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

Daniela Alves de Oliveira

Topics in finite fields: Artin-Schreier's curves, superelliptic curves and irreducible polynomials

Belo Horizonte
2023

Daniela Alves de Oliveira

Topics in finite fields: Artin-Schreier's curves, superelliptic curves and irreducible polynomials

Tese de doutorado apresentada como parte dos requisitos para obtenção do título de Doutora pelo Departamento de Matemática do Instituto de Ciências Exatas da Universidade Federal de Minas Gerais.

Orientador : Fabio Enrique Brochero Martínez

Belo Horizonte
Março de 2023

Oliveira, Daniela Alves de.

O48r Topics in finite fields[recurso eletrônico]: Artin-Schreier's curves, superelliptic curves and irreducible polynomials / Daniela Alves de Oliveira –2023.
1 recurso online (103 f. il, color.) : pdf.

Orientador: Fabio Enrique Brochero Martínez.

Tese (doutorado) - Universidade Federal de Minas Gerais, Instituto de Ciências Exatas, Departamento de Matemática.
Referências: f.99-103

1. Matemática – Teses. 2. Corpos finitos (Algebra) – Teses. 3. Formas Quadráticas – Teses. 4. Somas de Gauss – 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 Universidade Federal de Minas Gerais - ICEx

UNIVERSIDADE FEDERAL DE MINAS GERAIS
INSTITUTO DE CIÊNCIAS EXATAS
COLEGIADO DO CURSO DE PÓS-GRADUAÇÃO EM MATEMÁTICA

FOLHA DE APROVAÇÃO

Topics in finite fields: Artin-Schreier's curves, superelliptic curves and irreducible polynomials

DANIELA ALVES DE OLIVEIRA

Tese defendida e aprovada pela banca examinadora constituída por:

Prof. Fabio Enrique Brochero Martínez

UFMG

Prof. Daniel Nelson Panario Rodriguez

Carleton University

Prof. Herivelto Martins Borges Filho

USP

Prof. Lucas da Silva Reis

UFMG

Profa. Luciane Quoos Conte

UFRJ

Prof. Ricardo Alberto Podestá

Universidad Nacional de Cordoba - Argentina

Belo Horizonte, 10 de março de 2023.

Documento assinado eletronicamente por **Ricardo Alberto Podesta**, **Usuário Externo**, em 13/03/2023, às 17:13, 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 **Daniel Nelson Panario**, **Usuário Externo**, em 13/03/2023, às 17:28, 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 **Fabio Enrique Brochero Martinez**, **Professor do Magistério Superior**, em 13/03/2023, às 17:44, 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 **Luciane Quoos Conte**, **Usuário Externo**, em 13/03/2023, às 18:10, 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 **Herivelto Marins Borges Filho**, **Usuário Externo**, em 13/03/2023, às 20:28, 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 **Lucas da Silva Reis**, **Professor do Magistério Superior**, em 14/03/2023, às 10:23, conforme horário oficial de Brasília, com fundamento no art. 5° do Decreto n° 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 **2142486** e o código CRC **97C6DDF9**.

AGRADECIMENTOS

O percurso de um doutorado é longo e cheio de altos e baixos, de momentos de alegrias e também de desespero. O doutorado é uma constante luta pelo desconhecido, é aprender a ser resiliente com os erros, a descobrir sempre um novo jeito de pensar ou começar novamente do zero algum problema. É aprender que nenhum esforço é em vão e que os erros também são acompanhados de aprendizados. E principalmente, o doutorado é uma fase em que fazemos laços que serão lembrados por toda vida, pois quando eu olho para esses anos, fico imensamente grata por todas as pessoas que estiveram ao meu lado e tornaram essa longa jornada possível e mais leve.

Primeiramente, agradeço a minha família, por todo apoio e suporte que foi me dado ao longo desses anos. Por acreditarem em mim e estarem presente quando precisei. Aos meus pais, Maria e Geraldo, aos meus irmãos, Sabrina, Tiago e Diego e a minha avós Maria e Divina, o meu eterno obrigada.

Agradeço imensamente ao meu orientador Fabio Brochero, que muito mais do que um orientador, se tornou um grande amigo ao longo desses anos. Obrigada por me ensinar tanto, seja sobre matemática ou sobre a vida. Você acreditou em mim, mesmo nos momentos que eu mesma duvidei. Você acolheu meu desespero e minhas crises de choro, e nesses momentos, sempre me lembrou que nada está perdido e sempre temos a chance de começar novamente. Eu sempre serei eternamente grata por todos aprendizados e levarei comigo uma admiração enorme pelo profissional que você é e pela pessoa que me ensinou tanto nos últimos anos. Obrigada por tanto! Espero que possamos correr até os 100 anos.

Agradeço com o maior carinho ao meu amigo(e irmão) e também membro da banca: Lucas Reis. Apesar de sermos pessoas completamente opostas em certo sentido, você sempre me apoiou e me lembrou o quanto eu podia acreditar no processo. Você é um amigo para toda vida que surgiu pela matemática(OBMEP), e não existem palavras que descrevam a sensação de ter uma amizade assim. Muito obrigada por tudo!

A meu mais sincero obrigada ao professor Marcelo Hilário, que além de ter sido meu professor se tornou um grande amigo. Obrigada por todo apoio, pelas palavras de incentivo e por todos cafés. Pelas inúmeras conversas sobre corrida e por me incetivar tanto na matemática como na corrida. Levarei comigo sempre a admiração pelo excelente profissional que você é e também uma eterna gratidão por toda nossa amizade.

O meu eterno obrigada ao professor Michel Spira, meu primeiro orientador de IC e que me indicou procurar o Fabio para ser meu orientador de mestrado. Foi onde tudo começou e você me ensinou tanto. Obrigada pela revisão do artigo e por estar sempre disposto.

O meu muitíssimo obrigada a todos os professores do Departamento de Matemática da UFMG, que cruzaram o meu caminho nesses anos. Em especial, aos meus companheiros de café: Fabio, Marcelo, LG, Viktor, Gastão, Emerson, Carballo, Paulo Cupertino, Raphael Drumond, Ana, Andrea, Bernardo, Renato, Gilcione. Acreditem, vocês tornaram minha caminhada mais leve e me ensinaram tanto.

Agradeço imensamente aos professores da minha banca: Herivelto Borges, Daniel Panario, Luciane Quoos, Ricardo Podestá e Lucas, pelo tempo dedicado a este trabalho e por suas valiosas sugestões.

O meu mais carinhoso obrigada a família emprestada que ganhei: Família Brochero. Fabio, Lucas, Sávio, José, Lays, Lilian(in memoriam), Linda(in memoriam), Arthur, Hugo, José 2. Foram tantos risos, piadas e matemática envolvida. Essa relação de amizade e companherismo, me ganharam por completo. Obrigada por tudo!

Agradeço de coração a todos os meus amigos da Matemática. Esses anos, de aprendizados e amadurecimento, foram mais felizes porque tive vocês ao meu lado. Wesley, obrigada por ser quem você é, por estar sempre ao meu lado e pelo carinho de sempre. Rodrigo, obrigada por ser aquela pessoa super solicita e sempre me animar. Átila obrigada por me transmitir paz e calmaria sempre que eu precisei. Amanda, obrigada pelo carinho, simpatia e as boas risadas ao longo desses anos. Alberto, obrigada por me fazer rir, principalmente nos momentos que mais precisei, sua leveza me fez muito bem. José, obrigada por ser meu companheiro de estudos e reclamações, nossa jornada de irmãos Brochero foi essencial na minha caminhada. Para não me demorar muito: Geovana, Raul, Filiphe, Mattheus, João, Leo Saud, Ian, Maralice, Helen, André, Carlos, Célio, Gabi, Gabriel, Genilson, Isadora, José 2, Arthur, Patrícia, Marcela, Janaíne, Luiz, o meu muito obrigada por todo o tempo de convivência e pela amizade. Vocês foram essenciais em minha trajetória. Levarei vocês para sempre comigo. (Me desculpem se esqueci alguém, mas saibam:amo todos vocês).

Agradeço de coração as meninas que morei nos últimos anos: Dri, Ana e Letícia, por tornarem meus dias mais tranquilos. Em especial a Dri, que tornou o último ano mais leve e se tornou muito especial para mim.

Agradeço com muito carinho a Andréa e Kelli, que sempre foram super amigas e bem dispostas a resolver tudo. Vocês são especiais meninas.

Agradeço ao suporte financeiro oferecido pela CAPES, pois foi ele que tornou essa jornada possível.

"Do your best, in the condition you have, while you don't have better conditions, to do even better!"

Mário Sérgio Cortella

Resumo

Nesta tese estudamos alguns problemas da teoria de corpos finitos que são interessantes por suas aplicações em teoria de códigos, criptografia, comunicações e áreas relacionadas. Nosso primeiro problema é determinar o número de pontos racionais de uma família de curvas do tipo Artin-Schreier e de uma hipersuperfície de Artin-Schreier, assim como determinar condições para essas curvas/hipersuperfícies serem maximais ou minimais com respeito à cota de Hasse-Weil. Na sequência estudamos uma classe de curvas superelípticas e, sob algumas condições, descrevemos o número de pontos racionais dessas curvas. O último tópico deste trabalho é sobre polinômios irredutíveis, onde determinamos condições sobre n e q para os quais os fatores irredutíveis sobre $\mathbb{F}_q$ do binômio $x^n - 1$ são binômios e trinômios.

Palavras Chaves: Corpos Finitos, Formas Quadráticas, Curvas de Artin-Schreier, Hipersuperfícies de Artin-Schreier, Curvas Super Elípticas, Cota de Hasse-Weil, Soma de Gauss, Matrizes Circulantes, Polinômios Irredutíveis.

Abstract

In this thesis we study some problems in the finite field theory that interesting for their applications in coding theory, cryptography, communications and related areas. Our first problem is to determine the number of rational points of a family of Artin-Schreier curves and of an Artin-Schreier hypersurface, as well as to determine conditions for these curves/hypersurface to be maximal or minimal with respect to the Hasse-Weil bound. In the sequence, we study a class of superelliptic curves and, under some conditions, we describe the number of rational points of these curves. The last topic of this work is about irreducible polynomials, where we determine conditions on n and q for which the irreducible factors over $\mathbb{F}_q$ of the binomial $x^n - 1$ are binomials and trinomials.

Keywords: Finite Fields, Quadratic Forms, Artin-Schreier Curves, Artin-Schreier Hypersurfaces, Superelliptic Curves, Hasse-Weil's Bound, Gauss Sums, Circulant Matrices, Irreducible Polynomials.

List of Notations

- $\mathbb{F}_p$ the finite field with p (prime) elements;
- $\mathbb{F}_q$ the finite field with q elements;
- $\mathbb{F}_q^*$ the set of non-null elements of $\mathbb{F}_q$;
- ψ the canonical additive character of $\mathbb{F}_{q^n}$;
- $\tilde{\psi}$ the canonical additive character of $\mathbb{F}_q$;
- χ_m a multiplicative caracter of order m of $\mathbb{F}_q$;
- $G(\psi,\chi)$ the Gauss sum of ψ and a multiplicative character χ;
- $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ the trace function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$;
- $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ the norm function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$;
- $\left(\frac{u}{v}\right)$ the Legendre symbol of the prime numbers u and v;
- $v_p(n)$ the p-adic valuation of the integer n;
- $\Phi_n(x)$ the n-th cyclotomic polynomial over $\mathbb{F}_q$;
- $\mathscr{P}$ the $n \times n$ permutation matrix $\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \cdots & \cdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}$;
- $\tau = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4; \\ i & \text{if } p \equiv 3 \pmod 4; \end{cases}$
- $\varepsilon_\alpha = \begin{cases} q-1 & \text{if } \alpha = 0; \\ -1 & \text{if } \alpha \in \mathbb{F}_q^*; \end{cases}$
- $\varepsilon'_\alpha = \begin{cases} 0 & \text{if } \alpha = 0; \\ -1 & \text{if } \alpha \in \mathbb{F}_q^*; \end{cases}$

- $\theta_m(a,\epsilon) = \begin{cases} m-1 & \text{if } \chi_m(a) = \epsilon; \\ -1 & \text{otherwise.} \end{cases}$
- $\mathscr{C}_i$ the curve $y^q - y = x(x^{q^i} - x) - \lambda$;
- $\mathscr{H}_r$ the hypersurface $y^q - y = \sum_{j=1}^{r} a_j(x_j^{q^{i_j}+1} - x_j^2) - \lambda$;
- $N_n(\mathscr{C})$ the number of $\mathbb{F}_{q^n}$-rational points of the curve/surface $\mathscr{C}$.

Sumário

Página

Introduction

In this thesis, we approach some problems in the theory of finite fields. Our objects of study include the number of $\mathbb{F}_{q^n}$-rational points of Artin-Schreier curves and hypersurfaces, superelliptic curves and irreducible polynomials. In general, we discuss the number of rational points of a class of Artin-Schreier curves, its generalization for Artin-Schreier hypersurfaces and a class of superelliptic curves. We also discuss about when these curves attain the Hasse-Weil bound.

Moreover, we discuss the existence of positive integers n for which the binomial $x^n - 1$ splits over $\mathbb{F}_q$ only as irreducible binomials and trinomials.

Among other matters, this thesis compiles the original work contained in the following papers:

- [8] F. E. Brochero Martínez, J. A. Oliveira and D. Oliveira. The number of rational points of a class of superelliptic curves,

  ArXiv preprint: https://arxiv.org/abs/2209.06658, (2022).

- [9] F. E. Brochero Martínez and D. Oliveira, Artin-Schreier curves given by $\mathbb{F}_q$-linearized polynomials.

  ArXiv preprint: https://arxiv.org/abs/2012.01534, (2022).

- [36] D. Oliveira. On the number of rational points of hypersurfaces of Artin-Schreier.

  ArXiv preprint: `https://arxiv.org/abs/2211.11371`, (2022).

- [37] D. Oliveira and L. Reis. On polynomials $x^n - 1$ over binary fields whose irreducible factors are binomials and trinomials. *Finite Fields and Their Applications*, vol. **71**. p. 101837, (2021).

The content of the thesis is presented in four chapters. Chapter 1 provides background results in theory of finite fields that are used throughout this text. The remaining three chapters are divided as follows.

- Chapter 2: In this chapter we associate circulant matrices and quadratic forms to the Artin-Schreier curve $y^q - y = x \cdot F(x) - \lambda$, where $F(x)$ is a $\mathbb{F}_q$-linearized polynomial and $\lambda \in \mathbb{F}_{q^n}$. Our results provide a characterization of the number of affine rational points of this curve in the extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$. In the particular case $F(x) = x^{q^i} - x$, we have the curves

$$\mathscr{C}_i : y^q - y = x(x^{q^i} - x) - \lambda$$

and we give a complete description of the number of affine $\mathbb{F}_{q^n}$-rational points of $\mathscr{C}_i$ in terms of Legendre symbols and quadratic characters under the condition $\gcd(n,p) = 1$. We also determine the number of $\mathbb{F}_{q^n}$-affine rational points and when the curve $\mathscr{C}_i$ is maximal or minimal with respect to the Hasse-Weil bound (since this curve has only one point at the infinity), using permutation matrices and quadratic forms, including the case $\gcd(n,p) = p$ for $\lambda \in \mathbb{F}_{q^n}$. Moreover, we determine the number of affine rational points of Artin-Schreier hypersurfaces of the type

$$\mathscr{H}_r : y^q - y = \sum_{j=1}^{r} a_j(x_j^{q^{i_j}+1} - x_j^2) - \lambda,$$

with $a_j \in \mathbb{F}_q^*$ and some integers i_j, since this hypersurface has only one point at the infinity. We also give conditions when the curves $\mathscr{C}_i$ and the surface $\mathscr{H}_r$ in order to them to be maximal or minimal with respect the Hasse-Weil bound.

- Chapter 3: In this chapter, we study the number of $\mathbb{F}_{q^n}$-rational points on the affine curve $\mathscr{X}_{d,a,b}$ given by the equation

  $$\mathscr{X}_{d,a,b} : y^d = ax\mathrm{Tr}(x) + b,$$

  where Tr denotes the trace function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ and d is a positive integer. In particular, we present bounds for the number of $\mathbb{F}_{q^n}$-rational points and, for the cases when d satisfies a suitable condition, explicit formulas for the number of $\mathbb{F}_{q^n}$-rational points are obtained. In particular, a complete characterization is given for the case $d = 2$. As a consequence of our results, we compute the number of elements α in $\mathbb{F}_{q^n}$ such that α and $\mathrm{Tr}(\alpha)$ are quadratic residues in $\mathbb{F}_{q^n}$.

- Chapter 4: In this chapter, we assume that $\mathbb{F}_q$ is a finite field with q elements, where q is a power of 2. We study the positive integers n for which the irreducible factors of the polynomial $x^n - 1$ over $\mathbb{F}_q$ are all binomials and trinomials. In particular, we completely describe these integers for $q = 2, 4$.

Chapter 1

Preliminary results

In this chapter we present some classical and important results on finite fields, number theory and characters sums that are futher used.The most of this results can be found in [30].

1.1 Finite fields

For a prime p, the residue class ring $\mathbb{Z}/(p)$ forms a finite field with p elements. We denote this field by $\mathbb{F}_p$. The fields $\mathbb{F}_q$ play an important role in general field theory, since every field of characteristic p must contain a subfield isomorphic to $\mathbb{F}_p$. This result together with the fact that every finite field has prime characteristic is fundamental for the classification of finite fields. In this section we present, without proof the main results that will be used in this thesis. The proofs of these results can be found in [30]. Firstly, we present some important results about the characterization and structure of finite fields.

Theorem 1.1. *Let $\mathbb{F}$ be a finite field. Then $\mathbb{F}$ has p^n elements, where the prime p is the characteristic of $\mathbb{F}$ and n is the degree of $\mathbb{F}$ as an extension of its prime subfield.*

We denote any finite field with $q = p^n$ elements by $\mathbb{F}_q$.

Lemma 1.2. *Let $\mathbb{F}_q$ be a finite field with q elements, where $q = p^n$ for some prime p. Then,* *every $a \in \mathbb{F}_q$ satisfies $a^q = a$. Besides that, the polynomial $x^q - x \in \mathbb{F}_q[x]$ splits in $\mathbb{F}_q[x]$ as*

$$x^q - x = \prod_{a \in \mathbb{F}_q} (x - a)$$

and $\mathbb{F}_q$ is a splitting field of $x^q - x$ over $\mathbb{F}_p$.

For a finite field $\mathbb{F}_q$ we denote by $\mathbb{F}_q^*$ the multiplicative group of nonzero elements of $\mathbb{F}_q$. The following result describes a useful property of this group.

Theorem 1.3. *For every finite field $\mathbb{F}_q$, the multiplicative group $\mathbb{F}_q^*$ is cyclic.*

Definition 1.4. *A generator of the cyclic group $\mathbb{F}_q^*$ is a* primitive element *of $\mathbb{F}_q$.*

Theorem 1.5 (Existence and Uniqueness of Finite Fields). *For every prime p and every positive integer n, there exists a finite field with p^n elements. Any finite field with $q = p^n$ elements is isomorphic to the splitting field of $x^q - x$ over $\mathbb{F}_p$.*

Theorem 1.6 (Subfield Criterion). *Let $\mathbb{F}_q$ be the finite field with $q = p^n$ elements. Then every subfield of $\mathbb{F}_q$ has order p^m, where m is a positive divisor of n. Conversely, if m is a positive divisor of n, then there is exactly one subfield of $\mathbb{F}_q$ with p^m elements.*

1.1.1 Trace and Norm

In this section we introduce an important mapping from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$, where m is a positive integer and q is a prime power, which we will recall that is linear and very useful for the proofs of some results in chapter 2.

Definition 1.7. *Let $\mathbb{F}_{q^n}$ be an extension of the finite field $\mathbb{F}_q$. The trace map from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ is the map $\alpha \mapsto Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ where*

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}}.$$

The norm map from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ is the map $\alpha \mapsto N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ where

$$N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \alpha \cdot \alpha^q \cdots \alpha^{q^{n-1}} = \alpha^{\frac{q^n-1}{q-1}}.$$

For short we denote $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ by Tr and $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ by N, when the finite fields $\mathbb{F}_{q^n}$ and $\mathbb{F}_q$ are fixed.

Theorem 1.8. *Let $\mathbb{F}_{q^n}$ be an extension of the finite field $\mathbb{F}_q$. Then the trace and norm functions satisfy the following properties:*

(i) For all $\alpha, \beta \in \mathbb{F}_{q^n}$ we have that

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha+\beta) = Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) + Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta).$$

$$N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha\cdot\beta) = N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)\cdot N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta).$$

(ii) For all $c \in \mathbb{F}_q$ and $\alpha \in \mathbb{F}_{q^n}$ we have that $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(c\alpha) = cTr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$.

(iii) The map $\alpha \mapsto Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ is a linear transformation from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$, where both $\mathbb{F}_{q^n}$ and $\mathbb{F}_q$ are viewed as vector spaces over $\mathbb{F}_q$. Moreover, $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ maps $\mathbb{F}_{q^n}$ onto $\mathbb{F}_q$ and $\mathbb{F}^*_{q^n}$ onto $\mathbb{F}^*_q$.

(iv) For all $\alpha \in \mathbb{F}_q$ we have that $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = n\alpha$ and $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \alpha^n$.

(v) For all $\alpha \in \mathbb{F}_{q^n}$ we have that $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha^q) = Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ and $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha^q) = N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$.

Theorem 1.9 (Hilbert's Theorem 90)**.** *Let $\mathbb{F}_{q^n}$ be a finite extension of $\mathbb{F}_q$. Then, for every $\alpha \in \mathbb{F}_{q^n}$ we have*

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = 0 \quad \text{if and only if} \quad \alpha = \beta^q - \beta \text{ for some } \beta \in \mathbb{F}_{q^n}.$$

Theorem 1.10 (Transitivity of Trace and Norm)**.** *Let $\mathbb{F}_{q^n}$ be a finite extension of $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$ a finite extension of $\mathbb{F}_{q^n}$. Then*

$$Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(Tr_{\mathbb{F}_{q^m}/\mathbb{F}_{q^n}}(\alpha)),$$

$$N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(N_{\mathbb{F}_{q^m}/\mathbb{F}_{q^n}}(\alpha)),$$

for all $\alpha \in \mathbb{F}_{q^m}$.

1.1.2 Normal Basis

We now define normal basis of $\mathbb{F}_q$ and give the main result for them.

Definition 1.11. *A basis $\mathscr{B}$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is called a* normal basis *if there exists $\alpha \in \mathbb{F}_{q^n}$ such that*

$$\mathscr{B} = \{\alpha, \alpha^q, \dots, \alpha^{q^{n-1}}\}.$$

The elements of this basis are called normal elements *of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.*

Theorem 1.12 (Normal Basis Theorem)**.** *For any finite field $\mathbb{F}_q$ and any finite extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$, there exists a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.*

1.2 Cyclotomic Polynomials

In this section we describe some properties of the cyclotomic polynomials over finite fields. These polynomials are associated with the splitting field of $x^n - 1$.

Definition 1.13. *Let n be a positive integer and $\mathbb{F}_q$ a field of characteristic p. The splitting field of $x^n - 1$ over $\mathbb{F}_q$ is called the* n-th cyclotomic field *over $\mathbb{F}_q$ and is denoted by $\mathbb{F}_q^{(n)}$. The roots of $x^n - 1$ in $\mathbb{F}_q^{(n)}$ are called the* n-th roots of unity *over $\mathbb{F}_q$. If* $\gcd(n,p) = 1$*, a generator of the cyclic group of n-th roots is called a* primitive n-th root of unity *over $\mathbb{F}_q$.*

The n-th cyclotomic field will be useful in Chapter 4. The following result is well known and can be found in Chapter 2(section 4) of [30].

Theorem 1.14. *Let n be a positive integer and $\mathbb{F}_q$ a finite field with $q = p^s$ elements, where p is a prime. Then*

(i) If p does not divide n, the n-th roots of unity form a cyclic group of order n with respect to the multiplication in $\mathbb{F}_q^{(n)}$.

(ii) If p divides n, we write $n = mp^e$ with m and e being positive integers such that $\gcd(m,p) = 1$*. Then $\mathbb{F}_q^{(n)} = \mathbb{F}_q^{(m)}$ and the roots of $x^n - 1$ in $\mathbb{F}_q^{(n)}$ are the m-th roots of unity, each one with multiplicity p^e.*

We know that if $\gcd(n,p) = 1$ then there are exactly $\varphi(n)$ primitive n-th roots of unity over $\mathbb{F}_q^{(n)}$. If ζ is one of them, them all the primitive n-th roots of unity over $\mathbb{F}_q^{(n)}$ are given by ζ^i, where $1 \le i \le n$ and $\gcd(i,n) = 1$. The polynomial whose roots are precisely the primitive n-th roots of unity over $\mathbb{F}_q^{(n)}$ is of great interest.

Definition 1.15. *Let $\mathbb{F}_q$ be a field of characteristic p, n a positive integer that is not divisible by p, and ζ a primitive n-th root of unity over $\mathbb{F}_q$. Then the polynomial*

$$\Phi_n(x) = \prod_{\substack{s=1 \\ \gcd(s,n)=1}}^{n} (x - \zeta^s)$$

is called the n-th cyclotomic polynomial over $\mathbb{F}_q$.

The polynomial $\Phi_n(x)$ does not depend on the choice of ζ. The degree of $\Phi_n(x)$ is $\varphi(n)$, where $\varphi(n)$ is the Euler totient function, and its coefficients belong to the n-th cyclotomic field over $\mathbb{F}_q$. In fact, they are in the prime subfield of $\mathbb{F}_q$, as we show in the following theorem.

Theorem 1.16. *Let $\mathbb{F}_q$ be a finite field of characteristic p, n a positive integer not divisible by p and d the least positive integer such that $q^d \equiv 1 \pmod{n}$. Then*

(i) $x^n - 1 = \prod_{l|n} \Phi_l(x)$;

(ii) the coefficients of $\Phi_n(x)$ belong to the prime subfield $\mathbb{F}_p$ of $\mathbb{F}_q$;

(iii) $\Phi_n(x)$ splits into $\frac{\varphi(n)}{d}$ distinct monic irreducible polynomials in $\mathbb{F}_q[x]$ all of the same degree d. Moreover, $\mathbb{F}_q^{(n)}$ is the splitting field of any such irreducible factor over $\mathbb{F}_q$ and $[\mathbb{F}_q^{(n)} : \mathbb{F}_q] = d$.

The following results provide some classical results about cyclotomic polynomials that we will use in the proofs of some results in Chapter 4.

Corollary 1.17. *If p is a prime, then*

$$\Phi_p(x) = x^{p-1} + \cdots + x + 1.$$

Lemma 1.18. *([30], Exercise 2.57) Let m, t be positive integers and p a prime such that $q = p^s$. Then the following equality holds in $\mathbb{F}_q[x]$:*

$$\Phi_{mp^t}(x) = \Phi_{mp}(x^{p^{t-1}}).$$

1.3 Characters sums

Characters sums will be useful for us in Chapters 2 and 3. To this end, we recall the following definitions and classical results.

Definition 1.19. *1) Set $\zeta_p = e^{\frac{2\pi i}{p}}$ a $p-$th complex root of unity. An* additive character *ψ on $\mathbb{F}_q$ is a map from the group $\mathbb{F}_q$ into the group of complex roots of unity such that*

$$\psi(\alpha + \beta) = \psi(\alpha)\psi(\beta)$$

for all $\alpha, \beta \in \mathbb{F}_q$. The canonical additive character *ψ_1 of $\mathbb{F}_q$ is given by*

$$\psi_1(\alpha) = e^{2\pi i Tr_{\mathbb{F}_q/\mathbb{F}_p}(\alpha)/p},$$

where $Tr_{\mathbb{F}_q/\mathbb{F}_p}$ denotes the absolute trace of $\mathbb{F}_q$.

2) *A* multiplicative character χ *on* $\mathbb{F}_q^*$ *is a map from the cyclic group* $\mathbb{F}_q^*$ *into the group of complex roots of unity such that*

$$\chi(\alpha\beta) = \chi(\alpha)\chi(\beta)$$

for all $\alpha, \beta \in \mathbb{F}_q^*$ *. We extend* χ *to a function on* $\mathbb{F}_q$ *by setting* $\chi(0) = 1$*. The trivial character* χ_0 *satisfies* $\chi_0(\alpha) = 1$ *for every* $\alpha \in \mathbb{F}_q^*$*. The order of* χ *is the smallest positive integer n for which* $\chi^n = \chi_0$*. When q is odd, the unique character* χ *of order* 2 *is the quadratic character.*

The following theorem gives us the description of all additive and multiplicative characters of $\mathbb{F}_q$.

Theorem 1.20. *(i) For* $b \in \mathbb{F}_q$*, the function* ψ_b *defined by*

$$\psi_b(c) = \psi_1(bc)$$

for all $c \in \mathbb{F}_q$*, is an additive character of* $\mathbb{F}_q$ *and every additive character of* $\mathbb{F}_q$ *is obtained in this way.*

(ii) Let g be a fixed primitive element of $\mathbb{F}_q^*$*. For each* $j = 0, 1, \ldots, q-2$*, the function* χ_j *given by*

$$\chi_j(g^k) = e^{2\pi i jk/(q-1)} \quad \text{for } k = 0, 1, \ldots, q-2,$$

defines a multiplicative character of $\mathbb{F}_q$ *and every multiplicative character of* $\mathbb{F}_q$ *is obtained in this way.*

The following lemmas describe classical properties of characters.

Lemma 1.21 ([30, Theorem 5.4])**.** *Let* χ *be a multiplicative character of* $\mathbb{F}_{q^n}$*. Then*

$$\sum_{c \in \mathbb{F}_q} \chi(c) = \begin{cases} 0, & \textit{if } \chi \textit{ is nontrivial;} \\ q, & \textit{if } \chi \textit{ is trivial.} \end{cases}$$

Lemma 1.22. *([30, Schur's orthogonality, Theorem 5.4]) For* $u \in \mathbb{F}_q$ *and* ψ *a non-trivial character of* $\mathbb{F}_q$*, we have that*

$$\frac{1}{q} \sum_{c \in \mathbb{F}_q} \psi(uc) = \begin{cases} 0, & \textit{if } u \neq 0; \\ 1, & \textit{if } u = 0. \end{cases}$$

Lemma 1.23 ([30, Equation 5.4, p. 189])**.** *Let d be a divisor of $q-1$. If $c \in \mathbb{F}_q$, then*

$$\sum_{j=0}^{d-1} \chi_d^j(c) = \begin{cases} 1, & \textit{if } c = 0; \\ d, & \textit{if } c \textit{ is a } d\textit{-power in } \mathbb{F}_q^*; \\ 0, & \textit{otherwise.} \end{cases}$$

Definition 1.24. *Let ψ be an additive character of $\mathbb{F}_q$ and χ be a multiplicative character of $\mathbb{F}_q^*$. The Gauss sum of ψ and χ over $\mathbb{F}_q$ is*

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

Lemma 1.25. *([30, Theorems 5.11 and 5.12]) Let χ_0 denote the trivial multiplicative character of $\mathbb{F}_q^*$ and ψ be the canonical additive character of $\mathbb{F}_q$. If $\chi \neq \chi_0$ is a multiplicative character of $\mathbb{F}_q^*$, we have that*

(i) $G(\psi,\chi_0) = -1$;

(ii) $|G(\psi,\chi)| = \sqrt{q}$;

(iii) $G(\psi,\chi)G(\psi,\overline{\chi}) = \chi(-1)q$.

A Gauss sum $G(\psi,\chi)$ is *pure* if $G(\psi,\chi)^t \in \mathbb{R}$ for some positive integer t. The following result gives necessary and sufficient conditions for some Gauss sums to be simultaneously pure.

Theorem 1.26. *([17, Theorem 1]) Let ψ be the canonical additive character of $\mathbb{F}_{q^n}$ where $q = p^s$. Given a divisor $d > 2$ of $q^n - 1$ and a multiplicative character χ_d of $\mathbb{F}_{q^n}^*$ with order d, the following are equivalent:*

(i) there exists a positive integer r such that $d \mid (p^r + 1)$;

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

(iii) there exists a positive integer r such that $d \mid (p^r+1)$, $2r \mid ns$ and

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

for all $j \not\equiv 0 \pmod{d}$, where $u = \frac{p^r+1}{d}$.

The following definition is important for the explicit determination of Gauss sums.

Definition 1.27. *We set*

$$\tau = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4; \\ i & \text{if } p \equiv 3 \pmod 4). \end{cases}$$

Theorem 1.28. *([31, Theorem 5.15]) Let ψ be the canonical additive character of $\mathbb{F}_{q^n}$ and let χ_2 be the quadratic character of $\mathbb{F}_{q^n}^*$. Then*

$$G(\psi,\chi_2) = -(-1)^{sn}\tau^{sn}q^{n/2}.$$

Corollary 1.29. *Let $\mathbb{F}_{q^n}$ be a finite field where $q = p^s$. Let ψ be the canonical additive character of $\mathbb{F}_{q^n}$ and χ_2 be the quadratic character of $\mathbb{F}_{q^n}^*$. If ns is even, then*

$$G(\psi,\chi_2) = -(-1)^{ns(u+1)/2}q^{n/2},$$

where $u = \frac{p+1}{2}$.

1.4 Quadratic forms

A *quadratic form* in n indeterminates over $\mathbb{F}_q$ is a homogeneous polynomial in $\mathbb{F}_q[x_1,\ldots,x_n]$ of degree 2, or the zero polynomial. If q is odd we can write the mixed terms $a_{ij}x_ix_j(1 \le i < j \le n)$ as $\frac{1}{2}a_{ij}x_ix_j + \frac{1}{2}a_{ij}x_jx_i$ and this leads to the representation

$$f(x_1,\ldots,x_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j \quad \text{with} \quad a_{ij} = a_{ji}$$

for any quadratic form f over $\mathbb{F}_q$. This allows us to associate f with the $n \times n$ matrix A, whose entry (i,j) is a_{ij}. The matrix A is called the *coefficient matrix* of f. Let A^T denote the transpose matrix of A. Then $A^T = A$, that is, A is symmetric. If x is the column vector of indeterminates $x_1,\ldots,x_n$, we obtain that f is given by x^TAx.

Definition 1.30. *For any finite field $\mathbb{F}_q$, two quadratic forms f and g over $\mathbb{F}_q$ are called* equivalent *if f can be transformed into g by means of a nonsingular linear substitution of indeterminates. The* reduce equivalent quadratic form *of f is the quadratic form associated to the reduced non-singular matrix of A, where A is the coefficient matrix of f.*

A quadratic space is a pair $(Q,\mathbb{F}_{q^n})$ where $\mathbb{F}_{q^n}$ has dimension n over $\mathbb{F}_q$ and $Q : \mathbb{F}_{q^n} \to \mathbb{F}_q$ satisfies:

1. $Q(\alpha x) = \alpha^2 Q(x)$ for all $\alpha \in \mathbb{F}_q$ and $x \in \mathbb{F}_{q^n}$.

2. For char($\mathbb{F}_q$) = 2, we define $B_Q(x,y) = Q(x+y) - Q(x) - Q(y)$ to be a symmetric bilinear form of Q. In the case char($\mathbb{F}_q$) $\neq 2$, we define

$$B_Q(x,y) = \frac{1}{2}(Q(x+y) - Q(x) - Q(y))$$

to be the symmetric bilinear form of Q.

Quadratic form are equivalent to quadratic space, during this thesis we consider quadratic spaces. We now recall the following standard definition.

Definition 1.31. *Let $\mathbb{F}_{q^n}$ be a finite extension of $\mathbb{F}_q$, with q odd. Let $Q : \mathbb{F}_{q^n} \to \mathbb{F}_q$ denote a quadratic form and let $B_Q : \mathbb{F}_{q^n} \times \mathbb{F}_{q^n} \to \mathbb{F}_q$ be its associate symmetric bilinear form. The radical of the symmetric bilinear form B_Q is the $\mathbb{F}_q$−subspace*

$$rad(Q) = \{\alpha \in \mathbb{F}_{q^n} : B_Q(\alpha,\beta) = 0 \textit{ for all } \beta \in \mathbb{F}_{q^n}\}.$$

Moreover, Q is a non-degenerate quadratic form if $rad(Q) = \{0\}$.

Let $\mathscr{B} = \{v_1,\ldots,v_n\}$ be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. The $n \times n$ matrix $A = (a_{ij})$ defined by

$$a_{ij} = \begin{cases} Q(v_i) & \textit{if } i = j; \\ \frac{1}{2}(Q(v_i + v_j) - Q(v_i) - Q(v_j)) & \textit{if } i \neq j. \end{cases}$$

is the associated matrix of the quadratic form Q in the basis $\mathscr{B}$. In particular, the dimension of $rad(Q)$ is equal to $n - rank(A)$.

Let $Q_1 : \mathbb{F}_q^m \to \mathbb{F}_q$ and $Q_2 : \mathbb{F}_q^n \to \mathbb{F}_q$ be quadratic forms, where $m \geq n$. Let A and B be the associated matrix of Q_1 and Q_2, respectively. We say that Q_1 is equivalent to Q_2 if there exists $M \in GL_m(\mathbb{F}_q)$ such that

$$M^T A M = \left(\begin{array}{c|c} B & 0 \\ \hline 0 & 0 \end{array}\right) \in M_m(\mathbb{F}_q),$$

where $GL_m(\mathbb{F}_q)$ denotes the group of $m \times m$ invertible matrices over $\mathbb{F}_q$ and $M_m(\mathbb{F}_q)$ denotes the set of $m \times m$ matrices over $\mathbb{F}_q$. Furthermore, Q_2 is called a reduced form of Q_1 if $rad(Q_2) = \{0\}$.

The following theorem is a well known result about the number of the solutions of a special equation over finite fields, that will be important to our results in Chapters 2 and 3.

Theorem 1.32 ([30], Theorems 6.26 and 6.27)**.** *Let Q be a quadratic form over $\mathbb{F}_{q^n}$, where q is a power of an odd prime. Let B_Q be the bilinear symmetric form associated to Q, $v = \dim(Q)$ and $\tilde{Q}$ a reduced non degenerate quadratic form equivalent to Q. Set $S_\alpha := |\{x \in \mathbb{F}_{q^n} \mid Q(x) = \alpha\}|$, let Δ be the determinant of the quadratic form $\tilde{Q}$ and χ the quadratic character of $\mathbb{F}_q$. Then*

(i) If $n+v$ is even, then

$$S_\alpha = \begin{cases} q^{n-1} + Dq^{(n+v-2)/2}(q-1) & \text{if } \alpha = 0; \\ q^{n-1} - Dq^{(n+v-2)/2} & \text{if } \alpha \neq 0, \end{cases} \tag{1.1}$$

where $D = \chi((-1)^{(n-v)/2}\Delta)$.

(ii) If $n+v$ is odd, then

$$S_\alpha = \begin{cases} q^{n-1} & \text{if } \alpha = 0; \\ q^{n-1} + Dq^{(n+v-1)/2} & \text{if } \alpha \neq 0, \end{cases} \tag{1.2}$$

where $D = \chi((-1)^{(n-v-1)/2}\alpha\Delta)$.

In particular $D \in \{-1, 1\}$.

The following lemma associates quadratic forms and character sums and it will be useful in the results obtained in the next chapters. This lemma can be obtained from Theorem 1.32 by a straightforward calculation.

Lemma 1.33. *Let H be an $n \times n$ non null symmetric matrix over $\mathbb{F}_q$ and $l = rank(H)$. Then, there exists $M \in GL_n(\mathbb{F}_q)$ such that $D = MHM^T$ is a diagonal matrix, i.e., $D = diag(a_1, a_2, \dots, a_l, 0, \dots, 0)$ where $a_i \in \mathbb{F}_q^*$ for all $i = 1, \dots, l$. Let*

$$F : \mathbb{F}_q^n \to \mathbb{F}_q, \quad F(X) = XHX^T \quad (X = (x_1, \dots, x_n) \in \mathbb{F}_q^n),$$

be a quadratic form. We have that

$$\sum_{x \in \mathbb{F}_{q^n}} \psi\big(F(X)\big) = (-1)^{l(s+1)} \tau^{ls} \eta_2(\delta) q^{n-l/2},$$

where $\delta = a_1 \cdots a_l$, and ψ is the canonical additive character of $\mathbb{F}_q$.

Chapter 2

Quadratic forms and affine rational points of Artin-Schreier curves

Let $\mathbb{F}_q$ be a finite field with q elements, where q is a power of an odd prime p. In this chapter we associate circulant matrices and quadratic forms with the Artin-Schreier curve $y^q - y = x \cdot F(x) - \lambda$, where $F(x)$ is an $\mathbb{F}_q$-linearized polynomial and $\lambda \in \mathbb{F}_q$. Our results provide a characterization of the number of affine rational points of this curve in the extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$. The case $F(x) = x^{q^i} - x$ yields the curves $\mathscr{C}_i: \ y^q - y = x(x^{q^i} - x) - \lambda$, and we give a complete description of the number of their affine rational points in terms of Legendre symbols and quadratic characters. We also determine the number of affine rational points of Artin-Schreier hypersurfaces of the type $\mathscr{H}_r : y^q - y = \sum_{j=1}^{r} a_j(x_j^{q^{i_j}+1} - x_j^2) - \lambda$, with $a_j \in \mathbb{F}_q^*$ and $\lambda \in \mathbb{F}_{q^n}$. Moreover, we give conditions for the curves $\mathscr{C}_i$ and the surface $\mathscr{H}_r$ to be maximal or minimal with respect the Hasse-Weil bound.

2.1 Introduction

The number of affine rational points of algebraic curves and surfaces over finite fields has many applications in coding theory, cryptography, communications and related areas, e.g. [4, 21, 42, 46]. In this chapter we investigate the number of $\mathbb{F}_{q^n}$ affine rational points of plane curves given by

$$\mathscr{C}_g : y^q - y = g(x), \tag{2.1}$$

in extensions $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$ where $q = p^s$, p is an odd prime, $n, s \in \mathbb{N}$ and $g(x) \in \mathbb{F}_q[x]$. These curves are called Artin-Schreier curves and have been extensively studied in several contexts, e.g. [15, 16, 24, 38, 46].

For a polynomial $g(x) \in \mathbb{F}_q[x]$ and $\mathbb{F}_{q^n}$ a finite extension of $\mathbb{F}_q$ we can associate to it the map

$$\begin{array}{rccc} Q_g : & \mathbb{F}_{q^n} & \to & \mathbb{F}_q \\ & \alpha & \mapsto & \mathrm{Tr}(g(\alpha)), \end{array} \tag{2.2}$$

where $\mathrm{Tr} : \mathbb{F}_{q^n} \to \mathbb{F}_q$ denotes the trace function. Let $N_n(Q_g)$ denote the number of zeroes of Q_g in $\mathbb{F}_{q^n}$ and $N_n(\mathscr{C}_g)$ the number of affine rational points of $\mathscr{C}_g$ over $\left(\mathbb{F}_{q^n}\right)^2$. From Hilbert's Theorem 90 we have

$$N_n(\mathscr{C}_g) = qN_n(Q_g). \tag{2.3}$$

It follows that the determination of $N_n(\mathscr{C}_g)$ is equivalent to the determination of $N_n(Q_g)$. Details about this fact can be found in [2, 3, 39].

In [50], Wolfmann determined the number of rational points of the algebraic plane curve defined over $\mathbb{F}_{q^k}$ by the equation

$$y^q - y = ax^s + b$$

where $a \in \mathbb{F}_{q^k}^*$ and $b \in \mathbb{F}_{q^k}$, for k even and special integers s. In [16], Coulter determined the number of $\mathbb{F}_q$-rational points of the curve

$$y^{p^n} - y = ax^{p^\alpha + 1} + L(x),$$

where $a \in \mathbb{F}_q^*$, $t = \gcd(n, e)$ divides $d = \gcd(\alpha, e)$ and $L(x) \in \mathbb{F}_q[x]$ is an $\mathbb{F}_{p^t}$-linearized polynomial. In this chapter, we determine $N_n(\mathscr{C}_g)$ for some families of Artin-Schreier curves given by specific polynomials $g(x) \in \mathbb{F}_q[x]$.

The first aim of this chapter is to find $N_n(\mathscr{C}_g)$ when $g(x) = xF(x) - \lambda$, where $F(x)$ is a $\mathbb{F}_q$-linearized polynomial, $\lambda \in \mathbb{F}_q$ and $\gcd(n, p) = 1$. In this case, we denote $\mathscr{C}_g$ by $\mathscr{C}_{F,\lambda}$ for $F(x)$ and λ fixed. We prove that $Q_{g+\lambda}$ defines a quadratic form and use this form to find a connection between the number of affine rational points with the rank of an appropriate circulant matrix. Theorem 2.13 provides an explicit formula for $N_n(\mathscr{C}_{F,\lambda})$.

Also, assuming the hypothesis of Theorem 2.13, we study the case $F(x) = x^{q^i} - x$ when i is a positive integer, i.e., we consider the curves

$$\mathscr{C}_i : y^q - y = x^{q^i + 1} - x^2 - \lambda.$$

In Theorem 2.26 we find an expression of $N_n(\mathscr{C}_i)$ in terms of Legendre symbols and p-adic valuations.

When $i = 1$ and $\lambda = 0$ we obtain the curve $\mathscr{C}_i : y^q - y = x^{q+1} - x^2$, which is associated to the number of monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree n with the first two coefficients prescribed, i.e., the coefficients of x^{n-1} and x^{n-2}. To see this, consider the map

$$\begin{array}{rccc} T_2 : & \mathbb{F}_{q^n} & \to & \mathbb{F}_q \\ & \alpha & \mapsto & \sum\limits_{0 \le i < j \le n-1} \alpha^{q^i + q^j}. \end{array} \tag{2.4}$$

The coefficients of x^{n-1} and x^{n-2} of the characteristic polynomial of $\alpha \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$ are determined by $-\mathrm{Tr}(\alpha)$ and $T_2(\alpha)$, respectively. A straightforward calculation shows that $T_2(\beta^q - \beta) = \mathrm{Tr}(\beta^{q+1} - \beta^2)$ for all $\beta \in \mathbb{F}_{q^n}$. By Hilbert's Theorem 90 we have that $\mathrm{Tr}(\beta) = 0$ if and only if there exists $\alpha \in \mathbb{F}_{q^n}$ such that $\beta = \alpha^q - \alpha$ and therefore $\mathrm{Tr}(\beta) = 0$ and $T_2(\beta) = 0$ if and only if $0 = T_2(\beta) = T_2(\alpha^q - \alpha) = \mathrm{Tr}(\alpha^{q+1} - \alpha^2)$. Consequently, the number of irreducible polynomials of degree n with first two coefficients being zero can be related to the number of affine rational points of the curve $y^q - y = x^{q+1} - x^2$. For more details about this, see [10, 32]. In Section 2.5, we employ a method that allows us to compute the number $N_n(\mathscr{C}_i)$ when p divides n.

Finally, we study hypersurfaces of the type

$$\mathscr{H}_r : y^q - y = \sum_{j=1}^{r} a_j (x_j^{q^{i_j}+1} - x_j^2) - \lambda, \tag{2.5}$$

for $a_j \in \mathbb{F}_q^*$ and $\lambda \in \mathbb{F}_{q^n}$. We determine the number of rational points of $\mathscr{H}_r$ in $\mathbb{F}_{q^n}^{r+1}$ using techniques involving Gauss sums and the fact that $\mathrm{Tr}(ca_j(x_j^{q+1} - x_j^2))$ defines a quadratic form for any $c \in \mathbb{F}_q^*$.

This chapter is organized as follows. Section 2.2 provides background material and preliminary results. In Section 2.3 we discuss the case $g(x) = xF(x) - \lambda$ where $F(x)$ is an $\mathbb{F}_q$-linearized polynomial and $\lambda \in \mathbb{F}_q$. In Section 2.4 we give an explicit formula for $N_n(\mathscr{C}_i)$ when $\gcd(n,p) = 1$. Section 2.5 provides the number of affine rational points of the curves $\mathscr{C}_i$, including the case $\gcd(n,p) = p$. Moreover, we give necessary and sufficient conditions on the curve $\mathscr{C}_i$ to be maximal or minimal. In Section 2.6 we consider the Artin-Schreier hypersurface given by (2.5). We compute $N_n(\mathscr{H}_r)$ and give conditions on this surface to attain the Hasse-Weil bound.

2.2 Preliminary results

In this section, $\mathbb{F}_q$ denotes a finite field with $q = p^s$ elements and p is an odd prime. For a positive integer n, we already defined in Chapter 1 the trace function

$$\begin{aligned} \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q} : \mathbb{F}_{q^n} &\to \mathbb{F}_q \\ \alpha &\mapsto \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}} \end{aligned}$$

and, for simplicity, we denote by Tr. A polynomial $F(x) \in \mathbb{F}_q[x]$ is called $\mathbb{F}_q$*-linearized* if it is of the form $a_0x + a_1x^q + a_2x^{q^2} + \cdots + a_lx^{q^l}$, where $a_j \in \mathbb{F}_q$ for all $0 \le j \le l$. The polynomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_lx^l$ is called the *associated polynomial of* $F(x)$.

In what follows, for $F(x) \in \mathbb{F}_q[x]$ an $\mathbb{F}_q$-linearized and $\lambda \in \mathbb{F}_{q^n}$, $\mathscr{C}_{F,\lambda}$ denotes the curve determined by the equation

$$y^q - y = xF(x) - \lambda \tag{2.6}$$

and $Q_{xF(x)} : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ is the quadratic form given by $Q_{xF(x)}(\alpha) = \mathrm{Tr}(\alpha F(\alpha))$(see Remark 2.33 below). We observe that if $(\alpha, \beta) \in \mathbb{F}_{q^n}^2$ is a point of $\mathscr{C}_{F,\lambda}$, i.e., $\beta^q - \beta = \alpha F(\alpha) - \lambda$ then

$$0 = \mathrm{Tr}(\beta^q - \beta) = \mathrm{Tr}(\alpha F(\alpha) - \lambda) = \mathrm{Tr}(\alpha F(\alpha)) - n\lambda.$$

Conversely, if $\alpha \in \mathbb{F}_{q^n}$ satisfies the equation $\mathrm{Tr}(\alpha F(\alpha)) = n\lambda$, then $\mathrm{Tr}(\alpha F(\alpha) - \lambda) = 0$ and by Hilbert's Theorem 90 there exists $\beta \in \mathbb{F}_{q^n}$ such that $\beta^q - \beta = \alpha F(\alpha) - \lambda$. In addition, any other solution to the equation $y^q - y = \alpha F(\alpha) - \lambda$ is of the form $\beta + c$ for $c \in \mathbb{F}_q$. In particular,

$$N_n(\mathscr{C}_{F,\lambda}) = qN_n(Q_{xF(x)-\lambda}). \tag{2.7}$$

Remark 2.1. *Let $F(x)$ be an $\mathbb{F}_q$-linearized and n a positive integer. It can be easily verified that the map $\tilde{Q} : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ given by $\alpha \mapsto \alpha F(\alpha)$ is a quadratic form. Furthermore, since Tr is an $\mathbb{F}_q$-linear form, we have that the map $Q : \mathbb{F}_{q^n} \to \mathbb{F}_q$ given by $Q(\alpha) = Tr(\tilde{Q}(\alpha))$ is also a quadratic form. In fact, for all $c \in \mathbb{F}_q$ and $\beta \in \mathbb{F}_{q^n}$ we have*

$$Tr(c\beta F(c\beta)) = Tr(c^2\beta F(\beta)) = c^2 Tr(\beta F(\beta)),$$

hence $Tr((x+y)F(x+y)) - Tr(xF(x)) - Tr(yF(y))$ defines a symmetric billinear form.

An important result that we frequently use in this chapter is Theorem 1.32, which gives information on the number of the solutions of a quadratic form over finite fields.

Clearly, in order to determine the number S_α given in Theorem 1.32 we need to calculate the dimension of the radical of the respective quadratic form and the determinant of a reduced matrix associated to this quadratic form. In order to do this, we need to study the complete homogeneous symmetric polynomials and circulant matrices, which we define below.

Definition 2.2. *a) The* complete homogeneous symmetric polynomials *of degree k is defined by*

$$h_k(x_1,\ldots,x_n) = \sum_{1\le i_1\le\cdots\le i_k\le n} x_{i_1}\cdots x_{i_k}.$$

We denote this polynomial by $h_k(n)$.

b) Let $a_0,a_1,\ldots,a_{n-1}$ be elements of a finite field $\mathbb{F}_q$. The circulant matrix $C(a_0,a_1,\ldots,a_{n-1})$ *associated to the n-tuple $(a_0,a_1,\ldots,a_{n-1})$ is the $n\times n$ matrix $(c_{ij})_{i,j}$ with $c_{i,j}=a_k$ for each pair (i,j) such that $j-i\equiv k \pmod n$. The vector $(a_0,a_1,\ldots,a_{n-1})$ is the* generator vector *of C.*

c) The associated polynomial *of the circulant matrix $C(a_0,a_1,\ldots,a_{n-1})$ is $f(x)=\sum_{i=0}^{n-1} a_ix^i$.*

We will show that, under some additional hypotheses (see Proposition 2.12), that there exists a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ such that the associated matrix of the quadratic form $\mathrm{Tr}(Q_{g+\lambda})$ is circulant.

The following theorem, that can be found as an exercise in [41], describes another representation of the polynomial h_k.

Theorem 2.3 ([41], Ex. 7.4)**.** *The polynomial $h_k(n)$ can be expressed as*

$$h_k(n)=\sum_{l=1}^{n}\frac{x_l^{n+k-1}}{\prod_{\substack{m=1\\ m\neq l}}^{n}(x_l-x_m)}.$$

The polynomials h_k will be useful in the computation of the rank of some circulant matrices. When n is relatively prime with the characteristic of the field $\mathbb{F}_q$, it is well known (e.g. [25]) that the determinant of any circulant matrix $C=C(a_0,a_1,\ldots,a_{n-1})$ satisfies the relation

$$\det C=\prod_{i=1}^{n}(a_0+a_1\omega_i+\cdots+a_{n-1}\omega_i^{n-1}),$$

where $\omega_1,\ldots,\omega_n$ are the n-th roots of unity in some extension of $\mathbb{F}_q$. We will use this fact in order to determine the rank of C. More precisely, the rank of C is equal to the number of common roots of $f(x)=\sum_{i=0}^{n}-1a_ix^i$ and x^n-1, as we prove in Theorem 2.10. Before proving this, we need the following definition.

Definition 2.4. *For each $0<j\leq k$ integers, A_k and $A_{k,j}$ denote the polynomials*

a) $A_k(x_1,\dots,x_k)=\prod_{1\leq t<s\leq k}(x_s-x_t)$, *for all* $k\geq 2$.

b) $A_{k,j}(x_1,\dots,x_k)=(-1)^{j+1}\prod_{\substack{1\leq t<s\leq k\\ t,s\neq j}}(x_s-x_t)$, *for all* $k\geq 3$.

We have the following lemmas that show some relations between the complete homogeneous symmetric polynomials and the polynomials A_k and $A_{k,j}$.

Lemma 2.5. *Let n,k be positive integers and for each $1\leq j\leq k$, $h_{n,j}(k)$ be the polynomial $h_n(x_1,\dots,\hat{x}_j,\dots,x_k)$, where $\hat{x}_j$ means that the variable x_j is omitted. Then*

$$\sum_{j=1}^{k}x_j^{n-1}A_{k,j}h_{n-k+1,j}(k)=0,\ \textit{for all } k\geq 3.$$

Proof. Set

$$\epsilon_{l,j}=\begin{cases}1 & \text{if } l>j;\\ -1 & \text{if } l<j;\\ 0 & \text{if } l=j.\end{cases}$$

By Theorem 2.3 it follows that

$$\begin{aligned}\sum_{i=1}^{k}x_j^{n-1}A_{k,j}h_{n-k+1,j}(k) &= \sum_{j=1}^{k}x_j^{n-1}(-1)^{j+1}\prod_{\substack{1\leq t<s\leq k\\ t,s\neq j}}(x_s-x_t)\sum_{\substack{l=1\\ l\neq j}}^{k}\left(\frac{x_l^{n-1}}{\prod_{\substack{m=1\\ m\neq j,l}}^{k}(x_l-x_m)}\right)\\ &= \sum_{j=1}^{k}x_j^{n-1}(-1)^{j+1}\sum_{\substack{l=1\\ l\neq j}}^{k}x_l^{n-1}\prod_{\substack{1\leq t<s\leq k\\ t,s\neq j,l}}(x_s-x_t)(-1)^{k-l}\epsilon_{l,j}\\ &= \sum_{j=1}^{k}\sum_{\substack{l=1\\ l\neq j}}^{k}x_j^{n-1}x_l^{n-1}\prod_{\substack{1\leq t<s\leq k\\ t,s\neq j,l}}(x_s-x_t)(-1)^{k+j-l+1}\epsilon_{l,j}.\end{aligned}$$

For each l and j fixed, the sum runs over the term $(x_lx_j)^{n-1}=(x_jx_l)^{n-1}$ twice and then

$$x_j^{n-1}x_l^{n-1}\left(\prod_{\substack{1\leq t<s\leq k\\ t,s\neq j,l}}(x_s-x_t)(-1)^{k+j-l+1}(\epsilon_{l,j}+\epsilon_{j,l})\right)=0,$$

as we wanted to show. ■

Lemma 2.6. *For any $k \geq 2$ we have*

$$A_{k+1} = \sum_{j=1}^{k+1} \frac{x_1 \dots x_{k+1}}{x_j} A_{k+1,j}.$$

In addition,

$$\sum_{j=1}^{k} \frac{x_1 \cdots x_k}{x_j} \frac{1}{\prod_{\substack{r=1 \\ r \neq j}}^{k} (x_r - x_j)} = \frac{F(x_1, \dots, x_{k+1})}{A_{k+1}} = 1.$$

Proof. Set

$$F_{k+1} = \sum_{j=1}^{k+1} \frac{x_1 \dots x_{k+1}}{x_j} A_{k+1,j}.$$

We will prove that $A_{k+1} = F_{k+1}$ by induction on the number of variables. For $k = 2$ we have

$$\begin{aligned} F_3 &= \sum_{j=1}^{3} \frac{x_1 x_2 x_3}{x_j} (-1)^{j+1} \prod_{\substack{1 \leq s < t \leq 3 \\ s,t \neq j}} (x_t - x_s) \\ &= x_2 x_3 (x_3 - x_2) - x_1 x_3 (x_3 - x_1) + x_1 x_2 (x_2 - x_1) \\ &= (x_2 - x_1)(x_3 - x_1)(x_3 - x_2) = A_3. \end{aligned}$$

Now suppose that the result is true for some $k \geq 2$. The polynomial F_{k+1} has degree $\binom{k+1}{2}$ and if $x_i = x_j$ for some $1 \leq i < j \leq k+1$ it follows that $F_{k+1} = 0$, which implies that A_{k+1} divides F_{k+1}. Since A_{k+1} has the same degree of F_{k+1} we obtain that $F_{k+1} = cA_{k+1}$ for some $c \in \mathbb{F}_q$. From the fact that A_{k+1} is a monic polynomial with respect to the variable x_{k+1}, it remains to show that $c = 1$. In order to prove this, we equate the coefficients of x_{k+1}^k on both sides of $F_{k+1} = cA_{k+1}$ to get

$$\sum_{j=1}^{k} \frac{x_1 \cdots x_k}{x_j} (-1)^{j+1} \prod_{\substack{1 \leq s < t \leq k \\ s,t \neq j}} (x_t - x_s) = c \cdot \prod_{1 \leq s < t \leq k} (x_t - x_s)$$

and this means that $F_k = cA_k$. By the induction hypothesis, it follows that $c = 1$. ■

Lemma 2.7. *Let C be a circulant matrix over $\mathbb{F}_q$ with generator vector $(a_0, a_1, \dots, a_{n-1})$ and $f(x) = \sum_{i=0}^{n-1}$ be the associated polynomial to the matrix C. Let $g(x) = \gcd(f(x), x^n - 1)$ and $\alpha_1, \alpha_2, \dots, \alpha_m$ be the roots of $g(x)$. If $g(x)$ has only simple roots, then for each positive integer $j \leq m$ the relation*

$$(a_0, a_1, \dots, a_{n-j}) \cdot \big(1, h_1(\alpha_1, \dots, \alpha_j), \dots, h_{n-j}(\alpha_1, \dots, \alpha_j)\big) = 0 \tag{2.8}$$

is satisfied, where $\cdot$ denotes the inner product and $h_k(x_1, \dots, x_j)$ is the symmetric polynomial of degree k.

Proof. We set $\vec{\boldsymbol{\alpha}}_k = (\alpha_1, \dots, \alpha_{k+1})$. We proceed the proof by induction on the number of roots of g. For any α root of g we have

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0.$$

Then $(a_0, a_1, \dots, a_{n-1}) \cdot (1, \alpha, \dots, \alpha^{n-1}) = 0$ and this relation is equivalent to the first case of the induction. If $j = 2$, for each pair of roots α_1 and α_2, we have the relations

$$\begin{cases} a_0\alpha_1 + a_1\alpha_1^2 + \cdots + a_{n-1}\alpha_1^n = 0 \\ a_0\alpha_2 + a_1\alpha_2^2 + \cdots + a_{n-1}\alpha_2^n = 0. \end{cases}$$

Subtracting, we get

$$a_0(\alpha_2 - \alpha_1) + a_1(\alpha_2^2 - \alpha_1^2) + \cdots + a_{n-2}(\alpha_2^{n-1} - \alpha_1^{n-1}) = 0.$$

Since $A_2 = \alpha_2 - \alpha_1 \neq 0$ it follows that

$$\begin{aligned} 0 &= (a_0, a_1, \dots, a_{n-2}) \cdot \left(\alpha_2 - \alpha_1, \alpha_2^2 - \alpha_1^2, \dots, \alpha_2^{n-1} - \alpha_1^{n-1}\right) \\ &= (a_0, a_1, \dots, a_{n-2}) \cdot A_2(1, h_1(\alpha_1, \alpha_2), \dots, h_{n-2}(\alpha_1, \alpha_2)) \end{aligned}$$

and this relation proves the case $j = 2$. Let us suppose now that (2.8) is true for any choice of k different roots of g and let $\alpha_1, \dots, \alpha_{k+1}$ be $k+1$ roots of g. By the induction hypothesis, we have $k+1$ equations of the form (2.8), where for each one we do not consider one of the roots, i.e., the j-th equation is given by

$$(a_0, \dots, a_{n-k}) \cdot \left(1, h_{1,j}(\vec{\boldsymbol{\alpha}}_{k+1}), \dots, h_{n-k,j}(\vec{\boldsymbol{\alpha}}_{k+1})\right) = 0. \tag{2.9}$$

Multiplying the vector $\left(1, h_{1,j}(\vec{\boldsymbol{\alpha}}_{k+1}), \dots, h_{n-k,j}(\vec{\boldsymbol{\alpha}}_{k+1})\right)$ by $\alpha_j^{n-1}A_{k+1,j}$ and adding these vectors we obtain the vector

$$\vec{u} = \sum_{j=1}^{k+1} \alpha_j^{n-1}\left(A_{k+1,j}, A_{k+1,j}h_{1,j}(\vec{\boldsymbol{\alpha}}_{k+1}), \dots, A_{k+1,j}h_{n-k,j}(\vec{\boldsymbol{\alpha}}_{k+1})\right).$$

By Lemma 2.5, the last coordinate of $\vec{u}$ is

$$\sum_{j=1}^{k+1} \alpha_j^{n-1}A_{k+1,j}h_{n-k,j}(\vec{\boldsymbol{\alpha}}_{k+1}) = 0. \tag{2.10}$$

Let us put $\alpha = \alpha_1 \cdots \alpha_{k+1}$. The first coordinate of $\vec{u}$ is

$$a_0 \sum_{j=1}^{k+1} \alpha_j^{n-1} A_{k+1,j} = a_0 \sum_{j=1}^{k+1} \alpha_j^{n-1} \Big((-1)^{j+1} \prod_{\substack{1 \le s < t \le k+1 \\ s,t \neq j}} (\alpha_t - \alpha_s) \Big)$$

$$(2.11) \qquad = \frac{a_0}{\alpha} \sum_{j=1}^{k+1} \Big(\frac{\alpha}{\alpha_j} \prod_{\substack{1 \le s < t \le k+1 \\ s,t \neq j}} (\alpha_t - \alpha_s) \Big) = \frac{a_0}{\alpha} A_{k+1},$$

where in the last equality we use Lemma 2.6 and the fact that α_j's are n-th roots of unity. For $2 \le l \le n-k-1$, the l-th coordenate of $\vec{u}$ is equal to

$$a_l \sum_{j=1}^{k+1} \alpha_j^{n-1} A_{k+1,j} h_{l,j}(\vec{\boldsymbol{\alpha}}_{k+1}) = a_l \sum_{j=1}^{k+1} \alpha_j^{n-1} \left((-1)^{j+1} \prod_{\substack{1 \le s \le t \le k+1 \\ s,t \neq j}} (\alpha_t - \alpha_s) \sum_{\substack{i=1 \\ i \neq j}}^{k+1} \frac{\alpha_i^{l+k-1}}{\prod_{\substack{m=1 \\ m \neq i,j}}^{k+1} (\alpha_i - \alpha_m)} \right)$$

$$= a_l \sum_{j=1}^{k+1} \sum_{\substack{i=1 \\ i \neq j}}^{k+1} \left(\alpha_j^{n-1} \alpha_i^{l+k-1} (-1)^{j+1} (-1)^{k-i} \prod_{\substack{1 \le s \le t \le k+1 \\ s,t \neq i,j}} (\alpha_t - \alpha_s) \epsilon_{i,j} \right)$$

$$(2.12) \qquad = \frac{a_l}{\alpha} \sum_{j=1}^{k+1} \sum_{\substack{i=1 \\ i \neq j}}^{k+1} \left(\frac{\alpha}{\alpha_j} \alpha_i^{l+k-1} (-1)^{k+j-i+1} \prod_{\substack{1 \le s \le t \le k+1 \\ s,t \neq i,j}} (\alpha_t - \alpha_s) \epsilon_{i,j} \right).$$

Let G_{k+1} denote the polynomial

$$G_{k+1} = \sum_{j=1}^{k+1} \sum_{\substack{i=1 \\ i \neq j}}^{k+1} \left(\frac{x_1 \cdots x_{k+1}}{x_j} x_i^{l+k-1} (-1)^{k+j-i+1} \prod_{\substack{1 \le s \le t \le k+1 \\ s,t \neq i,j}} (x_t - x_s) \epsilon_{i,j} \right).$$

We observe that for $x_i = x_j$, $i \neq j$, we have $G_{k+1} = 0$ and therefore $(x_i - x_j)$ divides G_{k+1} for all $i \neq j$. We conclude that A_{k+1} divides G_{k+1} and we can write

$$\frac{G_{k+1}}{A_{k+1}} = \sum_{i=1}^{k+1} \frac{x_1 \cdots x_{k+1} x_i^{l+k-1}}{\prod_{\substack{m=1 \\ m \neq i}}^{k+1} (x_i - x_m)} \sum_{\substack{j=1 \\ j \neq i}}^{k+1} \frac{(x_i - x_j)}{\prod_{\substack{r=1 \\ r \neq i,j}}^{k+1} (x_r - x_j)}$$

$$= \sum_{i=1}^{k+1} \frac{x_i^{l+k}}{\prod_{\substack{m=1 \\ m \neq i}}^{k+1} (x_i - x_m)} \sum_{\substack{j=1 \\ j \neq i}}^{k+1} \frac{x_1 \cdots x_{k+1}}{x_i x_j} \frac{1}{\prod_{\substack{r=1 \\ r \neq i,j}}^{k+1} (x_r - x_j)}.$$

Fixing i, it follows from Lemma 2.6 that

$$\sum_{\substack{j=1 \\ j \neq i}}^{k+1} \frac{x_1 \cdots x_{k+1}}{x_i x_j} \frac{1}{\prod_{\substack{r=1 \\ r \neq i,j}}^{k+1} (x_r - x_j)} = 1.$$

Therefore

$$G_{k+1} = A_{k+1}\sum_{i=1}^{k+1}\frac{x_i^{l+k}}{\prod_{\substack{m=1\\ m\neq i}}^{k+1}(x_i - x_m)} = A_{k+1}h_l(k+1). \tag{2.13}$$

By (2.12) we have

$$a_l\sum_{j=1}^{k+1}\alpha_j^{r-1}A_{k+1,j}h_{l,j}(\vec{\boldsymbol{\alpha}}_{k+1}) = \frac{a_l}{\alpha}A_{k+1}h_l(k+1).$$

From (2.10), (2.11) and (2.13) we conclude that

$$(a_0,\ldots,a_{n-k-1})\cdot(1,h_1(k+1),\ldots,h_{n-k-1}(k+1) = 0.$$

■

Remark 2.8. *1. Let λ be a root of $g(x)$. Multiplying $f(\lambda)$ by λ^i we obtain*

$$a_{n-i} + a_{n-i+1}\lambda + \cdots + a_{n-i-1}\lambda^{n-i} = 0$$

and therefore Lemma 2.7 is true for any shift of the coefficients $a_0, a_1, \ldots, a_{n-1}$.

2. In particular, Lemma 2.7 is true if $\gcd(n,q) = 1$*, since in this case $g(x)$ has only simple roots.*

We have the following definition.

Definition 2.9. *Let $f(x) \in \mathbb{F}_q[x]$ be a monic polynomial of degree m such that $f(0) \neq 0$. The* reciprocal polynomial *f^* of the polynomial f is defined by $f^*(x) = \frac{1}{f(0)}x^m f\left(\frac{1}{x}\right)$. The polynomial f is* self-reciprocal *if $f = f^*$.*

The following theorem, shows us how to find the rank and an equivalent reduced matrix to the circulant matrix C in some cases.

Theorem 2.10. *Let $A = A(a_0, a_1, \ldots, a_{n-1})$ be a circulant matrix over $\mathbb{F}_q$ and assume that* $\gcd(n,p) = 1$*. Let $f(x)$ be the associated polynomial to A and assume that $g(x) =$* $\gcd(f(x), x^n - 1)$ *is a self-reciprocal polynomial with* $\deg g(x) = m$*. Then, $rank(A) = n - m = l$ and there exists $M \in GL_n(\mathbb{F}_q)$ such that $MAM^T = \left(\begin{array}{c|c} R & 0 \\ \hline 0 & 0 \end{array}\right)$, where $R = (r_{i,j})$ denotes the $l \times l$ matrix defined by $r_{ij} = a_{ij}$ for $0 \leq i,j \leq l$.*

Proof. Let $\alpha_1, \ldots, \alpha_m$ be the roots of $g(x)$. Let B_i be the matrix obtained from the identity matrix by changing the entries of the $n-i+1$-th row by

$$(1, h_1(\alpha_1, \ldots, \alpha_i), \ldots, h_{n-i}(\alpha_1, \ldots, \alpha_i), 0, \ldots, 0).$$

Observe that

$$B_1 = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \ddots & \cdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 1 & \alpha_1 & \cdots & \alpha_1^{n-2} & \alpha_1^{n-1} \end{pmatrix}.$$

Since α_1 and α_1^{-1} are roots of g, the last row and column of $B_1 A B_1^T$ are null. From Lemma 2.7 and Remark 2.8, it follows that $MAM^T = \left(\begin{array}{c|c} R & 0 \\ \hline 0 & 0 \end{array}\right)$, where $M = B_m B_{m-1} \cdots B_2 B_1$ and R is the matrix A reduced to its first l rows and l columns. ■

Example 2.11. *Let $q = 27$, $n = 7$ and Φ_7 denote the 7-th cyclotomic polynomial. Since* $\text{ord}_7\, q = 2$, Φ_7 *splits into three monic irreducible polynomials over $\mathbb{F}_q[x]$ of degree 2. Let $\langle a \rangle = \mathbb{F}_{27}^*$, where we can choose a with minimal polynomial $x^3 + 2x + 1$. Then*

$$\Phi_n(x) = (x^2 + 2a^2x + 1)(x^2 + (2a^2 + a + 2)x + 1)(x^2 + (2a^2 + 2a + 2)x + 1).$$

Let us define

$$\begin{aligned} f(x) =& (x^2 + 2a^2x + 1)(x^2 + (2a^2 + a + 2)x + 1)(x - a) \\ =& x^5 + x^4(a^2 + 2) + x^3(a^2 + a + 1) + x^2(2a + 1) + x(a^2 + 2a) + 2a. \end{aligned}$$

Therefore the circulant matrix associated to the polynomial $f(x)$ is

$$A = \begin{pmatrix} 2a & a^2{+}2a & 2a{+}1 & a^2{+}a{+}1 & a^2{+}2 & 1 & 0 \\ 0 & 2a & a^2{+}2a & 2a{+}1 & a^2{+}a{+}1 & a^2{+}2 & 1 \\ 1 & 0 & 2a & a^2{+}2a & 2a{+}1 & a^2{+}a{+}1 & a^2{+}2 \\ a^2{+}2 & 1 & 0 & 2a & a^2{+}2a & 2a{+}1 & a^2{+}a{+}1 \\ a^2{+}a{+}1 & a^2{+}2 & 1 & 0 & 2a & a^2{+}2a & 2a{+}1 \\ 2a{+}1 & a^2{+}a{+}1 & a^2{+}2 & 1 & 0 & 2a & a^2{+}2a \\ a^2{+}2a & 2a{+}1 & a^2{+}a{+}1 & a^2{+}2 & 1 & 0 & 2a \end{pmatrix}.$$

Since

$$\begin{aligned} g(x) = \gcd(f(x), x^n - 1) &= (x^2 + 2a^2x + 1)(x^2 + (2a^2 + a + 2)x + 1) \\ &= x^4 + (a^2 + a + 2)x^3 + (2a^2 + a)x^2 + (a^2 + a + 2)x + 1 \end{aligned}$$

is a self-reciprocal polynomial, it follows from Theorem 2.10 that rank(A) is 3 and the reduced matrix associated to A is $A' = \begin{pmatrix} 2a & a^2{+}2a & 2a{+}1 \\ 0 & 2a & a^2{+}2a \\ 1 & 0 & 2a \end{pmatrix}$. In addition,

$$\det A' = a^4 + 12a^3 + a = a^2 \neq 0.$$

2.3 The number of affine rational points of the curve $y^q - y = xF(x) - \lambda$

In this section, in order to find the number of affine rational points of the curve $y^q - y = xF(x) - \lambda$, where $F(x)$ is a $\mathbb{F}_q$-linearized and $\lambda \in \mathbb{F}_{q^n}$, we determine the number of solutions of the equation $\mathrm{Tr}(xF(x)) = \mathrm{Tr}(\lambda)$ in $\mathbb{F}_{q^n}$. In fact, by (2.7)

$$y^q - y = xF(x) - \lambda. \tag{2.14}$$

We recall that we have

$$N_n(\mathscr{C}_{F,\lambda}) = qS_{\mathrm{Tr}(\lambda)},$$

where $S_{\mathrm{Tr}(\lambda)} = |\{x \in \mathbb{F}_{q^n} \mid \mathrm{Tr}(xF(x)) = \mathrm{Tr}(\lambda)\}|$.

In what follows, $\mathscr{P}$ denotes the $n \times n$ cyclic permutation matrix

$$\mathscr{P} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \cdots & \ddots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}. \tag{2.15}$$

The following proposition associates the $\mathbb{F}_q$-linearized polynomial $F(x)$ with an appropriate circulant matrix.

Proposition 2.12. *Let $F(x) = \sum_{i=0}^{l} a_l x^{q^i}$ be $\mathbb{F}_q$-linearized. For $\lambda \in \mathbb{F}_{q^n}$, the number of solutions of $Tr(xF(x)) = Tr(\lambda)$ in $\mathbb{F}_{q^n}$ is equal to the number of solutions $\vec{z} = (z_1, z_2, \ldots, z_n)^T \in \mathbb{F}_q^n$ of the quadratic form*

$$\vec{z}^{\,T} A \vec{z} = Tr(\lambda)$$

where $A = \frac{1}{2}\sum_{i=0}^{l} a_i(\mathscr{P}^i + \left(\mathscr{P}^i\right)^T)$.

Proof. Let $\Gamma = \{\beta_1, \ldots, \beta_n\}$ be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and

$$N_\Gamma = \begin{pmatrix} \beta_1 & \beta_1^q & \cdots & \beta_1^{q^{n-1}} \\ \beta_2 & \beta_2^q & \cdots & \beta_2^{q^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_n & \beta_n^q & \cdots & \beta_n^{q^{n-1}} \end{pmatrix}.$$

Then N_Γ is an invertible matrix and for $x \in \mathbb{F}_{q^n}$ we can write $x = \sum_{j=1}^{n} \beta_j x_j$, where $x_1, \ldots, x_n \in \mathbb{F}_q$. The equation $\mathrm{Tr}(xF(x)) = \mathrm{Tr}(\lambda)$ is equivalent to

$$\sum_{j=0}^{n-1} x^{q^j} F(x)^{q^j} = \mathrm{Tr}(\lambda). \tag{2.16}$$

Since $F(x)$ is a $\mathbb{F}_q$-linearized and the trace is $\mathbb{F}_q$-linear, we need to express the monomials of the form $x \cdot x^{q^l}$ in terms of the basis Γ. We have

$$\mathrm{Tr}(x^{q^l+1}) = \sum_{j=0}^{n-1} x^{q^j} \cdot (x^{q^l})^{q^j} = \sum_{j=0}^{n-1} \left(\sum_{s=1}^{n} \beta_s x_s \right)^{q^j} \left(\sum_{k=1}^{n} \beta_k x_k \right)^{q^{j+l}} = \sum_{s,k=1}^{n} \left(\sum_{j=0}^{n-1} \beta_s^{q^j} \beta_k^{q^{j+l}} \right) x_s x_k .$$

Consequently $\mathrm{Tr}(x^{q^l+1})$ has the following symmetric representation

$$(x_1\, x_2\, \cdots\, x_n) B_l \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}, \text{ where } B_l = \frac{1}{2} N_\Gamma \left(\mathscr{P}^l + \left(\mathscr{P}^l \right)^T \right) N_\Gamma^T .$$

Making the change of variables $(z_1\, z_2\, \cdots\, z_n) = (x_1\, x_2\, \cdots\, x_n) N_\Gamma$ we get

$$\left(z_1\, z_2\, \cdots\, z_n \right) \left[\frac{1}{2} \left(\mathscr{P}^l + \left(\mathscr{P}^l \right)^T \right) \right] \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{pmatrix} = \mathrm{Tr}(\lambda)$$

which has the same number of solutions as $\mathrm{Tr}(x^{q^l+1}) = \mathrm{Tr}(\lambda)$ have. Using Equation (2.16) and the definition of A, the result follows. ■

The following theorem is straightforward consequence of Theorems 1.32,2.10 and Proposition 2.12.

Theorem 2.13. *Let $F(x) = \sum_{i=0}^{l} a_i x^{q^i}$ be $\mathbb{F}_q$-linearized and $f(x) = \sum_{i=0}^{l} a_i x^i$ its associated polynomial. We assume $\gcd(n,p) = 1$ and that $g(x) = \gcd(f(x), x^n - 1)$ is a self-reciprocal polynomial of degree m. Let also R be the matrix defined as in Theorem 2.10 and $a =$ det R. Then, for each $\lambda \in \mathbb{F}_{q^n}$, the number of affine rational points in $\mathbb{F}_{q^n}^2$ of the curve $y^q - y = xF(x) - \lambda$ is*

$$N_n(\mathscr{C}_{F,\lambda}) = \begin{cases} q^n - \chi((-1)^{(n-m)/2} a) q^{(n+m-2)/2}, & \text{if } n+m \text{ is even and } Tr(\lambda) \neq 0; \\ q^n + (q-1)\chi((-1)^{(n-m)/2} a) q^{(n+m-2)/2}, & \text{if } n+m \text{ is even and } Tr(\lambda) = 0; \\ q^n + \chi(2(-1)^{(n-m-1)/2} a Tr(\lambda)) q^{(n+m-1)/2}, & \text{if } n+m \text{ is odd.} \end{cases}$$

Corollary 2.14. *Let F, f and g be polynomials which satisfy the conditions of Theorem 2.13. Then,*

$$|N_n(\mathscr{C}_{F,\lambda}) - q^n| \leq (q-1) q^{\frac{n+m-2}{2}} .$$

In addition, the upper bound is attained if and only if $n+m$ is even, $Tr(\lambda)=0$ and $(-1)^{(n-m)/2}a$ is a square in $\mathbb{F}_q$.

The lower bound is attained if and only if $n+m$ is even, $Tr(\lambda)=0$ and $(-1)^{(n-m)/2}a$ is not a square in $\mathbb{F}_q$.

Remark 2.15. *The curve $\mathscr{C}_{F,\lambda}$, where $F(x)=\sum_{i=0}^{l} a_i x^{q^i}, a_i \in \mathbb{F}_q^*$ and $0 \le l < n$, has genus $g=\frac{(q-1)q^l}{2}$. The Hasse-Weil bound for $\mathscr{C}_{F,\lambda}$ is given by*

$$|N_n(\mathscr{C}_{F,\lambda})-(q^n+1)| \le (q-1)q^{\frac{2l+n}{2}},$$

since we has only one point at infinity. Consequently, this curve is not maximal or minimal with respect to the Hasse-Weil bound.

Example 2.16. *Let $q=27, n=7$ and $f(x)$, $g(x)$ be the polynomials of Example 2.11. The polynomial $F(x)=x^{q^5}+(a^2+2)x^{q^4}+(a^2+a+1)x^{q^3}+(2a+1)x^{q^2}+(a^2+2a)x^q+2ax$ is the $\mathbb{F}_q$-linearized polynomial of $f(x)$. Since $n-m$ is odd and $\det C'=a^2$, Theorem 2.13 implies that*

$$N_n(\mathscr{C}_{F,\lambda})=q^7+q^6\chi(Tr(\lambda))=\begin{cases} q^7+q^6 & \text{if } Tr(\lambda) \text{ is a square in } \mathbb{F}_q^*,\\ q^7-q^6 & \text{if } Tr(\lambda) \text{ is not a square in } \mathbb{F}_q^*,\\ q^7 & \text{if } Tr(\lambda)=0.\end{cases}$$

In the following section we compute the constant D in Theorem 1.32 for some some special polynomials $F(x)$.

2.4 The number of affine rational points over $\mathbb{F}_{q^n}$ of the curve $y^q-y=x\cdot(x^{q^i}-x)-\lambda$ with $\gcd(n,p)=1$

Throughout this section, for any prime t and a positive integer m, we denote by $\left(\frac{m}{t}\right)$ the Legendre symbol of m mod t and by $v_t(m)$ the t-adic valuation of m, i.e., the largest integer j such that t^j divides m. The aim of this section is to find an expression for the number of affine rational points of the curve

$$\mathscr{C}_i : y^q-y=x^{q^i+1}-x^2-\lambda$$

in $\mathbb{F}_{q^n}^2$ with $\lambda \in \mathbb{F}_{q^n}$.

In the previous section we used the fact that the number $N_n(\mathscr{C}_i)$ is q times the number of elements $x \in \mathbb{F}_{q^n}$ such that $\mathrm{Tr}(x(x^{q^i}-x))=\mathrm{Tr}(\lambda)$.

In order to determine the number of solutions of $\mathrm{Tr}(x(x^{q^i}-x))=\mathrm{Tr}(\lambda)$, it is necessary to establish the dimension of the symmetric bilinear form associated to this quadratic form, which is the subject of the next proposition.

Proposition 2.17. *Let $0<i<n$ be integers and $F(x)=\sum_{j=0}^{i} a_j x^{q^j}\in\mathbb{F}_q[x]$ be an $\mathbb{F}_q$-linearized polynomial. Let $Q_F(x)=Tr(xF(x))$. If $a_0\neq 0$, then*

$$\dim rad(Q_F)=\deg\Big(\gcd\Big(\sum_{j=0}^{i} a_j(x^j+x^{n-j}),x^n-1\Big)\Big). \tag{2.17}$$

Proof. In order to determine the dimension of the radical of Q_F it is sufficient to compute the dimension of the radical

$$\dim_{\mathbb{F}_q}\{x\in\mathbb{F}_{q^n}\,|\,Q_F(x,y)=0 \text{ for all } y\in\mathbb{F}_{q^n}\}.$$

In fact

$$\begin{aligned}
B_{Q_F}(x,y)&=\mathrm{Tr}\Big(\sum_{j=0}^{i} a_j(x+y)^{q^j+1}-\sum_{j=0}^{i} a_j x^{q^j+1}-\sum_{j=0}^{i} a_j y^{q^j+1}\Big)\\
&=\sum_{l=0}^{n-1}\big(\sum_{j=0}^{i} a_j(x+y)^{q^{j+l}+q^l}-\sum_{j=0}^{i} a_j x^{q^{j+l}+q^l}-\sum_{j=0}^{i} a_j y^{q^{j+l}+q^l}\big)\\
&=\sum_{j=0}^{i} a_j\big(\sum_{l=0}^{n-1} x^{q^{j+l}}y^{q^l}+x^{q^l}y^{q^{j+l}}\big)\\
&=\sum_{j=0}^{i} a_j\big(\sum_{j=0}^{n-1}((x^{q^j}+x^{q^{n-j}})y)^{q^l}\big)\\
&=\sum_{j=0}^{i} a_j\mathrm{Tr}((x^{q^j}+x^{q^{n-j}})y)=\mathrm{Tr}\big(\sum_{j=0}^{i} a_j(x^{q^j}+x^{q^{n-j}})y\big).
\end{aligned} \tag{2.18}$$

It follows that $Q_F(x,y)=0$ for all $y\in\mathbb{F}_{q^n}$ is equivalent to

$$\sum_{j=0}^{i} a_j(x^{q^j}+x^{q^{n-j}})=0. \tag{2.19}$$

The $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^n}$ determined by (2.19) is the set of roots of

$$g(x)=\gcd(H(x),x^{q^n}-x),\qquad \text{where } H(x)=\sum_{j=0}^{i} a_j(x^{q^j}+x^{q^{n-j}}).$$

Since g is a $\mathbb{F}_q$-linearized with coefficients in $\mathbb{F}_q$, the degree of the associated polynomial gives us the dimension of radical of Q_F, which is the degree of $\gcd\Big(x^n-1,\sum_{j=0}^{i} a_j(x^j+x^{n-j})\Big)$. This finishes the proof. ■

For the special case $y^q - y = x(x^{q^i} - x) - \lambda$ we explicitly determine the dimension of the quadratic form $\mathrm{Tr}(x(x^{q^i} - x))$. Moreover, we will use this information to compute $N_n(\mathscr{C}_i)$, that is given in Theorem 2.26. In order to simplify the notations, we define the following quadratic form.

Definition 2.18. *Let i,n be integers such that $0 < i < n$. We define*

$$\begin{aligned} Q_i : \mathbb{F}_{q^n} &\to \mathbb{F}_q \\ x &\mapsto Tr(x^{q^i+1} - x^2). \end{aligned}$$

The following corollary is a consequence of Proposition 2.17.

Corollary 2.19. *Let i,n be integers such that $0 < i < n$ and $B_i(x,y)$ the associated symmetric bilinear form of Q_i. Let $n = p^u\tilde{n}$ and $i = p^s\tilde{i}$, where u,s are non-negative integers such that $\gcd(p,\tilde{n}) = \gcd(p,\tilde{i}) = 1$. Then*

$$\dim rad\ (Q_i) = \gcd(\tilde{n},\tilde{i})\min(p^u, 2p^s). \tag{2.20}$$

Proof. By Proposition 2.17 it is enough to find the dimension of the linear space determined by the roots of

$$H(x) = \gcd(x^{q^i} + x^{q^{n-i}} - 2x, x^{q^n} - x). \tag{2.21}$$

Since $n = p^u\tilde{n}$, $i = p^s\tilde{i}$, the associated polynomial to the $\mathbb{F}_q$-linearized polynomial $H(x)$ is

$$\begin{aligned} h(x) &= \gcd\left(x^i - 2 + x^{n-i}, x^n - 1\right) = \gcd\left(x^{2i} - 2x^i + x^n, x^n - 1\right) \\ &= \gcd((x^{\tilde{i}} - 1)^{2p^s}, (x^{\tilde{n}} - 1)^{p^u}) = (x^{\gcd(\tilde{n},\tilde{i})} - 1)^{\min(p^u,2p^s)}. \end{aligned}$$

Since the degree of $h(x)$ is equals to the dimension of the radical, we conclude that dim rad $(Q_i) = \gcd(\tilde{n},\tilde{i})\min(p^u, 2p^s)$. ■

Using Theorem 1.32 and the previous corollary we can determine the number of solutions of $\mathrm{Tr}(x^{q^i+1} - x^2) = \mathrm{Tr}(\lambda)$ in $\mathbb{F}_{q^n}$, which will give us a complete description of $N_n(\mathscr{C}_i)$.

Lemma 2.20. *Let i,n be integers such that $0 < i < n$ and $\gcd(n,2p) = 1$. Let v be the dimension of the radical of the associated bilinear symmetric form Q_i. Let $i = p^s\tilde{i}$, where s*

is a non-negative integer and $\gcd(\tilde{i},p)=1$*. Then* $n+v$ *is even and, for* $\lambda \in \mathbb{F}_q^*$*, the constant* D *of Theorem 1.32 is given by*

$$D=\prod_{j=1}^{u}\left(\frac{q}{p_j}\right)^{\max\{0,\nu_{p_j}(n)-\nu_{p_j}(i)\}}.$$

where $n=p_1^{a_1}\cdots p_u^{a_u}$ *is the prime factorization of* n*.*

Proof. Let $M_{\mathrm{Tr}(\lambda)}$ be the set of solutions of $\mathrm{Tr}(x^{q^i+1}-x^2)=\mathrm{Tr}(\lambda)$ in $\mathbb{F}_{q^n}$. Then $S_{\mathrm{Tr}(\lambda)}=|M_{\mathrm{Tr}(\lambda)}|$ is given by Equation (1.1). For each possible value of $\mathrm{Tr}(\lambda)\in\mathbb{F}_q^*$, if $\mathrm{Tr}(x^{q^i+1}-x^2)=\mathrm{Tr}(\lambda)$ we have

$$\mathrm{Tr}((x^{q^j})^{q^i+1}-(x^{q^j})^2)=\mathrm{Tr}((x^{q^i+1}-x^2)^{q^j})=\mathrm{Tr}(x^{q^i+1}-x^2)=\mathrm{Tr}(\lambda), \tag{2.22}$$

for all $0\le j\le n-1$.

We first consider the case $n=p_1^a$, where p_1 is an odd prime and $\gcd(p_1,p)=1$. By Equation (2.22), for each $\alpha\in M_{\mathrm{Tr}(\lambda)}$ we can associate another $d-1$ elements of $M_{\mathrm{Tr}(\lambda)}$, where d is the smallest positive divisor of $n=p_1^a$ such that $\alpha^{q^d}=\alpha$. For each $\alpha\in M_{\mathrm{Tr}(\lambda)}$ we have $d>1$, since $\alpha^q=\alpha$ implies $\alpha^{q^i+1}-\alpha^2=\alpha^2-\alpha^2=0$, a contradiction with $\mathrm{Tr}(\lambda)\ne 0$. Then d is a multiple of p_1 and Equation (1.1) of Theorem 1.32 can be rewritten modulo p_1 as

$$q^{n-1}-Dq^{(n+v-2)/2}\equiv 0 \pmod{p_1},$$

which is equivalent to

$$D\equiv(q^{(n+v-2)/2})^{-1}\equiv q^{(n+v-2)/2} \pmod{p_1},$$

where in the last congruence we use the fact that $D=\pm1$. By Corollary 2.19 we obtain

$$\begin{aligned}
D &\equiv q^{({p_1}^a+{p_1}^{\min\{a,\nu_{p_1}(i)\}})/2-1} \pmod{p_1}\\
&\equiv q^{p_1^{\min(a,\nu_{p_1}(i))}(p_1^{(a-\min(a,\nu_{p_1}(i))}+1)/2-1} \pmod{p_1}\\
&\equiv q^{(p_1^{(a-\min(a,\nu_{p_1}(i))}-1)/2} \pmod{p_1}\\
&\equiv q^{(p_1^{\max\{0,a-\nu_{p_1}(i)\}}-1)/2} \pmod{p_1}\\
&\equiv \left(\frac{q}{p_1}\right)^{(p_1^{\max\{0,a-\nu_{p_1}(i)\}}-1)/(p_1-1)} \pmod{p_1}
\end{aligned}$$

Since $\left(\frac{q}{p_1}\right)$ assumes only the values $\{-1,1\}$ and $\frac{p_1^l-1}{p_1-1}\equiv l \pmod{2}$, we conclude that

$$D=\left(\frac{q}{p_1}\right)^{\max\{0,a-\nu_{p_1}(i)\}}.$$

Now we consider the general case $n = p_1^{a_1} \cdots p_u^{a_u}$, with $u \geq 1$. We will prove the result by induction on u. We already proved the case when $u = 1$. Now suppose that $u \geq 2$. It follows from Lemma 2.19 that the dimension of the radical of the bilinear symmetric form associated to $Q_i(x)$ is $v = \gcd(p_1^{a_1} \cdots p_u^{a_u}, i)$. Therefore v divides $p_1^{a_1} \cdots p_u^{a_u}$ and $n + v$ is even. Using Theorem 1.32, for $\mathrm{Tr}(\lambda) \in \mathbb{F}_q^*$, we obtain that

$$S_{\mathrm{Tr}(\lambda)} = q^{n-1} - Dq^{(n+v-2)/2}.$$

Now let $\mathrm{Tr}(\lambda) \in \mathbb{F}_q^*$ and $n = \tilde{n} p_u^{a_u}$ where $\tilde{n} = p_1^{a_1} \cdots p_{u-1}^{a_{u-1}}$. We now consider the subfield $\mathbb{F}_{q^{\tilde{n}}} \subset \mathbb{F}_{q^n}$. By the induction hypothesis, the number of solutions of $\mathrm{Tr}_{\mathbb{F}_{q^{\tilde{n}}}/\mathbb{F}_q}(x^{q^i+1} - x^2) = \mathrm{Tr}(\lambda)$ is

$$S_{\mathrm{Tr}(\lambda),\tilde{n}} = q^{\tilde{n}-1} - \prod_{j=1}^{u-1} \left(\frac{q}{p_j}\right)^{\max\{0, \nu_{p_j}(n) - \nu_{p_j}(i)\}} q^{(\tilde{n}+v_1-2)/2},$$

where v_1 is the dimension of radical of the bilinear symmetric form associated to $\mathrm{Tr}_{\mathbb{F}_{q^{\tilde{n}}}/\mathbb{F}_q}(x^{q^i+1} - x^2)$. From Lemma 2.19 we know that $v_1 = \gcd(\tilde{n}, i)$ and them $v = v_1 \cdot \gcd(p_u^{a_u}, i)$. Since $\mathbb{F}_{q^{\tilde{n}}} \cap \mathbb{F}_{q^{p_u^{a_u}}} = \mathbb{F}_q$, the solutions which are not in $\mathbb{F}_{q^{\tilde{n}}}$ can be grouped in sets of size divisible by p_u. In fact, since α is a solution then α^{q^j} is also a solution and $\alpha \in \mathbb{F}_{q^n}$, it follows that there exists $d > 1$ dividing $p_u^{a_u}$ such that $\alpha^{q^d} = \alpha$. Then

$$S_{\mathrm{Tr}(\lambda)} \equiv S_{\mathrm{Tr}(\lambda),\tilde{n}} \pmod{p_u},$$

which is equivalent to

$$q^{\tilde{n}p_u^{a_u}-1} - Dq^{(\tilde{n}p_u^{a_u}+v-2)/2} \equiv q^{\tilde{n}-1} - \prod_{j=1}^{u-1} \left(\frac{q}{p_j}\right)^{\max\{0, \nu_{p_j}(n) - \nu_{p_j}(i)\}} q^{(\tilde{n}+v_1-2)/2} \pmod{p_u}.$$

Since $q^{p_u} \equiv q \pmod{p_u}$, the previous equation is equivalent to

$$Dq^{(\tilde{n}p_u^{a_u}+v-2)/2} \equiv \prod_{j=1}^{u-1} \left(\frac{q}{p_j}\right)^{\max\{0, \nu_{p_j}(n) - \nu_{p_j}(i)\}} q^{(\tilde{n}+v_1-2)/2} \pmod{p_u}. \tag{2.23}$$

Now let $v_2 = \gcd(p_u^{a_u}, i)$. We observe that $q^{(p_u^{a_u}-1)/2} \equiv \left(\frac{q}{p_u}\right)^{a_u} \pmod{p_u}$ and them

$$\begin{aligned} q^{(\tilde{n}+v_1-\tilde{n}p_u^{a_u}-v)/2} &\equiv q^{-\tilde{n}\left(\frac{p_u^{a_u}-1}{2}\right)} q^{\left(\frac{v_1-v}{2}\right)} \pmod{p_u} \\ &\equiv \left(\frac{q}{p_u}\right)^{a_u\tilde{n}} q^{\left(\frac{v_1-v}{2}\right)} \pmod{p_u} \\ &\equiv \left(\frac{q}{p_u}\right)^{a_u\tilde{n}} q^{\frac{v_1(1-v_2)}{2}} \pmod{p_u} \\ &\equiv \left(\frac{q}{p_u}\right)^{a_u} q^{-v_1\frac{(p_u^{\min\{a_u, \nu_{p_u}(i)\}}-1)}{2}} \pmod{p_u}. \qquad (2.24) \end{aligned}$$

Equations (2.23) and (2.24) allow us to conclude that

$$\begin{aligned} D &\equiv \prod_{j=1}^{u-1} \left(\frac{q}{p_j}\right)^{\max\{0,\nu_{p_j}(n)-\nu_{p_j}(i)\}} q^{(\tilde{n}+v_1-\tilde{n}p_u^{a_u}-v)/2} \pmod{p_u} \\ &\equiv \prod_{j=1}^{u-1} \left(\frac{q}{p_j}\right)^{\max\{0,\nu_{p_j}(n)-\nu_{p_j}(i)\}} \left(\frac{q}{p_u}\right)^{a_u} q^{-v_1\frac{(p_u^{\min\{a_u,\nu_{p_u}(i)\}}-1)}{2}} \pmod{p_u} \\ &\equiv \prod_{j=1}^{u-1} \left(\frac{q}{p_j}\right)^{\max\{0,\nu_{p_j}(n)-\nu_{p_j}(i)\}} \left(\frac{q}{p_u}\right)^{a_u} \left(\frac{q}{p_u}\right)^{-\min\{a_u,\nu_{p_u}(i)\}} \pmod{p_u} \\ &\equiv \prod_{j=1}^{u} \left(\frac{q}{p_j}\right)^{\max\{0,\nu_{p_j}(n)-\nu_{p_j}(i)\}} \pmod{p_u} \end{aligned}$$

and consequently $D = \prod_{j=1}^{u} \left(\frac{q}{p_j}\right)^{\max\{0,\nu_{p_j}(n)-\nu_{p_j}(i)\}}$.

■

Remark 2.21. *From Theorem 1.32 we have that D does not depend on the value of $Tr(\lambda) \in \mathbb{F}_q$. Then, by Lemma 2.20, for $Tr(\lambda) = 0$ we have that the value of D in Equation* (1.1) *is* $D = \prod_{j=1}^{u} \left(\frac{q}{p_j}\right)^{\max\{0,\nu_{p_j}(n)-\nu_{p_j}(i)\}}$.

For extensions of degree a power of 2 we have the following result.

Lemma 2.22. *Let b, i, n be integers such that $0 < i < n$ and $n = 2^b$. Let v be the dimension of the radical of the associate bilinear symmetric form of Q_i. For any $\lambda \in \mathbb{F}_{q^n}$, the value of D as defined in Theorem 1.32 is given by*

$$D = \begin{cases} \chi(-Tr(\lambda)) & \text{if } b = 1, \\ (-1)^{(q-1)(2^b-v)/4} & \text{if } b \geq 2 \text{ and } n+v \text{ is even}, \\ (-1)^{(q+1)/2} \cdot \chi\left(-\frac{Tr(\lambda)}{2^{b-1}}\right) & \text{if } b \geq 2 \text{ and } n+v \text{ is odd}. \end{cases}$$

Proof. When $n = 2$ it follows that $i = 1$ and $\mathrm{Tr}(\alpha^{q+1} - \alpha^2) = \mathrm{Tr}(\lambda)$ is equivalent to

$$\alpha^{q^2+q} - \alpha^{2q} + \alpha^{q+1} - \alpha^2 = \mathrm{Tr}(\lambda). \tag{2.25}$$

The latter can be written as $(\alpha^q - \alpha)^2 = -\mathrm{Tr}(\lambda)$, since $\alpha^{q^2} = \alpha$. If $\mathrm{Tr}(\lambda) = 0$ we conclude that $\alpha^q - \alpha = 0$, and then $\alpha \in \mathbb{F}_q$. In this case (2.25) has q solutions in $\mathbb{F}_q$. For $\mathrm{Tr}(\lambda) \in \mathbb{F}_q^*$, let us consider the following maps:

$$\begin{aligned} \tau_1 : \mathbb{F}_{q^2} &\to \mathbb{F}_{q^2} \\ x &\mapsto x^q - x. \end{aligned} \qquad \text{and} \qquad \begin{aligned} \tau_2 : \mathbb{F}_{q^2} &\to \mathbb{F}_{q^2} \\ x &\mapsto x^2. \end{aligned}$$

In order to determine the number of solutions of Equation (2.25) it is enough to fix $\alpha \in \mathbb{F}_{q^2}$ such that $\tau_2(\tau_1(\alpha)) = -\mathrm{Tr}(\lambda)$. Let $\{1,\alpha\}$ be a basis of $\mathbb{F}_{q^2}/\mathbb{F}_q$. The image of $\{1,\alpha\}$ by τ_1 is $\{0,\beta\}$, where $\beta = \alpha^q - \alpha$. Since $\ker(\tau_1) = \mathbb{F}_q$, the image of τ_1 is generated by β. Therefore it is sufficient to consider the elements of the form $c\alpha$, with $c \in \mathbb{F}_q$, i.e.,

$$\tau_2(\tau_1(c\alpha)) = \tau_2(c\beta) = c^2\beta^2.$$

We now claim that $\beta \notin \mathbb{F}_q$. For that, suppose by contradiction that $\beta^q = \beta$. Then

$$\alpha^{q^2} - \alpha^q - \alpha^q + \alpha = 0$$

which only happens if $-2(\alpha^q - \alpha) = 0$. But this is not possible because $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and $p \neq 2$. Consequently $\tau_2(\tau_1(c\alpha)) = -\mathrm{Tr}(\lambda)$ if and only if $c^2\beta^2 = -\mathrm{Tr}(\lambda)$, and since $\beta \notin \mathbb{F}_q$, this equation has solutions if and only if $-\mathrm{Tr}(\lambda)$ is not a square in $\mathbb{F}_q$. In this case, Equation (2.25) has $2q$ solutions.

Now we consider the case when $n = 2^b$ with $b > 1$. Let $i = p^s\tilde{i}$, where $\gcd(p,\tilde{i}) = 1$. From Lemma 2.19 we know that $v = \gcd(2^b,\tilde{i})\min(1,2p^s) = \gcd(2^b,i)$, which implies that v is of the form 2^c with $0 \le c \le b$. Let $M_{\mathrm{Tr}(\lambda)}$ be the set of solutions of $\mathrm{Tr}(x^{q^i+1} - x^2) = \mathrm{Tr}(\lambda)$ in $\mathbb{F}_{q^n}$. We now consider two cases.

1. $n + v$ is even.

   In this case v and i are even. The number of solutions of $\mathrm{Tr}(x^{q^i+1} - x^2) = \mathrm{Tr}(\lambda)$ is given by Equation (1.1). If $\mathrm{Tr}(\alpha^{q^i+1} - \alpha^2) = \mathrm{Tr}(\lambda)$ for some $\alpha \in \mathbb{F}_q^*$, we have

   $$\mathrm{Tr}((\alpha^{q^j})^{q^i+1} - (\alpha^{q^j})^2) = \mathrm{Tr}((\alpha^{q^i+1} - \alpha^2)^{q^j}) = \mathrm{Tr}(\alpha^{q^i+1} - \alpha^2) = \mathrm{Tr}(\lambda), \tag{2.26}$$

   for each $0 \le j \le n-1$. Since $n = 2^b \ge 4$ and by Equation (2.26), for each $\alpha \in M_{\mathrm{Tr}(\lambda)}$ we can associate another $d-1$ elements of $M_{\mathrm{Tr}(\lambda)}$, where d is the smallest positive divisor of $n = 2^b$ such that $\alpha^{q^d} = \alpha$. We claim that $d > 2$. In fact, if $d = 1$ we have $(\alpha^{q^i+1} - \alpha^2)^q = \alpha^2 - \alpha^2 = 0$, and them $\mathrm{Tr}(\lambda) = 0$, a contradiction. If $d = 2$, for $\alpha \in \mathbb{F}_{q^2}$ we have $(\alpha^{q^i+1} - \alpha^2)^{q^2} = \alpha^{q^i+1} - \alpha^2 = \alpha^2 - \alpha^2 = 0$, since i is even. The latter also implies that $\mathrm{Tr}(\lambda) = 0$, a contradiction. In particular, Equation (2.26) does not have solutions for $d = 1,2$. Consequently $d > 2$ and then 4 divides d for any $\alpha \in M_{\mathrm{Tr}(\lambda)}$. From Equation (1.1) of Theorem 1.32, we obtain the relation

   $$q^{2^b-1} - Dq^{(2^b+v-2)/2} \equiv 0 \pmod 4,$$

   which is equivalent to

   $$D \equiv q^{2^b-1-(2^b+v-2)/2} \equiv q^{(2^b-v)/2} \pmod 4.$$

We conclude that, in this case, $D = (-1)^{(q-1)(2^b-v)/4}$.

2. $n+v$ is odd.

   In this case, v is odd and, since it also divides 2^b, we conclude that $v = 1$. By the same argument used in the previous case, the number of solutions of $\mathrm{Tr}(\alpha^{q^i+1} - \alpha^2) = \mathrm{Tr}(\lambda)$ is given by Equation (1.2). Furthermore, it follows that for $\mathrm{Tr}(\lambda) \in \mathbb{F}_q^*$ we have $\mathrm{Tr}(\alpha^{q^i+1} - \alpha^2) = \mathrm{Tr}(\lambda)$ if and only if

   $$\mathrm{Tr}((\alpha^{q^j})^{q^i+1} - (\alpha^{q^j})^2) = \mathrm{Tr}((\alpha^{q^i+1} - \alpha^2)^{q^j}) = \mathrm{Tr}(\alpha^{q^i+1} - \alpha^2) = \mathrm{Tr}(\lambda), \tag{2.27}$$

   for all $0 \le j \le n-1$. Therefore for each $\alpha \in M_{\mathrm{Tr}(\lambda)}$ we can associate another $d-1$ elements of $S_{\mathrm{Tr}(\lambda)}$, where d is the smallest divisor of $n = 2^b \ge 4$ such that $\alpha^{q^d} = \alpha$. The case $d = 1$ does not happen, otherwise we would have $\mathrm{Tr}(\lambda) = 0$.

   Suppose now that $\alpha \in \mathbb{F}_{q^2} \cap M_{\mathrm{Tr}(\lambda)} \subset \mathbb{F}_{q^n}$. We then have

   $$\mathrm{Tr}(\lambda) = \mathrm{Tr}(\alpha^{q^i+1} - \alpha^2) = 2^{b-1} \cdot ((\alpha^{q^{i+1}+q} - \alpha^{2q}) + \alpha^{q^i+1} - \alpha^2). \tag{2.28}$$

   As in the previous case, Equation (2.28) does not have solution in $\mathbb{F}_q$. Therefore $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and the equation

   $$\mathrm{Tr}(\lambda) = 2^{b-1} \cdot (\alpha^{q+1} + \alpha^{q+1} - \alpha^{2q} - \alpha^2)$$

   can be written as $(\alpha^q - \alpha)^2 = -\gamma$, where $\gamma = \frac{\mathrm{Tr}(\lambda)}{2^{b-1}}$. Using the same argument of item 1 of Lemma 2.22, we prove that $(\alpha^q - \alpha)^2 = -\gamma$ has solutions in $\mathbb{F}_{q^2}$ if and only if $-\gamma$ is not a square in $\mathbb{F}_q$. The latter is equivalent to $\frac{-\mathrm{Tr}(\lambda)}{2^{b-1}}$ not being a square in $\mathbb{F}_q$ and, in this case, we have $2q$ solutions for Equation (2.25) in $\mathbb{F}_{q^2}$. Consequently, the number of solutions of Equation (2.28) in $\mathbb{F}_{q^2}$ is $\left(1 - \chi\left(-\frac{\mathrm{Tr}(\lambda)}{2^{b-1}}\right)\right) q$ and then

   $$S_{\mathrm{Tr}(\lambda)} - \left(1 - \chi\left(-\frac{\mathrm{Tr}(\lambda)}{2^{b-1}}\right)\right) q \equiv 0 \pmod 4.$$

   By Theorem 1.32, it follows that

   $$q^{2^b-1} + Dq^{(2^b+v-1)/2} \equiv \left(1 - \chi\left(-\frac{\mathrm{Tr}(\lambda)}{2^{b-1}}\right)\right) q \pmod 4,$$

   i.e.,

   $$D \equiv \left(1 - \chi\left(-\frac{\mathrm{Tr}(\lambda)}{2^{b-1}}\right)\right) q^{1-(2^b+v-1)/2} - q^{(2^b-v-1)/2} \pmod 4.$$

   Therefore

   $$D \equiv \left(\left(1 - \chi\left(-\frac{\mathrm{Tr}(\lambda)}{2^{b-1}}\right)\right) q^{2-2^b} - 1\right) q^{(2^b-v-1)/2} \pmod 4.$$

Since $v = 1$ and $q^2 \equiv 1 \pmod 4$, we conclude that

$$D \equiv -q^{2^{b-1}-1} \cdot \chi\left(-\frac{\mathrm{Tr}(\lambda)}{2^{b-1}}\right) \equiv -q \cdot \chi\left(-\frac{\mathrm{Tr}(\lambda)}{2^{b-1}}\right) \pmod 4$$

and consequently

$$D = (-1)^{(q+1)/2} \cdot \chi\left(-\frac{\mathrm{Tr}(\lambda)}{2^{b-1}}\right).$$

The case $\mathrm{Tr}(\lambda) = 0$ follows from Theorem 1.32, which tells us that D is the same for any $\mathrm{Tr}(\lambda) \in \mathbb{F}_q$ if $n + v$ is even. In the case where $n + v$ is odd, we have $D = 0$. ■

The following definitions are helpful to allows us to rewrite the expressions of D in a more simpler way.

Definition 2.23. *For each $\alpha \in \mathbb{F}_q$ we define*

$$\varepsilon_\alpha = \begin{cases} q-1 & \textit{if } \alpha = 0, \\ -1 & \textit{otherwise,} \end{cases} \quad \textit{and} \quad \varepsilon'_\alpha = \begin{cases} 0 & \textit{if } \alpha = 0, \\ -1 & \textit{otherwise.} \end{cases}$$

In the following theorem we use Theorem 1.32 and Lemma 2.22, to determine the value of $S_{\mathrm{Tr}(\lambda)}$.

Theorem 2.24. *Let b, i, n be integers such that $0 < i < n$ and $n = 2^b$. For $\lambda \in \mathbb{F}_{q^n}$, the number of solutions $S_{Tr(\lambda)}$ of $Q_i(x) = Tr(\lambda)$ in $\mathbb{F}_{q^n}$ is given by*

$$S_{Tr(\lambda)} = \begin{cases} (1 - \chi(-Tr(\lambda)))q & \textit{if } b = 1; \\ q^{2^b-1} + (-1)^{(q-1)(2^b-v)/4} q^{(2^b+v-2)/2} \varepsilon_{Tr(\lambda)} & \textit{if } b \geq 2 \textit{ and } n+v \textit{ is even}; \\ q^{2^b-1} + (-1)^{(q-1)/2} \cdot \chi\left(-\frac{Tr(\lambda)}{2^{b-1}}\right) q^{(2^b+v-1)/2} \varepsilon'_{Tr(\lambda)} & \textit{if } b \geq 2 \textit{ and } n+v \textit{ is odd,} \end{cases}$$

where $v = \mathrm{gcd}(2^b, i)$ is the dimension of the radical of the bilinear symmetric form associated to Q_i.

The results obtained in Lemma 2.20 and Theorem 2.24 can be used inductively to obtain the following result for extensions of degree n satisfying $\mathrm{gcd}(n, p) = 1$.

Theorem 2.25. *Let b, i, n be integers such that $0 < i < n$, $n = 2^b \tilde{n}$, $\tilde{n} = p_1^{a_1} \cdots p_u^{a_u}$ is the prime factorization of $\tilde{n}$ and $\mathrm{gcd}(\tilde{n}, 2p) = 1$. For $\lambda \in \mathbb{F}_{q^n}$, the number of solutions of*

$Q_i(x) = Tr(\lambda)$ in $\mathbb{F}_{q^n}$ is

$$S_{Tr(\lambda)} = \begin{cases} q^{n-1} + \prod_{j=1}^{u} \left(\frac{q}{p_j}\right)^{\max\{0, \nu_{p_j}(\tilde{n}) - \nu_{p_j}(i)\}} q^{\frac{n+2v_0-2}{2}} \varepsilon_{Tr(\lambda)} & \textit{if } i \textit{ is even and } b = 1; \\ q^{n-1} + (-1)^{(q^{\tilde{n}}-1)(2^b - v_1)/4} q^{\frac{(n-\tilde{n}v_1-2)}{2}} \varepsilon_{Tr(\lambda)} & \textit{if } i \textit{ is even and } b \geq 2; \\ q^{n-1} + \prod_{j=1}^{u} \left(\frac{q}{p_j}\right)^{\max\{0, \nu_{p_j}(n) - \nu_{p_j}(i)\}} q^{\frac{(n+2^b v_0-2)}{2}} \varepsilon'_{Tr(\lambda)} & \textit{if } i \textit{ is odd and } b \geq 2. \end{cases}$$

where $v_0 = \gcd(\tilde{n}, i)$ and $v_1 = \gcd(2^b, i)$.

Proof. By Lemma 2.19 it follows that $v = \gcd(n, i)$. We split the proof in cases.

(i) *If i even and $b = 1$.*

Using the transitivity of the trace function, we obtain

$$\text{Tr}(\lambda) = \text{Tr}(\alpha^{q^i+1} - \alpha^2) = \text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\text{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^2}}(\alpha^{q^i+1} - \alpha^2)), \tag{2.29}$$

where α is such that $Q_i(\alpha) = \text{Tr}(\lambda)$. Let $\mu = \text{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^2}}(\alpha^{q^i+1} - \alpha^2) \in \mathbb{F}_{q^2}$. Then Equation (2.29) is equivalent to the following system of equations,

$$\begin{cases} \text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\mu) = \text{Tr}(\lambda); \\ \text{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^2}}(\alpha^{q^i+1} - \alpha^2) = \mu. \end{cases}$$

Let us define $Q = q^2$, then $Q^{\tilde{n}} = q^n$. Since $b = 1$, by Lemma 2.20 it follows that the number of solutions of $\text{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^2}}(x^{q^i+1} - x^2)) = \mu$ is

$$Q^{\tilde{n}-1} - \prod_{j=1}^{u} \left(\frac{q}{p_j}\right)^{\max\{0, \nu_{p_j}(\tilde{n}) - \nu_{p_j}(i)\}} Q^{\frac{\tilde{n}+v_0-2}{2}}.$$

The dimension of the radical of $\text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(x^{q^i+1} - x^2)$ is $v_0 = \gcd(\tilde{n}, i)$. The number of solutions of $\text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\mu) = \text{Tr}(\lambda)$ is q and then

$$\begin{aligned} S_{\text{Tr}(\lambda)} &= q\left(Q^{\tilde{n}-1} - \prod_{j=1}^{u} \left(\frac{q}{p_j}\right)^{\max\{0, \nu_{p_j}(\tilde{n}) - \nu_{p_j}(i)\}} Q^{\frac{\tilde{n}+v_0-2}{2}}\right) \\ &= q\left(q^{2\tilde{n}-2} - \prod_{j=1}^{u} \left(\frac{q}{p_j}\right)^{\max\{0, \nu_{p_j}(\tilde{n}) - \nu_{p_j}(i)\}} q^{\frac{2\tilde{n}+2v_0-4}{2}}\right) \\ &= q^{n-1} - \prod_{j=1}^{u} \left(\frac{q}{p_j}\right)^{\max\{0, \nu_{p_j}(\tilde{n}) - \nu_{p_j}(i)\}} q^{\frac{n+2v_0-2}{2}}. \end{aligned}$$

(ii) *If i even and* $b \geq 2$.

As above, we have that

$$\mathrm{Tr}(\lambda) = \mathrm{Tr}(\alpha^{q^i+1} - \alpha^2) = \mathrm{Tr}_{\mathbb{F}_{q^{\tilde{n}}}/\mathbb{F}_q}(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^{\tilde{n}}}}(\alpha^{q^i+1} - \alpha^2)), \tag{2.30}$$

where α is such that $Q_i(\alpha) = \mathrm{Tr}(\lambda)$.

In this case, Equation (2.30) is equivalent to the following system of equations:

$$\begin{cases} \mathrm{Tr}_{\mathbb{F}_{q^{\tilde{n}}}/\mathbb{F}_q}(\mu) = \mathrm{Tr}(\lambda); \\ \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^{\tilde{n}}}}(\alpha^{q^i+1} - \alpha^2) = \mu. \end{cases}$$

Set $Q = q^{\tilde{n}}$, hence $Q^{2^b} = q^n$. Since $b \geq 2$, it follows from Lemma 2.24(ii) that the number of solutions of $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^{\tilde{n}}}}(x^{q^i+1} - x^2)) = \mu$ is

$$S_\mu = Q^{2^b-1} - (-1)^{(Q-1)\frac{(2^b-v_1)}{4}} Q^{\frac{(2^b-v_1-2)}{2}},$$

where $v_1 = \gcd(2^b, i)$ is the dimension of the radical of $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^{\tilde{n}}}}(x^{q^i+1} - x^2)$. Besides that, the number of solutions of $\mathrm{Tr}_{\mathbb{F}_{q^{\tilde{n}}}/\mathbb{F}_q}(\mu) = \mathrm{Tr}(\lambda)$ is $q^{\tilde{n}-1}$. Therefore, the number of solutions of $Q_i(x) = \mathrm{Tr}(\lambda)$ is

$$\begin{aligned} q^{\tilde{n}-1}(Q^{2^b-1} - (-1)^{(Q-1)\frac{(2^b-v_1)}{4}} Q^{\frac{(2^b-v_1-2)}{2}}) &= q^{\tilde{n}-1}(q^{n-\tilde{n}} - (-1)^{q^{(\tilde{n}-1)\cdot\frac{(2^b-v_1)}{4}}} q^{\frac{(n-\tilde{n}v_1-2\tilde{n})}{2}}) \\ &= q^{n-1} - (-1)^{q^{(\tilde{n}-1)\frac{(2^b-v_1)}{4}}} q^{\frac{(n-\tilde{n}v_1-2)}{2}}. \end{aligned}$$

(iii) *Case i odd.*

We define $Q = q^{2^b}$; then $Q^{\tilde{n}} = q^n$ and

$$\mathrm{Tr}(\lambda) = \mathrm{Tr}(\alpha^{q^i+1} - \alpha^2) = \mathrm{Tr}_{\mathbb{F}_Q/\mathbb{F}_q}(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_Q}(\alpha^{q^i+1} - \alpha^2)), \tag{2.31}$$

where α is such that $Q_i(\alpha) = \mathrm{Tr}(\lambda)$. It follows that the number of solutions of (2.31) is equal to the number of solutions of the system

$$\begin{cases} \mathrm{Tr}_{\mathbb{F}_Q/\mathbb{F}_q}(\mu) = \mathrm{Tr}(\lambda); \\ \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_Q}(\alpha^{q^i+1} - \alpha^2)) = \mu. \end{cases}$$

By Corollary 2.20 we have that the number of solutions of $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_Q}(x^{q^i+1} - x^2)) = \mu$ with $\mu \neq 0$ is

$$Q^{\tilde{n}-1} - \prod_{j=1}^{u} \left(\frac{q}{p_j}\right)^{\max\{0, \nu_{p_j}(n) - \nu_{p_j}(i)\}} Q^{\frac{(\tilde{n}+v_0-2)}{2}},$$

where $v_0=\gcd(\tilde{n},i)$ is the dimension of the radical of $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_Q}(x^{q^i+1}-x^2)$. Since the number of solutions of $\mathrm{Tr}_{\mathbb{F}_Q/\mathbb{F}_q}(\mu)=\mathrm{Tr}(\lambda)$ is q^{2^b-1}, we conclude that the number of solutions of $Q_i(x)=\mathrm{Tr}(\lambda)$ is

$$\begin{aligned} S_{\mathrm{Tr}(\lambda)} &= q^{2^b-1}\left(Q^{\tilde{n}-1}-\prod_{j=1}^{u}\left(\frac{Q}{p_j}\right)^{\max\{0,\nu_{p_j}(n)-\nu_{p_j}(i)\}}Q^{\frac{(\tilde{n}+v_0-2)}{2}}\right)\\ &= q^{2^b-1}\left(q^{n-2^b}-\prod_{j=1}^{u}\left(\frac{q}{p_j}\right)^{\max\{0,\nu_{p_j}(n)-\nu_{p_j}(i)\}}q^{\frac{(n+2^bv_0-2^{b+1})}{2}}\right)\\ &= q^{n-1}-\prod_{j=1}^{u}\left(\frac{q}{p_j}\right)^{\max\{0,\nu_{p_j}(n)-\nu_{p_j}(i)\}}q^{\frac{(n+2^bv_0-2)}{2}}. \end{aligned}$$

The case $\mathrm{Tr}(\lambda)=0$ follows using the same ideas and the analogous formulas for S_0, for extensions of $\mathbb{F}_q$ of degree power of 2 or odd. ■

Using Lemma 2.20 and Theorem 2.25, we can determine the number of affine rational points of the curve $y^q-y=x^{q^i+1}-x^2-\lambda$, as shown in the following theorem.

Theorem 2.26. *Let i,n be integers such that $0<i<n$. Let $\tilde{n}$ be an integer such that $n=2^b\tilde{n}$, $\gcd(\tilde{n},2p)=1$ and $\tilde{n}=p_1^{a_1}\cdots p_u^{a_u}$ is the prime factorization of $\tilde{n}$. For $\lambda\in\mathbb{F}_{q^n}$ and the curve $\mathscr{C}_i: y^q-y=x(x^{q^i}-x)-\lambda$, we have that*

$$N_n(\mathscr{C}_i)=q^n+Dq^{(n+L)/2}$$

where

(i) $D=\prod_{j=1}^{u}\left(\frac{q}{p_j}\right)^{\max\{0,\nu_{p_j}(i)\}}$, $L=2\gcd(\tilde{n},i)$ *if* $b=1$ *and* i *is even;*

(ii) $D=(-1)^{(q-1)(2^b-\gcd(2^b,i))/4}\varepsilon_{Tr(\lambda)}$, $L=-\tilde{n}\gcd(2^b,i)$ *if* $b\geq 2$ *and* i *is even;*

(iii) $D=\prod_{j=1}^{u}\left(\frac{q}{p_j}\right)^{\max\{0,\nu_{p_j}(n)-\nu_{p_j}(i)\}}\varepsilon'_{Tr(\lambda)}$, $L=2^b\gcd(\tilde{n},i)$ *if* $b=0$ *or* $b\geq 1$ *and* i *is odd.*

Proof. Using (2.3) we know that

$$N_n(\mathscr{C}_i)=qN_n(Q_i).$$

We divide the proof in cases. Set $v_0=\gcd(\tilde{n},i)$ and $v_1=\gcd(2^b,i)$.

- $b=1$ and i is even.

  From Theorem 2.25 we have that

$$N_n(Q_i)=q^{n-1}+\prod_{j=1}^{u}\left(\frac{q}{p_j}\right)^{\max\{0,\nu_{p_j}(i)\}}q^{\frac{n+2v_0-2}{2}}\varepsilon_{\mathrm{Tr}(\lambda)}.$$

Then

$$N_n(\mathscr{C}_i) = q^n + \prod_{j=1}^{u} \left(\frac{q}{p_j}\right)^{\max\{0,\nu_{p_j}(i)\}} q^{\frac{n+2v_0}{2}} \varepsilon_{\mathrm{Tr}(\lambda)}.$$

In this case $L = 2\gcd(\tilde{n}, i)$.

- $b \geq 2$ and i is even. From Theorem 2.25 we have that

  $$N_n(Q_i) = q^{n-1} + (-1)^{(q^{\tilde{n}}-1)(2^b-v_1)/4} q^{\frac{n-\tilde{n}v_1-2}{2}} \varepsilon_{\mathrm{Tr}(\lambda)}.$$

  Therefore,

  $$N_n(\mathscr{C}_i) = q^n + (-1)^{(q^{\tilde{n}}-1)(2^b-v_1)/4} q^{\frac{n-\tilde{n}v_1}{2}} \varepsilon_{\mathrm{Tr}(\lambda)}.$$

  Here $L = -\tilde{n}\gcd(2^b, i)$.

- $b \geq 2$ and i is odd. From Theorem 2.25 we have that

  $$N_n(Q_i) = q^{n-1} + \prod_{j=1}^{u} \left(\frac{q}{p_j}\right)^{\max\{0,\nu_{p_j}(n)-\nu_{p_j}(i)\}} q^{\frac{n+2^b v_0-2}{2}} \varepsilon_{\mathrm{Tr}(\lambda)}.$$

  Consequently

  $$N_n(\mathscr{C}_i) = q^n + \prod_{j=1}^{u} \left(\frac{q}{p_j}\right)^{\max\{0,\nu_{p_j}(n)-\nu_{p_j}(i)\}} q^{\frac{n+2^b v_0}{2}} \varepsilon_{\mathrm{Tr}(\lambda)}.$$

  Here, $L = 2^b \gcd(\tilde{n}, i)$.

- If $b = 0$. Using Lemma 2.20 we have that

  $$N_n(Q_i) = q^{n-1} + \prod_{j=1}^{u} \left(\frac{q}{p_j}\right)^{\max\{0,\nu_{p_j}(n)-\nu_{p_j}(i)\}} q^{\frac{n+v_0-2}{2}} \varepsilon_{\mathrm{Tr}(\lambda)}.$$

  Then

  $$N_n(\mathscr{C}_i) = q^n + \prod_{j=1}^{u} \left(\frac{q}{p_j}\right)^{\max\{0,\nu_{p_j}(n)-\nu_{p_j}(i)\}} q^{\frac{n+v_0}{2}} \varepsilon_{\mathrm{Tr}(\lambda)}.$$

  In this case, $L = \gcd(\tilde{n}, i)$.

$\blacksquare$

2.5 The general case of $\mathbb{F}_{q^n}$-rational points of the curve $y^q - y = x(x^{q^i} - x) - \lambda$, including $\gcd(n,p) = p$

In this section we denote by $\mathscr{C}_i$ the curve

$$\mathscr{C}_i : y^q - y = x(x^{q^i} - x) - \lambda,$$

where $\lambda \in \mathbb{F}_{q^n}$. The number of $\mathbb{F}_{q^n}$-rational points of $\mathscr{C}_i$ is denoted by $N_n(\mathscr{C}_i)$. In Section 2.4 we compute the number $N_n(\mathscr{C}_1)$ when $\gcd(n,p)=1$ and $\lambda \in \mathbb{F}_{q^n}$. In this section we employ a method that allows us to compute the number $N_n(\mathscr{C}_i)$ when p divides n and $\lambda \in \mathbb{F}_{q^n}$.

Let $\mathscr{B} = \{\beta_1, \ldots, \beta_n\}$ be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and

$$B = \begin{pmatrix} \beta_1 & \beta_1^q & \cdots & \beta_1^{q^{n-1}} \\ \beta_2 & \beta_2^q & \cdots & \beta_2^{q^{n-1}} \\ \vdots & \cdots & \ddots & \vdots \\ \beta_n & \beta_n^q & \cdots & \beta_n^{q^{n-1}} \end{pmatrix}. \tag{2.32}$$

We use this matrix as a tool to associate $N_n(\mathscr{C}_i)$ with the number of $\alpha \in \mathbb{F}_{q^n}$ such that

$$\mathrm{Tr}(\alpha(\alpha^{q^i} - \alpha)) = \mathrm{Tr}(\lambda). \tag{2.33}$$

The number of solutions of $\mathrm{Tr}(\alpha(\alpha^{q^i} - \alpha)) = \mathrm{Tr}(\lambda)$ with $\alpha \in \mathbb{F}_{q^n}$ is denoted by $N_n(Q_i)$. From Hilbert's Theorem 90 we have that

$$N_n(\mathscr{C}_i) = qN_n(Q_i).$$

The following proposition associates $\mathrm{Tr}(x^{q^i+1} - x^2 - \lambda)$ with a quadratic form.

Proposition 2.27. *Let $f(x) = x^{q^i+1} - x^2 - \lambda$, where $\lambda \in \mathbb{F}_{q^n}$. The number of solutions of $Tr(f(x)) = 0$ in $\mathbb{F}_{q^n}$ is equal to the number of solutions in $\mathbb{F}_q^n$ of the quadratic form*

$$(x_1\, x_2\, \cdots\, x_n)A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = Tr(\lambda),$$

where $A = (a_{j,l})$ is the $n \times n$ matrix defined by the relations $a_{j,l} = \frac{1}{2}Tr(\beta_j^{q^i}\beta_l + \beta_l^{q^i}\beta_j - 2\beta_j\beta_l)$.

Proof. Let $x = \sum_{j=1}^n \beta_j x_j$. The equation $\mathrm{Tr}(f(x)) = 0$ is equivalent to

$$\sum_{k=0}^{n-1} f(x)^{q^k} = 0. \tag{2.34}$$

We have

$$\begin{aligned}\sum_{k=0}^{n-1} f(x)^{q^k} &= \sum_{k=0}^{n-1} \Big(\sum_{j=1}^n \beta_j x_j\Big)^{q^k} \Big(\sum_{l=1}^n (\beta_l^{q^i} - \beta_l)x_l\Big)^{q^k} - \mathrm{Tr}(\lambda) \\ &= \sum_{j,l=1}^n \Big(\sum_{k=0}^{n-1} \beta_j^{q^k}(\beta_l^{q^{i+k}} - \beta_l^{q^k})\Big)x_j x_l - \mathrm{Tr}(\lambda).\end{aligned}$$

Equation (2.34) implies us that

$$\sum_{j,l=1}^{n}\left(\sum_{k=0}^{n-1}\beta_j^{q^k}(\beta_l^{q^{i+k}}-\beta_l^{q^k})\right)x_jx_l=\mathrm{Tr}(\lambda).$$

Simetrizing this expression, we note that

$$\frac{1}{2}\sum_{k=0}^{n-1}\beta_j^{q^k}\beta_l^{q^k}\left(\beta_l^{q^{i+k}-q^k}+\beta_j^{q^{i+k}-q^k}-2\right)=\frac{1}{2}\mathrm{Tr}\left(\beta_j^{q^i}\beta_l+\beta_l^{q^i}\beta_j-2\beta_j\beta_l\right)=a_{j,l},$$

and the result follows. ■

The matrix A in Proposition 2.27 can be rewritten as

$$A=\frac{1}{2}(A_1+A_2-2A_3),$$

where $A_1=(\mathrm{Tr}(\beta_j^{q^i}\beta_l))_{j,l}$, $A_2=(\mathrm{Tr}(\beta_j\beta_l^{q^i}))_{j,l}$ and $A_3=(\mathrm{Tr}(\beta_j\beta_l))_{j,l}$. Recall that $\mathscr{P}$ is the $n\times n$ cyclic permutation matrix, given by

$$\mathscr{P}=\begin{pmatrix}0&1&0&\cdots&0\\0&0&1&\cdots&0\\\vdots&\cdots&\ddots&\cdots&\vdots\\0&0&0&\cdots&1\\1&0&0&\cdots&0\end{pmatrix}.$$

Since $\mathscr{P}^{-1}=\mathscr{P}^T$, it follows that $A_1=B\left(\mathscr{P}^i\right)^T B^T$, $A_2=B\left(\mathscr{P}^i\right)B^T$ and $A_3=BB^T$. Therefore $A=\frac{1}{2}BM_{n,i}B^T$ where

$$M_{n,i}=\left(\mathscr{P}^i\right)^T-2Id+\mathscr{P}^i,$$

and the matrix $M_{n,i}=(m_{k,l})$ is given by

$$m_{k,l}=\begin{cases}-2 & \text{if } k=l;\\ 1 & \text{if } |k-l|=i;\\ 0 & \text{otherwise,}\end{cases}$$

with the convention that we enumerate the rows and columns of the matrix from 0 to $n-1$, so $0\le k,l\le n-1$.

Since B is invertible, in order to determine the number of solutions of the quadratic form defined by A, it is enough to determine the rank of $M_{n,i}$ and the determinant of a reduced matrix of $M_{n,i}$.

In order to find these invariants of $M_{n,i}$, first we consider the case $i=1$.

2.5.1 The case $i = 1$.

The following proposition determines the rank of $M_{n,1}$ and the determinant of one of its reduced matrix.

Proposition 2.28. *The rank of the $n \times n$ matrix $M_{n,1} = \mathscr{P}^T - 2Id + \mathscr{P}$ over $\mathbb{F}_q$ is given by*

$$rank\ M_{n,1} = \begin{cases} n-1 & \textit{if } \gcd(n,p)=1; \\ n-2 & \textit{if } \gcd(n,p)=p. \end{cases}$$

Let $M'_{n,1}$ denote the principal submatrix of $M_{n,1}$ constructed from the first $rank(M_{n,1})$ rows and columns, then $M'_{n,1}$ is a reduced matrix of $M_{n,1}$ and

$$\det M'_{n,1} = \begin{cases} (-1)^{n-1}n & \textit{if } \gcd(n,p)=1; \\ (-1)^{n-1} & \textit{if } \gcd(n,p)=p. \end{cases}$$

Proof. Let us denote by M_n the matrix

$$M_n = \begin{pmatrix} -2 & 1 & 0 & \dots & 0 & 0 & 0 \\ 1 & -2 & 1 & \dots & 0 & 0 & 0 \\ 0 & 1 & -2 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & -2 & 1 & 0 \\ 0 & 0 & 0 & \dots & 1 & -2 & 1 \\ 0 & 0 & 0 & \dots & 0 & 1 & -2 \end{pmatrix}.$$

We note that $M_{n,1} = M_n + R_n$, where $R_n = (r_{i,j})$ with

$$r_{i,j} = \begin{cases} 1 & \text{if } (i,j) \in \{(1,n),(n,1)\}; \\ 0 & \text{otherwise.} \end{cases}$$

If we put

$$U = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 1 & 1 & 1 & \dots & 1 & 1 \end{pmatrix}$$

then

$$UM_{n,1}U^T = \begin{pmatrix} -2 & 1 & 0 & \dots & 0 & 0 & 0 \\ 1 & -2 & 1 & \dots & 0 & 0 & 0 \\ 0 & 1 & -2 & \dots & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & -2 & 1 & 0 \\ 0 & 0 & 0 & \dots & 1 & -2 & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 \end{pmatrix} = \left(\begin{array}{c|c} M_{n-1} & 0 \\ \hline 0 & 0 \end{array}\right).$$

We claim that $L_{n-1} = \det M_{n-1} = (-1)^{(n-1)}n$ for $n > 1$. In order to prove this, we expand the determinant of M_{n-1} by the first row and obtain the recursive relation

$$L_{n-1} = -2L_{n-2} - L_{n-3} \text{ for all } n \geq 4. \tag{2.35}$$

This implies that the sequence $\{L_n\}_{n\geq 2}$ satisfies a recurrence relation (2.35) with associated characteristic polynomial given by $z^2+2z+1=(z+1)^2$, which has -1 as a double root. Therefore $L_{n-1}=A(-1)^n+B(-1)^n n$, where $A,B\in\mathbb{F}_q$. Since $L_2=3$ and $L_3=-4$, we conclude that $A=0$ e $B=-1$ and consequently $L_{n-1}=(-1)^{(n-1)}n$, as we wanted.

Furthermore, if $\gcd(n,p)=1$, it follows that $L_{n-1}=(-1)^{(n-1)}n\neq 0$ and then the rank of M_{n-1} is $n-1$. This implies that the rank of $M_{n,1}$ is also $n-1$.

In the case $\gcd(n,p)=p$, defining V as

$$V=\begin{pmatrix} 1&0&0&\dots&0&0&0&0\\ 0&1&0&\dots&0&0&0&0\\ \vdots&\vdots&\vdots&\ddots&\vdots&\vdots&\vdots&\vdots\\ 0&0&0&\dots&1&0&0&0\\ 0&0&0&\dots&0&1&0&0\\ 1&2&3&\dots&n-3&\frac{n-4}{2}&-1&0\\ 0&0&0&\dots&0&0&0&1 \end{pmatrix},$$

we observe that V is an invertible matrix and

$$VUM_{n,1}U^TV^T=\left(\begin{array}{c|cc} M_{n-2} & 0 & 0\\ \hline 0\cdots 0 & n & 0\\ 0\cdots 0 & 0 & 0 \end{array}\right).$$

Therefore $L_{n-2}=\det M_{n-2}=(-1)^{n-2}(n-1)\neq 0$ and the rank of $M_{n,1}$ is $n-2$, from where the result follows. ∎

By Theorem 1.32 and Proposition 3.4 we have the following theorem.

Theorem 2.29. *Let $\lambda\in\mathbb{F}_{q^n}$ and n a positive integer. The number $N_n(\mathscr{C}_1)$ of affine rational points in $\mathbb{F}_{q^n}^2$ of the curve $\mathscr{C}_1$ determined by the equation $y^q-y=x^{q+1}-x^2-\lambda$ is*

$$N_n(\mathscr{C}_1)=\begin{cases} q^n+q^{(n+2)/2}\chi(2(-1)^{\frac{n}{2}}nTr(\lambda)) & \textit{if } \gcd(n,p)=1 \textit{ and } n \textit{ is even;}\\ q^n+q^{(n+1)/2}\varepsilon_{Tr(\lambda)}\chi((-1)^{(n-1)/2}n) & \textit{if } \gcd(n,p)=1 \textit{ and } n \textit{ is odd;}\\ q^n+q^{(n+2)/2}\varepsilon_{Tr(\lambda)}\chi((-1)^{n/2}) & \textit{if } \gcd(n,p)=p \textit{ and } n \textit{ is even;}\\ q^n+q^{(n+3)/2}\chi(2(-1)^{\frac{n-3}{2}}Tr(\lambda)) & \textit{if } \gcd(n,p)=p \textit{ and } n \textit{ is odd.} \end{cases}$$

This theorem allows us to determine when $\mathscr{C}_1$ is minimal or maximal with respect the Hasse-Weil bound, as we show in the following corollary.

Theorem 2.30. *Consider the curve $\mathscr{C}_1$ given by*

$$\mathscr{C}_1: y^q-y=x^{q+1}-x^2-\lambda.$$

Then $\mathscr{C}_1$ is minimal if and only if $Tr(\lambda)=0$ and one of the following holds

- *$2p$ divides n and $q \equiv 1 \pmod 4$;*

- *$4p$ divides n and $q \equiv 3 \pmod 4$.*

Moreover, $\mathscr{C}_1$ is maximal if and only if $Tr(\lambda) = 0$, $2p$ divides n, 4 does not divide n and $q \equiv 3 \pmod 4$.

Proof. The result follows from Theorem 2.29 and the fact that the genus of $\mathscr{C}_1$ is $g = \frac{q(q-1)}{2}$. ■

2.5.2 The curve $y^q - y = x(x^{q^i} - x) - \lambda$ with $i \geq 1$.

Proposition 2.31. *Let i, n be integers such that $0 < i < n$. Set $d = \gcd(i,n)$ and $l = \frac{n}{d}$. The rank of the $n \times n$ matrix $M_{n,i}$ is i if $n = 2i$ and, otherwise, we have that*

$$rank\ M_{n,i} = \begin{cases} n-d & \textit{if } \gcd(n,p) = 1; \\ n-2d & \textit{if } \gcd(n,p) = p. \end{cases}$$

In addition, the matrices

$$(2.36) \quad \tilde{M}_{n,i} = \left(\begin{array}{c|c|c|c} M_{l,1} & 0 & 0 & 0 \\ \hline 0 & M_{l,1} & 0 & 0 \\ \hline \vdots & \cdots & \ddots & \vdots \\ \hline 0 & 0 & 0 & M_{l,1} \end{array}\right) \quad \textit{and} \quad \tilde{M}'_{n,i} = \left(\begin{array}{c|c|c|c} M'_{l,1} & 0 & 0 & 0 \\ \hline 0 & M'_{l,1} & 0 & 0 \\ \hline \vdots & \cdots & \ddots & \vdots \\ \hline 0 & 0 & 0 & M'_{l,1} \end{array}\right)$$

are an equivalent matrix and a reduced matrix of $M_{n,i}$, respectively, where $\tilde{M}'_{l,1}$ is as the matrix given in Proposition 2.28.

The determinant of the matrix $\tilde{M}_{n,i}$ is $(-1)^i 2^i$ if $n = 2i$ and, otherwise we have that

$$\det \tilde{M}'_{n,i} = \begin{cases} (-1)^{n-d} l^d & \textit{if } \gcd(n,p) = 1; \\ (-1)^{n-2d}(l-1)^d & \textit{if } \gcd(n,p) = p. \end{cases}$$

Proof. For convenience, we enumerate the rows and columns of the matrix $M_{n,i}$ from 0 to $n-1$. Suppose that n is even and $i = \frac{n}{2}$. In this case, the matrix $M_{n,i}$ is given by

$$a_{k,l} = \begin{cases} -2 & \text{if } k = l, \\ 2 & \text{if } k - l \equiv 0 \pmod i, \\ 0 & \text{otherwise.} \end{cases}$$

Let us denote $D_{n/2} = 2Id_{n/2}$, where $Id_{n/2}$ is the $\frac{n}{2} \times \frac{n}{2}$ identity matrix. We have that

$$M_{n,n/2} = \left(\begin{array}{c|c} -D_{n/2} & D_{n/2} \\ \hline D_{n/2} & -D_{n/2} \end{array}\right),$$

that is equivalent to

$$\left(\begin{array}{c|c} D_{n/2} & 0 \\ \hline 0 & 0 \end{array}\right).$$

Therefore,

$$\operatorname{rank} M_{n,\frac{n}{2}} = \frac{n}{2} = i \quad \text{and} \quad \det \tilde{M}'_{n,\frac{n}{2}} = (-2)^{\frac{n}{2}} = (-2)^i \neq 0.$$

This proves the case $n = 2i$. For the other cases, first we show that it is enough to consider the case where $i = d$. After that, we obtain a block diagonal matrix composed by d matrices of the form $M_{l,1}$, where $n = ld$.

We observe that any permutation $\rho : \mathbb{Z}_n \to \mathbb{Z}_n$ defines a natural action over $\mathbb{F}_q^n$, given by the following map

$$\begin{array}{rccc} \rho: & \mathbb{F}_q^n & \to & \mathbb{F}_q^n \\ & (v_0,\ldots,v_{n-1}) & \mapsto & (v_{\rho(0)},\ldots,v_{\rho(n-1)}). \end{array}$$

This action is associated to an invertible matrix M_ρ such that

$$M_\rho \begin{pmatrix} v_0 \\ \vdots \\ v_{n-1} \end{pmatrix} = \begin{pmatrix} v_{\rho(0)} \\ \vdots \\ v_{\rho(n-1)}. \end{pmatrix}$$

Conversely, for any permutation matrix R, there exists a permutation $\rho' : \mathbb{Z}_n \to \mathbb{Z}_n$ such that $M_{\rho'} = R$. We observe that $\mathscr{P}^i$ determines the permutation

$$\begin{array}{rccc} \pi_i: & \mathbb{Z}_n & \to & \mathbb{Z}_n \\ & z & \mapsto & z+i. \end{array}$$

Let us consider the map

$$\sigma : \mathbb{Z}_n \to \mathbb{Z}_n$$
$$a \mapsto ai$$

where $a \in \mathbb{Z}_n$ is an element of $\mathbb{Z}_n$ satisfying that $\gcd(a,n) = 1$. Since a and n are relatively prime, σ is a permutation. In addition, σ induces a matrix M_σ and the matrix $M_\sigma \mathscr{P}^i M_\sigma^{-1}$

determines a permutation of $\mathbb{Z}_n$ given by

$$\begin{aligned}\sigma\circ\pi_i\circ\sigma^{-1}(z) &= \sigma(\pi_i(\sigma^{-1}(z)))\\ &= \sigma(\pi_i(a^{-1}z))\\ &= \sigma(a^{-1}z+i)\\ &= z+ai.\end{aligned}$$

We know that the congruence $ai \equiv u \pmod n$ has a solution if d divides u. In particular, since $d = \gcd(i,n)$, there exists $a \in \mathbb{Z}_n$ such that $\sigma\circ\pi_i\circ\sigma^{-1}(z) = z+\gcd(i,n)$. This shows that, without loss of generality, we can replace i by d.

For each $z \in [0,n-1]$, there exist unique integers r,s with $0 \le s \le l-1$ and $0 \le r \le d-1$ such that $z = sd+r$. Let us consider the map

$$\begin{array}{cccc}\varphi: & \mathbb{Z}_n & \to & \mathbb{Z}_n\\ & sd+r & \mapsto & s+lr.\end{array} \tag{2.37}$$

Claim: The map φ is a permutation of the elements of $\mathbb{Z}_n$. Let us suppose, that there exist distinct elements $z_1,z_2 \in \mathbb{Z}_n$ such $\varphi(z_1)=\varphi(z_2)$. By the Euclidean Division, there exist $0 \le s_1,s_2 \le l-1$ and $0 \le r_1,r_2 \le d-1$ with $z_1 = s_1d+r_1$ and $z_2 = s_2d+r_2$. Then

$$\varphi(s_1d+r_1)=\varphi(s_2d+r_2) \Leftrightarrow s_1+lr_1 = s_2+lr_2 \Leftrightarrow s_1-s_2 = l(r_2-r_1).$$

Since $0 \le s_1,s_2 \le l-1$, the latter implies that $s_1=s_2=0$ and $r_1=r_2=0$. But this contradicts the fact that $z_1 \neq z_2$. Therefore φ is a permutation.

We will use φ to permutate the rows and columns of $\mathscr{P}^d - 2Id + \left(\mathscr{P}^d\right)^T$ in order to obtain the diagonal blocks matrix $\tilde{M}_{n,i}$ with d blocks. We recall that, the matrix $\left(\mathscr{P}^d\right)^T - 2Id + \mathscr{P}^d$ is given by

$$a_{k,j} = \begin{cases} -2 & \text{if } k=j;\\ 1 & \text{if } |k-j| = d;\\ 0 & \text{otherwise.}\end{cases}$$

We obtain that $\varphi\circ\pi_d\circ\varphi^{-1}$ defines a permutation $\theta:\mathbb{Z}_n\to\mathbb{Z}_n$ given by

$$\begin{aligned}\theta(z) = \varphi\circ\pi_d\circ\varphi^{-1}(z) &= \varphi\circ\pi_d(\varphi^{-1}(s+rl))\\ &= \varphi\circ\pi_d(sd+r)\\ &= \varphi((s+1)d+r)\\ &= (s+1)+rl,\end{aligned}$$

where $z = sl + r$ with $0 \le s \le l-1$ and $0 \le r \le d-1$. We claim that

$$M_\varphi\left(\left(\mathscr{P}^d\right)^T - 2Id + \mathscr{P}^d\right)M_\varphi^{-1} = \tilde{M}_{n,d}.$$

In order to do this, we show that the product of the permutation matrix M_φ, M_φ^{-1} and $\left((\mathscr{P}^d)^T - 2Id + \mathscr{P}^d\right)$ takes the non-null entries of $M_{n,d}$ in the non-null entries of $\tilde{M}_{n,d}$. In the case $k = j$, writing $k = s + rl$ with $0 \le s \le l-1$ and $0 \le r \le d-1$, we have that

$$\theta(a_{k,k}) = a_{(s+1)+rl,(s+1)+rl} = a_{\theta(k),\theta(k)},$$

and this implies that the new matrix until have $a_{k,k} = -2$.

If $a_{k,k+d} = 1$, $k = s + rl$ with $0 \le s \le l-1$ and $0 \le r \le d-1$, we have that

$$\theta(a_{k,k+d}) = a_{(s+1)+rl,(s+2)+rl} = a_{\theta(k),\theta(k+d)},$$

therefore we have $a_{k,k+1} = 1$ viewing the indices modulo l. For $a_{k+d,k} = 1$ is the same, using the fact that $a_{k+d,k}$ is the entries transpose of $a_{k,k+d}$. The other entries are null, and their images are also null. Therefore, we obtain the matrix in Equation (2.36).

Using Proposition 2.28 and the fact that the matrix $M_{n,i}$ is a block diagonal matrix with d blocks equal to the matrix $M_{l,1}$, we determine the rank of $M_{n,i}$ and the determinant of the reduced matrix $\tilde{M}'_{n,i}$ of $M_{n,i}$. Consequently

$$\operatorname{rank} M_{n,i} = \begin{cases} (l-1)d = n-d & \text{if } \gcd(n,p) = 1, \\ (l-2)d = n-2d & \text{if } \gcd(n,p) = p, \end{cases}$$

and

$$\det \tilde{M}_{n,i} = \begin{cases} \left((-1)^{l-1}l\right)^d = (-1)^{n-d}l^d & \text{if } \gcd(n,p) = 1, \\ \left((-1)^{l-1}(l-1)\right)^d = (-1)^{n-2d}(l-1)^d & \text{if } \gcd(n,p) = p. \end{cases}$$

■

From Proposition 2.27, the matrix associated to the quadratic form $\operatorname{Tr}(cx(x^{q^i} - x))$ is

$$A = \frac{c}{2}B(\mathscr{P}^T - 2Id + \mathscr{P})B^T,$$

where B is given in Equation (2.32). Proposition 2.31 implies the following result.

Corollary 2.32. *Let $c \in \mathbb{F}_q^*$ and let i be an integer such that $0 < i < n$. Set $d = \gcd(i,n)$ and $l = \frac{n}{d}$. The rank of the $n \times n$ matrix $A = \frac{c}{2}B((\mathscr{P}^i)^T - 2Id + \mathscr{P}^i)B^T$ is given by*

$$\mathit{rank}\ A = \begin{cases} n-d & \mathit{if}\ \gcd(n,p) = 1, \\ n-2d & \mathit{if}\ \gcd(n,p) = p. \end{cases}$$

Let A' be a reduced matrix of A. Then

$$\chi(\det(A')) = \begin{cases} \chi((-2c)^{n-d} l^d) & \text{if } \gcd(n,p) = 1, \\ \chi((-2c)^{n-d}(l-1)^d) & \text{if } \gcd(n,p) = p. \end{cases}$$

By Theorem 1.32 and Propositions 2.27 and 2.31 we have the following theorem.

Theorem 2.33. *Let n,i be integers such that $0 < i < n$ and put $d = \gcd(i,n)$ and $l = \frac{n}{d}$. If $n = 2i$, the number $N_n(\mathscr{C}_i)$ of affine rational points in $\mathbb{F}_{q^n}^2$ of the curve determined by the equation $y^q - y = x^{q^i+1} - x^2 - \lambda$ is*

$$N_n(\mathscr{C}_i) = \begin{cases} q^n + q^{(3i+1)/2}\chi((-1)^{(i+1)/2} Tr(\lambda)) & \text{if } i \text{ is odd,} \\ q^n + q^{3i/2}\varepsilon_{Tr(\lambda)}\chi((-1)^{i/2}) & \text{if } i \text{ is even.} \end{cases}$$

If $n \neq 2i$, the number of affine rational points of $\mathscr{C}_i$ is

$$N_n(\mathscr{C}_i) = \begin{cases} q^n + \chi(2(-1)^{(n-d+1)/2} Tr(\lambda) l^d) q^{(n+d+1)/2} & \text{if } \gcd(n,p) = 1 \text{ and } n+d \text{ is odd,} \\ q^n + \varepsilon_{Tr(\lambda)}\chi((-1)^{(n-d)/2} l^d) q^{(n+d)/2} & \text{if } \gcd(n,p) = 1 \text{ and } n+d \text{ is even,} \\ q^n + \chi(2(-1)^{(n+1)/2} Tr(\lambda)(l-1)^d) q^{(n+2d+1)/2} & \text{if } \gcd(n,p) = p \text{ and } n \text{ is odd,} \\ q^n + \varepsilon_{Tr(\lambda)}\chi((-1)^{n/2}(l-1)^d) q^{(n+2d)/2} & \text{if } \gcd(n,p) = p \text{ and } n \text{ is even.} \end{cases}$$

Remark 2.34. *The curve $\mathscr{C}_i$ has genus $g = \frac{(q-1)q^i}{2}$. The Hasse-Weil bound of $\mathscr{C}_i$ is given by*

$$|N_n(\mathscr{C}_i) - q^n| \leq (q-1)q^{\frac{n+2i}{2}}.$$

Using Theorem 2.33, we can determine the conditions when the curve $\mathscr{C}_i$ is maximal (or minimal) with respect the Hasse-Weil bound.

Theorem 2.35. *Let n,i be integers such that $0 < i < n$, set $d = \gcd(i,n)$ and $l = \frac{n}{d}$.*

The curve

$$\mathscr{C}_i : y^q - y = x(x^{q^i} - x) - \lambda$$

is $\mathbb{F}_{q^n}$-maximal if and only if

- *$Tr(\lambda) = 0$, $2p$ divides n, i divides n and $(-1)^{n/2}(l-1)^d$ is a square in $\mathbb{F}_q$.*

The curve $\mathscr{C}_i$ is $\mathbb{F}_{q^n}$-minimal if and only if

- *$Tr(\lambda) = 0$, $2p$ divides n, i divides n and $(-1)^{n/2}(l-1)^d$ is not a square in $\mathbb{F}_q$.*

2.6 The number of affine rational points of the hypersufarce $y^q - y = \sum_{j=1}^r a_j x_j(x_j^{q^{i_j}} - x_j) - \lambda$

Let us denote by $\mathscr{H}_r$ the hypersufarce

$$\mathscr{H}_r : y^q - y = \sum_{j=1}^{r} a_j x_j(x_j^{q^{i_j}} - x_j) - \lambda,$$

where $a_j \in \mathbb{F}_q^*$ and $0 < i_j < n$ for $j \in \{1,\dots,r\}$. Let ψ and $\tilde{\psi}$ denote the canonical additive characters of $\mathbb{F}_{q^n}$ and $\mathbb{F}_q$, respectively. We know from Lemma 1.22 that

$$\sum_{c\in\mathbb{F}_{q^n}} \psi(uc) = \begin{cases} 0 & \text{if } u \neq 0; \\ q^n & \text{if } u = 0. \end{cases}$$

We can use this fact to compute the number $N_n(\mathscr{H}_r)$,

$$\begin{aligned} q^n N_n(\mathscr{H}_r) &= \sum_{c\in\mathbb{F}_{q^n}} \sum_{x_1\in\mathbb{F}_{q^n}} \cdots \sum_{x_r\in\mathbb{F}_{q^n}} \sum_{y\in\mathbb{F}_{q^n}} \psi\left(c\left(\sum_{j=1}^{r} a_j x_j(x_j^{q^{i_j}} - x_j) - y^q + y - \lambda\right)\right) \\ &= q^{(r+1)n} + \sum_{c\in\mathbb{F}_{q^n}^*} \sum_{x_1\in\mathbb{F}_{q^n}} \cdots \sum_{x_r\in\mathbb{F}_{q^n}} \psi\left(c\left(\sum_{i=1}^{r} a_j x_j(x_j^{q^{i_j}} - x_j) - \lambda\right)\right) \sum_{y\in\mathbb{F}_{q^n}} \psi\left(c\left(-y^q + y\right)\right) \\ &= q^{(r+1)n} + \sum_{c\in\mathbb{F}_{q^n}^*} \psi(-c\lambda) \prod_{j=1}^{r} \sum_{x_j\in\mathbb{F}_{q^n}} \psi\left(c\left(a_j x_j(x_j^{q^{i_j}} - x_j)\right)\right) \sum_{y\in\mathbb{F}_{q^n}} \psi\left(c\left(-y^q + y\right)\right) \\ &= q^{(r+1)n} + \sum_{c\in\mathbb{F}_{q^n}^*} \psi(-c\lambda) \prod_{j=1}^{r} \sum_{x_j\in\mathbb{F}_{q^n}} \psi\left(c\left(a_j x_j(x_j^{q^{i_j}} - x_j)\right)\right) \sum_{y\in\mathbb{F}_{q^n}} \psi\left(y\left(-c^{q^{n-1}} + c\right)\right). \end{aligned}$$

(2.38)

We observe that

$$\sum_{y\in\mathbb{F}_{q^n}} \psi\left(y\left(-c^{q^{n-1}} + c\right)\right) = \begin{cases} q^n & \text{if } c^{q^{n-1}} - c = 0; \\ 0 & \text{otherwise.} \end{cases}$$

Since $c^{q^{n-1}} - c = 0$ if and only if $c \in \mathbb{F}_{q^{n-1}}$, we conclude that the inner sum in (2.38) has non null terms if and only if $c \in \mathbb{F}_q$. In this case, $\psi(-c\lambda) = \tilde{\psi}(-c\mathrm{Tr}(\lambda))$ and then

$$N_n(\mathscr{H}_r) = q^{rn} + \sum_{c\in\mathbb{F}_q^*} \tilde{\psi}(-c\mathrm{Tr}(\lambda)) \prod_{j=1}^{r} \left(\sum_{x_j\in\mathbb{F}_{q^n}} \psi\left(ca\left(x_j(x_j^{q^{i_j}} - x_j)\right)\right)\right). \tag{2.39}$$

The following theorem gives explicit formulas for $N_n(\mathscr{H}_r)$.

Theorem 2.36. *Let $\mathscr{H}_r : y^q - y = \sum_{j=1}^{r} a_j x_j (x_j^{q^{i_j}} - x_j) - \lambda$ with $\lambda \in \mathbb{F}_{q^n}$, $a_j \in \mathbb{F}_q^*$ and $0 < i_j < n$. We denote*

- $d_j = \gcd(i_j, n)$, $D = \sum\limits_{j=1}^{r} d_j$,
- $l_j = \frac{n}{d_j}$, $L_1 = l_1^{d_1} \cdots l_r^{d_r}$, $L_2 = (l_1 - 1)^{d_1} \cdots (l_r - 1)^{d_r}$,
- $A_1 = a_1 \cdots a_r$, $A_2 = a_1^{d_1} \cdots a_r^{d_r}$.

The number $N_n(\mathscr{H}_r)$ of affine rational points of $\mathscr{H}_r$ in $\mathbb{F}_{q^n}^{r+1}$ is

$$N_n(\mathscr{H}_r) = \begin{cases} q^{rn} + \tau^{s(nr-D)} \varepsilon_{Tr(\lambda)} \chi(A_1^{nr} A_2^{-1} L_1) q^{\frac{nr+D}{2}} & \textit{if } \gcd(n,p) = 1, nr - D \textit{ is even}, \\ q^{rn} + \tau^{s(rn-D+1)} \chi(2Tr(\lambda) A_1^{nr} A_2^{-1} L_1) q^{\frac{nr+D+1}{2}} & \textit{if } \gcd(n,p) = 1, nr - D \textit{ is odd}, \\ q^{rn} + \tau^{s(rn-2D)} \varepsilon_{Tr(\lambda)} \chi(L_2) q^{\frac{nr+2D}{2}} & \textit{if } \gcd(n,p) = p, nr \textit{ is even}; \\ q^{rn} + \tau^{s(rn-2D+1)} \chi(2Tr(\lambda) A_1 L_2) q^{\frac{nr+2D+1}{2}} & \textit{if } \gcd(n,p) = p, nr \textit{ is odd}. \end{cases}$$

Proof. From Equation (2.39) we have that

$$N_n(\mathscr{H}_r) = q^{rn} + \sum_{c \in \mathbb{F}_q^*} \tilde{\psi}(-c\mathrm{Tr}(\lambda)) \prod_{j=1}^{r} \left(\sum_{x_j \in \mathbb{F}_{q^n}} \psi \left(c a_j \left(x_j (x_j^{q^{i_j}} - x_j) \right) \right) \right).$$

By Lemma 1.33 and Proposition 2.32, we obtain that $N_n(\mathscr{H}_r) = q^{rn} + N_{\mathscr{H}_r}$ where

$$N_{\mathscr{H}_r} = \begin{cases} \sum\limits_{c \in \mathbb{F}_q^*} \tilde{\psi}(-c\mathrm{Tr}(\lambda)) \prod\limits_{j=1}^{r} \left((-1)^{(s+1)(n-d_j)} \tau^{s(n-d_j)} \chi \left((-2ca_j)^{(n-d_j)} l_j^{d_j} \right) q^{\frac{n+d_j}{2}} \right) & \text{if } \gcd(n,p) = 1, \\ \sum\limits_{c \in \mathbb{F}_q^*} \tilde{\psi}(-c\mathrm{Tr}(\lambda)) \prod\limits_{j=1}^{r} \left((-1)^{(s+1)(n-2d_j)} \tau^{s(n-2d_j)} \chi \left((-2ca_j)^{(n-2d_j)} (l_j - 1)^{d_j} \right) q^{\frac{n+2d_j}{2}} \right) & \text{if } \gcd(n,p) = p. \end{cases}$$

Hence

$$N_{\mathscr{H}_r} = \begin{cases} (-1)^{(s+1)(rn-D)} \tau^{s(nr-D)} \sum\limits_{c \in \mathbb{F}_q^*} \tilde{\psi}(-c\mathrm{Tr}(\lambda)) \chi \left((-2c)^{nr-D} A_1^{nr} A_2^{-1} L_1 \right) q^{\frac{nr+D}{2}} & \text{if } \gcd(n,p) = 1, \\ (-1)^{rn(s+1)} \tau^{s(rn-2D)} \sum\limits_{c \in \mathbb{F}_q^*} \tilde{\psi}(-c\mathrm{Tr}(\lambda)) \chi \left((-2c)^{nr} A_1^{nr} A_2^{-2} L_2 \right) q^{\frac{nr+2D}{2}} & \text{if } \gcd(n,p) = p. \end{cases}$$

We split the proof into the following cases. We use Theorem 1.28 and that fact that χ is the quadratic character.

1) $\gcd(n,p)=1$ and $nr-D$ is even.

$$\begin{aligned} N_{\mathscr{H}_r} &= \tau^{s(nr-D)} q^{\frac{(nr+D)}{2}} \chi(A_1^{nr}A_2^{-1}L_1) \sum_{c\in\mathbb{F}_q^*} \tilde{\psi}(-c\mathrm{Tr}(\lambda)) \\ &= \tau^{s(nr-D)} \varepsilon_{\mathrm{Tr}(\lambda)} \chi(A_1^{nr}A_2^{-1}L_1) q^{\frac{nr+D}{2}}. \end{aligned}$$

2) $\gcd(n,p)=1$ and $nr-D$ is odd.

$$\begin{aligned} N_{\mathscr{H}_r} &= (-1)^{(s+1)} \tau^{s(rn-D)} \chi(A_1^{nr}A_2^{-1}L_1) q^{\frac{nr+D}{2}} \sum_{c\in\mathbb{F}_q^*} \tilde{\psi}(-c\mathrm{Tr}(\lambda))\chi(-2c) \\ &= \begin{cases} (-1)^{(s+1)} \tau^{s(rn-D)} \chi(A_1^{nr}A_2^{-1}L_1) q^{\frac{nr+D}{2}} \displaystyle\sum_{c\in\mathbb{F}_q^*} \chi(-2c) & \text{if } \mathrm{Tr}(\lambda)=0; \\ (-1)^{(s+1)} \tau^{s(rn-D)} q^{\frac{nr+D}{2}} \chi(2\mathrm{Tr}(\lambda)A_1^{nr}A_2^{-1}L_1) \displaystyle\sum_{c\in\mathbb{F}_q^*} \tilde{\psi}(-c\mathrm{Tr}(\lambda))\chi(-c\mathrm{Tr}(\lambda)) & \text{if } \mathrm{Tr}(\lambda)\neq 0; \end{cases} \\ &= \begin{cases} 0 & \text{if } \mathrm{Tr}(\lambda)=0; \\ (-1)^{(s+1)} \tau^{s(rn-D)} q^{\frac{nr+D}{2}} \chi(2\mathrm{Tr}(\lambda)A_1^{nr}A_2^{-1}L_1) G(\tilde{\psi},\chi) & \text{if } \mathrm{Tr}(\lambda)\neq 0; \end{cases} \\ &= \tau^{s(rn-D+1)} \chi(2\mathrm{Tr}(\lambda)A_1^{nr}A_2^{-1}L_1) q^{\frac{nr+D+1}{2}}. \end{aligned}$$

3) $\gcd(n,p)=p$ and nr is even.

$$\begin{aligned} N_{\mathscr{H}_r} &= \tau^{s(rn-2D)} \chi(A_1^{nr}L_2) q^{\frac{nr+2D}{2}} \sum_{c\in\mathbb{F}_q^*} \tilde{\psi}(-c\mathrm{Tr}(\lambda)) \\ &= \tau^{s(rn-2D)} \varepsilon_{\mathrm{Tr}(\lambda)} \chi(L_2) q^{\frac{nr+2D}{2}}. \end{aligned}$$

4) $\gcd(n,p)=p$ and nr is odd.

$$\begin{aligned} N_{\mathscr{H}_r} &= (-1)^{s+1} \tau^{s(rn-2D)} \chi(A_1L_2) q^{\frac{(nr+2D)}{2}} \sum_{c\in\mathbb{F}_q^*} \tilde{\psi}(-c\mathrm{Tr}(\lambda))\chi((-2c) \\ &= \begin{cases} (-1)^{s+1} \tau^{s(rn-2D)} \chi(A_1L_2) q^{\frac{nr+2D}{2}} \displaystyle\sum_{c\in\mathbb{F}_q^*} \chi(-2c) & \text{if } \mathrm{Tr}(\lambda)=0; \\ (-1)^{s+1} \tau^{s(rn-2D)} \chi(2\mathrm{Tr}(\lambda)A_1L_2) q^{\frac{nr+2D}{2}} \displaystyle\sum_{c\in\mathbb{F}_q^*} \tilde{\psi}(-c\mathrm{Tr}(\lambda))\chi((-c\mathrm{Tr}(\lambda)) & \text{if } \mathrm{Tr}(\lambda)\neq 0; \end{cases} \\ &= \begin{cases} 0 & \text{if } \mathrm{Tr}(\lambda)=0; \\ (-1)^{s+1} \tau^{s(rn-2D)} q^{\frac{nr+2D}{2}} \chi(2\mathrm{Tr}(\lambda)A_1L_2) G(\tilde{\psi},\chi) & \text{if } \mathrm{Tr}(\lambda)\neq 0; \end{cases} \\ &= \tau^{s(rn-2D+1)} \chi(2\mathrm{Tr}(\lambda)A_1L_2) q^{\frac{nr+2D+1}{2}}. \end{aligned}$$

This assures us the result of the theorem. ■

The well-known Weil bound tells us that

$$\left|N_n(\mathscr{H}_r) - q^{nr}\right| \le (q-1)\prod_{j=1}^{r} q^{i_j} q^{nr/2} = (q-1)q^{\frac{rn+2I}{2}},$$

where $I = \sum_{j=1}^{r} i_j$. By Theorem 2.36 this bound can be attained if and only if we are in the case $\gcd(n,p) = p, nr$ is even and $\mathrm{Tr}(\lambda) = 0$. Using this fact, we obtain the following theorem, that gives us conditions assuring that the hypersurface $\mathscr{H}_r$ is maximal or minimal.

Theorem 2.37. *Let $\mathscr{H}_r : y^q - y = \sum_{j=1}^{r} a_j x_j(x_j^{q^{i_j}} - x_j) - \lambda$ with $\lambda \in \mathbb{F}_{q^n}$, $a_j \in \mathbb{F}_q$ and $0 < i_j < n$. Let $d_j = \gcd(n, i_j)$, $D = \sum_{j=1}^{r} d_j$, $l_j = \frac{n}{d_j}$ for $1 \le j \le r$ and $L_2 = (l_1 - 1)^{d_1} \cdots (l_r - 1)^{d_r}$.*

The hypersurface $\mathscr{H}_r$ attains the upper Weil bound if and only if one of the following holds

- *$Tr(\lambda) = 0$, $\gcd(n,p) = p$, nr is even, $d_j = i_j$ for all $1 \le j \le r$, $(nr - 2D)s \equiv 0 \pmod 4$ and $\chi(L_2) = 1$;*
- *$Tr(\lambda) = 0$, $\gcd(n,p) = p$, nr is even, $d_j = i_j$ for all $1 \le j \le r$, $(nr - 2D)s \equiv 2 \pmod 4$ and $\chi(L_2) = -1$.*

The hypersurface $\mathscr{H}_r$ attains the lower bound if and only if one of the following holds

- *$Tr(\lambda) = 0$, $\gcd(n,p) = p$, nr is even, $d_j = i_j$ for all $1 \le j \le r$, $(nr - 2D)s \equiv 2 \pmod 4$ and $\chi(L_2) = 1$;*
- *$Tr(\lambda) = 0$, $\gcd(n,p) = p$, nr is even, $d_j = i_j$ for all $1 \le j \le r$, $(nr - 2D)s \equiv 0 \pmod 4$ and $\chi(L_2) = -1$.*

Example 2.38. *Let $q = 5^2$ and $n = 60$. We consider the Artin-Schreier hypersurface given by*

$$\mathscr{H} : y^q - y = x_1(x_1^{q^3} - x_1) + x_2(x_2^{q^4} - x_2) + x_3(x_3^{q^6} - x_3).$$

With the notation of Theorem 2.37, we have that $i_1 = d_1 = 3, i_2 = d_2 = 4, i_3 = d_3 = 6$, $l_1 = 20, l_2 = 15, l_3 = 10$ and $L_2 = 19^3 \cdot 15^4 \cdot 10^6$. Moreover, $\chi(L_2) = \chi(19) = 1$ and $(nr - 2D)s \equiv (180 - 26) \cdot 2 \equiv 0 \pmod 4$. It follows from Theorem 2.37 that $\mathscr{H}$ is $\mathbb{F}_{q^{60}}$-maximal .

CHAPTER 3

THE NUMBER OF RATIONAL POINTS OF A CLASS OF SUPERELLIPTIC CURVES

In this chapter, we study the number of $\mathbb{F}_{q^n}$-rational points on the affine curve $\mathscr{X}_{d,a,b}$ given by the equation

$$y^d = ax\mathrm{Tr}(x)+b,$$

where Tr denote the trace function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ and d is a positive integer. In particular, we present bounds for the number of $\mathbb{F}_{q^n}$-rational points and, for the cases where d satisfies a natural condition, explicit formulas for the number of rational points are obtained. In particular, a complete characterization is given for the case $d = 2$. As a consequence of our results, we compute the number of elements α in $\mathbb{F}_{q^n}$ such that α and $\mathrm{Tr}(\alpha)$ are quadratic residues in $\mathbb{F}_{q^n}$.

3.1 Introduction

Let $\mathbb{F}_{q^n}$ be a finite field with q^n elements, where $q = p^s$ and p is an odd prime. Throughout this chapter, $\mathrm{Tr}(x)$ denotes the trace function from $\mathbb{F}_{q^n}$ into $\mathbb{F}_q$. The study of the number and existence of special elements in finite fields dates back to the 1950s(Carlitz works). The famous *Primitive Normal Basis Theorem* was firstly proved by Lenstra and Schoof [29] in 1987.

More recently, sophisticated techniques have been created and employed in different problems regarding elements that satisfy special conditions (for example, see [1, 12, 13, 22]).

A problem that naturally arises is to find the number of elements $\alpha \in \mathbb{F}_{q^n}$ such that α and $\mathrm{Tr}(\alpha)$ are both quadratic residues in $\mathbb{F}_{q^n}$. This problem is easily solved in the case where n is even, since any element in $\mathbb{F}_q$ is a quadratic residue, so that, in particular, $\mathrm{Tr}(\alpha)$ does so. This problem gets more interesting for the case where n is odd. Heuristically, $q/4$ elements in $\mathbb{F}_q$ must satisfy these two conditions, but there is no result in the literature addressing this problem. In both cases, such number of special elements is closely related to the number of $\mathbb{F}_{q^n}$-rational points on the affine curve $y^2 = x\mathrm{Tr}(x)$ (see the proof of Theorem 3.14). In this chapter, we study a broader class of affine curves given by

$$\mathscr{X}_{d,a,b} : y^d = ax\mathrm{Tr}(x) + b,$$

where $a, b \in \mathbb{F}_{q^n}$ and d is a positive integer. The curve $\mathscr{X}_{d,a,b}$ belongs to a wide family of curves called *superelliptic* curves, whose points are given by the solutions of the equation

$$y^d = f(x). \tag{3.1}$$

There are some results in the literature regarding general superelliptic curves. For example, in [20] the authors give the distribution of points on smooth superelliptic curves over a finite field, when their degree goes to infinity. In [26] the authors describe the fluctuation in the number of points on a hyperelliptic curve, which are special class of superelliptic curves.

In general, it is hard to compute the number of rational points on superelliptic curves, but this can be done for some special classes of superelliptic curves, namely, for those that arise by choosing a suitable polynomial f in (3.1). For example, if $f(x) = x^m + b$, the curve is the well-known Fermat curve, for which explicit formulas and bounds for the number of points are known ([35, 51]). The curve defined by Equation (3.1) over $\mathbb{F}_{q^n}$ with $f(x) = x^q - x + b$ is known as Artin-Schreier curve. These special superellipic curves have also been well studied [14, 16, 50].

While these particular cases are well studied, a study of the number of rational points on $\mathscr{X}_{d,a,b}$ has not been provided. Our goal in this chapter is to study the number of rational points on this curve, providing bounds and explicit formulas for special cases.

In order to do that, we use the fact that the map $x \mapsto x\mathrm{Tr}(x)$ is a quadratic form over $\mathbb{F}_{q^n}$. We employ some classical results on quadratic forms over finite fields to provide an expression for the number of rational points on $\mathscr{X}_{d,a,b}$ in terms of Gauss sums (Proposition 3.7). Using this expression, we employ results on Gauss sums in order to obtain bounds for the number of rational points and, for suitable conditions on d, provide explicit formulas for this number. As a consequence of our results, we compute the number of elements α in $\mathbb{F}_{q^n}$ such that both α and $\mathrm{Tr}(\alpha)$ are quadratic residues (Theorem 3.14).

This chapter is organized as follows. In Section 3.2, we present some remarks, comments and statements of our main results and we provide an expression for the number of rational points on the curve $\mathscr{X}_{d,a,b}$ in terms of Gauss sums. Bounds and explicit formulas for the number of rational points are presented in Section 3.3. In Section **??**, we focus on the case where $\mathrm{Tr}(b/a) \neq 0$.

3.2 The number of rational points on the curve $\mathscr{X}_{d,a,b}$

In this section, we provide some definitions and results that will be useful along this chapter. We denote by ψ and $\tilde{\psi}$ the canonical additive characters of $\mathbb{F}_{q^n}$ and $\mathbb{F}_q$, respectively, i.e.,

$$\psi(x) = \exp\left(\frac{2\pi i \,\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_p}(x)}{p}\right) \quad \text{and} \quad \tilde{\psi}(x) = \exp\left(\frac{2\pi i \,\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)}{p}\right).$$

We denote by χ_{q^n-1} a fixed primitive multiplicative character of $\mathbb{F}_{q^n}^*$ and, for m a divisor of q^n-1, χ_m denotes the multiplicative character of order m defined by $\chi_m = \chi_{q^n-1}^{(q^n-1)/m}$. The restriction of χ_m to $\mathbb{F}_q^*$ is a multiplicative character of $\mathbb{F}_q^*$ of order $M = \frac{m}{\gcd(m,(q^n-1)/(q-1))}$ and it will be denoted by η_M.

Definition 3.1. *For multiplicative characters χ of $\mathbb{F}_{q^n}^*$ and η of $\mathbb{F}_q^*$, the Gauss sum of χ and η are the sums*

$$G_n(\chi) = \sum_{x\in\mathbb{F}_{q^n}^*} \chi(x)\psi(x) \quad \text{and} \quad G_1(\eta) = \sum_{x\in\mathbb{F}_q^*} \eta(x)\tilde{\psi}(x),$$

respectively.

For $a \in \mathbb{F}_{q^n}^*$ and $b \in \mathbb{F}_{q^n}$, we compute the number of $\mathbb{F}_{q^n}$-rational points of the curve $\mathscr{X}_{d,a,b}$ by using well-known properties of character sums. We have the following lemma.

Lemma 3.2. *Let $a \in \mathbb{F}_{q^n}^*, b \in \mathbb{F}_{q^n}$ and let d be an integer that divides q^n-1. The number of affine rational points of the curve $\mathscr{X}_{d,a,b}$ over $\mathbb{F}_{q^n}$ is*

$$|\mathscr{X}_{d,a,b}(\mathbb{F}_{q^n})| = q^n + \frac{1}{q^n}\sum_{\ell=1}^{d-1} G_n(\chi_d^\ell) \sum_{c\in\mathbb{F}_{q^n}^*} \psi(cb)\overline{\chi_d}^{\ell}(-c) \sum_{x\in\mathbb{F}_{q^n}} \psi\big(caxTr(x)\big).$$

Proof. It follows from Lemma 1.22 that

$$
\begin{aligned}
|\mathscr{X}_{d,a,b}(\mathbb{F}_{q^n})| &= \frac{1}{q^n}\sum_{c\in\mathbb{F}_{q^n}}\sum_{x,y\in\mathbb{F}_{q^n}}\psi\big(c(ax\mathrm{Tr}(x)+b-y^d)\big)\\
&= q^n+\frac{1}{q^n}\sum_{c\in\mathbb{F}_{q^n}^*}\psi(cb)\sum_{x\in\mathbb{F}_{q^n}}\psi\big(cax\mathrm{Tr}(x)\big)\sum_{y\in\mathbb{F}_{q^n}}\psi(-cy^d).
\end{aligned}
\tag{3.2}
$$

Now, let $y^d = z$ and using Lemma 1.23 we obtain

$$
|\mathscr{X}_{d,a,b}(\mathbb{F}_{q^n})| = q^n+\frac{1}{q^n}\sum_{c\in\mathbb{F}_{q^n}^*}\psi(cb)\sum_{x\in\mathbb{F}_{q^n}}\psi\big(cax\mathrm{Tr}(x)\big)\sum_{z\in\mathbb{F}_{q^n}}\psi(-cz)\left[1+\cdots+\chi_d^{d-1}(z)\right].
$$

Making the change of variable $w=-cz$ and using Lemma 1.22 we have that

$$
|\mathscr{X}_{d,a,b}(\mathbb{F}_{q^n})| = q^n+\frac{1}{q^n}\sum_{c\in\mathbb{F}_{q^n}^*}\sum_{\ell=1}^{d-1}\psi(cb)\overline{\chi_d}^{\ell}(-c)\sum_{x\in\mathbb{F}_{q^n}}\psi\big(cax\mathrm{Tr}(x)\big)\sum_{w\in\mathbb{F}_{q^n}}\psi(w)\chi_d^{\ell}(w).
$$

Therefore

$$
|\mathscr{X}_{d,a,b}(\mathbb{F}_{q^n})| = q^n+\frac{1}{q^n}\sum_{\ell=1}^{d-1}G_n(\chi_d^{\ell})\sum_{c\in\mathbb{F}_{q^n}^*}\psi(cb)\overline{\chi_d}^{\ell}(-c)\sum_{x\in\mathbb{F}_{q^n}}\psi\big(cax\mathrm{Tr}(x)\big).
\tag{3.3}
$$

■

In order to compute the value of the right-hand side sum of Equation (3.3), we will use the fact that $\mathrm{Tr}(cax\mathrm{Tr}(x))$ defines a quadratic form from $\mathbb{F}_{q^n}$ into $\mathbb{F}_q$. From now on, let $Q_c(x)$ be a quadratic form of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ defined by

$$
Q_c(x)=\mathrm{Tr}(cx\mathrm{Tr}(x))
$$

and let $B_c(x,y)$ be the bilinear symmetric form associated to Q_c.

Proposition 3.3. *For $c\in\mathbb{F}_{q^n}^*$, we have that*

$$
\dim_{\mathbb{F}_q}\big(rad(Q_c)\big)=\begin{cases} n-1 & \text{if } c\in\mathbb{F}_q^*,\\ n-2 & \text{if } c\in\mathbb{F}_{q^n}\setminus\mathbb{F}_q.\end{cases}
$$

Proof. The dimension of the radical of the quadratic form Q_c is given by the dimension of the radical of the bilinear form $B_c(x,y)$, i.e., the dimension of the subspace generated by the elements $x\in\mathbb{F}_{q^n}$ such that $B_c(x,y)=0$ for all $y\in\mathbb{F}_{q^n}$. We observe that

$$
\begin{aligned}
B_c(x,y) &= \mathrm{Tr}(c(x+y)\mathrm{Tr}(x+y))-\mathrm{Tr}(cx\mathrm{Tr}(x))-\mathrm{Tr}(cy\mathrm{Tr}(y))\\
&= \mathrm{Tr}(cx\mathrm{Tr}(y)+cy\mathrm{Tr}(x))\\
&= \mathrm{Tr}(y)\mathrm{Tr}(cx)+\mathrm{Tr}(x)\mathrm{Tr}(cy)\\
&= \mathrm{Tr}(y(\mathrm{Tr}(cx)+c\mathrm{Tr}(x))).
\end{aligned}
\tag{3.4}
$$

Then, $B_c(x,y)=0$ for all $y\in\mathbb{F}_{q^n}$ if and only if $\mathrm{Tr}(cx)+c\mathrm{Tr}(x)=0$. Therefore, we are interested in computing the dimension of

$$V=\{x\in\mathbb{F}_{q^n}:\mathrm{Tr}(cx)+c\mathrm{Tr}(x)=0\}.$$

We split the proof into two cases:

- For $c\in\mathbb{F}_q^*$, $\mathrm{Tr}(cx)+c\mathrm{Tr}(x)=c\mathrm{Tr}(x)+c\mathrm{Tr}(x)=2c\mathrm{Tr}(x)$, that implies

  $$|V|=|\{x\in\mathbb{F}_{q^n}:\mathrm{Tr}(x)=0\}|=q^{n-1}$$

  and then $\dim(V)=n-1$.

- For $c\in\mathbb{F}_{q^n}\setminus\mathbb{F}_q$, if $x\in\mathbb{F}_{q^n}$ is such that $\mathrm{Tr}(x)\neq 0$, then $\frac{\mathrm{Tr}(cx)}{\mathrm{Tr}(x)}\in\mathbb{F}_q$ and $\frac{\mathrm{Tr}(cx)}{\mathrm{Tr}(x)}\neq -c$. Therefore for any element $x\in V$ we have that $\mathrm{Tr}(x)=0$. It follows that $\mathrm{Tr}(cx)=-c\mathrm{Tr}(x)=0$, then $V=V_1\cap V_2$, where $V_1=\{x\in\mathbb{F}_{q^n}\mid\mathrm{Tr}(x)=0\}$ and $V_2=\{x\in\mathbb{F}_{q^n}\mid\mathrm{Tr}(cx)=0\}$. Since $c\in\mathbb{F}_{q^n}\setminus\mathbb{F}_q$ and $V_1\neq V_2$, we conclude $\dim(V)=n-2$ from the fact that $\dim(V_1)=\dim(V_2)=n-1$.

This completes the proof of our assertion.

■

Proposition 3.4. *Let H be the symmetric matrix associated to Q_c and let δ be as defined in Lemma 1.33 for some basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then*

$$\eta_2(\delta)=\begin{cases}\eta_2(c) & \text{if } c\in\mathbb{F}_q^*,\\ \eta_2(-1) & \text{if } c\in\mathbb{F}_{q^n}\setminus\mathbb{F}_q.\end{cases}$$

Proof. Since $\eta_2(\delta)$ does not depend on the basis, we set a basis $\alpha_0,\alpha_1,\dots,\alpha_{n-1}$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ such that

- $\alpha_0=n^{-1}$ and $\mathrm{Tr}(\alpha_i)=0$ for all $1\le i\le n-1$ if $\gcd(n,q)=1$;

- $\mathrm{Tr}(\alpha_0)=1$, $\alpha_1=1$ and $\mathrm{Tr}(\alpha_0\alpha_i)=\mathrm{Tr}(\alpha_i)=0$ for all $2\le i\le n-1$ if $\gcd(q,n)\neq 1$.

For $0\le i\le n-1$, let $x_i,y_i\in\mathbb{F}_q$ such that $y=\sum_{j=0}^{n-1}y_j\alpha_j$ and $x=\sum_{j=0}^{n-1}x_j\alpha_j$ and let us denote $X=(x_0,\dots,x_{n-1})$ and $Y=(y_0,\dots,y_{n-1})$. We recall that $Q_c(x)=XHX^T$ and

$$\begin{aligned}B_c(X,Y)&=(X+Y)H(X+Y)^T-XHX^T-YHY^T\\&=XHY^T+YHX^T\\&=YH^TX^T+YHX^T\\&=Y(2H)X^T.\end{aligned}\tag{3.5}$$

Therefore, we can determine δ from $B_c(x,y)$ by computing the determinant of the reduced matrix associated to $2H$. In order to do this, we observe that $\mathrm{Tr}(x) = x_0$ and

$$\mathrm{Tr}(cx) = \begin{cases} x_0c_0 + \sum\limits_{1\le i,j\le n-1} x_ic_j\beta_{i,j} & \text{if } p\nmid n; \\ x_0(c_1+c_0\beta_{0,0}) + c_0x_1 + \sum\limits_{2\le i,j\le n-1} x_ic_j\beta_{i,j} & \text{if } p\mid n, \end{cases}$$

where $\beta_{i,j} = \mathrm{Tr}(\alpha_i\alpha_j)$. We obtain expressions for $\mathrm{Tr}(y)$ and $\mathrm{Tr}(cy)$ by a similar process. Therefore, it follows from (3.4) that

$$\begin{aligned} B_c(x,y) &= \mathrm{Tr}(y)\mathrm{Tr}(cx) + \mathrm{Tr}(cy)\mathrm{Tr}(x) \\ &= \begin{cases} 2x_0y_0c_0 + \sum\limits_{1\le i,j\le n-1} c_j\beta_{i,j}(y_0x_i + x_0y_i), & \text{if } p\nmid n; \\ 2x_0y_0(c_1+c_0\beta_{0,0}) + c_0x_1y_0 + c_0x_0y_1 + \sum\limits_{2\le i,j\le n-1} c_j\beta_{i,j}(y_0x_i+x_0y_i) & \text{if } p\mid n. \end{cases} \end{aligned}$$

We obtain

$$2H = \begin{pmatrix} 2c_0 & \sum\limits_{j=1}^{n-1}\beta_{1,j}c_j & \cdots & \sum\limits_{j=1}^{n-1}\beta_{n-1,j}c_j \\ \sum\limits_{j=1}^{n-1}\beta_{1,j}c_j & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \sum\limits_{j=1}^{n-1}\beta_{n-1,j}c_j & 0 & \cdots & 0 \end{pmatrix}$$

in the case where $p\nmid n$ and

$$2H = \begin{pmatrix} 2(c_1+c_0\beta_{0,0}) & c_0 & \sum\limits_{j=2}^{n-1}\beta_{2,j}c_j & \cdots & \sum\limits_{j=2}^{n-1}\beta_{n-1,j}c_j \\ c_0 & 0 & 0 & \cdots & 0 \\ \sum\limits_{j=2}^{n-1}\beta_{2,j}c_j & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \sum\limits_{j=1}^{n-1}\beta_{n-1,j}c_j & 0 & 0 & \cdots & 0 \end{pmatrix}$$

in the case where $p\mid n$.

In order to compute the reduced form of $2H$, we observe that

- When $c\in\mathbb{F}_q$, we have that $c_0 = c$ and $c_1 = c_2 = \cdots = c_{n-1} = 0$ if $p\nmid n$ and $c_1 = c$, $c_0 = c_2 = \cdots = c_{n-1} = 0$ if $p\mid n$. Therefore, the associated reduced matrix is $(2c)$.

- When $c \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$, Proposition 3.3 implies that either there exists $k \in \{1,\ldots,n-1\}$ such that $\sum_{j=1}^{n-1} \beta_{k,j} c_j \neq 0$ if $p \nmid n$ and $c_0 \neq 0$ or there exists $k \in \{2,\ldots,n-1\}$ such that $\sum_{j=2}^{n-1} \beta_{k,j} c_j \neq 0$ if $p \mid n$. Then straightforward manipulations on the lines and columns shows that $2H$ reduces to a matrix of the form

  $$\begin{pmatrix} u & v \\ v & 0 \end{pmatrix},$$

  where $v \neq 0$.

In sum, we have that the quadratic character of the determinant δ of the reduced matrix of H is given by

$$\eta_2(\delta) = \begin{cases} \eta_2(c) & \text{if } c \in \mathbb{F}_q^*; \\ \eta_2(-1) & \text{if } c \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q. \end{cases}$$

This completes the proof. ■

Combining Lemma 1.33 and Proposition 3.3 and 3.4, we have the following result.

Theorem 3.5. *For $c \in \mathbb{F}_{q^n}^*$, we have*

$$\sum_{x \in \mathbb{F}_{q^n}} \psi(cxTr(x)) = \begin{cases} (-1)^{s+1} \eta_2(c) \tau^s q^{\frac{2n-1}{2}} & \text{if } c \in \mathbb{F}_q^*; \\ q^{n-1} & \text{if } c \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q. \end{cases}$$

Definition 3.6. *We define*

$$v = \gcd\left(d, \tfrac{q^n-1}{q-1}\right), \quad D = \frac{d}{v}, \quad B = Tr\left(\frac{b}{a}\right).$$

Theorem 3.5 allows us to express the number of $\mathbb{F}_{q^n}$-rational points of $\mathscr{X}_{d,a,b}$ in terms of Gauss sums.

Proposition 3.7. *Let v, D and B be as in Definition 3.6. Then*

$$|\mathscr{X}_{d,a,b}(\mathbb{F}_{q^n})| = q^n + \sum_{\ell=1}^{d-1} \chi_d^\ell(b) q^{n-1} + N,$$

where $N = N_{d,a,b,n}$ is given below.

1. *If D is odd and $B = 0$, then*

$$N = -\frac{q-1}{q} \sum_{j=1}^{v-1} G_n\left(\chi_d^{jD}\right) \chi_d^{jD}(-a).$$

2. *If D is odd and $B \neq 0$, then*

$$N = \frac{1}{q}\sum_{\ell=1}^{d-1} G_n\big(\chi_d^\ell\big)\Big[(-1)^{s+1}\chi_d^\ell(-aB)\chi_2(B)\tau^s\sqrt{q}\,G_1\big(\eta_{2D}^{D-2\ell}\big) - \chi_d^\ell(-aB)G_1\big(\eta_{2D}^{-2\ell}\big)\Big].$$

3. *If D is even and $B = 0$, then*

$$N = \frac{q-1}{q}\left((-1)^{s+1}\tau^s\sqrt{q}\sum_{j=0}^{v-1} G_n\big(\chi_d^{jD+\frac{D}{2}}\big)\chi_d^{jD+\frac{D}{2}}(-a) - \sum_{j=1}^{v-1} G_n\big(\chi_d^{jD}\big)\chi_d^{jD}(-a)\right).$$

4. *If D is even and $B \neq 0$, then*

$$N = \frac{1}{q}\sum_{\ell=1}^{d-1} G_n\big(\chi_d^\ell\big)\Big[(-1)^{s+1}\chi_d^\ell(-aB)\chi_2(B)\tau^s\sqrt{q}\,G_1\big(\eta_D^{\frac{D}{2}-\ell}\big) - \chi_d^\ell(-aB)G_1\big(\eta_D^{-\ell}\big)\Big].$$

Proof. Expand now from Lemma 3.2 and Theorem 3.5, we get that $|\mathscr{X}_{d,a,b}(\mathbb{F}_{q^n})|$ is equal to

$$q^n + \frac{1}{q}\sum_{\ell=1}^{d-1} G_n\big(\chi_d^\ell\big)\left[\sum_{ca\in\mathbb{F}_{q^n}\setminus\mathbb{F}_q} \psi(cb)\overline{\chi_d}^\ell(-c) + \sum_{ca\in\mathbb{F}_q^*}\psi(cb)\overline{\chi_d}^\ell(-c)\big((-1)^{s+1}\eta_2(ac)\tau^s\sqrt{q}\big)\right].$$

That can be rewritten as

$$q^n + \frac{1}{q}\sum_{\ell=1}^{d-1} G_n\big(\chi_d^\ell\big)\left[\sum_{ca\in\mathbb{F}_{q^n}^*} \psi(cb)\overline{\chi_d}^\ell(-c) + \sum_{ca\in\mathbb{F}_q^*}\psi(cb)\overline{\chi_d}^\ell(-c)\big((-1)^{s+1}\eta_2(ac)\tau^s\sqrt{q}-1\big)\right]. \tag{3.6}$$

Let $T = \sum_{\ell=1}^{d-1} G_n\big(\chi_d^\ell\big)\sum_{ca\in\mathbb{F}_{q^n}^*}\psi(cb)\overline{\chi_d}^\ell(-c)$. By Lemma 1.22, if $b=0$, then $T=0$. Otherwise, using the fact that

$$\sum_{ca\in\mathbb{F}_{q^n}^*}\psi(cb)\overline{\chi_d}^\ell(-c) = \sum_{ca\in\mathbb{F}_{q^n}^*}\psi(cb)\overline{\chi_d}^\ell(-c)\chi_d^\ell(b)\overline{\chi_d}^\ell(b) = \chi_d^\ell(b)G_n(\overline{\chi_d}^\ell)$$

and Lemma 1.25, we obtain that

$$T = \sum_{\ell=1}^{d-1}\chi_d^\ell(-b)G_n\big(\chi_d^\ell\big)G_n\big(\overline{\chi_d}^\ell\big) = \sum_{\ell=1}^{d-1}\chi_d^\ell(b)q^n. \tag{3.7}$$

Now, we compute $S_\ell = \sum_{z\in\mathbb{F}_q^*}\psi\big(z\frac{b}{a}\big)\overline{\chi_d}^\ell\big(\frac{-z}{a}\big)\big((-1)^{s+1}\eta_2(z)\tau^s\sqrt{q}-1\big)$.

We divide the proof in the cases D odd or even.

(i) Assume that D is odd.

We recall that η_D is the restriction of χ_d to $\mathbb{F}_q^*$ and that η_{2D} is such that $\eta_{2D}^2 = \eta_D$. Using this notation,

$$\begin{aligned} S_\ell &= (-1)^{s+1}\chi_d^\ell(-a)\tau^s\sqrt{q}\sum_{z\in\mathbb{F}_q^*}\psi\big(z\tfrac{b}{a}\big)\eta_{2D}^{D-2\ell}(z) - \chi_d^\ell(-a)\sum_{z\in\mathbb{F}_q^*}\psi\big(z\tfrac{b}{a}\big)\eta_{2D}^{-2\ell}(z) \\ &= (-1)^{s+1}\chi_d^\ell(-a)\tau^s\sqrt{q}\sum_{z\in\mathbb{F}_q^*}\tilde{\psi}(zB)\eta_{2D}^{D-2\ell}(z) - \chi_d^\ell(-a)\sum_{z\in\mathbb{F}_q^*}\tilde{\psi}(zB)\eta_{2D}^{-2\ell}(z). \end{aligned}$$

We split the proof into two cases.

- If $B = 0$, then it follows from Lemma 1.22 that

$$S_\ell = \begin{cases} 0 & \text{if } D \nmid \ell; \\ -\chi_d^\ell(-a)(q-1) & \text{if } D \mid \ell. \end{cases}$$

- If $B \neq 0$, then

$$\begin{aligned} S_\ell &= (-1)^{s+1}\chi_d^\ell(-a)\tau^s\sqrt{q}\,\eta_{2D}^{D-2\ell}(B^{-1})G_1\big(\eta_{2D}^{D-2\ell}\big) - \chi_d^\ell(-a)\eta_{2D}^{-2\ell}(B^{-1})G_1\big(\eta_{2D}^{-2\ell}\big) \\ &= (-1)^{s+1}\chi_d^\ell(-aB)\chi_2(B)\tau^s\sqrt{q}\,G_1\big(\eta_{2D}^{D-2\ell}\big) - \chi_d^\ell(-aB)G_1\big(\eta_{2D}^{-2\ell}\big). \end{aligned}$$

Our statement follows from the values of S_ℓ found and Equations (3.6) and (3.7).

(ii) Assume that D is even.

In this case, η_D is the restriction of χ_d to $\mathbb{F}_q^*$ and we have that η_D is such that $\eta_D^2 = \eta_{D/2}$. Using this notation,

$$\begin{aligned} S_\ell &= \sum_{z\in\mathbb{F}_q^*}\psi\left(z\frac{b}{a}\right)\chi_d^\ell\left(-\frac{z}{a}\right)\left((-1)^{s+1}\eta_2(z)\tau^s\sqrt{q}-1\right) \\ &= (-1)^{s+1}\chi_d^\ell(-a)\tau^s\sqrt{q}\sum_{z\in\mathbb{F}_q^*}\psi\left(z\frac{b}{a}\right)\eta_D^{D/2-\ell}(z) - \chi_d^\ell(-a)\sum_{z\in\mathbb{F}_q^*}\psi\left(z\frac{b}{a}\right)\eta_D^{-\ell}(z) \\ &= (-1)^{s+1}\chi_d^\ell(-a)\tau^s\sqrt{q}\sum_{z\in\mathbb{F}_q^*}\tilde{\psi}(zB)\eta_D^{D/2-\ell}(z) - \chi_d^\ell(-a)\sum_{z\in\mathbb{F}_q^*}\tilde{\psi}(zB)\eta_D^{-\ell}(z). \end{aligned}$$

We consider the following cases.

- If $B = 0$, it follows from Lemma 1.22 that

$$S_\ell = \begin{cases} 0 & \text{if } D \nmid \ell; \\ (-1)^{s+1}\chi_d^\ell(-a)\tau^s\sqrt{q}(q-1) - \chi_d(-a)(q-1) & \text{if } \frac{\ell}{D/2} \text{ is odd;} \\ -\chi_d^\ell(-a)(q-1) & \text{otherwise.} \end{cases}$$

- If $B \neq 0$, we obtain

$$
\begin{aligned}
S_\ell &= (-1)^{s+1}\chi_d^\ell(-a)\tau^s\sqrt{q}\sum_{z\in\mathbb{F}_q*}\tilde{\psi}(zB)\eta_D^{D/2-\ell}(zB)\eta_D^{D/2-\ell}(B^{-1}) - \chi_d^\ell(-a)\cdot \\
&\sum_{z\in\mathbb{F}_q^*}\tilde{\psi}(zB)\eta_D^{-\ell}(zB)\eta_D^{-\ell}(B^{-1}) \\
&= (-1)^{s+1}\chi_d^\ell(-a)\tau^s\sqrt{q}\eta_D^{D/2-\ell}(B^{-1})G_1(\eta_D^{D/2-\ell}) - \chi_d^\ell(-a)\eta_D^{-\ell}(B^{-1})G_1(\eta_D^{-\ell}) \\
&= (-1)^{s+1}\chi_d^\ell(-aB)\chi_2(B)\tau^s\sqrt{q}G_1(\eta_D^{D/2-\ell}) - \chi_d^\ell(-aB)G_1(\eta_D^{-\ell}).
\end{aligned}
$$

■

3.3 Bounds and explict formulas for the number of rational points on $\mathscr{X}_{d,a,b}$

In this section, we present our main results of this chapter, along with a few comments. We observe that the curves $\mathscr{X}_{d,a,b}(\mathbb{F}_{q^n})$ and $\mathscr{X}_{\gcd(d,q^n-1),a,b}(\mathbb{F}_{q^n})$ have the same number of $\mathbb{F}_{q^n}$-rational points. Therefore, we will assume without loss of generality that d divides q^n-1.

In [43], the authors give an improvement of the Hasse-Weil bound for curves with high genus. The curve $\mathscr{X}_{d,a,b}$ does not satisfy the conditions imposed in [43], but as a high genus curve, it is expected to be a curve whose the number of rational points given by the Hasse-Weil's bound is far. Indeed, it turns out that Hasse-Weil can be significantly improved for $\mathscr{X}_{d,a,b}$. In Theorem 3.8, we provide sharp bounds for the number of rational points on such curves. In order to present this result, we introduce some notation. For a divisor d of q^n-1, χ_d denotes a multiplicative character of $\mathbb{F}_{q^n}^*$ with order d.

Now we are able to present bounds for the number of $\mathbb{F}_{q^n}$-rational points on the curve $\mathscr{X}_{d,a,b}$.

Theorem 3.8. *The number of rational points of the curve $\mathscr{X}_{d,a,b}$ satisfies the following relations:*

$$
|\mathscr{X}_{d,a,b}(\mathbb{F}_{q^n})| = q^n - (-1)^s q^{n-1}\sum_{\ell=1}^{d-1}\chi_d^\ell(b) + N_{d,a,b,n}, \tag{3.8}
$$

where

$$
|N_{d,a,b,n}| \leq \begin{cases} \left(\frac{d}{D}-1\right)(q-1)q^{\frac{n}{2}-1}, & \textit{if } D \textit{ is odd and } B=0; \\ (q-1)\left(\frac{d}{D}q^{\frac{n-1}{2}} + \left(\frac{d}{D}-1\right)q^{\frac{n}{2}-1}\right), & \textit{if } D \textit{ is even and } B=0. \\ (d-1)\left(q^{\frac{n}{2}} + q^{\frac{n-1}{2}}\right) & \textit{if } B\neq 0. \end{cases}
$$

Proof. The result follows by a direct employment of Proposition 3.7 and Lemma 1.25. Let us consider the case when D is odd.

- If $B = 0$, by Propositions 3.7 we have

$$\begin{aligned} |N_{d,a,b,n}| &= \frac{1}{q}\left|-(q-1)\sum_{j=1}^{v-1} G_n\big(\chi_d^{jD}\big)\chi_d^{jD}(-a)\right| \\ &\leq \frac{(q-1)}{q}\sum_{j=1}^{v-1} |G_n\big(\chi_d^{jD}\big)| \\ &= (q-1)q^{n/2-1}\left(\frac{d}{D}-1\right). \end{aligned}$$

- If $B \neq 0$, then

$$\begin{aligned} |N_{d,a,b,n}| &= \frac{1}{q}\left|\sum_{\ell=1}^{d-1} G_n\big(\chi_d^{\ell}\big)\big[(-1)^{s+1}\chi_d^{\ell}(-aB)\chi_2(B)\tau^s\sqrt{q}\,G_1\big(\eta_{2D}^{D-2\ell}\big) - \chi_d^{\ell}(-aB)G_1\big(\eta_{2D}^{-2\ell}\big)\big]\right| \\ &\leq \frac{1}{q}\sum_{\ell=1}^{d-1} |G_n\big(\chi_d^{\ell}\big)|\big[\sqrt{q}|G_1\big(\eta_{2D}^{D-2\ell}\big)| + |G_1\big(\eta_{2D}^{-2\ell}\big)|\big] \\ &\leq (d-1)(q^{n/2} + q^{(n-1)/2}). \end{aligned}$$

These inequalities along with Proposition 3.7 assures us the result in the cases when D is odd. Now we consider the case when D is even.

- If $B = 0$, by Proposition 3.7 we have

$$\begin{aligned} |N_{d,a,b,n}| &= \frac{(q-1)}{q}\left|(-1)^{s+1}\tau^s\sqrt{q}\sum_{j=0}^{v-1} G_n\left(\chi_d^{jD+D/2}\right)\chi_d^{jD+D/2}(-a) - \sum_{j=1}^{v-1} G_n\left(\chi_d^{jD}\right)\chi_d^{jD}(-a)\right| \\ &\leq \frac{(q-1)}{q}\left(\sqrt{q}\sum_{j=0}^{v-1}\left|G_n\left(\chi_d^{jD+D/2}\right)\right| + \sum_{j=1}^{v-1}\left|G_n\left(\chi_d^{jD}\right)\right|\right) \\ &= (q-1)\left(vq^{\frac{n-1}{2}} + (v-1)q^{\frac{n}{2}-1}\right). \end{aligned}$$

- If $B \neq 0$, it follows that

$$\begin{aligned} |N_{d,a,b,n}| &= \frac{1}{q}\left|\sum_{\ell=1}^{d-1} G_n\big(\chi_d^{\ell}\big)\big[(-1)^{s+1}\chi_d^{\ell}(-aB)\chi_2(B)\tau^s\sqrt{q}\,G_1\big(\eta_D^{D/2-\ell}\big) - \chi_d^{\ell}(-aB)G_1\big(\eta_D^{-\ell}\big)\big]\right| \\ &\leq \frac{1}{q}\sum_{\ell=1}^{d-1} \left|G_n\big(\chi_d^{\ell}\big)\right|\big[\sqrt{q}\left|G_1\big(\eta_D^{D/2-\ell}\big)\right| + \left|G_1\big(\eta_D^{-\ell}\big)\right|\big] \\ &\leq (d-1)(q^{\frac{n}{2}} + q^{\frac{n-1}{2}}). \end{aligned}$$

Together with Proposition 3.7 the result follows.

■

We recall that the Hasse-Weil bound applied to $\mathscr{X}_{d,a,b}$ implies that

$$\left||\mathscr{X}_{d,a,b}(\mathbb{F}_{q^n})| - q^n\right| \le 2gq^{\frac{n}{2}},$$

where the genus g can be computed via Riemann-Hurwitz's formula [19] and equals, at a minimum, the number

$$\tfrac{1}{2}(d-1)(q^{n-1}-1)-d+1.$$

Note that Theorem 3.8 implies that

$$\left||\mathscr{X}_{d,a,b}(\mathbb{F}_{q^n})| - q^n\right| \le (d-1)q^{n-1} + (q-1)(dq^{\frac{n-1}{2}} + (d-1)q^{\frac{n}{2}-1}),$$

which represents a significant improvement of Hasse-Weil's bound.

From now on, our main goal is to provide explicit formulas for the value $N = N_{d,a,b,n}$ defined in Theorem 3.8. Our starting point is the case $d = 2$, for which we present a simple expression for the number of affine rational points, that is given in the next theorem.

Theorem 3.9. *The number of rational points of the curve $\mathscr{X}_{2,a,b}(\mathbb{F}_{q^n})$ is*

1. *If $Tr\left(\frac{b}{a}\right) = 0$*

$$|\mathscr{X}_{2,a,b}(\mathbb{F}_{q^n})| = q^n + q^{n-1}\chi_2(b) + N_1\tau^{ns}\chi_2(-a)(q-1),$$

where

$$N_1 = \begin{cases} q^{\frac{n-2}{2}} & \textit{if } n \textit{ is even;} \\ \tau^s q^{\frac{n-1}{2}} & \textit{if } n \textit{ is odd.} \end{cases}$$

2. *If $Tr\left(\frac{b}{a}\right) \ne 0$*

$$|\mathscr{X}_{2,a,b}(\mathbb{F}_{q^n})| = q^n + q^{n-1}\chi_2(b) - N_2\tau^{ns},$$

where

$$N_2 = \begin{cases} q^{\frac{n-2}{2}}[\chi_2(-a)\tau^{2s}q + \chi_2(-aB)] & \textit{if } n \textit{ is even;} \\ q^{\frac{n-1}{2}}\tau^s(\chi_2(-a) + \chi_2(-aB)) & \textit{if } n \textit{ is odd.} \end{cases}$$

Proof. We have that

$$D = \frac{2}{v} = \begin{cases} 1 & \text{if } n \text{ is even,} \\ 2 & \text{if } n \text{ is odd.} \end{cases}$$

To compute $|\mathscr{X}_{2,a,b}|$ we need to determine N in Proposition 3.7. In the case when n is even we have $D = 1$, therefore

1. If $B = 0$, then
$$\begin{aligned} N &= \frac{1}{q}\left(-(q-1)G_n(\chi_2)\chi_2(-a)\right) \\ &= q^{\frac{n-2}{2}}(q-1)(-1)^{ns+2}\tau^{ns}\chi_2(-a) \\ &= q^{\frac{n-2}{2}}(q-1)\tau^{ns}\chi_2(-a). \end{aligned}$$

2. If $B \neq 0$:
$$\begin{aligned} N &= \frac{1}{q}\left(G_n(\chi_2)\Big[(-1)^{s+1}\chi_2(-aB)\chi_2(B)\tau^s\sqrt{q}G_1\big(\eta_2\big) - \chi_2(-aB)G_1\big(\eta_2^2\big)\Big]\right) \\ &= (-1)^{ns+1}\tau^{ns}q^{\frac{n-2}{2}}\left[(-1)^{s+1}\chi_2(-a)\tau^{2s}(-1)^{s+1}q + \chi_2(-aB)\right] \\ &= -\tau^{ns}q^{\frac{n-2}{2}}\left[\chi_2(-a)\tau^{2s}q + \chi_2(-aB)\right]. \end{aligned}$$

In the case when n odd, we have that D is even, then

1. If $B = 0$:
$$\begin{aligned} N &= \frac{q-1}{q}\left((-1)^{s+1}\tau^s\sqrt{q}G_n(\chi_2)\chi_2(-a)\right) \\ &= \frac{q-1}{q}(-1)^{s+1}\tau^s(-1)^{ns-1}\tau^{ns}q^{\frac{n+1}{2}}\chi_2(-a) \\ &= \tau^{(n+1)s}(q-1)\chi_2(-a)q^{\frac{n-1}{2}}. \end{aligned}$$

2. If $B \neq 0$:
$$\begin{aligned} N &= \frac{1}{q}G_n(\chi_2)\Big[(-1)^{s+1}\chi_2(-aB)\chi_2(B)\tau^s\sqrt{q}G_1\big(\eta_2^0\big) - \chi_2(-aB)G_1\big(\eta_2\big)\Big] \\ &= (-1)^{ns-1}\tau^{ns}q^{\frac{n-2}{2}}\left[(-1)^{s+1}\chi_2(-a)\tau^s\sqrt{q}(-1) - \chi_2(-aB)(-1)^{s-1}\tau^s\sqrt{q}\right] \\ &= -\tau^{s(n+1)}q^{\frac{n-1}{2}}\left[\chi_2(-a) + \chi_2(-aB)\right]. \end{aligned}$$

Combined with Proposition 3.7, the theorem follows.

■

Corollary 3.10. *The number of rational points of the curve $\mathscr{X}_{2,1,0}(\mathbb{F}_{q^n})$ given by*

$$y^2 = xTr(x)$$

is

1. *If* $q \equiv 1 \pmod 4$
$$|\,\mathscr{X}_{2,1,0}(\mathbb{F}_{q^n})\,| = q^n + M_1(q-1),$$
where
$$M_1 = \begin{cases} q^{\frac{n-2}{2}} & \textit{if } n \textit{ is even;} \\ q^{\frac{n-1}{2}} & \textit{if } n \textit{ is odd.} \end{cases}$$

2. *If* $q \equiv 3 \pmod 4$

$$|\mathscr{X}_{2,1,0}(\mathbb{F}_{q^n})| = q^n + M_2(q-1),$$

where

$$M_2 = \begin{cases} i^{ns}(-1)^{\frac{n}{2}} q^{\frac{n-2}{2}} & \textit{if } n \textit{ is even;} \\ i^{(n+1)s}(-1)^{\frac{n-1}{2}} q^{\frac{n-1}{2}} & \textit{if } n \textit{ is odd.} \end{cases}$$

This result allows us to compute the number of rational points in specific curves, as in the following examples.

Example 3.11. *For the curve*

$$\mathscr{X}_{2,-1,0} : y^2 = -xTr(x),$$

it follows that $B = 0$*. Therefore, Theorem 3.9 yields the following number of rational points for a pair* (q,n)*:*

q	*n=2*	*n=3*	*n=4*	*n=5*	*n=6*
3	*7*	*33*	*87*	*225*	*711*
5	*29*	*145*	*645*	*3225*	*15725*
7	*43*	*385*	*2443*	*16513*	*117355*
9	*89*	*801*	*6633*	*59697*	*532089*
11	*111*	*1441*	*14751*	*159841*	*1770351*
25	*649*	*16225*	*391225*	*9780625*	*254281250*

Example 3.12. *For the curve*

$$\mathscr{X}_{2,-1,0} : y^2 = -xTr(x) + 1,$$

it follows that $B = Tr(-1) = -n$*. Therefore, Theorem 3.9 yields the following number of rational points for a pair* (q,n)*:*

q	*n=2*	*n=3*	*n=4*	*n=5*	*n=6*
3	*10*	*42*	*96*	*385*	*954*
5	*34*	*150*	*720*	*3850*	*18600*
7	*64*	*378*	*2688*	*19306*	*134162*
9	*80*	*882*	*7200*	*65448*	*591138*
11	*122*	*1452*	*15840*	*175692*	*1931402*
25	*625*	*16200*	*405600*	*10171250*	*253890000*

Remark 3.13. *We observe that in the cases when p divides n, we have that $B = -n = 0$. These cases are highlighted in the table.*

One can check the values obtained in these two examples by using the computer program SageMath. Nevertheless, the run time of the algorithm grows as q^n increases, making the computation unfeasible even for small values of q^n (such as $q^n > e^{20}$).

3.4 The number of elements $\alpha \in \mathbb{F}_{q^n}$ such that α and Tr(α) are quadratic residues

Now we return to the problem presented at the introduction: determine the number of elements $\alpha \in \mathbb{F}_{q^n}$ such that α and $\mathrm{Tr}(\alpha)$ are both quadratic residues in $\mathbb{F}_{q^n}$. Theorem 3.9 is a key tool to compute the number of these elements in $\mathbb{F}_{q^n}$, as we can see in the proof of the following result.

Theorem 3.14. *Let n be an odd positive integer. Then the number of elements $\alpha \in \mathbb{F}_{q^n}$ such that α and $Tr(\alpha)$ are both quadratic residues in $\mathbb{F}_{q^n}$ is*

$$\frac{q^n + q^{n-1} + \tau^{s(n-1)}(q-1)q^{\frac{n-1}{2}} + 2}{4}.$$

Proof. Let M be the number of elements $\alpha \in \mathbb{F}_{q^n}$ such that both α and $\mathrm{Tr}(\alpha)$ are quadratic residues in $\mathbb{F}_{q^n}$. Let Λ_2 be the set of quadratic residues in $\mathbb{F}_{q^n}^*$ and $\Lambda = \mathbb{F}_{q^n}^* \setminus \Lambda_2$. We recall that, for $x \in \mathbb{F}_{q^n}$, $\chi_2(x) = 1$ if and only if $x \in \Lambda_2$. Then we have that

$$[1+\chi_2(x)][1+\chi_2(\mathrm{Tr}(x))] = \begin{cases} 0, & \text{if either } x \in \Lambda \text{ or } \mathrm{Tr}(x) \in \Lambda; \\ 1, & \text{if } x = 0; \\ 2, & \text{if } x \in \Lambda_2 \text{ and } \mathrm{Tr}(x) = 0; \\ 4, & \text{if } x \in \Lambda_2 \text{ and } \mathrm{Tr}(x) \in \Lambda_2. \end{cases}$$

Therefore, Schur's orthogonality relations (Lemmas 1.22 and 1.23) imply that

$$M = \tfrac{1}{2} + \tfrac{1}{4} \sum_{x \in \mathbb{F}_{q^n}} [1+\chi_2(x)][1+\chi_2(\mathrm{Tr}(x))] + \tfrac{1}{4q} \sum_{x \in \mathbb{F}_{q^n}} [1+\chi_2(x)] \sum_{c \in \mathbb{F}_q} \tilde{\psi}(c\mathrm{Tr}(x)). \tag{3.9}$$

We note that Lemma 1.21 implies that

$$\sum_{x \in \mathbb{F}_{q^n}} [1+\chi_2(x)][1+\chi_2(\mathrm{Tr}(x))] = \sum_{x \in \mathbb{F}_{q^n}} [1+\chi_2(\mathrm{Tr}(x)) + \chi_2(x\mathrm{Tr}(x))]. \tag{3.10}$$

Since n is odd, χ_2 is also the multiplicative character of order 2 over $\mathbb{F}_q$. Since $\mathrm{Tr}(x)$ is a linear transformation over $\mathbb{F}_{q^n}$ whose image is $\mathbb{F}_q$, each element in $\mathbb{F}_q$ has q^{n-1} elements in its preimage. Therefore,

$$\sum_{x\in\mathbb{F}_{q^n}} \chi_2(\mathrm{Tr}(x)) = q^{n-1} \sum_{y\in\mathbb{F}_q} \chi_2(y) = 0. \tag{3.11}$$

We note that

$$|\mathscr{X}_{2,1,0}(\mathbb{F}_{q^n})| = \sum_{x\in\mathbb{F}_{q^n}} \left[1+\chi_2(x\mathrm{Tr}(x))\right] = q^n + \sum_{x\in\mathbb{F}_{q^n}} \chi_2(x\mathrm{Tr}(x)). \tag{3.12}$$

From (3.10), (3.11) and (3.12), it follows that

$$\sum_{x\in\mathbb{F}_{q^n}} \left[1+\chi_2(x)\right]\left[1+\chi_2(\mathrm{Tr}(x))\right] = |\mathscr{X}_{2,1,0}(\mathbb{F}_{q^n})|. \tag{3.13}$$

For the last sum in (3.9), Lemma 1.22 implies that

$$\sum_{x\in\mathbb{F}_{q^n}} \left[1+\chi_2(x)\right] \sum_{c\in\mathbb{F}_q} \tilde{\psi}(c\mathrm{Tr}(x)) = q^{n-1}\cdot q + \sum_{c\in\mathbb{F}_q}\sum_{x\in\mathbb{F}_{q^n}} \chi_2(x)\tilde{\psi}(c\mathrm{Tr}(x)). \tag{3.14}$$

The map $x \mapsto \mathrm{Tr}(x))$ is a linear map over $\mathbb{F}_q$ so that $c\mathrm{Tr}(x) = \mathrm{Tr}(cx)$ for all $c \in \mathbb{F}_q$ and then $\tilde{\psi}(c\mathrm{Tr}(x) = \tilde{\psi}(\mathrm{Tr}(cx)) = \psi(cx)$. Therefore, by setting $z = cx$, we obtain that

$$\begin{aligned}\sum_{c\in\mathbb{F}_q}\sum_{x\in\mathbb{F}_{q^n}} \chi_2(x)\tilde{\psi}(c\mathrm{Tr}(x)) &= \sum_{c\in\mathbb{F}_q} \chi_2(c) \sum_{z\in\mathbb{F}_{q^n}} \chi_2(z)\psi(z)\\ &= G_n(\chi_2)\sum_{c\in\mathbb{F}_q}\chi_2(c) \\ &= 0,\end{aligned} \tag{3.15}$$

where the last equality follows by Lemma 1.21. In sum, Equations (3.9), (3.13), (3.14) and (3.15) imply that

$$M = \frac{|\mathscr{X}_{2,1,0}(\mathbb{F}_{q^n})| + q^{n-1} + 2}{4}.$$

Now using Theorem 3.9, we have that

$$\mathscr{X}_{2,1,0}(\mathbb{F}_{q^n}) = q^n + \tau^{(n+1)s}\chi_2(-1)(q-1)q^{\frac{n-1}{2}} = q^n + \tau^{(n-1)s}(q-1)q^{\frac{n-1}{2}},$$

therefore

$$M = \frac{q^n + q^{n-1} + \tau^{(n-1)s}(q-1)q^{\frac{n-1}{2}} + 2}{4}.$$

■

3.5 The number of $\mathbb{F}_{q^n}$–rational points of $\mathscr{X}_{d,a,b}$ when $\mathbf{Tr}\left(\frac{b}{a}\right) = 0$

Now, in order to compute the value of N in Proposition 3.7, we present the following important definition, that is a generalization of a constant used by Wolfmann in [51] in the study of diagonal equations.

Definition 3.15. *For m a divisor of $q^n - 1$, $a \in \mathbb{F}_{q^n}^*$ and $\epsilon \in \{1, -1\}$, we set*

$$\theta_m(a,\epsilon) = \begin{cases} m-1 & \textit{if } \chi_m(a) = \epsilon; \\ -1 & \textit{otherwise.} \end{cases}$$

The following definition, that was introduced in the study of diagonal equations [35], will be useful in our results.

Definition 3.16. *Let r be a positive integer. An integer $d > 2$ is (p,r)-admissible if $d \mid (p^r + 1)$ and there exists no $r' < r$ such that $d \mid (p^{r'} + 1)$.*

If $d > 2$ is (p,r)-admissible, then $2r$ is the multiplicative order of p modulo d. Since d divides $q^n - 1$ and $q = p^s$, the condition of (p,r)-admissibility on d implies that $2r$ divides ns and, in particular, that ns is an even number.

Definition 3.17. *If d is a divisor of $q^n - 1$ and is (p,r)-admissible we define*

$$\varepsilon = (-1)^{\frac{ns}{2r}} \quad \textit{and} \quad u = \frac{p^r + 1}{d}.$$

We present now one of our main results, which provides a formula for the number of rational points on $\mathscr{X}_{d,a,b}$ in the case when $B = 0$ and some suitable conditions are required.

Theorem 3.18. *Let $d > 2$ be an integer, $a, b \in \mathbb{F}_{q^n}$ such that $B = Tr\left(\frac{b}{a}\right) = 0$ and $N = N_{d,a,b,n}$ defined as in Equation* (3.8)*. The following holds:*

1) If v is (p,r)-admissible and D is odd, then

$$N = \begin{cases} 0 & \textit{if } v = 1; \\ \tau^{sn}\chi_2(a)(q-1)q^{\frac{n-2}{2}} & \textit{if } v = 2; \\ \varepsilon\theta_v(-a,\varepsilon^u)(q-1)q^{\frac{n-2}{2}} & \textit{if } v > 2. \end{cases}$$

2) If $2v$ is (p,r)-admissible and D is even.

a) If $v = 1$ then

$$N = (-1)^s \tau^{(n+1)s} \chi_2(a)(q-1)q^{\frac{n-1}{2}}.$$

b) If $v = 2$ then

$$N = \big[(-1)^s \tau^s \sqrt{q}\,\varepsilon^{u\frac{D}{2}+1}(\chi_4(-a) + \overline{\chi}_4(a)) + \tau^{ns}\chi_2(a)\big](q-1)q^{\frac{n-2}{2}}.$$

c) If $v > 2$ then

$$N = \varepsilon\Big[(-1)^s \tau^s \sqrt{q}\,\chi_{2v}(-a)\varepsilon^{\frac{uD}{2}}[1 + \theta_v(-a,1)] + \theta_v(-a,1)\Big](q-1)q^{\frac{n-2}{2}}.$$

Proof. 1) Assume that v is (p,r)-admissible and D is odd. Proposition 3.7 states that

$$N = -\frac{q-1}{q}\sum_{j=1}^{v-1} G_n\big(\chi_d^{jD}\big)\chi_d^{jD}(-a).$$

We recall that χ_d^D has order $\frac{d}{D} = v$. If $v = 1$, then $N = 0$. If $v = 2$, then Theorem 1.28 entails that

$$N = -(q-1)(-\tau^{sn} q^{\frac{n-2}{2}} \chi_2(-1)\chi_2(a)) = (q-1)\tau^{sn} q^{\frac{n-2}{2}} \chi_2(a),$$

since $\chi_2(-1) = \tau^{2ns} = 1$. If $v > 2$, then Theorem 1.26 implies that

$$N = -\frac{q-1}{q}(-\varepsilon)q^{\frac{n}{2}}\sum_{j=1}^{v-1}\big(\varepsilon^{uD}\chi_d^D(-a)\big)^j = q^{\frac{n-2}{2}}(q-1)\varepsilon\theta_v(-a,\varepsilon^{uD}).$$

2) Let us assume that $2v$ is (p,r)-admissible and D is even. By Proposition 3.7 we have

$$N = \frac{q-1}{q}\left((-1)^{s+1}\tau^s\sqrt{q}\sum_{j=0}^{v-1} G_n\big(\chi_d^{jD+\frac{D}{2}}\big)\chi_d^{jD+\frac{D}{2}}(-a) - \sum_{j=1}^{v-1} G_n\big(\chi_d^{jD}\big)\chi_d^{jD}(-a)\right).$$

- If $v = 1$, $d = D$ and it follows that

$$\begin{aligned}
N &= \frac{q-1}{q}\left((-1)^{s+1}\tau^s\sqrt{q}\,G_n\big(\chi_d^{\frac{d}{2}}\big)\chi_d^{\frac{d}{2}}(-a)\right)\\
&= \frac{q-1}{q}(-1)^{s+1}\tau^s\sqrt{q}\,G_n(\chi_2)\chi_2(-a)\\
&= (-1)^{ns+s}(q-1)q^{\frac{n-1}{2}}\tau^{s(n+1)}\chi_2(a)\\
&= (-1)^s(q-1)q^{\frac{n-1}{2}}\tau^{s(n+1)}\chi_2(a).
\end{aligned}$$

- If $v = 2$, we have $d = 2D$. By hypotheses, 4 is (p,r)-admissible, and $u = \frac{p^r+1}{d} = \frac{p^r+1}{4 \cdot D/2}$. Then

$$\begin{aligned} N &= \frac{q-1}{q}\left((-1)^{s+1}\tau^s\sqrt{q}(G_n\big(\chi_d^{\frac{d}{4}}\big)\chi_d^{\frac{d}{4}}(-a) + G_n\big(\chi_d^{\frac{3d}{4}}\big)\chi_d^{\frac{3d}{4}}(-a)) - G_n\big(\chi_d^{\frac{d}{2}}\big)\chi_d^{\frac{d}{2}}(-a)\right) \\ &= \frac{q-1}{q}\big((-1)^{s+1}\tau^s\sqrt{q}(G_n(\chi_4)\chi_4(-a) + G_n(\overline{\chi_4})\overline{\chi_4}(-a)) - G_n(\chi_2)\chi_2(-a)\big) \\ &= \frac{q-1}{q}\left((-1)^{s+1}\tau^s\sqrt{q}(-\varepsilon^{u\frac{D}{2}+1}q^{\frac{n}{2}}\chi_4(-a) + \chi_4(-1)(-\varepsilon^{u\frac{D}{2}+1}q^{\frac{n}{2}})\overline{\chi_4}(-a)) + (-1)^{sn}\tau^{ns}q^{\frac{n}{2}}\chi_2(-a)\right) \\ &= q^{\frac{n-2}{2}}(q-1)\Big((-1)^s\tau^s\sqrt{q}\,\varepsilon^{u\frac{D}{2}+1}(\chi_4(-a) + \overline{\chi_4}(a)) + \tau^{ns}\chi_2(a)\Big). \end{aligned}$$

- If $v > 2$, then Theorem 1.26 implies that

$$\begin{aligned} N &= \frac{q-1}{q}\left((-1)^{s+1}\tau^s q^{\frac{n+1}{2}}\chi_{2v}(-a)(-\varepsilon^{1+\frac{uD}{2}})\sum_{j=0}^{v-1}\big(\varepsilon^{2u}\chi_v(-a)\big)^j - q^{\frac{n}{2}}(-\varepsilon)\sum_{j=1}^{v-1}\big(\varepsilon^{uD}\chi_v(-a)\big)^j\right) \\ &= \frac{q-1}{q}\left((-1)^s\tau^s q^{\frac{n+1}{2}}\chi_{2v}(-a)\varepsilon^{1+\frac{uD}{2}}[1+\theta_v(-a,1)] + q^{\frac{n}{2}}\varepsilon\theta_v(-a,1)\right) \\ &= (q-1)q^{\frac{n-2}{2}}\varepsilon\Big[(-1)^s\tau^s\sqrt{q}\,\chi_{2v}(-a)\varepsilon^{\frac{uD}{2}}[1+\theta_v(-a,1)] + \theta_v(-a,1)\Big]. \end{aligned}$$

■

By making use of this result, we can obtain a simple expression for the number of rational points in the case where a, b and d satisfy some restrictions.

Corollary 3.19. *If $d > 2$ is a (p,r)-admissible divisor of $\frac{q^n-1}{q-1}$ and $\frac{ns}{2r}$ is even, then*

$$N_{d,-1,0,n} = (d-1)(q-1)q^{\frac{n-2}{2}}.$$

Similar results to Theorem 3.18 can be obtained for the case $B \neq 0$, as we will see in the next section.

3.6 The number of $\mathbb{F}_{q^n}$–rational points of $\mathscr{X}_{d,a,b}$ when $\mathbf{Tr}\left(\frac{b}{a}\right) \neq 0$

Definition 3.20. *If D is (p,r_0)-admissible, we define*

$$\varepsilon_0 = (-1)^{\frac{s}{2r_0}} \quad \textit{and} \quad u_0 = \begin{cases} \frac{p^{r_0}+1}{2D}, & \textit{if } D \textit{ is odd;} \\ \frac{p^{r_0}+1}{D}, & \textit{if } D \textit{ is even.} \end{cases}$$

Theorem 3.21. *Let $a, b \in \mathbb{F}_{q^n}$ such that $B \neq 0$. If d is (p,r)-admissible, D is odd and (p,r_0)-admissible, then*

$$N = N_1 q^{\frac{n}{2}} + N_2 q^{\frac{n-1}{2}} + N_3 q^{\frac{n-2}{2}},$$

where

- $N_1 = (-1)^{s+1}\varepsilon\varepsilon_0^{1+u_0D}\tau^s\chi_2(B)\theta_d(-aB,\varepsilon^u)$;
- $N_2 = \varepsilon\varepsilon_0(-\theta_d(-aB,\varepsilon^u)+\theta_v(-aB,\varepsilon^u))$;
- $N_3 = -\varepsilon\theta_v(-aB,\varepsilon^u)$.

Proof. By hypothesis d is (p,r)-admissible and D is odd. By Proposition 3.7,

$$N = \frac{1}{q}\sum_{\ell=1}^{d-1} G_n\big(\chi_d^\ell\big)\Big[(-1)^{s+1}\chi_d^\ell(-aB)\chi_2(B)\tau^s\sqrt{q}\,G_1\big(\eta_{2D}^{D-2\ell}\big) - \chi_d^\ell(-aB)G_1\big(\eta_{2D}^{-2\ell}\big)\Big].$$

Since D is (p,r_0)-admissible and $p^{r_0}+1$ is even, it follows that $2D$ divides $p^{r_0}+1$. Therefore, Theorem 1.26 and Corollary 1.29 imply that

$$\begin{aligned}
N &= -q^{\frac{n-2}{2}}\sum_{\ell=1}^{d-1}\varepsilon^{u\ell+1}\chi_d^\ell(-aB)\Big[(-1)^s\tau^s\chi_2(B)\varepsilon_0^{u_0(2\ell+D)+1}q + \varepsilon_0^{2u_0\ell+1}\sqrt{q}\Big] + R\\
&= -q^{\frac{n-1}{2}}\varepsilon\varepsilon_0\Big((-1)^s\tau^s\chi_2(B)\varepsilon_0^{u_0D}\sqrt{q}+1\Big)\sum_{\ell=1}^{d-1}\big(\chi_d(-aB)\varepsilon^u\varepsilon_0^{2u_0}\big)^\ell + R\\
&= -q^{\frac{n-1}{2}}\varepsilon\varepsilon_0\Big((-1)^s\tau^s\chi_2(B)\varepsilon_0^{u_0D}\sqrt{q}+1\Big)\theta_d(-aB,\varepsilon^u) + R,
\end{aligned}$$

where R is the sum of the terms in the case when the multiplicative caracter is trivial, i.e.,

$$\begin{aligned}
R &= \frac{1}{q}\left(q^{\frac{n}{2}}\sum_{j=1}^{d/D-1}\varepsilon^{ujD+1}\chi_d^{jD}(-aB)\Big[-1+\sqrt{q}\,\varepsilon_0^{2u_0jD+1}\Big]\right)\\
&= -q^{\frac{n-2}{2}}\varepsilon\sum_{j=1}^{d/D-1}\Big[\big(\varepsilon^{uD}\chi_d^D(-aB)\big)^j - \varepsilon_0\big(\varepsilon^{uD}\varepsilon_0^{2u_0D}\chi_d^D(-aB)\big)^j\sqrt{q}\Big]\\
&= q^{\frac{n-2}{2}}\varepsilon(-1+\varepsilon_0\sqrt{q})\theta_v(-aB,\varepsilon^u).
\end{aligned}$$

Rearranging the terms, we obtain the expression

$$N = N_1 q^{\frac{n}{2}} + N_2 q^{\frac{n-1}{2}} + N_3 q^{\frac{n-2}{2}},$$

proving the statement. ∎

Theorem 3.22. *Assume that $B \neq 0$ and $d > 2$. We denote $\alpha_1 = \theta_d(-aB, \varepsilon^u \varepsilon_0^{u_0})$ and $\alpha_2 = \theta_v(-aB, 1)$. If d is (p,r)-admissible, D is even and (p,r_0)-admissible, then*

$$N = N_1 q^{\frac{n}{2}} + N_2 q^{\frac{n-1}{2}} + N_3 q^{\frac{n-2}{2}},$$

where

- $N_1 = (-1)^s \varepsilon\varepsilon_0 \tau^s \chi_2(B)\big[-\varepsilon_0^{u_0\frac{D}{2}}\alpha_1 + \varepsilon^{u\frac{D}{2}}\chi_{2v}(-aB)(1+\alpha_2)\big]$,
- $N_2 = \varepsilon\varepsilon_0\big(\alpha_2 - \alpha_1\big) - (-1)^s \varepsilon^{u\frac{D}{2}+1}\tau^s \chi_{2v}(-aB)\chi_2(B)(1+\alpha_2)$,
- $N_3 = -\varepsilon\alpha_2$.

Proof. By hypothesis d is (p,r)-admissible and D is even. By Proposition 3.7,

$$N = \frac{1}{q}\sum_{\ell=1}^{d-1} G_n\big(\chi_d^\ell\big)\Big[(-1)^{s+1}\chi_d^\ell(-aB)\chi_2(B)\tau^s\sqrt{q}\,G_1\big(\eta_D^{\frac{D}{2}-\ell}\big) - \chi_d^\ell(-aB)G_1\big(\eta_D^{-\ell}\big)\Big].$$

Therefore, since D is (p,r_0) admissible

$$\begin{aligned}
N &= -q^{\frac{n-2}{2}}\sum_{\ell=1}^{d-1}\varepsilon^{u\ell+1}\chi_d^\ell(-aB)\Big[-(-1)^{s+1}\tau^s\chi_2(B)\varepsilon_0^{u_0(\ell+\frac{D}{2})+1}q + \varepsilon_0^{u_0\ell+1}\sqrt{q}\Big] + R\\
&= -q^{\frac{n-1}{2}}\varepsilon\varepsilon_0\Big((-1)^s\tau^s\chi_2(B)\varepsilon_0^{u_0\frac{D}{2}}\sqrt{q}+1\Big)\sum_{\ell=1}^{d-1}\big(\chi_d(-aB)\varepsilon^u\varepsilon_0^{u_0}\big)^\ell + R,\\
&= -q^{\frac{n-1}{2}}\varepsilon\varepsilon_0\Big((-1)^s\tau^s\chi_2(B)\varepsilon_0^{u_0\frac{D}{2}}\sqrt{q}+1\Big)\theta_d(-aB,\varepsilon^u\varepsilon_0^{u_0}) + R,
\end{aligned}$$

where $R = R_1 + R_2$,

$$\begin{aligned}
R_1 &= -q^{\frac{n-2}{2}}\sum_{j=0}^{d/D-1}\varepsilon^{u\left(\frac{D}{2}(2j+1)\right)+1}\chi_d^{\frac{D}{2}(2j+1)}(-aB)(-1)^{s+1}\big[-\chi_2(B)\sqrt{q}\,\tau^s + \tau^s\chi_2(B)\varepsilon_0^{u_0\left(\frac{D}{2}(2j+1)+\frac{D}{2}\right)+1}q\big]\\
&= (-1)^s q^{\frac{n-1}{2}}\varepsilon^{u\frac{D}{2}+1}\tau^s\chi_{2v}(-aB)\chi_2(B)\sum_{j=0}^{d/D-1}\big(\varepsilon^{uD}\chi_v(-aB)\big)^j(-1+\sqrt{q}\,\varepsilon_0^{u_0Dj+u_0D+1})\\
&= (-1)^s q^{\frac{n-1}{2}}\varepsilon^{u\frac{D}{2}+1}\tau^s\chi_{2v}(-aB)\chi_2(B)\sum_{j=0}^{d/D-1}\big[-\big(\varepsilon^{uD}\chi_v(-aB)\big)^j + \big(\varepsilon^{uD}\varepsilon_0^{u_0D}\chi_v(-aB)\big)^j\varepsilon_0^{u_0D+1}\sqrt{q}\big]\\
&= (-1)^s q^{\frac{n-1}{2}}\varepsilon^{u\frac{D}{2}+1}\tau^s\chi_{2v}(-aB)\chi_2(B)\big[-(1+\theta_v(-aB,\varepsilon^{uD})) + (1+\theta_v(-aB,\varepsilon^{uD}\varepsilon_0^{u_0D}))\varepsilon_0^{u_0D+1}\sqrt{q}\big]\\
&= (-1)^s q^{\frac{n-1}{2}}\varepsilon^{u\frac{D}{2}+1}\tau^s\chi_{2v}(-aB)\chi_2(B)(1+\theta_v(-aB,1))(\varepsilon_0^{\frac{uD}{2}}\sqrt{q}-1)
\end{aligned}$$

and

$$\begin{aligned}
R_2 &= -q^{\frac{n-2}{2}}\sum_{j=1}^{d/D-1}\varepsilon^{ujD+1}\chi_d^{jD}(-aB)\Big[1-\sqrt{q}\,\varepsilon_0^{u_0jD+1}\Big]\\
&= -q^{\frac{n-2}{2}}\varepsilon\sum_{j=1}^{d/D-1}\Big[\big(\varepsilon^{uD}\chi_v(-aB)\big)^j - \varepsilon_0\big(\varepsilon^{uD}\varepsilon_0^{u_0D}\chi_v(-aB)\big)^j\sqrt{q}\Big]\\
&= -q^{\frac{n-2}{2}}\varepsilon\Big[\theta_v(-aB,1) - \varepsilon_0\theta_v(-aB,1)\sqrt{q}\Big]\\
&= -q^{\frac{n-2}{2}}\varepsilon\theta_v(-aB,1)(1-\varepsilon_0\sqrt{q}).
\end{aligned}$$

Altogether, we have shown that

$$N = N_1 q^{\frac{n}{2}} + N_2 q^{\frac{n-1}{2}} + N_3 q^{\frac{n-2}{2}},$$

proving the statement. ■

CHAPTER 4

Polynomials over binary fields with sparse factors

Let $\mathbb{F}_q$ be a finite field with q elements, where q is a power of 2. In this chapter we study the positive integers n for which the irreducible factors of the polynomial $x^n - 1$ over $\mathbb{F}_q$ are all binomials and trinomials. In particular, we completely describe these integers for $q = 2, 4$.

4.1 Introduction

The factorization of polynomials is a classical topic of study in the theory of finite fields, playing important roles in a wide variety of applications such as coding theory [5] and cryptography [28]. One remarkable class of polynomials that nicely exemplifies this applicability is the class of binomials $x^n - 1$: each irreducible factor of $x^n - 1$ over a finite field $\mathbb{F}$ determines a cyclic code of length n over $\mathbb{F}$ (see [47]). The binomials $x^n - 1$ naturally decomposes into a product of cyclotomic polynomials. However, in contrast to the rational field case, they are usually reducible over finite fields. This makes the factorization of binomials $x^n - 1$ over finite fields a challenging problem. Many authors have explored the issue of factorizing $x^n - 1$ under special conditions [6, 11, 33, 49]. Perhaps, the most notable result is given in [7], where the explicit factorization of $x^n - 1$ over $\mathbb{F}$ is given under the condition that each prime factor of n divides $q^2 - 1$, where q is the order of the field $\mathbb{F}$. Moreover, under this condition, an interesting phenomena occurs: all the irreducible factors of $x^n - 1$ over $\mathbb{F}$ are binomials and trinomials.

Motivated by the results in [7], in this chapter we explore the aforementioned phenomena over binary fields. In other words, given a finite field $\mathbb{F}_q$ of even order q, we study the positive integers n for which the polynomial $x^n - 1$ factors into irreducible binomials and trinomials over $\mathbb{F}_q$. Our main results provide the complete description of such n's for $q = 2, 4$. Moreover, for such values of n, the explicit factorization of $x^n - 1$ over $\mathbb{F}_q$ is readily obtained. For more details, see Theorems 4.10 and 4.13. The key idea in the proofs of our main results is to explore the prime numbers satisfying this property, as they already restrict the possible prime factors of n. Our methods rely on basic combinatorial arguments, combined with classical results on cyclotomic polynomials and irreducible trinomials over binary fields.

The chapter is organized as follows. In Section 4.2 we provide a series of auxiliary lemmas and definitions that are used throughout the chapter. In Section 4.3 we state and prove our main results.

4.2 Preparation

Throughout this chapter, q is always a power of 2. For an integer $n > 1$, we recall that $\mathrm{rad}(n)$ denotes the product of the distinct prime factors of n. Moreover, if a, b are positive integers with $\gcd(a, b) = 1$, $\mathrm{ord}_b a$ is the order of a modulo b, i.e., the least positive integer u such that $a^u \equiv 1 \pmod{b}$. The following definition is extensively used in the chapter and it will be quite helpful in presenting and proving the results.

Definition 4.1. *For a positive integer n, the pair (n, q) is* 3-sparse *if the irreducible factors of the polynomial $x^n - 1$ over $\mathbb{F}_q$ are all binomials and trinomials.*

It follows directly by the definition that the pair $(1, q)$ is 3-sparse. We recall the definition of cyclotomic polynomials over finite fields, specializing to binary fields. For an odd integer $d \ge 1$, the d-th cyclotomic polynomial $\Phi_d(x) \in \mathbb{F}_q[x]$ is given by the recursive formula $x^d - 1 = \prod_{e|d} \Phi_e(x)$. The following is easily checked.

Remark 4.2. *(a) For every positive integers s and n, we have that $x^{2^s \cdot n} - 1 = (x^n - 1)^{2^s}$. In particular, for every $s \ge 1$, either both or none of the pairs (n, q) and $(2^s \cdot n, q)$ are 3-sparse.*

(b) If (n, q) is 3-sparse and $d \ge 1$ is any divisor of n, then (d, q) is 3-sparse.

In particular, we only need to look at pairs (n,q), where $n>1$ is odd. Moreover, the prime numbers play an important role in the description of the 3-sparse pairs.

4.2.1 Lemmata

Here we present a series of lemmas that are frequently employed throughout this chapter. Although most of them hold for general finite fields, for simplicity, we state them in the context of binary fields.

Recall that for a polynomial $f \in \mathbb{F}_q[x]$, not divisible by x, the exponent (or order) of f is the least positive integer e such that f divides $x^e - 1$. Clearly, if d is odd, $\Phi_d(x)$ has exponent d. We have the following result.

Lemma 4.3. *([30], Theorem 3.35) Let n be a positive integer and let $f \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree m and exponent e. Then the polynomial $f(x^n)$ is irreducible over $\mathbb{F}_q$ if and only if the following conditions are satisfied:*

(i) rad(n) divides e;

(ii) $\gcd\left(n, \frac{q^m-1}{e}\right) = 1$ and

(iii) if 4 divides n, then 4 divides $q^m - 1$.

In addition, if $f(x^n)$ is irreducible, then it has degree mn and exponent en.

The following classical result, due to Swan, concerns about the irreducibility of trinomials over the field $\mathbb{F}_2$.

Lemma 4.4. *([44], Corollary 5) Let $n > k$ be positive integers and suppose that exactly one of the elements n, k is odd. Furthermore, let r be the number of irreducible factors of $f(x) = x^n + x^k + 1$ over $\mathbb{F}_2$. Then $r \equiv 0 \pmod 2$ in the following cases:*

1. *n is even and k is odd, $n \neq 2k$ and $\frac{nk}{2} \equiv 0, 1 \pmod 4$*
2. *n is odd and k is even, k does not divide 2n and $n \equiv 3, 5 \pmod 8$*
3. *n is odd and k is even, k divides 2n and $n \equiv 1, 7 \pmod 8$.*

Moreover, the polynomials $f^*(x) = x^n + x^{n-k} + 1 \in \mathbb{F}_2[x]$ and $f(x)$ have the same number of irreducible factors over $\mathbb{F}_2$.

Results like Lemma 4.4 were discovered for fields of odd characteristic [23] and high extensions of $\mathbb{F}_2$. One of them, contained in the following lemma, covers even degree extensions of $\mathbb{F}_2$.

Lemma 4.5. *([48],Corollary 5.1) Let K be an even degree extension of $\mathbb{F}_2$. Then every trinomial of even degree is reducible over K, except possibly for $x^{2d} + ax^d + b \in K[x]$, where $t^2 + at + b$ has no roots in K.*

The following result from [7] characterizes the binomial divisors of $x^n - 1$ over $\mathbb{F}_q$.

Lemma 4.6. *Let t, n be positive integers and let $a \in \mathbb{F}_q^*$ be an element of order M. Then $x^t - a$ divides $x^n - 1$ if and only if n is divisible by tM.*

Proof. Let α be a root of $x^t - a$. Let suppose that $x^t - a$ divides $x^n - 1$, then $\alpha^{tM} = a^M = 1$. Since M is the order of a and $\alpha^n = 1$, we conclude that n is divisible by tM.

Now let suppose that tM divides n. From the fact that $\alpha^t = a$ we have that $\alpha^{tM} = a^n = 1$ and this implies that $\alpha^n = \left(\alpha^{tM}\right)^{\frac{n}{tM}} = 1$. Therefore α is also a root of $x^n - 1$ and $x^t - a$ divides $x^n - 1$. ■

The following lemma characterizes a special class of irreducible polynomials over $\mathbb{F}_2$.

Lemma 4.7. *Let $t \geq 3$ be an odd integer and let f be an irreducible polynomial over $\mathbb{F}_2$ that splits into two t-degree irreducible trinomials over $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$. Then there exists a positive integer $k < t$ such that f has one of the following forms:*

$$F_{k,t}(x) := x^{2t} + x^{t+k} + x^{2k} + x^k + 1 = (x^t + \alpha x^k + 1)(x^t + \alpha^2 x^k + 1),$$
$$G_{k,t}(x) := x^{2t} + x^{t+k} + x^{2k} + x^t + 1 = (x^t + \alpha x^k + \alpha)(x^t + \alpha^2 x^k + \alpha^2),$$
$$H_{k,t}(x) := x^{2t} + x^t + x^{2k} + x^k + 1 = (x^t + x^k + \alpha)(x^t + x^k + \alpha^2).$$

Proof. Let $\sigma : \mathbb{F}_4 \to \mathbb{F}_4$ be the $\mathbb{F}_2$-automorphism with $\sigma(\beta) = \beta^2$. We observe that σ has a natural extension for the polynomial ring $\mathbb{F}_4[x]$ and for simplicity, σ also denotes this extension. If $g(x) = x^t + ax^k + b$ is one of the irreducible factors of f over $\mathbb{F}_4$, then $g \not\in \mathbb{F}_2[x]$ since f is irreducible over $\mathbb{F}_2$. In particular, we have that $f(x) = g(x) \cdot \sigma(g(x))$, where $\sigma(g(x)) = x^t + a^2 x^k + b^2$. Since g is irreducible, it follows that $g(1) \neq 0$. The latter, combined with the fact that $g \not\in \mathbb{F}_2[x]$, implies that g has one of the following forms

$$\{x^t + \beta x^k + 1, x^t + \beta x^k + \beta, x^t + x^k + \beta\},$$

where $\beta = \alpha$ or $\beta = \alpha^2$. The result follows from the equality $f(x) = g(x) \cdot \sigma(g(x))$. ■

We emphasize that, since t is odd, the polynomials in the previous lemma are indeed pentanomials, i.e., there is no monomial cancellation.

4.3 Main results

In this section we state and prove our main results of this chapter. The following lemma provides some general information on 3-sparse pairs over binary fields.

Lemma 4.8. *Let p be an odd prime, set $t = \operatorname{ord}_p q$ and suppose that (p,q) is 3-sparse. If $t > 1$, the irreducible factors of $\Phi_p(x)$ over $\mathbb{F}_q$ are all trinomials. In particular, if q is an even power of 2, then $t = 2$ or t is odd.*

Proof. Lemma 4.6 entails that, if $t > 1$, then $x-1$ is the only irreducible binomial divisor of $x^p - 1 = (x-1)\cdot\Phi_p(x)$ over $\mathbb{F}_q$. This proves the first statement. For the second statement, suppose that t is even and q is an even power of 2. It suffices to prove that $t = 2$. From Lemma 1.16 and the first statement, we obtain that

$$\Phi_p(x) = x^{p-1} + \cdots + x + 1 = \prod_i^{\ell}(x^t + a_i x^{k_i} + b_i),$$

where $\ell = \frac{p-1}{t}$, $a_i, b_i \in \mathbb{F}_q^*$ and $0 < k_i < t$. Comparing both sides of the previous equality, we conclude that $k_i = 1$ for some $1 \le i \le l$. In particular, it follows that there exists an irreducible trinomial $x^t + ax + b \in \mathbb{F}_q[x]$. Since t is even and q is an even power of 2, Lemma 4.4 entails that $t = 2$. ∎

We obtain the following corollary.

Corollary 4.9. *Let n be odd, let q be an even power of 2 and suppose that $\gcd(n, q^2-1) = \gcd(n, q-1)$. If the pair (n,q) is 3-sparse, then (n,q^2) is also 3-sparse.*

Proof. Let p be a prime that divides n. Then (p,q) is 3-sparse and, from Lemma 4.8, we have that $t = \operatorname{ord}_p q$ is odd or $t = 2$. The case $t = 2$ cannot occur since $\gcd(n, q-1) = \gcd(n, q^2-1)$ and so t is odd. In particular, if d is any divisor of n, we have that $\operatorname{ord}_d q$ is also odd and so $\operatorname{ord}_d q = \operatorname{ord}_d q^2$. Therefore, from Lemma 1.16, the irreducible factors of $x^n - 1$ over $\mathbb{F}_q$ coincide with the ones over $\mathbb{F}_{q^2}$. In particular, if (n,q) is 3-sparse, then (n,q^2) is also 3-sparse. ∎

We are ready to classify the integers n such that $(n,2)$ is 3-sparse.

Theorem 4.10. *Let $n > 1$ be odd. The pair $(n,2)$ is 3-sparse if and only if $n = 3^k$ or $n = 7^k$ for some positive integer k. Furthermore, we have the following factorizations into irreducible polynomials over $\mathbb{F}_2$:*

(i) $\Phi_{3^k}(x) = (x^{2\cdot 3^{k-1}} + x^{3^{k-1}} + 1)$.

(ii) $\Phi_{7^k}(x) = (x^{3\cdot 7^{k-1}} + x^{2\cdot 7^{k-1}} + 1)(x^{3\cdot 7^{k-1}} + x^{7^{k-1}} + 1)$.

Proof. Let $p > 3$ be a prime, set $t = \mathrm{ord}_p 2$ and suppose that $(p,2)$ is 3-sparse. Since $p > 3$, we have that $t > 2$ and so Lemma 4.8 implies that

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \prod_{i=1}^{s}(x^t + x^{a_i} + 1), \tag{4.1}$$

where s and $a_1 < a_2 < \cdots < a_s < t$ are positive integers. Since $p > 3$ and $t > 2$, a comparison on the monomials appearing in both sides of Eq. (4.1) implies that $a_1 = 1$ and $a_2 = 2$. In particular, the polynomials $x^t + x + 1$ and $x^t + x^2 + 1$ are irreducible over $\mathbb{F}_2$, hence t is odd. Lemma 4.4 entails that $x^t + x^{t-1} + 1$ is also irreducible over $\mathbb{F}_2$. In particular, the number of irreducible factors of $x^t + x^2 + 1$ and $x^t + x^{t-1} + 1$ over $\mathbb{F}_2$ are both odd. Since 2 divides $2t$, Lemma 4.4 implies that $t \equiv 3, 5 \pmod 8$ and $t - 1$ divides $2t$. Since $t > 2$, the latter implies that $t = 3$ and so $p = 7$. In conclusion, if p is an odd prime and $(p,2)$ is 3-sparse, then $p = 3, 7$. Therefore, if $n > 1$ is odd and $(n,2)$ is 3-sparse, from Remark 4.2 we obtain that $\mathrm{rad}(n) \in \{3, 7, 21\}$. We split the proof into cases:

(i) $n = 3^k$. In this case, Lemma 1.18 entails that

$$\Phi_{3^k}(x) = \Phi_3(x^{3^{k-1}}) = x^{2\cdot 3^{k-1}} + x^{3^{k-1}} + 1.$$

Lemma 4.3 ensures that, for every $k \geq 1$, the polynomial $\Phi_{3^k}(x)$ is irreducible over $\mathbb{F}_2$.

(ii) $n = 7^k$. Since $\Phi_7(x) = (x^3 + x^2 + 1)(x^3 + x + 1)$, Lemma 1.18 entails that

$$\Phi_{7^k}(x) = (x^{3\cdot 7^{k-1}} + x^{2\cdot 7^{k-1}} + 1)(x^{3\cdot 7^{k-1}} + x^{7^{k-1}} + 1).$$

From Lemma 4.3, the latter is the factorization of $\Phi_{7^k}(x)$ into irreducible polynomials over $\mathbb{F}_2$.

(iii) $\mathrm{rad}(n) = 21$. This case cannot occur since we have the following factorization of $\Phi_{21}(x)$ into irreducible polynomials over $\mathbb{F}_2$:

$$\Phi_{21}(x) = (x^6 + x^4 + x^2 + x + 1)(x^6 + x^5 + x^4 + x^2 + 1).$$

■

We proceed to the characterization of the pairs $(n,4)$ that are 3-sparse. The following two results are crucial.

Lemma 4.11. *Let $p > 7$ be a prime number, set $t = \mathrm{ord}_p 4$ and suppose that the pair $(p,4)$ is 3-sparse. Then every irreducible factor of $\Phi_p(x)$ over $\mathbb{F}_2$ equals one of the pentanomials given in Lemma 4.7.*

Proof. Since $p > 7$, we have that $t = \mathrm{ord}_p 4 > 2$. In particular, since 4 is an even power of 2, Lemma 4.8 entails that t is odd and all the irreducible factors of $\Phi_p(x)$ over $\mathbb{F}_4$ are trinomials. If we set $s = \mathrm{ord}_p 2$, we have that $s = t$ or $s = 2t$. If $s = t$, Lemma 1.16 entails that the factorization of $\Phi_p(x)$ into irreducible polynomials over $\mathbb{F}_2$ coincides with the one over $\mathbb{F}_4$, hence the pair $(p,2)$ is also 3-sparse.The latter contradicts Theorem 4.10 since $p > 7$. Therefore, $s = 2t$ and then, from Lemma 1.16, we conclude that each irreducible factor of $\Phi_p(x)$ over $\mathbb{F}_2$ has degree $2t$ and splits into two irreducible trinomials over $\mathbb{F}_4$, each of degree t. The result follows from Lemma 4.7. ■

We obtain the following result.

Proposition 4.12. *Let $p > 7$ be a prime such that $(p,4)$ is 3-sparse and set $t = \mathrm{ord}_p 4$. Then one of the polynomials $F_{3,t}(x)$, $H_{3,t}(x)$, given in Lemma 4.7, divides $\Phi_p(x)$ and $t \equiv 0 \pmod 3$.*

Proof. From Lemma 4.11, there exist sets $A, B, C \subseteq \mathbb{N}_{>0}$ such that

$$\Phi_p(x) = x^{p-1} + \cdots + x + 1 = \left(\prod_{a\in A} F_{a,t}(x)\right) \cdot \left(\prod_{b\in B} G_{b,t}(x)\right) \cdot \left(\prod_{c\in C} H_{c,t}(x)\right), \tag{4.2}$$

where $F_{a,t}(x)$, $G_{b,t}(x)$ and $H_{c,t}(x)$ are irreducible pentanomials over $\mathbb{F}_2$ given in Lemma 4.7. Our idea is to obtain information on the sets A, B and C by comparing the monomials appearing in both sides of Eq. (4.2). Since $p > 7$, we have that $t > 3$ and the monomials x^i with $1 \le i \le 3$ appear in the LHS of Eq. (4.2), so the same must hold in the RHS. We observe that only $F_{1,t}(x)$ and $H_{1,t}(x)$ have the monomial x, hence $1 \in A \cup C$. Since the product $F_{1,t}(x)H_{1,t}(x)$ does not have the term x, it follows that $1 \notin A \cap C$. The latter implies that the monomial x^2 does not appear as a product $x \cdot x$ in the RHS of Eq. (4.2). Therefore, if s denotes the number of pentanomials in the RHS of Eq. (4.2) having the term x^2, it follows that s is odd. For $t > 3$, we list all the pentanomials given in Lemma 4.7, containing term x^2:

$$\{F_{1,t}(x), F_{2,t}(x), G_{1,t}(x), H_{1,t}(x), H_{2,t}(x)\}.$$

Since $1 \notin A \cap C$, it follows that $s < 5$ and so $s = 1, 3$. We split into cases.

(i) $s = 1$. In this case, since $1 \in A \cup C$, we have exactly two possibilities: $\{F_{1,t}(x)\}$ or $\{H_{1,t}(x)\}$. In both cases, no monomial x^3 is generated by a product $x \cdot x^2$. In particular, a pentanomial with the term x^3 must appear in the RHS of Eq. (4.2). Since $t > 3$, we have exactly two pentanomials having the term x^3: $F_{3,t}(x)$ and $H_{3,t}(x)$.

(ii) $s = 3$. Since $1 \notin A \cap C$, we have exactly two possibilities

$$\{F_{1,t}(x), F_{2,t}(x), G_{1,t}(x)\} \quad \text{or} \quad \{H_{1,t}(x), H_{2,t}(x), G_{1,t}(x)\}.$$

Since $1 \notin A \cap C$ and the monomial x^2 appears three times we have exactly six possibilities: all of them containing exactly one of the polynomials $\{F_{1,t}, H_{1,t}\}$ and two more polynomials in the set $\{F_{2,t}, G_{1,t}, H_{2,t}\}$. In both cases, the product of the corresponding polynomials does not produce the term x^3. Similarly to the case $s = 1$, we conclude that either $F_{3,t}(x)$ or $H_{3,t}(x)$ must appear in the RHS of Eq. (4.2).

For $\alpha \in \mathbb{F}_4 \setminus \mathbb{F}_2$, we observe that $F_{3,t}(\alpha) = H_{3,t}(\alpha) = \alpha^{2t} + \alpha^t + 1$. For $t \not\equiv 0 \pmod 3$, it follows that $\alpha^{2t} + \alpha^t + 1 = 0$. The latter implies that $F_{3,t}(x)$ and $H_{3,t}(x)$ have a root in $\mathbb{F}_4$ if $t \not\equiv 0 \pmod 3$, a contradiction with the fact that these pentanomials split into exactly two irreducible trinomials over $\mathbb{F}_4$. Therefore, $t \equiv 0 \pmod 3$. ■

We now describe the pairs $(n, 4)$ that are 3-sparse, where $n > 1$ is odd.

Theorem 4.13. *Let $n > 1$ be odd. Then the pair $(n, 4)$ is 3-sparse if and only if n has one of the following forms:*

$$3^k, 5^k, 7^k, 3^m \cdot 5^k, 3 \cdot 7^k,$$

where m, k are positive integers. Moreover, for $\alpha \in \mathbb{F}_4 \setminus \mathbb{F}_2$, we have the following factorizations into irreducible polynomials over $\mathbb{F}_4$

(i) $\Phi_{3^k}(x) = (x^{3^{k-1}} + \alpha)(x^{3^{k-1}} + \alpha^2)$;

(ii) $\Phi_{5^k}(x) = (x^{2\cdot 5^{k-1}} + \alpha x^{5^{k-1}} + 1)(x^{2\cdot 5^{k-1}} + \alpha^2 x^{5^{k-1}} + 1)$;

(iii) $\Phi_{7^k}(x) = (x^{3\cdot 7^{k-1}} + x^{2\cdot 7^{k-1}} + 1)(x^{3\cdot 7^{k-1}} + x^{7^{k-1}} + 1)$;

(iv) $\Phi_{3^m \cdot 5^k}(x) = \prod_{i=1}^{2} (x^{2\cdot 3^{m-1}\cdot 5^{k-1}} + x^{3^{m-1}\cdot 5^{k-1}} + \alpha^i)(x^{2\cdot 3^{m-1}\cdot 5^{k-1}} + \alpha^i x^{3^{m-1}\cdot 5^{k-1}} + \alpha^i)$;

(v) $\Phi_{3\cdot 7^k}(x) = \prod_{i=1}^{2} (x^{3\cdot 7^{k-1}} + \alpha^i x^{2\cdot 7^{k-1}} + 1)(x^{3\cdot 7^{k-1}} + \alpha^i x^{7^{k-1}} + 1)$.

Proof. Suppose that $p > 7$ is a prime such that $(p,4)$ is 3-sparse. From Lemma 4.7 and Proposition 4.12, it follows that some irreducible factor of $\Phi_p(x)$ over $\mathbb{F}_4$ is of the form $x^{3\ell} + ax^3 + b$. From Lemma 4.3, such polynomial has exponent divisible by 3, hence 3 divides p and so $p = 3$. The latter contradicts our assumption $p > 7$. In particular, if p is an odd prime and $(p,4)$ is 3-sparse, then $p = 3,5,7$. Therefore, if $n > 1$ is odd and $(n,4)$ is 3-sparse, from Remark 4.2 we obtain that $\mathrm{rad}(n) \in \{3,5,7,15,21,35,105\}$. We split the proof into cases:

(i) $n = 3^k$. We observe that

$$\Phi_3(x) = (x-\alpha)(x-\alpha^2).$$

From Lemma 1.18, we have that $\Phi_{3^k}(x) = \Phi_3(x^{3^{k-1}})$. Using the criterion described in Lemma 4.3, we conclude that the polynomials $x^{3^{k-1}} + \alpha^i$ with $i \in \{1,2\}$ are irreducible over $\mathbb{F}_4$ for every $k \geq 1$.

(ii) $n = 5^k$. We observe that

$$\Phi_5(x) = (x^2 + \alpha x + 1)(x^2 + \alpha^2 x + 1).$$

From Lemma 1.18, we have that $\Phi_{5^k}(x) = \Phi_5(x^{5^{k-1}})$. Using the criterion described in Lemma 4.3, we conclude that the polynomials $x^{2\cdot 5^{k-1}} + \alpha^i x^{5^{k-1}} + 1$ with $i \in \{1,2\}$, are irreducible over $\mathbb{F}_4$ for every $k \geq 1$.

(iii) $n = 7^k$. In this case, $\mathrm{ord}_{7^k} 2 = \mathrm{ord}_{7^k} 4 = 3 \cdot 7^{k-1}$. From Lemma 1.16, the factorization of $\Phi_{7^k}(x)$ into irreducible polynomials over $\mathbb{F}_2$ coincides with the one over $\mathbb{F}_4$. The result follows from Theorem 4.10.

(iv) $\mathrm{rad}(n) = 15$. We observe that

$$\Phi_{15}(x) = \prod_{i=1}^{2}(x^2 + x + \alpha^i)(x^2 + \alpha^i x + \alpha^i).$$

Moreover, from Lemma 1.18, we have that $\Phi_{3^m.5^k}(x) = \Phi_{15}(x^{3^{m-1}.5^{k-1}})$ and applying the criterion described in Lemma 4.3, we conclude that the polynomials $(x^{2\cdot 3^{m-1}.5^{k-1}} + x^{3^{m-1}.5^{k-1}} + \alpha^i)(x^{2\cdot 3^{m-1}.5^{k-1}} + \alpha^i x^{3^{m-1}.5^{k-1}} + \alpha^i)$ with $i \in \{1,2\}$, are irreducible over $\mathbb{F}_4$ for every $k, m \geq 1$.

(v) $\mathrm{rad}(n) = 21$. We observe that

$$\Phi_{21}(x) = \prod_{i=1}^{2}(x^3 + \alpha^i x^2 + 1)(x^3 + \alpha^i x + 1).$$

Lemma 1.18 implies that $\Phi_{3.7^k}(x) = \Phi_{21}(x^{7^{k-1}})$ and, using the criterion described in Lemma 4.3, we conclude that the polynomials $x^{3\cdot 7^{j-1}} + \alpha^i x^{j\cdot 7^{k-1}} + 1$ with $i, j \in \{1,2\}$, are irreducible over $\mathbb{F}_4$ for every $k \geq 1$. However, if 63 divides n it follows that $\Phi_{63}(x)$ is a factor of $x^n - 1$. We directly verify that the irreducible factors of $\Phi_{63}(x)$ over $\mathbb{F}_4$ are not all binomials and trinomials and so $(n,4)$ is not 3-sparse.

(vi) $\mathrm{rad}(n) = 35, 105$. In this case, $\Phi_{35}(x)$ is a factor of $x^n - 1$. We directly verify that the irreducible factors of $\Phi_{35}(x)$ and $\Phi_{105}(x)$ over $\mathbb{F}_4$ are not all binomials and trinomials and so $(n,4)$ is not 3-sparse.

■

The possible values for n such that the binomial $x^n - 1$ splits into irreducible binomials and trinomials over $\mathbb{F}_q$ in the cases $q = 2$ or $q = 4$ are describe in the following table.

Table 4.1: Polynomials that are 3-sparse for $q = 2$ or $q = 4$
m, k are positive integers

q	n	Factorization of $\Phi_n(x)$
2	3^k	$\Phi_{3^k}(x) = (x^{2\cdot 3^{k-1}} + x^{3^{k-1}} + 1)$
2	7^k	$\Phi_{7^k}(x) = (x^{3\cdot 7^{k-1}} + x^{2\cdot 7^{k-1}} + 1)(x^{3\cdot 7^{k-1}} + x^{7^{k-1}} + 1)$
4	3^k	$\Phi_{3^k}(x) = (x^{3^{k-1}} + \alpha)(x^{3^{k-1}} + \alpha^2)$
4	5^k	$\Phi_{5^k}(x) = (x^{2\cdot 5^{k-1}} + \alpha x^{5^{k-1}} + 1)(x^{2\cdot 5^{k-1}} + \alpha^2 x^{5^{k-1}} + 1)$
4	7^k	$\Phi_{7^k}(x) = (x^{3\cdot 7^{k-1}} + x^{2\cdot 7^{k-1}} + 1)(x^{3\cdot 7^{k-1}} + x^{7^{k-1}} + 1)$
4	$3^m \cdot 5^k$	$\Phi_{3^m . 5^k}(x) = \prod_{i=1}^{2} (x^{2\cdot 3^{m-1}.5^{k-1}} + x^{3^{m-1}.5^{k-1}} + \alpha^i)(x^{2\cdot 3^{m-1}.5^{k-1}} + \alpha^i x^{3^{m-1}.5^{k-1}} + \alpha^i)$
4	$3 \cdot 7^k$	$\Phi_{3.7^k}(x) = \prod_{i=1}^{2} (x^{3\cdot 7^{k-1}} + \alpha^i x^{2\cdot 7^{k-1}} + 1)(x^{3\cdot 7^{k-1}} + \alpha^i x^{7^{k-1}} + 1)$

Chapter 5

Concluding remarks and further research

In this chapter we present some comments on future research works that naturally arises from the topics in this thesis.

5.1 Quadratic forms and affine rational points of Artin-Schreier curves

In Chapter 2 we studied the number of affine rational points of Artin-Schreier curves of the type

$$\mathscr{C}_{F,\lambda} : y^q - y = xF(x) - \lambda,$$

for F a $\mathbb{F}_q$-linearized polynomial and $\lambda \in \mathbb{F}_{q^n}$. We note that in Theorem 2.13 we determined the number of affine rational points in $\mathbb{F}_{q^n}^2$ when $F(x)$ is an $\mathbb{F}_q$ linearized and such that $g(x) = \gcd(f(x), x^n - 1)$ is self-reciprocal, where f is the associated to F. We then have two problems:

Problem 5.1. *Determine $N_n(\mathscr{C}_{F,\lambda})$ when $F(x) = xS(x) + Tr(x)$ where $S(x)$ is a $\mathbb{F}_q$-linearized polynomial.*

Problem 5.2. *Determine $N_n(\mathscr{C}_{F,\lambda})$ when g is not self-reciprocal.*

In [27], the authors show that the number of monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree n and with the first and third coefficients prescribed is related to the number of affine rational points of the curve

$$y^q - y = x^{2q+1} - x^{q+2},$$

in $\mathbb{F}_{q^n}$. Then, we have the following problem.

Problem 5.3. *Determine $N_r(\mathscr{C}_{xFG})$ when $F, G \in \mathbb{F}_q[x]$ are $\mathbb{F}_q$-linearized.*

5.2 The number of rational points of a class of superelliptic curves

In Chapter 3 we studied the number of $\mathbb{F}_{q^n}$-rational points of the superelliptic curve determined by

$$\mathscr{X}_{d,a,b} : y^d = ax\mathrm{Tr}(x) + b,$$

for suitable values of d and $a \in \mathbb{F}_{q^n}^*, b \in \mathbb{F}_{q^n}$ in odd characteristic. For this type of curves we have the following problems.

Problem 5.4. *Determine the number of $\mathbb{F}_{q^n}$-rational points of $\mathscr{X}_{d,a,b}$ in even characteristic.*

Problem 5.5. *Determine another quadratic form Q such that we can compute the number of $\mathbb{F}_{q^n}$-rational points of the superelliptic curve*

$$\mathscr{X}_Q : y^d = Q(x).$$

Problem 5.6. *Determine a family $\mathscr{Q}$ of quadratic forms such that is possible to calculate the number of $\mathbb{F}_{q^n}$-rational points, or give bounds for this number, of the curve*

$$y^d = Q(x), \quad \textit{for} \quad Q \in \mathscr{Q}.$$

5.3 Polynomials over binary fields with sparse factors

In Chapter 4 we have described the integers n such that the binomial $x^n - 1$ splits into irreducible binomials and trinomials over $\mathbb{F}_q$, where $q = 2, 4$. We have also provided some minor results for generic powers of 2. We propose the following problem.

Problem 5.7. *Describe the 3-sparse pairs (n, q), where $q > 4$ is a power of two.*

We believe that the methods employed here for $q = 2,4$ are not sufficient to explore Problem 5.7 in its great generality, but it can be helpful for small q (e.g., $q = 8,16$). The case of even characteristic is more treatable since we have strong results on the irreducibility of trinomials over binary fields. Nevertheless, we have seen that prime numbers are crucial in the study of 3-sparse pairs. So exploring the primes p such that (p,q) is 3-sparse, where q is odd, could be interesting. In this context, we propose the following problem.

Problem 5.8. *Let q be a prime power. Prove or disprove: the set of prime numbers p such that (p,q) is 3-sparse is finite.*

In the context of Problem 5.8, Lemmas 1.16 and 4.6 imply that if $\gcd(p,q) = 1$, $t = \mathrm{ord}_p q > 1$ and (p,q) is 3-sparse, then $\Phi_p(x) = x^{p-1} + \cdots + x + 1$ splits into $s := \frac{p-1}{t}$ irreducible trinomials over $\mathbb{F}_q$. In particular, if $C_{q,t}$ is the number of distinct t-degree monic irreducible trinomials over $\mathbb{F}_q$, we have that $C_{q,t} \geq s$ and so $t \geq \frac{p-1}{C_{q,t}}$. We have the trivial bound $s \leq C_{q,t} \leq (q-1)^2 \cdot (t-1)$, but we may need something more precise. On the other hand, the product of s trinomials generates at most 3^s distinct monomials, hence $3^s \geq p$ and so $t \leq \frac{p-1}{\log_3 p}$. In conclusion,

$$\frac{p-1}{C_{q,t}} \leq t \leq \frac{p-1}{\log_3 p}$$

A more detailed account into the possible central monomials appearing in the trinomial factors of $\Phi_p(x)$ over $\mathbb{F}_q$ could be helpful in providing sharper bounds on s.

BIBLIOGRAPHY

[1] J. J. R. Aguirre and V. G. Neumann, Existence of primitive 2-normal elements in finite fields. *Finite Fields and Their Applications*, **73**, p. 101864 (2021).

[2] N. Anbar and W. Meidl, More on quadratic functions and maximal Artin-Schreier curves. *Applicable Algebra in Engineering, Communication and Computing*, **26**(5) 409-426, (2015).

[3] N. Anbar and W. Meidl, Quadratic functions and maximal Artin-Schreier curves, *Finite Fields and Their Applications,* **30** 49-71, (2014).

[4] Y. Aubry, Reed-Muller Codes associated to projective algebraic varieties. *Coding theory and algebraic geometry,* Springer 4-17, (1992).

[5] E. R. Berlekamp. *Algebraic Coding Theory*. McGraw-Hill, New York (1968).

[6] I.F. Blake, S. Gao, R. C. Mullin, Explicit factorization of $x^{2^k}+1$ over $\mathbb{F}_p$ with $p \equiv 3 \pmod 4$, *Applicable Algebra in Engineering, Communication and Computing* **4**, 89-94 (1993).

[7] F. E. Brochero Martínez, C. R. Giraldo Vergara, L. B. de Oliveira, Explicit factorization of $x^n - 1 \in \mathbb{F}_q[x]$. *Designs, Codes and Cryptography,* 77(1), 277-286 (2015).

[8] F. E. Brochero Martínez, J. A. Oliveira and D. Oliveira. *The number of rational points of a class of superelliptic curves*, *arXiv preprint:* `https://arxiv.org/abs/2209.06658`

[9] F. E. Brochero Martínez and D. Oliveira, Artin-Schreier curves given by $\mathbb{F}_q$-linearized polynomials. preprint: https://arxiv.org/abs/2012.01534, (2022).

[10] K. Cattell, C. R. Miers, F. Ruskey, M. Serra and J. Sawada, The number of irreducible polynomials over GF(2) with given trace and subtrace. *Journal of Combinatorial Mathematics and Combinatorial Computing,* **47**, 31 - 64 (2003).

[11] B. Chen, L. Li, R. Tuerhong, Explicit factorization of $x^{2^m p^n} - 1$ over a finite field. *Finite Fields and Their Applications,* **24**, 95-104 (2013).

[12] S. D. Cohen, H. Sharma and R. Sharma, Primitive values of rational functions at primitive elements of a finite field. *Journal of Number Theory,* **219**, 237-246 (2021).

[13] S. D. Cohen and T. Trudgian, Lehmer numbers and primitive roots modulo a prime. *Journal of Number Theory,* **203**, 68-79 (2019).

[14] R. S. Coulter. Explicit evaluations of some Weil sums. *Acta Arithmetica,* **83.3**, 241-251 (1998).

[15] A. Coşgun, F. Özbudak and Z. Saygi, Z, 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,* **79.3**, 423-441 (2016).

[16] R. S. Coulter, The number of affine rational points of a class of Artin–Schreier curves. *Finite Fields and Their Applications,* **8**, 397-413 (2002).

[17] R. J. Evans, Pure Gauss Sums over Finite Fields. *Mathematika,* **28.2**, 239-248 (1981).

[18] S. Farnell and R. Pries, Families of Artin-Schreier curves with Cartier–Manin matrix of constant rank. *Linear Algebra and its Applications,* **439**(7), 2158-2166, (2013).

[19] S. Galbraith, S. Paulus and N. Smart, Arithmetic on superelliptic curves. *Mathematics of Computation,* **71.237**, 393-405 (2002).

[20] C. Gilyoung, M. M. Wood and A. Zaman, The distribution of points on superelliptic curves over finite fields. *Proceedings of the American Mathematical Society,* **143.4**, 1365-1375 (2005).

[21] C. Güneri and F. Özbudak, Multidimensional cyclic codes and Artin-Schreier type hypersurfaces over finite fields. *Finite Fields and Their Applications,* **14.1**, 44-058 (2008).

[22] A. Gupta, R. K. Sharma and S. D. Cohen. Primitive element pairs with one prescribed trace over a finite field. *Finite Fields and Their Applications,* **54**, 1-14 (2018).

[23] B. Hanson, D. Panario and D. Thomson, Swan-like results for binomials and trinomials over finite fields of odd characteristic. *Designs. Codes and Cryptography,* **61(3)**, 273-283, (2011).

[24] A. Hefez and N. Kakuta, Polars of Artin-Schreier curves *Acta Arithmetica,* **77**, 57-70 (1996).

[25] I. Kra and S. R. Simanca, *On Circulant Matrices.* Notices of the AMS, (2012).

[26] P. Kulberg and Z. R. Rudnick, The fluctuations in the number of points on a hyperelliptic curve over a finite field. *Journal of Number Theory,* **129.3**, 580-587 (2009).

[27] M. Lalin and O. Larocque, The number of irreducible polynomials with the first two prescribed coefficients over a finite field. *Rocky Mountain Journal of Mathematics,* **46** no. 5, 1587-1618 (2016).

[28] H. W. Lenstra Jr, On the Chor–Rivest knapsack cryptosystem. *Journal of Cryptology,* **3**, 149-155 (1991).

[29] H. W. Lenstra Jr and R. J. Schoof, Primitive normal bases for finite fields. *Mathematics of Computation*, pp. 217-231 (1987).

[30] R. Lidl, H. Niederreiter, *Finite Fields*. Encyclopedia of Mathematics and its Applications, Vol **20**, Addison-Wesley (1983).

[31] R. Lidl and H. Niederreiter, *Finite Fields.* Cambridge University Press, Vol. **20.** (1997).

[32] G. McGuire and E. S. Yılmaz, The Number of Irreducible Polynomials with the First Two Coefficients Fixed over Finite Fields of Odd Characteristic. *Arxiv ID: 1609.02314.*

[33] H. Meyn H., Factorization of the cyclotomic polynomials $x^{2^n}+1$ over finite fields. *Finite Fields and Their Applications* 2, 439-442 (1996).

[34] H. Niederreiter and C. Xing, *Rational Points on Curves over Finite Fields: Theory and Applications*, Cambridge Uni. Press (2001).

[35] J. A. Oliveira. On diagonal equations over finite fields. *Finite Fields and Their Applications,* **76**, p. 101927 (2021).

[36] D. Oliveira. On the number of rational points of hypersuperficies of Artin-Schreier. `arxiv.` (2022)

[37] D. Oliveira and L. Reis. On polynomials $x^n - 1$ over binary fields whose irreducible factors are binomials and trinomials. *Finite Fields and Their Applications,* vol. **71**. p. 101837, (2021).

[38] F. Ozbudak and Z. Saygı, Rational points of the curve $y^{q^n} - y = \gamma x^{q^h+1} - \alpha$ over $\mathbb{F}_{q^m}$, *Applied Algebra and Number Theory.* Cambridge University Press, (2014).

[39] F. Ozbudak and Z. Saygi, Explicit maximal and minimal curves over finite fields of odd characteristics. *Finite Fields and Their Applications,* **42**, 81-92 (2016).

[40] A. Rojas-León, and D. Wan, Improvements of the Weil bound for Artin-Schreier curves. *Mathematische Annalen*, **351.2**, 417-442 (2011).

[41] R. P. Stanley, *Enumerative Combinatorics*. Cambridge University Press, Vol **2**, (1999).

[42] S. A. Stepanov, *Codes on algebraic curves.* Springer Science & Business Media (2012).

[43] K. O. Stohr and J. F. Voloch, Weierstrass points and curves over finite fields. *Proceedings of the London Mathematical Society*, **3.1** , 1-19 (1986).

[44] R. G. Swan . Factorization of polynomials over Finite Fields. *Pacific Journal of Mathematics* **12(2)**, 1099-1106 (1962).

[45] M. Tsfasman, S. Vlăduţ and D. Nogin, Algebraic geometric codes: basic notions. *Mathematical Surveys and Monographs*, **139**. AMS (2007).

[46] G. Van der Geer and M. Van der Vlugt, Fibre products of Artin-Schreier curves and generalized Hamming weights of codes. *Journal of Combinatorial Theory, Series A,* **70**, 337-348 (1995).

[47] J.H. Van Lint, *Introduction to Coding Theory*, 3rd edn. Graduate Texts in Mathematics, **86**. Springer, New York (1998).

[48] U. Vishne, Factorization of Trinomials over Galois Fields of Characteristic 2. *Finite Fields and Their Applications,* **3(4)**, 370-377 (1997).

[49] L. Wang, Q. Wang, On explicit factors of cyclotomic polynomials over finite fields. *Designs, Codes and Cryptography,* **63(1)**, 87-104 (2012).

[50] J. Wolfmann, The number of points on certain algebraic curves over finite fields. *Communications in Algebra,* **17**, 2055-2060 (1989).

[51] J. Wolfmann. The number of solutions of certain diagonal equations over finite fields. *Journal of Number Theory,* **42.3**, 247-257 (1992).