UNIVERSIDADE DE SÃO PAULO
Instituto de Ciências Matemáticas e de Computação

On Weierstrass points and some properties of curves of Hurwitz type

Grégory Duran Cunha

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

ICMC USP SÃO CARLOS

Grégory Duran Cunha

On Weierstrass points and some properties of curves of Hurwitz type

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
February 2018

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

D948o

Duran Cunha, Grégory
On Weierstrass points and some properties of curves of Hurwitz type / Grégory Duran Cunha; orientador Herivelto Martins Borges Filho. -- São Carlos, 2018.
64 p.

Tese (Doutorado - Programa de Pós-Graduação em Matemática) -- Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, 2018.

1. algebraic curves. 2. finite fields. 3. Weierstrass semigroup. 4. Goppa codes. I. Martins Borges Filho, Herivelto, orient. II. Título.

Bibliotecários responsáveis pela estrutura de catalogação da publicação de acordo com a AACR2:
Gláucia Maria Saia Cristianini - CRB - 8/4938
Juliana de Souza Moraes - CRB - 8/6176

Grégory Duran Cunha

Pontos de Weierstrass e algumas propriedades das curvas do tipo Hurwitz

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

Área de Concentração: Matemática

Orientador: Prof. Dr. Herivelto Martins Borges Filho

USP – São Carlos
Fevereiro de 2018

To God, my mother and friends.

ACKNOWLEDGEMENTS

First of all I thank God Almighty for giving me the knowledge and wisdom for taking up this study.

I am deeply grateful to my advisor Herivelto Borges for the patient guidance, encouragement and valuable suggestions which have contributed greatly to the improvement of the thesis.

I am also very thankful to Professor Gábor Korchmáros for his support, expert advice and inspiration he has provided throughout my time in Italy.

I am specially thankful to my mother for her love and constant encouragement. Her support gives me strength to carry on.

Thank to all my friends and colleagues from ICMC, who made me spend a very nice time in São Carlos. Special thanks to Rafaela, Mariele, Ana Maria, Miriane, Cirilo, Naldo, Joás, Alex, Alexandre, Thiago and many others that I do not list here but kindly ask to not fell forgotten.

Finally, I would like to thank FAPESP (grant 2014/03366-9) for the financial support.

“If I have been able to see further,
it was only because I stood on the shoulders of giants.”
(Isaac Newton)

ABSTRACT

DURAN CUNHA, G. **On Weierstrass points and some properties of curves of Hurwitz type**. 2018. 64 p. Tese (Doutorado em Ciências – Matemática) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2018.

This work presents several results on curves of Hurwitz type, defined over a finite field. In 1961, Tallini investigated plane irreducible curves of minimum degree containing all points of the projective plane $PG(2,q)$ over a finite field of order q. We prove that such curves are $\mathbb{F}_{q^{3(q^2+q+1)}}$-projectively equivalent to the Hurwitz curve of degree $q+2$, and compute some of its Weierstrass points. In addition, we prove that when q is prime the curve is ordinary, that is, the p-rank equals the genus of the curve. We also compute the automorphism group of such curve and show that some of the quotient curves, arising from some special cyclic automorphism groups, are still curves of Hurwitz type. Furthermore, we solve the problem of explicitly describing the set of all Weierstrass pure gaps supported by two or three special points on Hurwitz curves. Finally, we use the latter characterization to construct Goppa codes with good parameters, some of which are current records in the Mint table.

Keywords: algebraic curves, finite fields, Weierstrass semigroup, Goppa codes.

RESUMO

DURAN CUNHA, G. **Pontos de Weierstrass e algumas propriedades das curvas do tipo Hurwitz**. 2018. 64 p. Tese (Doutorado em Ciências – Matemática) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2018.

Este trabalho apresenta vários resultados em curvas do tipo Hurwitz, definidas sobre um corpo finito. Em 1961, Tallini investigou curvas planas irredutíveis de grau mínimo contendo todos os pontos do plano projetivo $PG(2,q)$ sobre um corpo finito de ordem q. Provamos que tais curvas são $\mathbb{F}_{q^{3(q^2+q+1)}}$-projetivamente equivalentes à curva de Hurwitz de grau $q+2$, e calculamos alguns de seus pontos de Weierstrass. Em adição, provamos que, quando q é primo, a curva é ordinária, isto é, o p-rank é igual ao gênero da curva. Também calculamos o grupo de automorfismos desta curva e mostramos que algumas das curvas quocientes, construídas a partir de certos grupos cíclicos de automorfismos, são ainda curvas do tipo Hurwitz. Além disso, solucionamos o problema de descrever explicitamente o conjunto de todos os gaps puros de Weierstrass suportados por dois ou três pontos especiais em curvas de Hurwitz. Finalmente, usamos tal caracterização para construir códigos de Goppa com bons parâmetros, sendo alguns deles recordes na tabela Mint.

Palavras-chave: curvas algébricas, corpos finitos, semigrupo de Weierstrass, códigos de Goppa.

CONTENTS

INTRODUCTION

The study of Weierstrass points is a fascinating topic in the theory of compact Riemann surfaces and algebraic projective curves, rich in geometrical applications and still a prospering area of research. The history of Weierstrass points begins in the early 1860s when Weierstrass stated and proved his Lückensatz (or "gap" theorem). The gap theorem appeared for the first time in the dissertation of Weierstrass' student Schottky in 1875. This theorem was generalized by Noether in 1882. Noether used the existence of Weierstrass points in the study of the geometry of a curve. In (NOETHER, 1882) he gave an algebraic proof (based on elimination theory) of the theorem of Schwarz (SCHWARZ, 1879), according to which the group of automorphisms $\mathrm{Aut}(\mathcal{X})$ of a curve $\mathcal{X}$ of genus $g > 1$ is discrete. One year later in the addendum (NOETHER, 1883), Noether showed that $\mathrm{Aut}(\mathcal{X})$ is actually finite. This theorem is commonly awarded to Schwarz but actually he only proved that $\mathrm{Aut}(\mathcal{X})$ cannot be continuous. It seems that the first proof of the finiteness of $\mathrm{Aut}(\mathcal{X})$ is due to F. Klein (see (POINCARÉ, 1884, p.16)). In 1939 Schmidt (SCHMIDT, 1939) extended, using the Wronskian, the concept of Weierstrass point for curves defined over a field of positive characteristic.

The notion of Weierstrass semigroups at several points was introduced by Arbarello, Cornalba, Griffiths, and Harris (ARBARELLO *et al.*, 1985, p.365). The arithmetical properties involved in the special case of two points was extensively investigated by Kim (KIM, 1994) and Homma (HOMMA, 1996) (see also their joint work (HOMMA; KIM, 2001)). Since these papers were published, many works have arisen mainly pursuing explicit descriptions of Weierstrass semigroups of specific curves in order to be applied in the analysis of algebraic-geometric codes (also known as Goppa codes).

A Goppa code is a general type of linear code constructed by using an algebraic curve over a finite field. Such codes were introduced by Valerii Denisovich Goppa in the early 1980s, see (GOPPA, 1977) and (GOPPA, 1988). After that, much work has been done to better understand these codes and their parameters. Many old codes were found to be algebraic-geometric codes themselves or subsets of Goppa codes (like the BCH-codes and Reed-Solomon codes, for example) thus allowing mathematicians to examine them afresh from an algebraic-geometric point of view. Also, and more importantly, many new codes were discovered whose characteristics were better in certain ways than other "old" codes.

In order to construct Goppa codes with good parameters, it is important the study of Weierstrass semigroups and pure gaps. In fact, Weierstrass pure gaps at several points of a curve have been used to find better bounds on the minimum distances of certain algebraic-geometric

codes. The concept of pure gaps of a pair of points on a curve was initiated by Homma and Kim (HOMMA; KIM, 2001), and it had been pushed forward by Carvalho and Torres (CARVALHO; TORRES, 2005) to several points.

In this thesis, we will obtain several results on curves of Hurwitz type defined over a finite field. For example, the Hurwitz curve of degree $q+2$ is related to the Tallini work (TALLINI, 1961a; TALLINI, 1961b), where he investigated plane irreducible curves of (minimum) degree $q+2$ containing all points of the projective plane $PG(2,q)$ over a finite field of order q. In this direction, we will study these curves from the function field point of view to obtain results related to the Weierstrass semigroup and important invariants such as the Hasse-Witt invariant, via Cartier operator, and the automorphism group. We also consider Hurwitz curves of arbitrary degree in order to give a complete description for the set of all Weierstrass pure gaps supported by two or three special points. Moreover, we will give some applications by constructing Goppa codes with good parameters.

We now give an outline of the content of this thesis:

In Chapter 1, the basic theoretical foundations in algebraic function fields and algebraic curves over finite fields are laid. These ideas will be used throughout the entire work. In this chapter we introduce the basic definitions and results of the theory of algebraic function fields: valuations, places, divisors, Riemann-Roch spaces, Riemann-Roch Theorem, Goppa codes, Weierstrass semigroup, Cartier operator and automorphism group. The results quoted in this chapter are all very well-known and most of the time the reader is referred to standard text books for their proofs.

The topics discussed in Chapter 2 were studied when the author was visiting the Università degli Studi della Basilicata in Italy. A plane irreducible curve defined over a finite field $\mathbb{F}_q$ attaining the the Hasse-Weil bound

$$S_q \leq q+1+(n-1)(n-2)\sqrt{q}$$

where n is the degree of the curve and S_q is the number of its points lying in the projective plane $PG(2,q)$ of order q, is said to be maximal. Any plane (possibly reducible) curve containing all points of $PG(2,q)$ has degree at least $q+1$, and if equality holds then the curve splits into the $q+1$ lines of a pencil in $PG(2,q)$. A complete classification of plane irreducible curves of degree $q+2$ containing all points of $PG(2,q)$ was given by G. Tallini (TALLINI, 1961a; TALLINI, 1961b); see also (ABATANGELO; KORCHMÁROS, 2009), and (HOMMA; KIM, 2013). Up to projective transformations in $PG(2,q)$, each such curve $\mathcal{X}$ has homogeneous equation of type

$$(aX_0+bX_1+cX_2)\varphi_{01}-X_0\varphi_{02}+X_2\varphi_{12}=0,$$

where $\varphi_{ij}=X_i^qX_j-X_iX_j^q$ and a,b,c are elements in $\mathbb{F}_q$ such that the cubic equation

$$X^3-cX^2-aX-b=0$$

is irreducible over $\mathbb{F}_q$. This curve is named *Tallini curve*. Tallini proved that the automorphism group of $\mathcal{X}$ defined over $\mathbb{F}_q$ contains a Singer cycle, that is, a cyclic subgroup S of $PGL(3,q)$ of order q^2+q+1 acting on $PG(2,q)$ as a regular permutation group. In this chapter we go on with the study of the Tallini curves, also from the function field point of view. We look at the Tallini curves in the projective plane $PG(2,K)$ defined over the algebraic closure K of $\mathbb{F}_q$. Our Theorem 2.1.2 shows that up to projective equivalence in $PG(2,K)$, the Tallini curve $\mathcal{X}$ is projectively equivalent to Hurwitz the curve

$$\mathcal{X}_q\colon X_1^{q+1}X_2+X_2^{q+1}X_0+X_0^{q+1}X_1=0.$$

We mention that the curve $\mathcal{X}_q$ was first investigated in (PELLIKAAN, 1998), and we refer to it as the *Pellikaan curve*. From the proof of Theorem 2.1.2, the smallest projective plane $PG(2,q^{3i})$ where this equivalency occurs is in general much larger than $PG(2,q^3)$ as $\mathbb{F}_{q^{3i}}$ turns out to be the smallest overfield of $\mathbb{F}_{q^3}$ containing the roots of the equation $X^{q^2+q+1}=(\alpha^q-\alpha)^{q^2+q-2}$ where α is a root of X^3-cX^2-aX-b. Here i divides q^2+q+1 and the automorphism group of $\mathcal{X}$ in $PG(2,K)$ is isomorphic to $S\rtimes C_3$ where S is defined over $\mathbb{F}_q$ but C_3 is in general defined over $\mathbb{F}_{q^{3i}}$.

For every divisor d of q^2+q+1, the curve $\mathcal{X}_q$ has a quotient curve $\mathcal{X}_q/C_d$ with respect to a cyclic group C_d of order d. In case where q is a square, that is, $q=p^{2i}$ with p prime and $i\geq 1$, the factorization $p^{4i}+p^{2i}+1=(p^{2i}+p^i+1)(p^{2i}-p^i+1)$ raises the question whether the quotient curve $\mathcal{X}_q/C_d$ with $d=p^{2i}-p^i+1$ is isomorphic to $\mathcal{X}_{p^i}$. The answer is affirmative, see Theorem 2.4.3.

We also show that $\mathcal{X}_p$ is an ordinary curve, that is, its genus $g=\frac{1}{2}p(p+1)$ coincides with its Hasse-Witt invariant. For this purpose, we prove that no exact differential of $K(\mathcal{X}_p)$ is regular, and then use the properties of the Cartier operator to show that $\mathcal{X}_p$ is ordinary. It should be noticed that this result does not hold true for $q>p$; see (MONTANUCCI; SPEZIALI, 2016). The results of this chapter have been published in (CUNHA, 2017).

Chapter 3 presents a study of Weierstrass pure gaps on curves of Hurwitz type. We consider a family of non-singular curves

$$\mathcal{X}\colon a_1XY^{n+1}+a_2ZX^{n+1}+a_3YZ^{n+1}+XYZ\cdot G(X,Y,Z)=0,$$

where $a_1,a_2,a_3\in K$ and $a_1a_2a_3\neq 0$. This is a rich family containing the Hurwitz curves and, in particular, many maximal curves. One of them is the famous Klein Quartic

$$X_0X_1^3+X_1X_2^3+X_2X_0^3=0$$

which is $\mathbb{F}_{q^2}$-maximal if and only if $q\equiv 6 \pmod 7$. Its automorphism group is isomorphic to $PSL(2,7)$. In characteristic 0, the Klein quartic has maximum number of automorphisms for curves of genus 3 as the Riemann-Hurwitz formula shows that the number of automorphisms, of curves of genus $g>1$, is at most $84(g-1)$. Another curve included in this family is the Pellikaan curve studied in Chapter 2 as it is isomorphic to the Tallini curve.

In section 3.1, we investigate the set $G_0(\mathcal{P}_1,\mathcal{P}_2)$ of Weierstrass pure gaps of $\mathcal{X}$ at $(\mathcal{P}_1,\mathcal{P}_2)$ where $\mathcal{P}_1$ and $\mathcal{P}_2$ are the places associated to the infinity points $(1:0:0)$ and $(0:1:0)$, respectively. The methods used in this section are based on Homma and Kim results (HOMMA; KIM, 2001). Let g be the genus of $\mathcal{X}$ and $G(\mathcal{P}_1)=\{n_1,\ldots,n_g\}$, $G(\mathcal{P}_2)=\{m_1,\ldots,m_g\}$. They proved that the set of all pure gaps at $(\mathcal{P}_1,\mathcal{P}_2)$ is given by the pair $(n_i,m_{\sigma(j)})$ with $i<j$ and $\sigma(i)>\sigma(j)$, where σ is the permutation of $\{1,\ldots,g\}$ induced by the bijection

$$\begin{aligned}\beta : G(\mathcal{P}_1) &\to G(\mathcal{P}_2)\\ n_i &\mapsto m_{\sigma(i)}=\min\{t:\ (n_i,t)\in H(\mathcal{P}_1,\mathcal{P}_2)\}.\end{aligned}$$

Considering the curve $\mathcal{X}$, we proved that β permutes the elements of $G(\mathcal{P}_1)=G(\mathcal{P}_2)$ in the following way:

$$\begin{array}{ccccc} 1 & 2 & 3 & \cdots & n \\ & n+2 & n+3 & \cdots & 2n \\ & & 2n+3 & \cdots & 3n \\ & & & \ddots & \vdots \\ & & & & n^2 \end{array} \xrightarrow{\beta} \begin{array}{ccccc} n^2 & \cdots & 2n+3 & n+2 & 1 \\ & \ddots & \vdots & n+3 & 2 \\ & & 3n & \vdots & 3 \\ & & & 2n & \vdots \\ & & & & n \end{array}.$$

This allowed us to prove the main result of the section, where we explicitly characterize the set $G_0(\mathcal{P}_1,\mathcal{P}_2)$ (see Theorem 3.1.6). After this characterization, it is natural to consider the problem of explicitly describing the set of all Weierstrass pure gaps of $\mathcal{X}$ supported by $(\mathcal{P}_1,\mathcal{P}_2,\mathcal{P}_3)$, where $\mathcal{P}_3$ is the place associated to $(0:0:1)$. We do that in section 3.2, see Theorem 3.2.8. In section 3.3, we use the characterizations of $G_0(\mathcal{P}_1,\mathcal{P}_2)$ and $G_0(\mathcal{P}_1,\mathcal{P}_2,\mathcal{P}_3)$ to construct Goppa codes with good parameters, some of which are current records in the Mint table.

CHAPTER

1

PRELIMINARIES AND BASIC RESULTS

In this beginning chapter, we shall collect most of the needed background in algebraic function field theory and algebraic curves. For a more comprehensive approach we refer the reader to (STICHTENOTH, 2008).

1.1 Places and divisors of a function field

An algebraic function field F/k of one variable over a field k is an extension field $k \subset F$ such that F is a finite extension of $k(x)$ for some transcendent element $x \in F$ over k. For brevity, we shall simply refer to F/k as a function field.

Any function field F/k can be represented as a simple algebraic field extension of a rational function field $k(x)$, that is, $F = k(x,y)$ where $p(y) = 0$ for some irreducible polynomial $p(t) \in k(x)[t]$. Therefore, we can associate each function field F/k to the irreducible curve $p(x,y) = 0$ defined over k. This defines a biunivocal correspondence between function fields F/k and irreducible curves $p(x,y) = 0$ defined over k.

Definition 1.1.1. A valuation ring of the function field F/k is a ring $\mathcal{O} \subset F$ with the following properties:

(1) $k \subsetneq \mathcal{O} \subsetneq F$, and

(2) for any $z \in F$, we have $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.

From commutative algebra we know that a valuation ring $\mathcal{O}$ is a local ring, that is, $\mathcal{O}$ has a unique maximal ideal $\mathcal{P} = \mathcal{O} \setminus \mathcal{O}^*$, where $\mathcal{O}^*$ is the group of units of the ring $\mathcal{O}$.

Definition 1.1.2. A place $\mathcal{P}$ of the function field F/k is the maximal ideal of some valuation ring $\mathcal{O}$ of F/k. Any element $t \in \mathcal{P}$ such that $\mathcal{P} = t\mathcal{O}$ is called a prime element for $\mathcal{P}$ (t is also

called a local parameter or a uniformizing variable). We denote the set of all places of F/k by $\mathbb{P}_F$.

If $\mathcal{O}$ is a valuation ring of F/k and $\mathcal{P}$ is its maximal ideal, then $\mathcal{O}$ is uniquely determined by $\mathcal{P}$, namely $\mathcal{O} = \{z \in F : z^{-1} \notin \mathcal{P}\}$. Hence $\mathcal{O}_\mathcal{P} := \mathcal{O}$ is called the valuation ring of the place $\mathcal{P}$.

Definition 1.1.3. Let $\mathcal{P} \in \mathbb{P}_F$.

(a) $F_\mathcal{P} := \mathcal{O}_\mathcal{P}/\mathcal{P}$ is the residue class field of $\mathcal{P}$. The map $x \mapsto x(\mathcal{P})$ from $\mathcal{O}_\mathcal{P}$ to $F_\mathcal{P}$ is called the residue class map with respect to $\mathcal{P}$.

(b) $\deg\mathcal{P} := [F_\mathcal{P} : k]$ is called the degree of $\mathcal{P}$.

Definition 1.1.4. A discrete valuation of F/k is a function $v : F \to \mathbb{Z} \cup \{\infty\}$ with the following properties:

(1) $v(x) = \infty \iff x = 0$.

(2) $v(xy) = v(x) + v(y)$ for all $x, y \in F$.

(3) $v(x+y) \geq \min\{v(x), v(y)\}$ for all $x, y \in F$.

(4) There exists an element $z \in F$ with $v(z) = 1$.

(5) $v(a) = 0$ for all $0 \neq a \in k$.

Lemma 1.1.5. (STICHTENOTH, 2008, Lemma 1.1.11). Let v be a discrete valuation of F/k and let $x, y \in F$ with $v(x) \neq v(y)$. Then $v(x+y) = \min\{v(x), v(y)\}$.

Definition 1.1.6. To a place $\mathcal{P} \in \mathbb{P}_F$ we associate a discrete valuation $v_\mathcal{P} : F \to \mathbb{Z} \cup \{\infty\}$: Choose a prime element t for $\mathcal{P}$. Then every $0 \neq z \in F$ has a unique representation $z = t^n u$ with $u \in \mathcal{O}_\mathcal{P}^*$ and $n \in \mathbb{Z}$. Define $v_\mathcal{P}(z) := n$ and $v_\mathcal{P}(0) := \infty$.

Definition 1.1.7. (1) The place $\mathcal{P}$ is a zero of $z \in F$ if $v_\mathcal{P}(z) > 0$.

(2) The place $\mathcal{P}$ is a pole of $z \in F$ if $v_\mathcal{P}(z) < 0$.

The set $\tilde{k} := \{z \in F : z \text{ is algebraic over } k\}$ is a subfield of F and it is called the field of constants of F/k. The field $\tilde{k}$ of constants of an algebraic function field F/k is a finite extension field of k, and F can also be regarded as a function field over $\tilde{k}$. Therefore, from here on, we assume that F/k will always denote an algebraic function field of one variable such that k is the full constant field of F/k.

Definition 1.1.8. The divisor group of F/k is defined as the (additively written) free abelian group which is generated by the places of F/k; it is denoted by $\mathrm{Div}(F)$. The elements of $\mathrm{Div}(F)$ are called divisors of F/k. In other words, a divisor is a formal sum

$$D = \sum_{\mathcal{P}\in\mathbb{P}_F} n_{\mathcal{P}}\mathcal{P} \text{ with } n_{\mathcal{P}} \in \mathbb{Z}, \text{ almost all } n_{\mathcal{P}} = 0.$$

The support of D is defined as

$$\mathrm{supp}(D) := \{\mathcal{P} \in \mathbb{P}_F : n_{\mathcal{P}} \neq 0\}.$$

The degree of a divisor is defined by

$$\mathrm{deg}D := \sum_{\mathcal{P}\in\mathbb{P}_F} n_{\mathcal{P}} \cdot \mathrm{deg}\mathcal{P}$$

and we define $v_{\mathcal{P}}(D) := n_{\mathcal{P}}$. A partial ordering on $\mathrm{Div}(F)$ is defined by

$$D_1 \leq D_2 \iff v_{\mathcal{P}}(D_1) \leq v_{\mathcal{P}}(D_2) \text{ for all } \mathcal{P} \in \mathbb{P}_F.$$

A divisor $D \geq 0$ is called positive (or effective).

Definition 1.1.9. Let $0 \neq x \in F$ and denote by Z (resp. N) the set of zeros (resp. poles) of x. Then we define

$$(x)_0 := \sum_{\mathcal{P}\in Z} v_{\mathcal{P}}(x)\mathcal{P}, \text{ the zero divisor of } x,$$

$$(x)_\infty := \sum_{\mathcal{P}\in N} (-v_{\mathcal{P}}(x))\mathcal{P}, \text{ the pole divisor of } x,$$

$$(x) := (x)_0 - (x)_\infty, \text{ the principal divisor of } x.$$

The elements $0 \neq x \in F$ which are constant are characterized by

$$x \in k \iff (x) = 0.$$

Theorem 1.1.10. Any principal divisor has degree zero. More precisely: Let $x \in F \setminus k$, then

$$\deg(x)_0 = \deg(x)_\infty = [F : k(x)].$$

Proof. See Theorem 5.33 and Theorem 5.34 in (HIRSCHFELD; KORCHMÁROS; TORRES, 2008). □

Definition 1.1.11. Two divisors $D, E \in \mathrm{Div}(F)$ are said to be equivalent, written $D \equiv E$, if $D = E + (x)$ for some $x \in F \setminus \{0\}$. This is easily verified to be an equivalence relation.

1.2 Riemann-Roch space

Definition 1.2.1. For a divisor $A \in \mathrm{Div}(F)$ we define the Riemann-Roch space associated to A by

$$\mathcal{L}(A) := \{x \in F : (x) \geq -A\} \cup \{0\}.$$

Lemma 1.2.2. (STICHTENOTH, 2008, Lemma 1.4.6, Lemma 1.4.7). Let $A \in \mathrm{Div}(F)$. Then we have:

(a) $\mathcal{L}(A)$ is a finite dimensional vector space over k.

(b) If A' is a divisor equivalent to A, then $\mathcal{L}(A) \cong \mathcal{L}(A')$ (isomorphic as vector spaces over k).

(c) $\mathcal{L}(0) = k$.

(d) If $A < 0$ then $\mathcal{L}(A) = \{0\}$.

Definition 1.2.3. For $A \in \mathrm{Div}(F)$ the integer $\ell(A) := \dim \mathcal{L}(A)$ is called the dimension of the divisor A.

Proposition 1.2.4. (STICHTENOTH, 2008, Corollary 1.4.12).

(a) Let A, A' be divisors with $A \equiv A'$. Then we have $\ell(A) = \ell(A')$ and $\deg(A) = \deg(A')$.

(b) If $\deg(A) < 0$ then $\ell(A) = 0$.

(c) Let A be a divisor of degree zero. Then A is principal if and only if $\ell(A) = 1$.

Proposition 1.2.5. (STICHTENOTH, 2008, Proposition 1.4.14). There is a constant $\delta \in \mathbb{Z}$ such that for all divisors $A \in \mathrm{Div}(F)$ the following holds:

$$\deg(A) - \ell(A) \leq \delta.$$

The emphasis here lies on the fact that δ is independent of the divisor A; it depends only on the function field F/k.

Definition 1.2.6. The genus g of F/k is defined by

$$g := \max\{\deg(A) - \ell(A) + 1 : A \in \mathrm{Div}(F)\}.$$

Observe that this definition makes sense by Proposition 1.2.5. For $A = 0$, we have $\deg(0) - \ell(0) + 1 = 0$. Hence, the genus of F/k is a non-negative integer.

Definition 1.2.7. For $A \in \mathrm{Div}(F)$ the integer

$$i(A) := \ell(A) - \deg(A) + g - 1$$

is called the index of specialty of A.

Definition 1.2.8. A divisor W is said to be canonical if $\deg(W) = 2g-2$ and $\ell(W) \geq g$.

Theorem 1.2.9 (Riemann-Roch Theorem)**.** (STICHTENOTH, 2008, Theorem 1.5.15). Let W be a canonical divisor of F/k. Then for each divisor $A \in \mathrm{Div}(F)$,

$$\ell(A) = \deg(A) + 1 - g + \ell(W - A).$$

Theorem 1.2.10. (STICHTENOTH, 2008, Theorem 1.5.17). If A is a divisor of F/k with $\deg(A) \geq 2g-1$ then

$$\ell(A) = \deg(A) - g + 1.$$

1.3 Goppa Codes

The theory of error-correcting codes is applied in many situations which have as a common feature that information coming from some source is transmitted over a noisy communication channel to a receiver. Examples are telephone conversations, storage devices like magnetic tape units which feed some stored information to the computer, telegraph, etc.

Let $\mathbb{F}_q$ denote a finite field with q elements. We consider the n-dimensional vector space $\mathbb{F}_q^n$ whose elements are n-tuples $a = (a_1, \ldots, a_m)$ with $a_i \in \mathbb{F}_q$.

Definition 1.3.1. For $a = (a_1, \ldots, a_m)$ and $b = (b_1, \ldots, b_m) \in \mathbb{F}_q^n$ let

$$d(a,b) := \#\{i \colon a_i \neq b_i\}.$$

This function d is called the Hamming distance on $\mathbb{F}_q^n$. The weight of an element $a \in \mathbb{F}_q^n$ is defined as

$$\mathrm{wt}(a) := d(a,0).$$

The Hamming distance is a metric on $\mathbb{F}_q^n$ as one can verify immediately. In particular, the Triangle Inequality $d(a,c) \leq d(a,b) + d(b,c)$ holds for all $a,b,c \in \mathbb{F}_q^n$.

Definition 1.3.2. A code C (over the alphabet $\mathbb{F}_q$) is a linear subspace of $\mathbb{F}_q^n$, the elements of C are called codewords. We call n the length of C and $\dim(C)$ (as $\mathbb{F}_q$-vector space) the dimension of C. An $[n,k]$ code is a code of length n and dimension k.
The minimum distance $d(C)$ of a code $C \neq 0$ is defined as

$$d(C) := \min\{d(a,b) \colon a,b \in C,\ a \neq b\} = \min\{\mathrm{wt}(c) \colon 0 \neq c \in C\}.$$

An $[n,k]$ code with minimum distance d will be referred to as an $[n,k,d]$ code.

A Goppa code is a general type of linear code constructed by using an algebraic curve over a finite field. Such codes were introduced by Valerii Denisovich Goppa in the early 1980s, see (GOPPA, 1977) and (GOPPA, 1988). Many old codes were found to be algebraic-geometric

codes themselves or subsets of Goppa codes (like the BCH-codes and Reed-Solomon codes, for example) thus allowing mathematicians to examine them afresh from an algebraic-geometric point of view. Also, and more importantly, many new codes were discovered whose characteristics were better in certain ways than other "old" codes.

A Goppa code coming from a curve $\mathcal{X}$ of genus g over a finite field $\mathbb{F}_q$ is made from an effective divisor $D = P_1 + \cdots + P_n$ consisting of pairwise distinct $\mathbb{F}_q$-rational points $P_1, \ldots, P_n$ of $\mathcal{X}$ and an $\mathbb{F}_q$-rational divisor F with the support of F being disjoint from that of D. There are two ways of making a code from D and F; one is the so-called L-construction using the function module $\mathcal{L}(F)$ over $\mathbb{F}_q$ and the other is the Ω-construction using the differential module $\Omega(F-D)$ over $\mathbb{F}_q$; and the two codes made from the pair (D,F) are dual to each other. Then we define the Goppa code $C_\Omega(D,F) \subset \mathbb{F}_q^n$ as the image of the $\mathbb{F}_q$-linear map $\Omega(F-D) \to \mathbb{F}_q^n$ defined by

$$\omega \mapsto (\mathrm{res}_{P_1}(\omega), \ldots, \mathrm{res}_{P_n}(\omega)),$$

where $\mathrm{res}_{P_i}(\omega)$ is the residue of ω at P_i.

Theorem 1.3.3. (STICHTENOTH, 2008, Theorem 2.2.7). $C_\Omega(D,F)$ is an $[n,k,d]$ code with parameters

$$k = i(G-D) - i(G) \text{ and } d \geq \deg(F) - (2g-2).$$

1.4 Weierstrass semigroup

The theory of Weierstrass points arose in the 19th century to Riemann surfaces and in the 1930s it was generalized to curves defined over fields of any characteristic. This theory has contributed to the development of many areas, theoretical and applied. After the construction of linear error-correcting codes through algebraic geometric tools by Goppa, the Weierstrass semigroups have played a crucial role in the study of these combinatorial objects.

Definition 1.4.1. Let $\mathcal{P} \in \mathbb{P}_F$. An integer $n \geq 0$ is called a pole number at $\mathcal{P}$ if there is an element $x \in F$ with $(x)_\infty = n\mathcal{P}$. Otherwise n is called a gap number at $\mathcal{P}$. The set of gap numbers at $\mathcal{P}$ is denoted by $G(\mathcal{P})$.

Proposition 1.4.2. (STICHTENOTH, 2008, Proposition 1.6.6). Let $\mathcal{P} \in \mathbb{P}_F$. Then each $n \geq 2g$ is a pole number at $\mathcal{P}$.

The set of pole numbers at $\mathcal{P}$ is a sub-semigroup of the additive semigroup $\mathbb{N}$, called the Weierstrass semigroup of F/k at $\mathcal{P}$ and denoted by $H(\mathcal{P})$ (to see this note that, if $(x_1)_\infty = n_1\mathcal{P}$ and $(x_2)_\infty = n_2\mathcal{P}$ then x_1x_2 has the pole divisor $(x_1x_2)_\infty = (n_1+n_2)\mathcal{P}$).

Theorem 1.4.3 (Weierstrass Gap Theorem)**.** (STICHTENOTH, 2008, Theorem 1.6.8). Suppose that F/k has genus $g > 0$ and $\mathcal{P}$ is a place of degree one. Then there are exactly g gap numbers $i_1 < \cdots < i_g$ at $\mathcal{P}$. We have

$$i_1 = 1 \text{ and } i_g \leq 2g-1.$$

Remark 1.4.4. Suppose that k is algebraically closed. Then one can show that almost all places of F/k have the same sequence of gap numbers (which are therefore called the gap numbers of the function field F/k). Such places of F/k are said to be ordinary places. Every non-ordinary place is called a Weierstrass point of F/k. If the genus of F/k is ≥ 2, there exists at least one Weierstrass point, see (HIRSCHFELD; KORCHMÁROS; TORRES, 2008).

Let $\mathcal{X}$ be a projective, geometrically irreducible, non-singular algebraic curve defined over a perfect field $\mathbb{F}$. Given m $\mathbb{F}$-rational places $\mathcal{P}_1,\ldots,\mathcal{P}_m$ of $\mathcal{X}$, we define the Weierstrass semigroup at $(\mathcal{P}_1,\ldots,\mathcal{P}_m)$ by

$$H(\mathcal{P}_1,\ldots,\mathcal{P}_m)=\{(x_1,\ldots,x_m)\in\mathbb{N}_0^m:\ \exists f\in\mathbb{F}(\mathcal{X}) \text{ with } (f)_\infty = x_1\mathcal{P}_1+\cdots+x_m\mathcal{P}_m\},$$

where $\mathbb{N}_0$ denotes the set of nonnegative integers.

Lemma 1.4.5. (CARVALHO; TORRES, 2005, Lemma 2.2). Let $(x_1,\ldots,x_m)\in\mathbb{N}_0^m$, and suppose that $\#\mathbb{F}\geq m$. Then $(x_1,\ldots,x_m)\in H(\mathcal{P}_1,\ldots,\mathcal{P}_m)$ if and only if

$$\ell\left(\sum_{i=1}^m x_i\mathcal{P}_i\right)=\ell\left(\sum_{i=1}^m x_i\mathcal{P}_i-\mathcal{P}_j\right)+1,$$

for all $j\in\{1,\ldots,m\}$.

The elements of the complement $G(\mathcal{P}_1,\ldots,\mathcal{P}_m):=\mathbb{N}_0^m\setminus H(\mathcal{P}_1,\ldots,\mathcal{P}_m)$ will be called Weierstrass gaps at $(\mathcal{P}_1,\ldots,\mathcal{P}_m)$.

Observe that $G(\mathcal{P}_1,\ldots,\mathcal{P}_m)$ is a finite set and if $\#\mathbb{F}\geq m$ then $(x_1,\ldots,x_m)$ is a Weierstrass gap at $(\mathcal{P}_1,\ldots,\mathcal{P}_m)$ if and only if

$$\ell\left(\sum_{i=1}^m x_i\mathcal{P}_i\right)=\ell\left(\sum_{i=1}^m x_i\mathcal{P}_i-\mathcal{P}_j\right),$$

for some $j\in\{1,\ldots,m\}$.

Definition 1.4.6. We say that $(x_1,\ldots,x_m)\in\mathbb{N}_0^m$ is a pure gap at $(\mathcal{P}_1,\ldots,\mathcal{P}_m)$ if

$$\ell\left(\sum_{i=1}^m x_i\mathcal{P}_i\right)=\ell\left(\sum_{i=1}^m x_i\mathcal{P}_i-\mathcal{P}_j\right),$$

for all $j\in\{1,\ldots,m\}$. We denote the set of all pure gaps by $G_0(\mathcal{P}_1,\ldots,\mathcal{P}_m)$.

For $x=(x_1,\ldots,x_m)\in\mathbb{N}_0^m$ and $i\in\{1,\ldots,m\}$, we set

$$\nabla_i^m(x):=\{(y_1,\ldots,y_m)\in H(\mathcal{P}_1,\ldots,\mathcal{P}_m):\ y_i=x_i \text{ and } y_j\leq x_j\ \forall j\neq i\}.$$

The following result was proved by Carvalho and Torres in (CARVALHO; TORRES, 2005, Lemma 2.5).

Theorem 1.4.7. Let $x = (x_1, \ldots, x_m) \in \mathbb{N}_0^m$ and suppose that $\#\mathbb{F} \geq m$. Then the following statements are equivalent:

(1) $x \in G_0(\mathcal{P}_1, \ldots, \mathcal{P}_m)$;

(2) $\nabla_i^m(x) = \emptyset$ for all $i = 1, \ldots, m$;

(3) $\ell(\sum_{i=1}^m x_i \mathcal{P}_i) = \ell(\sum_{i=1}^m (x_i - 1)\mathcal{P}_i)$.

Corollary 1.4.8. (CARVALHO; TORRES, 2005, Corollary 2.6). Assume that $\#\mathbb{F} \geq m$.

(1) If $(x_1, \ldots, x_m) \in G_0(\mathcal{P}_1, \ldots, \mathcal{P}_m)$ then $x_i \in G(\mathcal{P}_i)$ for each $i = 1, \ldots, m$;

(2) If $(1, \ldots, 1) \in H(\mathcal{P}_1, \ldots, \mathcal{P}_m)$ then $G_0(\mathcal{P}_1, \ldots, \mathcal{P}_m) = \emptyset$.

1.5 Cartier operator

The relevant geometric properties of a (projective, geometrically irreducible, algebraic) curve defined over an algebraically closed field K of characteristic $p > 0$ are encoded in its birational invariants, the most important being the genus, the automorphism group, and the p-rank. The p-rank (also called the Hasse-Witt invariant) can be seen as the dimension of the span of the vectors in the space of holomorphic differentials that are fixed under the action of an $1/p$-linear map, called the Cartier operator. Computing the p-rank of a curve may be a rather challenging task.

Here we give some definitions and basics results on Cartier operator. For more detail see (HIRSCHFELD; KORCHMÁROS; TORRES, 2008).

Let $\Sigma = K(\mathcal{X})$ be the function field of a curve $\mathcal{X}$ of genus $\mathfrak{g}$ defined over an algebraically closed field K of positive characteristic p. Let x be a separable variable of Σ, that is, $x \in \Sigma \setminus \Sigma^p$. Any function $f \in \Sigma$ can be written uniquely in the form

$$f = u_0^p + u_1^p x + \cdots + u_{p-1}^p x^{p-1},$$

where $u_i \in \Sigma$, for $0 \leq i \leq p-1$. Let $\Delta_\Sigma = \{udx \mid u \in \Sigma\}$ be the differential module of Σ. The Cartier operator $C : \Delta_\Sigma \to \Delta_\Sigma$ is a $1/p$-linear map defined by

$$C(fdx) = u_{p-1}dx.$$

Some fundamental properties of the Cartier operator are the following:

(i) $C(fdx)$ is independent of the choice of x;

(ii) $C(y_1^p w_1 + y_2^p w_2) = y_1 C(w_1) + y_2 C(w_2)$, for $y_1, y_2 \in \Sigma$ and $w_1, w_2 \in \Delta_\Sigma$;

(iii) if $w \in \Delta_\Sigma$ is holomorphic, that is, the divisor (w) is effective, then $C(w)$ is also holomorphic;

(iv) $C(w) = 0$ if and only if w is exact, that is, $w = df$ for some $f \in \Sigma$;

(v) $C(w) = w$ if and only if w is logarithmic, that is, $w = df/f$ for $f \neq 0$ in Σ.

The space $\Delta_\Sigma^{(1)}$ of holomorphic differentials is a $\mathfrak{g}$-dimensional K-vector subspace of Δ_Σ such that $C(\Delta_\Sigma^{(1)}) \subset \Delta_\Sigma^{(1)}$.

Let Δ^s be the subspace of $\Delta_\Sigma^{(1)}$ spanned by the holomorphic logarithmic differentials and let Δ^0 be the subspace of $\Delta_\Sigma^{(1)}$ formed by differentials w such that there exists $n \in \mathbb{N}$ such that $C^n(w) = 0$. From a result by Hasse and Witt, $\Delta_\Sigma^{(1)} = \Delta^s \oplus \Delta^0$; see (HASSE; WITT, 1936).

The dimension of Δ^s is the Hasse-Witt invariant of $\mathcal{X}$ and it is equal to the p-rank γ of $\mathcal{X}$.

Let $\mathcal{B} = \{w_1, \ldots, w_\mathfrak{g}\}$ be a basis for $\Delta_\Sigma^{(1)}$. The representation matrix (h_{ij}) over K of C is the Hasse-Witt matrix of $\mathcal{X}$. Since C is a $1/p$-linear map, the operator C^n is represented with respect to $\mathcal{B}$ by the matrix

$$(h_{ij})(h_{ij}^p)\cdots(h_{ij}^{p^{n-1}})$$

and the p-rank of $\mathcal{X}$ coincides with the rank of the matrix

$$(h_{ij})(h_{ij}^p)\cdots(h_{ij}^{p^{\mathfrak{g}-1}}).$$

Theorem 1.5.1. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 6.96) The p-rank is less than or equal to the genus $\mathfrak{g}$.

When the p-rank of $\mathcal{X}$ equals $\mathfrak{g}$, then $\mathcal{X}$ is said to be an ordinary curve.

1.6 Automorphism group of a curve

The automorphism group of an algebraic curve is one of its most important invariants. Such a group is finite, except for rational and elliptic curves. It has been known for a long time that for any ground field K and any finite group G, there exists an algebraic curve $\mathcal{X}$ such that $\mathrm{Aut}(\mathcal{X}) \cong G$. The construction and classification of curves with large automorphism groups with respect to their genus has been considered a relevant problem in algebraic geometry.

Let $\mathcal{X}$ be a (projective, geometrically irreducible, non-singular) algebraic curve defined over an algebraically closed field K of characteristic $p \geq 0$. Let $K(\mathcal{X})$ be the function field of $\mathcal{X}$. The K-automorphism group $\mathrm{Aut}(\mathcal{X})$ of $\mathcal{X}$ is defined to be the automorphism group consisting of those automorphisms of $K(\mathcal{X})$ which fix each element of K. $\mathrm{Aut}(\mathcal{X})$ has a faithful action on the set of points of $\mathcal{X}$.

For a finite subgroup G of $\mathrm{Aut}(\mathcal{X})$ the subfield $K(\mathcal{X})^G$ consisting of all elements of $K(\mathcal{X})$ fixed by every element in G, also has transcendency degree one over K. Let $\mathcal{Y}$ be a non-singular

model of $K(\mathcal{X})^G$, that is, a projective, non-singular, geometrically irreducible, algebraic curve with function field $K(\mathcal{X})^G$. We call $\mathcal{Y}$ the quotient curve of $\mathcal{X}$ by G and it is denoted by $\mathcal{X}/G$.

Definition 1.6.1. Let G be a subgroup of $\mathrm{Aut}(\mathcal{X})$. If P is a point of $\mathcal{X}$, the stabilizer G_P of P in G is the subgroup of G consisting of all elements fixing P. The orbit

$$\mathcal{O}_G(P) := \{\alpha(P) \colon \alpha \in G\}$$

is long if $|\mathcal{O}_G(P)| = |G|$, otherwise $\mathcal{O}_G(P)$ is short. In the latter case G is said to ramify at P.

Theorem 1.6.2 (Riemann-Hurwitz)**.** (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 11.57). Let G be a finite K-automorphism group of an irreducible curve $\mathcal{F}$. If $|G_P|$ is prime to p for every place P of $K(\mathcal{F})$, then

$$2g-2 = n(2g'-2) + \sum_{i=1}^{s}(n-l_i),$$

where $n = |G|$, g and g' are the genus of $\mathcal{F}$ and its quotient curve $\mathcal{F}/G$, while $l_1,\ldots,l_s$ denote the sizes of the short orbits of G.

Theorem 1.6.3 (Deuring-Shafarevich)**.** (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 11.62). Let G be K-automorphism group of an irreducible curve $\mathcal{F}$ whose order n is a power of p. then

$$\gamma-1 = n(\gamma'-1) + \sum_{i=1}^{s}(n-l_i),$$

where γ and γ' are the p-ranks of $\mathcal{F}$ and its quotient curve $\mathcal{F}/G$, while $l_1,\ldots,l_s$ denote the sizes of the short orbits of G on the places of $K(\mathcal{F})$.

CHAPTER

2

CURVES CONTAINING ALL POINTS OF A FINITE PROJECTIVE GALOIS PLANE

A fundamental result on plane irreducible (algebraic) curves defined over a finite field $\mathbb{F}_q$ is the Hasse-Weil bound

$$S_q \leq q+1+(n-1)(n-2)\sqrt{q}$$

where n is the degree of the curve and S_q is the number of its points lying in the projective plane $PG(2,q)$ of order q; see (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Section 9.6). Any plane (possibly reducible) curve containing all points of $PG(2,q)$ has degree at least $q+1$, and if equality holds then the curve splits into the $q+1$ lines of a pencil in $PG(2,q)$. A complete classification of plane irreducible curves of degree $q+2$ containing all points of $PG(2,q)$ was given by G. Tallini (TALLINI, 1961b; TALLINI, 1961a); see also (ABATANGELO; KORCHMÁROS, 2009), and (HOMMA; KIM, 2013). Up to projective transformations in $PG(2,q)$, each such curve $\mathcal{X}$ has homogeneous equation of type

$$(aX_0+bX_1+cX_2)\varphi_{01}-X_0\varphi_{02}+X_2\varphi_{12}=0, \tag{2.1}$$

where $\varphi_{ij}=X_i^qX_j-X_iX_j^q$ and a,b,c are elements in $\mathbb{F}_q$ such that the cubic equation

$$X^3-cX^2-aX-b=0 \tag{2.2}$$

is irreducible over $\mathbb{F}_q$. The above irreducible curve $\mathcal{X}$ of degree $n=q+2$ is named *Tallini curve*.

G. Tallini proved that $\mathcal{X}$ has no singular points in $PG(2,q)$. Homma and Kim (HOMMA; KIM, 2013, Section 3) extended his result to any point in $PG(2,K)$ where K is the algebraic closure of $\mathbb{F}_q$. Therefore, $\mathcal{X}$ is a plane nonsingular curve of genus $\mathfrak{g}=\frac{1}{2}(n-1)(n-2)=\frac{1}{2}q(q+1)$.

G. Tallini showed that the automorphism group G_q of $\mathcal{X}$ over $\mathbb{F}_q$ contains a Singer cycle, that is, a cyclic subgroup S of $PGL(3,q)$ of order q^2+q+1 acting on $PG(2,q)$ as a regular

permutation group. He also claimed that G_q may be a bit larger but only for some special curves, named harmonic and equianharmonic curves in (TALLINI, 1961b; TALLINI, 1961a). More precisely, Homma and Kim proved (HOMMA; KIM, 2013, Theorem 5.4) that if G_q with $q > 2$ is larger than S then G_q is the normalizer of S in $PGL(3,q)$, that is, $G_q = S \rtimes C_3$, the semidirect product of S by a group C_3 of order 3.

In this work we go on with the study of the Tallini curves, mainly from the function field point of view. We look at the Tallini curves in the projective plane $PG(2,K)$ defined over the algebraic closure K of $\mathbb{F}_q$. Our Theorem 2.1.2 shows that up to projective equivalence in $PG(2,K)$, the Tallini curve $\mathcal{X}$ is projectively equivalent to the curve

$$\mathcal{X}_q : X_1^{q+1}X_2 + X_2^{q+1}X_0 + X_0^{q+1}X_1 = 0. \tag{2.3}$$

For $q = 2$, $\mathcal{X}_q$ is the famous plane Klein quartic whose automorphism group is isomorphic to $PSL(2,7)$. We mention that the curve $\mathcal{X}_q$ was first investigated in (PELLIKAAN, 1998), and we refer to it as the *Pellikaan curve*. From the proof of Theorem 2.1.2, the smallest projective plane $PG(2,q^{3i})$ where this equivalency occurs is in general much larger than $PG(2,q^3)$ as $\mathbb{F}_{q^{3i}}$ turns out to be the smallest overfield of $\mathbb{F}_{q^3}$ containing the roots of the equation $X^{q^2+q+1} = (\alpha^q - \alpha)^{q^2+q-2}$ where α is a root of (2.2). Here i divides q^2+q+1 and the automorphism group of $\mathcal{X}$ in $PG(2,K)$ is isomorphic to $S \rtimes C_3$ where S is defined over $\mathbb{F}_q$ but C_3 is in general defined over $\mathbb{F}_{q^{3i}}$.

For every divisor d of q^2+q+1, the curve $\mathcal{X}_q$ has a quotient curve $\mathcal{X}_q/C_d$ with respect to a cyclic group C_d of order d. In case where q is a square, that is, $q = p^{2i}$ with p prime and $i \geq 1$, the factorization $p^{4i} + p^{2i} + 1 = (p^{2i} + p^i + 1)(p^{2i} - p^i + 1)$ raises the question whether the quotient curve $\mathcal{X}_q/C_d$ with $d = p^{2i} - p^i + 1$ is isomorphic to $\mathcal{X}_{p^i}$. The answer is affirmative, see Theorem 2.4.3.

We also show that $\mathcal{X}_p$ is an ordinary curve, that is, its genus $\mathfrak{g} = \frac{1}{2}p(p+1)$ coincides with its Hasse-Witt invariant. For this purpose, we prove that no exact differential of $K(\mathcal{X}_p)$ is regular, and then use the properties of the Cartier operator to show that $\mathcal{X}_p$ is ordinary. It should be noticed that this result does not hold true for $q > p$; see (MONTANUCCI; SPEZIALI, 2016).

Since there are no irreducible plane curves of degree $q+1$ containing all the q^2+q+1 points of $PG(2,q)$, is natural to ask what is the maximum number of points that such a curve can have in $PG(2,q)$. In (HOMMA; KIM, 2009), Homma and Kim proved that a projective plane curve of degree $q+1$ containing no $\mathbb{F}_q$-line as a component has at most q^2+1 points of $PG(2,q)$. This bound is sharp as the nonsingular curve defined by

$$X^{q+1} - X^2Z^{q-1} + Y^qZ - YZ^q = 0 \tag{2.4}$$

over $\mathbb{F}_q$ contains q^2+1 points of $PG(2,q)$. Moreover, they proved that if a plane curve $\mathcal{C}$ over $\mathbb{F}_q$ of degree $q+1$ without an $\mathbb{F}_q$-linear component contains q^2+1 points of $PG(2,q)$ and all the q points of $PG(2,q) \setminus \mathcal{C}$ are collinear, then $\mathcal{C}$ is projectively equivalent to the curve defined by (2.4).

2.1 Irreducible curves of minimal degree containing all points of $PG(2,q)$

Let $\mathcal{X}$ be an irreducible plane curve of degree $q+2$ defined over $\mathbb{F}_q$ containing all points of $PG(2,q)$. In his paper (TALLINI, 1961b), Tallini proved that such a curve exists and it has equation (2.1).

Now, we recall some facts from (TALLINI, 1961b). The polar net of $\mathcal{X}$ is a net of conics and it is easy to see that this net is homaloidal with the three base points, namely $A_0 = (\alpha_0 : 1 : \alpha_0^2)$, $A_1 = (\alpha_1 : 1 : \alpha_1^2)$ and $A_2 = (\alpha_2 : 1 : \alpha_2^2)$ where $\alpha_0, \alpha_1, \alpha_2$ are the three solutions of (2.2) in $\mathbb{F}_{q^3}$. In particular, the points A_0, A_1 and A_2 are conjugate over $\mathbb{F}_{q^3}$. Furthermore, they belong to $\mathcal{X}$ and they are simple points for it. We call each of these three points a base point of $\mathcal{X}$.

Also in (TALLINI, 1961b), Tallini showed that the automorphism group of $\mathcal{X}$ contains a Singer cycle, that is, a cyclic subgroup $S = \langle \phi \rangle$ of $PGL(3,q)$ of order q^2+q+1 acting on $PG(2,q)$ as a regular permutation group. Moreover, S, viewed as a subgroup of $PGL(3,q^3)$, fixes A_0, A_1, A_2.

The following result is claimed in (HOMMA; KIM, 2013) without proof.

Theorem 2.1.1. The curve $\mathcal{X}$ is non-singular.

Proof. If P is a singular point of $\mathcal{X}$ then its orbit under the projetivity ϕ

$$\mathcal{O} = \{\phi^i(P) \mid 0 \leq i \leq q^2+q\}$$

consists of singular points of $\mathcal{X}$. Note that the size of $\mathcal{O}$ is 1 or q^2+q+1. Since the number of singular points of $\mathcal{X}$ is at most $q(q+1)/2$, then $\mathcal{O} = \{P\}$. This yields that every singular point of $\mathcal{X}$ is fixed by S. Since S fixes only A_0, A_1 and A_2, which are simple points, it follows that $\mathcal{X}$ has no singular points. □

Theorem 2.1.2. Any Tallini curve is projectively equivalent to the Pellikaan curve over $\mathbb{F}_{q^{3(q^2+q+1)}}$.

Proof. Let $\alpha_0, \alpha_1, \alpha_2 \in \mathbb{F}_{q^3}$ be the distinct solutions of (2.2), and let $\mathcal{Y}$ be the image of $\mathcal{X}$ under the linear map associated to the non-singular matrix

$$M = \begin{pmatrix} \alpha_0 & \alpha_1 & \alpha_2 \\ 1 & 1 & 1 \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 \end{pmatrix}.$$

That is, $\mathcal{Y}$ is the curve given by $G(X_0, X_1, X_2) = 0$, where

$$G = F\Big(\sum_{i=0}^{2} \alpha_i X_i, \sum_{i=0}^{2} X_i, \sum_{i=0}^{2} \alpha_i^2 X_i\Big), \tag{2.5}$$

and $\mathcal{X} = \mathbf{v}(F)$ is the Tallini curve. A straightforward computation gives

$$G = c_{01}X_0^{q+1}X_1 + c_{02}X_0^{q+1}X_2 + c_{10}X_1^{q+1}X_0 + c_{12}X_1^{q+1}X_2 + c_{20}X_2^{q+1}X_0 + c_{21}X_2^{q+1}X_1,$$

where

$$c_{ij} = (\alpha_i - \alpha_j)^2(\alpha_i^q - \alpha_i)(\alpha_j - \alpha_i^q), \quad \text{for } 0 \le i, j \le 2.$$

Note that $c_{ij} = 0$ whenever $\alpha_j = \alpha_i^q$. Since the Frobenius map acts transitively on $\{\alpha_0, \alpha_1, \alpha_2\}$, it follows that either $(\alpha_0, \alpha_1, \alpha_2) = (\alpha_1^q, \alpha_2^q, \alpha_0^q)$ or $(\alpha_0, \alpha_1, \alpha_2) = (\alpha_2^q, \alpha_0^q, \alpha_1^q)$. In the former case, we have $c_{10} = c_{02} = c_{21} = 0$ and then

$$G = c_{01}X_0^{q+1}X_1 + c_{12}X_1^{q+1}X_2 + c_{20}X_2^{q+1}X_0, \tag{2.6}$$

whereas the latter case gives $c_{01} = c_{12} = c_{20} = 0$ and

$$G = c_{02}X_0^{q+1}X_2 + c_{10}X_1^{q+1}X_0 + c_{21}X_2^{q+1}X_1. \tag{2.7}$$

We prove the result in the case G is given by (2.6), and then case (2.7) will follow analogously. Note that from $(\alpha_0, \alpha_1, \alpha_2) = (\alpha_1^q, \alpha_2^q, \alpha_0^q)$, equation (2.6) can be written as

$$(\alpha_1^q - \alpha_1)X_0^{q+1}X_2 + (\alpha_1^q - \alpha_1)^q X_1^{q+1}X_0 + (\alpha_1 - \alpha_1^{q^2})X_2^{q+1}X_1 = 0. \tag{2.8}$$

Finally, one can easily check that the curve given by (2.8) is the image of $\mathcal{X}_q$ under the transformation

$$(X_0, X_1, X_2) \mapsto (\mu X_0, \lambda X_1, X_2)$$

where $\mu, \lambda \in \mathbb{F}_{q^{3(q^2+q+1)}}$ satisfy

$$\lambda^{q^2+q+1} = \frac{(\alpha_1^q - \alpha_1)^3}{(\alpha_1^q - \alpha_1)^{q^2+q+1}} \text{ and } \mu = \frac{\lambda^{q+1}(\alpha_1^{q^2} - \alpha_1^q)}{\alpha_1 - \alpha_1^{q^2}}.$$

This finishes the proof. □

2.2 Weierstrass semigroup at a base point

Let $\Sigma = K(x, y)$, with $xy^{q+1} + x^{q+1} + y = 0$, be the function field of the Pellikaan curve $\mathcal{X}_q$ and consider the fundamental triangle

$$O = (0:0:1),\ X_\infty = (1:0:0),\ Y_\infty = (0:1:0).$$

The tangent lines to $\mathcal{X}_q$ at O, X_∞ and Y_∞ are $l_Y = \mathbf{v}(Y)$, $l_Z = \mathbf{v}(Z)$ and $l_X = \mathbf{v}(X)$, respectively. Note that the points in $l_Y \cap \mathcal{X}_q$ are O and X_∞ with

$$I(O, l_Y \cap \mathcal{X}_q) = q + 1 \text{ and } I(X_\infty, l_Y \cap \mathcal{X}_q) = 1,$$

the points in the intersection $l_Z \cap \mathcal{X}_q$ are X_∞ and Y_∞ with

$$I(X_\infty, l_Z \cap \mathcal{X}_q) = q+1 \text{ and } I(Y_\infty, l_Z \cap \mathcal{X}_q) = 1,$$

and the points in the intersection $l_X \cap \mathcal{X}_q$ are Y_∞ and O with

$$I(Y_\infty, l_X \cap \mathcal{X}_q) = q+1 \text{ and } I(O, l_X \cap \mathcal{X}_q) = 1.$$

From (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 6.42) the principal divisor of x is given by

$$\begin{aligned}(x) &= l_X \cdot \mathcal{X}_q - l_Z \cdot \mathcal{X}_q \\ &= I(O, l_X \cap \mathcal{X}_q)O + I(Y_\infty, l_X \cap \mathcal{X}_q)Y_\infty - I(X_\infty, l_Z \cap \mathcal{X}_q)X_\infty - I(Y_\infty, l_Z \cap \mathcal{X}_q)Y_\infty \\ &= O + (q+1)Y_\infty - (q+1)X_\infty - Y_\infty \\ &= O + qY_\infty - (q+1)X_\infty\end{aligned}$$

and the principal divisor of y is given by

$$\begin{aligned}(y) &= l_Y \cdot \mathcal{X}_q - l_Z \cdot \mathcal{X}_q \\ &= I(O, l_Y \cap \mathcal{X}_q)O + I(X_\infty, l_Y \cap \mathcal{X}_q)X_\infty - I(X_\infty, l_Z \cap \mathcal{X}_q)X_\infty - I(Y_\infty, l_Z \cap \mathcal{X}_q)Y_\infty \\ &= (q+1)O + X_\infty - (q+1)X_\infty - Y_\infty \\ &= (q+1)O - qX_\infty - Y_\infty.\end{aligned}$$

For $1 \leq n \leq q+1$, the above relations give

$$\left(\frac{y}{x^n}\right) = (q+1-n)O + (n(q+1)-q)X_\infty - (nq+1)Y_\infty,$$

hence the divisor of poles of y/x^n is

$$\left(\frac{y}{x^n}\right)_\infty = (nq+1)Y_\infty, \quad \text{for } 1 \leq n \leq q+1.$$

Theorem 2.2.1. The Weierstrass semigroup at a base point of $\mathcal{X}_q$ is the semigroup generated by $q+1, 2q+1, \ldots, (q+1)q+1$.

Proof. We may assume that the base point is Y_∞. From the above discussion, the numbers

$$q+1, 2q+1, \ldots, (q+1)q+1$$

belong to the Weierstrass semigroup $H(Y_\infty)$. Let $H := \langle q+1, 2q+1, \ldots, (q+1)q+1 \rangle$ be the semigroup generated by $q+1, 2q+1, \ldots, (q+1)q+1$. Since $H \subset H(Y_\infty)$ and the number of gaps in H is $q(q+1)/2$, which is the number of gaps in $H(Y_\infty)$, the assertion follows. □

Theorem 2.2.2. If the function field of $\mathcal{X}_q$ is given by $K(x,y)$, with $xy^{q+1} + x^{q+1} + y = 0$, then the divisor of the differential dx is

$$(dx) = (q^2+2q)Y_\infty - (q+2)X_\infty.$$

Proof. The curve $\mathcal{X}_q$ is constituted by two points in the infinity X_∞, Y_∞ and the affine points $P=(a:b:1)$, with $ab^{q+1}+a^{q+1}+b=0$. The tangent line to $\mathcal{X}_q$ at an affine point $P=(a,b)$ is not vertical, in fact, suppose by contradiction that $X=0$ is the tangent to $\mathcal{X}_q=\mathbf{v}(F)$ at P. Then $\frac{\partial F}{\partial Y}=0$ in the point $P=(a,b)$. It means that $ab^q+1=0$ and hence $a\neq 0$. On the other hand, $ab^{q+1}+a^{q+1}+b=0$ becomes $-b+a^{q+1}+b=0$, and therefore $a=0$, a contradiction. Thus, a primitive parametrization of $\mathcal{X}_q$ at P is given by

$$x(t)=a+t,$$

$$y(t)=b_0+b_1t+\cdots,\ \ b_0=b.$$

Therefore, $\mathrm{ord}_P dx=0$, for all affine point P in $\mathcal{X}_q$. So it follows that $(dx)=nX_\infty+mY_\infty$ with $n+m=2g-2$, where $g=q(q+1)/2$ is the genus of the curve $\mathcal{X}_q$. Since $(x)=qY_\infty+O-(q+1)X_\infty$ and $q+1$ is not divisible by p, $\mathrm{ord}_{X_\infty}dx=-(q+2)$, that is, $n=-(q+2)$. From $n+m=2g-2$ it follows that $m=q^2+2q$. □

2.3 The automorphism group

Again, let $K(\mathcal{X}_q)=K(x,y)$, with $xy^{q+1}+x^{q+1}+y=0$, be the function field of the Pellikaan curve $\mathcal{X}_q$ and let $\lambda\in K$ be a primitive (q^2+q+1)-root of unity and define the linear collineations

$$\sigma:(X_0,X_1,X_2)\mapsto(X_0,\lambda X_1,\lambda^{q+1}X_2).$$

and

$$\tau:(X_0,X_1,X_2)\mapsto(X_2,X_0,X_1).$$

It is straightforward to see that the automorphism group of $\mathcal{X}_q$ in $PG(2,K)$ contains $S\rtimes C_3$ as a subgroup, where $S=\langle\sigma\rangle$ and $C_3=\langle\tau\rangle$.

Observe that S has order q^2+q+1. Therefore, going back to the original equation (2.1) of $\mathcal{X}$, S becomes a Singer cycle of $PG(2,q)$.

To show that $S\rtimes C_3$ is actually the whole automorphism group of $\mathcal{X}_q$ over K, we need some lemmas.

Lemma 2.3.1. If Q is a point in $\mathcal{X}_q$ and t_Q is its tangent line, then

$$I(Q,\mathcal{X}_q\cap t_Q)=\begin{cases} q+1, & \text{if} \quad Q\in\{X_\infty,Y_\infty,O\}\\ 2, & \text{if} \quad Q\notin\{X_\infty,Y_\infty,O\}.\end{cases}$$

Proof. We have this result for the points in the fundamental triangle, see section 3. Suppose $Q=(a,b)$ with $ab^{q+1}+a^{q+1}+b=0$ and $ab\neq 0$. The tangent line t_Q to $\mathcal{X}_q$ at Q is given by

$$T(X,Y)=\frac{b}{a}X+\frac{a^{q+1}}{b}Y+ab^{q+1}=0.$$

A primitive parametrization of $\mathcal{X}_q$ at Q is given by

$$x(t) = a + t$$

$$y(t) = b - \frac{b^2}{a^{q+2}}t - \frac{b^{q+3}}{a^{2q+3}}t^2 - \frac{b^{2q+4}}{a^{3q+4}}t^3 - \cdots.$$

Therefore $T(x(t), y(t)) = -(b/a)^{q+2}t^2 + \cdots$ has order 2, that is, $I(Q, \mathcal{X}_q \cap t_Q) = 2$. □

Lemma 2.3.2. Every automorphism in $\mathrm{Aut}(\mathcal{X}_q)$ preserves the triangle $\{X_\infty, Y_\infty, O\}$.

Proof. Let $\alpha \in \mathrm{Aut}(\mathcal{X}_q)$ and suppose $\alpha : P \mapsto Q$ with $P \in \{X_\infty, Y_\infty, O\}$ and $Q \notin \{X_\infty, Y_\infty, O\}$. Consider the lines t_Q and l_Q given by

$$t_Q : \ T(X,Y) = 0$$

$$l_Q : \ L(X,Y) = 0$$

such that t_Q is the tangent line to $\mathcal{X}_q$ at Q and l_Q is a secant line through Q. Consider the curve $\mathcal{C}$ of degree $q-1$ given by

$$T(X,Y)L(X,Y)^{q-2} = 0.$$

By the Lemma 2.3.1,

$$I(Q, \mathcal{X}_q \cap \mathcal{C}) = I(Q, \mathcal{X}_q \cap t_Q) + (q-2)I(Q, \mathcal{X}_q \cap l_Q) = 2 + (q-2) = q.$$

Observe that $W := \mathcal{X}_q \cdot \mathcal{C}$ is a canonical divisor such that $\mathcal{L}(W - qQ) \neq \mathcal{L}(W - (q+1)Q)$. Thus, by Riemann-Roch Theorem, $\ell((q+1)Q) = \ell(qQ)$. Hence $q+1$ is a gap number at Q, but this is a contradiction as $q+1$ is a non-gap at P. □

Theorem 2.3.3. $\mathrm{Aut}(\mathcal{X}_q) = S \rtimes C_3$.

Proof. Let $\alpha \in \mathrm{Aut}(\mathcal{X}_q)$. Since $\mathcal{X}_q$ is non-singular, α can be represented as a matrix A in $PGL(3,K)$. By the Lemma 2.3.2, α preserves the fundamental triangle. First, suppose that α fixes all vertices of the fundamental triangle, then

$$A = \begin{pmatrix} \xi & 0 & 0 \\ 0 & \eta & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Since α preserves $\mathcal{X}_q$,

$$\xi\eta^{q+1}xy^{q+1} + \xi^{q+1}x^{q+1} + \eta y = 0$$

in $K(\mathcal{X}_q) = K(x,y)$. Hence $\eta = \xi^{q+1}$ and $\xi^{q^2+q+1} = 1$. Therefore $\alpha \in S$. Now, suppose that α fixes no vertices of the fundamental triangle. In that case, $\alpha = \tau$ or $\alpha = \tau^2$. To complete the

proof we only need to show that the case when α fixes only one point in the fundamental triangle does not happen. Suppose that α only fixes the origin, thus α interchanges X_∞ and Y_∞. Hence,

$$A = \begin{pmatrix} 0 & \xi & 0 \\ \eta & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

where $\xi, \eta \in K$. Since α preserves $\mathcal{X}_q$,

$$\xi\eta^{q+1}yx^{q+1} + \xi^{q+1}y^{q+1} + \eta x = 0$$

in $K(x,y)$. It means that, there exists $c \neq 0$ in K such that

$$\xi\eta^{q+1}YX^{q+1} + \xi^{q+1}Y^{q+1} + \eta X = c(XY^{q+1} + X^{q+1} + Y),$$

which is a contradiction. The cases when α fixes only X_∞ or Y_∞ are analogues. □

Theorems 2.3.3 and 2.1.2 have the following corollary.

Corollary 2.3.4. The automorphism group of $\mathcal{X}$ is $S \rtimes C_3$, where S is defined over $\mathbb{F}_q$ but C_3 is defined over $\mathbb{F}_{q^i}$ with $i = 3(q^2+q+1)$.

2.4 Quotient curve

Suppose that q is a square, say $q = p^{2i}$, $i \geq 1$. Thus

$$q^2 + q + 1 = (p^{2i} + p^i + 1)(p^{2i} - p^i + 1).$$

Let λ be a primitive (q^2+q+1)-root of unity in K. A straightforward computation shows that α defined by

$$\alpha(x) = \lambda x, \quad \alpha(y) = \lambda^{q+1}y,$$

is a K-automorphism of $K(\mathcal{X}_q)$ of order q^2+q+1, where $K(\mathcal{X}_q) = K(x,y)$, with $xy^{q+1} + x^{q+1} + y = 0$, is the function field of $\mathcal{X}_q$.

Let $h = \alpha^{p^{2i}+p^i+1}$. The group $H = \langle h \rangle$ has order $p^{2i} - p^i + 1$. The next results provide equations for the quotient curve $\mathcal{X}_q/H$ and one of those equations turns out to be

$$XY^{p^i+1} + X^{p^i+1} + Y = 0,$$

which is indeed the equation of the Tallini curve $\mathcal{X}_{p^i}$.

Proposition 2.4.1. The quotient curve $\mathcal{X}_q/H$ is isomorphic to the curve given by the equation

$$X^{p^{2i}+p^i+1}Y^{q+1} + Y + 1 = 0.$$

Proof. Take ξ, η from $K(x,y) = K(\mathcal{X}_q)$ given by

$$\xi = x^{p^{2i}-p^i+1}, \quad \eta = x^{-(q+1)}y.$$

Clearly $h(\xi) = \xi$ and $h(\eta) = \eta$, then $K(\xi,\eta) \subset K(x,y)^H$. Note that $K(x,y) = K(\xi,\eta)(x)$ and $T^{p^{2i}-p^i+1} - \xi$ is a polynomial in $K(\xi,\eta)[T]$ which has x as a root. Thus $[K(x,y) : K(\xi,\eta)] \leq p^{2i} - p^i + 1$. Note that $[K(x,y) : K(x,y)^H] = |H| = p^{2i} - p^i + 1$, hence $[K(x,y)^H : K(\xi,\eta)] = 1$, therefore $K(x,y)^H = K(\xi,\eta)$.

Finally, since $xy^{q+1} + x^{q+1} + y = 0$ and $\eta = x^{-(q+1)}y$ we get

$$x^{q^2+2q+2}\eta^{q+1} + x^{q+1} + x^{q+1}\eta = 0.$$

Thus, $x^{q^2+q+1}\eta^{q+1} + 1 + \eta = 0$. Since $\xi = x^{p^{2i}-p^i+1}$ and $q^2+q+1 = (p^{2i}+p^i+1)(p^{2i}-p^i+1)$ we get

$$\xi^{p^{2i}+p^i+1}\eta^{q+1} + \eta + 1 = 0.$$

□

Proposition 2.4.2. The quotient curve $\mathcal{X}_q/H$ is isomorphic to the curve given by the equation

$$X^{p^{2i}+p^i+1} + Y^{p^i+1} + Y^{p^i} = 0.$$

Proof. By the previous proposition, $K(\mathcal{X}_q/H) = K(x,y)$, with

$$x^{p^{2i}+p^i+1}y^{q+1} + y + 1 = 0,$$

that is,

$$x^{p^{2i}+p^i+1} + \frac{1}{y^q} + \frac{1}{y^{q+1}} = 0.$$

Putting $\xi = x$ and $\eta = 1/y$ gives

$$\xi^{p^{2i}+p^i+1} + \eta^q + \eta^{q+1} = 0.$$

Dividing by $\eta^{p^{2i}+p^i+1}$ and using $q = p^{2i}$ gives

$$\frac{\xi^{p^{2i}+p^i+1}}{\eta^{p^{2i}+p^i+1}} + \frac{1}{\eta^{p^i+1}} + \frac{1}{\eta^{p^i}} = 0.$$

Replacing $u = \xi/\eta$ and $v = 1/\eta$ gives

$$u^{p^{2i}+p^i+1} + v^{p^i+1} + v^{p^i} = 0.$$

□

Theorem 2.4.3. The quotient curve $\mathcal{X}_q/H$ is isomorphic to the curve $\mathcal{X}_{p^i}$ given by the equation

$$XY^{p^i+1} + X^{p^i+1} + Y = 0.$$

Proof. Consider the function field $K(\mathcal{X}_{p^i}) = K(x,y)$, with $xy^{p^i+1} + x^{p^i+1} + y = 0$. We have that

$$x(y^{p^i+1} + x^{p^i}) + y = 0.$$

Raising to the p^i-th power gives

$$x^{p^i}(y^{p^i+1} + x^{p^i})^{p^i} + y^{p^i} = 0.$$

Multiplying by x gives

$$x^{p^i+1}(y^{p^i+1} + x^{p^i})^{p^i} + xy^{p^i} = 0.$$

This also can be written as,

$$x^{p^{2i}+p^i+1} + (-xy^{p^i} - 1)^{p^i}(-xy^{p^i}) = 0.$$

Putting $u = x$ and $v = -xy^{p^i} - 1$ gives

$$u^{p^{2i}+p^i+1} + v^{p^i+1} + v^{p^i} = 0.$$

Note that $K(u,v) = K(x,y^{p^i}) \subset K(x,y)$. Since $xy^{p^i+1} + x^{p^i+1} + y = 0$,

$$y = -\frac{x^{p^i+1}}{xy^{p^i} + 1},$$

that is, y belongs to $K(x,y^{p^i})$. Therefore, $K(u,v) = K(x,y)$. □

2.5 The Hasse-Witt invariant

In this section $q = p$ is a prime number. Let $\Sigma = K(x,y)$, with $xy^{p+1} + x^{p+1} + y = 0$, be the function field of the Pellikaan curve $\mathcal{X}_p$, $\mathfrak{g}$ its genus and γ its Hasse-Witt invariant. The partial derivative of $F(X,Y) = XY^{p+1} + X^{p+1} + Y$ with respect to Y is $F_Y(X,Y) = XY^p + 1$.

Let $\Delta_\Sigma = \{udx \mid u \in \Sigma\}$ be the differential module of Σ and

$$C : \Delta_\Sigma^{(1)} \to \Delta_\Sigma^{(1)}$$

the Cartier operator defined on the space of holomorphic differentials

$$\Delta_\Sigma^{(1)} = \{w \in \Delta_\Sigma \mid (w) \geq 0\}.$$

Theorem 2.5.1. The Hasse-Witt invariant of $\mathcal{X}_p$ is equal to its genus.

Proof. Let w be an exact differential in $\Delta_\Sigma^{(1)}$, that is, $C(w) = 0$. Then w can be written in the form

$$w = (u_1^p + u_2^p x + \cdots + u_{p-2}^p x^{p-2})dx.$$

From (GORENSTEIN, 1952), a basis for the K-vector space $\Delta_{\Sigma}^{(1)}$ is given by

$$\mathfrak{B} = \left\{ \frac{x^i y^j}{F_Y(x,y)} dx \mid 0 \leq i+j \leq p-1 \right\}.$$

Thus

$$u_1^p + u_2^p x + \cdots + u_{p-2}^p x^{p-2} = \frac{u(x,y)}{F_Y(x,y)}$$

where $u(X,Y)$ is a polynomial in $K[X,Y]$ of degree at most $p-1$. Let

$$u(x,y) = \sum_{i+j \leq p-1} a_{ij} x^i y^j.$$

Since $xy^{p+1} + x^{p+1} + y = 0$ then

$$\frac{1}{y} = -\frac{xy^p + 1}{x^{p+1}}.$$

Thus we have

$$\frac{u(x,y)}{F_Y(x,y)} = \frac{u(x,y)}{xy^p+1} = \frac{1}{xy^p+1} \sum_{i+j \leq p-1} a_{ij} x^i y^j =$$

$$\frac{y^p}{xy^p+1} \sum_{i+j \leq p-1} a_{ij} x^i \left(\frac{1}{y}\right)^{p-j} =$$

$$\frac{y^p}{xy^p+1} \sum_{i+j \leq p-1} a_{ij} x^i \left(-\frac{xy^p+1}{x^{p+1}}\right)^{p-j} =$$

$$\sum_{i+j \leq p-1} (-1)^{j+1} a_{ij} \frac{y^p}{x^{p^2+p-jp}} x^{i+j} (xy^p+1)^{p-1-j} =$$

$$\sum_{i+j \leq p-1} (-1)^{j+1} a_{ij} \frac{y^p}{x^{p^2+p-jp}} x^{i+j} \sum_{k=0}^{p-1-j} \binom{p-1-j}{k} x^k y^{kp} =$$

$$\sum_{i+j \leq p-1} \sum_{k=0}^{p-1-j} (-1)^{j+1} \binom{p-1-j}{k} a_{ij} (x^{jp-p^2-p} y^{(k+1)p}) x^{i+j+k} =$$

$$\sum_{i+j \leq p-1} \sum_{k=0}^{p-1-j} w_{ijk}^p x^{i+j+k}$$

where

$$w_{ijk} = \left((-1)^{j+1} \binom{p-1-j}{k} a_{ij} \right)^{1/p} x^{j-p-1} y^{k+1}.$$

Hence,

$$u_1^p + u_2^p x + \cdots + u_{p-2}^p x^{p-2} = \sum_{i+j \leq p-1} \sum_{k=0}^{p-1-j} w_{ijk}^p x^{i+j+k}.$$

The term of degree $p-1$ in x on the right side is

$$\left(\sum_{i+j \leq p-1} w_{ijk_0}^p \right) x^{p-1}$$

where $k_0 = p-1-j-i$. It means that

$$\sum_{i+j\leq p-1} w^p_{ijk_0} = 0.$$

Note that

$$\sum_{i+j\leq p-1} w^p_{ijk_0} = 0 \quad \Rightarrow \sum_{i+j\leq p-1} w_{ijk_0} = 0 \quad \Rightarrow$$

$$\sum_{i+j\leq p-1} \left((-1)^{j+1}\binom{p-1-j}{k_0} a_{ij}\right)^{1/p} x^{j-p-1}y^{k_0+1} = 0 \quad \Rightarrow$$

$$\sum_{i+j\leq p-1} \left((-1)^{j+1}\binom{p-1-j}{p-1-j-i} a_{ij}\right)^{1/p} x^{j-p-1}y^{p-(i+j)} = 0 \quad \Rightarrow$$

$$\sum_{i+j\leq p-1} \left((-1)^{j+1}\binom{p-1-j}{p-1-j-i} a_{ij}\right)^{1/p} x^{j}y^{p-(i+j)} = 0.$$

Since the last equation has degree at most p, it must be equal to zero. Thus all coefficients a_{ij} are equal to zero, and therefore $u(x,y) = 0$. This shows that $w = 0$, that is, the Cartier operator $C : \Delta^{(1)}_\Sigma \to \Delta^{(1)}_\Sigma$ has trivial kernel.

Let V^0 be the space of all $w \in \Delta^{(1)}_\Sigma$ such that $C^i(w) = 0$ for some $i \geq 1$. Note that if $C^i(w) = 0$, then $C^{i-1}(w) \in \ker(C)$. Hence $V^0 = \{0\}$. This implies that the Hasse-Witt matrix (h_{ij}) over K of C has maximum rank equal to $\mathfrak{g}$, and consequently the matrix

$$M = (h_{ij})(h^p_{ij}) \cdots (h^{p^{g-1}}_{ij})$$

has rank $\mathfrak{g}$. Therefore, $\gamma = \mathfrak{g}$. □

CHAPTER

3

PURE GAPS AND GOPPA CODES OF CURVES OF HURWITZ TYPE

In (GOPPA, 1977) Goppa constructed algebraic geometric codes (also called Goppa codes) from several rational places by using algebraic curves, which led to an important research line in coding theory. Nowadays a great deal of works are devoted to determining or improving the parameters of Goppa codes. Weierstrass semigroups and pure gaps are of significant use in the construction and analysis of Goppa codes for their applications in obtaining codes with good parameters. In (GARCIA; KIM; LAX, 1993),(GARCIA; LAX, 1992), Garcia, Kim and Lax improved the Goppa bound using the arithmetical structure of the Weierstrass gaps at only one place. Homma and Kim (HOMMA; KIM, 2001) introduced the concept of pure gaps and demonstrated a similar result for a pair of places. And this was generalized to several places by Carvalho and Torres in (CARVALHO; TORRES, 2005). In this chapter, we will study Weierstrass pure gaps at two and three points of a family of curves that contains the curves of Hurwitz type and we will provide some examples of Goppa codes constructed using pure gaps.

3.1 Pure gaps at two points

In this section we consider a family of curves containing the non-singular curves of Hurwitz type which have homogeneous equation given by

$$\mathcal{H}_n\colon X_0X_1^n + X_1X_2^n + X_2X_0^n = 0,$$

where $n^2 - n + 1 \not\equiv 0 \pmod{p}$. The curve $\mathcal{H}_n$ is covered by the Fermat curve

$$X^{n^2-n+1} + Y^{n^2-n+1} + Z^{n^2-n+1} = 0$$

(via an unramified morphism). All the $\mathbb{F}_{q^2}$-maximal Hurwitz curves are characterized by

$$\mathcal{H}_n \text{ is } \mathbb{F}_{q^2}\text{-maximal} \iff q+1 \equiv 0 \pmod{n^2-n+1}.$$

Note that for $n=3$, $X_0X_1^3+X_1X_2^3+X_2X_0^3=0$ is the famous Klein quartic which is $\mathbb{F}_{q^2}$-maximal if and only if $q\equiv 6 \pmod 7$. Its automorphism group is isomorphic to $PSL(2,7)$. In characteristic 0, the Klein quartic has maximum number of automorphisms for curves of genus 3 as the Riemann-Hurwitz formula shows that the number of automorphisms, of curves of genus $g>1$, is at most $84(g-1)$, see (BARS, 2004).

For $n=q+1$, we get the Pellikaan curve $\mathcal{X}_q\colon X_0X_1^{q+1}+X_1X_2^{q+1}+X_2X_0^{q+1}=0$. By Theorem 2.1.2, $\mathcal{X}_q$ is projectively equivalent to the Tallini curve

$$(aX_0+bX_1+cX_2)\varphi_{01}-X_0\varphi_{02}+X_2\varphi_{12}=0,$$

where $\varphi_{ij}=X_i^qX_j-X_iX_j^q$ and a,b,c are elements in $\mathbb{F}_q$ such that the cubic equation

$$X^3-cX^2-aX-b=0$$

is irreducible over $\mathbb{F}_q$.

Let K be the algebraic closure of the finite field $\mathbb{F}_q$ of characteristic p. Let $n\geq 2$ be an integer with $n^2+n+1\not\equiv 0 \pmod p$. Consider a nonsingular curve of degree $n+2$ given by the homogeneous equation

$$\mathcal{X}\colon a_1XY^{n+1}+a_2ZX^{n+1}+a_3YZ^{n+1}+XYZ\cdot G(X,Y,Z)=0,$$

where $G(X,Y,Z)$ is zero or a homogeneous polynomial of degree $n-1$ and $a_1,a_2,a_3\in K$ with $a_1a_2a_3\neq 0$.

Let $K(\mathcal{X})=K(x,y)$, with $a_1xy^{n+1}+a_2x^{n+1}+a_3y+xy\cdot G(x,y,1)=0$, be the function field of $\mathcal{X}$, consider the three fundamental points

$$P_1=(1:0:0),\ P_2=(0:1:0),\ P_3=(0:0:1)$$

and let $\mathcal{P}_i$ denote the place associated to P_i, for $i=1,2,3$. The goal of this section is to characterize the set $G_0(\mathcal{P}_1,\mathcal{P}_2)$ of all pure gaps of $\mathcal{X}$ and as an application we use these pure gaps to construct Goppa codes with good parameters.

The tangent lines to $\mathcal{X}$ at P_1, P_2 and P_3 are $l_Z=\mathbf{v}(Z)$, $l_X=\mathbf{v}(X)$ and $l_Y=\mathbf{v}(Y)$, respectively. Note that the points in $l_Z\cap\mathcal{X}$ are P_1 and P_2 with

$$I(P_1,l_Z\cap\mathcal{X})=n+1 \text{ and } I(P_2,l_Z\cap\mathcal{X})=1,$$

the points in $l_X\cap\mathcal{X}$ are P_2 and P_3 with

$$I(P_2,l_X\cap\mathcal{X})=n+1 \text{ and } I(P_3,l_X\cap\mathcal{X})=1,$$

and the points in $l_Y\cap\mathcal{X}$ are P_1 and P_3 with

$$I(P_3,l_Y\cap\mathcal{X})=n+1 \text{ and } I(P_1,l_Y\cap\mathcal{X})=1.$$

Thus, it follows from (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Theorem 6.42) that the principal divisor of x is given by

$$\begin{aligned}(x) &= l_X \cdot \mathcal{X} - l_Z \cdot \mathcal{X} \\ &= I(P_2, l_X \cap \mathcal{X})\mathcal{P}_2 + I(P_3, l_X \cap \mathcal{X})\mathcal{P}_3 - I(P_1, l_Z \cap \mathcal{X})\mathcal{P}_1 - I(P_2, l_Z \cap \mathcal{X})\mathcal{P}_2 \\ &= (n+1)\mathcal{P}_2 + \mathcal{P}_3 - (n+1)\mathcal{P}_1 - \mathcal{P}_2 \\ &= -(n+1)\mathcal{P}_1 + n\mathcal{P}_2 + \mathcal{P}_3\end{aligned}$$

and the principal divisor of y is given by

$$\begin{aligned}(y) &= l_Y \cdot \mathcal{X} - l_Z \cdot \mathcal{X} \\ &= I(P_3, l_Y \cap \mathcal{X})\mathcal{P}_3 + I(P_1, l_Y \cap \mathcal{X})\mathcal{P}_1 - I(P_1, l_Z \cap \mathcal{X})\mathcal{P}_1 - I(P_2, l_Z \cap \mathcal{X})\mathcal{P}_2 \\ &= (n+1)\mathcal{P}_3 + \mathcal{P}_1 - (n+1)\mathcal{P}_1 - \mathcal{P}_2 \\ &= -n\mathcal{P}_1 - \mathcal{P}_2 + (n+1)\mathcal{P}_3.\end{aligned}$$

Theorem 3.1.1. The Weierstrass semigroup $H(\mathcal{P}_i)$, for $i = 1,2,3$, is the semigroup generated by

$$S := \{sn+1 \colon 1 \leq s \leq n+1\}.$$

Proof. Using the relations

$$(x) = -(n+1)\mathcal{P}_1 + n\mathcal{P}_2 + \mathcal{P}_3$$

and

$$(y) = -n\mathcal{P}_1 - \mathcal{P}_2 + (n+1)\mathcal{P}_3,$$

we get

$$\begin{aligned}\left(\frac{y}{x^s}\right) &= (s(n+1)-n)\mathcal{P}_1 - (sn+1)\mathcal{P}_2 + (n+1-s)\mathcal{P}_3, \\ \left(\frac{x^{s-1}}{y^s}\right) &= (-(s-1)(n+1)+sn)\mathcal{P}_1 + ((s-1)n+s)\mathcal{P}_2 - (sn+1)\mathcal{P}_3, \\ (xy^{s-1}) &= -(sn+1)\mathcal{P}_1 + (n+1-s)\mathcal{P}_2 + ((s-1)(n+1)+1)\mathcal{P}_3,\end{aligned}$$

for $1 \leq s \leq n+1$. Thus,

$$\begin{aligned}\left(\frac{y}{x^s}\right)_\infty &= (sn+1)\mathcal{P}_2, \\ \left(\frac{x^{s-1}}{y^s}\right)_\infty &= (sn+1)\mathcal{P}_3, \\ (xy^{s-1})_\infty &= (sn+1)\mathcal{P}_1,\end{aligned}$$

for $1 \leq s \leq n+1$. Given $i \in \{1,2,3\}$, the above relations imply that $S \subset H(\mathcal{P}_i)$. From a result on arithmetic progressions, $|\mathbb{N} \setminus \langle S \rangle| = \frac{1}{2}n(n+1)$. Since $\langle S \rangle \subset H(\mathcal{P}_i)$ and the number of gaps at $\mathcal{P}_i$ is $\frac{1}{2}n(n+1)$, the Weierstrass semigroup $H(\mathcal{P}_i)$ is generated by S. □

Now, since $G(\mathcal{P}_s) = \mathbb{N} \setminus H(\mathcal{P}_s)$, for $s = 1,2,3$, it can be easily checked that the gap sequence at $\mathcal{P}_s$ is given by

$$G(\mathcal{P}_s) = \{(i-1)n + j \colon 1 \leq i \leq j \leq n\}, \quad s = 1,2,3.$$

For a gap a at $\mathcal{P}_1$, we define $\beta_a = \min\{t : (a,t) \in H(\mathcal{P}_1,\mathcal{P}_2)\}$. This number β_a was first introduced by Kim in (KIM, 1994) to investigate the cardinality of the set of gaps at two points. Kim proved that $\{\beta_a : a \in G(\mathcal{P}_1)\} = G(\mathcal{P}_2)$, hence

$$\begin{aligned} \beta : G(\mathcal{P}_1) &\to G(\mathcal{P}_2) \\ a &\mapsto \beta_a \end{aligned}$$

is a bijection map between $G(\mathcal{P}_1)$ and $G(\mathcal{P}_2)$.

Consider $G(\mathcal{P}_1) = \{n_1,\ldots,n_g\}$ and $G(\mathcal{P}_2) = \{m_1,\ldots,m_g\}$. Thus $\beta : G(\mathcal{P}_1) \to G(\mathcal{P}_2)$ is given by $n_i \mapsto m_{\sigma(i)}$ for some permutation σ of the set $\mathbb{N}_{\leq g} := \{1,\ldots,g\}$. Define

$$R(\sigma) = \{(i,j) \in \mathbb{N}_{\leq g} \times \mathbb{N}_{\leq g} : i < j \text{ and } \sigma(i) > \sigma(j)\}.$$

In (HOMMA; KIM, 2001), Homma and Kim described the set of all pure gaps at two points using the permutation σ as follows:

Proposition 3.1.2. The set of all pure gaps at $(\mathcal{P}_1,\mathcal{P}_2)$ is given by

$$G_0(\mathcal{P}_1,\mathcal{P}_2) = \{(n_i, m_{\sigma(j)}) : (i,j) \in R(\sigma)\}.$$

Moreover, $\#G_0(\mathcal{P}_1,\mathcal{P}_2) = \#R(\sigma)$.

Proof. See (HOMMA; KIM, 2001, Theorem 2.1). □

The next result shows how the function β permutes the elements of $G(\mathcal{P}_s)$, $s = 1,2,3$.

Theorem 3.1.3. For each $1 \leq i \leq j \leq n$,

$$\beta_{(i-1)n+j} = (n-j)n + n + i - j.$$

Proof. The divisors of x and y are given by

$$(x) = -(n+1)\mathcal{P}_1 + n\mathcal{P}_2 + \mathcal{P}_3 \text{ and } (y) = -n\mathcal{P}_1 - \mathcal{P}_2 + (n+1)\mathcal{P}_3.$$

The gap sequence at $\mathcal{P}_1$ (and at $\mathcal{P}_2$) is given by the diagram

$$\begin{array}{ccccc} 1 & 2 & 3 & \cdots & n \\ & n+2 & n+3 & \cdots & 2n \\ & & 2n+3 & \cdots & 3n \\ & & & \ddots & \vdots \\ & & & & n^2 \end{array} \tag{3.1}$$

Then for each $1 \leq i \leq j \leq n$, $(i-1)n+j$ is the number on the i-th row and j-th column. Note that,

$$\left(\frac{y^{n+i-j}}{x^{n-j}}\right)_\infty = ((i-1)n+j)\mathcal{P}_1 + ((n-j)n+n+i-j)\mathcal{P}_2.$$

Therefore, $((i-1)n+j,(n-j)n+n+i-j) \in H(\mathcal{P}_1,\mathcal{P}_2)$. To see that this gives the β_a as claimed, start with $j=n$ and $1 \leq i \leq n$. This gives $(in,i) \in H(\mathcal{P}_1,\mathcal{P}_2)$ for $1 \leq i \leq n$. Hence $\beta_{in} = i$ for $1 \leq i \leq n$, which gives β_a for all gaps a at $\mathcal{P}_1$ on the n-th column in (3.1). Now let $j = n-1$ and $1 \leq i \leq n-1$ to get $\beta_{in-1} = n+1+i$ for $1 \leq i \leq n-1$, which gives β_a for all gaps a at $\mathcal{P}_1$ on the $(n-1)$-th column in (3.1). Continuing in this manner, from the n-th column to the first column, we get the result. □

Therefore the behaviour of β can be described by the following diagram:

$$\begin{array}{ccccc} 1 & 2 & 3 & \cdots & n \\ & n+2 & n+3 & \cdots & 2n \\ & & 2n+3 & \cdots & 3n \\ & & & \ddots & \vdots \\ & & & & n^2 \end{array} \quad \xrightarrow{\beta} \quad \begin{array}{ccccc} n^2 & \cdots & 2n+3 & n+2 & 1 \\ & \ddots & \vdots & n+3 & 2 \\ & & 3n & \vdots & 3 \\ & & & 2n & \vdots \\ & & & & n \end{array} \tag{3.2}$$

Proposition 3.1.4. The number of pure gaps at $(\mathcal{P}_1,\mathcal{P}_2)$ is $\frac{1}{12}(n-1)n(n+1)(n+2)$.

Proof. Fix $1 \leq i \leq j \leq n$. Since $\#G_0(\mathcal{P}_1,\mathcal{P}_2) = \#R(\sigma)$, we need to count all pairs (I,J) such that

$$(i-1)n+j < (I-1)n+J \tag{3.3}$$

and

$$\beta((i-1)n+j) > \beta((I-1)n+J). \tag{3.4}$$

Note that (3.3) is equivalent to

$$(i-I)n < J-j$$

and (3.4) is equivalent to

$$(J-j)(n+1) > I-i.$$

First consider the case $J=j$. Since $(J-j)(n+1)=0$, in order to satisfy (3.4), we must have $I<i$. However, (3.3) fails when $I<i$. Hence, there is no such pairs (I,J) when $J=j$. Now suppose $J<j$. Note that (3.4) is equivalent to $(j-J)(n+1) < i-I$. Hence, $i-I \leq n-1$ (since $1 \leq i,I \leq n$) and $n+1 \leq (j-J)(n+1)$ (since $1 \leq j,J \leq n$) imply that (3.4) fails. The only case left to consider is $j<J$. Here, (3.4) always holds since

$$I-i \leq n-1 < n+1 \leq (J-j)(n+1).$$

If $I<i$, then (3.3) fails since

$$J-j \leq n-1 < n \leq (i-I)n.$$

If $i \leq I$, then $(i-I)n \leq 0 < J-j$ and so (3.3) holds.

The number of pais (I,J) with $j<J$ and $i\leq I$ is

$$\#\{(I,J)\colon i\leq I,\ j<J,\ 1\leq I\leq J\leq n\}=N_1+N_2,$$

where

$$N_1=\#\{(I,J)\colon i\leq I\leq j<J\leq n\}$$

and

$$N_2=\#\{(I,J)\colon j<I\leq J\leq n\}.$$

It is easy to see that $N_1=(j-i+1)(n-j)$ and $N_2=\frac{1}{2}(n-j)(n-j+1)$. Thus,

$$\#G_0(\mathcal{P}_1,\mathcal{P}_2)=\sum_{i=1}^{n}\sum_{j=i}^{n}(N_1+N_2)=\sum_{i=1}^{n}\sum_{j=i}^{n}\frac{1}{2}(n-j)(j-2i+n+3).$$

For each $1\leq i\leq n$,

$$\sum_{j=i}^{n}\frac{1}{2}(n-j)(j-2i+n+3)=\frac{1}{3}\left(-i^3+3(n+1)i^2-(3n^2+6n+2)i+n^3+3n^2+2n\right).$$

Therefore,

$$\#G_0(\mathcal{P}_1,\mathcal{P}_2)=\sum_{i=1}^{n}\frac{1}{3}\left(-i^3+3(n+1)i^2-(3n^2+6n+2)i+n^3+3n^2+2n\right)=$$

$$\frac{1}{12}(n^4+2n^3-n^2-2n)=\frac{1}{12}(n-1)n(n+1)(n+2).$$

□

Proposition 3.1.5. The number of gaps at $(\mathcal{P}_1,\mathcal{P}_2)$ is $\frac{1}{4}n(n+1)(n^2+n+2)$.

Proof. By (HOMMA; KIM, 2001), the number of gaps at $(\mathcal{P}_1,\mathcal{P}_2)$ is given by

$$\#G(\mathcal{P}_1,\mathcal{P}_2)+\#G_0(\mathcal{P}_1,\mathcal{P}_2)=\sum_{x\in G(\mathcal{P}_1)}x+\sum_{y\in G(\mathcal{P}_2)}y.$$

Note that,

$$\sum_{x\in G(\mathcal{P}_1)}x=\sum_{i=1}^{n}\sum_{j=i}^{n}((i-1)n+j).$$

For each $1\leq i\leq n$,

$$\sum_{j=i}^{n}((i-1)n+j)=\frac{1}{2}\left(-(2n+1)i^2+(2n^2+4n+1)i-n^2-n\right).$$

Thus,

$$\sum_{x\in G(\mathcal{P}_1)}x=\sum_{i=1}^{n}\sum_{j=i}^{n}((i-1)n+j)=$$

$$\sum_{i=1}^{n}\frac{1}{2}\left(-(2n+1)i^2+(2n^2+4n+1)i-n^2-n\right)=$$

$$\frac{1}{2}\left(-\frac{1}{6}(2n+1)^2(n+1)n+\frac{1}{2}(2n^2+4n+1)(n+1)n-(n^2+n)n\right)=$$
$$\frac{1}{6}n(n+1)(n^2+n+1).$$

Finally,

$$\#G(\mathcal{P}_1,\mathcal{P}_2)=2\cdot\sum_{i=1}^{n}\sum_{j=i}^{n}((i-1)n+j)-\#G_0(\mathcal{P}_1,\mathcal{P}_2)=$$
$$\frac{1}{3}n(n+1)(n^2+n+1)-\frac{1}{12}(n-1)n(n+1)(n+2)=\frac{1}{4}n(n+1)(n^2+n+2).$$

□

For positive integers i,j with $2\leq i+j\leq n$, define the square-like subset S_{ij} of $\mathbb{N}_0^2$ by

$$S_{ij}=\left\{(a,b)\in\mathbb{N}_0^2\;\middle|\;\begin{array}{rcccl}(i-1)n+i & \leq & a & \leq & in-j\\ (j-1)n+i+j-1 & \leq & b & \leq & jn\end{array}\right\}.$$

Theorem 3.1.6. The set of pure gaps at the pair $(\mathcal{P}_1,\mathcal{P}_2)$ is

$$G_0(\mathcal{P}_1,\mathcal{P}_2)=\bigcup_{1<i+j\leq n}S_{ij}.$$

Proof. First we show that $S_{ij}\subset G_0(\mathcal{P}_1,\mathcal{P}_2)$. Take $(a,b)\in S_{ij}$. Then,

$$\begin{array}{rcccl}(i-1)n+i & \leq & a & \leq & in-j\\ (j-1)n+i+j-1 & \leq & b & \leq & jn\end{array}$$

that is,

$$\begin{array}{rcccl}(i-1)n+i & \leq & a & \leq & (i-1)n+(n-j)\\ t_1 & \leq & b & \leq & t_2,\end{array}$$

where $t_1=(n-(n-j+1))n+(n+i-(n-j+1))$ and $t_2=(n-(n-j+1))n+(n+(n-j+1)-(n-j+1))$. Thus, a is on the i-th row in (3.1) and b is on the $(n-j+1)$-th column in (3.2). Let $\bar{b}\in G(\mathcal{P}_1)$ such that $\beta_{\bar{b}}=b$. Then, $\bar{b}$ is on the $(n-j+1)$-th column and t-th row in (3.1), for some $i\leq t\leq n-j+1$. Hence,

$$(i-1)n+(n-j+1)\leq\bar{b}\leq((n-j+1)-1)n+(n-j+1).$$

Furthermore, β_a is on the i-th row and h-th column in (3.2), for some $i\leq h\leq n-j$. Hence,

$$(n-i)n+(n+i-i)\leq\beta_a\leq(n-(n-j))n+(n+i-(n-j)).$$

It follows from $i+j<n+1$ that $jn<(n+1-i)n$, then

$$b\leq jn<(n+1-i)n\leq\beta_a.$$

Moreover,

$$a\leq(i-1)n+(n-j)<(i-1)n+(n-j+1)\leq\bar{b}.$$

Since $a < \bar{b}$ and $\beta_a > \beta_{\bar{b}}$ we conclude that $(a,b) \in G_0(\mathcal{P}_1,\mathcal{P}_2)$.

The union of all S_{ij} is disjoint, in fact, suppose that $(a,b) \in S_{ij} \cup S_{uv}$. Then a is on the i-th row and u-th row in (3.1), then $i = u$. And b is on the $(n-j+1)$-th column and $(n-v+1)$-th column in (3.1), then $j = v$. Hence, $S_{ij} = S_{uv}$.

Note that $\#S_{ij} = ((i+j)-(n+1))((i+j)-(n+2))$. Thus,

$$\#\left(\bigcup_{1<i+j\leq n} S_{ij}\right) = \sum_{1<i+j\leq n} \#S_{ij} = \sum_{r=1}^{n-1} r(n-(r-1))(n-r) = \frac{1}{12}(n-1)n(n+1)(n+2),$$

which is the same number of elements in $G_0(\mathcal{P}_1,\mathcal{P}_2)$, by Proposition 3.1.4. This finishes the proof. □

Example 3.1.7. Let $q = 41$ and consider the $\mathbb{F}_{q^2}$-maximal curve $\mathcal{X}$ of genus 10 defined by

$$X_0X_1^5 + X_1X_2^5 + X_2X_0^5 = 0.$$

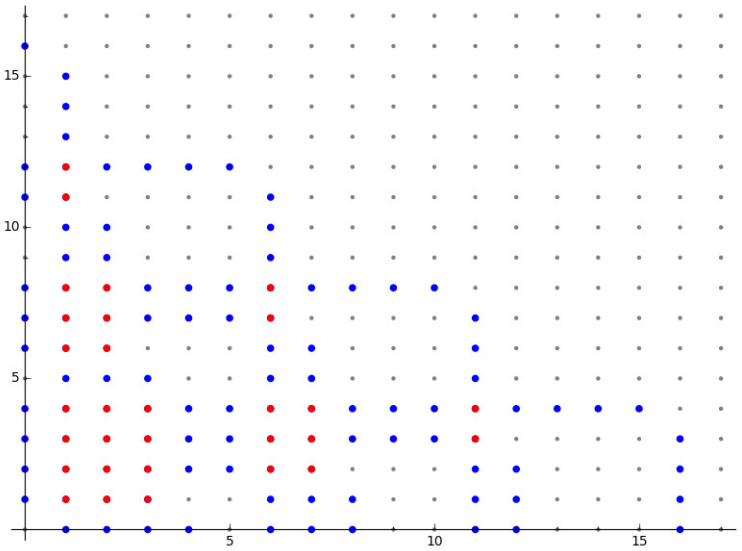

Figure 1 – The pure gaps at (P_1,P_2)

The set of gaps of $\mathcal{X}$ at one place of $\{\mathcal{P}_1,\mathcal{P}_2,\mathcal{P}_3\}$ is given by

$$G(\mathcal{P}_i) = \{1,2,3,4,6,7,8,11,12,16\}$$

and the function $\beta : G(\mathcal{P}_1) \to G(\mathcal{P}_2)$ is given by

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ & 6 & 7 & 8 \\ & & 11 & 12 \\ & & & 16 \end{array} \xrightarrow{\beta} \begin{array}{cccc} 16 & 11 & 6 & 1 \\ & 12 & 7 & 2 \\ & & 8 & 3 \\ & & & 4 \end{array}.$$

It follows from Propositions 3.1.4 and 3.1.5 that

$$\#G_0(\mathcal{P}_1,\mathcal{P}_2) = 30,\ \#G(\mathcal{P}_1,\mathcal{P}_2) = 90.$$

These results are displayed in Figure 2, where the red points represent the pure gaps at $(\mathcal{P}_1, \mathcal{P}_2)$, the blue points represent the gaps that are not pure gaps, that is, the elements of $G(\mathcal{P}_1, \mathcal{P}_2) \setminus G_0(\mathcal{P}_1, \mathcal{P}_2)$.

3.2 Pure gaps at three points

Let K be the algebraic closure of the finite field $\mathbb{F}_q$ of characteristic p. Let $n \geq 2$ be an integer with $n^2 + n + 1 \not\equiv 0 \pmod{p}$. Consider a nonsingular curve of degree $n+2$ given by the homogeneous equation

$$\mathcal{X}\colon a_1 XY^{n+1} + a_2 ZX^{n+1} + a_3 YZ^{n+1} + XYZ \cdot G(X,Y,Z) = 0,$$

where $G(X,Y,Z)$ is zero or a homogeneous polynomial of degree $n-1$ and $a_1, a_2, a_3 \in K$ with $a_1 a_2 a_3 \neq 0$. Suppose that $(x,y,z) \mapsto (z,x,y)$ is an K-automorphism of $\mathcal{X}$.

Let $K(\mathcal{X}) = K(x,y)$, with $a_1 xy^{n+1} + a_2 x^{n+1} + a_3 y + xy \cdot G(x,y,1) = 0$, be the function field of $\mathcal{X}$ and consider the three points

$$P_1 = (1:0:0),\ P_2 = (0:1:0),\ P_3 = (0:0:1).$$

and let $\mathcal{P}_i$ denote the place associated to P_i, for $i = 1,2,3$. In this section we characterize the set of all pure gaps of $\mathcal{X}$ at $(\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3)$. But first, a few Lemmas is needed in order to give us enough tools to prove the main results.

Lemma 3.2.1. For $e = 1, \ldots, n+1$, the sets

$$\mathcal{B} = \{x^i y^j : 1 \leq i \leq e-1 \text{ and } 1 \leq j \leq e-1-i\}$$

and

$$\mathcal{B} \cup \{1, x, \ldots, x^{e-1}\}$$

are bases for $\mathcal{L}(en\mathcal{P}_1 - e\mathcal{P}_3)$ and $\mathcal{L}(en\mathcal{P}_1)$, respectively. In particular,

(i) $\ell(e(n\mathcal{P}_1 - \mathcal{P}_3)) = \frac{(e-1)(e-2)}{2}$, and

(ii) $\ell(en\mathcal{P}_1) = \frac{e^2-e+2}{2}$.

Proof. The fact that $\mathcal{B} \cup \{1, x, \ldots, x^{e-1}\}$ is a basis for $\mathcal{L}(en\mathcal{P}_1)$ follows from the known description of $G(\mathcal{P}_1)$. Now, for $f \in \mathcal{L}(en\mathcal{P}_1 - e\mathcal{P}_3)$, we use that $\mathcal{L}(en\mathcal{P}_1 - e\mathcal{P}_3) \subseteq \mathcal{L}(en\mathcal{P}_1)$, and write

$$f = \sum_{i=0}^{e-1} a_i x^i + \sum_{x^i y^j \in \mathcal{B}} b_{ij} x^i y^j$$

with $a_i, b_{ij} \in \mathbb{F}_q$. Note $f \in \mathcal{L}(en\mathcal{P}_1 - e\mathcal{P}_3)$ if and only if $f \in \mathcal{L}(en\mathcal{P}_1)$ and $v_{\mathcal{P}_3}(f) \geq e$. Since $v_{\mathcal{P}_3}(x) = 1$ and $v_{\mathcal{P}_3}(y) = n+1$, triangular inequality gives $f \in \mathcal{L}(en\mathcal{P}_1 - e\mathcal{P}_3)$ if and only if $a_0 = a_1 = \cdots = a_{e-1} = 0$. Thus $\mathcal{B}$ is a basis for $\mathcal{L}(en\mathcal{P}_1 - e\mathcal{P}_3)$. □

Lemma 3.2.2. For $i,j,k \in \mathbb{Z}$, set $d := i+j+k$ and consider the divisor

$$S_d = (k(n+1)+j)\mathcal{P}_1 + (i(n+1)+k)\mathcal{P}_2 + (j(n+1)+i)\mathcal{P}_3.$$

Then

$$\ell(S_d) = \begin{cases} 0, & \text{if } d < 0 \\ \frac{(d+2)(d+1)}{2}, & \text{if } 0 \leq d \leq n-1 \\ (n+2)d - g + 1, & \text{if } d \geq n. \end{cases}$$

Proof. Note that $(x^i y^j) = -(in+jn+i)\mathcal{P}_1 + (in-j)\mathcal{P}_2 + (i+j(n+1))\mathcal{P}_3$, and then

$$S_d = (x^i y^j) + d((n+1)\mathcal{P}_1 + \mathcal{P}_2). \tag{3.5}$$

Thus the result follows directly from the fact that $(n+1)\mathcal{P}_1 + \mathcal{P}_2$ is the divisor cut out on $\mathcal{C}$ by the line $z = 0$. □

Lemma 3.2.3. Notation as in Lemma 3.2.2. If $0 \leq d \leq n-1$ and $d+e = n-1$, then

$$\ell(S_d + e(\mathcal{P}_1 + \mathcal{P}_2 + \mathcal{P}_3)) = \frac{(d+2)(d+1)}{2}.$$

Proof. Let $i_1, i_2, i_3 \in \mathbb{Z}$ be such that $i_1 + i_2 + i_3 = e$. Since $d + e = n-1$, it follows that S_{d+e} is a canonical divisor. Thus for $D := S_d + e(\mathcal{P}_1 + \mathcal{P}_2 + \mathcal{P}_3)$, we have

$$S_{d+e} - D = S_e - e(\mathcal{P}_1 + \mathcal{P}_2 + \mathcal{P}_3) = (x^{i_1} y^{j_1}) + e(n\mathcal{P}_1 - \mathcal{P}_3),$$

where the second equality above follows from (3.2). Therefore, by Riemann-Roch theorem

$$\ell(D) = \deg D + 1 - g + \ell(e(n\mathcal{P}_1 - \mathcal{P}_3)).$$

From Lemma 3.2.1, we have $\ell(e(n\mathcal{P}_1 - \mathcal{P}_3)) = \frac{(e-1)(e-2)}{2}$, and then

$$\ell(D) = d(n+2) + 3e + 1 - \frac{n(n+1)}{2} + \frac{(e-1)(e-2)}{2} = \frac{(d+2)(d+1)}{2}.$$

□

The next result gives us a subset of the set of pure gaps at $(\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3)$. Later we will prove that this subset is indeed $G_0(\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3)$.

Theorem 3.2.4. If $i,j,k \in \mathbb{N}_0$ are such that $i+j+k = d \leq n-2$, and $r,s,t \in \{0,\ldots,n-2-d\}$ then

$$(a,b,c) := \Big(k(n+1)+j+r+1, i(n+1)+k+s+1, j(n+1)+i+t+1\Big)$$

are pure gaps at $(\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3)$. Moreover,

$$D = a\mathcal{P}_1 + b\mathcal{P}_2 + c\mathcal{P}_3$$

and

$$E = (a-1)\mathcal{P}_1 + (b-1)\mathcal{P}_2 + (c-1)\mathcal{P}_3.$$

have dimension $(d+1)(d+2)/2$.

Proof. It follows immediately from Lemmas 3.2.2 and 3.2.3. □

The action of the order 3 automorphism $\sigma\colon (x,y,z) \mapsto (z,x,y)$ on $\{\mathcal{P}_1,\mathcal{P}_2,\mathcal{P}_3\}$ gives the following result.

Lemma 3.2.5. If $(a,b,c) \in H(\mathcal{P}_1,\mathcal{P}_2,\mathcal{P}_3)$, then $(c,a,b),(b,c,a) \in H(\mathcal{P}_1,\mathcal{P}_2,\mathcal{P}_3)$.

Proof. Let $(a,b,c) \in H(\mathcal{P}_1,\mathcal{P}_2,\mathcal{P}_3)$. Then, there exists $f \in K(\mathcal{X})$ such that

$$(f)_\infty = a\mathcal{P}_1 + b\mathcal{P}_2 + c\mathcal{P}_3$$

and $a = v_{\mathcal{P}_1}(f)$, $b = v_{\mathcal{P}_2}(f)$, $c = v_{\mathcal{P}_3}(f)$. Now, consider the K-automorphism

$$\sigma\colon (x,y,z) \mapsto (z,x,y)$$

of $\mathcal{X}$. The action of σ on the places $\mathcal{P}_1,\mathcal{P}_2,\mathcal{P}_3$ is given by $(\mathcal{P}_1,\mathcal{P}_2,\mathcal{P}_3) \mapsto (\mathcal{P}_2,\mathcal{P}_3,\mathcal{P}_1)$. Hence,

$$\begin{aligned}(\sigma(f))_\infty &= v_{\mathcal{P}_1}(\sigma(f))\mathcal{P}_1 + v_{\mathcal{P}_2}(\sigma(f))\mathcal{P}_2 + v_{\mathcal{P}_3}(\sigma(f))\mathcal{P}_3\\ &= v_{\mathcal{P}_2}(f)\mathcal{P}_1 + v_{\mathcal{P}_3}(f)\mathcal{P}_2 + v_{\mathcal{P}_1}(f)\mathcal{P}_3\\ &= b\mathcal{P}_1 + c\mathcal{P}_2 + a\mathcal{P}_3\end{aligned}$$

and

$$\begin{aligned}(\sigma^2(f))_\infty &= v_{\mathcal{P}_1}(\sigma^2(f))\mathcal{P}_1 + v_{\mathcal{P}_2}(\sigma^2(f))\mathcal{P}_2 + v_{\mathcal{P}_3}(\sigma^2(f))\mathcal{P}_3\\ &= v_{\mathcal{P}_3}(f)\mathcal{P}_1 + v_{\mathcal{P}_1}(f)\mathcal{P}_2 + v_{\mathcal{P}_2}(f)\mathcal{P}_3\\ &= c\mathcal{P}_1 + a\mathcal{P}_2 + b\mathcal{P}_3.\end{aligned}$$

Therefore, $(c,a,b),(b,c,a) \in H(\mathcal{P}_1,\mathcal{P}_2,\mathcal{P}_3)$. □

We know that if $(a,b,c) \in G_0(\mathcal{P}_1,\mathcal{P}_2,\mathcal{P}_3)$, then $a,b,c \in G(\mathcal{P}_1)$. The next Lemma shows that a,b,c cannot divide n. Thus, we define G_* as the set of gaps at $\mathcal{P}_1$ that are not divisible by n, that is,

$$G_* = \{a \in G(\mathcal{P}_1)\colon n \nmid a\}.$$

Lemma 3.2.6. If $(a,b,c) \in G_0(\mathcal{P}_1,\mathcal{P}_2,\mathcal{P}_3)$, then $a,b,c \in G_*$.

Proof. Suppose that $a \in G(\mathcal{P}_1) \setminus G_*$. Then, $a = tn$, for some $t \in \{1,\ldots,n\}$. Note that $\beta(tn) = t$, thus $(tn,t,0) \in H(\mathcal{P}_1,\mathcal{P}_2,\mathcal{P}_3)$. Since $(tn,b,c) \in G_0(\mathcal{P}_1,\mathcal{P}_2,\mathcal{P}_3)$, by Theorem 1.4.7, $b < t$ and $(bn,b,0) \in G(\mathcal{P}_1,\mathcal{P}_2,\mathcal{P}_3)$, absurd, as $(bn,b,0) = (bn,\beta(bn),0) \in H(\mathcal{P}_1,\mathcal{P}_2,\mathcal{P}_3)$. Hence $a \in G_*$. Now, suppose that $b \in G(\mathcal{P}_1) \setminus G_*$. Then, $b = sn$, for some $s \in \{1,\ldots,n\}$. Note that $\beta(sn) = s$, thus $(sn,s,0) \in H(\mathcal{P}_1,\mathcal{P}_2,\mathcal{P}_3)$. By Lemma 3.2.5, $(0,sn,s) \in H(\mathcal{P}_1,\mathcal{P}_2,\mathcal{P}_3)$. Since $(a,sn,c) \in G_0(\mathcal{P}_1,\mathcal{P}_2,\mathcal{P}_3)$, by Theorem 1.4.7, $c < s$ and $(0,cn,c) \in G(\mathcal{P}_1,\mathcal{P}_2,\mathcal{P}_3)$, absurd, as $(0,cn,c) = (0,cn,\beta(cn)) \in H(\mathcal{P}_1,\mathcal{P}_2,\mathcal{P}_3)$. Hence $b \in G_*$. The same idea proves that $c \in G_*$. □

Lemma 3.2.7. Let $a \in G_*$. Then there are $k \in \{0,\ldots,n-2\}$ and $a_0 \in \{1,\ldots,(n-1)-k\}$ such that $a = k(n+1) + a_0$.

Proof. There are $k \in \mathbb{N}_0$ and $a_0 \in \{0,\dots,n\}$ such that

$$a = k(n+1)+a_0.$$

Suppose that $k \geq n-1$, then $a = k(n+1)+a_0 \geq (n-1)(n+1)+a_0 > n^2-n-1$, but this cannot happen as $\max(G_*) = n^2-n-1$. Hence, $k \leq n-2$.
Since the multiples of $n+1$ are elements of $H(\mathcal{P}_1)$, then $a_0 \geq 1$. Note that

$$k(n+1) < a < (k+1)(n+1)$$

and there is no element $u \in G_*$ with $(k+1)n \leq u \leq (k+1)(n+1)$, then

$$k(n+1) < a < (k+1)n.$$

Thus, $a < (k+1)n$, gives $a_0 \leq n-1-k$. □

Again, consider the function $\beta : G(\mathcal{P}_1) \longrightarrow G(\mathcal{P}_2)$ given by

$$\beta(a) = \min\{t : (a,t) \in H(\mathcal{P}_1,\mathcal{P}_2)\}.$$

By Theorem 3.1.3,

$$\beta((i-1)n+j) = (n-j)n+n+i-j,$$

for $1 \leq i \leq j \leq n$.

For any $a,b,c \in G(\mathcal{P}_1)$ consider the following conditions:

$$\begin{array}{ll} (i) & a < \beta(c) \\ (ii) & b < \beta(a) \\ (iii) & c < \beta(b) \\ (iv) & a < \beta^{-1}(b) \\ (v) & b < \beta^{-1}(c) \\ (vi) & c < \beta^{-1}(a) \end{array}.$$

Set

$$\mathbb{S} := \Big\{(a,b,c) = \Big(k(n+1)+j+r+1, i(n+1)+k+s+1, j(n+1)+i+t+1\Big) :$$

$$0 \leq i+j+k \leq n-2 \text{ and } r,s,t \in \{0,\dots,n-2-(i+j+k)\}\Big\}$$

and

$$R(\beta) := \{(a,b,c) \in G(\mathcal{P}_1)^3 : a,b,c \text{ satisfies } (i),\dots,(vi)\}.$$

The next Theorem gives us a characterization of the set of all pure gaps of $\mathcal{X}$ at $(\mathcal{P}_1,\mathcal{P}_2,\mathcal{P}_3)$.

Theorem 3.2.8. Let $a,b,c \in G_*$. The following are equivalent:

(i) $(a,b,c) \in G_0(\mathcal{P}_1,\mathcal{P}_2,\mathcal{P}_3)$;

(ii) $(a,b,c) \in R(\beta)$;

(iii) $(a,b,c) \in \mathbb{S}$.

Proof. $(iii) \Rightarrow (i)$: It follows from Theorem 3.2.4.
$(i) \Rightarrow (ii)$: Suppose that $(a,b,c) \in G_0(\mathcal{P}_1,\mathcal{P}_2,\mathcal{P}_3)$. Since $(a,\beta(a)) \in H(\mathcal{P}_1,\mathcal{P}_2)$,

$$(a,\beta(a),0),(\beta^{-1}(b),b,0) \in H(\mathcal{P}_1,\mathcal{P}_2,\mathcal{P}_3).$$

It follows from Lemma 3.2.5, that

$$(0,b,\beta(b)),(\beta(c),0,c),(0,\beta^{-1}(c),c),(a,0,\beta^{-1}(a)) \in H(\mathcal{P}_1,\mathcal{P}_2,\mathcal{P}_3).$$

By Theorem 1.4.7, a,b,c satisfies $(i),\ldots,(vi)$.
$(ii) \Rightarrow (iii)$: Let $a,b,c \in G_*$ satisfying $(i),\ldots,(vi)$. By Lemma 3.2.7, we can write

$$a = k(n+1)+a_0,$$

$$b = i(n+1)+b_0,$$

$$c = j(n+1)+c_0,$$

with $i,j,k \in \{0,\ldots,n-2\}$ and

$$1 \leq a_0 \leq (n-1)-k,$$

$$1 \leq b_0 \leq (n-1)-i,$$

$$1 \leq c_0 \leq (n-1)-j.$$

An easy computation shows that

(a) $\beta(a) = (n-a_0-k)n+n+1-a_0$;

(b) $\beta(b) = (n-b_0-i)n+n+1-b_0$;

(c) $\beta(c) = (n-c_0-j)n+n+1-c_0$;

(d) $\beta^{-1}(a) = (a_0-1)n+n-k$;

(e) $\beta^{-1}(b) = (b_0-1)n+n-i$;

(f) $\beta^{-1}(c) = (c_0-1)n+n-j$.

It follows from $b < \beta(a)$ that

$$in+(b_0+i) \leq (n-a_0-k)n+(n-a_0).$$

Then, $i \leq n-a_0-k$ and if the equality $i = n-a_0-k$ holds, then $b_0+i \leq n-a_0$, that is, $b_0 \leq k$. Therefore, $b < \beta(a)$, $c < \beta(b)$ and $a < \beta(c)$ give

$$\begin{cases} i \leq n-a_0-k \\ j \leq n-b_0-i \\ k \leq n-c_0-j \end{cases} \tag{3.6}$$

and

$$\begin{cases} i = n-a_0-k \Rightarrow b_0 \leq k \\ j = n-b_0-i \Rightarrow c_0 \leq i \\ k = n-c_0-j \Rightarrow a_0 \leq j. \end{cases} \tag{3.7}$$

It follows from $a < \beta^{-1}(b)$ that

$$kn+(a_0+k) \leq (b_0-1)n+(n-i-1).$$

Then, $k \leq b_0-1$ and if the equality $k = b_0-1$ holds, then $a_0+k \leq n-i-1$, that is, $a_0+b_0 \leq n-i$. Therefore, $a < \beta^{-1}(b)$, $b < \beta^{-1}(c)$ and $c < \beta^{-1}(a)$ give

$$\begin{cases} k \leq b_0-1 \\ i \leq c_0-1 \\ j \leq a_0-1 \end{cases} \tag{3.8}$$

and

$$\begin{cases} k = b_0-1 \Rightarrow a_0+b_0 \leq n-i \\ i = c_0-1 \Rightarrow b_0+c_0 \leq n-j \\ j = a_0-1 \Rightarrow c_0+a_0 \leq n-k. \end{cases} \tag{3.9}$$

Consider $d := i+j+k$ and $e := r+s+t$ where

$$r := a_0-j-1$$

$$s := b_0-k-1$$

$$t := c_0-i-1.$$

Thus,

$$a = k(n+1)+j+r+1$$

$$b = i(n+1)+k+s+1$$

$$c = j(n+1)+i+t+1.$$

By (3.8), $s \geq 0$, $t \geq 0$ and $r \geq 0$.

Claim 1: $d \leq n-2$. To prove this, first consider the case $e = 0$, that is, $r = s = t = 0$. Then, (3.9) means

$$\begin{cases} s = 0 \Rightarrow a_0+b_0 \leq n-i \\ t = 0 \Rightarrow b_0+c_0 \leq n-j \\ r = 0 \Rightarrow c_0+a_0 \leq n-k. \end{cases}$$

Adding the three above inequalities, we get

$$2(a_0+b_0+c_0) \leq 3n-d,$$

that is, $2(d+e+3) \leq 3n-d$, hence, $d \leq n-2$.
Now, suppose that $e>0$. By (3.6), $d \leq 3n-(d+e+3)-d$, that is, $d \leq n-1-\frac{e}{3}$. Hence, $d \leq n-2$.
Claim 2: $r,s,t \in \{0,\ldots,n-2-d\}$.
By (3.6), $i \leq n-a_0-k$. Suppose by contradiction that $i=n-a_0-k$, then by (3.7), $b_0 \leq k$, that is, $s+k+1 \leq k$, then $s<0$, contradiction. Hence,

$$i < n-a_0-k.$$

It means that $i+j+k<n-1-r$, that is, $r \leq n-2-d$. Analogously, the inequalities $j<n-b_0-i$ and $k<n-c_0-j$ imply that $s,t \in \{0,\ldots,n-2-d\}$. This finishes the proof. □

Proposition 3.2.9. The number of pure gaps at $(\mathcal{P}_1,\mathcal{P}_2,\mathcal{P}_3)$ is $\frac{1}{120}(n-1)n(n+1)(n+2)(n^2+n-1)$.

Proof. We need to count the number of elements in $\mathbb{S}$. For each $d \in \{0,\ldots,n-2\}$, the number of triples (r,s,t) with $r,s,t \in \{0,\ldots,n-2-d\}$ is $(n-d-1)^3$ and the number of triples $(i,j,k) \in \mathbb{N}_0^3$ with $i+j+k=d$ is

$$\binom{d+2}{2} = \frac{1}{2}(d+1)(d+2).$$

Hence, the number of pure gaps at $(\mathcal{P}_1,\mathcal{P}_2,\mathcal{P}_3)$ is

$$\sum_{d=0}^{n-2} \frac{1}{2}(d+1)(d+2)(n-(d+1))^3 = \frac{1}{2}\sum_{t=1}^{n-1} t(t+1)(n-t)^3 = \frac{1}{120}(n-1)n(n+1)(n+2)(n^2+n-1).$$

□

Example 3.2.10. Let $q=61$ and consider the $\mathbb{F}_{q^2}$-maximal curve $\mathcal{X}$ of genus 15 defined by

$$X_0X_1^6+X_1X_2^6+X_2X_0^6=0.$$

The gaps of $\mathcal{X}$ at one point of $\{\mathcal{P}_1,\mathcal{P}_2,\mathcal{P}_3\}$ are given by

$$G(\mathcal{P}_i) = \{1,2,3,4,5,7,8,9,10,13,14,15,19,20,25\}$$

and the function $\beta : G(\mathcal{P}_1) \to G(\mathcal{P}_2)$ is given by

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ & 7 & 8 & 9 & 10 \\ & & 13 & 14 & 15 \\ & & & 19 & 20 \\ & & & & 25 \end{array} \quad \xrightarrow{\beta} \quad \begin{array}{ccccc} 25 & 19 & 13 & 7 & 1 \\ & 20 & 14 & 8 & 2 \\ & & 15 & 9 & 3 \\ & & & 10 & 4 \\ & & & & 5 \end{array}$$

It follows from Proposition 3.2.9 that

$$\#G_0(\mathcal{P}_1,\mathcal{P}_2,\mathcal{P}_3) = 203.$$

These results are displayed in Figure 2, where the red points represent the pure gaps at $(\mathcal{P}_1,\mathcal{P}_2,\mathcal{P}_3)$.

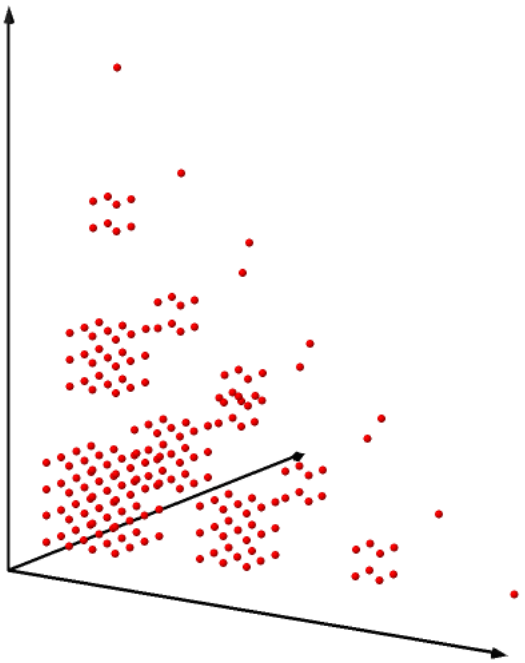

Figure 2 – The pure gaps at $(\mathcal{P}_1,\mathcal{P}_2,\mathcal{P}_3)$

3.3 Goppa codes supported by two points

As an application on the pure gaps results, we will construct Goppa codes supported by two points with good bound on the minimum distance. Let

$$\mathcal{X}\colon a_1XY^{n+1} + a_2ZX^{n+1} + a_3YZ^{n+1} + XYZ\cdot G(X,Y,Z) = 0$$

be a nonsingular curve defined over $\mathbb{F}_q$ with $n^2+n+1 \not\equiv 0 \pmod{p}$ and $a_1a_2a_3 \neq 0$. Let $P_1 = (1:0:0)$ and $P_2 = (0:1:0)$. It follows from Theorem 3.1.6 that the pairs

$$(\alpha_1,\alpha_2) = ((i-1)n+i,(j-1)n+i+j-1) \text{ and } (\beta_1,\beta_2) = (in-j,jn)$$

are pure gaps at (P_1,P_2), for $1 < i+j \leq n$. Choose mutually distinct m-points, say $Q_1,\ldots,Q_m$ from $\mathcal{X}(\mathbb{F}_q)\setminus\{P_1,P_2\}$ and consider the divisors $D := Q_1+\cdots+Q_m$ and

$$F := (\alpha_1+\beta_1-1)P_1 + (\alpha_2+\beta_2-1)P_2.$$

Let $C_\Omega(D,F)$ be the Goppa code supported by (P_1,P_2). With this notation we have the following result.

Theorem 3.3.1. If $\frac{n+3}{2} \leq i+j \leq n$ and $m > 2n^2-3$ then $i(F)=0$ and $\ell(F-D)=0$; hence $C_\Omega(D,F)$ is a code with

$$\text{length}(C_\Omega(D,F)) = m,$$

$$\dim C_\Omega(D,F) = m + \frac{1}{2}n^2 + \left(\frac{5}{2} - 2(i+j)\right)n - 2i + 2,$$

$$d_\Omega(D,F) \geq -n^2 + (2(i+j)-1)n - 2j + 2.$$

Proof. The length of $C_\Omega(D,F)$ is $\deg(D) = m$. Since $\frac{(n+3)}{2} \leq i+j$ implies that $\deg(F) > 2g-2$, where $g = n(n+1)/2$ is the genus of $\mathcal{X}$, we have $i(F)=0$. Moreover, $m > 2n^2-3$ implies that $\deg(F-D) < 0$, then $\ell(F-D)=0$. Hence,

$$\dim C_\Omega(D,F) = i(F-D) - i(F) = i(F-D) =$$

$$\ell(F-D) - \deg(F-D) + g - 1 = \deg(D) - \deg(F) + g - 1 =$$

$$m + \frac{1}{2}n^2 + \left(\frac{5}{2} - 2(i+j)\right)n - 2i + 2.$$

By (HOMMA; KIM, 2001, Theorem 3.3), $d_\Omega(D,F) \geq \deg(F) - (2g-2) + t_1 + t_2 + 2$, where $t_i = \beta_i - \alpha_i$ $(i = 1,2)$. Therefore,

$$d_\Omega(D,F) \geq -n^2 + (2(i+j)-1)n - 2j + 2.$$

□

Example 3.3.2. Consider the Pellikaan curve $\mathcal{X}_q$ with homogeneous equation

$$X_0X_1^{q+1} + X_1X_2^{q+1} + X_2X_0^{q+1} = 0$$

defined over $\mathbb{F}_q$. Let $P_1 = (1:0:0)$, $P_2 = (0:1:0)$ and $Q_1, \ldots, Q_m$ mutually distinct m-points such that $\{Q_1, \ldots, Q_m\} = \mathcal{X}_q(\mathbb{F}_{q^3}) \setminus \{P_1, P_2\}$. Set

$$D := Q_1 + \cdots + Q_m.$$

Given integers i, j with $\frac{(q+3)}{2} \leq i+j \leq q$, consider the pure gaps

$$(\alpha_1, \alpha_2) = ((i-1)q + i, (j-1)q + i + j - 1)$$

$$(\beta_1, \beta_2) = (iq - j, jq)$$

and the divisor

$$F = (\alpha_1 + \beta_1 - 1)P_1 + (\alpha_2 + \beta_2 - 1)P_2.$$

The number of $\mathbb{F}_{q^3}$-rational points of $\mathcal{X}_q$ is equal to

$$2q^3 + 1 + (1 - \varepsilon_q)(q^2 + q + 1),$$

where ε_q is the remainder in $\{0,1,2\}$ of $q+1$ modulo 3, see (PELLIKAAN, 1998, Theorem 3.6). Since $m = 2q^3 - 1 + (1-\varepsilon_q)(q^2+q+1)$, Theorem 3.3.1 implies that $C_\Omega(D,F)$ is a code with

$$\dim C_\Omega(D,F) = 2q^3 + \frac{1}{2}q^2 - \left(2(i+j) - \frac{5}{2}\right)q - 2i + 1 + (1-\varepsilon_q)(q^2+q+1),$$

$$\text{length}(C_\Omega(D,F)) = 2q^3 - 1 + (1-\varepsilon_q)(q^2+q+1),$$

$$d_\Omega(D,F) \geq -q^2 + 2\left(i+j-\frac{1}{2}\right)q - 2j + 2.$$

Example 3.3.3. Consider the Hurwitz curve $\mathcal{C}$ with equation

$$X_0X_1^q + X_1X_2^q + X_2X_0^q = 0$$

defined over $\mathbb{F}_q$. Let $P_1 = (1:0:0)$, $P_2 = (0:1:0)$ and $Q_1, \ldots, Q_m$ mutually distinct m-points such that $\{Q_1, \ldots, Q_m\} = \mathcal{C}(\mathbb{F}_{q^6}) \setminus \{P_1, P_2\}$. Set

$$D := Q_1 + \cdots + Q_m.$$

Given integers i, j with $\frac{(q+2)}{2} \leq i + j \leq q-1$, consider the pure gaps

$$(\alpha_1, \alpha_2) = ((i-1)(q-1) + i, (j-1)(q-1) + i + j - 1)$$

$$(\beta_1, \beta_2) = (i(q-1) - j, j(q-1))$$

and the divisor

$$F = (\alpha_1 + \beta_1 - 1)P_1 + (\alpha_2 + \beta_2 - 1)P_2.$$

By (COSSIDENTE; KORCHMÁROS; TORRES, 1999, Proposition 4.6), $\mathcal{C}$ is $\mathbb{F}_{q^3}$-isomorphic to the Hermitian curve

$$x^{q+1} + y^{q+1} + z^{q+1} = 0.$$

Since $\mathcal{C}$ is $\mathbb{F}_{q^6}$-maximal, it has $q^6 + q^5 - q^4 + 1$ $\mathbb{F}_{q^6}$-rational points. Hence, $\deg(D) = q^6 + q^5 - q^4 - 1$. It follows from Theorem 3.3.1 that $C_\Omega(D,F)$ is a code with

$$\dim C_\Omega(D,F) = q^6 + q^5 - q^4 + \frac{1}{2}q^2 + \left(\frac{3}{2} - 2(i+j)\right)q + 2j - 1,$$

$$\text{length}(C_\Omega(D,F)) = q^6 + q^5 - q^4 - 1,$$

$$d_\Omega(D,F) \geq -q^2 + (2(i+j)+1)q - 2i - 4j + 2.$$

3.4 Goppa codes supported by three points

In order to construct Goppa codes of $\mathcal{X}$ supported by three points, let $P_1 = (1:0:0), P_2 = (0:1:0), P_3 = (0:0:1)$. Observe that $(n_1,n_2,n_3) = (n^2-n-1, n-1, 1)$ and $(p_1,p_2,p_3) = (1, n^2-n-1, n-1)$ belong to $\mathbb{S}$, and therefore both are pure gaps at (P_1,P_2,P_3). Choose mutually

distinct m-points, say $Q_1,\ldots,Q_m$ from $\mathcal{X}(\mathbb{F}_q)\setminus\{P_1,P_2,P_3\}$ and consider the divisors $D:=Q_1+\cdots+Q_m$ and

$$F:=\sum_{i=1}^{3}(n_i+p_i-1)P_i.$$

Let $C_\Omega(D,F)$ be the Goppa code supported by (P_1,P_2,P_3). With this notation we have the following result.

Theorem 3.4.1. If $n\geq 3$ and $m>2n^2-5$ then $i(F)=0$ and $\ell(F-D)=0$; hence the Goppa code $C_\Omega(D,F)$ satisfies

$$\begin{aligned}\text{length}(C_\Omega(D,F))&=m,\\ \dim C_\Omega(D,F)&=m-\frac{3}{2}n^2+\frac{1}{2}n+4,\\ d_\Omega(D,F)&\geq n^2-n.\end{aligned}$$

Proof. Clearly, $\text{length}(C_\Omega(D,F))=\deg(D)=m$. Note that, $\deg(F)=2n^2-5>2g-2$, where $g=n(n+1)/2$ is the genus of $\mathcal{X}$, then $i(F)=0$. Moreover, $m>2n^2-5$ implies that $\deg(F-D)<0$, then $\ell(F-D)=0$. Hence,

$$\dim C_\Omega(D,F)=i(F-D)-i(F)=i(F-D)=$$

$$\ell(F-D)-\deg(F-D)+g-1=\deg(D)-\deg(F)+g-1=m-\frac{3}{2}n^2+\frac{1}{2}n+4.$$

By (CARVALHO; TORRES, 2005, Theorem 3.3),

$$d_\Omega(D,F)\geq\deg(F)-(2g-2)+3=n^2-n.$$

□

Example 3.4.2. Let $\mathcal{X}_q$ be the Pellikaan curve with equation

$$X_0X_1^{q+1}+X_1X_2^{q+1}+X_2X_0^{q+1}=0$$

defined over $\mathbb{F}_q$. Let $P_1=(1:0:0)$, $P_2=(0:1:0)$, $P_3=(0:0:1)$ and $Q_1,\ldots,Q_m$ mutually distinct m-points such that $\{Q_1,\ldots,Q_m\}=\mathcal{X}_q(\mathbb{F}_{q^3})\setminus\{P_1,P_2,P_3\}$ and consider the two pure gaps $(n_1,n_2,n_3)=(q^2-q-1,q-1,1)$ and $(p_1,p_2,p_3)=(1,q^2-q-1,q-1)$ of $\mathcal{X}_q$ at (P_1,P_2,P_3). Set $D:=Q_1+\cdots+Q_m$ and

$$F:=\sum_{i=1}^{3}(n_i+p_i-1)P_i.$$

The number of $\mathbb{F}_{q^3}$-rational points of $\mathcal{X}_q$ is equal to

$$2q^3+1+(1-\varepsilon_q)(q^2+q+1),$$

where ε_q is the remainder in $\{0,1,2\}$ of $q+1$ modulo 3, see (PELLIKAAN, 1998, Theorem 3.6). Hence, by Theorem 3.4.1, $C_\Omega(D,F)$ is a code with

$$\text{length}(C_\Omega(D,F))=2q^3-2+(1-\varepsilon_q)(q^2+q+1),$$

$$\dim C_\Omega(D,F) = 2q^3 - \frac{3}{2}q^2 - \frac{1}{2}q + 2 + (1-\varepsilon_q)(q^2+q+1),$$
$$d_\Omega(D,F) \geq q^2 - q.$$

Example 3.4.3. Let $\mathcal{C}$ be the Hurwitz curve of degree $q+1$ with equation

$$X_0X_1^q + X_1X_2^q + X_2X_0^q = 0$$

defined over $\mathbb{F}_q$. Let $P_1 = (1:0:0)$, $P_2 = (0:1:0)$, $P_3 = (0:0:1)$ and $Q_1,\ldots,Q_m$ mutually distinct m-points such that $\{Q_1,\ldots,Q_m\} = \mathcal{C}(\mathbb{F}_{q^6}) \setminus \{P_1,P_2,P_3\}$. Consider the two pure gaps $(n_1,n_2,n_3) = (q^2-3q+1, q-2, 1)$ and $(p_1,p_2,p_3) = (1, q^2-3q+1, q-2)$ of $\mathcal{C}$ at (P_1,P_2,P_3). Set $D := Q_1 + \cdots + Q_m$ and

$$F := \sum_{i=1}^{3} (n_i + p_i - 1)P_i.$$

By (COSSIDENTE; KORCHMÁROS; TORRES, 1999, Proposition 4.6), $\mathcal{C}$ is $\mathbb{F}_{q^3}$-isomorphic to the Hermitian curve

$$x^{q+1} + y^{q+1} + z^{q+1} = 0.$$

Since $\mathcal{C}$ is $\mathbb{F}_{q^6}$-maximal, it has $q^6+q^5-q^4+1$ $\mathbb{F}_{q^6}$-rational points. Hence, $m = q^6+q^5-q^4-2$. It follows from Theorem 3.4.1 that $C_\Omega(D,F)$ is a code with

$$\text{length}(C_\Omega(D,F)) = q^6+q^5-q^4-2,$$
$$\dim C_\Omega(D,F) = q^6+q^5-q^4-\frac{3}{2}q^2+\frac{7}{2}q,$$
$$d_\Omega(D,F) \geq q^2-3q+2.$$

BIBLIOGRAPHY

ABATANGELO, V.; KORCHMÁROS, G. Irreducible hypersurfaces of minimal degree containing all points of a finite projective space over a finite field. **Trends in incidence and Galois geometries: a tribute to Giuseppe Tallini**, v. 19, p. 1–17, 2009. Citations on pages 18 and 31.

ARBARELLO, E.; CORNALBA, M.; GRIFFITHS, P.; HARRIS, J. **Geometry of algebraic curves**. [S.l.]: Springer-Verlag, 1985. Citation on page 17.

BARS, F. Automorphism groups of genus 3 curves. **Notes del Seminari de Teoria Nombres UB-UAB-UPC**, v. 5, 2004. Citation on page 44.

CARVALHO, C.; TORRES, F. On goppa codes and weierstrass gaps at several points. **Des. Codes and Cryptogr.**, v. 35, p. 211–225, 2005. Citations on pages 18, 27, 28, 43, and 61.

COSSIDENTE, A.; KORCHMÁROS, G.; TORRES, F. On curves covered by the hermitian curve. **J. Algebra**, v. 216, p. 56–76, 1999. Citations on pages 60 and 62.

CUNHA, G. D. Curves containing all points of a finite projective galois plane. **Journal of Pure and Applied Algebra**, p. –, 2017. ISSN 0022-4049. Available: <https://www.sciencedirect.com/science/article/pii/S0022404917302736>. Citation on page 19.

GARCIA, A.; KIM, S. J.; LAX, R. F. Consecutive weierstrass gaps and minimum distance of goppa codes. **Journal of Pure and Applied Algebra**, v. 84, p. 199–207, 1993. Citation on page 43.

GARCIA, A.; LAX, R. F. Goppa codes and weierstrass gaps. In: ____. **Coding Theory and Algebraic Geometry: Proceedings of the International Workshop held in Luminy, France, June 17–21, 1991**. Berlin, Heidelberg: Springer Berlin Heidelberg, 1992. p. 33–42. ISBN 978-3-540-47267-4. Available: <https://doi.org/10.1007/BFb0087991>. Citation on page 43.

GOPPA, V. Codes associated with divisors. **Problemy Peredachi Informatsii**, v. 13, p. 33–39, 1977. Citations on pages 17, 25, and 43.

____. **Geometry and Codes**. [S.l.]: Kluwer Academic Publishers, 1988. (Mathematics and its applications). Citations on pages 17 and 25.

GORENSTEIN, D. An arithmetic theory of adjoint plane curves. **Trans. Amer. Math Soc.**, v. 72, p. 414–436, 1952. Citation on page 41.

HASSE, H.; WITT, E. Zyklische unverzweigte erweiterungskörper vom primzahlgrade p über einen algebraischen funktionenkörper der characteristik p. **Monatsh. Math. Phys.**, v. 43, p. 477–492, 1936. Citation on page 29.

HIRSCHFELD, J.; KORCHMÁROS, G.; TORRES, F. **Algebraic Curves Over a Finite Field**. Princeton: Princeton University Press, 2008. Citations on pages 23, 27, 28, 29, 30, 31, 35, and 45.

HOMMA, M. The weierstrass semigroup of a pair of points on a curve. **Arch. Math.**, v. 67, p. 337–348, 1996. Citation on page 17.

HOMMA, M.; KIM, S. Nonsingular plane filling curves of minimum degree over a finite field and their automorphism groups: supplements to a work of tallini. **Linear Algebra Appl.**, v. 438, p. 969–985, 2013. Citations on pages 18, 31, 32, and 33.

HOMMA, M.; KIM, S. J. Goppa codes with weierstrass pairs. **Journal of Pure and Applied Algebra**, v. 162, n. 2-3, p. 273–290, 2001. Citations on pages 17, 18, 20, 43, 46, 48, and 59.

____. Around sziklai's conjecture on the number of points of a plane curve over a finite field. **Finite Fields Appl**, v. 15, p. 468–474, 2009. Citation on page 32.

KIM, S. J. On the index of the weierstrass semigroup of a pair of points on a curve. **Arch. Math.**, v. 62, p. 73–82, 1994. Citations on pages 17 and 46.

MONTANUCCI, M.; SPEZIALI, P. The a-numbers of fermat and hurwitz curves. **Journal of Pure and Applied Algebra**, v. 222, n. 2, p. 477–488, 2016. Citations on pages 19 and 32.

NOETHER, M. Note über die algebraischen curven, welche eine schaar eindeutiger transformationen in sich zulassen. **Math. Ann.**, XX, p. 59–62, 1882. Citation on page 17.

____. Nachtrag zur "note über die algebraischen curven, welche eine schaar eindeutiger transformationen in sich zulassen. **Math. Ann.**, XXI, p. 138–140, 1883. Citation on page 17.

PELLIKAAN, R. The klein quartic, the fano plane and curves representing designs. In: ____. **Codes, Curves, and Signals: Common Threads in Communications**. Boston, MA: Springer US, 1998. p. 9–20. Available: <https://doi.org/10.1007/978-1-4615-5121-8_2>. Citations on pages 19, 32, 60, and 61.

POINCARÉ, H. Sur un théorème de m. fuchs. **C. R. Ac. Sc Paris**, v. 99, p. 75–77, 1884. Citation on page 17.

SCHMIDT, F. K. Zur arithmetischen theorie der algebraischen functionen ii. **Math. Zeitschrift**, v. 45, p. 75–96, 1939. Citation on page 17.

SCHWARZ, A. über diejenigen algebraischen gleichungen zwischen zwei veränderlichen. **Math. Ann.**, v. 87, p. 139–145, 1879. Citation on page 17.

STICHTENOTH, H. **Algebraic Function Fields and Codes**. 2. ed. [S.l.]: Springer-Verlag, 2008. (Graduate Texts in Mathematics, v. 254). Citations on pages 21, 22, 24, 25, and 26.

TALLINI, G. Le ipersuperficie irriducibili d'ordine minimo che invadono uno spazio di galois. **Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat.**, v. 30, n. 8, p. 706–712, 1961. Citations on pages 18, 31, and 32.

____. Sulle ipersuperfici irriducibili d'ordine minimo che contengono tutti i punti di uno spazio di galois $s_{r,q}$. **Rend. Mat. e Appl.**, v. 20, n. 5, p. 431–479, 1961. Citations on pages 18, 31, 32, and 33.


ICMC
USP
SÃO CARLOS