-s}} + b^{q^l}_{n-l}x) + L_2(c)^{\rho q^l}(b^{q^l}_{n-s-l}x^{q^{sk-s}} + b^{q^l}_{n-l}x^{q^{sk}})\Big) \\ &+ a_{l+s}\Big(L_1(c)^{\rho q^{l+s}}(b^{q^{l+s}}_{n-s-l}x + b^{q^{l+s}}_{n-l}x^{q^s}) + L_2(c)^{\rho q^{l+s}}(b^{q^{l+s}}_{n-l}x^{q^{sk}} + b^{q^{l+s}}_{n-l}x^{q^{sk+s}})\Big). \end{aligned}$$

Since $\phi_1 \circ (L_1(c)^\rho x + L_2(c)^\rho x^{q^{sk}}) \circ \phi_2 \in \mathcal{H}_{k,r}(M_1, M_2)$ (and under the condition (H) in the case $k = 2$ and $k = n-2$), it follows that $a_l L_1(c)^{\rho q^l} b^{q^l}_{n-s-l} = 0$ and $a_{l+s} L_2(c)^{\rho q^{l+s}} b^{q^{l+s}}_{n-l} = 0$. Then $a_l = 0$ and $b_{n-l} = 0$ (or $a_{l+s} = 0$ and $b_{n-s-l} = 0$) and our result follows. The case $r = n-s$ can be obtained in the same way.

Now assume that $k = n-2$ and $r \not\equiv \pm s \pmod{n}$. Under the condition (H), it follows (by the same argument employed in the case $n = s$) that there exist elements $\alpha, \beta \in \mathbb{F}^*_{q^n}$ and an integer l satisfying $0 \leq l \leq n-1$ such that $\phi_1(x) = \alpha x^{q^l}$ and $\phi_2(x) = \beta x^{q^{n-l+s-r}}$. We recall that each element $f(x) = \eta_0 x + \eta_k x^{q^{sk}} \in \mathcal{H}_{k,r}(M_1, M_2)$ is such that $\eta_0 = M_1(c)$ and $\eta_k = M_2(c)$ for some $c \in \mathbb{F}_{q^n}$. Since $r - s \not\equiv 0 \pmod{n}$, $r - s \not\equiv ks \pmod{n}$ and $r - s \not\equiv -s \pmod{n}$, we must have

$$\phi_1 \circ y^\rho x^{q^{r-s}} \circ \phi_2 = \alpha y^{\rho q^l} \beta^{q^{r-s+l}} x \in \mathcal{H}_{k,r}(M_1, M_2)$$

for all $y \in \mathbb{F}_{q^n}$, which is a contradiction since $M_2(x) \not\equiv 0$. Therefore $\mathcal{H}_{k,s}(L_1, L_2)$ is not equivalent to $\mathcal{H}_{k,r}(M_1, M_2)$ in this case.

Suppose $k = 2$ and $r \not\equiv \pm s \pmod{n}$. By Equation (8.4) and Lemma 8.8 there exists a non-negative integer $l \leq n-1$ for which one of following holds:

1. $a_j = 0$ for every $j \neq l$ and $b_j = 0$ for every $j \notin \{-s-l, -s+r-l, -s+2r-l\}$;
2. $b_j = 0$ for every $j \neq l$ and $a_j = 0$ for every $j \notin \{-s-l, -s+r-l, -s+2r-l\}$;
3. $a_j = 0$ for every $j \notin \{l, l+r\}$ and $b_j = 0$ for every $j \notin \{-s-l, -s+r-l\}$.

Since $\phi_1 \circ y^{\rho} x^{q^s} \circ \phi_2 \in \mathcal{H}_{k,r}(M_1, M_2)$ and condition (H) holds, it is direct to verify that each one of the cases $(a), (b)$, and (c) implies that there exist elements $\alpha, \beta \in \mathbb{F}_{q^n}^*$ and an integer l satisfying $0 \leq l \leq n-1$ such that $\phi_1(x) = \alpha x^{q^l}$ and $\phi_2(x) = \beta x^{q^{n-l+s-r}}$. By employing the same argument used in the case $k = n-2$, we conclude that $\mathcal{H}_{k,s}(L_1, L_2)$ is not equivalent to $\mathcal{H}_{k,r}(M_1, M_2)$ in this case.

For the remaining possible values of r and s (namely $r \not\equiv \pm s \pmod{n}$, $k \neq 2$ and $k \neq n-2$), the Equation (8.4) and Lemma 8.8 imply that if $a_m \neq 0$ for some m, then $b_{j-m} = 0$ for all $j \in \mathbb{Z}_n \backslash \Gamma_{r,s,k,n}$. It is straightforward to compute that if $\phi_1 \circ f^{\varphi} \circ \phi_2 \in \mathcal{H}_{k,r}(M_1, M_2)$ for all $f \in \mathcal{H}_{k,s}(L_1, L_2)$, then $b_j = 0$ for every $j = 0, \ldots, n$, which is a contradiction. ■

The following lemma is a trivial result from linear algebra and it will be used in the next theorem.

Lemma 8.11. *Let $M(x), L(x) \in \mathscr{L}_{n,q}[x]$. If $\mathrm{Im}(M) = \mathrm{Im}(L)$, then there exists a bijective linearized polynomial $T(x) \in \mathscr{L}_{n,q}[x]$ such that $M(x) = L(T(x))$.*

Theorem 8.12. *Let $n \geq 4$ and let k be an integer satisfying $2 \leq k \leq n-2$. If $k = 2$ or $k = n-2$, assume that (L_1, L_2) and (M_1, M_2) satisfy the condition (H). The codes $\mathcal{H}_{k,s}(L_1, L_2)$ and $\mathcal{H}_{k,s}(M_1, M_2)$ are equivalent if and only if there exist $c, d \in \mathbb{F}_q$, $\varphi \in \mathrm{Aut}(\mathbb{F}_{q^n})$, an integer l satisfying $0 \leq l \leq n-1$ and a bijective linearized polynomial $T \in \mathscr{L}_{n,p}[x]$ such that $M_1(x) = ab\varphi\left(L_1(T(x))\right)^{q^l}$ and $M_2(x) = ab^{q^{sk}}\varphi\left(L_2(T(x))\right)^{q^l}$.*

Proof. The necessity follows immediately from Theorem 8.10. Let us prove the converse. Let $l \leq n-1$ be an integer, $\phi_1(x) = ax^{q^l}$, $\phi_2 = b^{q^{n-l}} x^{q^{n-l}}$ and an automorphism $\varphi \in \mathrm{Aut}(\mathbb{F}_{q^n})$ such that $\varphi(c) = c^{p^\nu}$ for all $c \in \mathbb{F}_{q^n}$. Since $\mathcal{H}_{k,s}(L_1, L_2) = \langle L_1(a_0)x + L_2(a_0)x^{q^{sk}}, a_1 x^{q^s}, \ldots, a_{k-1} x^{q^{s(k-1)}} \rangle_{a_i \in \mathbb{F}_{q^n}}$, we only need to prove that the set of images of these elements under the equivalence map is a basis of $\mathcal{H}_{k,s}(M_1, M_2)$. For $1 \leq i \leq k-1$, we have that

$$\phi_1 \circ a_i^{\rho} x^{q^{si}} \circ \phi_2 = a a_i^{\rho q^l} b^{q^{si}} x^{q^{si}} \in \mathcal{H}_{k,s}(M_1, M_2)$$

for all $a_i \in \mathbb{F}_q$. For $a_0 \in \mathbb{F}_q$,

$$\phi_1 \circ (L_1(a_0)^{\rho} x + L_2(a_0)^{\rho} x^{q^{sk}}) \circ \phi_2 = abL_1(a_0)^{\rho q^l} x + ab^{q^{sk}} L_2(a_0)^{\rho q^l} x^{q^{sk}} \in \mathcal{H}_{k,s}(M_1, M_2)$$

where $\rho = p^\nu$ for an integer $\nu \geq 0$. Since we need

$$\langle abL_1(a_0)^{\rho q^l} x + ab^{q^{sk}} L_2(a_0)^{\rho q^l} x^{q^{sk}}, a a_i^{\rho q^l} b^{q^{si}} x^{q^{si}} \rangle_{1 \leq i \leq k-1, a_i \in \mathbb{F}_{q^n}} = \mathcal{H}_{k,s}(M_1, M_2),$$

our result follows from Lemma 8.11. ■

A very similar result can be obtained for the case $r = n - s$, where the role of L_1 and L_2 is changed. As a consequence of Theorem 8.12, one can easily show Theorems 11, 12 and 13 of Trombetti-Zhou [99].

Corollary 8.13. *Let k and n be integers satisfying the hypothesis of Theorem 8.12. If $k = 2$ or $k = n-2$, assume that $(x, L(x))$ and $(x, H(x))$ satisfy the condition (H). Then $\mathcal{H}_{k,s}(x, L(x))$ is equivalent to $\mathcal{H}_{k,s}(x, M(x))$ if and only if there exist $a, b \in \mathbb{F}_{q^n}$, an automorphism $\varphi \in \mathrm{Aut}(\mathbb{F}_{q^n})$ and an integer l satisfying $0 \leq l \leq n-1$ such that $M(x) = ab^{q^{sk+l}} \varphi\big(L(\varphi^{-1}(x/ab^{q^l})^{q^{n-l}})\big)^{q^l}$.*

Remark 8.14. *For $2 < k < n-2$, Corollary 8.13 generalizes Theorem 4.4 of Lunardon, Trombetti and Zhou [53] for the case $L(x) = \eta x^{q^{sg}}$ and $M(x) = \theta x^{q^{sh}}$. However, our result do not cover the case $k = 2$ and $k = n-2$ studied in [53], since the condition (H) does not hold for Generalized Twisted Gabidulin Codes. In particular, the cases $n = 4$ and $n = 5$ are not covered by Corollary 8.13.*

8.3 Codes of the form $\mathcal{H}_{k,s}(x, L(x))$

Throughout this section, we let $L = \sum_{i=0}^{n-1} \eta_i x^{q^{si}}$ denote a linearized polynomial in $\mathscr{L}_{n,q}[x]$. In this section, we fully characterize the invariants of the codes $\mathcal{H}_{k,s}(x, L(x))$. The following lemma is a well-known fact on adjoint codes.

Lemma 8.15. *For $a, b \in \mathbb{F}_{q^n}$, we have that*

$$\mathrm{Tr}_{q^n/q}\left(bL(a)\right) = \mathrm{Tr}_{q^n/q}\left(a\hat{L}(b)\right),$$

where $\hat{L}$ is the adjoint of L.

Theorem 8.16. *The Delsarte dual of $\mathcal{H}_{k,s}(x, L(x))$ is equivalent to $\mathcal{H}_{n-k,s}(x, -\hat{L}(x))$, where $\hat{L}$ is the adjoint of L.*

Proof. We note that $\mathcal{H}_{n-k,s}(x, -\hat{L}(x))$ is equivalent to

$$\mathcal{J} := \left\{ -\hat{L}(b_k) + \sum_{i=k}^{n-1} b_i x^{q^{si}} : b_i \in \mathbb{F}_{q^n} \right\}.$$

Since the dimension of the code $\mathcal{J}$ over $\mathbb{F}_q$ is $n-k$, we only need to show that $\mathcal{J} \subset \mathcal{H}_{k,s}(x, L(x))^{\perp}$. If $g(x) = \sum_{i=0}^{n-1} b_i x^{q^{si}} \in \mathcal{J}$ and $f(x) = \sum_{i=0}^{n-1} a_0 x^{q^{si}} \in \mathcal{H}_{k,s}(x, L(x))$, then

$$b(f,g) = \sum_{i=0}^{n-1} \mathrm{Tr}_{q^n/q}(a_i b_i) = \mathrm{Tr}_{q^n/q}\left(b_k L(a_0)\right) - \mathrm{Tr}_{q^n/q}\left(a_0 \hat{L}(b_k)\right)$$

and our result follows from Lemma 8.15. ∎

This result was already established earlier by Lunardon, Trombetti and Zhou [53, Proposition 4.2] for the case where $L(x) = \eta x^{q^h}$.

Lemma 8.17. *Assume that $L(x) = \sum_{i=0}^{m} a_i x^{q^{e_i}}$, where $a_i \in \mathbb{F}_{q^n}^*$ and m is a positive integer and $e_0 < e_1 < \ldots < e_m$ are non-negative integers. Let $d = \gcd(e_0, \ldots e_m, n)$. Then $L(\alpha x) = \alpha L(x)$ if and only if $\alpha \in \mathbb{F}_{q^d}$.*

Proof. Suppose that $L(\alpha x) = \alpha L(x)$. We have that

$$\alpha \sum_{i=0}^{m} a_i c^{q^{e_i}} - \sum_{i=0}^{m} a_i (\alpha c)^{q^{e_i}} = \sum_{i=0}^{m} a_i [\alpha - \alpha^{q^{e_i}}] c^{q^{e_i}} \equiv 0$$

for all $c \in \mathbb{F}_{q^n}$, then $\alpha^{q^{e_i}} = \alpha$ from Lemma 8.2, which implies that $\alpha \in \mathbb{F}_{q^d}$. The converse is trivial. ∎

Theorem 8.18. *Let $n \geq 3$. Assume $L(x) = \sum_{i=0}^{m} \eta_{e_i} x^{q^{se_i}}$, where $\eta_{e_i} \in \mathbb{F}_{q^n}^*$ and m is a positive integer and $e_0 < e_1 < \ldots < e_m < n$ are non-negative integers. Let $d = \gcd(e_0, \ldots, e_m, n)$. The right nucleus of $\mathcal{H}_{k,s}(x, L(x))$ is*

$$\mathcal{N}_r(\mathcal{H}_{k,s}(x, L(x))) = \{ax : a \in \mathbb{F}_{q^d}\}.$$

The middle nucleus of $\mathcal{H}_{k,s}(x, L(x))$ is

$$\mathcal{N}_m(\mathcal{H}_{k,s}(x, L(x))) = \{ax : a \in \mathbb{F}_{q^d}\}.$$

Proof. We will compute only the right nucleus, since the middle nucleus can be computed in a similar way by doing the needed changes. By the duality presented in Theorem 8.16 and the Delsarte dual operation, we can suppose without loss of generality that $k \leq \frac{n}{2}$. We can write $L(x)$ as $\sum_{j=0}^{n-1} \eta_j x^{q^{sj}}$ by setting $\eta_j = 0$ if $j \notin \{e_i : i = 0, \ldots, m\}$. Now let $g(x) = \sum_{i=0}^{n-1} b_i x^{q^{si}} \in \mathcal{N}_r(\mathcal{H}_{k,s}(x, L(x)))$.

Claim 1. $b_i = b_{i-k} = 0$ for all $i = k+1, \ldots, n-1$.

Proof of the Claim 1. For every $c \in \mathbb{F}_{q^n}$, we have that

$$g\big(cx + L(c)x^{q^{sk}}\big) = \sum_{i=0}^{n-1} x^{q^{si}} \left(b_i c^{q^{si}} + b_{i-k} L(c)^{q^{s(i-k)}} \right) \in \mathcal{H}_{k,s}(x, L(x)).$$

By Lemma 8.2, for i satisfying $k+1 \leq i \leq n-1$, we have that the linearized polynomial $b_i c^{q^{si}} + b_{i-k} L(c)^{q^{s(i-k)}}$ is identically null. In particular, $b_{i-k} \eta_j^{q^{s(i-k)}} = 0$ for all $j \neq k$. Since $m \geq 1$, there exists an integer $\delta \neq k$ such that $\eta_\delta \neq 0$, then $b_{i-k} \eta_\delta^{q^{s(i-k)}} = 0$ implies that $b_{i-k} = 0$. Besides that, since $b_i + b_{i-k} \eta_k^{q^{s(i-k)}} = 0$ we have $b_i = 0$, proving the claim.

Claim 2. If $2 \leq k \leq n-2$, then $b_i = 0$ for all $i = 2, \ldots, n-2$.

Proof of the Claim 2. For j satisfying $1 \leq j \leq k-1$, we have that $g(x^{q^{sj}}) = \sum_{i=0}^{n-1} b_{i-j} x^{q^{si}}$. Therefore $b_{i-j} = 0$ for all $i = k+1, \ldots, n-1$, proving the claim.

The claims 1 and 2 together imply that $b_i = 0$ for all $i \neq 0$. Now we consider $g(x) = b_0 x \in \mathcal{N}_r(\mathcal{H}_{k,s}(x, L(x)))$. Since

$$b_0 cx + b_0 L(c) x^{q^{sk}} \in \mathcal{H}_{k,s}(x, L(x)),$$

we must have $L(b_0 c) = b_0 L(c)$ for all $c \in \mathbb{F}_{q^n}$ and our result follows from Lemma 8.17. ■

8.4 The automorphism group

Let $\big(\mathscr{L}_{n,q}^{\times}[x], \circ\big)$ denote the group of elements in $\mathscr{L}_{n,q}[x]$ that are invertible with respect to the usual composition of maps. The *automorphism group* of an additive code $\mathcal{C} \subset \mathscr{L}_{n,q}[x]$ is the set of semi-linear rank-metric-equivalence maps f such that $f(\mathcal{C}) = \mathcal{C}$ (For more details, see [58]). Each one of these maps can be represented by an element in the group $G(\mathcal{C}) := \{(\phi_1, \phi_2, \varphi) \in \mathscr{L}_{n,q}^{\times}[x] \times \mathscr{L}_{n,q}^{\times}[x] \times \mathrm{Aut}(\mathbb{F}_{q^n}) : \phi_1 \circ \mathcal{C}^{\varphi} \circ \phi_2 = \mathcal{C}\}$, but there is not only one representative for each map. Indeed, one can verify that the group action $* : G(\mathcal{C}) \times \mathcal{C} \to \mathcal{C}$, defined by

$$\big((\phi_1, \phi_2, \varphi), f\big) \mapsto \phi_1 \circ f^{\varphi} \circ \phi_2,$$

is not faithful, fact that was already studied by Morrison [58]. Consequently, we have that

$$\mathrm{Aut}(\mathcal{C}) \cong G(\mathcal{C})/N(\mathcal{C}), \tag{8.5}$$

where $N(\mathcal{C})$ is the kernel of the group action $*$. Sheekey computed the automorphism group of Gabidulin codes (Theorem 4 of [84]) and Twisted Gabidulin codes (Theorem 7 of [84]). Throughout this section, k is an integer with $2 \leq k \leq n-2$. With Theorem 8.12, we are able to describe the automorphism group of $\mathcal{H}_{k,s}(x, L(x))$. For a set $\mathcal{I} \subseteq [0, n-1]$, let $D(\mathcal{I}) = \{i - j : i, j \in \mathcal{I}, i > j\}$ be the set of distinct differences in $\mathcal{I}$. Let $i_1, \ldots, i_u$ be the elements of $D(\mathcal{I})$. In order to present the automorphism group of $\mathcal{H}_{k,s}(x, L(x))$, we define the function

$$\kappa_{q^n}(\mathcal{I}) = \gcd(q^{i_1} - 1, \ldots, q^{i_u} - 1, q^n - 1) = q^{\gcd(i_1, \ldots, i_u, n)} - 1.$$

Along the proof of the following result, we will extensively use the well-known fact that $\gcd(q^i - 1, q^j - 1) = q^{\gcd(i,j)} - 1$ for positive integers i, j and q. From now on, for a divisor d of $q^n - 1$, let χ_d be a multiplicative character of $\mathbb{F}_{q^n}^*$ of order d. For convenience, we extend χ_d to $\mathbb{F}_{q^n}$ by setting $\chi_d(0) = 0$. In order to present the cardinality of $\mathrm{Aut}\big(\mathcal{H}_{k,s}(x, L(x))\big)$, we need the following result.

Lemma 8.19. *Suppose that $L(x)$ is not a monomial if $k = 2$ or $k = n - 2$. Then*

$$N(\mathcal{H}_{k,s}(x, L(x))) = \left\{ \left(a x^{q^l}, a^{-1} x^{q^{n-l}}, x^{p^{\lambda(n-l)}} \right) : 0 \leq l < n, a \in \mathbb{F}_q^* \right\}.$$

Therefore, $|N(\mathcal{H}_{k,s}(x, L(x)))| = n(q-1)$.

Proof. Let $(\phi_1, \phi_2, \varphi) \in N(\mathcal{H}_{k,s}(x, L(x)))$. By Theorem 8.10, we have that

$$G\big(\mathcal{H}_{k,s}(x, L(x))\big) \subset \left\{ \left(a x^{q^l}, b x^{q^{n-l}}, x^{p^\nu} \right) \colon a, b \in \mathbb{F}_{q^n}^*, 0 \leq l < n, 0 \leq \nu < \lambda n \right\}.$$

Therefore, $(\phi_1, \phi_2, \varphi) = (a x^{q^l}, b x^{q^{n-l}}, x^{p^\nu})$ for some integers l, ν such that $0 \leq l < n$ and $0 \leq \nu < \lambda n$ and $a, b \in \mathbb{F}_{q^n}^*$. For all $y \in \mathbb{F}_{q^n}$, we have that $\phi_1 \circ \varphi(y) x \circ \phi_2 = yx$, so that $a b^{q^l} y^{p^{\nu + l\lambda}} x = yx$. Therefore, $\nu = \lambda(n-l)$ and $a b^{q^l} = 1$. In the same way, we have that $a b^{q^{l+s}} y x^{q^s} = y x^{q^s}$ for all $y \in \mathbb{F}_{q^n}$, which implies that $a b^{q^{l+s}} = 1$. Therefore $b^{q^s - 1} = 1$ and then, since $\gcd(s, n) = 1$, we have that $b \in \mathbb{F}_q^*$. We conclude the proof by observing that $a b^{q^l} = ab = 1$ implies that $b = a^{-1}$. ∎

Theorem 8.20. *Let $\mathcal{I} \subseteq [0, n-1]$ be a nonempty set and $d = \gcd(q^k - 1, q^n - 1) = q^{\gcd(k,n)} - 1$. Suppose $L(x) = \sum_{i=0}^{n-1} \eta_i x^{q^i}$ where $\eta_i \neq 0$ if $i \in \mathcal{I}$ and $\eta_i = 0$ otherwise. Assume that $|\mathcal{I}| > 1$ if $k = 2$ or $k = n - 2$. Let $\gcd(\mathcal{I})$ denote the greatest common divisor of the elements in the set $\mathcal{I} \cup \{n\}$. The group $G\big(\mathcal{H}_{k,s}(x, L(x))\big)$ is given by*

$$\left\{ \left(a x^{q^l}, b x^{q^{n-l}}, x^{p^\nu} \right) \colon a, b \in \mathbb{F}_{q^n}^*, 0 \leq l < n, 0 \leq \nu < \lambda n \text{ and } \eta_i^{p^\nu q^l - 1} = \tfrac{(a b^{q^l})^{q^i}}{a b^{q^{l+sk}}} \text{ for all } i \in \mathcal{I} \right\}.$$

Furthermore, if $|\mathcal{I}| \geq 2$, then

$$\left|\mathrm{Aut}\left(\mathcal{H}_{k,s}(x, L(x))\right)\right| = \frac{\kappa d}{n(q-1)} \left| \left\{ (\nu, l) \in \mathcal{B} \,\middle|\, \begin{array}{l} \exists\ \alpha, \beta \in \mathbb{F}_{q^n}^* \text{ such that } \chi_d(\alpha\beta) = 1 \\ \text{and } \eta_i^{p^\nu q^l - 1} = \alpha \beta^{q^i} \text{ for all } i \in \mathcal{I} \end{array} \right\} \right|$$

where $\mathcal{B} = [0, \lambda n - 1] \times [0, n-1]$ and $\kappa = \gcd\left(\kappa_{q^n}(\mathcal{I}), \frac{(q^{\gcd(\mathcal{I})} - 1)(q^n - 1)}{d}\right)$.

Proof. By Theorem 8.10, we can assume that an element of $G\big(\mathcal{H}_{k,s}(x, L(x))\big)$ is of the form $\big(ax^{q^l}, bx^{q^{n-l}}, \varphi\big)$ where $a, b \in \mathbb{F}_{q^n}^*$, $\varphi \in \mathrm{Aut}(\mathbb{F}_{q^n})$ and l and ν are integers satisfying $0 \leq l \leq n-1$ and $\varphi(c) = c^{p^\nu}$ for all $c \in \mathbb{F}_{q^n}$. By Theorem 8.12, we have that

$$\sum_{i=0}^{n-1} \eta_i x^{q^i} = L(x) = ab^{q^{sk+l}} L((x/ab^{q^l})^{p^{n\lambda-\nu}q^{n-l}})^{p^\nu q^l} = ab^{q^{sk+l}} \sum_{i=0}^{n-1} \eta_i^{p^\nu q^l} \frac{1}{(ab^{q^l})^{q^i}} x^{q^i}.$$

The first part of our result follows from Lemma 8.2. Now let

$$\Delta_{\nu,l} = \{(\alpha, \beta) \in \mathbb{F}_{q^n}^2 : \eta_i^{p^\nu q^l - 1} = \alpha\beta^{q^i} \text{ for all } i \in \mathcal{I}\}.$$

Claim 1. For each pair $(\alpha, \beta) \in \Delta_{\nu,l}$ the following hold:

1. If $\chi_d(\alpha\beta) = 1$, then there exist exactly d pairs $(a, b) \in \mathbb{F}_{q^n}^2$ such that $\big(ax^{q^l}, bx^{q^{n-l}}, \varphi\big) \in G\big(\mathcal{H}_{k,s}(x, L(x))\big), \beta = ab^{q^l}$ and $\alpha^{-1} = ab^{q^{l+sk}}$;
2. If $\chi_d(\alpha\beta) \neq 1$, then there exists no pair $(a, b) \in \mathbb{F}_{q^n}^2$ such that $\big(ax^{q^l}, bx^{q^{n-l}}, \varphi\big) \in G\big(\mathcal{H}_{k,s}(x, L(x))\big), \beta = ab^{q^l}$ and $\alpha^{-1} = ab^{q^{l+sk}}$.

Proof of the Claim 1. Let $(\nu, l) \in \mathcal{B}$ and assume that there exist $\alpha, \beta \in \mathbb{F}_{q^n}^*$ such that $\eta_i^{p^\nu q^l - 1} = \alpha\beta^{q^i}$ for all $i \in \mathcal{I}$. If $\big(ax^{q^l}, bx^{q^{n-l}}, \varphi\big) \in G\big(\mathcal{H}_{k,s}(x, L(x))\big), \beta = ab^{q^l}$ and $\alpha^{-1} = ab^{q^{l+sk}}$, then a straightforward computation shows that

$$b^{q^{sk}-1} = (\alpha\beta)^{-q^{n-l}} \text{ and } a = \beta b^{-q^l}.$$

Therefore $\chi_d(\alpha\beta) = 1$. Furthermore, for each β there exist d elements $b \in \mathbb{F}_{q^n}$ such that $b^{q^{sk}-1} = (\alpha\beta)^{-q^{n-l}}$. Then for each pair $(\alpha, \beta) \in \Delta_{\nu,l}$, there exist d pairs $(a, b) \in \mathbb{F}_{q^n}^2$ such that $\big(ax^{q^l}, bx^{q^{n-l}}, \varphi\big) \in G\big(\mathcal{H}_{k,s}(x, L(x))\big)$, proving the claim.

Now we let

$$\Delta'_{\nu,l} = \{(\alpha, \beta) \in \mathbb{F}_{q^n}^2 : \eta_i^{p^\nu q^l - 1} = \alpha\beta^{q^i} \text{ for all } i \in \mathcal{I} \text{ and } \chi_d(\alpha\beta) = 1\}.$$

Claim 2. For each pair $(\nu, l) \in \mathcal{B}$, we have that the value $|\Delta'_{\nu,l}|$ equals either 0 or $\gcd\left(\kappa_{q^n}(\mathcal{I}), \frac{(q^{\gcd(\mathcal{I})}-1)(q^n-1)}{d}\right)$.

Proof of the Claim 2. Let (α_1, β_1) and (α_2, β_2) be two elements (distinct or not) in $\Delta'_{\nu,l}$. For $i > j$ elements in $\mathcal{I}$, we have that

$$\beta_1^{q^i - q^j} = \eta_i^{p^\nu q^l - 1} \eta_j^{-(p^\nu q^l - 1)} = \beta_2^{q^i - q^j}$$

and then it follows that $\beta_1 = \delta\beta_2$ where δ is a $(q^{\gcd(i-j,n)} - 1)$-th root of unity in $\mathbb{F}_{q^n}$. Since i and j were taken arbitrarily, it follows that $\beta_2 = \xi\beta_1$ where ξ is a $\kappa_{q^n}(\mathcal{I})$-th root of unity in $\mathbb{F}_{q^n}$ and then

$$\Delta'_{\nu,l} \subseteq \{(\xi^{-iq^j}\alpha_1, \xi^i\beta_1) : 0 \leq i < \kappa_{q^n}(\mathcal{I})\}$$

for ξ a primitive $\kappa_{q^n}(\mathcal{I})$-th root of unity and $j \in \mathcal{I}$. We observe that

$$\chi_d(\xi^{-iq^j}\alpha_1\xi^i\beta_1) = \chi_d(\xi^{i(1-q^j)})\chi_d(\alpha_1\alpha_2) = \chi_d(\xi^{i(1-q^j)}),$$

so that $(\xi^{-iq^j}\alpha_1, \xi^i\beta_1) \in \Delta'_{\nu,l}$ if and only if $i(1-q^j)\frac{q^n-1}{d} \equiv 0 \pmod{\kappa_{q^n}(\mathcal{I})}$. Since $\gcd(\kappa_{q^n}(\mathcal{I}), q^j - 1) = q^{\gcd(\mathcal{I})} - 1$, we have that $(\xi^{-iq^j}\alpha_1, \xi^i\beta_1) \in \Delta'_{\nu,l}$ if and only if $i(q^{\gcd(\mathcal{I})} - 1)\frac{q^n-1}{d} \equiv 0 \pmod{\kappa_{q^n}(\mathcal{I})}$. Therefore

$$|\Delta'_{\nu,l}| = \frac{\kappa_{q^n}(\mathcal{I})}{\gcd\left(\kappa_{q^n}(\mathcal{I}), \frac{(q^{\gcd(\mathcal{I})}-1)(q^n-1)}{d}\right)} = \gcd\left(\kappa_{q^n}(\mathcal{I}), \frac{(q^{\gcd(\mathcal{I})}-1)(q^n-1)}{d}\right),$$

proving the claim.

We observe that

$$G\big(\mathcal{H}_{k,s}(x,L(x))\big) = \bigcup_{(\nu,l)\in\mathcal{B}} \bigcup_{(\alpha,\beta)\in\Delta'_{\nu,l}} \left\{ \left(ax^{q^l}, bx^{q^{n-l}}, x^{p^\nu}\right) : \beta = ab^{q^l}, \alpha^{-1} = ab^{q^{l+sk}} \right\} \tag{8.6}$$

and the sets in this union are disjoint by definition. Our assertion follows from Equations (8.6) and (8.5) by applying Claims 1 and 2 and Lemma 8.19. ■

As an immediate consequence we have the following result.

Corollary 8.21. *Let L be a linearized polynomial and n, k and let κ be integers under the same conditions as Theorem 8.20. Let $\mathcal{I} \subseteq [0, n-1]$ be a set with $|\mathcal{I}| \geq 2$. Then*

$$\left|\mathrm{Aut}\left(\mathcal{H}_{k,s}(x,L(x))\right)\right| = \frac{\kappa\lambda n(q^{\gcd(k,n)}-1)}{\tau(L)(q-1)} \leq \frac{\kappa\lambda n(q^{\gcd(k,n)}-1)}{q-1},$$

where

$$\tau(L) = \min\left\{ m|\lambda n \middle| \exists \alpha,\beta \in \mathbb{F}_{q^n}^* \text{ such that } \chi_d(\alpha\beta)=1 \text{ and } \eta_i^{p^m-1} = \alpha\beta^{q^i} \text{ for all } i \in \mathcal{I} \right\}.$$

Proof. Let

$$A = \{m|\lambda n : \exists \alpha,\beta \in \mathbb{F}_{q^n}^* \text{ such that } \chi_d(\alpha\beta)=1 \text{ and } \eta_i^{p^m-1} = \alpha\beta^{q^i} \text{ for all } i \in \mathcal{I}\}.$$

We only need to show that if $m_1, m_2 \in A$, then $\gcd(m_1,m_2) \in A$, since for each $m \in A$, it is easy to note that $lm \in A$ for any integer l. For m_1, m_2 and $m = \gcd(m_1,m_2)$, let a and b be integers such that $a(p^{m_1}-1) + b(p^{m_2}-1) = p^m - 1$. Suppose that $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{F}_{q^n}^*$ are such that $\eta_i^{p^{m_1}-1} = \alpha_1\beta_1^{q^i}$ and $\eta_i^{p^{m_2}-1} = \alpha_2\beta_2^{q^i}$ for all $i \in \mathcal{I}$. Then

$$\eta_i^{p^m-1} = \eta_i^{a(p^{m_1}-1)+b(p^{m_2}-1)} = \left(\alpha_1\beta_1^{q^i}\right)^a \left(\alpha_2\beta_2^{q^i}\right)^b = (\alpha_1^a\alpha_2^b)(\beta_1^a\beta_2^b)^{q^i} \text{ for all } i \in \mathcal{I}.$$

Our result follows from Theorem 8.20 by observing that $\chi_d(\alpha_1\beta_1)=1$ and $\chi_d(\alpha_2\beta_2)=1$ imply that $\chi_d(\alpha_1^a\alpha_2^b\beta_1^a\beta_2^b)=1$. ■

In particular, in the case where there exist $\alpha,\beta \in \mathbb{F}_{q^n}^*$ such that $\chi_d(\alpha\beta)=1$ and $\eta_i = \alpha\beta^i$ for all $i \in \mathcal{I}$, the integers ν and l can be arbitrarily chosen. Then

$$\left|\mathrm{Aut}\left(\mathcal{H}_{k,s}(x,L(x))\right)\right| = \frac{\kappa\lambda n(q^{\gcd(k,n)}-1)}{q-1}.$$

The remaining case is $L(x) = \eta x^{q^h}$. For this case, let g be a primitive element of $\mathbb{F}_{q^n}^*$ and let $\eta = g^u$, where u is an integer.

Corollary 8.22. *Assume that $2 < k < n-2$. If $\eta = g^u \in \mathbb{F}_{q^n}$ and $d = q^{\gcd(n,h,sk-h)} - 1 = q^{\gcd(n,h,k)} - 1$, then*

$$\left|\mathrm{Aut}\left(\mathcal{H}_{k,s}(x,\eta x^{q^h})\right)\right| = \frac{nd\lambda(q^n-1)}{\tau(g^u,h)(q-1)},$$

where

$$\tau(g^u,h) = \min\left\{m|\lambda n : d \text{ divides } (u(p^m-1))\right\}.$$

Proof. Let $\Delta = \{m|\lambda n : (q^{\gcd(n,h,sk-h)} - 1) \text{ divides } (u(p^m-1))\}$. By Theorem 8.20, if $\left(ax^{q^l}, bx^{q^{n-l}}, \varphi\right) \in G\left(\mathcal{H}_{k,s}(x, \eta x^{q^h})\right)$ then

$$(g^u)^{p^\nu q^l - 1} = \frac{(ab^{q^l})^{q^h}}{ab^{q^{l+sk}}} = a^{q^h-1}b^{q^l(q^h-q^{sk})} = a^{q^h-1}b^{q^{l+h}(1-q^{sk-h})}.$$

Set $d_1 = q^h - 1$, $d_2 = 1 - q^{sk-h}$ and $d = \gcd(q^n - 1, d_1, d_2)$. We have that

$$\left(g^{u(p^\nu q^l-1)}\right)^{\frac{q^n-1}{d}} = \left(a^{d_1}b^{q^{l+h}d_2}\right)^{\frac{q^n-1}{d}} = 1$$

and then $d|(u(p^\nu q^l - 1))$. In particular, $(\nu + \lambda l) \in \Delta$. Hence, if $a = g^i$ and $b^{q^{l+h}} = g^j$, then

$$g^{id_1}g^{jd_2} = g^{u(p^\nu q^l-1)}. \tag{8.7}$$

The number solutions (i, j) of the Equation (8.7) with $0 \leq i, j < q^n - 1$ is equal to d^2 multiplied by the number of pairs (i, j) with $0 \leq i, j < \frac{q^n-1}{d}$ satisfying the equation

$$i\left(\tfrac{d_1}{d}\right) + j\left(\tfrac{d_2}{d}\right) \equiv \tfrac{u(p^\nu q^l-1)}{d} \pmod{\tfrac{q^n-1}{d}}, \tag{8.8}$$

which is a Diophantine equation over $\mathbb{Z}_{(q^n-1)/d}$. For a pair (i, j), let $f(i, j) = i\left(\frac{d_1}{d}\right) + j\left(\frac{d_2}{d}\right)$. Let $(i_0, j_0) \in \mathbb{Z}_{(q^n-1)/d}$ satisfying $f(i_0, j_0) = e$ with $e := \gcd(d_1/d, d_2/d)$. We recall that e is an unity in $\mathbb{Z}_{(q^n-1)/d}$, then $e^{-1} \in \mathbb{Z}_{(q^n-1)}$. For $A \in \mathbb{Z}_{(q^n-1)/d}$, let

$$\Upsilon_A = \{(i, j) \in \mathbb{Z}^2_{(q^n-1)/d} : f(i, j) \equiv A \pmod{\tfrac{q^n-1}{d}}\} \tag{8.9}$$

be the set of solutions of $f(i, j) = A$ and let $n_A = |\Upsilon_A|$. It is direct to verify that $\sum_A n_A \leq (\frac{q^n-1}{d})^2$ and $(i_A, j_A) := (i_0e^{-1}A, j_0e^{-1}A) \in \Upsilon_A$. Furthermore, if $(i_{A,t}, j_{A,t})$ is given by $i_{A,t} = i_A + t\frac{d_2}{d}$ and $j_{A,t} = j_A - t\frac{d_1}{d}$ with $t \in \mathbb{Z}_{(q^n-1)/d}$, then $(i_{A,t}, j_{A,t}) \in \Upsilon_A$. Then

$$\Upsilon'_A := \left\{\left(i_A + t\tfrac{d_2}{d}, j_A - t\tfrac{d_1}{d}\right) : 0 \leq t < \tfrac{q^n-1}{d}\right\} \subset \Upsilon_A. \tag{8.10}$$

Set $d'_1 = \gcd(\frac{q^n-1}{d}, \frac{d_1}{d})$ and $d'_2 = \gcd(\frac{q^n-1}{d}, \frac{d_2}{d})$. We observe that $i_{A,t} = i_{A,t'}$ if and only if $t \equiv t' \pmod{\frac{q^n-1}{dd'_1}}$. Furthermore, $j_{A,t} = j_{A,t'}$ if and only if $t \equiv t' \pmod{\frac{q^n-1}{dd'_2}}$, so that $(i_{A,t}, j_{A,t}) = (i_{A,t'}, j_{A,t'})$ if and only if $t \equiv t' \pmod{\operatorname{lcm}\left(\frac{q^n-1}{dd'_1}, \frac{q^n-1}{dd'_2}\right)}$. Since $\operatorname{lcm}\left(\frac{q^n-1}{d}, \frac{d_1}{d}, \frac{d_2}{d}\right) = 1$, it follows that $\operatorname{lcm}\left(\frac{q^n-1}{dd'_1}, \frac{q^n-1}{dd'_2}\right) = \frac{q^n-1}{d}$ and then $|\Upsilon'_A| = \frac{q^n-1}{d}$. Therefore $n_A \geq \frac{q^n-1}{d}$ by the inclusion in (8.19). Since $\sum_{A\in\mathbb{Z}_{(q^n-1)/d}} n_A \leq (\frac{q^n-1}{d})^2$ and $n_A \geq \frac{q^n-1}{d}$, we must have $n_A = \frac{q^n-1}{d}$ for all $A \in \mathbb{Z}_{(q^n-1)/d}$. In particular, $\Upsilon_\ell = \frac{q^n-1}{d}$ for $\ell = \frac{u(p^\nu q^l-1)}{d}$ and then the number of solutions of Equation (8.7) is $d^2\frac{q^n-1}{d} = d(q^n - 1)$. More generally, we have that the number of pairs (a, b) for which $\left(ax^{q^l}, bx^{q^{n-l}}, \varphi\right) \in G\left(\mathcal{H}_{k,s}(x, \eta x^{q^h})\right)$ equals $d(q^n - 1)$ provided $(\nu + \lambda l) \in \Delta$ and then we only need to compute the number of such pairs (ν, l).

It is direct to verify the number of pairs (ν, l) such that $(\nu + \lambda l) \in \Delta$ is exactly $n \cdot |\Delta|$. Similarly to the proof of the previous result, we can show that

$$\Delta = \left\{l\tau(g^u, h) : 0 < l \leq \tfrac{\lambda n}{\tau(g^u,h)}\right\}$$

and then $|\Delta| = \frac{\lambda n}{\tau(g^u,h)}$, from where our result follows. ■

In particular, Corollary 8.22 gives us the number of automorphisms of Generalized Twisted Gabidulin codes in the cases where k satisfies $2 < k < n - 2$.

Example 8.23. *Let g be a primitive element of $\mathbb{F}_{q^n}$ and let h be a positive integer. Let k be a integer such that $2 < k < n-2$. For an integer u such that $\gcd(u,d) = 1$, the number of elements of the automorphism group of the code $\mathcal{H}_{k,s}(x, g^u x^{q^h})$ equals $\frac{nd(q^n-1)}{\gcd(n,h,k)(q-1)}$, since we have that $\tau(g^u, h) = \lambda \gcd(n,h,k)$.*

CHAPTER 9

Conclusion and future work

This thesis compiles works on finite fields in different themes. In this chapter, we summarize the results obtained in the thesis and provide comments on future research work that arise from the present thesis. We separate the topics according to the order of corresponding chapters.

9.1 Rational points on curves of low degree

In Chapter 2 we related the number of $\mathbb{F}_q$-rational points of curves given by an equation of the form $y^d = f(x)$ for the following positive integers d and polynomials $f(x)$:

d	$f(x)$	Conditions	Result
2	$(ax^3+bx^2+cx+d)(x+e)$	$a \neq 0$	Theorem 2.18
2	$ax^6+bx^4+cx^2+d$	$a \neq 0$	Theorem 2.20
2	ax^4+bx^2+c	$a \neq 0$	Theorem 2.22
2	$(ax^2+bx+c)(Ax^2+Bx+C)$	$b^2 \neq 4ac$ and $B^2 \neq 4AC$	Corollary 2.26
3	$(x+a)(Ax^2+Bx+C)$	$A \neq 0$ and $Aa^2 \neq Ba-C$	Theorem 2.28
3	$(x+a)^2(Ax^2+Bx+C)^2$	$A \neq 0$ and $Aa^2 \neq Ba-C$	Theorem 2.28
3	ax^3+b	$a \neq 0$	Theorem 2.30
3	ax^6+b	$a \neq 0$ and $b \neq 0$	Theorem 2.2
4	ax^4+bx^2+c	$a \neq 0$ and $q \equiv 1 \pmod 4$	Theorem 2.4
4	ax^4+bx^2+c	$a \neq 0$ and $p \equiv 3 \pmod 4$	Corollary 2.35

We observe that for $d = 2$ the single remaining case is when f is an irreducible polynomial over $\mathbb{F}_q$. In our future works we intend to study wild families of curves in order to present a more general result.

9.2 Hypersurfaces of Fermat type

Chapter 3 provided a counting on the number of $\mathbb{F}_q$-rational points on Fermat hypersurfaces given by an equation of the form $a_1x_1^{d_1} + \cdots + a_sx_s^{d_s} = b$ with $x_i \in \mathbb{F}_{p^{t_i}}$ satisfying conditions on the exponents, namely d_i is (p, r_i)-admissible. The cases $t_i \neq n$ for some i had never been studied using our approach. Indeed, there were not explicit formulas for restricted solution sets' case in the literature. We can go further our results and look for the roots of the partial zeta function associated to the number of solutions of Equation (3.1). From here, we pose the following general problem.

Problem 9.1. *Assuming that d_i is (p, r_i)-admissible, present the inverse of the roots of the polynomials associated to the partial zeta function of the number of solution of* (3.1).

If $t_1 = \cdots = t_s = n$, then it is direct to compute the inverse of the roots, that are essentially Jacobi Sums. If d_i is (p, r_i)-admissible, then the value of these Jacobi Sums is known (see Theorem 1 of [23]). Our counting results for $t_1 = \cdots = t_s = n$ extend the main result of [109] and some results of [13]. In the general situation where no conditions are imposed under the exponents, an explicit general formula for such number is unknown. Indeed, the problem of counting the number of $\mathbb{F}_q$-rational points on Fermat hypersurfaces in a general setting is still an open problem. Many authors have studied particular cases in the last few years. From here, we pose the following open problem.

Problem 9.2. *Find an explicit formula for $N_s(\vec{a}, \vec{d}, \vec{t}, q, b)$ (with $b \neq 0$) without assuming d_i is (p, r_i)-admissible.*

There exist some few articles in this direction (e.g. see [8, 56]). In fact, the difficult of the general situation comes from the fact that we can not say so much about the value of $J_b(\chi_{d_1}^{\ell_1}, \ldots, \chi_{d_s}^{\ell_s})$, which is well known if d_i is (p, r_i)-admissible (e.g. see [3, 23]).

9.3 On maximal and minimal hypersurfaces of Fermat type

In Chapter 4 we provide results characterizing Fermat hypersurfaces whose number of points are maximal or minimal with respect to Weil's bound. The approach used here is completely new and consist in the use of the well celebrated Hasse-Davenport Relation. Our effort in this chapter yields a characterization of maximal and minimal Fermat hypersurfaces in the following cases:

b	s	Exponents	Additional condition	Result
$b = 0$	$s \geq 3$	$d_1 = \cdots = d_s = d \geq 2$	$(s, d) \neq (4, 3)$	Theorem 4.1
$b \neq 0$	$s \geq 2$	$d_1 = \cdots = d_s = d \geq 2$	$(s, d) \neq (3, 3)$	Theorem 4.1
$b \neq 0$	$s = 2$	$d_i \geq 2$	none	Theorem 4.3
$b \neq 0$	$s \geq 4$	$d_i \geq 2$	$\gcd(d_1, \ldots, d_s) > 1$	Theorem 4.3

The conditions appearing here comes from technical obstructions in the proof of the theorems. We actually do not known if similar results holds in these cases. The next step is to study these

cases in order to find conditions for maximality and minimality of such hypersurfaces, that to date remains being open problems.

9.4 On the number of rational points on Artin-Schreier hypersurfaces

Chapter 5 provides a broad study of the number of rational points on Artin-Schreier hypersurfaces. As well as in Chapter 3, the condition that the exponents are admissible was necessary in order to obtain a formula for the number of points (Theorem 5.5). The next step in this direction consists in find a formula without assuming the the exponents satisfy this condition. In this chapter we provided bounds for the number of rational points that improve Weil's bound (Theorem 5.2) and presented conditions for Weil's bound to be attained. In particular, our results yields conditions in which our bounds in Theorem 5.2 are attained in the case $\mathrm{Tr}_{p^n/p}(b) = 0$. A good question here is to find similar conditions for the case $\mathrm{Tr}_{p^n/p}(b) \neq 0$.

9.5 Dynamics of polynomial maps over finite fields

In Chapter 6 we study the functional graph associated to polynomials $f \in \mathbb{F}_q[x]$ whose polynomial associated ψ_f satisfies a property of injectivity on the set μ_m. An interesting problem here is to use the same approach for other similar conditions that guarantee some kind of regularity in the graph associated to a function f as soon as it is provided some special structure in the functional graph associated to the function f on some subset $U \subset \mathbb{F}_q$.

9.6 On iterations of rational functions over perfect fields

Section 7 studies the number $\Delta_{\alpha,R}(n)$ of solutions of the equation $R^{(n)}(x) = \alpha$ over $\overline{\mathbb{F}_q}$. We prove that the growth of $\Delta_{\alpha,R}(n)$ is exponential in d if α is not R-critical (Theorem 7.2). The R-critical case is also studied (see Theorem 7.3). From here, we present some open problems that are proposed in [79]. In what follows, $R \in \mathbb{F}_q(x)$ is a rational function and $f \in \mathbb{F}_q[x]$ is a polynomial of positive degree with at least one root that is not R-critical. Theorem 7.21 implies that $M_{f,R}$ may have linear or exponential growth if $f \in \mathcal{M}_q$. We believe that these are the only possible cases.

Problem 9.3. *Prove or disprove: either* $M_{f,R}(n) \approx n$ *or* $\log M_{f,R}(n) \gg n$.

We observe that $M_{f,R}(n) \cdot N_{f,R}(n) \geq \delta_{f,R}(n)$ for every $n \geq 0$. In particular, there exists $d_0 > 1$ such that for every $n \gg 1$, either $M_{f,R}(n) > d_0^n$ or $N_{f,R}(n) > d_0^n$. However, this is not sufficient to conclude that at least one of these functions have exponential growth. Motivated by these observations, we propose the following problem.

Problem 9.4. *Prove or disprove: either* $\log M_{f,R}(n) \gg n$ *or* $\log N_{f,R}(n) \gg n$.

Since $M_{f,R}(n) \cdot N_{f,R}(n) \geq \delta_{f,R}(n)$, a positive answer to Problem 9.3 implies a positive answer to Problem 9.4.

Problem 9.5. *Prove or disprove:* $A_{f,R}(n) \gg n$.

We have seen that $A_{f,R}(n) \approx n$ for infinitely many rational functions R. In particular, Positive answer to Problem 9.5 implies that the bound $A_{f,R}(n) \gg n$ is sharp on the growth type.

9.7 Rank metric codes arising from linearized polynomials

In Section 8 we studied when two twisted Gabidulin codes are equivalent (Theorem 8.10). The next step here is to find new families of MRD-codes and then use Theorem 8.10 to prove that these new families are not equivalent to the known families of MRD twisted Gabidulin codes. In our second important result of the chapter, namely Theorem 8.20, we provided the automorphism group of the code $\mathcal{H}_{k,s}(x, L(x))$, which allowed us to present the number of automorphisms for some special polynomials L. We can go further this problem by expanding the class of codes studied and finding their automorphism group and/or its cardinality.

Bibliography

[1] M. Abdón, J. Bezerra, and L. Quoos, *Further examples of maximal curves*, Journal of Pure and Applied Algebra, 213 (2009), pp. 1192–1196.

[2] A. Akbary, D. Ghioca, and Q. Wang, *On constructing permutations of finite fields*, Finite Fields and Their Applications, 17 (2011), pp. 51–67.

[3] S. Akiyama, *On the pure Jacobi sums*, Acta Arithmetica, 75 (1996), pp. 97–104.

[4] N. Ali, *Stabilité des polynômes*, Acta Arithmetica, 119 (2005), pp. 53–63.

[5] Y. Aubry, *Reed-Muller codes associated to projective algebraic varieties*, in Coding theory and algebraic geometry, Springer, 1992, pp. 4–17.

[6] Y. Aubry and M. Perret, *A Weil theorem for singular curves*, (1996).

[7] M. Ayad and D. McQuillan, *Irreducibility of the iterates of a quadratic polynomial over a field*, Acta Arithmetica, 93 (2000), pp. 87–97.

[8] I. Baoulina, *On the number of solutions to certain diagonal equations over finite fields*, International Journal of Number Theory, 6 (2010), pp. 1–14.

[9] I. N. Baoulina, *On a class of diagonal equations over finite fields*, Finite Fields and Their Applications, 40 (2016), pp. 201–223.

[10] R. Benedetto, P. Ingram, R. Jones, M. Manes, J. Silverman, and T. Tucker, *Current trends and open problems in arithmetic dynamics*, Bulletin of the American Mathematical Society, 56 (2019), pp. 611–685.

[11] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi sums*, Wiley New York, 1998.

[12] W. Cao and Q. Sun, *Factorization formulae on counting zeros of diagonal equations over finite fields*, Proceedings of the American Mathematical Society, 135 (2007), pp. 1283–1291.

[13] X. Cao, W.-S. Chou, and J. Gu, *On the number of solutions of certain diagonal equations over finite fields*, Finite Fields and Their Applications, 42 (2016), pp. 225–252.

[14] W.-S. Chou and I. E. Shparlinski, *On the cycle structure of repeated exponentiation modulo a prime*, Journal of Number Theory, 107 (2004), pp. 345–356.

[15] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren, *Handbook of elliptic and hyperelliptic curve cryptography*, Chapman and Hall/CRC, 2005.

[16] A. Coşgun, F. Özbudak, and Z. Saygi, *Further results on rational points of the curve $y^{q^n} - y = \gamma x^{q^h+1} - \alpha$ over $\mathbb{F}_{q^m}$*, Designs, Codes and Cryptography, 79 (2016), pp. 423–441.

[17] A. Cossidente, J. Hirschfeld, G. Korchmáros, and F. Torres, *On plane maximal curves*, Compositio Mathematica, 121 (2000), pp. 163–181.

[18] R. S. Coulter, *Explicit evaluations of some Weil sums*, Acta Arithmetica, 83 (1998), pp. 241–251.

[19] ——, *The number of rational points of a class of Artin-Schreier curves*, Finite Fields and Their Applications, 8 (2002), pp. 397–413.

[20] P. Delsarte, *Bilinear forms over a finite field, with applications to coding theory*, Journal of Combinatorial Theory, Series A, 25 (1978), pp. 226–241.

[21] I. Duursma and K.-H. Mak, *On maximal curves which are not Galois subcovers of the Hermitian curve*, Bulletin of the Brazilian Mathematical Society, New Series, 43 (2012), pp. 453–465.

[22] I. M. Duursma, *Two-point coordinate rings for GK-curves*, IEEE Transactions on Information Theory, 57 (2011), pp. 593–600.

[23] R. J. Evans, *Pure Gauss sums over finite fields*, Mathematika, 28 (1981), pp. 239–248.

[24] S. Fanali and M. Giulietti, *One-point AG codes on the GK maximal curves*, IEEE Transactions on Information Theory, 56 (2009), pp. 202–210.

[25] E. M. Gabidulin, *Theory of codes with maximum rank distance*, Problemy Peredachi Informatsii, 21 (1985), pp. 3–16.

[26] M. Gadouleau and Z. Yan, *Properties of codes with the rank metric*, in IEEE Globecom 2006, IEEE, 2006, pp. 1–5.

[27] A. Garcia, *On curves with many rational points over finite fields*, in Finite Fields with Applications to Coding Theory, Cryptography and Related Areas, Springer, 2002, pp. 152–163.

[28] ——, *A note on the Giulietti-Korchmaros maximal curve*, Contemporary Mathematics, 14 (2009), p. 83.

[29] A. Garcia, C. Güneri, and H. Stichtenoth, *A generalization of the Giulietti-Korchmáros maximal curve*, Adv. Geom., 10 (2010), pp. 427–434.

[30] A. Garcia and H. Stichtenoth, *A maximal curve which is not a Galois subcover of the Hermitian curve.*, Bulletin of the Brazilian Mathematical Society, 37 (2006).

[31] ——, *A note on a maximal curve*, in Arithmetic, geometry, cryptography and coding theory 2009, vol. 521 of Contemp. Math., 2010, pp. 55–58.

[32] A. Garcia and S. Tafazolian, *Cartier operators and maximal curves*, Acta Arithmetica, 135 (2008), pp. 199–218.

[33] ——, *Certain maximal curves and Cartier operators*, Acta Arithmetica, 135 (2008), pp. 199–218.

[34] T. A. Gassert, *Chebyshev action on finite fields*, Discrete Mathematics, 315 (2014), pp. 83–94.

[35] M. Giulietti and G. Korchmáros, *A new family of maximal curves over a finite field*, Mathematische Annalen, 343 (2009), pp. 229–245.

[36] D. Gómez-Pérez, A. Ostafe, and I. E. Shparlinski, *On irreducible divisors of iterated polynomials*, Revista Matemática Iberoamericana, 30 (2014), pp. 1123–1134.

[37] C. Güneri and F. Özbudak, *Multidimensional cyclic codes and Artin–Schreier type hypersurfaces over finite fields*, Finite Fields and Their Applications, 14 (2008), pp. 44–58.

[38] D. R. Heath-Brown and G. Micheli, *Irreducible polynomials over finite fields produced by composition of quadratics*, Revista Matemática Iberoamericana, 35 (2019), pp. 847–855.

[39] J. Hirschfeld and G. Korchmáros, *On the number of rational points on an algebraic curve over a finite field*, Bulletin of the Belgian Mathematical Society-Simon Stevin, 5 (1998), pp. 313–340.

[40] J. W. P. Hirschfeld, G. Korchmáros, F. Torres, and F. E. T. Orihuela, *Algebraic curves over a finite field*, Princeton University Press, 2008.

[41] X.-D. Hou and C. Sze, *On certain diagonal equations over finite fields*, Finite Fields and Their Applications, 15 (2009), pp. 633–643.

[42] S. Hu, S. Hong, and W. Zhao, *The number of rational points of a family of hypersurfaces over finite fields*, Journal of Number Theory, 156 (2015), pp. 135–153.

[43] L. Hua and H. Vandiver, *Characters over certain types of rings with applications to the theory of equations in a finite field*, Proceedings of the National Academy of Sciences of the United States of America, 35 (1949), p. 94.

[44] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, vol. 84, Springer, 1982.

[45] D. Johnson, A. Menezes, and S. Vanstone, *The elliptic curve digital signature algorithm (ECDSA)*, International Journal of Information Security, 1 (2001), pp. 36–63.

[46] R. Jones, *The density of prime divisors in the arithmetic dynamics of quadratic polynomials*, Journal of the London Mathematical Society, 78 (2008), pp. 523–544.

[47] R. Jones and N. Boston, *Settled polynomials over finite fields*, Proceedings of the American Mathematical Society, 140 (2012), pp. 1849–1863.

[48] D. B. Leep and C. C. Yeomans, *The number of points on a singular curve over a finite field*, Archiv der Mathematik, 63 (1994), pp. 420–426.

[49] R. Lercier and F. Morain, *Counting the number of points on elliptic curves over finite fields: strategies and performances*, in International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 1995, pp. 79–94.

[50] R. Lidl and H. Niederreiter, *Finite Fields*, vol. 20, Cambridge University Press, 1997.

[51] D. Liebhold and G. Nebe, *Automorphism groups of Gabidulin-like codes*, Archiv der Mathematik, 107 (2016), pp. 355–366.

[52] G. Lunardon, *MRD-codes and linear sets*, Journal of Combinatorial Theory, Series A, 149 (2017), pp. 1–20.

[53] G. Lunardon, R. Trombetti, and Y. Zhou, *Generalized twisted Gabidulin codes*, Journal of Combinatorial Theory, Series A, 10 (2016), pp. 475–488.

[54] ——, *On kernels and nuclei of rank metric codes*, Journal of Algebraic Combinatorics, 46 (2017), pp. 313–340.

[55] R. Martins, D. Panario, and C. Qureshi, *A survey on iterations of mappings over finite fields*, in Combinatorics and Finite Fields, De Gruyter, 2019, pp. 135–172.

[56] M. Moisio, *On the number of rational points on some families of Fermat curves over finite fields*, Finite Fields and Their Applications, 13 (2007), pp. 546–562.

[57] C. Moreno, *Algebraic Curves over Finite Fields*, no. 97, Cambridge University Press, 1993.

[58] K. Morrison, *Equivalence for rank-metric and matrix codes and automorphism groups of Gabidulin codes*, IEEE Transactions on Information Theory, 60 (2014), pp. 7035–7046.

[59] G. L. Mullen and D. Panario, *Handbook of Finite Fields*, Chapman and Hall/CRC, 2013.

[60] K. Nelson, J. Solymosi, F. Tom, and C. Wong, *The number of rational points of hyperelliptic curves over subsets of finite fields*, Involve, a Journal of Mathematics, 12 (2019), pp. 755–765.

[61] R. W. Odoni, *The Galois theory of iterates and composites of polynomials*, Proceedings of the London Mathematical Society, 3 (1985), pp. 385–414.

[62] J. A. Oliveira, *Equivalence, group of automorphism and invariants of a family of rank metric codes arising from linearized polynomials*, Linear Algebra and its Applications, 630 (2021), pp. 274–292.

[63] ——, *On diagonal equations over finite fields*, Finite Fields and Their Applications, 76 (2021), p. 101927.

[64] ——, *On maximal and minimal hypersurfaces of Fermat type*, arXiv preprint arXiv:2110.07452, (2021).

[65] J. A. Oliveira, *Rational points on cubic, quartic and sextic curves over finite fields*, Journal of Number Theory, 224 (2021), pp. 191–216.

[66] J. A. Oliveira, D. Oliveira, and L. Reis, *On iterations of rational functions over perfect fields*, arXiv preprint arXiv:2008.02619, (2020).

[67] R. Oliver, *Gauss sums over finite fields and roots of unity*, Proceedings of the American Mathematical Society, 139 (2011), pp. 1273–1276.

[68] K. Otal and F. Özbudak, *Additive rank metric codes*, IEEE Transactions on Information Theory, 63 (2016), pp. 164–168.

[69] D. Panario and L. Reis, *The functional graph of linear maps over finite fields and applications*, Designs, Codes and Cryptography, 87 (2019), pp. 437–453.

[70] D. Panario, L. Reis, and Q. Wang, *Construction of irreducible polynomials through rational transformations*, Journal of Pure and Applied Algebra, 224 (2020), p. 106241.

[71] A. Peinado, F. Montoya, J. Munoz, and A. Yuste, *Maximal periods of $x^2 + c$ in $\mathbb{F}_q$*, in International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, Springer, 2001, pp. 219–228.

[72] S. Qi and W. Daqing, *On the solvability of the equation and its application*, Proceedings of the American Mathematical Society, (1987), pp. 220–224.

[73] C. Qureshi and D. Panario, *Rédei actions on finite fields and multiplication map in cyclic group*, SIAM Journal on Discrete Mathematics, 29 (2015), pp. 1486–1503.

[74] ——, *The graph structure of chebyshev polynomials over finite fields and applications*, Designs, Codes and Cryptography, 87 (2019), pp. 393–416.

[75] C. Qureshi and L. Reis, *Dynamics of the a-map over residually finite dedekind domains and applications*, Journal of Number Theory, 204 (2019), pp. 134–154.

[76] ——, *On the functional graph of the power map over finite groups*, arXiv preprint arXiv:2107.00584, (2021).

[77] A. Ravagnani, *Rank-metric codes and their duality theory*, Designs, Codes and Cryptography, 80 (2016), pp. 197–216.

[78] L. Reis, *Counting solutions of special linear equations over finite fields*, Finite Fields and Their Applications, 68 (2020), p. 101759.

[79] ——, *On the factorization of iterated polynomials*, Revista Matemática Iberoamericana, 36 (2020), pp. 1957–1978.

[80] T. D. Rogers, *The graph of the square mapping on the prime fields*, Discrete Mathematics, 148 (1996), pp. 317–324.

[81] A. Rojas-León, *On the number of rational points on curves over finite fields with many automorphisms*, Finite Fields and Their Applications, 19 (2013), pp. 1–15.

[82] R. Schoof, *Counting points on elliptic curves over finite fields*, Journal de Théorie des Nombres de Bordeaux, 7 (1995), pp. 219–254.

[83] I. R. Shafarevich and M. Reid, *Basic algebraic geometry*, vol. 2, Springer, 1994.

[84] J. Sheekey, *A new family of linear maximum rank distance codes*, Advances in Mathematics of Communications, (2015).

[85] ——, *MRD codes: constructions and connections*, Combinatorics and Finite Fields: Difference Sets, Polynomials, Pseudorandomness and Applications, 23 (2019).

[86] ——, *New semifields and new MRD codes from skew polynomial rings*, Journal of the London Mathematical Society, 101 (2020), pp. 432–456.

[87] T. Shioda and T. Katsura, *On Fermat varieties*, Tohoku Mathematical Journal, Second Series, 31 (1979), pp. 97–115.

[88] J. H. Silverman, *The Arithmetic of Elliptic Curves*, vol. 106, Springer Science & Business Media, 2009.

[89] C. Small, *Diagonal equations over large finite fields*, Canadian Journal of Mathematics, 36 (1984), pp. 249–262.

[90] S. A. Stepanov, *Codes on algebraic curves*, Springer Science & Business Media, 2012.

[91] H. Stichtenoth, *Algebraic function fields and codes*, vol. 254, Springer Science & Business Media, 2009.

[92] H. Stichtenoth and A. Topuzoğlu, *Factorization of a class of polynomials over finite fields*, Finite Fields and Their Applications, 18 (2012), pp. 108–122.

[93] Q. Sun and D. Q. Wan, *On the solvability of the equation* $\sum x_i/d_i \equiv 0 \pmod 1$ *and its application*, Proceedings of the American Mathematical Society, 100 (1987), pp. 220–224.

[94] Q. Sun and P.-Z. Yuan, *On the number of solutions of diagonal equations over a finite field*, Finite Fields and Their Applications, 2 (1996), pp. 35–41.

[95] Z.-H. Sun, *Congruences concerning Legendre polynomials II*, Journal of Number Theory, 133 (2013), pp. 1950–1976.

[96] S. Tafazolian, *A characterization of maximal and minimal Fermat curves*, Finite Fields and Their Applications, 16 (2010), pp. 1–3.

[97] S. Tafazolian and F. Torres, *On maximal curves of Fermat type*, Advances in Geometry, 13 (2013), pp. 613–617.

[98] ——, *On the curve $y^n = x^m + x$ over finite fields*, Journal of Number Theory, 145 (2014), pp. 51–66.

[99] R. Trombetti and Y. Zhou, *A new family of MRD codes in $\mathbb{F}_{q^{2n\times 2n}}$ with right and middle nuclei $\mathbb{F}_{q^n}$*, IEEE Transactions on Information Theory, 65 (2018), pp. 1054–1062.

[100] S. Ugolini, *Functional graphs of rational maps induced by endomorphisms of ordinary elliptic curves over finite fields*, Periodica Mathematica Hungarica, 77 (2018), pp. 237–260.

[101] M. Ulas, *Rational points on certain hyperelliptic curves over finite fields*, Bulletin of the Polish Academy of Sciences Mathematics, 55 (2007), pp. 97–104.

[102] D. Wan, *Partial zeta functions of algebraic varieties over finite fields*, Finite Fields and Their Applications, 7 (2001), pp. 238–251.

[103] ——, *Rationality of partial zeta functions*, Indagationes Mathematicae, 14 (2003), pp. 285–292.

[104] Q. Wang, *Polynomials over finite fields: an index approach*, in Combinatorics and Finite Fields, De Gruyter, 2019, pp. 319–348.

[105] A. Weil et al., *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc, 55 (1949), pp. 497–508.

[106] M. J. Wiener and R. J. Zuccherato, *Faster attacks on elliptic curve cryptosystems*, in International workshop on selected areas in cryptography, Springer, 1998, pp. 190–200.

[107] K. S. Williams, *Evaluation of character sums connected with elliptic curves*, Proceedings of the American Mathematical Society, 73 (1979), pp. 291–299.

[108] J. Wolfmann, *The number of points on certain algebraic curves over finite fields*, Communications in Algebra, 17 (1989), pp. 2055–2060.

[109] ——, *The number of solutions of certain diagonal equations over finite fields*, Journal of Number Theory, 42 (1992), pp. 247–257.

[110] H. Zhou and Y. Sun, *Counting points on diagonal equations over Galois rings $GR(p^2, p^{2r})$*, Finite Fields and Their Applications, 56 (2019), pp. 266–284.