Matteo Bonini

Intersections of Algebraic Curves and their link to the weight enumerators of Algebraic-Geometric Codes

Dottorato in Matematica, Trento (2019).

<http://www.bdim.eu/item?id=tesi_2019_BoniniMatteo_1>

UNIVERSITÀ DEGLI STUDI DI TRENTO

Dipartimento di Matematica

DOTTORATO DI RICERCA IN MATEMATICA

XXXI CICLO

A thesis submitted for the degree of Doctor of Philosophy

Matteo Bonini

Intersections of Algebraic Curves and their link to the weight enumerators of Algebraic-Geometric Codes

Supervisor:

Prof. Massimiliano Sala

Dott. Giancarlo Rinaldo

Introduction

Channel coding is the branch of Information Theory which studies the noise that can occur in data transmitted through a channel. Algebraic Coding Theory is the part of Channel Coding which studies the possibility to detect and correct errors using algebraic and geometric techniques. Nowadays, the best performing linear codes are known to be mostly algebraic geometry codes, also named Goppa codes, which arise from an algebraic curve over a finite field, by the pioneering construction due to V. D. Goppa. The best choices for curves on which Goppa's construction and its variants may provide codes with good parameters are those with many rational points, especially maximal curves attaining the Hasse-Weil upper bound for the number of rational points compared with the genus of the curve. Unfortunately, maximal curves are difficult to find. The best known examples of maximal curves are the Hermitian curve, the Ree curve, the Suzuki curve, the GK curve and the GGS curve.

In the present thesis, we construct and investigate algebraic geometry codes (shortly AG codes), their parameters and automorphism groups.

In the first part, mostly dedicated to background and preliminary results, we collect basic facts on algebraic function fields, and give a purely algebraic description of Goppa's method. An advantage is that the principal tools in Goppa's construction, that is, the Riemann-Roch theorem and its corollaries, can be more quickly introduced in the function field setting rather than within Algebraic Geometry. We also report some basic definitions from classic Algebraic Geometry, in particular we introduce the notion of an algebraic curve $\mathcal{X}$ in a projective space over a finite field $\mathbb{F}_q$. We also explain how these geometric concepts are related to algebraic concepts in the corresponding function field $K(\mathcal{X})$. Afterwards, we point out that combining the algebraic and geometric ideas and tools can provide algebraic-geometric codes whose parameters are often better than those of other codes.

The original idea of Goppa was to construct a code C on the set $\mathcal{X}(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points of a curve $\mathcal{X}$, from two divisors D and G whose supports are two disjoint subsets of $\mathcal{X}(\mathbb{F}_q)$. Here the length of C coincides with |Supp(D)|, while its dimension is upper bounded by the dimension of the Riemann-Roch space $\mathcal{L}(D)$. The current literature on Coding Theory is rich of various constructions but only a few of them give useful information on the minimum distance of the code. Fortunately algebraic geometry codes are of this latter kind, since a lower bound, called the designed minimum distance, can easily been computed when $\mathcal{X}(\mathbb{F}_q)$ is large enough. In many cases, the designed minimum distance coincides with its true value. Since long codes are better for correcting errors, we are interested in studying curves with many $\mathbb{F}_q$-rational points. It should be noticed that such curves (especially maximal curves) often have large automorphism group. Curves enjoying large automorphism group include the well-known 1-dimensional Deligne Lusztig varieties (the Hermitian, Suzuki and Ree curves) together with the more recent GK curve and Norm-Trace curve, the last being a natural generalization of Hermitian curve.

The second part of the thesis presents the original results. In the fourth chapter, the automorphism group of the abovementioned curves are discussed. Their automorphism group is known, except for the Norm-trace curve. We focus on the automorphism group of the Norm-trace curve, which we determine here. We also use it to construct multi-point algebraic-geometric codes which turn out be monomially equivalent to one-point codes. Since the automorphisms of the curve which preserve both divisors in Goppa's construction is induced by the arising algebraic-geometry code, these multi-point algebraic-geometric codes have a large automorphism group. This is a very useful property for the decoding process, as codes with a large automorphism groups often admit quicker decoding. The main results of these chapter appear in a joint work with M. Montanucci and G. Zini, see [10].

In the fifth and the sixth chapters, we investigate the general problem of determining the minimum distance and the weight enumerator polynomial of algebraic-geometric codes. We adopt an approach based on the intersection of the curve defining the code and other curves. More in details, the first part of the fifth chapter deals with the GK-curve. It should be noticed that the GK-curve is the first maximal curve shown not to be covered by the

Hermitian curve. In the same section, we compute the maximal number of intersections that the GK curve can have with a plane curve of degree lower or equal to three. The results are used to determine the minimum distance and the number of minimum weight codewords of one-point AG-codes arising from the GK-curve. The main results appeared in a joint paper with D. Bartoli; see [5].

The second part of the fifth chapter is based on a joint work with L. Girardi and M. Sala. Our aim is to extend the results of the previous section to a generalization of the GK-curve, due to A. Garcia, C. Güneri and H. Stichtenoth. We apply some techniques, similar to those used in the previous section, to the study of the number of intersections between a line and the GGS curve. Unfortunately, this curve has singularity in its point at the infinity, which does not allow us to proceed analogously. We obtain an upper bound for the minimum distance of some AG-codes arising from the GGS curve.

In the final chapter, which comes from a joint work with M. Sala (see [11]), we study the possible intersections between the Norm-Trace curve and a plane curve with equation of the form $y = ax^3 + bx^2 + cx + d$. One aim is to extend the results obtained in [50]. We have not been able to determine the full spectrum of the intersections between these two curves. Nevertheless, we obtain sharp bounds. For this purpose, we translate the problem of finding the intersection of these two curves into that of determining the $\mathbb{F}_q$-rational points of a certain cubic surface. We treat differently the smooth and singular cases using a variety of both theoretical and applied results: such as the classification of the singularities of a cubic irreducible surface, the Cremona map and elimination ideals. Moreover, the solution of some particular cases of our investigation was also supported by the software MAGMA.

Contents

List of Notations

$\mathbb{P}_F$	set of the places of F/K
v_P	valuation corresponding to a place
P_∞	the infinite place of $K(x)$
$\mathrm{Div}(F)$	divisor group of F
$\mathrm{supp}(D)$	support of D
$\deg(D)$	degree of D
g	the genus of F
$\mathcal{L}(D)$	Riemann-Roch space of D
$\ell(D)$	dimension of $\mathcal{L}(D)$
Ω_F	space of Weil differentials of F
$\mathrm{res}_P(\omega)$	residue of ω at the place P
$\mathbb{F}_q$	the finite field with q elements
$\mathcal{X}(\mathbb{F}_q)$	the set of $\mathbb{F}_q$-rational places on $\mathcal{X}$
$\overline{K}$	the algebraic closure of the field K
$\mathbb{A}^n_K$	the n-dimensional affine space over K
$\mathbb{P}^n_K$	the n-dimensional projective space over K
$\mathrm{Aut}(\mathcal{X})$	the automorphism group of the curve $\mathcal{X}$
$G \rtimes H$	semidirect product between G and H
$d(a,b)$	Hamming distance between a and b
$\mathrm{w}(a)$	Hamming weight of a
$d(C)$	distance of the code C
$C^\perp$	the dual code of C
$C_\mathcal{L}(D,G)$	the algebraic geometry code associated to the divisors D and G
$C_\Omega(D,G)$	the differential code associated to the divisors D and G
$\mathrm{Aut}(C)$	the automorphism group of the code $\mathcal{C}$

Part I

Preliminaries

Chapter 1

Algebraic Function Fields

Algebraic function fields of one variable arise naturally in the study of algebraic curves. Branches of a curve (or points of a nonsingular model of the curve) are bijectively associated to places of a function field, the property of singularity can be verified studying the valuation ring of a the associated place.

In this chapter we introduce the basic definitions and results of the theory of function fields: places, valuations, divisors, genus, adeles, Weil differential and the Riemann-Roch theorem. We present algebraic extensions of function fields, one of the most important tools for working with concrete function fields, and also decomposition of places in a finite extension, ramification index and Hurwitz genus formula. These tools are useful for the computation of the genus and the number of rational points on the associated curves.

In our applications the base field is always finite. The theory of function fields is developed for an arbitrary ground field K, except for the section on the extensions, where K is assumed to be perfect. We recall that K is called perfect if all algebraic extension L/K are separable. For example K is perfect if the field has characteristic zero, it is algebraically closed or it is finite.

For details and proof we refer to [65].

1.1 Places and valuations

Definition 1.1. An *algebraic function field* F/K of one variable over K is an extension field $F \supset K$ such that F is a finite algebraic extension of $K(x)$ for some $x \in F$, with x is transcendental over K.

We call $\widetilde{K} = \{z \in F \mid z \text{ algebraic over } K\}$ the *field of constants* of F/K. The field K is said to be algebraically closed in F if $\tilde{K} = K$. Note that $F/\tilde{K}$ is a function field over $\tilde{K}$.

Definition 1.2. A *valuation ring of the function field* F/K is a proper subring $K \subsetneq \mathcal{O} \subsetneq F$ such that for every $z \in F$ we have that $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.

A valuation ring $\mathcal{O}$ of F/K has the following properties:

(i) $\mathcal{O}$ is a local ring, with unique maximal ideal $P = \mathcal{O} \setminus \mathcal{O}^*$, where $\mathcal{O}^*$ is the group of units of $\mathcal{O}$;

(ii) for each $z \in F \setminus \{0\}$, then $z \in P \iff z^{-1} \notin \mathcal{O}$;

(iii) $\tilde{K} \subset \mathcal{O}$ and $\tilde{K} \cap P = \{0\}$;

(iv) $\mathcal{O}$ is a principal ideal domain (shortly PID);

(v) let $t \in P$ be a generator for P, then every element z in $F \setminus \{0\}$ can be written in the form $z = t^n u$, where $u \in \mathcal{O}^*$.

Thus $\mathcal{O}$ is also a discrete valuation ring, that is a principal ideal domain with exactly one non-zero maximal ideal.

Definition 1.3. A *place* P of the function field F/K is the maximal ideal of some valuation ring $\mathcal{O}$ of F/K. An element $t \in P$ such that $P = t\mathcal{O}$ is called *uniformizer*. The set $\mathcal{O}_P := \{z \in F \mid z^{-1} \notin P\}$ is the *valuation ring of the place* P.

It can be proved that every function field has infinitely many places. The set of all places of a function field F/K is denoted with $\mathbb{P}_F$.

Definition 1.4. A *discrete valuation of the function field* F/K (shortly DVR) is a function $v : F \to \mathbb{Z} \cup \{\infty\}$ such that for every $x, y \in F$:

(i) $v(x) = \infty$ if and only if $x = 0$

(ii) $v(xy) = v(x) + v(y)$

(iii) $v(x + y) \geq \min\{v(x), v(y)\}$

(iv) there exists an element $z \in F$ such that $v(z) = 1$

(v) $v(a) = 0$, for all $a \in K \setminus \{0\}$

Proposition 1.5 (Strict Triangle Inequality)**.** *Let v be a discrete valuation of F/K and $x, y \in F$ with $v(x) \neq v(y)$. Then*

$$v(x + y) = \min\{v(x), v(y)\}.$$

Definition 1.6. Let P be a place and t be a uniformizer. We define a function $v_P : F \to \mathbb{Z} \cup \{\infty\}$ as follows: for every $z \in F \setminus \{0\}$ write $z = t^n u$, where u is a unity of $\mathcal{O}_P$ and $n \in \mathbb{Z}$, then $v_P(z) = n$ and $v_P(0) = \infty$.

Observe that this definition depends only on P, not on the choice of the uniformizer t, because all generators of P differ by a unit.

For a place P of F/K the function v_P described above is a discrete valuation. We have:

- $\mathcal{O}_P = \{z \in F \mid v_P(z) \geq 0\}$
- $\mathcal{O}_P^{\times} = \{z \in F \mid v_P(z) = 0\}$
- $P = \{z \in F \mid v_P(z) > 0\}$

An element $t \in P$ is a uniformizer for the place P if and only if $v_P(t) = 1$.

Conversely we can construct a place from a discrete valuation v for the function field F/K in this way: the set $P = \{z \in F \mid v(z) \geq 0\}$ is a place of F/K and $\mathcal{O}_P = \{z \in F \mid v(z) \geq 0\}$ is the corresponding valuation ring. For this reason we can say that places, valuation rings and discrete valuations of a function field essentially correspond to the same thing.

Let P be a place of F/K and let $\mathcal{O}_P$ be its valuation ring. Since P is a maximal ideal, the residue class ring $\mathcal{O}_P/P$ is a field. We know that $\widetilde{K} \subset \mathcal{O}_P$ and $\widetilde{K} \cap P = \{0\}$, so the residue class map $\mathcal{O}_P \to \mathcal{O}_P/P$ induces a canonical embedding of $\widetilde{K}$ into $\mathcal{O}_P/P$. Henceforth we shall always consider K and $\widetilde{K}$ as subfields of $\mathcal{O}_P/P$ via this embedding.

Definition 1.7. Let P be a place of F/K and $F_P := \mathcal{O}_P/P$ its residue class field. Then we define the *degree* of P to be $\deg(P) := [F_P : K]$. A place of degree one is called *rational place*.

Definition 1.8. Let $z \in F$, P a place of F/K, then

(i) if $v_P(z) = m > 0$, the place P is a *zero* of z of order m;

(ii) if $v_P(z) = -m < 0$, the place P is a *pole* of z of order m.

Proposition 1.9. *Let F/K be a function field, $z \in F \setminus \{0\}$, then:*

(i) z has only finitely many zeros and poles;

(ii) if z is transcendental over K, then z has at least one zero and one pole.

Example 1.10. *Let x be a transcendental element over the field K and let $F = K(x)$ be the* rational function field. *Let $p(x) \in K[x]$ an arbitrary monic, $p(x)$ irreducible polynomial, the set*

$$\mathcal{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)} \;\middle|\; f(x), g(x) \in K[x],\ \ p(x) \nmid g(x) \right\}$$

is a valuation ring *of $K(x)/K$. Its maximal ideal*

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)} \;\middle|\; f(x), g(x) \in K[x],\ \ p(x) \mid f(x),\ \ p(x) \nmid g(x) \right\}$$

is a place *of $K(x)/K$.*
Note that if $q(x)$ is another irreducible polynomial, then $\mathcal{O}_{p(x)} \neq \mathcal{O}_{q(x)}$.

There is another valuation ring of $K(x)/K$, namely

$$\mathcal{O}_\infty := \left\{ \frac{f(x)}{g(x)} \;\middle|\; f(x), g(x) \in K[x],\ \ \deg(f(x)) \leq \deg(g(x)) \right\}$$

with maximal ideal

$$P_\infty = \left\{ \frac{f(x)}{g(x)} \;\middle|\; f(x), g(x) \in K[x],\ \ \deg(f(x)) < \deg(g(x)) \right\}.$$

This is called the infinite *place of $K(x)$. Moreover, it is possible to prove the following properties*

(i) Let $P = P_{p(x)}$ be the place defined by the monic polynomial $p(x) \in K[x]$. Then $p(x)$ is a uniformizer, and the corresponding discrete valuation v_P can be described as follows: if $Z \in K(x) \setminus \{0\}$ is written in the form $z = (p(x))^n \cdot (f(x)/g(x))$, with $n \in \mathbb{Z}$, $f(x), g(x)$ polynomial of $K[x]$ that are not divided by $p(x)$, then $v_P(z) = n$. The residue class field $K(x)_P = \mathcal{O}_P/P$ is isomorphic to $K(x)/(p(x))$. Consequently, $\deg(P_{p(x)}) = \deg(p(x))$.

(ii) *In the special case $P = x - \alpha$, with $\alpha \in K$, the degree of $P = P_{x-\alpha}$ is one. For any $z \in K(x)$ write $z = f(x)/g(x)$, with relative prime polynomials $f(x), g(x) \in K[x]$. Then the residue class map is given by*

$$z(P) = \begin{cases} f(\alpha)/g(\alpha) & \text{if } g(\alpha) \neq 0, \\ \infty & \text{if } g(\alpha) = 0. \end{cases}$$

(iii) *In the special case $P = P_\infty$, the degree is one. A uniformizer for P_∞ is $t = 1/x$. For any $z \in K(x)$ write*

$$z = \frac{a_n x^n + \cdots + a_0}{b_m x^m + \cdots + b_0},$$

with $a_n, b_m \in K \setminus \{0\}$. Then the residue class map is given by

$$z(P_\infty) = \begin{cases} a_n/b_m, & \text{if } n = m, \\ 0 & \text{if } n < m, \\ \infty & \text{if } n > m. \end{cases}$$

(iv) *K is the full constant field of $K(x)/K$.*

(v) *There are no places of the rational function fields other than $P_{p(x)}$ and P_∞.*

(vi) *The places of $K(x)/K$ of degree one are in 1-1 correspondence with $K \cup \{\infty\}$.*

1.2 Divisors and Riemann-Roch Theorem

In this section we introduce divisors, the Riemann-Roch space and Weil differentials. These tools will be used to define the AG codes and to determine their parameters.

Remark 1.11. The field $\widetilde{K}$ of constants of an algebraic function field F/K is a finite extension field of K and F can be seen as a function field over $\tilde{K}$. Therefore from here on, F/K will always denote an algebraic function field of one variable such that K is the full constant field of F/K.

Definition 1.12. The *divisor group* of F/K is defined as the (additive) free abelian group which is generated by the places of F/K and it is denoted

by $\mathcal{D}_F$. The elements of $\mathcal{D}_F$ are called *divisors* of F/K. In other words, a *divisor* is a formal sum

$$D = \sum_{P \in \mathbb{P}_F} n_P P,$$

with $n_P \in \mathbb{Z}$, almost all $n_P = 0$.

We make a list of definitions and properties that will help us work with divisors.

(i) The *support* of D is defined as $Supp(D) = \{P \in \mathbb{P}_F \mid n_p \neq 0\}$.

(ii) A divisor of the form $D = P$ with $P \in \mathbb{P}_F$ is called *prime divisor*.

(iii) The sum of two divisors is defined as the sum componentwise: let $D = \sum n_P P$ and $D' = \sum n'_P P$, then

$$D + D' = \sum (n_P + n'_P) P.$$

(iv) The zero element of the divisor group $\mathcal{D}_F$ is the divisor

$$0 := \sum r_P P, \quad \text{all } r_P = 0.$$

(v) For $Q \in \mathbb{P}_F$ and $D = \sum n_P P \in \mathcal{D}_F$ we define $v_Q(D) := n_Q$.

(vi) A partial ordering on $\mathcal{D}_F$ is defined by:

$$D_1 \leq D_2 \iff v_P(D_1) \leq v_P(D_2), \quad \text{for all } P \in \mathbb{P}_F.$$

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

(viii) The *degree* of a divisor is defined as

$$\deg(D) := \sum v_P \deg(P).$$

(ix) The function $\deg : \mathcal{D}_F \to \mathbb{Z}$ is an homomorphism.

Definition 1.13. Let $f \in F \setminus \{0\}$ and denote by Z the set of zeros, N the set of poles of f in $\mathbb{P}_F$. Then we define

$$(f)_0 = \sum_{P \in Z} v_P(f) P, \quad \text{the } \textit{zero divisor} \text{ of } x;$$
$$(f)_\infty = \sum_{P \in N} (-v_P(f)) P, \quad \text{the } \textit{pole divisor} \text{ of } x;$$
$$(f) = (f)_0 - (f)_\infty = \sum_{P \in \mathbb{P}_F} (-v_P(f)) P, \quad \text{the } \textit{principal divisor} \text{ of } x.$$

Since we assumed K to be the full constant field, from Proposition 1.9 we have that if $f \in F$ enjoys $(f) = 0$, then $f \in K$.

Definition 1.14. For a divisor $D \in \mathcal{D}_F$ we define the *Riemann-Roch space* associated to D by

$$\mathcal{L}(D) = \{f \in F \mid (f) \geq -D\} \cup \{0\}.$$

An element $f \in F$ is contained in $\mathcal{L}(D)$ if and only if $v_P(f) \geq -v_P(A)$ for all $P \in \mathbb{P}_F$. If $D = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j$, with $n_i, m_j > 0$, then $\mathcal{L}(D)$ consists of all $f \in F$ such that:

(i) f has zeros of order greater or equal to m_j at Q_j $(j = 1 \dots s)$;

(ii) f may have poles only at the places $P_1, \dots, P_r$, with the pole order at P_i being bounded by n_i $(i = 1, \dots, r)$.

For every $D \in \mathcal{D}_F$ the Riemann-Roch space $\mathcal{L}(D)$ is a finite dimensional vector space over K. So we define the integer $\ell(D) = \mathcal{L}(D)$ to be the *dimension* of the divisor D. The following facts hold:

- $\mathcal{L}(0) = K$ and $\ell(0) = 1$;
- if $A < 0$, then $\mathcal{L}(A) = \{0\}$ and $\ell(A) = 0$;
- all principal divisors have degree zero and dimension one;
- if $\deg(D) < 0$, then $\mathcal{L}(D) = \{0\}$ and $\ell(D) = 0$.

Example 1.15. *Once again we consider the rational function field $F = K(x)$ as in Example 1.10. For $z \in K(x) \setminus \{0\}$ write $z = a \cdot f(x)/g(x)$ with $a \in K \setminus \{0\}$, $f(x), g(x) \in K[x]$ monic and relatively prime. Let*

$$f(x) = \prod_{i=1}^{r} p_i(x)^{n_i}, \quad g(x) = \prod_{j=1}^{s} q_j(x)^{m_j},$$

with pairwise distinct irreducible monic polynomials $p_i(x), q_j(x)$. Then the principal divisor of z in $\mathcal{D}_F$ is

$$(z) = \sum_{i=1}^{r} n_i P_{p_i(x)} - \sum_{j=0}^{s} m_j P_{q_j(x)} + (\deg(g) - \deg(f)) P_\infty.$$

Proposition 1.16. *There is a constant $\gamma \in \mathbb{Z}$ such that for all divisors $D \in \mathcal{D}_F$:*

$$\deg(D) - \ell(D) \leq \gamma.$$

Definition 1.17. The *genus* g of F/K is defined by

$$g := \max\{\deg(D) - \ell(D) + 1 \mid D \in \mathcal{D}_F\}.$$

We observe that this definition makes sense by the previous proposition. Moreover the genus is a non-negative integer; indeed consider the divisor 0, then $\deg(0) - \ell(0) + 1 = 0$.

Definition 1.18. An *adele* of F/K is a mapping $\alpha : \mathbb{P}_F \to F$ such that $\alpha(P) = \alpha_P \in \mathcal{O}_P$ for almost all $P \in \mathbb{P}_F$.

We regard an adele as an element of the direct product $\prod_{P \in \mathbb{P}_F} F$ and, therefore, use the notation $\alpha = (\alpha_P)$. The set $\mathcal{A}_F := \{\alpha \mid \alpha \text{ is an adele of } F/K\}$ is called the *adele space* of F/K. It is seen as a vector space over K. The *principal adele* of an element $x \in F$ is the adele all of whose components are equal to x. This gives an embedding of F into $\mathcal{A}_F$, called *diagonal embedding*. A valuation v_P of F/K extends naturally to $\mathcal{A}_F$ by setting $v_P(\alpha) = v_P(\alpha_P)$. By definition, $v_P(\alpha) \geq 0$ for almost all $P \in \mathbb{P}_F$.

Definition 1.19. For $D \in \mathcal{D}_F$ we define

$$\mathcal{A}_F(D) = \{\alpha \in \mathcal{A}_F \mid v_P(\alpha) \geq -v_P(D) \text{ for all } P \in \mathbb{P}_F\}.$$

Obviously, this is a K-subspace of $\mathcal{A}_F$. We define the *index of speciality* of the divisor D to be the integer

$$i(D) = \dim(\mathcal{A}_F/(\mathcal{A}_F(D) + F)).$$

Definition 1.20. A *Weil differential* of F/K is a K-linear map $\omega : \mathcal{A}_F \to K$ vanishing on $\mathcal{A}_F(D) + F$ for some divisor $D \in \mathcal{D}_F$.

We call $\Omega_F := \{\omega \mid \omega \text{ is a Weil differential of } F/K\}$. It is easy to prove that Ω_F is a vector space with respect to K. For $D \in \mathcal{D}_F$ let $\Omega_F(D) := \{\omega \mid \omega \text{ vanishes on } \mathcal{A}_F(D) + F\}$. Clearly it is a subspace of Ω_F and its dimension is exactly the index of speciality $i(D)$.

We intend to attach a divisor to any Weil differential $\omega \neq 0$. To this end, consider the set of divisors $M(\omega) := \{D \in \mathcal{D}_F \mid \omega \text{ vanishes on } \mathcal{A}_F(D) + F\}$.

There is a uniquely determined divisor $W \in M(\omega)$ such that $D \leq W$ for any $D \in M(\omega)$. Such element is called *canonical divisor* and denoted by (ω). Is easy to prove that

$$\Omega_F(D) = \{\omega \in \Omega_F \mid \omega = 0 \text{ or } (\omega) \geq D\}.$$

For any canonical divisor W, we have $\deg(W) = 2g - 2$ and $\ell(W) = g$.

Theorem 1.21 (Riemann-Roch Theorem)**.** *Let W be a canonical divisor of F/K. Then for any $D \in \mathcal{D}_F$,*

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

It can be proved that $\ell(W - D) = i(D)$, so another way to state the same theorem is

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

We note that if D is a divisor of F/K of degree strictly greater than $2g-2$, then $\deg(W-D) < 0$, so $\ell(W-D) = i(D) = 0$. Thus $\ell(D) = \deg(D)+1-g$.

Example 1.22. *As an application of the Riemann-Roch theorem, we want to show that the rational function field $K(x)/K$ has genus $g = 0$. Let P_∞ denote the pole divisor of x. Consider, for $r \geq 0$, the vector space $\mathcal{L}(rP_\infty)$; obviously, the elements $1, x, \ldots, x^r$ generate $\mathcal{L}(rP_\infty)$. Let $r > 2g - 2$, we have*

$$r + 1 \leq \ell(rP_\infty) = \deg(rP_\infty) + 1 - g = r + 1 - g.$$

Thus $g \leq 0$. Since $g \geq 0$ for any function field, the assertion follows.

The last thing we introduce is the residue of a differential at a place P.

Definition 1.23. Suppose that P is a place of F/K of degree one and $t \in F$ is a P-prime element. If $z \in F$ has the P-adic expansion $z = \sum_{i=n}^{\infty} a_i t^i$ with $n \in \mathbb{Z}$ and $a_i \in K$ we define its *residue* with respect to P and t by

$$\mathrm{res}_{P,t}(z) := a_{-1}.$$

Definition 1.24. Let $\omega \in \Omega_F$ be a differential and let $P \in \mathbb{P}_F$ be a place of degree one. Choose a P-prime element $t \in F$ and write $\omega = u\, dt$ with $u \in F$. Then we define the *residue* of ω at P by

$$\mathrm{res}_P(\omega) := \mathrm{res}_{P,t}(u).$$

1.3 Extension of algebraic function fields

Any function field over K can be seen as a finite field extension of a rational function field $K(x)$. This is one of the reasons why it is of interest to investigate field extensions F'/F of algebraic function fields. This section will give us the tools for the computation of the genus of some non-trivial function fields and to determine the discrete valuation associated with some places.

Two common types of extensions are Kummer extension and Artin-Schreier extensions. We summarize the main properties of these extensions in two theorems at the end of the section.

Remark 1.25. Throughout the whole subsection, K is assumed to be perfect.

Definition 1.26. An algebraic function field F'/K' is called an *algebraic extension* of F/K if $F' \supseteq F$ is an algebraic field extension and $K' \supseteq K$. A place $P' \in \mathbb{P}_{F'}$ is said to *lie over* $P \in \mathbb{P}_F$ if $P \subseteq P'$. We also say that P' is an *extension* of P, or that P *lies under* P', and write $P'|P$.

If $P \subset P'$ than also $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$. Moreover there exists an integer $e \geq 1$ such that $v_{P'}(z) = e \cdot v_P(z)$ for all $z \in F$. The integer e is called *ramification index* of P' over P and denoted by $e(P'|P)$.
We say that $P'|P$ is *ramified* if $e(P'|P) > 1$ and $P'|P$ is *unramified* if $e(P'|P) = 1$.

There is a canonical embedding of the residue class field $F_P = \mathcal{O}_P/P$ into the residue class field $F'_{P'} = \mathcal{O}_{P'}/P'$, therefore we can consider F_P as a subfield of $F'_{P'}$. The value $f(P'|P) := [F'_{P'} : F_P]$ is called the *relative degree* of P' over P.
Note that $f(P'|P)$ can be finite or infinite; in particular it is finite if and only if $[F' : F]$ is finite.

If F''/K'' is an algebraic extension of F'/K' and $P'' \in \mathbb{P}_{F''}$ lies over P', then

$$e(P''|P) = e(P''|P')e(P'|P),$$
$$f(P''|P) = f(P''|P')f(P'|P).$$

Proposition 1.27. *Let F'/K' be an algebraic extension of F/K. Then for any place $P' \in \mathbb{P}_{F'}$ there is exactly one place $P \in \mathbb{P}_F$ such that $P'|P$, namely $P = P' \cap F$. Conversely, any place $P \in \mathbb{P}_F$ has at least one, but only finitely many, extensions $P' \in \mathbb{P}_{F'}$.*

Theorem 1.28. *Let F'/K' be a finite extension of F/K, P a place of F/K and $P_1, \ldots, P_m \in \mathbb{P}_{F'}$ all the places that lay over P. Let $e_i := e(P_i|P)$ and $f_i := f(P_i|P)$, then*

$$\sum_{i=1}^{m} e_i f_i = [F' : F].$$

Therefore the number of places P_i that lies over P is at most $[F' : F]$. Moreover if P' lies over P then an upper bound of the ramification index $e(P'|P)$ and the relative degree $f(P'|P)$ is $[F' : F]$.

Definition 1.29. Let F'/F be an algebraic extension of function fields of degree $[F' : F] = n$ and let $P \in \mathbb{P}_F$.

(i) P *splits completely* in F'/F if there are exactly n distinct places $P' \in \mathbb{P}_{F'}$ with $P'|P$.

(ii) An extension P' of P in F' is said to be *tamely ramified* if $e(P'|P) > 1$ and $\mathrm{char}(K)$ does not divide $e(P'|P)$; it is said to be *wildly ramified* if $\mathrm{char}(K)$ divides $e(P'|P)$.

(iii) We say that P is *ramified* in F'/F if there is at least one $P' \in \mathbb{P}_{F'}$ over P such that $P'|P$ is ramified. Otherwise P is *unramified*. If there is at least one wildly ramified place $P'|P$ we say that P is *wildly ramified* in F'/F; otherwise P is *tamely ramified*.

(iv) P is *totally ramified* in F'/F if there is only one extension $P' \in \mathbb{P}_{F'}$ of P in F', and the ramification index is $e(P'|P) = n$.

(v) F'/F is said to be *tame* if no place $P \in \mathbb{P}_F$ is wildly ramified in F'/F.

Theorem 1.30 (Hurwitz Genus Formula)**.** *Suppose that F'/F is a* tame *finite separable extension of algebraic function fields having the same constant field K. Let g (resp. g') denote the genus of F/K (resp. F'/K). Then*

$$2g' - 2 = [F' : F] \cdot (2g - 2) + \sum_{P \in \mathbb{P}_F} \sum_{P'|P} (e(P'|P) - 1) \cdot \deg(P').$$

The formula makes sense because almost all places $P \in \mathbb{P}_F$ are unramified in F'/F.

In positive characteristic the Hurwitz Genus Formula is much more complicated when $[F' : F]$ is nontame. Since in the remaining part of this section we only consider tame extensions we delay the reporting of the Hurwitz

genus formula for the general case to the section about automorphisms of algebraic curves. For details and proof see [36] and [65].

Any function field F/K can be seen as a finite separable extension of a rational function field $K(x)$. The Hurwitz Genus Formula is a powerful tool that allows determination of the genus of F.

The following theorems describe two type of extensions in which it is simple to compute the ramification index of all points. Thus there is a direct formula to compute the genus of the extensions.

Theorem 1.31 (Kummer Extension)**.** *Let F/K be an algebraic function field in which K contains a primitive n-th root of unity (with $n > 1$ and n relatively prime to $char(K)$). Suppose that $u \in F$ is an element satisfying*

$$u \neq w^d \quad \text{for all } w \in F \text{ and } d \mid n,\ d > 1.$$

Let $F' = F(y)$ with $y^n = u$. An extension such as F' is said to be a Kummer extension *of F. We have:*

1. *Let $P \in \mathbb{P}_F$ and $P' \in \mathbb{P}_{F'}$ be an extension of P. Then*

$$e(P'|P) = \frac{n}{r_P},$$

where $r_P := gcd(n, v_P(u))$ is the greatest common divisor of n and $v_P(u)$.

2. *If K' denotes the constant field of F', g and g' denote the genus of F/K and F'/K' respectively, then*

$$g' = 1 + \frac{n}{[K' : K]}\left(g - 1 + \frac{1}{2}\sum_{P \in \mathbb{P}_F}\left(1 - \frac{r_P}{n}\right)\deg(P)\right).$$

Theorem 1.32 (Artin-Schreier Extension)**.** *Consider an algebraic function field F/K with constant field K of characteristic $p > 0$, and an additive separable polynomial $a(T) \in K[T]$ of degree p^n which has all its roots in K. Let $u \in F$. Suppose that for any $P \in \mathbb{P}_F$ there is an element $z \in F$ (depending on P) such that one of the following holds:*

(i) $v_P(u - a(z)) \geq 0$,

(ii) $v_P(u - a(z)) = -m$, *with* $m > 0$ *and* $m \not\equiv 0 \mod p$.

Define $m_P := -1$ *in case* (a) *and* $m_P := m$ *in case* (b). *Then* m_P *is a well-defined integer. Consider the extension field* $F' = F(y)$ *of* F *where* y *satisfies the equation* $a(y) = u$. *If there exists at least one place* $Q \in \mathbb{P}_F$ *with* $m_Q > 0$, *we have:*

(i) K *is algebraically closed in* F'.

(ii) Any $P \in \mathbb{P}_F$ *with* $m_P = -1$ *is unramified in* F'/F.

(iii) Any $P \in \mathbb{P}_F$ *with* $m_P > 0$ *is totally ramified in* F'/F.

(iv) Let g *and* g' *be the genus of* F *and* F' *respectively. Then*

$$g' = p^n \cdot g + \frac{p^n - 1}{2}\Big(- 2 + \sum_{P \in \mathbb{P}_F} (m_P + 1) \cdot \deg(P)\Big).$$

Chapter 2

Algebraic Geometry

In this section we start by defining some basic notions of algebraic geometry.

We start with defining a variety $\mathcal{X}$ over an affine space and associate it to a function field $K(\mathcal{X})$, whose transcendental degree is equal to the degree of $\mathcal{X}$. We call algebraic curve a variety of degree one; in this case the associated function field is the same of Definition 1.1. We use the tools studied in the last chapter to define properties of the curve that are also defined from a geometrical point of view: genus, valuations, divisors and the Riemann-Roch space (see [22, 36]).

The homogenization of an affine variety embeds it into a projective space, for this reason we define projective varieties and associate a function field. After defining the projective closure $\mathcal{X}^*$ of an affine variety $\mathcal{X}$ we will see that the associated function fields are isomorphic. Moreover, birationally equivalent varieties have isomorphic function fields. If $\mathcal{X}$ is a curve with function field $K(\mathcal{X})$ we can read off all information about $\mathcal{X}$ from $K(\mathcal{X})$.

In the first part of the chapter the base field K is assumed to be algebraically closed, mostly because in classical books of algebraic geometry the Hilbert Nullstellensatz is strongly used to define and work with varieties. The last section is focused on curves defined over finite field and we will see that most of the properties remain. We can view a curve $\mathcal{X}$ over a finite field $\mathbb{F}_q$ as a curve over the algebraic closure $\overline{\mathbb{F}}_q$ of which we can see only a fraction of all its points.

For a more extensive exposition of concepts and methods of algebraic geometry we refer to [22, 36, 62].

2.1 Affine varieties

Remark 2.1. We assume that K is an algebraically closed field.

Define the n-dimensional *affine space* over K, denoted $\mathbb{A}^n_K$ (or simply $\mathbb{A}^n$), to be the set of n-tuples of elements of K. An element $P = (a_1, \ldots, a_n) \in \mathbb{A}^n$ is called a *point*, $a_1, \ldots, a_n \in K$ are called *coordinates* of P.

Let $K[X_1, \ldots, X_n]$ be the polynomial ring in n variables over K. We can consider polynomial as functions from $\mathbb{A}^n$ to K, by defining $f(P) = f(a_1, \ldots, a_n)$, where $f \in A$ and $P \in \mathbb{A}^n$. A *zero* of f is a point $P \in \mathbb{A}^n$ such that $f(P) = 0$. If S is any subset of $K[X_1, \ldots, X_n]$, we define the set of common zeros of all polynomials $f \in S$:

$$V(S) = \{P \in \mathbb{A}^n \mid f(x) = 0 \text{ for all } f \in S\}.$$

A subset $\mathcal{X} \in \mathbb{A}^n$ is an *algebraic set* if there is a subset $S \subseteq K[X_1, \ldots, X_n]$ such that $\mathcal{X} = V(S)$. If $\mathfrak{a}$ is the ideal generated by S, then $\mathcal{X}$ can be considered as the set $V(\mathfrak{a})$. Since $K[X_1, \ldots, X_n]$ is a Noetherian ring, any ideal has a finite set of generators. Therefore if $f_1, \ldots, f_r$ are generators of $\mathfrak{a}$, than $\mathcal{X}$ can be expressed as the set of common zeros of a finite number of polynomials.

It is easy to see that the union of two algebraic sets is an algebraic set and the intersection of any family of algebraic sets is an algebraic set. The empty set and the whole space are algebraic sets.

We define the *Zariski topology* on $\mathbb{A}^n$ by taking the open subsets to be the complements of the algebraic sets. This is well defined for what said above.

For any subset $\mathcal{X} \subseteq \mathbb{A}^n$ let us define the *vanishing ideal* of $\mathcal{X}$ in $K[X_1, \ldots, X_n]$ by

$$I(\mathcal{X}) = \{f \in K[X_1, \ldots, X_n] \mid f(P) = 0 \text{ for all } P \in \mathcal{X}\}.$$

An algebraic set $\mathcal{X}$ is *irreducible* if it cannot be expressed as the union $\mathcal{X} = \mathcal{X}' \cup \mathcal{X}''$, where $\mathcal{X}'$ and $\mathcal{X}''$ are two proper algebraic subsets of $\mathcal{X}$. Equivalently, $\mathcal{X}$ is irreducible if and only if $I(\mathcal{X})$ is prime in $K[X_1, \ldots, X_n]$.

An *affine algebraic variety* (or simply *affine variety*) is an irreducible algebraic set $\mathcal{X} \in \mathbb{A}^n$.

The quotient ring $K[\mathcal{X}] = K[X_1, \ldots, X_n]/I(\mathcal{X})$ is called the *coordinate ring* of the affine variety $\mathcal{X}$. Since $I(\mathcal{X})$ is a prime ideal, $K[\mathcal{X}]$ is an integral

domain and a finitely generated K-algebra. Its field of quotient $K(\mathcal{X})$ is called the *function field* (or *field of rational functions*) on $\mathcal{X}$. It contains K as a subfield.

Definition 2.2. If $\mathcal{X}$ is a topological space, we define the dimension of $\mathcal{X}$ to be the supremum of all integers n such that there exists a chain $\mathcal{X}_0 \subset \mathcal{X}_1 \subset \cdots \subset \mathcal{X}_n = X$ of distinct closed irreducible subset of $\mathcal{X}$. We define the *dimension* of an affine variety to be its dimension as a topological space (considered with the Zariski topology).

Theorem 2.3. *The dimension of an affine variety $\mathcal{X}$ is equal to the transcendence degree of the field $K(\mathcal{X})$ over K.*

Let P be a point of an affine variety $\mathcal{X}$. Let U be an open neighborhood of P. We say that a continuous map $f : U \to K$ is a *regular function* at P if there exist polynomials $g, h \in K[X_1, \ldots, X_n]$ such that $h(x) \neq 0$ and $f = g/h$ in an open neighborhood of P. It is called regular on U if it is regular at all points $P \in U$.

Define an equivalence relation

$$(U, f) \sim (U', f') \text{ if and only if } f = f' \text{ on } U \cup U'.$$

The equivalence classes form a ring, denoted $\mathcal{O}_P(\mathcal{X})$. It is a local ring with unique maximal ideal

$$\mathfrak{m}_P(\mathcal{X}) = \{\text{equivalence classes of } (U, f) \mid f(P) = 0\}.$$

The equivalence classes, called *rational functions*, can be seen as element of $K(\mathcal{X})$, so we can write

$$\mathcal{O}_P(\mathcal{X}) = \{f \in K(\mathcal{X}) \mid f = g/h \text{ with } g, h \in K[\mathcal{X}],\ h(P) \neq 0\},$$
$$\mathfrak{m}_P(\mathcal{X}) = \{f \in K(\mathcal{X}) \mid f = g/h \text{ with } g, h \in K[\mathcal{X}],\ h(P) \neq 0, f(P) = 0\}.$$

Let $\mathcal{X} \in \mathbb{A}^n$ be an affine variety and let $f_1, \ldots, f_r \in K[X_1, \ldots, X_n]$ be generators for the ideal $I(\mathcal{X})$. The variety $\mathcal{X}$ is *non-singular at a point P*, if the rank of the matrix

$$\left(\frac{\partial f_i}{\partial X_j}(P)\right)_{i,j}$$

is $n - d$, where d is the dimension of $\mathcal{X}$. The variety $\mathcal{X}$ is *non-singular* (or *smooth*) if it is non-singular at every point.

Theorem 2.4. *Let $\mathcal{X} \in \mathbb{A}^n$ be an affine variety and let P be a point of $\mathcal{X}$. Then $\mathcal{X}$ is non-singular at P if and only if the local ring $\mathcal{O}_P(\mathcal{X})$ of P is a regular local ring.*

2.2 Projective varieties

Define the n-dimensional *projective space* over K, denoted $\mathbb{P}^n_K$ (or simply $\mathbb{P}^n$), to be the set of equivalence classes of $(n+1)$-tuples $(a_0, a_1, \ldots, a_n)$ of elements of K, not all zero, under the equivalence relation given by $(a_0, a_1, \ldots, a_n) \sim (\lambda a_0, \lambda a_1, \ldots, \lambda a_n)$ for all $\lambda \in K \setminus \{0\}$. Another way of saying this is that $\mathbb{P}^n$, as a set, is the quotient of the set $\mathbb{A}^{n+1} \setminus \{0\}$ under the equivalence relation which identifies points lying on the same line through the origin.

An equivalence class $P = (a_0 : a_1 : \ldots : a_n)$ is called a *point* of $\mathbb{P}^n$. If $P = (a_0 : a_1 : \ldots : a_n)$ is a point, then any $(n+1)$-tuple $(\lambda a_0, \lambda a_1, \ldots, \lambda a_n)$ in the equivalence class P is called a *set of homogeneous coordinates* for P.

A polynomial $F \in K[X_0, X_1, \ldots, X_n]$ is called *homogeneous* if

$$F(\lambda X_0, \ldots, \lambda X_n) = \lambda^m F(X_0, \ldots, X_n),$$

for some $m \in \mathbb{N}$ (called the degree of F) and all $\lambda \neq 0$ in K. So the property of being zero or not, when evaluated in a point P, depends only on the equivalence of P. An ideal $\mathfrak{a}$ in $K[X_0, X_1, \ldots, X_n]$ is called *homogeneous* if it can be generated by homogeneous elements.

If S is a subset of homogeneous polynomial of $K[X_0, X_1, \ldots, X_n]$, we define the set of common zeros of all polynomials $f \in S$:

$$V(S) = \{P \in \mathbb{P}^n \mid f(x) = 0 \text{ for all } f \in S\}.$$

If $\mathfrak{a}$ is a homogeneous ideal, $V(\mathfrak{a}) = V(T)$, where T is the set of all homogeneous element of $\mathfrak{a}$. Since $K[X_0, X_1, \ldots, X_n]$ is a Noetherian ring, let $F_1, \ldots, F_r$ be a set of generator of $\mathfrak{a}$, then $V(\mathfrak{a}) = V(\{F_1, \ldots, F_r\})$.

A subset $\mathcal{X} \in \mathbb{P}^n$ is an *algebraic set* if there exists a set T of homogeneous polynomial so that $\mathcal{X} = V(T)$. We define the Zariski topology on $\mathbb{P}^n$ by taking the open sets to be the complements of algebraic sets.

For any subset $\mathcal{X} \in \mathbb{P}^n$ let us define the *homogeneous ideal* of $\mathcal{X}$ in $K[X_0, X_1, \ldots, X_n]$ by

$$I(\mathcal{X}) = \{f \in K[X_0, X_1, \ldots, X_n] \mid f \text{ homogeneous}, f(P) = 0 \text{ for all } P \in \mathcal{X}\}.$$

A *projective algebraic variety* $\mathcal{X}$ (or simply *projective variety*) is an irreducible algebraic set in $\mathbb{P}^n$. As before $\mathcal{X}$ is irreducible if and only if $I(\mathcal{X})$ is a prime ideal. The quotient ring $K[\mathcal{X}] = K[X_0, X_1, \ldots, X_n]/I(\mathcal{X})$ is

the homogeneous coordinate ring. An element $f \in K[\mathcal{X}]$ is said to be a *form* of degree d, if $f = F + I(\mathcal{X})$ for some homogeneous polynomial $F \in K[X_0, X_1, \ldots, X_n]$ with $\deg(F) = d$. The *function field* of $\mathcal{X}$ is defined by

$$K(\mathcal{X}) = \left\{ \frac{g}{h} \mid g, h \in K[\mathcal{X}] \text{ are forms of the same degree and } h \neq 0 \right\}.$$

The dimension of a projective variety is its dimension as a topological space (with the topology of Zariski). It is equal to the transcendence degree of $K(\mathcal{X})$ over K.

Let $P = (a_0 : \cdots : a_n) \in \mathcal{X}$ and $f \in K(\mathcal{X})$. Write $f = g/h$, where $g = G + I(\mathcal{X}), h = H + I(\mathcal{X}) \in K[\mathcal{X}]$ and G, H are homogeneous polynomial of degree d. Since

$$\frac{G(\lambda a_o, \ldots, \lambda a_n)}{H(\lambda a_o, \ldots, \lambda a_n)} = \frac{\lambda^d \cdot G(a_0, \ldots, a_n)}{\lambda^d \cdot H(a_0, \ldots, a_n)} = \frac{G(a_0, \ldots, a_n)}{H(a_0, \ldots, a_n)},$$

we can set $f(P) = G(a_0, \ldots, a_n)/H(a_0, \ldots, a_n) \in K$, if $H(P) \neq 0$. Then we say that f is defined at P. The ring

$$\mathcal{O}_P(\mathcal{X}) = \{f \in K(\mathcal{X}) \mid f \text{ is defined at } P\}$$

is a local ring with maximal ideal

$$\mathfrak{m}_P(\mathcal{X}) = \{f \in \mathcal{O}_P \mid f(P) = 0\}.$$

Our next objective is to show that projective n-space has an open covering by affine n-spaces, and hence that every projective variety has an open covering by affine varieties.

Let $H_i = \{(a_0 : \ldots : a_n) \mid a_i = 0\}$ be the set of zeros of X_i. Let U_i be the open set $\mathbb{P}^n \setminus H_i$. Then $\mathbb{P}^n$ is covered by the open sets U_i, because if $P = (a_0 : \ldots : a_n)$ is a point, then at least one $a_i \neq 0$, hence $P \in U_i$. We define a mapping $\varphi : U_i \to \mathbb{A}^n$ as follows: if $P = (a_0 : \ldots : a_n)$, then $\varphi_i(P) = Q$, where Q is the point with affine coordinates

$$\left(\frac{a_0}{a_i}, \ldots, \frac{a_n}{a_i} \right),$$

with a_i/a_i omitted. Note that φ_i is well-defined, since the ration a_j/a_i are independent of the choice of homogeneous coordinates.

Let $\mathcal{X}$ be a projective variety. Suppose that $\mathcal{X} \cap U_i \neq \emptyset$. Then $\mathcal{X}_i := \varphi_i(X \cap U_i)$ is an affine variety. Moreover $\mathcal{X} = \bigcup_{i=0}^{n}(\mathcal{X} \cap U_i)$, so $\mathcal{X}$ is covered by open sets homeomorphic to affine varieties.

If $F \in K[X_0, X_1, \ldots, X_n]$ is a form, we define $F_* \in K[X_1, \ldots, X_n]$ by setting $F_* = F(1, X_1 \ldots, X_n)$. Conversely, for any polynomial $f \in K[X_1, \ldots, X_n]$ of degree d, write $f = f_0 + f_1 + \cdots + f_d$, where f_i is a form of degree i, and define $f* \in K[X_0, X_1, \ldots, X_n]$ by setting $f^* = X_0^d f_0 + X_0^{d-1} f_1 + \cdots + f_d = X_0^d f(X_1/X_0, \ldots, X_n/X_0)$; f^* is a form of degree d. These processes are often described as *dehomogenizing* and *homogenizing* polynomials with respect to X_0.

Consider now an affine variety $\mathcal{X} \in \mathbb{A}^n$ and the corresponding ideal $I = I(\mathcal{X}) \subset K[X_1, \ldots, X_n]$. Let I^* be the ideal in $K[X_0, X_1, \ldots, X_n]$ generated by $\{F^* \mid F \in I\}$. This is a homogeneous ideal; we define the *projective closure* of $\mathcal{X}$ to be $\mathcal{X}^* := V(I^*) \subset \mathbb{P}^n$. Except for projective varieties lying on H_0, there is a natural one-to-one correspondence between nonempty affine and projective varieties.

If $f \in K[\mathcal{X}^*]$ is a form of degree d, we may define $f_* \in K[\mathcal{X}]$ as follows: take a form $F \in K[X_0, X_1, \ldots, X_n]$ so that $f = F + I(\mathcal{X}^*)$, and let f_* to be the residue class of F_* in $K[\mathcal{X}]$ (this is independent of the choice of F). We then define $\alpha : K(\mathcal{X}) \to K(\mathcal{X}^*)$ as follows: $\alpha(f/g) = f_*/g_*$, where f, g are forms of the same degree on $\mathcal{X}^*$.

Let $P \in \mathcal{X}$ be an affine point, we may consider $P \in \mathcal{X}^*$ (by means of φ_0) and then α induces an isomorphism of $\mathcal{O}_P(\mathcal{X}^*)$ with $\mathcal{O}_P(\mathcal{X})$. We usually use α to identify $K(\mathcal{X})$ with $K(\mathcal{X}^*)$, and $\mathcal{O}_P(\mathcal{X})$ with $\mathcal{O}_P(\mathcal{X}^*)$.

Since the concept of non-singularity seen in the affine case depends only on the local ring of a point we can extend the definition to projective varieties.

Definition 2.5. A projective variety $\mathcal{X}$ is *non-singular at a point* P if the local ring $\mathcal{O}_P(\mathcal{X})$ is a regular local ring. The variety $\mathcal{X}$ is *non-singular* (or *smooth*) if it is non-singular at every point.

2.3 Maps between varieties

An open subset of a projective algebraic variety is called a *quasi-projective variety.*

Definition 2.6. Let V be a quasi-projective variety in $\mathbb{P}^n$. A function $f : V \to K$ is *regular at a point* $P \in V$ if there is an open neighbourhood U with $P \in U \subseteq V$, and polynomials $G, H \in K[X_0, X_1, \ldots, X_n]$, of the same degree, such that H is nowhere zero on U and $f = G/H$ on U. We say that f is regular on V if it is *regular* at every point.

A regular function is necessarily continuous. An important consequence of this is the fact that if f and g are regular functions on a variety $\mathcal{X}$, and if $f = g$ on some non-empty open subset $U \subseteq \mathcal{X}$, then $f = g$ everywhere.

For the rest of this section we call variety both a projective and a quasi-projective variety.

Definition 2.7. Let $\mathcal{X}, \mathcal{Y}$ be two varieties. A *morphism* $\varphi : \mathcal{X} \to \mathcal{Y}$ is a continuous map such that for every open set $V \in \mathcal{Y}$, and for every regular function $f : V \in K$, the function $f \circ \varphi : \varphi^{-1}(V) \to K$ is regular.

Let φ and ψ be two morphisms from $\mathcal{X}$ to $\mathcal{Y}$, and suppose there is a non-empty open subset $U \subseteq \mathcal{X}$ such that $\varphi|_U = \psi|_U$. Then $\varphi = \psi$ everywhere.

Clearly the composition of two morphisms is a morphism, in particular we have the notion of isomorphism: an *isomorphism* $\varphi : \mathcal{X} \to \mathcal{Y}$ of two projective varieties is a morphism which admits an inverse morphism $\psi : \mathcal{Y} \to \mathcal{X}$ with $\psi \circ \varphi = Id_{\mathcal{X}}$ and $\varphi \circ \psi = Id_{\mathcal{Y}}$.

Definition 2.8. Let $\mathcal{X}, \mathcal{Y}$ be varieties. A *rational map* $\varphi : \mathcal{X} \to \mathcal{Y}$ is an equivalence class of pairs $\langle U, \varphi_U \rangle$ where U is a non-empty subset of $\mathcal{X}$, φ_U is a morphism of U to $\mathcal{Y}$, and where $\langle U, \varphi_U \rangle$ and $\langle V, \varphi_V \rangle$ are equivalent if φ_U and φ_V agree on $U \cap V$. The rational map φ is *dominant* if for some (and hence every) pair $\langle U, \varphi_U \rangle$, the image of φ_U is dense in $\mathcal{Y}$.

Note that the relation on pairs $\langle U, \varphi_U \rangle$ just described is an equivalence relation.

Definition 2.9. A *birational map* $\varphi : \mathcal{X} \to \mathcal{Y}$ is a rational map which admits an inverse, namely a rational map $\psi : \mathcal{Y} \to \mathcal{X}$, such that $\psi \circ \varphi = Id_{\mathcal{X}}$ and $\varphi \circ \psi = Id_{\mathcal{Y}}$ as rational maps. If there is a birational map from $\mathcal{X}$ to $\mathcal{Y}$, we say that $\mathcal{X}$ and $\mathcal{Y}$ are *birationally equivalent*.

Let $\mathcal{X}$ and $\mathcal{Y}$ be two birationally equivalent variety, than $K(\mathcal{X})$ and $K(\mathcal{Y})$ are isomorphic as K-algebras.

2.4 Algebraic curves

A *projective algebraic curve* $\mathcal{X}$ is a projective variety of dimension one. This means that the field $K(\mathcal{X})$ of rational functions on $\mathcal{X}$ is an algebraic function field of one variable, in the sense of Definition 1.1.

A point $P \in \mathcal{X}$ is *non-singular* (or *smooth*) if and only if the local ring $\mathcal{O}_P(\mathcal{X})$ is a discrete valuation ring (i.e. a principal ideal domain with exactly one maximal ideal). On the other hand, if the curve is singular, then there exist only finitely many singular points on the curve. Let us introduce now a very important result of classical algebraic geometry.

Theorem 2.10. *Every curve is birationally equivalent to a non-singular projective curve.*

Hence, if we study the function field associated to a non-smooth curve $\mathcal{X}$, we can derive all the properties of a smooth curve (that is birationally equivalent to $\mathcal{X}$).

Let $\mathcal{X}$ be a smooth projective curve and $F = K(\mathcal{X})$ be its function field. There is a 1-1 correspondence between the points $P \in \mathcal{X}$ and the places of F/K, given by

$$P \mapsto \mathfrak{m}_P(\mathcal{X}),$$

the maximal ideal of the local ring $\mathcal{O}_P(\mathcal{X})$. This correspondence makes it possible to translate definitions and results from algebraic function fields to algebraic curves (and vice versa). We give the following examples:

(i) The *genus* of the curve $\mathcal{X}$ is the genus of the function field $K(\mathcal{X})$.

(ii) A *divisor* of $\mathcal{X}$ is a formal sum $D = \sum_{P\in\mathcal{X}} n_P P$, where $n_P \in \mathbb{Z}$ and almost all $n_P = 0$. The *degree* of D is $\deg(D) = \sum_{P\in\mathcal{X}} n_P$. The divisors of $\mathcal{X}$ from an additive group $\mathcal{D}(\mathcal{X})$, the *divisor group* of $\mathcal{X}$.

(iii) The *order* of a rational function at a point $P \in \mathcal{X}$ is defined to be $v_P(f)$, where v_P is the discrete valuation of $K(\mathcal{X})$ corresponding to the valuation ring $\mathcal{O}_P(X)$.

(iv) The *principal divisor* (f) of a rational function $0 \neq f \in K(\mathcal{X})$ is $(f) = \sum_{P\in\mathcal{X}} v_P(f)P$. The degree of a principal divisor is zero.

(v) For $D \in \mathcal{D}(\mathcal{X})$, the space $\mathcal{L}(D)$ is defined as in the function field case. It is a finite-dimensional vector space over K, its dimension given by the Riemann-Roch Theorem.

Note that if a curve $\mathcal{X}$ contains a finite number of singular points all the properties of $\mathcal{X}$ are derived from the function field $K(\mathcal{X})$, thus are the same of the non-singular curve associated to $K(\mathcal{X})$.

Example 2.11. *Let $\mathbb{P}^1_K$ denote the projective line over K. This can be seen as $K \cup \{\infty\}$. The associated function field is the rational function field $K(x)$. The 1-1 correspondence between the points of $\mathbb{P}^1_K$ and the places of $K(x)$ is given by*

$$\begin{aligned} \alpha &\mapsto P_{x-\alpha}, \quad \text{for all } \alpha \in K \\ \infty &\mapsto P_\infty. \end{aligned}$$

Hence, by 1.22, the genus of a projective line is zero.

2.5 Curves over a finite field

In the previous sections we have assumed that the ground field K is algebraically closed. However, to apply algebraic geometry to coding theory, we have to study curves defined over $\mathbb{F}_q$ and their points with coordinates in $\mathbb{F}_q$ (such points are called $\mathbb{F}_q$-*rational*).

Let $K = \mathbb{F}_q$ be a finite field and let $\mathbb{K}$ be an algebraically closed field containing K as a subfield. Let $\mathfrak{p}$ be a prime ideal of $K[X_1, \ldots, X_n]$ which generates a prime ideal $\mathfrak{p}'$ in $\mathbb{K}[X_1, \ldots, X_n]$. Then $\mathfrak{p}'$ defines an affine variety $\mathcal{X} = V(\mathfrak{p}')$ *defined over* K. Similarly a projective variety *defined over* K is given by a homogeneous prime ideal of $K[X_0, X_1, \ldots, X_n]$ which remains prime being extended to $\mathbb{K}[X_0, X_1, \ldots, X_n]$.

We call $\mathcal{X}$ *smooth* if, after extension of K to its algebraic closure $\mathbb{K}$, the curve is a smooth curve.

We can view a curve $\mathcal{X}$ over K as a curve over $\mathbb{K}$ of which we can see only a fraction of its points.

We say that a point $P = (a_1, \ldots, a_n) \in \mathbb{A}^n_{\mathbb{K}}$ is K-*rational* if $a_i \in K$ for all $i = 1, \ldots, n$. A point $P = (a_0 : a_1 : \ldots : a_n) \in \mathbb{P}^n_{\mathbb{K}}$ is called K-*rational* if $x_i \neq 0$ implies $x_j/x_i \in K$ for all $j = 0, 1, \ldots, n$.

An affine variety $\mathcal{X} \in \mathbb{A}^n_{\mathbb{K}}$ is defined over K if its associated ideal $I(\mathcal{X})$ has a basis $\{f_1, \ldots, f_r\}$ consisting of polynomials with coefficients in K. Similarly a projective variety $\mathcal{X} \subset \mathbb{P}^n_{\mathbb{K}}$ is defined over K if $I(\mathcal{X})$ is generated

by homogeneous polynomial $F_1, \ldots, F_r \in K[X_0, X_1, \ldots, X_n]$. The subset of K-rational points of $\mathcal{X}$ is denoted by $\mathcal{X}(K)$.

Let $I(\mathcal{X}) \subset \mathbb{K}[X]$ be the ideal of the variety $\mathcal{X} \subset \mathbb{A}^n_{\mathbb{K}}$ generated by $f_1, \ldots, f_r$. Let $I(\mathcal{X}/K) \subset K[X]$ be the prime ideal generated by $f_1, \ldots, f_r$. Then we have

$$I(\mathcal{X}/K) = I(\mathcal{X}) \cap K[X].$$

We define the coordinate ring $K[\mathcal{X}] = K[X_1, \ldots, X_n]/I(\mathcal{X}/K)$. Its field of quotient $K(\mathcal{X})$ is the field of K-rational function of $\mathcal{X}$; $K(\mathcal{X})/K$ is a function field over K in the sense of Definition 1.1. In the same manner the field of K-rational functions of a projective variety can be defined.

Let $\mathcal{X}$ be a variety. If $G = Gal(\mathbb{K}/K)$ is the Galois group of $\mathbb{K}$ over K and if $P \in \mathcal{X}$ then $\sigma(P) \in \mathcal{X}$ for every $\sigma \in G$. Moreover if $P \in \mathcal{X}(K)$ we have $\sigma(P) = P$ for every $\sigma \in G$. Thus

$$\mathcal{X}(K) = \{P \in \mathcal{X}(\mathbb{K}) \mid \sigma(P) = P \text{ for all } \sigma \in G\},$$

$$K(\mathcal{X}) = \{f \in \mathbb{K}(\mathcal{X}) \mid \sigma(f) = f \text{ for all } \sigma \in G\}.$$

Consider a projective curve $\mathcal{X} \subset \mathbb{P}^n_{\mathbb{K}}$ which is defined over K. Denote by σ the Frobenious automorphism of the field K,

$$\sigma : P = (a_0 : a_1 : \ldots : a_n) \mapsto \sigma(P) = (a_0^q : a_1^q : \ldots : a_n^q).$$

A divisor $D = \sum_{P \in \mathcal{X}} n_P P \in \mathcal{D}(\mathcal{X})$ is called K-rational if $\sigma(D) = D$, where

$$\sigma(D) = \sum_{P \in \mathcal{X}} n_P \sigma(P).$$

This means that $n_{\sigma(P)} = n_P$ for all $P \in \mathcal{X}$. The divisors of $\mathcal{X}$ defined over K form a subgroup $\mathcal{D}(\mathcal{X}/K) \subseteq \mathcal{D}(\mathcal{X})$. For $D \in \mathcal{D}(\mathcal{X}/K)$ the space $\mathcal{L}_K(D)$ is given by

$$\mathcal{L}_K(D) = K(\mathcal{X}) \cap \mathcal{L}(D).$$

It is a finite-dimensional K-vector space, and its dimension (over K) equals the dimension of $\mathcal{L}(D)$ (over $\mathbb{K}$).

A divisor $Q \in \mathcal{L}_K(D)$ with $Q > 0$ is called a *prime divisor* of $\mathcal{X}(\mathbb{K})$ if Q cannot be written as $Q = Q_1 + Q_2$ with positive divisors $Q_1, Q_2 \in \mathcal{D}(\mathcal{X}/K)$. It is easily seen that the divisor group $\mathcal{D}(\mathcal{X}/K)$ is the free abelian group generated by the prime divisors. Prime divisors of $\mathcal{X}(K)$ correspond to

the places of the function field $K(\mathcal{X})/K$; under this correspondence, prime divisors of degree one (i.e., K-rational points) of $\mathcal{X}$ correspond to the places of $K(\mathcal{X})/K$ of degree one.

An important theorem of algebraic geometry is the Hasse-Weil bound: it provides an estimate of the number of $\mathbb{F}_q$-rational points on curve, bounding the value both above and below.

Theorem 2.12 (Hasse-Weil Bound)**.** *Let X be a projective curve of genus g defined over a finite field $\mathbb{F}_q$ and let N be the number of $\mathbb{F}_q$-rational points. Then*

$$|N - q - 1| \leq 2gq^{1/2}.$$

We say that a curve $\mathcal{X}$ is $\mathbb{F}_q$-maximal if its number of maximal points over $\mathbb{F}_q$ reaches the Hasse-Weil upper bound

$$|\mathcal{X}(\mathbb{F}_q)| = q + 1 + 2gq^{1/2},$$

where g is the genus of $\mathcal{X}$. Here the cardinality q of the finite field will always be a square.

In general, curves with many $\mathbb{F}_q$-rational points with respect to their genus give rise to AG codes with good parameters. For this reason maximal curves have been widely investigated in the literature: for example the Hermitian curve and its quotients, the Suzuki curve, the Klein quartic and the Giulietti-Korchmáros curve.

2.6 Automorphisms of algebraic curves

In this subsection we deal with the automorphisms of an algebraic curve, which represent an important birational invariant of the curve. The study of the automorphisms of a curve relies on algebraic methods, since the set of the automorphisms of an algebraic curve forms a group respect to the composition. Moreover, any curve can be embedded into a projective space in which it is smooth, and because in this embedding the automorphisms of the curve correspond to the collineations of the projective space, then everything can be seen in a geometrical way. For details and proof we refer to [38].

Let us introduce Galois covering.

Proposition 2.13. *Given a finite and separable extension* $[M : L]$ *and called*

$$\Gamma(M, L) = \{\sigma : M \mapsto M \mid \sigma \text{ automorphism such that } \sigma(l) = l \text{ for each } l \text{ in } L\},$$

we have that

$$|\Gamma(M, L)| \leq [M : L].$$

Definition 2.14. A field extension finite and separable $M : L$ is called a Galois extension if $|\Gamma(M, L)| = [M : L]$.

Definition 2.15. For a non-constant rational map $\phi : \mathcal{X} \mapsto \mathcal{Y}$ defined on two algebraic curves $\mathcal{X}$ and $\mathcal{Y}$, with pull-back ϕ^*, $\Gamma(\mathcal{X}, \mathcal{Y})$ is called the group of automorphisms $\Gamma(\mathbb{K}(\mathcal{X}), \phi^*(\mathbb{K}(\mathcal{Y})))$. We have then

$$\Gamma(\mathcal{X}, \mathcal{Y}) = \{\sigma : \mathbb{K}(\mathcal{X}) \mapsto \mathbb{K}(\mathcal{X}) | \sigma \text{ automorphism such that } \sigma(\alpha) = \alpha \text{ for all } \alpha \text{ in } \phi^*(\mathbb{K}(\mathcal{Y}))\}.$$

The map ϕ is called a *Galois map* if this field extension $K(\mathcal{X}) : \phi^*(\mathbb{K}(\mathcal{Y}))$ does. The curve $\mathcal{Y}$ is called *quotient curve* $\mathcal{X}$ with respect to the automorphism group $\Gamma(\mathcal{X}, \mathcal{Y})$.

Theorem 2.16. *Given a finite group of* K*-automorphisms* G *of an algebraic curve* $\mathcal{X}$ *let*

$$L = \{\alpha \in K(\mathcal{X}) \mid \sigma(\alpha) = \alpha \text{ for all } \alpha \in G\}.$$

It comes out that the extension $K(\mathcal{X}) : L$ *is a Galois extension and* $\Gamma(K(\mathcal{X}), L) = G$.

Corollary 2.17. *The Galois covering of* $\mathcal{X}$ *are in bijection with the finite automorphism subgroups of* $K(\mathcal{X})$.

Definition 2.18. The quotient curve of $\mathcal{X}$ with respect to the automorphism group G is denoted with $\mathcal{X}^G$ or $\mathcal{X}/G$.

We recall that DVR means discrete valuation ring, for its definition see the previous chapter. In Algebraic Geometry the results are usally given in terms of DVRs and not in terms of places, which is a term belonging to the theory of function fields. For this reason in this section we will report the results using the language of Algebraic Geometry.

Lemma 2.19. *Let* O *and* O' *respectively DVR of* $K(\mathcal{X})$ *and* $K(\mathcal{Y})$ *and let them such that* $O|O'$. *Let* $\sigma \in \Gamma(\mathcal{X}, \mathcal{Y})$, *we have that*

(i) $\sigma(O)$ *is a DVR of* $\mathbb{K}(\mathcal{X})$;

(ii) $ord_{\sigma(O)}(y) = ord_O(\sigma^{-1}(y))$;

(iii) $\sigma(O)|O'$;

(iv) $e_{\sigma(O)} = e_O$.

Lemma 2.20. *Let $K(\mathcal{X}) : \phi^*(\mathbb{K}(\mathcal{Y}))$ be a Galois extension. we have that*

$$\phi^*(K(\mathcal{Y})) = \{\alpha \in K(\mathcal{X}) \,|\, \sigma(\alpha) = \alpha \text{ for all } \sigma \in \Gamma(\mathcal{X}, \mathcal{Y})\}.$$

The following result allows us to tell that the DVR of $\mathcal{X}$ which are in the same DVR of $\mathcal{Y} = \mathcal{X}^G$ lie all on the same orbit in the action of the automorphism group G.

Theorem 2.21. *Given a Galois map $\phi : \mathcal{X} \mapsto \mathcal{Y}$, a DVR O' of $\mathbb{K}(\mathcal{Y})$ and two DVR O_1, O_2 such that $O_1|O'$ and $O_2|O'$ we have that there exists $\sigma \in \Gamma(\mathcal{X}, \mathcal{Y})$ such that $O_2 = \sigma(O_1)$.*

Corollary 2.22. *Given a Galois map $\phi : \mathcal{X} \mapsto \mathcal{Y}$ with degree n and a DVR O of $\mathbb{K}(\mathcal{X})$ we have that e_O coincides with the size of the stabilizer G_O of O in $\Gamma(\mathcal{X}, \mathcal{Y})$.*

Theorem 2.23 (Hurwitz bound)**.** *Let G be the automorphisms group of a curve $\mathcal{X}$ with genus $g \geq 2$. If G is finite and $char(\mathbb{K}) = 0$ or $char(\mathbb{K}) = p$ with p prime such that $\gcd(p, |G|) = 1$, then*

$$|G| \leq 84(g - 1) \tag{2.1}$$

Definition 2.24. An automorphism of a curve $\mathcal{X}$ is said to be $\mathbb{F}_q$*-rational* if the maps that define it are $\mathbb{F}_q$-rational.

Theorem 2.25. *The set of the automorphisms of an algebraic curve $\mathcal{X}$ is a group with the operation of composition. If the curve is not rational or elliptic then this group is finite.*

Definition 2.26. For a curve $\mathcal{X}$ over the field K we indicate with $Aut(\mathcal{X}) := Aut_K(\mathcal{X})$ its group of automorphisms. If $\alpha \in Aut(\mathcal{X})$ is and automorphism and P a DVR of $\mathcal{X}$ we define $P^\alpha := \alpha(P)$.

Theorem 2.27. *If $\alpha \in Aut(\mathcal{X})$ is an automorphism of $\mathcal{X}$ such that $P^\alpha = P$ for an infinite number of DVR of $\mathcal{X}$ then $\alpha = id$.*

Lemma 2.28. *A non-trivial K-automorphism α of $\mathcal{X}$ fixes at most $2g + 2$ DVR.*

Theorem 2.29. *Let $\mathcal{X}$ be an irreducible algebraic curve over a field K with characteristic p. Each $\mathbb{K}$-automorphism of $\mathcal{X}$ which fixes a DVR has at most order $2p(g+1)(2g+1)^2$.*

Definition 2.30. Let G be a group of automorphisms of a curve $\mathcal{X}$ and let P be a DVR of $\mathcal{X}$. The *orbit* of P under G is defined as the set $P^G = \{P^\alpha \,|\, \alpha \in G\}$. The *stabilizer* of P in G is defined as the subgroup $G_P = \{\alpha \in G \,|\, P^\alpha = P\}$. The orbit P^G is said to be *long* or *short* depending on the banality of G_P.

An important relation between $\mathcal{X}$ and its quotient curve $\mathcal{X}^G$ with G group of automorphisms $\mathcal{X}$ is given by the following lemma.

Lemma 2.31. *Let G be a finite subgroup of $Aut(\mathcal{X})$. Two DVRs of $\mathcal{X}^G$ lie on the same DVR of $\mathcal{X}^G$ if and only if they are in the same orbit of $\mathcal{X}$ under G.*

Theorem 2.32. *Let P be a DVR of $\mathcal{X}$ which lies on the DVR P' of $\mathcal{X}^G$. Said $n = |G|$ and $m = |G_P|$, the number of distinct DVR which lie over P' is n/m and the ramification index of each of them is $e_P = m$.*

Theorem 2.33. *Let $\mathcal{X}$ be an algebraic curve with genus $g > 0$ and P one of its DVR. The subgroup G_P of $Aut(\mathcal{X})$ which fixes P is finite and its structure is determined as follows*

(i) if $p = 0$ then G_P is cyclic with order at most $8(2g+1)^3$;

(ii)

- *if $p > 0$ then there exists a p-Sylow N, normal subgroup of G_P and such that*
$$|N| \leq p^2(g+1)(2g-1)^2,$$
with a quotient group G_P/N which is cyclic and such that
$$|G_P/N| \leq 2p(2g+1)^2(g+1).$$
- *G_P contains a cyclic subgroup $H \simeq G_P/N$ and such that $G_P = N \rtimes H$. All the subgroups H with such properties are conjugates in G_P.*
- *$|G_P|$ has a upper bound only depending on p e g.*

As a corollary we have the following result.

Theorem 2.34. *The stabilizer of a DVR of a curve $\mathcal{X}$ with a tame automorphism group is cyclic.*

Definition 2.35. A short orbit of a curve G of K-automorphisms is said *tame* or *non-tame (wild)* depending on the fact that the order of G_P for one (and then for each) of its points is prime or not with the characteristic p of K.

We stress that in zero characteristic any orbit is tame. We can now expose the complete Hurwitz bound, already anticipated in Theorem 2.23.

Theorem 2.36 (Hurwitz bound)**.** *Let $\mathcal{X}$ be an algebraic irreducible curve over the field K with genus $g \geq 2$ and let G be its full automorphisms group.*

- *If all the orbits of $\mathcal{X}$ under the action of G are tame then*

$$|G| \leq 84(g-1).$$

- *If there exist not tame orbits (and then p is positive) then ther can be an exeption to Hurwitz bound if and only if the quotient curve $\mathcal{X}^G$ is rational and G acts with at most three short orbits. The structure of the short orbitscan only be one of the following*

  (1) $p \geq 3$ and G has exactly three short orbits, two of them tame and one wild;

  (2) G has two short orbits and they are not tame;

  (3) G has only a short orbit, not tame;

  (4) G has exactly two short orbits, one tame and one wild.

In the case of tame automorphisms groups there exist many characterizations useful for the determination of the automorphism group of the curve.

Theorem 2.37. *Let G be the group of $\mathbb{K}$-automophisms of an irreducible curve $\mathcal{X}$. Let $n = |G|$, g be the genus of $\mathcal{X}$ and g' the genus of $\mathcal{X}^G$. If for each DVR P of $\mathcal{X}$ the order of the stabilizer $|G_P|$ of G in P is prime with p then*

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

where $l_1, \ldots, l_s$ are the lenghts of the short orbits of G.

Theorem 2.38. *Let α be a non-trivial and tame automorphism of the automorphism group of $\mathcal{X}$ and let n be the order of α and $\rho(\alpha)$ the number of DVRs which it fixes. We have that*

$$2g - 2 = n(2g' - 2) + \rho(\alpha)(n - 1),$$

where g and g' are the genera of $\mathcal{X}$ and of $\mathcal{X}^\alpha$ respectively.

Theorem 2.39. *Let $\mathcal{X}$ be an irreducible curve with genus $g > 0$ and let G_P be the stabilizer of a DVR P of $\mathcal{X}$. If $n = |G_P|$ is coprime with p then*

$$n \leq 4g + 2.$$

Definition 2.40. The *i-th group of ramification* of the DVR P of the curve $\mathcal{X}$ is defined as the group

$$G_P^{(i)} = \{\alpha \in G_P \,|\, ord_P(\alpha(x) - x) \geq i + 1\},$$

where x is a local parameter of $\mathcal{X}$ in P.

It can be seen that the ramification groups form a chain

$$G_P^{(0)} \geq G_P^{(1)} \geq \dots$$

Theorem 2.41. *With the same notation above:*

(i) $G_P^{(0)}$ *is the stabilizer of* P.

(ii) $G_P^{(1)}$ *is the only Sylow p-subgroup of* G_P.

(iii) For $i \geq 1$ the group $G_P^{(i)}$ is normal in G_P and the group $G_P^{(i)}/G_P^{(i+1)}$ is a elementar abelian p-group.

Lemma 2.42. *Let G be an abelian subgroup of the automorphisms group of the curve $\mathcal{X}$ which fixes $m \geq 1$ DVRs. We have that*

(i) If P is a fixed DVR and g' is the genus of the quotient curve $\mathcal{C}^G$ then

$$2g - 2 \geq |G|(2g' - 2) + m|G| - 1 + \frac{|G|}{|G_P^{(1)}|}(|G_P^{(1)}| - 1)). \tag{2.2}$$

(ii) If the full automorphism group $\mathcal{C}$ is not tame then

$$2g - 2 \geq |G| \left(2g' + \frac{3}{2}m - 2\right) - m. \tag{2.3}$$

Lemma 2.43. *Let $\mathcal{C}$ be a curve and G be an abelian not tame subgroup of $Aut_K(\mathcal{C})$. If $G = G_P^{(1)} \rtimes H$ where $p \nmid |H|$ then we have that*

$$2g \geq 2g'|G_P^{(1)}| + (|H| - 1)(|G_P^{(1)}| - 1).$$

Theorem 2.44. *Let $\mathcal{C}$ be an irreducible curve with genus $g \geq 1$ and let G_P be a subgroup of the automorphisms group which fixes a DVR P. Then*

$$|G_P^{(1)}| \leq \frac{4p}{p-1} g^2. \tag{2.4}$$

In particular if $\mathcal{C}_i$ is the quotient curve of $\mathcal{X}$ respect to $|G_P^{(i)}|$ then one of the following holds

(i) $\mathcal{C}_1$ is not rational and $|G_P^{(1)}| \leq g$;

(ii) $\mathcal{C}_1$ is rational, $G_P^{(1)}$ has a short orbit further P and

$$|G_P^{(1)}| \leq \frac{p}{p-1} g;$$

(iii) $\mathcal{C}_1$ and $\mathcal{C}_2$ are rationals, $\{P\}$ is the only short orbit of $G_P^{(1)}$ and

$$|G_P^{(1)}| \leq \frac{4p}{(p-1)^2} g^2.$$

Theorem 2.45. *Given an abelian subgroup G of the group of K-automorphisms of an irreducible curve $\mathcal{C}$ with genus $g \geq 2$. We have that*

$$|G| \leq \begin{cases} 4g + 4 \text{ if } p \neq 2; \\ 4g + 2 \text{ if } p = 2. \end{cases} \tag{2.5}$$

Chapter 3

Linear codes

Claude Shannon's seminal paper "A mathematical theory of communication" stated the beginning of Information Theory and error-correcting codes. Given a communication channel which may corrupt messages passing through it, the task of an error-correcting code is to provide a systematic way of adding redundancy to a message so that it can be recovered if some corruptions happen during the transmission. Since the publication of Shannon's work, mathematicians have developed connections between error-correcting coding and aspects of algebra and combinatorics and sophisticated mathematical techniques have proved useful for coding problems. Linear codes also have found a lot of applications in cryptography. We start this section introducing what a linear code is, for a complete exposition of the concepts see [48].

Definition 3.1. Let $\mathbb{F}_q$ be the finite field with q elements. Let $k, n \in \mathbb{N}$ such that $k \leq n$. Let C be a k-dimensional vector subspace of $(\mathbb{F}_q)^n$: we say that C is an $\mathbb{F}_q$ *linear block code* (or simply *code*) of dimension k and length n. An element of C is called a *codeword* of C.

Definition 3.2. Let $(\mathbb{F}_q)^n$ be any n-dimensional vector space on a finite field $\mathbb{F}_q$. For any two vectors $x, y \in (\mathbb{F}_q)^n$, the *Hamming distance* between x and y, denoted by $d(x, y)$, is the number of coordinates where the two words differ.

Definition 3.3. Given $x \in (\mathbb{F}_q)^n$, we define the *Hamming weight* of x as the number of non-zero coordinates of x. We denote it by $\mathrm{w}(x)$.

Definition 3.4. Let C be a linear block code. We define the *minimum*

distance of C (or simply *distance*) as the minimum distance between any two different words of C.

Clearly the distance of C is in fact also the minimum in the set of the weights of its non-zero words.

Definition 3.5. Given an $[n, k, d]$ code C, we denote by A_i the number of words of weight i. The set $\{A_i\}$ is also called the *weight distribution* of C, and the $\{A_i\}$ are also called the *weight elements* of C.

Remark 3.6. We observe that $A_0 = 1$ and $A_i = 0$ for $i \in \{1, \ldots, d-1\}$ or $i > n$. Also, $\sum_{i=0}^{n} A_i = q^k$.

Definition 3.7. Define $W_C(x, y) \in \mathbb{Z}[x, y]$ to be the *weight enumerator* of C as

$$W_C(x, y) = \sum_{i=0}^{n} A_i x^{n-i} y^i$$

$W_C(x, y)$ is a polynomial containing all information regarding the weight distribution of the code.

Definition 3.8. Let C be an $\mathbb{F}_q$ $[n, k, d]$ code. The *brute force* decoding procedure for C is the algorithm that computes the distance between x and any word of C and outputs

- either the word of C that is nearest to x, if it exists,
- or the distance of x from C (failure warning).

This is also known as *nearest-neighbour* decoding.

Proposition 3.9. *An* $\mathbb{F}_q$ $[n, k, d]$ *code* C *has detection capability* $d - 1$ *and correction capability* $t = \lfloor \frac{d-1}{2} \rfloor$.

Proposition 3.10 (Singleton Bound)**.** *Let* C *be a* $[n, k, d]_q$ *code, then*

$$d \leq n - k + 1.$$

A code achieving this bound is called Maximum Distance Separable.

Since a code C is a vector subspace, it can be represented by a matrix formed by a minimum set of its linear generators. This matrix is called the *generator matrix* of C and is traditionally denoted by G. G is a $k \times n$ matrix with coefficients in $\mathbb{F}_q$. The code can then be described by the image of G in $(\mathbb{F}_q)^n$.

Definition 3.11. Let C be an $[n, k, d]$ code. Its *dual code* $C^{\perp}$ is the set of all n-vectors that are orthogonal to all code words.

The dual code of an $[n, k, d]$ code is obviously an $[n, n-k, d']$ code. A generator matrix for $C^{\perp}$, traditionally denoted by H, is called a *parity-check matrix* for C. To check if an n-vector x is a word of C, it is necessary and sufficient that $xH^T = Hx^T = \mathbf{0}$. Conversely, any generator matrix for C is a parity-check matrix for $C^{\perp}$.

Proposition 3.12. *Let C be an $[n, k, d]$ code and H its parity-check matrix. Then for any code word of weight w there is a linear dependence relation among w columns of H and, conversely, for any linear dependence relation involving w columns of H there is a code word of weight w.*

Proposition 3.13. *Let C be an $[n, k, d]$ code with parity-check matrix H. Then $d \geq w$ if and only if every choice of $w-1$ or fewer columns of H is linearly independent.*

Let us consider what happens if a word x is sent, some errors occur and the received vector y *is* another word of C. If this happens, there is no way for the receiver to detect any error. The probability that this undesirable situation occurs is called the *Probability of the Undetected Error* (PUE).

Let P denote the error rate associated to a channel. We can suppose that we send the word 0 and we have an error e, so that the received word is exactly e, due to the linearity of the code. If the receiver is deceived it means that $e \in C$. Let $i = w(e)$ be the weight of e; there have then been i errors, that is *exactly i bits changed and exactly $(n-i)$ remained unchanged.*

Given e, the probability that this will occur is $P^i(1-P)^{n-i}$. With e varying among the words of C of weight i, the probability is $A_i P^i (1-P)^{n-i}$. Finally, if $e \in C$ is arbitrary we have:

$$\mathrm{PUE} = \sum_{i=0}^{n} A_i P^i (1-P)^{n-i}.$$

Observe that normally P is significantly smaller than $1/2$, so the addenda $P^i(1-P)^i$ are negligible for large i and it is the first elements of the weight distribution that most significantly influence the PUE.

3.1 Algebraic Geometry codes

In this section we recall some basic facts on AG-codes. For a detailed introduction we refer to [65].

Let $\mathcal{X}$ be a curve of genus g over $\mathbb{F}_q$, $\mathbb{F}_q(\mathcal{X})$ be the field of $\mathbb{F}_q$-rational functions on $\mathcal{X}$, $\mathcal{X}(\mathbb{F}_q)$ be the set of $\mathbb{F}_q$-rational places of $\mathcal{X}$. For an $\mathbb{F}_q$-rational divisor $D = \sum_{P \in \mathcal{X}(\mathbb{F}_q)} n_P P$ on $\mathcal{X}$, denote by

$$\mathcal{L}(D) := \{f \in \mathbb{F}_q(\mathcal{X}) \setminus \{0\} \mid (f) + D \geq 0\} \cup \{0\}$$

the Riemann-Roch space associated to D, whose dimension over $\mathbb{F}_q$ is denoted by $\ell(D)$. Consider a divisor $D = P_1 + \cdots P_n$ where $P_i \in \mathcal{X}(\mathbb{F}_q)$ and $P_i \neq P_j$ for $i \neq j$, and a second $\mathbb{F}_q$-rational divisor G whose support is disjoint from the support of D. The *functional AG code* $C_{\mathcal{L}}(D, G)$ is defined as the image of the linear evaluation map

$$\begin{array}{rccc} e_D: & \mathcal{L}(G) & \to & \mathbb{F}_q^n \\ & f & \mapsto & e_D(f) = (f(P_1), f(P_2), \ldots, f(P_n)) \end{array}.$$

The code $C_{\mathcal{L}}(D, G)$ has length n, dimension $k = \ell(G) - \ell(G - D)$, and minimum distance $d \geq d^* = n - \deg(G)$; d^* is called the *designed minimum distance* (or Goppa minimum distance). If $n > \deg(G)$, then e_D is injective and $k = \ell(G)$. If $\deg(G) > 2g - 2$, then $k = \deg(G) + 1 - g$. The *differential code* $C_\Omega(D, G)$ is defined as

$$C_\Omega(D, G) = \{(\mathrm{res}_{P_1}(\omega), \mathrm{res}_{P_2}(\omega), \ldots, \mathrm{res}_{P_n}(\omega) \mid \omega \in \Omega(G - D)\},$$

where $\Omega(G - D) = \{\omega \in \Omega(\mathcal{X}) \mid (\omega) \geq G - D\} \cup \{0\}$. The linear code $C_\Omega(D, G)$ has dimension $n - \deg(G) + g - 1$ and minimum distance at least $\deg(G) - 2g + 2$.

Now we define the automorphism group of $C_{\mathcal{L}}(D, G)$; see [27, 44]. Let $\mathcal{M}_{n,q} \leq \mathrm{GL}(n, q)$ be the subgroup of matrices having exactly one non-zero element in each row and column. For $\gamma \in \mathrm{Aut}(\mathbb{F}_q)$ and $M = (m_{i,j})_{i,j} \in \mathrm{GL}(n, q)$, let M^γ be the matrix $(\gamma(m_{i,j}))_{i,j}$. Let $\mathcal{W}_{n,q}$ be the semidirect product $\mathcal{M}_{n,q} \rtimes \mathrm{Aut}(\mathbb{F}_q)$ with multiplication $M_1\gamma_1 \cdot M_2\gamma_2 := M_1 M_2^{\gamma} \cdot \gamma_1\gamma_2$. The *automorphism group* $\mathrm{Aut}(C_{\mathcal{L}}(D, G))$ of $C_{\mathcal{L}}(D, G)$ is the subgroup of $\mathcal{W}_{n,q}$ preserving $C_{\mathcal{L}}(D, G)$, that is,

$$M\gamma(x_1, \ldots, x_n) := ((x_1, \ldots, x_n) \cdot M)^\gamma \in C_{\mathcal{L}}(D, G) \text{ for any } (x_1, \ldots, x_n) \in C_{\mathcal{L}}(D, G).$$

Let $\mathrm{Aut}_{\mathbb{F}_q}(\mathcal{X})$ be the $\mathbb{F}_q$-automorphism group of $\mathcal{X}$ and

$$\mathrm{Aut}_{\mathbb{F}_q, D, G}(\mathcal{X}) := \{\sigma \in \mathrm{Aut}_{\mathbb{F}_q}(\mathcal{X}) \mid \sigma(D) = D, \sigma(G) \approx_D G\},$$

where $G' \approx_D G$ if and only if there exists $u \in \mathbb{F}_q(\mathcal{X})$ such that $G' - G = (u)$ and $u(P_i) = 1$ for $i = 1, \ldots, n$; note that $\sigma(G) = G$ implies $\sigma(G) \approx_D G$. Then the following holds.

Proposition 3.14. ([6, Proposition 2.3]) *If any non-trivial element of* $\mathrm{Aut}_{\mathbb{F}_q}(\mathcal{X})$ *fixes less than* n $\mathbb{F}_q$*-rational places of* $\mathcal{X}$*, then* $\mathrm{Aut}(C_{\mathcal{L}}(D,G))$ *contains a subgroup isomorphic to*

$$(\mathrm{Aut}_{\mathbb{F}_q,D,G}(\mathcal{X}) \rtimes \mathrm{Aut}(\mathbb{F}_q)) \rtimes \mathbb{F}_q^*.$$

In the construction of AG codes, the condition $\mathrm{supp}(D) \cap \mathrm{supp}(G) = \emptyset$ can be removed as follows; see [68, Sec. 3.1.1]. Let $P_1, \ldots, P_n$ be distinct $\mathbb{F}_q$-rational places of $\mathcal{X}$ and $D = P_1 + \ldots + P_n$, $G = \sum n_P P$ be $\mathbb{F}_q$-rational divisors of $\mathcal{X}$. For any $i = 1, \ldots, n$ let t_i be a local parameter at P_i. The map

$$\begin{array}{rccl} e'_D: & \mathcal{L}(G) & \to & \mathbb{F}_q^n \\ & f & \mapsto & e'_D(f) = ((t^{n_{P_1}} f)(P_1), (t^{n_{P_2}} f)(P_2), \ldots, (t^{n_{P_n}} f)(P_n)) \end{array}$$

is linear. We define the *extended AG code* $C_{ext}(D,G) := e'(\mathcal{L}(G))$. Note that e'_D is not well-defined since it depends on the choise of the local parameters; yet, different choices yield extended AG codes which are equivalent. The code C_{ext} is a lengthening of $C_{\mathcal{L}}(\hat{D}, G)$, where $\hat{D} = \sum_{P_i : n_{P_i}=0} P_i$. The extended code C_{ext} is an $[n,k,d]_q$-code for which the following properties still hold

(i) $d \geq d^* := n - \deg(G)$.

(ii) $k = \ell(G) - \ell(G - D)$.

(iii) If $n > \deg(G)$, then $k = \ell(G)$; if $n > \deg(G) > 2g - 2$, then $k = \deg(G) + 1 - g$.

The differential code $C_\Omega(D,G)$ is the linear code defined by

$$C_\Omega(D,G) := \{(res_{P_1}(\omega), \ldots, res_{P_n}(\omega)) | \omega \in \Omega(G - D)\} \subset \mathbb{F}_q^n,$$

where $\Omega(G-D)$ is the space of $\mathbb{F}_q$-rational differentials η on $\mathcal{X}$ such that either $\eta = 0$ or $div(\eta) \geq G - D$ and $res_{P_j}(\eta)$ is the residue of η at P_j.

The differential code is an $[n, n - \ell(G) + \ell(G - D), d']_q$ code, where $d' \geq d^* = \deg(G) - 2g + 2$ and d^* denotes the dual designed minimum distance. It is known (see [65]) that $C_\Omega(D,G) = C_{\mathcal{L}}(D,G)^\perp$.

Definition 3.15. An algebraic curve $\mathcal{X}$ contained in a projective space of dimension n is said to be a complete intersection if the ideal I associated with $V(\mathcal{X})$ is generated by exactly $n-1$ polynomials.

One of the aims of this thesis is to find the minimum distance of some dual Algebraic-Geometric codes. To achieve this goal in some occasions we will use the following result which is a byproduct of [16, Theorem 3.5]. In what follows, we will consider a nonnegative integer m and a divisor G_m on $\mathcal{X}$ which is linearly equivalent to a scheme-theoretic intersection of $\mathcal{X}$ with a hypersurface of degree m. Also, $D = P_1 + \cdots + P_s$, $P_i \neq P_j$ is a divisor whose support is disjoint from the support of G_m.

Theorem 3.16 (Theorem 3.5, [16])**.** *Let $\mathcal{X} \subset \mathbb{P}^r$ be a non-singular curve which is a complete intersection. Consider G_m, $m \geq 2$, and D as above. If d is the minimum distance of the code $C(D, G_m)^\perp$ then*

1. *$d = m+2$ if and only if $m+2$ points of the $P_i's$ are collinear in $\mathbb{P}^r$;*
2. *$d = 2m+2$ if and only if no $m+2$ points of the $P_i's$ are collinear and there exist $2m+2$ points of the $P_i's$ lying on a plane conic (possibly reducible);*
3. *$d = 3m$ if and only if no $m+2$ points of the $P_i's$ are collinear, no $2m+2$ points lie on a plane conic, and there exist $3m$ points of the $P_i's$ coplanar and belonging to the intersection of a cubic curve and a curve of degree m having no common irreducible components;*
4. *$d \geq 3m+1$ if and only if no sub-family of the points of the $P_i's$ satisfies one of the three above configurations.*

3.2 Affine variety codes

We introduce now affine variety codes, see [21] for further information.

Let $t \geq 1$ and consider an ideal $I = \langle g_1, \ldots, g_s \rangle$ of $\mathbb{F}_q[X_1, \ldots, X_t]$, $\{X_1^q - X_1, \ldots, X_t^q - X_t\} \subset I$. The ideal I is zero-dimensional and radical; see [60]. Let $V(I) = \{P_1, \ldots, P_n\}$ be the variety of I and $R = \mathbb{F}_q[X_1, \ldots, X_t]/I$.

Definition 3.17. An affine variety code $C(I, L)$ is the image $\phi(L)$ of $L \subseteq R$, a $\mathbb{F}_q$-vector subspace of R of dimension r, given by the following isomorphism

of $\mathbb{F}_q$-vector spaces:

$$\begin{aligned} \phi : R &\longrightarrow \mathbb{F}_q^n \\ f &\longmapsto (f(P_1), \ldots, f(P_n)). \end{aligned}$$

Let L be generated by $b_1, \ldots, b_r$. Then the matrix

$$H := \begin{pmatrix} b_1(P_1) & b_1(P_2) & \ldots & b_1(P_n) \\ b_2(P_1) & b_2(P_2) & \ldots & b_2(P_n) \\ \vdots & \vdots & \vdots & \vdots \\ b_r(P_1) & b_r(P_2) & \ldots & b_r(P_n) \end{pmatrix}$$

is a generator matrix for $C(I, L)$. It is clear that there is a strong connection between affine variety codes and algebraic-geometric codes and that, depending on the choice of L, they can coincide.

Since we are interested in computing the number of minimum weight codewords of particular AG codes, the next proposition will give us a useful criterion.

Proposition 3.18. *[51, Proposition 1] Let $1 \leq w \leq n$. Let $I = \langle g_1, \ldots, g_s \rangle$ be an ideal of $\mathbb{F}_q[X_1, \ldots, X_t]$ such that $\{X_1^q - X_1, \ldots, X_t^q - X_t\} \subset I$. Let L be a subspace of $\mathbb{F}_{q^2}[X_1, \ldots, X_t]/I$ of dimension r generated by $\{b_1, \ldots, b_r\}$. Let J_w be the ideal in*

$$\mathbb{F}_q[X_{1,1}, \ldots, X_{1,t}, \ldots, X_{w,1}, \ldots, X_{w,t}, X_1, \ldots, X_w]$$

generated by

$$\begin{aligned} &\textstyle\sum_{i=1}^{w} X_i b_j(X_{i,1}, \ldots, X_{i,t}) && \text{for } j = 1, \ldots, r, \\ &g_h(X_{i,1}, \ldots, X_{i,t}) && \text{for } i = 1, \ldots, w \text{ and } h = 1, \ldots, s, \\ &Z_i^{q-1} - 1 && \text{for } i = 1, \ldots, w, \\ &\textstyle\prod_{1 \leq l \leq t}((X_{j,l} - X_{i,l})^{q-1} - 1) && \text{for } 1 \leq j < i \leq w. \end{aligned}$$

Then any solution of J_w corresponds to a codeword of $C(I, L)^{\perp}$ of weight w. Also, the number $A_w(C(I, L)^{\perp})$ of codewords of weight w is

$$A_w(C(I, L)^{\perp}) = \frac{|V(J_w)|}{w!},$$

where $V(J_w) = \left\{ y \in \mathbb{F}_q^{(t+1)w} \,\middle|\, h(y) = 0, \text{ for any } h \in J_w \right\}$.

Part II

Main results

Chapter 4

Automorphisms of algebraic curves given by separated polynomials and AG codes from the Norm-Trace curve

Deep results on automorphism groups of algebraic curves, defined over a field of characteristic zero, have been achieved after the work of Hurwitz who was the first to prove that complex curves, other than the rational and the elliptic ones, can only have a finite number of automorphisms. Afterwards, a proof of Hurwitz's result which is independent from the characteristic of the ground field was provided, increasing the interest of studying curves defined over fields of positive characteristic, as e.g. finite fields. Indeed recall that curves in positive characteristic may happen to have much larger K-automorphism group compared to their genus, as the Hurwitz bound $|G| \leq 84(g-1)$ for a K-automorphism G of a curve of genus $g \geq 2$ may do not hold when $|G|$ is divisible by the characteristic of the ground field. Artin-Schreier curves and, in particular, Hermitian curves are of this type. A family of such plane curves arises from separated polynomial. It consists of curves $\mathcal{C} : A(Y) - B(X)$ where $p \nmid m$ with $m = \deg B(X) \geq 2$ and $A(Y)$ is an additive separable polynomial. The main known properties of $\mathcal{C}$ are extracted from the local analysis of its unique singular point P_∞; see [63], where the genus, the Weierstrass semigroup at P_∞, and partial information about the ramification structure of $\mathrm{Aut}(\mathcal{X})$ at P_∞ are provided. The full

K-automorphism group of $\mathcal{C}$ fixes P_∞ except in two cases, namely, when $\mathcal{C}$ is the Hermitian curve $Y^{p^n} - Y - X^{p^n} + 1 = 0$ or the curve, $Y^{p^n} + Y - X^m = 0$ with $m < p^n$, and $p^n \equiv -1 \pmod{m}$ but now other informations are known in the literature. For $p > 2$ and $m = 2$, the latter curve is hyperelliptic. Notably for $p > 2$, these hyperelliptic curves and the Hermitian curves are the only curves whose K-automorphism groups have order larger than $8g^3$; see [37]. Deligne-Lusztig curves provide other examples of significant curves over finite fields, namely the DLS curves of Suzuki type and the DLR curves of Ree type. They are characterised by their genera and K-automorphism groups. For $p = 2$, the Hermitian curves, the DLS curves, and the hyperelliptic curves $Y^2 + Y + X^{2^h} + 1 = 0$ are the only curves with K-automorphism groups of order larger than $8g^3$.

In this chapter we compute the full automorphism group of $\mathcal{C}$ when $m \not\equiv 1 \pmod{p^n}$ and $B(X) = X^m$. Moreover, some sufficient conditions for $\mathrm{Aut}(\mathcal{X})$ to imply that $B(X) = X^m$ up to an affine transformation are provided. Also, the full automorphism group of the Norm-Trace curve $\mathcal{C} : X^{(q^r-1)/(q-1)} = Y^{q^{r-1}} + Y^{q^{r-2}} + \ldots + Y$ is computed. An important application of curves over finite fields is the construction of certain linear codes, called Algebraic Geometric codes (AG codes for short). The parameters of an AG code constructed from a curve $\mathcal{C}$ strictly depend on the geometry of $\mathcal{C}$, and in particular on two fixed divisors on $\mathcal{C}$. The Norm-Trace curve was used in the literature to construct one-point or two-point AG codes; see [4, 26, 57]. In this chapter we determine explicitly the parameters of a class of one-point AG codes on the Norm-Trace curve, starting from divisors on $\mathcal{C}$ which are invariant under the whole automorphism group of the curve. Such codes turn out to inherit many automorphisms from the Norm-Trace curve.

4.1 Curves given by separated polynomials

Throughout the chapter, $\mathcal{C}$ is a projective plane curve defined over the algebraic closure K of a finite field of prime order $\mathbb{F}_p$ by an affine equation

$$A(Y) = B(X), \tag{4.1}$$

satisfying the following conditions:

1. $\deg(\mathcal{C}) \geq 4$;
2. $A(Y) = a_n Y^{p^n} + a_{n-1} Y^{p^{n-1}} + \ldots + a_0 Y$, $a_j \in K$, $a_0, a_n \neq 0$;

3. $B(X) = b_m X^m + b_{m-1} X^{m-1} + \ldots + b_1 X + b_0$, $b_j \in K$, $b_m \neq 0$;

4. $m \not\equiv 0 \pmod{p}$;

5. $n \geq 1$, $m \geq 2$.

Note that 2 occurs if and only if $A(Y + a) = A(Y) + A(a)$ for every $a \in K$, that is, the polynomial $A(Y)$ is additive. The basic properties of $\mathcal{C}$ are collected in the following lemmas; see [38, Section 12.1] and [63].

In the following, the couple (X, Y) and the triple (Z, X, Y) are used to denote affine and homogeneous coordinates of points of $\mathcal{C}$ in $\mathbb{P}^2(K)$, respectively.

Lemma 4.1. *The curve $\mathcal{C}$ is an irreducible plane curve with at most one singular point.*

(i) *If $|m - p^n| = 1$, then $\mathcal{C}$ is non-singular.*

(ii) (a) *If $m > p^n + 1$, then $P_\infty = (0, 0, 1)$ is an $(m - p^n)$-fold point of $\mathcal{C}$.*

(b) *If $p^n > m + 1$, then $P_\infty = (0, 1, 0)$ is a $(p^n - m)$-fold point of $\mathcal{C}$.*

(c) *In both cases, P_∞ is the centre of only one branch of $\mathcal{C}$; also, P_∞ is the unique infinite point of $\mathcal{C}$.*

(iii) *$\mathcal{C}$ has genus $g = \frac{(p^n-1)(m-1)}{2}$;*

(iv) *Let $K(x, y)$ with $A(y) = B(x)$ denote the function field of $\mathcal{C}$.*

(a) *A transformation $\tau_a : (x, y) \mapsto (x, y + a)$ preserves $\mathcal{C}$ if and only if $A(a) = 0$;*

(b) *The set $G = \{\tau_a \mid A(a) = 0\}$ is an elementary abelian subgroup of $\mathrm{Aut}_K(K(x, y))$ of order p^n. Every nontrivial element of G fixes the unique place $\mathcal{P}_\infty$ centered at P_∞, and G acts transitively on the zeros of x;*

(c) *the sequence of ramification subgroups of G at $\mathcal{P}_\infty$ is*

$$G = G^{(1)}_{\mathcal{P}_\infty} = G^{(2)}_{\mathcal{P}_\infty} = \ldots = G^{(m)}_{\mathcal{P}_\infty}, \quad G^{(m+1)}_{\mathcal{P}_\infty} = \{1\};$$

(d) *$\{\mathcal{P}_\infty\}$ is the unique short orbit of G, and the different divisor in the Hilbert different formula ([38, Theorem 11.70]) applied to the extension $K(x, y)/K(x, y)^G$ is*

$$(p^n - 1)(m + 1)\mathcal{P}_\infty;$$

(e) *$K(x,y)^G$ is rational, and $\mathcal{C}$ has p-rank zero.*

An automorphism of the function field $K(x,y)$ with $A(y) = B(x)$ of $\mathcal{C}$ defined as in (iv)(a) will be referred to as a *translation.*

Lemma 4.2. *Let M be a K-automorphism group of $\mathcal{C}$, and let $M_{\mathcal{P}_\infty} = M^{(1)}_{\mathcal{P}_\infty} \rtimes H$ where $p \nmid |H|$. Then*

(i) *$|H|$ divides $m(p^n-1)$;*

(ii) *$|M^{(1)}_{\mathcal{P}_\infty}| \le p^n(m-1)^2 = \frac{4p^n}{(p^n-1)^2} g^2$;*

(iii) *$|M^{(1)}_{\mathcal{P}_\infty}| = p^n$ when $m \not\equiv 1 \pmod{p^n}$, and so $g \not\equiv 0 \pmod{p^n}$;*

(iv) *$|M^{(2)}_{\mathcal{P}_\infty}| = p^n$ when $m \equiv 1 \pmod{p^n}$, and so $g \equiv 0 \pmod{p^n}$.*

Lemma 4.3. *The K-automorphism group $\mathrm{Aut}_K(\mathcal{C})$ fixes the place $\mathcal{P}_\infty$ except in the following two cases.*

1. (a) *Up to a linear substitution on X and Y, $\mathcal{C}$ is the curve $Y^{p^n} + Y = X^m$, with $m < p^n$, $p^n \equiv -1 \pmod{m}$;*

   (b) *$\mathrm{Aut}_K(\mathcal{C})$ contains a cyclic normal subgroup C_m of order m such that $\mathrm{Aut}_K(\mathcal{C})/C_m \cong PGL(2,p^n)$;*

   (c) *C_m fixes each of the p^n+1 places with the same Weierstrass semigroup as $\mathcal{P}_\infty$;*

   (d) *$\mathrm{Aut}_K(\mathcal{C})/C_m$ acts on the set of such p^n+1 places as $PGL(2,p^n)$.*

2. (a) *Up to a linear substitution on X and Y, $\mathcal{C}$ is the Hermitian curve $\mathcal{H}_{p^n} : Y^{p^n} + Y = X^{p^n+1}$;*

   (b) *$\mathrm{Aut}_K(\mathcal{C}) \cong PGU(3,p^n)$;*

   (c) *$\mathrm{Aut}_K(\mathcal{C})$ acts on the set of all places with the same Weierstrass semigroup as $\mathcal{P}_\infty$;*

   (d) *$\mathrm{Aut}_K(\mathcal{C})$ acts on the set of such places as $PGU(3,q)$ on the Hermitian unital.*

4.2 On the automorphism group of $\mathcal{C}$

At first we consider the Norm-Trace curve $\mathcal{N}_{q,r}$ with affine equation

$$X^{\frac{q^r-1}{q-1}} = Y^{q^{r-1}} + Y^{q^{r-2}} + \cdots + Y,$$

where q is a p-power and r is a positive integer. For $r = 2$, this is the $\mathbb{F}_{q^2}$-maximal Hermitian curve, with automorphism group isomorphic to $PGU(3, q)$. For $r > 2$, we determine the automorphism group of $\mathcal{N}_{q,r}$.

Theorem 4.4. *For $r \geq 3$, $\mathrm{Aut}_K(\mathcal{N}_{q,r})$ has order $q^{r-1}(q^r - 1)$ and is a semidirect product $G \rtimes C$, where*

$$G = \left\{(x, y) \mapsto (x, y + a) \mid Tr_{q^r|q}(a) = 0\right\}, \quad C = \{(x, y) \mapsto (bx, b^{\frac{q^r-1}{q-1}} y) \mid b \in \mathbb{F}_{q^r}^*\}.$$

Proof. Suppose that $\mathcal{N}_{q,r} \cong \mathcal{H}_{\bar{q}}$ for some p-power $\bar{q}$. From Lemma 4.1 (iii), $g(\mathcal{N}_{q,r}) = g(\mathcal{H}_{\bar{q}})$ reads $\frac{(\frac{q^r-1}{q-1}-1)(q^{r-1}-1)}{2} = \frac{\bar{q}(\bar{q}-1)}{2}$. This implies $\bar{q} = q$ and $r = 2$, a contradiction to the assumption on r.

Now suppose that $\mathcal{N}_{q,r}$ is isomorphic to the curve $\mathcal{X} : X^s = Y^{\bar{q}} + Y$ for some p-power $\bar{q}$, with $s < \bar{q}$, $s \mid (\bar{q} + 1)$. From Lemma 4.2(iii), the Sylow p-subgroups $\mathrm{Aut}_K(\mathcal{N}_{q,r})^{(1)}_{\mathcal{P}_\infty}$ and $\mathrm{Aut}_K(\mathcal{X})^{(1)}_{\mathcal{P}_\infty}$ of $\mathrm{Aut}_K(\mathcal{N}_{q,r})_{\mathcal{P}_\infty}$ and $\mathrm{Aut}_K(\mathcal{X})_{\mathcal{P}_\infty}$ have order q^{r-1} and $\bar{q}$, respectively. From Lemma 4.1(e) $\mathcal{N}_{q,r}$ and $\mathcal{X}$ have zero p-rank. Hence, $\mathrm{Aut}_K(\mathcal{N}_{q,r})^{(1)}_{\mathcal{P}_\infty}$ and $\mathrm{Aut}_K(\mathcal{X})^{(1)}_{\mathcal{P}_\infty}$ are Sylow p-subgroups of $\mathrm{Aut}_K(\mathcal{N}_{q,r}) \cong \mathrm{Aut}_K(\mathcal{X})$; see [38, Lemma 11.129]. Therefore $q^{r-1} = \bar{q}$. Then $g(\mathcal{N}_{q,r}) = g(\mathcal{X})$ yields $s = \frac{q^r-1}{q-1} = \bar{q} + \cdots + q + 1$, a contradiction to $s < \bar{q}$.

From Lemma 4.3, this proves that $\mathrm{Aut}_K(\mathcal{N}_{q,r})$ fixes $\mathcal{P}_\infty$. By direct checking $\mathrm{Aut}_K(\mathcal{N}_{q,r})$ contains the group $G \rtimes C$ defined in the statement of the theorem. From Lemma 4.3, $\mathrm{Aut}_K(\mathcal{N}_{q,r}) = G \rtimes H$, where H is a cyclic group. From Schur-Zassenhaus Theorem, H contains C up to conjugation. By Lemma 4.1(e) the quotient curve $\mathcal{N}_{q,r}/G$ is rational, and its function field is $K(x)$. Hence the automorphism group $\bar{H} \cong H$ of $\mathcal{N}_{q,r}/G$ induced by H has exactly two fixed places and acts semiregularly elsewhere; see [41, Hauptsatz 8.27]. Since $C \leq H$, the two places fixed by $\bar{H}$ are the place $\bar{\mathcal{P}}_\infty$ under $\mathcal{P}_\infty$ and the zero $\bar{P}_0$ of x. Let $\Omega = \{P_{(0,0)}, P_{(0,a_2)}, \ldots, P_{(0,a_{q^r-1})}\}$ be the orbit of G lying over $\bar{P}_0$, so that $\mathrm{Aut}_K(\mathcal{N}_{q,r})$ acts on Ω; we denote by $P_{(0,0)} \in \Omega$ the zero of y, centered at the origin $(0, 0)$. The group H has a fixed point in Ω by the Orbit-Stabilizer theorem, and $P_{(0,0)}$ is the only fixed place of C other than $\mathcal{P}_\infty$; thus, H fixes $P_{(0,0)}$.

Therefore, H fixes the unique pole of x and y, fixes the unique zero of y, and acts on the q^{r-1} simple zeros of x. This implies that a generator h of H acts as $h(x) = \mu x$, $h(y) = \rho y$ for some $\mu, \rho \in K^*$. By direct computation, h is an automorphism of $\mathcal{N}_{q,r}$ if and only if $\rho = \rho^q$ and $\mu^{\frac{q^r-1}{q-1}} = \rho$. Hence, $H = C$. □

The following result generalizes Theorem 4.4.

Theorem 4.5. *Suppose that $m \not\equiv 1 \pmod{p^n}$ and $B(X) = X^m$. Then one of the following two cases occurs.*

(i) m divides $p^n + 1$ and $A(Y)$ is p^n-linearized, that is, $A(Y) = a_n Y^{p^n} + a_0 Y$. In this case, $\mathcal{C}$ is projectively equivalent to the curve $\mathcal{Q}_m$ with equation $X^m = Y^{p^n} + Y$ described in Case 1 of Lemma 4.3.

(ii) m does not divide $p^n + 1$ or $A(Y)$ is not p^n-linearized. Let $d = \gcd(j \geq 1 : a_j \neq 0)$ be the largest integer such that $A(Y)$ is p^d-linearized. Then $\mathrm{Aut}_K(\mathcal{C})$ has order $p^n m(p^d - 1)$ and $\mathrm{Aut}_K(\mathcal{C}) = G \rtimes C$, where $G = \{(x, y) \mapsto (x, y + a) \mid A(a) = 0\}$ and $C = \{(x, y) \mapsto (bx, b^m y) \mid b^{m(p^d-1)} = 1\}$.

Proof. Let S be the stabilizer of $\mathcal{P}_\infty$ in $\mathrm{Aut}_K(\mathcal{C})$. By direct checking, S contains the semidirect product $G \rtimes C$. By Lemma 4.2, $S = G \rtimes H$, where H is a cyclic group of order coprime to p. By Schur-Zassenhaus Theorem, H contains C up to conjugation. Arguing as in the proof of Theorem 4.4, we have that $\mathcal{C}/G$ is rational, and any nontrivial of the induced automorphism group $\bar{H} \cong H \leq \mathrm{Aut}_K(\mathcal{C}/G)$ fixes the pole $\bar{\mathcal{P}}_\infty$ and the zero $\bar{P}_0$ of x. Hence H acts on the p^n distinct places of $\mathcal{C}$ lying over $\bar{P}$, and H fixes one of them by the Orbit-Stabilizer theorem. The only fixed place of C different from $\mathcal{P}_\infty$ is the unique zero P_0 of y, centered at the origin $(0, 0)$. Let h be a generator of H. We have shown that h fixes the zero and the pole of y, which implies $h(y) = \rho y$ for some $\rho \in K$. Also, h fixes the pole and acts on the simple zeros of x; this implies $h(x) = \mu x$ for some $\mu \in K$. By direct checking, h normalizes G if and only if $A(\mu a) = 0$ for all $a \in K$ satisfying $A(a) = 0$. As $A(Y)$ is separable, this happens if and only if $A(\mu Y) = A(Y)$. This is equivalent to $\mu \in \mathbb{F}^*_{p^d}$, with d defined as in the statement of the theorem. Then, in order for h to be an automorphism of $\mathcal{C}$, we have $\rho^m = \mu$. We have shown that $S = G \rtimes C$.

By Lemma 4.3, either $\mathrm{Aut}_K(\mathcal{C}) = G \rtimes C$ and Case *(ii)* holds, or $\mathcal{C}$ is isomorphic to the curve $\mathcal{Q}_s : X^s = Y^{\bar{q}} + Y$ with $s \mid (\bar{q} + 1)$, $s < \bar{q}$. Suppose that $\mathcal{C} \cong \mathcal{Q}_s$. By Lemma 4.2 the Sylow p-subgroups of $\mathrm{Aut}_K(\mathcal{C})$ and $\mathrm{Aut}_K(\mathcal{Q}_s)$ have size p^n and $\bar{q}$ respectively, so that $\bar{q} = p^n$; as $g(\mathcal{C}) = g(\mathcal{Q}_s)$, we have $s = m$. The normalizer in $\mathrm{Aut}_K(\mathcal{Q}_m)$ of a Sylow p-subgroup contains a cyclic group of order $p^n - 1$, by Lemma 4.3(b). Hence, the same

holds in $\mathrm{Aut}_K(\mathcal{C})$ and $d = n$; this means that $\mathcal{C}$ has equation $X^m = a_n Y^{p^n} + a_0 Y$.

Conversely, if $\mathcal{C}$ has equation $X^m = a_n Y^{p^n} + a_0 Y$, then $\mathcal{C}$ is isomorphic to $\mathcal{Q}_m$. In fact, define $\varphi : (x, y) \mapsto (x', y') := (\gamma x, \delta a_0 y)$ with $\delta^{p^n-1} = ab^{-p^n}$ and $\gamma^m = \delta$. Then $K(x, y) = K(x', y')$ and $\varphi(\mathcal{C}) = \mathcal{Q}_m$. Now the proof is complete. □

Next result provides a converse to Theorem 4.5 and extends [38, Theorem 12.8].

Theorem 4.6. *Let $d = \gcd(j \geq 1 : a_j \neq 0)$ be the largest integer such that $A(Y)$ is p^d-linearized. If $|\mathrm{Aut}_K(\mathcal{C})_{P_\infty}|/|\mathrm{Aut}_K(\mathcal{C})^{(1)}_{P_\infty}| \geq m(p^d-1)$, then equality holds, and $B(X) = X^m$ up to an affine transformation in X.*

Proof. Let S be the stabilizer of $\mathcal{P}_\infty$ in $\mathrm{Aut}_K(\mathcal{C})$, H be a cyclic complement of $S^{(1)}$ in S, and α be a generator of H. By Lemma 4.2, $G = \{(x, y) \mapsto (x, y + a) \mid A(a) = 0\}$ is normal in S. Hence, α induces an automorphism $\bar{\alpha}$ of the quotient curve $\mathcal{C}/G$; by Lemma 4.1(e), $\mathcal{C}/G$ is rational with function field $K(x)$. From [41, Haptsatz 8.27], $\bar{\alpha}$ has two fixed places in $K(x)$ and acts semiregularly elsewhere. Up to an affine substitution in x, these two place are the pole $\bar{\mathcal{P}}_\infty$ and the zero of x. Thus, $\alpha(x) = \bar{\alpha}(x) = bx$, for some $b \in K^*$ of order $ord(b) = ord(\alpha)$. Since α fixes the unique pole $\mathcal{P}_\infty$ of y and the Weierstrass semigroup $H(\mathcal{P}_\infty)$ is generated by $-v_{\mathcal{P}_\infty}(y) = p^n$ and $-v_{\mathcal{P}_\infty}(x) = m$, we have that $\alpha(y) = ay + Q(x)$, where $a \in K^*$ and $Q(X)$ is a polynomial satisfying either $Q(X) = 0$ or $\deg(Q(X)) \cdot p^n < m$. Since α is an automorphism of $\mathcal{C}$, the polynomial $A(aY + Q(X)) - B(bX)$ is a multiple of $A(Y) - B(X)$, say

$$A(aY + Q(X)) - B(bX) = k_1(A(Y) - B(X)) \tag{4.2}$$

with $k_1 \in K^*$. As A is a separable polynomial, Equation (4.2) implies $A(aY) = kA(Y)$ and hence $k_1 = a^{p^j}$ for any j such that $a_j \neq 0$; thus, $k_1 = a$ and $a^{p^d-1} = 1$. Equation (4.2) also implies $B(bX) = k_1 B(X) + A(Q(X))$ and hence $k_1 = b^m$; thus, $(b^m)^{p^d-1} = 1$ which yields $|H| = m(p^d - 1)$.

Note that $\beta := \alpha^{p^d-1}$ has order m and that it acts as $\beta(x) = b^{p^d-1}x$, $\beta(y) = y + Q(b^{p^d-2}x)$. As $\beta \in \mathrm{Aut}_K(\mathcal{C})$, we have

$$A(Y + Q(b^{p^d-2}X)) - B(b^{p^d-1}X) = k_2(A(Y) - B(X))$$

with $k_2 \in K^*$. Then $k_2 = 1$ and

$$B(b^{p^d-1}X) - B(X) = A(Q(b^{p^d-2}X)). \tag{4.3}$$

We want to show that $\beta(y) = y$. Suppose by contradiction that $Q(b^{p^d-2}X) \neq 0$. If $b^{p^d-1} = 1$ or $Q(b^{p^d-2}X)$ is a nonzero constant, then the $ord(\beta)$ is a multiple of p, a contradiction to $ord(\beta) = m$. If $b^{p^d-1} \neq 1$ and $\deg(Q(b^{p^d-2}X)) > 1$, then the left-hand side and the right-hand side in Equation (4.3) have degree m and $p^n \cdot \deg(Q(b^{p^d-2}X))$, respectively; a contradiction to $p \nmid m$. Therefore, $\beta(x) = b^{p^d-1}x$ and $\beta(y) = y$, with $ord(b) = m(p^d-1)$. Since $\beta \in \mathrm{Aut}(\mathcal{C})$, $B(X) = \lambda X^m$ for some $\lambda \in K^*$, that is, $B(X) = X^m$ up to scaling. □

Even if $B(X)$ is not a monomial, the argument of the proof of Theorem 4.6 shows the following result.

Proposition 4.7. *Let* $\mathrm{Aut}_K(\mathcal{C})_{P_\infty} = \mathrm{Aut}_K(\mathcal{C})^{(1)}_{P_\infty} \rtimes H$ *with* $H = \langle \alpha \rangle$, *and let* $d = \gcd(j \geq 1 : a_j \neq 0)$ *be the largest integer such that* $A(Y)$ *is* p^d*-linearized. Then* $\alpha(x) = bx + c$ *for some* $b, c \in K$, *and* $\alpha(B(x)) = aB(x)$ *for some* $a \in \mathbb{F}^*_{p^d}$.

Remark 4.8. Once that $B(X)$ is explicitely given, Proposition 4.7 provides a method to find H. In fact, H has one fixed place in $K(x)$ centered at an affine point and acts semiregularly on the other places centered at affine points; also, H acts on the zeros of $B(x)$ with the same multiplicity. For instance:

- If $B(X)$ has more than one root, but only one root with fixed multiplicity $M > 1$, then $|H|$ divides either M or $M - 1$.
- If $B(X)$ has more than one root, and all the root have the same multiplicity $M > 1$, then H is trivial and $\mathrm{Aut}_K(\mathcal{C})$ is a p-group of order p^n.

4.3 One-point AG codes on the Norm-Trace curves

Let $\ell, r \in \mathbb{N}$, $r \geq 3$, and let $\mathcal{N}_{q,r}$ be the Norm-Trace curve of genus g as defined in Section 4.2. Let $\Omega = \{P_{(0,y_1)}, \ldots, P_{(0,y_{q^{r-1}})}\}$ be the set of the q^{r-1} $\mathbb{F}_{q^r}$-rational places of $\mathcal{N}_{q,r}$ which are the zeros of x; here, $P_{(a,b)}$ denotes the unique place centered at the affine point (a, b) of $\mathcal{N}_{q,r}$. Let $\Theta :=$

$\mathcal{N}_{q,r}(\mathbb{F}_{q^r}) \setminus (\Omega \cup \mathcal{P}_\infty)$, where $\mathcal{P}_\infty$ is the place at infinity of $\mathcal{N}_{q,r}$. As pointed out in the proof of Theorem 4.4, the principal divisors of the coordinate functions are the following:

- $(x) = \sum_{P \in \Omega} P - q^{r-1}\mathcal{P}_\infty$;
- $(y) = \frac{q^r-1}{q-1} P_{(0,0)} - \frac{q^r-1}{q-1}\mathcal{P}_\infty$.

Define the $\mathbb{F}_{q^r}$-divisors

$$G := \ell q^{r-1}\mathcal{P}_\infty \quad \text{and} \quad D := \sum_{P \in \Theta} P.$$

Since $|\mathcal{N}_{q,r}(\mathbb{F}_{q^r})| = q^{2r-1} + 1$ (see [26, Lemma 2]), D has degree $q^{2r-1} - q^{r-1}$. Denote by $C := C_{\mathcal{L}}(D, G)$ the associated functional one-point AG code over $\mathbb{F}_{q^r}$ having length $n = q^{2r-1} - q^{r-1}$, dimension k, and minimum distance d. The designed minimum distance is

$$d^* = n - \deg(G) = q^{2r-1} - (\ell + 1)q^{r-1}.$$

The parameters of one-point AG codes on the Norm-Trace curves have been investigated by several authors, such as Miura and Kamiya [55] and Geil [26].

Proposition 4.9 ([55, Theorem 5]; see also [26, Theorem 2])**.** *The code C attains the designed minimum distance d^*.*

Now we turn to the dimension of C.

If $\frac{q^r-1}{q-1} - 2 \leq \ell \leq q^r - 2$, then $n > \deg(G) > 2g-2$ and the Riemann-Roch Theorem can be applied to conclude that

$$k = \deg(G) + 1 - g = \ell q^{r-1} + 1 - \frac{1}{2}\left(\frac{q^r - 1}{q - 1} - 1\right)\left(q^{r-1} - 1\right).$$

If $\ell < \frac{q^r-1}{q-1} - 2$, then k can be computed via the Weierstrass semigroup $H(\mathcal{P}_\infty)$ at $\mathcal{P}_\infty$, which is known to be generated by q^{r-1} and $\frac{q^r-1}{q-1}$; see [4]. In fact, k equals the number of non-gaps at $\mathcal{P}_\infty$ which are smaller than or equal to ℓq^{r-1}, as pointed out in [55, Theorem 5]. We provide an explicit formula for k.

Proposition 4.10. *If $1 \leq \ell \leq \frac{q^r-1}{q-1} - 3$, then the dimension of C is*

$$k = \ell + 1 + \frac{(q-1)}{2}\left\lfloor \frac{\ell}{q} \right\rfloor \left(\left\lfloor \frac{\ell}{q} \right\rfloor + 1 \right) + \frac{(q^2 - 3q + 2)}{2} + \Delta,$$

where,

$$\Delta = \frac{(q-1)^2}{2}\left(\frac{\ell}{q}-1\right)^2 + \left(\frac{(q-3)(q-1)}{2}\right)\left(\frac{\ell}{q}-1\right) + \frac{q(q-1)}{2}\left(\frac{\ell}{q}-1\right),$$

if $\ell \equiv 0 \pmod q$*;*

$$\Delta = \frac{(q-1)^2}{2}\left\lfloor\frac{\ell}{q}\right\rfloor^2 + \left(\frac{(q-3)(q-1)}{2}\right)\left\lfloor\frac{\ell}{q}\right\rfloor + \frac{q(q-1)}{2}\left\lfloor\frac{\ell}{q}\right\rfloor,$$

if $\ell \equiv -1 \pmod q$*;*

$$\Delta = \frac{(q-1)}{2}\left[\left(\ell-\left\lfloor\frac{\ell}{q}\right\rfloor q\right)\left\lfloor\frac{\ell}{q}\right\rfloor^2+\left(q-\ell+\left\lfloor\frac{\ell}{q}\right\rfloor q-1\right)\left(\left\lfloor\frac{\ell}{q}\right\rfloor-1\right)^2\right]+\left(\frac{q-3}{2}\right)\left[\left(\ell-\left\lfloor\frac{\ell}{q}\right\rfloor q\right)\left\lfloor\frac{\ell}{q}\right\rfloor\right.$$
$$\left.+\left(q-\ell+\left\lfloor\frac{\ell}{q}\right\rfloor q-1\right)\left(\left\lfloor\frac{\ell}{q}\right\rfloor-1\right)\right]+\frac{1}{2}\left\lfloor\frac{\ell}{q}\right\rfloor\left(\ell-\left\lfloor\frac{\ell}{q}\right\rfloor q\right)\left(\ell-\left\lfloor\frac{\ell}{q}\right\rfloor q+1\right)$$
$$+\frac{1}{2}\left(\left\lfloor\frac{\ell}{q}\right\rfloor-1\right)\left(q-1-\ell+\left\lfloor\frac{\ell}{q}\right\rfloor q\right)\left(q+\ell-\left\lfloor\frac{\ell}{q}\right\rfloor q\right),$$

otherwise.

Proof. Let $c := (q^r-1)/(q-1)$. By the assumption on ℓ, $\deg(G) < n$; hence, $k = \ell(G)$. This means that k equals the number of non-gaps $h \in H(\mathcal{P}_\infty)$ at $\mathcal{P}_\infty$ satisfying $h \le \ell q^{r-1}$. From [26] (see also [4]), k is the number of couples $(i,j) \in \mathbb{N}^2$ such that

$$0 \le i < q^r, \quad 0 \le j < q^{r-1}, \quad iq^{r-1} + jc \le \ell q^{r-1}.$$

Since $\ell \le c-3$, this implies

$$k = \sum_{i=0}^{\ell}\left(\left\lfloor\frac{(\ell-i)q^{r-1}}{c}\right\rfloor + 1\right) = \ell + 1 + \sum_{s=0}^{\ell}\left\lfloor\frac{sq^{r-1}}{c}\right\rfloor.$$

Write $s = aq+b$ with $a \ge 0$ and $1 \le b \le q$. The condition $s \le \ell$ is equivalent to $a \le \lfloor\frac{\ell-b}{q}\rfloor$ when $b < q$, and to $a \le \lfloor\frac{\ell}{q}\rfloor - 1$ when $b = q$. Hence,

$$k = \ell + 1 + \sum_{a=0}^{\lfloor\frac{\ell}{q}\rfloor-1}\left\lfloor\frac{(aq+q)q^{r-1}}{c}\right\rfloor + \sum_{b=1}^{q-1}\sum_{a=0}^{\lfloor\frac{\ell-b}{q}\rfloor}\left\lfloor\frac{(aq+b)q^{r-1}}{c}\right\rfloor. \tag{4.4}$$

By direct computation,

$$\sum_{a=0}^{\lfloor\frac{\ell}{q}\rfloor-1}\left\lfloor\frac{(aq+q)q^{r-1}}{c}\right\rfloor = \sum_{a=0}^{\lfloor\frac{\ell}{q}\rfloor-1}\left\lfloor(a+1)(q-1)+\frac{a+1}{c}\right\rfloor = \sum_{a=0}^{\lfloor\frac{\ell}{q}\rfloor-1}(a+1)(q-1) = \frac{1}{2}(q-1)\left\lfloor\frac{\ell}{q}\right\rfloor\left(\left\lfloor\frac{\ell}{q}\right\rfloor+1\right). \tag{4.5}$$

Also,

$$\frac{(aq+b)q^{r-1}}{c} = a(q-1)+b-1+\frac{q^r-1+a(q-1)-b(q^{r-1}-1)}{q^r-1}.$$

Assume that $1 \leq b \leq q-1$ and $0 \leq a \leq \left\lfloor \frac{\ell-b}{q} \right\rfloor \leq \left\lfloor \frac{\ell}{q} \right\rfloor$. By the assumption on ℓ follows $a \leq q\frac{q^{r-2}-1}{q-1}$. Thus,

$$\frac{q^r-1+a(q-1)-b(q^{r-1}-1)}{q^r-1} > 0, \quad \frac{q^r-1+a(q-1)-b(q^{r-1}-1)}{q^r-1} < 1,$$

so that $\left\lfloor \frac{(aq+b)q^{r-1}}{c} \right\rfloor = a(q-1)+b-1$. Thus,

$$\sum_{b=1}^{q-1}\sum_{a=0}^{\lfloor \frac{\ell-b}{q} \rfloor} \left\lfloor \frac{(aq+b)q^{r-1}}{c} \right\rfloor = \sum_{b=1}^{q-1}\sum_{a=0}^{\lfloor \frac{\ell-b}{q} \rfloor} (a(q-1)+b-1) =$$

$$\frac{(q-1)}{2}\sum_{b=1}^{q-1}\left\lfloor \frac{\ell-b}{q} \right\rfloor^2 + \left(\frac{q-3}{2}\right)\sum_{b=1}^{q-1}\left\lfloor \frac{\ell-b}{q} \right\rfloor + \sum_{b=1}^{q-1} b\left\lfloor \frac{\ell-b}{q} \right\rfloor + \frac{q^2-3q+2}{2}.$$

Denote by,

$$A = \frac{(q-1)}{2}\sum_{b=1}^{q-1}\left\lfloor \frac{\ell-b}{q} \right\rfloor^2, \quad B = \left(\frac{q-3}{2}\right)\sum_{b=1}^{q-1}\left\lfloor \frac{\ell-b}{q} \right\rfloor, \quad C = \sum_{b=1}^{q-1} b\left\lfloor \frac{\ell-b}{q} \right\rfloor.$$

We note that for a given $b = 1, \ldots, q-1$, holds that $\left\lfloor \frac{\ell-b}{q} \right\rfloor \neq \left\lfloor \frac{\ell-b-1}{q} \right\rfloor$ if and only if $\ell - b \equiv 0 \pmod{q}$. Thus if $\ell \equiv 0 \pmod{q}$ then $\left\lfloor \frac{\ell-b}{q} \right\rfloor = \frac{\ell}{q} - \left\lceil \frac{b}{q} \right\rceil = \frac{\ell}{q} - 1$, for every $b = 1, \ldots, q-1$; if $\ell \equiv q-1 \pmod{q}$ then $\left\lfloor \frac{\ell-b}{q} \right\rfloor = \left\lfloor \frac{\ell}{q} \right\rfloor$; while $\left\lfloor \frac{\ell-b}{q} \right\rfloor = \left\lfloor \frac{\ell}{q} \right\rfloor$ for $b = 1, \ldots, \ell - \left\lfloor \frac{\ell}{q} \right\rfloor q$ and $\left\lfloor \frac{\ell-b}{q} \right\rfloor = \left(\left\lfloor \frac{\ell}{q} \right\rfloor - 1\right)$ for $b = \ell - \left\lfloor \frac{\ell}{q} \right\rfloor q + 1, \ldots, q-1$, if $\ell \not\equiv 0, q-1 \pmod{q}$. In particular this implies that

$$A = \frac{(q-1)}{2}\sum_{b=1}^{q-1}\left(\frac{\ell}{q}-1\right)^2 = \frac{(q-1)^2}{2}\left(\frac{\ell}{q}-1\right)^2,$$

if $\ell \equiv 0 \pmod{q}$,

$$A = \frac{(q-1)}{2}\sum_{b=1}^{q-1}\left\lfloor \frac{\ell}{q} \right\rfloor^2 = \frac{(q-1)^2}{2}\left\lfloor \frac{\ell}{q} \right\rfloor^2,$$

if $\ell \equiv q-1 \pmod q$, and

$$A = \frac{(q-1)}{2} \sum_{b=1}^{\ell-\left\lfloor \frac{\ell}{q} \right\rfloor q} \left\lfloor \frac{\ell}{q} \right\rfloor^2 + \frac{(q-1)}{2} \sum_{b=\ell-\left\lfloor \frac{\ell}{q} \right\rfloor q+1}^{q-1} \left(\left\lfloor \frac{\ell}{q} \right\rfloor - 1 \right)^2 =$$

$$\frac{(q-1)}{2} \left[\left(\ell - \left\lfloor \frac{\ell}{q} \right\rfloor q \right) \left\lfloor \frac{\ell}{q} \right\rfloor^2 + \left(q - \ell + \left\lfloor \frac{\ell}{q} \right\rfloor q - 1 \right) \left(\left\lfloor \frac{\ell}{q} \right\rfloor - 1 \right)^2 \right],$$

otherwise. Analagously,

$$B = \frac{(q-3)}{2} \sum_{b=1}^{q-1} \left(\frac{\ell}{q} - 1 \right) = \frac{(q-3)(q-1)}{2} \left(\frac{\ell}{q} - 1 \right),$$

if $\ell \equiv 0 \pmod q$,

$$B = \frac{(q-3)}{2} \sum_{b=1}^{q-1} \left\lfloor \frac{\ell}{q} \right\rfloor = \frac{(q-1)(q-3)}{2} \left\lfloor \frac{\ell}{q} \right\rfloor,$$

if $\ell \equiv q-1 \pmod q$, while

$$B = \frac{(q-3)}{2} \sum_{b=1}^{\ell-\left\lfloor \frac{\ell}{q} \right\rfloor q} \left\lfloor \frac{\ell}{q} \right\rfloor + \frac{(q-3)}{2} \sum_{b=\ell-\left\lfloor \frac{\ell}{q} \right\rfloor q+1}^{q-1} \left(\left\lfloor \frac{\ell}{q} \right\rfloor - 1 \right) =$$

$$\left(\frac{q-3}{2} \right) \left[\left(\ell - \left\lfloor \frac{\ell}{q} \right\rfloor q \right) \left\lfloor \frac{\ell}{q} \right\rfloor + \left(q - \ell + \left\lfloor \frac{\ell}{q} \right\rfloor q - 1 \right) \left(\left\lfloor \frac{\ell}{q} \right\rfloor - 1 \right) \right]$$

otherwise, and

$$C = \sum_{b=1}^{q-1} b \left(\frac{\ell}{q} - 1 \right) = \frac{q(q-1)}{2} \left(\frac{\ell}{q} - 1 \right),$$

if $\ell \equiv 0 \pmod q$,

$$C = \sum_{b=1}^{q-1} b \left\lfloor \frac{\ell}{q} \right\rfloor = \frac{q(q-1)}{2} \left\lfloor \frac{\ell}{q} \right\rfloor,$$

if $\ell \equiv q-1 \pmod q$ and

$$C = \sum_{b=1}^{\ell-\left\lfloor \frac{\ell}{q} \right\rfloor q} b \left\lfloor \frac{\ell}{q} \right\rfloor + \sum_{b=\ell-\left\lfloor \frac{\ell}{q} \right\rfloor q+1}^{q-1} b \left(\left\lfloor \frac{\ell}{q} \right\rfloor - 1 \right) =$$

$$\frac{1}{2} \left\lfloor \frac{\ell}{q} \right\rfloor \left(\ell - \left\lfloor \frac{\ell}{q} \right\rfloor q \right) \left(\ell - \left\lfloor \frac{\ell}{q} \right\rfloor q + 1 \right) + \frac{1}{2} \left(\left\lfloor \frac{\ell}{q} \right\rfloor - 1 \right) \left(q - 1 - \ell + \left\lfloor \frac{\ell}{q} \right\rfloor q \right) \left(q + \ell - \left\lfloor \frac{\ell}{q} \right\rfloor q \right),$$

otherwise. The claim now follows writing $k = \ell + 1 + \frac{(q-1)}{2} \left\lfloor \frac{\ell}{q} \right\rfloor \left(\left\lfloor \frac{\ell}{q} \right\rfloor + 1 \right) + \frac{(q^2-3q+2)}{2} + A + B + C$. □

We show that the automorphism group of $\mathcal{N}_{q,r}$ is inherited by the code C.

Proposition 4.11. *The automorphism group of C has a subgroup isomorphic to*

$$(\mathrm{Aut}_K(\mathcal{N}_{q,r}) \rtimes \mathrm{Aut}_K(\mathbb{F}_{q^r})) \rtimes \mathbb{F}_{q^r}^*.$$

Proof. By Theorem 4.4, $\mathrm{Aut}_K(\mathcal{N}_{q,r})$ is defined over $\mathbb{F}_{q^r}$, so that $\mathrm{Aut}_{\mathbb{F}_{q^r}}(\mathcal{N}_{q,r}) = \mathrm{Aut}_K(\mathcal{N}_{q,r})$. The support $supp(G) = \{\mathcal{P}_\infty\}$ of G and Ω are two orbits of $\mathrm{Aut}_K(\mathcal{N}_{q,r})$; hence, $\mathrm{Aut}_K(\mathcal{N}_{q,r})$ acts on the support $supp(D) = \mathcal{N}_{q,r}(\mathbb{F}_{q^r}) \setminus (\Omega \cup \{\mathcal{P}_\infty\})$ of D. Also, all places contained in $supp(D)$ have the same weight in D, which implies $\sigma(D) = D$ for any $\sigma \in \mathrm{Aut}_K(\mathcal{N}_{q,r})$; analogously, $\sigma(G) = G$. Therefore, $\mathrm{Aut}_{\mathbb{F}_{q^r},D,G}(\mathcal{N}_{q,r})$ is isomorphic to $\mathrm{Aut}_K(\mathcal{N}_{q,r})$.

From the proof of Theorem 4.4 follows that $\mathrm{Aut}_K(\mathcal{N}_{q,r})$ has exactly two short orbits on $\mathcal{N}_{q,r}$, namely the singleton $\{\mathcal{P}_\infty\}$ and the orbit Ω with size q^{r-1}. Hence, any non-trivial element $\sigma \in \mathrm{Aut}_K(\mathcal{N}_{q,r})$ fixes at most $q^{r-1}+1$ places on $\mathcal{N}_{q,r}$. Since the length n of C is bigger than $q^{r-1}+1$, the claim follows from Proposition 3.14. □

Remark 4.12. Let $D' = D + \mathcal{P}_\infty$ and $\tilde{G} = \sum_{P\in\Omega} \ell P$. Define the extended one point code $C' := C_{ext}(D', G)$ with $D' = D + \mathcal{P}_\infty$ and the multi-point code $\tilde{C} := C_{\mathcal{L}}(D', \tilde{G})$. Then $\tilde{G} = G + (x^\ell)$, so that C' and $\tilde{C}$ are monomially equivalent.

The code C' has the same dimension of C as k depends on the divisor G, which is the same. Also, C' attains the designed minimum distance $d'^* = n+1-\deg G = q^{2r-1}+1-(\ell+1)q^{r-1}$ since C attains $d^* = n-\deg(G)$; in fact, any codeword $c \in C$ with weight d^* extends to a codeword $c' \in C'$ with weight d'^*. By the monomial equivalence, the multi point code $\tilde{C}$ has the same parameters as C'.

Chapter 5

GK and GGS curves

Let $\mathcal{X}$ be an algebraic curve defined over the finite field $\mathbb{F}_q$ of order q. We recall that a curve $\mathcal{X}$ is called $\mathbb{F}_q$- maximal if its number of rational points over $\mathbb{F}_q$ reaches the Hasse-Weil upper bound

$$|\mathcal{X}(\mathbb{F}_q)| = q + 1 + 2g(\mathcal{X})q^{1/2},$$

where $g(\mathcal{X})$ is the genus of $\mathcal{X}$. A curve $\mathcal{Y}$ is said to be a *cover* of $\mathcal{X}$ over $\mathbb{F}_q$ if there exists a surjective map $\varphi : \mathcal{Y} \to \mathcal{X}$, where φ and the two curves are defined over $\mathbb{F}_q$. There have been extensive studies on maximal curve, see for instance [2, 16, 26, 27].

Since codes with good parameters can be constructed from these curves, many authors studied their properties, see [5–7, 34, 50, 51, 53, 54, 72]. Most of the known examples have been shown to be subcovers of the Hermitian curve $\mathcal{H}$, which is defined over $\mathbb{F}_{q^2}$ by the equation

$$Y^{q+1} = X^q + X.$$

This led to the question whether every maximal curve is a subcover of the Hermitian curve or not. This question has a negative answer: in [28], Giulietti and Korchmáros introduced an infinity family of curves $\mathcal{C}'$, the so called GK curve, which is maximal over $\mathbb{F}_{q^6}$. Garcia, Güneri and Stichtenoth generalized this construction to a family of curves $\mathcal{C}_n$, called GGS curves, indexed by an odd integer $n \geq 3$, such that $\mathcal{C}_n$ is maximal over $\mathbb{F}_{q^{2n}}$ (see [24]).

The parameters of the AG codes associated with $\mathcal{X}$ strictly depend on some characteristics of the underlying curve $\mathcal{X}$. In general, curves with many $\mathbb{F}_q$-rational places with respect to their genus give rise to AG codes with good

parameters. For this reason, maximal curves, that is curves attaining the Hasse-Weil upper bound, have been widely investigated in the literature: for example the Hermitian curve and its quotients, the Suzuki curve, and the Klein quartic; see [7, 34, 53, 54, 64, 67, 70–72]. More recently, AG codes were obtained from the Giulietti-Korchmáros curve [28] ($\mathcal{GK}$ in the following); see [6, 15, 19].

In most cases, the weight distribution of a given code is hard to be computed. Even the problem of computing codewords of minimum weight can be a difficult task apart from specific cases. In [51], following the approach of [3, 58], the authors compute the number of minimum weight codewords of certain dual AG codes arising from the Hermitian curve. For this purpose, they provide a useful algebraic-geometric description for codewords with a given weight which belong to a fixed affine-variety code.

In the first part of this chapter we deal with AG codes arising from the Giulietti-Korchmáros maximal curve. The link between the minimum distance of such codes and the underlying curve is given by a result of [16]; see Theorem 3.16. We compute the maximal intersections between the curve $\mathcal{GK}$ and lines, plane conics, and plane cubics. Such information is used in Section 4 to compute the number of minimum weight codewords of some dual codes from the Giulietti-Korchmáros curve.

5.1 The Giulietti-Korchmáros curve

Denote by $PG(3, q^6)$ the three dimensional projective space over the field $\mathbb{F}_{q^6}$ with q^6 element. The Giulietti-Korchmáros curve $\mathcal{GK}$ is a non-singular curve in $PG(3, q^6)$, introduced in [28], defined by the affine equations

$$\begin{cases} Z^{q^2-q+1} = Y^{q^2} - Y \\ Y^{q+1} = X^q + X \end{cases} . \tag{5.1}$$

This curve has genus $g = \frac{(q^3+1)(q^2-2)}{2} + 1$, $q^8 - q^6 + q^5 + 1$ $\mathbb{F}_{q^6}$-rationals points and a unique point at infinity $P_\infty = (1 : 0 : 0 : 0)$.

Theorem 5.1 (Theorem 6, [28]). $\mathrm{Aut}(\mathcal{GK})$ *has order* $q^3(q^3+1)(q^2-1)(q^2-q+1)$ *and has a normal subgroup isomorphic to* $\mathrm{SU}(3, q)$ *defined over* $\mathbb{F}_{q^{2n}}$.

(i) If $\gcd(3, n+1) = 3$ *then* $\mathrm{Aut}(\mathcal{GK}) \cong \mathrm{SU}(3, q) \times C_{q^2-q+1}$

(ii) if $\gcd(3, n+1) = 1$ *then* $\mathrm{Aut}(\mathcal{GK})$ *has a normal subgroup* M *of index* 3 *such that* $M \cong \mathrm{SU}(3, q) \times C_{q^2-q+1/3}$

The set $\mathcal{GK}(\mathbb{F}_{q^6})$ of the $\mathbb{F}_{q^6}$-rational points splits into two orbits under the action of $Aut(\mathcal{GK})$: the first one coincides with $\mathcal{GK}(\mathbb{F}_{q^2})$ of the $\mathbb{F}_{q^2}$-rational points of $\mathcal{GK}$, coinciding with the intersection between $\mathcal{GK}$ and the plane $Z = 0$; the second one is formed by all the points in $\mathcal{GK}(\mathbb{F}_{q^6}) \setminus \mathcal{GK}(\mathbb{F}_{q^2})$. The curve $\mathcal{GK}$ is $\mathbb{F}_{q^6}$-maximal, that is, it attains the Hasse-Weil bound $|\mathcal{GK}(\mathbb{F}_{q^6})| = q^6 + 1 + 2gq^3$; see [65, Theorem 5.2.3]. Moreover, for $q > 2$, $\mathcal{GK}$ is not covered by the Hermitian curve (see [28]): this is the first example in the literature of a family of maximal curves with this feature.

The curve $\mathcal{GK}$ is an example of a complete intersection curve in $PG(3, q^6)$; see [28, Section 2].

Consider now the function field $\mathbb{F}_{q^6}(\mathcal{GK})$ associated with $\mathcal{GK}$ and let $x, y, z \in \mathbb{F}_{q^6}(\mathcal{GK})$ be its coordinate functions, which satisfy $y^{q+1} = x^q + x$ and $z^{q^2-q+1} = y^{q^2} - y$.

Concerning the functions $x, y, z \in \mathbb{F}_{q^6}(\mathcal{GK})$ it is easily proved that

- $(x) = (q^3+1)P_0 - (q^3+1)P_\infty$,
- $(y) = (q^2-q+1)(\sum_{a:a^q+a=0} P_{(a,0,0)}) - (q^3-q^2+q)P_\infty$,
- $(z) = \left(\sum_{P \in \mathcal{X}(\mathbb{F}_{q^2}) \setminus \{P_\infty\}} P\right) - q^3 P_\infty$,

where $P_{(a,b,c)}$ denotes the affine point (a, b, c) and $P_0 = P_{(0,0,0)}$.

5.2 Intersection between the Giulietti-Korchmáros curve and lines or conics

In this section we study the possible intersections between a line or a plane conic and the curve $\mathcal{GK}$ as in (5.1). In particular, we are interested in its maximum size.

Proposition 5.2. *Let* $r \subset PG(3, q^6)$ *be a line. Then*

$$|r \cap \mathcal{GK}| \leq q^2 - q + 1.$$

Also, any (q^2-q+1)*-secant is parallel to the* z*-axis and all the* (q^2-q+1) *common points are not* $\mathbb{F}_{q^2}$*-rational.*

Proof. As already mentioned, the $\mathbb{F}_{q^6}$-rational points of $\mathcal{GK}$ are divided into two orbits $\mathcal{O}_1 = \mathcal{GK}(\mathbb{F}_{q^2})$ and $\mathcal{O}_2 = \mathcal{GK}(\mathbb{F}_{q^6}) \setminus \mathcal{GK}(\mathbb{F}_{q^2})$.

Suppose that $r \cap \mathcal{GK}(\mathbb{F}_{q^6})$ contains at least an $\mathbb{F}_{q^2}$-rational point P_1. Without loss of generality we can assume that $P_1 = (0,0,0)$ since the automorphism group of the curve is transitive on $\mathcal{GK}(\mathbb{F}_{q^2})$ and linear (so it maps secant lines to secant lines preserving the number of their intersections). Let $P_2 = (x,y,z) \in \mathcal{GK}(\mathbb{F}_{q^6}) \setminus \{P_1,\ P_\infty\}$. Suppose $y \neq 0$; this implies $x \neq 0$. An $\mathbb{F}_{q^6}$-rational point P on the line r through P_1 and P_2 has coordinates

$$\left(\frac{\lambda x}{1+\lambda}, \frac{\lambda y}{1+\lambda}, \frac{\lambda z}{1+\lambda}\right),$$

for some $\lambda \in \mathbb{F}_{q^6}$. If such a point belongs to $\mathcal{GK}$ then

$$\left(\frac{\lambda y}{1+\lambda}\right)^{q+1} = \left(\frac{\lambda x}{1+\lambda}\right)^{q} + \frac{\lambda x}{1+\lambda},$$

that is

$$\lambda^{q+1} y^{q+1} = \lambda^q x^q (1+\lambda) + \lambda x (1+\lambda)^q.$$

The condition $y^{q+1} = x^q + x$ yields $\lambda^q x^q + \lambda x = 0$. The roots $\{a_1, \ldots, a_q\}$ of the polynomial $T^q + T$ are all distinct and belong to $\mathbb{F}_{q^6}$. It is easily seen that points in $r \cap \mathcal{GK}$ correspond to values λ among $\{a_1/x, \ldots, a_q/x\} \cup \{-1\}$.

A direct computation shows that the same result holds true for the line through P_1 and $P_\infty = (1:0:0)$.

Suppose now that $r \cap \mathcal{GK}(\mathbb{F}_{q^6})$ contains no points of $\mathcal{O}_1$. Let $P_1 = (x_1, y_1, z_1), P_2 = (x_2, y_2, z_2) \in \mathcal{O}_2$ two points of r. An $\mathbb{F}_{q^6}$-rational point P of r is

$$P = \left(\frac{x_1 + \lambda x_2}{1+\lambda}, \frac{y_1 + \lambda y_2}{1+\lambda}, \frac{z_1 + \lambda z_2}{1+\lambda}\right)$$

for some $\lambda \in \mathbb{F}_{q^6}$. If $P \in \mathcal{GK}$ then, by the second equation in (5.1),

$$\left(\frac{y_1 + \lambda y_2}{1+\lambda}\right)^{q+1} = \left(\frac{x_1 + \lambda x_2}{1+\lambda}\right)^{q} + \frac{x_1 + \lambda x_2}{1+\lambda}.$$

Recalling that $y_1^{q+1} = x_1^q + x_1$ and $y_2^{q+1} = x_2^q + x_2$, we obtain

$$\lambda^q (x_1 + x_2^q - y_1 y_2^q) + \lambda (x_1^q + x_2 - y_1^q y_2) = 0.$$

If $(x_1 + x_2^q - y_1 y_2^q) \neq 0$ or $(x_1^q + x_2 - y_1^q y_2) \neq 0$ then $|r \cap \mathcal{GK}(\mathbb{F}_{q^6})| \leq q+1$. On the other hand, if $x_1 + x_2^q - y_1 y_2^q = x_1^q + x_2 - y_1^q y_2 = 0$ then

$$(x_1 + x_1^q) + (x_2 + x_2^q) - y_1 y_2^q - y_1^q y_2 = 0, \qquad y_1^{q+1} + y_2^{q+1} - y_1 y_2^q - y_1^q y_2 = (y_1 - y_2)^{q+1} = 0,$$

that is $y_1 = y_2$. Finally, from $x_1 + x_2^q - y_1 y_2^q = 0$, we get $x_1 = x_2$. This means that if $|r \cap \mathcal{GK}(\mathbb{F}_{q^6})| > q+1$ then r has equation $X = x_1$, $Y = y_1$, with $x_1^q + x_1 = y_1^{q+1}$. Clearly $y_1 \notin \mathbb{F}_{q^2}$ otherwise P_1 and P_2 belong to $\mathcal{O}_1$. A direct computation shows that the line r has exactly $q^2 - q + 1$ points in common with the curve $\mathcal{GK}$. □

Proposition 5.3. *The total number of $(q^2 - q + 1)$-secants of $\mathcal{GK}$ is $(q+1)(q^5 - q^3)$.*

Proof. Recall that $|\mathcal{O}_2| = q^8 - q^6 + q^5 - q^3$. Also, each point in $\mathcal{O}_2$ lies on exactly one (q^2-q+1)-secant $r : X = x_1, Y = y_1$ such that $(r \cap \mathcal{GK}(\mathbb{F}_{q^6})) \subset \mathcal{O}_2$. Therefore the number of such lines is

$$\frac{(q^8 - q^6 + q^5 - q^3)}{(q^2 - q + 1)} = (q+1)(q^5 - q^3).$$

□

Proposition 5.4. *Let $\mathcal{C}$ be a plane conic in $PG(3, q^6)$. Then the size $|\mathcal{C} \cap \mathcal{GK}(\mathbb{F}_{q^6})|$ is at most*

$$\begin{cases} 2(q^2 - q + 1), & \text{if } \mathcal{C} \text{ is reducible,} \\ 2(q+1), & \text{if } \mathcal{C} \text{ is absolutely irreducible.} \end{cases}$$

Proof. Let $\mathcal{C}$ be contained in the plane defined by $G(X, Y, Z) = \alpha X + \beta Y + \gamma Z + \delta = 0$. Suppose that $\mathcal{C}$ is absolutely irreducible.

Suppose $\gamma \neq 0$. The points $P = (x, y, z)$ in $\mathcal{C} \cap \mathcal{GK}(\mathbb{F}_{q^6})$ satisfy

$$\begin{cases} z^{q^2-q+1} = y^{q^2} - y \\ y^{q+1} = x^q + x \\ ax^2 + by^2 + cxy + dx + ey + f = 0 \\ G(x, y, z) = 0, \end{cases}$$

where $a, b, c, d, e, f, g \in \mathbb{F}_{q^6}$. By Bézout's Theorem (see [69, Theorem 3.14]) the number of pairs (x, y) satisfying $y^{q+1} = x^q + x$ and $ax^2 + by^2 + cxy + dx + ey + f = 0$ is at most $2(q+1)$. Clearly, for each such pair (x, y) there exists a unique z satisfying $G(x, y, z) = 0$. Therefore $|\mathcal{C} \cap \mathcal{GK}(\mathbb{F}_{q^6})| \leq 2(q+1)$.

Suppose now $\gamma = 0$ and $\beta \neq 0$. The points $P = (x, y, z)$ in $\mathcal{C} \cap \mathcal{GK}(\mathbb{F}_{q^6})$ satisfy

$$\begin{cases} z^{q^2-q+1} = y^{q^2} - y \\ y^{q+1} = x^q + x \\ ax^2 + bz^2 + cxz + dx + ez + f = 0 \\ G(x, y) = 0, \end{cases}$$

where $a, b, c, d, e, f, g \in \mathbb{F}_{q^6}$. As above, there are at most $q + 1$ pairs (x, y) such that $y^{q+1} = x^q + x$ and $G(x, y) = 0$. Clearly, for each such pair (x, y) there exist at most 2 values z such that $ax^2 + bz^2 + cxz + dx + ez + f = 0$, since the $\mathcal{C}$ is absolutely irreducible. Therefore $|\mathcal{C} \cap \mathcal{GK}(\mathbb{F}_{q^6})| \leq 2(q + 1)$.

The case $\gamma = 0$ and $\alpha \neq 0$ is similar and omitted.

If the conic $\mathcal{C}$ splits into two lines, then, by Proposition 5.2, it is clear that $|\mathcal{C} \cap \mathcal{GK}(\mathbb{F}_{q^6})|$ is at most $2(q^2 - q + 1)$. Note that if the two lines are both $(q^2 - q + 1)$-secants then they are parallel to the z axis (see the proof of Proposition 5.2) and therefore their common point is $(0, 0, 1, 0) \notin \mathcal{GK}$. This shows that the upper bound $2(q^2 - q + 1)$ is attained. □

The previous result can be generalized to a plane curve of degree $\alpha \leq q$.

Proposition 5.5. *Let $\mathcal{X}$ be a curve of degree $\alpha \leq q$ in $PG(3, q^6)$. Then the size $|\mathcal{X} \cap \mathcal{GK}(\mathbb{F}_{q^6})|$ is at most*

$$\begin{cases} \alpha(q^2 - q + 1), & \text{if } \mathcal{X} \text{ is reducible,} \\ \alpha(q + 1), & \text{if } \mathcal{X} \text{ is absolutely irreducible.} \end{cases}$$

Proof. The argument is the same as in Proposition 5.4. Note that such bound holds only if $\alpha \leq$ since a plane can contain at most q lines parallel to the z-axis which are $(q^2 - q + 1)$-secants. In fact, each of these lines intersects the plane $z = 0$ in an point of $\mathcal{GK}(\mathbb{F}_{q^6}) \setminus \mathcal{GK}(\mathbb{F}_{q^2})$; there are at most q such collinear points (they correspond to the $\mathbb{F}_{q^6}$-rational intersection points of a line with the Hermitian curve $y^{q+1} = x^q + x$ which are not $\mathbb{F}_{q^2}$-rational). □

We conclude this section with the following proposition.

Proposition 5.6. *There exist $3(q^2 - q + 1)$ coplanar points contained in $\mathcal{GK}(\mathbb{F}_{q^6})$ lying on the intersection between a cubic curve and a curve $\mathcal{Y}$ of degree $q^2 - q + 1$.*

Proof. Let $\overline{y} \in \mathbb{F}_{q^6} \setminus \mathbb{F}_{q^2}$. Consider three lines r_i of equations $X = x_i$, $Y = \overline{y}$, $i = 1, 2, 3$, with $x_i^q + x_i = \overline{y}^{q+1}$. Such three lines are coplanar and $(q^2 - q + 1)$-secants; see also Proposition 5.2.

Let $\mathcal{X}$ be the plane cubic consisting of the union of r_1, r_2, and r_3. Clearly, $|\mathcal{X} \cap \mathcal{GK}(\mathbb{F}_{q^6})| = 3(q^2 - q + 1)$. To conclude the proof we have to show that these points lie on a plane curve of degree $m = q^2 - q + 1$.

It is enough to observe that the points in $\mathcal{X} \cap \mathcal{GK}(\mathbb{F}_{q^6})$ are

$$(x_i, \overline{y}, z_j), \qquad i = 1, 2, 3,\ j = 1, \ldots, q^2 - q + 1,$$

with $z_j^{q^2-q+1} = \overline{y}^{q^2} - \overline{y}$. Such $3(q^2 - q + 1)$ points are contained in the $q^2 - q + 1$ lines s_j of equations

$$s_j := \begin{cases} Y = \overline{y} \\ Z = z_j \end{cases} .$$

Therefore $\mathcal{X} \cap \mathcal{GK}(\mathbb{F}_{q^6})$ is contained also in $\mathcal{Y} = \bigcup_{j=1}^{q^2-q+1} s_j$. □

Remark 5.7. Proposition 5.2 and [8, Theorem 4.2] allow us to compute the gonality of the curve $\mathcal{GK}$; see [38, Definition 9.49]. Since $\mathcal{GK}$ is a smooth complete intersection curve of degree q^3+1 in a projective space of dimension three, its gonality is given by

$$\gamma(\mathcal{GK}) = q^3 + 1 - (q^2 - q + 1) = q^3 - q^2 + q;$$

see [8, Theorem 4.2]. Such a value is also the smallest non-gap at a point of $\mathcal{GK}$; see [9]. This information could help to construct lattices from function fields; see [2].

5.3 Minimum distance and number of minimum weight codewords of one point codes on the Giulietti-Korchmáros curve

We first determine the minimum distance of the one point AG code $C_{\mathcal{L}}(D, G_m)^{\perp}$, where $G_m = m(q^3+1)P_\infty$, $P_\infty = (1 : 0 : 0 : 0)$, and $D = \sum_{P \in \mathcal{GK}(\mathbb{F}_{q^6}) \setminus \{P_\infty\}} P$, applying Theorem 3.16.

Proposition 5.8. *The minimum distance d of $C_{\mathcal{L}}(D, G_m)^{\perp}$, $m \geq 2$, is*

1. *$d = m + 2$ when $m \leq^2 -q - 1$;*

2. $d = 2m + 2$ *when* $m = q^2 - q$;

3. $d = 3m$ *when* $m = q^2 - q + 1$;

4. $d \geq 3m + 1$ *when* $q^2 - q + 1 < m \leq^2 -1$;

5. $d \geq d^*$ *when* $m > q^2 - 1$,

where d^* *is the designed Goppa minimum distance of* $C_{\mathcal{L}}(D, G_m)^{\perp}$.

Proof. We apply Theorem 3.16.

1. By Proposition 5.2 there exist $m + 2 \leq q^2 - q + 1$ collinear points in $\mathcal{GK}$ and therefore the minimum distance is $d = m + 2$.

2. If $m = q^2 - q$ then $m+2 = q^2 - q+2$ points of $\mathcal{GK}$ cannot be collinear. Since there exist $2m+2 = 2(q^2 - q+1)$ points contained in a reducible plane conic (see the proof of Proposition 5.4) the minimum distance is exactly $d = 2m + 2 = 2(q^2 - q + 1)$.

3. If $m = q^2 - q + 1$ then no line contains $m + 2$ points and no plane conic contains $2m + 2$ points of $\mathcal{GK}$. By Proposition 5.6 there exist plane cubics with $3m$ points which are also contained in a curve of degree m having no common components with the cubic. Therefore the minimum distance is $3m = 3(q^2 - q + 1)$.

4. If $m > q^2 - q + 1$, none of the previous cases applies and therefore the minimum distance is at least $3m + 1$.

5. It is enough to observe that $3m+1$ is larger than the designed minimum distance $d^* = m(q^3 + 1) - q^5 + 2q^3 - q^2 + 2$ only when

$$3m+1 \geq m(q^3+1)-q^5+2q^3-q^2+2 \iff m \leq^2 -2+\frac{3q^2-5}{q^3-2} \iff m \leq q^2-1.$$

□

Remark 5.9. It is worth noting that if $q = 2$ the above proposition can be applied for $m = 2, 3$. In these cases the codes $C(D, 18P_\infty)^{\perp}$ and $C(D, 27P_\infty)^{\perp}$ have minimum distance 6 and 9 and confirm [19, Table 2] (they are a $[224, 214, 6]$ and a $[224, 206, 9]$-code respectively).

If $q = 3$, the parameters of the codes corresponding to $m = 2, \ldots, 8$ are summarized in Table 5.1. In particular, $k \leq 6074 - 28(m - 7/2) - 1$ and

Table 5.1: Codes $C(D, 28mP_\infty)^\perp$ for $m = 2, \ldots, 8$, with $q = 3$

m	G_m	n	k	d
2	$56P_\infty$	6074	≤ 6074	4
3	$84P_\infty$	6074	≤ 6074	5
4	$112P_\infty$	6074	≤ 6059	6
5	$140P_\infty$	6074	≤ 6031	7
6	$168P_\infty$	6074	≤ 6003	14
7	$196P_\infty$	6074	≤ 5975	21
8	$224P_\infty$	6074	$= 5947$	22

equality holds if $\deg(G_m) > 2g - 2$, that is $m \geq 8$. None of these codes is better than the corresponding ones in [19, Table 4].

It would be very interesting to compare, in general, the improvements to the designed minimum distance d^* of a Goppa code given by the Feng-Rao approach with those given by Theorem 3.16.

5.3.1 Number of minimum weight codewords

In this section we determine the number of minimum weight codewords in $C_{\mathcal{L}}(D, G_m)^\perp$, $G_m = m(q^3+1)P_\infty$, in the case $q - 1 \leq m \leq 2(q-1)$.

Recall that for the code $C(D, G_m)^\perp$ the designed Goppa minimum distance is

$$d^* = \deg(G_m) - 2g(\mathcal{GK}) + 2 = m(q^3+1) - q^5 + 2q^3 - q^2 + 2.$$

Consider the ideal $I = \langle Z^{q^2-q+1} - Y^{q^2} + Y, Y^{q+1} - X^q - X, X^{q^6} - X, Y^{q^6} - Y, Z^{q^6} - Z \rangle$ of $\mathbb{F}_{q^6}[X, Y, Z]$ and let $R = \mathbb{F}_{q^6}[X, Y, Z]/I$. Also, let

$$\mathcal{B}_{q,m} = \left\{ X^i Y^j Z^k + I \mid i \in [0, \ldots, q-1],\ j \in [0, \ldots, q^2 - q],\ k \in [0, \ldots, m] \right\}$$

and $L = \langle \mathcal{B}_{q,m} \rangle \subseteq R$. By [19], $\mathcal{B}_{q,m}$ induces, in the coordinate functions x, y, z of $\mathbb{F}_{q^6}(\mathcal{GK})$, a basis for the Riemann-Roch space $\mathcal{L}(G_m)$.

To count the exact number of the minimum weight codewords of $C(D, mP_\infty)^\perp$ we use Proposition 3.18. Let $w \geq d\left(C(D, mP_\infty)^\perp\right)$. Using the same nota-

tions, we consider the ideal J_w of $\mathbb{F}_{q^6}[X,Y,Z]$ given by

$$J_w = \Bigg\langle \left\{\sum_{i=1}^{w} u_i X_i^r Y_i^s Z_i^t\right\}_{X^rY^sZ^t+I\in\mathcal{B}_{q,m}}, \left\{Z_i^{q^2-q+1} - Y_i^{q^2} + Y_i\right\}_{i=1,\dots,w}, \left\{Y_i^{q+1} - X_i^q - X_i\right\}_{i=1,\dots,w},$$
$$\left\{X_i^{q^6-1} - 1\right\}_{i=1,\dots,w}, \left\{Y_i^{q^6-1} - 1\right\}_{i=1,\dots,w}, \left\{Z_i^{q^6-1} - 1\right\}_{i=1,\dots,w},$$
$$\left\{((X_i - X_j)^{q^6-1} - 1)((Y_i - Y_j)^{q^6-1} - 1)((Z_i - Z_j)^{q^6-1} - 1)\right\}_{1\le i<j\le w}\Bigg\rangle.$$

A point in $V(J_w)$ is a $4w$-tuple

$$(\bar{x}_1,\dots,\bar{x}_w,\bar{y}_1,\dots,\bar{y}_w,\bar{z}_1,\dots,\bar{z}_w,\bar{u}_1,\dots,\bar{u}_w) \in \mathbb{F}_{q^6}^{4w}$$

which corresponds to a set of w points $(\bar{x}_i,\bar{y}_i,\bar{z}_i)$, $i=1,\dots,w$, in $\mathcal{GK}(\mathbb{F}_{q^6})$.

Theorem 5.10. *Let $q-1 \le m \le 2(q-1)$. The number of minimum weight codewords in $C_{\mathcal{L}}(D,G_m)^{\perp}$ is*

$$A_d(C_{\mathcal{L}}(D,G_m)^{\perp}) = (q+1)(q^5-q^3)(q^6-1)\binom{q^2-q+1}{m+2}.$$

Proof. By Proposition 3.18, we have to count the number $4d$-tuples

$$(\bar{x}_1,\dots,\bar{x}_d,\bar{y}_1,\dots,\bar{y}_d,\bar{z}_1,\dots,\bar{z}_d,\bar{u}_1,\dots,\bar{u}_d) \in \mathbb{F}_{q^6}^{4d}$$

which differ in the first $3d$ coordinates, and such that $\bar{z}_i^{q^2-q+1} = \bar{y}_i^{q^2} - \bar{y}_i$, $\bar{y}_i^{q+1} = \bar{x}_i^q + \bar{x}_i$, and

$$\begin{cases} \bar{u}_1 + \cdots + \bar{u}_d = 0 \\ \bar{x}_1\bar{u}_1 + \cdots + \bar{x}_d\bar{u}_d = 0 \\ \bar{y}_1\bar{u}_1 + \cdots + \bar{y}_d\bar{u}_d = 0 \\ \bar{z}_1\bar{u}_1 + \cdots + \bar{z}_d\bar{u}_d = 0 \\ \vdots \\ \bar{x}_1^{q-1}\bar{y}_1^{q^2-q}z_1^{d-2}\bar{u}_1 + \cdots + x_d^{q-1}\bar{y}_d^{q^2-q}z_d^{d-2}\bar{u}_d = 0. \end{cases} \tag{5.2}$$

To each tuple $(\bar{x}_1,\dots,\bar{x}_d,\bar{y}_1,\dots,\bar{y}_d,\bar{z}_1,\dots,\bar{z}_d,\bar{u}_1,\dots,\bar{u}_d)$ we can associate d points $(\bar{x}_i,\bar{y}_i,\bar{z}_i)$, $i=1,\dots,d$, in $\mathcal{GK}(\mathbb{F}_{q^6})$. Suppose that the number of different values $\bar{y}_i$ is $\alpha \le d \le q^2-q$. Without loss of generality, let $\bar{y}_1,\dots,\bar{y}_\alpha$ be pairwise distinct.

Suppose $\alpha > 1$. Let $I_i = \{\bar{y}_j : \bar{y}_j = \bar{y}_i\}$, for $i = 1,\dots,\alpha$. We may suppose $|I_1| \le |I_2| \le \ldots \le |I_\alpha|$ and let $\beta = |I_1|$. Note that $\beta \le d/2 \le q-1$

since $d \leq 2(q-1)$. System (5.2) contains the equations

$$\begin{array}{rcl} \bar{y}_1^r \bar{u}_1 + \cdots + \bar{y}_d^r \bar{u}_d & = & 0, \\ \bar{x}_1 \bar{y}_1^r \bar{u}_1 + \cdots + \bar{x}_d \bar{y}_1^r \bar{u}_d & = & 0, \\ \vdots & & \\ \bar{x}_1^{q-1} \bar{y}_1^r \bar{u}_1 + \cdots + \bar{x}_d^{q-1} \bar{y}_1^r \bar{u}_d & = & 0, \end{array}$$

for $r = 0, \ldots, \alpha - 1$. Let us define for $i = 1, \ldots, \alpha$, $u_i = \sum_{j \,:\, y_j = y_i} \bar{u}_j$ and $x_i^{r,s} = \sum_{j \,:\, y_j = y_i} \bar{x}_j^r \bar{z}_j^s \bar{u}_j$, $r = 0, \ldots, q-1$, $s = 0, \ldots, d-2$. The above set of equations can be written as

$$\begin{cases} u_1 + \cdots + u_\alpha = 0 \\ \bar{y}_1 u_1 + \cdots + \bar{y}_\alpha u_\alpha = 0 \\ \bar{y}_1^2 u_1 + \cdots + \bar{y}_\alpha^2 u_\alpha = 0 \\ \vdots \\ \bar{y}_1^{\alpha-1} u_1 + \cdots + \bar{y}_\alpha^{\alpha-1} u_\alpha = 0 \end{cases}, \qquad \begin{cases} x_1^{r,s} + \cdots + x_\alpha^{r,s} = 0 \\ \bar{y}_1 x_1^{r,s} + \cdots + \bar{y}_\alpha x_\alpha^{r,s} = 0 \\ \bar{y}_1^2 x_1^{r,s} + \cdots + \bar{y}_\alpha^2 x_\alpha^{r,s} = 0 \\ \vdots \\ \bar{y}_1^{\alpha-1} x_1^{r,s} + \cdots + \bar{y}_\alpha^{\alpha-1} x_\alpha^{r,s} = 0 \end{cases}.$$

Each of the previous systems can be seen as a system in the indeterminates $u_1, \ldots, u_\alpha$, or $x_1^{r,s}, \ldots, x_\alpha^{r,s}$. Such systems are Vandermonde systems with the same coefficients. Since $\bar{y}_1, \ldots, \bar{y}_\alpha$ are pairwise distinct the unique solutions is $u_1 = \cdots = u_\alpha = x_1^{r,s} = \cdots = x_\alpha^{r,s} = 0$.

Among the elements of $A := \{\bar{x}_i \,:\, \bar{y}_i = \bar{y}_1\}$, the number of distinct elements is at most $\gamma \leq \beta \leq q-1$. Suppose $\gamma > 1$. Let $A = \{x_{i_1}, \ldots, x_{i_\beta}\}$. Consider the systems $u_1 = x_1^{1,0} = \cdots = x_1^{\gamma-1,0} = 0$, …, $u_1 = x_1^{1,d-2} = \cdots = x_1^{\gamma-1,d-2} = 0$.

Let $J_j = \{k \,:\, \bar{x}_{i_k} \in A,\ \bar{x}_{i_k} = \bar{x}_{i_j}\}$ and $v_j^r = \sum_{k \in J_j} \bar{z}_{i_k}^r \bar{u}_{i_k}$, $j = 1, \ldots, \gamma$, $r = 0, \ldots, d-2$. We may suppose that $x_{i_1}, \ldots, x_{i_\gamma}$ are pairwise distinct. The previous systems can be written as

$$\begin{cases} v_1^r + \cdots + v_\gamma^r = 0 \\ \sum_{j=1}^{\gamma} \bar{x}_{i_j} v_j^r = 0 \\ \sum_{j=1}^{\gamma} \bar{x}_{i_j}^1 v_j^r = 0 \\ \vdots \\ \sum_{j=1}^{\gamma} \bar{x}_{i_j}^{\gamma-1} v_j^r = 0 \end{cases},$$

and it can been seen as a system in the indeterminates $v_1^r, \ldots, v_\gamma^r$. Since the coefficients $\bar{x}_{i_1}, \ldots, \bar{x}_{i_\gamma}$ are pairwise distinct, the above system has as

unique solutions $v_1^r = \cdots = v_\gamma^r = 0$, $r = 0, \ldots, d-2$. Since $(\bar{x}_{i_1}, \bar{y}_{i_1}) = \cdots = (\bar{x}_{i_\gamma}, \bar{y}_{i_\gamma})$, all the values $\bar{z}_{i_1}, \ldots, \bar{z}_{i_\gamma}$ must be pairwise distinct. Therefore, from

$$\begin{cases} \bar{u}_{i_1} + \cdots + \bar{u}_{i_\gamma} = 0 \\ \bar{z}_{i_1}\bar{u}_{i_1} + \cdots + \bar{z}_{i_\gamma}\bar{u}_{i_\gamma} = 0 \\ \bar{z}_{i_1}^2\bar{u}_{i_1} + \cdots + \bar{z}_{i_\gamma}^2\bar{u}_{i_\gamma} = 0 \\ \vdots \\ \bar{z}_{i_1}^{d-2}\bar{u}_{i_1} + \cdots + \bar{z}_{i_\gamma}^{d-2}\bar{u}_{i_\gamma} = 0, \end{cases}$$

we get that the unique solution is $\bar{u}_{i_1} = \cdots = \bar{u}_{i_\gamma} = 0$, a contradiction.

This shows that $\alpha = 1$, that is $\bar{y}_1 = \cdots = \bar{y}_d$. Using a similar argument we can prove that $\bar{x}_1 = \cdots = \bar{x}_d$ and therefore the values $\bar{z}_i$, $i = 1, \ldots, d$, are pairwise distinct. In other words, all the points $(\bar{x}_i, \bar{y}_i, \bar{z}_i)$, $i = 1, \ldots, d$, lie on a fixed line parallel to the z-axis. We conclude the proof computing the exact number of solution of System (5.2). Since $\bar{x}_1 = \cdots = \bar{x}_d$ and $\bar{y}_1 = \cdots = \bar{y}_d$ this system reduces to

$$\begin{cases} \bar{u}_1 + \cdots + \bar{u}_d = 0 \\ \bar{z}_1\bar{u}_1 + \cdots + \bar{z}_d\bar{u}_d = 0 \\ \vdots \\ \bar{z}_1^{d-2}\bar{u}_1 + \cdots + \bar{z}_d^{d-2}\bar{u}_d = 0. \end{cases} \tag{5.3}$$

By Proposition 5.3, we have $(q+1)(q^5 - q^3)$ different choices for the $(q^2 - q + 1)$-secant line r; we need d points $P_i = (x_i, y_i, z_i)$, $i \in \{1, \ldots, d\}$, among r (up to permutations). So the total number of d-tuples of points is

$$(q+1)(q^5 - q^3)\binom{q^2 - q + 1}{d} d!.$$

The matrix of System (5.3) is a Vandermonde matrix and the solution space has linear dimension 1: the number of u_i's is $|\mathbb{F}_{q^6}^*| = q^6 - 1$ and finally

$$A_d = \frac{(q+1)(q^5 - q^3)(q^6 - 1)\binom{q^2-q+1}{d} d!}{d!} = (q+1)(q^5 - q^3)(q^6 - 1)\binom{q^2 - q + 1}{d}.$$

□

In the case $2(q-1) < m < q^2 - q - 1$ we can give a lower bound on the number of minimum weight codewords. If we consider d collinear points of

the type $(\bar{x}, \bar{y}, \bar{z}_i)$, $i = 1, \ldots, d$, then System (5.2) collapses to System (5.3) (note that the $\bar{z}_i$'s must be pairwise distinct) and therefore the number of the corresponding u_i's is $|\mathbb{F}_{q^6}^*| = q^6 - 1$. Using again Proposition 5.3 we can prove the following.

Theorem 5.11. *Let $2(q-1) < m < q^2 - q - 1$. The number of minimum weight codewords in $C_{\mathcal{L}}(D, G_m)^{\perp}$ is at least:*

$$A_d(C_{\mathcal{L}}(D, G_m)^{\perp}) \geq (q+1)(q^5 - q^3)(q^6 - 1)\binom{q^2 - q + 1}{d}.$$

5.4 Garcia-Güneri-Stichtenoth Curve

Our aim in this section is to generalize their result obtained in the previous one to the GGS curve, so we will study the intersection between lines and the Garcia-Güneri-Stichtenoth curve. Unfortunately, the generalization of the GK curve has a singularity, so we cannot apply the same tools used before: we will only find an upper bound for minimum distance of one point codes on the GGS curve.

Let $n \geq 3$ be an odd integer, consider the curve $\mathcal{C}_n$ over $\mathbb{F}_{q^{2n}}$ defined by the following equations:

$$\mathcal{C}_n : \begin{cases} Y^{q+1} = X^q + X \\ Z^m = Y^{q^2} - Y, \end{cases} \tag{5.4}$$

where $m = (q^n + 1)/(q + 1)$.

Note that the first equation defines a maximal curve in $PG(2, q^{2n})$ since it is the Hermitian curve and n is odd.

The curve defined by the second equation was shown to be maximal in $PG(2, q^{2n})$ for any odd $n \geq 3$ by Abdón, Bezerra and Quoos; see [1].

From what we said before $\mathcal{C}_n$ is a fibre product of two maximal curves over $\mathbb{F}_{q^{2n}}$ and we will see that $\mathcal{C}_n$ itself is maximal over $\mathbb{F}_{q^{2n}}$.

Note that $\mathcal{C}_3$ defines $\mathcal{GK}$, so the Giulietti-Korchmáros curve is a special case of the curve define in (5.4).

Let $n \geq 5$, then the inequality $m \geq q^2$ holds for any power of a prime q. We consider the homogenization of (5.4):

$$\begin{cases} X_2^{q+1} = X_1^q X_0 + X_1 X_0^q \\ X_3^m = X_2^{q^2} X_0^{m-q^2} - X_2 X_0^{m-1} \end{cases} \tag{5.5}$$

If $X_0 = 0$, then $X_2 = X_3 = 0$ so the only point at the infinity is $P_\infty = [0 : 1 : 0 : 0]$. This is the only singular point of $\mathcal{C}_n$, because the Jacobian matrix

$$J = \begin{bmatrix} -X_1^q & -X_0^q & X_2^q & 0 \\ -X_0^{m-q^2-1} X_2^{q^2} & 0 & X_0^{m-1} & X_3^{m-1} \end{bmatrix}$$

has rank one only for $X_0 = 0$, which occurs only for P_∞.

Theorem 5.12 (Theorem 3.22, [33]). *Let $n \geq 5$ odd,* $\mathrm{Aut}(\mathcal{C}_n)$ *fixes the point*

at the infinity on $\mathcal{C}_n$ *and is isomorphic to* $\Gamma = Q \rtimes_\Phi \Sigma$*, where*

$$Q_{a,b} = \begin{pmatrix} 1 & b^q & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}, \qquad g_\zeta(x,y,z) = (\zeta^{q^n+1}x, \zeta^m y, \zeta z)$$

$Q = \{Q_{a,b} : a, b \in \mathbb{F}_{q^2}\ a^q + a = b^{q+1}\}$ *and* $\Sigma = \{g_\zeta : \zeta$ *is a* $(q^n+1)(q-1)$*-th root of unity*$\}$.

5.5 Intersection between the GSS curve and lines

We study the intersection between a line r and the curve $\mathcal{C} = \mathcal{C}_n$ in the three-dimensional projective space over $\mathbb{F}_{q^{2n}}$. In particular we are interested in the lines that are maximal secants.

Let r be a secant to $\mathcal{C}_n$.

Suppose that $\mathbb{P}_\infty = [0:1:0:0]$ belongs to $r \cap \mathcal{C}$. Let $P = [1:x:y:z]$ a different point of $r \cap \mathcal{C}$. Each point on the line r can be written in the parametric form $Q = \mu P + \lambda P_\infty = [\mu : \mu x + \lambda : \mu y : \mu z]$, where $\mu, \lambda \in \mathbb{F}_{q^{2n}}$.

Our aim is to count the number of points Q that lie also on $\mathcal{C}$.

If $\mu = 0$ we have $Q = P_\infty$, so we can take $\mu \neq 0$. We can divide by μ and write $Q = [1 : x + \nu : y : z]$, where $\nu = \lambda/\mu \in \mathbb{F}_{q^{2n}}$. The point P is a point of the curve $\mathcal{C}$, in particular $y^{q+1} = x^q + x$. If $Q \in C$ then from the first equation in (2)

$$\begin{aligned} y^{q+1} &= (x+\nu)^q + (x+\nu) \\ y^{q+1} &= x^q + \nu^q + x + \nu \\ \nu^q + \nu &= 0. \end{aligned}$$

This last equation has at most q solutions, so we have at most q different intersections. Thus a secant line through P_∞ intersects the curve $\mathcal{C}$ in at most $q+1$ different points.

Since the GSS curve has only one point at infinity, we now work in the affine space: we suppose r is a line that does not intersect P_∞.
Let $P_1 = (x_1, y_1, z_1)$, $P_2 = (x_2, y_2, z_2)$ be two distinct points in $r \cap \mathcal{C}$. We have the equations:

$$\begin{cases} y_1^{q+1} = x_1^q + x_1 \\ z_1^m = y_1^{q^2} - y_1 \end{cases} \qquad \begin{cases} y_2^{q+1} = x_2^q + x_2 \\ z_2^m = y_2^{q^2} - y_2 \end{cases} \tag{5.6}$$

A generic point of the line r trough P_1 and P_2 is

$$P_3 = P_1 + \lambda\overline{P_2P_1} = ((1-\lambda)x_1 + \lambda x_2, (1-\lambda)y_1 + \lambda y_2, (1-\lambda)z_1 + \lambda z_2)$$

for some $\lambda \in \mathbb{F}_{q^{2n}}$. If $P_3 \in \mathcal{C}$, then

$$[(1-\lambda)y_1 + \lambda y_2]^{q+1} = [(1-\lambda)x_1 + \lambda x_2]^q + [(1-\lambda)x_1 + \lambda x_2]$$
$$\lambda^{q+1}(y_2 - y_1)^{q+1} + \lambda^q(y_1y_2^q - x_1 - x_2^q) + \lambda(y_1^q y_2 - x_1^q - x_2) = 0$$

where we used the equations in (3). If one of $(y_2 - y_1)$, $(y_1y_2^q - x_1 - x_2^q)$, $(y_1^q y_2 - x_1^q - x_2)$ is non-zero, the last is a non-trivial equation in λ with at most $q+1$ solutions. Thus in this case there are at most $q+1$ points in the intersection $r \cap \mathcal{C}$.

If $y_2 - y_1 = y_1y_2^q - x_1 - x_2^q = y_1^q y_2 - x_1^q - x_2 = 0$ then $y_1 = y_2$ and $x_1 = x_2$; the line has equation

$$r : \begin{cases} X = x_1 \\ Y = y_1 \end{cases}$$

with $y_1^{q+1} = x_1^q + x_1$. Moreover we have $y_1 \notin \mathbb{F}_{q^2}$. Indeed, if $y_1 \in \mathbb{F}_{q^2}$, then $y_1^{q^2} - y_1 = 0$ and $z_1 = z_2 = 0$, so the only point in the intersection between r and $\mathcal{C}$ is $P = (x_1, y_1, 0)$. Let $\gamma = y_1^{q^2} - y_1 \neq 0$. The points in $r \cap \mathcal{C}$ are all the points of the form $P = (x_1, y_1, z)$ with $z^m = \gamma$, $z \in \mathbb{F}_{q^{2n}}$. Since in $\mathbb{F}_{q^{2n}}$ there is a primitive m-th root of unity, namely ζ, then if $z_1 \neq 0$ is a solution, also $\zeta^k z$ is a solution for $k = 1, \ldots, m-1$.

Thus the equation $Z^m - \gamma = 0$ has exactly m distinct solutions in $\mathbb{F}_{q^{2n}}$ and $|r \cap \mathcal{C}| = m$.

Theorem 5.13. *Let $r \subset \mathbb{P}^3_{q^{2n}}$ be a line. If r is parallel to the Z-axis then $|r \cap \mathcal{C}| \in \{0, 1, m\}$. Moreover*

(i) if r is m-secant all the m common points are not $\mathbb{F}_{q^2}$-rational;

(ii) if r is not parallel to the Z-axis, it has at most $q+1$ points in common with the curve $\mathcal{C}$.

Note that, since the number of line parallel to the Z axis in $\mathbb{P}^3_{q^{2n}}$ is q^{2n} and the number of $\mathbb{F}_{q^{2n}}$-rational points of $\mathcal{C}_n$ is $N = q^{2n} + 2gq^n + 1 > q^{2n}$, there exist at least one line with m points of intersection with the curve $\mathcal{C}_n$.

5.6 On the minimum distance of one point codes arising from the GGS curve

Denote by $\mathcal{C}$ the GGS curve with the following parameters: q a power of a prime and $n \geq 5$ an odd integer. Let D denote the divisor constructed by the formal sum of all the affine points of $\mathcal{C}$,

$$D = \sum_{P \in \mathcal{C} \setminus \{P_\infty\}} P.$$

Let $C_\ell = C_{\mathcal{L}}(D, \ell P_\infty)$ the evaluation code associated with the divisors D and $G = \ell P_\infty$. Its dual code is $C_\Omega(D, \ell P_\infty)$.

In [32] the authors showed that a basis for the Riemann-Roch space $\mathcal{L}(\ell P_\infty)$ is given by

$$\mathcal{B}_\ell = \{X^i Y^j Z^k \mid i(q^n+1) + jmq + kq^3 \leq \ell, 0 \leq i < q, 0 \leq j < q^2, k \geq 0\}.$$

Example 5.14. *We have that*

1. *the set* $\{1, Z\}$ *forms a basis for* $\mathcal{L}(q^3 P_\infty)$.
2. *the set* $\{1, Y, Z, \ldots, Z^s\}$, *with* $s = \left\lfloor \frac{m}{q^2} \right\rfloor$, *forms a basis for* $\mathcal{L}(mqP_\infty)$.
3. *the set* $\{1, X, Z, \ldots, Z^s, Y, YZ, \ldots, YZ^r\}$, *with* $s = \left\lfloor \frac{q^n+1}{q^3} \right\rfloor$ *and* $r = \left\lfloor \frac{m}{q^3} \right\rfloor$, *forms a basis for* $\mathcal{L}((q^n+1)P_\infty)$.

Note that the monomial with the highest degree in the basis $\mathcal{B}_\ell$ *is* z^s, *with* $s = \left\lfloor \frac{\ell}{q^3} \right\rfloor$.

A generator matrix for C_ℓ is

$$G = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots \\ X^i Y^j Z^k(P_1) & X^i Y^j Z^k(P_2) & \cdots & X^i Y^j Z^k(P_n) \\ \vdots & \vdots & \vdots & \vdots \end{bmatrix}$$

where $P_1, \ldots, P_n$ are all the affine points in $\mathcal{C}$ and every row of G is associated to a different elements of $\mathcal{B}_\ell$.

We use the result on the intersections between lines and the GGS curve to find an upper bound on the minimum distance of the code $C_\Omega(D, \ell P_\infty)$.

Theorem 5.15. *Let $\ell \leq q^3(m-2)$ and $s = \left\lfloor \frac{\ell}{q^3} \right\rfloor$ be two non-negative integers. Let d denote the minimum distance of the code $C_\ell^\perp = C_\Omega(D, \ell P_\infty)$. Then*

$$d \leq s + 2.$$

Proof. Let $\ell \leq q^3(m-2)$, then $s \leq m-2$. By Theorem 5.13 we have that there is a line, parallel to Z, that intersect the curve C in m points. Choose $s+2$ distinct points on this line, namely

$$Q_1 = (a, b, c_1), \ldots, Q_{s+2} = (a, b, c_{s+2}).$$

We claim that the columns associated to the Q_i are linearly dependent. Consider the submatrix M given by the columns associated to the Q_i. Since the points have the same X and Y coordinate we have that a line associated to the monomial $X^iY^jZ^k$ is a multiple of the line associated to the monomial Z^k. Hence the submatrix M has at most $s+1$ linearly independent row equivalently the columns of M are linearly dependent.

We found $s+2$ columns of G that are linearly dependent, so we have that there is a word of weight less or equal than $s+2$ in the dual code $C_\ell^\perp$. Hence the distance d is limited from above by $s+2$. □

Chapter 6

Intersections between the Norm-Trace curve and some low degree curves

As we have seen in the previous chapter the determination of the intersection of a given curve and curves with low degree is often useful for the determination of useful information of the algebraic-geometric codes arising from the curve; see [4, 5, 16, 50, 51].

The Norm-Trace curve, already introduced in the fourth chapter, is a natural generalization of the Hermitian curve to any extension field $\mathbb{F}_{q^r}$ and it has been widely studied for coding theoretical purposes; see [4, 20, 26, 45, 52, 57].

In this chapter, we focus our attention on Norm-Trace curves, we determine the intersection between the Norm-Trace curve over $\mathbb{F}_{q^3}$ and the curves of the form $y = ax^3 + bx^2 + cx + d$ giving a complete characterization of the intersection between the curve and the parabolas and sharp bounds for the other cases. We use it to deduce the weight distribution of the corresponding one point codes arising from the Norm-Trace curve. To do so we use geometrical techniques coming from the properties of irreducible cubic surfaces over finite fields.

6.1 Preliminary Results

Let q be a power of a prime and consider $\mathbb{F}_q$, the finite field with q elements. Let $C \subset (\mathbb{F}_q)^n$ be a linear subspace, then C is a linear code and we will indicate, as usual, with $[n, k, d]$ its parameters, where d is its Hamming minimum distance. We define once again the Norm-Trace curve, for simplicity in this chapter we just call it $\mathcal{N}$.

6.1.1 The Norm-Trace curve

The *Norm-Trace curve* $\mathcal{N}$ is the plane curve defined over $\mathbb{F}_{q^r}$ by the affine equation

$$x^{\frac{q^r-1}{q-1}} = y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y^q + y. \tag{6.1}$$

The *norm* $\mathrm{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}$ and the *trace* $\mathrm{T}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}$ are two well-known functions from $\mathbb{F}_{q^r}$ to $\mathbb{F}_q$ such that

$$\mathrm{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}(x) = x^{\frac{q^r-1}{q-1}} = x^{q^{r-1}+q^{r-2}+\cdots+q+1}$$

and

$$\mathrm{T}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}(x) = x^{q^{r-1}} + x^{q^{r-2}} + \cdots + x^q + x.$$

When q and r are understood, we will write $\mathrm{N} = \mathrm{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}$ and $\mathrm{T} = \mathrm{T}_{\mathbb{F}_q}^{\mathbb{F}_{q^r}}$.

The equation $x^{\frac{q^r-1}{q-1}} = y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y^q + y$ has precisely q^{2r-1} solutions in $\mathbb{A}^2(\mathbb{F}_{q^r})$, so the curve $\mathcal{N}$ has $q^{2r-1}+1$ rational points: q^{2r-1} of them are affine points plus a single point at the infinity P_∞.

If $r = 2$ $\mathcal{N}$ coincides with the Hermitian curve and if $r \geq 3$ $\mathcal{N}$ is singular in P_∞. Moreover it is known that its Weierstrass semigroup in P_∞ is generated by $\left\langle q^{r-1}, \frac{q^r-1}{q-1} \right\rangle$.

Our main aim is the study of the intersection between $\mathcal{N}$ and the cubics of the form $y = ax^3 + bx^2 + cx + d$, where $a, b, c, d \in \mathbb{F}_{q^r}$. In particular we focus on the intersections between $\mathcal{N}$ and parabolas. The case $r = 2$ is completely investigated in [17, 50], so we deal with the more difficult case $r \geq 3$.

6.1.2 Algebraic-Geometric Codes

In this section we introduce some basics notions on AG codes. For a detailed introduction we refer to [65].

Let $\mathcal{N}$ be a projective curve over the finite field $\mathbb{F}_q$, consider the rational function field $\mathbb{F}_q(\mathcal{N})$ and the set $\mathcal{N}(\mathbb{F}_q) = \{P_1, \ldots, P_N\}$ given by the $\mathbb{F}_q$-rational places of $\mathcal{N}$. Given an $\mathbb{F}_q$-rational divisor $D = \sum_{i=1,\ldots,n} m_i P_i$, where $n < N$, the Riemann-Roch space associated to D on $\mathcal{N}$ is the vector space $\mathcal{L}(D)$ over $\mathbb{F}_q$ defined as

$$\mathcal{L}(D) = \{f \in \mathbb{F}_q(\mathcal{N}) \mid (f) + D \geq 0\} \cup \{0\}.$$

It is known that $\mathcal{L}(D)$ is a finite dimensional $\mathbb{F}_q$-vector space and the exact dimension can be computed using the Riemann-Roch theorem. We write $\ell(D) = \dim_{\mathbb{F}_q} \mathcal{L}(D)$.

Consider now the divisor $D = \sum_{P \in S} P$, $S = \{P_1, \ldots, \mathbb{P}_n\} \subsetneq \mathcal{N}(\mathbb{F}_q)$, where all the P's have weight one. Let G be another $\mathbb{F}_q$-rational divisor such that $\mathrm{supp}(G) \cap \mathrm{supp}(D) = \emptyset$. Consider the evaluation map

$$\mathrm{ev} : \mathcal{L}(G) \to (\mathbb{F}_q)^n \qquad \mathrm{ev}(f) = (f(P_1), \ldots, f(P_n)).$$

This map is $\mathbb{F}_q$-linear and it is injective if $n > \deg(G)$.

The AG-code $C_{\mathcal{L}}(D, G)$ associated with the divisors D and G is then defined as $\mathrm{ev}(\mathcal{L}(G))$. It is well known that $\ell(G) > \ell(G - D)$ and that $C_{\mathcal{L}}(D, G)$ is an $[n, \ell(G) - \ell(G - D), d]_q$ code, where $d \geq d^* = n - \deg(G)$, with d^* is the so called *designed minimum distance* of the code.

6.2 Intersections between $\mathcal{N}$ and $y = A(x)$

Our aim is to find out the intersection over $\mathbb{F}_{q^3}$ of $\mathcal{N}$ with the curve defined by the polynomial $y = A(x)$ of degree h, so $A(x) = A_h x^h + \cdots + A_0$, where $A_h \neq 0$ and $A_i \in \mathbb{F}_{q^r}$. More precisely, given two curves $\mathcal{N}$ and $\mathcal{Y}$ lying in the affine space $\mathbb{A}^2(\mathbb{F}_{q^r})$ we call *planar intersection* (or simply intersection) the number of points in $\mathbb{A}^2(\mathbb{F}_{q^r})$ that lie in both curves, disregarding multiplicity. Substituting $y = A(x)$ in the equation of the Norm-Trace curve, we get, by the linearity of T,

$$\mathrm{N}(x) = \mathrm{T}(A_h x^h) + \cdots + \mathrm{T}(A_1 x) + \mathrm{T}(A_0).$$

Given a linear basis $\mathcal{B} = \{w_0, \ldots, w_{r-1}\}$ of $\mathbb{F}_{q^r}$ with respect to $\mathbb{F}_q$, we know that there is a vector space isomorphism $\Phi_{\mathcal{B}} : (\mathbb{F}_q)^r \to \mathbb{F}_{q^r}$ such that $\Phi_{\mathcal{B}}(s_0, \ldots, s_{r-1}) = \sum_{i=0}^{r-1} s_i w_i$. If we consider the maps N,T: $\mathbb{F}_{q^r} \to \mathbb{F}_q$, we

can interpret them from $(\mathbb{F}_q)^r$ to $\mathbb{F}_q$ in this way

$$\widetilde{\mathrm{N}} : (\mathbb{F}_q)^r \to \mathbb{F}_q \qquad \widetilde{\mathrm{T}} : (\mathbb{F}_q)^r \to \mathbb{F}_q$$
$$\widetilde{\mathrm{N}} = \mathrm{N} \circ \Phi_{\mathcal{B}} \qquad \widetilde{\mathrm{T}} = \mathrm{T} \circ \Phi_{\mathcal{B}}$$

and call $\mathrm{T}_i := \mathrm{T}(A_i x^i)$ and $\widetilde{\mathrm{T}}_i := \mathrm{T}_i \circ \Phi_{\mathcal{B}}$, $1 \leq i \leq h$. From now on, we will take as $\mathcal{B}$ a normal basis, i.e. a basis $\mathcal{B} = \{\alpha, \alpha^q, \ldots, \alpha^{q^{r-1}}\}$. We know that such a basis exists, see [46, Theorem 2.35]. A simple manipulation shows that $\widetilde{\mathrm{N}}$ and $\widetilde{\mathrm{T}}_i$ are homogeneous polynomials of degree respectively r and i in $\mathbb{F}_q[x_0, \ldots, x_{r-1}]$. Therefore

$$\widetilde{\mathrm{N}}(x_0, \ldots, x_{r-1}) = \widetilde{\mathrm{T}}_h(x_0, \ldots, x_{r-1}) + \cdots + \widetilde{\mathrm{T}}_1(x_0, \ldots, x_{r-1}) + D \qquad (6.2)$$

which is the equation of a hypersurface of $\mathbb{A}^r(\overline{\mathbb{F}}_q)$, where $D = \mathrm{T}(A_0)$. Notice that the LHS has degree r, while the RHS has degree h.

6.3 Case $r = 3$ and $h = 2$

We are interested in this case to find the number of possible intersections between the Norm-Trace curve and the parabolas. By parabola we mean a curve $y = Ax^2 + Bx + C$, $A, B, C \in \mathbb{F}_{q^3}$ and $A \neq 0$. These numbers help to determine some weights for the corresponding AG code, see Section 6. From now on, $\mathcal{B} = \{\alpha, \alpha^q, \alpha^{q^2}\}$.

Specializing to $y = Ax^2 + Bx + C$, equation (6.2) becomes

$$\widetilde{\mathrm{N}}(x_0, x_1, x_2) = \widetilde{\mathrm{T}}_2(x_0, x_1, x_2) + \widetilde{\mathrm{T}}_1(x_0, x_1, x_2) + D \qquad (6.3)$$

The map $\Phi_{\mathcal{B}}^{-1} : \mathbb{F}_{q^3} \to (\mathbb{F}_q)^3$ induces a correspondence between $\mathbb{F}_q[x_0, x_1, x_2]$ and $\mathbb{F}_{q^3}[x]$ such that we can substitute x with $x_0\alpha + x_1\alpha^q + x_2\alpha^{q^2}$ and x^2 with

$$x_0^2\alpha^2 + x_1^2\alpha^{2q} + x_2^2\alpha^{2q^2} + 2x_0x_1\alpha^{q+1} + 2x_0x_2\alpha^{q^2+1} + 2x_1x_2\alpha^{q^2+q}$$

and the following results holds.

Remark 6.1. Chosen two elements $A = A_0\alpha + A_1\alpha^q + A_2\alpha^{q^2}$ and $B = B_0\alpha + B_1\alpha^q + B_2\alpha^{q^2}$ then

$$\mathrm{T}(AB) = A_0B_0 + A_1B_1 + A_2B_2$$

Proof.

$$\begin{aligned}\mathrm{T}(AB) &= \mathrm{T}((A_0\alpha + A_1\alpha^q + A_2\alpha^{q^2})(B_0\alpha + B_1\alpha^q + B_2\alpha^{q^2})) \\ &= \mathrm{T}(A_0B_0\alpha^2 + A_0B_1\alpha^{q+1} + A_0B_1\alpha^{q^2+1} + A_1B_0\alpha^{q+1} + A_1B_1\alpha^{2q} + A_1B_2\alpha^{q^2+q} + A_2B_2\alpha^{2q^2}) \\ &= A_0B_0 + A_1B_1 + A_2B_2\end{aligned}$$

□

Using these relations we want to write down the explicit equation of the surface (6.3).

$$\begin{aligned}\widetilde{\mathrm{T}}_1 &= B(x_0\alpha + x_1\alpha^q + x_2\alpha^{q^2}) + B^q(x_0\alpha^q + x_1\alpha^{q^2} + x_2\alpha) + B^{q^2}(x_0\alpha^{q^2} + x_1\alpha + x_2\alpha^q) \\ &= x_0\mathrm{T}(\alpha B) + x_1\mathrm{T}(\alpha B^{q^2}) + x_2\mathrm{T}(\alpha B^q)\end{aligned}$$

$$\begin{aligned}\widetilde{\mathrm{T}}_2 =& A(x_0\alpha + x_1\alpha^q + x_2\alpha^{q^2})^2 + A^q(x_0\alpha^q + x_1\alpha^{q^2} + x_2\alpha)^2 + A^{q^2}(x_0\alpha^{q^2} + x_1\alpha + x_2\alpha^q)^2 \\ =& x_0^2\mathrm{T}(A\alpha^2) + x_1^2\mathrm{T}(A\alpha^{2q}) + x_2^2\mathrm{T}(A\alpha^{2q^2}) + 2x_0x_1\mathrm{T}(A\alpha^{q+1}) + 2x_0x_2\mathrm{T}(A\alpha^{q^2+1}) + 2x_1x_2\mathrm{T}(A\alpha^{q^2+q})\end{aligned}$$

$$\begin{aligned}\widetilde{\mathrm{N}} =& (x_0\alpha^{q^2} + x_1\alpha + x_2\alpha^q)(x_0\alpha^q + x_1\alpha^{q^2} + x_2\alpha)(x_0\alpha + x_1\alpha^q + x_2\alpha^{q^2}) \\ =& (x_0^3 + x_1^3 + x_2^3)\mathrm{N}(\alpha) + (x_0^2x_1 + x_1^2x_2 + x_2^2x_0)\mathrm{T}(\alpha^{q+2}) + (x_0^2x_2 + x_1^2x_0 + x_2^2x_1)\mathrm{T}(\alpha^{2q+1}) \\ &+ x_0x_1x_2(3\mathrm{N}(\alpha) + \mathrm{T}(\alpha^3))\end{aligned}$$

Therefore (6.3) becomes

$$\begin{aligned}0 =& -(x_0^3 + x_1^3 + x_2^3)\mathrm{N}(\alpha) - (x_0^2x_1 + x_1^2x_2 + x_2^2x_0)\mathrm{T}(\alpha^{q+2}) - (x_0^2x_2 + x_1^2x_0 + x_2^2x_1)\mathrm{T}(\alpha^{2q+1}) \\ &- x_0x_1x_2(3\mathrm{N}(\alpha) - \mathrm{T}(\alpha^3)) + x_0^2\mathrm{T}(A\alpha^2) + x_1^2\mathrm{T}(A\alpha^{2q}) + x_2^2\mathrm{T}(A\alpha^{2q^2}) + 2x_0x_1\mathrm{T}(A\alpha^{q+1}) \\ &+ 2x_0x_2\mathrm{T}(A\alpha^{q^2+1}) + 2x_1x_2\mathrm{T}(A\alpha^{q^2+q}) + x_0\mathrm{T}(\alpha B) + x_1\mathrm{T}(\alpha B^{q^2}) + x_2\mathrm{T}(\alpha B^q) + D\end{aligned} \tag{6.4}$$

and we call $\mathcal{S}_1 = \mathcal{S}_1(\overline{\mathbb{F}}_q)$ the surface having this equation, which is clearly defined over $\mathbb{F}_q$. Here and in the following, if $\mathcal{N}$ is a surface or a curve, we denote with $\mathcal{N}(\mathbb{F}_q)$ only its affine $\mathbb{F}_q$-rational points.

Remark 6.2. By construction the $\mathbb{F}_q$-rational points of $\mathcal{S}_1$, i.e. the points in $\mathcal{S}_1(\mathbb{F}_q)$, correspond to the intersections in $\mathbb{A}^2(\mathbb{F}_{q^3})$ between the Norm-Trace curve and the parabola $y = Ax^2 + Bx + C$.

Equation (6.4) can be also written as

$$\begin{aligned}0 =& -(x_0\alpha + x_1\alpha^q + x_2\alpha^{q^2})(x_0\alpha^q + x_1\alpha^{q^2} + x_2\alpha)(x_0\alpha^{q^2} + x_1\alpha + x_2\alpha^q) + A(x_0\alpha + x_1\alpha^q + x_2\alpha^{q^2})^2 \\ &+ A^q(x_0\alpha^q + x_1\alpha^{q^2} + x_2\alpha)^2 + A^{q^2}(x_0\alpha^{q^2} + x_1\alpha + x_2\alpha^q)^2 + B(x_0\alpha + x_1\alpha^q + x_2\alpha^{q^2}) \\ &+ B^q(x_0\alpha^q + x_1\alpha^{q^2} + x_2\alpha) + B^{q^2}(x_0\alpha^{q^2} + x_1\alpha + x_2\alpha^q) + D.\end{aligned}$$

If we apply the following linear change of coordinates in $\mathrm{GL}(3, \overline{\mathbb{F}}_q)$

$$\begin{cases} X_0 = x_0\alpha + x_1\alpha^q + x_2\alpha^{q^2} \\ X_1 = x_0\alpha^q + x_1\alpha^{q^2} + x_2\alpha \\ X_2 = x_0\alpha^{q^2} + x_1\alpha + x_2\alpha^q \end{cases}$$

we obtain a new surface $\mathcal{S}_2 = \mathcal{S}_2(\overline{\mathbb{F}}_q)$, defined over $\mathbb{F}_{q^3}$, with equation

$$X_0X_1X_2 = AX_0^2 + A^qX_1^2 + A^{q^2}X_2^2 + BX_0 + B^qX_1 + B^{q^2}X_2 + D. \quad (6.5)$$

Note that this change of coordinates is bijective since its associated matrix is

$$M = \begin{pmatrix} \alpha & \alpha^q & \alpha^{q^2} \\ \alpha^q & \alpha^{q^2} & \alpha \\ \alpha^{q^2} & \alpha & \alpha^q \end{pmatrix}$$

which is a Moore matrix, and its determinant is different from zero since we are dealing with three linearly independent elements, see [46, Corollary 2.38].

Remark 6.3. Clearly, all the $\mathbb{F}_q$-rational points of $\mathcal{S}_1$ are mapped to all $\mathbb{F}_{q^3}$-rational points of $\mathcal{S}_2$ of the form $(\beta, \beta^q, \beta^{q^2})$, $\beta \in \mathbb{F}_{q^3}$. Similarly, $\mathbb{F}_q$-rational lines contained in $\mathcal{S}_1$ are mapped to $\mathbb{F}_{q^3}$-rational lines contained in $\mathcal{S}_2$ having direction $(\beta, \beta^q, \beta^{q^2})$, $\beta \in \mathbb{F}_{q^3}$. The affinity preserves the absolutely irreducible components of the surfaces and the singularities, since it is in $\mathrm{GL}(3, \overline{\mathbb{F}}_\mathrm{q})$.

Proposition 6.4. *$\mathcal{S}_1$ is an absolutely irreducible cubic surface.*

Proof. By Remark 6.3 it is sufficient to prove that $\mathcal{S}_2$ is absolutely irreducible. We proceed by contradiction. If $\mathcal{S}_2$ is reducible, since its degree is three, then it must contain a plane. In this case we would have

$$\begin{aligned} &(h_0X_0^2 + h_1X_1^2 + h_2X_2^2 + h_3X_0X_1 + h_4X_0X_2 + h_5X_1X_2 + h_6X_0 + h_7X_1 + h_8X_2 + h_9)\cdot \\ &(k_0X_0 + k_1X_1 + k_2X_2 + k_3) = X_0X_1X_2 - AX_0^2 - A^qX_1^2 + -A^{q^2}X_2^2 - BX_0 - B^qX_1 - B^{q^2}X_2 - D \end{aligned} \quad (6.6)$$

where $h_i, k_j \in \overline{\mathbb{F}}_q$, $i \in \{0, \ldots, 9\}$ and $j \in \{0, \ldots, 3\}$, and at least one among $h_0, \ldots, h_5$ nonzero and at least one of k_0, k_1, k_2 nonzero. Applying the identity principle for polynomials to the third degree terms, we obtain

$$\begin{cases} h_0k_0 = h_1k_1 = h_2k_2 = 0 \\ h_0k_1 + h_3k_0 = h_0k_2 + h_4k_0 = 0 \\ h_1k_0 + h_3k_1 = h_1k_2 + h_5k_1 = 0 \\ h_2k_0 + h_4k_2 = h_2k_1 + h_5k_2 = 0 \\ h_3k_2 + h_4k_1 + h_5k_0 = 1 \end{cases} \tag{6.7}$$

There are three possibilites (up to a permutation of the indices):

1. $k_0 \neq 0$ and $k_1 = k_2 = 0$. We have that $h_0 = 0$ and (6.7) becomes

$$\begin{cases} h_3k_0 = h_4k_0 = 0 \\ h_1k_0 = 0 \\ h_2k_0 = 0 \\ h_5k_0 = 1 \end{cases}$$

which means $h_1 = h_2 = h_3 = h_4 = 0$ and $h_5 \neq 0$. At this point (6.6) becomes

$$(h_5X_1X_2+h_6X_0+h_7X_1+h_8X_2+h_9)(k_0X_0+k_3) = X_0X_1X_2-AX_0^2-A^qX_1^2-A^{q^2}X_2^2-BX_0-B^qX_1-B^{q^2}X_2-D$$

and since $A^q \neq 0$ and the LHS does not contain any X_1^2 term we have that this cannot happen.

2. $k_0, k_1 \neq 0$ and $k_2 = 0$. We have that $h_1 = h_2 = 0$ and (6.7) becomes

$$\begin{cases} h_3k_0 = h_4k_0 = 0 \\ h_3k_1 = h_5k_1 = 0 \\ h_2k_0 = h_2k_1 = 0 \\ h_4k_1 + h_5k_0 = 1 \end{cases}$$

which means $h_2 = h_3 = h_4 = h_5 = 0$ and this is a contradiction;

3. $k_0, k_1, k_2 \neq 0$. We have that $h_0 = h_1 = h_2 = 0$ and (6.7) becomes

$$\begin{cases} h_3k_0 = h_4k_0 = 0 \\ h_3k_1 = h_5k_1 = 0 \\ h_4k_2 = h_5k_2 = 0 \\ h_3k_2 + h_4k_1 + h_5k_0 = 1 \end{cases}$$

which means $h_2 = h_3 = h_4 = h_5 = 0$ and this is a contradiction.

□

What we want to do now is to estimate the number of $\mathbb{F}_q$-rational points of $\mathcal{S}_1$. Since they correspond to the intersections between $\mathcal{N}$ and $y = Ax^2 + Bx + C$, by applying the Bézout theorem we get that

$$|\mathcal{S}_1(\mathbb{F}_q)| \leq 2(q^2 + q + 1).$$

This bound can be improved, as we will see. Using the fact that the surface is irreducible, we can apply the well-known Lang-Weil bound.

Theorem 6.5 ([47]). *Given nonnegative integers n, d and r, with $d > 0$, there is a positive constant $A(n, d, r)$ such that for every finite field $\mathbb{F}_q$, and every irreducible subvariety $\mathcal{N} \subseteq \mathbb{P}^n(\mathbb{F}_q)$ of dimension r and degree d, we have*

$$||\mathcal{N}(\mathbb{F}_q)| - q^r| \leq (d-1)(d-2)q^{r-\frac{1}{2}} + A(n, d, r)q^{r-1}$$

Corollary 6.6. *The number of $\mathbb{F}_q$-rational points on the surface $\mathcal{S}_1(\mathbb{F}_q)$ is limited by*

$$q^2 + 2q^{\frac{3}{2}} + A(3, 3, 2)q.$$

This bound is better than Bézout's, and other theoretical estimates are known (see [12]), but we want to improve the estimation and arrive at a bound in the form

$$\mathcal{S}_1(\mathbb{F}_q) \leq q^2 + \eta q + \mu$$

where $\mu < q$ and η is upper bounded by a constant (independent from q and μ). Experimentally we found the following

Fact 6.7. *For $q \in \{2, \ldots, 29\}$ it is $|\eta| \leq 2$ and $\mu = 1$.*

Conjecture 1. *$|\eta| \leq 2$ and $\mu = 1$ for all q.*

Let us recall some previous results

Theorem 6.8 (Theorem 27.1, [49]). *Let $\mathcal{S}$ be a cubic surface over $\mathbb{F}_q$. If $\mathcal{S}$ is birationally trivial then*

$$|S(\mathbb{F}_q)| \equiv 1 \mod q.$$

In the case in which S_1 is smooth we also know the possible values for $|S_1(\mathbb{F}_q)|$.

Theorem 6.9 (Theorem 23.1, [49]). *Let $\mathcal{S}$ be a smooth irreducible cubic surface over $\mathbb{F}_q$, then the number of points of $\mathcal{S}(\mathbb{F}_q)$ is exactly*

$$|\mathcal{S}(\mathbb{F}_q)| = q^2 + \eta q + 1$$

where $\eta \in \{-2, -1, 0, 1, 2, 3, 4, 5, 7\}$.

Theorem (6.9) suggests us to to consider separately the case in which $\mathcal{S}_1$ is smooth from the case in which it is singular, indeed (6.9) gives a good bound for the smooth case.

6.4 Preliminaries on the singular case

From now on we investigate when $\mathcal{S}_1$ is singular. We start with observing that the possible singular points can only be isolated double points, since $\mathcal{S}_1$ is a cubic irreducible surface. In this context the following result is very helpful.

Theorem 6.10 ([13]). *Let $\mathcal{S} \subset \mathbb{P}^3(\mathbb{K})$ be a singular irreducible cubic surface defined on the field $\mathbb{K}$. Let $\bar{\mathcal{S}} = \mathcal{S}(\overline{\mathbb{K}})$ be the surface defined by $\mathcal{S}$ over $\overline{\mathbb{K}}$, the algebraic closure of $\mathbb{K}$. Let δ be the number of isolated double points of $\bar{\mathcal{S}}$. Then $\delta \leq 4$ and $\mathcal{S}$ is birationally equivalent (over $\mathbb{K}$) to*

(i) $\mathbb{P}^2(\mathbb{K})$ *if* $\delta = 1, 4$;

(ii) a smooth Del Pezzo surface of degree 4 if $\delta = 2$;

(iii) a smooth Del Pezzo surface of degree 6 if $\delta = 3$.

Recall that a smooth Del Pezzo surface is a smooth projective surface V whose anticanonical class is ample. Many arithmetic properties of these surfaces were investigated by Manin; see [49].

What we want to do now is to find a bound in the desired form for the four possible cases of singularities ($\delta = 1, 2, 3, 4$).

Clearly the singular points on $\mathcal{S}_2$ correspond to the solutions of

$$\begin{cases} X_0X_1X_2 = AX_0^2 + A^qX_1^2 + A^{q^2}X_2^2 + BX_0 + B^qX_1 + B^{q^2}X_2 + D \\ X_1X_2 = 2AX_0 + B \\ X_0X_2 = 2A^qX_1 + B^q \\ X_0X_1 = 2A^{q^2}X_2 + B^{q^2} \end{cases} \tag{6.8}$$

Remark 6.11. Since $\mathcal{S}_1$ is defined over $\mathbb{F}_q$ if $P \in \mathcal{S}_1(\mathbb{F}_q)$ is a singular point then its conjugates with respect to the Frobenius automorphism are singular.

Remark 6.12. Notice also if a singular point of $\mathcal{S}_2$ is $\mathbb{F}_{q^6}$-rational the corresponding singularity of $\mathcal{S}_1$ will be $\mathbb{F}_{q^2}$-rational.

Before delving into the classification of the four cases arising from different values of δ, we need to examine separately the case $B = 0$, which turns out ot be special.

6.4.1 Case B=0

In this case the singularities of the surface correspond to the solutions of

$$\begin{cases} X_0X_1X_2 = AX_0^2 + A^qX_1^2 + A^{q^2}X_2^2 + D \\ X_1X_2 = 2AX_0 \\ X_0X_2 = 2A^qX_1 \\ X_0X_1 = 2A^{q^2}X_1 \end{cases} \tag{6.9}$$

A direct computation leads to the fact that if $(\bar{x}_0, \bar{x}_1, \bar{x}_2) \neq (0,0,0)$ is a singular point, then each $\bar{x}_i$ is different from zero.

Proposition 6.13. *The possible singular case for $B = 0$ are*

(i) $P = (0,0,0)$ is the only singular point, this happens if and only if $D = 0$;

(ii) q is odd and $\delta = 4$, this happens if and only if $-\frac{D}{A}$ is a square.

Proof. Direct computations show that (i) comes from Equation (6.9), so we are left with the case q odd and $(0,0,0)$ not singular. Substituting the derivatives into the equation that defines the surface we get

$$\begin{cases} -AX_0^2 + A^qX_1^2 + A^{q^2}X_2^2 + D = 0 \\ AX_0^2 - A^qX_1^2 + A^{q^2}X_2^2 + D = 0 \\ AX_0^2 + A^qX_1^2 - A^{q^2}X_2^2 + D = 0. \end{cases}$$

Summing pairwise the equations gives us

$$\begin{cases} 2AX_0^2 + 2D = 0 \\ 2A^qX_1^2 + 2D = 0 \\ 2A^{q^2}X_2^2 + 2D = 0 \end{cases}$$

and, since q is odd and $A \neq 0$, we can deduce the system

$$\begin{cases} X_0^2 = -\frac{D}{A} \\ X_1^2 = -\frac{D}{A^q} \\ X_2^2 = -\frac{D}{A^{q^2}} \end{cases} \tag{6.10}$$

The fact that $\beta \in \mathbb{F}_q$ is a square if and only if β^q is a square implies that all the equations of (6.10) are solvable if and only if the first one is. Therefore (6.10) is solvable if and only if $-\frac{D}{A}$ is a square.

Suppose that $-\frac{D}{A}$ is a square, $-\frac{D}{A} = \gamma^2$. From the equation of the surface it follows that $\mathcal{S}_2$ has four singularities of the form $(\gamma, \gamma^q, \gamma^{q^2})$, $(\gamma, -\gamma^q, -\gamma^{q^2})$, $(-\gamma, \gamma^q, -\gamma^{q^2})$, $(-\gamma, -\gamma^q, \gamma^{q^2})$.

□

Remark 6.14. Notice that in case $D \neq 0$ and $-\frac{D}{A}$ square, the four singular points cannot be all conjugates with respect to the Frobenius automorphism.

6.4.2 One singular point

From now on we can consider $B \neq 0$. From Remark 6.11 if $\mathcal{S}_1$ has one singular (double) point P then P has to be $\mathbb{F}_q$-rational, otherwise also its conjugate should be singular. Consider now the sheaf of $\mathbb{F}_q$-rational lines passing through P: each line, not contained in $\mathcal{S}_1(\mathbb{F}_q)$, can intersect $\mathcal{S}_1(\mathbb{F}_q)$ in at most one more point since P is a double point and $\mathcal{S}_1$ has degree three. So the number of $\mathbb{F}_q$-rational points of $\mathcal{S}_1$ is given by

$$|S_1(\mathbb{F}_q)| \leq (q^2 + 1) + h(q - 1) = q^2 + hq + 1 - h$$

where h is the number of lines contained in $\mathcal{S}_1$ and passing through P.

Proposition 6.15. *With the same notation as before we have* $h = 0$.

Proof. We want to give a bound for the maximal number of ($\mathbb{F}_q$-rational) lines fully contained in $\mathcal{S}_1$ and passing through P. For simplicity we proceed with the computations on $\mathcal{S}_2$, since the number of these lines will be the same. Suppose the corresponding singular point Q on $\mathcal{S}_2$ has coordinates (a, a^q, a^{q^2}). Then, since it is the only singular point, we have that Q is the only point that satisfies (6.8). Consider now the sheaf of lines passing

through Q, which has parametric equation, for $b \neq 0$

$$\begin{cases} X_0 = bt + a \\ X_1 = b^q t + a^q \\ X_2 = b^{q^2} t + a^{q^2} \end{cases}$$

and after doing the substitution we get that, if the line is contained into $\mathcal{S}_2$,

$$p_3 t^3 + p_2 t^2 + p_1 t$$

has to be the zero polynomial in $\mathbb{F}_q[t]$, where

$$p_3 = b^{q^2+q+1}$$
$$p_2 = -Ab^2 - (Ab^2)^q - (Ab^2)^{q^2} + b^{q+1}a^{q^2} + b^{q^2+1}a^q + b^{q^2+q}a$$
$$p_1 = -2Aab - 2(Aab)^q - 2(Aab)^{q^2} - Bb - (Bb)^q - (Bb)^{q^2} + ba^{q^2+q} + b^q a^{q^2+1} + b^{q^2}a^{q+1}$$

From the fact that $p_3 = 0$ we have that $\mathrm{N}(b)$ has to be equal to zero, but this means that b is equal to zero, which is a contradiction. □

Putting together the previous observations we have the following result.

Proposition 6.16. *If $\mathcal{S}_1$ has one singular $\mathbb{F}_q$-rational point then*

$$|S_1(\mathbb{F}_q)| \leq q^2 + 1. \tag{6.11}$$

6.4.3 Two singular points

Call P_1 and P_2 the two singular points of $\mathcal{S}_1$, from Remark 6.11 there are two possibilities:

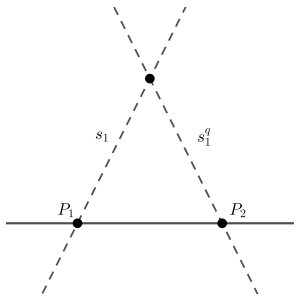
(i) P_1 and P_2 are $\mathbb{F}_q$-rational;

(ii) P_1 and P_2 are $\mathbb{F}_{q^2}$-rational and conjugates.

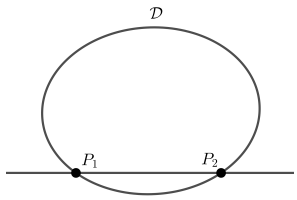
If (i) happens then (6.11) holds and we can use that bound.

We look for a bound when (ii) happens: call r the line passing through P_1 and P_2, since it fixes the conjugate points then it has to be $\mathbb{F}_q$-rational and moreover this line has to be contained in $\mathcal{S}_1(\mathbb{F}_q)$ since the intersection multiplicity of this line is at least 2 in both P_1 and P_2 and the surface has degree 3. Now consider the pencil of planes passing through r and consider the cubic curve $\mathcal{C}$ defined as intersection between any of these planes and $\mathcal{S}_1$. Clearly $\mathcal{C}$ is reducible and there are two possible situations

1. $\mathcal{C}$ is completely reducible. In this case $\mathcal{C}$ is the product of three lines contained in the surface. Call s and s' the two lines different from r: s and s' cannot be $\mathbb{F}_q$-rational since they do not fix the conjugates, so they are $\mathbb{F}_{q^2}$-rational. From the fact that they are contained in $\mathcal{S}_1$ and they pass through conjugate points we have that $s' = s^q$. From this fact we have that the number of $\mathbb{F}_q$-rational points on $\mathcal{C} \setminus r$ is 1 and that point is $s \cap s'$.



2. $\mathcal{C}$ is the product of r and an irreducible conic $\mathcal{D}$ contained in the surface and it contains exactly q points, see [40, Lemma 7.2.3]. In this case the number of $\mathbb{F}_q$ rational points of $\mathcal{D}$ not contained in r is exactly $q-2$.



From the analysis of the two possible cases, recalling that the maximum number of lines contained in a cubic surface is 27 (see [49, Chapter IV]), the first situation can happen at most in 13 cases, and so we have:

$$q + (q-13)(q-2) + 13 \leq |S_1(\mathbb{F}_q)| \leq q(q-2) + q$$

Putting together the previous observations we have the following result.

Proposition 6.17. *If $\mathcal{S}_1$ has two singular $\mathbb{F}_{q^2}$-rational conjugate points then*

$$q^2 - 14q + 39 \leq |S_1(\mathbb{F}_q)| \leq q^2 - q. \tag{6.12}$$

6.4.4 Three singular points

Call P_1, P_2 and P_3 the singular points of $\mathcal{S}_1$, from Remark 6.11 we have the following configurations:

(i) At least one among P_1, P_2 and P_3 is $\mathbb{F}_q$-rational;

(ii) P_1, P_2 and P_3 are $\mathbb{F}_{q^3}$-rational and conjugates.

If (i) happens then (6.11) holds, so our task now is to find a bound when (ii) happens.

We start with observing that the three points cannot be collinear, which comes directly from the following proposition.

Proposition 6.18. *Let $\mathcal{C}$ be a cubic curve such that it has three double points. Then $\mathcal{C}$ is completely reducible and splits in the product of three lines, each passing through a pair of its singular points.*

Proof. Direct consequence of Bézout's theorem. □

In order to get an estimation of $|\mathcal{S}_1(\mathbb{F}_q)|$ for (ii) we change the model of the surface as the following proposition suggests.

Proposition 6.19. *Let $\mathcal{S}$ be a cubic surface over $\mathbb{P}^3(\mathbb{F}_q)$, considered with projective coordinates $[r_0 : r_1 : r_2 : T]$, and such that it has exactly three conjugates $\mathbb{F}_{q^3}$-rational double points, namely P_1, P_2 and P_3. Then $\mathcal{S}$ is projectively equivalent to the surface having affine equation, for certain $\beta, \gamma \in \mathbb{F}_{q^3}$*

$$r_0r_1r_2 + \beta r_0r_1 + \beta^q r_1r_2 + \beta^{q^2} r_0r_2 + \gamma r_0 + \gamma^q r_1 + \gamma^{q^2} r_2 = 0.$$

Proof. Up to a change of projective frame we can consider the following situation

- The plane passing trough the three points is the plane at the infinity $T = 0$ and the triangle of lines through them in that plane is given by r_0, r_1 and r_2;
- $\mathcal{O} = (0 : 0 : 0 : 1) \in \mathcal{S}$.

From these choices we obtain the following equation for the surface $\mathcal{S}$

$$r_0r_1r_2+T(\alpha_0r_0^2+\alpha_1r_1^2+\alpha_2r_2^2+\beta_0r_0r_1+\beta_1r_1r_2+\beta_2r_0r_2)+T^2(\gamma_0r_0+\gamma_1r_1+\gamma_2r_2) = 0$$

where $\alpha_i, \beta_i, \gamma_i \in \mathbb{F}_{q^3}$ for $i \in \{0, 1, 2\}$. From the fact that P_1, P_2 and P_3 are conjugates it follows that r_0, r_1 and r_2 are conjugates and then we get that $\alpha_1 = \alpha_0^q$,

$\alpha_2 = \alpha_0^{q^2}$, $\beta_1 = \beta_0^q$, $\beta_2 = \beta_0^{q^2}$, $\gamma_1 = \gamma_0^q$ and $\gamma_2 = \gamma_0^{q^2}$. Consider now the plane π passing trough P_1, P_2 and $\mathcal{O}$. Without loss of generality, P_1 is the singular point satisfying $T = r_1 = r_2 = 0$, then its coordinates will be $P_1 = (p_1, p_2, p_3, 0)$. Consider now the line, namely s passing through P_1 and $\mathcal{O}$. A general point on that line has coordinates $P_{\lambda,\mu} = (\lambda p_0, \lambda p_1, \lambda p_2, \mu)$. Substituting the coordinates of $P_{\lambda,\mu}$ into the equation of $\mathcal{S}$ we obtain

$$0 = \alpha_0 \lambda r_0^2(P_{\lambda,\mu}) + \beta_0 \lambda^2 r_0(P_{\lambda,\mu}) = \lambda(\alpha_0 r_0^2(P_{\lambda,\mu}) + \beta_0 \lambda r_0(P_{\lambda,\mu})).$$

Now since $r_0(P_1) \neq 0$ and we want $(0, \mu)$ as double solution then $\alpha_0 = 0$. Iterating this process the equation of the surface becomes

$$r_0 r_1 r_2 + T(\beta_0 r_0 r_1 + \beta_0^q r_1 r_2 + \beta_0^{q^2} r_0 r_2) + T^2(\gamma_0 r_0 + \gamma_0^q r_1 + \gamma_0^{q^2} r_2) = 0.$$

□

We want to reduce the problem of counting the points in the form $(\alpha, \alpha^q, \alpha^{q^2})$ on the cubic surface to the problem of counting the points in the same form on a certain quadric. To achieve the result we apply the Cremona transform, call

$$z_1 := \frac{1}{r_1} \quad z_2 := \frac{1}{r_2} \quad z_3 := \frac{1}{r_3},$$

dividing the equation of the surface by $r_1 r_2 r_3$ we obtain

$$\mathcal{Q} : \beta z_3 + \beta^q z_1 + \beta^{q^2} z_2 + \gamma z_2 z_3 + \gamma^q z_1 z_3 + \gamma^{q^2} z_1 z_2 - 1 = 0.$$

Note that if $\gamma = 0$ then $\mathcal{Q}$ collapse to a plane.

Proposition 6.20. *The quadric surface $\mathcal{Q}$ is absolutely irreducible.*

Proof. If $\gamma = 0$ there is nothing to prove, since $\mathcal{Q}$ is a plane. Suppose $\gamma \neq 0$ and that $\mathcal{Q}$ splits in the product of two planes π_1 and π_2, then

$$\beta z_3 + \beta^q z_1 + \beta^{q^2} z_2 + \gamma z_2 z_3 + \gamma^q z_1 z_3 + \gamma^{q^2} z_1 z_2 - 1 = (a_1 z_1 + a_2 z_2 + a_3 z_3 + a_4)(d_1 z_1 + d_2 z_2 + d_3 z_3 + d_4).$$

From the identity principles of polynomials we get that $a_1 d_1 = a_2 d_2 = a_3 d_3 = 0$ Without loss of generality we can consider $a_1 = a_2 = d_3 = 0$ and then the equation becomes

$$\beta z_3 + \beta^q z_1 + \beta^{q^2} z_2 + \gamma z_2 z_3 + \gamma^q z_1 z_3 + \gamma^{q^2} z_1 z_2 - 1 = (a_3 z_3 + a_4)(d_1 z_1 + d_2 z_2 + d_4)$$

and this cannot happen since in the right hand side of this equality we do not have the term $z_1 z_2$. □

We want to count the points on the quadric $\mathcal{Q}$ in the form $(\delta, \delta^q, \delta^{q^2})$, where $\delta \in \mathbb{F}_{q^3}$. Writing down δ on the normal basis $\mathcal{B}$ we get $\delta = w_1\alpha + w_2\alpha^q + w_3\alpha^{q^2}$. Taking w_1, w_2 and w_3 as a set of variables (on $\mathbb{F}_q$) we obtain a $\mathbb{F}_q$-rational quadric surface and its $\mathbb{F}_q$-rational points are in one-to-one correspondence with the searched ones.

$$\beta(w_1\alpha^{q^2} + w_2\alpha + w_3\alpha^q) + \beta^q(w_1\alpha + w_2\alpha^q + w_3\alpha^{q^2}) + \beta^{q^2}(w_1\alpha^q + w_2\alpha^{q^2} + w_3\alpha) +$$
$$\gamma(w_1\alpha + w_2\alpha^q + w_3\alpha^{q^2})(w_1\alpha^q + w_2\alpha^{q^2} + w_3\alpha) + \gamma^q(w_1\alpha^{q^2} + w_2\alpha + w_3\alpha^q)(w_1\alpha^q + w_2\alpha^{q^2} + w_3\alpha) +$$
$$\gamma^{q^2}(w_1\alpha^{q^2} + w_2\alpha + w_3\alpha^q)(w_1\alpha + w_2\alpha^q + w_3\alpha^{q^2}) - 1 = 0.$$

The points we were looking for of the first surface are in one-to-one correspondence with the $\mathbb{F}_q$-rational points on the quadric surface above. It is widely known (see [39, Section 15.3]) that, in this case

$$|S_1(\mathbb{F}_q)| = q^2 + \eta q + 1, \quad \eta \in \{0, 1, 2\} \tag{6.13}$$

since the quadric surface $\mathcal{Q}$ is irreducible.

6.4.5 Four singular points

Call P_1, P_2, P_3 and P_4 the singular points of $\mathcal{S}_1$, applying Remark 6.11 we have the following possibilities:

(i) At least one among P_1, P_2, P_3 and P_4 is $\mathbb{F}_q$-rational;

(ii) There are two couples of $\mathbb{F}_{q^2}$-rational and conjugates singular points.

(iii) P_1, P_2, P_3 and P_4 are $\mathbb{F}_{q^4}$-rational and conjugates.

If (i) or (ii) hold then we have already found out a good bound before, the last thing we have to do is show that (iii) never holds.

Proposition 6.21. *Case (iii) never holds.*

Proof. In order to solve this problem we use a multivariate approach, calculating the elimination ideal with respect to all the variables less one. Consider the equations in (6.8): it is clear that, given X_1 and X_2, the value of X_0 is uniquely determined. For this reason we proceed with eliminating the variables X_0 and X_1 and we obtain the elimination ideal $I_{x_0,x_1} = \langle p_1, p_2 \rangle$, where

$$\begin{aligned}p_1(X_1) =& 2X_1^5A^q + X_1^4B^q - 16X_1^3A^{q^2+q+1} - 8X_1^2A^{q^2+1}B^q - X_1^2B^{q^2+1} + 32X_1A2q^2 + q + 2\\ &- 2X_1AB^{2q^2} - 2X_1A^{q^2}B^2 + 16A^{2q^2+2}B^q - 4A^{q^2+1}B^{q^2+1}\\ p_2(X_1) =& (X_1^2 - 4A^{q^2+1})(X_1^4A^q + X_1^3B^q - 4X_1^2A^{q^2+q+1} + X_1^2D - 4X_1A^{q^2+1}B^q\\ &+ x1B^{q^2+1} - 4A^{q^2+1}D + AB^{2q^2} + A^{q^2}B^2).\end{aligned}$$

On the other hand, if we prooced eliminating the variables X_0 and X_1 we get the elimination ideal $J_{x_0,x_2} = \langle q_1, q_2\rangle$, where $q_1 = p_1(X_2)^q$ and $q_2 = p_2(X_2)^q$. The fact that the two ideals are generated by conjugate polynomials will continue to be true after symmetric annihilation of some of their terms. After further computations using the software MAGMA, which can be completely seen in Section 4.5, we get that one of the generators of I_{x_1,x_2} is a polynomial of degree lower or equal to two, namely $f(X_1)$, and one of the generators of J_{x_0,x_2} is $f(X_2)^q$. From this fact we get that the singularities of $\mathcal{S}_2$ are at most four and if this value is achieved then they belong (at most) to the field $\mathbb{F}_{q^6}$, which means that the singularities of $\mathcal{S}_1$ are at most in the field $\mathbb{F}_{q^2}$. □

6.5 Case $r = 3$ and $h = 3$

Consider the case of the intersection over $\mathbb{F}_{q^3}$ between $\mathcal{N}$ and the curves $y = Ax^3 + Bx^2 + Cx + D$, $A, B, C, D \in \mathbb{F}_{q^3}$ and $A \neq 0$. After doing similar computations to those done for the case $r = 3$ and $h = 2$ we arrive at an equation of a cubic surface $\widehat{\mathcal{S}}_1 = \widehat{\mathcal{S}}_1(\overline{\mathbb{F}}_q)$ defined over $\mathbb{F}_q$, affinely equivalent to a surface $\widehat{\mathcal{S}}_2 = \widehat{\mathcal{S}}_2(\overline{\mathbb{F}}_q)$ defined over $\mathbb{F}_{q^3}$, having equation

$$X_0X_1X_2 = AX_0^3+A^qX_1^3+A^{q^2}X_2^3+BX_0^2+B^qX_1^2+B^{q^2}X_2^2+CX_0+C^qX_1+C^{q^2}X_2+E$$

where $E = \mathrm{T}(D)$. In this more general case $\widehat{\mathcal{S}}_1$ may be reducible, which can possibly increase the number of $\mathbb{F}_q$-rational points of $\widehat{\mathcal{S}}_1$, but on the other hand the reasonings done for $r = 3$ and $h = 2$ can be completely extended if $\widehat{\mathcal{S}}_1$ is irreducible, so we claim the following result.

Theorem 6.22. *Let $r = h = 3$ and consider the $\mathbb{F}_q$-rational cubic surface $\widehat{\mathcal{S}}_1$ associated to the intersections between $\mathcal{N}$ and $y = Ax^3 + Bx^2 + Cx + D$. If $\widehat{\mathcal{S}}_1$ is irreducible then*

$$|\widehat{\mathcal{S}}_1| \leq q^2 + 7q + 1.$$

6.6 AG codes from the Norm-Trace curves

Consider the Norm-Trace curve over the field $\mathbb{F}_{q^3}$: since $r = 3$, $\mathcal{N}$ has $N = q^{2r-1} = q^5$ $\mathbb{F}_{q^3}$-rational points in $\mathbb{A}^2(\mathbb{F}_{q^3})$. We also know that $\mathcal{L}_{\mathbb{F}_q}(2q^2P_\infty) = \{ay + bx^2 + cx + d \,|\, a, b, c, d \in \mathbb{F}_{q^3}\}$. Considering the evaluation map

$$\begin{aligned} \text{ev} : \ & \mathcal{L}_{\mathbb{F}_{q^3}}(2q^2P_\infty) \longrightarrow (\mathbb{F}_{q^3})^{q^5} \\ & f = \tilde{a}y + \tilde{b}x^2 + \tilde{c}x + \tilde{d} \longmapsto (f(P_1), \ldots, f(P_N)) \end{aligned}$$

the associated one-point code will be $C_{\mathcal{L}}(D, 2q^2P_\infty) = \text{ev}(\mathcal{L}_{\mathbb{F}_{q^3}}(2q^2P_\infty))$, where the divisor D is the formal sum of all the q^5-rational affine points of $\mathcal{N}(\mathbb{F}_{q^3})$. The weight of a codeword associated to the evaluation of a function $f \in \mathcal{L}_{\mathbb{F}_{q^3}}(2q^2P_\infty)$ corresponds to

$$\text{w}(\text{ev}(f)) = |\mathcal{N}(\mathbb{F}_{q^3})| - |\{\mathcal{N}(\mathbb{F}_{q^3}) \cap \{\tilde{a}y + \tilde{b}x^2 + \tilde{c}x + \tilde{d} = 0\}\}|.$$

1. If $\tilde{a} = 0$ then we have to study the common zeroes of $\tilde{b}x^2 + \tilde{c}x + \tilde{d}$ and $\mathcal{N}(\mathbb{F}_{q^3})$.
   (a) if $\tilde{b} = \tilde{c} = \tilde{d} = 0$ then $\text{w}(\text{ev}(f)) = 0$;
   (b) if $\tilde{b} = \tilde{c} = 0$ and $\tilde{d} \neq 0$ then $\text{w}(\text{ev}(f)) = q^5$;
   (c) if $\tilde{b} = 0$ and $\tilde{c} \neq 0$ then $\text{w}(\text{ev}(f)) = q^5 - q^2$;
   (d) if $\tilde{c} \neq 0$ and $\tilde{c}^2 - 4\tilde{b}\tilde{d} = 0$ then $\text{w}(\text{ev}(f)) = q^5 - q^2$;
   (e) otherwise $\text{w}(\text{ev}(f)) = q^5 - 2q^2$.
2. On the other hand, if $\tilde{a} \neq 0$ then we have to study the common zeroes between $\mathcal{N}(\mathbb{F}_{q^3})$ and $\tilde{a}y + \tilde{b}x^2 + \tilde{c}x + \tilde{d}$.
   (a) if $\tilde{b} = \tilde{c} = \tilde{d} = 0$ then $\text{w}(\text{ev}(f)) = q^5 - 1$;
   (b) if $\tilde{b} = \tilde{c} = 0$ and $\tilde{d} \neq 0$ then $\text{w}(\text{ev}(f)) = q^5 - q^2$;
   (c) if $\tilde{b} = 0$ and $\tilde{c} \neq 0$ then, applying Bézout theorem, we have that $\text{w}(\text{ev}(f)) \geq q^5 - (q^2 + q + 1)$;
   (d) otherwise, from what we said previously, $\text{w}(\text{ev}(f)) \geq q^5 - (q^2 + 7q + 1)$.

We can summarize our reasonings in the following result.

Theorem 6.23. *Consider the Norm-Trace curve $\mathcal{N}$ over the field $\mathbb{F}_{q^3}$, $q \geq 8$, and the AG code $C = C_{\mathcal{L}}(D, 2q^2 P_\infty)$ arising from $\mathcal{N}$, where $D = \sum_{P \in \mathcal{N}(\mathbb{F}_{q^3}) \setminus P_\infty} P$. Let $\{A_{\mathrm{w}}\}_{0 \leq \mathrm{w} \leq q^5}$ be the weight distribution of C, then the following results hold*

(i) $A_0 = 1$;

(ii) The minimum distance of C is $q^5 - 2q^2$;

(iii) If $\mathrm{w} > q^5 - 2q^2$ and $A_{\mathrm{w}} \neq 0$ then $\mathrm{w} \geq q^5 - q^2 - 7q - 1$;

We conclude this chapter with the weight distribution of the cases $q < 8$, i.e. $q = 2, 3, 5, 7$. In the second column of Table 6.1 the symbol i^j means that the code contains j codewords of weight i.

6.7 MAGMA code

As we said before there are many results obtained with the software MAGMA. This is the commented code.

```
K<x0,x1,x2,A,Aq,Aqq,B,Bq,Bqq,D> := PolynomialRing(Integers(),10);

Sup := x0*x1*x2  - A*x0^2 -Aq*x1^2 -Aqq*x2^2 -B*x0 -Bq*x1-Bqq*x2-D;

Dx0 := Derivative(Sup,x0);
Dx1 := Derivative(Sup,x1);
Dx2 := Derivative(Sup,x2);
```

Table 6.1: Weight distribution

q	Weight Distribution of the corresponding code
2	$0^1\, 24^{196}\, 25^{224}\, 27^{1568}\, 28^{112}\, 29^{1568}\, 31^{224}\, 32^{203}$
3	$0^1\, 225^{9126}\, 227^{6084}\, 230^{64350}\, 233^{225108}\, 234^{1404}\, 236^{185562}\, 239^{30420}\, 242^{234}\, 243^{9152}$
4	$0^1\, 992^{127008}\, 999^{317520}\, 1003^{2733696}\, 1007^{6921936}\, 1008^{8064}\, 1011^{5588352}\, 1015^{952560}\, 1023^{1008}\, 1024^{127071}$
5	$0^1\, 3075^{961000}\, 3089^{5766000}\, 3094^{46717000}\, 3099^{96484400}\, 3100^{31000}\, 3104^{79763000}\, 3109^{13454000}\, 3124^{3100}\, 3125^{961124}$
7	$0^1\, 16709^{20059326}\, 16743^{401186520}\, 16750^{3143683494}\, 16757^{5060681388}\, 16758^{234612}\, 16764^{4473229698}\, 16771^{722135736}\, 16806^{16758}\, 16807^{20059668}$

```
CC := {Sup,Dx0,Dx1,Dx2};

CC1 := {Resultant(pol,Dx0,x0) : pol in CC};

{Factorization(pol) : pol in CC1 | pol ne 0};

CC2 := {Resultant(pol,x1*x2^2 - 4*x1*A*Aq - x2*B - 2*A*Bq,x1) : pol in CC1};

{Factorization(pol) : pol in CC2 | pol ne 0};

p1 := 2*x2^5*Aqq + x2^4*Bqq - 16*x2^3*A*Aq*Aqq - 8*x2^2*A*Aq*Bqq - x2^2*B*Bq
+ 32*x2*A^2*Aq^2*Aqq - 2*x2*A*Bq^2 - 2*x2*Aq*B^2 + 16*A^2*Aq^2*Bqq -
4*A*Aq*B*Bq;

p2 := (x2^2 - 4*A*Aq)*(x2^4*Aqq + x2^3*Bqq - 4*x2^2*A*Aq*Aqq + x2^2*D -
4*x2*A*Aq*Bqq + x2*B*Bq - 4*A*Aq*D + A*Bq^2 + Aq*B^2);

RR := Resultant(p1,p2,x2);

p3 := p1*Coefficients(p2,x2)[7]*x2- p2*Coefficients(p1,x2)[6];

//Case 1 --> B!=0 so p3 has degree 5
p4 := p1*Coefficients(p3,x2)[6]- p3*Coefficients(p1,x2)[6];
Coefficients(p4,x2);

//Case 1.1 --> 4*Aqq^2*D - Aqq*Bqq^2!=0 --> 4*Aqq*D - Bqq^2!=0
//p4 has degree 4
p5 := p4*Coefficients(p3,x2)[6]*x2- p3*Coefficients(p4,x2)[5];

//Case 1.1.1 -> 3*Aqq*B*Bq*Bqq - 4*Aqq*D^2 + Bqq^2*D!=0
//p5 has degree 4
p6 := p5*Coefficients(p4,x2)[5]- p4*Coefficients(p5,x2)[5];


//Case 1.1.1.1 --> 8*A*Aqq^2*Bq^2*D - 2*A*Aqq*Bq^2*Bqq^2
+ 8*Aq*Aqq^2*B^2*D -2*Aq*Aqq*B^2*Bqq^2 - 9*Aqq^2*B^2*Bq^2
+ 4*Aqq*B*Bq*Bqq*D - B*Bq*Bqq^3!=0
//p6 has degree 3
p7 := p6*Coefficients(p5,x2)[5]*x2- p5*Coefficients(p6,x2)[4];
Coefficients(p7,x2);

//Case 1.1.1.1.1 --> Coefficients(p7,x2)[4]!=0
//p7 has degree 3
p8 := p7*Coefficients(p6,x2)[4]- p6*Coefficients(p7,x2)[4];
```

```
Coefficients(p8,x2);
Factorization(Coefficients(p8,x2)[3]);
//SE Coefficients(p8,x2)[3]!=0
//then at most there are 4 singular points

//Case 1.1.1.1.2 -->     Coefficients(p7,x2)[4]=0
//p7 has degree 2
//then at most there are 4 singular points

//Case 1.1.1.2 -->       8*A*Aqq^2*Bq^2*D - 2*A*Aqq*Bq^2*Bqq^2
+ 8*Aq*Aqq^2*B^2*D -2*Aq*Aqq*B^2*Bqq^2 - 9*Aqq^2*B^2*Bq^2
 + 4*Aqq*B*Bq*Bqq*D - B*Bq*Bqq^3=0
//p6 has degree 2
//then at most there are 4 singular points

//Case 1.1.2 ->          3*Aqq*B*Bq*Bqq - 4*Aqq*D^2 + Bqq^2*D=0
(note that D!=0, otherwise B=0)

CC2_0 := {K!((3*B*Bq*Bqq - 4*D^2)^(Degree(pol,A)+Degree(pol,Aq)
+Degree(pol,Aqq)+3)*Evaluate(pol,[x0,x1,x2,- B^2*D/(3*B*Bq*Bqq - 4*D^2),
- Bq^2*D/(3*B*Bq*Bqq - 4*D^2),- Bqq^2*D/(3*B*Bq*Bqq - 4*D^2),B,Bq,Bqq,D]))
 : pol in CC2};
{Factorization(pol) : pol in CC2_0| pol ne 0};

pp1:=(3*x2*B*Bq*Bqq - 4*x2*D^2 - 2*B*Bq*D)*
(3*x2*B*Bq*Bqq - 4*x2*D^2 + 2*B*Bq*D)*
(3*x2^3*B*Bq*Bqq^3*D - 4*x2^3*Bqq^2*D^3
- 9*x2^2*B^2*Bq^2*Bqq^3 + 26*x2^2*B*Bq*Bqq^2*D^2
- 16*x2^2*Bqq*D^4 - 15*x2*B^2*Bq^2*Bqq^2*D
+  32*x2*B*Bq*Bqq*D^3 - 16*x2*D^5 - 9*B^3*Bq^3*Bqq^2
+ 18*B^2*Bq^2*Bqq*D^2 - 8*B*Bq*D^4);
pp2:=(3*x2*B*Bq*Bqq - 4*x2*D^2 - 2*B*Bq*D)*
(6*x2*B*Bq*Bqq^2*D - 8*x2*Bqq*D^3 - 9*B^2*Bq^2*Bqq^2
+ 28*B*Bq*Bqq*D^2 - 16*D^4)*(3*x2^2*B*Bq*Bqq^2
- 4*x2^2*Bqq*D^2 + 2*x2*B*Bq*Bqq*D - 3*B^2*Bq^2*Bqq + 4*B*Bq*D^2);
pp3:=Coefficients(pp1,x2)[6]*pp2*x2-Coefficients(pp2,x2)[5]*pp1;
Factorization(Coefficients(pp3,x2)[5];
//pp3 has degree exactly 4
pp4:=Coefficients(pp3,x2)[5]*pp2-Coefficients(pp2,x2)[5]*pp3;
Factorization(Coefficients(pp4,x2)[4]);
//pp4 has degree exactly 3
pp5:=Coefficients(pp3,x2)[5]*pp4*x2-Coefficients(pp4,x2)[4]*pp3;
Degree(pp4,x2);
//I have at most 4 points
```

```
//case 1.2 -->  4*Aqq*D - Bqq^2=0 (note that D!=0, otherwise B=0)
CC2_0 := {K!((4*D)^(Degree(pol,A)+Degree(pol,Aq)+Degree(pol,Aqq)+3)
*Evaluate(pol,[x0,x1,x2,B^2/(4*D),Bq^2/(4*D),Bqq^2/(4*D),B,Bq,Bqq,D]))
 : pol in CC2};
{Factorization(pol) : pol in CC2_0| pol ne 0};
CC3_0 := {Resultant(2*x2*D - B*Bq,pol,x2) : pol in CC2_0};
{Factorization(pol) : pol in CC3_0| pol ne 0};
//then 2*x2*D - B*Bq=0 has not solution
CC3_0 := {Resultant(2*x2*D + B*Bq,pol,x2) : pol in CC2_0};
{Factorization(pol) : pol in CC3_0| pol ne 0};
//then 2*x2*D - B*Bq=0 could be a solution
CC3_0 := {Resultant(2*x2^3*Bqq^2*D - x2^2*B*Bq*Bqq^2 + 8*x2^2*Bqq*D^2 -
        4*x2*B*Bq*Bqq*D + 8*x2*D^3 + 4*B*Bq*D^2,pol,x2) : pol in CC2_0};
{Factorization(pol) : pol in CC3_0| pol ne 0};
//then B*Bq*Bqq - 8*D^2=0 or
//B^2*Bq^2*Bqq^2 + 20*B*Bq*Bqq*D^2 - 8*D^4=0

//in the first case
CC4_0 := {Resultant(B*Bq*Bqq - 8*D^2,pol,B) : pol in CC2_0};
{Factorization(pol) : pol in CC4_0| pol ne 0};
Resultant(x2*Bqq - 4*D,x2^2*Bqq^2 - 4*x2*Bqq*D - 8*D^2,x2);
//i have two solutions for x2
//in the second case
CC4_0 := {Resultant(B^2*Bq^2*Bqq^2 + 20*B*Bq*Bqq*D^2 - 8*D^4,pol,B) :
// pol in CC2_0};
{Factorization(pol) : pol in CC4_0| pol ne 0};
/*{
        [
        <2, 44>,
        <D, 30>,
        <Bq, 8>,
        <x2^2*Bqq^2 - 10*x2*Bqq*D - 2*D^2, 2>,
        <x2^2*Bqq^2 + 2*x2*Bqq*D - 2*D^2, 1>,
        <x2^2*Bqq^2 + 8*x2*Bqq*D + 4*D^2, 2>,
        <x2^2*Bqq^2 + 10*x2*Bqq*D - 2*D^2, 1>
        ],
        [
        <2, 38>,
        <D, 22>,
        <Bqq, 2>,
```

```
        <Bq, 8>,
        <x2^2*Bqq^2 - 10*x2*Bqq*D - 2*D^2, 2>,
        <x2^2*Bqq^2 + 2*x2*Bqq*D - 2*D^2, 1>,
        <x2^2*Bqq^2 + 8*x2*Bqq*D + 4*D^2, 1>,
        <x2^2*Bqq^2 + 14*x2*Bqq*D + 22*D^2, 1>
        ]
}

> Resultant(x2^2*Bqq^2 - 10*x2*Bqq*D - 2*D^2,x2^2*Bqq^2
+ 2*x2*Bqq*D - 2*D^2,x2);
-288*Bqq^4*D^4
> Resultant(x2^2*Bqq^2 - 10*x2*Bqq*D - 2*D^2,x2^2*Bqq^2
+ 8*x2*Bqq*D + 4*D^2,x2);
468*Bqq^4*D^4
> Resultant(x2^2*Bqq^2 - 10*x2*Bqq*D - 2*D^2,x2^2*Bqq^2
+ 10*x2*Bqq*D - 2*D^2,x2);
-800*Bqq^4*D^4
> Resultant(x2^2*Bqq^2 + 2*x2*Bqq*D - 2*D^2,x2^2*Bqq^2
+ 8*x2*Bqq*D + 4*D^2,x2);
-108*Bqq^4*D^4
> Resultant(x2^2*Bqq^2 + 2*x2*Bqq*D - 2*D^2,x2^2*Bqq^2
+ 10*x2*Bqq*D - 2*D^2,x2);
-128*Bqq^4*D^4
> Resultant(x2^2*Bqq^2 + 8*x2*Bqq*D + 4*D^2,x2^2*Bqq^2
+ 10*x2*Bqq*D - 2*D^2,x2);
148*Bqq^4*D^4
> Resultant(x2^2*Bqq^2 + 14*x2*Bqq*D + 22*D^2,x2^2*Bqq^2
+ 8*x2*Bqq*D + 4*D^2,x2);
-396*Bqq^4*D^4
> Resultant(x2^2*Bqq^2 + 14*x2*Bqq*D + 22*D^2,x2^2*Bqq^2
+ 2*x2*Bqq*D - 2*D^2,x2);
-288*Bqq^4*D^4
> Resultant(x2^2*Bqq^2 + 14*x2*Bqq*D + 22*D^2,x2^2*Bqq^2
- 10*x2*Bqq*D - 2*D^2,x2);
5184*Bqq^4*D^4
*/
//at most four solutions




//case 2 --> B=0
CC2_0 := {Evaluate(pol,[x0,x1,x2,A,Aq,Aqq,0,0,0,D]) : pol in CC2};
{Factorization(pol) : pol in CC2_0| pol ne 0};
//case 2.1 ---> D=0 --> done
```

```
//case 2.1 ---> D!=0 --> done
```

Bibliography

[1] M. Abdón, J. Bezerra, L. Quoos. *Further examples of maximal curves*. Journal of Pure and Applied Algebra **213**, 1192-1196 (2009).

[2] L. Ateş, H. Stichtenoth. *A note on short vectors in lattices from function fields*. Finite Fields Appl. 39, 264–271 (2016).

[3] D. Augot. *Description of the minimum weight codewords of cyclic codes by algebraic system*. Finite Fields Appl. **2**, 138–152 (1996).

[4] E. Ballico, A. Ravagnani. *On the duals of geometric Goppa codes from norm-trace curves*. Finite Fields Appl. **20**, 30-39, (2013).

[5] D. Bartoli, M. Bonini, *Minimum weight codewords in dual algebraic-geometric codes from the Giulietti-Korchmáros curve*, Des. Codes Cryptography, to appear (https://doi.org/10.1007/s10623-018-0541-y) (2018).

[6] D. Bartoli, M. Montanucci, G. Zini. *Multi point AG codes on the GK maximal curve*. Des. Codes Cryptogr., DOI 10.1007/s10623-017-0333-9.

[7] D. Bartoli, M. Montanucci, G. Zini. *AG codes and AG quantum codes from the GGS curve*. Des. Codes Cryptogr. (2017). DOI:10.1007/s10623-017-0450-5

[8] B. Basili. *Indice de Clifford des intersections complétes de l'espace*. Bull. Soc. Math. France 124, 61–95 (1996).

[9] P. Beelen, M. Montanucci. *Weierstrass semigroups on the Giulietti-Korchmáros curve*. Finite Fields Appl. 52, 10–29 (2018).

[10] M. Bonini, M. Montanucci, G. Zini. *On plane curves given by separated polynomials and their automorphisms*, Advances in Geometry, accepted.

[11] M. Bonini, M. Sala. *Intersections between the norm-trace curve and some low degree curves*, submitted.

[12] T.D. Browning. *The Lang-Weil estimate for cubic hypersurfaces*, Canad. Math. Bull. 56, 500–502 (2013).

[13] D.F. Coray, M.A. Tsfasman. *Arithmetic on singular Del Pezzo surfaces.* Proceedings of the London Mathematical Society 3.1 (1988): 25-87.

[14] A. Cossidente, G. Korchmáros, F. Torres. *Curves of large genus covered by the Hermitian curve.* Comm. Algebra 28, 4707-4728, (2000).

[15] A.S. Castellanos, G.C. Tizziotti. *Two-point AG Codes on the GK maximal curves.* IEEE Trans. Inf. Theory **62**(2), 681–686 (2016).

[16] A. Couvreur, *The dual minimum distance of arbitrary-dimensional algebraic–geometric codes.* Journal of Algebra **350**, 84-107 (2012).

[17] G. Donati, N.Durante, G.Korchmáros. *On the intersection pattern of a unital and an oval in* $PG(2, q^2)$. Finite Fields and Their Applications **15**, 785–795 (2009).

[18] I. Duursma. *Two-point coordinate rings for GK-curves.* IEEE Trans. Inf. Theory **57**(2), 593–600 (2011).

[19] S. Fanali, M. Giulietti. *One-point AG codes on the GK Maximal Curves.* IEEE Trans. Inf. Theory **56**(1), 202–210 (2010).

[20] J.I. Farrán, C. Munuera, G. C. Tizziotti, F. Torres. *Gröbner basis for norm-trace codes.* Journal of Symbolic Computation **48**, 54–63 (2013).

[21] J. Fitzgerald, R.F. Lax. *Decoding affine variety codes using Gröbner bases.* Des. Codes Cryptogr. **13**(2), 147–158 (1998).

[22] W. Fulton, *Algebraic curves, An Introduction to Algebraic Geometry.* 2008.

[23] A. Garcia. *Curves over finite fields attaining the Hasse–Weil upper bound.* In: European Congress of Mathematics, Vol. II (Barcelona, 2000), Progr. Math. 202, pp. 199–205. Birkhauser, Basel (2001).

[24] A. Garcia, C. Güneri, H. Stichtenoth, *A generalization of the Giulietti-Korchmáros curve.* Adv. Geom. **10**, 427-434 (2010).

[25] A. Garcia, H. Stichtenoth, C.P. Xing. *On subfields of the Hermitian function field*. Compositio Math., vol. 120, 137-170 (2000).

[26] O. Geil,(2003). *On codes from norm–trace curves*. Finite fields and their Applications **9** (3), 351–371.

[27] M. Giulietti, G. Korchmáros. *On automorphism groups of certain Goppa codes*. Des. Codes Cryptogr. **48** (2008), 177–190.

[28] M. Giulietti, G. Korchmáros. *A new family of maximal curves over a finite field*. Math. Ann. **343**(1), 229–245 (2009).

[29] V.D. Goppa. *Geometry and Codes, Mathematics and its applications*. 24, Kluwer Academic Publishers, Dordrecht-Boston-London, (1988).

[30] V.D. Goppa. *Codes on algebraic curves*. Dokl. Akad. NAUK SSSR **259**, 1289–1290 (1981).

[31] V.D. Goppa. *Algebraic-geometric codes*. Izv. Akad. NAUK SSSR **46**, 75–91 (1982).

[32] C. Güneri, M.Özdemir, H. Stichtenoth, *The automorphism group of the generalized Giulietti–Korchmáros function field*. Advances in Geometry **13**, 369-380 (2013).

[33] R. Guralnick, B. Malmskogb, R. Pries, *The automorphism groups of a family of maximal curves*. Journal of Algebra **361**, 92–106 (2012).

[34] J.P. Hansen. *Codes on the Klein quartic, ideals and decoding*. IEEE Trans. Inf. Theory **33**(6), 923–925 (1987).

[35] R.W. Hartley. *Determination of the ternary collineation groups whose coefficients lie in the* $GF(2n)$. Ann. of Math. Second Series 27 (2), 140–158, (1925).

[36] R. Hartshorne, *Algebraic geometry*. Springer Science & Business Media, (2013).

[37] H.-W. Henn. *Funktionenkörper mit grosser Automorphismengruppe*. J. Reine Angew. Math **302**, 96–115 (1978).

[38] J.W.P. Hirschfeld, G. Korchmáros and F. Torres. *Algebraic Curves over a Finite Field, Princeton Series in Applied Mathematics*, Princeton (2008).

[39] J.W.P. Hirschfeld. *Finite projective spaces of three dimensions*. Oxford University Press, 1985.

[40] J.W.P. Hirschfeld. *Projective Geometries Over Finite Fields*. Oxford Mathematical Monographs. New York: Oxford University Press, 1998.

[41] B. Huppert. *Endliche Gruppen I*, Grundlehren der Mathematischen Wissenschaften **134**, Springer, Berlin, 1967.

[42] N. E. Hurt. *Many Rational Points. Coding Theory and Algebraic Geometry*. Mathematics and Its Applications, 564, Springer Netherlands, (2003).

[43] Y. Ihara. *Some remarks on the number of rational points of algebraic curves over Finite Fields*, J. Fac. Sci. Tokio, 28, 721–724, (1981).

[44] D. Joiner, A. Ksir. *Automorphism groups of some AG codes*. IEEE Trans. Inf. Theory **52** (7) (2006), 3325–3329.

[45] B. Kim, Y. Lee. *The minimum weights of two-point AG codes on norm-trace curves*. Finite Fields and their Applications **53**, 113-–139.

[46] R. Lidl, H. Niederreiter. *Finite fields*. Vol. 20. Cambridge university press, 1997.

[47] S. Lang, A. Weil. *Number of points of varieties in finite fields*. Amer. J. Math. **76**, 819–827 (1954).

[48] F.J. MacWilliams, N. J. A. Sloane. *The theory of error-correcting codes*. Elsevier, 1977.

[49] Y.I. Manin. *Cubic forms: algebra, geometry, arithmetic*. Vol. 4. Elsevier (1986).

[50] C. Marcolla, M. Pellegrini, M. Sala. *On the Hermitian curve and its intersection with some conics*. Finite Fields and Their Applications 28 (2014) 166–187.

[51] C. Marcolla, M. Pellegrini, M. Sala. *On the small-weight codewords of some Hermitian codes*. J. Symbolic Comput. **73**, 27–45 (2016).

[52] C. Marcolla, M. Roggero. Minimum-weight codewords of the Hermitian codes are supported on complete intersections, Journal of Pure and Applied Algebra, to appear (https://doi.org/10.1016/j.jpaa.2018.12.007).

[53] G.L. Matthews, *Codes from the Suzuki function field*. IEEE Trans. Inf. Theory **50**, 3298-3302 (2004).

[54] G.L. Matthews, *Weierstrass semigroups and codes from a quotient of the Hermitian curve*. Des. Codes Cryptogr. **37**, 473-492 (2005).

[55] S. Miura, N. Kamiya. *Geometric Goppa codes on some maximal curves and their minimum distance*. Proc. IEEE Workshop on Information Theory, Susono-shi, Japan (1993), 85–86.

[56] C. Munuera, A. Sepulveda, and F. Torres. *Algebraic Geometry codes from Castle curves*. Coding Theory and Applications. Springer, Berlin, Heidelberg, (2008), 117-127.

[57] C. Munuera, G. C. Tizziotti, F. Torres. *Two-point codes on Norm-Trace curves*. Coding Theory and Applications. Springer, Berlin, Heidelberg. 128–136 (2008).

[58] M. Sala. *Gröbner basis techniques to compute weight distributions of shortened cyclic codes*. J. Algebra Appl. **6**(3), 403–404 (2007).

[59] B. Segre. *Forme e geometrie hermitiane, con particolare riguardo al caso finito*. Ann. Mat. Pura Appl. 70, 1-201, (1965).

[60] A. Seidenberg. *Constructions in algebra*, Trans. Am. Math. Soc. **197**, 273–313 (1974).

[61] Lachaud, G. *Sommes d'Eisenstein et nombre de points de certaines courbes algebriques sur les corps Enis*. C.R. Acad. Sci. Paris, 305, Serie I, 729–732, (1987).

[62] S. Stepanov, *Codes on algebraic curves*. Springer Science & Business Media, (2012).

[63] H. Stichtenoth. *Uber die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik.* II. Ein spezieller Typ von Funktionenkörpern, Arch. Math. **24** (1973), 615-631.

[64] H. Stichtenoth. *A note on Hermitian codes over* $GF(q^2)$. IEEE Trans. Inf. Theory **34**(5), 1345–1348 (1988).

[65] H. Stichtenoth. *Algebraic function fields and codes.* Graduate Texts in Mathematics **254**, Springer, Berlin (2009).

[66] J. Tate. *Endomorphisms of abelian varieties over finite fields.* Matematika, **12**:6 (1968), 31–40; Invent. Math., **2**, 134–144, (1966).

[67] H.J. Tiersma. *Remarks on codes from Hermitian curves.* IEEE Trans. Inf. Theory **33**(4), 605–609 (1987).

[68] M.A. Tsfasman, S.G. Vladut. *Algebraic-Geometric Codes*, Kluwer, Amsterdam (1991).

[69] R. J. Walker. *Algebraic curves.* Princeton University Press (1950).

[70] C.P. Xing, S. Ling. *A class of linear codes with good parameters from algebraic curves.* IEEE Trans. Inf. Theory **46**(4), 1527–1532 (2000).

[71] C.P. Xing, H. Chen, *Improvements on parameters of one-point AG codes from Hermitian curves.* IEEE Trans. Inf. Theory **48**(2), 535–537 (2002).

[72] K. Yang, P.V. Kumar. *On the true minimum distance of Hermitian codes.* Coding Theory and Algebraic Geometry **1518**, Lecture Notes in Math., 99–107 (1992).