UNIVERSIDADE DE SÃO PAULO

Instituto de Ciências Matemáticas e de Computação

Three topics in algebraic curves over finite fields

Mariana de Almeida Nery Coutinho

Tese de Doutorado do Programa de Pós-Graduação em
Matemática (PPG-Mat)

SERVIÇO DE PÓS-GRADUAÇÃO DO ICMC-USP

Data de Depósito:

Assinatura: _____

Mariana de Almeida Nery Coutinho

Three topics in algebraic curves over finite fields

Doctoral dissertation submitted to the Institute of Mathematics and Computer Sciences – ICMC-USP, in partial fulfillment of the requirements for the degree of the Doctorate Program in Mathematics. *FINAL VERSION*

Concentration Area: Mathematics

Advisor: Prof. Dr. Herivelto Martins Borges Filho

USP – São Carlos
May 2019

Ficha catalográfica elaborada pela Biblioteca Prof. Achille Bassi
e Seção Técnica de Informática, ICMC/USP,
com os dados inseridos pelo(a) autor(a)

C871t Coutinho, Mariana de Almeida Nery
Three topics in algebraic curves over finite
fields / Mariana de Almeida Nery Coutinho;
orientador Herivelto Martins Borges Filho. -- São
Carlos, 2019.
150 p.

Tese (Doutorado - Programa de Pós-Graduação em
Matemática) -- Instituto de Ciências Matemáticas e
de Computação, Universidade de São Paulo, 2019.

1. Plane and space curves. 2. Curves over finite
fields. 3. Rational points. 4. Zeta functions. 5.
Automorphisms. I. Borges Filho, Herivelto Martins,
orient. II. Título.

Mariana de Almeida Nery Coutinho

Três tópicos em curvas algébricas sobre corpos finitos

Tese apresentada ao Instituto de Ciências Matemáticas e de Computação – ICMC-USP, como parte dos requisitos para obtenção do título de Doutora em Ciências – Matemática. *VERSÃO REVISADA*

Área de Concentração: Matemática

Orientador: Prof. Dr. Herivelto Martins Borges Filho

USP – São Carlos
Maio de 2019

Para Luciana, Marcelo e Marcelinho.

ACKNOWLEDGEMENTS

O verbete gratidão é proveniente da palavra latina *gratia*, a qual significa graça, ou da palavra *gratus*, que traduz-se como agradável. Por extensão, gratidão é o reconhecimento agradável por tudo quanto se recebe ou se lhe é concedido. Assim, nessa parte agradeço (isto é, manifesto a minha gratidão) a todos que contribuíram, direta ou indiretamente, para que esse trabalho pudesse ser escrito.

Ao professor Herivelto, pelo imenso apoio, paciência e atenção ao longo dos últimos quatro anos; pelo exemplo de pessoa, professor e orientador; pelo entusiasmo que sempre colocou em cada explicação e questão a ser analisada; mas, especialmente, por ter me mostrado a importância de se fazer perguntas e de não se ter medo de errar.

A cada um dos professores do ICMC com os quais tive a oportunidade conviver. Em especial, agradeço ao professor Sérgio Monari, pelo acolhimento em todos esses anos, e ao professor Daniel Levcovitz, por ter me aceitado como aluna tantas vezes e pela enorme ajuda.

Aos professores Abramo Hefez, Daniel Levcovitz (novamente) e Fernando Torres, pela participação na banca que examinou esse trabalho, bem como por cada uma das sugestões e comentários que contribuíram para a melhoria desse texto.

À equipe da cantina do ICMC, pela alegria com que sempre me recebeu.

Aos amigos da minha turma de doutorado, Alex (Francisco e Silva), Angelina, Camila, Carol, Jean, Liliam e Pedro, que de diversas formas muito especiais marcaram essa trajetória.

Aos amigos “INCA” (Interessados Nas Curvas Algébricas), Alex, Cirilo, Grégory, Lucas, Nazar, Pietro e Roberto, por todo apoio e tudo que me ensinaram.

Aos amigos do ICMC que não se enquadram nos dois grupos acima, Cesar, Eduardo, Hellen, Jackson, Marielle, Pryscilla, Renan e Wilker.

Aos professores do Departamento de Matemática da UFJF. Em especial agradeço à professora e orientadora Beatriz Motta pelo imenso incentivo para que eu pudesse iniciar o doutorado, bem como pela presença e apoio nesses últimos quatro anos.

Aos professores do Departamento de Física da UFJF. Em especial agradeço ao professor Maikel Ballester pela enorme contribuição para a minha formação acadêmica e pessoal enquanto sua aluna de iniciação científica.

Aos amigos da UFJF, Adriele, Janaina, Leandro, Sandra e Santiago, que mesmo com a distância sempre estiveram ao meu lado.

Ao amigo Eli Vilela, pelas conversas sobre Matemática, violão, piano e diversos outros assuntos.

À minha família (na mais ampla acepção desse termo), simplesmente por *tudo*.

Aos amigos da FEAK, pelo imenso carinho.

Às minhas amigas de infância, por todos os momentos especiais.

Ao amigo Bruno Marques, pelo apoio incondicional.

A cada um dos motoristas de ônibus que com o seu trabalho permitiram que a distância entre Juiz de Fora e São Carlos ficasse um pouco menor.

À Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – (Brasil) CAPES – Código de Financiamento 001, e ao CNPq – Processo 154359/2016-5, pela bolsa de doutorado.

“A ciência é neta da curiosidade e filha do estudo.”
(Emmanuel)

ABSTRACT

COUTINHO, M. A. N. **Three topics in algebraic curves over finite fields.** 2019. 150 p. Tese (Doutorado em Ciências – Matemática) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2019.

Inserted in the context of algebraic curves defined over finite fields, the present thesis addresses the study of the following three topics: plane sections of Fermat surfaces over finite fields; bounds for the number of $\mathbb{F}_q$ -rational points on $aX^dY^d - X^d - Y^d + b = 0$ and the number of chords of an affinely regular polygon inscribed in a hyperbola passing through a given point; the number of $\mathbb{F}_{q^n}$ -rational points, the L-polynomial and the automorphism group of the generalized Suzuki curve.

Keywords: Plane and space curves, Curves over finite fields, Rational points, Zeta functions, Automorphisms.

RESUMO

COUTINHO, M. A. N. **Três tópicos em curvas algébricas sobre corpos finitos.** 2019. 150 p. Tese (Doutorado em Ciências – Matemática) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2019.

Inserida no contexto das curvas algébricas definidas sobre corpos finitos, a presente tese aborda o estudo dos seguintes três tópicos: seções planas das superfícies de Fermat sobre corpos finitos; cotas para o número de pontos $\mathbb{F}_q$ -racionais em $aX^dY^d - X^d - Y^d + b = 0$ e o número de cordas passando por um determinado ponto de um polígono afinamente regular inscrito em uma hipérbole; o número de pontos $\mathbb{F}_{q^n}$ -racionais, o L-polinômio e o grupo automorfismos da curva de Suzuki generalizada.

Palavras-chave: Curvas planas e espaciais, Curvas sobre corpos finitos, Pontos racionais, Funções zeta, Automorfismos.

LIST OF FIGURES

Figure 1 – A comparison with the Hasse-Weil bound	119
---	-----

LIST OF TABLES

Table 1	– The number of $\mathbb{F}_q$ -rational points on $\mathcal{C}$ with $i \in \{1, 2\}$ zero coordinates.	90
Table 2	– The number $N_{(1)} + N_{(2)} + N_{(3)}$	92
Table 3	– Linear components of $\mathcal{C}$ for $e_0 e_1 e_2 \neq 0$	95
Table 4	– Curve $\mathcal{F}$ for d odd.	101
Table 5	– Curve $\mathcal{F}$ for d even.	101
Table 6	– $\mathbb{F}_q$ -points with zero coordinates on $\mathcal{C}$ for d odd	103
Table 7	– $\mathbb{F}_q$ -points with zero coordinates on $\mathcal{C}$ for d even	103

CONTENTS

INTRODUCTION	23
I FOUNDATIONS	25
1 PROJECTIVE ALGEBRAIC CURVES	27
1.1 Plane curves	27
1.1.1 <i>First definitions</i>	27
1.1.2 <i>Branches of plane curves</i>	30
1.1.2.1 <i>Branch representations and branches</i>	30
1.1.2.2 <i>Order and tangent of branch representations and branches</i>	32
1.1.2.3 <i>Intersection multiplicity</i>	33
1.1.3 <i>Function fields of irreducible plane curves</i>	34
1.2 Algebraic function fields	35
1.2.1 <i>Plane models</i>	36
1.2.2 <i>Places</i>	36
1.2.3 <i>Some remarks</i>	37
1.2.4 <i>Expansion of a function at a local parameter</i>	38
1.2.5 <i>Separating variables</i>	39
1.2.6 <i>Derivatives</i>	39
1.2.7 <i>Hasse derivatives</i>	41
1.2.8 <i>Differentials and the notion of genus</i>	42
1.2.9 <i>Divisors and linear series</i>	44
1.2.10 <i>Linear systems of plane curves</i>	46
1.3 Space curves	47
1.3.1 <i>Rational transformations and morphisms</i>	50
1.3.2 <i>Some remarks</i>	52
1.3.3 <i>Morphisms $\times$ linear series</i>	53
1.3.3.1 <i>Morphisms from linear series</i>	53
1.3.3.2 <i>Linear series from morphisms</i>	55
2 PROJECTIVE ALGEBRAIC CURVES DEFINED OVER FINITE FIELDS	57
2.1 Plane curves defined over $\mathbb{F}_q$	57

2.2	$\mathbb{F}_q$ -rational branches of plane curves	58
2.3	$\mathbb{F}_q$ -rational function fields and $\mathbb{F}_q$ -rational places	59
2.3.1	<i>Some remarks</i>	60
2.4	$\mathbb{F}_q$ -rational divisors and linear series	60
2.5	Space curves defined over $\mathbb{F}_q$	61
2.5.1	<i>Rational transformations and morphisms defined over $\mathbb{F}_q$</i>	62
2.5.2	<i>Nonsingular models defined over $\mathbb{F}_q$</i>	62
2.6	The Zeta function of a curve defined over $\mathbb{F}_q$	62
2.7	The Hasse-Weil theorem and maximal curves	65
3	THE STÖHR-VOLOCH THEORY	67
3.1	Morphisms and Weierstrass points	67
3.1.1	<i>Hermitian invariants and osculating spaces</i>	68
3.1.2	<i>Order sequence and ramification divisor</i>	69
3.2	The Stöhr-Voloch theorem	73
II	THREE TOPICS IN ALGEBRAIC CURVES OVER FI- NITE FIELDS	79
4	PLANE SECTIONS OF FERMAT SURFACES OVER FINITE FIELDS	81
4.1	Introduction	81
4.2	Notation	82
4.3	Rudiments of the Stöhr-Voloch theory	83
4.4	Points and linear components of curve $\mathcal{C}$	89
4.4.1	<i>Points with zero coordinates</i>	89
4.4.2	<i>Points without zero coordinates</i>	90
4.4.3	<i>Linear components</i>	92
4.5	Preliminary result	95
4.6	Main result	98
4.6.1	<i>Frobenius classicality and absolute irreducibility</i>	98
4.6.2	<i>Proof of Theorem 4.1.1</i>	100
5	ON SOME GENERALIZED FERMAT CURVES AND CHORDS OF AN AFFINELY REGULAR POLYGON INSCRIBED IN A HYPER- BOLA	105
5.1	Introduction	105
5.2	Notation	106
5.3	The curve $\mathcal{F}$	107
5.3.1	<i>The case $q = p$</i>	110
5.3.1.1	<i>Preliminaries</i>	110

5.3.1.2	<i>The proof of Theorem 5.3.4</i>	114
5.4	Affinely regular polygons	116
5.4.1	<i>A brief introduction to affinely regular polygons</i>	116
5.4.2	<i>Number of chords of an affinely regular polygon inscribed in a hyperbola passing through a given point</i>	118
6	ON THE ZETA FUNCTION AND THE AUTOMORPHISM GROUP OF THE GENERALIZED SUZUKI CURVE	121
6.1	Introduction	121
6.2	Notation	124
6.3	Preliminaries	125
6.3.1	<i>L-polynomials and supersingular curves</i>	125
6.3.2	<i>Elementary abelian p-extensions of algebraic function fields</i>	126
6.3.3	<i>On the number of $\mathbb{F}_{q^n}$-rational points of $Y^p - Y = XR(X)$</i>	127
6.3.4	<i>The curve $\mathcal{G}_{\mathcal{F}}$</i>	129
6.3.5	<i>Automorphism group</i>	130
6.4	Proof of Theorem 6.1.1	131
6.5	Proof of Theorem 6.1.2	136
6.5.1	<i>Proof</i>	136
6.6	Examples	139
6.6.1	<i>The L-polynomial of $\mathcal{K}_{\mathcal{G}_{\mathcal{F}}}$ for $p = 3$</i>	139
6.6.2	<i>The L-polynomial of $\mathcal{K}_{\mathcal{G}_{\mathcal{F}}}$ for $p = 5$</i>	140
6.6.3	<i>The L-polynomial of $\mathcal{K}_{\mathcal{G}_{\mathcal{F}}}$ for $p = 7$</i>	140
6.6.4	<i>The L-polynomial of $\mathcal{K}_{\mathcal{G}_{\mathcal{F}}}$ for $p = 11$</i>	140
6.6.5	<i>The L-polynomial of $\mathcal{K}_{\mathcal{G}_{\mathcal{F}}}$ for $p = 13$</i>	141
6.6.6	<i>The L-polynomial of $\mathcal{K}_{\mathcal{G}_{\mathcal{F}}}$ for $p = 17$</i>	141
6.6.7	<i>The L-polynomial of $\mathcal{K}_{\mathcal{G}_{\mathcal{F}}}$ for $p = 19$</i>	142
6.7	Proof of Theorem 6.1.3	142
6.8	Final remarks	144
	BIBLIOGRAPHY	145

INTRODUCTION

The theory of algebraic curves, or the theory of algebraic function fields in one variable, which is the field-theoretic counterpart of algebraic curves, is the result of the efforts of several mathematicians over the past centuries. A more precise formulation (over the complex field) dates back to the nineteenth century, with the works of R. Dedekind, H. M. Weber, K. Hensel and G. Landsberg, and from a geometric point of view, with the works of Max Noether, A. Clebsch and P. Gordan (see (CHEVALLEY, 1951, Introduction)).

In the first half of the twentieth century, further development on the theory of algebraic curves was provided by the works of E. Artin, H. Hasse, F. K. Schmidt and A. Weil, where fields other than the complex were also taken into account. This fact led, among other aspects, to the emergence of the theory of algebraic curves defined over finite fields, which appears in the intersection of important areas of mathematics, such as finite geometry, coding theory, cryptography and number theory, being nowadays a broad issue of study and research.

Divided into two parts, each one containing three chapters, this thesis is inserted in the context of algebraic curves defined over finite fields.

Part I establishes the theoretical basis for the study of algebraic curves, as well as the fundamental tools and terminology used in the second part. Presenting the topics as commonly found in textbooks, however without providing the proofs, this part was drawn up considering its use for a consultation on the subjects and the connections between them, and was not therefore elaborated aiming at a linear reading of the text. Chapters 1 and 2 are based essentially on (HIRSCHFELD; KORCHMÁROS; TORRES, 2008). Chapter 1 describes the theory of projective algebraic curves in arbitrary characteristic. There, a comparison between the concept of place as constructed in (SEIDENBERG, 1968) and (HIRSCHFELD; KORCHMÁROS; TORRES, 2008) and that which is usually considered in the literature (see (GOLDSCHMIDT, 2003) and (STICHTENOTH, 2009) for instance) is made. Chapter 2 gives an introduction to the projective algebraic curves defined over finite fields, ending with the definition of the Zeta function and with the remarkable Hasse-Weil theorem. Finally, Chapter 3 collects the main elements of the Stöhr-Voloch theory, which is the basis of two of the three chapters in the second part. It is worth pointing out that, although the issue *automorphism group of projective curves* is important for the development of Chapter 6, this topic is not presented in this first part of the thesis, being only addressed in the referred chapter.

Part II is the heart of this work. In it, three independent topics, although related in their essence to the study of the number of rational points on curves defined over finite fields,

are considered. The order chosen to present the subjects follows the chronological order of development of them.

In Chapter 4, all curves defined over $\mathbb{F}_q$ arising from a plane section

$$P : X_3 - e_0X_0 - e_1X_1 - e_2X_2 = 0$$

of the Fermat surface

$$S : X_0^d + X_1^d + X_2^d + X_3^d = 0,$$

where $q = p^m = 2d + 1$ is a prime power, $p > 3$, and $e_0, e_1, e_2 \in \mathbb{F}_q$, are characterized. In particular, it is proved that any nonlinear component $\mathcal{F} \subseteq P \cap S$ is a nonsingular classical curve of degree $d \leq d$ attaining the Stöhr-Voloch bound

$$\#\mathcal{F}(\mathbb{F}_q) \leq \frac{1}{2}d(d+q-1) - \frac{1}{2}i(d-2),$$

with $i \in \{0, 1, 2, 3, d, 3d\}$.

Now, let $\mathcal{F}$ be the projective plane curve defined over $\mathbb{F}_q$, with affine equation given by

$$aX^dY^d - X^d - Y^d + b = 0,$$

where $q = p^m$ is a prime power and $ab \notin \{0, 1\}$. Considering for each $s \in \{2, \dots, d-1\}$ the base-point-free linear series $\mathcal{D}_s^{P_1, P_2}$ cut out on $\mathcal{F}$ by the linear system of all curves of degree s passing through the singular points $P_1 = (1 : 0 : 0)$ and $P_2 = (0 : 1 : 0)$ of $\mathcal{F}$, Chapter 5 determines an upper bound for the number $N_q(\mathcal{X})$ of $\mathbb{F}_q$ -rational points on the nonsingular model $\mathcal{X}$ of $\mathcal{F}$ defined over $\mathbb{F}_q$ in cases where $\mathcal{D}_s^{P_1, P_2}$ is $\mathbb{F}_q$ -Frobenius classical. As a consequence, when $\mathbb{F}_q$ is the prime field $\mathbb{F}_p$, the bound obtained for $N_q(\mathcal{X})$ improves in several cases the known bounds for the number of chords of an affinely regular polygon inscribed in a hyperbola passing through a given point distinct from its vertices.

Last (but not least), for p an odd prime number, $q_0 = p^t$ and $q = p^m = p^{2t-1}$, Chapter 6 studies the nonsingular model defined over $\mathbb{F}_q$ of

$$Y^q - Y = X^{q_0}(X^q - X)$$

from the point of view of its number of $\mathbb{F}_{q^n}$ -rational points and automorphism group. As a consequence, a description of the L-polynomial of this curve is provided.

Part I

Foundations

PROJECTIVE ALGEBRAIC CURVES

The purpose of this chapter is to present some background on the subject *projective algebraic curves*. Based on (FULTON, 2008, Chapters 3, 5, 7 and Appendix A), (GOLDSCHMIDT, 2003, Chapters 1 and 2), (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Chapters 1, 2, 4, 5, 6 and 7), (SEIDENBERG, 1968, Chapters 12, 13, 14, 16, 19 and 20), (STICHTENOTH, 2009, Chapters 1, 3 and 4) and (TORRES, 2000, Sections 1 and 2), the main concepts to develop the second part of this work are here collected. The way chosen to organize the topics does not follow in several circumstances the natural order required to prove the results, which are only stated. Also, in many cases, the objects introduced in the text are assumed to be well defined without proofs or other comments in this direction.

Throughout this chapter, $\mathbb{K}$ denotes a fixed algebraically closed field of characteristic $p \geq 0$.

1.1 Plane curves

1.1.1 First definitions

Definition 1.1.1. We define $\sim$ as the following equivalence relation on the set of nonzero homogeneous polynomials in $\mathbb{K}[X, Y, Z]$:

$$F(X, Y, Z) \sim G(X, Y, Z) \Leftrightarrow \text{There exists } \lambda \in \mathbb{K}^* \text{ such that } F(X, Y, Z) = \lambda G(X, Y, Z).$$

Definition 1.1.2. Let $F(X, Y, Z) \in \mathbb{K}[X, Y, Z]$ be a nonzero homogeneous polynomial of degree $d \geq 1$.

1. The *projective plane algebraic curve* in $\mathbb{P}^2(\mathbb{K})$

$$\mathcal{F} : F(X, Y, Z) = 0,$$

sometimes denoted only by $\mathcal{F}$, is the equivalence class of $F(X, Y, Z)$ with respect to $\sim$.

2. The *degree* of $\mathcal{F}$ is the positive integer d .
3. If $F(X, Y, Z) = \prod_{i=1}^k G_i(X, Y, Z)^{l_i}$, with $G_i(X, Y, Z)$ irreducible over $\mathbb{K}$, then each $\mathcal{G}_i : G_i(X, Y, Z) = 0$ is called a *component* of $\mathcal{F}$ and l_i is its *multiplicity*. Also, $\mathcal{F}$ is *irreducible* if $F(X, Y, Z)$ is an irreducible polynomial over $\mathbb{K}$. Otherwise, $\mathcal{F}$ is called *reducible*.
4. The point set of $\mathcal{F}$, here also denoted by $\mathcal{F}$, is the set

$$\left\{ (\alpha : \beta : \gamma) \in \mathbb{P}^2(\mathbb{K}) : F(\alpha, \beta, \gamma) = 0 \right\}.$$

Notation 1.1.3. Hereafter, the expression *plane curve* means a projective plane algebraic curve in $\mathbb{P}^2(\mathbb{K})$.

Remark 1.1.4. In some cases, a plane curve $\mathcal{F}$ is denoted in *affine coordinates* by

$$\mathcal{F} : F(X, Y) = 0,$$

where $F(X, Y) \in \mathbb{K}[X, Y]$ is a polynomial of degree $d \geq 1$. In this case,

$$\mathcal{F} : F^*(X, Y, Z) = 0$$

and the point set of $\mathcal{F}$ is described as follows:

$$\begin{aligned} \mathcal{F} &= \left\{ (\alpha : \beta : \gamma) \in \mathbb{P}^2(\mathbb{K}) : F^*(\alpha, \beta, \gamma) = 0 \right\} \\ &= \left\{ (\alpha : \beta : 1) \in \mathbb{P}^2(\mathbb{K}) : F(\alpha, \beta) = 0 \right\} \cup \left\{ (\alpha : \beta : 0) \in \mathbb{P}^2(\mathbb{K}) : F^*(\alpha, \beta, 0) = 0 \right\}, \end{aligned}$$

where

$$\left\{ (\alpha : \beta : 1) \in \mathbb{P}^2(\mathbb{K}) : F(\alpha, \beta) = 0 \right\}$$

is the set of *affine points* of $\mathcal{F}$ and

$$\left\{ (\alpha : \beta : 0) \in \mathbb{P}^2(\mathbb{K}) : F^*(\alpha, \beta, 0) = 0 \right\}$$

is the set of *points at infinity* of $\mathcal{F}$. Here, d is also the degree of $\mathcal{F}$, and $\mathcal{F}$ is irreducible if and only if $F(X, Y)$ (or equivalently $F^*(X, Y, Z)$) is irreducible.

Definition 1.1.5. A plane curve is called a *line* or a *conic* if its degree is equal to 1 or 2, respectively.

Definition 1.1.6. Let $\mathcal{F} : F(X, Y, Z) = 0$ be a plane curve.

1. A *singular point* of $\mathcal{F}$ is a point $P \in \mathcal{F}$ such that

$$\left. \frac{\partial F}{\partial X} \right|_P = \left. \frac{\partial F}{\partial Y} \right|_P = \left. \frac{\partial F}{\partial Z} \right|_P = 0.$$

Otherwise, P is called a *nonsingular point* of $\mathcal{F}$.

2. If P is a nonsingular point of $\mathcal{F}$, then the *tangent line* to $\mathcal{F}$ at P is given by

$$\mathcal{T}_P : \left. \frac{\partial F}{\partial X} \right|_P X + \left. \frac{\partial F}{\partial Y} \right|_P Y + \left. \frac{\partial F}{\partial Z} \right|_P Z = 0.$$

3. If all the points of $\mathcal{F}$ are nonsingular, then $\mathcal{F}$ is a *nonsingular plane curve*. Otherwise, $\mathcal{F}$ is called a *singular plane curve*.

The following two properties, that are well established in the literature, relate the nonsingularity of a plane curve and its irreducibility.

Proposition 1.1.7. Let $\mathcal{F}$ be a plane curve. If $\mathcal{F}$ is nonsingular, then $\mathcal{F}$ is also irreducible.

Proposition 1.1.8. Let $\mathcal{F}$ be an irreducible plane curve. Then $\mathcal{F}$ has a finite number of singular points.

Remark 1.1.9. Let $\mathcal{F} : F(X, Y) = 0$ be a plane curve of degree d . For each $P = (\alpha : \beta : 1) \in \mathbb{P}^2(\mathbb{K})$, write

$$F(X + \alpha, Y + \beta) = F_m(X, Y) + F_{m+1}(X, Y) + \cdots + F_d(X, Y),$$

where $F_i(X, Y) \in \mathbb{K}[X, Y]$ is a homogeneous polynomial of degree i , for $i = m, m+1, \dots, d$, and $F_m(X, Y) \neq 0$. Also, for $m \geq 1$, $F_m(X, Y)$ may be written as

$$F_m(X, Y) = \prod L_k(X, Y)^{l_k},$$

where the $L_k(X, Y)$ are distinct homogeneous polynomials of degree 1. From this, it follows that P lies on $\mathcal{F}$ if and only if $m > 0$. Further, P is a nonsingular point of $\mathcal{F}$ if and only if $m = 1$, and in this case

$$\mathcal{T}_P : F_1(X - \alpha, Y - \beta) = 0.$$

Definition 1.1.10. Consider the notation as in Remark 1.1.9. Then, $m_P := m$ is the *multiplicity* of $\mathcal{F}$ at P . Further:

1. For $m_P \geq 1$, the $\mathcal{T}_k : L_k(X - \alpha, Y - \beta) = 0$ are the *tangent lines* to $\mathcal{F}$ at P .
2. For $m_P \geq 2$, P is called an *ordinary singular point* of $\mathcal{F}$ if $\mathcal{F}$ has m_P distinct tangent lines at P .

Remark 1.1.11. Suppose that the plane curve $\mathcal{F}$ is given by the equation $F(X, Y, Z) = 0$ and let $P = (\alpha : \beta : \gamma) \in \mathbb{P}^2(\mathbb{K})$. In order to define the multiplicity of $\mathcal{F}$ at P , one may proceed as in Remark 1.1.9 by considering the curve $\mathcal{F}$ given in affine coordinates by $F(X, Y, 1) = 0$, $F(X, 1, Z) = 0$ or $F(1, Y, Z) = 0$ according to whether γ , β or α are different from zero, respectively.

1.1.2 Branches of plane curves

1.1.2.1 Branch representations and branches

Definition 1.1.12. A branch representation $\mathfrak{b}$ is a point of $\mathbb{P}^2(\mathbb{K}((T))) \setminus \mathbb{P}^2(\mathbb{K})$.

Definition 1.1.13. The coordinates $(\tilde{\alpha}(T) : \tilde{\beta}(T) : \tilde{\gamma}(T))$ of a branch representation $\mathfrak{b}$ are *special* if $\text{ord}_T(\tilde{\alpha}(T)) \geq 0$, $\text{ord}_T(\tilde{\beta}(T)) \geq 0$, $\text{ord}_T(\tilde{\gamma}(T)) \geq 0$, and at least one of these orders is equal to zero.

Remark 1.1.14. Every branch representation $\mathfrak{b}$ can be written in special coordinates. Indeed, writing $\mathfrak{b} = (\tilde{\alpha}(T) : \tilde{\beta}(T) : \tilde{\gamma}(T))$ and defining

$$e = -\min \left\{ \text{ord}_T(\tilde{\alpha}(T)), \text{ord}_T(\tilde{\beta}(T)), \text{ord}_T(\tilde{\gamma}(T)) \right\},$$

it follows that

$$\mathfrak{b} = (T^e \tilde{\alpha}(T) : T^e \tilde{\beta}(T) : T^e \tilde{\gamma}(T)),$$

where $\text{ord}_T(T^e \tilde{\alpha}(T)) \geq 0$, $\text{ord}_T(T^e \tilde{\beta}(T)) \geq 0$, $\text{ord}_T(T^e \tilde{\gamma}(T)) \geq 0$, and at least one of these orders is equal to zero.

Definition 1.1.15. Let $\mathfrak{b}$ be a branch representation and suppose that $(\tilde{\alpha}(T) : \tilde{\beta}(T) : \tilde{\gamma}(T))$ are special coordinates for $\mathfrak{b}$. Then, $(\tilde{\alpha}(0) : \tilde{\beta}(0) : \tilde{\gamma}(0)) \in \mathbb{P}^2(\mathbb{K})$ is the *center* of $\mathfrak{b}$.

Definition 1.1.16. Let $\mathfrak{b}$ be a branch representation and let $(\tilde{\alpha}(T) : \tilde{\beta}(T) : \tilde{\gamma}(T))$ be special coordinates for $\mathfrak{b}$. If $\tilde{\gamma}(T) = 1$ (resp. $\tilde{\alpha}(T) = 1$ or $\tilde{\beta}(T) = 1$), then the coordinates $(\tilde{\alpha}(T), \tilde{\beta}(T))$ (resp. $(\tilde{\beta}(T), \tilde{\gamma}(T))$ or $(\tilde{\alpha}(T), \tilde{\gamma}(T))$) are the *special affine coordinates* of $\mathfrak{b}$ with respect to Z (resp. X or Y).

Definition 1.1.17. 1. Two elements $(\tilde{\zeta}_1(T), \tilde{\eta}_1(T))$ and $(\tilde{\zeta}_2(T), \tilde{\eta}_2(T))$ of $\mathbb{K}[[T]]^2$ are *equivalent* if there exists a $\mathbb{K}$ -automorphism σ of $\mathbb{K}[[T]]$ such that

$$\tilde{\zeta}_1(T) = \sigma(\tilde{\zeta}_2(T)) \text{ and } \tilde{\eta}_1(T) = \sigma(\tilde{\eta}_2(T)).$$

2. An element $(\tilde{\zeta}(T), \tilde{\eta}(T)) \in \mathbb{K}[[T]]^2$ is *imprimitive* if there exist $(\tilde{\zeta}_1(T), \tilde{\eta}_1(T)) \in \mathbb{K}[[T]]^2$ and a $\mathbb{K}$ -monomorphism σ of $\mathbb{K}[[T]]$ that is not a $\mathbb{K}$ -automorphism satisfying

$$\tilde{\zeta}(T) = \sigma(\tilde{\zeta}_1(T)) \text{ and } \tilde{\eta}(T) = \sigma(\tilde{\eta}_1(T)).$$

Otherwise, $(\tilde{\zeta}(T), \tilde{\eta}(T))$ is called *primitive*.

Definition 1.1.18. 1. Two branch representations are *equivalent* if they have special affine coordinates with respect to the same variable (X , Y or Z) that are equivalent.

2. A branch representation is *imprimitive* if it has imprimitive special affine coordinates with respect to X , Y or Z . Otherwise, it is called *primitive*.

Proposition 1.1.19. Let $\mathfrak{b}$ be an imprimitive branch representation with imprimitive special affine coordinates $(\tilde{\alpha}(T), \tilde{\beta}(T))$ with respect to Z . Then, there exists a primitive branch representation $\mathfrak{b}_1$ with primitive special affine coordinates $(\tilde{\alpha}_1(T), \tilde{\beta}_1(T))$ with respect to Z such that

$$\tilde{\alpha}(T) = \sigma(\tilde{\alpha}_1(T)) \text{ and } \tilde{\beta}(T) = \sigma(\tilde{\beta}_1(T))$$

for some $\mathbb{K}$ -monomorphism σ of $\mathbb{K}[[T]]$ that is not a $\mathbb{K}$ -automorphism. An analogous situation holds for an imprimitive branch representation that admits imprimitive special affine coordinates with respect to X or Y .

Proof. The result follows from (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 4.20). ■

Definition 1.1.20. Let $\mathfrak{b}$ be an imprimitive branch representation and, without loss of generality, suppose that it has imprimitive special affine coordinates $(\tilde{\alpha}(T), \tilde{\beta}(T))$ with respect to Z . Let $\mathfrak{b}_1$ be a primitive branch representation with primitive special affine coordinates $(\tilde{\alpha}_1(T), \tilde{\beta}_1(T))$ with respect to Z satisfying

$$\tilde{\alpha}(T) = \sigma(\tilde{\alpha}_1(T)) \text{ and } \tilde{\beta}(T) = \sigma(\tilde{\beta}_1(T)),$$

for some $\mathbb{K}$ -monomorphism σ of $\mathbb{K}[[T]]$ that is not a $\mathbb{K}$ -automorphism. Then, the *ramification index* of $\mathfrak{b}$ is the order

$$\text{ord}_T(\sigma(T)).$$

Proposition 1.1.21. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Corollary 4.25). Equivalent imprimitive branch representations have the same ramification index. Further, the primitive branch representations to which they give rise are also equivalent.

Finally, this subsection ends with the notions of branch and branch of a plane curve.

Definition 1.1.22. A *branch* $\mathfrak{b}$ is an equivalence class of primitive branch representations. The *center of a branch* is the center of any of its primitive representations.

Definition 1.1.23. A branch $\mathfrak{b}$ is a *branch of a plane curve* $\mathcal{F} : F(X, Y, Z) = 0$ if its primitive representations $\mathfrak{b} = (\tilde{\alpha}(T) : \tilde{\beta}(T) : \tilde{\gamma}(T))$ satisfy

$$F(\tilde{\alpha}(T), \tilde{\beta}(T), \tilde{\gamma}(T)) = 0.$$

Theorem 1.1.24. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 4.30). The center of a branch of a plane curve is a point of the curve.

Conversely, the following occurs.

Theorem 1.1.25. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorems 4.32, 4.45 and 4.46). Each point P of a plane curve $\mathcal{F}$ is the center of at least one and at most m_P branches of $\mathcal{F}$, where m_P is the multiplicity of $\mathcal{F}$ at P . Also, the following occurs:

1. If P is a nonsingular point of $\mathcal{F}$, then P is the center of a unique branch of $\mathcal{F}$.
2. If P is an ordinary singular point of $\mathcal{F}$, then P is the center of exactly m_P branches of $\mathcal{F}$.

Theorem 1.1.26. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 4.37). Let $\mathcal{F}$ and $\mathcal{G}$ be distinct irreducible plane curves. Then $\mathcal{F}$ and $\mathcal{G}$ do not have branches in common.

1.1.2.2 Order and tangent of branch representations and branches

Let $(\tilde{\alpha}(T) : \tilde{\beta}(T) : \tilde{\gamma}(T))$ be special coordinates for a branch representation $\mathfrak{b}$. If $\tilde{\alpha}(T)$, $\tilde{\beta}(T)$ and $\tilde{\gamma}(T)$ are linearly independent over $\mathbb{K}$, then

$$\left\{ \text{ord}_T(\alpha\tilde{\alpha}(T) + \beta\tilde{\beta}(T) + \gamma\tilde{\gamma}(T)) : (\alpha : \beta : \gamma) \in \mathbb{P}^2(\mathbb{K}) \right\} = \left\{ j_0, j_1, j_2 \right\},$$

where j_0, j_1 and j_2 are non-negative integers satisfying $0 = j_0 < j_1 < j_2$. Further, j_1 is given by

$$\min \left\{ \text{ord}_T(\alpha\tilde{\alpha}(T) + \beta\tilde{\beta}(T) + \gamma\tilde{\gamma}(T)) : (\alpha : \beta : \gamma) \in \mathbb{P}^2(\mathbb{K}) \text{ and } \alpha\tilde{\alpha}(0) + \beta\tilde{\beta}(0) + \gamma\tilde{\gamma}(0) = 0 \right\},$$

and

$$j_2 = \text{ord}_T(\alpha_0\tilde{\alpha}(T) + \beta_0\tilde{\beta}(T) + \gamma_0\tilde{\gamma}(T))$$

for a unique point $(\alpha_0 : \beta_0 : \gamma_0) \in \mathbb{P}^2(\mathbb{K})$.

Definition 1.1.27. 1. The *order of* $\mathfrak{b}$ is the positive number j_1 .

2. The *order sequence of* $\mathfrak{b}$ is the sequence (j_0, j_1, j_2) .

3. The *tangent line of* $\mathfrak{b}$ is defined by

$$\mathcal{T}_{\mathfrak{b}} : \alpha_0 X + \beta_0 Y + \gamma_0 Z = 0.$$

Remark 1.1.28. When $\tilde{\alpha}(T)$, $\tilde{\beta}(T)$ and $\tilde{\gamma}(T)$ are linearly dependent, the same previous definitions hold by considering $j_2 = \infty$.

Definition 1.1.29. The *order*, *order sequence* and *tangent* of a branch $\mathfrak{b}$ are, respectively, the order, order sequence and tangent of any of its primitive representations.

This subsection ends with the following definition.

Definition 1.1.30. A branch is *linear* if its order is equal to 1.

1.1.2.3 Intersection multiplicity

Definition 1.1.31. Let $\mathcal{G} : G(X, Y, Z) = 0$ be a plane curve and let $\mathfrak{b}$ be a branch centered at the point P . If $(\tilde{\alpha}(T) : \tilde{\beta}(T) : \tilde{\gamma}(T))$ are special coordinates for a primitive representation $\tilde{b}$ of $\mathfrak{b}$, then the *intersection multiplicity of $\mathcal{G}$ and $\mathfrak{b}$* is defined by

$$I(P, \mathcal{G} \cap \mathfrak{b}) := \begin{cases} \text{ord}_T(G(\tilde{\alpha}(T), \tilde{\beta}(T), \tilde{\gamma}(T))), & \text{if } \mathfrak{b} \text{ is not a branch of } \mathcal{G} \\ \infty, & \text{otherwise.} \end{cases}$$

Definition 1.1.32. Let $\mathcal{F}$ be a plane curve and let P be a point of $\mathcal{F}$. If $\mathcal{G}$ is another plane curve, then the *intersection multiplicity of $\mathcal{F}$ and $\mathcal{G}$ at P* is defined by

$$I(P, \mathcal{F} \cap \mathcal{G}) = \sum_{\substack{\mathfrak{b} \text{ is a branch of } \mathcal{F} \\ \text{centered at } P}} I(P, \mathcal{G} \cap \mathfrak{b}).$$

Remark 1.1.33. From the considerations at the end of Section 4.4 of (HIRSCHFELD; KORCHMÁROS; TORRES, 2008), the intersection multiplicity of two plane curves $\mathcal{F} : F(X, Y, Z) = 0$ and $\mathcal{G} : G(X, Y, Z) = 0$ at a point P , as established in Definition 1.1.32, satisfies the following postulates:

- I 1) $I(P, \mathcal{F} \cap \mathcal{G})$ is a non-negative integer if $\mathcal{F}$ and $\mathcal{G}$ have no common component through P .
- I 2) $I(P, \mathcal{F} \cap \mathcal{G}) = \infty$ if $\mathcal{F}$ and $\mathcal{G}$ have a common component through P .
- I 3) $I(P, \mathcal{F} \cap \mathcal{G}) = 0$ if and only if $P \notin \mathcal{F} \cap \mathcal{G}$.
- I 4) $I(P, \mathcal{F} \cap \mathcal{G}) = 1$ if $\mathcal{F}$ and $\mathcal{G}$ are two distinct lines through P .
- I 5) $I(P, \mathcal{F} \cap \mathcal{G}) = I(P, \mathcal{G} \cap \mathcal{F})$.
- I 6) $I(P, \mathcal{F} \cap (\mathcal{G} + \mathcal{H}\mathcal{F})) = I(P, \mathcal{F} \cap \mathcal{G})$ for any $\mathcal{H} : H(X, Y, Z) = 0$, where

$$\mathcal{G} + \mathcal{H}\mathcal{F} : G(X, Y, Z) + H(X, Y, Z)F(X, Y, Z) = 0.$$

- I 7) $I(P, \mathcal{F} \cap \mathcal{G}\mathcal{H}) = I(P, \mathcal{F} \cap \mathcal{G}) + I(P, \mathcal{F} \cap \mathcal{H})$ for any $\mathcal{H} : H(X, Y, Z) = 0$, where

$$\mathcal{G}\mathcal{H} : G(X, Y, Z)H(X, Y, Z) = 0.$$

Since a number satisfying the previous postulates is unique by Theorem (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 3.8), Definition 1.1.32 coincides with other definitions found in the literature, among which it is possible to mention (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 3.9 and Definition 3.12) and (FULTON, 2008, Theorem 3 of Chapter 3 and considerations on Page 54).

In particular, if $\mathcal{F} : F(X, Y, Z) = 0$ is an arbitrary plane curve and $\mathcal{L} : L(X, Y, Z) = 0$ is a line, then $I(P, \mathcal{F} \cap \mathcal{L})$ can be determined as follows.

Without loss of generality, suppose that $P = (\alpha : \beta : 1)$ and define

$$F_*(X, Y) := F(X, Y, 1)$$

$$L_*(X, Y) := L(X, Y, 1).$$

Then, writing $F_*(X + \alpha, Y + \beta) = F_{m_P}(X, Y) + F_{m_P+1}(X, Y) + \cdots + F_d(X, Y)$ as in Remark 1.1.9, where d is the degree of $\mathcal{F}$, it follows that

$$I(P, \mathcal{F} \cap \mathcal{L}) = \min \left\{ i : L_*(X + \alpha, Y + \beta) \nmid F_i(X, Y) \right\}.$$

Now, the following result is a straightforward consequence of Definitions 1.1.10, 1.1.27, 1.1.29 and 1.1.32.

Proposition 1.1.34. Let $\mathcal{F}$ be a plane curve and let $P \in \mathcal{F}$. If $\mathcal{L}$ is a line, then $\mathcal{L}$ is tangent to $\mathcal{F}$ at P if and only if $\mathcal{L}$ is the tangent line of some branch $\mathfrak{b}$ of $\mathcal{F}$ centered at P .

Theorem 1.1.35. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 3.7). Let $\mathcal{F} : F(X, Y, Z) = 0$ and $\mathcal{G} : G(X, Y, Z) = 0$ be plane curves. If $m_P^{\mathcal{F}}$ and $m_P^{\mathcal{G}}$ are the multiplicities of $\mathcal{F}$ and $\mathcal{G}$ at P , respectively, then

$$I(P, \mathcal{F} \cap \mathcal{G}) \geq m_P^{\mathcal{F}} m_P^{\mathcal{G}}, \quad (1.1)$$

with equality occurring in (1.1) if and only if $\mathcal{F}$ and $\mathcal{G}$ have no common tangent at P .

Theorem 1.1.36 (Bézout's Theorem). Let $\mathcal{F} : F(X, Y, Z) = 0$ and $\mathcal{G} : G(X, Y, Z) = 0$ be plane curves of degrees d_1 and d_2 , respectively. If $\mathcal{F}$ and $\mathcal{G}$ do not have a common component, then

$$\sum_{P \in \mathcal{F} \cap \mathcal{G}} I(P, \mathcal{F} \cap \mathcal{G}) = d_1 d_2.$$

Proof. A proof of this result can be found in (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 3.14). ■

This subsection ends with the following definition, which is important in Part II.

Definition 1.1.37. Let $\mathcal{F}$ be a plane curve, let P be a nonsingular point of $\mathcal{F}$, and consider $\mathcal{T}_P$ the tangent line to $\mathcal{F}$ at P . P is an *inflection point* of $\mathcal{F}$ if

$$I(P, \mathcal{F} \cap \mathcal{T}_P) \geq 3.$$

Further, if $d \geq 2$, then P is called a *total inflection point* of $\mathcal{F}$ if it is the only point of $\mathcal{F}$ on the tangent line $\mathcal{T}_P$. In this case, $I(P, \mathcal{F} \cap \mathcal{T}_P) = d$.

1.1.3 Function fields of irreducible plane curves

Definition 1.1.38. Let $\mathcal{F} : F(X, Y, Z) = 0$ be a plane curve. A *generic point* of $\mathcal{F}$ is a point $(x : y : z)$ satisfying the following conditions:

1. The elements x, y and z are in some extension of $\mathbb{K}$ and satisfy $F(x, y, z) = 0$.
2. If $G(X, Y, Z) \in \mathbb{K}[X, Y, Z]$ is a homogeneous polynomial such that $G(x, y, z) = 0$, then $F(X, Y, Z) \mid G(X, Y, Z)$.

Theorem 1.1.39. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 5.3). A plane curve has a generic point if and only if it is irreducible.

Example 1.1.40. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Corollary 5.8). Let $\mathcal{F} : F(X, Y, Z) = 0$ be an irreducible plane curve and let $\mathfrak{b}$ be a branch of $\mathcal{F}$. Then, all primitive representations b of $\mathfrak{b}$ are generic points of $\mathcal{F}$.

Definition 1.1.41. Let $\mathcal{F} : F(X, Y, Z) = 0$ be an irreducible plane curve and let $(x : y : z)$ be a generic point of $\mathcal{F}$. The *function field of $\mathcal{F}$* , denoted by $\mathbb{K}(\mathcal{F})$, is the subfield of $\mathbb{K}(x, y, z)$

$$\left\{ \frac{A(x, y, z)}{B(x, y, z)} : \begin{array}{l} A(X, Y, Z), B(X, Y, Z) \text{ are homogeneous polynomials} \\ \text{in } \mathbb{K}[X, Y, Z] \text{ of the same degree, and } B(x, y, z) \neq 0 \end{array} \right\}.$$

Proposition 1.1.42. Let $\mathcal{F} : F(X, Y, Z) = 0$ be an irreducible plane curve. Then its function field $\mathbb{K}(\mathcal{F})$ is uniquely determined up to $\mathbb{K}$ -isomorphisms.

Proof. The result follows from (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 5.7). ■

Remark 1.1.43. Let $\mathcal{F} : F(X, Y, Z) = 0$ be an irreducible plane curve and let $(x : y : z)$ be a generic point of $\mathcal{F}$. If $z \neq 0$, then $\mathbb{K}(\mathcal{F})$ is $\mathbb{K}$ -isomorphic to $\mathbb{K}\left(\frac{x}{z}, \frac{y}{z}\right)$, where $F(x/z, y/z, 1) = 0$. A similar fact occurs if $x \neq 0$ or $y \neq 0$.

Definition 1.1.44. Two irreducible plane curves are *birationally equivalent* if their function fields are $\mathbb{K}$ -isomorphic.

This subsection ends with the following property concerning the function field of an irreducible plane curve.

Proposition 1.1.45. Let $\mathcal{F} : F(X, Y, Z) = 0$ be an irreducible plane curve. Then $\mathbb{K}(\mathcal{F})$ is an extension of transcendence degree 1 over $\mathbb{K}$.

Proof. The result follows from (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 5.10). ■

1.2 Algebraic function fields

In all this section, let Σ be a field of transcendence degree 1 over $\mathbb{K}$. In general, $\Sigma/\mathbb{K}$ is called an *algebraic function field of one variable over $\mathbb{K}$* or simply a *function field*, and the elements of $\Sigma \setminus \mathbb{K}$ are called *functions*.

1.2.1 Plane models

Theorem 1.2.1 (Theorem of the Primitive Element). If $x \in \Sigma$ is a transcendent element over $\mathbb{K}$, then there exists $y \in \Sigma$ such that $\Sigma = \mathbb{K}(x, y)$.

Proof. A proof of this result can be found in (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem A.5). ■

Definition 1.2.2. A *plane model* of Σ is a pair $(\mathcal{F}, (x, y))$, where $\Sigma = \mathbb{K}(x, y)$ and $\mathcal{F} : F(X, Y) = 0$ is an irreducible plane curve having $(x : y : 1)$ as a generic point.

As a consequence of Remark 1.1.43, Definition 1.1.44 and Theorem 1.2.1, the following occurs.

Corollary 1.2.3. There exists a plane model of Σ . Further, if $(\mathcal{F}, (x_1, y_1))$ and $(\mathcal{G}, (x_2, y_2))$ are two plane models of Σ , then $\mathcal{F}$ and $\mathcal{G}$ are birationally equivalent.

1.2.2 Places

Let $(\mathcal{F}, (x, y))$ be a plane model of Σ .

- Definition 1.2.4.**
1. A *place representation* of Σ is a $\mathbb{K}$ -monomorphism $\tau : \Sigma \rightarrow \mathbb{K}((T))$.
 2. A place representation τ of Σ is *primitive* if $\mathfrak{b} = (\tau(x) : \tau(y) : 1)$ is a primitive branch representation.
 3. Two place representations τ_1 and τ_2 are *equivalent* if there exists a $\mathbb{K}$ -automorphism σ of $\mathbb{K}((T))$ such that $\tau_1 = \sigma \circ \tau_2$.
 4. A *place* $\mathcal{P}$ of Σ is an equivalence class of primitive place representations.

Theorem 1.2.5. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 5.28). The places of Σ and the branches of $\mathcal{F}$ are in a natural one-to-one correspondence.

Definition 1.2.6. Let $\mathcal{P}$ be a place of Σ . The *order* of $f \in \Sigma$ at $\mathcal{P}$ is the number

$$v_{\mathcal{P}}(f) := \text{ord}_T(\tau(f)),$$

where τ is a primitive representation of $\mathcal{P}$.

Definition 1.2.7. Let $\mathcal{P}$ be a place of Σ . A *local parameter* at $\mathcal{P}$ is an element $t \in \Sigma$ such that $v_{\mathcal{P}}(t) = 1$.

Proposition 1.2.8. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Lemma 5.31). For every place $\mathcal{P}$ of Σ there exists a local parameter at $\mathcal{P}$.

Definition 1.2.9. Let $f \in \Sigma$ and let $\mathcal{P}$ be a place of Σ .

1. If $v_{\mathcal{P}}(f) > 0$, then $\mathcal{P}$ is a *zero* of f of *multiplicity* $v_{\mathcal{P}}(f)$.

2. If $v_{\mathcal{P}}(f) < 0$, then $\mathcal{P}$ is a pole of f of multiplicity $-v_{\mathcal{P}}(f)$.

Theorem 1.2.10. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorems 5.33, 5.34 and 5.35). Every function $f \in \Sigma \setminus \mathbb{K}$ has only finitely many zeros and poles. Further, the number of zeros and the number of poles of f (counted with their multiplicities) are equal and given by $[\Sigma : \mathbb{K}(f)]$.

Definition 1.2.11. Let $f \in \Sigma$ and let $\mathcal{P}$ be a place of Σ such that $v_{\mathcal{P}}(f) \geq 0$. Then, one can define $f(\mathcal{P}) := \alpha$, where α is the only element in $\mathbb{K}$ satisfying $v_{\mathcal{P}}(f - \alpha) > 0$.

From the definitions, the following properties hold.

Proposition 1.2.12. Let $\mathcal{P}$ be a place of Σ and let $f_1, f_2 \in \Sigma$ be such that $v_{\mathcal{P}}(f_1) \geq 0$ and $v_{\mathcal{P}}(f_2) \geq 0$. Then, $(f_1 + f_2)(\mathcal{P}) = f_1(\mathcal{P}) + f_2(\mathcal{P})$ and $(f_1 f_2)(\mathcal{P}) = f_1(\mathcal{P}) f_2(\mathcal{P})$.

1.2.3 Some remarks

Definition 1.2.13. A valuation ring of $\Sigma/\mathbb{K}$ is a ring $\mathcal{O}$ satisfying the following properties:

1. $\mathbb{K} \subsetneq \mathcal{O} \subsetneq \Sigma$.
2. For each $f \in \Sigma$, $f \in \mathcal{O}$ or $f^{-1} \in \mathcal{O}$.

Definition 1.2.14. A discrete valuation of $\Sigma/\mathbb{K}$ is a surjective function $v : \Sigma \rightarrow \mathbb{Z} \cup \{\infty\}$ satisfying:

1. $v(f) = \infty$ if and only if $f = 0$.
2. $v(f_1 f_2) = v(f_1) + v(f_2)$, for all $f_1, f_2 \in \Sigma$.
3. $v(f_1 + f_2) \geq \min\{v(f_1), v(f_2)\}$, for all $f_1, f_2 \in \Sigma$.
4. $v(\alpha) = 0$, for all $\alpha \in \mathbb{K}$.

Theorem 1.2.15. (STICHTENOTH, 2009, Theorem 1.1.13). Each valuation ring of $\Sigma/\mathbb{K}$ gives rise to a discrete valuation and vice-versa.

Considering Theorem 1.2.15, the following result establishes an important connection between the definition of a place given in Subsection 1.2.2 and the usual one, which defines a place of Σ as the maximal ideal of a valuation ring of $\Sigma/\mathbb{K}$.

Theorem 1.2.16. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 7.137). For each place $\mathcal{P}$ of Σ , $v_{\mathcal{P}}$ defines a discrete valuation of $\Sigma/\mathbb{K}$. Conversely, every discrete valuation of $\Sigma/\mathbb{K}$ is of the form $v_{\mathcal{P}}$ for some place $\mathcal{P}$ of Σ .

1.2.4 Expansion of a function at a local parameter

Let $\mathcal{P}$ be a place of Σ .

Definition 1.2.17. $\hat{\Sigma}_{\mathcal{P}}$ is a completion of Σ with respect to the discrete valuation $v_{\mathcal{P}}$ if:

1. $\hat{\Sigma}_{\mathcal{P}}$ is a field extension of Σ .
2. $\hat{\Sigma}_{\mathcal{P}}$ has a discrete valuation $\hat{v}_{\mathcal{P}}$ that extends $v_{\mathcal{P}}$.
3. $\hat{\Sigma}_{\mathcal{P}}$ is complete with respect to $\hat{v}_{\mathcal{P}}$, that is, every sequence $(\hat{f}_i)_{i \geq 0}$ in $\hat{\Sigma}_{\mathcal{P}}$ satisfying the property that

for all $k \in \mathbb{R}$ there is an index $i_0 \in \mathbb{N}$ such that $\hat{v}_{\mathcal{P}}(\hat{f}_{i_1} - \hat{f}_{i_2}) \geq k$ whenever $i_1, i_2 \geq i_0$

is convergent in the following sense:

there exists $\hat{f} \in \hat{\Sigma}_{\mathcal{P}}$ satisfying the condition that for all $k \in \mathbb{R}$ there is an index $i_0 \in \mathbb{N}$ such that $\hat{v}_{\mathcal{P}}(\hat{f} - \hat{f}_i) \geq k$ whenever $i \geq i_0$.

4. Σ is dense in $\hat{\Sigma}_{\mathcal{P}}$, that is, for each $\hat{f} \in \hat{\Sigma}_{\mathcal{P}}$ there is a sequence $(f_i)_{i \geq 0}$ in Σ such that $\lim_{i \rightarrow \infty} f_i = \hat{f}$.

Proposition 1.2.18. (STICHTENOTH, 2009, Proposition 4.2.3). There exists a completion $\hat{\Sigma}_{\mathcal{P}}$ of Σ with respect to $v_{\mathcal{P}}$. Moreover, this completion is unique in the following sense: if $\hat{\Sigma}_{\mathcal{P}}^{(1)}$ is another completion of Σ with respect to $v_{\mathcal{P}}$, then there is a unique isomorphism between $\hat{\Sigma}_{\mathcal{P}}$ and $\hat{\Sigma}_{\mathcal{P}}^{(1)}$ such that the following diagram commutes

$$\begin{array}{ccc} \hat{\Sigma}_{\mathcal{P}} & \cong & \hat{\Sigma}_{\mathcal{P}}^{(1)} \\ \searrow \hat{v}_{\mathcal{P}} & & \swarrow \hat{v}_{\mathcal{P}}^{(1)} \\ & \mathbb{Z} \cup \{\infty\} & \end{array}$$

where $\hat{v}_{\mathcal{P}}^{(1)}$ is the discrete valuation of $\hat{\Sigma}_{\mathcal{P}}^{(1)}$ that extends $v_{\mathcal{P}}$.

Based on Proposition 1.2.18, from now on $\hat{\Sigma}_{\mathcal{P}}$ denotes the completion of Σ with respect to the valuation $v_{\mathcal{P}}$.

Definition 1.2.19. A series $\sum_{i=k}^{\infty} f_i$ is convergent in $\hat{\Sigma}_{\mathcal{P}}$ if its sequence of partial sums is convergent.

With this definition, the following result holds.

Theorem 1.2.20. (STICHTENOTH, 2009, Theorem 4.2.6). Let $t \in \Sigma$ be a local parameter at $\mathcal{P}$. Then, every element $\hat{f} \in \hat{\Sigma}_{\mathcal{P}}$ has a unique representation of the form $\hat{f} = \sum_{i=k}^{\infty} \alpha_i t^i$, with $k \in \mathbb{Z}$

and $\alpha_i \in \mathbb{K}$. Conversely, if $(\alpha_i)_{i \geq k}$ is a sequence in $\mathbb{K}$, then the series $\sum_{i=k}^{\infty} \alpha_i t^i$ is convergent in $\hat{\Sigma}_{\mathcal{P}}$

and $\hat{v}_{\mathcal{P}}\left(\sum_{i=k}^{\infty} \alpha_i t^i\right) = \min \left\{ i : \alpha_i \neq 0 \right\}$.

Now, let τ be a primitive representation of $\mathcal{P}$ and let $\mathfrak{t} \in \Sigma$ be a local parameter at $\mathcal{P}$. Since $\text{ord}_T(\tau(\mathfrak{t})) = 1$, given $f \in \Sigma \setminus \{0\}$, one may write

$$\tau(f) = \sum_{i=v_{\mathcal{P}}(f)}^{\infty} \beta_i \tau(\mathfrak{t})^i,$$

with $\beta_i \in \mathbb{K}$. Further, for any other primitive representation τ_1 of $\mathcal{P}$, $\tau_1 = \sigma \circ \tau$, for some $\mathbb{K}$ -automorphism σ of $\mathbb{K}((T))$, and then

$$\tau_1(f) = \sigma \circ \tau(f) \stackrel{1}{=} \sum_{i=v_{\mathcal{P}}(f)}^{\infty} \beta_i (\sigma \circ \tau)(\mathfrak{t})^i = \sum_{i=v_{\mathcal{P}}(f)}^{\infty} \beta_i \tau_1(\mathfrak{t})^i,$$

which shows that the coefficients β_i are uniquely determined by $\mathcal{P}$ and $\mathfrak{t}$.

As a consequence of Theorem 1.2.20, especially of its proof, the following equality occurs:

$$f = \sum_{i=v_{\mathcal{P}}(f)}^{\infty} \beta_i \mathfrak{t}^i \in \hat{\Sigma}_{\mathcal{P}}.$$

Definition 1.2.21. The representation $f := \sum_{i=v_{\mathcal{P}}(f)}^{\infty} \beta_i \mathfrak{t}^i \in \hat{\Sigma}_{\mathcal{P}}$ is the $\mathcal{P}$ -adic expansion of f at the local parameter $\mathfrak{t}$ at $\mathcal{P}$.

1.2.5 Separating variables

Definition 1.2.22. A *separating variable* of Σ is an element $x \in \Sigma$ such that the extension $\Sigma/\mathbb{K}(x)$ is separable.

Proposition 1.2.23. If $\Sigma = \mathbb{K}(x, y)$, then either x or y is a separating variable of Σ .

Proof. The result follows from (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Lemma 5.38). ■

Proposition 1.2.24. Let $\mathcal{P}$ be a place of Σ . Then, every local parameter $\mathfrak{t}$ at $\mathcal{P}$ is a separating variable.

Proof. The result follows from (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Lemma 5.38). ■

1.2.6 Derivatives

Let $x \in \Sigma$ be a separating variable of Σ .

¹ An idea for the proof of this equality can be found in (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Considerations on Page 67).

Definition 1.2.25. The *formal derivative* in $\mathbb{K}[x]$ is the $\mathbb{K}$ -linear mapping

$$\begin{aligned} \frac{d}{dx} : \quad \mathbb{K}[x] &\rightarrow \mathbb{K}[x] \\ F(x) = \sum_{k=0}^l \alpha_k x^k &\mapsto \frac{dF(x)}{dx} := \sum_{k=1}^l k \alpha_k x^{k-1}. \end{aligned}$$

A straightforward verification shows the following result.

Proposition 1.2.26. The formal derivative in $\mathbb{K}[x]$ is a derivation of $\mathbb{K}[x]$ into itself, that is, it satisfies the *product rule*:

$$\frac{dF(x)G(x)}{dx} = F(x) \frac{dG(x)}{dx} + G(x) \frac{dF(x)}{dx}$$

for each $F(x), G(x) \in \mathbb{K}[x]$. Further, $\frac{d}{dx}$ is *over* $\mathbb{K}$, that is, $\frac{d\alpha}{dx} = 0$, for all $\alpha \in \mathbb{K}$, and it has a unique extension to a derivation of $\mathbb{K}(x)$ into itself, which satisfies

$$\frac{dF(x)/G(x)}{dx} = \frac{G(x) \frac{dF(x)}{dx} - F(x) \frac{dG(x)}{dx}}{G(x)^2},$$

for each $F(x), G(x) \in \mathbb{K}[x]$, with $G(x) \neq 0$.

Since x is a separating variable of Σ , and then $\Sigma/\mathbb{K}(x)$ is a separable extension, the following occurs.

Proposition 1.2.27. (STICHTENOTH, 2009, Proposition 4.1.4). There exists a unique extension of $\frac{d}{dx}$ to a derivation of Σ into itself.

Remark 1.2.28. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Definition 5.47). For each $f \in \Sigma$, let $F(X, Y) \in \mathbb{K}[X, Y]$ be an irreducible polynomial such that $F(x, f) = 0$. Then, $\frac{df}{dx}$ can be explicitly defined by

$$\frac{df}{dx} := -\frac{\frac{\partial F}{\partial X}|_{(x,f)}}{\frac{\partial F}{\partial Y}|_{(x,f)}}.$$

Finally, this subsection ends with the following definition.

Definition 1.2.29. Let $f \in \Sigma$ be an arbitrary element. Then, it is possible to define

$$\frac{d^0 f}{dx^0} := f, \quad \frac{d^1 f}{dx^1} := \frac{df}{dx}$$

and, for each $i \geq 2$,

$$\frac{d^i f}{dx^i} := \frac{d(d^{i-1} f / dx^{i-1})}{dx},$$

which is called the *i-th higher derivative* of $f \in \Sigma$.

1.2.7 Hasse derivatives

Let $x \in \Sigma$ be a separating variable of Σ .

Definition 1.2.30. For $i, k \in \mathbb{N}$, define

$$D_x^{(i)}(x^k) := \binom{k}{i} x^{k-i}.$$

The i -th Hasse derivative on $\mathbb{K}[x]$ is the $\mathbb{K}$ -linear extension of $D_x^{(i)}$ to $\mathbb{K}[x]$.

From Definition 1.2.30, the following holds.

Proposition 1.2.31. The mappings $D_x^{(i)}$ on $\mathbb{K}[x]$ satisfy:

$$D_x^{(i)}(f_1 f_2) = \sum_{k=0}^i D_x^{(k)}(f_1) D_x^{(i-k)}(f_2), \text{ for all } f_1, f_2 \in \mathbb{K}[x].$$

Proposition 1.2.32. The mappings $D_x^{(i)}$ on $\mathbb{K}[x]$ extend uniquely to $\mathbb{K}$ -linear mappings of $\mathbb{K}(x)$ into itself. These mappings are called the i -th Hasse derivative on $\mathbb{K}(x)$ and satisfy

$$D_x^{(i)}(f_1 f_2) = \sum_{k=0}^i D_x^{(k)}(f_1) D_x^{(i-k)}(f_2), \text{ for all } f_1, f_2 \in \mathbb{K}(x).$$

Proof. The result follows from (GOLDSCHMIDT, 2003, Lemma 1.3.9). ■

Since x is a separating variable of Σ , and then $\Sigma/\mathbb{K}(x)$ is a separable extension, the following occurs.

Proposition 1.2.33. (GOLDSCHMIDT, 2003, Theorem 1.3.11). The mappings $D_x^{(i)}$ on $\mathbb{K}(x)$ extend uniquely to $\mathbb{K}$ -linear mappings of Σ into itself. These mappings are called the i -th Hasse derivative on Σ and satisfy

$$D_x^{(i)}(f_1 f_2) = \sum_{k=0}^i D_x^{(k)}(f_1) D_x^{(i-k)}(f_2), \text{ for all } f_1, f_2 \in \Sigma.$$

Proposition 1.2.34. (GOLDSCHMIDT, 2003, Lemma 1.3.13). If $p = 0$ or if $i < p$, then

$$D_x^{(i)}(f) = \frac{1}{i!} \frac{d^i f}{dx^i}$$

for each $f \in \Sigma$.

Remark 1.2.35. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Definition 5.78). Let $f \in \Sigma$ and let $F(X, Y) \in \mathbb{K}[X, Y]$ be an irreducible polynomial satisfying $F(x, f) = 0$. One can

define $D_x^{(i)}(f)$ recursively using $F(X, Y)$. More precisely, for $i \in \mathbb{N}$, the i -th Hasse derivative $D_x^{(i)}$ of $f \in \Sigma$ can be defined by $D_x^{(0)}(f) := f$ and for $i \geq 1$

$$D_x^{(i)}(f) := -\frac{1}{\left.\frac{\partial F}{\partial Y}\right|_{(x,f)}} \left[\left.\frac{\partial^{(i)} F}{\partial X^{(i)}}\right|_{(x,f)} + \sum_{k=1}^{i-1} \left.\frac{\partial^{(i-k+1)} F}{\partial X^{(i-k)} \partial Y}\right|_{(x,f)} D_x^{(k)}(f) \right. \\ \left. + \sum_{k=2}^i \sum_{l=k}^i \sum_{i_1+\dots+i_k=l} \left.\frac{\partial^{(i-l+k)} F}{\partial X^{(i-l)} \partial Y^{(k)}}\right|_{(x,f)} D_x^{(i_1)}(f) \cdots D_x^{(i_k)}(f) \right],$$

where writing $F(X, Y) = \sum \alpha_{k_1, k_2} X^{k_1} Y^{k_2}$,

$$\frac{\partial^{(i_1+i_2)} F}{\partial X^{(i_1)} \partial Y^{(i_2)}} := \sum \alpha_{k_1, k_2} \binom{k_1}{i_1} \binom{k_2}{i_2} X^{k_1-i_1} Y^{k_2-i_2}.$$

Proposition 1.2.36. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Lemma 5.80 and Theorem 5.82). The i -th Hasse derivative on Σ , as established in Proposition 1.2.33 and Remark 1.2.35, satisfy:

1. $D_x^{(i_1)} \circ D_x^{(i_2)} = \binom{i_1+i_2}{i_1} D_x^{(i_1+i_2)}$, for all $i_1, i_2 \in \mathbb{N}$.
2. If $x_1 \in \Sigma$ is another separating variable, then, for each $f \in \Sigma$,

$$D_{x_1}^{(i)}(f) = \left(\frac{dx}{dx_1} \right)^i D_x^{(i)}(f) + \sum_{k=1}^{i-1} f_k D_{x_1}^{(k)}(f),$$

where $f_1, \dots, f_{i-1} \in \Sigma$ are polynomials in the indeterminates $D_{x_1}^{(k)}(x)$, for $1 \leq k \leq i$.

Let $\mathcal{P}$ be a place of Σ and consider t a local parameter at $\mathcal{P}$. This subsection ends with the following result which associates the $\mathcal{P}$ -adic expansions of f and $D_t^{(i)}(f)$ at the local parameter t at $\mathcal{P}$, for each $f \in \Sigma$ and $i \in \mathbb{N}$.

Theorem 1.2.37. (GOLDSCHMIDT, 2003, Theorem 2.5.13). If $f = \sum_{k=v_{\mathcal{P}}(f)}^{\infty} \alpha_k t^k$ is the $\mathcal{P}$ -adic expansion of $f \in \Sigma$ at the local parameter t at $\mathcal{P}$, then, for each $i \in \mathbb{N}$, $D_t^{(i)}(f) = \sum_{k=v_{\mathcal{P}}(f)}^{\infty} \binom{k}{i} \alpha_k t^{k-i}$ is the $\mathcal{P}$ -adic expansion of $D_t^{(i)}(f)$ at the local parameter t at $\mathcal{P}$.

1.2.8 Differentials and the notion of genus

Definition 1.2.38. Let x be a separating variable of Σ .

1. A *differential* is an element $f dx \in \Sigma(dx)$, where $f \in \Sigma$ and $\Sigma(dx)$ is a transcendental extension of Σ by the symbol dx .
2. For $f \in \Sigma$, the *differential of f* , denoted by df , is the differential

$$\frac{df}{dx} dx.$$

Remark 1.2.39. Let $x, x_1 \in \Sigma$ be two separating variables. Identifying dx_1 with $\frac{dx_1}{dx}dx$, then, from (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 5.49), for each $f \in \Sigma$ it follows that

$$\frac{df}{dx_1}dx_1 = \frac{df}{dx_1} \cdot \frac{dx_1}{dx}dx = \frac{df}{dx}dx.$$

In other words, the definition of df does not depend (in the previous sense) on the separating variable considered.

Definition 1.2.40. Let $x \in \Sigma$ be a separating variable. For each place $\mathcal{P}$ of Σ , the *order* $v_{\mathcal{P}}(dx)$ of dx at $\mathcal{P}$ is defined by

$$v_{\mathcal{P}}(dx) := \text{ord}_T \frac{d\tau(x)}{dT},$$

where τ is a primitive representation of $\mathcal{P}$. In this case, $\mathcal{P}$ is a *zero* (resp. a *pole*) of dx if $v_{\mathcal{P}}(dx) > 0$ (resp. $v_{\mathcal{P}}(dx) < 0$).

Proposition 1.2.41. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Lemma 5.53). If $x \in \Sigma$ is a separating variable, then $v_{\mathcal{P}}(dx) = 0$ for almost all places $\mathcal{P}$ of Σ .

Proposition 1.2.42. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Lemma 5.54). Let x, x_1 be two separating variables of Σ . Then

$$\sum_{\mathcal{P} \text{ is a place of } \Sigma} v_{\mathcal{P}}(dx) = \sum_{\mathcal{P} \text{ is a place of } \Sigma} v_{\mathcal{P}}(dx_1).$$

Definition 1.2.43. The *genus* g of Σ is the non-negative integer defined by the following equation

$$\sum_{\mathcal{P} \text{ is a place of } \Sigma} v_{\mathcal{P}}(dx) = 2g - 2,$$

where $x \in \Sigma$ is a separating variable.

Definition 1.2.44. The *genus of an irreducible plane curve* $\mathcal{F}$ is the genus of its function field $\mathbb{K}(\mathcal{F})$.

Theorem 1.2.45. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 5.57 and Comments on Page 135). Let $\mathcal{F}$ be an irreducible plane curve of genus g and degree d .

1. If $\mathcal{F}$ is nonsingular, then $g = \frac{(d-1)(d-2)}{2}$.
2. If $\mathcal{F}$ is a singular curve and $\{P_1, \dots, P_k\}$ is the set of its singularities, then

$$g \leq \frac{(d-1)(d-2)}{2} - \sum_{i=1}^k \frac{m_{P_i}(m_{P_i}-1)}{2}, \quad (1.2)$$

where, for each $i \in \{1, \dots, k\}$, m_{P_i} is the multiplicity of $\mathcal{F}$ at P_i . Moreover, if all the singularities of $\mathcal{F}$ are ordinary, then the equality in (1.2) holds.

1.2.9 Divisors and linear series

Definition 1.2.46. The group of divisors of Σ , denoted by $\text{Div}(\Sigma)$, is the free abelian group generated by the places of Σ . Its elements are called *divisors of Σ* .

Definition 1.2.47. Let $D = \sum_{\mathcal{P} \text{ is a place of } \Sigma} n_{\mathcal{P}} \mathcal{P} \in \text{Div}(\Sigma)$.

1. The *multiplicity of a place $\mathcal{P}$ in D* is the number $v_{\mathcal{P}}(D) := n_{\mathcal{P}}$.
2. The *support of D* is the finite set

$$\text{Supp}(D) := \left\{ \mathcal{P} \text{ is a place of } \Sigma : v_{\mathcal{P}}(D) \neq 0 \right\}.$$

Remark 1.2.48. The relation

$$D_1 \geq D_2 \text{ if and only if } v_{\mathcal{P}}(D_1) \geq v_{\mathcal{P}}(D_2) \text{ for all places } \mathcal{P} \text{ of } \Sigma$$

is a partial ordering on $\text{Div}(\Sigma)$.

Definition 1.2.49. If $D \geq 0$, then D is an *effective divisor*. Otherwise, D is called a *virtual divisor*.

Definition 1.2.50. The *degree of $D \in \text{Div}(\Sigma)$* is defined by

$$\deg(D) := \sum_{\mathcal{P} \text{ is a place of } \Sigma} v_{\mathcal{P}}(D).$$

Remark 1.2.51. The mapping

$$\begin{aligned} \deg : \text{Div}(\Sigma) &\rightarrow \mathbb{Z} \\ D &\mapsto \deg(D) \end{aligned}$$

is a homomorphism of groups.

From Theorem 1.2.10, the following definition is obtained.

Definition 1.2.52. Let $f \in \Sigma \setminus \{0\}$.

1. The *zero divisor of f* is the divisor $\text{div}(f)_0 := \sum_{\substack{\mathcal{P} \text{ is a place of } \Sigma \\ v_{\mathcal{P}}(f) > 0}} v_{\mathcal{P}}(f) \mathcal{P}$.
2. The *pole divisor of f* is the divisor $\text{div}(f)_{\infty} := \sum_{\substack{\mathcal{P} \text{ is a place of } \Sigma \\ v_{\mathcal{P}}(f) < 0}} -v_{\mathcal{P}}(f) \mathcal{P}$.
3. The *principal divisor of f* is the divisor $\text{div}(f) := \text{div}(f)_0 - \text{div}(f)_{\infty}$.

Definition 1.2.53. Two divisors D_1 and D_2 of Σ are *equivalent* if $D_1 = \text{div}(f) + D_2$, for some $f \in \Sigma \setminus \{0\}$. In this case, the relation between D_1 and D_2 is denoted by $D_1 \sim D_2$.

Remark 1.2.54. The relation established in Definition 1.2.53 is an equivalence relation.

The following property follows immediately from the definitions.

Proposition 1.2.55. If $D_1 \sim D_2$, then $\deg(D_1) = \deg(D_2)$.

Definition 1.2.56. Let $x \in \Sigma$ be a separating variable.

1. The *canonical divisor* associated with the differential dx is defined by

$$\operatorname{div}(dx) := \sum_{\mathcal{P} \text{ is a place of } \Sigma} v_{\mathcal{P}}(dx).$$

2. For $f \in \Sigma \setminus \{0\}$, the *canonical divisor* associated with the differential $f dx$ is defined by

$$\operatorname{div}(f dx) := \operatorname{div}(f) + \operatorname{div}(dx).$$

In particular, by definition, the divisors $\operatorname{div}(f dx)$, with $f \in \Sigma \setminus \{0\}$, constitute a class of divisors, which is called the *canonical class*.

Remark 1.2.57. In terms of the identification presented in Remark 1.2.39, the definition of the canonical class does not depend on the separating variable considered.

Definition 1.2.58. For each $D \in \operatorname{Div}(\Sigma)$, the *Riemann-Roch space associated to D* is the vector space over $\mathbb{K}$ defined by

$$\mathcal{L}(D) := \left\{ f \in \Sigma \setminus \{0\} : \operatorname{div}(f) + D \geq 0 \right\} \cup \{0\}.$$

Notation 1.2.59. For each $D \in \operatorname{Div}(\Sigma)$, the dimension of $\mathcal{L}(D)$ over $\mathbb{K}$ is denoted by $\ell(D)$.

Proposition 1.2.60. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Lemma 6.69). Let D , D_1 and D_2 be divisors of Σ .

1. If $D \geq 0$, then $\ell(D) \leq \deg(D) + 1$. More generally, if $D_2 \geq D_1$, then $\ell(D_2) - \ell(D_1) \leq \deg(D_2) - \deg(D_1)$.
2. If $D_1 \sim D_2$, then $\mathcal{L}(D_1)$ and $\mathcal{L}(D_2)$ are $\mathbb{K}$ -isomorphic.

Theorem 1.2.61 (Riemann-Roch Theorem). Let $x \in \Sigma$ be a separating variable. For each $D \in \operatorname{Div}(\Sigma)$,

$$\ell(D) = \deg(D) - g + 1 + \ell(\operatorname{div}(dx) - D),$$

where g is the genus of Σ .

Proof. A proof of this result can be found in (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 6.70). ■

Definition 1.2.62. For any place $\mathcal{P}$ of Σ , a non-negative integer i is a *pole number* of $\mathcal{P}$ if there is a function $f \in \Sigma$ such that $\operatorname{div}(f)_{\infty} = i\mathcal{P}$. Otherwise, i is called a *gap number* of $\mathcal{P}$.

Definition 1.2.63. Associated to a divisor $E \in \text{Div}(\Sigma)$, it is possible to define the following set:

$$|E| := \left\{ \text{div}(f) + E : f \in \mathcal{L}(E) \setminus \{0\} \right\}.$$

Remark 1.2.64. Let $E \in \text{Div}(\Sigma)$. Then, the mapping

$$\text{div}(f) + E \in |E| \mapsto [f] \in \mathbb{P}(\mathcal{L}(E))$$

provides a structure of projective space on $|E|$.

Notation 1.2.65. For $E \in \text{Div}(\Sigma)$, the following notation is used: $|E| \cong \mathbb{P}(\mathcal{L}(E))$.

Definition 1.2.66. A linear series $\mathcal{D}$ on Σ is a subset of some $|E|$ of the form

$$\left\{ \text{div}(f) + E : f \in \mathcal{S} \setminus \{0\} \right\},$$

where $\mathcal{S}$ is a $\mathbb{K}$ -linear subspace of $\mathcal{L}(E)$. The numbers $\mathfrak{d} := \deg(E)$ and $N = \dim(\mathcal{D}) := \dim(\mathcal{S}) - 1$ are, respectively, the *degree* and the *dimension of $\mathcal{D}$* , and $\mathcal{D}$ is said to be a $g_{\mathfrak{d}}^N$ on Σ . Further, $\mathcal{D}$ is called *complete* if $\mathcal{D} = |E|$.

Notation 1.2.67. In terms of Definition 1.2.66, for a linear series $\mathcal{D}$ the following notation is used: $\mathcal{D} \cong \mathbb{P}(\mathcal{S}) \subseteq |E|$.

Definition 1.2.68. Let $x \in \Sigma$ be a separating variable and let $g > 1$ be the genus of Σ . The complete linear series $|\text{div}(dx)|$ of degree $2g - 2$ and dimension $g - 1$ is the *canonical linear series*.

Definition 1.2.69. The linear series $\mathcal{D}_1 \cong \mathbb{P}(\mathcal{S}_1) \subseteq |E_1|$ is a *subseries* of $\mathcal{D}_2 \cong \mathbb{P}(\mathcal{S}_2) \subseteq |E_2|$ if $\mathcal{L}(E_1) \subseteq \mathcal{L}(E_2)$ and $\mathcal{S}_1 \subseteq \mathcal{S}_2$.

1.2.10 Linear systems of plane curves

Definition 1.2.70. For each $i = 0, \dots, M$, let $\mathcal{F}_i : F_i(X, Y, Z) = 0$ be a plane curve of degree $\mathfrak{d}$, with $F_0(X, Y, Z), \dots, F_M(X, Y, Z)$ linearly independent over $\mathbb{K}$. Then, the set

$$\left\{ \mathcal{F} : \sum_{i=0}^M \alpha_i F_i(X, Y, Z) = 0 : (\alpha_0 : \dots : \alpha_M) \in \mathbb{P}^M(\mathbb{K}) \right\}$$

is the *linear system of degree $\mathfrak{d}$ and dimension M generated by $\mathcal{F}_0, \dots, \mathcal{F}_M$* .

Definition 1.2.71. Let $(\mathcal{F}, (x, y))$ be a plane model of Σ . If $\mathcal{G}$ is a plane curve not containing $\mathcal{F}$ as a component, then the *intersection divisor cut out on $\mathcal{F}$ by $\mathcal{G}$* is defined by

$$\mathcal{G} \bullet \mathcal{F} = \sum_{\mathcal{P} \text{ is a place of } \Sigma} \mathbf{I}(\mathcal{P}, \mathcal{G} \cap \mathfrak{b}) \mathcal{P},$$

where, for each place $\mathcal{P}$ of Σ , $\mathfrak{b}$ is the corresponding branch of $\mathcal{F}$ and $P \in \mathcal{F}$ is its center.

Theorem 1.2.72. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 6.46). Let $(\mathcal{F}, (x, y))$ be a plane model of Σ . The plane curves of a linear system of degree $\mathfrak{d}$ that not contain $\mathcal{F}$ as a component cut out on $\mathcal{F}$ the divisors of a linear series. Further, the converse holds, up to a fixed divisor.

Proposition 1.2.73. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Remark 6.47 and Comments on Page 172). Let $(\mathcal{F}, (x, y))$ be a plane model of Σ of degree d . If $\mathcal{D}$ is the linear series cut out on $\mathcal{F}$ by the plane curves (not containing $\mathcal{F}$ as a component) of a linear system of degree $\mathfrak{d} < d$, then the dimension of $\mathcal{D}$ is equal to the dimension of the linear system.

1.3 Space curves

Let M be a positive integer.

Definition 1.3.1. A *branch representation* $\mathfrak{b}$ is a point of $\mathbb{P}^M(\mathbb{K}((T))) \setminus \mathbb{P}^M(\mathbb{K})$.

All definitions and results presented in Subsection 1.1.2 remain true for a general M . In particular, the notions of *special coordinates*, *center of a branch representation*, *affine (special) coordinates*, *equivalent branch representations*, *(im)primitive branch representations*, and *ramification index* still hold, and also:

Definition 1.3.2. A *branch* $\mathfrak{b}$ is an equivalence class of primitive branch representations. The *center of a branch* is the center of any of its primitive representations.

Definition 1.3.3. A *hypersurface* $\Delta \subseteq \mathbb{P}^M(\mathbb{K})$ is the point set given by the solutions of

$$F(X_0, \dots, X_M) = 0$$

in $\mathbb{P}^M(\mathbb{K})$, for some homogeneous polynomial $F(X_0, \dots, X_M) \in \mathbb{K}[X_0, \dots, X_M]$ of degree $d \geq 1$. In this case, d is the *degree of* Δ . Further, if $d = 1$, then Δ is called a *hyperplane*.

Definition 1.3.4. Let $\Delta : F(X_0, \dots, X_M) = 0$ be a hypersurface and let $\mathfrak{b}$ be a branch centered at the point Q . If $(\tilde{\alpha}_0(T) : \dots : \tilde{\alpha}_M(T))$ are special coordinates for a primitive representation $\tilde{\mathfrak{b}}$ of $\mathfrak{b}$, then the *intersection multiplicity of* Δ *and* $\mathfrak{b}$ is defined by

$$I(Q, \Delta \cap \mathfrak{b}) := \text{ord}_T(F(\tilde{\alpha}_0(T), \dots, \tilde{\alpha}_M(T))).$$

Definition 1.3.5. Let $\mathfrak{b}$ be a branch centered at the point Q . Then $\mathfrak{b}$ is *linear* if $I(Q, \Delta \cap \mathfrak{b}) = 1$ for some hyperplane Δ .

Now, let Σ be a field of transcendence degree 1 over $\mathbb{K}$ and let $(x_0 : \dots : x_M) \in \mathbb{P}^M(\Sigma)$ be such that

$$\Sigma = \mathbb{K}\left(\frac{x_0}{x_k}, \dots, \frac{x_M}{x_k}\right)$$

for some $k \in \{0, \dots, M\}$ satisfying $x_k \neq 0$. Note that if $x_l \neq 0$ for another $l \in \{0, \dots, M\}$, then the following equality also occurs:

$$\Sigma = \mathbb{K} \left(\frac{x_0}{x_l}, \dots, \frac{x_M}{x_l} \right).$$

Proposition 1.3.6. There exists $i \in \{0, \dots, M\}$ such that $\frac{x_i}{x_k}$ is a separating variable of Σ .

Proof. The result follows from Proposition 1.2.23 and (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Lemma 5.38). ■

For each place $\mathcal{P}$ of Σ , let τ be a primitive representation of $\mathcal{P}$. Then,

$$\mathfrak{b} = (\tau(x_0) : \dots : \tau(x_M))$$

is a primitive branch representation.

Definition 1.3.7. The branch $\mathfrak{b}$ with primitive representation given by $\mathfrak{b} = (\tau(x_0) : \dots : \tau(x_M))$ is the *branch associated to the place $\mathcal{P}$ with respect to $(x_0 : \dots : x_M) \in \mathbb{P}^M(\Sigma)$* .

Based on this, the notion of a projective irreducible algebraic curve can be established.

Definition 1.3.8. A *projective irreducible algebraic curve $\mathcal{X}$ in $\mathbb{P}^M(\mathbb{K})$* is a set of the form

$$\left\{ (\alpha_0 : \dots : \alpha_M) \in \mathbb{P}^M(\mathbb{K}) : (\alpha_0 : \dots : \alpha_M) \text{ is the center of a branch associated to a place } \mathcal{P} \text{ of } \Sigma \text{ with respect to } (x_0 : \dots : x_M) \in \mathbb{P}^M(\Sigma) \right\},$$

where Σ is a field of transcendence degree 1 over $\mathbb{K}$ and $(x_0 : \dots : x_M) \in \mathbb{P}^M(\Sigma)$ is a fixed element such that

$$\Sigma = \mathbb{K} \left(\frac{x_0}{x_k}, \dots, \frac{x_M}{x_k} \right)$$

for some $k \in \{0, \dots, M\}$ satisfying $x_k \neq 0$. In this case, $\mathbb{K}(\mathcal{X}) := \Sigma$ is the *function field of $\mathcal{X}$* , the branches associated to the places of Σ with respect to $(x_0 : \dots : x_M) \in \mathbb{P}^M(\Sigma)$ are the *branches of $\mathcal{X}$* , the *genus of $\mathcal{X}$* is the genus of $\mathbb{K}(\mathcal{X})$, and

$$(\mathcal{X}, (x_0 : \dots : x_M))$$

is a *model of Σ in $\mathbb{P}^M(\mathbb{K})$* . Further, $x_0, \dots, x_M$ are called the *coordinate functions of $\mathcal{X}$* .

Notation 1.3.9. Hereafter, the expression *irreducible curve* means a projective irreducible algebraic curve. Further, if Σ is a field of transcendence degree 1 over $\mathbb{K}$, $(x_0 : \dots : x_M) \in \mathbb{P}^M(\Sigma)$ is a fixed element such that

$$\Sigma = \mathbb{K} \left(\frac{x_0}{x_k}, \dots, \frac{x_M}{x_k} \right)$$

for some $k \in \{0, \dots, M\}$ satisfying $x_k \neq 0$, and

$$\mathcal{X} = \left\{ (\alpha_0 : \dots : \alpha_M) \in \mathbb{P}^M(\mathbb{K}) : \begin{array}{l} (\alpha_0 : \dots : \alpha_M) \text{ is the center of a branch associated to a place} \\ \mathcal{P} \text{ of } \Sigma \text{ with respect to } (x_0 : \dots : x_M) \in \mathbb{P}^M(\Sigma) \end{array} \right\},$$

then $\mathcal{X}$ is sometimes called the irreducible curve given by $(x_0 : \dots : x_M)$, without mention the function field Σ .

Theorem 1.3.10. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 7.2). Let $\mathcal{X}$ be an irreducible curve. Then each point of $\mathcal{X}$ is the center of a finite number of branches of $\mathcal{X}$.

Theorem 1.3.11. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 7.3). Let $\mathcal{X}$ be an irreducible curve. Then $\mathcal{X}$ has an infinite number of points.

Theorem 1.3.12. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 7.5). Let $\mathcal{X}$ be an irreducible curve given by the point $(x_0 : \dots : x_M)$.

1. The hypersurface $\Delta : F(X_0, \dots, X_M) = 0$ contains $\mathcal{X}$ if and only if $F(x_0, \dots, x_M) = 0$.
2. If Δ is a hypersurface not containing $\mathcal{X}$, then $\Delta \cap \mathcal{X}$ is a finite set.

Theorem 1.3.13. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 7.6). Let $\mathfrak{b}$ be a branch centered at a point Q of an irreducible curve $\mathcal{X}$, and let $(\tilde{\alpha}_0(T), \dots, \tilde{\alpha}_M(T))$ be special coordinates for a primitive representation $\tilde{\mathfrak{b}}$ of $\mathfrak{b}$. If $\Delta : F(X_0, \dots, X_M) = 0$ is a hypersurface not containing $\mathcal{X}$, then $I(Q, \Delta \cap \mathfrak{b})$ is finite, that is, $F(\tilde{\alpha}_0(T), \dots, \tilde{\alpha}_M(T)) \neq 0$.

Definition 1.3.14. Let $\mathcal{X}$ be an irreducible curve and let Δ be a hypersurface not containing $\mathcal{X}$. The *intersection divisor of $\mathcal{X}$ and Δ* is defined by

$$\Delta \bullet \mathcal{X} := \sum_{\substack{\mathfrak{b} \text{ is a branch of } \mathcal{X} \text{ centered at } Q \\ \text{and associated to the place } \mathcal{P} \text{ of } \mathbb{K}(\mathcal{X})}} I(Q, \Delta \cap \mathfrak{b}) \mathcal{P}.$$

Theorem 1.3.15. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 7.7). Let $\mathcal{X}$ be an irreducible curve given by the point $(x_0 : \dots : x_M)$ and let $\Delta : F(X_0, \dots, X_M) = 0$ be a hypersurface of degree d not containing $\mathcal{X}$. If $\Delta_i : X_i = 0$ does not contain $\mathcal{X}$, that is, if $x_i \neq 0$, then

$$\Delta \bullet \mathcal{X} = \text{div}(F(x_0/x_i, \dots, x_M/x_i)) + d(\Delta_i \bullet \mathcal{X}).$$

Definition 1.3.16. Let $\mathcal{X}$ be an irreducible curve. If Δ is a hyperplane not containing $\mathcal{X}$, then the *degree of $\mathcal{X}$* is defined by

$$\deg(\mathcal{X}) := \deg(\Delta \bullet \mathcal{X}).$$

Corollary 1.3.17. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Corollary 7.9). Let $\mathcal{X}$ be an irreducible curve given by the point $(x_0 : \dots : x_M)$ and let $\Delta : F(X_0, \dots, X_M) = 0$ be a hypersurface of degree d not containing $\mathcal{X}$. Then

$$\deg(\Delta \bullet \mathcal{X}) = d \cdot \deg(\mathcal{X}).$$

Definition 1.3.18. Let $\mathcal{X}$ be an irreducible curve. A point Q of $\mathcal{X}$ is *singular* if it is either the center of at least two branches or the center of one nonlinear branch of $\mathcal{X}$. Otherwise, Q is called *nonsingular*.

This subsection ends with the following result regarding the number of singularities of an irreducible curve.

Theorem 1.3.19. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 7.15). Let $\mathcal{X}$ be an irreducible curve. Then $\mathcal{X}$ has a finite number of singular points.

1.3.1 Rational transformations and morphisms

Let Σ be a field of transcendence degree 1 over $\mathbb{K}$ and let $(x_0 : \cdots : x_M) \in \mathbb{P}^M(\Sigma)$ be such that

$$\Sigma = \mathbb{K}\left(\frac{x_0}{x_i}, \dots, \frac{x_M}{x_i}\right)$$

for some $i \in \{0, \dots, M\}$. Also, let $\mathcal{X}$ be the irreducible curve given by $(x_0 : \cdots : x_M)$.

Definition 1.3.20. A rational transformation ϕ on $\mathcal{X}$ is an element $\phi := (f_0 : \cdots : f_N) \in \mathbb{P}^N(\Sigma)$. In this case, $f_0, \dots, f_N \in \Sigma$ are called *the coordinates of ϕ* .

Definition 1.3.21. Let $\phi = (f_0 : \cdots : f_N) \in \mathbb{P}^N(\Sigma)$ be a rational transformation on $\mathcal{X}$ and let $Q = (\alpha_0 : \cdots : \alpha_M) \in \mathcal{X}$. ϕ is defined at Q if it is possible to write

$$(f_0 : \cdots : f_N) = (A_0(x_0, \dots, x_M) : \cdots : A_N(x_0, \dots, x_M)) \in \mathbb{P}^N(\Sigma),$$

where $A_0(X_0, \dots, X_M), \dots, A_N(X_0, \dots, X_M) \in \mathbb{K}[X_0, \dots, X_M]$ are homogeneous polynomials of the same degree, and $A_k(\alpha_0, \dots, \alpha_M) \neq 0$ for some $k \in \{0, \dots, N\}$. In this case,

$$\phi(Q) := (A_0(\alpha_0, \dots, \alpha_M) : \cdots : A_N(\alpha_0, \dots, \alpha_M)).$$

Notation 1.3.22. A rational transformation $\phi = (f_0 : \cdots : f_N) \in \mathbb{P}^N(\Sigma)$ on $\mathcal{X}$ is denoted by

$$\phi = (f_0 : \cdots : f_N) : \mathcal{X} \dashrightarrow \mathbb{P}^N(\mathbb{K}).$$

Definition 1.3.23. A rational transformation $\phi = (f_0 : \cdots : f_N) : \mathcal{X} \dashrightarrow \mathbb{P}^N(\mathbb{K})$ is a *morphism* if it is defined at every point of $\mathcal{X}$. In this case, the notation $\phi = (f_0 : \cdots : f_N) : \mathcal{X} \rightarrow \mathbb{P}^N(\mathbb{K})$ is used.

Remark 1.3.24. Let $\phi = (f_0 : \cdots : f_N) : \mathcal{X} \dashrightarrow \mathbb{P}^N(\mathbb{K})$ be a rational transformation on $\mathcal{X}$ and let

$$\Sigma' = \mathbb{K}\left(\frac{f_0}{f_l}, \dots, \frac{f_N}{f_l}\right) \subseteq \Sigma,$$

where $l \in \{0, \dots, N\}$ is such that $f_l \neq 0$. Then one of the following situations occurs:

1. $\mathbb{K} = \Sigma'$: in this case, $\phi = (f_0 : \cdots : f_N) \in \mathbb{P}^N(\mathbb{K})$ and, in particular, ϕ is a constant morphism.
2. $\mathbb{K} \subsetneq \Sigma'$: in this case, Σ' is also a field of transcendence degree 1 over $\mathbb{K}$ and so it is possible to define the irreducible curve $\mathcal{Y}$ given by the point $(f_0/f_1 : \cdots : f_N/f_1) \in \mathbb{P}^N(\Sigma')$

$$\mathcal{Y} := \left\{ (\beta_0 : \cdots : \beta_N) \in \mathbb{P}^N(\mathbb{K}) : (\beta_0 : \cdots : \beta_N) \text{ is the center of a branch associated to a place } \mathcal{P}' \text{ of } \Sigma' \text{ with respect to } (f_0/f_1 : \cdots : f_N/f_1) \in \mathbb{P}^N(\Sigma') \right\}.$$

Proposition 1.3.25. Considering the notation as in Remark 1.3.24, if Σ' is a field of transcendence degree 1 over $\mathbb{K}$ and ϕ is defined at $Q \in \mathcal{X}$, then $\phi(Q) \in \mathcal{Y}$.

Proof. The result follows from (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Considerations on Section 7.2). ■

Definition 1.3.26. Consider the notation as in Remark 1.3.24.

1. If Σ' is a field of transcendence degree 1 over $\mathbb{K}$, then $\mathcal{Y}$ is the *image curve* of ϕ and $\deg(\phi) := [\Sigma : \Sigma']$ is the *degree* of ϕ . Further, in this case the notation $\phi = (f_0 : \cdots : f_N) : \mathcal{X} \dashrightarrow \mathcal{Y}$ is used, and ϕ is called a *covering*.
2. If $\Sigma' = \Sigma$, then $\mathcal{X}$ and $\mathcal{Y}$ are said to be *birationally equivalent* and ϕ is a *birational transformation*. In this case, there exists a rational transformation $\phi^{-1} : \mathcal{Y} \dashrightarrow \mathcal{X}$ satisfying $\phi^{-1} \circ \phi = Id_{\mathcal{X}}$ and $\phi \circ \phi^{-1} = Id_{\mathcal{Y}}$, where $\phi^{-1} \circ \phi = Id_{\mathcal{X}}$ means that, for each $Q \in \mathcal{X}$ such that ϕ is defined at Q and ϕ^{-1} is defined at $\phi(Q)$, the equality $\phi^{-1}(\phi(Q)) = Q$ holds, and similarly for $\phi \circ \phi^{-1} = Id_{\mathcal{Y}}$.
3. If $\Sigma' = \Sigma$ and ϕ is a morphism, then ϕ is called a *birational morphism*. Further, if ϕ^{-1} is also a morphism, then ϕ is called an *isomorphism*.

Theorem 1.3.27. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 7.17). Every irreducible curve is birationally equivalent to an irreducible plane curve.

Definition 1.3.28. Two arbitrary irreducible curves $\mathcal{X}$ and $\mathcal{Y}$ are *birationally equivalent* if their function fields are $\mathbb{K}$ -isomorphic.

Proposition 1.3.29. Let $\phi = (f_0 : \cdots : f_N) : \mathcal{X} \dashrightarrow \mathbb{P}^N(\mathbb{K})$ be a rational transformation on $\mathcal{X}$. If $Q \in \mathcal{X}$ is the center of only one branch of $\mathcal{X}$, then ϕ is defined at Q . Moreover, $\phi(Q)$ can be determined as follows: let $\mathcal{P}$ be the unique place of Σ corresponding to $Q \in \mathcal{X}$, let

$$e_{\mathcal{P}} = -\min \left\{ v_{\mathcal{P}}(f_0), \dots, v_{\mathcal{P}}(f_N) \right\},$$

and let $t \in \Sigma$ be a local parameter at $\mathcal{P}$. Then, $v_{\mathcal{P}}(t^{e_{\mathcal{P}}} f_i) \geq 0$, for all $i = 0, \dots, N$, and $v_{\mathcal{P}}(t^{e_{\mathcal{P}}} f_i) = 0$ for at least one $i = 0, \dots, N$. Therefore,

$$\phi(Q) = ((t^{e_{\mathcal{P}}} f_0)(\mathcal{P}) : \cdots : (t^{e_{\mathcal{P}}} f_N)(\mathcal{P})) \in \mathbb{P}^N(\mathbb{K}),$$

where $(t^{e_{\mathcal{P}}} f_i)(\mathcal{P})$ is given by Definition 1.2.11, for each $i \in \{0, \dots, N\}$.

Proof. The result follows from (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Considerations on Section 7.2). ■

As a consequence of Proposition 1.3.29, the following result holds.

Corollary 1.3.30. Let $\phi = (f_0 : \cdots : f_N) : \mathcal{X} \dashrightarrow \mathbb{P}^N(\mathbb{K})$ be a rational transformation on $\mathcal{X}$. If $\mathcal{X}$ is nonsingular, then ϕ is a morphism.

Definition 1.3.31. Let $\phi = (f_0 : \cdots : f_N) : \mathcal{X} \rightarrow \mathbb{P}^N(\mathbb{K})$ be a morphism. Then, ϕ is called *nondegenerate* if its image is not contained in a hyperplane of $\mathbb{P}^N(\mathbb{K})$, which occurs by Theorem 1.3.12 if and only if $f_0, \dots, f_N$ are linearly independent over $\mathbb{K}$.

1.3.2 Some remarks

In general, an irreducible curve is defined as a *projective algebraic variety of dimension 1*, being this concept equivalent to that one presented in Definition 1.3.8. More details on this subject can be found in (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Section 7.17).

Now, let Σ be a field of transcendence degree 1 over $\mathbb{K}$ and let $(\mathcal{X}, (x_0 : \cdots : x_M))$ be a model of Σ in $\mathbb{P}^M(\mathbb{K})$. Using the notion of projective algebraic varieties, the following result establishes the existence of a nonsingular model of Σ .

Theorem 1.3.32. (FULTON, 2008, Theorem 3 in Chapter 7). There exist a nonsingular irreducible curve $\mathcal{X}_1$ and a birational morphism $\phi_1 : \mathcal{X}_1 \rightarrow \mathcal{X}$. Further, if $\mathcal{X}_2$ is another nonsingular irreducible curve for which there exists a birational morphism $\phi_2 : \mathcal{X}_2 \rightarrow \mathcal{X}$, then there is a unique isomorphism $\phi : \mathcal{X}_1 \rightarrow \mathcal{X}_2$ such that the following diagram commutes

$$\begin{array}{ccc} \mathcal{X}_1 & \xrightarrow{\phi} & \mathcal{X}_2 \\ & \searrow \phi_1 & \swarrow \phi_2 \\ & \mathcal{X} & \end{array}$$

Definition 1.3.33. The nonsingular irreducible curve $\mathcal{X}_1$ given in Theorem 1.3.32 is the *nonsingular model* of $\mathcal{X}$.

Finally, from the definitions, the following property says that the notation introduced below is well defined.

Proposition 1.3.34. Suppose that $\mathcal{X}$ is a nonsingular irreducible curve. Then, there exist the following one-to-one correspondences:

$$\text{Places of } \Sigma \quad \xleftrightarrow{1-1} \quad \text{Branches of } \mathcal{X} \quad \xleftrightarrow{1-1} \quad \text{Points of } \mathcal{X}.$$

Notation 1.3.35. From now on, whenever $\mathcal{X}$ is considered a nonsingular irreducible curve, the main structures involving the places of $\Sigma = \mathbb{K}(\mathcal{X})$ are expressed in terms of the corresponding

points of $\mathcal{X}$. For instance, if $Q \in \mathcal{X}$ is the point corresponding to the place $\mathcal{P}$ of Σ , then the expressions v_Q , $\text{Div}(\mathcal{X})$ and $\sum_{Q \in \mathcal{X}} n_Q Q \in \text{Div}(\mathcal{X})$ are used instead of $v_{\mathcal{P}}$, $\text{Div}(\Sigma)$ and

$\sum_{\mathcal{P} \text{ is a place of } \Sigma} n_{\mathcal{P}} \mathcal{P} \in \text{Div}(\Sigma)$, respectively.

1.3.3 Morphisms $\times$ linear series

Let $\mathcal{X}$ be a nonsingular irreducible curve and let $\mathbb{K}(\mathcal{X})$ be its function field.

1.3.3.1 Morphisms from linear series

Let $\mathcal{D} \cong \mathbb{P}(\mathcal{S}) \subseteq |E|$ be a linear series of dimension N and degree $\mathfrak{d} = \deg(E)$ on $\mathcal{X}$.

Definition 1.3.36. For each $Q \in \mathcal{X}$ and $i \in \mathbb{N}$, define

$$\mathcal{D}_i(Q) := \left\{ D \in \mathcal{D} : D \geq iQ \right\}.$$

Proposition 1.3.37. (TORRES, 2000, Lemma 1.3). Let $Q \in \mathcal{X}$. For each $i \in \mathbb{N}$, the following holds.

1. $\mathcal{D}_i(Q)$ is a subseries of $\mathcal{D}$, namely $\mathcal{D}_i(Q) \cong \mathbb{P}(\mathcal{S} \cap \mathcal{L}(E - iQ)) \subseteq |E|$.
2. $\mathcal{D}_{i+1}(Q) \subseteq \mathcal{D}_i(Q)$ and $\mathcal{D}_i(Q) = \emptyset$ if $i > \mathfrak{d}$.
3. $\dim(\mathcal{D}_i(Q)) \leq \dim(\mathcal{D}_{i+1}(Q)) + 1$.

Definition 1.3.38. Let $Q \in \mathcal{X}$. The *multiplicity* $\mathfrak{b}(Q)$ of $\mathcal{D}$ at Q is defined by

$$\mathfrak{b}(Q) := \min \left\{ v_Q(D) : D \in \mathcal{D} \right\}.$$

From the definitions, the following occurs.

Proposition 1.3.39. Let $Q \in \mathcal{X}$. Then $\mathfrak{b}(Q) > 0$ if and only if $Q \in \text{Supp}(D)$ for all $D \in \mathcal{D}$. In particular, $\mathfrak{b}(Q) = 0$ for almost all points $Q \in \mathcal{X}$.

Definition 1.3.40. The *base locus* of $\mathcal{D}$ is the divisor B of $\mathcal{X}$ given by

$$B := \sum_{Q \in \mathcal{X}} \mathfrak{b}(Q)Q.$$

If $B = 0$, then $\mathcal{D}$ is called a *base-point-free linear series*.

Proposition 1.3.41. (TORRES, 2000, Considerations on Page 7). Let B be the base locus of $\mathcal{D}$. Then

$$\mathcal{D}^B := \left\{ D - B : D \in \mathcal{D} \right\}$$

is a base-point-free subseries of $\mathcal{D}$ of dimension N and degree $\mathfrak{d} - \deg(B)$, namely

$$\mathcal{D}^B \cong \mathbb{P}(\mathcal{S}) \subseteq |E - B|.$$

Proposition 1.3.42. (TORRES, 2000, Lemma 1.4). Let $\{f_0, \dots, f_M\}$ be a set of generators for $\mathcal{S}$. Then E is determined by $\mathcal{D}$, that is, for each $Q \in \mathcal{X}$

$$v_Q(E) = b(Q) - \min \left\{ v_Q(f_0), \dots, v_Q(f_M) \right\}.$$

Now, a morphism ϕ is associated to $\mathcal{D}$. In a coordinate-invariant description, since $\mathcal{D} = \mathcal{D}_{b(Q)}(Q) \supsetneq \mathcal{D}_{b(Q)+1}(Q)$ and thus $\dim(\mathcal{D}_{b(Q)+1}(Q)) = d - 1$ by Proposition 1.3.37, define

$$\begin{aligned} \phi : \mathcal{X} &\rightarrow \mathcal{D}^* \cong \mathbb{P}(\mathcal{S})^* \\ Q &\mapsto \mathcal{D}_{b(Q)+1}(Q) \end{aligned}.$$

In order to provide coordinates for ϕ , let $\{f_0, \dots, f_N\}$ be a basis for $\mathcal{S}$. If t is a local parameter at Q , then, for each $f \in \mathcal{S}$,

$$\begin{aligned} \operatorname{div}(f) + E \in \mathcal{D}_{b(Q)+1}(Q) &\Leftrightarrow v_Q(t^{v_Q(E)-b(Q)}f) \geq 1 \\ &\Leftrightarrow (t^{v_Q(E)-b(Q)}f)(Q) = 0. \end{aligned}$$

Therefore, writing $f = \sum_{k=0}^N \alpha_k f_k$, with $(\alpha_0 : \dots : \alpha_N) \in \mathbb{P}^N(\mathbb{K})$,

$$\begin{aligned} \mathcal{D}_{b(Q)+1}(Q) &\cong \left\{ (\alpha_0 : \dots : \alpha_N) \in \mathbb{P}^N(\mathbb{K}) : \sum_{k=0}^N (t^{v_Q(E)-b(Q)}f_k)(Q) \alpha_k = 0 \right\} \in \mathbb{P}^N(\mathbb{K})^* \\ &\cong ((t^{v_Q(E)-b(Q)}f_0)(Q) : \dots : (t^{v_Q(E)-b(Q)}f_N)(Q)) \in \mathbb{P}^N(\mathbb{K}), \end{aligned}$$

which leads to define

$$\phi := (f_0 : \dots : f_N) : \mathcal{X} \rightarrow \mathbb{P}^N(\mathbb{K}).$$

Formally:

Proposition 1.3.43. (TORRES, 2000, Lemma 1.5). Each basis $\{f_0, \dots, f_N\}$ of $\mathcal{S}$ over $\mathbb{K}$ defines a nondegenerate morphism $\phi = (f_0 : \dots : f_N) : \mathcal{X} \rightarrow \mathbb{P}^N(\mathbb{K})$. Moreover, a nondegenerate morphism associated to $\mathcal{D}$ is uniquely determined by $\mathcal{D}$ up to a projective equivalence.

Remark 1.3.44. From the previous discussion, the morphisms that come from $\mathcal{D}$ and $\mathcal{D}^B$ have the same coordinate description.

This subsection ends with the definition and some properties of the *canonical curve*.

Definition 1.3.45. Let $x \in \mathbb{K}(\mathcal{X})$ be a separating variable and let $|\operatorname{div}(dx)|$ be the canonical linear series on $\mathcal{X}$. The *canonical curve* is the irreducible image curve of the morphism that comes from $|\operatorname{div}(dx)|$.

Theorem 1.3.46. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 7.45). The canonical curve is a nonsingular irreducible curve in $\mathbb{P}^{g-1}(\mathbb{K})$, where g is the genus of $\mathcal{X}$.

1.3.3.2 Linear series from morphisms

Let $\phi = (f_0 : \dots : f_N) : \mathcal{X} \rightarrow \mathbb{P}^N(\mathbb{K})$ be a morphism on $\mathcal{X}$ and, for each $Q \in \mathcal{X}$, let

$$e_Q = -\min \left\{ v_Q(f_0), \dots, v_Q(f_N) \right\}.$$

Since $e_Q = 0$ for almost all points $Q \in \mathcal{X}$, then the divisor

$$E = \sum_{Q \in \mathcal{X}} e_Q Q$$

is well defined. Further:

Proposition 1.3.47. For each $i \in \{0, \dots, N\}$, $f_i \in \mathcal{L}(E)$.

Therefore, defining $\mathcal{S}$ as the $\mathbb{K}$ -linear subspace of $\mathcal{L}(E)$ generated by $\{f_0, \dots, f_N\}$, it is possible to consider the base-point-free linear series on $\mathcal{X}$

$$\mathcal{D} = \left\{ \operatorname{div}(f) + E : f \in \mathcal{S} \right\} \subseteq |E|.$$

More precisely, the following holds.

Proposition 1.3.48. (TORRES, 2000, Lemma 1.9). Associated to a morphism

$$\phi = (f_0 : \dots : f_N) : \mathcal{X} \rightarrow \mathbb{P}^N(\mathbb{K})$$

there exists a base-point-free linear series $\mathcal{D} \cong \mathbb{P}(\mathcal{S}) \subseteq |E|$, where $\mathcal{S}$ is the $\mathbb{K}$ -linear subspace of $\mathcal{L}(E)$ generated by $\{f_0, \dots, f_N\}$, and E is defined by

$$v_Q(E) = -\min \left\{ v_Q(f_0), \dots, v_Q(f_N) \right\}.$$

The linear series $\mathcal{D}$ is uniquely determined by ϕ and it is invariant under projective equivalence of morphisms. Further, if ϕ is nondegenerate, then $\dim(\mathcal{D}) = N$.

Now, suppose that $\phi = (f_0 : \dots : f_N) : \mathcal{X} \rightarrow \mathbb{P}^N(\mathbb{K})$ is a nondegenerate morphism on $\mathcal{X}$. Then, as before, the corresponding linear series $\mathcal{D}$ is given by

$$\mathcal{D} = \left\{ \operatorname{div} \left(\sum_{i=0}^N \alpha_i f_i \right) + E : (\alpha_0 : \dots : \alpha_N) \in \mathbb{P}^N(\mathbb{K}) \right\},$$

and since $(\alpha_0 : \dots : \alpha_N)$ can be identified with the hyperplane

$$\Delta : \sum_{i=0}^N \alpha_i X_i = 0,$$

it is possible to write

$$\mathcal{D} = \left\{ \phi^*(\Delta) : \Delta \text{ is a hyperplane in } \mathbb{P}^N(\mathbb{K}) \right\},$$

where $\phi^*(\Delta) := \operatorname{div} \left(\sum_{i=0}^N \alpha_i f_i \right) + E$ is the *pullback* of Δ by ϕ .

Proposition 1.3.49. (TORRES, 2000, Lemma 1.11). Considering the previous notation:

1. $Q \in \text{Supp}(\phi^*(\Delta))$ if and only if $\phi(Q) \in \Delta$. Therefore, $\text{Supp}(\phi^*(\Delta)) = \phi^{-1}(\phi(\mathcal{X}) \cap \Delta)$, where $\phi(\mathcal{X})$ is the image curve of ϕ .
2. $\deg(\mathcal{D}) = \deg(\phi) \deg(\phi(\mathcal{X}))$. In particular, if ϕ is a birational morphism, then $\deg(\mathcal{D}) = \deg(\phi(\mathcal{X}))$.
3. If ϕ is a birational morphism, then, identifying the branches of $\phi(\mathcal{X})$ with the points of $\mathcal{X}$, $\Delta \bullet \phi(\mathcal{X}) = \phi^*(\Delta)$ for each hyperplane Δ .

PROJECTIVE ALGEBRAIC CURVES DEFINED OVER FINITE FIELDS

Based on (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Chapters 8 and 9) and (GOLDSCHMIDT, 2003, Chapter 3), the purpose of this chapter is to provide some background on the topic *projective algebraic curves defined over finite fields*. As in the previous chapter, in many cases the objects introduced in the text are assumed to be well defined without proofs or other comments in this direction.

Here, let $\mathbb{F}_q$ be the finite field with $q = p^m$ elements, where p is a prime number, and consider $\overline{\mathbb{F}_q}$ the algebraic closure of $\mathbb{F}_q$.

2.1 Plane curves defined over $\mathbb{F}_q$

Definition 2.1.1. A plane curve $\mathcal{F} : F(X, Y, Z) = 0$ in $\mathbb{P}^2(\overline{\mathbb{F}_q})$ is *defined over $\mathbb{F}_q$* if there exists $\lambda \in \overline{\mathbb{F}_q}$ satisfying $\lambda F(X, Y, Z) \in \mathbb{F}_q[X, Y, Z]$.

Proposition 2.1.2. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Lemma 8.2). Let $\mathcal{F} : F(X, Y, Z) = 0$ be an irreducible plane curve in $\mathbb{P}^2(\overline{\mathbb{F}_q})$. Then, $\mathcal{F}$ is defined over $\mathbb{F}_q$ if and only if $(\alpha^q : \beta^q : \gamma^q) \in \mathcal{F}$, for all $(\alpha : \beta : \gamma) \in \mathcal{F}$.

Proposition 2.1.3. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Lemma 8.3). Let $\mathcal{F} : F(X, Y, Z) = 0$ be an irreducible plane curve in $\mathbb{P}^2(\overline{\mathbb{F}_q})$. Then, $\mathcal{F}$ is defined over $\mathbb{F}_q$ if and only if, for every generic point $(x : y : z)$ of $\mathcal{F}$, $(x^q : y^q : z^q)$ is also a generic point of $\mathcal{F}$.

Definition 2.1.4. Let $\mathcal{F} : F(X, Y, Z) = 0$ be a plane curve in $\mathbb{P}^2(\overline{\mathbb{F}_q})$ defined over $\mathbb{F}_q$. Then, $\mathcal{F}$ is *absolutely or geometrically irreducible* if $F(X, Y, Z)$ is irreducible in $\overline{\mathbb{F}_q}[X, Y, Z]$.

2.2 $\mathbb{F}_q$ -rational branches of plane curves

Definition 2.2.1. The *conjugate map* of $\overline{\mathbb{F}_q}((T))$ is the automorphism

$$\begin{aligned} \kappa : \overline{\mathbb{F}_q}((T)) &\rightarrow \overline{\mathbb{F}_q}((T)) \\ \sum \alpha_i T^i &\mapsto \sum \alpha_i^q T^i \end{aligned}$$

of $\overline{\mathbb{F}_q}((T))$.

Remark 2.2.2. The following occurs.

1. κ is not an $\overline{\mathbb{F}_q}$ -automorphism of $\overline{\mathbb{F}_q}((T))$.
2. If σ is an $\overline{\mathbb{F}_q}$ -automorphism of $\overline{\mathbb{F}_q}((T))$, then $\kappa \circ \sigma \circ \kappa^{-1}$ is also an $\overline{\mathbb{F}_q}$ -automorphism of $\overline{\mathbb{F}_q}((T))$. In particular, in terms of Definition 1.1.17, if the elements $(\tilde{\zeta}_1(T), \tilde{\eta}_1(T))$ and $(\tilde{\zeta}_2(T), \tilde{\eta}_2(T))$ of $\overline{\mathbb{F}_q}[[T]]^2$ are equivalent (resp. the element $(\tilde{\zeta}(T), \tilde{\eta}(T))$ of $\overline{\mathbb{F}_q}[[T]]^2$ is primitive), then $(\kappa(\tilde{\zeta}_1(T)), \kappa(\tilde{\eta}_1(T)))$ and $(\kappa(\tilde{\zeta}_2(T)), \kappa(\tilde{\eta}_2(T)))$ are also equivalent (resp. $(\kappa(\tilde{\zeta}(T)), \kappa(\tilde{\eta}(T)))$ is also primitive).

Definition 2.2.3. The *Frobenius image* $\Phi(\mathfrak{b})$ of a branch $\mathfrak{b}$ is the branch with primitive representation

$$\Phi(\mathfrak{b}) := (\kappa(\tilde{\alpha}(T)) : \kappa(\tilde{\beta}(T)) : \kappa(\tilde{\gamma}(T))),$$

where $\mathfrak{b} = (\tilde{\alpha}(T) : \tilde{\beta}(T) : \tilde{\gamma}(T))$ is a primitive representation of $\mathfrak{b}$.

Definition 2.2.4. A branch $\mathfrak{b}$ is $\mathbb{F}_q$ -rational if it has a primitive representation $\mathfrak{b}$ with special coordinates $(\tilde{\alpha}(T) : \tilde{\beta}(T) : \tilde{\gamma}(T))$ satisfying $\kappa(\tilde{\alpha}(T)) = \tilde{\alpha}(T)$, $\kappa(\tilde{\beta}(T)) = \tilde{\beta}(T)$ and $\kappa(\tilde{\gamma}(T)) = \tilde{\gamma}(T)$. In particular, $\Phi(\mathfrak{b}) = \mathfrak{b}$.

Remark 2.2.5. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Comments on Page 279). Let $\mathfrak{b}$ be an $\mathbb{F}_q$ -rational branch with primitive representation $\mathfrak{b} = (\tilde{\alpha}(T) : \tilde{\beta}(T) : \tilde{\gamma}(T))$ in special coordinates satisfying $\kappa(\tilde{\alpha}(T)) = \tilde{\alpha}(T)$, $\kappa(\tilde{\beta}(T)) = \tilde{\beta}(T)$ and $\kappa(\tilde{\gamma}(T)) = \tilde{\gamma}(T)$. Then, another primitive branch representation $\mathfrak{b}_1 = (\tilde{\alpha}_1(T) : \tilde{\beta}_1(T) : \tilde{\gamma}_1(T))$ in special coordinates of $\mathfrak{b}$ does not satisfy the property $\kappa(\tilde{\alpha}_1(T)) = \tilde{\alpha}_1(T)$, $\kappa(\tilde{\beta}_1(T)) = \tilde{\beta}_1(T)$ and $\kappa(\tilde{\gamma}_1(T)) = \tilde{\gamma}_1(T)$ unless there exists an $\overline{\mathbb{F}_q}$ -automorphism σ of $\overline{\mathbb{F}_q}[[T]]$ such that $\sigma(\mathbb{F}_q[[T]]) \subseteq \mathbb{F}_q[[T]]$.

Theorem 2.2.6. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 8.9). Let $\mathcal{F}$ be an absolutely irreducible plane curve defined over $\mathbb{F}_q$ and consider P a nonsingular point of $\mathcal{F}$. Then $P \in \mathbb{P}^2(\mathbb{F}_q)$ if and only if the unique branch of $\mathcal{F}$ centered at P is $\mathbb{F}_q$ -rational.

Theorem 2.2.7. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 8.10). Let $\mathcal{F}$ be an absolutely irreducible plane curve defined over $\mathbb{F}_q$ and consider $P \in \mathbb{P}^2(\mathbb{F}_q)$ a singular point of $\mathcal{F}$. For a linear branch $\mathfrak{b}$ of $\mathcal{F}$ centered at P , $\mathfrak{b}$ is $\mathbb{F}_q$ -rational if and only if the tangent line of $\mathfrak{b}$ is defined over $\mathbb{F}_q$.

Theorem 2.2.8. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 8.13). If $\mathfrak{b}$ is a branch of an absolutely irreducible plane curve $\mathcal{F}$ defined over $\mathbb{F}_q$, then $\mathfrak{b}$ is $\mathbb{F}_{q^n}$ -rational for some positive integer n .

2.3 $\mathbb{F}_q$ -rational function fields and $\mathbb{F}_q$ -rational places

Let $\mathcal{F} : F(X, Y) = 0$ be an absolutely irreducible plane curve defined over $\mathbb{F}_q$ and, in terms of Remark 1.1.43, let $\overline{\mathbb{F}_q}(\mathcal{F}) = \overline{\mathbb{F}_q}(x, y)$ be the function field of $\mathcal{F}$, where $(x : y : 1)$ is a generic point of $\mathcal{F}$.

Definition 2.3.1. The $\mathbb{F}_q$ -rational function field of $\mathcal{F}$, denoted by $\mathbb{F}_q(\mathcal{F})$, is the subfield of $\overline{\mathbb{F}_q}(\mathcal{F})$ described by

$$\left\{ \frac{A(x, y)}{B(x, y)} : A(X, Y), B(X, Y) \in \mathbb{F}_q[X, Y] \text{ and } B(x, y) \neq 0 \right\}.$$

The elements of $\mathbb{F}_q(\mathcal{F})$ are called $\mathbb{F}_q$ -rational functions of $\overline{\mathbb{F}_q}(\mathcal{F})$.

Definition 2.3.2. If

$$C^{(1)}(X, Y) := \sum \alpha_{ik}^q X^i Y^k$$

for each $C(X, Y) = \sum \alpha_{ik} X^i Y^k \in \overline{\mathbb{F}_q}[X, Y]$, then the *conjugate map* of $\overline{\mathbb{F}_q}(\mathcal{F})$ is the automorphism

$$\begin{aligned} \iota : \overline{\mathbb{F}_q}(\mathcal{F}) &\rightarrow \overline{\mathbb{F}_q}(\mathcal{F}) \\ f = \frac{A(x, y)}{B(x, y)} &\mapsto f^{(1)} := \frac{A^{(1)}(x, y)}{B^{(1)}(x, y)} \end{aligned}$$

of $\overline{\mathbb{F}_q}(\mathcal{F})$.

Remark 2.3.3. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Lemmas 8.14 and 8.15).

1. The definition of ι does not depend on the representation of the functions $f \in \overline{\mathbb{F}_q}(\mathcal{F})$.
2. $\iota(f) = f$ if and only if $f \in \mathbb{F}_q(\mathcal{F})$.

Definition 2.3.4. Let $\mathcal{P}$ be a place of $\overline{\mathbb{F}_q}(\mathcal{F})$ and let $\mathfrak{b}$ be the corresponding branch of $\mathcal{F}$. The *Frobenius image* of $\mathcal{P}$, denoted by $\Phi(\mathcal{P})$, is the place of $\overline{\mathbb{F}_q}(\mathcal{F})$ corresponding to the branch $\Phi(\mathfrak{b})$.

Remark 2.3.5. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Comments on Page 283).

Let τ be a primitive representation of a place $\mathcal{P}$ of $\overline{\mathbb{F}_q}(\mathcal{F})$. Then,

$$\kappa \circ \tau \circ \iota^{-1}$$

is a primitive representation of $\Phi(\mathcal{P})$.

Definition 2.3.6. Let $\mathcal{P}$ be a place of $\overline{\mathbb{F}_q}(\mathcal{F})$. Then, $\mathcal{P}$ is an $\mathbb{F}_q$ -rational place if $\Phi(\mathcal{P}) = \mathcal{P}$.

Corollary 2.3.7. By Theorem 2.2.8, if $\mathcal{P}$ is a place of $\overline{\mathbb{F}_q}(\mathcal{F})$, then $\mathcal{P}$ is $\mathbb{F}_{q^n}$ -rational for some positive integer n .

Theorem 2.3.8. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Lemma 8.17 and Theorem 8.31). The place $\mathcal{P}$ of $\overline{\mathbb{F}_q}(\mathcal{F})$ is $\mathbb{F}_q$ -rational if and only if the corresponding branch $\mathfrak{b}$ of $\mathcal{F}$ is $\mathbb{F}_q$ -rational.

Theorem 2.3.9. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 8.18). Let P be a nonsingular point of $\mathcal{F}$. Then $P \in \mathbb{P}^2(\mathbb{F}_q)$ if and only if the place $\mathcal{P}$ of $\overline{\mathbb{F}_q}(\mathcal{F})$ corresponding to the unique branch $\mathfrak{b}$ of $\mathcal{F}$ centered at P is $\mathbb{F}_q$ -rational.

2.3.1 Some remarks

In terms of the notation and the correspondence briefly introduced in Subsection 1.2.3, let us consider the function field $\overline{\mathbb{F}_q}(x, y)/\overline{\mathbb{F}_q}$ as a *constant field extension* of $\mathbb{F}_q(x, y)/\mathbb{F}_q$. Then, the following definition, which is equivalent to Definition 2.3.6, holds.

Definition 2.3.10. (GOLDSCHMIDT, 2003, Page 75). A place $\mathcal{P}$ of $\overline{\mathbb{F}_q}(x, y)/\overline{\mathbb{F}_q}$ is an $\mathbb{F}_q$ -rational place if $\mathcal{P} \cap \mathbb{F}_q(x, y)$ is a place of degree one of $\mathbb{F}_q(x, y)/\mathbb{F}_q$, or, equivalently, if $\mathcal{P} = \text{Con}_{\overline{\mathbb{F}_q}/\mathbb{F}_q(x, y)}(\mathcal{P}')$ for some place of degree one $\mathcal{P}'$ of $\mathbb{F}_q(x, y)/\mathbb{F}_q$, where $\text{Con}_{\overline{\mathbb{F}_q}/\mathbb{F}_q(x, y)}$ is the conorm map.

For more details on the topics and definitions above mentioned, we refer to (GOLDSCHMIDT, 2003, Section 3.2) and (STICHTENOTH, 2009, Section 3.6) for instance.

2.4 $\mathbb{F}_q$ -rational divisors and linear series

Let $\mathcal{F} : F(X, Y) = 0$ be an absolutely irreducible plane curve defined over $\mathbb{F}_q$ and, in terms of Remark 1.1.43, let $\overline{\mathbb{F}_q}(\mathcal{F}) = \overline{\mathbb{F}_q}(x, y)$ be the function field of $\mathcal{F}$, where $(x : y : 1)$ is a generic point of $\mathcal{F}$.

Definition 2.4.1. For $D = \sum_{\mathcal{P} \text{ is a place of } \overline{\mathbb{F}_q}(\mathcal{F})} n_{\mathcal{P}} \mathcal{P} \in \text{Div}(\overline{\mathbb{F}_q}(\mathcal{F}))$, define

$$\Phi(D) := \sum_{\mathcal{P} \text{ is a place of } \overline{\mathbb{F}_q}(\mathcal{F})} n_{\mathcal{P}} \Phi(\mathcal{P}).$$

Definition 2.4.2. Let $D \in \text{Div}(\overline{\mathbb{F}_q}(\mathcal{F}))$. D is an $\mathbb{F}_q$ -rational divisor if $\Phi(D) = D$. Further, the subgroup of $\text{Div}(\overline{\mathbb{F}_q}(\mathcal{F}))$ consisting of all $\mathbb{F}_q$ -rational divisors is denoted by $\text{Div}(\mathbb{F}_q(\mathcal{F}))$.

Remark 2.4.3. Let $D \in \text{Div}(\overline{\mathbb{F}_q}(\mathcal{F}))$. If $\mathcal{P}$ is $\mathbb{F}_q$ -rational, for all $\mathcal{P} \in \text{Supp}(D)$, then D is an $\mathbb{F}_q$ -rational divisor. However, the converse is not true in general. In fact, based on Corollary 2.3.7, let $\mathcal{P}$ be a place of $\overline{\mathbb{F}_q}(\mathcal{F})$ and consider n the smallest positive integer such that $\mathcal{P}$ is $\mathbb{F}_{q^n}$ -rational. Then, the divisor

$$D = \mathcal{P} + \Phi(\mathcal{P}) + \cdots + \Phi^{n-1}(\mathcal{P})$$

is $\mathbb{F}_q$ -rational even if $\mathcal{P}$ is not, that is, if $n > 1$. The divisor D is called the *closed place* of $\mathcal{P}$.

Definition 2.4.4. For a place $\mathcal{P}$ of $\overline{\mathbb{F}_q}(\mathcal{F})$, consider the notation given as in Remark 2.4.3. Then, the *degree* of $\mathcal{P}$ is defined by

$$\deg(\mathcal{P}) := n.$$

Proposition 2.4.5. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Lemmas 8.23 and 8.24). If $f \in \mathbb{F}_q(\mathcal{F}) \setminus \{0\}$, then both $\text{div}(f)$ and $\text{div}(df)$ are $\mathbb{F}_q$ -rational divisors. Conversely, if $f \in \overline{\mathbb{F}_q}(\mathcal{F}) \setminus \{0\}$ and $\text{div}(f)$ is an $\mathbb{F}_q$ -rational divisor, then $f \in \mathbb{F}_q(\mathcal{F})$ up to a constant factor.

Definition 2.4.6. A linear series $\mathcal{D}$ on $\overline{\mathbb{F}_q}(\mathcal{F})$ is $\mathbb{F}_q$ -rational if $\mathcal{D} \cong \mathbb{P}(\mathcal{S}) \subseteq |E|$, where $\mathcal{S} \subseteq \mathcal{L}(E)$ has a basis consisting of $\mathbb{F}_q$ -rational functions and E is an $\mathbb{F}_q$ -rational divisor.

Theorem 2.4.7. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 8.26). If E is an $\mathbb{F}_q$ -rational divisor, then $|E|$ is an $\mathbb{F}_q$ -rational linear series.

Corollary 2.4.8. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Remark 8.27). The canonical linear series is an $\mathbb{F}_q$ -rational linear series.

2.5 Space curves defined over $\mathbb{F}_q$

Let $\mathcal{F} : F(X, Y) = 0$ be an absolutely irreducible plane curve defined over $\mathbb{F}_q$ and let $\overline{\mathbb{F}_q}(\mathcal{F}) = \overline{\mathbb{F}_q}(x, y)$ be the function field of $\mathcal{F}$, where $(x : y : 1)$ is a generic point of $\mathcal{F}$. Further, consider $\mathcal{X}$ an irreducible curve in $\mathbb{P}^M(\overline{\mathbb{F}_q})$ such that $\overline{\mathbb{F}_q}(\mathcal{X}) = \overline{\mathbb{F}_q}(\mathcal{F})$.

In terms of Notation 1.3.9, it is possible to establish the following definition.

Definition 2.5.1. A curve $\mathcal{X}$ is defined over $\mathbb{F}_q$ if it is given by a point

$$(x_0 : \cdots : x_M) \in \mathbb{P}^M(\overline{\mathbb{F}_q}(\mathcal{F})),$$

with $x_i \in \mathbb{F}_q(\mathcal{F})$ for all $i = 0, \dots, M$.

Notation 2.5.2. If $\mathcal{X}$ is defined over $\mathbb{F}_q$, then $\mathcal{X}$ is called a *geometrically irreducible curve defined over $\mathbb{F}_q$* .

Definition 2.5.3. Suppose that $\mathcal{X}$ is defined over $\mathbb{F}_q$ and given by the point $(x_0 : \cdots : x_M) \in \mathbb{P}^M(\overline{\mathbb{F}_q}(\mathcal{F}))$, with $x_i \in \mathbb{F}_q(\mathcal{F})$ for all $i = 0, \dots, M$. A branch $\mathfrak{b}$ of $\mathcal{X}$ associated to the place $\mathcal{P}$ of $\overline{\mathbb{F}_q}(\mathcal{F})$ is $\mathbb{F}_q$ -rational if there exists a primitive representation τ of $\mathcal{P}$ such that the primitive representation $\mathfrak{b} = (\tau(x_0) : \cdots : \tau(x_M))$ of $\mathfrak{b}$ satisfies $\kappa(\tau(x_i)) = \tau(x_i)$ for all $i = 0, \dots, M$, where κ is given as in Definition 2.2.1.

Theorem 2.5.4. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 8.29). Suppose that $\mathcal{X}$ is defined over $\mathbb{F}_q$ and that Q is a nonsingular point of $\mathcal{X}$. Then, the following assertions are equivalent.

1. $Q \in \mathbb{P}^M(\mathbb{F}_q)$.
2. The unique branch $\mathfrak{b}$ of $\mathcal{X}$ centered at Q is $\mathbb{F}_q$ -rational.
3. The place $\mathcal{P}$ of $\overline{\mathbb{F}_q}(\mathcal{F})$ associated to $\mathfrak{b}$ is $\mathbb{F}_q$ -rational.

Theorem 2.5.5. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 8.31). If $\mathcal{X}$ is defined over $\mathbb{F}_q$, then a branch $\mathfrak{b}$ of $\mathcal{X}$ is $\mathbb{F}_q$ -rational if and only if the associated place $\mathcal{P}$ of $\overline{\mathbb{F}_q}(\mathcal{F})$ is $\mathbb{F}_q$ -rational.

2.5.1 Rational transformations and morphisms defined over $\mathbb{F}_q$

Let $\mathcal{F} : F(X, Y) = 0$ be an absolutely irreducible plane curve defined over $\mathbb{F}_q$ and let $\overline{\mathbb{F}_q}(\mathcal{F}) = \overline{\mathbb{F}_q}(x, y)$ be the function field of $\mathcal{F}$, where $(x : y : 1)$ is a generic point of $\mathcal{F}$. Also, consider $\mathcal{X}$ a geometrically irreducible curve defined over $\mathbb{F}_q$ such that $\overline{\mathbb{F}_q}(\mathcal{X}) = \overline{\mathbb{F}_q}(\mathcal{F})$.

Definition 2.5.6. Let $\phi = (f_0 : \cdots : f_N) \in \mathbb{P}^N(\overline{\mathbb{F}_q}(\mathcal{F}))$ be a rational transformation on $\mathcal{X}$. ϕ is said to be defined over $\mathbb{F}_q$ if $(f_0 : \cdots : f_N) \in \mathbb{P}^N(\mathbb{F}_q(\mathcal{F}))$. If $\mathcal{Y}$ is the image curve of ϕ and ϕ is defined over $\mathbb{F}_q$, then $\mathcal{Y}$ is also defined over $\mathbb{F}_q$ and $\phi : \mathcal{X} \dashrightarrow \mathcal{Y}$ is called an $\mathbb{F}_q$ -rational covering.

Remark 2.5.7. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Remark 8.19). Let $\mathcal{Y}$ be a geometrically irreducible curve defined over $\mathbb{F}_q$. If $\mathcal{X}$ and $\mathcal{Y}$ are birationally equivalent over $\overline{\mathbb{F}_q}$, then, in general, they do not have to be birationally equivalent over $\mathbb{F}_q$ as well.

2.5.2 Nonsingular models defined over $\mathbb{F}_q$

Let $\mathcal{F} : F(X, Y) = 0$ be an absolutely irreducible plane curve defined over $\mathbb{F}_q$ and let $\overline{\mathbb{F}_q}(\mathcal{F}) = \overline{\mathbb{F}_q}(x, y)$ be the function field of $\mathcal{F}$, where $(x : y : 1)$ is a generic point of $\mathcal{F}$. Also, consider $\mathcal{X}$ a geometrically irreducible curve defined over $\mathbb{F}_q$ such that $\overline{\mathbb{F}_q}(\mathcal{X}) = \overline{\mathbb{F}_q}(\mathcal{F})$.

The following remark discuss the existence of nonsingular models of $\mathcal{X}$ defined over $\mathbb{F}_q$.

Remark 2.5.8. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Remark 8.30). Theorem 2.4.7 provides a tool to construct nonsingular models defined over $\mathbb{F}_q$ of $\mathcal{X}$. Particularly, if $\mathcal{X}$ is neither rational, nor elliptic, nor hyperelliptic, the canonical curve is a nonsingular model defined over $\mathbb{F}_q$ of $\mathcal{X}$.

Lastly, in addition to Proposition 1.3.34 and Notation 1.3.35, the following correspondences are a consequence of Theorem 2.5.5.

Proposition 2.5.9. Suppose that $\mathcal{X}$ is nonsingular. Then, there exist the following one-to-one correspondences:

$$\mathbb{F}_q\text{-rational places of } \overline{\mathbb{F}_q}(\mathcal{X}) \xleftrightarrow{1-1} \mathbb{F}_q\text{-rational branches of } \mathcal{X} \xleftrightarrow{1-1} \mathbb{F}_q\text{-rational points on } \mathcal{X}.$$

2.6 The Zeta function of a curve defined over $\mathbb{F}_q$

Let $\mathcal{X}$ be a nonsingular geometrically irreducible curve of genus g in $\mathbb{P}^M(\overline{\mathbb{F}_q})$ defined over $\mathbb{F}_q$.

Definition 2.6.1. Let $D = \sum_{Q \in \mathcal{X}} n_Q Q$ be a divisor of $\mathcal{X}$. Then, it is possible to define

$$\deg(D) := \sum_{Q \in \mathcal{X}} n_Q \deg(Q),$$

where, for each $Q \in \mathcal{X}$, $\deg(Q)$ is considered as in Definition 2.4.4. Also, one may define

$$\mathcal{N}(D) := q^{\deg(D)} = \prod_{Q \in \mathcal{X}} \mathcal{N}(Q)^{n_Q},$$

where $\mathcal{N}(Q) := q^{\deg(Q)}$.

Definition 2.6.2. For a complex variable s , the *Zeta function of $\mathcal{X}$ over $\mathbb{F}_q$* is defined by

$$\zeta(\mathcal{X}, s) := \sum_{D \text{ is an effective } \mathbb{F}_q\text{-rational divisor}} \mathcal{N}(D)^{-s}.$$

Theorem 2.6.3 (Euler product). For $s \in \mathbb{C}$ such that $\operatorname{Re}(s) > 1$, the product

$$\prod_{Q \in \mathcal{X}} (1 - \mathcal{N}(Q)^{-s})^{-1} \quad (2.1)$$

is absolutely convergent to the function $\zeta(\mathcal{X}, s)$. In particular, the product (2.1) is independent of the order of its factors.

Proof. A proof of this result can be found in (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 9.3). ■

Theorem 2.6.4. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 9.5). For $s \in \mathbb{C}$ such that $\operatorname{Re}(s) > 1$,

$$\zeta(\mathcal{X}, s) = \frac{L(q^{-s})}{(1 - q^{-s})(1 - q^{1-s})},$$

where $L(T) = \sum_{i=0}^{2g} a_i T^i \in \mathbb{Z}[T]$, with $a_0 = 1$ and $a_{2g} = q^g$.

Theorem 2.6.5 (Functional equation). For $s \in \mathbb{C}$ such that $\operatorname{Re}(s) > 1$,

$$q^{(g-1)(2s-1)} \zeta(\mathcal{X}, s) = \zeta(\mathcal{X}, 1-s).$$

Proof. A proof of this result can be found in (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 9.6). ■

Definition 2.6.6. For $s \in \mathbb{C}$ such that $\operatorname{Re}(s) > 1$, define

$$t = t(s) := q^{-s}.$$

Definition 2.6.7. For $s \in \mathbb{C}$ such that $\operatorname{Re}(s) > 1$, consider t given as in Definition 2.6.6. Then, one can denote by

$$Z(\mathcal{X}, t)$$

the expression of $\zeta(\mathcal{X}, s)$, where q^{-s} is replaced by t .

Theorem 2.6.8. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 9.7). Consider t given as in Definition 2.6.6. If $|t| < q^{-1}$, then

$$Z(\mathcal{X}, t) = \exp\left(\sum_{n=1}^{\infty} \frac{N_{q^n}(\mathcal{X})}{n} t^n\right),$$

where $N_{q^n}(\mathcal{X})$ denotes the number of $\mathbb{F}_{q^n}$ -rational points on $\mathcal{X}$ for each positive integer n .

Proposition 2.6.9. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Remarks on Page 339). Consider t given as in Definition 2.6.6. If $|t| < q^{-1}$, then

$$Z(\mathcal{X}, t) = 1 + \sum_{n=1}^{\infty} A_n t^n,$$

where A_n is the number of effective $\mathbb{F}_q$ -rational divisors of $\mathcal{X}$ of degree n .

The following result is a straightforward consequence of Theorem 2.6.4 and Definition 2.6.6.

Proposition 2.6.10. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Comments on Page 339). Consider t given as in Definition 2.6.6. If $|t| < q^{-1}$, then

$$Z(\mathcal{X}, t) = \frac{L(t)}{(1-t)(1-qt)}$$

where

$$L(T) = L_q(T) = \begin{cases} 1, & \text{if } g = 0 \\ 1 + \sum_{i=1}^{2g-1} a_i T^i + a_{2g} T, & \text{otherwise} \end{cases} \quad (2.2)$$

belongs to $\mathbb{Z}[T]$.

Definition 2.6.11. The polynomial given in (2.2) is the *L-polynomial of $\mathcal{X}$ over $\mathbb{F}_q$* .

Proposition 2.6.12. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Proposition 9.9). The L-polynomial of $\mathcal{X}$ over $\mathbb{F}_q$ given by (2.2) satisfies the following properties:

1. $L(T) = q^g T^{2g} L((qT)^{-1})$.
2. $a_{2g-i} = q^{g-i} a_i$ for all $i = 0, \dots, g$.

Theorem 2.6.13. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 9.10). Consider the factorization

$$L(T) = \prod_{i=1}^{2g} (1 - \omega_i T)$$

of the L-polynomial of $\mathcal{X}$ over $\mathbb{F}_q$ given in (2.2). Then,

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

where $N_{q^n}(\mathcal{X})$ is the number of $\mathbb{F}_{q^n}$ -rational points on $\mathcal{X}$ for each positive integer n .

Proposition 2.6.14. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Proposition 9.12). For each $i \in \{1, \dots, g\}$, the coefficient a_i of the L-polynomial of $\mathcal{X}$ over $\mathbb{F}_q$ given in (2.2) satisfies the following relation:

$$ia_i = N_i + N_{i-1}a_1 + \dots + N_1a_{i-1},$$

where $N_i = N_{q^i}(\mathcal{X}) - (q^i + 1)$ and, for each $i \in \{1, \dots, g\}$, $N_{q^i}(\mathcal{X})$ is the number of $\mathbb{F}_{q^i}$ -rational points on $\mathcal{X}$.

Proposition 2.6.15. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Propositions 9.15 and 9.16). Considering the factorization

$$L(T) = \prod_{i=1}^{2g} (1 - \omega_i T)$$

of the L-polynomial of $\mathcal{X}$ over $\mathbb{F}_q$ given in (2.2), the L-polynomial $L_{q^n}(T)$ of $\mathcal{X}$ over $\mathbb{F}_{q^n}$ is given by

$$L_{q^n}(T) = \prod_{i=1}^{2g} (1 - \omega_i^n T).$$

Now, this section ends with the following important result.

Theorem 2.6.16 (Serre). Let $\mathcal{Y}$ be a nonsingular geometrically irreducible curve defined over $\mathbb{F}_q$. Suppose that there exists an $\mathbb{F}_q$ -rational covering $\phi : \mathcal{X} \rightarrow \mathcal{Y}$. Then, the L-polynomial of $\mathcal{Y}$ over $\mathbb{F}_q$ divides the L-polynomial of $\mathcal{X}$ over $\mathbb{F}_q$.

Proof. A proof of this result can be found in (AUBRY; PERRET, 2004). ■

2.7 The Hasse-Weil theorem and maximal curves

Let $\mathcal{X}$ be a nonsingular geometrically irreducible curve of genus g in $\mathbb{P}^M(\overline{\mathbb{F}_q})$ defined over $\mathbb{F}_q$. Further, let us consider the factorization

$$L(T) = \prod_{i=1}^{2g} (1 - \omega_i T)$$

of the L-polynomial of $\mathcal{X}$ over $\mathbb{F}_q$.

The following theorem, which is the Riemann hypothesis for irreducible curves defined over finite fields, is fundamental in the theory. It was first proved by Hasse for $g = 1$ (HASSE, 1936a), (HASSE, 1936b), (HASSE, 1936c) and then by Weil for $g > 1$ (WEIL, 1948).

Theorem 2.7.1 (Hasse-Weil). For each $i \in \{1, \dots, 2g\}$,

$$|\omega_i| = q^{1/2}.$$

Proof. A proof of this result can be found in (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Section 9.2). ■

As a consequence of the Hasse-Weil theorem (Theorem 2.7.1), the following bound for the number $N_q(\mathcal{X})$ of $\mathbb{F}_q$ -rational points on $\mathcal{X}$ can be obtained from Theorem 2.6.13:

Theorem 2.7.2 (Hasse-Weil bound).

$$|N_q(\mathcal{X}) - (q + 1)| \leq 2gq^{1/2}. \quad (2.3)$$

Proof. A proof of this result can be found in (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Section 9.2). ■

The previous theorem leads us to the following definition.

Definition 2.7.3. The curve $\mathcal{X}$ is called *maximal* (resp. *minimal*) over $\mathbb{F}_q$ if it attains the Hasse-Weil upper (resp. lower) bound (2.3), or, equivalently, if $\omega_i = -q^{1/2}$ (resp. $\omega_i = q^{1/2}$) for each $i \in \{1, \dots, 2g\}$.

Finally, the following result is an immediate consequence of Theorem 2.6.16 and Definition 2.7.3.

Theorem 2.7.4 (Serre). Let $\mathcal{Y}$ be a nonsingular geometrically irreducible curve defined over $\mathbb{F}_q$. Suppose that there exists an $\mathbb{F}_q$ -rational covering $\phi : \mathcal{X} \rightarrow \mathcal{Y}$. If $\mathcal{X}$ is either $\mathbb{F}_{q^{2n}}$ -maximal or $\mathbb{F}_{q^{2n}}$ -minimal, then $\mathcal{X}$ is $\mathbb{F}_{q^{2n}}$ -maximal (resp. $\mathbb{F}_{q^{2n}}$ -minimal) if and only if $\mathcal{Y}$ is $\mathbb{F}_{q^{2n}}$ -maximal (resp. $\mathbb{F}_{q^{2n}}$ -minimal).

THE STÖHR-VOLOCH THEORY

Based on (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Chapters 7 and 8), (TORRES, 2000, Sections 1 and 2) and (STÖHR; VOLOCH, 1986), the purpose of this chapter is to establish a general background on the *Stöhr-Voloch Theory*.

Considering p a prime number and $q = p^m$ for some positive integer m , the following theorem, whose proof follows essentially by an application of Bézout's Theorem (see Theorem 1.1.36), is a slightly simpler version of the main result of (STÖHR; VOLOCH, 1986). Nowadays, this is sometimes called the *Baby Stöhr-Voloch Theorem*.

Theorem 3.0.1. (STÖHR; VOLOCH, 1986, Theorem 0.1). Let $p > 2$ and let $\mathcal{F} : F(X, Y, Z) = 0$ be an absolutely irreducible plane curve of degree d defined over $\mathbb{F}_q$. If $\mathcal{F}$ has a finite number of inflection points and $N_q(\mathcal{F})$ is defined by

$$N_q(\mathcal{F}) := \# \left\{ (\alpha : \beta : \gamma) \in \mathbb{P}^2(\mathbb{F}_q) : F(\alpha, \beta, \gamma) = 0 \right\},$$

then $N_q(\mathcal{F})$ satisfies

$$N_q(\mathcal{F}) \leq \frac{d(d+q-1)}{2}.$$

3.1 Morphisms and Weierstrass points

Throughout this section, let $\mathbb{K}$ be an algebraically closed field of characteristic $p \geq 0$ and let $\mathcal{X}$ be a nonsingular irreducible curve of genus g over $\mathbb{K}$. Also, let

$$\phi = (f_0 : \cdots : f_N) : \mathcal{X} \rightarrow \mathbb{P}^N(\mathbb{K})$$

be a nondegenerate morphism on $\mathcal{X}$ and, as discussed on Subsection 1.3.3.2, let $\mathcal{D}$ be the corresponding base-point-free linear series of dimension N and degree $\mathfrak{d}$, that is, let

$$\begin{aligned}\mathcal{D} &= \left\{ \operatorname{div} \left(\sum_{i=0}^N \alpha_i f_i \right) + E : (\alpha_0 : \dots : \alpha_N) \in \mathbb{P}^N(\mathbb{K}) \right\} \\ &= \left\{ \phi^*(\Delta) : \Delta \text{ is a hyperplane in } \mathbb{P}^N(\mathbb{K}) \right\},\end{aligned}$$

where $E = \sum_{Q \in \mathcal{X}} e_Q Q$ is defined by

$$e_Q = -\min \left\{ v_Q(f_0), \dots, v_Q(f_N) \right\}$$

and $\phi^*(\Delta) = \operatorname{div} \left(\sum_{i=0}^N \alpha_i f_i \right) + E$ is the pullback of the hyperplane $\Delta : \sum_{i=0}^N \alpha_i X_i = 0$ by ϕ .

3.1.1 Hermitian invariants and osculating spaces

Definition 3.1.1. Let $Q \in \mathcal{X}$. An integer j is a *Hermitian Q -invariant* or a $(\mathcal{D}, Q)$ -*order* if there exists a divisor $D \in \mathcal{D}$ such that $v_Q(D) = j$.

From Proposition 1.3.37, the following occurs.

Proposition 3.1.2. Let $Q \in \mathcal{X}$. An integer j is a $(\mathcal{D}, Q)$ -order if and only if $\mathcal{D}_j(Q) \supsetneq \mathcal{D}_{j+1}(Q)$. In particular, there are exactly $N+1$ $(\mathcal{D}, Q)$ -orders, namely $0 = j_0 < \dots < j_N \leq \mathfrak{d}$.

Definition 3.1.3. Let $Q \in \mathcal{X}$ and let $0 = j_0 < \dots < j_N \leq \mathfrak{d}$ be given as in Proposition 3.1.2. Then $(j_0, \dots, j_N)$ is the *sequence of $(\mathcal{D}, Q)$ -orders*.

As a consequence of the Riemann-Roch Theorem (see Theorem 1.2.61), the following result holds.

Proposition 3.1.4. Suppose that $\mathcal{D}$ is the canonical linear series. For each $Q \in \mathcal{X}$, j is a $(\mathcal{D}, Q)$ -order if and only if $j+1$ is a gap number of Q .

Definition 3.1.5. Let $Q \in \mathcal{X}$. For each $i \in \{0, \dots, N-1\}$, the *i -th osculating space at Q* , denoted by $L_i(Q)$, is defined by

$$L_i(Q) := \bigcap_{\substack{\Delta \text{ is a hyperplane in } \mathbb{P}^N(\mathbb{K}) \\ \text{such that } v_Q(\phi^*(\Delta)) \geq j_{i+1}}} \Delta,$$

where $(j_0, \dots, j_N)$ is the sequence of $(\mathcal{D}, Q)$ -orders. In the particular case $i = N-1$, $L_{N-1}(Q)$ is called the *osculating hyperplane at Q* .

It follows from the definitions that, for each $Q \in \mathcal{X}$, $L_0(Q) \subseteq \dots \subseteq L_{N-1}(Q)$. Furthermore, the following occurs.

Theorem 3.1.6. (STÖHR; VOLOCH, 1986, Theorem 1.1 and Scholium 1.2). Let $Q \in \mathcal{X}$, let $\mathfrak{t}$ be a local parameter at Q , and let $(j_0, \dots, j_N)$ be the sequence of $(\mathcal{D}, Q)$ -orders, where $j_0 = 0$.

1. For each $i \geq 1$,

$$j_i(Q) = \min \left\{ j : \begin{array}{l} (D_{\mathfrak{t}}^{(j_0)} \mathfrak{t}^{e_Q} f_0(Q), \dots, D_{\mathfrak{t}}^{(j_0)} \mathfrak{t}^{e_Q} f_N(Q)), \dots, (D_{\mathfrak{t}}^{(j_{i-1})} \mathfrak{t}^{e_Q} f_0(Q), \dots, D_{\mathfrak{t}}^{(j_{i-1})} \mathfrak{t}^{e_Q} f_N(Q)), \\ (D_{\mathfrak{t}}^{(j)} \mathfrak{t}^{e_Q} f_0(Q), \dots, D_{\mathfrak{t}}^{(j)} \mathfrak{t}^{e_Q} f_N(Q)) \text{ are linearly independent over } \mathbb{K} \end{array} \right\}.$$

2. Let $\mathcal{S}_i(Q)$ be the $\mathbb{K}$ -linear subspace of $\mathbb{K}^{N+1}$ generated by

$$(D_{\mathfrak{t}}^{(j_0)} \mathfrak{t}^{e_Q} f_0(Q), \dots, D_{\mathfrak{t}}^{(j_0)} \mathfrak{t}^{e_Q} f_N(Q)), \dots, (D_{\mathfrak{t}}^{(j_i)} \mathfrak{t}^{e_Q} f_0(Q), \dots, D_{\mathfrak{t}}^{(j_i)} \mathfrak{t}^{e_Q} f_N(Q)).$$

Then, $L_i(Q) = \mathbb{P}(\mathcal{S}_i(Q)) \subseteq \mathbb{P}^N(\mathbb{K})$. In particular, $\dim(L_i(Q)) = i$.

3. Let $k_0 < \dots < k_i$ be non-negative integers, with $i \leq N$, such that the vectors

$$(D_{\mathfrak{t}}^{(k_0)} \mathfrak{t}^{e_Q} f_0(Q), \dots, D_{\mathfrak{t}}^{(k_0)} \mathfrak{t}^{e_Q} f_N(Q)), \dots, (D_{\mathfrak{t}}^{(k_i)} \mathfrak{t}^{e_Q} f_0(Q), \dots, D_{\mathfrak{t}}^{(k_i)} \mathfrak{t}^{e_Q} f_N(Q))$$

are linearly independent over $\mathbb{K}$. Then $j_l \leq k_l$, for each $l \in \{0, \dots, i\}$.

Corollary 3.1.7. (STÖHR; VOLOCH, 1986, Corollary 1.3). Let $Q \in \mathcal{X}$, let $\mathfrak{t}$ be a local parameter at Q , and let $(j_0, \dots, j_N)$ be the sequence of $(\mathcal{D}, Q)$ -orders, where $j_0 = 0$. Then, the osculating hyperplane at Q is given by the equation

$$\det \begin{bmatrix} X_0 & \cdots & X_N \\ D_{\mathfrak{t}}^{(j_0)} \mathfrak{t}^{e_Q} f_0(Q) & \cdots & D_{\mathfrak{t}}^{(j_0)} \mathfrak{t}^{e_Q} f_N(Q) \\ \vdots & & \vdots \\ D_{\mathfrak{t}}^{(j_{N-1})} \mathfrak{t}^{e_Q} f_0(Q) & \cdots & D_{\mathfrak{t}}^{(j_{N-1})} \mathfrak{t}^{e_Q} f_N(Q) \end{bmatrix} = 0.$$

3.1.2 Order sequence and ramification divisor

Now, the study of the linear series $\mathcal{D}$ at a general point is addressed. For this, let $Q_0 \in \mathcal{X}$ be a fixed element such that $e_{Q_0} = 0$, and let $\mathfrak{t}_0$ be a local parameter at Q_0 . Note that, in particular, $\mathfrak{t}_0$ is a separating variable of $\mathbb{K}(\mathcal{X})$ (see Proposition 1.2.24).

Let $M \geq 0$ be any non-negative integer.

Definition 3.1.8. A *wronskian* on $\mathcal{X}$ is a function of $\mathbb{K}(\mathcal{X})$ of type

$$W_{g_0, \dots, g_M; y}^{k_0, \dots, k_M} := \det \begin{bmatrix} D_y^{(k_0)} g_0 & \cdots & D_y^{(k_0)} g_M \\ \vdots & & \vdots \\ D_y^{(k_M)} g_0 & \cdots & D_y^{(k_M)} g_M \end{bmatrix},$$

where $(k_0, \dots, k_M)$ is a sequence of non-negative integers satisfying $k_0 < \dots < k_M$, $g_0, \dots, g_M \in \mathbb{K}(\mathcal{X})$, and $y \in \mathbb{K}(\mathcal{X})$ is a separating variable.

Definition 3.1.9. If $g_0, \dots, g_M \in \mathbb{K}(\mathcal{X})$ and y is a separating variable of $\mathbb{K}(\mathcal{X})$, then one may define

$$\mathcal{A}(g_0, \dots, g_M; y) := \left\{ (k_0, \dots, k_M) \in \mathbb{N}^{M+1} : k_0 < \dots < k_M \text{ and } W_{g_0, \dots, g_M; y}^{k_0, \dots, k_M} \neq 0 \right\}.$$

Definition 3.1.10. In $\mathbb{N}^{M+1}$, the *lexicographic order* is the partial ordering $<_{\text{lex}}$ given as follows. Let $(k_0, \dots, k_M)$ and $(l_0, \dots, l_M) \in \mathbb{N}^{M+1}$. Then, $(k_0, \dots, k_M) <_{\text{lex}} (l_0, \dots, l_M)$ if in $(l_0 - k_0, \dots, l_M - k_M) \in \mathbb{Z}^{M+1}$ the leftmost nonzero entry is positive.

Proposition 3.1.11. (COX; LITTLE; O'SHEA, 2007, Proposition 4 on Chapter 2). The lexicographic order $<_{\text{lex}}$ in $\mathbb{N}^{M+1}$ is a well-ordering. In particular, every non-empty set in $\mathbb{N}^{M+1}$ has a minimum element with respect to $<_{\text{lex}}$.

Now, consider the wronskians of the form

$$W_{f_0, \dots, f_N; \mathbf{t}_0}^{k_0, \dots, k_N}.$$

Proposition 3.1.12. Let $(j_0, \dots, j_N)$ be the sequence of $(\mathcal{D}, Q_0)$ -orders, where $j_0 = 0$. Then $(j_0, \dots, j_N) \in \mathcal{A}(f_0, \dots, f_N; \mathbf{t}_0)$. In particular, $\mathcal{A}(f_0, \dots, f_N; \mathbf{t}_0)$ has a minimum element with respect to the lexicographic order, namely $(\varepsilon_0, \dots, \varepsilon_N)$, where $\varepsilon_0 = 0$.

Proof. The result follows from Theorem 3.1.6 and Proposition 3.1.11. ■

Proposition 3.1.13. (STÖHR; VOLOCH, 1986, Considerations on Page 5). Let $(\varepsilon_0, \dots, \varepsilon_N)$ be given as in Proposition 3.1.12. Similarly to items 1 and 3 of Theorem 3.1.6, the following occurs.

1. For each $i \geq 1$,

$$\varepsilon_i = \min \left\{ \varepsilon : \begin{array}{l} (D_{\mathbf{t}_0}^{(\varepsilon_0)} f_0, \dots, D_{\mathbf{t}_0}^{(\varepsilon_0)} f_N), \dots, (D_{\mathbf{t}_0}^{(\varepsilon_{i-1})} f_0, \dots, D_{\mathbf{t}_0}^{(\varepsilon_{i-1})} f_N), \\ (D_{\mathbf{t}_0}^{(\varepsilon)} f_0, \dots, D_{\mathbf{t}_0}^{(\varepsilon)} f_N) \text{ are linearly independent over } \mathbb{K}(\mathcal{X}) \end{array} \right\}.$$

2. Let $k_0 < \dots < k_i$ be non-negative integers, with $i \leq N$, such that the vectors

$$(D_{\mathbf{t}_0}^{(k_0)} f_0, \dots, D_{\mathbf{t}_0}^{(k_0)} f_N), \dots, (D_{\mathbf{t}_0}^{(k_i)} f_0, \dots, D_{\mathbf{t}_0}^{(k_i)} f_N)$$

are linearly independent over $\mathbb{K}(\mathcal{X})$. Then $\varepsilon_l \leq k_l$, for each $l \in \{0, \dots, i\}$.

Proposition 3.1.14. (STÖHR; VOLOCH, 1986, Proposition 1.4). Let $(\varepsilon_0, \dots, \varepsilon_N)$ be given as in Proposition 3.1.12.

1. For each $i \in \{0, \dots, N\}$, let $f'_i = \sum_{k=0}^N \alpha_{ik} f_k$, where $(\alpha_{ik}) \in \text{GL}_{N+1}(\mathbb{K})$. Then,

$$W_{f'_0, \dots, f'_N; \mathbf{t}_0}^{\varepsilon_0, \dots, \varepsilon_N} = \det(\alpha_{ik}) W_{f_0, \dots, f_N; \mathbf{t}_0}^{\varepsilon_0, \dots, \varepsilon_N}.$$

2. If $f \in \mathbb{K}(\mathcal{X})$, then

$$W_{f f_0, \dots, f f_N; \mathbf{t}_0}^{\varepsilon_0, \dots, \varepsilon_N} = f^{N+1} W_{f_0, \dots, f_N; \mathbf{t}_0}^{\varepsilon_0, \dots, \varepsilon_N}.$$

3. If $x \in \mathbb{K}(\mathcal{X})$ is another separating variable, then

$$W_{f_0, \dots, f_N; x}^{\varepsilon_0, \dots, \varepsilon_N} = \left(\frac{dt_0}{dx} \right)^{\varepsilon_0 + \dots + \varepsilon_N} W_{f_0, \dots, f_N; t_0}^{\varepsilon_0, \dots, \varepsilon_N}.$$

Remark 3.1.15. Proposition 3.1.14 shows that the sequence $(\varepsilon_0, \dots, \varepsilon_N)$ given in Proposition 3.1.12 depends only on the linear series $\mathcal{D}$. In other words, for each $(\alpha_{ik}) \in \mathrm{GL}_{N+1}(\mathbb{K})$, $f \in \mathbb{K}(\mathcal{X}) \setminus \{0\}$ and $x \in \mathbb{K}(\mathcal{X})$ a separating variable, if $f'_i = \sum_{k=0}^N \alpha_{ik} f f_k$, with $i \in \{0, \dots, N\}$, then

$$\mathcal{A}(f'_0, \dots, f'_N; x) \neq \emptyset,$$

and the minimum with respect to the lexicographic order in $\mathcal{A}(f'_0, \dots, f'_N; x)$ is given by $(\varepsilon_0, \dots, \varepsilon_N)$.

Definition 3.1.16. Let $(\varepsilon_0, \dots, \varepsilon_N)$ be given as in Proposition 3.1.12 and Remark 3.1.15. For each $i \in \{0, \dots, N\}$, ε_i is a $\mathcal{D}$ -order, and the sequence $(\varepsilon_0, \dots, \varepsilon_N)$ is the *sequence of $\mathcal{D}$ -orders*. Further, $\mathcal{D}$ is called *classical* if $(\varepsilon_0, \dots, \varepsilon_N) = (0, \dots, N)$. Otherwise, $\mathcal{D}$ is called *nonclassical*.

From now until the end of this subsection, let us consider the wronskian

$$W_{f_0, \dots, f_N; x}^{\varepsilon_0, \dots, \varepsilon_N},$$

where x is a separating variable of $\mathbb{K}(\mathcal{X})$. Using the local expansion of a function at a local parameter, one can easily obtain the following result.

Lemma 3.1.17. (STÖHR; VOLOCH, 1986, Proof of Theorem 1.5). Let Q be a point of $\mathcal{X}$ such that x is a local parameter at $Q \in \mathcal{X}$ and $e_Q = 0$. If $(j_0, \dots, j_N)$ is the sequence of $(\mathcal{D}, Q)$ -orders, then

$$v_Q(W_{f_0, \dots, f_N; x}^{\varepsilon_0, \dots, \varepsilon_N}) \geq \sum_{i=0}^N (j_i - \varepsilon_i),$$

with the equality holding if and only if

$$\det \left(\binom{j_i}{k} \right) \not\equiv 0 \pmod{p}.$$

If $Q \in \mathcal{X}$ is an arbitrary point, let t be a local parameter at Q . Applying Proposition 3.1.14, one may obtain that

$$\begin{aligned} W_{f_0, \dots, f_N; x}^{\varepsilon_0, \dots, \varepsilon_N} &= \left(\frac{dt}{dx} \right)^{\varepsilon_0 + \dots + \varepsilon_N} W_{f_0, \dots, f_N; t}^{\varepsilon_0, \dots, \varepsilon_N} \\ &= \left(\frac{dt}{dx} \right)^{\varepsilon_0 + \dots + \varepsilon_N} \left(\frac{1}{t^{e_Q}} \right)^{N+1} W_{t^{e_Q} f_0, \dots, t^{e_Q} f_N; t}^{\varepsilon_0, \dots, \varepsilon_N} \end{aligned}$$

and thus

$$v_Q(W_{f_0, \dots, f_N; x}^{\varepsilon_0, \dots, \varepsilon_N}) = -(\varepsilon_0 + \dots + \varepsilon_N)v_Q(\operatorname{div}(dx)) - (N+1)v_Q(E) + v_Q(W_{t^{\varepsilon_Q} f_0, \dots, t^{\varepsilon_Q} f_N; t}^{\varepsilon_0, \dots, \varepsilon_N}),$$

where

$$-\min \left\{ v_Q(t^{\varepsilon_Q} f_0), \dots, v_Q(t^{\varepsilon_Q} f_N) \right\} = 0.$$

Now, it is possible to define the divisor

$$D_{\text{Ram}} := \operatorname{div}(W_{f_0, \dots, f_N; x}^{\varepsilon_0, \dots, \varepsilon_N}) + (\varepsilon_0 + \dots + \varepsilon_N)\operatorname{div}(dx) + (N+1)E.$$

As a consequence of Proposition 3.1.14 and the previous considerations, the following occurs.

Proposition 3.1.18. The divisor D_{Ram} depends only on the linear series $\mathcal{D}$. Further, the multiplicity of D_{Ram} at the point $Q \in \mathcal{X}$ is given by the multiplicity of the wronskian

$$W_{t^{\varepsilon_Q} f_0, \dots, t^{\varepsilon_Q} f_N; t}^{\varepsilon_0, \dots, \varepsilon_N}$$

at Q , where t is a local parameter at Q .

Definition 3.1.19. The divisor D_{Ram} is the *ramification divisor* of $\mathcal{D}$.

From Lemma 3.1.17 and Proposition 3.1.18, the ramification divisor of $\mathcal{D}$ satisfies the following property.

Theorem 3.1.20. (STÖHR; VOLOCH, 1986, Theorem 1.5). If $(j_0, \dots, j_N)$ is the sequence of $(\mathcal{D}, Q)$ -orders, then

$$v_Q(D_{\text{Ram}}) \geq \sum_{i=0}^N (j_i - \varepsilon_i),$$

with the equality holding if and only if

$$\det \left(\binom{j_i}{k} \right) \not\equiv 0 \pmod{p}.$$

Corollary 3.1.21. The ramification divisor D_{Ram} has the following properties:

1. D_{Ram} is an effective divisor.
2. For each $Q \in \mathcal{X}$, $v_Q(D_{\text{Ram}}) = 0$ if and only if $j_i = \varepsilon_i$ for all $i = 0, \dots, N$, where $(j_0, \dots, j_N)$ is the sequence of $(\mathcal{D}, Q)$ -orders. In particular, $(\varepsilon_0, \dots, \varepsilon_N)$ is the sequence of $(\mathcal{D}, Q)$ -orders for almost all points $Q \in \mathcal{X}$.

Definition 3.1.22. A point $Q \in \mathcal{X}$ is a $\mathcal{D}$ -ordinary point if its sequence of $(\mathcal{D}, Q)$ -orders is equal to $(\varepsilon_0, \dots, \varepsilon_N)$. Otherwise, $Q \in \mathcal{X}$ is a $\mathcal{D}$ -Weierstrass point. In particular,

$$\operatorname{Supp}(D_{\text{Ram}}) = \left\{ Q \in \mathcal{X} : Q \text{ is a } \mathcal{D}\text{-Weierstrass point} \right\}.$$

This section ends with the following criterion for the classicality of $\mathcal{D}$.

Proposition 3.1.23. (STÖHR; VOLOCH, 1986, Corollaries 1.7 and 1.8). Let $Q \in \mathcal{X}$ and let $(j_0, \dots, j_N)$ be the sequence of $(\mathcal{D}, Q)$ -orders. If the integer

$$\prod_{i>k} \frac{j_i - j_k}{i - k}$$

is not divisible by p , then $\mathcal{D}$ is classical and

$$v_Q(D_{\text{Ram}}) = \sum_{i=0}^N (j_i - i).$$

In particular, if $p > \mathfrak{d}$ or $p = 0$, then $\mathcal{D}$ is classical.

3.2 The Stöhr-Voloch theorem

Throughout this section, let $p > 0$ be a prime number, let $\mathbb{F}_q$ be the finite field with $q = p^m$ elements and let $\overline{\mathbb{F}_q}$ be the algebraic closure of $\mathbb{F}_q$. Also, let $\mathcal{X}$ be a nonsingular irreducible curve of genus g defined over $\mathbb{F}_q$, let

$$\phi = (f_0 : \dots : f_N) : \mathcal{X} \rightarrow \mathbb{P}^N(\overline{\mathbb{F}_q})$$

be a nondegenerate morphism on $\mathcal{X}$, with $f_0, \dots, f_N \in \mathbb{F}_q(\mathcal{X})$, and let $\mathcal{D}$ be the corresponding base-point-free linear series of dimension N and degree $\mathfrak{d}$, that is, let

$$\begin{aligned} \mathcal{D} &= \left\{ \operatorname{div} \left(\sum_{i=0}^N \alpha_i f_i \right) + E : (\alpha_0 : \dots : \alpha_N) \in \mathbb{P}^N(\overline{\mathbb{F}_q}) \right\} \\ &= \left\{ \phi^*(\Delta) : \Delta \text{ is a hyperplane in } \mathbb{P}^N(\overline{\mathbb{F}_q}) \right\}, \end{aligned}$$

where $E = \sum_{Q \in \mathcal{X}} e_Q Q$ is defined by

$$e_Q := -\min \left\{ v_Q(f_0), \dots, v_Q(f_N) \right\}$$

and $\phi^*(\Delta) = \operatorname{div} \left(\sum_{i=0}^N \alpha_i f_i \right) + E$ is the pullback of the hyperplane $\Delta : \sum_{i=0}^N \alpha_i X_i = 0$ by ϕ . Note here that E and $\mathcal{D}$ are defined over $\mathbb{F}_q$.

In order to obtain an upper bound for the number of $\mathbb{F}_q$ -rational points on $\mathcal{X}$, one may consider the possibly larger set of all points $Q \in \mathcal{X}$ such that the image of $\phi(Q)$ under the Frobenius map of $\mathbb{P}^N(\overline{\mathbb{F}_q})$ is in the osculating hyperplane $L_{N-1}(Q)$ at Q . From Corollary 3.1.7, a point $Q \in \mathcal{X}$ with $e_Q = 0$ is in this set if and only if

$$\det \begin{bmatrix} f_0(Q)^q & \cdots & f_N(Q)^q \\ D_t^{(j_0)} f_0(Q) & \cdots & D_t^{(j_0)} f_N(Q) \\ \vdots & & \vdots \\ D_t^{(j_{N-1})} f_0(Q) & \cdots & D_t^{(j_{N-1})} f_N(Q) \end{bmatrix} = 0,$$

where t is a local parameter at Q .

Thus, if $x \in \overline{\mathbb{F}_q}(\mathcal{X})$ is a separating variable, then one is lead to study determinants of the form

$$\det \begin{bmatrix} f_0^q & \cdots & f_N^q \\ D_x^{(k_0)} f_0 & \cdots & D_x^{(k_0)} f_N \\ \vdots & & \vdots \\ D_x^{(k_{N-1})} f_0 & \cdots & D_x^{(k_{N-1})} f_N \end{bmatrix},$$

where $k_0 < \cdots < k_{N-1}$ are non-negative integers.

Thus, let $M \geq 0$ be a non-negative integer.

Definition 3.2.1. If $(k_0, \dots, k_{M-1})$ is a sequence of non-negative integers satisfying $k_0 < \cdots < k_{M-1}$, $g_0, \dots, g_M \in \overline{\mathbb{F}_q}(\mathcal{X})$, and $y \in \overline{\mathbb{F}_q}(\mathcal{X})$ is a separating variable, define

$$W_y^{k_0, \dots, k_{M-1}}(g_0, \dots, g_M) := \det \begin{bmatrix} g_0^q & \cdots & g_M^q \\ D_y^{(k_0)} g_0 & \cdots & D_y^{(k_0)} g_M \\ \vdots & & \vdots \\ D_y^{(k_{M-1})} g_0 & \cdots & D_y^{(k_{M-1})} g_M \end{bmatrix}.$$

Definition 3.2.2. If $g_0, \dots, g_M \in \overline{\mathbb{F}_q}(\mathcal{X})$ and y is a separating variable of $\overline{\mathbb{F}_q}(\mathcal{X})$, then one may define

$$\mathcal{B}(g_0, \dots, g_M; y) := \left\{ (k_0, \dots, k_{M-1}) \in \mathbb{N}^M : k_0 < \cdots < k_{M-1} \text{ and } W_y^{k_0, \dots, k_{M-1}}(g_0, \dots, g_M) \neq 0 \right\}.$$

Proposition 3.2.3. (STÖHR; VOLOCH, 1986, Proposition 2.1). Considering the previous notation, $\mathcal{B}(f_0, \dots, f_N; x) \neq \emptyset$. Therefore, in terms of Proposition 3.1.11, let $(v_0, \dots, v_{N-1})$ be the minimum of $\mathcal{B}(f_0, \dots, f_N; x)$ with respect to the lexicographic order. Then there exists an integer $i \in \{1, \dots, N\}$ such that

$$v_k = \begin{cases} \varepsilon_k, & \text{if } k < i \\ \varepsilon_{k+1}, & \text{otherwise} \end{cases},$$

where $(\varepsilon_0, \dots, \varepsilon_N)$ is the sequence of $\mathcal{D}$ -orders.

Proposition 3.2.4. (STÖHR; VOLOCH, 1986, Considerations on Page 9). Let $(v_0, \dots, v_{N-1})$ be given as in Proposition 3.2.3 and let $k_0 < \cdots < k_i$ be non-negative integers, with $i \leq N-1$, such that the vectors

$$(f_0^q, \dots, f_N^q), (D_x^{(k_0)} f_0, \dots, D_x^{(k_0)} f_N), \dots, (D_x^{(k_i)} f_0, \dots, D_x^{(k_i)} f_N)$$

are linearly independent over $\overline{\mathbb{F}_q}(\mathcal{X})$. Then $v_l \leq k_l$, for each $l \in \{0, \dots, i\}$.

Similarly to Proposition 3.1.14, the following holds.

Proposition 3.2.5. (STÖHR; VOLOCH, 1986, Proposition 2.2). Let $(v_0, \dots, v_{N-1})$ be given as in Proposition 3.2.3.

1. For each $i \in \{0, \dots, N\}$, let $f'_i = \sum_{k=0}^N \alpha_{ik} f_k$, where $(\alpha_{ik}) \in \text{GL}_{N+1}(\mathbb{F}_q)$. Then,

$$W_x^{v_0, \dots, v_{N-1}}(f'_0, \dots, f'_N) = \det(\alpha_{ik}) W_x^{v_0, \dots, v_{N-1}}(f_0, \dots, f_N).$$

2. If $f \in \overline{\mathbb{F}_q}(\mathcal{X})$, then

$$W_x^{v_0, \dots, v_{N-1}}(f f_0, \dots, f f_N) = f^{N+q} W_x^{v_0, \dots, v_{N-1}}(f_0, \dots, f_N).$$

3. If $x' \in \overline{\mathbb{F}_q}(\mathcal{X})$ is another separating variable, then

$$W_{x'}^{v_0, \dots, v_{N-1}}(f_0, \dots, f_N) = \left(\frac{dx}{dx'} \right)^{v_0 + \dots + v_{N-1}} W_x^{v_0, \dots, v_{N-1}}(f_0, \dots, f_N).$$

Corollary 3.2.6. The sequence $(v_0, \dots, v_{N-1})$ given in Proposition 3.2.3 depends only on the linear series $\mathcal{D}$ and on q .

Therefore, it is possible to establish the following definition.

Definition 3.2.7. Let $(v_0, \dots, v_{N-1})$ be given as in Proposition 3.2.3. For each $i \in \{0, \dots, N-1\}$, v_i is a $\mathbb{F}_q$ -Frobenius order of $\mathcal{D}$, and the sequence $(v_0, \dots, v_{N-1})$ is the sequence of $\mathbb{F}_q$ -Frobenius orders of $\mathcal{D}$. Further, $\mathcal{D}$ is called $\mathbb{F}_q$ -Frobenius classical if $(v_0, \dots, v_{N-1}) = (0, \dots, N-1)$. Otherwise, $\mathcal{D}$ is called $\mathbb{F}_q$ -Frobenius nonclassical.

Now, defining the divisor

$$D_{SV} := \text{div}(W_x^{v_0, \dots, v_{N-1}}(f_0, \dots, f_N)) + (v_0 + \dots + v_{N-1})\text{div}(dx) + (N+q)E$$

of degree

$$(v_0 + \dots + v_{N-1})(2g-2) + (N+q)d,$$

as a consequence of Proposition 3.2.5, the following result occurs.

Proposition 3.2.8. The divisor D_{SV} depends only on the linear series $\mathcal{D}$ and on q . Further, the multiplicity of D_{SV} at a point $Q \in \mathcal{X}$ is given by the multiplicity of the function

$$W_t^{v_0, \dots, v_{N-1}}(t^{e_Q} f_0, \dots, t^{e_Q} f_N)$$

at Q , where $t \in \overline{\mathbb{F}_q}(\mathcal{X})$ is a local parameter at Q . In particular, D_{SV} is an effective divisor and the following holds:

1. Let $Q \in \mathcal{X}$ be such that its sequence of $(\mathcal{D}, Q)$ -orders $(j_0, \dots, j_N)$ satisfies $(j_0, \dots, j_{N-1}) = (v_0, \dots, v_{N-1})$. Then $Q \in \text{Supp}(D_{SV})$ if and only if the image of $\phi(Q)$ under the Frobenius map of $\mathbb{P}^N(\overline{\mathbb{F}_q})$ is contained in the osculating hyperplane at Q .

2. Let $Q \in \mathcal{X}$ be such that its sequence of $(\mathcal{D}, Q)$ -orders $(j_0, \dots, j_N)$ satisfies $v_i < j_i$. Then $Q \in \text{Supp}(D_{\text{SV}})$.
3. Every $\mathbb{F}_q$ -rational point of $\mathcal{X}$ is in the support of D_{SV} .

Definition 3.2.9. The divisor D_{SV} is the *Stöhr-Voloch divisor* of $\mathcal{D}$.

Using the local expansion of a function at a local parameter, one can obtain the following result.

Proposition 3.2.10. (STÖHR; VOLOCH, 1986, Proposition 2.4). For $Q \in \mathcal{X}$, let $(j_0, \dots, j_N)$ be its sequence of $(\mathcal{D}, Q)$ -orders.

1. If Q is a $\mathbb{F}_q$ -rational point of $\mathcal{X}$, then

$$v_Q(D_{\text{SV}}) \geq \sum_{i=1}^N (j_i - v_{i-1}),$$

with the equality holding if and only if

$$\det \left(\begin{pmatrix} j_i \\ v_k \end{pmatrix} \right)_{\substack{1 \leq i \leq N \\ 0 \leq k \leq N-1}} \not\equiv 0 \pmod{p}.$$

2. If Q is an arbitrary point of $\mathcal{X}$, then

$$v_Q(D_{\text{SV}}) \geq \sum_{i=1}^{N-1} (j_i - v_i),$$

with the strictly inequality holding if

$$\det \left(\begin{pmatrix} j_i \\ v_k \end{pmatrix} \right)_{\substack{0 \leq i \leq N-1 \\ 0 \leq k \leq N-1}} \not\equiv 0 \pmod{p}.$$

Proposition 3.2.11. (STÖHR; VOLOCH, 1986, Corollary 2.6). If Q is a $\mathbb{F}_q$ -rational point of $\mathcal{X}$ and $(j_0, \dots, j_N)$ is its sequence of $(\mathcal{D}, Q)$ -orders, then

$$v_Q(D_{\text{SV}}) \geq N j_1.$$

As a consequence, one may obtain the following upper bound for the number $N_q(\mathcal{X})$ of $\mathbb{F}_q$ -rational points on $\mathcal{X}$, which is a refinement of (STÖHR; VOLOCH, 1986, Theorem 2.13) obtained from some remarks at the beginning of (STÖHR; VOLOCH, 1986, Section 3).

Theorem 3.2.12 (Stöhr-Voloch).

$$N_q(\mathcal{X}) \leq \frac{(v_0 + \dots + v_{N-1})(2g - 2) + (N + q)d - \sum A(Q)}{N},$$

where

$$A(Q) = \begin{cases} \sum_{i=1}^N (j_i(Q) - v_{i-1}) - N, & \text{if } Q \text{ is a } \mathbb{F}_q \text{ rational point on } \mathcal{X} \\ \sum_{i=0}^{N-1} (j_i(Q) - v_i), & \text{otherwise.} \end{cases}$$

Finally, this section ends with the following criterion for the $\mathbb{F}_q$ -Frobenius classicality of $\mathcal{D}$.

Proposition 3.2.13. (STÖHR; VOLOCH, 1986, Corollary 2.7). Let Q be an $\mathbb{F}_q$ -rational point on $\mathcal{X}$ and let $(j_0, \dots, j_N)$ be the sequence of $(\mathcal{D}, Q)$ -orders. If the integer

$$\prod_{i>k} \frac{j_i - j_k}{i - k}$$

is not divisible by p , then $\mathcal{D}$ is $\mathbb{F}_q$ -Frobenius classical and

$$v_Q(D_{\text{SV}}) = N + \sum_{i=1}^N (j_i - i).$$

In particular, if $p > \mathfrak{d}$, then $\mathcal{D}$ is $\mathbb{F}_q$ -Frobenius classical.

Part II

Three topics in algebraic curves over finite fields

PLANE SECTIONS OF FERMAT SURFACES OVER FINITE FIELDS

The present chapter is an adapted version of (BORGES; COOK; COUTINHO, 2018). Here, in some excerpts, further details and explanations are provided.

4.1 Introduction

Let F be the plane curve obtained by the intersection of the Fermat surface

$$S : X_0^d + X_1^d + X_2^d + X_3^d = 0$$

with the plane

$$P : X_3 - e_0X_0 - e_1X_1 - e_2X_2 = 0,$$

where d is a positive integer, $e_0, e_1, e_2 \in \mathbb{F}_q$, and $\mathbb{F}_q$ is the finite field with $q = p^m$ elements, for a prime number p . In other words, let

$$F : X_0^d + X_1^d + X_2^d + (e_0X_0 + e_1X_1 + e_2X_2)^d = 0. \quad (4.1)$$

Characterizing this general plane curve in terms of its rational points and its irreducible and nonsingular components presents many challenges. For instance, the case $p = 2$ and $e_0 = e_1 = e_2 = 1$ has been extensively investigated over the past decades (see (van LINT; WILSON, 1986), (JANWA; WILSON, 1993), (JANWA; MCGUIRE; WILSON, 1995) and (HERNANDO; MCGUIRE, 2011)), where in particular the following result was essential in Hernando and McGuire's proof of an important conjecture regarding exceptional numbers.

Theorem. (HERNANDO; MCGUIRE, 2011). The polynomial

$$\frac{X_0^d + X_1^d + X_2^d + (X_0 + X_1 + X_2)^d}{(X_0 + X_1)(X_0 + X_2)(X_1 + X_2)}$$

has an absolutely irreducible factor defined over $\mathbb{F}_2$ for all d not of the form $d = 2^i + 1$ or $d = 2^{2i} - 2^i + 1$.

In this chapter, the problem of studying the plane curve given in (4.1) is considered from a somewhat different point of view. Based on techniques developed by Carlin and Voloch in (CARLIN; VOLOCH, 2004), the plane curve

$$\mathcal{C} : C(X_0, X_1, X_2) = X_0^d + X_1^d + X_2^d + (e_0X_0 + e_1X_1 + e_2X_2)^d = 0, \quad (4.2)$$

is characterized in cases where $q = p^m = 2d + 1$ is a prime power, $p > 3$, and e_0, e_1 and e_2 are arbitrary elements in $\mathbb{F}_q$. More precisely, a complete description of its irreducible and nonsingular components is given, and also their number of $\mathbb{F}_q$ -rational points is provided. Consequently, a family of plane curves attaining the Stöhr-Voloch bound is constructed and the following theorem, which is the main result of this chapter, is proved.

Theorem 4.1.1. If $\mathcal{C}$ is not the union of d lines, then the following statements hold.

1. $\mathcal{C}$ is the union of $n \in \{0, 1, 2, 3\}$ lines defined over $\mathbb{F}_q$ and a nonsingular classical plane curve $\mathcal{F}$ of degree d .
2. The possibilities for the number of $\mathbb{F}_q$ -rational points on $\mathcal{F}$ are

$$\frac{1}{2}d(d + q - 1) - \frac{1}{2}i(d - 2),$$

with $i \in \{0, 1, 2, 3, d, 3d\}$. In particular, $\mathcal{F}$ meets the Stöhr-Voloch bound in (4.7).

It is worth mentioning that few examples of curves attaining the Stöhr-Voloch bound are known. Such explicit constructions are of interest in areas such as finite geometry and coding theory.

This chapter is organized as follows. In Section 4.4, the $\mathbb{F}_q$ -points and linear components of $\mathcal{C}$ are detailed. In particular, it is shown that if $\mathcal{C}$ is not the union of d lines, then

$$C(X_0, X_1, X_2) = (e_0X_0 + e_1X_1)^{i_0}(e_0X_0 + e_2X_2)^{i_1}(e_1X_1 + e_2X_2)^{i_2}F(X_0, X_1, X_2),$$

where $i_0, i_1, i_2 \in \{0, 1\}$ and $F(X_0, X_1, X_2)$ has no linear factors. In Section 4.5, it is shown that the plane curve $\mathcal{F} : F(X_0, X_1, X_2) = 0$ is $\mathbb{F}_q$ -disjoint from any linear component of $\mathcal{C}$. These facts are used to prove Theorem 4.1.1, which relies on important results obtained in (STÖHR; VOLOCH, 1986), (VILLEGAS; VOLOCH, 1999) and (CARLIN; VOLOCH, 2004). Full details are given in Subsection 4.6.1.

4.2 Notation

The following notation is used throughout this chapter.

- Here, $\mathbb{F}_q \setminus \{0\}$ is denoted by $\mathbb{F}_q^*$.

- The set of points of $\mathbb{P}^2(\mathbb{F}_q)$ on a plane curve $\mathcal{G}$ defined over $\mathbb{F}_q$ is denoted by $\mathcal{G}(\mathbb{F}_q)$ and its cardinality is denoted by $\#\mathcal{G}(\mathbb{F}_q)$.
- The quadratic character of $\mathbb{F}_q$ is denoted by η . That is,

$$\eta(\alpha) = \begin{cases} 1, & \text{if } \alpha \text{ is a nonzero square} \\ 0, & \text{if } \alpha = 0 \\ -1, & \text{if } \alpha \text{ is a non-square,} \end{cases}$$

for all $\alpha \in \mathbb{F}_q$. In particular, since $d = \frac{q-1}{2}$, it follows that $\eta(\alpha) = \alpha^d$, for all $\alpha \in \mathbb{F}_q$.

- The notation $\{\eta(e_0), \eta(e_1), \eta(e_2)\} = \{0, 1, 1\}$ means that two of the values $\eta(e_0), \eta(e_1), \eta(e_2)$ are equal to 1 and one is equal to 0; similarly for the other cases.
- The points $(1 : 0 : 0)$, $(0 : 1 : 0)$ and $(0 : 0 : 1)$ in $\mathbb{P}^2(\mathbb{F}_q)$ are denoted by P_0, P_1 and P_2 , respectively. The points $(-e_1 : e_0 : 0)$, $(-e_2 : 0 : e_0)$ and $(0 : -e_2 : e_1)$ are denoted by $P_{01} = P_{10}$, $P_{02} = P_{20}$ and $P_{12} = P_{21}$, respectively.
- The sets

$$\left\{ (0 : \alpha_1 : 1) \in \mathbb{P}^2(\mathbb{F}_q) : \eta(\alpha_1) = -1 \right\},$$

$$\left\{ (\alpha_0 : 0 : 1) \in \mathbb{P}^2(\mathbb{F}_q) : \eta(\alpha_0) = -1 \right\}$$

and

$$\left\{ (\alpha_0 : 1 : 0) \in \mathbb{P}^2(\mathbb{F}_q) : \eta(\alpha_0) = -1 \right\}$$

are denoted by $\mathcal{A}_0, \mathcal{A}_1$ and $\mathcal{A}_2$, respectively.

4.3 Rudiments of the Stöhr-Voloch theory

In this section, some notions and basic facts from the Stöhr-Voloch theory are presented. We believe the results here are well known by the specialists. Nevertheless, as some of them are not explicitly stated in the literature, their proofs are provided.

Definition 4.3.1. For any homogeneous polynomial $A(X_0, X_1, X_2) \in \mathbb{F}_q[X_0, X_1, X_2]$, consider the polynomial

$$\Phi_q(A) := X_0^q \frac{\partial A}{\partial X_0} + X_1^q \frac{\partial A}{\partial X_1} + X_2^q \frac{\partial A}{\partial X_2}. \quad (4.3)$$

An absolutely irreducible plane curve $\mathcal{G} : G(X_0, X_1, X_2) = 0$ defined over $\mathbb{F}_q$ is called $\mathbb{F}_q$ -Frobenius nonclassical if

$$G \mid \Phi_q(G). \quad (4.4)$$

Otherwise, $\mathcal{G}$ is called $\mathbb{F}_q$ -Frobenius classical.

Note that (4.4) has a geometric meaning: the Frobenius map $P \mapsto P^q$ takes each nonsingular point $P \in \mathcal{G}$ to the tangent line to $\mathcal{G}$ at P .

The following result, which is important to prove the absolute irreducibility of $\mathcal{F}$, is based essentially on (CARLIN; VOLOCH, 2004, Theorem 1).

Theorem 4.3.2. Let $\mathcal{G}$ be a plane curve of degree $\mathfrak{d}$ defined over $\mathbb{F}_q$. If all absolutely irreducible components of $\mathcal{G}$ defined over $\mathbb{F}_q$ are $\mathbb{F}_q$ -Frobenius classical, then

$$\#\mathcal{G}(\mathbb{F}_q) \leq \frac{\mathfrak{d}(\mathfrak{d} + q - 1)}{2}.$$

Moreover, if $\#\mathcal{G}(\mathbb{F}_q) \geq \frac{\mathfrak{d}(\mathfrak{d} + q - 1)}{2} - \max\{\mathfrak{d} - 1, 2\mathfrak{d} - 5\}$, then $\mathcal{G}$ is absolutely irreducible.

Proof. Let $\mathcal{G}_1, \dots, \mathcal{G}_l$ be the (irreducible but not necessarily absolutely irreducible) components of $\mathcal{G}$ defined over $\mathbb{F}_q$, and let $\mathfrak{d}_i$ be the degree of $\mathcal{G}_i$. By hypothesis, $\mathfrak{d}_i > 1$ for all i (since the condition ‘all absolutely irreducible components of $\mathcal{G}$ defined over $\mathbb{F}_q$ are $\mathbb{F}_q$ -Frobenius classical’ implies in particular that $\mathcal{G}_i$ is not a line). If $\mathcal{G}_i$ is absolutely irreducible, then Theorem 3.0.1 yields

$$\#\mathcal{G}_i(\mathbb{F}_q) \leq \mathfrak{d}_i(\mathfrak{d}_i + q - 1)/2. \quad (4.5)$$

On the other hand, from (VILLEGAS; VOLOCH, 1999, Lemma 3.3), if $\mathcal{G}_i$ is not absolutely irreducible, then $\#\mathcal{G}_i(\mathbb{F}_q) \leq \mathfrak{d}_i^2/4$. Since $\mathfrak{d}_i^2/4 < \mathfrak{d}_i(\mathfrak{d}_i + q - 1)/2$, the bound (4.5) is also obtained in cases where $\mathcal{G}_i$ is not absolutely irreducible. Now

$$\#\mathcal{G}(\mathbb{F}_q) \leq \sum \#\mathcal{G}_i(\mathbb{F}_q) \leq \sum \mathfrak{d}_i(\mathfrak{d}_i + q - 1)/2. \quad (4.6)$$

From $\sum \mathfrak{d}_i = \mathfrak{d}$,

$$\sum \mathfrak{d}_i(\mathfrak{d}_i + q - 1)/2 = \sum \mathfrak{d}(\mathfrak{d} + q - 1)/2 - \sum_{i < k} \mathfrak{d}_i \mathfrak{d}_k,$$

which combined with (4.6) gives the first statement of the theorem.

To prove the second statement, suppose that $\mathcal{G}$ is not absolutely irreducible. If $l > 1$, then assume without loss of generality that $\mathfrak{d}_1 \leq \mathfrak{d}_i$, for all $i > 1$. It follows that

$$\sum_{i < k} \mathfrak{d}_i \mathfrak{d}_k \geq \mathfrak{d}_1(\mathfrak{d}_2 + \dots + \mathfrak{d}_l) \geq 2(\mathfrak{d}_2 + \dots + \mathfrak{d}_l) \geq \mathfrak{d}_1 + \dots + \mathfrak{d}_l = \mathfrak{d}$$

and that

$$\sum_{i < k} \mathfrak{d}_i \mathfrak{d}_k \geq \mathfrak{d}_1(\mathfrak{d}_1 + \dots + \mathfrak{d}_l) - \mathfrak{d}_1 \mathfrak{d}_1 = \mathfrak{d}_1 \mathfrak{d} - \mathfrak{d}_1^2 \geq 2\mathfrak{d} - 4,$$

where the last inequality follows from the fact that $\mathfrak{d}_1^2 - \mathfrak{d}_1 \mathfrak{d} + 2\mathfrak{d} - 4 \leq 0$ for $2 \leq \mathfrak{d}_1 \leq \mathfrak{d} - 2$. If $l = 1$, then $\mathcal{G}$ is irreducible but not absolutely irreducible and, again by (VILLEGAS; VOLOCH, 1999, Lemma 3.3), $\#\mathcal{G}(\mathbb{F}_q) \leq \mathfrak{d}^2/4$. This implies that $\#\mathcal{G}(\mathbb{F}_q) \leq \frac{\mathfrak{d}(\mathfrak{d} + q - 1)}{2} - \mathfrak{d}$ unless $q = 2$ and $\mathfrak{d} = 1$, case in which $\mathcal{G}$ is absolutely irreducible, a contradiction with the hypothesis. Also, this implies that $\#\mathcal{G}(\mathbb{F}_q) \leq \frac{\mathfrak{d}(\mathfrak{d} + q - 1)}{2} - (2\mathfrak{d} - 4)$, which completes the proof. ■

Finally, the proofs of the nonsingularity and the classicality of $\mathcal{F}$ are based on Theorems 4.3.3 and 4.3.4, which are slightly adapted versions of Theorem 3.0.1 and (HIRSCHFELD; KORCHMÁROS, 2001, Theorem 1.3), respectively.

Theorem 4.3.3. Let $\mathcal{G} : G(X_0, X_1, X_2) = 0$ be an $\mathbb{F}_q$ -Frobenius classical plane curve of degree $\mathfrak{d}$ and let $\tilde{P}_1, \dots, \tilde{P}_k$ be the distinct inflection points of $\mathcal{G}$ defined over $\mathbb{F}_q$. If $\mathcal{T}_{\tilde{P}_i}$ is the tangent line to $\mathcal{G}$ at $\tilde{P}_i$ and $j_2^{(i)} = I(\tilde{P}_i, \mathcal{G} \cap \mathcal{T}_{\tilde{P}_i}) \geq 3$ is the intersection multiplicity of $\mathcal{G}$ and $\mathcal{T}_{\tilde{P}_i}$ at $\tilde{P}_i$, for $i = 1, \dots, k$, then

$$\#\mathcal{G}(\mathbb{F}_q) \leq \frac{\mathfrak{d}(\mathfrak{d} + q - 1) - \sum_{i=1}^k (j_2^{(i)} - 2)}{2}. \quad (4.7)$$

Moreover, if equality holds in (4.7), then $\mathcal{G}$ is nonsingular.

Proof. Let $\mathcal{H} : \Phi_q(G) = 0$. Since $\mathcal{G}$ is $\mathbb{F}_q$ -Frobenius classical, from Bézout's Theorem (see Theorem 1.1.36) one may have

$$\sum_{P \in \mathcal{G} \cap \mathcal{H}} I(P, \mathcal{G} \cap \mathcal{H}) = \mathfrak{d}(\mathfrak{d} + q - 1).$$

Also, from Euler's Formula,

$$\mathfrak{d} G(X_0, X_1, X_2) = X_0 \frac{\partial G}{\partial X_0} + X_1 \frac{\partial G}{\partial X_1} + X_2 \frac{\partial G}{\partial X_2} \quad (4.8)$$

and therefore $\mathcal{G}(\mathbb{F}_q) \subseteq \mathcal{H}(\mathbb{F}_q)$, which implies that

$$\sum_{P \in \mathcal{G}(\mathbb{F}_q)} I(P, \mathcal{G} \cap \mathcal{H}) \leq \sum_{P \in \mathcal{G} \cap \mathcal{H}} I(P, \mathcal{G} \cap \mathcal{H}) = \mathfrak{d}(\mathfrak{d} + q - 1). \quad (4.9)$$

In order to complete the proof, the left side of the above inequality needs to be analyzed, which is done in two steps.

Step 1: $I(P, \mathcal{G} \cap \mathcal{H}) \geq 2$, for all $P \in \mathcal{G}(\mathbb{F}_q)$. Moreover, if $P \in \mathcal{G}(\mathbb{F}_q)$ is a singular point of $\mathcal{G}$, then the strict inequality holds, that is, $I(P, \mathcal{G} \cap \mathcal{H}) > 2$.

Proof of Step 1.

First, for each $i \in \{0, 1, 2\}$,

$$\begin{aligned} \frac{\partial \Phi_q(G)}{\partial X_i} &= qX_i^{q-1} \frac{\partial G}{\partial X_i} + X_0^q \frac{\partial^2 G}{\partial X_0 \partial X_i} + X_1^q \frac{\partial^2 G}{\partial X_1 \partial X_i} + X_2^q \frac{\partial^2 G}{\partial X_2 \partial X_i} \\ &= X_0^q \frac{\partial^2 G}{\partial X_i \partial X_0} + X_1^q \frac{\partial^2 G}{\partial X_i \partial X_1} + X_2^q \frac{\partial^2 G}{\partial X_i \partial X_2} \\ &= \Phi_q \left(\frac{\partial G}{\partial X_i} \right), \end{aligned}$$

and so, if $P \in \mathcal{G}(\mathbb{F}_q) \subseteq \mathcal{H}(\mathbb{F}_q)$, then

$$\left. \frac{\partial \Phi_q(G)}{\partial X_i} \right|_P = (\mathfrak{d} - 1) \left. \frac{\partial G}{\partial X_i} \right|_P$$

by Euler's Formula applied to $\frac{\partial G}{\partial X_i}$. In particular, if $P \in \mathcal{G}(\mathbb{F}_q) \subseteq \mathcal{H}(\mathbb{F}_q)$ is a singular point of $\mathcal{G}$, then P is also a singular point of $\mathcal{H}$, and, by Theorem 1.1.35,

$$I(P, \mathcal{G} \cap \mathcal{H}) \geq m_P^{\mathcal{G}} m_P^{\mathcal{H}} \geq 2 \cdot 2 = 4 > 2,$$

where $m_P^{\mathcal{G}}$ and $m_P^{\mathcal{H}}$ are the multiplicities of P at $\mathcal{G}$ and $\mathcal{H}$, respectively. Further, if $P \in \mathcal{G}(\mathbb{F}_q) \subseteq \mathcal{H}(\mathbb{F}_q)$ is a nonsingular point of $\mathcal{G}$, then either P is a singular point of $\mathcal{H}$ (if $p \mid (d-1)$) or P is a nonsingular point of $\mathcal{H}$ (if $p \nmid (d-1)$) and the tangent line to $\mathcal{H}$ at P coincides with the tangent line to $\mathcal{G}$ at P . Therefore, in both circumstances

$$I(P, \mathcal{G} \cap \mathcal{H}) \geq 2,$$

which completes the proof of Step 1. □

Step 2: $I(\tilde{P}_i, \mathcal{G} \cap \mathcal{H}) \geq j_2^{(i)}$, for all $i = 1, \dots, k$.

Proof of Step 2.

Consider $i \in \{1, \dots, k\}$. From a particular case of (ARAKELIAN; BORGES, 2017, Lemma 3.3), the result of this step follows provided that $I(\tilde{P}_i, \mathcal{H} \cap \mathcal{T}_{\tilde{P}_i}) \geq j_2^{(i)}$.

In order to simplify the notation, define $P := \tilde{P}_i$ and $j_2 := j_2^{(i)}$, and write $\mathcal{T}_P : L(X_0, X_1, X_2) = 0$. Also, without loss of generality, suppose that $P = (\alpha_0 : \alpha_1 : 1)$, with $\alpha_0, \alpha_1 \in \mathbb{F}_q$.

First, note that if $p \mid d$, then

$$I(P, \mathcal{H} \cap \mathcal{T}_P) = I(P, \tilde{\mathcal{H}} \cap \mathcal{T}_P),$$

and if $p \nmid d$, then

$$I(P, \mathcal{H} \cap \mathcal{T}_P) \geq \min \left\{ I(P, \mathcal{G} \cap \mathcal{T}_P), I(P, \tilde{\mathcal{H}} \cap \mathcal{T}_P) \right\},$$

where $\tilde{\mathcal{H}} : H(X_0, X_1, X_2) = (X_0^q - X_0 X_2^{q-1}) \frac{\partial G}{\partial X_0} + (X_1^q - X_1 X_2^{q-1}) \frac{\partial G}{\partial X_1} = 0$. Indeed, by Euler's Formula (4.8)

$$\begin{aligned} \Phi_q(G) &= X_0^q \frac{\partial G}{\partial X_0} + X_1^q \frac{\partial G}{\partial X_1} + X_2^q \frac{\partial G}{\partial X_2} \\ &= X_0^q \frac{\partial G}{\partial X_0} + X_1^q \frac{\partial G}{\partial X_1} + X_2^{q-1} X_2 \frac{\partial G}{\partial X_2} \\ &= X_0^q \frac{\partial G}{\partial X_0} + X_1^q \frac{\partial G}{\partial X_1} + X_2^{q-1} \left(dG(X_0, X_1, X_2) - X_0 \frac{\partial G}{\partial X_0} - X_1 \frac{\partial G}{\partial X_1} \right) \\ &= (X_0^q - X_0 X_2^{q-1}) \frac{\partial G}{\partial X_0} + (X_1^q - X_1 X_2^{q-1}) \frac{\partial G}{\partial X_1} + dX_2^{q-1} G(X_0, X_1, X_2). \end{aligned}$$

Therefore, one needs to show that

$$I(P, \tilde{\mathcal{H}} \cap \mathcal{T}_P) \geq j_2.$$

Writing

$$\begin{aligned} G_*(X_0 + \alpha_0, X_1 + \alpha_1) &= G(X_0 + \alpha_0, X_1 + \alpha_1, 1) \\ &= G_1(X_0, X_1) + G_2(X_0, X_1) + \cdots + G_d(X_0, X_1), \end{aligned}$$

where $G_l(X_0, X_1)$ is a homogeneous polynomial of degree l for each $l \in \{1, 2, \dots, d\}$, and

$$H_*(X_0, X_1) = H(X_0, X_1, 1) = (X_0^q - X_0) \frac{\partial G_*}{\partial X_0} + (X_1^q - X_1) \frac{\partial G_*}{\partial X_1},$$

since $\alpha_0, \alpha_1 \in \mathbb{F}_q$, it follows that

$$\begin{aligned} H_*(X_0 + \alpha_0, X_1 + \alpha_1) &= (X_0^q - X_0) \frac{\partial G_1}{\partial X_0} + (X_1^q - X_1) \frac{\partial G_1}{\partial X_1} + \\ &+ (X_0^q - X_0) \frac{\partial G_2}{\partial X_0} + (X_1^q - X_1) \frac{\partial G_2}{\partial X_1} + \\ &\cdots \\ &+ (X_0^q - X_0) \frac{\partial G_d}{\partial X_0} + (X_1^q - X_1) \frac{\partial G_d}{\partial X_1}. \end{aligned}$$

Now, applying Euler's Formula to $G_l(X_0, X_1)$ for each $l \in \{1, 2, \dots, d\}$,

$$\begin{aligned} H_*(X_0 + \alpha_0, X_1 + \alpha_1) &= -1 \cdot G_1(X_0, X_1) - 2 \cdot G_2(X_0, X_1) - \cdots - d \cdot G_d(X_0, X_1) + \\ &+ X_0^q \frac{\partial G_1}{\partial X_0} + X_1^q \frac{\partial G_1}{\partial X_1} + \\ &+ X_0^q \frac{\partial G_2}{\partial X_0} + X_1^q \frac{\partial G_2}{\partial X_1} + \\ &\cdots \\ &+ X_0^q \frac{\partial G_d}{\partial X_0} + X_1^q \frac{\partial G_d}{\partial X_1}. \end{aligned}$$

By Remark 1.1.33, $L_*(X_0 + \alpha_0, X_1 + \alpha_1) \mid G_l(X_0, X_1)$, for all $1 \leq l < j_2$, and $L_*(X_0 + \alpha_0, X_1 + \alpha_1) \nmid G_{j_2}(X_0, X_1)$.

If the homogeneous components of degree l of $H_*(X_0 + \alpha_0, X_1 + \alpha_1)$ are exactly of the form $-l \cdot G_l(X_0, X_1)$, for all $1 \leq l < j_2$, then the result follows by applying the above considerations and Remark 1.1.33 to the polynomial $H_*(X_0 + \alpha_0, X_1 + \alpha_1)$.

On the other hand, if the homogeneous component of degree l of $H_*(X_0 + \alpha_0, X_1 + \alpha_1)$ is of the form $-l \cdot G_l(X_0, X_1) + X_0^q \frac{\partial G_{l_1}}{\partial X_0} + X_1^q \frac{\partial G_{l_1}}{\partial X_1}$ for some $1 \leq l < j_2$, where $l_1 = l + 1 - q < l < j_2$, then writing $L_*(X_0 + \alpha_0, X_1 + \alpha_1) = \beta_0 X_0 + \beta_1 X_1$, with $\beta_0, \beta_1 \in \mathbb{F}_q$ (which is possible since $P = (\alpha_0 : \alpha_1 : 1) \in \mathbb{P}^2(\mathbb{F}_q)$ is a nonsingular point of $\mathcal{G}$), and

$$G_{l_1}(X_0, X_1) = L_*(X_0 + \alpha_0, X_1 + \alpha_1) \tilde{G}_{l_1}(X_0, X_1),$$

it follows that

$$\begin{aligned}
X_0^q \frac{\partial G_{l_1}}{\partial X_0} + X_1^q \frac{\partial G_{l_1}}{\partial X_1} &= X_0^q \left(\beta_0 \tilde{G}_{l_1}(X_0, X_1) + L_*(X_0 + \alpha_0, X_1 + \alpha_1) \frac{\partial \tilde{G}_{l_1}}{\partial X_0} \right) \\
&+ X_1^q \left(\beta_1 \tilde{G}_{l_1}(X_0, X_1) + L_*(X_0 + \alpha_0, X_1 + \alpha_1) \frac{\partial \tilde{G}_{l_1}}{\partial X_1} \right) \\
&= (\beta_0 X_0^q + \beta_1 X_1^q) \tilde{G}_{l_1}(X_0, X_1) + L_*(X_0 + \alpha_0, X_1 + \alpha_1) \left(X_0^q \frac{\partial \tilde{G}_{l_1}}{\partial X_0} + X_1^q \frac{\partial \tilde{G}_{l_1}}{\partial X_1} \right) \\
&= (\beta_0 X_0 + \beta_1 X_1)^q \tilde{G}_{l_1}(X_0, X_1) + L_*(X_0 + \alpha_0, X_1 + \alpha_1) \left(X_0^q \frac{\partial \tilde{G}_{l_1}}{\partial X_0} + X_1^q \frac{\partial \tilde{G}_{l_1}}{\partial X_1} \right)
\end{aligned}$$

is also divisible by $L_*(X_0 + \alpha_0, X_1 + \alpha_1) = \beta_0 X_0 + \beta_1 X_1$.

Therefore, from Remark 1.1.33,

$$I(P, \tilde{\mathcal{H}} \cap \mathcal{T}_P) \geq j_2,$$

and the proof of Step 2 follows. $\square$

From the previous two steps,

$$\begin{aligned}
\sum_{P \in \mathcal{G}(\mathbb{F}_q)} I(P, \mathcal{G} \cap \mathcal{H}) &= \sum_{i=1}^k I(\tilde{P}_i, \mathcal{G} \cap \mathcal{H}) + \sum_{P \in \mathcal{G}(\mathbb{F}_q) \setminus \{\tilde{P}_1, \dots, \tilde{P}_k\}} I(P, \mathcal{G} \cap \mathcal{H}) \\
&\geq \sum_{i=1}^k j_2^{(i)} + 2 \cdot \#\mathcal{G}(\mathbb{F}_q) \setminus \{\tilde{P}_1, \dots, \tilde{P}_k\} \\
&= \sum_{i=1}^k (j_2^{(i)} - 2) + 2 \cdot \#\mathcal{G}(\mathbb{F}_q),
\end{aligned}$$

and thus from (4.9)

$$\#\mathcal{G}(\mathbb{F}_q) \leq \frac{\mathfrak{d}(\mathfrak{d} + q - 1) - \sum_{i=1}^k (j_2^{(i)} - 2)}{2}.$$

Assuming equality in (4.7),

$$\sum_{i=1}^k j_2^{(i)} + 2 \cdot \#\mathcal{G}(\mathbb{F}_q) \setminus \{\tilde{P}_1, \dots, \tilde{P}_k\} = \mathfrak{d}(\mathfrak{d} + q - 1) = \sum_{P \in \mathcal{G} \cap \mathcal{H}} I(P, \mathcal{G} \cap \mathcal{H}),$$

and then the following occurs:

1. $I(P, \mathcal{G} \cap \mathcal{H}) = 2$, for all $P \in \mathcal{G}(\mathbb{F}_q) \setminus \{\tilde{P}_1, \dots, \tilde{P}_k\}$;
2. $I(\tilde{P}_i, \mathcal{G} \cap \mathcal{H}) = j_2^{(i)}$, for all $i = 1, \dots, k$;
3. $\mathcal{G} \cap \mathcal{H} = \mathcal{G}(\mathbb{F}_q)$.

From the definition of $\mathcal{H}$, it follows that any singular point $P \in \mathcal{G}$ must be a point of $\mathcal{H}$ and then assertion 3 above gives that $P \in \mathcal{G}(\mathbb{F}_q)$. However, if $P \in \mathcal{G}(\mathbb{F}_q)$ is singular, then $I(P, \mathcal{G} \cap \mathcal{H}) > 2$ by Step 1, which contradicts assertion 1. Hence, $\mathcal{G}$ is a nonsingular plane curve. $\blacksquare$

Theorem 4.3.4. Let $\mathcal{G} : G(X_0, X_1, X_2) = 0$ be an $\mathbb{F}_q$ -Frobenius classical plane curve of degree $\mathfrak{d} < q$. If $\mathcal{G}$ has an infinite number of inflection points, then

$$\#\mathcal{G}(\mathbb{F}_q) \leq \frac{\mathfrak{d}(\mathfrak{d} + q - 1)}{p^k} \quad (4.10)$$

for some $k \geq 1$.

Proof. Considering the notation as in (HIRSCHFELD; KORCHMÁROS, 2001), let B_q be the number of branches of $\mathcal{G}$ centered at points of $\mathbb{P}^2(\mathbb{F}_q)$. Therefore, since $\#\mathcal{G}(\mathbb{F}_q) \leq B_q$, all that is needed is to show that for some $k \geq 1$

$$B_q \leq \frac{(2g - 2) + (q + 2)\mathfrak{d}}{p^k} \leq \frac{\mathfrak{d}(\mathfrak{d} + q - 1)}{p^k}, \quad (4.11)$$

where g is the genus of $\mathcal{G}$. Note that the second inequality in (4.11) is trivial. The first one is proved by considering $v = 1$ in inequality (3.1) in the proof of (HIRSCHFELD; KORCHMÁROS, 2001, Theorem 1.3). In fact, following the notation therein, since $\mathcal{G}$ is $\mathbb{F}_q$ -Frobenius classical,

$$v_P(S) \geq v_P([\bar{x}(t)D_t^{(1)}\bar{y}(t) - \bar{y}(t)D_t^{(1)}\bar{x}(t)]) \geq r + s - 1 \geq \varepsilon,$$

if $v_P(S) < rq$, and

$$v_P(S) \geq rq > rm \geq rs \geq \varepsilon$$

otherwise. Hence, since $\mathcal{G}$ has infinitely many inflection points, and then $\varepsilon = p^k$ for some $k \geq 1$ (see (GARCIA; VOLOCH, 1987, Proposition 2)), the first inequality in (4.11) follows. ■

4.4 Points and linear components of curve $\mathcal{C}$

In this section, the $\mathbb{F}_q$ -rational points and linear components of $\mathcal{C}$ given in (4.2) are investigated.

4.4.1 Points with zero coordinates

The following lemma follows from the definitions.

Lemma 4.4.1. If $e_0 = e_1 = e_2 = 0$, then a point $(\alpha_0 : \alpha_1 : \alpha_2) \in \mathbb{P}^2(\mathbb{F}_q)$ is on $\mathcal{C}$ if and only if $\{\eta(\alpha_0), \eta(\alpha_1), \eta(\alpha_2)\} = \{-1, 0, 1\}$. In particular, $\#\mathcal{C}(\mathbb{F}_q) = 3d$.

Lemma 4.4.2. For a point $P = (\alpha_0 : \alpha_1 : \alpha_2) \in \mathbb{P}^2(\mathbb{F}_q)$ with $\alpha_0\alpha_1\alpha_2 = 0$, the following occurs.

1. For $i = 0, 1, 2$,

$$P_i \in \mathcal{C}(\mathbb{F}_q) \text{ if and only if } \eta(e_i) = -1;$$

2. Let $i, k \in \{0, 1, 2\}$ be distinct elements such that $\alpha_i\alpha_k \neq 0$. Then $P \in \mathcal{C}(\mathbb{F}_q)$ if and only if

$$e_i = e_k = 0 \text{ and } \eta(\alpha_i\alpha_k) = -1$$

or

$$\eta(-e_ie_k) = -1 \text{ and } P = P_{ik}.$$

Proof. Let $P = (\alpha_0 : \alpha_1 : \alpha_2)$ be a point of $\mathbb{P}^2(\mathbb{F}_q)$ with $\alpha_0 \alpha_1 \alpha_2 = 0$. Statement 1 follows directly from the definition of $\mathcal{C}$. Now, suppose without loss of generality that $\alpha_0 \alpha_1 \neq 0$ and $\alpha_2 = 0$. Then the following assertions are equivalent:

- $P \in \mathcal{C}(\mathbb{F}_q)$;
- $\alpha_0^d + \alpha_1^d + (e_0 \alpha_0 + e_1 \alpha_1)^d = 0$;
- $e_0 \alpha_0 + e_1 \alpha_1 = 0$ and $\eta(\alpha_0 \alpha_1) = -1$;
- Either $e_0 = e_1 = 0$ and $\eta(\alpha_0 \alpha_1) = -1$ or $\eta(-e_0 e_1) = -1$ and $P = P_{01}$,

which completes the proof. ■

Based on these results, the number of $\mathbb{F}_q$ -rational points on $\mathcal{C}$ with zero coordinates is summarized in Table 1, for all possible quadratic characters of e_0, e_1 and e_2 .

$\{\eta(e_0), \eta(e_1), \eta(e_2)\}$	$i = 2$	$i = 1$ and d odd	$i = 1$ and d even
$\{1, 1, 1\}$	0	3	0
$\{-1, 1, 1\}$	1	1	2
$\{-1, -1, 1\}$	2	1	2
$\{-1, -1, -1\}$	3	3	0
$\{0, 1, 1\}$	0	1	0
$\{-1, 0, 1\}$	1	0	1
$\{-1, -1, 0\}$	2	1	0
$\{0, 0, 1\}$	0	d	d
$\{-1, 0, 0\}$	1	d	d
$\{0, 0, 0\}$	0	$3d$	$3d$

Table 1 – The number of $\mathbb{F}_q$ -rational points on $\mathcal{C}$ with $i \in \{1, 2\}$ zero coordinates.

4.4.2 Points without zero coordinates

A point $P = (1 : \alpha_1 : \alpha_2) \in \mathbb{P}^2(\mathbb{F}_q)$, with $\alpha_1 \alpha_2 \neq 0$, is on $\mathcal{C}(\mathbb{F}_q)$ if and only if one of the following cases occurs:

- (1) $\eta(\alpha_1) = 1, \eta(\alpha_2) = -1$ and $\eta(e_0 + e_1 \alpha_1 + e_2 \alpha_2) = -1$;
- (2) $\eta(\alpha_1) = -1, \eta(\alpha_2) = 1$ and $\eta(e_0 + e_1 \alpha_1 + e_2 \alpha_2) = -1$;
- (3) $\eta(\alpha_1) = -1, \eta(\alpha_2) = -1$ and $\eta(e_0 + e_1 \alpha_1 + e_2 \alpha_2) = 1$.

If $N_{(i)}$ is the number of points satisfying case (i), for $i \in \{1, 2, 3\}$, then $N_{(1)}, N_{(2)}$ and $N_{(3)}$ are the cardinalities of the sets

$$\left\{ (\gamma_1^2, \lambda \gamma_2^2, \lambda \gamma_3^2) \in \mathbb{F}_q^{*3} : \gamma_i \in \mathbb{F}_q^*, \text{ for } i = 1, 2, 3, \text{ and } e_0 + e_1 \gamma_1^2 + e_2 \lambda \gamma_2^2 = \lambda \gamma_3^2 \right\},$$

$$\left\{ (\lambda \gamma_1^2, \gamma_2^2, \lambda \gamma_3^2) \in \mathbb{F}_q^{*3} : \gamma_i \in \mathbb{F}_q^*, \text{ for } i = 1, 2, 3, \text{ and } e_0 + e_1 \lambda \gamma_1^2 + e_2 \gamma_2^2 = \lambda \gamma_3^2 \right\},$$

and

$$\left\{ (\lambda \gamma_1^2, \lambda \gamma_2^2, \gamma_3^2) \in \mathbb{F}_q^{*3} : \gamma_i \in \mathbb{F}_q^*, \text{ for } i = 1, 2, 3, \text{ and } e_0 + e_1 \lambda \gamma_1^2 + e_2 \lambda \gamma_2^2 = \gamma_3^2 \right\},$$

respectively, where λ is a fixed non-square element of $\mathbb{F}_q$.

Let

$$N\left(\sum_{k=1}^l \beta_k Y_k^2 = \beta\right)$$

represent the number of solutions $(\gamma_1, \dots, \gamma_l) \in \mathbb{F}_q^l$ of the equation

$$\sum_{k=1}^l \beta_k Y_k^2 = \beta$$

defined over $\mathbb{F}_q$, and let

$$a_1 = e_1, a_2 = \lambda e_2, a_3 = -\lambda, \alpha = -e_0, \text{ if } i = 1,$$

$$a_1 = \lambda e_1, a_2 = e_2, a_3 = -\lambda, \alpha = -e_0, \text{ if } i = 2,$$

and

$$a_1 = \lambda e_1, a_2 = \lambda e_2, a_3 = -1, \alpha = -e_0, \text{ if } i = 3.$$

Then the number $N_{(i)}$, with $i \in \{1, 2, 3\}$, is determined by the following expressions, for all possible cases of e_0, e_1 and e_2 .

1. Case $e_0 e_1 e_2 \neq 0$

$$\begin{aligned} 8N_{(i)} &= N(a_1 Y_1^2 + a_2 Y_2^2 + a_3 Y_3^2 = \alpha) - \sum_{k=1}^3 N\left(\sum_{l=1, l \neq k}^3 a_l Y_l^2 = \alpha\right) \\ &+ \sum_{k=1}^3 N(a_k Y_k^2 = \alpha). \end{aligned}$$

2. Case $e_0 e_k \neq 0, e_{k_1} = 0$, with $k, k_1 \in \{1, 2\}$

$$8N_{(i)} = (q-1) \left[N(a_k Y_k^2 + a_3 Y_3^2 = \alpha) - \sum_{l=1, l \neq k_1}^3 N(a_l Y_l^2 = \alpha) \right].$$

3. Case $e_1 e_2 \neq 0, e_0 = 0$

$$\begin{aligned} 8N_{(i)} &= N(a_1 Y_1^2 + a_2 Y_2^2 + a_3 Y_3^2 = \alpha) - \sum_{k=1}^3 N\left(\sum_{l=1, l \neq k}^3 a_l Y_l^2 = \alpha\right) \\ &+ \sum_{k=1}^3 N(a_k Y_k^2 = \alpha) - 1. \end{aligned}$$

4. Case $e_0 \neq 0, e_1 = e_2 = 0$

$$8N_{(i)} = (q-1)^2 N(a_3 Y_3^2 = \alpha).$$

5. Case $e_k \neq 0, e_0 = e_{k_1} = 0$, with $k, k_1 \in \{1, 2\}$

$$8N_{(i)} = (q-1) \left[N(a_k Y_k^2 + a_3 Y_3^2 = \alpha) - \sum_{l=1, l \neq k_1}^3 N(a_l Y_l^2 = \alpha) + 1 \right].$$

Table 2 presents the values of $N_{(1)} + N_{(2)} + N_{(3)}$, which are calculated using the following lemma given by Propositions 1 and 2 of (JOLY, 1973, Chapter 6).

Lemma 4.4.3. Let $p > 2$ and l a positive integer. The number of solutions in $\mathbb{F}_q^l$ of the equation $\beta_1 Y_1^2 + \dots + \beta_l Y_l^2 = \beta$, with $\beta_k \in \mathbb{F}_q^*$ for all $k = 1, \dots, l$, is given by:

$$\begin{cases} q^{l-1} + \eta((-1)^{l/2} \beta_1 \dots \beta_l) (q^{l/2} - q^{(l-2)/2}), & \text{if } \beta = 0 \text{ and } l \equiv 0 \pmod{2}, \\ q^{l-1} - \eta((-1)^{l/2} \beta_1 \dots \beta_l) q^{(l-2)/2}, & \text{if } \beta \neq 0 \text{ and } l \equiv 0 \pmod{2}, \\ q^{l-1}, & \text{if } \beta = 0 \text{ and } l \equiv 1 \pmod{2}, \\ q^{l-1} + \eta((-1)^{(l-1)/2} \beta_1 \dots \beta_l \beta) q^{(l-1)/2}, & \text{if } \beta \neq 0 \text{ and } l \equiv 1 \pmod{2}. \end{cases}$$

$e_0 e_1 e_2 \neq 0$		
$\{\eta(e_0), \eta(e_1), \eta(e_2)\}$	d odd	d even
$\{1, 1, 1\}$	$\frac{3(q-1)(q-3)}{8}$	$\frac{3(q-1)^2}{8}$
$\{-1, 1, 1\}$	$\frac{3q^2-6q+7}{8}$	$\frac{3(q-1)(q-3)}{8}$
$\{-1, -1, 1\}$	$\frac{3(q-1)(q-3)}{8}$	$\frac{3q^2-6q+11}{8}$
$\{-1, -1, -1\}$	$\frac{3(q^2-2q+5)}{8}$	$\frac{3(q-1)(q-3)}{8}$
Exactly one of the elements e_0, e_1, e_2 is zero		
$\{\eta(e_0), \eta(e_1), \eta(e_2)\}$	d odd	d even
$\{0, 1, 1\}$	$\frac{(q-1)(3q-5)}{8}$	$\frac{3(q-1)^2}{8}$
$\{-1, 0, 1\}$	$\frac{(q-1)(3q-5)}{8}$	$\frac{(q-1)(3q-7)}{8}$
$\{-1, -1, 0\}$	$\frac{3(q-1)(q-3)}{8}$	$\frac{(q-1)(3q-7)}{8}$
Exactly two of the elements e_0, e_1, e_2 are zero		
$\{\eta(e_0), \eta(e_1), \eta(e_2)\}$	d odd	d even
$\{0, 0, 1\}$	$\frac{(q-1)^2}{4}$	$\frac{(q-1)^2}{4}$
$\{-1, 0, 0\}$	$\frac{(q-1)^2}{2}$	$\frac{(q-1)^2}{2}$

Table 2 – The number $N_{(1)} + N_{(2)} + N_{(3)}$.

4.4.3 Linear components

Here, Lemmas 4.4.4 and 4.4.8 provide a description of the linear components of $\mathcal{C}$, which are summarized, for $e_0 e_1 e_2 \neq 0$, in Table 3.

Lemma 4.4.4. The linear components of $\mathcal{C}$ and the circumstances in which they arise are as follows:

1. The plane curve $\mathcal{C}$ is a union of d lines if and only if $\{\eta(e_0), \eta(e_1), \eta(e_2)\} = \{-1, 0, 0\}$;

2. If $\mathcal{C}$ is not a union of d lines, then a line $\mathcal{L}$ is a component of $\mathcal{C}$ if and only if $\mathcal{L}$ is given by $e_i X_i + e_k X_k = 0$ and $\eta(-e_i e_k) = \eta(e_l) = -1$, with $\{i, k, l\} = \{0, 1, 2\}$.

To prove the previous result, the following proposition and its corollary need to be considered first.

Proposition 4.4.5. Let $\mathbb{K}$ be an algebraically closed field of arbitrary characteristic p and consider $\mathcal{G} : G(X_0, X_1, X_2) = 0$ a nonsingular plane curve in $\mathbb{P}^2(\mathbb{K})$ of degree $\mathfrak{d} \geq 2$. Suppose that $p \nmid \mathfrak{d}$. If k is the number of total inflection points of $\mathcal{G}$, then the surface in $\mathbb{P}^3(\mathbb{K})$

$$\mathcal{S} : X_3^{\mathfrak{d}} - G(X_0, X_1, X_2) = 0$$

contains exactly $k\mathfrak{d}$ lines.

Proof. Let $\mathcal{L}$ be a line on $\mathcal{S}$ given by the intersection of two distinct hyperplanes. After a suitable rotation of the planes around $\mathcal{L}$, one may assume that one of them is given by $X_2 = \alpha_0 X_0 + \alpha_1 X_1$, $\alpha_0, \alpha_1 \in \mathbb{K}$. Thus $X_3^{\mathfrak{d}} - G(X_0, X_1, \alpha_0 X_0 + \alpha_1 X_1)$ has a linear factor, say $X_3 - \beta_0 X_0 - \beta_1 X_1 \in \mathbb{K}[X_0, X_1, X_3]$, corresponding to the other plane. This implies by the Euclidean algorithm for divisibility of polynomials¹ that $G(X_0, X_1, \alpha_0 X_0 + \alpha_1 X_1) = (\beta_0 X_0 + \beta_1 X_1)^{\mathfrak{d}}$, which is equivalent to $X_2 = \alpha_0 X_0 + \alpha_1 X_1$ being the tangent to $\mathcal{G}$ at some total inflection point $P \in \mathcal{G}$.

On the other hand, let P be any total inflection point of $\mathcal{G}$. Without loss of generality, one can suppose that the tangent line $\mathcal{T}_P$ to $\mathcal{G}$ at P is given by $X_2 = \alpha_0 X_0 + \alpha_1 X_1$, with $\alpha_0, \alpha_1 \in \mathbb{K}$. Then, $G(X_0, X_1, \alpha_0 X_0 + \alpha_1 X_1) = (\beta_0 X_0 + \beta_1 X_1)^{\mathfrak{d}}$, for some $\beta_0, \beta_1 \in \mathbb{K}$, which gives rise to the $\mathfrak{d}$ lines on $\mathcal{S}$

$$\mathcal{L}_i : \begin{cases} X_2 &= \alpha_0 X_0 + \alpha_1 X_1 \\ \xi_i X_3 &= \beta_0 X_0 + \beta_1 X_1, \end{cases} \quad (4.12)$$

where $\xi_1, \dots, \xi_{\mathfrak{d}}$ are the $\mathfrak{d}$ -th roots of unity.

Since distinct total inflection points $P \in \mathcal{C}$ yield disjoint sets of $\mathfrak{d}$ lines, the result follows. ■

Remark 4.4.6. Suppose that $\mathbb{K} = \overline{\mathbb{F}_q}$ and that $\mathcal{G}$ is defined over $\mathbb{F}_q$. Also, suppose that $\mathbb{F}_q$ has the $\mathfrak{d}$ -th roots of unity. Then, from the proof of Proposition 4.4.5 and considering the notation therein, the following assertion holds.

If k is the number of total inflection points of $\mathcal{G}$ defined over $\mathbb{F}_q$, then the surface $\mathcal{S}$ contains exactly $k\mathfrak{d}$ lines defined over $\mathbb{F}_q$.

¹ Let R be any (commutative) ring and $Y^i - \alpha, Y^l - \beta \in R[Y]$, with $\alpha, \beta \in R \setminus \{0\}$ and $1 \leq i \leq l$. Applying the Euclidean algorithm for divisibility of polynomials (which can be used here since $Y^i - \alpha$ is a monic polynomial), we have that

$$(Y^i - \alpha) \mid (Y^l - \beta) \Leftrightarrow i \mid l \text{ and } \alpha^{\frac{l}{i}} = \beta.$$

Corollary 4.4.7. Let $d \geq 3$ be an integer such that $p \nmid d$. If $d = p^i + 1$ for some $i \geq 1$, then the Fermat surface in $\mathbb{P}^3(\overline{\mathbb{F}}_q)$

$$\mathcal{S} : X_0^d + X_1^d + X_2^d + X_3^d = 0$$

has $(p^i + 1)(p^{3i} + 1)$ lines. Otherwise, the number of lines is $3d^2$.

Proof. It is well known that the Hermitian curve

$$\mathcal{H} : X_0^{p^i+1} + X_1^{p^i+1} + X_2^{p^i+1} = 0$$

has $p^{3i} + 1$ rational points over $\mathbb{F}_{p^{2i}}$, and that those are all the total inflection points of $\mathcal{H}$.

We claim that all Fermat curves of degree $d \neq p^i + 1$ have only the well-known $3d$ total inflection points, namely the points on $X_0X_1X_2 = 0$.

In fact, let $P = (\alpha_0 : \alpha_1 : 1)$, with $\alpha_0\alpha_1 \neq 0$, be a total inflection point of

$$\mathcal{G} : X_0^d + X_1^d + X_2^d = 0,$$

and let $\mathcal{T}_P : \alpha_0^{d-1}X_0 + \alpha_1^{d-1}X_1 + X_2 = 0$ be the tangent line to $\mathcal{G}$ at P . Thus, for $\alpha = -\frac{1}{\alpha_1^{d-1}}$ and $\beta = (\frac{\alpha_0}{\alpha_1})^{d-1} \neq 0$, it follows that α_0 is the only zero of

$$X_0^d + (\alpha - \beta X_0)^d + 1,$$

and then the only zero of its derivative

$$d \left(X_0^{d-1} - \beta(\alpha - \beta X_0)^{d-1} \right).$$

The latter is equivalent to

$$\left(\frac{X_0}{\alpha - \beta X_0} \right)^{d-1} = \beta$$

having only one root, which clearly happens if and only if $d - 1$ is a power of p . This proves the claim.

Now the result follows immediately from Proposition 4.4.5. ■

Proof of Lemma 4.4.4. Statements 1 and 2 ($\Leftrightarrow$) follow from the definition of the plane curve $\mathcal{C}$.

To prove statement 2 ($\Rightarrow$), suppose that $\mathcal{C}$ is not a union of d lines, and let $\mathcal{L}$ be a linear component of $\mathcal{C}$.

Let us look at $\mathcal{C}$ as the plane curve on the Fermat surface $\mathcal{S} : X_0^d + X_1^d + X_2^d + X_3^d = 0$ cut out by the hyperplane $P : X_3 - e_0X_0 - e_1X_1 - e_2X_2$, and let $\tilde{\mathcal{L}}$ be the corresponding line.

Then, without loss of generality such line $\tilde{\mathcal{L}}$ is given by

$$\tilde{\mathcal{L}} : \begin{cases} X_0 &= \xi_1 X_1 \\ X_3 &= \xi_2 X_2, \end{cases} \quad (4.13)$$

where $\xi_1, \xi_2 \in \mathbb{F}_q$ are d -th roots of -1 , that is, $\eta(\xi_i) = -1$, for $i = 1, 2$. Note that P and $X_3 = \xi_2 X_2$ are not the same hyperplane as, otherwise, $\mathcal{C}$ would be a union of the d lines. Therefore, $\mathcal{L}$ is in the intersection of the following hyperplanes

$$\begin{cases} X_0 &= \xi_1 X_1 \\ X_3 &= \xi_2 X_2 \\ X_3 &= e_0 X_0 + e_1 X_1 + e_2 X_2, \end{cases} \quad (4.14)$$

which implies that $\xi_1 = -e_1/e_0$, $\xi_2 = e_2$, and then $\mathcal{L}$ must be given by $e_0 X_0 + e_1 X_1 = 0$. ■

Lemma 4.4.8. If e_0, e_1 and e_2 are all nonzero, then the linear components of $\mathcal{C}$ have multiplicity at most 1. That is, none of $(e_0 X_0 + e_1 X_1)^2$, $(e_0 X_0 + e_2 X_2)^2$ or $(e_1 X_1 + e_2 X_2)^2$ divides $C(X_0, X_1, X_2)$.

Proof. Without loss of generality, assume that $\mathcal{L}_{01} : e_0 X_0 + e_1 X_1 = 0$ is a component of $\mathcal{C}$, and then $\eta(e_2) = -1$ by Lemma 4.4.4. Since

$$\begin{aligned} C(X_0, X_1, X_2) &= X_0^d + X_1^d + X_2^d + (e_0 X_0 + e_1 X_1)^d + (e_2 X_2)^d + \\ &\quad + \sum_{i=1}^{d-1} \binom{d}{i} (e_0 X_0 + e_1 X_1)^i (e_2 X_2)^{d-i}, \end{aligned}$$

it follows that $(e_0 X_0 + e_1 X_1) \mid (X_0^d + X_1^d)$. If $(e_0 X_0 + e_1 X_1)^2 \mid C(X_0, X_1, X_2)$ and

$$(e_0 X_0 + e_1 X_1)^2 \mid (X_0^d + X_1^d + d(e_0 X_0 + e_1 X_1)(e_2 X_2)^{d-1}),$$

then $e_2 = 0$, which is a contradiction. ■

$(\eta(e_0), \eta(e_1), \eta(e_2))$	d odd	d even
$(1, 1, 1)$	-	-
$(1, 1, -1)$	$e_0 X_0 + e_1 X_1$	-
$(1, -1, 1)$	$e_0 X_0 + e_2 X_2$	-
$(-1, 1, 1)$	$e_1 X_1 + e_2 X_2$	-
$(1, -1, -1)$	-	$e_0 X_0 + e_1 X_1, e_0 X_0 + e_2 X_2$
$(-1, 1, -1)$	-	$e_0 X_0 + e_1 X_1, e_1 X_1 + e_2 X_2$
$(-1, -1, 1)$	-	$e_0 X_0 + e_2 X_2, e_1 X_1 + e_2 X_2$
$(-1, -1, -1)$	$e_0 X_0 + e_1 X_1, e_0 X_0 + e_2 X_2, e_1 X_1 + e_2 X_2$	-

Table 3 – Linear components of $\mathcal{C}$ for $e_0 e_1 e_2 \neq 0$.

4.5 Preliminary result

Theorem 4.5.1. Let $\mathcal{C}$ be the plane curve given in (4.2). The union of the linear components of $\mathcal{C}$ is $\mathbb{F}_q$ -disjoint from its remaining components.

Proof. Let $n \in \{0, 1, 2, 3, d\}$ be the number of linear components of $\mathcal{C}$. If $n \in \{0, d\}$, then the proof is complete. Now, each of the remaining cases is considered separately.

Case $n = 1$

Without loss of generality, let $\mathcal{L}_{01} : e_0X_0 + e_1X_1 = 0$ be the linear component of $\mathcal{C}$. Then, d is odd, $\eta(e_0) = \eta(e_1) = 1$, and $\eta(e_2) = \eta(-e_0e_1) = -1$ (see Table 3).

Assume that the point $P = (\alpha_0 : \alpha_1 : \alpha_2) \in \mathbb{P}^2(\mathbb{F}_q)$ lies on $\mathcal{L}_{01}$ and on an additional component of $\mathcal{C}$. Then the polynomial

$$R(X_1) = \alpha_0^d + X_1^d + \alpha_2^d + (e_0\alpha_0 + e_1X_1 + e_2\alpha_2)^d$$

vanishes at α_1 with multiplicity at least two. Therefore,

$$\frac{dR}{dX_1}(\alpha_1) = d\alpha_1^{d-1} + de_1(e_2\alpha_2)^{d-1} = 0,$$

that is, $\alpha_1^{d-1} + e_1(e_2\alpha_2)^{d-1} = 0$.

If $\alpha_1 = 0$, then $\alpha_0 = \alpha_2 = 0$. Since this cannot occur, it follows that $\alpha_1 \neq 0$ and

$$e_1 \left(\frac{e_2\alpha_2}{\alpha_1} \right)^{d-1} = -1.$$

This implies that $\eta(-1) = 1$, which contradicts the fact that d is odd. Indeed,

$$e_1 \left(\frac{e_2\alpha_2}{\alpha_1} \right)^{d-1} = e_1 \left(\frac{e_2\alpha_2}{\alpha_1} \right)^d \left(\frac{\alpha_1}{e_2\alpha_2} \right) = -1.$$

Therefore, if $\eta(\alpha_1) = \eta(\alpha_2)$, then $\eta\left(\frac{e_2\alpha_2}{\alpha_1}\right) = \left(\frac{e_2\alpha_2}{\alpha_1}\right)^d = -1$ and

$$\eta(-1) = \eta\left(-e_1\left(\frac{\alpha_1}{e_2\alpha_2}\right)\right) = \eta(e_1) = 1.$$

Further, if $\eta(\alpha_1) \neq \eta(\alpha_2)$, then $\eta\left(\frac{e_2\alpha_2}{\alpha_1}\right) = \left(\frac{e_2\alpha_2}{\alpha_1}\right)^d = 1$ and

$$\eta(-1) = \eta\left(e_1\left(\frac{\alpha_1}{e_2\alpha_2}\right)\right) = \eta(e_1) = 1.$$

□

Case $n = 2$

Without loss of generality, let $\mathcal{L}_{01} : e_0X_0 + e_1X_1 = 0$ and $\mathcal{L}_{02} : e_0X_0 + e_2X_2 = 0$ be the linear components of $\mathcal{C}$. Then d is even, $\eta(e_0) = 1$, and $\eta(e_1) = \eta(e_2) = -1$ (see Table 3).

Note that if $d = 2$ (which occurs if and only if $q = 5$), then the proof is complete. Therefore, hereafter let us consider $d > 2$.

Assume that $P = (\alpha_0 : \alpha_1 : \alpha_2) \in \mathbb{P}^2(\mathbb{F}_q)$ lies on $\mathcal{L}_{01}$ and on an additional component of $\mathcal{C}$, but not on $\mathcal{L}_{02}$. Then the polynomial

$$R(X_1) = \alpha_0^d + X_1^d + \alpha_2^d + (e_0\alpha_0 + e_1X_1 + e_2\alpha_2)^d$$

vanishes at α_1 with multiplicity at least two and, therefore,

$$\frac{dR}{dX_1}(\alpha_1) = d\alpha_1^{d-1} + de_1(e_2\alpha_2)^{d-1} = 0,$$

that is, $\alpha_1^{d-1} + e_1(e_2\alpha_2)^{d-1} = 0$.

If $\alpha_1 = 0$, then $\alpha_0 = \alpha_2 = 0$. Since this is impossible, it follows that $\alpha_1 \neq 0$ and so

$$e_1 \left(\frac{e_2\alpha_2}{\alpha_1} \right)^{d-1} = e_1 \left(\frac{e_2\alpha_2}{\alpha_1} \right)^d \left(\frac{\alpha_1}{e_2\alpha_2} \right) = -1,$$

which implies that

$$e_1\eta(\alpha_1\alpha_2) = \frac{e_2\alpha_2}{\alpha_1}.$$

If $\eta(\alpha_1\alpha_2) = 1$, then $e_1\alpha_1 = e_2\alpha_2$ and P lies on $\mathcal{L}_{02}$, which is a contradiction. On the other hand, if $\eta(\alpha_1\alpha_2) = -1$, then $e_1 = -\frac{e_2\alpha_2}{\alpha_1}$ and $\eta(e_1) = 1$, which is also a contradiction since $\eta(e_1) = -1$.

Analogously, one can show that $P = (\alpha_0 : \alpha_1 : \alpha_2) \in \mathbb{P}^2(\mathbb{F}_q)$ lying on $\mathcal{L}_{02}$ and on an additional component of $\mathcal{C}$, but not on $\mathcal{L}_{01}$ leads to a contradiction.

Now, assume that the point $P \in \mathcal{L}_{01} \cap \mathcal{L}_{02}$ lies on an additional component of $\mathcal{C}$. Then

$$\tilde{R}(X_0) = X_0^d + \alpha_1^d + \alpha_2^d + (e_0X_0 + e_1\alpha_1 + e_2\alpha_2)^d$$

vanishes at α_0 with multiplicity at least three. Therefore,

$$\frac{d^2\tilde{R}}{dX_0^2}(\alpha_0) = d(d-1)\alpha_0^{d-2} + d(d-1)e_0^2(e_2\alpha_2)^{d-2} = 0,$$

that is, $\alpha_0^{d-2} + e_0^2(e_2\alpha_2)^{d-2} = 0$. However, since $e_0\alpha_0 + e_2\alpha_2 = 0$, d is even and $\eta(e_0) = 1$, it follows that $2\alpha_0^{d-2} = 0$, that is, $\alpha_0 = \alpha_1 = \alpha_2 = 0$, which is impossible. $\square$

Case $n = 3$

Suppose that $\mathcal{C}$ has as linear components the lines $\mathcal{L}_{01} : e_0X_0 + e_1X_1 = 0$, $\mathcal{L}_{02} : e_0X_0 + e_2X_2 = 0$, and $\mathcal{L}_{12} : e_1X_1 + e_2X_2 = 0$. Then $\eta(e_0) = \eta(e_1) = \eta(e_2) = -1$ and d is odd (see Table 3).

Assume that $P = (\alpha_0 : \alpha_1 : \alpha_2) \in \mathbb{P}^2(\mathbb{F}_q)$ lies on $\mathcal{L}_{01}$ and on an additional component of $\mathcal{C}$, but not on $\mathcal{L}_{02}$ and $\mathcal{L}_{12}$. Thus

$$R(X_1) = \alpha_0^d + X_1^d + \alpha_2^d + (e_0\alpha_0 + e_1X_1 + e_2\alpha_2)^d$$

vanishes at α_1 with multiplicity at least two. Therefore,

$$\frac{dR}{dX_1}(\alpha_1) = d\alpha_1^{d-1} + de_1(e_2\alpha_2)^{d-1} = 0,$$

that is, $\alpha_1^{d-1} + e_1(e_2\alpha_2)^{d-1} = 0$.

If $\alpha_1 = 0$, then $\alpha_0 = \alpha_2 = 0$. Since this cannot occur, it follows that $\alpha_1 \neq 0$ and, as in the previous case, it is possible to write

$$e_1\eta(\alpha_1\alpha_2) = \frac{e_2\alpha_2}{\alpha_1}.$$

If $\eta(\alpha_1\alpha_2) = 1$, then $e_1\alpha_1 = e_2\alpha_2$ and $P \in \mathcal{L}_{02}$, which is a contradiction. If $\eta(\alpha_1\alpha_2) = -1$, then $e_1\alpha_1 + e_2\alpha_2 = 0$ and $P \in \mathcal{L}_{12}$, which is also a contradiction.

Analogously, one can show that $P = (\alpha_0 : \alpha_1 : \alpha_2) \in \mathbb{P}^2(\mathbb{F}_q)$ lying on $\mathcal{L}_{02}$ and on an additional component of $\mathcal{C}$, but not on $\mathcal{L}_{01}$ and $\mathcal{L}_{12}$, and $P = (\alpha_0 : \alpha_1 : \alpha_2) \in \mathbb{P}^2(\mathbb{F}_q)$ lying on $\mathcal{L}_{12}$ and on an additional component of $\mathcal{C}$, but not on $\mathcal{L}_{01}$ and $\mathcal{L}_{02}$, lead us also to a contradiction.

Finally, without loss of generality, assume that $P \in \mathcal{L}_{01} \cap \mathcal{L}_{02}$ (and then $P \notin \mathcal{L}_{12}$) lies on an additional component of $\mathcal{C}$. Then

$$\tilde{R}(X_0) = X_0^d + \alpha_1^d + \alpha_2^d + (e_0X_0 + e_1\alpha_1 + e_2\alpha_2)^d$$

vanishes at α_0 with multiplicity at least three. Therefore,

$$\frac{d^2\tilde{R}}{dX_0^2}(\alpha_0) = d(d-1)\alpha_0^{d-2} + d(d-1)e_0^2(e_2\alpha_2)^{d-2} = 0,$$

that is, $\alpha_0^{d-2} + e_0^2(e_2\alpha_2)^{d-2} = 0$. However, since $e_0\alpha_0 + e_2\alpha_2 = 0$, d is odd (and then $d-2 \geq 1$) and $\eta(e_0) = -1$, it follows that $2\alpha_0^{d-2} = 0$, that is, $\alpha_0 = \alpha_1 = \alpha_2 = 0$, which is impossible. $\square$

Hence, for all possible cases, it has been shown that assuming $P \in \mathbb{P}^2(\mathbb{F}_q)$ to be a point on a linear component of $\mathcal{C}$ and on an additional nonlinear component of $\mathcal{C}$ leads to a contradiction. $\blacksquare$

4.6 Main result

Before proving the central result of this work in Subsection 4.6.2, the absolute irreducibility of $\mathcal{F}$ needs to be studied. This is done in Subsection 4.6.1.

4.6.1 Frobenius classicality and absolute irreducibility

Let $\mathcal{F}$ be the union of the nonlinear components of $\mathcal{C}$. Our objective here is to show that $\mathcal{F}$ consists of only one absolutely irreducible nonlinear component.

In cases where $\{\eta(e_0), \eta(e_1), \eta(e_2)\}$ is either $\{0, 0, 0\}$ or $\{0, 0, 1\}$, $\mathcal{F} = \mathcal{C}$ is a Fermat curve, for which the absolute irreducibility is well known.

The study of the remaining cases is centered around Theorem 4.3.2. However, in order to apply it, the following result is necessary. Note that the notation here is given as in Definition 4.3.1.

Theorem 4.6.1. Each nonlinear absolutely irreducible component $\mathcal{G} \subseteq \mathcal{C}$ defined over $\mathbb{F}_q$ is an $\mathbb{F}_q$ -Frobenius classical plane curve.

Proof. Suppose that $\mathcal{G}$ is given by

$$G(X_0, X_1, X_2) = 0,$$

where $G(X_0, X_1, X_2) \in \mathbb{F}_q[X_0, X_1, X_2]$ is an absolutely irreducible homogeneous polynomial. Then, it is necessary to show that $G \nmid \Phi_q(G)$.

Let $H(X_0, X_1, X_2) \in \mathbb{F}_q[X_0, X_1, X_2]$ be such that

$$C(X_0, X_1, X_2) = G(X_0, X_1, X_2)H(X_0, X_1, X_2)$$

and note that

$$\Phi_q(C) = G\Phi_q(H) + \Phi_q(G)H.$$

Therefore, it suffices to prove that $G \nmid \Phi_q(C)$.

Since $C(X_0, X_1, X_2) = X_0^d + X_1^d + X_2^d + X_3^d$, with $X_3 = e_0X_0 + e_1X_1 + e_2X_2$ and $d = (q - 1)/2$, it follows that

$$\Phi_q(C) = d(X_0^{3d} + X_1^{3d} + X_2^{3d} + X_3^{3d}).$$

Indeed,

$$\begin{aligned} \Phi_q(C) &= X_0^q[dX_0^{d-1} + de_0(e_0X_0 + e_1X_1 + e_2X_2)^{d-1}] + \\ &+ X_1^q[dX_1^{d-1} + de_1(e_0X_0 + e_1X_1 + e_2X_2)^{d-1}] + \\ &+ X_2^q[dX_2^{d-1} + de_2(e_0X_0 + e_1X_1 + e_2X_2)^{d-1}] \\ &= d(X_0^{3d} + X_1^{3d} + X_2^{3d}) + d(e_0X_0 + e_1X_1 + e_2X_2)^{d-1}(e_0X_0^q + e_1X_1^q + e_2X_2^q) \\ &= d(X_0^{3d} + X_1^{3d} + X_2^{3d}) + d(e_0X_0 + e_1X_1 + e_2X_2)^{d-1}(e_0X_0 + e_1X_1 + e_2X_2)^q \\ &= d(X_0^{3d} + X_1^{3d} + X_2^{3d}) + d(e_0X_0 + e_1X_1 + e_2X_2)^{3d} \\ &= d(X_0^{3d} + X_1^{3d} + X_2^{3d} + X_3^{3d}). \end{aligned}$$

Finally, from the polynomial identity

$$\begin{aligned} X_0^{3d} + X_1^{3d} + X_2^{3d} + X_3^{3d} &= C(X_0, X_1, X_2)^3 - 3X_3^d(X_0^d + X_1^d + X_2^d)C(X_0, X_1, X_2) - \\ &- 3(X_0^d + X_1^d)(X_0^d + X_2^d)(X_1^d + X_2^d), \end{aligned}$$

it follows that if $G \mid \Phi_q(C)$, then $G \mid (X_0^d + X_1^d)(X_0^d + X_2^d)(X_1^d + X_2^d)$, which contradicts $\deg(G) > 1$. Hence, $\mathcal{G}$ is $\mathbb{F}_q$ -Frobenius classical. ■

Now, if d is the degree of $\mathcal{F}$, based on Tables 4 and 5,

$$\#\mathcal{F}(\mathbb{F}_q) \geq \frac{d(d+q-1)}{2} - \max\{d-1, 2d-5\},$$

if and only if at least two of e_0, e_1 and e_2 are nonzero, which includes all cases where

$$\#\mathcal{F}(\mathbb{F}_q) = \frac{1}{2}d(d+q-1) - \frac{1}{2}(d-2).$$

Therefore, in these cases, $\mathcal{F}$ is absolutely irreducible by Theorem 4.3.2.

4.6.2 Proof of Theorem 4.1.1

Given a specific set $\{\eta(e_0), \eta(e_1), \eta(e_2)\}$, the number of $\mathbb{F}_q$ -rational points with zero coordinates on $\mathcal{C}$, denoted by $N_{(0)}$, is listed in Table 1, and the number $N_{(1)} + N_{(2)} + N_{(3)}$ of $\mathbb{F}_q$ -rational points without zero coordinates on $\mathcal{C}$ is determined in Subsection 4.4.2 and summarized in Table 2. Hence,

$$\#\mathcal{C}(\mathbb{F}_q) = N_{(0)} + N_{(1)} + N_{(2)} + N_{(3)}.$$

By Subsection 4.4.3, $\mathcal{C}$ has:

- exactly one linear component, if d is odd and $\{\eta(e_0), \eta(e_1), \eta(e_2)\} = \{-1, 1, 1\}$, in which case $\#\mathcal{F}(\mathbb{F}_q) = \#\mathcal{C}(\mathbb{F}_q) - (q+1)$ and $d = (q-3)/2$;
- exactly two linear components, if d is even and $\{\eta(e_0), \eta(e_1), \eta(e_2)\} = \{-1, -1, 1\}$, in which case $\#\mathcal{F}(\mathbb{F}_q) = \#\mathcal{C}(\mathbb{F}_q) - (2q+1)$ and $d = (q-5)/2$;
- exactly three linear components, if d is odd and $\{\eta(e_0), \eta(e_1), \eta(e_2)\} = \{-1, -1, -1\}$, in which case $\#\mathcal{F}(\mathbb{F}_q) = \#\mathcal{C}(\mathbb{F}_q) - 3q$ and $d = (q-7)/2$.

In all other cases, $\mathcal{C}$ does not have a linear component, $\#\mathcal{F}(\mathbb{F}_q) = \#\mathcal{C}(\mathbb{F}_q)$, and $d = (q-1)/2$.

Tables 4 and 5 summarize the number n of linear components of $\mathcal{C}$, the degree d of $\mathcal{F}$, and the value of $\#\mathcal{F}(\mathbb{F}_q)$ for the cases in which d is odd and even, respectively. Note that rows (1) and (4) in Table 4 and rows (2) and (5) in Table 5 present two classes of plane curves. A simple check shows that two plane curves arising from any of the two classes in a particular row are projectively equivalent.

	$\{\eta(e_0), \eta(e_1), \eta(e_2)\}$	n	d	$\#\mathcal{F}(\mathbb{F}_q)$
(1)	$\{1, 1, 1\}, \{-1, -1, 1\}$	0	$(q-1)/2$	$d(d+q-1)/2 - 3(d-2)/2$
(2)	$\{-1, 1, 1\}$	1	$(q-3)/2$	$d(d+q-1)/2$
(3)	$\{-1, -1, -1\}$	3	$(q-7)/2$	$d(d+q-1)/2$
(4)	$\{0, 1, 1\}, \{-1, 0, 1\}$	0	$(q-1)/2$	$d(d+q-1)/2 - (d-2)/2$
(5)	$\{-1, -1, 0\}$	0	$(q-1)/2$	$d(d+q-1)/2 - 3(d-2)/2$
(6)	$\{0, 0, 1\}$	0	$(q-1)/2$	$d(d+q-1)/2 - d(d-2)/2$
(7)	$\{-1, 0, 0\}$	d	-	-
(8)	$\{0, 0, 0\}$	0	$(q-1)/2$	$(d+q-1)/2 - 3d(d-2)/2$

Table 4 – Curve $\mathcal{F}$ for d odd.

	$\{\eta(e_0), \eta(e_1), \eta(e_2)\}$	n	d	$\#\mathcal{F}(\mathbb{F}_q)$
(1)	$\{1, 1, 1\}$	0	$(q-1)/2$	$d(d+q-1)/2$
(2)	$\{-1, 1, 1\}, \{-1, -1, -1\}$	0	$(q-1)/2$	$d(d+q-1)/2 - 3(d-2)/2$
(3)	$\{-1, -1, 1\}$	2	$(q-5)/2$	$d(d+q-1)/2$
(4)	$\{0, 1, 1\}$	0	$(q-1)/2$	$d(d+q-1)/2$
(5)	$\{-1, 0, 1\}, \{-1, -1, 0\}$	0	$(q-1)/2$	$d(d+q-1)/2 - (d-2)$
(6)	$\{0, 0, 1\}$	0	$(q-1)/2$	$d(d+q-1)/2 - d(d-2)/2$
(7)	$\{-1, 0, 0\}$	d	-	-
(8)	$\{0, 0, 0\}$	0	$(q-1)/2$	$d(d+q-1)/2 - 3d(d-2)/2$

Table 5 – Curve $\mathcal{F}$ for d even.

The first part of statement 2 follows directly from the results in Tables 4 and 5.

Now the nonsingularity and the classicality of $\mathcal{F}$ are discussed. First, recall that the absolute irreducibility of $\mathcal{F}$ was justified in Subsection 4.6.1. Therefore, the idea is to show that $\mathcal{F}$ attains the Stöhr-Voloch bound (4.7) (proving in particular the second part of statement 2) and consequently show that it is nonsingular by Theorem 4.3.3.

If

$$\#\mathcal{F}(\mathbb{F}_q) = \frac{1}{2}d(d+q-1),$$

then the proof is complete.

In all other cases, $\mathcal{F} = \mathcal{C}$ and a direct calculation using the information of Tables 6 and 7 shows that, for an $\mathbb{F}_q$ -rational point P with zero coordinates on $\mathcal{C}$ and tangent line $\mathcal{T}_P$, the intersection multiplicity of $\mathcal{C}$ and $\mathcal{T}_P$ at P is $I(P, \mathcal{C} \cap \mathcal{T}_P) = d$. It follows immediately from Theorem 4.3.3 and Tables 4 and 5 that the $\mathbb{F}_q$ -rational points with zero coordinates on $\mathcal{C}$ are exactly its (total) $\mathbb{F}_q$ -inflection points and that the Stöhr-Voloch bound (4.7) is attained. Hence, $\mathcal{F}$ is nonsingular.

Finally, the classicality of $\mathcal{F}$ is an immediate consequence of Theorem 4.3.4, since

$$\#\mathcal{F}(\mathbb{F}_q) > \frac{d(d+q-1)}{p^k}$$

for every $k \geq 1$ and, by the considerations in Subsection 4.6.1, $\mathcal{F}$ is an $\mathbb{F}_q$ -Frobenius classical plane curve of degree $d < q$. ■

$\{\eta(e_0), \eta(e_1), \eta(e_2)\}$	Points	Tangent lines
$\eta(e_0) = 1, \eta(e_1) = 1, \eta(e_2) = 1$	P_{01}	$e_1^{d-1}X_0 + e_0^{d-1}X_1 = 0$
	P_{02}	$e_2^{d-1}X_0 + e_0^{d-1}X_2 = 0$
	P_{12}	$e_2^{d-1}X_1 + e_1^{d-1}X_2 = 0$
$\eta(e_i) = -1, \eta(e_k) = -1, \eta(e_l) = 1$	P_i	$e_k e_i^{d-1}X_k + e_l e_i^{d-1}X_l = 0$
	P_k	$e_i e_k^{d-1}X_i + e_l e_k^{d-1}X_l = 0$
	P_{ik}	$e_k^{d-1}X_i + e_i^{d-1}X_k = 0$
$\eta(e_i) = 0, \eta(e_k) = 1, \eta(e_l) = 1$	P_{kl}	$e_l^{d-1}X_k + e_k^{d-1}X_l = 0$
$\eta(e_i) = -1, \eta(e_k) = 0, \eta(e_l) = 1$	P_i	$X_l = 0$
$\eta(e_i) = -1, \eta(e_k) = -1, \eta(e_l) = 0$	P_i	$X_k = 0$
	P_k	$X_i = 0$
	P_{ik}	$e_k^{d-1}X_i + e_i^{d-1}X_k = 0$
$\eta(e_i) = 0, \eta(e_k) = 0, \eta(e_l) = 1$	Set $\mathcal{A}_l$	$\{\alpha_i^{d-1}X_i + X_k = 0 : \eta(\alpha_i) = -1\}$
$\eta(e_0) = 0, \eta(e_1) = 0, \eta(e_2) = 0$	Set $\mathcal{A}_0$	$\{\alpha_1^{d-1}X_1 + X_2 = 0 : \eta(\alpha_1) = -1\}$
	Set $\mathcal{A}_1$	$\{\alpha_0^{d-1}X_0 + X_2 = 0 : \eta(\alpha_0) = -1\}$
	Set $\mathcal{A}_2$	$\{\alpha_0^{d-1}X_0 + X_1 = 0 : \eta(\alpha_0) = -1\}$

Table 6 – $\mathbb{F}_q$ -points P with zero coordinates on $\mathcal{C}$ with their respective tangent lines, for d odd and $\{\eta(e_i), \eta(e_k), \eta(e_l)\} = \{\eta(e_0), \eta(e_1), \eta(e_2)\}$, only in cases where $\#\mathcal{F}(\mathbb{F}_q) < \frac{1}{2}d(d+q-1)$.

$\{\eta(e_0), \eta(e_1), \eta(e_2)\}$	Points	Tangent lines
$\eta(e_i) = -1, \eta(e_k) = 1, \eta(e_l) = 1$	P_i	$e_k e_i^{d-1}X_k + e_l e_i^{d-1}X_l = 0$
	P_{ik}	$e_k^{d-1}X_i - e_i^{d-1}X_k = 0$
	P_{il}	$e_l^{d-1}X_i - e_i^{d-1}X_l = 0$
$\eta(e_0) = -1, \eta(e_1) = -1, \eta(e_2) = -1$	P_0	$e_1 e_0^{d-1}X_1 + e_2 e_0^{d-1}X_2 = 0$
	P_1	$e_0 e_1^{d-1}X_0 + e_2 e_1^{d-1}X_2 = 0$
	P_2	$e_0 e_2^{d-1}X_0 + e_1 e_2^{d-1}X_1 = 0$
$\eta(e_i) = -1, \eta(e_k) = 0, \eta(e_l) = 1$	P_i	$X_l = 0$
	P_{il}	$e_l^{d-1}X_i - e_i^{d-1}X_l = 0$
$\eta(e_i) = -1, \eta(e_k) = -1, \eta(e_l) = 0$	P_i	$X_k = 0$
	P_k	$X_i = 0$
$\eta(e_i) = 0, \eta(e_k) = 0, \eta(e_l) = 1$	Set $\mathcal{A}_l$	$\{\alpha_i^{d-1}X_i + X_k = 0 : \eta(\alpha_i) = -1\}$
$\eta(e_0) = 0, \eta(e_1) = 0, \eta(e_2) = 0$	Set $\mathcal{A}_0$	$\{\alpha_1^{d-1}X_1 + X_2 = 0 : \eta(\alpha_1) = -1\}$
	Set $\mathcal{A}_1$	$\{\alpha_0^{d-1}X_0 + X_2 = 0 : \eta(\alpha_0) = -1\}$
	Set $\mathcal{A}_2$	$\{\alpha_0^{d-1}X_0 + X_1 = 0 : \eta(\alpha_0) = -1\}$

Table 7 – $\mathbb{F}_q$ -points P with zero coordinates on $\mathcal{C}$ with their respective tangent lines, for d even and $\{\eta(e_i), \eta(e_k), \eta(e_l)\} = \{\eta(e_0), \eta(e_1), \eta(e_2)\}$, only in cases where $\#\mathcal{F}(\mathbb{F}_q) < \frac{1}{2}d(d+q-1)$.

ON SOME GENERALIZED FERMAT CURVES AND CHORDS OF AN AFFINELY REGULAR POLYGON INSCRIBED IN A HYPERBOLA

The present chapter is an extended and adapted version of (BORGES; COUTINHO, 2019).

5.1 Introduction

Let $\mathbb{F}_q$ be the finite field with $q = p^m$ elements, where p is a prime number, and let $\mathcal{Y}$ be a nonsingular geometrically irreducible curve of genus g defined over $\mathbb{F}_q$. A fundamental problem in the theory of curves over finite fields is estimating the number $N_q(\mathcal{Y})$ of $\mathbb{F}_q$ -rational points on $\mathcal{Y}$. Apart from a few classes of curves (see (MOISIO, 2007) and (ARAKELIAN; BORGES, 2017) for instance), there is usually no explicit formula for $N_q(\mathcal{Y})$. Nevertheless, some effective upper bounds for this number can be found in the literature. A famous example, as introduced in Chapter 2, is the Hasse-Weil bound

$$N_q(\mathcal{Y}) \leq q + 1 + 2gq^{1/2}. \quad (5.1)$$

Another noteworthy approach to bound $N_q(\mathcal{Y})$ was established by Stöhr and Voloch in 1986. Their method, more geometric in nature, provides bounds that are dependent on the choice of an embedding of the curve in some $\mathbb{P}^M(\overline{\mathbb{F}_q})$, and which improve (5.1) in several circumstances (see (GARCIA; VOLOCH, 1988) for instance). For more details on the Stöhr-Voloch theory, see also Chapter 3.

For $a, b \in \mathbb{F}_q$ satisfying $ab \notin \{0, 1\}$, let $\mathcal{F}$ be the plane curve with affine equation given by

$$F(X, Y) = aX^d Y^d - X^d - Y^d + b = 0. \quad (5.2)$$

This provides an example of a generalized Fermat curve, having been studied from the point of view of its automorphism group in (ARAKELIAN; SPEZIALI, 2017).

The number $N_q(\mathcal{X})$ of $\mathbb{F}_q$ -rational points on the nonsingular model $\mathcal{X}$ defined over $\mathbb{F}_q$ of $\mathcal{F}$ was first investigated in the context of finite geometry to study the number of chords of an affinely regular polygon in $\mathbb{A}^2(\mathbb{F}_q)$ passing through a given point (see (ABATANGELO; KORCHMÁROS, 1997), (GIULIETTI, 2008)). More precisely, using the Stöhr-Voloch theory, in (ABATANGELO; KORCHMÁROS, 1997) Abatangelo and Korchmáros provided an upper bound for $N_q(\mathcal{X})$ based on the choice of an embedding of $\mathcal{X}$ in $\mathbb{P}^5(\overline{\mathbb{F}_q})$, and then on the study of its $\mathbb{F}_q$ -Frobenius (non)classicality. Later on, Giulietti remarkably improved Abatangelo and Korchmáros' bound by considering a suitable embedding of $\mathcal{X}$ in $\mathbb{P}^3(\overline{\mathbb{F}_q})$ (GIULIETTI, 2008). Further, more recently, and also using the Stöhr-Voloch theory, the number $N_q(\mathcal{X})$ was investigated in (FANALI; GIULIETTI, 2012) in the context of generalized Fermat curves.

Accordingly, in terms of the Stöhr-Voloch theory, for $\overline{\mathbb{F}_q}(\mathcal{X}) = \overline{\mathbb{F}_q}(x, y)$, where x, y satisfy the polynomial equation given by $\mathcal{F}$, and $s \in \{2, \dots, d-1\}$, in this chapter an upper bound for $N_q(\mathcal{X})$ with respect to the nondegenerate morphism

$$(\dots : x^i y^k : \dots) : \mathcal{X} \rightarrow \mathbb{P}^N(\overline{\mathbb{F}_q}), \quad (5.3)$$

with i, k integers satisfying $0 \leq i, k \leq s-1$ and $0 \leq i+k \leq s$, is determined in cases where it is $\mathbb{F}_q$ -Frobenius classical.

Further, based on techniques developed by Garcia and Voloch in (GARCIA; VOLOCH, 1988, Section 3) and improved by Mattarei in (MATTAREI, 2007), the attention is focused on the case where $q = p$ is prime. In particular, if $d = (p-1)/n \geq 3$ is a proper divisor of $p-1$, and $p \leq d^4/4$, for an affinely regular n -gon inscribed in a hyperbola, it is obtained that the number $n_{(a,b)}$ of its chords passing through $(a, b) \in \mathbb{A}^2(\mathbb{F}_q)$ is bounded roughly by

$$3 \cdot (2^{-1} \cdot n)^{2/3}, \quad (5.4)$$

which improves in several cases the upper bound for $n_{(a,b)}$ given in (GIULIETTI, 2008, Theorem 4.1):

$$n_{(a,b)} \leq \frac{n+1}{3}. \quad (5.5)$$

This chapter is organized as follows. In Section 5.3, the number $N_q(\mathcal{X})$ is studied. For each $s \in \{2, \dots, d-1\}$, an upper bound for $N_q(\mathcal{X})$ is provided in cases where the morphism (5.3) is $\mathbb{F}_q$ -Frobenius classical. In Subsection 5.3.1, the particular case in which $\mathbb{F}_q$ is the prime field $\mathbb{F}_p$ is addressed. Finally, in Subsection 5.4.1 some aspects of the theory of affinely regular polygons are established, with the bound (5.4) being presented in Subsection 5.4.2.

5.2 Notation

The following notation is used throughout this chapter.

- Here, for an arbitrary field $\mathbb{K}$, $\mathbb{K} \setminus \{0\}$ is denoted by $\mathbb{K}^*$.
- P_1 and P_2 are the points $(1 : 0 : 0)$ and $(0 : 1 : 0)$ of $\mathbb{P}^2(\overline{\mathbb{F}_q})$, respectively.
- Unless otherwise stated, a curve denotes a geometrically irreducible curve.
- For a nonsingular curve $\mathcal{Y}$ defined over $\mathbb{F}_q$, $\overline{\mathbb{F}_q}(\mathcal{Y})$ is its function field, $\mathbb{F}_q(\mathcal{Y})$ is its $\mathbb{F}_q$ -rational function field, $\mathcal{Y}(\mathbb{F}_q)$ is the set of its $\mathbb{F}_q$ -rational points, and $N_q(\mathcal{Y})$ is its number of $\mathbb{F}_q$ -rational points.

5.3 The curve $\mathcal{F}$

The following result, which provides basic information about $\mathcal{F}$, can be found in (ABATANGELO; KORCHMÁROS, 1997, Proposition 3.3).

Proposition 5.3.1. Let d be a divisor of $q - 1$. Then, the following holds:

1. The curve $\mathcal{F}$ is geometrically irreducible.
2. The genus of $\mathcal{F}$ is $(d - 1)^2$.
3. The only singular points of $\mathcal{F}$ are P_1 and P_2 , and each singularity is ordinary with multiplicity d . Also, the tangent lines to $\mathcal{F}$ at P_1 and P_2 are given by the affine equations $Y = \alpha$ and $X = \alpha$, respectively, where $\alpha^d = a^{-1}$, and those tangent lines intersect $\mathcal{F}$ at the corresponding points with multiplicity $2d$.
4. The intersection multiplicity of a branch centered at P_1 or P_2 with its tangent line is $d + 1$.
5. The points $(\beta : 0 : 1)$ and $(0 : \beta : 1)$, with $\beta^d = b$, are inflection points of $\mathcal{F}$. Further, the tangent lines to $\mathcal{F}$ at $(\beta : 0 : 1)$ and $(0 : \beta : 1)$ are given by the affine equations $X = \beta$ and $Y = \beta$, respectively, and those tangent lines intersect $\mathcal{F}$ at the corresponding points with multiplicity d .

For each $s \in \{2, \dots, d - 1\}$, consider the base-point-free linear series $\mathcal{D}_s^{P_1, P_2} \subset \text{Div}(\mathcal{X})$ corresponding to the nondegenerate morphism given in (5.3). In other words, let $\mathcal{D}_s^{P_1, P_2}$ be the base-point-free linear series cut out on $\mathcal{F}$ by all plane curves (not necessarily irreducible) of degree s passing through the singularities P_1 and P_2 of $\mathcal{F}$.

The following proposition presents some important facts related to the linear series $\mathcal{D}_s^{P_1, P_2}$.

Proposition 5.3.2. For each $s \in \{2, \dots, d - 1\}$, the following occurs:

1. The linear series $\mathcal{D}_s^{P_1, P_2}$ has dimension $N = \binom{s+2}{2} - 3$ and degree $\mathbf{d} = 2d \cdot (s - 1)$.
2. For $Q \in \mathcal{X}$ corresponding to a point of $\mathcal{F}$ of the form $(\beta : 0 : 1)$ or $(0 : \beta : 1)$, with $\beta^d = b$, the $(\mathcal{D}_s^{P_1, P_2}, Q)$ -order sequence is given by the elements of

$$\left\{ i + kd : 0 \leq i, k \leq s - 1 \text{ and } 0 \leq i + k \leq s \right\}.$$

3. For $Q_b \in \mathcal{X}$ corresponding to a branch $\mathfrak{b}$ of $\mathcal{F}$ centered at P_1 or P_2 , the $(\mathcal{D}_s^{P_1, P_2}, Q_b)$ -order sequence is given by the elements of

$$\left\{ i + k(d+1) - 1 : 0 \leq i, k \text{ and } 0 \leq i + k \leq s \right\} \setminus \left\{ -1, s(d+1) - 1 \right\}.$$

Proof. Considering the definitions given in Subsection 1.2.10, for each $s \in \{2, \dots, d-1\}$, let $\Sigma_s^{P_1, P_2}$ be the linear system of all plane curves (not necessarily irreducible) of degree s passing through the singularities P_1 and P_2 of $\mathcal{F}$, and let

$$\tilde{\mathcal{D}}_s^{P_1, P_2} = \left\{ \mathcal{G} \bullet \mathcal{F} : \mathcal{G} \in \Sigma_s^{P_1, P_2} \right\}$$

be the linear series cut out on $\mathcal{F}$ by the linear system $\Sigma_s^{P_1, P_2}$. Since $\Sigma_s^{P_1, P_2}$ has dimension $\binom{s+2}{2} - 3$, and $s < 2d$, $\tilde{\mathcal{D}}_s^{P_1, P_2}$ has also dimension equal to $\binom{s+2}{2} - 3$ by Proposition 1.2.73. Further, by Bézout's Theorem (see Theorem 1.1.36), $\tilde{\mathcal{D}}_s^{P_1, P_2}$ has degree $2ds$.

The base locus of $\tilde{\mathcal{D}}_s^{P_1, P_2}$ is the divisor

$$\mathcal{L}_\infty \bullet \mathcal{F} = Q_1^{(1)} + \dots + Q_d^{(1)} + Q_1^{(2)} + \dots + Q_d^{(2)}$$

of degree $2d$, where, for $i = 1, 2$ and $k = 1, \dots, d$, the $Q_k^{(i)}$'s are all the distinct points on $\mathcal{X}$ for which the corresponding branches are centered at P_i , and $\mathcal{L}_\infty : Z = 0$.

Therefore,

$$\mathcal{D}_s^{P_1, P_2} = \tilde{\mathcal{D}}_s^{P_1, P_2} - \mathcal{L}_\infty \bullet \mathcal{F} = \left\{ D - \mathcal{L}_\infty \bullet \mathcal{F} : D \in \tilde{\mathcal{D}}_s^{P_1, P_2} \right\} \quad (5.6)$$

has dimension $\binom{s+2}{2} - 3$ and degree $2ds - 2d = 2d \cdot (s - 1)$, which proves statement 1.

To prove statement 2, let $Q \in \mathcal{X}$ be a point corresponding to $P \in \mathcal{F}$, where P is equal to $(\beta : 0 : 1)$ or $(0 : \beta : 1)$, with $\beta^d = b$, and for $i = 1, 2$, let $\mathcal{L}_i$ be the line passing through P and P_i . One can verify that none of the lines $\mathcal{L}_1$ and $\mathcal{L}_2$ is equal to $\mathcal{L}_\infty$, and exactly one of them is the tangent line to $\mathcal{F}$ at P . Further, from Proposition 5.3.1, the $(\mathcal{D}_1, Q)$ -order sequence is $(0, 1, d)$, where $\mathcal{D}_1$ is the base-point-free linear series cut out on $\mathcal{F}$ by the linear system of lines. Therefore, considering the reducible plane curves $\mathcal{C}$ given by the union of s lines chosen (with multiplicity) in the set $\{\mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_\infty\}$, the $(\mathcal{D}_s^{P_1, P_2}, Q)$ -order sequence is given by the elements of

$$\left\{ i + kd : 0 \leq i, k \leq s - 1 \text{ and } 0 \leq i + k \leq s \right\}.$$

Finally, if $Q_b \in \mathcal{X}$ corresponds to a branch $\mathfrak{b}$ of $\mathcal{F}$ centered at P_1 or P_2 , from Proposition 5.3.1, the $(\mathcal{D}_1, Q_b)$ -order sequence is $(0, 1, d+1)$. Thus, considering the reducible plane curves $\mathcal{C}$ passing through P_1 and P_2 , and given by the union of s lines (possibly chosen with multiplicity), equation (5.6) shows that the $(\mathcal{D}_s^{P_1, P_2}, Q_b)$ -order sequence is comprised by the elements of

$$\left\{ i + k(d+1) - 1 : 0 \leq i, k \text{ and } 0 \leq i + k \leq s \right\} \setminus \left\{ -1, s(d+1) - 1 \right\},$$

which completes the proof. ■

Based on Theorem 3.2.12 and Proposition 5.3.2, the following result provides an upper bound for the number $N_q(\mathcal{X})$ in cases where $\mathcal{D}_s^{P_1, P_2}$ is $\mathbb{F}_q$ -Frobenius classical.

Corollary 5.3.3. Let $s \in \{2, \dots, d-1\}$. If $\mathcal{D}_s^{P_1, P_2}$ is $\mathbb{F}_q$ -Frobenius classical, then

$$N_q(\mathcal{X}) \leq (N-1) \cdot (d^2 - 2d) + \frac{d \cdot (q+N)}{N} - 2 \cdot \frac{d_1 \cdot \Upsilon_1 + d_2 \cdot \Upsilon_2 + d \cdot \Upsilon}{N}, \quad (5.7)$$

where

- d_1 and d_2 are the number of roots in $\mathbb{F}_q$ of the polynomials $T^d - b$ and $T^d - a^{-1}$, respectively;
- $\Upsilon_1 = 1 + (s-1) \cdot d - N$;
- $\Upsilon_2 = (s-1) \cdot (d+1) - N$;
- $\Upsilon = 2(d+1) - s \cdot (4d+3) - N \cdot (N-1) + (s \cdot (2d+3) - 3) \cdot \frac{N+3}{3}$.

Proof. The part

$$(N-1) \cdot (d^2 - 2d) + \frac{d \cdot (q+N)}{N}$$

of (5.7) follows directly from Theorem 3.2.12, since $\mathcal{D}_s^{P_1, P_2}$ is $\mathbb{F}_q$ -Frobenius classical and the genus of $\mathcal{F}$ is $(d-1)^2$ by Proposition 5.3.1.

Further, let $Q \in \mathcal{X}$ be a point corresponding to $(\beta : 0 : 1)$ or $(0 : \beta : 1) \in \mathcal{F}$, with $\beta^d = b$, and let $Q_b \in \mathcal{X}$ be a point corresponding to a branch $\mathfrak{b}$ of $\mathcal{F}$ centered at P_1 or P_2 . Using the same notation of Theorem 3.2.12, from Proposition 5.3.2, the numbers $A(Q)$ and $A(Q_b)$ are given by the following expressions:

$$A(Q) = \begin{cases} s \cdot (d+1) \cdot \frac{-6 + (s+1) \cdot (s+2)}{6} - \frac{N \cdot (N-1)}{2} - N, & \text{if } Q \in \mathcal{X}(\mathbb{F}_q) \\ s \cdot (d+1) \cdot \frac{-6 + (s+1) \cdot (s+2)}{6} - \frac{N \cdot (N-1)}{2} - (1 + (s-1) \cdot d), & \text{otherwise} \end{cases} \quad (5.8)$$

and

$$A(Q_b) = \begin{cases} 2 - s \cdot (d+1) + (s \cdot (d+2) - 3) \cdot \frac{(s+1) \cdot (s+2)}{6} - \frac{N(N-1)}{2}, & \text{if } Q_b \in \mathcal{X}(\mathbb{F}_q) \\ 2 - s \cdot (d+1) + (s \cdot (d+2) - 3) \cdot \frac{(s+1) \cdot (s+2)}{6} - \frac{N(N-1)}{2} - (s-1) \cdot (d+1), & \text{otherwise} \end{cases} \quad (5.10)$$

since

$$\sum_{i=1}^N j_i(Q) = s \cdot (d+1) \cdot \frac{-6 + (s+1) \cdot (s+2)}{6} \text{ with } j_N(Q) = 1 + (s-1) \cdot d,$$

and

$$\sum_{i=1}^N j_i(Q_b) = 2 - s \cdot (d+1) + (s \cdot (d+2) - 3) \cdot \frac{(s+1) \cdot (s+2)}{6} \text{ with } j_N(Q_b) = (s-1) \cdot (d+1).$$

Therefore,

$$\begin{aligned} N_q(\mathcal{X}) &\leq (N-1) \cdot (d^2 - 2d) + \frac{d \cdot (q+N)}{N} \\ &\quad - \frac{2d_1 \cdot A(Q)^{(5.8)} + 2(d-d_1) \cdot A(Q)^{(5.9)} + 2d_2 \cdot A(Q_b)^{(5.10)} + 2(d-d_2) \cdot A(Q_b)^{(5.11)}}{N} \\ &= (N-1) \cdot (d^2 - 2d) + \frac{d \cdot (q+N)}{N} - 2 \cdot \frac{d_1 \cdot \Upsilon_1 + d_2 \cdot \Upsilon_2 + d \cdot \Upsilon}{N}, \end{aligned}$$

where

- d_1 and d_2 are the number of roots in $\mathbb{F}_q$ of the polynomials $T^d - b$ and $T^d - a^{-1}$, respectively;
- $\Upsilon_1 = A(Q)^{(5.8)} - A(Q)^{(5.9)} = 1 + (s-1) \cdot d - N$;
- $\Upsilon_2 = A(Q_b)^{(5.10)} - A(Q_b)^{(5.11)} = (s-1) \cdot (d+1) - N$;
- $\Upsilon = A(Q)^{(5.9)} + A(Q_b)^{(5.11)} = 2(d+1) - s \cdot (4d+3) - N \cdot (N-1) + (s \cdot (2d+3) - 3) \cdot \frac{N+3}{3}$.

■

5.3.1 The case $q = p$

From now on, let $\mathbb{F}_q$ be the prime field $\mathbb{F}_p$. Our purpose here is to prove the following theorem, which is the main result of this chapter.

Theorem 5.3.4. Let $d \geq 3$ be a proper divisor of $p-1$ and $n = (p-1)/d$. If $p-1 \leq d \cdot \left(\frac{(d+3) \cdot (d+4) \cdot (3d-1)}{12} - 3 \right)$, then

$$N_p(\mathcal{X}) \leq d^2 \cdot \left(3 \cdot (2^{1/2} \cdot n)^{2/3} - \frac{103}{19} \cdot (2^{1/2} \cdot n)^{1/3} + \frac{13}{3} \right).$$

However, before proving it, some lemmas, which are presented in Subsection 5.3.1.1, need to be introduced.

5.3.1.1 Preliminaries

For each $u \in [2, +\infty)$ and $t_0 \in [6, +\infty)$, let us define

$$\begin{aligned} f_u : [6, +\infty) &\rightarrow \mathbb{R} \\ t &\mapsto \frac{3t^2 - 23t + 26}{6} + 4 \cdot \frac{u+3}{t}, \end{aligned}$$

and

$$n_{t_0} := \frac{t_0 \cdot (t_0 + 1) \cdot (3t_0 - 10)}{12} - 3 = \frac{1}{4}t_0^3 - \frac{7}{12}t_0^2 - \frac{5}{6}t_0 - 3.$$

Lemma 5.3.5. The following occurs:

1. For $u \in [2, +\infty)$, f_u is continuous in $[6, +\infty)$, and has derivatives of all orders in $(6, +\infty)$.

2. Let $t_0 \in [6, +\infty)$. For $u \in [2, +\infty)$,

$$u \leq n_{t_0} \quad \text{if and only if} \quad f_u(t_0) \leq f_u(t_0 + 1).$$

3. Fixed $u \in [n_6, +\infty)$,

a) There is only one $t_0 \in [6, +\infty)$ such that $u = n_{t_0}$.

b) f_u has a local minimum at some $t_{\min} \in (t_0, t_0 + 1)$. Moreover: since f_u is decreasing in $[6, t_{\min}]$ and increasing in $[t_{\min}, +\infty)$, $t_{\min}$ is the global minimum point of f_u .

Proof. The proof of item 1 is straightforward. Also, item 2 follows from the following equivalences

$$\begin{aligned} f_u(t_0) \leq f_u(t_0 + 1) &\Leftrightarrow \frac{3t_0^2 - 23t_0 + 26}{6} + 4 \cdot \frac{u+3}{t_0} \leq \frac{3(t_0+1)^2 - 23(t_0+1) + 26}{6} + 4 \cdot \frac{u+3}{t_0+1} \\ &\Leftrightarrow 4 \cdot \frac{u+3}{t_0} - 4 \cdot \frac{u+3}{t_0+1} \leq \frac{3(t_0+1)^2 - 23(t_0+1) + 26}{6} - \frac{3t_0^2 - 23t_0 + 26}{6} \\ &\Leftrightarrow 4 \cdot \frac{u+3}{t_0 \cdot (t_0+1)} \leq \frac{6t_0 + 3 - 23}{6} \\ &\Leftrightarrow u+3 \leq \frac{t_0 \cdot (t_0+1) \cdot (3t_0 - 10)}{12}. \end{aligned}$$

In order to prove item 3-a), let us consider the function

$$\begin{aligned} f: [6, +\infty) &\rightarrow \mathbb{R} \\ t &\mapsto \frac{t \cdot (t+1) \cdot (3t-10)}{12} - 3 = \frac{1}{4}t^3 - \frac{7}{12}t^2 - \frac{5}{6}t - 3. \end{aligned}$$

Since

$$\frac{df}{dt}(t) = \frac{3}{4}t^2 - \frac{7}{6}t - \frac{5}{6} > 0$$

for all $t \in (6, +\infty)$, this function is increasing and thus a bijection over its image $[n_6, +\infty)$. In particular, for each $u \in [n_6, +\infty)$, there is only one $t_0 \in [6, +\infty)$ such that $u = n_{t_0}$.

Now, to prove item 3-b), let us fix $u \in [n_6, +\infty)$ and let $t_0 \in [6, +\infty)$ be such that $u = n_{t_0}$. Then, by item 2, $f_u(t_0) = f_u(t_0 + 1)$, and thus, by Rolle's Theorem

$$\frac{df_u}{dt}(t_{\min}) = 0$$

for some $t_{\min} \in (t_0, t_0 + 1)$. Since

$$\frac{d^2f_u}{dt^2}(t_{\min}) = 1 + 8 \cdot \frac{u+3}{t_{\min}^3} > 0,$$

$t_{\min}$ is a local minimum point of f_u . Also, from

$$\frac{df_u}{dt}(t) = \frac{6t - 23}{6} - 4 \cdot \frac{u+3}{t^2}$$

for all $t \in (6, +\infty)$, it follows that

$$\frac{df_u}{dt}(t) < 0$$

for all $t \in (6, t_{min})$, and

$$\frac{df_u}{dt}(t) > 0$$

for all $t \in (t_{min}, +\infty)$. Indeed,

$$\begin{aligned} \frac{df_u}{dt}(t) = 0 &\Leftrightarrow t^3 - \frac{23}{6}t^2 - 4(u+3) = 0 \\ &\Leftrightarrow t = t_{min}, \end{aligned}$$

as the discriminant $\Delta(u) = -432u^2 - \frac{94318}{27}u - \frac{59326}{9}$ of the polynomial $T^3 - \frac{23}{6}T^2 - 4(u+3)$ is negative. Hence, the statement follows from the continuity of $\frac{df_u}{dt}$ in $(6, +\infty)$, since $t_0 \geq 6$ implies that

$$\frac{df_u}{dt}(t_0) = \frac{6t_0 - 23}{6} - 4 \cdot \left(\frac{3}{12}t_0 - \frac{7}{12} - \frac{10}{12} \cdot \frac{1}{t_0} \right) = -\frac{46}{12} + \frac{28}{12} + \frac{40}{12} \cdot \frac{1}{t_0} = \frac{-18t_0 + 40}{12t_0} < 0,$$

and

$$\begin{aligned} \frac{df_u}{dt}(t_0 + 1) &= \frac{6(t_0 + 1) - 23}{6} - 4 \cdot \left(\frac{3t_0^3 - 7t_0^2 - 10t_0}{12(t_0 + 1)^2} \right) \\ &= \frac{12(t_0 + 1)^3 - 46(t_0 + 1)^2 - 4 \cdot (3t_0^3 - 7t_0^2 - 10t_0)}{12(t_0 + 1)^2} \\ &= \frac{18t_0^2 - 16t_0 - 34}{12(t_0 + 1)^2} \\ &> 0. \end{aligned}$$

Therefore, f_u is decreasing in $[6, t_{min}]$ and increasing in $[t_{min}, +\infty)$, which gives in particular that t_{min} is a global minimum point of f_u . This completes the proof. $\blacksquare$

Lemma 5.3.6. Let $t_0 \in \mathbb{Z} \cap [6, +\infty)$. If $n_{t_0} \leq u \leq n_{t_0+1}$, then

$$\min \left\{ f_u(t) : t \in \mathbb{Z} \cap [6, +\infty) \right\} = f_u(t_0 + 1). \quad (5.12)$$

Furthermore, if $2 \leq u < n_6$, then

$$\min \left\{ f_u(t) : t \in \mathbb{Z} \cap [6, +\infty) \right\} = f_u(6). \quad (5.13)$$

Proof. If $u = n_{t_0}$, then from item 3 of Lemma 5.3.5,

$$\min \left\{ f_u(t) : t \in [6, +\infty) \right\} = f_u(t_{min}),$$

for some $t_{min} \in (t_0, t_0 + 1)$, and f_u is decreasing in $[6, t_{min}]$ and increasing in $[t_{min}, +\infty)$. Therefore,

$$\min \left\{ f_u(t) : t \in \mathbb{Z} \cap [6, +\infty) \right\} = f_u(t_0) = f_u(t_0 + 1).$$

Analogously, if $u = n_{t_0+1}$, then

$$\min \left\{ f_u(t) : t \in \mathbb{Z} \cap [6, +\infty) \right\} = f_u(t_0 + 1) = f_u(t_0 + 2).$$

Thus, in the previous two cases, (5.12) holds.

Now, consider $n_{t_0} < u < n_{t_0+1}$. From item 2 of Lemma 5.3.5, since $u < n_{t_0+i}$, for all $i \in \mathbb{Z} \cap [1, +\infty)$, it is obtained that

$$f_u(t_0 + 1) < f_u(t_0 + 2) < f_u(t_0 + 3) < \dots$$

Also, since $n_{t_0-i} < u$, for all $i \in \{0, \dots, t_0 - 6\}$, again from item 2 of Lemma 5.3.5, it follows that

$$f_u(t_0 + 1) < f_u(t_0) < f_u(t_0 - 1) < f_u(t_0 - 2) < \dots < f_u(6).$$

This completes the proof of (5.12).

Further, if $2 \leq u < n_6$, since $n_6 < n_{6+i}$, for all $i \in \mathbb{Z} \cap [1, +\infty)$, then, from item 2 of Lemma 5.3.5,

$$f_u(6) < f_u(7) < f_u(8) < \dots$$

This proves the equality (5.13). ■

Lemma 5.3.7. Let $d \geq 3$ be a proper divisor of $p - 1$, and $n = (p - 1)/d$. Then,

$$\min \left\{ f_n(t) : t \in \mathbb{Z} \cap [6, d + 3] \text{ and } t \leq n/2 + 5 \right\} = \min \left\{ f_n(t) : t \in \mathbb{Z} \cap [6, d + 3] \right\}.$$

Moreover: if $n \leq n_{d+3}$, then

$$\min \left\{ f_n(t) : t \in \mathbb{Z} \cap [6, d + 3] \text{ and } t \leq n/2 + 5 \right\} = \min \left\{ f_n(t) : t \in \mathbb{Z} \cap [6, +\infty) \right\}.$$

Proof. Let $t_0 = \lfloor n/2 + 5 \rfloor$. Then,

$$t_0 = \begin{cases} n/2 + 5, & \text{if } n \text{ is even} \\ (n+9)/2, & \text{if } n \text{ is odd} \end{cases}$$

and $n < n_{t_0}$. Also, $n_{t_0} < n_{t_0+i}$, for all $i \in \mathbb{Z} \cap [1, +\infty)$, implies by item 2 of Lemma 5.3.5 that

$$f_n(t_0) < f_n(t_0 + 1) < f_n(t_0 + 2) < f_n(t_0 + 3) < \dots$$

Therefore,

$$\min \left\{ f_n(t) : t \in \mathbb{Z} \cap [6, d + 3] \text{ and } t \leq n/2 + 5 \right\} = \min \left\{ f_n(t) : t \in \mathbb{Z} \cap [6, d + 3] \right\}.$$

Further, $n_{d+3} < n_{d+3+i}$, for all $i \in \mathbb{Z} \cap [1, +\infty)$. In particular, if $n \leq n_{d+3}$, then item 2 of Lemma 5.3.5 implies also that

$$f_n(d + 3) \leq f_n(d + 4) < f_n(d + 5) < f_n(d + 6) < \dots$$

and thus

$$\min \left\{ f_n(t) : t \in \mathbb{Z} \cap [6, d + 3] \text{ and } t \leq n/2 + 5 \right\} = \min \left\{ f_n(t) : t \in \mathbb{Z} \cap [6, +\infty) \right\},$$

which completes the proof. ■

5.3.1.2 The proof of Theorem 5.3.4

Let $d \geq 3$ be a proper divisor of $p - 1$. If $n = (p - 1)/d$, from Corollary 5.3.3 and its proof,

$$\begin{aligned}
 N_p(\mathcal{X}) &\leq (N - 1) \cdot (d^2 - 2d) + \frac{d \cdot (p + N)}{N} - 2 \cdot \frac{d_1 \cdot \Upsilon_1 + d_2 \cdot \Upsilon_2 + d \cdot \Upsilon}{N} \\
 &\leq (N - 1) \cdot (d^2 - 2d) + \frac{d \cdot (p + N)}{N} - \frac{2d \cdot \Upsilon}{N} \\
 &= \frac{\frac{1}{2}s^3 + \frac{13}{6}s^2 - \frac{7}{3}s - 4}{s + 4} \cdot d^2 + \frac{4d \cdot (p \cdot (s - 1) + 1)}{(s + 4) \cdot (s - 1)} \\
 &= \frac{\frac{1}{2}s^3 + \frac{13}{6}s^2 - \frac{7}{3}s - 4}{s + 4} \cdot d^2 + \frac{4d \cdot ((p - 1) \cdot (s - 1) + s)}{(s + 4) \cdot (s - 1)} \\
 &\leq \frac{\frac{1}{2}s^3 + \frac{13}{6}s^2 - \frac{7}{3}s - 4}{s + 4} \cdot d^2 + \frac{4d \cdot ((p - 1) \cdot (s - 1) + d)}{(s + 4) \cdot (s - 1)} \\
 &= \frac{\frac{1}{2}s^3 + \frac{13}{6}s^2 - \frac{7}{3}s - 4}{s + 4} \cdot d^2 + \frac{4d \cdot (d \cdot n \cdot (s - 1) + d)}{(s + 4) \cdot (s - 1)} \\
 &= d^2 \cdot \left(\frac{\frac{1}{2}s^3 + \frac{13}{6}s^2 - \frac{7}{3}s - 4}{s + 4} + 4 \cdot \left(\frac{n}{s + 4} + \frac{1}{(s + 4) \cdot (s - 1)} \right) \right) \\
 &\leq d^2 \cdot \left(\frac{\frac{1}{2}s^3 + \frac{13}{6}s^2 - \frac{7}{3}s - 4}{s + 4} + 4 \cdot \frac{n + 1}{s + 4} \right),
 \end{aligned}$$

for each $s \in \{2, \dots, d - 1\}$ satisfying $2d \cdot (s - 1) \leq p - 1$, since the latter condition, together with Propositions 3.2.13 and Proposition 5.3.2, implies that $\mathcal{D}_s^{P_1, P_2}$ is $\mathbb{F}_p$ -Frobenius classical. Hence, defining $t := s + 4$, it follows that

$$N_p(\mathcal{X}) \leq d^2 \cdot \left(\frac{3t^2 - 23t + 26}{6} + 4 \cdot \frac{n + 3}{t} \right),$$

for all $t \in \{6, \dots, d + 3\}$ satisfying $t \leq \frac{n}{2} + 5$, and

$$\frac{N_p(\mathcal{X})}{d^2} \leq V(n) := \min \left\{ \frac{3t^2 - 23t + 26}{6} + 4 \cdot \frac{n + 3}{t} : t \in \{6, \dots, d + 3\} \text{ and } t \leq \frac{n}{2} + 5 \right\}.$$

Consider the notation given as in Subsection 5.3.1.1. From the hypotheses, $n \leq n_{d+3} = \frac{(d+3) \cdot (d+4) \cdot (3d-1)}{12} - 3$. Therefore, Lemma 5.3.7 implies the equality

$$V(n) = \min \left\{ f_n(t) : t \in \mathbb{Z} \cap [6, +\infty) \right\}.$$

The objective is to determine a suitable function W such that $W(n) \geq V(n)$, for all prime numbers p and for all proper divisors $d \geq 3$ of $p - 1$, where $n = (p - 1)/d$. Defining for each $u \in [2, +\infty)$

$$\tilde{V}(u) := \min \left\{ f_u(t) : t \in \mathbb{Z} \cap [6, +\infty) \right\},$$

Lemma 5.3.6 implies that

$$\tilde{V}(u) = \begin{cases} f_u(t_0 + 1), & \text{if } n_{t_0} \leq u \leq n_{t_0+1} \text{ for some } t_0 \in \mathbb{Z} \cap [6, +\infty) \\ f_u(6), & \text{if } 2 \leq u \leq n_6, \end{cases}$$

and by Lemma 5.3.5

$$\tilde{V}(n_{t_0}) = f_{n_{t_0}}(t_0) = \frac{3}{2}t_0^2 - \frac{37}{6}t_0 + 1,$$

for $t_0 \in \mathbb{Z} \cap [6, +\infty)$. Thus, one may choose a convenient concave function W such that $W(n_{t_0}) \geq \tilde{V}(n_{t_0})$ for all $t_0 \in \mathbb{Z} \cap [6, +\infty)$, and such that $W(u) \geq \tilde{V}(u)$, for all integers $2 \leq u < n_6$. Indeed, fixed $u \in [n_6, +\infty)$, if $n_{t_0} \leq u \leq n_{t_0+1}$, for some $t_0 \in \mathbb{Z} \cap [6, +\infty)$, let $u = u_1 n_{t_0} + u_2 n_{t_0+1}$, where $0 \leq u_1, u_2 \leq 1$ and $u_1 + u_2 = 1$. Then

$$\begin{aligned} W(u) &= W(u_1 n_{t_0} + u_2 n_{t_0+1}) \\ &\geq u_1 W(n_{t_0}) + u_2 W(n_{t_0+1}) \text{ (by the concavity of function } W) \\ &\geq u_1 \tilde{V}(n_{t_0}) + u_2 \tilde{V}(n_{t_0+1}) \\ &= u_1 f_{n_{t_0}}(t_0) + u_2 f_{n_{t_0+1}}(t_0 + 1) \\ &= u_1 f_{n_{t_0}}(t_0 + 1) + u_2 f_{n_{t_0+1}}(t_0 + 1) \\ &= u_1 \cdot \left[\frac{3(t_0 + 1)^2 - 23(t_0 + 1) + 26}{6} + 4 \cdot \frac{n_{t_0} + 3}{t_0 + 1} \right] + \\ &\quad + u_2 \cdot \left[\frac{3(t_0 + 1)^2 - 23(t_0 + 1) + 26}{6} + 4 \cdot \frac{n_{t_0+1} + 3}{t_0 + 1} \right] \\ &= (u_1 + u_2) \cdot \frac{3(t_0 + 1)^2 - 23(t_0 + 1) + 26}{6} + 4 \cdot \frac{u_1 n_{t_0} + u_2 n_{t_0+1} + 3 \cdot (u_1 + u_2)}{t_0 + 1} \\ &= \frac{3(t_0 + 1)^2 - 23(t_0 + 1) + 26}{6} + 4 \cdot \frac{u + 3}{t_0 + 1} \\ &= f_u(t_0 + 1) \\ &= \tilde{V}(u). \end{aligned}$$

Let us consider the family of concave functions W_λ defined in $[2, +\infty)$ by

$$W_\lambda(u) = 3 \cdot (2^{1/2} \cdot u)^{2/3} - \frac{103}{19} \cdot (2^{1/2} \cdot u)^{1/3} + \lambda,$$

where λ is a constant.

Direct computation shows that the smallest λ such that $W_\lambda(n_{t_0}) \geq \tilde{V}(n_{t_0})$ for all $t_0 \in \mathbb{Z} \cap [6, +\infty)$, and such that $W_\lambda(u) \geq \tilde{V}(u) = f_u(6)$ for all integers $2 \leq u < n_6$, is

$$\frac{10}{3} - \frac{103}{19} \cdot 2^{1/2} \cong \frac{13}{3}.$$

Therefore, if W is defined in $[2, +\infty)$ by

$$W(u) = 3 \cdot (2^{1/2} \cdot u)^{2/3} - \frac{103}{19} \cdot (2^{1/2} \cdot u)^{1/3} + \frac{13}{3}$$

then the proof follows. ■

5.4 Affinely regular polygons

5.4.1 A brief introduction to affinely regular polygons

This subsection is based on the survey article (KORCHMÁROS; SZŐNYI, 2008) and in some references therein. Here, $\mathbb{F}$ denotes an arbitrary field of characteristic $p \geq 0$ and $\mathbb{A}^2(\mathbb{F})$ is the affine plane over $\mathbb{F}$.

Definition 5.4.1. An n -gon in $\mathbb{A}^2(\mathbb{F})$ is a set of n pairwise distinct points arranged in a cyclic order. If no three vertices of it are collinear, then the n -gon is called *nondegenerate*.

From now on, only nondegenerate n -gons are considered.

Definition 5.4.2. If $B = B_1B_2 \dots B_n$ is a regular n -gon in the Euclidean plane, then an n -gon $A = A_1A_2 \dots A_n$ in the affine plane $\mathbb{A}^2(\mathbb{F})$ is *affinely regular* if the bijection $B_i \mapsto A_i$ preserves all parallelisms between chords (sides and diagonals). Symbolically,

$$B_{i_0}B_{k_0} \parallel B_{i_1}B_{k_1} \Leftrightarrow A_{i_0}A_{k_0} \parallel A_{i_1}A_{k_1},$$

for all $1 \leq i_0 < k_0 \leq n$ and $1 \leq i_1 < k_1 \leq n$.

The first part of the following theorem presents a remarkable property pointed out in (KORCHMÁROS, 1974) and independently in (CRAATS; SIMONIS, 1986). Further, the classification in the second part can be found in (KORCHMÁROS, 1976a) and (KORCHMÁROS, 1976b).

Theorem 5.4.3. (KORCHMÁROS; SZŐNYI, 2008, Theorem 2.1 and Lemma 2.2). Every affinely regular polygon in $\mathbb{A}^2(\mathbb{F})$ is inscribed in an irreducible conic. More specifically, the affinely regular polygons in $\mathbb{A}^2(\mathbb{F})$ are exactly given by the following examples and their images under the affinities of $\mathbb{A}^2(\mathbb{F})$.

1. (Hyperbola). Let $H : XY = 1$ and consider $\mathbb{G}$ a finite multiplicative subgroup of $\mathbb{F}$ of order n . If $\alpha \in \mathbb{F}^*$ and g is a generator of $\mathbb{G}$, then $A = A_1A_2 \dots A_n$ is an affinely regular n -gon inscribed in H , where $A_i = (g^i\alpha, (g^i\alpha)^{-1})$ for each $i \in \{1, 2, \dots, n\}$.
2. (Parabola, $p > 0$). Let $P : Y = X^2$ and consider $\alpha \in \mathbb{F}$. Then $A = A_1A_2 \dots A_p$ is an affinely regular p -gon inscribed in P , where $A_i = (\alpha + i, (\alpha + i)^2)$ for each $i \in \{1, 2, \dots, p\}$.
3. (Ellipse). Let $T^2 - \gamma T + 1$ be an irreducible polynomial over a field $\mathbb{F}$ and consider $E : X^2 + Y^2 - \gamma XY = 1$. If θ is such that $\theta^2 - \gamma\theta + 1 = 0$ and $\mathbb{E} = \mathbb{F}(\theta)$ is a quadratic extension of $\mathbb{F}$, then, identifying $(\alpha, \beta) \in \mathbb{A}^2(\mathbb{F})$ with $\alpha + \beta\theta \in \mathbb{E}$, the points of E are those elements $\alpha + \beta\theta \in \mathbb{E}$ which satisfy the equation $(\alpha + \beta\theta) \cdot (\alpha + \beta\theta^{-1}) = 1$. Now, considering $\alpha + \beta\theta \in \mathbb{E}^*$ and g a generator of a multiplicative subgroup $\mathbb{G}$ of $\mathbb{E}$ of order n , it follows that $A = A_1A_2 \dots A_n$ is an affinely regular n -gon inscribed in E , where $A_i = g^i(\alpha + \beta\theta)$.

The following result was first proved in (KORCHMÁROS, 1974).

Theorem 5.4.4. (KORCHMÁROS; SZŐNYI, 2008, Theorem 2.3). In $\mathbb{A}^2(\mathbb{F}_q)$, an affinely regular n -gon exists if and only if one of the following cases occurs:

1. $n \mid (q - 1)$ and the n -gon is inscribed in a hyperbola.
2. $n = p$ and the n -gon is inscribed in a parabola.
3. $n \mid (q + 1)$ and the n -gon is inscribed in an ellipse.

Now, from (KORCHMÁROS, 1983), (SZŐNYI, 1987) and (KORCHMÁROS; STORME; SZŐNYI, 1997), the subsequent result follows.

Theorem 5.4.5. (KORCHMÁROS; SZŐNYI, 2008, Theorem 5.9). Let $A = A_1A_2 \dots A_n$ be an affinely regular n -gon in $\mathbb{A}^2(\mathbb{F}_q)$ inscribed in the irreducible conic C . If $q/n < q^{1/4}/2$, then the chords of A cover all points of $\mathbb{A}^2(\mathbb{F}_q)$ except the points of C and possibly the center of C .

The previous result raises a natural question: what is the number of chords of an affinely regular n -gon of $\mathbb{A}^2(\mathbb{F}_q)$ passing through a given point distinct from its vertices?

In the particular case of a n -gon $A = A_1A_2 \dots A_n$ inscribed in a hyperbola (resp. an ellipse), it was shown that determining the number of chords of A passing through a point distinct from its vertices is equivalent to determine the number of rational affine points lying in an appropriate subset of the plane (resp. the number of rational affine points) of a curve of the form of curve $\mathcal{F}$. More precisely, from (ABATANGELO; KORCHMÁROS, 1997, Proposition 3.2) and (GIULIETTI, 2008, Proposition 2.1), the following result holds.

Theorem 5.4.6. Let $A = A_1A_2 \dots A_n$ be an affinely regular n -gon in $\mathbb{A}^2(\mathbb{F}_q)$.

1. Suppose that A is inscribed in a hyperbola H . Up to a change of coordinates, it is possible to assume that H has equation $XY = 1$, and that $A_i = (\gamma^i, \gamma^{-i})$ for each $i \in \{1, 2, \dots, n\}$, where γ is a primitive n -th root of unity in $\mathbb{F}_q$. If $(\alpha, \beta) \in \mathbb{A}^2(\mathbb{F}_q) \setminus H$ and $n_{(\alpha, \beta)}$ denotes the number of chords of A passing through (α, β) , then

$$n_{(\alpha, \beta)} = \frac{N}{2d^2},$$

where $d = (q - 1)/n$ and N is the number of $\mathbb{F}_q$ -rational affine points not lying on the coordinate axes or the line of equation $X = Y$ of the geometrically irreducible plane curve given in affine coordinates by

$$\alpha X^d Y^d - X^d - Y^d + \beta = 0.$$

2. Suppose that A is inscribed in an ellipse E . Up to a change of coordinates, one may assume that E has equation $X^2 + Y^2 - \gamma XY = 1$, where $\gamma \in \mathbb{F}_q$ is such that $T^2 - \gamma T + 1$ is irreducible over $\mathbb{F}_q$. Further, identifying $\mathbb{A}^2(\mathbb{F}_q)$ with $\mathbb{F}_{q^2}$ as in Theorem 5.4.3, after a

change of coordinates, it is possible to assume that $A_1, A_2, \dots, A_n$ are the d -th powers in $\mathbb{F}_{q^2}$, with $d = (q^2 - 1)/n$. If $(\alpha, \beta) \in \mathbb{A}^2(\mathbb{F}_q)$ and $n_{(\alpha, \beta)}$ denotes the number of chords of A passing through (α, β) , then

$$\left| n_{(\alpha, \beta)} - \frac{N}{2d^2} \right| \leq 2,$$

where N is the number of $\mathbb{F}_{q^2}$ -rational affine points of the geometrically irreducible plane curve given in affine coordinates by

$$(\alpha + \beta\theta)^q X^d Y^d - X^d - Y^d + (\alpha + \beta\theta) = 0,$$

and θ is a root of $T^2 - \gamma T + 1$ in $\mathbb{F}_{q^2}$.

Based on the previous result and using the Stöhr-Voloch theory, in (ABATANGELO; KORCHMÁROS, 1997) and (GIULIETTI, 2008) bounds for the number of chords of affinely regular polygons inscribed in a hyperbola or an ellipse were studied. In the next subsection, for the particular case of an affinely regular n -gon $A = A_1 A_2 \dots A_n$ in $\mathbb{A}^2(\mathbb{F}_p)$ inscribed in a hyperbola, an upper bound for the number $n_{(a, b)}$ of chords of A passing through $(a, b) \in \mathbb{A}^2(\mathbb{F}_p)$ distinct from its vertices is provided.

5.4.2 Number of chords of an affinely regular polygon inscribed in a hyperbola passing through a given point

Let $\mathbb{F}_q$ be the prime field $\mathbb{F}_p$ and consider $A = A_1 A_2 \dots A_n$ an affinely regular polygon with $n = (p - 1)/d$ vertices inscribed in a hyperbola H of $\mathbb{A}^2(\mathbb{F}_p)$. As presented in Subsection 5.4.1, changing variable, one may consider H given by the equation $XY = 1$.

From Theorems 5.3.4 and 5.4.6, the following upper bound for the number $n_{(a, b)}$ of chords of A passing through $(a, b) \in \mathbb{A}^2(\mathbb{F}_p)$ distinct from its vertices is obtained.

Corollary 5.4.7. If $d \geq 3$ is a proper divisor of $p - 1$ such that

$$p - 1 \leq d \cdot \left(\frac{(d + 3) \cdot (d + 4) \cdot (3d - 1)}{12} - 3 \right),$$

then

$$n_{(a, b)} \leq \frac{1}{2} \cdot \left(3 \cdot (2^{1/2} \cdot n)^{2/3} - \frac{103}{19} \cdot (2^{1/2} \cdot n)^{1/3} + \frac{13}{3} \right). \quad (5.14)$$

Remark 5.4.8. One can check that bound (5.14) improves that given in (5.5) for $n \geq 44$. On the other hand, for each $2 \leq n < 44$, bounds (5.5) and (5.14) effectively differ by at most one unit. Moreover, considering the definition of $V(n) = \tilde{V}(n)$ as given in the proof of Theorem 5.3.4, for $25 < n < 44$, it is obtained that $n_{(a, b)} \leq \lfloor \frac{1}{2} V(n) \rfloor \leq \lfloor \frac{n+1}{3} \rfloor$, with $\frac{n+1}{3}$ as in (5.5). For an illustration of the region where (5.14) is better than the bound for $n_{(a, b)}$ derived from the Hasse-Weil bound, see also Figure 1.

Figure 1 – Contour plot of the difference $\Delta(p, d) = \left(\frac{p+1+2 \cdot (d-1)^2 \cdot p^{1/2}}{2 \cdot d^2} \right) - \frac{1}{2} \cdot \left(3 \cdot (2^{1/2} \cdot n)^{2/3} - \frac{103}{19} \cdot (2^{1/2} \cdot n)^{1/3} + \frac{13}{3} \right)$ between the bounds for the number $n_{(a,b)}$ obtained from the Hasse-Weil bound and Corollary 5.4.7, for $d < p - 1 \leq d \cdot \left(\frac{(d+3) \cdot (d+4) \cdot (3d-1)}{12} - 3 \right)$ and $n = (p - 1)/d$. In red, the curve $p - 1 = d \cdot \left(\frac{(d+3) \cdot (d+4) \cdot (3d-1)}{12} - 3 \right)$.

ON THE ZETA FUNCTION AND THE AUTOMORPHISM GROUP OF THE GENERALIZED SUZUKI CURVE

The present chapter is an extended and adapted version of (BORGES; COUTINHO, Preprint 2019).

6.1 Introduction

For a nonsingular geometrically irreducible curve $\mathcal{Y}$ of genus g defined over the finite field $\mathbb{F}_q$, where q is a power of a prime number p , consider the problem of determining the number $N_q(\mathcal{Y})$ of $\mathbb{F}_q$ -rational points on $\mathcal{Y}$. In this direction, the remarkable Hasse-Weil bound (see Section 2.7) states that

$$|N_q(\mathcal{Y}) - (q + 1)| \leq 2gq^{1/2}.$$

Curves attaining the previous upper (resp. lower) bound are called $\mathbb{F}_q$ -maximal (resp. $\mathbb{F}_q$ -minimal). For $p = 2$, an important example is the Deligne-Lusztig curve associated to the Suzuki group $Sz(q)$ (see (DELIGNE; LUSZTIG, 1976), (HANSEN; STICHTENOTH, 1990), (HANSEN, 1992)), here for simplicity called the Suzuki curve, which is the nonsingular model $\mathcal{Y}_{\mathcal{S}}$ defined over $\mathbb{F}_q$ of the plane curve¹

$$\mathcal{S} : Y^q - Y = X^{q_0}(X^q - X), \tag{6.1}$$

where $q_0 = 2^t$ and $q = 2^{2t-1}$. Indeed, in (HANSEN, 1992, Proposition 4.3), together with the expression for the Zeta function of $\mathcal{Y}_{\mathcal{S}}$, the explicit formula for the number of rational points on $\mathcal{Y}_{\mathcal{S}}$ shows that it is $\mathbb{F}_{q^4}$ -maximal.

¹ This plane model for the Suzuki curve is not the most commonly found in the literature, where in general $q_0 = p^t$ and $q = p^{2t+1}$. However, from (GARCIA; STICHTENOTH, 1991, Proposition 4.2), these two representations are equivalent.

The Suzuki curve is optimal in the sense that its number of $\mathbb{F}_q$ -rational points coincides with the maximum number of $\mathbb{F}_q$ -rational points that a curve of its genus can have (see (HANSEN; STICHTENOTH, 1990, Proposition 2.1)). Moreover, in (FUHRMANN; TORRES, 1998, Theorem 5.1), it is shown that this curve can be characterized by its genus and number of $\mathbb{F}_q$ -rational points.

In addition to its maximality and optimality properties, the Suzuki curve is also known for its large automorphism group with respect to the genus. Specifically, it is one of the four examples of curves of genus $g \geq 2$ having an automorphism group of size greater than or equal to $8g^3$ (see (HENN, 1978), (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 11.127)). Furthermore, in (GIULIETTI; KORCHMÁROS; TORRES, 2006) and (BASSA *et al.*, 2013), the investigation of genera and plane models for quotients of the Suzuki curve is addressed. Other studies examining embeddings in $\mathbb{P}^N$ (see (BALLICO; RAVAGNANI, 2015), (DUURSMA; EID, 2015)), class field theory (LAUTER, 1999), the invariant a -number (FRIEDLANDER *et al.*, 2013), the Weierstrass semigroups and coding theory (see (KIRFEL; PELLIKAAN, 1995), (CHEN; DUURSMA, 2003), (MATTHEWS, 2004), (GIULIETTI; KORCHMÁROS, 2008), (DUURSMA; PARK, 2012), (EID *et al.*, 2016), (BARTOLI; MONTANUCCI; ZINI, 2018)) were also carried out over the past years. More recently, the construction in (SKABELUND, 2018) of a Galois cover of the Suzuki curve raised a number of other issues to be investigated (see (GIULIETTI *et al.*, 2018), (MONTANUCCI; TIMPANELLA; ZINI, 2018)).

Most of the aforementioned applications was based on the knowledge of the number of $\mathbb{F}_{q^n}$ -rational points and the automorphism group of the Suzuki curve. Motivated by this, let $p > 2$, $q_0 = p^t$ and $q = p^m$, where m, t are positive integers satisfying the relation $m = 2t - 1$. If $\mathcal{G}_{\mathcal{S}}$ is the projective geometrically irreducible (see Proposition 6.3.12) plane curve defined over $\mathbb{F}_q$ given in affine coordinates by

$$\mathcal{G}_{\mathcal{S}} : Y^q - Y = X^{q_0}(X^q - X), \quad (6.2)$$

let $\mathcal{X}_{\mathcal{G}_{\mathcal{S}}}$ be its nonsingular model defined over $\mathbb{F}_q$, which is called here the generalized Suzuki curve.

The objective of this chapter is twofold. On the one hand, the number of $\mathbb{F}_{q^n}$ -rational points on $\mathcal{X}_{\mathcal{G}_{\mathcal{S}}}$ is investigated². As a consequence, the L-polynomial over $\mathbb{F}_q$ of $\mathcal{X}_{\mathcal{G}_{\mathcal{S}}}$ is recovered. The L-polynomial of a curve $\mathcal{Y}$ defined over $\mathbb{F}_q$ encodes information on the order of the group $\text{Pic}_0(\mathbb{F}_q(\mathcal{Y}))$, the zero-degree $\mathbb{F}_q$ -divisor class group. Using this fact, some constructions of curves with many rational points are presented in (VOLOCH, 2000). Moreover, considering the $\mathbb{F}_q$ -Frobenius endomorphism Φ on the Jacobian variety of $\mathcal{Y}$, then the characteristic polynomial

² We point out here that for $n = 1$, the number $N_{q^n}(\mathcal{X}_{\mathcal{G}_{\mathcal{S}}})$ was already studied in (PEDERSEN; SØRENSEN, 1990) in connection with geometric Goppa codes. Also, for $p = 3$ and considering (GARCIA; STICHTENOTH, 1991, Proposition 4.2), the curve $\mathcal{X}_{\mathcal{G}_{\mathcal{S}}}$ is $\mathbb{F}_q$ -covered by the so-called Ree curve, and then the information on its maximality given by Theorem 6.1.1 could be recovered by Theorem 2.7.4.

of Φ is described exactly by the reciprocal of the L-polynomial of $\mathcal{Y}$ over $\mathbb{F}_q$, and from its factorization the degree of the Frobenius linear series on $\mathcal{Y}$ is obtained. For further details on this topic, see (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Sections 9.7 and 9.8).

On the other hand, the automorphism group of $\mathcal{X}_{g,\mathcal{Y}}$ is presented. More generally, for p an arbitrary prime number, $q = p^m$ and $q_0 = p^t$, where m, t are positive integers satisfying the relation $2t > m \geq t$, with $m \neq 2t - 1$ if $p = 2$, we note that considering $\mathcal{X}$ the nonsingular model defined over $\mathbb{F}_q$ of

$$Y^q - Y = X^{q_0}(X^q - X),$$

a straightforward verification shows that our main result on the automorphism group of $\mathcal{X}_{g,\mathcal{Y}}$, Theorem 6.1.3 below, also holds for $\mathcal{X}$. Consequently, for $p = 2$ this extension of Theorem 6.1.3 completes the description of the whole automorphism group of $\mathcal{X}$ started in (GIULIETTI; KORCHMÁROS, 2014).

The following are the main results of this work.

Theorem 6.1.1. If g denotes the genus of $\mathcal{X}_{g,\mathcal{Y}}$, then the number $N_{q^n}(\mathcal{X}_{g,\mathcal{Y}})$ of $\mathbb{F}_{q^n}$ -rational points on $\mathcal{X}_{g,\mathcal{Y}}$ is described as follows.

1. If $p \mid n$, then

$$N_{q^n}(\mathcal{X}_{g,\mathcal{Y}}) = \begin{cases} q^n + 1, & \text{if } n \text{ is odd} \\ q^n + 1 - 2gq^{n/2}, & \text{if } n \text{ is even and } p \equiv 1 \pmod{4} \\ q^n + 1 - 2gq^{n/2}, & \text{if } n \equiv 0 \pmod{4} \text{ and } p \equiv 3 \pmod{4} \\ q^n + 1 + 2gq^{n/2}, & \text{if } n \equiv 2 \pmod{4} \text{ and } p \equiv 3 \pmod{4}. \end{cases}$$

2. If $p \nmid n$, then

$$N_{q^n}(\mathcal{X}_{g,\mathcal{Y}}) = \begin{cases} q^n + 1, & \text{if } n \text{ is even} \\ q^n + 1 + 2gq^{n/2}p^{-1/2} \left(\frac{(-1)^{(n-1)/2}n}{p} \right), & \text{if } n \text{ is odd} \end{cases},$$

where $\left(\frac{*}{p} \right)$ is the Legendre symbol.

Now, define

$$\tilde{p}^{1/2} := \begin{cases} p^{1/2}, & \text{if } p \equiv 1 \pmod{4} \\ \mathbf{i}p^{1/2}, & \text{if } p \equiv 3 \pmod{4} \end{cases}. \quad (6.3)$$

Theorem 6.1.2. If g denotes the genus of $\mathcal{X}_{g,\mathcal{Y}}$ and $\mathcal{M}_p(T)$ is the minimal polynomial of $-\zeta_p/\tilde{p}^{1/2}$ over $\mathbb{Q}$, where ζ_p is the primitive p -th root of unity $\mathbf{e}^{\frac{2\pi\mathbf{i}}{p}}$, then the L-polynomial $L_{\mathcal{X}_{g,\mathcal{Y}}}(T)$ of $\mathcal{X}_{g,\mathcal{Y}}$ over $\mathbb{F}_q$ is given by

$$L_{\mathcal{X}_{g,\mathcal{Y}}}(T) = \left(p^{p-1}((-1)^{\frac{p+1}{2}} + qT^2) \cdot \mathcal{M}_p(p^{t-1}T)^2 \right)^{\frac{g}{p}}.$$

Finally, if $\overline{\mathbb{F}_q}(\mathcal{X}_{q_0})$ is the function field of $\mathcal{X}_{q_0}$ and $x, y \in \overline{\mathbb{F}_q}(\mathcal{X}_{q_0})$ are such that $\overline{\mathbb{F}_q}(\mathcal{X}_{q_0}) = \overline{\mathbb{F}_q}(x, y)$ and $y^q - y = x^{q_0}(x^q - x)$, then the automorphism group of $\mathcal{X}_{q_0}$ is described as follows.

Theorem 6.1.3. The automorphism group $\mathbb{G}$ of $\mathcal{X}_{q_0}$ has order $q^2(q-1)$ and is given by the maps

$$(x, y) \mapsto (\alpha x + \beta, \alpha \beta^{q_0} x + \alpha^{q_0+1} y + \gamma),$$

where $\alpha \in \mathbb{F}_q^*$ and $\beta, \gamma \in \mathbb{F}_q$. Moreover,

$$\mathbb{G} = \mathbb{G}_1 \rtimes \mathbb{H},$$

where $\mathbb{G}_1$ is the Sylow p -subgroup of $\mathbb{G}$ consisting of the maps

$$(x, y) \mapsto (x + \beta, \beta^{q_0} x + y + \gamma),$$

with $\beta, \gamma \in \mathbb{F}_q$, and $\mathbb{H}$ is the cyclic complement of $\mathbb{G}_1$ in $\mathbb{G}$, which can be described by the maps

$$(x, y) \mapsto (\alpha x, \alpha^{q_0+1} y),$$

with $\alpha \in \mathbb{F}_q^*$.

This chapter is organized as follows. In Section 6.3, the general background necessary to prove Theorems 6.1.1, 6.1.2 and 6.1.3 is established. The proofs are presented in Sections 6.4, 6.5 and 6.7, respectively. Further, in Section 6.6 some examples of the L-polynomial of $\mathcal{X}_{q_0}$ for $p = 3, 5, 7, 11, 13, 17$ and 19 are considered, and an application of this fact is presented in Section 6.8.

6.2 Notation

The following notation is used throughout this text.

- p is a prime number, $q = p^m$ and $q_0 = p^t$ for some positive integers m, t .
- For each positive integer n , $\mathbb{F}_{q^n}$ is the finite field with q^n elements and $\mathbb{F}_{q^n}^* := \mathbb{F}_{q^n} \setminus \{0\}$.
- $\text{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_p}$ and $\text{N}_{\mathbb{F}_{q^n}/\mathbb{F}_p}$ denote the absolute trace and norm functions of $\mathbb{F}_{q^n}$, respectively.
- The word *curve* means a projective nonsingular geometrically irreducible algebraic curve. Also, as established in Notation 1.1.3, the term *plane curve* means a projective plane algebraic curve.
- For a curve $\mathcal{Y}$, $N_{q^n}(\mathcal{Y})$ denotes its number of $\mathbb{F}_{q^n}$ -rational points.
- e is the Euler's number, i is the imaginary unity and $\zeta_k := e^{\frac{2\pi i}{k}}$ for each positive integer k .
- For each positive integer k ,

$$\mu_k = \left\{ \zeta_k^i : 1 \leq i \leq k \text{ and } \gcd(i, k) = 1 \right\}$$

is the set of roots of the k -th cyclotomic polynomial.

6.3 Preliminaries

6.3.1 *L*-polynomials and supersingular curves

Let $\mathcal{Y}$ be a curve of genus g defined over the finite field $\mathbb{F}_q$, and let $L_{\mathcal{Y}}(T)$ be the L -polynomial (defined over $\mathbb{F}_q$) of $\mathcal{Y}$, which is the numerator of the Zeta function (over $\mathbb{F}_q$) of $\mathcal{Y}$ (see Section 2.6).

If $\omega_1, \dots, \omega_{2g} \in \mathbb{C}$ are the roots of the reciprocal polynomial of $L_{\mathcal{Y}}(T)$, then from Theorem 2.6.13 the following holds:

$$N_{q^n}(\mathcal{Y}) = q^n + 1 - \sum_{i=1}^{2g} \omega_i^n. \quad (6.4)$$

Recall that from the Hasse-Weil theorem (see Theorem 2.7.1), $|\omega_i| = q^{1/2}$, for all $i = 1, \dots, 2g$, and then $\omega_i = q^{1/2} \xi_i$, with $|\xi_i| = 1$ for each i . In particular, (6.4) can be rewritten as

$$N_{q^n}(\mathcal{Y}) = q^n + 1 - q^{n/2} \sum_{i=1}^{2g} \xi_i^n, \quad (6.5)$$

and $\mathcal{Y}$ is $\mathbb{F}_{q^{2n}}$ -maximal (resp. $\mathbb{F}_{q^{2n}}$ -minimal) if and only if $\xi_i^{2n} = -1$ (resp. $\xi_i^{2n} = 1$) for each $i \in \{1, \dots, 2g\}$.

Definition 6.3.1. The curve $\mathcal{Y}$ is *supersingular* if ξ_i , with $i = 1, \dots, 2g$, are roots of unity. In this case, the number

$$s := \min \left\{ n : \xi_i^n = 1 \text{ for all } i = 1, \dots, 2g \right\}$$

is called the *period* of $\mathcal{Y}$ over $\mathbb{F}_q$.

This subsection ends with the following result, which is important to prove Theorem 6.1.1.

Theorem 6.3.2. (MCGUIRE; YILMAZ, 2018, Theorem 1). Let $\mathcal{Y}$ be a supersingular curve of genus g defined over $\mathbb{F}_q$ with period s . Let n be a positive integer, let $n_1 = \gcd(n, s)$ and write $n = n_1 k$. If q is odd, then the following occurs:

1. If $n_1 m$ is even, then

$$N_{q^n}(\mathcal{Y}) - (q^n + 1) = q^{(n-n_1)/2} \left[N_{q^{n_1}}(\mathcal{Y}) - (q^{n_1} + 1) \right].$$

2. If $n_1 m$ is odd and $p \mid k$, then

$$N_{q^n}(\mathcal{Y}) - (q^n + 1) = q^{(n-n_1)/2} \left[N_{q^{n_1}}(\mathcal{Y}) - (q^{n_1} + 1) \right].$$

3. If $n_1 m$ is odd and $p \nmid k$, then

$$N_{q^n}(\mathcal{Y}) - (q^n + 1) = q^{(n-n_1)/2} \left[N_{q^{n_1}}(\mathcal{Y}) - (q^{n_1} + 1) \right] \left(\frac{(-1)^{(k-1)/2} k}{p} \right),$$

where $\left(\frac{*}{p} \right)$ is the Legendre symbol.

6.3.2 Elementary abelian p -extensions of algebraic function fields

Let Σ_2/Σ_1 be a Galois extension of algebraic function fields and suppose that Σ_1 has characteristic $p > 0$.

Definition 6.3.3. The extension Σ_2/Σ_1 is an *elementary abelian p -extension* if its Galois group, $\text{Gal}(\Sigma_2/\Sigma_1)$, is elementary abelian of exponent p . In this case, the degree of the extension, denoted here by $[\Sigma_2 : \Sigma_1]$, is equal to $q = p^m$ for some positive integer m .

The following result provides a description of elementary abelian p -extensions Σ_2/Σ_1 of degree $q = p^m$ in cases in which Σ_1 contains the finite field $\mathbb{F}_q$.

Proposition 6.3.4. (GARCIA; STICHTENOTH, 1991, Propositions 1.1 and 1.2). Suppose that Σ_2/Σ_1 is an elementary abelian p -extension of degree q and that $\mathbb{F}_q \subseteq \Sigma_1$. Then, there is an element $\eta \in \Sigma_2$ such that $\Sigma_2 = \Sigma_1(\eta)$ and whose minimal polynomial over Σ_1 is of the form

$$T^q - T - \mathfrak{z}$$

for some $\mathfrak{z} \in \Sigma_1$. Conversely, if $\mathbb{F}_q \subseteq \Sigma_1$ and, for some $\mathfrak{z} \in \Sigma_1$, the polynomial

$$T^q - T - \mathfrak{z}$$

is irreducible over Σ_1 , then the extension $\Sigma_1(\eta)/\Sigma_1$, with η satisfying $\eta^q - \eta - \mathfrak{z} = 0$, is an elementary abelian p -extension of degree q . Further, the intermediate fields $\Sigma_1 \subseteq \Sigma \subseteq \Sigma_1(\eta)$ with $[\Sigma : \Sigma_1] = p$ are the following ones: $\Sigma = \Sigma_\mu := \Sigma_1(\eta_\mu)$, where $\mu \in \mathbb{F}_q^*$,

$$\eta_\mu := (\mu\eta)^{p^{m-1}} + (\mu\eta)^{p^{m-2}} + \cdots + (\mu\eta)^p + \mu\eta,$$

and η_μ satisfies the equation

$$\eta_\mu^p - \eta_\mu = \mu\mathfrak{z}.$$

Remark 6.3.5. Considering the notation as in Proposition 6.3.4, we have that $\Sigma_{\mu_1} = \Sigma_{\mu_2}$ if and only if $\mu_1 = \mu\mu_2$ for some $\mu \in \mathbb{F}_p^*$. Therefore, there are exactly

$$\frac{q-1}{p-1}$$

intermediate fields Σ of $\Sigma_1(\eta)/\Sigma_1$ such that $[\Sigma : \Sigma_1] = p$.

Now, let Σ_2/Σ_1 be an elementary abelian p -extension of degree q and suppose that Σ_1 contains the finite field $\mathbb{F}_q$. Also, let

$$\left\{ \Sigma_{\mu_i} : i = 1, \dots, \frac{q-1}{p-1} \right\}$$

be the set of all intermediate fields of Σ_2/Σ_1 , and let $\mathcal{Y}_2$ and $\mathcal{Y}_{\mu_i}$, with $i = 1, \dots, \frac{q-1}{p-1}$, be the nonsingular models defined over $\mathbb{F}_q$ of Σ_2 and Σ_{μ_i} , respectively.

This subsection ends with the following result, which relates the L-polynomial (over $\mathbb{F}_q$) of $\mathcal{Y}_2$ with the L-polynomials (over $\mathbb{F}_q$) of $\mathcal{Y}_{\mu_i}$, for $i = 1, \dots, \frac{q-1}{p-1}$. As a consequence, one can express the number of $\mathbb{F}_{q^n}$ -rational points on $\mathcal{Y}_2$ as a function of the number of $\mathbb{F}_{q^n}$ -rational points on $\mathcal{Y}_{\mu_i}$, where $i = 1, \dots, \frac{q-1}{p-1}$, for each positive integer n .

Proposition 6.3.6. (DUURSMA; STICHTENOTH; VOSS, 1996, Corollary 6.7) Considering the previous notation, then it follows that $L_{\mathcal{Y}_2}(T) = \prod_{i=1}^{\frac{q-1}{p-1}} L_{\mathcal{Y}_{\mu_i}}(T)$. In particular,

$$N_{q^n}(\mathcal{Y}_2) - (q^n + 1) = \sum_{i=1}^{\frac{q-1}{p-1}} \left(N_{q^n}(\mathcal{Y}_{\mu_i}) - (q^n + 1) \right)$$

for each positive integer n .

6.3.3 On the number of $\mathbb{F}_{q^n}$ -rational points of $Y^p - Y = XR(X)$

Suppose that p is an odd prime number. For each positive integer n , the number of $\mathbb{F}_{q^n}$ -rational points on the nonsingular model $\mathcal{Y}_R$ defined over $\mathbb{F}_q$ of the plane curve given in affine coordinates by

$$\mathcal{F}_R : Y^p - Y = XR(X),$$

where $R(X)$ is a p -polynomial defined over $\mathbb{F}_q$, that is,

$$R(X) = \alpha_k X^{p^k} + \alpha_{k-1} X^{p^{k-1}} + \dots + \alpha_0 X,$$

with $\alpha_k, \alpha_{k-1}, \dots, \alpha_0 \in \mathbb{F}_q$ and $\alpha_k \neq 0$, is studied.

The following proposition collects some properties of $\mathcal{F}_R$.

Proposition 6.3.7. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Lemma 12.1). The plane curve $\mathcal{F}_R$ is geometrically irreducible. Moreover:

1. The genus g of $\mathcal{F}_R$ is given by

$$g = \frac{p^k(p-1)}{2}.$$

2. $P = (0 : 1 : 0) \in \mathbb{P}^2(\overline{\mathbb{F}_q})$ is the unique point at infinity of $\mathcal{F}_R$. If $k = 1$, then $\mathcal{F}_R$ is nonsingular. Otherwise, P is the unique singular point of $\mathcal{F}_R$. In both cases, P has multiplicity $p^k - p + 1$ and it is the center of only one $\mathbb{F}_q$ -rational branch of $\mathcal{F}_R$.

Corollary 6.3.8. The number of $\mathbb{F}_{q^n}$ -rational points on $\mathcal{Y}_R$ is given by the number of solutions in $\mathbb{F}_{q^n}^2$ of the equation

$$Y^p - Y = XR(X) \quad (6.6)$$

added to 1.

The main reference from now until the end of this subsection is (BOUW *et al.*, 2016, Section 2). To count the number of solutions in $\mathbb{F}_{q^n}^2$ of (6.6), set

$$\begin{aligned} B_R^{(n)} : \mathbb{F}_{q^n}^2 &\rightarrow \mathbb{F}_p \\ (\alpha, \beta) &\mapsto \frac{1}{2} \text{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_p}(\alpha R(\beta) + \beta R(\alpha)) \end{aligned}$$

One can check that $B_R^{(n)}$ is an $\mathbb{F}_p$ -symmetric bilinear form in $\mathbb{F}_{q^n}$, with associated quadratic form

$$\begin{aligned} Q_R^{(n)} : \mathbb{F}_{q^n} &\rightarrow \mathbb{F}_p \\ \alpha &\mapsto \text{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_p}(\alpha R(\alpha)) \end{aligned}$$

which satisfies $Q_R^{(n)}(\lambda \alpha) = \lambda^2 Q_R^{(n)}(\alpha)$ for all $\lambda \in \mathbb{F}_p$, and also

$$B_R^{(n)}(\alpha, \beta) = \frac{1}{2} Q_R^{(n)}(\alpha + \beta) - \frac{1}{2} Q_R^{(n)}(\alpha) - \frac{1}{2} Q_R^{(n)}(\beta)$$

for each $(\alpha, \beta) \in \mathbb{F}_{q^n}^2$.

Considering the radical (kernel) of $B_R^{(n)}$

$$W_R^{(n)} = \left\{ \alpha \in \mathbb{F}_{q^n} : B_R^{(n)}(\alpha, \beta) = 0 \text{ for each } \beta \in \mathbb{F}_{q^n} \right\},$$

which is an $\mathbb{F}_p$ -linear subspace of $\mathbb{F}_{q^n}$, the following properties hold.

Proposition 6.3.9. (BOUW *et al.*, 2016, Proposition 2.1). The following occurs.

1. Let $\alpha \in \mathbb{F}_{q^n}$. If $\alpha \in W_R^{(n)}$, then $Q_R^{(n)}(\alpha) = 0$.
2. The set $W_R^{(n)}$ consists of the roots in $\mathbb{F}_{q^n}$ of the polynomial

$$E_R(T) = R(T)^{p^k} + \sum_{i=0}^k (\alpha_i T)^{p^{k-i}}.$$

Based on Corollary 6.3.8, a connection between the number of $\mathbb{F}_{q^n}$ -rational points on $\mathcal{Y}_R$ and the dimension of $V_R^{(n)} := \mathbb{F}_{q^n}/W_R^{(n)}$ over $\mathbb{F}_p$ is now established.

Proposition 6.3.10. (BOUW *et al.*, 2016, Proposition 2.4). Let $\overline{B}_R^{(n)}$ be the projection of $B_R^{(n)}$ onto $V_R^{(n)}$, that is, define

$$\overline{B}_R^{(n)}(\alpha + W_R^{(n)}, \beta + W_R^{(n)}) := B_R^{(n)}(\alpha, \beta)$$

for each $\alpha + W_R^{(n)}, \beta + W_R^{(n)} \in V_R^{(n)}$. Then, $\overline{B}_R^{(n)}$ is a nondegenerate bilinear form on $V_R^{(n)} \times V_R^{(n)}$.

As a consequence of the previous result, it follows that the quadratic form

$$\begin{aligned} \overline{Q}_R^{(n)} : V_R^{(n)} &\rightarrow \mathbb{F}_p \\ \alpha + W_R^{(n)} &\mapsto \text{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_p}(\alpha R(\alpha)) \end{aligned} ,$$

is nondegenerate, and therefore its zero locus

$$\left\{ \alpha + W_R^{(n)} \in V_R^{(n)} : \overline{Q}_R^{(n)}(\alpha) = 0 \right\},$$

defines a smooth quadric over $\mathbb{F}_p$. In (JOLY, 1973), the author provides an expression for the cardinality of a nondegenerate quadratic form. Using this, then the number of solutions in $\mathbb{F}_{q^n}^2$ of (6.6) in terms of the dimension of $V_R^{(n)}$ over $\mathbb{F}_p$,

$$\dim_{\mathbb{F}_p}(V_R^{(n)}) = \dim_{\mathbb{F}_p}(\mathbb{F}_{q^n}) - \dim_{\mathbb{F}_p}(W_R^{(n)}) = mn - \dim_{\mathbb{F}_p}(W_R^{(n)}),$$

can be described by the following proposition.

Proposition 6.3.11. (BOUW *et al.*, 2016, Proposition 2.6). The number of solutions in $\mathbb{F}_{q^n}^2$ of (6.6) is

1. q^n , if $mn - \dim_{\mathbb{F}_p}(W_R^{(n)})$ is odd.
2. $q^n \pm (p-1)p^{\dim_{\mathbb{F}_p}(W_R^{(n)})/2} q^{n/2}$, if $mn - \dim_{\mathbb{F}_p}(W_R^{(n)})$ is even.

6.3.4 The curve $\mathcal{G}_{\mathcal{S}}$

Let $\mathcal{G}_{\mathcal{S}}$ be given as in (6.2). From (PEDERSEN; SØRENSEN, 1990, Theorem 1), (GARCIA; STICHTENOTH, 1991, Proposition 4.1) and a straightforward calculation, the following result holds.

Proposition 6.3.12. $\mathcal{G}_{\mathcal{S}}$ is a geometrically irreducible plane curve of genus g given by

$$g = \frac{q_0(q-1)}{2}.$$

Further, $P = (0 : 1 : 0) \in \mathbb{P}^2(\overline{\mathbb{F}_q})$ is the unique point at infinity of $\mathcal{G}_{\mathcal{S}}$, which is also its only singular point, having multiplicity equal to q_0 .

Consider $\mathcal{K}_{\mathcal{G}_{\mathcal{S}}}$ the nonsingular model of $\mathcal{G}_{\mathcal{S}}$ defined over $\mathbb{F}_q$, and let $\overline{\mathbb{F}_q}(\mathcal{K}_{\mathcal{G}_{\mathcal{S}}})$ be its function field. If $x, y \in \overline{\mathbb{F}_q}(\mathcal{K}_{\mathcal{G}_{\mathcal{S}}})$ are such that $\overline{\mathbb{F}_q}(\mathcal{K}_{\mathcal{G}_{\mathcal{S}}}) = \overline{\mathbb{F}_q}(x, y)$ and $y^q - y = x^{q_0}(x^q - x)$, then the following occurs.

Proposition 6.3.13. (DEOLALIKAR, 2002, Theorem 3.3). The extension $\overline{\mathbb{F}_q}(x, y)/\overline{\mathbb{F}_q}(x)$ is a Galois extension of degree q . Moreover, the only ramified place of $\overline{\mathbb{F}_q}(x)$ is the infinite place $\mathcal{P}_\infty$, which is totally ramified in $\overline{\mathbb{F}_q}(x, y)$.

Using the one-to-one correspondence between ($\mathbb{F}_q$ -rational) points on $\mathcal{X}_{\mathcal{G}_{\mathcal{F}}}$ and ($\mathbb{F}_q$ -rational) places of $\overline{\mathbb{F}_q}(\mathcal{X}_{\mathcal{G}_{\mathcal{F}}})$ (see Proposition 2.5.9), let Q_∞ be the $\mathbb{F}_q$ -rational point (see Subsection 2.3.1) of $\mathcal{X}_{\mathcal{G}_{\mathcal{F}}}$ corresponding to the unique ($\mathbb{F}_q$ -rational) place $\mathcal{Q}_\infty$ of $\overline{\mathbb{F}_q}(x, y)$ lying over the infinity place $\mathcal{P}_\infty$ of $\overline{\mathbb{F}_q}(x)$. Then, the following holds.

Proposition 6.3.14. (PEDERSEN; SØRENSEN, 1990, Proof of Lemma 2). The pole divisors of x and y are given by

$$\operatorname{div}(x)_\infty = qQ_\infty \text{ and } \operatorname{div}(y)_\infty = (q + q_0)Q_\infty,$$

respectively.

This subsection ends with the following two results.

Theorem 6.3.15. (PEDERSEN; SØRENSEN, 1990, Theorem 7). The sets $\{1, x\}$ and $\{1, x, y\}$ are bases for the Riemann-Roch spaces $\mathcal{L}(qQ_\infty)$ and $\mathcal{L}((q + q_0)Q_\infty)$, respectively.

Corollary 6.3.16. $P = (0 : 1 : 0)$ is the center of a unique $\mathbb{F}_q$ -rational branch of $\mathcal{G}_{\mathcal{F}}$, namely the branch of $\mathcal{G}_{\mathcal{F}}$ corresponding to the point $Q_\infty \in \mathcal{X}_{\mathcal{G}_{\mathcal{F}}}$.

6.3.5 Automorphism group

Let $\mathcal{Y}$ be a curve of genus g defined over the finite field $\mathbb{F}_q$.

Definition 6.3.17. The *automorphism group* $\mathbb{G}$ of $\mathcal{Y}$ is defined as the group of $\overline{\mathbb{F}_q}$ -automorphisms of the function field $\overline{\mathbb{F}_q}(\mathcal{Y})$.

Definition 6.3.18. Considering the action of $\mathbb{G}$ on the points of $\mathcal{Y}$ (see (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Section 11.1)) for $Q \in \mathcal{Y}$, the *stabilizer of $\mathbb{G}$ at Q* , denoted by $\mathbb{G}_Q$, is the subgroup of $\mathbb{G}$ consisting of all automorphisms fixing Q under this action. Further, for each non-negative integer i , the *i -th ramification group $\mathbb{G}_Q^{(i)}$ at Q* is defined by

$$\mathbb{G}_Q^{(i)} = \left\{ \sigma \in \mathbb{G}_Q : v_Q(\sigma(t) - t) \geq i + 1 \right\},$$

where $t \in \overline{\mathbb{F}_q}(\mathcal{Y})$ is a local parameter at Q and $\mathbb{G}_Q^{(i)} \supseteq \mathbb{G}_Q^{(i+1)}$ for all $i \geq 0$.

The following result summarizes properties of these subgroups.

Theorem 6.3.19. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Lemma 11.44 and Theorem 11.74). The equality $\mathbb{G}_Q^{(0)} = \mathbb{G}_Q$ holds. Moreover, $\mathbb{G}_Q^{(1)}$ is the unique Sylow p -subgroup of $\mathbb{G}_Q$ and $\mathbb{G}_Q = \mathbb{G}_Q^{(1)} \rtimes \mathbb{H}$, where $\mathbb{H}$ is a cyclic subgroup of $\mathbb{G}_Q$ of order coprime to p .

Lastly, the following result is used in the proof of Theorem 6.1.3.

Theorem 6.3.20. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 11.140). Suppose that $g \geq 2$, and let $Q \in \mathcal{Y}$ be an $\mathbb{F}_q$ -rational point satisfying

$$|\mathbb{G}_Q^{(1)}| > 2g + 1.$$

Then, one of the following cases occurs:

1. $\mathbb{G} = \mathbb{G}_Q$.
2. $\mathcal{Y}$ is birationally equivalent to one of the following curves:
 - a) the Hermitian curve over $\mathbb{F}_q$

$$\mathcal{H} : Y^q - Y = X^{q+1} \quad (6.7)$$

- b) the Suzuki curve over $\mathbb{F}_q$, given by the nonsingular model defined over $\mathbb{F}_q$ of (6.1)
- c) the Ree curve over $\mathbb{F}_q$, given by the nonsingular model defined over $\mathbb{F}_q$ of

$$\mathcal{R} : Y^{q^2} - [1 + (X^q - X)^{q-1}]Y^q + (X^q - X)^{q-1}Y - X^q(X^q - X)^{q+3q_0} = 0, \quad (6.8)$$

where $q = 3^m$, $q_0 = 3^t$ and $m = 2t - 1$.

6.4 Proof of Theorem 6.1.1

Using the notation introduced in Subsection 6.3.4, the proof of Theorem 6.1.1 is presented. To better organize the ideas, it is separated in a sequence of steps.

Step 1: elementary abelian p -extension

From Proposition 6.3.4, $\overline{\mathbb{F}_q}(x, y)/\overline{\mathbb{F}_q}(x)$ is an elementary abelian p -extension of degree q . The set of intermediate fields $\overline{\mathbb{F}_q}(x) \subseteq E \subseteq \overline{\mathbb{F}_q}(x, y)$ such that $[E : \overline{\mathbb{F}_q}(x)] = p$ is described by

$$\left\{ E_\alpha : \alpha \in \mathbb{F}_q^* \right\},$$

where for each $\alpha \in \mathbb{F}_q^*$, E_α is the intermediate field of $\overline{\mathbb{F}_q}(x, y)/\overline{\mathbb{F}_q}(x)$ given by

$$E_\alpha := \overline{\mathbb{F}_q}(x, y_\alpha),$$

and $y_\alpha := (\alpha y)^{p^{m-1}} + (\alpha y)^{p^{m-2}} + \cdots + (\alpha y)^p + \alpha y$ satisfies the equation $y_\alpha^p - y_\alpha = \alpha x^{q_0}(x^q - x)$.

Further, from Remark 6.3.5, let $\left\{ \alpha_i : i = 1, \dots, \frac{q-1}{p-1} \right\} \subseteq \mathbb{F}_q^*$ be such that

$$\left\{ E_\alpha : \alpha \in \mathbb{F}_q^* \right\} = \left\{ E_{\alpha_i} : i = 1, \dots, \frac{q-1}{p-1} \right\}.$$

For each $\alpha \in \mathbb{F}_q^*$, consider the plane model $(\mathcal{F}_\alpha, (x, y_\alpha))$ defined over $\mathbb{F}_q$ of E_α , where $\mathcal{F}_\alpha$ is the geometrically irreducible³ plane curve defined over $\mathbb{F}_q$ given in affine coordinates by

$$\mathcal{F}_\alpha : Y^p - Y = \alpha X^{q_0}(X^q - X).$$

Also, let $\mathcal{X}_\alpha$ be the nonsingular model of $\mathcal{F}_\alpha$ defined over $\mathbb{F}_q$, and let $L_{\mathcal{X}_\alpha}(T)$ be the L-polynomial of $\mathcal{X}_\alpha$ over $\mathbb{F}_q$.

From Proposition 6.3.6, the following occurs.

Corollary 6.4.1. For each positive integer n , $N_{q^n}(\mathcal{X}_{\mathcal{G}_\mathcal{F}}) - (q^n + 1) = \sum_{i=1}^{\frac{q-1}{p-1}} \left(N_{q^n}(\mathcal{X}_{\alpha_i}) - (q^n + 1) \right)$.

The following lemmas are important to describe the number $N_{q^n}(\mathcal{X}_{\mathcal{G}_\mathcal{F}})$ for each positive integer n .

Lemma 6.4.2. For each $\alpha \in \mathbb{F}_q^*$, E_α is $\overline{\mathbb{F}_q}$ -isomorphic to E_1 , with the $\overline{\mathbb{F}_q}$ -isomorphism inducing an $\mathbb{F}_q$ -isomorphism between $\mathbb{F}_q(x, y_\alpha)$ and $\mathbb{F}_q(x, y_1)$. In particular, from Corollary 6.4.1,

$$N_{q^n}(\mathcal{X}_{\mathcal{G}_\mathcal{F}}) - (q^n + 1) = \frac{q-1}{p-1} \left(N_{q^n}(\mathcal{X}_1) - (q^n + 1) \right)$$

for each positive integer n .

Proof. Recall that $q = p^m$ and $q_0 = p^t$, where $m = 2t - 1$, which implies that $m - t = t - 1$. For $\alpha \in \mathbb{F}_q^*$, let $\beta := \alpha^{p^{m-t} + p^{m-t-1} + \dots + p + 1} \in \mathbb{F}_q$ and $\gamma := N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) \in \mathbb{F}_p$. Then

$$\begin{aligned} \beta^{q_0} \beta &= \left(\alpha^{p^{m-t} + p^{m-t-1} + \dots + p + 1} \right)^{p^t} \alpha^{p^{m-t} + p^{m-t-1} + \dots + p + 1} \\ &= \alpha^{p^m + p^{m-1} + \dots + p^{t+1} + p^t} \cdot \alpha^{p^{m-t} + p^{m-t-1} + \dots + p + 1} \\ &= \alpha^{p^m + p^{m-1} + \dots + p^{t+1} + p^t} \cdot \alpha^{p^{t-1} + p^{t-2} + \dots + p + 1} \\ &= \alpha^{p^m} \alpha^{p^{m-1} + \dots + p + 1} \\ &= \alpha \gamma, \end{aligned}$$

$E_\alpha = \overline{\mathbb{F}_q}(x, y_\alpha) = \overline{\mathbb{F}_q}(\beta x, \gamma y_\alpha)$ and $\mathbb{F}_q(x, y_\alpha) = \mathbb{F}_q(\beta x, \gamma y_\alpha)$, with

$$\begin{aligned} (\beta x)^{q_0} ((\beta x)^q - (\beta x)) &= \beta^{q_0} \beta x^{q_0} (x^q - x) \\ &= \alpha \gamma x^{q_0} (x^q - x) \\ &= \gamma (y_\alpha^p - y_\alpha) \\ &= (\gamma y_\alpha)^p - (\gamma y_\alpha). \end{aligned}$$

Therefore,

$$\begin{array}{ccc} E_\alpha & \rightarrow & E_1 \\ \frac{A(\beta x, \gamma y_\alpha)}{B(\beta x, \gamma y_\alpha)} & \mapsto & \frac{A(x, y_1)}{B(x, y_1)} \end{array},$$

³ The geometric irreducibility of $\mathcal{F}_\alpha$ for each $\alpha \in \mathbb{F}_q^*$ follows from the geometric irreducibility of $\mathcal{G}_\mathcal{F}$ (GARCIA; STICHTENOTH, 1991, Lemma 1.3).

where $A(X, Y), B(X, Y) \in \overline{\mathbb{F}_q}[X, Y]$ and $B(\beta x, \gamma y_\alpha) \neq 0$, is an $\overline{\mathbb{F}_q}$ -isomorphism between E_α and E_1 that induces an $\mathbb{F}_q$ -isomorphism between $\mathbb{F}_q(x, y_\alpha)$ and $\mathbb{F}_q(x, y_1)$. This completes the proof. $\square$

Lemma 6.4.3. For each $\alpha \in \mathbb{F}_q^*$, $E_1 = \overline{\mathbb{F}_q}(x, z_1)$ and $\mathbb{F}_q(x, y_1) = \mathbb{F}_q(x, z_1)$, where $z_1 \in \mathbb{F}_q(x, y_1)$ is defined by

$$z_1 := y_1 - x^{\frac{q}{p}} x^{\frac{q_0}{p}} - x^{\frac{q}{p^2}} x^{\frac{q_0}{p^2}} - \dots - x^{\frac{q}{q_0}} x^{\frac{q_0}{q_0}}$$

and satisfies $z_1^p - z_1 = x(x^{\frac{q}{q_0}} - x^{q_0})$. In particular, if $\tilde{\mathcal{F}}_1$ is the geometrically irreducible plane curve given by

$$\tilde{\mathcal{F}}_1 : Y^p - Y = X(X^{\frac{q}{q_0}} - X^{q_0})$$

and $\mathcal{X}_1$ is its nonsingular model defined over $\mathbb{F}_q$, then $(\tilde{\mathcal{F}}_1, (x, z_1))$ is another plane model defined over $\mathbb{F}_q$ of E_1 and

$$N_{q^n}(\mathcal{X}_{\mathcal{G}_{\mathcal{F}}}) - (q^n + 1) = \frac{q-1}{p-1} \left(N_{q^n}(\mathcal{X}_1) - (q^n + 1) \right)$$

for each positive integer n .

Proof. The equalities $E_1 = \overline{\mathbb{F}_q}(x, z_1)$ and $\mathbb{F}_q(x, y_1) = \mathbb{F}_q(x, z_1)$ follow immediately from the definition of z_1 . Also, we have that

$$\begin{aligned} z_1^p - z_1 &= y_1^p - y_1 - x^q x^{q_0} + x^{\frac{q}{q_0}} x^{\frac{q_0}{q_0}} \\ &= x^{q_0} (x^q - x) - x^q x^{q_0} + x^{\frac{q}{q_0}} x \\ &= x(x^{\frac{q}{q_0}} - x^{q_0}), \end{aligned}$$

as desired. Finally, the other statements follow from the geometric irreducibility of $\tilde{\mathcal{F}}_1$ given by Proposition 6.3.7. $\square$

Step 2: the number of $\mathbb{F}_{q^n}$ -rational points on $\tilde{\mathcal{F}}_1 : Y^p - Y = X(X^{\frac{q}{q_0}} - X^{q_0})$

Considering the notation given as in Subsection 6.3.3, let $\tilde{\mathcal{F}}_1 = \mathcal{F}_R$, where $R(X) = X^{\frac{q}{q_0}} - X^{q_0}$.

To apply Proposition 6.3.11, let us determine the dimension of $W_R^{(n)}$ over $\mathbb{F}_p$ based on the characterization provided by Proposition 6.3.9. For this, first note that here

$$E_R(T) = (T - T^q)^p - (T - T^q).$$

and thus, the following statements are equivalent for an element $\alpha \in \mathbb{F}_{q^n}$:

1. $\alpha \in W_R^{(n)}$;
2. $E_R(\alpha) = 0$;
3. $\alpha^q - \alpha \in \mathbb{F}_p$.

This part starts with the following lemma, which is a consequence of the results in (COULTER; HENDERSON, 2004) and (LIANG, 1978).

Lemma 6.4.4. Let $\beta \in \mathbb{F}_p$ be fixed. Then

$$\#\left\{\alpha \in \mathbb{F}_{q^n} : \alpha^q - \alpha - \beta = 0\right\} = \begin{cases} q, & \text{if } n\beta = 0 \\ 0, & \text{otherwise.} \end{cases}$$

In particular, the splitting field of $E_R(T)$ is $\mathbb{F}_{q^p}$,

$$\#W_R^{(n)} = \begin{cases} pq, & \text{if } p \mid n \\ q, & \text{otherwise} \end{cases},$$

and

$$\dim_{\mathbb{F}_p}(W_R^{(n)}) = \begin{cases} m+1, & \text{if } p \mid n \\ m, & \text{otherwise.} \end{cases}$$

Recall that m is odd. Therefore, since Proposition 6.3.7 provides that the genus of $\tilde{\mathcal{X}}_1$ is given by

$$g(\tilde{\mathcal{X}}_1) := p^t(p-1)/2,$$

as a consequence of Corollary 6.3.8, Proposition 6.3.11, and Lemma 6.4.4, the following holds.

Lemma 6.4.5. The number of $\mathbb{F}_{q^n}$ -rational points on $\tilde{\mathcal{X}}_1$ can be described as follows.

1. If $p \mid n$, then

$$N_{q^n}(\tilde{\mathcal{X}}_1) = \begin{cases} q^n + 1, & \text{if } n \text{ is odd} \\ q^n + 1 \pm 2g(\tilde{\mathcal{X}}_1)q^{n/2}, & \text{if } n \text{ is even.} \end{cases} \quad (6.9)$$

2. If $p \nmid n$, then

$$N_{q^n}(\tilde{\mathcal{X}}_1) = \begin{cases} q^n + 1, & \text{if } n \text{ is even} \\ q^n + 1 \pm 2g(\tilde{\mathcal{X}}_1)q^{n/2}p^{-1/2}, & \text{if } n \text{ is odd.} \end{cases} \quad (6.10)$$

In particular, $\tilde{\mathcal{X}}_1$ is $\mathbb{F}_{q^n}$ -maximal or minimal if and only if $p \mid n$ and n is even, and also $N_q(\tilde{\mathcal{X}}_1) = qp + 1$.

Therefore, to determine the sign $\pm$ in (6.9) and (6.10) it is necessary to separate the analysis in two cases.

The case $p \mid n$

Since the splitting field of $E_R(T)$ is the field $\mathbb{F}_{q^p}$, with the following result one can determine the sign in (6.9).

Lemma 6.4.6. (BOUW *et al.*, 2016, Comments on Page 105 and Theorem 7.4). There exist $\delta \in \mathbb{F}_{q^p}$ and an $\mathbb{F}_{q^p}$ -rational morphism $\phi : \tilde{\mathcal{X}}_1 \rightarrow \mathcal{X}_\delta$, where $\mathcal{X}_\delta$ is the nonsingular model defined over $\mathbb{F}_{q^p}$ of

$$Y^p - Y = \delta X^2.$$

Based on Lemma 6.4.6, consider all the structures $\tilde{\mathcal{X}}_1$, $\mathcal{X}_\delta$ and ϕ defined over the extensions $\mathbb{F}_{q^n}$ of $\mathbb{F}_{q^p}$, with n even. In particular, δ is a square in all these extensions, and since m is odd, the following occurs.

Proposition 6.4.7. (BOUW *et al.*, 2016, Lemma 9.1). Let n be an even positive integer such that $p \mid n$. Then, $\mathcal{X}_\delta$ is $\mathbb{F}_{q^n}$ -maximal if and only if

$$p \equiv 3 \pmod{4} \text{ and } n \equiv 2 \pmod{4}.$$

Therefore, from Theorem 2.7.4, the sign in (6.9) is obtained.

Lemma 6.4.8. Let n be an even positive integer such that $p \mid n$. The curve $\tilde{\mathcal{X}}_1$ is $\mathbb{F}_{q^n}$ -maximal if and only if $p \equiv 3 \pmod{4}$ and $n \equiv 2 \pmod{4}$. In particular, (6.9) can be rewritten in the form

$$N_{q^n}(\tilde{\mathcal{X}}_1) = \begin{cases} q^n + 1, & \text{if } n \text{ is odd} \\ q^n + 1 - 2g(\tilde{\mathcal{X}}_1)q^{n/2}, & \text{if } n \text{ is even and } p \equiv 1 \pmod{4} \\ q^n + 1 - 2g(\tilde{\mathcal{X}}_1)q^{n/2}, & \text{if } n \equiv 0 \pmod{4} \text{ and } p \equiv 3 \pmod{4} \\ q^n + 1 + 2g(\tilde{\mathcal{X}}_1)q^{n/2}, & \text{if } n \equiv 2 \pmod{4} \text{ and } p \equiv 3 \pmod{4}. \end{cases}$$

The case $p \nmid n$

Let s be the period of $\tilde{\mathcal{X}}_1$ over $\mathbb{F}_q$. By Lemma 6.4.8, it follows that

$$s = \begin{cases} 2p, & \text{if } p \equiv 1 \pmod{4} \\ 4p, & \text{if } p \equiv 3 \pmod{4}. \end{cases} \quad (6.11)$$

Since $\gcd(n, s) = 1$, for each odd positive integer n such that $p \nmid n$, and $N_q(\tilde{\mathcal{X}}_1) = qp + 1$ by Lemma 6.4.5, the sign in (6.10) is obtained as a straightforward application of Theorem 6.3.2.

Lemma 6.4.9. If $p \nmid n$, then

$$N_{q^n}(\tilde{\mathcal{X}}_1) = \begin{cases} q^n + 1, & \text{if } n \text{ is even} \\ q^n + 1 + 2g(\tilde{\mathcal{X}}_1)q^{n/2}p^{-1/2} \left(\frac{(-1)^{(n-1)/2}n}{p} \right), & \text{if } n \text{ is odd} \end{cases},$$

where $\left(\frac{*}{p} \right)$ is the Legendre symbol.

Step 3: conclusion

Theorem 6.1.1 follows from Lemmas 6.4.3, 6.4.8 and 6.4.9. ■

6.5 Proof of Theorem 6.1.2

In this section, the proof of Theorem 6.1.2 is presented. For this, the following proposition recalls two properties: the first is the well-known Quadratic Gauss Sum (see (LIDL; NIEDERREITER, 1997, Theorem 5.15)), while the second follows by the definition of μ_p .

Proposition 6.5.1. The following holds.

1. Let $\tilde{p}^{1/2}$ be given as in (6.3). Then

$$\tilde{p}^{1/2} = \sum_{i=0}^{p-1} \left(\frac{i}{p}\right) \zeta_p^i.$$

2. If $r_0, r_1, \dots, r_{p-1} \in \mathbb{Q}$ are such that

$$r_0 + r_1 \zeta_p + \dots + r_{p-1} \zeta_p^{p-1} = 0,$$

then $r_0 = r_1 = \dots = r_{p-1}$.

6.5.1 Proof

By Proposition 6.3.6 and Lemma 6.4.3

$$L_{\mathcal{X}_{q,\mathcal{J}}}(T) = \left(L_{\tilde{\mathcal{X}}_1}(T) \right)^{\frac{q-1}{p-1}},$$

which shows that $L_{\mathcal{X}_{q,\mathcal{J}}}(T)$ is essentially determined by $L_{\tilde{\mathcal{X}}_1}(T)$. Considering $M_{\tilde{\mathcal{X}}_1}(T)$ the reciprocal of the polynomial $L_{\tilde{\mathcal{X}}_1}(q^{-1/2}T) \in \mathbb{Q}(p^{1/2})[T]$, then

$$M_{\tilde{\mathcal{X}}_1}(T) = \prod_{i=1}^{2g(\tilde{\mathcal{X}}_1)} (T - \xi_i),$$

where, for $i = 1, \dots, 2g(\tilde{\mathcal{X}}_1)$, the elements $\xi_i \in \mathbb{C}$ satisfy

$$-q^{-n/2} \left[N_{q^n}(\tilde{\mathcal{X}}_1) - (q^n + 1) \right] = \sum_{i=1}^{2g(\tilde{\mathcal{X}}_1)} \xi_i^n. \quad (6.12)$$

Note that $M_{\tilde{\mathcal{X}}_1}(T)$ is a self-reciprocal polynomial, that is, $M_{\tilde{\mathcal{X}}_1}(T) = L_{\tilde{\mathcal{X}}_1}(q^{-1/2}T)$. Further, since $\tilde{\mathcal{X}}_1$ is a supersingular curve with period s given by (6.11), the following holds

$$\min \left\{ n : \xi_i^n = 1 \text{ for all } i = 1, \dots, 2g(\tilde{\mathcal{X}}_1) \right\} = \begin{cases} 2p, & \text{if } p \equiv 1 \pmod{4} \\ 4p, & \text{if } p \equiv 3 \pmod{4}. \end{cases} \quad (6.13)$$

Thus, to determine the L-polynomial $L_{\tilde{\mathcal{X}}_1}(T)$, it is necessary to describe the polynomial $M_{\tilde{\mathcal{X}}_1}(T)$.

From (6.13) and Lemma 6.4.8,

$$\xi_i^2 \in \begin{cases} \mu_p \cup \{1\}, & \text{if } p \equiv 1 \pmod{4} \\ \mu_{2p} \cup \{-1\}, & \text{if } p \equiv 3 \pmod{4}, \end{cases}$$

and so

$$\sum_{i=1}^{2g(\tilde{\mathcal{X}}_1)} \xi_i^2 = \begin{cases} r_0 + r_1 \zeta_p + \cdots + r_{p-1} \zeta_p^{p-1}, & \text{if } p \equiv 1 \pmod{4} \\ r_0(-1) + r_1(-\zeta_p) + \cdots + r_{p-1}(-\zeta_p^{p-1}), & \text{if } p \equiv 3 \pmod{4}, \end{cases} \quad (6.14)$$

with $r_i \in \mathbb{N}$ being such that $\sum_{i=0}^{p-1} r_i = 2g(\tilde{\mathcal{X}}_1) = p^t(p-1)$. Also, (6.12) and Lemma 6.4.9 imply

that $\sum_{i=1}^{2g(\tilde{\mathcal{X}}_1)} \xi_i^2 = 0$, and then the second assertion of Proposition 6.5.1 gives $r_0 = r_1 = \cdots = r_{p-1} = p^{t-1}(p-1)$. Thus

$$M_{\tilde{\mathcal{X}}_1}(T) = \prod_{i=1}^{2g(\tilde{\mathcal{X}}_1)} (T - \xi_i) = \prod_{i=0}^{p-1} (T - \lambda_i)^{m_i} (T + \lambda_i)^{n_i}, \quad (6.15)$$

where $m_i, n_i \in \mathbb{N}$ are such that $m_i + n_i = p^{t-1}(p-1)$, and $\pm \lambda_i$ are the square roots of the p elements in

$$\begin{cases} \mu_p \cup \{1\}, & \text{if } p \equiv 1 \pmod{4} \\ \mu_{2p} \cup \{-1\}, & \text{if } p \equiv 3 \pmod{4}, \end{cases}$$

for each $i = 0, \dots, p-1$.

Label the elements λ_i in a way that

$$\lambda_i = \begin{cases} \zeta_p^i, & \text{if } p \equiv 1 \pmod{4} \\ \mathbf{i} \zeta_p^i, & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

Furthermore, from (6.12) and Lemmas 6.4.8, 6.4.9, $\sum_{i=1}^{2g(\tilde{\mathcal{X}}_1)} \xi_i^p = 0$ and

$$\sum_{i=1}^{2g(\tilde{\mathcal{X}}_1)} \xi_i = -p^{t-1}(p-1)p^{1/2}.$$

Since (6.13) and Lemma 6.4.8 imply that

$$\xi_i^p = \begin{cases} \pm 1, & \text{if } p \equiv 1 \pmod{4} \\ \pm \mathbf{i}, & \text{if } p \equiv 3 \pmod{4}, \end{cases}$$

by the choice of λ_i and equation (6.15),

$$g(\tilde{\mathcal{X}}_1) = \sum_{i=0}^{p-1} m_i = \sum_{i=0}^{p-1} n_i \quad (6.16)$$

$$-p^{t-1}(p-1)p^{1/2} = \sum_{i=0}^{p-1} (m_i - n_i) \lambda_i. \quad (6.17)$$

In (6.17), using the first assertion of Proposition 6.5.1, one may replace $p^{1/2}$ by

$$\begin{cases} \sum_{i=0}^{p-1} \left(\frac{i}{p}\right) \lambda_i, & \text{if } p \equiv 1 \pmod{4} \\ -\sum_{i=0}^{p-1} \left(\frac{i}{p}\right) \lambda_i, & \text{if } p \equiv 3 \pmod{4}. \end{cases} \quad (6.18)$$

Hence, the second item of Proposition 6.5.1, combined with (6.16) and $m_i + n_i = p^{t-1}(p-1)$, yields $n_0 = m_0 = \frac{p^{t-1}(p-1)}{2}$ and, for $1 \leq i \leq p-1$,

$$(m_i, n_i) = \begin{cases} (0, p^{t-1}(p-1)), & \text{if } \left(\frac{i}{p}\right) = 1 \text{ and } p \equiv 1 \pmod{4} \\ (p^{t-1}(p-1), 0), & \text{if } \left(\frac{i}{p}\right) = 1 \text{ and } p \equiv 3 \pmod{4} \\ (p^{t-1}(p-1), 0), & \text{if } \left(\frac{i}{p}\right) = -1 \text{ and } p \equiv 1 \pmod{4} \\ (0, p^{t-1}(p-1)), & \text{if } \left(\frac{i}{p}\right) = -1 \text{ and } p \equiv 3 \pmod{4}. \end{cases}$$

Thus, (6.15) becomes

$$\begin{aligned} M_{\mathcal{X}_1}(T) &= \prod_{i=1}^{2g(\tilde{\mathcal{X}}_1)} (T - \xi_i) \\ &= \begin{cases} \left(T^2 - 1\right)^{\frac{p^{t-1}(p-1)}{2}} \left(\prod_{\left(\frac{i}{p}\right)=1} (T + \lambda_i) \prod_{\left(\frac{i}{p}\right)=-1} (T - \lambda_i) \right)^{p^{t-1}(p-1)}, & \text{if } p \equiv 1 \pmod{4} \\ \left(T^2 + 1\right)^{\frac{p^{t-1}(p-1)}{2}} \left(\prod_{\left(\frac{i}{p}\right)=1} (T - \lambda_i) \prod_{\left(\frac{i}{p}\right)=-1} (T + \lambda_i) \right)^{p^{t-1}(p-1)}, & \text{if } p \equiv 3 \pmod{4}. \end{cases} \end{aligned}$$

Let $\sigma_k \in \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ be such that $\sigma_k(\zeta_p) = \zeta_p^k$, with $1 \leq k \leq p-1$. Then, the first item of Proposition 6.5.1 implies

$$\sigma_k(\tilde{p}^{1/2}) = \begin{cases} \tilde{p}^{1/2}, & \text{if } \left(\frac{k}{p}\right) = 1 \\ -\tilde{p}^{1/2}, & \text{if } \left(\frac{k}{p}\right) = -1, \end{cases}$$

where $\tilde{p}^{1/2} \in \mathbb{Q}(\zeta_p)$ is defined as in (6.3). In particular,

$$\lambda_i/p^{1/2} = \begin{cases} \zeta_p^i/\tilde{p}^{1/2} = \sigma_i(\zeta_p/\tilde{p}^{1/2}), & \text{if } \left(\frac{i}{p}\right) = 1 \text{ and } p \equiv 1 \pmod{4} \\ -\zeta_p^i/\tilde{p}^{1/2} = \sigma_i(-\zeta_p/\tilde{p}^{1/2}), & \text{if } \left(\frac{i}{p}\right) = 1 \text{ and } p \equiv 3 \pmod{4} \\ \zeta_p^i/\tilde{p}^{1/2} = \sigma_i(-\zeta_p/\tilde{p}^{1/2}), & \text{if } \left(\frac{i}{p}\right) = -1 \text{ and } p \equiv 1 \pmod{4} \\ -\zeta_p^i/\tilde{p}^{1/2} = \sigma_i(\zeta_p/\tilde{p}^{1/2}), & \text{if } \left(\frac{i}{p}\right) = -1 \text{ and } p \equiv 3 \pmod{4} \end{cases}$$

for each $i \in \{1, \dots, p-1\}$. Thus, if $p \equiv 1 \pmod{4}$, then

$$\begin{aligned} \prod_{\left(\frac{i}{p}\right)=1} (p^{1/2}T + \lambda_i) \prod_{\left(\frac{i}{p}\right)=-1} (p^{1/2}T - \lambda_i) &= p^{(p-1)/2} \prod_{\left(\frac{i}{p}\right)=1} (T + \lambda_i/p^{1/2}) \prod_{\left(\frac{i}{p}\right)=-1} (T - \lambda_i/p^{1/2}) \\ &= p^{(p-1)/2} \prod_{i=1}^{p-1} \left(T - \sigma_i(-\zeta_p/\tilde{p}^{1/2}) \right) \\ &= p^{(p-1)/2} \prod_{\sigma \in \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})} \left(T - \sigma(-\zeta_p/\tilde{p}^{1/2}) \right). \end{aligned}$$

Also, for $p \equiv 3 \pmod{4}$

$$\begin{aligned} \prod_{\left(\frac{i}{p}\right)=1} (p^{1/2}T - \lambda_i) \prod_{\left(\frac{i}{p}\right)=-1} (p^{1/2}T + \lambda_i) &= p^{(p-1)/2} \prod_{\left(\frac{i}{p}\right)=1} (T - \lambda_i/p^{1/2}) \prod_{\left(\frac{i}{p}\right)=-1} (T + \lambda_i/p^{1/2}) \\ &= p^{(p-1)/2} \prod_{i=1}^{p-1} \left(T - \sigma_i(-\zeta_p/\tilde{p}^{1/2}) \right) \\ &= p^{(p-1)/2} \prod_{\sigma \in \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})} \left(T - \sigma(-\zeta_p/\tilde{p}^{1/2}) \right). \end{aligned}$$

Therefore, the proof follows by the equalities $L_{\tilde{\mathcal{X}}_1}(T) = M_{\tilde{\mathcal{X}}_1}(q^{1/2}T) = M_{\tilde{\mathcal{X}}_1}(p^{t-1}p^{1/2}T)$. ■

6.6 Examples

In what follows, we consider the cases $p = 3, 5, 7, 11, 13, 17$ and 19 to illustrate Theorem 6.1.2.

6.6.1 The L -polynomial of $\mathcal{X}_{\mathcal{G}_{\mathcal{P}}}$ for $p = 3$

In this case, $p \equiv 3 \pmod{4}$ and

$$3 \cdot \mathcal{M}_3(T) = 3T^2 + 3T + 1,$$

where $\mathcal{M}_3(T)$ is the minimal polynomial of $-\zeta_3/(\mathbf{i}3^{1/2})$ over $\mathbb{Q}$. Therefore,

$$3 \cdot \mathcal{M}_3(3^{t-1}T) = qT^2 + q_0T + 1,$$

which gives that

$$L_{\mathcal{X}_{\mathcal{G}_{\mathcal{P}}}}(T) = \left((qT^2 + 1) \cdot \left(qT^2 + q_0T + 1 \right)^2 \right)^{\frac{q_0(q-1)}{6}}$$

by Theorem 6.1.2.

6.6.2 The L -polynomial of $\mathcal{X}_{q,\mathcal{F}}$ for $p = 5$

Here $p \equiv 1 \pmod{4}$ and

$$5^2 \cdot \mathcal{M}_5(T) = 25T^4 + 25T^3 + 15T^2 + 5T + 1,$$

where $\mathcal{M}_5(T)$ is the minimal polynomial of $-\zeta_5/5^{1/2}$ over $\mathbb{Q}$. Therefore,

$$5^2 \cdot \mathcal{M}_5(5^{t-1}T) = q^2T^4 + qq_0T^3 + 3qT^2 + q_0T + 1,$$

which gives that

$$L_{\mathcal{X}_{q,\mathcal{F}}}(T) = \left((qT^2 - 1) \cdot \left(q^2T^4 + qq_0T^3 + 3qT^2 + q_0T + 1 \right)^2 \right)^{\frac{q_0(q-1)}{10}}$$

by Theorem 6.1.2.

6.6.3 The L -polynomial of $\mathcal{X}_{q,\mathcal{F}}$ for $p = 7$

In this case, $p \equiv 3 \pmod{4}$ and

$$7^3 \cdot \mathcal{M}_7(T) = 343T^6 + 343T^5 + 147T^4 + 49T^3 + 21T^2 + 7T + 1,$$

where $\mathcal{M}_7(T)$ is the minimal polynomial of $-\zeta_7/(\mathbf{i}7^{1/2})$ over $\mathbb{Q}$. Therefore,

$$7^3 \cdot \mathcal{M}_7(7^{t-1}T) = q^3T^6 + q^2q_0T^5 + 3q^2T^4 + qq_0T^3 + 3qT^2 + q_0T + 1,$$

which gives that

$$L_{\mathcal{X}_{q,\mathcal{F}}}(T) = \left((qT^2 + 1) \cdot \left(q^3T^6 + q^2q_0T^5 + 3q^2T^4 + qq_0T^3 + 3qT^2 + q_0T + 1 \right)^2 \right)^{\frac{q_0(q-1)}{14}}$$

by Theorem 6.1.2.

6.6.4 The L -polynomial of $\mathcal{X}_{q,\mathcal{F}}$ for $p = 11$

In this case, $p \equiv 3 \pmod{4}$ and

$$\begin{aligned} 11^5 \cdot \mathcal{M}_{11}(T) &= 161051T^{10} + 161051T^9 + 73205T^8 + 14641T^7 - 1331T^6 - 1331T^5 \\ &\quad - 121T^4 + 121T^3 + 55T^2 + 11T + 1 \\ &= 11^5T^{10} + 11^5T^9 + 5 \cdot 11^4T^8 + 11^4T^7 - 11^3T^6 - 11^3T^5 - 11^2T^4 + 11^2T^3 \\ &\quad + 5 \cdot 11T^2 + 11T + 1 \end{aligned}$$

where $\mathcal{M}_{11}(T)$ is the minimal polynomial of $-\zeta_{11}/(\mathbf{i}11^{1/2})$ over $\mathbb{Q}$. Therefore,

$$\begin{aligned} 11^5 \cdot \mathcal{M}_{11}(11^{t-1}T) &= q^5T^{10} + q^4q_0T^9 + 5q^4T^8 + q^3q_0T^7 - q^3T^6 - q^2q_0T^5 - q^2T^4 + qq_0T^3 \\ &\quad + 5qT^2 + q_0T + 1 \end{aligned}$$

and

$$L_{\mathcal{X}_{q,\mathcal{F}}}(T) = \left((qT^2 + 1) \cdot \left(11^5 \cdot \mathcal{M}_{11}(11^{t-1}T) \right)^2 \right)^{\frac{q_0(q-1)}{22}}$$

by Theorem 6.1.2.

6.6.5 The L -polynomial of $\mathcal{X}_{q,\mathcal{F}}$ for $p = 13$

Here $p \equiv 1 \pmod{4}$ and

$$\begin{aligned} 13^6 \cdot \mathcal{M}_{13}(T) &= 4826809T^{12} + 4826809T^{11} + 2599051T^{10} + 1113879T^9 + 428415T^8 \\ &\quad + 142805T^7 + 41743T^6 + 10985T^5 + 2535T^4 + 507T^3 + 91T^2 + 13T + 1 \\ &= 13^6T^{12} + 13^6T^{11} + 7 \cdot 13^5T^{10} + 3 \cdot 13^5T^9 + 15 \cdot 13^4T^8 + 5 \cdot 13^4T^7 \\ &\quad + 19 \cdot 13^3T^6 + 5 \cdot 13^3T^5 + 15 \cdot 13^2T^4 + 3 \cdot 13^2T^3 + 7 \cdot 13T^2 + 13T + 1 \end{aligned}$$

where $\mathcal{M}_{13}(T)$ is the minimal polynomial of $-\zeta_{13}/13^{1/2}$ over $\mathbb{Q}$. Therefore,

$$\begin{aligned} 13^6 \cdot \mathcal{M}_{13}(13^{t-1}T) &= q^6T^{12} + q^5q_0T^{11} + 7q^5T^{10} + 3q^4q_0T^9 + 15q^4T^8 + 5q^3q_0T^7 \\ &\quad + 19q^3T^6 + 5q^2q_0T^5 + 15q^2T^4 + 3qq_0T^3 + 7qT^2 + q_0T + 1 \end{aligned}$$

and

$$L_{\mathcal{X}_{q,\mathcal{F}}}(T) = \left((qT^2 - 1) \cdot \left(13^6 \cdot \mathcal{M}_{13}(13^{t-1}T) \right)^2 \right)^{\frac{q_0(q-1)}{26}}$$

by Theorem 6.1.2.

6.6.6 The L -polynomial of $\mathcal{X}_{q,\mathcal{F}}$ for $p = 17$

Here $p \equiv 1 \pmod{4}$ and

$$\begin{aligned} 17^8 \cdot \mathcal{M}_{17}(T) &= 6975757441T^{16} + 6975757441T^{15} + 3693048057T^{14} + 1231016019T^{13} \\ &\quad + 265513259T^{12} + 24137569T^{11} - 7099285T^{10} - 4259571T^9 - 1252815T^8 \\ &\quad - 250563T^7 - 24565T^6 + 4913T^5 + 3179T^4 + 867T^3 + 153T^2 + 17T + 1 \\ &= 17^8T^{16} + 17^8T^{15} + 9 \cdot 17^7T^{14} + 3 \cdot 17^7T^{13} + 11 \cdot 17^6T^{12} + 17^6T^{11} \\ &\quad - 5 \cdot 17^5T^{10} - 3 \cdot 17^5T^9 - 15 \cdot 17^4T^8 - 3 \cdot 17^4T^7 - 5 \cdot 17^3T^6 + 17^3T^5 \\ &\quad + 11 \cdot 17^2T^4 + 3 \cdot 17^2T^3 + 9 \cdot 17T^2 + 17T + 1 \end{aligned}$$

where $\mathcal{M}_{17}(T)$ is the minimal polynomial of $-\zeta_{17}/17^{1/2}$ over $\mathbb{Q}$. Therefore,

$$\begin{aligned} 17^8 \cdot \mathcal{M}_{17}(17^{t-1}T) &= q^8T^{16} + q^7q_0T^{15} + 9q^7T^{14} + 3q^6q_0T^{13} + 11q^6T^{12} + q^5q_0T^{11} - 5q^5T^{10} \\ &\quad - 3q^4q_0T^9 - 15q^4T^8 - 3q^3q_0T^7 - 5q^3T^6 + q^2q_0T^5 + 11q^2T^4 + 3qq_0T^3 \\ &\quad + 9qT^2 + q_0T + 1 \end{aligned}$$

and

$$L_{\mathcal{X}_{q,\mathcal{F}}}(T) = \left((qT^2 - 1) \cdot \left(17^8 \cdot \mathcal{M}_{17}(17^{t-1}T) \right)^2 \right)^{\frac{q_0(q-1)}{34}}$$

by Theorem 6.1.2.

6.6.7 The L -polynomial of $\mathcal{X}_{\mathcal{G}_{\mathcal{S}}}$ for $p = 19$

In this case, $p \equiv 3 \pmod{4}$ and

$$\begin{aligned}
 19^9 \cdot \mathcal{M}_{19}(T) &= 322687697779T^{18} + 322687697779T^{17} + 152852067369T^{16} \\
 &\quad + 50950689123T^{15} + 15195819563T^{14} + 4469358695T^{13} + 1270238787T^{12} \\
 &\quad + 329321167T^{11} + 76759069T^{10} + 17332693T^9 + 4039951T^8 \\
 &\quad + 912247T^7 + 185193T^6 + 34295T^5 + 6137T^4 + 1083T^3 + 171T^2 + 19T + 1 \\
 &= 19^9T^{18} + 19^9T^{17} + 9 \cdot 19^8T^{16} + 3 \cdot 19^8T^{15} + 17 \cdot 19^7T^{14} + 5 \cdot 19^7T^{13} \\
 &\quad + 27 \cdot 19^6T^{12} + 7 \cdot 19^6T^{11} + 31 \cdot 19^5T^{10} + 7 \cdot 19^5T^9 + 31 \cdot 19^4T^8 + 7 \cdot 19^4T^7 \\
 &\quad + 27 \cdot 19^3T^6 + 5 \cdot 19^3T^5 + 17 \cdot 19^2T^4 + 3 \cdot 19^2T^3 + 9 \cdot 19T^2 + 19T + 1
 \end{aligned}$$

where $\mathcal{M}_{19}(T)$ is the minimal polynomial of $-\zeta_{19}/(\mathbf{i}19^{1/2})$ over $\mathbb{Q}$. Therefore,

$$\begin{aligned}
 19^9 \cdot \mathcal{M}_{19}(19^{t-1}T) &= q^9T^{18} + q^8q_0T^{17} + 9q^8T^{16} + 3q^7q_0T^{15} + 17q^7T^{14} + 5q^6q_0T^{13} \\
 &\quad + 27q^6T^{12} + 7q^5q_0T^{11} + 31q^5T^{10} + 7q^4q_0T^9 + 31q^4T^8 + 7q^3q_0T^7 \\
 &\quad + 27q^3T^6 + 5q^2q_0T^5 + 17q^2T^4 + 3qq_0T^3 + 9qT^2 + q_0T + 1
 \end{aligned}$$

and

$$L_{\mathcal{X}_{\mathcal{G}_{\mathcal{S}}}}(T) = \left((qT^2 + 1) \cdot \left(19^9 \cdot \mathcal{M}_{19}(19^{t-1}T) \right) \right)^2 \frac{q_0(q-1)}{38}$$

by Theorem 6.1.2.

6.7 Proof of Theorem 6.1.3

Consider the notation in Subsections 6.3.4 and 6.3.5. Let $\mathbb{G}_{Q_\infty}$ be the stabilizer of $Q_\infty \in \mathcal{X}_{\mathcal{G}_{\mathcal{S}}}$, $\mathbb{G}_{Q_\infty}^{(1)}$ be the unique Sylow p -subgroup of $\mathbb{G}_{Q_\infty}$, and let $\mathbb{H}$ be the cyclic complement of $\mathbb{G}_{Q_\infty}^{(1)}$ in $\mathbb{G}_{Q_\infty}$.

Let $\mathfrak{G}$ be the set of maps on $\overline{\mathbb{F}_q}(\mathcal{X}_{\mathcal{G}_{\mathcal{S}}}) = \overline{\mathbb{F}_q}(x, y)$ given by

$$(x, y) \mapsto (\alpha x + \beta, \alpha \beta^{q_0} x + \alpha^{q_0+1} y + \gamma),$$

where $\alpha \in \mathbb{F}_q^*$ and $\beta, \gamma \in \mathbb{F}_q$. One can check that $\mathfrak{G}$ is a subgroup of $\mathbb{G}$ of order $q^2(q-1)$. Moreover, the following lemma holds.

Lemma 6.7.1. $\mathfrak{G} = \mathbb{G}_{Q_\infty}$.

Proof. To show the inclusion $\mathfrak{G} \subseteq \mathbb{G}_{Q_\infty}$, consider the one-to-one correspondence between the places of $\overline{\mathbb{F}_q}(\mathcal{X}_{\mathcal{G}_{\mathcal{S}}})$ and the points on $\mathcal{X}_{\mathcal{G}_{\mathcal{S}}}$. In this sense, let τ be a primitive representation of

the place $\mathcal{Q}_\infty$. Then $(\tau(x) : \tau(y) : 1)$ is a primitive branch representation whose respective branch is the unique branch of $\mathcal{G}_\mathcal{S}$ centered at $P = (0 : 1 : 0)$. If $\sigma \in \mathfrak{G}$ is given by

$$(x, y) \mapsto (\alpha x + \beta, \alpha \beta^{q_0} x + \alpha^{q_0+1} y + \gamma),$$

where $\alpha \in \mathbb{F}_q^*$ and $\beta, \gamma \in \mathbb{F}_q$, then $\tau \circ \sigma$ is a primitive representation for the image of $\mathcal{Q}_\infty$ by σ . Moreover, using Theorem 6.3.15, one can verify that

$$(\tau \circ \sigma(x) : \tau \circ \sigma(y) : 1) = (\alpha \tau(x) + \beta : \alpha \beta^{q_0} \tau(x) + \alpha^{q_0+1} \tau(y) + \gamma : 1)$$

is also a primitive branch representation whose respective branch is a branch of $\mathcal{G}_\mathcal{S}$ centered at P . By the uniqueness of the branch of $\mathcal{G}_\mathcal{S}$ centered at P , $(\tau(x) : \tau(y) : 1)$ and $(\tau \circ \sigma(x) : \tau \circ \sigma(y) : 1)$ are equivalent branch representations, and therefore τ and $\tau \circ \sigma$ are equivalent, which implies that $\mathcal{Q}_\infty$ is fixed by σ .

For the other inclusion, let $\sigma \in \mathbb{G}_{Q_\infty}$. By Theorem 6.3.15, $\{1, x\}$ and $\{1, x, y\}$ are bases for the Riemann–Roch spaces $\mathcal{L}(qQ_\infty)$ and $\mathcal{L}((q + q_0)Q_\infty)$, respectively. Therefore, $\sigma(x) \in \mathcal{L}(qQ_\infty)$, $\sigma(y) \in \mathcal{L}((q + q_0)Q_\infty)$,

$$\sigma(x) = \alpha x + \gamma \text{ and } \sigma(y) = \alpha_1 x + \beta_1 y + \gamma_1,$$

for some $\alpha, \alpha_1, \beta_1, \gamma, \gamma_1 \in \overline{\mathbb{F}_q}$, with $\alpha \beta_1 \neq 0$ ⁴. Since σ is an $\overline{\mathbb{F}_q}$ -automorphism,

$$0 = \sigma(0) = \sigma(y^q - y - x^{q_0}(x^q - x)) = \sigma(y)^q - \sigma(y) - \sigma(x)^{q_0}(\sigma(x)^q - \sigma(x))$$

and thus

$$\begin{aligned} & (\alpha_1 X + \beta_1 Y + \gamma_1)^q - (\alpha_1 X + \beta_1 Y + \gamma_1) - (\alpha X + \gamma)^{q_0}((\alpha X + \gamma)^q - (\alpha X + \gamma)) \\ &= \lambda \left(Y^q - Y - X^{q_0}(X^q - X) \right) \end{aligned} \tag{6.19}$$

for some $\lambda \in \overline{\mathbb{F}_q}^*$. Therefore, comparing the coefficients in both sides of (6.19), it follows that

- $\alpha \in \mathbb{F}_q^*$
- $\gamma \in \mathbb{F}_q$
- $\alpha_1 = \alpha \gamma^{q_0} \in \mathbb{F}_q$
- $\beta_1 = \alpha^{q_0+1}$ and
- $\gamma_1 \in \mathbb{F}_q$,

which completes the proof. □

⁴ This condition is necessary for the map to be invertible.

Consider the subgroup of $\mathbb{G}_{Q_\infty}$ consisting of the maps

$$(x, y) \mapsto (x + \beta, \beta^{q_0}x + y + \gamma),$$

where $\beta, \gamma \in \mathbb{F}_q$, which is a Sylow p -subgroup of $\mathbb{G}_{Q_\infty}$ (of order q^2). By Theorem 6.3.19, this describes the subgroup $\mathbb{G}_{Q_\infty}^{(1)}$. Also, the cyclic complement $\mathbb{H}$ of $\mathbb{G}_{Q_\infty}^{(1)}$ in $\mathbb{G}_{Q_\infty}$ can be given by the maps

$$(x, y) \mapsto (\alpha x, \alpha^{q_0+1}y),$$

where $\alpha \in \mathbb{F}_q^*$, which has order $q - 1$, and in this case

$$\mathbb{G}_{Q_\infty} = \mathbb{G}_{Q_\infty}^{(1)} \rtimes \mathbb{H}.$$

Finally, by Theorem 6.3.20, $\mathbb{G} = \mathbb{G}_{Q_\infty}$, which completes the proof. Indeed, $|\mathbb{G}_{Q_\infty}^{(1)}| = q^2 > q_0(q - 1) + 1 = 2g(\mathcal{X}_{\mathcal{G}_\mathcal{F}}) + 1$, where $g(\mathcal{X}_{\mathcal{G}_\mathcal{F}}) = \frac{q_0(q-1)}{2}$ is the genus of $\mathcal{X}_{\mathcal{G}_\mathcal{F}}$, and also, since $p \neq 2$, a comparison of genus (when $t > 1$) and inflection points (when $m = t = 1$) shows that $\mathcal{X}_{\mathcal{G}_\mathcal{F}}$ is not birationally equivalent to any of the curves (6.7), (6.1) and (6.8). ■

6.8 Final remarks

Based on (VOLOCH, 2000), this section illustrates an application of the description of $L_{\mathcal{X}_{\mathcal{G}_\mathcal{F}}}(T)$ provided in Section 6.6.

It is well known (see (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 9.70)) that the number of $\mathbb{F}_{q^n}$ -rational points on the Jacobian variety of $\mathcal{X}_{\mathcal{G}_\mathcal{F}}$ is given by the number $L_{\mathcal{X}_{\mathcal{G}_\mathcal{F}}/\mathbb{F}_{q^n}}(1)$, where $L_{\mathcal{X}_{\mathcal{G}_\mathcal{F}}/\mathbb{F}_{q^n}}(T)$ is the L-polynomial of $\mathcal{X}_{\mathcal{G}_\mathcal{F}}$ over $\mathbb{F}_{q^n}$ and $L_{\mathcal{X}_{\mathcal{G}_\mathcal{F}}/\mathbb{F}_q}(T) = L_{\mathcal{X}_{\mathcal{G}_\mathcal{F}}}(T)$.

One can check that $N_q(\mathcal{X}_{\mathcal{G}_\mathcal{F}}) = N_{q^2}(\mathcal{X}_{\mathcal{G}_\mathcal{F}})$ by Theorem 6.1.1, and that

$$L_{\mathcal{X}_{\mathcal{G}_\mathcal{F}}}(1) < L_{\mathcal{X}_{\mathcal{G}_\mathcal{F}}/\mathbb{F}_{q^2}}(1) = \left(((-1)^{\frac{p+1}{2}} + q)(q^{p-1} + q^{p-2} + \cdots + q + 1) \right)^{\frac{q_0(q-1)}{p}}$$

for $p = 3, 5, 7, 11, 13, 17$ and 19 . Accordingly, in these cases the group generated by the $\mathbb{F}_{q^2}$ -rational points of $\mathcal{X}_{\mathcal{G}_\mathcal{F}}$ is not the whole group of $\mathbb{F}_{q^2}$ -rational points of the Jacobian variety of $\mathcal{X}_{\mathcal{G}_\mathcal{F}}$, which will be denoted here as $J_{\mathcal{X}_{\mathcal{G}_\mathcal{F}}/\mathbb{F}_{q^2}}$.

Using the construction presented in the main result of (VOLOCH, 2000) and considering $p = 3, 5, 7, 11, 13, 17, 19$, for any subgroup G of $J_{\mathcal{X}_{\mathcal{G}_\mathcal{F}}/\mathbb{F}_{q^2}}$ containing $J_{\mathcal{X}_{\mathcal{G}_\mathcal{F}}/\mathbb{F}_q}$ it is possible to obtain an étale cover of $\mathcal{X}_{\mathcal{G}_\mathcal{F}}$ of degree $i = [J_{\mathcal{X}_{\mathcal{G}_\mathcal{F}}/\mathbb{F}_{q^2}} : G]$ with at least $i(q^2 + 1)$ rational points over $\mathbb{F}_{q^2}$ and genus $i(g - 1) + 1$, and i can be considered as being any divisor of $L_{\mathcal{X}_{\mathcal{G}_\mathcal{F}}/\mathbb{F}_{q^2}}(1)/L_{\mathcal{X}_{\mathcal{G}_\mathcal{F}}}(1)$.

BIBLIOGRAPHY

ABATANGELO, V.; KORCHMÁROS, G. Una generalizzazione di un teorema di B. Segre sui punti regolari rispetto ad una ellisse di un piano affine di Galois. **Annali di Matematica Pura ed Applicata**, v. 172, n. 1, p. 87–102, 1997. Citations on pages 106, 107, 117, and 118.

ARAKELIAN, N.; BORGES, H. Frobenius nonclassicality of Fermat curves with respect to cubics. **Israel Journal of Mathematics**, v. 218, n. 1, p. 273–297, 2017. Citations on pages 86 and 105.

ARAKELIAN, N.; SPEZIALI, P. On generalizations of Fermat curves over finite fields and their automorphisms. **Communications in Algebra**, v. 45, n. 11, p. 4926–4938, 2017. Citation on page 106.

AUBRY, Y.; PERRET, M. Divisibility of zeta functions of curves in a covering. **Archiv der Mathematik**, v. 82, n. 3, p. 205–213, 2004. Citation on page 65.

BALLICO, E.; RAVAGNANI, A. Embedding Suzuki curves in $\mathbb{P}^4$. **Journal of Commutative Algebra**, v. 7, n. 2, p. 149–166, 2015. Citation on page 122.

BARTOLI, D.; MONTANUCCI, M.; ZINI, G. Weierstrass semigroups at every point of the Suzuki curve. 2018. Available: <<https://arxiv.org/pdf/1811.07890.pdf>>. Accessed: 29/01/2019. Citation on page 122.

BASSA, A. *et al.* Towards a characterization of subfields of the Deligne-Lusztig function fields. **Journal of Combinatorial Theory, Series A**, v. 120, n. 7, p. 1351–1371, 2013. Citation on page 122.

BORGES, H.; COOK, G.; COUTINHO, M. Plane sections of Fermat surfaces over finite fields. **Finite Fields and Their Applications**, v. 52, p. 156–173, 2018. Citation on page 81.

BORGES, H.; COUTINHO, M. On some generalized Fermat curves and chords of an affinely regular polygon inscribed in a hyperbola. To appear in *Journal of Pure and Applied Algebra*. 2019. Citation on page 105.

_____. On the Zeta function and the automorphism group of the generalized Suzuki curve. Preprint 2019. Citation on page 121.

BOUW, I. *et al.* Zeta Functions of a Class of Artin-Schreier Curves with Many Automorphisms. In: EISCHEN, E. *et al.* (Ed.). **Directions in Number Theory**: Proceedings of the 2014 WIN3 Workshop. Cham: Springer, 2016. p. 87–124. Citations on pages 128, 129, and 135.

CARLIN, M.; VOLOCH, J. F. Plane curves with many points over finite fields. **Rocky Mountain Journal of Mathematics**, v. 34, n. 4, p. 1255–1259, 2004. Citations on pages 82 and 84.

CHEN, C. Y.; DUURSMA, I. Geometric Reed-Solomon codes of length 64 and 65 over $\mathbb{F}_8$. **IEEE Transactions on Information Theory**, v. 49, n. 5, p. 1351–1353, 2003. Citation on page 122.

CHEVALLEY, C. **Introduction to the Theory of Algebraic Functions of One Variable**. Providence: American Mathematical Society, 1951. Citation on page 23.

COULTER, R.; HENDERSON, M. A note on the roots of trinomials over a finite field. **Bulletin of the Australian Mathematical Society**, v. 69, n. 3, p. 429–432, 2004. Citation on page 134.

COX, D.; LITTLE, J.; O'SHEA, D. **Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra**. 3. ed. New York: Springer-Verlag New York, 2007. Citation on page 70.

CRAATS, V.; SIMONIS, J. Affinely regular polygons. **Nieuw Archief voor Wiskunde**, v. 4, n. 4, p. 225–240, 1986. Citation on page 116.

DELIGNE, P.; LUSZTIG, G. Representations of reductive groups over finite fields. **Annals of Mathematics**, v. 103, n. 1, p. 103–161, 1976. Citation on page 121.

DEOLALIKAR, V. Determining irreducibility and ramification groups for an additive extension of the rational function fields. **Journal of Number Theory**, v. 97, n. 2, p. 269–286, 2002. Citation on page 130.

DUURSMA, I.; EID, A. Smooth embeddings for the Suzuki and Ree curves. In: BALLEST, S.; PERRET, M.; ZAYTSEV, A. (Ed.). **Algorithmic arithmetic, geometry, and coding theory: 14th International Conference on Arithmetic, Geometry, Cryptography, and Coding Theory**, June 3-7 2013, CIRM Marseille, France. Providence: American Mathematical Society, 2015. p. 251–291. Citation on page 122.

DUURSMA, I.; PARK, S. Delta sets for divisors supported in two points. **Finite Fields and Their Applications**, v. 18, p. 865–885, 2012. Citation on page 122.

DUURSMA, I.; STICHTENOTH, H.; VOSS, C. Generalized Hamming weights for duals of BCH codes, and maximal algebraic function fields. In: PELLIKAAN, R.; PERRET, M.; VLADUT, S. G. (Ed.). **Arithmetic, Geometry and Coding Theory: Proceedings of the International Conference held at Centre International de Rencontres de Mathématiques (CIRM), Luminy, France, June 28 - July 2, 1993**. Berlin, Boston: De Gruyter, 1996. p. 53–66. Citation on page 127.

EID, A. *et al.* Suzuki-invariant codes from the Suzuki curve. **Designs, Codes and Cryptography**, v. 81, n. 3, p. 413–425, 2016. Citation on page 122.

FANALI, S.; GIULIETTI, M. On the number of rational points of generalized Fermat curves over finite fields. **International Journal of Number Theory**, v. 8, n. 4, p. 1087–1097, 2012. Citation on page 106.

FRIEDLANDER, H. *et al.* The a-numbers of Jacobians of Suzuki curves. **Proceedings of the American Mathematical Society**, v. 141, n. 9, p. 3019–3028, 2013. Citation on page 122.

FUHRMANN, R.; TORRES, F. On Weierstrass points and optimal curves. **Supplemento ai Rendiconti del Circolo matematico di Palermo**, v. 51, p. 25–46, 1998. Citation on page 122.

FULTON, W. **Algebraic Curves: An Introduction to Algebraic Geometry**. [s.n.], 2008. Available: <<http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf>>. Accessed: 29/01/2019. Citations on pages 27, 33, and 52.

GARCIA, A.; STICHTENOTH, H. Elementary abelian p -extensions of algebraic function fields. **Manuscripta Mathematica**, v. 72, n. 1, p. 67–79, 1991. Citations on pages [121](#), [122](#), [126](#), [129](#), and [132](#).

GARCIA, A.; VOLOCH, J. F. Wronskians and linear independence in fields of prime characteristic. **Manuscripta Mathematica**, v. 59, n. 4, p. 457–469, 1987. Citation on page [89](#).

_____. Fermat curves over finite fields. **Journal of Number Theory**, v. 30, n. 3, p. 345–356, 1988. Citations on pages [105](#) and [106](#).

GIULIETTI, M. On the number of chords of an affinely regular polygon passing through a given point. **Acta Scientiarum Mathematicarum (Szeged)**, v. 74, n. 3-4, p. 901–913, 2008. Citations on pages [106](#), [117](#), and [118](#).

GIULIETTI, M.; KORCHMÁROS, G. On automorphism groups of certain Goppa codes. **Designs, Codes and Cryptography**, v. 47, n. 1-3, p. 177–190, 2008. Citation on page [122](#).

_____. Garden of curves with many automorphisms. In: NIEDERREITER, H. *et al.* (Ed.). **Algebraic Curves and Finite Fields: Cryptography and Other Applications**. Berlin, Boston: De Gruyter, 2014. p. 93–120. Citation on page [123](#).

GIULIETTI, M.; KORCHMÁROS, G.; TORRES, F. Quotients curves of the Suzuki curve. **Acta Arithmetica**, v. 122, n. 3, p. 245–274, 2006. Citation on page [122](#).

GIULIETTI, M. *et al.* On some Galois covers of the Suzuki and Ree curves. **Journal of Number Theory**, v. 189, p. 220–254, 2018. Citation on page [122](#).

GOLDSCHMIDT, D. M. **Algebraic Functions and Projective Curves**. New York: Springer-Verlag New York, 2003. Citations on pages [23](#), [27](#), [41](#), [42](#), [57](#), and [60](#).

HANSEN, J. P. Deligne-Lusztig varieties and group codes. In: STICHTENOTH, H.; TSFASMAN, M. A. (Ed.). **Coding Theory and Algebraic Geometry: Proceedings of the International Workshop held in Luminy, France, June 17-21, 1991**. Berlin, Heidelberg: Springer-Verlag, 1992. p. 63–81. Citation on page [121](#).

HANSEN, J. P.; STICHTENOTH, H. Group codes on certain algebraic curves with many rational points. **Applicable Algebra in Engineering, Communication and Computing**, v. 1, n. 1, p. 67–77, 1990. Citations on pages [121](#) and [122](#).

HASSE, H. Zur Theorie der abstrakten elliptischen Funktionenkörper I: Die Struktur der Gruppe der Divisorenklassen endlicher Ordnung. **Journal für die reine und angewandte Mathematik**, v. 1936, n. 175, p. 55–62, 1936. Citation on page [65](#).

_____. Zur Theorie der abstrakten elliptischen Funktionenkörper II: Automorphismen und Mero-morphismen. Das Additionstheorem. **Journal für die reine und angewandte Mathematik**, v. 1936, n. 175, p. 69–88, 1936. Citation on page [65](#).

_____. Zur Theorie der abstrakten elliptischen Funktionenkörper III: Die Struktur des Meromorphismenrings. Die Riemannsche Vermutung. **Journal für die reine und angewandte Mathematik**, v. 1936, n. 175, p. 193–208, 1936. Citation on page [65](#).

HENN, H. W. Funktionenkörper mit großer Automorphismengruppe. **Journal für die reine und angewandte Mathematik**, v. 1978, n. 302, p. 96–115, 1978. Citation on page [122](#).

HERNANDO, F.; MCGUIRE, G. Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions. **Journal of Algebra**, v. 343, n. 1, p. 78–92, 2011. Citation on page 81.

HIRSCHFELD, J. W. P.; KORCHMÁROS, G. On the Number of Solutions of an Equation Over a Finite Field. **Bulletin of the London Mathematical Society**, v. 33, n. 1, p. 16–24, 2001. Citations on pages 85 and 89.

HIRSCHFELD, J. W. P.; KORCHMÁROS, G.; TORRES, F. **Algebraic Curves over a Finite Field**. Princeton: Princeton University Press, 2008. Citations on pages 23, 27, 31, 32, 33, 34, 35, 36, 37, 39, 40, 41, 42, 43, 45, 47, 48, 49, 50, 51, 52, 54, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 122, 123, 127, 130, 131, and 144.

JANWA, H.; MCGUIRE, G.; WILSON, R. M. Double-Error-Correcting Cyclic Codes and Absolutely Irreducible Polynomials over GF(2). **Journal of Algebra**, v. 178, n. 2, p. 665–676, 1995. Citation on page 81.

JANWA, H.; WILSON, R. M. Hyperplane sections of Fermat varieties in P^3 in char. 2 and some applications to cyclic codes. In: COHEN, G.; MORA, T.; MORENO, O. (Ed.). **Applied Algebra, Algebraic Algorithms and Error-Correcting Codes: AAECC**, 1993. Berlin, Heidelberg: Springer Berlin Heidelberg, 1993. p. 180–194. Citation on page 81.

JOLY, J.-R. Équations et variétés algébriques sur un corps fini. **L'Enseignement Mathématique**, v. 19, n. 2, p. 1–117, 1973. Citations on pages 92 and 129.

KIRFEL, C.; PELLIKAAN, R. The minimum distance of codes in an array coming from telescopic semigroups. **IEEE Transactions on Information Theory**, v. 41, n. 6, p. 1720–1732, 1995. Citation on page 122.

KORCHMÁROS, G. Poligoni affini regolari dei piani di Galois di ordine dispari. **Atti della Accademia Nazionale dei Lincei. Rendiconti della Classe di Scienze Fisiche, Matematiche e Naturali**, v. 56, p. 690–697, 1974. Citations on pages 116 and 117.

_____. Eine geometrische Begründung zur Theorie der affin-regulären n -Ecke von F. Bachmann and E. Schmidt. **Periodica Polytechnica (Budapest)**, v. 5, p. 29–42, 1976. Citation on page 116.

_____. Estensioni del concetto di poligono affin regolare ad un qualunque piano affine. **Atti della Accademia Nazionale dei Lincei. Rendiconti della Classe di Scienze Fisiche, Matematiche e Naturali**, v. 60, n. 8, p. 119–125, 1976. Citation on page 116.

_____. New examples of k -arcs in $PG(2, q)$. **European Journal of Combinatorics**, v. 4, n. 4, p. 329–334, 1983. Citation on page 117.

KORCHMÁROS, G.; STORME, L.; SZŐNYI, T. Space-filling subsets of a normal rational curve. **Journal of Statistical Planning and Inference**, v. 58, n. 1, p. 93–110, 1997. Citation on page 117.

KORCHMÁROS, G.; SZŐNYI, T. Affinely regular polygons in an affine plane. **Contributions to Discrete Mathematics**, v. 3, n. 1, p. 20–38, 2008. Citations on pages 116 and 117.

LAUTER, K. Deligne-Lusztig curves as ray class fields. **Manuscripta Mathematica**, v. 98, n. 1, p. 87–96, 1999. Citation on page 122.

LIANG, J. On the solutions of trinomial equations over finite fields. **Bulletin of the Calcutta Mathematical Society**, v. 70, p. 379–382, 1978. Citation on page 134.

LIDL, R.; NIEDERREITER, H. **Finite Fields**. Cambridge: Cambridge University Press, 1997. Citation on page 136.

MATTAREI, S. On a bound of Garcia and Voloch for the number of points of a Fermat curve over a prime field. **Finite Fields and Their Applications**, v. 13, n. 4, p. 773–777, 2007. Citation on page 106.

MATTHEWS, G. L. Codes from the Suzuki function field. **IEEE Transactions on Information Theory**, v. 50, n. 12, p. 3298–3302, 2004. Citation on page 122.

MCGUIRE, G.; YILMAZ, E. On the zeta functions of supersingular curves. **Finite Fields and Their Applications**, v. 54, p. 65–79, 2018. Citation on page 125.

MOISIO, M. On the number of rational points on some families of Fermat curves over finite fields. **Finite Fields and Their Applications**, v. 13, n. 3, p. 546–562, 2007. Citation on page 105.

MONTANUCCI, M.; TIMPANELLA, M.; ZINI, G. AG codes and AG quantum codes from cyclic extensions of the Suzuki and Ree curves. **Journal of Geometry**, v. 109, n. 1 (Article 23), 2018. Citation on page 122.

PEDERSEN, J. P.; SØRENSEN, A. B. Codes from certain algebraic function fields with many rational places. **Mat-Report 1990-11, Technical University of Denmark**, 1990. Citations on pages 122, 129, and 130.

SEIDENBERG, A. **Elements of the Theory of Algebraic Curves**. Reading: Addison-Wesley, 1968. Citations on pages 23 and 27.

SKABELUND, D. C. New maximal curves as ray class fields over Deligne-Lusztig curves. **Proceedings of the American Mathematical Society**, v. 146, n. 2, p. 525–540, 2018. Citation on page 122.

STICHTENOTH, H. **Algebraic Function Fields and Codes**. 2. ed. Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg, 2009. Citations on pages 23, 27, 37, 38, 40, and 60.

STICHTENOTH, H.; VOSS, C. Generalized Hamming weights of trace codes. **IEEE Transactions on Information Theory**, v. 40, n. 2, p. 554–558, 1994. No citation.

STÖHR, K.-O.; VOLOCH, J. F. Weierstrass Points and Curves over Finite Fields. **Proceedings of the London Mathematical Society**, s3-52, n. 1, p. 1–19, 1986. Citations on pages 67, 69, 70, 71, 72, 73, 74, 75, 76, 77, and 82.

SZŐNYI, T. Note on the order of magnitude of k for complete k -arcs in $PG(2, q)$. **Discrete Mathematics**, v. 66, n. 3, p. 279–282, 1987. Citation on page 117.

TORRES, F. The approach of Stöhr-Voloch to the Hasse-Weil bound with applications to optimal curves and plane arcs. 2000. Available: <<https://arxiv.org/pdf/math/0011091.pdf>>. Accessed: 29/01/2019. Citations on pages 27, 53, 54, 55, 56, and 67.

van der GEER, G.; van der VLUGT, M. Fibre products of Artin-Schreier curves and generalized hamming weights of codes. **Jornal of Combinatorial Theory, Series A**, v. 70, n. 2, p. 337–348, 1995. No citation.

_____. How to construct curves over finite fields with many points. 1996. Available: <<https://arxiv.org/pdf/alg-geom/9511005.pdf>>. Accessed: 29/01/2019. No citation.

van LINT, J.; WILSON, R. On the minimum distance of cyclic codes. **IEEE Transactions on Information Theory**, v. 32, n. 1, p. 23–40, 1986. Citation on page 81.

VILLEGAS, F. R.; VOLOCH, J. F. On certain plane curves with many integral points. **Experimental Mathematics**, v. 8, n. 1, p. 57–62, 1999. Citations on pages 82 and 84.

VOLOCH, J. F. Jacobians of curves over finite fields. **Rocky Mountain Journal of Mathematics**, v. 30, n. 2, p. 755–759, 2000. Citations on pages 122 and 144.

WEIL, A. **Sur les courbes algébriques et les variétés qui s'en déduisent**. Paris: Hermann, 1948. Citation on page 65.