UNICAMP

UNIVERSIDADE ESTADUAL DE CAMPINAS

Instituto de Matemática, Estatística e Computação Científica

WALTEIR DE PAULA FERREIRA

On plane curves reaching Sziklai's bound over a finite field

Sobre curvas planas que atingem o limite de Sziklai sobre um corpo finito

Campinas

2025

Walteir de Paula Ferreira

On plane curves reaching Sziklai's bound over a finite field

Sobre curvas planas que atingem o limite de Sziklai sobre um corpo finito

Tese apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Doutor em Matemática.

Thesis presented to the Institute of Mathematics, Statistics and Scientific Computing of the University of Campinas in partial fulfillment of the requirements for the degree of Doctor in Mathematics.

Supervisor: Pietro Speziali

Este trabalho corresponde à versão final da Tese defendida pelo aluno Walteir de Paula Ferreira e orientada pelo Prof. Dr. Pietro Speziali.

Campinas

2025

Ficha catalográfica
Universidade Estadual de Campinas (UNICAMP)
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Ana Regina Machado - CRB 8/5467

Ferreira, Walteir de Paula, 1997-
F413o On plane curves reaching Sziklai's bound over a finite field / Walteir de Paula Ferreira. – Campinas, SP : [s.n.], 2025.

Orientador: Pietro Speziali.
Tese (doutorado) – Universidade Estadual de Campinas (UNICAMP), Instituto de Matemática, Estatística e Computação Científica.

1. Curvas algébricas. 2. Pontos racionais (Geometria). 3. Limite superior de Sziklai. I. Speziali, Pietro, 1989-. II. Universidade Estadual de Campinas (UNICAMP). Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações complementares

Título em outro idioma: Sobre curvas planas que atingem o limite de Sziklai sobre um corpo finito
Palavras-chave em inglês:
Algebraic curves
Rational points (Geometry)
Sziklai upper bound
Área de concentração: Matemática
Titulação: Doutor em Matemática
Banca examinadora:
Pietro Speziali [Orientador]
Cícero Fernandes de Carvalho
Herivelto Martins Borges Filho
Nazar Arakelian
Victor Gonzalo Lopez Neumann
Data de defesa: 29-01-2025
Programa de Pós-Graduação: Matemática

Identificação e informações acadêmicas do(a) aluno(a)
- ORCID do autor: https://orcid.org/0000-0003-3652-8328
- Currículo Lattes do autor: http://lattes.cnpq.br/2753461434323704

Tese de Doutorado defendida em 29 de janeiro de 2025 e aprovada pela banca examinadora composta pelos Profs. Drs.

Prof. Dr. PIETRO SPEZIALI

Prof. Dr. CÍCERO FERNANDES DE CARVALHO

Prof. Dr. HERIVELTO MARTINS BORGES FILHO

Prof. Dr. NAZAR ARAKELIAN

Prof. Dr. VICTOR GONZALO LOPEZ NEUMANN

A Ata da Defesa, assinada pelos membros da Comissão Examinadora, consta no SIGA/Sistema de Fluxo de Dissertação/Tese e na Secretaria de Pós-Graduação do Instituto de Matemática, Estatística e Computação Científica.

Entre todas as honrarias e títulos que eu possa receber, o que mais me enche de orgulho é ser reconhecido como filho de Anivercino Ferreira de Aquino (in memoriam) e Fatima Francisco de Paula.

Acknowledgements

Em primeiro lugar, expresso minha profunda gratidão aos meus pais, Anivercino Ferreira de Aquino (in memoriam) e Fátima Francisco de Paula, e aos meus irmãos, Vanessa Francisco de Aquino (in memoriam), Walter Francisco de Aquino e Kelly Marques da Silva, pelo amor incondicional. Sou igualmente grato pela compreensão diante da minha ausência enquanto me dedicava à realização deste sonho.

Manifesto também minha sincera gratidão ao Prof. Dr. Pietro Speziali, meu orientador, por sua orientação, apoio e incentivo ao longo de todo o processo de elaboração desta tese. Agradeço ainda às amizades que conquistei nessa longa caminhada, tornando o percurso mais leve e significativo.

Por fim, deixo meu agradecimento a todos que, de forma direta ou indireta, contribuíram para a concretização deste sonho.

Este trabalho foi realizado com o apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) – Brasil, Código de Financiamento 001.

"Our Ancestors knew that healing comes in cycles and circles.
One generation carries the pain so that the next can live and heal.
One cannot live without the other, each is the other's hope, meaning and strength.
(Gemma B. Benton)

Resumo

Neste trabalho, os principais objetos de estudos são curvas algébrica com muitos pontos $\mathbb{F}_q$-racionais. Estamos interessados nas curvas que atingem o limite superior de Sziklai. Nosso resultado principal completa a classificação das curvas extremais em relação ao limite superior de Sziklai; mais precisamente, provamos que se uma curva plana não-singular $\mathcal{X}$ de grau $q-1$ definida sobre $\mathbb{F}_q$ ($q \geqslant 5$) sem componentes $\mathbb{F}_q$-lineares atinge o limite superior de Sziklai $(d-1)q+1 = (q-1)^2$ para o número de pontos $\mathbb{F}_q$-racionais, então $\mathcal{X}$ é projetivamente equivalente sobre $\mathbb{F}_q$ à curva $\mathcal{X}_{(\alpha,\beta,\gamma)} : \alpha X^{q-1} + \beta Y^{q-1} + \gamma Z^{q-1} = 0$ para alguns $\alpha, \beta, \gamma \in \mathbb{F}_q^*$ tais que $\alpha + \beta + \gamma = 0$. Além disso, como o limite de Sziklai é igual ao limite de Stöhr-Voloch para curvas planas de grau $q-1$, este resultado classifica as curvas planas $\mathbb{F}_q$-Frobenius clássicas não-singulares extremais de grau $q-1$.

Palavras-chave: Curvas Algébricas. Pontos $\mathbb{F}_q$-racionais. Limite superior de Sziklai. Curvas Extremais.

Abstract

In this work, the main objects to study are algebraic curves with many $\mathbb{F}_q$-rational points. We are interested in curves attaining the Sziklai upper bound. Our main result completes the classification of curves that are extremal with respect to the Sziklai bound; more precisely, we prove that if a plane curve $\mathcal{X}$ of degree $q-1$ defined over $\mathbb{F}_q$ ($q \geqslant 5$) without $\mathbb{F}_q$-linear components attains the Sziklai upper bound $(d-1)q+1 = (q-1)^2$ for the number of its $\mathbb{F}_q$-rational points, then $\mathcal{X}$ is projectively equivalent over $\mathbb{F}_q$ to the curve $\mathcal{X}_{(\alpha,\beta,\gamma)} : \alpha X^{q-1} + \beta Y^{q-1} + \gamma Z^{q-1} = 0$ for some $\alpha, \beta, \gamma \in \mathbb{F}_q^*$ such that $\alpha + \beta + \gamma = 0$. Also, since the Sziklai bound is equal to the Stöhr-Voloch bound for plane curves of degree $q-1$, this result classifies the $\mathbb{F}_q$-Frobenius extremal classical nonsingular plane curves of degree $q-1$.

Keywords: Algebraic curves. $\mathbb{F}_q$-Rational points. Sziklai upper bound. Optimal curves.

List of symbols

$\mathbb{F}_q$ the finite field with q elements;

$\mathbb{F}_q^*$ the nonzero elements of $\mathbb{F}_q$;

$K := \overline{\mathbb{F}}_q$ the algebraic closure of $\mathbb{F}_q$;

$\mathcal{X}(\mathbb{F}_q)$ the set of $\mathbb{F}_q$-rational points of $\mathcal{X}$;

$\mathrm{I}(P, \mathcal{F} \cap \mathcal{G})$ the intersection number of curves $\mathcal{F}$ and $\mathcal{G}$ at a point P;

$\mathrm{N}_q(\mathcal{X})$ the number of rational points on the nonsingular model of $\mathcal{X}$;

$\mathrm{GL}(3, K)$ the general linear group of degree three over K;

$\mathrm{GL}(3, q) := \mathrm{GL}_3(\mathbb{F}_q)$ the general linear group of degree three over $\mathbb{F}_q$;

$\mathrm{PGL}(3, K)$ the projective general linear group of degree three over K;

$\mathrm{PGL}(3, q) := \mathrm{PGL}(3, \mathbb{F}_q)$ the projective general linear group over $\mathbb{F}_q$;

$\Psi_q : \mathbb{P}^2 \to \mathbb{P}^2$ the $\mathbb{F}_q$-Frobenius map with $\Psi_q(x : y : z) := (x^q : y^q : z^q)$;

$K(\mathcal{X})$ the function field of $\mathcal{X}$ over K;

$\check{\mathbb{P}}^2 := \check{\mathbb{P}}^2(K)$ the dual projective space over K;

$\check{\mathbb{P}}^2(\mathbb{F}_q)$ the dual projective space over $\mathbb{F}_q$;

$\check{P}(\mathbb{F}_q)$ the set of lines $l \in \check{\mathbb{P}}^2(\mathbb{F}_q)$ such that $P \in l$.

$\mathrm{Div}(\mathcal{X})$ the divisor group of $\mathcal{X}$;

$Z_{\mathcal{X}}(t)$ the Zeta function of $\mathcal{X}$;

$L_{\mathcal{X}}(t)$ the L-polynomial of $\mathcal{X}$;

$\mathcal{K}$ a (k, n)-arc in $\mathbb{P}^2(\mathbb{F}_q)$;

$\mathcal{A}_i(\mathcal{K})$ the set of lines $l \in \check{\mathbb{P}}^2(\mathbb{F}_q)$ such that $\#(l \cap \mathcal{K}) = i$;

$a_i(\mathcal{K})$ the cardinality of $\mathcal{A}_i(\mathcal{K})$;

$C_d(\mathbb{F}_q)$ the set of plane curves of degree $d \geqslant 2$ defined over $\mathbb{F}_q$ without $\mathbb{F}_q$-linear components;

$\psi_i : \mathbb{P}^2(\mathbb{F}_q) \to \{0, 1, ..., q+1\}$ defined by $\psi_i(P) := \#(\check{P}(\mathbb{F}_q) \cap \mathcal{A}_i(\mathcal{X}))$;

$Z(\mathcal{X}) := \mathbb{P}^2(\mathbb{F}_q) \backslash \mathcal{X}(\mathbb{F}_q)$;

Contents

Introduction **12**
1 Preliminaries and Notations **15**
1.1 Algebraic Plane Curves over a Finite Field 15
1.1.1 Genus and Zeta Function 19
1.2 The Theory of Stöhr-Voloch for a Plane Curve 22
1.3 Arcs and Codes 23
2 The Sziklai Bound and Optimal Plane Curves **25**
2.1 Hasse-Weil Bound and Refinements 25
2.2 The Sziklai Upper Bound 27
2.3 Optimal Plane Curves over Finite Fields 30
3 Optimal Plane Curves of Degree $q-1$ **32**
3.1 Preliminary results 32
3.2 Characterization of Optimal Sziklai Curves of Degree $q-1$ 41
4 Concluding Remarks **50**
4.1 On $\mathbb{F}_q$-Frobenius classical curves with many points 50
4.2 On hypersurfaces with many rational points 50
4.3 Future Work 53

BIBLIOGRAPHY **57**

Introduction

Algebraic curves defined over a finite field have been much studied in recent years for their applications in finite geometry, number theory, error-correcting codes, and cryptology. Let $\mathcal{X}$ be a projective, geometrically irreducible, algebraic curve defined over a finite field $\mathbb{F}_q$ where q is a power of a prime number p. We denote by $\mathcal{X}(\mathbb{F}_q)$ its set of $\mathbb{F}_q$-rational points. It is a classical problem to count the number $\mathrm{N}_q(\mathcal{X}) := \#(\mathcal{X}(\mathbb{F}_q))$ of $\mathbb{F}_q$-rational points of $\mathcal{X}$. However, since this problem is rather hard to solve, it is often desirable to find good upper bounds for $\mathrm{N}_q(\mathcal{X})$ depending on some invariants of the curve $\mathcal{X}$. For instance, the famous Hasse-Weil upper bound states that

$$\mathrm{N}_q(\mathcal{X}) \leqslant q + 1 + 2 \cdot \mathfrak{g}(\mathcal{X}) \cdot q^{\frac{1}{2}} \quad \text{(The Hasse-Weil Theorem)}$$

where $\mathfrak{g} = \mathfrak{g}(\mathcal{X})$ is the genus of $\mathcal{X}$. Note that the same bound holds for any curve defined over $\mathbb{F}_q$ and genus $\mathfrak{g}$. Once we have a bound, it is a natural question to see whether such a bound is sharp or not, and then, it is also natural to try to classify the optimal curves, that is, the curves attaining said bound. In the context of the Hasse-Weil upper bound, such optimal curves do exist and are called $\mathbb{F}_q$-maximal curves. Maximal curves may exist when $q = n^2$ is a square, and it is known that the genus of an $\mathbb{F}_q$-maximal curve is upper bounded by $n(n-1)/2$ (Ihara's Theorem). Also, Ihara's Theorem for the genus of a $\mathbb{F}_q$-maximal curves cannot be improved in general. Up to birational equivalence, there is exactly one $\mathbb{F}_q$-maximal curve of genus $n(n-1)/2$: the Hermitian curve $\mathcal{H}_n$ given by the homogeneous equation

$$\mathcal{H}_n : Y^n Z + Y Z^n = X^{n+1}$$

has genus $\mathfrak{g}(\mathcal{H}_n) = n(n-1)/2$. It is a classical and yet unsolved problem to find the spectrum of the genera of $\mathbb{F}_q$-maximal curves; see (ARAKELIAN; TAFAZOLIAN; TORRES, 2016). When q is not a square, Serre refines Hasse-Wiel upper bound:

$$\mathrm{N}_q(\mathcal{X}) \leqslant q + 1 + \mathfrak{g}(\mathcal{X}) \cdot m \quad \text{(The Serre Theorem)}$$

with $m = [2q^{\frac{1}{2}}]$, where $[x]$ denotes the largest integer $\leqslant x$. Note that, if q is a square, this "refined Hasse-Weil upper bound" coincides with Hasse-Weil upper bound.

In this work, we are interested in plane curves with many $\mathbb{F}_q$-rational points. Let $\mathcal{X}$ be a plane curve of degree $d \geqslant 2$ without $\mathbb{F}_q$-linear components. In (SZIKLAI, 2008), Sziklai conjectured the following result:

$$\mathrm{N}_q(\mathcal{X}) \leqslant (d-1)q + 1 \quad \text{(The Sziklai Conjecture)}.$$

In (HOMMA; KIM, 2009, section 3), Homma and Kim proved that the Sziklai Conjecture fails for curves of degree 4 over $\mathbb{F}_4$, as the plane curve with equation

$$X^4 + Y^4 + Z^4 + X^2Y^2 + Y^2Z^2 + Z^2X^2 + X^2YZ + XY^2Z + XYZ^2 = 0 \qquad (1)$$

has 14 points over $\mathbb{F}_4$ while Sziklai's bound is equal to 13. Also, they proved that the curve defined by (1) over $\mathbb{F}_4$ is a unique curve up to projective equivalence with degree 4 and 14 $\mathbb{F}_4$-rational points. So, Homma and Kim modify The Sziklai Conjecture: unless $\mathcal{X}$ is a curve defined over $\mathbb{F}_4$ which is projectively equivalent to the curve defined by (1) over $\mathbb{F}_4$, we might have $\mathrm{N}_q(\mathcal{X}) \leqslant (d-1)q+1$. Later on, in a sequence of three papers (HOMMA; KIM, 2009; HOMMA; KIM, 2010b; HOMMA; KIM, 2010a), Homma and Kim proved The Modified Sziklai Conjecture 1.

We are interested in curves attaining the Sziklai bound. Let $\mathcal{X}$ be a nonsingular plane curve of degree d that is optimal with respect to the Sziklai upper bound, that is, $\mathrm{N}_q(\mathcal{X}) = (d-1)q+1$, then, by (HOMMA; KIM, 2010b, Section 5), its degree d must belong to the set

$$\{2, \sqrt{q}+1, q-1, q, q+1, q+2\}.$$

This means that the spectrum of the degrees of optimal Sziklai curves is pretty small, hence, it seems feasible to classify, up to projective equivalence, the nonsingular plane curves of degree d attaining the Sziklai bound. Previously, it was only known in cases

$$d = 2, \sqrt{q}+1, q, q+1 \text{ or } q+2 \quad \text{(see, Theorem 2.3.1)}.$$

For the case $d = q-1$, a family of optimal curves is given by the homogeneous equation

$$\mathcal{X}_{(\alpha,\beta,\gamma)} : \alpha X^{q-1} + \beta Y^{q-1} + \gamma Z^{q-1} = 0$$

with $\alpha, \beta, \gamma \in \mathbb{F}_q^*$ and $\alpha+\beta+\gamma = 0$. This curve $\mathcal{X}_{(\alpha,\beta,\gamma)}$ is nonsingular and the set of its $\mathbb{F}_q$-rational points is

$$\mathcal{X}_{(\alpha,\beta,\gamma)}(\mathbb{F}_q) = \mathbb{P}^2(\mathbb{F}_q) \backslash (\mathbf{v}(X) \cup \mathbf{v}(Y) \cup \mathbf{v}(Z)).$$

In (HOMMA, 2024), Homma has stated the following question:

Question 1. *Are there curves of degree $q-1$ that attain the Sziklai upper bound such that they are not projectively equivalent over $\mathbb{F}_q$ to a curve of type $\mathcal{X}_{(\alpha,\beta,\gamma)}$?*

In the same preprint, he gives a positive solution to this problem for $q = 4$, since in this case, the Hermitian cubic

$$\mathcal{H}_3 : X^3 + Y^3 + Z^3 = 0$$

attains Sziklai's bound but is not projectively equivalent to any $\mathcal{X}_{(\alpha,\beta,\gamma)}$.

In this work, we give a negative answer to Question 1 for $q \geqslant 5$ (see, Theorem 3.2.4), thus completing the classification of optimal Sziklai curves. This work is organized as follows:

In Chapter 1, we give basic facts about plane curves defined over a finite field; also, we give the necessary background on a particular case of the Stöhr-Voloch theorem for plane curves.

In Chapter 2, we briefly survey the existing literature on the Sziklai bound and related topics.

In Chapter 3, first, we will give several technical results that are necessary to prove our classification of curves of degree $q-1$ that are optimal with respect to the Sziklai bound. Later, is devoted to the proof of Theorem 3.2.4, which is the main result of our work. Here, we remark that while our technique applies to all $q \geqslant 8$, the cases $q = 5, 7$ need to be dealt with by using two different approaches, which are of independent interest. The former needs the knowledge of L-polynomial of curves of genus 3 with small defect (LAUTER; SERRE, 2002), the latter is based on the classification on $(36, 6)$-arcs in $\mathbb{P}^2(\mathbb{F}_7)$ (BOUYUKLIEV et al., 2020).

Finally, in Chapter 5, we give a brief discussion regarding topics that are directly linked to or possible applications of our results. More in detail, we show as our main result is related to the $\mathbb{F}_q$-Frobenius classical plane curves of degree $q-1$ attaining the Stöhr-Voloch upper bound. Further, curves attaining the Sziklai upper bound are related to nonsingular hypersurfaces with many $\mathbb{F}_q$-rational points in even-dimensional projective spaces; see (DATTA, 2019; TIRONI, 2022).

1 Preliminaries and Notations

In this chapter, basic facts about plane curves defined over a finite field are presented. Also, we introduce the notations that will be used throughout the thesis and present some general results.

1.1 Algebraic Plane Curves over a Finite Field

Algebraic curves defined over a finite field have been much studied in recent years. In this section, we provide a concise overview of the theory of plane curves over finite fields, based on (HIRSCHFELD; KORCHMÁROS; TORRES, 2008) and (FULTON, 2008), to which we refer the reader to for further details.

Let $\mathbb{F}_q$ be a finite field with $q = p^h$ elements and $K := \overline{\mathbb{F}}_q$ be the algebraic closure of $\mathbb{F}_q$, where p is a prime number. A (projective) plane curve $\mathcal{X}$ in the projective plane $\mathbb{P}^2 := \mathbb{P}^2_K$ of homogeneous equation $F(X,Y,Z) = 0$, where $F \in K[X,Y,Z]$ is a homogeneous polynomial, is denoted by $\mathcal{X} = \mathbf{v}(F)$ and consists of all points $(x : y : z) \in \mathbb{P}^2$ such that $F(x,y,z) = 0$; namely,

$$\mathcal{X} = \mathbf{v}(F) := \{(x : y : z) \in \mathbb{P}^2 \mid F(x,y,z) = 0\}.$$

Also, the degree of $\mathcal{X}$, denoted by $\deg(\mathcal{X})$, is $\deg(F)$. A curve of degree one is called a line.

Definition 1.1.1. *A plane curve $\mathcal{X} = \mathbf{v}(F)$ is said to be defined over $\mathbb{F}_q$ if there is a non-zero constant $\lambda \in K$ such that $\lambda \cdot F(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$. Also, the points $(x : y : z) \in \mathbb{P}^2(\mathbb{F}_q)$ such that $F(x,y,z) = 0$ are called $\mathbb{F}_q$-rational points (or simply, rational points) of $\mathcal{X}$ and $\mathcal{X}(\mathbb{F}_q)$ denotes the set of all $\mathbb{F}_q$-rational points of $\mathcal{X}$.*

A component of $\mathcal{X} = \mathbf{v}(F)$ is a plane curve $\mathbf{v}(G)$ such that G divides F. If $\mathbf{v}(G)$ is defined over $\mathbb{F}_q$, then we say that $\mathbf{v}(G)$ is an $\mathbb{F}_q$-component of $\mathcal{X}$. Also, if $\deg(\mathbf{v}(G)) = 1$, we say that $\mathbf{v}(G)$ is an $\mathbb{F}_q$-linear component of $\mathcal{X}$. The plane curve $\mathbf{v}(F)$ defined over $\mathbb{F}_q$ is irreducible if F is irreducible over $\mathbb{F}_q$ and absolutely irreducible if F is irreducible over K.

A projective transformation $\varphi_A : \mathbb{P}^2 \to \mathbb{P}^2$ is defined as follows:

$$\varphi_A(x : y : z) = \mathbf{u} \quad \text{with } \mathbf{u}^t = A \cdot (x : y : z)^t,$$

where $A \in \mathrm{GL}(3,K)$. It is also called a projectivity. The projectivities of $\mathbb{P}^2$ constitute its projective general linear group $\mathrm{PGL}(3,K)$. Also, the projectivities of $\mathbb{P}^2$ with $A \in \mathrm{GL}(3,\mathbb{F}_q)$ is denoted by $\mathrm{PGL}(3,q) := \mathrm{PGL}(3,\mathbb{F}_q) < \mathrm{PGL}(3,K)$. Another interesting map in $\mathbb{P}^2$ is the $\mathbb{F}_q$-Frobenius map $\Psi_q : \mathbb{P}^2 \to \mathbb{P}^2$ with $\Psi_q(x : y : z) := (x^q : y^q : z^q)$.

Definition 1.1.2. *Let $\mathcal{F}$ and $\mathcal{G}$ plane curves. We say that $\mathcal{F}$ and $\mathcal{G}$ are projectively equivalent over $\mathbb{F}_q$, denoted by $\mathcal{F} \simeq_{proj} \mathcal{G}$, if there is a projectivity φ_A with $A \in \mathrm{GL}(3, \mathbb{F}_q)$ such that*

$$\varphi_A(\mathcal{F}) = \mathcal{G}.$$

The dual projective space $\check{\mathbb{P}}^2 := \check{\mathbb{P}}^2_K$ is the space of all lines in $\mathbb{P}^2$ and by $\check{\mathbb{P}}^2(\mathbb{F}_q)$ we mean the set of lines defined over $\mathbb{F}_q$ of $\check{\mathbb{P}}^2$. For a point $P \in \mathbb{P}^2(\mathbb{F}_q)$, we define

$$\check{P}(\mathbb{F}_q) := \{l \in \check{\mathbb{P}}^2(\mathbb{F}_q) \mid P \in l\}.$$

Remark 1.1.3. *It is a basic fact that every line in $\mathbb{P}^2$ can be expressed as*

$$l(a_0, a_1, a_2) := \{(x_0 : x_1 : x_2) \in \mathbb{P}^2;\ a_0x_0 + a_1x_1 + a_2x_2 = 0\}$$

for some $(0, 0, 0) \neq (a_0, a_1, a_2) \in K^3$, where

$$l(a_0, a_1, a_2) = l(b_0, b_1, b_2) \Leftrightarrow (a_0 : a_1 : a_2) = (b_0 : b_1 : b_2) \in \mathbb{P}^2.$$

Thus the map $l(a_0, a_1, a_2) \to [a_0 : a_1 : a_2]$ allows us to identify $\mathbb{P}^2$ with $\check{\mathbb{P}}^2$. As $\mathrm{PGL}(3, K)$ acts transitively on the set of all triple of non-collinear points of $\mathbb{P}^2$, then $\mathrm{PGL}(3, K)$ acts transitively on the set of all triple of non-concurrent lines of $\mathbb{P}^2$.

For a definition the intersection number of two plane curves at a point, which can be somewhat unintuitive, for simplicity, consider a curve in the affine plane

$$\mathbb{A}^2_K := K \times K = \{(x, y) \mid x, y \in K\}$$

as simply an equivalence class of polynomials in $K[X, Y]$ under multiplication by a non-zero scalar. So, given two curves F and G in $\mathbb{A}^2_K$, the intersection number $\mathrm{I}(P, F \cap G)$ of F and G at the point $P = (x, y) \in \mathbb{A}^2_K$ is defined by the seven properties we want this intersection number to have:

(I1) $\mathrm{I}(P, F \cap G) \in \mathbb{N}$ when F and G have no common component through P;

(I2) $\mathrm{I}(P, F \cap G) = \infty$ if F and G have a common component through P;

(I3) $\mathrm{I}(P, F \cap G) = 0$ if and only if $P \notin F \cap G$;

(I4) $\mathrm{I}(P, F \cap G) = 1$ if F and G are two distinct lines through P;

(I5) $\mathrm{I}(P, F \cap G) = \mathrm{I}(P, G \cap F)$;

(I6) $\mathrm{I}(P, F \cap (G + AF)) = \mathrm{I}(P, F \cap G)$ for any $A \in K[X, Y]$;

(I7) $\mathrm{I}(P, F \cap GH) = \mathrm{I}(P, F \cap G) + \mathrm{I}(P, F \cap H)$ for any $H \in K[X, Y]$.

For the existence and uniqueness of the function $\mathrm{I}(P, F \cap G)$, see (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 3.8 and 3.9) or (FULTON, 2008, Section 3.3: Theorem 3). For the projective curves $\mathcal{F} = \mathbf{v}(F)$, $\mathcal{G} = \mathbf{v}(G)$, and the point $O = (0 : 0 : 1)$, the intersection number is

$$\mathrm{I}(O, \mathcal{F} \cap \mathcal{G}) := \mathrm{I}((0,0), F_* \cap G_*)$$

where $F_*(X, Y) := F(X, Y, 1)$ and $G_*(X, Y) := G(X, Y, 1)$. Intersection numbers of $\mathcal{F}$ and $\mathcal{G}$ at another point P are calculated by using covariant properties; that is, a projectivity is applied to change P to $(0 : 0 : 1)$.

Theorem 1.1.4. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 3.14: Bézout's Theorem) *If the projective plane curves $\mathcal{F}$ and $\mathcal{G}$ have degrees m and n, and no common component, then*

$$\sum \mathrm{I}(P, \mathcal{F} \cap \mathcal{G}) = mn.$$

The next result provides a method to find all plane curves passing through a given set of points of $\mathbb{P}^2(\mathbb{F}_q)$:

Theorem 1.1.5. (FULTON, 2008, Section 5.5: Noether's "AF + BG" Theorem) *Let $\mathcal{F} = \mathbf{v}(F)$ and $\mathcal{G} = \mathbf{v}(G)$ be two plane curves defined over $\mathbb{F}_q$ with no common components. Suppose that*

$$\mathcal{F} \cap \mathcal{G} = \{P_1, ..., P_s\} \quad \text{and} \quad \mathrm{I}(P_i, \mathcal{F} \cap \mathcal{G}) = 1$$

for $i = 1, ..., s$. Then for all plane curve $\mathcal{X} = \mathbf{v}(H)$ defined over $\mathbb{F}_q$ with $\mathcal{F} \cap \mathcal{G} \subseteq \mathcal{X}$ there are $A, B \in \mathbb{F}_q[X, Y, Z]$ such that $H = AF + BG$.

Definition 1.1.6. *A point $P = (x : y : z)$ of $\mathcal{X}$ is singular if*

$$\frac{\partial F}{\partial X}(x, y, z) = \frac{\partial F}{\partial Y}(x, y, z) = \frac{\partial F}{\partial Z}(x, y, z) = 0.$$

Otherwise, P is nonsingular (or smooth) and the tangent line at P is

$$\mathbb{T}_P(\mathcal{X}) := \mathbf{v}\left(\frac{\partial F}{\partial X}(x, y, z) \cdot X + \frac{\partial F}{\partial Y}(x, y, z) \cdot Y + \frac{\partial F}{\partial Z}(x, y, z) \cdot Z\right).$$

Also, a nonsingular point P of $\mathcal{X}$ is a point of inflexion of $\mathcal{X}$ if

$$\mathrm{I}(P, \mathbb{T}_P(\mathcal{X}) \cap \mathcal{X}) \geqslant 3.$$

Here, P is also called an inflexion.

We conclude this section with a brief discussion of algebraic curves in higher-dimensional spaces. A subset $\mathcal{V} \subseteq \mathbb{P}^n := \mathbb{P}^n_K$ is a projective algebraic set if there exists a set of homogeneous polynomials $M \subseteq K[X_0, X_1, ..., X_n]$ such that

$$\mathcal{V} = \{(x_0 : x_1 : \cdots : x_n) \in \mathbb{P}^n \mid F(x_0, x_1, ..., x_n) = 0 \quad \text{for all} \quad F \in M\}.$$

The ideal $\mathbb{I}(\mathcal{V}) \subseteq K[X_0, X_1, ..., X_n]$ which is generated by all homogeneous polynomials F with $F(x_0, x_1, ..., x_n) = 0$ for all $(x_0 : x_1 : \cdots : x_n) \in \mathcal{V}$, is called the ideal of $\mathcal{V}$. It is a homogeneous ideal. An algebraic set $\mathcal{V} \subseteq \mathbb{P}^n$ is irreducible if it is not the union of two smaller algebraic sets. We have that $\mathcal{V} \subseteq \mathbb{P}^n$ is irreducible if, and only if, $\mathbb{I}(\mathcal{V})$ is a homogeneous prime ideal in $K[X_0, X_1, ..., X_n]$. A projective variety is an irreducible projective algebraic set.

Given a non-empty variety $\mathcal{V} \subseteq \mathbb{P}^n$, we define its homogeneous coordinate ring by

$$\Gamma_h(\mathcal{V}) := \frac{K[X_0, X_1, ..., X_n]}{\mathbb{I}(\mathcal{V})};$$

this is an integral domain containing K. The function field of $\mathcal{V}$ is defined by

$$K(\mathcal{V}) := \left\{ \frac{f}{g} \mid f, g \in \Gamma_h(V) \text{ are forms of the same degree and } g \neq 0 \right\}$$

which is a subfield of the quotient field of $\Gamma_h(\mathcal{V})$. The dimension of V is the transcendence degree of $K(\mathcal{V})$ over K.

Definition 1.1.7. *A projective algebraic curve $\mathcal{X} \subseteq \mathbb{P}^n$ $(n \geqslant 3)$ is a projective variety of dimension one. A point $P = (x_0 : x_1 : \cdots : x_n) \in \mathcal{X}$ is nonsingular if the local ring*

$$\mathcal{O}_P(\mathcal{X}) := \left\{ \frac{f}{g} \in K(\mathcal{X}) \mid g(x_0, x_1, ..., x_n) \neq 0 \right\} \subseteq K(\mathcal{X})$$

is a discrete valuation ring. The curve $\mathcal{X}$ is called nonsingular if all points $P \in \mathcal{X}$ are nonsingular.

Remark 1.1.8. *An irreducible plane curve can be defined as above.*

Let $\mathcal{V} \subseteq \mathbb{P}^m$ and $\mathcal{W} \subseteq \mathbb{P}^n$ be projective varieties. A rational map $\phi : \mathcal{V} \to \mathcal{W}$ is defined by $\phi = (F_0 : \cdots : F_n)$ where $F_0, ..., F_n \in K[X_0, ..., X_m]$ are homogeneous polynomials with the following properties:

(a) $F_0, ..., F_n$ have the same degree;

(b) not all F_i are in $\mathbb{I}(\mathcal{V})$;

(c) for all $H \in \mathbb{I}(\mathbf{W})$ holds $H(F_0, ..., F_n) \in \mathbb{I}(\mathcal{V})$.

Two curves $\mathcal{X}_1$, $\mathcal{X}_2$ are birationally equivalent if there are rational maps $\phi_1 : \mathcal{X}_1 \to \mathcal{X}_2$ and $\phi_2 : \mathcal{X}_2 \to \mathcal{X}_1$ such that $\phi_1 \circ \phi_2$ and $\phi_2 \circ \phi_1$ are the identity maps on $\mathcal{X}_2$ and $\mathcal{X}_1$, respectively. We have that $\mathcal{X}_1$ and $\mathcal{X}_2$ are birationally equivalent if and only if their function fields $K(\mathcal{X}_1)$ and $K(\mathcal{X}_2)$ are K-isomorphic.

Theorem 1.1.9. (FULTON, 2008, Section 7.5: Theorem 3) *Every irreducible plane curve $\mathcal{X}$ is birationally equivalent to a nonsingular curve (not necessarily a plane curve), called a nonsingular model of $\mathcal{X}$.*

Remark 1.1.10. *In this thesis work, we are interested in the rational points of an algebraic plane curve $\mathcal{X}$, that is, $\mathcal{X} \cap \mathbb{P}^2(\mathbb{F}_q)$. In general, there is no bijection between $\mathcal{X} \cap \mathbb{P}^2(\mathbb{F}_q)$ and the rational points of its nonsingular model. Therefore, from this point onward, $\mathrm{N}_q(\mathcal{X})$ will represent the number of rational points on the nonsingular model of $\mathcal{X}$. Note that, if $\mathcal{X}$ is nonsingular, then $\mathrm{N}_q(\mathcal{X}) = |\mathcal{X}(\mathbb{F}_q)|$.*

1.1.1 Genus and Zeta Function

An algebraic function field F/K of one variable over K is an extension field $F \supset K$ such that F is a finite algebraic extension of $K(x)$ for some element $x \in F$ which is transcendental over K. For instance, the function field $K(\mathcal{X})$ of a curve $\mathcal{X}$ is an algebraic function field of one variable over K.

Proposition 1.1.11. (FULTON, 2008, Section 7.5: Corollary of Theorem 3) *There is a natural one-to-one correspondence between nonsingular projective curves $\mathcal{X}$ and algebraic function fields in one variable over K.*

This correspondence makes it possible to translate definitions and results from algebraic function fields to algebraic curves (and vice versa). For the basic definitions and results of the theory of algebraic function fields, see (STICHTENOTH, 2009, Chapter 1).

Throughout this chapter, $\mathcal{X} \subseteq \mathbb{P}^n$ denotes a nonsingular model of an irreducible projective curve. For each $P = (x_0 : x_1 : \cdots : x_n) \in \mathcal{X}$, we know that $\mathcal{O}_P(\mathcal{X})$ is a discrete valuation ring with maximal ideal

$$\mathrm{M}_P(\mathcal{X}) := \left\{ \frac{f}{g} \in \mathcal{O}_P(\mathcal{X}) \mid f(x_0, x_1, ..., x_n) = 0 \right\}.$$

In this case, $\mathrm{M}_P(\mathcal{X}) = t \cdot \mathcal{O}_P(\mathcal{X})$ is a principal ideal and each $0 \neq z \in K(\mathcal{X})$ has a unique representation of the form $z = t^n \cdot u$ for some $n \in \mathbb{Z}$ and $u \in \mathcal{O}_P^{\times}(\mathcal{X})$. Define

$$\mathrm{ord}_P(z) := n \quad \text{and} \quad \mathrm{ord}_P(0) := \infty.$$

The divisor group of $\mathcal{X}$ is defined as the (additively written) free abelian group which is generated by the points of $\mathcal{X}$; it is denoted by $\mathrm{Div}(\mathcal{X})$. The elements of $\mathrm{Div}(\mathcal{X})$ are called divisors of $\mathcal{X}$. In other words, a divisor is a formal sum

$$D = \sum_{P \in \mathcal{X}} \mathrm{n}_P \cdot P \quad \text{with} \quad \mathrm{n}_P \in \mathbb{Z}, \text{ almost all } \mathrm{n}_P = 0.$$

Two divisors $D = \sum n_P P$ and $D' = \sum m_P P$ are added coefficientwise

$$D + D' := \sum_{P \in \mathbb{P}_F} (n_P + m_P)P.$$

For $Q \in \mathcal{X}$ and $D = \sum n_P P$, we define $\nu_Q(D) := n_Q$. A partial ordering on Div(F) is defined by

$$D_1 \leqslant D_2 \Leftrightarrow \nu_P(D_1) \leqslant \nu_P(D_2) \text{ for all } P \in \mathcal{X}.$$

A divisor $D \geqslant 0$ is called an effective (or positive) divisor. The degree of a divisor is defined as

$$\deg(D) := \sum_{P \in \mathbb{P}_F} \nu_P(D) \cdot \deg(P) \text{ where } \deg(P) := [\mathcal{O}_P(\mathcal{X})/M_P(\mathcal{X}) : K].$$

Remark 1.1.12. *The rational points P of $\mathcal{X}$ are the points $P \in \mathcal{X}$ such that* $\deg(P) = 1$.

A nonzero element $z \in K(\mathcal{X})$ has only finitely many points $P \in \mathcal{X}$ such that $\mathrm{ord}_P(z) \neq 0$; so we can define

$$\mathrm{div}(z) := \sum_{P \in \mathcal{X}} \mathrm{ord}_P(z) \cdot P,$$

called the principal divisor of z. For a divisor $D \in \mathrm{Div}(\mathcal{X})$, we define the Riemann-Roch space associated to D (which is a vector space over K) by

$$\mathscr{L}(D) := \{z \in K(\mathcal{X}) \mid \mathrm{div}(z) + D \geqslant 0\} \cup \{0\}$$

and $l(D) := \dim_K(\mathscr{L}(D)) < \infty$.

Proposition 1.1.13. (STICHTENOTH, 2009, Proposition 1.4.14) *There is a constant $\gamma \in \mathbb{Z}$ such that for all divisors $D \in \mathrm{Div}(\mathcal{X})$ the following holds:* $\deg(D) - l(D) \leqslant \gamma$.

The emphasis here lies on the fact that γ is independent of the divisor D; it depends only on the function field $K(\mathcal{X})$. The genus $\mathfrak{g}$ of $K(\mathcal{X})/K$ is defined by

$$\mathfrak{g} := \max\{\ \deg(D) - l(D) + 1 \mid D \in \mathrm{Div}(\mathcal{X})\ \}.$$

Note that this definition makes sense by Proposition 1.1.13.

Definition 1.1.14. *The genus $\mathfrak{g} = \mathfrak{g}(\mathcal{X})$ of an irreducible algebraic curve $\mathcal{X}$ is the genus of its function field $K(\mathcal{X})/K$.*

Theorem 1.1.15. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 5.57) *Let $\mathcal{X}$ an irreducible plane curve of degree d. If $\mathcal{X}$ is nonsingular, then*

$$\mathfrak{g}(\mathcal{X}) = \frac{1}{2} \cdot (d-1)(d-2).$$

For every $n \geqslant 0$ there exist only finitely many positive divisors of degree n; see (STICHTENOTH, 2009, Lemma 5.1.1). So, we can define the power series

$$Z_{\mathcal{X}}(t) := \sum_{n=0}^{\infty} A_n t^n \in \mathbb{C}[[t]],$$

where

$$A_n := \#\{D \in \mathrm{Div}(\mathcal{X}) \mid D \geqslant 0 \text{ and } \deg(D) = n\},$$

called the Zeta function of $\mathcal{X}$. By (STICHTENOTH, 2009, Corollary 5.1.12), the power series $Z_{\mathcal{X}}(t)$ is convergent when $q|t| < 1$; also, converges to a rational function of the form

$$Z_{\mathcal{X}}(t) = \frac{p(t)}{(1-t)(1-qt)}$$

where $p(t) \in \mathbb{C}[t]$.

Definition 1.1.16. *The polynomial*

$$L_{\mathcal{X}}(t) := (1-t)(1-qt)Z_{\mathcal{X}}(t)$$

is called the L-polynomial of $\mathcal{X}$.

Theorem 1.1.17. (STICHTENOTH, 2009, Theorem 5.1.15) *The L-polynomial $L_{\mathcal{X}}(t)$ of $\mathcal{X}$ factors in $\mathbb{C}[t]$ in the form*

$$L_{\mathcal{X}}(t) = \prod_{i=1}^{2g}(1-\alpha_i t) \tag{1.1}$$

The complex numbers $\alpha_1, ..., \alpha_{2g}$ are algebraic integers, and they can be arranged in such a way that $\alpha_i \alpha_{g+i} = q$ holds for $i = 1, ..., g = g(\mathcal{X})$. (We note that a complex number α is called an algebraic integer if it satisfies an equation $\alpha^m + c_{m-1}\alpha^{m-1} + \cdots + c_1\alpha + c_0 = 0$ with coefficients $c_i \in \mathbb{Z}$).

Corollary 1.1.18. (STICHTENOTH, 2009, Corollary 5.1.16) *For all $r \geqslant 1$,*

$$|\mathcal{X}(\mathbb{F}_{q^r})| = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r$$

where $\alpha_1, ..., \alpha_{2g} \in \mathbb{C}$ are the reciprocals of the roots of $L_{\mathcal{X}}(t)$. In particular, we have

$$|\mathcal{X}(\mathbb{F}_q)| = q + 1 - \sum_{i=1}^{2g} \alpha_i.$$

Theorem 1.1.19. (STICHTENOTH, 2009, Theorem 5.2.1 (Hasse-Weil)) *The reciprocals of the roots of $L_{\mathcal{X}}(t)$ satisfy*

$$|\alpha_i| = q^{1/2} \quad \textit{for} \quad i = 1, ..., 2g.$$

1.2 The Theory of Stöhr-Voloch for a Plane Curve

In (STÖHR; VOLOCH, 1986), Stöhr and Voloch gave a geometric method to obtain upper bounds for the number of $\mathbb{F}_q$-rational points of a curve of $\mathbb{P}^n_K$. Here, we give the necessary background on a particular case of the Stöhr-Voloch theorem for plane curves.

Let $\mathcal{X}$ an irreducible plane curve defined over $\mathbb{F}_q$ in $\mathbb{P}^2$. The order-sequence at a point $P \in \mathcal{X}$, denoted by $j_0(P) < j_1(P) < j_2(P)$, is defined to be the set of intersection multiplicities at P of $\mathcal{X}$ with the lines of $\mathbb{P}^2$. If P is nonsingular, then the order-sequence of P is

$$j_0(P) = 0,\ j_1(P) = 1 \ \text{ and } \ j_2(P) = \mathrm{I}(P, \mathbb{T}_P(\mathcal{X}) \cap \mathcal{X}).$$

Almost all point of $\mathcal{X}$ have the same order-sequence which is called the order-sequence of $\mathcal{X}$ and is denoted by $\epsilon_0 < \epsilon_1 < \epsilon_2$. Now, since $\mathcal{X}$ is defined over $\mathbb{F}_q$, there exists a smallest integer $\nu \in \{1, \epsilon_2\}$ such that

$$W^{\nu}_{\zeta}(x_0, x_1, x_2) := \det \begin{pmatrix} x_0^q & x_1^q & x_2^q \\ x_0 & x_1 & x_2 \\ D^{(\nu)}_{\zeta} x_0 & D^{(\nu)}_{\zeta} x_1 & D^{(\nu)}_{\zeta} x_2 \end{pmatrix} \not\equiv 0$$

where $D^{(k)}_{\zeta}$ is the k-th Hasse derivative with respect to a separating variable ζ of $K(\mathcal{X})/K$, and x_0, x_1, x_2 are the coordinate functions on $\mathcal{X} \subseteq \mathbb{P}^2$.

Definition 1.2.1. *The number ν is called the $\mathbb{F}_q$-Frobenius order of $\mathcal{X}$, and such a curve is called $\mathbb{F}_q$-Frobenius classical if $\nu = 1$. Otherwise, $\mathcal{X}$ is called $\mathbb{F}_q$-Frobenius nonclassical.*

Theorem 1.2.2. *Let $\mathcal{X}$ be an irreducible plane curve of degree d and genus g defined over $\mathbb{F}_q$. If ν denotes the $\mathbb{F}_q$-Frobenius order of $\mathcal{X}$, then*

$$\mathrm{N}_q(\mathcal{X}) \leqslant \frac{\nu(2g-2) + (q+2)d}{2}.$$

In particular, if $\mathcal{X}$ is $\mathbb{F}_q$-Frobenius classical, then

$$\mathrm{N}_q(\mathcal{X}) \leqslant \frac{1}{2} d(d+q-1).$$

Theorem 1.2.3. (HEFEZ; VOLOCH, 1990, Theorem 1) *Let $\mathcal{X}$ be an irreducible plane curve of degree d and genus g defined over $\mathbb{F}_q$. If $\mathcal{X}$ is nonsingular and such that $\nu > 1$, then*

$$\mathrm{N}_q(\mathcal{X}) = d(q-1) - (2g-2).$$

A refined version of theorem 1.2.2 can be obtained if one can gather sufficient information on the number and the weight of the $\mathbb{F}_q$-rational inflection points. Indeed, consider the Frobenius divisor $S_{\mathcal{X}}$ of $\mathcal{X}$, then $\deg(S_{\mathcal{X}}) = \nu(2g-2) + (q+2)d$ and

$P \in \mathrm{Supp}(S_{\mathcal{X}})$ for all $P \in \mathcal{X}(\mathbb{F}_q)$. Also, by (STÖHR; VOLOCH, 1986, Theorem 2.4(a)), for $P \in \mathcal{X}(\mathbb{F}_q)$ we must have

$$\nu_P(S_{\mathcal{X}}) \geqslant 1 + j_2(P) - \nu.$$

This implies that $\nu_P(S_{\mathcal{X}}) - j_2(P) + \nu - 1 \geqslant 0 \Rightarrow \nu_P(S_{\mathcal{X}}) - j_2(P) + \nu + 1 \geqslant 2$. Hence, we get the following result

Theorem 1.2.4. *Let $\mathcal{X} \subseteq \mathbb{P}^2$ be an irreducible nonsingular algebraic curve of genus g and degree d defined over $\mathbb{F}_q$. If ν is the $\mathbb{F}_q$-Frobenius order of $\mathcal{X}$, then*

$$\mathrm{N}_q(\mathcal{X}) \leqslant \frac{1}{2}\left(\nu(2g-2) + (q+2)d - \sum_{P \in \mathcal{X}} A(P)\right)$$

where $A(P) = j_2(P) - \nu - 1$ if $P \in \mathcal{X}(\mathbb{F}_q)$ and $A(P) = 0$ otherwise.

1.3 Arcs and Codes

The following brief account of the theory of plane arcs and their relationship to linear codes is based on (BIERBRAUER, 2016, Chapter 10 and 17), to which we refer the reader to for further details.

Definition 1.3.1. *A (k,n)-arc $\mathcal{K}$ in $\mathbb{P}^2(\mathbb{F}_q)$ is a set of k points such that each line contains at most n point of $\mathcal{K}$ and there is a line that contains exactly n points of $\mathcal{K}$. A $(k,2)$-arc is simply called an arc.*

If $\mathcal{K} \subseteq \mathbb{P}^2(\mathbb{F}_q)$ be a (k,n)-arc, then for $0 \leqslant i \leqslant q+1$, we define

$$\mathcal{A}_i(\mathcal{K}) := \{l \in \check{\mathbb{P}}^2(\mathbb{F}_q) \mid \#(l \cap \mathcal{K}) = i\}$$

$$a_i(\mathcal{K}) := \#\mathcal{A}_i(\mathcal{K}) \quad \text{and} \quad k_0(\mathcal{K}) := \min\{i \mid a_i(\mathcal{K}) \neq 0\}.$$

When there is no possibility of confusion we will denote them simply by $\mathcal{A}_i$, a_i and k_0.

Definition 1.3.2. *A linear subspace $\mathcal{C}$ of $\mathbb{F}_q^n$ of dimension k is called an $[n,k]_q$-code. The elements of a linear code $\mathcal{C}$ are called codewords.*

The weight of a codeword $x = (x_1, ..., x_n) \in \mathcal{C} \subseteq \mathbb{F}_q^n$ is the number of nonzero coordinates in x, denoted by $wt(x)$. The minimum distance of $\mathcal{C}$ is

$$\min\{\ wt(x) \mid x \in \mathcal{C}, x \neq 0\}.$$

If the minimum distance of $\mathcal{C}$ is d, then we write that $\mathcal{C}$ is an $[n,k,d]_q$-code. A generator matrix G of an $[n,k,d]_q$-code $\mathcal{C}$ is a matrix with k rows and n columns whose rows form a basis of $\mathcal{C}$. The code $\mathcal{C}$ is recovered from G by taking all linear combinations of the rows

of G. If $\mathcal{C}$ contains c_i codewords of weight i, for $i = 1, ..., n$, then the weight enumerator is defined by

$$W_{\mathcal{C}}(z) := c_0 + c_1 z + c_2 z^2 + \cdots + c_n z^n \in \mathbb{Z}[z].$$

Now, let $\mathcal{C}$ be a linear $[n, 3, d]_q$-code described by a generator matrix G. We assume that there is no 0 column in G. We can then consider the columns of G as generators of points in $\mathbb{P}^2(\mathbb{F}_q)$. A linear $[n, 3, d]_q$-code $\mathcal{C}$ is called projective if there is a generator matrix whose columns generate different points in $\mathbb{P}^2(\mathbb{F}_q)$. For a projective $[n, 3, d]_q$-code $\mathcal{C}$ with a generator matrix G, the n points in $\mathbb{P}^2(\mathbb{F}_q)$ corresponding to columns of G form an $(n, n-d)$-arc in $\mathbb{P}^2(\mathbb{F}_q)$. For each i in $0, \ldots, n-d$, the number a_i of lines in $\mathcal{A}_i$ is related to the coefficients c_i of the weight enumerator as follows:

$$(q-1) \cdot (a_0, \cdots, a_{n-d}) = (c_n, \cdots, c_d).$$

2 The Sziklai Bound and Optimal Plane Curves

Let $\mathcal{X}$ be a (projective, geometrically irreducible, algebraic) curve defined over a finite field $\mathbb{F}_q$. It is a classical problem to count the number $\mathrm{N}_q(\mathcal{X})$ of $\mathbb{F}_q$-rational points of $\mathcal{X}$. However, since this problem is rather hard to solve, it is often desirable to find good upper bounds for $\mathrm{N}_q(\mathcal{X})$ depending on some invariants of the curve $\mathcal{X}$. Once we have a bound, it is a natural question to see whether such a bound is sharp or not, and then, it is also natural to try and classify the optimal curves, that is, the curves attaining said bound. In this chapter, we will talk about the Sziklai upper bound and optimal curves.

2.1 Hasse-Weil Bound and Refinements

Before discussing the Sziklai bound, in this section, we will first explore some known bounds. For instance, an important consequence from the Hasse-Weil Theorem 1.1.19 is the famous Hasse-Weil bound:

Theorem 2.1.1. (STICHTENOTH, 2009, Theorem 5.2.3: The Hasse-Weil Bound) *Let $\mathcal{X}$ be a curve of genus $\mathfrak{g} = \mathfrak{g}(\mathcal{X}) \geqslant 0$ defined over $\mathbb{F}_q$. If $\mathrm{N} = \mathrm{N}_q(\mathcal{X})$, then*

$$|\mathrm{N} - (q+1)| \leqslant 2\mathfrak{g}q^{\frac{1}{2}}.$$

The nonsingular plane curves $\mathcal{X}$ defined over $\mathbb{F}_q$ with $\mathrm{N}_q(\mathcal{X}) = q + 1 + 2\mathfrak{g}q^{\frac{1}{2}}$ are called $\mathbb{F}_q$-maximal curves. Maximal curves may exist when $q = n^2$ is a square, and it is known that the genus of a maximal curve is upper bounded by $n(n-1)/2$ (STICHTENOTH, 2009, Proposition 5.3.3 (Ihara)). It is a classical and yet unsolved problem to find the spectrum of the genera of $\mathbb{F}_q$-maximal curves; see (ARAKELIAN; TAFAZOLIAN; TORRES, 2016). When q is not a square, Serre refines this bound:

Theorem 2.1.2. (SERRE et al., 2020, Theorem 2.1.1: The Serre Bound) *Let $\mathcal{X}$ be a curve of genus $g \geqslant 0$ over a finite field $\mathbb{F}_q$. If $\mathrm{N} = \mathrm{N}_q(\mathcal{X})$, then*

$$|\mathrm{N} - (q+1)| \leqslant gm,$$

with $m = [2q^{\frac{1}{2}}]$, where $[x]$ denotes the largest integer $\leqslant x$.

Note that, if q is a square, this "refined Hasse-Weil bound" coincides with the Hasse-Weil Bound (Theorem 2.1.1).

Definition 2.1.3. *Let $\alpha_1, ..., \alpha_{2g} \in \mathbb{C}$ the reciprocals of the roots of the L-polynomial $L_{\mathcal{X}}(t)$ of $\mathcal{X}$ with $\alpha_{g+i} = \overline{\alpha}_i$ for $i = 1, ..., g$. If*

$$x_i := -(\alpha_i + \alpha_{g+i}) \quad \text{for} \quad i = 1, ..., g$$

then we say that $\mathcal{X}$ has zeta function of type $(x_1, ..., x_g)$. Also, a curve $\mathcal{X}$ has defect k if $\mathrm{N}_q(\mathcal{X}) = q + 1 + gm - k$ with $m = [2q^{\frac{1}{2}}]$.

Note that, by Corollary 1.1.18, we have $\mathrm{N}_q(\mathcal{X}) = q + 1 - \sum_{i=1}^{2g} \alpha_i = q + 1 + \sum_{i=1}^{g} x_i$.

Theorem 2.1.4. (SERRE et al., 2020, Theorem 2.2.1)

(1) If $x_1 + x_2 + \cdots + x_g = gm$ (defect 0 case), then $x_i = m$ for $i = 1, ..., m$.

(2) If $x_1 + x_2 + \cdots + x_g = gm - 1$ (defect 1 case), there are two possibilities for $(x_1, ..., x_g)$, namely:

$$(m, m, ..., m, m-1) \quad \text{for} \quad g(\mathcal{X}) \geqslant 1$$

and

$$\left(m, m, ..., m + \frac{-1+\sqrt{5}}{2}, m + \frac{-1-\sqrt{5}}{2}\right) \quad \text{for} \quad g(\mathcal{X}) \geqslant 2.$$

(3) If $x_1 + x_2 + \cdots + x_g = gm - 2$ (defect 2 case), then there are seven possibilities $(x_1, ..., x_g)$, namely:

$$\begin{aligned}
&(m, m, ..., m, m-2) && g \geqslant 1,\\
&(m, m, ..., m, m-1, m-1) && g \geqslant 2,\\
&(m, m, ..., m, m+\sqrt{2}-1, m-\sqrt{2}-1) && g \geqslant 2,\\
&(m, m, ..., m, m+\sqrt{3}-1, m-\sqrt{3}-1) && g \geqslant 2,\\
&\left(m, m, ..., m, m-1, m + \frac{-1+\sqrt{5}}{2}, m + \frac{-1-\sqrt{5}}{2}\right) && g \geqslant 3,\\
&\left(m, m, ..., m, m + \frac{-1+\sqrt{5}}{2}, m + \frac{-1+\sqrt{5}}{2}, m + \frac{-1-\sqrt{5}}{2}, m + \frac{-1-\sqrt{5}}{2}\right) && g \geqslant 4\\
&(m, m, ..., m, m_1, m_2, m_3) && g \geqslant 3
\end{aligned}$$

where $m_k = m + 1 - 4\cos^2(k\pi/7)$ for $k = 1, 2, 3$.

Proposition 2.1.5. (SERRE et al., 2020, Corollary 2.5.2) *Defect 1 is impossible for $g(\mathcal{X}) > 2$.*

Remark 2.1.6. (LAUTER; SERRE, 2002, Fact 3.3) *By the Hasse-Weil Theorem 1.1.19,*

$$|x_i| = |\alpha_i + \alpha_{g+i}| \leqslant |\alpha_i| + |\alpha_{g+i}| = 2q^{\frac{1}{2}} = m + \{2q^{\frac{1}{2}}\}$$

where $\{x\}$ denotes the fractional part of x. Any entry in the table not satifying this condition for all i can be eliminated. So, if $\{2q^{\frac{1}{2}}\} < \sqrt{3} - 1$, $\mathrm{N}_q(\mathcal{X}) = q + gm - 1$ (defect 2) and $g \neq 4$, then $(x_1, ..., x_g) = (m, m, ..., m, m-2)$. The proof of this follows from the fact that the last cases in Theorem 2.1.4 are only possible when $\{2q^{1/2}\}$ is large enough.

2.2 The Sziklai Upper Bound

As we have already mentioned, maximal curves may exist only when $q = n^2$ is a perfect square. When q is not a square, Theorem 2.1.4 item (1) also indicates that curves achieving the Serre Bound (Theorem 2.1.2) are rare due to the constraints imposed in x_i. In this section, we will discuss the Sziklai Upper Bound, which provides an enhancement over the Serre Bound in certain situations.

In this section, we denote by $C_d(\mathbb{F}_q)$ the set of plane curves of degree $d \geqslant 2$ defined over $\mathbb{F}_q$ without $\mathbb{F}_q$-linear components. For $\mathcal{X} \in C_d(\mathbb{F}_q)$, in (SZIKLAI, 2008, Conjecture 1), Sziklai conjectured the bound

$$\mathrm{N}_q(\mathcal{X}) \leqslant (d-1)q + 1 \quad (\text{ The Sziklai Conjecture }) \tag{2.1}$$

and proof a weaker inequality

$$\mathrm{N}_q(\mathcal{X}) \leqslant (d-1)q + \left\lfloor \frac{d}{2} \right\rfloor \tag{2.2}$$

where $\lfloor x \rfloor$ denotes the integer part of x. Actually, as noted by Homma and Kim in (HOMMA; KIM, 2009, Section 1), the bound (2.2) had been already proved by Segre (SEGRE, 1959, Theorem II on page 30).

In (HOMMA; KIM, 2009, section 3), they proved that the Sziklai Conjecture (2.1) fails for curves of degree 4 over $\mathbb{F}_4$, as the plane curve with equation

$$X^4 + Y^4 + Z^4 + X^2Y^2 + Y^2Z^2 + Z^2X^2 + X^2YZ + XY^2Z + XYZ^2 = 0 \tag{2.3}$$

has 14 points over $\mathbb{F}_4$ while Sziklai's bound is equal to 13. Also, they proved that the curve defined by (2.3) over $\mathbb{F}_4$ is a unique curve up to projective equivalence with degree 4 and 14 $\mathbb{F}_4$-rational points:

Theorem 2.2.1. (HOMMA; KIM, 2009, Theorem 3.3) *Let $\mathcal{X} \in C_4(\mathbb{F}_4)$. If $\mathrm{N}_4(\mathcal{X}) = 14$, then $\mathcal{X}$ is projectively equivalent to the curve defined by (2.3) over $\mathbb{F}_4$.*

So, Homma and Kim modify The Sziklai Conjecture (2.1):

Conjecture 1. (HOMMA; KIM, 2010b, Section 1: The Modified Sziklai Conjecture) *Unless $\mathcal{X}$ is a curve defined over $\mathbb{F}_4$ which is projectively equivalent to the curve defined by (2.3) over $\mathbb{F}_4$, we might have*

$$\mathrm{N}_q(\mathcal{X}) \leqslant (d-1)q + 1.$$

Later on, in a sequence of three papers (HOMMA; KIM, 2009; HOMMA; KIM, 2010b; HOMMA; KIM, 2010a), Homma and Kim proved The Modified Sziklai Conjecture 1. Since the proof of this conjecture is spread across three paper, we will provide a concise

overview of the proof main idea, along with some essential results, in preparation for the next chapter: First, note that The Modified Sziklai Conjecture 1 is true if $d \geqslant q+2$; in this case, we have $(d-1)q+1 \geqslant (q+1)q+1$. As an obvious bound to the cardinality of the set of all $\mathbb{F}_q$-rational points of $\mathcal{X}$ is $\mathrm{N}_q(\mathcal{X}) \leqslant q^2+q+1 = (q+1)q+1$, which comes from $\mathcal{X}(\mathbb{F}_q) \subseteq \mathbb{P}^2(\mathbb{F}_q)$, then

$$\mathrm{N}_q(\mathcal{X}) \leqslant q^2+q+1 \leqslant (d-1)q+1.$$

So they consider the conjecture for $2 \leqslant d \leqslant q+1$. In the first paper (HOMMA; KIM, 2009, Corollary 2.2), they proved a new bound

$$\mathrm{N}_q(\mathcal{X}) \leqslant (d-1)q + (q+2-d) \tag{2.4}$$

The bound (2.4) implies that The Modified Sziklai Conjecture 1 is true for $d = q+1$.

Now, for a nonsingular plane curve $\mathcal{X} \in C_d(\mathbb{F}_q)$ with $2 \leqslant d \leqslant q-1$, as noted by Homma and Kim in (HOMMA; KIM, 2010b, Theorem 4.1), the Sziklai conjecture is true by the theory of Stöhr-Voloch for a Plane Curve. In fact, note that

$$(d-1)q+1-\frac{1}{2}\cdot d(d+q-1) = \frac{1}{2}\cdot(d-2)(q-d-1) \geqslant 0;$$

so, if $\mathcal{X}$ is $\mathbb{F}_q$-Frobenius classical, by Theorem 1.2.2, then $\mathrm{N}_q(\mathcal{X}) \leqslant \frac{1}{2}\cdot d(d+q-1) \leqslant (d-1)q+1$. Also, we have that

$$(d-1)q+1-d(q-d+2) = (d-\sqrt{q}-1)(d+\sqrt{q}-1).$$

So, if $\mathcal{X}$ is $\mathbb{F}_q$-Frobenius nonclassical, by (HEFEZ; VOLOCH, 1990, Proposition 6), we must have $d \geqslant \sqrt{q}+1$ and, by Theorem 1.2.3,

$$\mathrm{N}_q(\mathcal{X}) = d(q-1)-(2g-2) = d(q-d+2) \leqslant (d-1)q+1.$$

Also, as noted in (HOMMA; KIM, 2010b, Remark 4.2), Stöhr-Voloch bound 1.2.2 is effective even if an irreducible $\mathbb{F}_q$-Frobenius classical curve $\mathcal{X}$ has singularities.

To settle the Modified Sziklai's Conjecture 1 affirmatively for other cases, the following results prove that they can assume that the $\mathcal{X}$ curve is absolutely irreducible without a singular $\mathbb{F}_q$-rational point:

Proposition 2.2.2. (HOMMA; KIM, 2010b, Proposition 2.1) *If $\mathcal{X}$ is reducible over $\mathbb{F}_q$, then $\mathrm{N}_q(\mathcal{X}) < (d-1)q$.*

Proposition 2.2.3. (HOMMA; KIM, 2010b, Proposition 2.2) *If $\mathcal{X}$ has an irreducible component which is not defined over $\mathbb{F}_q$, then $\mathrm{N}_q(\mathcal{X}) \leqslant (d-1)q$.*

Proposition 2.2.4. (HOMMA; KIM, 2010b, Proposition 2.3) *If $\mathcal{X}$ has a singular point which is an $\mathbb{F}_q$-rational point, then $\mathrm{N}_q(\mathcal{X}) \leqslant (d-1)q$.*

For the case $d = q$, the following results provide conditions for the lines defined over $\mathbb{F}_q$ to intersect the curve at q rational points; In addition to being the main results that help to prove the case $d = q$, they help to characterize the curves of degree q with $\mathrm{N}_q(\mathcal{X}) = (q-1)q+1$ (see, (HOMMA; KIM, 2012)):

Proposition 2.2.5. (HOMMA; KIM, 2010b, Proposition 3.1) *Let $\mathcal{X} \in C_q(\mathbb{F}_q)$. Fix an $\mathbb{F}_q$-point $P_0 \in \mathcal{X}$ and an $\mathbb{F}_q$-line $l_\infty \subset \mathbb{P}^2$ with $P_0 \notin l_\infty$. Suppose there are $\mathbb{F}_q$-lines $l_1, ..., l_t$ with $q \geqslant t \geqslant 3$ passing thorugh P_0 such that the q $\mathbb{F}_q$-points of $l_i \backslash l_\infty$ are contained in $\mathcal{X}$. For an $\mathbb{F}_q$-line $l \in \check{P}_0$ other than these t lines, if $\#((l \backslash l_\infty) \cap \mathcal{X}(\mathbb{F}_q)) \geqslant q - t + 2$, then all the q $\mathbb{F}_q$-points of $l \backslash l_\infty$ are contained in $\mathcal{X}$.*

Proposition 2.2.6. (HOMMA; KIM, 2010b, Proposition 3.2) *Let $\mathcal{X} \in C_q(\mathbb{F}_q)$. Fix an $\mathbb{F}_q$-point $Q_0 \in \mathbb{P}^2(\mathbb{F}_q) \backslash \mathcal{X}$. Suppose there are $\mathbb{F}_q$-lines $l_1, ..., l_t$ with $q - 1 \geqslant t \geqslant 2$ passing thorugh Q_0 such that $l_i(\mathbb{F}_q) \backslash \{Q_0\} \subset \mathcal{X}$. For an $\mathbb{F}_q$-line $l \in \check{Q}_0$ other than these t lines, if $\#(l \cap \mathcal{X}(\mathbb{F}_q)) \geqslant q - t + 2$, then $l(\mathbb{F}_q) \backslash \{Q_0\} \subset \mathcal{X}$.*

These two propositions establish the validity of the Modified Sziklai's Conjecture 1 for $d = q > 4$ (see, (HOMMA; KIM, 2010b, Theorem 3.3)). Also, as previously discussed, these two results aid in characterizing curves $\mathcal{X}$ of degree q with $\mathrm{N}_q(\mathcal{X}) = (q-1)q+1$. In Chapter 3, we will prove a similar proposition for curves $\mathcal{X}$ of degree $q-1$ (Proposition 3.1.9) in order to characterize curves of degree $q-1$ with $\mathrm{N}_q(\mathcal{X}) = ((q-1)-1)q+1 = (q-1)^2$.

Therefore, to settle the conjecture, remains to be considered $\mathbb{F}_q$-Frobenius nonclassical plane curves of degree d with $2 \leqslant d \leqslant q-1$. In this case, Homma and Kimm proved the following result:

Theorem 2.2.7. (HOMMA; KIM, 2010a, Theorem 2.3) *Let q be a power of a prime number p, and say $q = p^e$. Let $\mathcal{X}$ be an $\mathbb{F}_q$-Frobenius nonclassical irreducible curve of degree d over $\mathbb{F}_q$, and p^i the intersection multiplicity $i(Q, \mathcal{X} \cap \mathbb{T}_Q(\mathcal{X}))$ for a general point $Q \in \mathcal{X}$. If $d \neq p^{e-i} + 1$, then $\mathrm{N}_q(\mathcal{X}) \leqslant (d-1)q$.*

Therefore, they established the following theorem:

Theorem 2.2.8 (Sziklai's upper bound)**.** *If $\mathcal{X} \in C_d(\mathbb{F}_q)$, then*

$$\mathrm{N}_q(\mathcal{X}) \leqslant (d-1)q + 1, \tag{2.5}$$

except for the curve over $\mathbb{F}_4$ which is projectively equivalent to the curve defined by (2.3).

Once we have a bound, it is natural to try and classify the optimal curves, that is, the curves attaining said bound. Regarding the Sziklai upper bound (2.5), we make the following observation:

Remark 2.2.9. (HOMMA; KIM, 2010b, section 2) *If $(d, q) \neq (4, 4)$ and $\mathrm{N}_q(\mathcal{X}) = (d-1)q+1$, then $\mathcal{X}$ is absolutely irreducible and any rational point of $\mathcal{X}$ is nonsingular.*

2.3 Optimal Plane Curves over Finite Fields

In (HOMMA; KIM, 2010b, Remark 5.1), Homma and Kim observe that the possible degrees d of a nonsingular curve with $(d-1)q+1$ rational points are $q+2, q+1$, $q, q-1, \sqrt{q}+1$ and 2. Also, for each degree d in the list, there exists a nonsingular curve of degree d that attains the bound. For $d \neq q-1$, the complete classification of such optimal curves is known; we summarize these results in the following Theorem:

Theorem 2.3.1. *Let $\mathcal{X} \in C_d(\mathbb{F}_q)$ a nonsingular curve with $\mathrm{N}_q(\mathcal{X}) = (d-1)q+1$.*

(i) (HIRSCHFELD, 1998, Section 5.1) *If $d = 2$, then $\mathcal{X} \simeq_{\mathrm{proj}} \mathbf{v}(X^2 + YZ)$ over $\mathbb{F}_q$.*

(ii) (HIRSCHFELD et al., 1991) *If $d = \sqrt{q}+1$, then*

$$\mathcal{X} \simeq_{\mathrm{proj}} \mathbf{v}(X^{\sqrt{q}+1} + Y^{\sqrt{q}+1} + Z^{\sqrt{q}+1})$$

over $\mathbb{F}_q$ when $q > 4$ is a square.

(iii) (TALLINI, 1961; HOMMA; KIM, 2013) *If $d = q+2$, then $\mathcal{X}$ is projectively equivalent over $\mathbb{F}_q$ to the curve of type*

$$\mathbf{v}(Y(Y^qZ - YZ^q) + Z(Z^qX - ZX^q) + (aX + bY + cZ)(X^qY - XY^q))$$

where $t^3 - (ct^q + bt + a)$ is irreducible over $\mathbb{F}_q$.

(iv) (HOMMA; KIM, 2011, Theorem 1.3) *If $d = q+1$, then $\mathcal{X}$ is projectively equivalent over $\mathbb{F}_q$ to the curve*

$$\mathcal{X}_{q+1} := \mathbf{v}(X^{q+1} - X^2Z^{q-1} + Y^qZ - YZ^q)$$

when $q \geqslant 5$ or $q = 2$. If $q = 4$, then $\mathcal{X}$ is projectively equivalent over $\mathbb{F}_4$ to either $\mathcal{X}_5$ or the curve

$$\mathbf{v}(\mu G(X,Y,Z) + XYZ(\mu^2(X^2+Y^2+Z^2) + XY + YZ + ZX))$$

where $G(X,Y,Z) = X^4Y + XY^4 + Y^4Z + YZ^4 + Z^4X + ZX^4$ and $\mu^2 + \mu + 1 = 0$. Moreover, those two curves are not projectively equivalent to each other over $\mathbb{F}_4$. If $q = 3$, then $\mathcal{X}$ is projectively equivalent over $\mathbb{F}_3$ either to $\mathcal{X}_4$ or to the curve

$$\mathbf{v}(X^3Y - XY^3 + Y^3Z - YZ^3 + Z^3X - ZX^3 + XYZ(X + Y - Z)).$$

Moreover, those two curves are not projectively equivalent to each other over $\mathbb{F}_3$.

(v) (HOMMA; KIM, 2012, Main Theorem) *If $d = q$, then*

$$\mathcal{X} \simeq_{\mathrm{proj}} \mathbf{v}(X^q - XZ^{q-1} + Y^{q-1}Z - Z^q)$$

over $\mathbb{F}_q$.

For $d = q-1$, as it was mentioned by Sziklai in (SZIKLAI, 2008), the curve

$$\mathcal{X}_{(\alpha,\beta,\gamma)} := \mathbf{v}(\alpha X^{q-1} + \beta Y^{q-1} + \gamma Z^{q-1})$$

with $\alpha, \beta, \gamma \in \mathbb{F}_q^*$ and $\alpha + \beta + \gamma = 0$ has $(q-1)^2$ rational points. This curve is nonsingular and the set of its $\mathbb{F}_q$-rational points is

$$\mathcal{X}_{(\alpha,\beta,\gamma)}(\mathbb{F}_q) = \mathbb{P}^2(\mathbb{F}_q) \backslash (\mathbf{v}(X) \cup \mathbf{v}(Y) \cup \mathbf{v}(Z)).$$

In (HOMMA, 2024), Homma has studied the number of projective equivalence classes over $\mathbb{F}_q$ in this family of curves. More precisely, he proves the following theorem.

Theorem 2.3.2. (HOMMA, 2024, Theorem 1.3) *The number ν_q of projective equivalence classes over $\mathbb{F}_q$ in the family of curves*

$$\{\mathcal{X}_{(\alpha,\beta,\gamma)} \mid \alpha, \beta, \gamma \in \mathbb{F}_q^*,\ \alpha + \beta + \gamma = 0\}$$

is as follows:

(i) *Suppose that the characteristic of $\mathbb{F}_q$ is neither 2 nor 3.*

  (1) *If $q \equiv 2 \mod 3$, then $\nu_q = (q+1)/6$.*

  (2) *If $q \equiv 1 \mod 3$, then $\nu_q = (q+5)/6$.*

(ii) *Suppose that q is a power of 3. Then $\nu_q = (q+3)/6$.*

(iii) *Suppose that q is a power of 2:*

  (1) *If $q \equiv 2 \mod 3$, then $\nu_q = (q-2)/6$.*

  (2) *If $q \equiv 1 \mod 3$, then $\nu_q = (q+2)/6$.*

In the same paper, the curves of degree 3 with 9 $\mathbb{F}_4$-rational points are classified.

Theorem 2.3.3. (HOMMA, 2024, Theorem 3.1) *Let $\mathcal{X}$ be a nonsingular plane curve of degree 3 over $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$. If $\mathrm{N}_4(\mathcal{X}) = 9$, then $\mathcal{X}$ is either*

(i) the Hermitian cubic $\mathcal{H}_3$ given by $\mathbf{v}(X^3 + Y^3 + Z^3)$ or

(ii) projectively equivalent to the curve $\mathcal{X}_\alpha$ given by $\mathbf{v}(X^3 + \alpha Y^3 + \alpha^2 Z^3)$.

Remark 2.3.4. (HOMMA, 2024, Section 4) *The Hermitian cubic $\mathcal{H}_3$ and the curve $\mathcal{X}_\alpha$ are birationally equivalent over $\mathbb{F}_4$. Also, they are projectively equivalent over $\mathbb{F}_{2^6}$.*

In the same paper, Homma has stated the following Question 1: Are there curves of degree $q-1$ that attain the Sziklai's upper bound such that they are not projectively equivalent over $\mathbb{F}_q$ to a curve of type $\mathcal{X}_{(\alpha,\beta,\gamma)}$?

In the next section, we give a negative answer to Question 1 for $q \geqslant 5$.

3 Optimal Plane Curves of Degree $q-1$

Let $q \geqslant 5$ be a prime power. In this chapter, we complete the classification of curves that are extremal with respect to the Sziklai bound; more precisely, we prove that if a plane curve $\mathcal{X}$ of degree $q-1$ defined over $\mathbb{F}_q$ without $\mathbb{F}_q$-linear components attains the Sziklai upper bound $(d-1)q+1 = (q-1)^2$ for the number of its $\mathbb{F}_q$-rational points, then $\mathcal{X}$ is projectively equivalent over $\mathbb{F}_q$ to the curve $\mathcal{X}_{(\alpha,\beta,\gamma)} : \alpha X^{q-1} + \beta Y^{q-1} + \gamma Z^{q-1} = 0$ for some $\alpha, \beta, \gamma \in \mathbb{F}_q^*$ such that $\alpha + \beta + \gamma = 0$ (Theorem 3.2.4). Also, since the Sziklai bound is equal to the Stöhr-Voloch bound for plane curves of degree $q-1$, this result classifies the $\mathbb{F}_q$-Frobenius extremal classical nonsingular plane curves of degree $q-1$.

3.1 Preliminary results

In this section, we give several technical results that are necessary to prove our main result (Theorem 3.2.4).

The following result is of independent interest; however, it will effectively be used only on the proof of Proposition 3.2.1, where the case $q = 5$ is dealt with. Recall that, by Theorem 2.3.3, this is the smallest case to be considered.

Theorem 3.1.1. *Let $\mathcal{X} \in C_{q-1}(\mathbb{F}_q)$ with $\mathrm{N}_q(\mathcal{X}) = (q-1)^2$. Then, $\mathcal{X}$ is nonsingular.*

Proof. Let $F(X,Y,Z) \in \mathbb{F}_q[X,Y,Z]$ be a homogeneous equation for $\mathcal{X}$ over $\mathbb{F}_q$. By Remark 2.2.9, $\mathcal{X}$ is absolutely irreducible and any $\mathbb{F}_q$-rational point of $\mathcal{X}$ is nonsingular. Also, by Theorem 2.2.7, $\mathcal{X}$ is $\mathbb{F}_q$-Frobenius classical. Let $\mathcal{Y}$ be the curve defined by the homogeneous equation $G(X,Y,Z) := X^q \cdot F_X + Y^q \cdot F_Y + Z^q \cdot F_Z \in \mathbb{F}_q[X,Y,Z]$. If $(x:y:z) \in \mathcal{X}(\mathbb{F}_q)$, by Euler's formula, we have that

$$\begin{aligned} G(x,y,z) &= x^q \cdot F_X(x,y,z) + y^q \cdot F_Y(x,y,z) + z^q \cdot F_Z(x,y,z) \\ &= x \cdot F_X(x,y,z) + y \cdot F_Y(x,y,z) + z \cdot F_Z(x,y,z) \\ &= (q-1) \cdot F(x,y,z) = 0. \end{aligned}$$

Hence, $\mathcal{X}(\mathbb{F}_q) \subseteq \mathcal{Y}$. Let $\mathrm{Sing}(\mathcal{X})$ be the set of all singularities of $\mathcal{X}$. If $(x:y:z) \in \mathrm{Sing}(\mathcal{X})$, then $F_X(x,y,z) = F_Y(x,y,z) = F_Z(x,y,z) = 0$; hence, $\mathrm{Sing}(\mathcal{X}) \subseteq \mathcal{Y}$. Since $\mathrm{N}_q(\mathcal{X})$ attains also the Stöhr-Voloch bound 1.2.2, then $\mathrm{I}(P, \mathcal{X} \cap \mathcal{Y}) = 2$ for each $P \in \mathcal{X}(\mathbb{F}_q)$ and $2\mathrm{N}_q(\mathcal{X}) = (q-1) \cdot 2(q-1) = \partial(F) \cdot \partial(G)$. Hence, by Bézout's theorem 1.1.4,

$$\mathcal{X} \cdot \mathcal{Y} := \sum_P I(P, \mathcal{X} \cap \mathcal{Y}) P = \sum_{P \in \mathcal{X}(\mathbb{F}_q)} 2P.$$

Since $\mathrm{Sing}(\mathcal{X}) \subseteq \mathcal{Y}$, then any singular point of $\mathcal{X}$ must appear in the support of the intersection divisor $\mathcal{X} \cdot \mathcal{Y}$. Therefore, $\mathcal{X}$ is nonsingular.

□

The next result is crucial to our strategy:

Proposition 3.1.2. (HOMMA, 2024, Proposition 2.1) *Let $\mathcal{X}$ be a possibly reducible plane curve over $\mathbb{F}_q$ of degree $q-1$. Then*

$$\mathcal{X} \in \{\mathcal{X}_{(\alpha,\beta,\gamma)} \mid \alpha,\beta,\gamma \in \mathbb{F}_q^*,\ \alpha+\beta+\gamma=0\} \Leftrightarrow \mathcal{X}(\mathbb{F}_q) = \mathbb{P}^2(\mathbb{F}_q)\backslash(\mathbf{v}(X)\cup\mathbf{v}(Y)\cup\mathbf{v}(Z)).$$

Now, fix a curve $\mathcal{X} \in C_{q-1}(\mathbb{F}_q)$ with $\mathrm{N}_q(\mathcal{X}) = (q-1)^2$. Let

$$Z(\mathcal{X}) := \mathbb{P}^2(\mathbb{F}_q)\backslash\mathcal{X}(\mathbb{F}_q).$$

Note that, by Proposition 3.1.2, if $Z(\mathcal{X}) = (\mathbf{v}(X)\cup\mathbf{v}(Y)\cup\mathbf{v}(Z))(\mathbb{F}_q)$, then $\mathcal{X} = \mathcal{X}_{(\alpha,\beta,\gamma)}$ for some $\alpha,\beta,\gamma \in \mathbb{F}_q^*$ such that $\alpha+\beta+\gamma=0$. By Remark 1.1.3, the general projective linear group $\mathrm{PGL}(3,q)$ acts 3-transitively on the set of non concurrent lines of $\mathbb{P}^2(\mathbb{F}_q)$. So, as $\#Z(\mathcal{X}) = 3q$, if there are three lines $l_1,l_2,l_3 \in \check{\mathbb{P}}^2(\mathbb{F}_q)$ such that $Z(\mathcal{X}) = (l_1\cup l_2\cup l_3)(\mathbb{F}_q)$, then l_1,l_2,l_3 are not concurrent and we can choose coordinates X,Y,Z of $\mathbb{P}^2$ such that $l_1 = \mathbf{v}(X), l_2 = \mathbf{v}(Y)$ and $l_3 = \mathbf{v}(Z)$. This means that, in order to prove our main result (Theorem 3.2.4), it is enough to show the existence of such three lines. To do this, we first prove that $\mathcal{X}(\mathbb{F}_q)$ has a structure of (n,k)-arc in $\mathbb{P}^2(\mathbb{F}_q)$:

Lemma 3.1.3. *The set $\mathcal{X}(\mathbb{F}_q) \subseteq \mathbb{P}^2(\mathbb{F}_q)$ is a $((q-1)^2, q-1)$-arc.*

Proof. Since $\deg(\mathcal{X}) = q-1$, then $\#(l\cap\mathcal{X}(\mathbb{F}_q)) \leqslant q-1$ for every line $l \in \check{\mathbb{P}}^2(\mathbb{F}_q)$. Let

$$t := \max\{\#(l\cap\mathcal{X}(\mathbb{F}_q)) \mid l \in \check{\mathbb{P}}^2(\mathbb{F}_q)\} \leqslant q-1.$$

If $P \in \mathcal{X}(\mathbb{F}_q)$, then each line in $\check{P}(\mathbb{F}_q)$ contains at most t points of $\mathcal{X}(\mathbb{F}_q)$. Since $\#\check{P}(\mathbb{F}_q) = q+1$ then $(q-1)^2 = \mathrm{N}_q(\mathcal{X}) \leqslant 1+(q+1)(t-1)$. Hence,

$$q-1 \geqslant t \geqslant \frac{q(q-2)}{q+1} + 1 = q-2+\frac{3}{q+1} > q-2.$$

This implies that $t = q-1$. Therefore, $\mathcal{X}(\mathbb{F}_q)$ is a $((q-1)^2, q-1)$-arc in $\mathbb{P}^2(\mathbb{F}_q)$.

□

For $0 \leqslant i \leqslant q+1$, recall the definition of

$$\mathcal{A}_i = \{l \in \check{\mathbb{P}}^2(\mathbb{F}_q) \mid \#(l\cap\mathcal{X}(\mathbb{F}_q)) = i\} \text{ and } a_i = \#\mathcal{A}_i.$$

Since $\deg(\mathcal{X}) = q-1$, then $a_q = a_{q+1} = 0$. A line $l \in \check{\mathbb{P}}^2(\mathbb{F}_q)$ is called an i-line if $l \in \mathcal{A}_i$. A point $P \in \mathbb{P}(\mathbb{F}_q)$ is said to be of type $i_1^{r_1}...i_t^{r_t}$ ($i_1 > \cdots > i_t$ and $r_1,...,r_t \geqslant 0$) if the number of i_j-lines through P is r_j for $j = 1,...,t$. Also, as $\mathcal{X}(\mathbb{F}_q)$ is a $((q-1)^2, q-1)$-arc, we may use the following result:

Lemma 3.1.4. (HIRSCHFELD, 1979, Lemma 12.1.1) *With the same notation as above, we have the following equalities.*

(i) $\sum_{i=0}^{q-1} a_i = q^2+q+1.$

(ii) $\sum_{i=1}^{q-1} ia_i = (q+1)(q-1)^2.$

(iii) $\sum_{i=2}^{q-1} i(i-1)a_i = q(q-2)(q-1)^2.$

Lemma 3.1.5. *Let $P \in \mathbb{P}^2(\mathbb{F}_q)$ be a point of type $i_1^{r_1}...i_t^{r_t}$. Then $r_1+\cdots+r_t = q+1$. Moreover,*

(i) If $P \in \mathcal{X}$, then $i_j \geqslant 1$ for all $j = 1,...,t$ and $1+\sum r_j(i_j-1) = (q-1)^2$.

(ii) If $P \notin \mathcal{X}$ then $\sum r_j i_j = (q-1)^2$.

Proof. Since the $\mathbb{F}_q$-lines through P cover the whole plane $\mathbb{P}^2(\mathbb{F}_q)$ and $\mathrm{N}_q(\mathcal{X}) = (q-1)^2$, the proof is straightforward.

□

Corollary 3.1.6. *Let i and j be (not necessarily distinct) non-negative integers. Suppose that there are different $\mathbb{F}_q$-lines l_1, l_2 with $l_1 \in \mathcal{A}_i$ and $l_2 \in \mathcal{A}_j$. If $P = l_1 \cap l_2 \in \mathcal{X}(\mathbb{F}_q)$, then $i+j \geqslant q$.*

Proof. Suppose that P is of type $i_1^{r_1}...i_t^{r_t}$. By Lemma 3.1.5 item (i), we have

$$\begin{aligned}(q-1)^2 &= 1+\sum r_j(i_j-1)\\ &\leqslant 1+(i-1)+(j-1)+(q-1)(q-2)\\ &= i+j-1+q^2-3q+2\\ &= i+j-q+(q-1)^2.\end{aligned}$$

Therefore, $i+j \geqslant q$.

□

To simplify our notation, we give the following definition.

Definition 3.1.7. *For $i = 0,\ldots,q-1$ we define $\psi_i : \mathbb{P}^2(\mathbb{F}_q) \to \{0,1,...,q+1\}$ as*

$$\psi_i(P) := \#(\check{P}(\mathbb{F}_q) \cap \mathcal{A}_i).$$

Lemma 3.1.8. *If $P \in \mathcal{X}(\mathbb{F}_q)$, then $\psi_{q-1}(P) \geqslant 3$. In particular, $a_{q-1} \geqslant 3(q-1)$. Also, if $\psi_{q-1}(P) = 3$, then P is of type $(q-1)^3(q-2)^{q-2}$.*

Proof. Let $r_P = \psi_{q-1}(P)$. By Lemma 3.1.5 (i), if P is of type $i_1^{r_1}...i_t^{r_t}$ then

$$\begin{aligned}(q-1)^2 &= 1 + \sum r_j(i_j - 1)\\ &\leqslant 1 + r_P(q-2) + (q+1-r_P)(q-3)\\ &= 1 + qr_P - 2r_P + q^2 - 3q + q - 3 - qr_P + 3r_P\\ &= r_P + (q-1)^2 - 3,\end{aligned}$$

hence, $r_P \geqslant 3$. We get $3(q-1)^2 = 3 \cdot \mathrm{N}_q(\mathcal{X})$ lines in $\mathcal{A}_{q-1}$. However, each line was counted at most $(q-1)$ times. This implies $a_{q-1} \geqslant 3(q-1)$. If $\psi_{q-1}(P) = 3$, let $s_P = \psi_{q-2}(P)$, then

$$\begin{aligned}(q-1)^2 &= 1 + \sum r_j(i_j - 1)\\ &\leqslant 1 + 3(q-2) + s_P(q-3) + (q-2-s_P)(q-4)\\ &= 3q - 5 + qs_P - 3s_P + q^2 - 4q - 2q + 8 - qs_P + 4s_P\\ &= s_P + (q-1)^2 + 2 - q,\end{aligned}$$

hence, $s_P \geqslant q-2$. This means that the other lines in $\check{P}(\mathbb{F}_q)$ are in $\mathcal{A}_{q-2}$. Therefore, P is of type $(q-1)^3(q-2)^{q-2}$.

□

Roughly speaking, in order to prove our result, we need to prove the existence of a point $Q_0 \in Z(\mathcal{X})$ such that $\psi_{q-1}(Q_0)$ is *big enough*. In order to do so, we prove the following proposition, which is inspired by Proposition 2.2.5 and 2.2.6:

Proposition 3.1.9. *Fix a point $Q_0 \in Z(\mathcal{X})$ and $l_\infty \in \check{\mathbb{P}}^2(\mathbb{F}_q)\backslash\check{Q}_0(\mathbb{F}_q)$. Suppose there are lines $l_1, ..., l_t \in \check{Q}_0(\mathbb{F}_q)$ $(2 \leqslant t \leqslant q-1)$ such that $l_i(\mathbb{F}_q)\backslash(\{Q_0\} \cup l_\infty) \subseteq \mathcal{X}(\mathbb{F}_q)$. For a line $l \in \check{Q}_0(\mathbb{F}_q)$ other than these t lines, if $\#((l\backslash l_\infty) \cap \mathcal{X}(\mathbb{F}_q)) \geqslant q-t$, then*

$$l(\mathbb{F}_q)\backslash(\{Q_0\} \cup l_\infty(\mathbb{F}_q)) \subseteq \mathcal{X}(\mathbb{F}_q).$$

Proof. Choose coordinates X, Y, Z of $\mathbb{P}^2$ such that $l_1 = \mathbf{v}(X), l_2 = \mathbf{v}(Y)$ and $l_\infty = \mathbf{v}(Z)$, whence $Q_0 = (0:0:1)$. Let

$$G_0 := Z^{q-1} - X^{q-1} - Y^{q-1},\ G_1 := XY \in \mathbb{F}_q[X, Y, Z].$$

Note that $\mathbf{v}(G_0)$ and $\mathbf{v}(G_1)$ are plane curves with no common components. A direct computation shows that $\#(\mathbf{v}(G_0) \cap \mathbf{v}(G_1)) = 2(q-1) = \partial(G_0) \cdot \partial(G_1)$; more precisely, we have

$$\mathbf{v}(G_0) \cap \mathbf{v}(G_1) = \{(0:1:\alpha),\ (1:0:\alpha) \mid \alpha \in \mathbb{F}_q^*\} = (l_1 \cup l_2)(\mathbb{F}_q)\backslash(\{Q_0\} \cup l_\infty).$$

Hence, by Bézout's Theorem 1.1.4, $\mathrm{I}(P, \mathbf{v}(G_0) \cap \mathbf{v}(G_1)) = 1$ for each $P \in \mathbf{v}(G_0) \cap \mathbf{v}(G_1)$. Also, since $l_i(\mathbb{F}_q) \backslash (\{Q_0\} \cup l_\infty) \subseteq \mathcal{X}(\mathbb{F}_q)$ for $i = 1, 2$, then $\mathbf{v}(G_0) \cap \mathbf{v}(G_1) \subseteq \mathcal{X}(\mathbb{F}_q)$. Let F be a homogeneous equation for $\mathcal{X}$ over $\mathbb{F}_q$; by Noether's "AF + BG" Theorem 1.1.5, we can write

$$F(X,Y,Z) = a_{00}(Z^{q-1} - X^{q-1} - Y^{q-1}) + XY(g_{q-3}(X,Y) + g_{q-4}(X,Y)Z + \cdots + g_0 Z^{q-3})$$

where $g_\nu \in \mathbb{F}_q[X,Y,Z]$ is homogeneous of degree ν and $a_{00} \in \mathbb{F}_q^*$. In general, any line $L \in \check{Q}_0(\mathbb{F}_q) \backslash \{l_1, l_2\}$ is defined by an equation of the form $Y - \mu X = 0$ for some $\mu \in \mathbb{F}_q^*$. Hence

$$L(\mathbb{F}_q) \backslash (\{Q_0\} \cup l_\infty(\mathbb{F}_q)) = \{(1 : \mu : \beta) \mid \beta \in \mathbb{F}_q^*\}.$$

Since $a_{00}(\beta^{q-1} - 1 - \mu^{q-1}) = -a_{00}$ when $\beta, \mu \in \mathbb{F}_q^*$, then

$$F(1,\mu,\beta) = (\mu(g_{q-3}(1,\mu) - a_{00}) + \mu q_{q-4}(1,\mu)\beta + \cdots + \mu g_0 \beta^{q-3}. \tag{3.1}$$

In particular, if $l_{2+\mu} = \mathbf{v}(Y - a_\mu X)$ with $\mu = 1, ..., t-2$, we must have $a_\mu \neq 0$. Let

$$B = \begin{pmatrix} & \vdots & & & \\ 1 & \beta & \beta^2 & \cdots & \beta^{q-3} \\ & \vdots & & & \end{pmatrix}_{\beta \in \mathbb{F}_q^* \backslash \{1\}}.$$

Since $l_{2+\mu}(\mathbb{F}_q) \backslash (\{Q_0\} \cup l_\infty) \subseteq \mathcal{X}(\mathbb{F}_q)$, by equation (3.1), then

$$B \cdot \begin{pmatrix} a_\mu g_{q-3}(1, a_\mu) - a_{00} \\ a_\mu g_{q-4}(1, a_\mu) \\ \vdots \\ a_\mu g_0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Since B is a Vandermonde matrix, we have $\det(B) \neq 0$. This implies that

$$g_{q-4}(1, a_\mu) = \cdots = g_0(1, a_\mu) = 0.$$

If $\nu < t-2$, since $g_\nu(1,y)$ has $t-2$ roots $\{a_1, ..., a_{t-2}\}$ but its degree is less than $t-2$, then $g_\nu(1,y) \equiv 0$ as a polynomial in y. Therefore,

$$F(1,y,z) = a_{00}(z^{q-1} - y^{q-1}) + (y g_{q-3}(1,y) - a_{00}) + y q_{q-4}(1,y)z + \cdots + y g_{t-2}(1,y) z^{q-t-1}.$$

Let $l = \mathbf{v}(Y - \mu X)$, where $\mu \in \mathbb{F}_q^*$, and $\{(1, \mu, \beta_i) \mid 1 \leqslant i \leqslant q-t\}$ is a set of chosen points of $(l \backslash l_\infty)(\mathbb{F}_q) \cap \mathcal{X}$. Then $\mu \neq 0$ and $\beta_i \neq 0$ for $i = 1, ..., q-t$. Hence,

$$\begin{pmatrix} & \vdots & & & \\ 1 & \beta_i & \beta_i^2 & \cdots & \beta_i^{q-t-1} \\ & \vdots & & & \end{pmatrix}_{i=1,\ldots,q-t} \begin{pmatrix} \mu g_{q-3}(1,\mu) - a_{00} \\ \mu g_{q-4}(1,\mu) \\ \vdots \\ \mu g_{t-2}(1,\mu) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

This implies that $\mu g_{q-3}(1,\mu) - a_{00} = \mu g_{q-4}(1,\mu) = \cdots = \mu g_{t-2}(1,\mu) = 0$. So $F(1,\mu,\beta) = 0$ for any $\beta \in \mathbb{F}_q^*$. Therefore, $l(\mathbb{F}_q) \backslash (\{Q_0\} \cup l_\infty(\mathbb{F}_q)) \subseteq \mathcal{X}(\mathbb{F}_q)$.

□

Corollary 3.1.10. *Suppose that there is a point $Q \in Z(\mathcal{X})$ such that $r = \psi_{q-1}(Q) \geqslant 2$. If these r lines are $l_1, ..., l_r$, then $\{(l_i(\mathbb{F}_q)\backslash\{Q\}) \cap Z(\mathcal{X}) \mid i = 1, ..., r\}$ is contained in a line.*

Proof. Let $Q_i = (l_i(\mathbb{F}_q)\backslash\{Q\}) \cap Z(\mathcal{X})$ with $i = 1, ..., r$. Since $r \geqslant 2$, we can consider the line $l_\infty := \overline{Q_1Q_2}$. Since $l_i \in \mathcal{A}_{q-1}$, then $\#(l_i\backslash l_\infty) \cap \mathcal{X}(\mathbb{F}_q) \geqslant (q+1)-3 = q-2$ for $i = 3, ..., r$. By Proposition 3.1.9, we have $l_i\backslash(l_\infty \cup \{Q\}) \subseteq \mathcal{X}(\mathbb{F}_q)$. Therefore,

$$\{(l_i(\mathbb{F}_q)\backslash\{Q\}) \cap Z(\mathcal{X}) \mid i = 1, ..., r\} \subseteq l_\infty.$$

□

Remark 3.1.11. *Let $Q \in Z(\mathcal{X})$. Suppose that $\check{Q}(\mathbb{F}_q) \cap \mathcal{A}_{q-1} = \{l_1, l_2, ..., l_r\}$ with $r \geqslant 2$. By Corollary 3.1.10, $\{(l_i(\mathbb{F}_q)\backslash\{Q\}) \cap Z(\mathcal{X}) \mid i = 1, 2, ..., r\} \subseteq l_\infty$ is contained in a line. Then, by Proposition 3.1.9, for any $l \in \check{Q}_0(\mathbb{F}_q)\backslash\{l_1, l_2, ..., l_r\}$, one has that*

$$\#((l\backslash l_\infty) \cap \mathcal{X}(\mathbb{F}_q)) \leqslant q - r - 1.$$

This, in turn, implies that

$$\#(l \cap \mathcal{X}(\mathbb{F}_q)) \leqslant q - r.$$

We now prove some interesting Corollaries to Proposition 3.1.9. They can be thought of as partial negative answers to Question 1 when assuming stronger conditions on the structure of $Z(\mathcal{X})$.

Corollary 3.1.12. *If $a_0 \geqslant 2$, then $a_0 = 3$.*

Proof. Let $Z^*(\mathcal{X}) := Z(\mathcal{X})\backslash(l_\infty^1 \cup l_\infty^2)$ and $Q \in l_\infty^1 \cap l_\infty^2$ where $l_\infty^1, l_\infty^2 \in \mathcal{A}_0$. Since $\#Z(\mathcal{X}) = 3q$, we have $\#Z^*(\mathcal{X}) = q - 1$. As $\#\check{Q}(\mathbb{F}_q)\backslash\{l_\infty^1, l_\infty^2\} = q - 1$ and $\deg(\mathcal{X}) = q - 1$, then each line $l \in \check{Q}(\mathbb{F}_q)\backslash\{l_\infty^1, l_\infty^2\}$ contains exactly one point of $Z^*(\mathcal{X})$. By Corollary 3.1.10, $Z^*(\mathcal{X})$ is contained in a line. Therefore, $a_0 = 3$.

□

Corollary 3.1.13. *Let $q \geqslant 8$. If $Q \in Z(\mathcal{X})$ is a point such that $r = \psi_{q-1}(Q) \geqslant 4$, then $r = q - 1$. In particular, $a_0 = 3$.*

Proof. Since $r \geqslant 4$, Remark 3.1.11 implies that

$$\begin{aligned} q^2 - 2q + 1 = (q-1)^2 &\leqslant r(q-1) + (q+1-r)(q-r) \\ &= qr - r + q^2 + q - qr - qr - r + r^2 \\ &= q^2 + q - qr + r(r-2). \end{aligned}$$

Hence $q(r-3) \leqslant r(r-2) - 1$. Since $q \geqslant 8$, we must have $r \geqslant 7$. So

$$q \leqslant \frac{r(r-2)-1}{r-3} = \frac{(r+1)(r-3)+2}{r-3} = r + 1 + \frac{2}{r-3}.$$

Since $r \leqslant q-1$, this implies that $r = q-1$. Therefore, Q is of type $(q-1)^{q-1}0^2$ and, by Corollary 3.1.12, $a_0 = 3$.

□

Corollary 3.1.14. *Let $q \geqslant 7$. If $a_0 \geqslant 1$, then $a_0 = 3$.*

Proof. By Lemma 3.1.8, $a_{q-1} \geqslant 3(q-1)$. Let $l_\infty^1 \in \mathcal{A}_0$. Since $q \geqslant 7$, if $\psi_{q-1}(Q) \leqslant 2$ for every point $Q \in l_1^\infty$ then

$$a_{q-1} \leqslant 2(q+1) < 3(q-1),$$

a contradiction. Hence, there is a point $Q \in l_\infty^1$ such that $r = \psi_{q-1}(Q) \geqslant 3$. By Remark 3.1.11, we have that

$$\begin{aligned} q^2 - 2q + 1 = (q-1)^2 &\leqslant 0 + r(q-1) + (q-r)(q-r) \\ &= qr - r + q^2 - 2qr + r^2 \\ &= q^2 - qr + r(r-1). \end{aligned}$$

Hence, $q(r-2) \leqslant r(r-1) - 1$. Since $q \geqslant 7$, we must have $r \geqslant 6$. So

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

Since $r \leqslant q-1$, this implies that $r = q-1$. Therefore, Q is of type $(q-1)^{q-1}0^2$. Then the result follows from Corollary 3.1.12.

□

Let $k_0 := \min\{i \mid a_i \neq 0\}$. By the previous Corollary, in order to prove our main result for $q \geqslant 7$, it is enough to show that $k_0 = 0$. We start by giving an upper bound for k_0.

Lemma 3.1.15. *$k_0 \leqslant q-4$.*

Proof. Suppose that $k_0 \geqslant q-3$; then Lemma 3.1.4 leads to the following linear system:

$$\begin{cases} a_{q-3} + & a_{q-2} + & a_{q-1} = q^2 + q + 1 \\ (q-3)a_{q-3} + & (q-2)a_{q-2} + & (q-1)a_{q-1} = (q+1)(q-1)^2 \\ (q-3)(q-4)a_{q-3} + & (q-2)(q-3)a_{q-2} + & (q-1)(q-2)a_{q-1} = q(q-2)(q-1)^2. \end{cases}$$

A direct computation shows that the system above implies that

$$2a_{q-3} = 3(q^2 - 3q + 2),\ a_{q-2} = -2(q^2 - 5q + 4) \text{ and } 2a_{q-1} = 3(q^2 - 3q + 4).$$

Since $q \geqslant 5$, then

$$a_{q-2} = -2(q^2 - 5q + 4) < 0,$$

a contradiction. Therefore, $k_0 \leqslant q-4$.

□

We now prove a lower bound for k_0 whenever $k_0 \neq 0$. We start with the following lemma:

Lemma 3.1.16. $\sum_{i=k_0}^{q-1}(i-k_0)(i-q+2)a_i = 3(q-1)^2 - 3k_0$. *In particular,*

$$(q-k_0-1)a_{q-1} \geqslant 3(q-1)^2 - 3k_0.$$

Proof. Let $S := \sum_{i=k_0}^{q-1}(i-k_0)(i-q+2)a_i$. First, note that

$$\begin{aligned}(i-k_0)(i-q+2) &= i(i-1) + i(3-q) + k_0(q-2-i)\\ &= i(i-1) + i(3-q) - ik_0 + k_0(q-2)\\ &= i(i-1) + i(3-q-k_0) + k_0(q-2).\end{aligned}$$

By Lemma 3.1.4, we have

$$\begin{aligned}S &= \sum_{i=k_0}^{q-1} i(i-1)a_i + (3-q-k_0)\sum_{i=k_0}^{q-1} ia_i + k_0(q-2)\sum_{i=k_0}^{q-1} a_i\\ &= q(q-2)(q-1)^2 + (3-q-k_0)(q+1)(q-1)^2 + k_0(q-2)(q^2+q+1)\\ &= 3(q-1)^2 - 3k_0.\end{aligned}$$

Moreover, if $i = q-1$ then $(i-k_0)(i-q+2) = (q-k_0-1)$ and if $k_0 \leqslant i \leqslant q-2$ then $(i-k_0)(i-q+2) \leqslant 0$. Also, by Lemma 3.1.15, $k_0 \leqslant q-4$. Hence, $3(q-1)^2 - 3k_0 \geqslant 0$. Therefore,

$$(q-k_0-1)a_{q-1} \geqslant 3(q-1)^2 - 3k_0.$$

□

Proposition 3.1.17. *Let $q \geqslant 7$. If $k_0 \neq 0$, then $k_0 \geqslant 2$.*

Proof. Suppose that $k_0 = 1$. Let $l_1 \in \mathcal{A}_1$. Also, consider $P_0 = l_1 \cap \mathcal{X}(\mathbb{F}_q)$ and

$$l_1 \cap Z(\mathcal{X}) = \{Q_1, ..., Q_q\}.$$

by Corollary 3.1.6, P_0 is of type $(q-1)^q 1^1$. If $r_i := \psi_{q-1}(Q_i)$ for $i = 1, ..., q$ then

$$r_i(q-1) + 1 \leqslant \mathrm{N}_q(\mathcal{X}) = (q-1)^2$$

Hence, $r_i \leqslant q-2$. If $r_i \geqslant 3$, then, again, by Remark 3.1.11,

$$\begin{aligned} q^2-2q+1=(q-1)^2 &\leqslant 1+r_i(q-1)+(q-r_i)(q-r_i) \\ &= 1+r_iq-r_i+q^2-2qr_i+r_i^2 \\ &= q^2+1-qr_i+r_i(r_i-1), \end{aligned}$$

hence, $q(r_i-2) \leqslant (r_i-1)r_i$. Since $q \geqslant 7$, we must have $r_i \geqslant 6$. Hence,

$$q \leqslant \frac{(r_i-1)r_i}{(r_i-2)} = \frac{(r_i+1)(r_i-2)+2}{r_i-2} = r_i+1+\frac{2}{r_i-2}.$$

This implies that $r_i \geqslant q-1$, a contradiction. Therefore $r_i \leqslant 2$ for $i=1,...,q$; hence, $a_{q-1} \leqslant q+2q=3q$. By Lemma 3.1.16, $(q-2)a_{q-1} \geqslant 3(q-1)^2-3=3q(q-2)$. So $a_{q-1}=3q$. By Lemma 3.1.16, we have

$$\sum_{i=1}^{q-1}(i-1)(i-q+2)a_i = 3q(q-2).$$

Since $(q-2)a_{q-1}=3q(q-2)$, one has that $a_2=\cdots=a_{q-3}=0$. Then, by Lemma 3.1.4, we get the following linear system:

$$\begin{cases} a_1+ \qquad\qquad a_{q-2} = q^2+q+1-3q \\ a_1+(q-2)a_{q-2} = (q+1)(q-1)^2-3q(q-1). \end{cases}$$

A direct computation shows that the system above implies that

$$(q-3)a_1 = 3(q-1) \quad \text{and} \quad (q-3)a_{q-2} = q(q^2-5q+4).$$

Note that

$$a_1 = \frac{3(q-1)}{q-3} = 3+\frac{6}{q-3}.$$

As a_1 must be an integer, then $(q-3)|6$. Since $q \geqslant 7$, this implies that $q=9$. In this case, $a_1=4$. Let $l_1 \in \mathcal{A}_1$. Suppose that $l_1 \cap \mathcal{X}(\mathbb{F}_q)=\{P_0\}$ and $l_1 \cap Z(\mathcal{X})=\{Q_1,...,Q_9\}$. Since $\psi_8(P_0)=9$ and $\psi_8(Q_j) \leqslant 2$ $(j=1,...,9)$, counting the number $a_8=27$ of 8-lines along $\{P_0,Q_1,...,Q_9\}$, we must have that $\psi_8(Q_j)=2$. Since $a_2=\cdots=a_6=0$, then the other seven lines than two 8-lines and l_1 of $\check{Q}_j(\mathbb{F}_9)$ are either a 7-line or a 1-line. Let $s=\psi_7(Q_j)$. Then

$$64=(9-1)^2=1\cdot 1+2\cdot 8+s\cdot 7+(7-s)\cdot 1=6s+24,$$

which is impossible because s must be an integer. Therefore, $k_0 \geqslant 2$.

□

If $q \geqslant 8$, by Corollary 3.1.13, it is enough to prove that there exist a point $Q \in Z(\mathcal{X})$ such that $\psi_{q-1}(Q) \geqslant 4$. We now give a lemma in case this does not happen:

Lemma 3.1.18. *Suppose that $\psi_{q-1}(Q) \leqslant 3$ for every point $Q \in Z(\mathcal{X})$:*

(i) If there exist $P_0 \in \mathcal{X}(\mathbb{F}_q)$ such that $\psi_{q-1}(P_0) = 3$, then $a_{q-1} \leqslant 3(q+1)$.

(ii) If there exist $P_0 \in \mathcal{X}(\mathbb{F}_q)$ such that $\psi_{q-1}(P_0) = 4$, then $a_{q-1} \leqslant 3(q+2)$.

Proof. For (i), by Lemma 3.1.8, P_0 is of type $(q-1)^3(q-2)^{q-2}$. Let $l \in \check{P}(\mathbb{F}_q) \cap \mathcal{A}_{q-2}$ and $Q \in l \cap Z(\mathcal{X})$. If $r_Q := \psi_{q-1}(Q) = 3$, by Proposition 3.1.9 and Corollary 3.1.10, then $l \in \mathcal{A}_{q-1}$, a contradiction. So there are at least $3(q-2)$ points in $Z(\mathcal{X})$ such that $r_Q \leqslant 2$. Therefore, $2a_{q-1} \leqslant 2(3(q-2)) + 3 \cdot 6$. Hence,

$$a_{q-1} \leqslant 3(q-2) + 9 = 3(q+1).$$

Next, we prove item (ii). Let $s = \psi_{q-2}(P)$. We have

$$\begin{aligned}(q-1)^2 &\leqslant 1 + 4(q-2) + s(q-3) + (q-3-s)(q-4)\\ &= 4q - 7 + sq - 3s + q^2 - 3q - sq - 4q + 12 + 4s\\ &= (q-1)^2 + 4 + s - q.\end{aligned}$$

This implies that $s \geqslant q-4$; hence, P is of type $(q-1)^4(q-2)^{q-4}(q-5)^1$. As in the previous case, there are at least $3(q-4)$ points in $Z(\mathcal{X})$ such that the image by ψ_{q-1} is less than or equal to 2. Therefore, $2a_{q-1} \leqslant 2(3(q-4)) + 3 \cdot 12$; in particular,

$$a_{q-1} \leqslant 3(q-4) + 18 = 3(q+2).$$

□

3.2 Characterization of Optimal Sziklai Curves of Degree $q-1$

In this section, we provide the characterization of optimal Sziklai curves of degree $q-1$. First, we deal with the cases $q = 5, 7$, as they need some *ad hoc* techniques.

Proposition 3.2.1. *If $\mathcal{X} \in C_4(\mathbb{F}_5)$ and $\mathrm{N}_5(\mathcal{X}) = 16$, then there exist $\alpha, \beta, \gamma \in \mathbb{F}_5^*$ with $\alpha + \beta + \gamma = 0$ such that $\mathcal{X} \simeq_{\mathrm{proj}} \mathcal{X}_{(\alpha,\beta,\gamma)}$ over $\mathbb{F}_5$.*

Proof. By Theorem 3.1.1, $\mathcal{X}$ is nonsingular of degree 4. By Theorem 1.1.15, $\mathcal{X}$ has genus

$$g(\mathcal{X}) = \frac{(4-1)(4-2)}{2} = 3.$$

By Lemma 3.1.15, we have $k_0 \leqslant 1$. Suppose that $k_0 = 1$. Let $l_1 \in \mathcal{A}_1$ with $l_1 \cap \mathcal{X}(\mathbb{F}_5) = \{P_0\}$. By Corollary 3.1.6, P_0 is of type $4^5 1^1$. In this case, l_1 is the tangent line to $\mathcal{X}$ at P_0. Since $\deg(\mathcal{X}) = 4$, then we have the following expression for the intersection divisor $l_1 \cdot \mathcal{X}$:

$$l_1 \cdot \mathcal{X} = \sum \mathrm{I}(P, l_1 \cap \mathcal{X})P = 2P_0 + R_1 + R_2,$$

for some points $R_1, R_2 \in l_1 \cap \mathcal{X}$. Since the divisor $l_1 \cdot \mathcal{X}$ is defined over $\mathbb{F}_5$, by applying the 5-Frobenius map Ψ_5, we have that $R_1 + R_2 + 2P_0 = \Psi_5(R_1) + \Psi_5(R_2) + 2P_0$, which implies that $R_1, R_2 \in \mathbb{P}^2(\mathbb{F}_{25})$. If $R_1 = R_2$, then $R_1 = R_2 = P_0$ and P_0 is an inflexion point; so $\mathrm{I}(P_0, l_1 \cap \mathcal{X}) = j_2(P_0) \geqslant 3$. On the other hand, by Stohr-Voloch Theorem 1.2.4, we have

$$32 = 2\mathrm{N}_q(\mathcal{X}) \leqslant 32 - \sum_{P \in \mathcal{X}} A(P).$$

So $0 = A(P_0) = j_2(P_0) - 2$, hence, $\mathrm{I}(P_0, l_1 \cap \mathcal{X}) = j_2(P_0) = 2$, a contradiction. Therefore, $R_1 \neq R_2$ and $R_1, R_2 \in \mathbb{P}^2(\mathbb{F}_{25}) \backslash \mathbb{P}^2(\mathbb{F}_5)$. Again, by Lemma 3.1.4 we are lead to the following linear system:

$$\begin{cases} a_1 + \ a_2 + \ a_3 + \ \ a_4 = 31 \\ a_1 + 2a_2 + 3a_3 + \ 4a_4 = 96 \\ \qquad 2a_2 + 6a_3 + 12a_4 = 240. \end{cases}$$

By solving the system above by standard Gaussian elimination, we get

$$a_1 = 21 - a_4, \ \ a_2 = 3(a_4 - 15) \ \ \text{and} \ \ a_3 = 55 - 3a_4.$$

Since $a_1, a_2, a_3 \geqslant 0$, then $15 \leqslant a_4 \leqslant 18$. In particular, $a_1 \geqslant 3$; in turn, this implies that

$$\mathrm{N}_{25}(\mathcal{X}) \geqslant 16 + 3 \cdot 2 = 22.$$

By Theorem 1.1.17, let $L(t) = \prod_{i=1}^{6}(1 - \omega_i t)$ be the factorization of the L-polynomial of $\mathcal{X}$ into linear factors in some finite extension of $\mathbb{Q}$. By Corollary 1.1.18, we have

$$\mathrm{N}_{q^n}(\mathcal{X}) = q^n + 1 - \sum_{i=1}^{6} \omega_i^n.$$

Since $16 = \mathrm{N}_5(\mathcal{X}) = 5 + 1 + 3 \cdot 4 - 2 = 5 + 3 \cdot 4 - 1$, by Remark 2.1.6, the curve $\mathcal{X}$ has zeta function of type $[4, 4, 2]$. This means that

$$\omega_1 + \overline{\omega_1} = -4, \ \ \omega_2 + \overline{\omega_2} = -4 \text{ and } \omega_3 + \overline{\omega_3} = -2.$$

Hence,

$$\sum_{i=1}^{6} \omega_i^2 = 36 - 2(|\omega_1|^2 + |\omega_2|^2 + |\omega_3|^2).$$

By Hasse-Weil Theorem 1.1.19, $|\omega_i|^2 = 5$. This implies that

$$22 \leqslant \mathrm{N}_{25}(\mathcal{X}) = 26 - \sum_{i=1}^{6} \omega_i^2 = 26 - (36 - 30) = 20,$$

a contradiction. Then, $k_0 = 0$.

Suppose that $a_1 \neq 0$. Let $l_0 \in \mathcal{A}_0$ and $l_1 \in \mathcal{A}_1$. By Corollary 3.1.6, we have

$$Q = l_0 \cap l_1 \in Z(\mathcal{X}).$$

If $r_Q = \psi_4(Q)$, by Lemma 3.1.5, we have $16 \leqslant 0 + 1 + 4r_Q + 3(4 - r_Q) = 13 + r_Q$, hence, $r_Q \geqslant 3$. This means that Q is of type $4^3 3^1 1^1 0^1$. On the other hand, since $\psi_4(Q) \geqslant 3$, by Proposition 3.1.9 and Corollary 3.1.10, we must have $\psi_3(Q) = 0$, a contradiction. Hence, $a_1 = 0$. By Lemma 3.1.4 we get:

$$\begin{cases} a_0 + \ a_2 + \ a_3 + \ \ a_4 = 31 \\ \quad\ 2a_2 + 3a_3 + \ 4a_4 = 96 \\ \quad\ 2a_2 + 6a_3 + 12a_4 = 240. \end{cases}$$

It is easy to see that the system above implies that

$$3a_0 = 21 - a_4, \ \ a_2 = 2(a_4 - 12) \ \ \text{and} \ \ 3a_3 = 144 - 8a_4.$$

If $a_0 = 1$, then $a_2 = 12$ and $a_3 = 0$. Let $l_2 \in \mathcal{A}_2$ and $P_0 \in l_2 \cap \mathcal{X}(\mathbb{F}_5)$. If $r = \psi_4(P_0)$, by Lemma 3.1.5, we have $16 \leqslant 2 + 3r + 2(5 - r) = 12 + r$. Since $2 + 3r \leqslant 16$, this implies that $r = 4$. Hence, $\psi_2(P_0) = 1$, $\psi_3(P_0) = 1$ and $\psi_4(P_0) = 4$, a contradiction ($a_3 = 0$). Therefore, $a_0 \geqslant 2$ and the result follows from Corollary 3.1.12.

□

Proposition 3.2.2. *If $\mathcal{X} \in C_6(\mathbb{F}_7)$ and $\mathrm{N}_7(\mathcal{X}) = 36$, then there exist $\alpha, \beta, \gamma \in \mathbb{F}_7^*$ with $\alpha + \beta + \gamma = 0$ such that $\mathcal{X} \simeq_{\mathrm{proj}} \mathcal{X}_{(\alpha,\beta,\gamma)}$ over $\mathbb{F}_7$.*

Proof. First, recall the definition of $k_0 = \min\{i \mid a_i \neq 0\}$. Note that, by Proposition 3.1.17 and Corollary 3.1.14, it is enough to prove that $k_0 \leqslant 1$.

By Lemma 3.1.3, we have that $\mathcal{X}(\mathbb{F}_7) \subseteq \mathbb{P}^2(\mathbb{F}_7)$ is a $(36, 6)$-arc. Up to projective equivalence, there are exactly 194 $(36, 6)$-arcs in $\mathbb{P}^2(\mathbb{F}_7)$, see (BOUYUKLIEV et al., 2020, Remark 1). The full list can be found online at <http://mars39.lomo.jp/opu/36_3_30.txt>, where the points of such arcs are arranged as a generator matrix for a $[36, 3, 30]_7$-code together with the weight enumerator. Recall that, by the relation between projective $[n, 3, d]_q$-codes and $(n, n - d)$-arcs in $\mathbb{P}^2(\mathbb{F}_q)$, we have

$$6 \cdot (a_0, a_1, a_2, a_3, a_4, a_5, a_6) = (c_{36}, c_{35}, c_{34}, c_{33}, c_{32}, c_{31}, c_{30}).$$

By Lemma 3.1.15, $k_0 \leqslant 3$. Hence, from our initial observation, it is enough to prove that the condition $k_0 \in \{2, 3\}$ leads to a contradiction; equivalently, the six $(36, 6)$-arcs corresponding to the $[36, 3, 30]_7$-codes such that the weight of a codeword is at most 34 are not projectively equivalent to $\mathcal{X}(\mathbb{F}_7)$.

Suppose that $k_0 = 3$. Since there is only one $[36, 3, 30]_7$-code such that the maximal weight of a codeword is exactly 33, then there is only one $(36, 6)$-arc with $k_0 = 3$, up to projective equivalence. So we can choose coordinates X, Y, Z of $\mathbb{P}^2$ such that

$$\begin{aligned}\mathcal{X}(\mathbb{F}_7) = \{&(1:1:3),(1:1:5),(1:2:3),(1:2:5),(1:2:6),(1:3:3),\\ &(1:3:4),(1:3:5),(1:3:6),(1:3:0),(1:4:2),(1:4:4),\\ &(1:4:5),(1:4:6),(1:4:0),(1:5:2),(1:5:3),(1:5:4),\\ &(1:5:6),(1:5:0),(1:6:1),(1:6:3),(1:6:4),(1:6:5),\\ &(1:6:0),(1:0:1),(1:0:2),(1:0:4),(1:0:6),(1:0:0),\\ &(0:1:3),(0:1:4),(0:1:5),(0:1:6),(0:1:0),(0:0:1)\}.\end{aligned}$$

Let

$$G = YZ(Z-3Y)(Z-4Y)(Z-5Y)(Z-6Y) \in \mathbb{F}_7[X,Y,Z]$$

$$H = X(X+Y-Z)(2X+Y-Z)(X+2Y-2Z) \in \mathbb{F}_7[X,Y,Z]$$

A direct computation shows that $\#(\mathbf{v}(G) \cap \mathbf{v}(H)) = 24 = 6 \cdot 4 = \partial(\mathbf{v}(G)) \cdot \partial(\mathbf{v}(H))$ and $\mathbf{v}(G) \cap \mathbf{v}(H) \subseteq \mathcal{X}(\mathbb{F}_7)$; more precisely, we have

$$\begin{aligned}\mathbf{v}(G) \cap \mathbf{v}(H) = \{&(1:1:3),(1:1:5),(1:2:3),(1:2:6),(1:3:4),(1:3:5),\\ &(1:3:0),(1:4:5),(1:4:6),(1:5:2),(1:5:6),(1:5:0),\\ &(1:6:1),(1:6:3),(1:6:0),(1:0:1),(1:0:2),(1:0:4),\\ &(0:1:3),(0:1:4),(0:1:5),(0:1:6),(0:1:0),(0:0:1)\}.\end{aligned}$$

Hence, by Bézout's Theorem 1.1.4, $\mathrm{I}(P, \mathbf{v}(G) \cap \mathbf{v}(H)) = 1$ for each $P \in \mathbf{v}(G) \cap \mathbf{v}(H)$. Let $F \in \mathbb{F}_7[X,Y,Z]$ be a homogeneous equation for $\mathcal{X}$ over $\mathbb{F}_7$; then, by Remark 2.2.9 and Noether's "AF + BG" Theorem 1.1.5, we can write $F = G + (\alpha_1 X^2 + \alpha_2 Y^2 + \alpha_3 Z^2 + \alpha_4 XY + \alpha_5 XZ + \alpha_6 YZ) \cdot H$ for some $\alpha_1, ..., \alpha_6 \in \mathbb{F}_7$. Since

$$\begin{aligned}0 = F(1,0,0) &= G(1,0,0) + \alpha_1 H(1,0,0)\\ &= 2\alpha_1,\\ 0 = F(1,5,4) &= G(1,5,4) + (\alpha_1 + 5^2\alpha_2 + 4^2\alpha_3 + 5\alpha_4 + 4\alpha_5 + 20\alpha_6)H(1,5,4)\\ &= 4(\alpha_1 + 4\alpha_2 + 2\alpha_3 + 5\alpha_4 + 4\alpha_5 + 6\alpha_6),\\ 0 = F(1,4,0) &= G(1,4,0) + (\alpha_1 + 4^2\alpha_2 + 4\alpha_4)H(1,4,0)\\ &= 4(\alpha_1 + 2\alpha_2 + 4\alpha_4),\\ 0 = F(1,0,6) &= G(1,0,6) + (\alpha_1 + 6^2\alpha_3 + 6\alpha_5)H(1,0,6)\\ &= 4(\alpha_1 + \alpha_3 + 6\alpha_5),\\ 0 = F(1,2,5) &= G(1,2,5) + (\alpha_1 + 2^2\alpha_2 + 5^2\alpha_3 + 2\alpha_4 + 5\alpha_5 + 10\alpha_6)H(1,2,5)\\ &= 4(\alpha_1 + 4\alpha_2 + 4\alpha_3 + 2\alpha_4 + 5\alpha_5 + 3\alpha_6),\\ 0 = F(1,6,4) &= G(1,6,4) + (\alpha_1 + 6^2\alpha_2 + 4^2\alpha_3 + 6\alpha_4 + 4\alpha_5 + 24\alpha_6)H(1,6,4)\\ &= 4(\alpha_1 + \alpha_2 + 2\alpha_3 + 6\alpha_4 + 4\alpha_5 + 3\alpha_6).\end{aligned}$$

It is easy to check that this implies that $\alpha_1 = \cdots = \alpha_6 = 0$. Therefore, $F = G$ and $\mathcal{X}$ has $\mathbb{F}_7$-linear components, a contradiction.

Now, suppose that $k_0 = 2$. Since there are five $[36, 3, 30]_7$-codes such that the maximal weight of a codeword is exactly 34, then there are five $(36, 6)$-arcs with $k_0 = 2$, up to projective equivalence. For instance, we can choose coordinates X, Y, Z of $\mathbb{P}^2$ such that

$$\begin{aligned}\mathcal{X}(\mathbb{F}_7) = \{&(1:1:4),(1:1:5),(1:1:6),(1:1:0),(1:2:2),(1:2:4),\\ &(1:2:6),(1:2:0),(1:3:2),(1:3:3),(1:3:4),(1:3:5),\\ &(1:4:2),(1:4:3),(1:4:5),(1:4:6),(1:5:3),(1:5:5),\\ &(1:5:6),(1:5:0),(1:6:1),(1:6:2),(1:6:4),(1:6:6),\\ &(1:6:0),(1:0:2),(1:0:3),(1:0:4),(1:0:5),(1:0:0),\\ &(0:1:3),(0:1:4),(0:1:5),(0:1:6),(0:1:0),(0:0:1)\}.\end{aligned}$$

Let $Q_0 = (1:5:2) \in Z(\mathcal{X})$. A direct computation shows that

$$\check{Q}_0(\mathbb{F}_7) = \{5x+z, y+z, 2x+2y+z, 4x+3y+z, 6x+4y+z, x+5y+z, 3x+6y+z, 2x+y\},$$

$$\check{Q}_0(\mathbb{F}_7) \cap \mathcal{A}_6 = \{y+z, 4x+3y+z, x+3z\} \text{ and } \check{Q}_0(\mathbb{F}_7) \cap \mathcal{A}_5 = \{x+3y+6z, x+4y\}.$$

Since $\psi_6(Q_0) = 3$, by Corollary 3.1.10 and Proposition 3.1.9, we must have $\psi_5(Q_0) = 0$, a contradiction. The other four $(36, 6)$-arcs with $k_0 = 2$ can be dealt with by using a similar argument:

(1) For

$$\begin{aligned}\mathcal{X}(\mathbb{F}_7) = \{&(1:1:3),(1:1:5),(1:1:6),(1:2:4),(1:2:5),(1:2:6),\\ &(1:2:0),(1:3:1),(1:3:2),(1:3:3),(1:3:5),(1:3:0),\\ &(1:4:2),(1:4:3),(1:4:4),(1:4:6),(1:5:2),(1:5:4),\\ &(1:5:6),(1:5:0),(1:6:3),(1:6:4),(1:6:5),(1:6:6),\\ &(1:6:0),(1:0:2),(1:0:3),(1:0:4),(1:0:5),(1:0:0),\\ &(0:1:3),(0:1:4),(0:1:5),(0:1:6),(0:1:0),(0:0:1)\}.\end{aligned}$$

Let $Q = (1:1:4)$. In this case, we have

$$\check{Q}(\mathbb{F}_7) = \{3x+z, 2x+y+z, x+2y+z, 3y+z, 6x+4y+z, 5x+5y+z, 4x+6y+z, 6x+y\},$$

$$\check{Q}(\mathbb{F}_7) \cap \mathcal{A}_6 = \{3y+z, x+3y+6z, x+5z\} \text{ and } \check{Q}(\mathbb{F}_7) \cap \mathcal{A}_5 = \{x+y+3z, x+y+z\}.$$

(2) For

$$\begin{aligned}\mathcal{X}(\mathbb{F}_7) = \{&(1:1:2),(1:1:5),(1:1:0),(1:2:2),(1:2:3),(1:2:4),\\ &(1:2:6),(1:3:2),(1:3:4),(1:3:5),(1:3:6),(1:3:0),\\ &(1:4:3),(1:4:4),(1:4:5),(1:4:6),(1:5:3),(1:5:4),\\ &(1:5:6),(1:5:0),(1:6:1),(1:6:3),(1:6:5),(1:6:6),\\ &(1:6:0),(1:0:2),(1:0:3),(1:0:4),(1:0:5),(1:0:0),\\ &(0:1:3),(0:1:4),(0:1:5),(0:1:6),(0:1:0),(0:0:1)\}.\end{aligned}$$

Let $Q=(1:1:4)$. In this case, we have

$$\check{Q}(\mathbb{F}_7) = \{3x+z, 2x+y+z, x+2y+z, 3y+z, 6x+4y+z, 5x+5y+z, 4x+6y+z, 6x+y\},$$

$$\check{Q}(\mathbb{F}_7)\cap\mathcal{A}_6 = \{x+5z, 2x+y+z, x+2y+z\} \text{ and } \check{Q}(\mathbb{F}_7)\cap\mathcal{A}_5 = \{y+5z\}.$$

(3) For

$$\begin{aligned}\mathcal{X}(\mathbb{F}_7) = \{&(1:1:2),(1:1:5),(1:1:6),(1:2:3),(1:2:4),(1:2:6),\\ &(1:2:0),(1:3:1),(1:3:4),(1:3:5),(1:3:6),(1:3:0),\\ &(1:4:2),(1:4:3),(1:4:5),(1:4:0),(1:5:2),(1:5:3),\\ &(1:5:5),(1:5:6),(1:6:2),(1:6:3),(1:6:4),(1:6:5),\\ &(1:6:0),(1:0:2),(1:0:3),(1:0:4),(1:0:6),(1:0:0),\\ &(0:1:3),(0:1:4),(0:1:5),(0:1:6),(0:1:0),(0:0:1)\}.\end{aligned}$$

Let $Q=(1:1:0)$. In this case, we have

$$\check{Q}(\mathbb{F}_7) = \{z, 6x+y+z, 5x+2y+z, 4x+3y+z, 3x+4y+z, 2x+5y+z, x+6y+z, 6x+y\},$$

$$\check{Q}(\mathbb{F}_7)\cap\mathcal{A}_6 = \{z, 4x+3y+z, 3x+4y+z\} \text{ and } \check{Q}(\mathbb{F}_7)\cap\mathcal{A}_5 = \{6x+y+z\}.$$

(4) For

$$\begin{aligned}\mathcal{X}(\mathbb{F}_7) = \{&(1:1:2),(1:1:4),(1:1:0),(1:2:2),(1:2:3),(1:2:4),\\ &(1:2:5),(1:3:3),(1:3:4),(1:3:6),(1:3:0),(1:3:2),\\ &(1:4:4),(1:4:5),(1:4:6),(1:4:0),(1:5:3),(1:5:4),\\ &(1:5:5),(1:5:6),(1:5:0),(1:6:2),(1:6:3),(1:6:5),\\ &(1:6:6),(1:0:1),(1:0:2),(1:0:3),(1:0:5),(1:0:0),\\ &(0:1:3),(0:1:4),(0:1:5),(0:1:6),(0:1:0),(0:0:1)\}.\end{aligned}$$

Let $Q=(1:1:1)$. In this case, we have

$$\check{Q}(\mathbb{F}_7) = \{6x+z, 5x+y+z, 4x+2y+z, 3x+3y+z, 2x+4y+z, x+5y+z, 6y+z, 6x+y\},$$

$$\check{Q}(\mathbb{F}_7)\cap\mathcal{A}_6 = \{6y+z, 2x+4y+z, x+3y+3z\} \text{ and } \check{Q}(\mathbb{F}_7)\cap\mathcal{A}_5 = \{x+y+5z, 4x+2y+z\}.$$

In each of these cases, $\psi_6(Q_0) = 3$. By Corollary 3.1.10 and Proposition 3.1.9, we must have $\psi_5(Q_0) = 0$, a contradiction. Therefore, none of these $(36, 6)$-arcs can be projectively equivalent to $\mathcal{X}(\mathbb{F}_7)$, and our assertion follows.

□

Remark 3.2.3. *As a byproduct of Proposition 3.2.2, we have that, of the 194 nonequivalent $(36, 6)$-arcs in $\mathbb{P}^2(\mathbb{F}_7)$, only one is obtained as the set of rational points of an irreducible plane curve of degree 6.*

We are now in a position to prove our main result.

Theorem 3.2.4. *Let $\mathcal{X} \in C_{q-1}(\mathbb{F}_q)$. If $\mathrm{N}_q(\mathcal{X}) = (q-1)^2$ and $q \geqslant 5$, then there exist $\alpha, \beta, \gamma \in \mathbb{F}_q^*$ with $\alpha + \beta + \gamma = 0$ such that $\mathcal{X} \simeq_{\mathrm{proj}} \mathcal{X}_{(\alpha,\beta,\gamma)}$ over $\mathbb{F}_q$.*

Proof. Let $k_0 = \min\{i \mid a_i \neq 0\}$. If $q \geqslant 8$, then by Proposition 3.1.17 and Corollary 3.1.13, it is enough to prove that either $k_0 \leqslant 1$ or there exists a point $Q \in Z(\mathcal{X})$ such that $\psi_{q-1}(Q) \geqslant 4$.

By way of contradiction, assume that $k_0 \geqslant 2$ and $r_Q := \psi_{q-1}(Q) \leqslant 3$ for every point $Q \in Z(\mathcal{X})$. Since $\#Z(\mathcal{X}) = 3q$, the latter hypothesis implies that $2a_{q-1} \leqslant 9q$.

Now, assume that $q \geqslant 11$. If for every point $P \in \mathcal{X}(\mathbb{F}_q)$ we have $\psi_{q-1}(P) \geqslant 5$, then $a_{q-1} \geqslant 5(q-1) > 9q/2$, a contradiction. Let $P_0 \in \mathcal{X}(\mathbb{F}_q)$ such that $r_0 = \psi_{q-1}(P) \leqslant 4$. By Lemma 3.1.8, we have that $r_0 \in \{3, 4\}$. We distinguish two cases, namely $r_0 = 3$ or $r_0 = 4$.

If $r_0 = 3$, then by Lemma 3.1.8, $a_{q-1} \leqslant 3(q+1)$. By Lemma 3.1.15, $k_0 \leqslant q-4$ and, by Lemma 3.1.16, we have

$$\frac{3(q-1)^2 - 3k_0}{q - k_0 - 1} \leqslant a_{q-1} \leqslant 3(q+1).$$

This implies that $3q(k_0 - 2) + 6 = 3(q-1)^2 - 3k_0 - (q - k_0 - 1)(3q + 3) \leqslant 0$. Therefore, $k_0 \leqslant 2 - 2/q < 2$, a contradiction.

We now suppose that $r_0 = 4$. Then, by Lemma 3.1.18, $a_{q-1} \leqslant 3(q+2)$. Since $q \geqslant 11$, there is point $P \in \mathcal{X}(\mathbb{F}_q)$ such that $\psi_{q-1}(P) = 3$, otherwise, $a_{q-1} \geqslant 4(q-1) > 3(q+2)$. Again, this implies that $k_0 < 2$, a contradiction.

We are then left with the cases $q = 5, 7, 8, 9$. As the cases $q = 5, 7$ have already been dealt with in Propositions 3.2.1 and 3.2.2, respectively, we only need to consider the cases $q = 8, 9$. We proceed with a careful case-by-case analysis.

For $q = 9$, by Lemma 3.1.16, we have

$$\frac{3(64 - k_0)}{8 - k_0} \leqslant a_8 \leqslant 40 = \left\lfloor \frac{9q}{2} \right\rfloor. \tag{3.2}$$

By Lemma 3.1.15, we have $k_0 \leqslant 5$, and then $37k_0 - 128 = 3(64 - k_0) - 40(8 - k_0) \leqslant 0$. This in turn implies $k_0 \in \{2, 3\}$.

Now, we prove that the condition $k_0 = 2$ leads to a contradiction for $q = 9$. If $k_0 = 2$, by the inequality (3.2), $a_8 \geqslant 31$. Let $l_2 \in \mathcal{A}_2$ with

$$l_2 \cap \mathcal{X}(\mathbb{F}_9) = \{P_0, P_1\} \text{ and } l_2 \cap Z(\mathcal{X}) = \{Q_2, ..., Q_9\}.$$

Let $r_j := \psi_8(P_j)$ and $r_i := \psi_8(Q_i)$ where $j = 0, 1$ and $i = 2, ..., 9$. By Lemma 3.1.5, if $j \in \{0, 1\}$, then

$$64 \leqslant 2 + 7r_j + 6(9 - r_j) = 56 + r_j.$$

Since $2 + 7r_j \leqslant 64$, this implies that $r_j = 8$ for $j = 0, 1$. If $r_i = 3$ for some $i \in \{2, ..., 9\}$, by Remark 3.1.11, the other lines in $\check{Q}_i(\mathbb{F}_q)$ contain at most 6 points of $\mathcal{X}(\mathbb{F}_9)$, hence,

$$64 \leqslant 2 + 3 \cdot 8 + 6 \cdot 6 = 62,$$

a contradiction. Then $r_i \leqslant 2$ when $i = 2, ..., 9$. This implies that $a_8 \leqslant 2 \cdot 8 + 8 \cdot 2 = 32$. If $r_P = \psi_8(P) \geqslant 4$ for every point $P \in \mathcal{X}(\mathbb{F}_q) \backslash \{P_1, P_2\}$, then

$$a_8 \geqslant \frac{8 \cdot 2 + 4((q-1)^2 - 2)}{q - 1} = 33,$$

a contradiction. Then there is a point $P \in \mathcal{X}(\mathbb{F}_q)$ such that $r_P = 3$. By Lemma 3.1.18, this implies that $a_8 \leqslant 3(q + 1) = 30$, a contradiction.

We now prove that the condition $k_0 = 3$ leads to a contradiction for $q = 9$. If $k_0 = 3$, by inequality (3.2), $a_8 \geqslant 37$. Let $l_3 \in \mathcal{A}_3$ with

$$l_3 \cap \mathcal{X}(\mathbb{F}_9) = \{P_0, P_1, P_2\} \text{ and } l_3 \cap Z(\mathcal{X}) = \{Q_3, ..., Q_9\}.$$

Let $r_j := \psi_8(P_j)$ and $r_i := \psi_8(Q_i)$ where $j = 0, 1, 2$ and $i = 3, ..., 9$. By Lemma 3.1.5, if $j \in \{0, 1, 2\}$, then

$$64 \leqslant 3 + 7r_j + 6(9 - r_j) = 57 + r_j.$$

Since $3 + 7r_j \leqslant 64$, this implies that $r_j \in \{7, 8\}$ for $j = 0, 1, 2$. If $r_i = 3$ for some $i \in \{3, ..., 9\}$, by Remark 3.1.11, the other lines in $\check{Q}_i(\mathbb{F}_q)$ contain at most 6 points of $\mathcal{X}(\mathbb{F}_9)$, hence, $64 \leqslant 3 + 3 \cdot 8 + 6 \cdot 6 = 63$, a contradiction. Then $r_i \leqslant 2$ when $i = 3, ..., 9$. This implies that $a_8 \leqslant 3 \cdot 8 + 7 \cdot 2 = 38$. If $r_P = \psi_8(P) \geqslant 5$ for every point $P \in \mathcal{X}(\mathbb{F}_q)$, then $a_8 \geqslant 5(q-1) = 40$, a contradiction. There is then a point $P \in \mathcal{X}(\mathbb{F}_q)$ such that $\psi_8(P) \leqslant 4$. By Lemma 3.1.18, this implies that $a_8 \leqslant 3(q + 2) = 33$, a contradiction.

We are then left with the case $q = 8$. In this case, by Lemma 3.1.16, we have

$$\frac{3(49 - k_0)}{7 - k_0} \leqslant a_7 \leqslant 36 = \frac{9q}{2} \tag{3.3}$$

By Lemma 3.1.15, we know that $k_0 \leqslant 4$. Then $3(11k_0 - 35) = 3(49 - k_0) - 36(7 - k_0) \leqslant 0$. Hence, $k_0 \in \{2, 3\}$.

As previously done, we prove that the condition $k_0 = 2$ leads to a contradiction. If $k_0 = 2$, by the inequality (3.3), $a_7 \geqslant 29$. Let $l_2 \in \mathcal{A}_2$ with

$$l_2 \cap \mathcal{X}(\mathbb{F}_8) = \{P_0, P_1\} \quad \text{and} \quad l_2 \cap Z(\mathcal{X}) = \{Q_2, ..., Q_8\}.$$

Let $r_j := \psi_7(P_j)$ and $r_i := \psi_7(Q_i)$ where $j = 0, 1$ and $i = 2, ..., 8$. By Lemma 3.1.5 if $j \in \{0, 1\}$, then

$$49 \leqslant 2 + 6r_j + 5(8 - r_j) = 42 + r_j.$$

Since $2 + 6r_j \leqslant 49$, then $r_j = 7$ for $j = 0, 1$. If $r_i = 3$ for some $i = 2, ..., 8$, by Remark 3.1.11, the other lines in $\check{Q}_i(\mathbb{F}_q)$ contain at most 5 points of $\mathcal{X}(\mathbb{F}_8)$. We thus obtain that $49 \leqslant 2 + 3 \cdot 7 + 5 \cdot 5 = 48$, a contradiction. Hence, $r_i \leqslant 2$ when $i = 2, ..., 8$. Therefore $a_7 \leqslant 2 \cdot 7 + 7 \cdot 2 = 28$, a contradiction.

Finally, we prove that the condition $k_0 = 3$ leads to a contradiction for $q = 8$. If $k_0 = 3$, by the inequality (3.3), $a_7 \geqslant 35$. Let $l_3 \in \mathcal{A}_3$ with

$$l_3 \cap \mathcal{X}(\mathbb{F}_8) = \{P_0, P_1, P_2\} \quad \text{and} \quad l_2 \cap Z(\mathcal{X}) = \{Q_3, ..., Q_8\}.$$

Let $r_j := \psi_7(P_j)$ and $r_i := \psi_7(Q_i)$ where $j = 0, 1, 2$ and $i = 3, ..., 8$. By Lemma 3.1.5, if $j \in \{0, 1, 2\}$ then

$$49 \leqslant 3 + 6r_j + 5(8 - r_j) = 43 + r_j.$$

Since $3 + 6r_j \leqslant (q-1)^2 = 49$, then $r_j \in \{6, 7\}$ for $i = 0, 1, 2$. If $r_i = 3$ for some $i = 2, ..., 8$, by Remark 3.1.11, the other lines in $\check{Q}_i(\mathbb{F}_q)$ contain at most 5 points of $\mathcal{X}(\mathbb{F}_8)$. So $49 \leqslant 3 + 3 \cdot 7 + 5 \cdot 5 = 49$. This means that the other 5 lines in $\check{Q}_j(\mathbb{F}_q)$ are in $\mathcal{A}_5$. By Lemma 3.1.16, we have $-2a_4 - 2a_5 + 4a_7 = 138$. This implies that $4a_7 \geqslant 138 + 2a_5 \geqslant 138 + 10 = 148$, hence $a_7 \geqslant 37$, a contradiction. So $r_j \leqslant 2$ when $j = 2, \ldots, 8$. Therefore, $a_7 \leqslant 3 \cdot 7 + 6 \cdot 2 = 33$, a contradiction.

The proof of our theorem is then completed.

□

4 Concluding Remarks

4.1 On $\mathbb{F}_q$-Frobenius classical curves with many points

Let $\mathcal{C} \subseteq \mathbb{P}^2$ be an irreducible nonsingular algebraic curve of degree d defined over $\mathbb{F}_q$. If $\mathcal{C}$ is $\mathbb{F}_q$-Frobenius classical, by Theorem 1.2.2, we have

$$\mathrm{N}_q(\mathcal{C}) \leqslant \frac{1}{2}d(d+q-1). \tag{4.1}$$

Note that if $d = q-1$ then $d(d+q-1)/2 = (q-1)^2$. This means that the Stöhr-Voloch upper bound for a nonsingular $\mathbb{F}_q$-Frobenius classical plane curve of degree $q-1$ is equal to the Sziklai upper bound. Also, by the proof of our main result, it is inferred that the curves attaining the Sziklai bound are $\mathbb{F}_q$-Frobenius classical and have no $\mathbb{F}_q$-rational point of inflection. In other words, Theorem 3.2.4 classifies the $\mathbb{F}_q$-Frobenius classical nonsingular curves of degree $q-1$ attaining the Stöhr-Voloch upper bound (4.1) up to projective equivalence.

4.2 On hypersurfaces with many rational points

A (projective) hypersurface $\mathcal{X}$ in the n-dimensional projective space $\mathbb{P}^n := \mathbb{P}^n_K$ of homogeneous equation $F(X_0, X_1, ..., X_n) = 0$, where $F \in K[X_0, X_1, ..., X_n]$, is denoted by $\mathcal{X} = \mathbf{v}(F)$ and consists of all points $(x_0 : x_1 : \cdots : x_n) \in \mathbb{P}^n$ such that $F(x_0, x_1, ..., x_n) = 0$; namely,

$$\mathcal{X} = \mathbf{v}(F) := \{(x_0 : x_1 : \cdots : x_n) \in \mathbb{P}^n \mid F(x_0, x_1, ..., x_n) = 0\}.$$

Also, the degree of $\mathcal{X}$, written $\deg(\mathcal{X})$, is $\deg(F)$. A hypersurface of degree one is called a hyperplane. When $n = 2$, a projective hypersurface is just a projective plane curve.

Definition 4.2.1. *A hypersurface $\mathcal{X} = \mathbf{v}(F)$ is said to be defined over $\mathbb{F}_q$ if there is a non-zero constant $\lambda \in K$ such that*

$$\lambda \cdot F(X_0, X_1, ..., X_n) \in \mathbb{F}_q[X_0, X_1, ..., X_n].$$

Also, the points $(x_0 : x_1 : \cdots : x_n) \in \mathbb{P}^n(\mathbb{F}_q)$ such that $F(x_0, x_1, \cdots, x_n) = 0$ are called $\mathbb{F}_q$-rational points (or simply, rational points) of $\mathcal{X}$ and $\mathcal{X}(\mathbb{F}_q)$ denotes the set of all $\mathbb{F}_q$-rational points of $\mathcal{X}$.

A component of $\mathcal{X} = \mathbf{v}(F)$ is a hypersurface $\mathbf{v}(G)$ such that G divides F. If $\mathbf{v}(G)$ is defined over $\mathbb{F}_q$, then we say that $\mathbf{v}(G)$ is an $\mathbb{F}_q$-component of $\mathcal{X}$. Also, if $\deg(\mathbf{v}(G)) = 1$, we say that $\mathbf{v}(G)$ is an $\mathbb{F}_q$-linear component of $\mathcal{X}$.

A projectivity $\varphi : \mathbb{P}^n \to \mathbb{P}^n$ is given as follows:

$$\varphi(x_0 : x_1 : \cdots : x_n) = \mathbf{u} \text{ with } \mathbf{u}^t = A \cdot (x_0 : x_1 : \cdots : x_n)^t,$$

where $A \in \mathrm{GL}(n+1, K)$. It is also called a projective transformation; the projectivities of $\mathbb{P}^n$ constitute its projective general linear group $\mathrm{PGL}(n+1, K)$. Also, the projectivities of $\mathbb{P}^n$ with $A \in \mathrm{GL}(n+1, \mathbb{F}_q)$ is denoted by $\mathrm{PGL}(n+1, q) := \mathrm{PGL}(n+1, \mathbb{F}_q) < \mathrm{PGL}(n+1, K)$.

Definition 4.2.2. *Let $\mathcal{F}$ and $\mathcal{G}$ hypersurfaces. We say that $\mathcal{F}$ and $\mathcal{G}$ are projectively equivalent over $\mathbb{F}_q$, denoted by $\mathcal{F} \simeq_{proj} \mathcal{G}$, if there is a projectivity φ with $A \in \mathrm{GL}(n+1, \mathbb{F}_q)$ such that*

$$\varphi(\mathcal{F}) = \mathcal{G}.$$

Definition 4.2.3. *A point $P = (x_0 : x_1 : \cdots : x_n)$ of $\mathcal{X}$ is singular if*

$$\frac{\partial F}{\partial X_0}(x_0, x_1, \cdots, x_n) = \frac{\partial F}{\partial X_1}(x_0, x_1, \cdots, x_n) = \cdots = \frac{\partial F}{\partial X_n}(x_0, x_1, \cdots, x_n) = 0.$$

Otherwise, P is nonsingular (or smooth) and the tangent hyperplane at P is

$$\mathbb{T}_P(\mathcal{X}) := \mathbf{v}\left(\frac{\partial F}{\partial X_0}(x_0, x_1, \cdots, x_n) \cdot X_0 + \cdots + \frac{\partial F}{\partial X_n}(x_0, x_1, \cdots, x_n) \cdot X_n\right).$$

In (HOMMA; KIM, 2017), Homma and Kim gave an upper bound for the number $\mathrm{N}_q(\mathcal{X}) := |\mathcal{X}(\mathbb{F}_q)|$ of $\mathbb{F}_q$-rational points of a nonsingular hypersurface $\mathcal{X}$ defined over $\mathbb{F}_q$ in an odd-dimensional projective space $\mathbb{P}^n$:

Theorem 4.2.4. (HOMMA; KIM, 2017, Theorem 1.1) *Let n be an odd integer at least 3. If $\mathcal{X}$ is a nonsingular hypersurface of degree $d \geqslant 2$ in $\mathbb{P}^n$ defined over $\mathbb{F}_q$. Then*

$$N_q(\mathcal{X}) \leqslant \theta_q(m)\left((d-1)q^m + 1\right), \tag{4.2}$$

where $2m = n - 1$ and $\theta_q(m) := |\mathbb{P}^m(\mathbb{F}_q)| = q^m + \cdots + q + 1$. Also, equality holds if and only if either

(i) *$d = 2$ and $\mathcal{X}$ is a nonsingular hyperbolic quadric hypersurface, that is, $\mathcal{X}$ is projectively equivalent over $\mathbb{F}_q$ to the hypersurface*

$$\sum_{i=0}^{(n-1)/2} X_{2i}X_{2i+1} = 0; \quad \textit{or}$$

(ii) *$d = \sqrt{q} + 1$, where q is square, and $\mathcal{X}$ is a nonsingular Hermitian hypersurface, that is, $\mathcal{X}$ is projectively equivalent over $\mathbb{F}_q$ to the hypersurface*

$$\sum_{i=0}^{(n-1)/2} \left(X_{2i}^{\sqrt{q}}X_{2i+1} + X_{2i}X_{2i+1}^{\sqrt{q}}\right) = 0; \quad \textit{or}$$

(iii) *$d = q + 1$ and $\mathcal{X}$ is a nonsingular $\mathbb{P}^n$-filling hypersurface over $\mathbb{F}_q$, that is, $\mathcal{X}$ is projectively equivalent over $\mathbb{F}_q$ to the hypersurface*

$$\sum_{i=0}^{(n-1)/2} (X_{2i}^q X_{2i+1} + X_{2i} X_{2i+1}^q) = 0.$$

In the same paper, they also conjectured the following for the even-dimensional case: if $\mathcal{X} \subseteq \mathbb{P}^n$ is a nonsingular hypersurface defined over $\mathbb{F}_q$ of degree d with n even, then

$$\mathrm{N}_q(\mathcal{X}) \leqslant \Theta_n^{d,q} := \theta_q \, (m-1) \, ((d-1)q^m + 1) \tag{4.3}$$

where $2m = n$.

This conjecture was then proved by Datta in the case $n = 4$:

Theorem 4.2.5. (DATTA, 2019, Theorem 4.8) *Fix a positive integer d with $2 \leqslant d \leqslant q$. Let $\mathcal{X} \subset \mathbb{P}^4$ be a nonsingular threefold of degree d defined over $\mathbb{F}_q$. If $(d, q) \neq (4, 4)$ we have,*

$$N_q(\mathcal{X}) \leqslant (d-1)q^3 + (d-1)q^2 + q + 1.$$

Moreover, the bound is attained by a nonsingular threefold $\mathcal{X}$ of degree d only if there exists a point $P \in \mathcal{X}(\mathbb{F}_q)$ such that $\mathcal{X} \cap \mathbb{T}_P(\mathcal{X})$ is a cone, with center at P, over a plane curve $\mathcal{C}$ of degree d defined over $\mathbb{F}_q$ that does not contain a line defined over $\mathbb{F}_q$ and $N_q(\mathcal{C}) = (d-1)q + 1$.

For $n \geqslant 6$, this conjecture was then proved by Tironi:

Theorem 4.2.6. (TIRONI, 2022, Theorem 2) *Let $\mathcal{X}^n \subset \mathbb{P}^{n+1}$ be a nonsingular hypersurface of degree $d \geqslant 2$ defined over $\mathbb{F}_q$ with $n \geqslant 5$ an odd integer. If $d \leqslant q$, then*

$$\mathrm{N}_q(\mathcal{X}) \leqslant \Theta_n^{d,q}.$$

Moreover, the equality is reached by a nonsingular hypersurfaces $\mathcal{X}^n \subseteq \mathbb{P}^{n+1}$ only if there exists an $\mathbb{F}_q$-point $P \in \mathcal{X}^n$ such that $\mathcal{X}^n \cap \mathbb{T}_P(\mathcal{X}^n)$ is a cone $P * \mathcal{Y}$ with vertex P over a nonsingular hypersurface $\mathcal{Y} \subset \mathbb{P}^{n-1}$ such that $N_q(\mathcal{Y}) = \Theta_{n-2}^{d,q}$.

Also, in the same paper, Tironi proof the case $d = q + 1$ for $n = 4$.

Here, a link with curves that are optimal with respect to the Sziklai bound appears when considering hypersurfaces attaining (4.3). In fact, let $\mathcal{X}$ be a hypersurface in $\mathbb{P}^4$ attaining the bound (4.3); then, by Theorem 4.2.5, there exists a point $P \in \mathcal{X}(\mathbb{F}_q)$ such that $\mathcal{X} \cap \mathbb{T}_P(\mathcal{X})$ is a cone with center P over a plane curve $\mathcal{C}$ of degree d defined over $\mathbb{F}_q$ without $\mathbb{F}_q$-linear components and $\mathrm{N}_q(\mathcal{C})$ attains the Sziklai bound. Also, by (TIRONI, 2022, Theorem 1), this curve must be nonsingular. For $n \geqslant 6$, by Theorem 4.2.6, we have an analogous result. Therefore, the extremal hypersurfaces in even dimension can be characterized inductively by starting with the ones in $\mathbb{P}^4$, which in turn can be constructed from optimal Sziklai curves. This gives a possible application of the classification of extremal Sziklai curves, and in particular, of Theorem 3.2.4.

4.3 Future Work

As mentioned earlier, a potential application of the classification of extremal Sziklai curves is the inductive characterization of extremal nonsingular hypersurfaces in even dimensions. In this final section, we will examine specific cases.

Since the characterization may be done inductively, first consider the case in $\mathbb{P}^4$: in this case, the upper bound of Theorem 4.2.5 is attained by a nonsingular threefold $\mathcal{X}$ of degree d only if there exists a point $P \in \mathcal{X}(\mathbb{F}_q)$ such that $\mathcal{X} \cap \mathbb{T}_P(\mathcal{X})$ is a cone, with center at P, over a nonsingular plane curve $\mathcal{C}$ of degree d defined over $\mathbb{F}_q$ that does not contain a line defined over $\mathbb{F}_q$ and $\mathrm{N}_q(\mathcal{C}) = (d-1)q + 1$. Hence, its degree d must belong to the set

$$\{2, \sqrt{q}+1, q-1, q, q+1\}.$$

Now, fixe $\mathcal{X} \subset \mathbb{P}^4$ be a nonsingular threefold of degree d defined over $\mathbb{F}_q$.

Definition 4.3.1. *We say that $P \in \mathcal{X}(\mathbb{F}_q)$ is of cone type over a plane curve $\mathcal{C}$ if $\mathcal{X} \cap \mathbb{T}_P(\mathcal{X})$ is a cone, with center at P, over a plane curve $\mathcal{C}$ of degree d.*

A natural question is the following:

Question 2. *To guarantee that $\mathrm{N}_q(\mathcal{X}) = (d-1)q^3 + (d-1)q^2 + q + 1$, how many points $P \in \mathcal{X}(\mathbb{F}_q)$ of cone type over a nonsingular optimal Sziklai curve $\mathcal{C}$ of degree d must there be at a minimum?*

First, we will examine the known cases. We are aware that the nonsingular quadric $\mathcal{Q} \subseteq \mathbb{P}^4$ over $\mathbb{F}_q$ and the nonsingular Hermitian $\mathcal{H} \subseteq \mathbb{P}^4$ over $\mathbb{F}_{q^2}$ attained the limit of Theorem 4.2.5. In this case, by (HIRSCHFELD; THAS, 1991, Section 1.3 and 2.2) and (TIRONI, 2022, Proposition 6), all points are of cone type over a nonsingular optimal Sziklai curve.

Now, we will determine the minimum number of points of cone type that should exist.

Proposition 4.3.2. *If $\mathrm{N}_q(\mathcal{X}) = (d-1)q^3 + (d-1)q^2 + q + 1$, then there exists at least $q+1$ point $P \in \mathcal{X}(\mathbb{F}_q)$ of cone type.*

Proof. Suppose that $\mathrm{N}_q(\mathcal{X}) = (d-1)q^3 + (d-1)q^2 + q + 1$ and that there exist a point $P \in \mathcal{X}(\mathbb{F}_q)$ not of the cone type over a nonsingular optimal Sziklai curve $\mathcal{C}$ of degree d. By (DATTA, 2019, Lemma 4.2), $|\mathcal{X}(\mathbb{F}_q) \cap \mathbb{T}_P(\mathcal{X})^C| \leqslant (d-1)q^3$. Hence,

$$|\mathcal{X}(\mathbb{F}_q) \cap \mathbb{T}_P(\mathcal{X})| \geqslant (d-1)q^2 + q + 1.$$

Let $r := \#\mathcal{L}_q(P, \mathcal{X})$, where $\mathcal{L}_q(P, \mathcal{X})$ is the set of lines defined over $\mathbb{F}_q$ satisfying $P \in l \subseteq \mathcal{X}$. By (DATTA, 2019, Lemma 4.3), we must have $r \geqslant 1$. If $l \in \check{P}(\mathbb{F}_q)\backslash\mathcal{L}_q(P, \mathcal{X})$ and $l \subseteq \mathbb{T}_P(\mathcal{X})$, then $|\mathcal{X}(\mathbb{F}_q) \cap (l\backslash\{P\})| \leqslant d-2$. So

$$\begin{aligned}(d-1)q^2 + q + 1 &\leqslant |\mathcal{X}(\mathbb{F}_q) \cap \mathbb{T}_P(\mathcal{X})| \\ &\leqslant 1 + (q^2 + q + 1 - r)(d-2) + rq \\ &= 1 + (q^2 + q + 1)(d-2) + r(q + 2 - d).\end{aligned}$$

This implies that $r \geqslant q + 1$. Now, by proof of (DATTA, 2019, Theorem 4.8), for each line $l \in \mathcal{L}_q(P, \mathcal{X})$ there exists a point of cone type over a nonsingular optimal Sziklai curve $\mathcal{C}$ of degree d. Hence, exists at least $q + 1$ point of cone type.

□

Also, the lower bound $q + 1$ cannot be improved:

Example 4.3.3. *Consider the following polynomial* $F \in \mathbb{F}_2[X_0, X_1, X_2, X_3, X_4]$*:*

$$\begin{aligned}F := X_0^2X_1 + X_0X_1^2 + X_0X_1X_2 + X_0X_2^2 + X_1X_2^2 + X_2^3 + X_0X_2X_3 + X_2^2X_3 + X_0^2X_4 + \\ + X_0X_1X_4 + X_1X_2X_4 + X_0X_3X_4 + X_2X_3X_4 + X_3^2X_4 + X_2X_4^2 + X_3X_4^2.\end{aligned}$$

Then, $\mathcal{X} = \mathbf{v}(F) \subseteq \mathbb{P}^4$ *is a nonsingular hypersurface of degree* 3 *over* $\mathbb{F}_2$ *with* $\mathrm{N}_q(\mathcal{X}) = 27 = (d-1)q^3 + (d-1)q^2 + q + 1$*. Let*

$$P_1 := (0:1:0:1:0),\ P_2 := (1:0:1:0:1),\ P_3 := (1:1:1:1:1) \in \mathcal{X}(\mathbb{F}_q).$$

We see from Magma program

```
q := 2;
d := q + 1;
F<t> := GF(q);
P4<x0,x1,x2,x3,x4> := ProjectiveSpace(F, 4);
F1 := x0^2*x1 + x0*x1^2 + x0*x1*x2 + x0*x2^2 + x1*x2^2 +
x2^3 + x0*x2*x3 + x2^2*x3 + x0^2*x4 + x0*x1*x4 + x1*x2*x4 +
x0*x3*x4 + x2*x3*x4 + x3^2*x4 + x2*x4^2 + x3*x4^2;
X := Scheme(P4,[F1]);
u := #Points(X);
PX := Points(X);
for x in [1 .. u] do
P := Points(X)[x];
Tp := TangentSpace(X,P);
S := Tp meet X;
TC := TangentCone(S,P);
```

```
16 if TC eq S then
17 P;
18 end if;
19 end for;
```

that P_i is a point of cone type over a nonsingular optimal Sziklai curve $\mathcal{C}$ of degree 3 for $i = 1, 2, 3$ and no other point of $\mathcal{X}(\mathbb{F}_q)$ satisfies this condition.

Indeed, for $d \in \{q-1, q, q+1\}$, not all $\mathbb{F}_q$-rational points of $\mathcal{X}$ are of cone type: let $P \in \mathcal{X}(\mathbb{F}_q)$ be a point of cone type, then

$$\#(l \cap \mathcal{X}(\mathbb{F}_q)) \in \{1, d, q+1\} \quad \text{for } l \in \check{P}(\mathbb{F}_q).$$

On the other hand, for a Sziklai optimal curve of degree $d \in \{q-1, q, q+1\}$ there exists a $\mathbb{F}_q$-line l such that $\#(l \cap \mathcal{X}(\mathbb{F}_q)) = d-1$. Therefore, not all $\mathbb{F}_q$-rational points of $\mathcal{X}$ are of cone type. We can see this by (HIRSCHFELD; THAS, 1980, Theorem 29), if all $\mathbb{F}_q$-rational points of $\mathcal{X}$ are of cone type, then $\mathcal{X}(\mathbb{F}_q)$ is of type $(1, d, q+1)$; hence, $\mathcal{X}(\mathbb{F}_q) \cap \mathbb{T}_P(\mathcal{X})$ is of type $(1, d, q+1)$ in $\mathbb{T}_P(\mathcal{X}) \simeq \mathbb{P}^3$, but there is no set of type $(1, d, q+1)$ in $\mathbb{P}^3(\mathbb{F}_q)$ with $(d-1)q^2 + q + 1$ $(= \#(\mathcal{X}(\mathbb{F}_q) \cap \mathbb{T}_P(\mathcal{X}))$ if $P \in \mathcal{X}(\mathbb{F}_q)$ is of cone type) points. Also, the existence of $q+1$ points is not enough for the hypersurface to be extremal:

Example 4.3.4. *Consider the following polynomial $F \in \mathbb{F}_5[X_0, X_1, X_2, X_3, X_4]$:*

$$F = X_0^4 + X_1^4 - 2X_2^4 + X_3^4 - X_4^4.$$

Then, $\mathcal{X} = \mathbf{v}(F) \subseteq \mathbb{P}^4$ is a nonsingular hypersurface of degree 4 over $\mathbb{F}_5$ with

$$\mathrm{N}_q(\mathcal{X}) = 316 < 456 = (d-1)q^3 + (d-1)q^2 + q + 1.$$

Again, by Magma program

```
1  q := 5;
2  d := q - 1;
3  F<t> := GF(q);
4  P4<x0,x1,x2,x3,x4> := ProjectiveSpace(F, 4);
5  F1 := x0^d + x1^d - 2*x2^d + x3^d - x4^d;
6  X := Scheme(P4,[F1]);
7  u := #Points(X);
8  PX := Points(X);
9  for x in [1 .. u] do
10 P := Points(X)[x];
11 Tp := TangentSpace(X,P);
12 S := Tp meet X;
```

```
TC := TangentCone(S,P);
if TC eq S then
P;
end if;
end for;
```

All points of cone type are listed below:

$$\{(1:0:0:0:1),(2:0:0:0:1),(3:0:0:0:1),(4:0:0:0:1),$$
$$(0:0:0:1:1),(0:0:0:2:1),(0:0:0:3:1),(0:0:0:4:1),$$
$$(0:1:0:0:1),(0:2:0:0:1),(0:3:0:0:1),(0:4:0:0:1)\},$$

that is, $\mathcal{X}$ is not extremal and has 12 ($> 6 = q+1$) *point of cone type.*

The last example (Example 4.3.4) contains more than $q+1$ points of cone type. However, there is a potentially important difference when compared to Example 4.3.3, which has $q+1$ aligned points of cone type (something that does not occur in Example 4.3.4). We still do not have any concrete example of the existence of these hypersurfaces, we believe that they do not exist due to the specific structure they must have for $d \in \{q-1, q, q+1\}$ with $q > 2$.

Bibliography

ARAKELIAN, N.; TAFAZOLIAN, S.; TORRES, F. On the spectrum for the genera of maximal curves over small fields. *arXiv preprint arXiv:1609.04797*, 2016. Citado 2 vezes nas páginas 12 and 25.

BIERBRAUER, J. *Introduction to coding theory*. [S.l.]: Chapman and Hall/CRC, 2016. Citado na página 23.

BOUYUKLIEV, I.; CHEON, E. J.; MARUTA, T.; OKAZAKI, T. On the (29, 5)-arcs in pg (2, 7) and some generalized arcs in pg (2, q). *Mathematics*, MDPI, v. 8, n. 3, p. 320, 2020. Citado 2 vezes nas páginas 14 and 43.

DATTA, M. Maximum number of fq-rational points on nonsingular threefolds in p4. *Finite Fields and Their Applications*, Elsevier, v. 59, p. 86–96, 2019. Citado 4 vezes nas páginas 14, 52, 53, and 54.

FULTON, W. Algebraic curves. *An Introduction to Algebraic Geom*, v. 54, 2008. Citado 3 vezes nas páginas 15, 17, and 19.

HEFEZ, A.; VOLOCH, J. F. Frobenius non classical curves. *Archiv der Mathematik*, Springer, v. 54, n. 3, p. 263–273, 1990. Citado 2 vezes nas páginas 22 and 28.

HIRSCHFELD, J. Projective geometry over finite fields. *Oxford math. Monographs*, Clarendon Press, 1979. Citado na página 34.

HIRSCHFELD, J.; STORME, L.; THAS, J.; VOLOCH, J. A characterization of hermitian curves. *Journal of Geometry*, Springer, v. 41, p. 72–78, 1991. Citado na página 30.

HIRSCHFELD, J.; THAS, J. Sets of type (1, n, q+ 1) in pg (d, q). *Proceedings of the London Mathematical Society*, Wiley Online Library, v. 3, n. 2, p. 254–278, 1980. Citado na página 55.

HIRSCHFELD, J. W. P. *Projective geometries over finite fields*. [S.l.]: Oxford University Press, 1998. Citado na página 30.

HIRSCHFELD, J. W. P.; KORCHMÁROS, G.; TORRES, F. *Algebraic curves over a finite field*. [S.l.]: Princeton University Press, 2008. v. 20. Citado 3 vezes nas páginas 15, 17, and 20.

HIRSCHFELD, J. W. P.; THAS, J. A. *General Galois Geometries*. [S.l.]: Oxford Mathematical Monographs/The Clarendon Press, Oxford University Press, 1991. Citado na página 53.

HOMMA, M. On maximal plane curves of degree 3 over $\mathbb{F}_4$, and sziklai's example of degree $q-1$ over $\mathbb{F}_q$. *Journal of Algebra Combinatorics Discrete Structures and Applications*, p. 127–138, 2024. Citado 3 vezes nas páginas 13, 31, and 33.

HOMMA, M.; KIM, S. J. Around sziklai's conjecture on the number of points of a plane curve over a finite field. *Finite Fields and Their Applications*, Elsevier, v. 15, n. 4, p. 468–474, 2009. Citado 4 vezes nas páginas 12, 13, 27, and 28.

_____. Sziklai's conjecture on the number of points of a plane curve over a finite field iii. *Finite Fields and Their Applications*, Elsevier, v. 16, n. 5, p. 315–319, 2010. Citado 3 vezes nas páginas 13, 27, and 29.

_____. Sziklai's conjecture on the number of points of a plane curve over a finite field ii. *Finite Fields: Theory and Applications, in: Contemp. Math*, v. 518, p. 225–234, 2010. Citado 5 vezes nas páginas 13, 27, 28, 29, and 30.

_____. Toward determination of optimal plane curves with a fixed degree over a finite field. *Finite Fields and Their Applications*, Elsevier, v. 17, n. 3, p. 240–253, 2011. Citado na página 30.

_____. The uniqueness of a plane curve of degree q attaining sziklai's bound over fq. *Finite Fields and Their Applications*, Elsevier, v. 18, n. 3, p. 567–580, 2012. Citado 2 vezes nas páginas 29 and 30.

_____. Nonsingular plane filling curves of minimum degree over a finite field and their automorphism groups: Supplements to a work of tallini. *Linear Algebra and its Applications*, Elsevier, v. 438, n. 3, p. 969–985, 2013. Citado na página 30.

_____. Number of points of a nonsingular hypersurface in an odd-dimensional projective space. *Finite Fields and Their Applications*, Elsevier, v. 48, p. 395–419, 2017. Citado na página 51.

LAUTER, K.; SERRE, J.-P. The maximum or minimum number of rational points on genus three curves over finite fields. *Compositio Mathematica*, London Mathematical Society, v. 134, n. 1, p. 87–111, 2002. Citado 2 vezes nas páginas 14 and 26.

SEGRE, B. Le geometrie di galois. *Annali di Matematica pura ed applicata*, Springer, v. 48, p. 1–96, 1959. Citado na página 27.

SERRE, J.-P.; HOWE, E. W.; OESTERLE, J.; RITZENTHALER, C. *Rational points on curves over finite fields*. [S.l.]: Société mathématique de France, 2020. Citado 2 vezes nas páginas 25 and 26.

STICHTENOTH, H. *Algebraic function fields and codes*. [S.l.]: Springer Science & Business Media, 2009. v. 254. Citado 4 vezes nas páginas 19, 20, 21, and 25.

STÖHR, K.-O.; VOLOCH, J. F. Weierstrass points and curves over finite fields. *Proceedings of the London Mathematical Society*, Oxford Academic, v. 3, n. 1, p. 1–19, 1986. Citado 2 vezes nas páginas 22 and 23.

SZIKLAI, P. A bound on the number of points of a plane curve. *Finite Fields and Their Applications*, Elsevier, v. 14, n. 1, p. 41–43, 2008. Citado 3 vezes nas páginas 12, 27, and 31.

TALLINI, G. Sulle ipersuperficie irriducibili d'ordine minimo che contengono tutti i punti di uno spazio di galois sr, q. *Rend. Mat. e Appl.(5)*, v. 20, p. 431–479, 1961. Citado na página 30.

TIRONI, A. L. On a homma–kim conjecture for nonsingular hypersurfaces. *Annali di Matematica Pura ed Applicata (1923-)*, Springer, v. 201, n. 2, p. 617–635, 2022. Citado 3 vezes nas páginas 14, 52, and 53.