On Supersingular Curves over Finite Fields

Saeed Tafazolian

PhD Thesis

Instituto Nacional de Matemática Pura e Aplicada

February 2008

Abstract

In this work we will discuss on minimal and maximal curves over a finite field k. Our method is to consider the curve over $\bar{k}$, the algebraic closure of k, and look at some invariants of the curve which are unchanged with respect to constant field extensions. For example, the p-adic Newton polygon, the Hasse-Witt matrix and the p-rank of the curve. Using these arguments, we characterize some classical maximal and minimal curves, such as Fermat curves, Artin-Schreier curves and also hyperelliptic curves.

Acknowledgements

I would like to thank my advisor Arnaldo Garcia for collaboration and many insightful discussions. I am indebted to him for advice, support and enormous encouragement.

I learned a lot from Karl Otto Stöhr and to him is dedicated this thesis.

I am also grateful to Abramo Hefez, Amilcar Pacheco, Carolina Araujo, Eduardo Steves, Fernando Torres and Hossein Movasati for useful conversations and comments.

I also wish to acknowledge the hospitality of IASBS, ICTP, University of Gottingen where I spend several weeks in the last four years. I also wish to acknowledge the financial support of ClayMath for my visit of University of Gottingen.

I wish to stress the remarkable research atmosphere at IMPA and to acknowledge financial support of IMPA-CNPq.

Many thanks to my friends in Rio: Alex, Ali, Alireza, Amin, André, Delia, Hossein, Julliana, Jusselino, Mahboubeh, Mahdi, Mehdi, Meysam, Miriam, Mohammad, Mostafa and Martin, Parham, Roberto Pescador, Rodrigo, Roger, Said, Tiago.

Finally, I have no words to express my gratitude to my wife.

To my teacher:

Karl Otto Stöhr

Contents

Chapter 1

Introduction

The theory of equations over finite fields (or the theory of congruences) is in the basis of classical number theory. Its foundations were laid, among others, by mathematicians like Fermat, Euler, Lagrange, Gauss, and Galois. Historically, the object of the first investigations in this theory were the congruences of the special form

$$y^2 \equiv f(x) \text{ (modulo a prime number)} \tag{1.1}$$

where $f(x)$ is a polynomial (or rational function) with integer coefficients. Such congruences were used to get results such as the representability of integers as sum of four squares, or the distribution of pairs of quadratic residues, or even the estimation of the sum of Legendre's quadratic residues symbols. E. Artin constructed a quadratic extension of the field $\mathbb{F}_p(x)$, p a prime, by adjoining the roots of the congruence (1.1) and he introduced a zeta-function for this field, in analogy with Dedekind's zeta-function for quadratic extensions of the field of rational numbers. Assuming that Riemann's hypothesis was valid for his zeta-function, Artin conjectured an upper bound for the number of solutions of congruences such as the one in (1.1) above. Artin's conjecture was then proved by Hasse for polynomials $f(x)$ of degrees 3 and 4 over arbitrary finite fields, and widely generalized by A. Weil (see [52]) as follows:

Let $\mathcal{C}$ be a projective geometrically irreducible nonsingular algebraic curve of genus g, defined over a finite field $\mathbb{F}_q$ with q elements, then we have the so-called Hasse-Weil bounds:

$$q + 1 - 2g\sqrt{q} \leq \#\mathcal{C}(\mathbb{F}_q) \leq q + 1 + 2g\sqrt{q} \tag{1.2}$$

where $\mathcal{C}(\mathbb{F}_q)$ denotes the set of $\mathbb{F}_q$-rational points of the curve $\mathcal{C}$. In general, this bound is sharp. In fact if q is square, there exist several curves that attain the upper and lower bounds above.

There are however situations in which the bounds can be improved. For instance, if q is not a square there is a non-trivial improvement due to Serre:

$$q + 1 - g[2\sqrt{q}] \leq \#\mathcal{C}(\mathbb{F}_q) \leq q + 1 + g[2\sqrt{q}],$$

where $[a]$ denotes the integer part of the real number a.

The interest on curves over finite fields was renewed because of applications to Coding Theory and to Finite Geometry. Goppa constructed the so-called algebraic geometric codes. For these codes arising from curves, one has a good lower bound for their minimum distance.

Here we will be interested in *maximal*(resp. *minimal*) curves over $\mathbb{F}_{q^2}$, that is, we will consider curves $\mathcal{C}$ attaining Hasse-Weil's upper (resp. lower) bound:

$$\#\mathcal{C}(\mathbb{F}_{q^2}) = q^2 + 1 + 2gq \text{ (resp. } q^2 + 1 - 2gq).$$

There are three important problems on maximal curves over $\mathbb{F}_{q^2}$:

1. Determination of the *possible genera* of maximal curves over $\mathbb{F}_{q^2}$.
2. Determination of *explicit equations* for maximal curves over $\mathbb{F}_{q^2}$.
3. *Classification* of maximal curves over $\mathbb{F}_{q^2}$ of a given genus.

The methods used to deal with these three problems are: the action of the Frobenius morphism on the Jacobian of a maximal curve (see Section 4.1 here), Weierstrass

Point Theory (including Stöhr-Voloch theory of Frobenius orders of a morphism), Castelnuovo's genus bound for curves in projective spaces and Riemann-Hurwitz genus formula for separable coverings of algebraic curves.

In this thesis, we will discuss on minimal and maximal curves over a finite field k. Our method is to consider the curve over $\bar{k}$, the algebraic closure of k, and look at some invariants of the curve which are unchanged with respect to constant field extensions. For example, the p-adic Newton polygon, the Hasse-Witt matrix and the p-rank of the curve. The Newton polygon is a nice way to describe p-adic values of the zeros and poles of zeta functions and L-functions (see here Section 2.3.5). Maximal and minimal curves are supersingular. Furthermore as we will see here (Theorem 2.61), supersingular curves are minimal over some extension of the base field. Thus their Newton polygons are also maximal in the sense that all slopes are equal to $1/2$. The Hasse-Witt matrix $\mathscr{H}$ of a non-singular algebraic curve $\mathcal{C}$ over a finite field $\mathbb{F}_q$ is the matrix of the Frobenius mapping (p-th power mapping) with respect to any basis for the differentials of the first kind. It is a $g \times g$ matrix where g is the genus of $\mathcal{C}$. We know also the dual of Frobenius mapping which is the so-called Cartier operator acting on differential 1-forms. As maximal curves are supersingular, we have that the Cartier operator is nilpotent (see Section 4.1). Finally the p-rank of a curve is exactly equal to the length of the slope zero segment of its Newton polygon (see Section 2.3.5 and Proposition 2.54). Clearly, the p-rank of a maximal (or minimal) curve is zero.

In Chapter 2, the basic theoretical foundations in algebraic function fields and algebraic curves over finite fields are laid. These ideas will be used throughout the entire work.

In this chapter we introduce the basic definitions and results of the theory of algebraic function fields: valuations, places, adeles, algebraic extensions of function fields, extension of places, ramification index, the decomposition of a place and some Galois extensions of algebraic function fields (Kummer and Artin-Schreier extensions).

The zeta function of curves over finite fields, and some its fundamental properties are also revisited. We also recall Weil's conjectures about the zeta function of varieties.

As a prerequisite to the study of maximal curves, we briefly present fundamental concepts from algebraic curves over a field of positive characteristic. We define the Hasse-Witt matrix, Cartier operator, p-rank of abelian varieties, p-adic Newton polygon. Finally in last section of Chapter 2, we describe some exponential sums (Gauss sum and Jacobi sum). In fact as Hasse, Davenport and Weil have shown, there are deep connections between exponential sums and the zeta function of curves (see Equations (3.5) and (4.5)).

The reader who is well acquainted with all these concepts can concentrate on the notation introduced.

Chapter 3 is part of a joint work ([16]) with Arnaldo Garcia. Let k be a field of positive characteristic p. An additive polynomial in $k[x]$ is a polynomial of the form

$$A(x) = \sum_{i=0}^{n} a_i x^{p^i}.$$

The polynomial $A(x)$ is separable if and only if $a_0 \neq 0$. We consider in this chapter maximal curves $\mathcal{C}$ over $\mathbb{F}_{q^2}$ of the form

$$A(x) = F(y) \tag{1.3}$$

where $A(x)$ is an additive and separable polynomial in $\mathbb{F}_{q^2}[x]$ and where $F(y) \in \mathbb{F}_{q^2}[y]$ is a polynomial of degree m prime to the characteristic $p > 0$. The assumption that $F(y)$ is a polynomial is not too restrictive (see Lemma 3.13 and Remark 3.14). The genus of the curve $\mathcal{C}$ is given by

$$2g(\mathcal{C}) = (degA - 1)(m - 1). \tag{1.4}$$

Maximal curves given by equations as in (1.3) above were already studied. In [3] they are classified under the assumption $m = q + 1$ and a hypothesis on Weierstrass nongaps at a point; in [11] it is shown that if $A(x)$ has coefficients in the finite field $\mathbb{F}_q$ and $F(y) = y^{q+1}$, then the curve $\mathcal{C}$ is covered by the Hermitian curve ; and in [12] it is shown that if $\deg F(y) = m = q + 1$, then the maximality of the curve $\mathcal{C}$ implies that the polynomial $A(x)$ has all roots in the finite field $\mathbb{F}_{q^2}$.

Here we generalize the above mentioned result from [12]; i.e., we show that a maximal curve $\mathcal{C}$ over $\mathbb{F}_{q^2}$ given by Equation (1.3) is such that all roots of $A(x)$ belong to $\mathbb{F}_{q^2}$ (see Theorem 3.15).

Our main result in this chapter is the following theorem. For the proof we will use the p-adic Newton polygon of Artin-Schreier curves that is described in Section 2.3.5.

Theorem 1.1. *Let $\mathcal{C}$ be a maximal curve over $\mathbb{F}_{q^2}$ given by an equation of the form*

$$A(x) = y^m \quad with \quad gcd(p, m) = 1, \tag{1.5}$$

where $A(x) \in \mathbb{F}_{q^2}[x]$ is an additive and separable polynomial. Then we must have that m divides $q + 1$.

Part of the material in Chapter 4 which is based on studying the Hasse-Witt matrix of maximal curves, is another joint work ([17]) with Arnaldo Garcia. First in Section 4.1, we show that if a curve is maximal over $\mathbb{F}_{q^2}$ with $q = p^n$, then we have $\mathscr{C}^n = 0$, where $\mathscr{C}$ is the Cartier operator. For this we discuss the action of the Frobenius morphism on the Jacobian of a maximal curve. We will also describe the Witt cohomology to obtain an elementary proof that $\mathscr{C}^n = 0$.

Using this new theorem, stating $\mathscr{C}^n = 0$, in next sections of chapter 4 we find some classifications for maximal and minimal curves. First in Section 4.2.1, we consider the Fermat curve $\mathcal{C}(m)$ over $\mathbb{F}_{q^2}$, defined by the affine equation $y^m = 1 - x^m$. We

show that $\mathcal{C}(m)$ is maximal over $\mathbb{F}_{q^2}$ if and only if we have that m divides $(q+1)$. This generalizes [1, Corollary 3.5] which deals with the particular case when m belongs to the set of values of the polynomial $T^2 - T + 1$, and it also generalizes [30, Corollary 1] which deals with the case $q = p$ prime (see Remark 4.20).

In Section 4.2.2 we consider maximal curves $\mathcal{C}$ over $\mathbb{F}_{q^2}$ given by an affine equation $y^q - y = f(x)$, where $f(x)$ is a polynomial in $\mathbb{F}_{q^2}[x]$ with degree d prime to the characteristic p. We show that d is a divisor of $q + 1$ and that the maximal curve $\mathcal{C}$ is isomorphic to the curve given by $y^q + y = x^d$ (see Theorem 4.30). In particular this result shows that the hypothesis that d is a divisor of $q + 1$ in Proposition 4.28 (which is due to Wolfmann [54]) is superfluous and also that the maximal curves $\mathcal{C}$ in Theorem 4.30 are covered by the Hermitian curve over $\mathbb{F}_{q^2}$ (see Remark 4.31). The main ideas in Section 4.2.2 come from [28] which deals with the case $q = p$ prime.

In Section 4.2.3 we deal with maximal and minimal hyperelliptic curves $\mathcal{C}$ over $\mathbb{F}_{q^2}$ in characteristic $p > 2$. The genus of $\mathcal{C}$ satisfies $g(\mathcal{C}) \leq (q-1)/2$ and the main result of this section is to to show that the curve $\mathcal{C}$ given by the affine equation

$$y^2 = x^q + x$$

is the unique maximal hyperelliptic curve over $\mathbb{F}_{q^2}$ with genus satisfying $g = (q-1)/2$ (see Theorem 4.36). The main ideas here come from [50] which deals with hyperelliptic curves with zero Hasse-Witt matrix (see Remark 4.37).

Finally in the last section, we study SW-maximal Artin-Schreier curves. A curve $\mathcal{C}$ over $\mathbb{F}_q$, with q non-square, is called SW-maximal if

$$\#\mathcal{C}(\mathbb{F}_q) = q + 1 + [2\sqrt{q}].g(\mathcal{C}).$$

In this thesis the word *curve* will mean a projective nonsingular and geometrically irreducible algebraic curve defined over a perfect field of characteristic $p > 0$. Most

of the time the perfect field will be a finite field or its algebraic closure. Also quite often we represent a curve by an affine plane model with singularities.

Chapter 2

Preliminaries

In this beginning chapter, we shall collect most of the needed background in algebraic function field theory and algebraic curves. For a more comprehensive approach we refer the reader to [43], [40] and [34].

2.1 Algebraic Function Fields

Throughout Sections 2.1.1, 2.1.3 and 2.1.4, k denotes an arbitrary field.

2.1.1 Places and Divisors

Definition 2.1. *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 element $x \in F$ which is transcendental over k.

For brevity, we shall simply refer to F/k as a *function field*. The set $\tilde{k} := \{z \in F | z \text{ is algebraic over } k\}$ is a subfield of F and it is called the *field of constants* of F/k. The field $\tilde{k}$ of constants of an algebraic function field F/k is a finite extension field of k, and F can also be regarded as a function field over $\tilde{k}$. Therefore the following assumption is not critical:

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; i.e., we have that $\tilde{k} = k$.

The simplest example of an algebraic function field is the *rational function field*; F/k is called *rational* if $F = k(x)$ for some $x \in F$ transcendental over k. Any arbitrary function field F/k is often represented as a simple algebraic field extension of a rational function field $k(x)$, i.e., $F = k(x, y)$ where $\varphi(y) = 0$ for some irreducible polynomial $\varphi(T) \in k(x)[T]$.

Definition 2.2. A *valuation ring* of the function field F/k is a ring $\mathcal{O} \subset F$ with the following properties:

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

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

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

Definition 2.3. (a) A *place* P of the function field F/k is the maximal ideal of some valuation ring $\mathcal{O}$ of F/k. Any element $t \in P$ such that $P = t\mathcal{O}$ is called a *prime element* for P (t is also called a *local parameter* or a *uniformizing variable*).

(b) $\mathbb{P}_F := \{P | P \text{ is a place of } F/k\}$.

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

Definition 2.4. Let P be a place.

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

(b) *deg* $P := [F_P : k]$ is called the *degree* of P.

Definition 2.5. A discrete valuation of the function field F/k is a function $\upsilon : F \to \mathbb{Z} \cup \{\infty\}$ with the following properties:

(1) $\upsilon(x) = \infty \Leftrightarrow x = 0$.

(2) $\upsilon(xy) = \upsilon(x) + \upsilon(y)$ for any $x, y \in F$.

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

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

(5) If $x \in k^*$ then $\upsilon(x) = 0$.

Lemma 2.6 ([43], Lemma I.1.10)**.** *Let υ be a discrete valuation of F/k and $x, y \in F$ with $\upsilon(x) \neq \upsilon(y)$. Then $\upsilon(x + y) = min\{\upsilon(x), \upsilon(y)\}$.*

To any place $P \in \mathbb{P}_F$ we associate a function $\upsilon_P : F \to \mathbb{Z} \cup \{\infty\}$ that is a discrete valuation of F/k: Choose a prime element t for P. Then every $0 \neq z \in F$ has a unique representation $z = t^n u$ with $u \in \mathcal{O}_P^*$ and $n \in \mathbb{Z}$. Define $\upsilon_P(z) := n$ and $\upsilon(0) := \infty$.

Definition 2.7. The (additively written) free abelian group which is generated by the places of F/k is denoted by $\mathcal{D}(F)$ and it is called the *divisor group* of F/k.

The elements of $\mathcal{D}(F)$ are called *divisors* of F/k. In the other word, a divisor is a formal sum

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

The *support* of D is the finite set defined by

$$supp\ D := \{P \in \mathbb{P}_F | n_P \neq 0\}.$$

A divisor D is called *positive* if $n_P \geq 0$, for all P; in this case we write $D \geq 0$. The *degree* of a divisor is defined by

$$\deg\ D := \sum_{P \in \mathbb{P}_F} n_P \deg\ P.$$

For a divisor $D = \sum n_p P$, we denote by $\upsilon_P(D) := n_P$.

Definition 2.8. Let $0 \neq x \in F$ and denote by Z (resp. N) the set of zeros (poles) of x in $\mathbb{P}_F$. Then we define

$$div_0(x) := \sum_{P \in Z} \upsilon_P(x)P, \text{ the } \textit{zero divisor} \text{ of } x,$$

$$div_\infty(x) := \sum_{P \in N} (-\upsilon_P(x))P, \text{ the } \textit{pole divisor} \text{ of } x,$$

$$div(x) := div_0(x) - div_\infty(x), \text{ the } \textit{principal divisor} \text{ of } x.$$

Definition 2.9.

$$\mathcal{P}_F := \{div(x) | 0 \neq x \in F\}$$

is called the *group of principal divisor* of F/k. This is a subgroup of $\mathcal{D}_F$, since for $0 \neq x, y \in F$, we have $div(xy) = div(x) + div(y)$. The factor group

$$\mathcal{C}\ell(F) := \mathcal{D}(F)/\mathcal{P}(F)$$

is called the *divisor class group*.

Theorem 2.10 ([43], Theorem I.4.11)**.** *Any principal divisor has degree zero. More precisely: Let $x \in F \setminus k$, then*

$$deg\ div_0(x) = deg\ div_\infty(x) = [F : k(x)].$$

Definition 2.11. Let $P \in \mathbb{P}_F$. An integer $n > 0$ is called a *pole number* of P if and only if there is an element $x \in F$ with $(x)_\infty = nP$. Otherwise n is called a *gap number* (or a *Weierstrass gap*) of P.

The *Weierstrass semigroup* at P is the set

$$H(P) := \mathbb{N} \setminus G(P),$$

where

$$G(P) := \{l \in \mathbb{Z} : l \text{ is a Weierstrass gap at } P\}.$$

Theorem 2.12 ([43], Theorem I.6.7)**.** *Suppose that F/k has genus $g > 0$ and P is a place of degree one. Then there are exactly g gap numbers $i_1 < i_2 < \ldots < i_g$ of P. We have*

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

2.1.2 Adeles

Let $\mathcal{C}$ be a curve defined over an algebraically closed field k of characteristic $p > 0$. Let $F = k(\mathcal{C})$ be the field of rational functions on $\mathcal{C}$.

Definition 2.13. An *adele* (or a *repartition*) of F/k is a mapping

$$\alpha : \begin{cases} \mathbb{P}_F & \to \quad F, \\ P & \mapsto \quad \alpha_P, \end{cases}$$

such that $\alpha_P \in \mathcal{O}_P$ 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

$$\mathscr{A}_F := \{\alpha | \alpha \text{ is an adele of } F/k\}$$

is called the *adele space* of F/k.

The *principal adele* of an element $x \in F$ is the adele with all components α_P satisfying $\alpha_P = x$ (note this definition makes sense because any element $0 \neq x \in F$ has only finitely many zeros and poles). This gives an embedding $F \hookrightarrow \mathscr{A}_F$. The valuations v_P of F/k extend naturally to $\mathscr{A}_F$ by setting $v_P(\alpha) := v_P(\alpha_P)$.

Definition 2.14. For $D \in \mathcal{D}_F$ we define

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

Obviously, $\mathscr{A}_F(D)$ is a k-subspace of the adele space $\mathscr{A}_F$.

We can consider F as a constant sheaf on $\mathcal{C}$, containing the structure sheaf $\mathscr{O}$ as a subsheaf. Then we have the following exact sequence :

$$0 \to \mathscr{O} \to F \to F/\mathscr{O} \to 0. \tag{2.1}$$

As F is a constant sheaf and $\mathcal{C}$ is irreducible we have $H^1(\mathcal{C}, F) = 0$. Thus from the long exact sequence associated to (2.1) we obtain:

$$F \to H^0(\mathcal{C}, F/\mathscr{O}) \to H^1(\mathcal{C}, \mathscr{O}) \to 0. \tag{2.2}$$

This last exact sequence is easy to interpret. Let $\mathscr{A}_F$ be the adeles of F. Adeles $\alpha = (\alpha_P)$ such that $\alpha_P \in \mathcal{O}_P$ for any P form sub-ring $\mathscr{A}_F(0)$ of $\mathscr{A}_F$. Then one can see easily that $\mathscr{A}_F/\mathscr{A}_F(0)$ is canonically isomorphic to $H^0(\mathcal{C}, F/\mathscr{O})$. Finally from the (2.2) we get

$$\mathscr{A}_F/(\mathscr{A}_F(0) + F) \cong H^1(\mathcal{C}, \mathscr{O}), \tag{2.3}$$

since F can be identified as a subring of $\mathscr{A}_F$.

2.1.3 Extensions of Algebraic Function Fields

Any function field over k can be regarded 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.

Definition 2.15. An algebraic function field F'/k' is called an *algebraic extension* of F/k if $F' \supseteq F$ is an algebraic field extension and $k' \supseteq k$. The algebraic extension

F'/k' of F/k is called a *finite extension* if $[F' : F] < \infty$.

Now let us study the relation between the places of F and F'.

Definition 2.16. Consider an algebraic extension F'/k' of F/k. A place $P' \in \mathbb{P}_{F'}$ is said to *lie over* $P \in \mathbb{P}_F$ if $P \subset P'$. We also say that P' is an extension of P or that P *lies under* P', and we write $P'|P$.

Definition 2.17. Let F'/k' be an algebraic extension of F/k, and let $P' \in \mathbb{P}_{F'}$ be a place of F'/k' lying over $P \in \mathbb{P}_F$.

(a) The positive integer $e(P'|P) := e$ with

$$v_{P'}(x) = ev_P(x) \text{ for any } \ x \in F$$

is called the *ramification index* of P' over P. We say that $P'|P$ is *ramified* if $e(P'|P) > 1$, and that $P'|P$ is *unramified* if $e(P'|P) = 1$.

(b) $f(P'|P) := [F'_{P'} : F_P]$ is called the *relative degree* of P' over P.

Note that $f(P'|P)$ can be finite or infinite; in fact it is finite if and only if $[F' : F] < \infty$ (see [43, Proposition III.1.6]).

The place P is said to be *decomposed completely* in an algebraic extension of F if $e(Q|P) = f(Q|P) = 1$ for all places Q of the extension field that lie over P. Note that the existence of a place that decomposes completely implies that $k' = k$. The place P is called *totally ramified* if there is only one place Q lying over P and $e(Q|P) = [F' : F]$.

Definition 2.18. Let F'/k' be an algebraic extension of F/k. For a place $P \in \mathbb{P}_F$ we define its *conorm* (with respect to F'/F) by

$$Con_{F'/F}(P) := \sum_{P'|P} e(P'|P)P',$$

where the sum runs over all places $P' \in \mathbb{P}_{F'}$ lying over P.

Clearly the conorm map is extended to a homomorphism from $\mathcal{D}_F$ to $\mathcal{D}_{F'}$ by setting

$$Con_{F'/F}(\sum n_P P) := \sum n_P Con_{F'/F}(P).$$

Theorem 2.19 ([43], Theorem III.1.11)**.** *Let F'/k' be a finite extension of F/k, P a place of F/k and $P_1, \ldots, P_m$ all the places of F'/k' lying over P. Let $e_i := e(P_i|P)$ denote the ramification index and $f_i := f(P_i|P)$ the relative degree of $P_i|P$. Then*

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

Corollary 2.20 ([43], Corollary III.1.13)**.** *Let $F^{'}/k^{'}$ be a finite extension of F/k. Then for any divisor $A \in \mathcal{D}_F$,*

$$deg\ Con_{F'|F}(A) = \frac{[F^{'} : F]}{[k^{'} : k]}\ deg\ A.$$

Next we want to describe a method which can often be used to determine all extensions of a place $P \in \mathbb{P}_F$ in $F^{'}$. For convenience, we introduce some notation.

$\bar{F} := F_P$ is the residue class field of P.

$\bar{a} := a(P) \in \bar{F}$ is the residue class of $a \in \mathcal{O}_P$.

If $\psi(T) = \sum c_i T^i$ is a polynomial with coefficients $c_i \in \mathcal{O}_P$, we set

$$\bar{\psi}(T) := \sum \bar{c}_i T^i \in \bar{F}[T].$$

Obviously, any polynomial $\gamma(T) \in \bar{F}[T]$ can be represented as $\gamma(T) = \bar{\psi}(T)$ with $\psi(T) \in \mathcal{O}_P[T]$ and deg $\psi(T) =$ deg$\gamma(T)$. With these notations, we have the following theorem due to Kummer.

Theorem 2.21 ([43], Theorem III.3.7)**.** *Suppose that $F^{'} = F(y)$ where y is integral*

over $\mathcal{O}_P$, and consider the minimal polynomial $\varphi(T) \in \mathcal{O}_P[T]$ of y over F. Let

$$\bar{\varphi}(T) = \Pi_{i=1}^{r} \gamma_i(T)^{\epsilon_i}$$

be the decomposition of $\bar{\varphi}(T)$ into irreducible factors over $\bar{F}$ (i.e. the polynomials $\gamma_1(T), \ldots, \gamma_r(T)$ are irreducible, monic pairwise distinct in $\bar{F}[T]$ and $\epsilon_i \geq 1$). Choose monic polynomials $\varphi_i(T) \in \mathcal{O}_P[T]$ with

$$\bar{\varphi}_i(T) = \gamma_i(T) \quad \textit{and} \quad deg\ \varphi_i(T) = deg\ \gamma_i(T).$$

Then, for $1 \leq i \leq r$, there are places $P_i \in \mathbb{P}_{F'}$ satisfying

$$P_i|P, \quad \varphi_i(y) \in P_i \quad \textit{and} \quad f(P_i|P) \geq deg\ \gamma_i(T).$$

The places $P_1, \ldots, P_r$ are distinct.

Moreover if $\epsilon_i = 1$ for all $i = 1, \ldots, r$, then there exists, for $1 \leq i \leq r$, exactly one place $P_i \in \mathbb{P}_{F'}$ with $P_i|P$ and $\varphi_i(y) \in P_i$. The places $P_1, \ldots, P_r$ are all the places of F' lying over P, and we have

$$Con_{F'/F}(P) = \sum_{i=1}^{r} P_i,$$

i.e., $e(P_i|P) = 1$. We also have $f(P_i|P) = deg\ \gamma_i(T)$.

Let F'/k' be a finite separable extension of a function field F/k and P a place of F/k. Then we have the very useful following theorem that yields a formula for the genus of F', the *Hurwitz Genus Formula*. Let $\mathcal{O}'_P$ denote the integral closure of $\mathcal{O}_P$ in F'. Then the set

$$\mathcal{C}_P := \{z \in F' | Tr_{F'/F}(z.\mathcal{O}'_P) \subset \mathcal{O}_P\}$$

is called *complementary module* over $\mathcal{O}_P$. Note that F'/F is assumed to be a separable

extension, hence the $Tr_{F'/F}$ is not identically zero.

One can shows (see [43, Proposition III.4.2]) that there is an element $t \in F'$ (depending on P) such that $\mathcal{C}_P = t.\mathcal{O}'_P$. Then we define for $P'|P$, the *differential exponent* of P' over P by

$$d(P'|P) := \upsilon_{P'}(t).$$

We refer to Section III.5 of [43] for results on the different.

Theorem 2.22 ([43], Theorem III.4.12)**.** Let F/k be an algebraic function field of genus g and F'/F be a finite separable extension. Let k' denote the constant field of F' and g' the genus of F'/k'. Then we have

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

2.1.4 Galois Extensions

Definition 2.23. An extension F'/k' of a function field F/k is said to be *Galois* if F'/F is a Galois extension of finite degree.

Here we would like to recall two simple types of Galois extensions of a function field, namely Kummer extensions and Artin-Schreier extensions. The following two propositions are due to Hasse.

Proposition 2.24 ([43], Proposition III.7.3)**.** *Let F/k be an algebraic function field in which k contains a primitive $n-$th root of unity (with $n \geq 1$ and n relatively prime to the characteristic of k). Suppose that $u \in F$ is an element satisfying*

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

Let

$$F' = F(y) \text{ with } y^n = u.$$

We have:

(a) The polynomial $\Phi(T) = T^n - u$ *is the minimal polynomial of* y *over the subfield* F*. The extension* F'/F *is Galois of degree* n*; its Galois group is cyclic, and all automorphisms of* F'/F *are given by* $\sigma(y) = \zeta y$*, where* $\zeta \in k$ *is an* $n-$*th root of unity.*

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

$$e(P'|P) = \frac{n}{r_P} \quad \text{and} \quad d(P'|P) = \frac{n}{r_P} - 1, \text{ where } r_P := gcd(n, \upsilon_P(u)) > 0.$$

(c) If k' *denotes the constant field of* F' *and* g *(resp.* g'*) is the genus of* F/k *(resp. of* F'/k'*), then*

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

Proposition 2.25 ([43], Proposition III.7.8)**.** *Let* F/k *be an algebraic function field of characteristic* $p > 0$*. Suppose that* $u \in F$ *is an element which satisfies the following condition:*

$$u \neq w^p - w \text{ for all } w \in F.$$

Let

$$F' = F(y) \text{ with } y^p - y = u.$$

For a place $P \in \mathbb{P}_F$ *we define the integer* m_P *by*

$$m_P := \begin{cases} m & \text{if there is an element } z \in F \text{ satisfying} \\ & \upsilon_P(u - (z^p - z)) = -m < 0 \text{ and } gcd(p, m) = 1 \\ -1 & \text{if } \upsilon_P(u - (z^p - z)) \geq 0 \text{ for some } z \in F. \end{cases}$$

We have then:

(a) F'/F *is a cyclic Galois extension of degree* p*. The automorphisms of* F'/F

are given by $\sigma(y) = y + \theta$, *with* $\theta = 0, \ldots, p-1$.

(b) P *is unramified in* F'/F *if and only if* $m_P = -1$.

(c) P *is totally ramified in* F'/F *if and only if* $m_P > 0$. *Denote by* P' *the unique place of* F' *lying over* P. *Then the different exponent* $d(P'|P)$ *is given by*

$$d(P'|P) = (p-1)(m_P + 1).$$

(d) If at least one place $Q \in \mathbb{P}_F$ *satisfies* $m_Q > 0$, *then* k *is algebraically closed in* F', *and*

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

where g' *(resp.* g*) is the genus of* F'/k *(resp. of* F/k*.)*

We need also the following theorem; it is the so-called Hilbert 90 Theorem.

Theorem 2.26 ([36], Theorem 10.5)**.** *Let* K_1 *be a cyclic Galois extension of an arbitrary field* K, *and let* σ *be a generator of the Galois group* $Gal(K_1/K)$. *If* $u \in K_1$, *then* $Tr_{K_1/K}(u) = 0$ *if and only if* $u = \sigma(a) - a$ *for some* $a \in K_1$.

In the particular case of finite fields $K = \mathbb{F}_q$ and $K_1 = \mathbb{F}_{q^m}$ we get for an element $u \in K_1$ that

$$Tr_{K_1/K}(u) = 0 \quad \text{if and only if} \quad u = \beta^q - \beta \ \text{ for some } \beta \in K_1.$$

2.1.5 Algebraic Function Fields over Finite Fields

In this section we consider function fields over a finite constant field. We are mainly interested in the places of degree one of a function field. This number can be estimated by the Hasse-Weil bound.

Throughout this section, F *denotes an algebraic function field of genus* g *whose constant field is the finite field* $k = \mathbb{F}_q$.

As before, $\mathcal{D}_F$ denotes the divisor group of the function field F/k. It is easy to see that there exist only finitely many positive divisors of degree n, for any $n \geq 0$. So we can define

$$A_n := |\{A \in \mathcal{D}_F | A \geq 0 \text{ and } deg\ A = n\}|. \tag{2.4}$$

For instance, $A_0 = 1$ and A_1 is the number of places $P \in \mathbb{P}_F$ of degree one.

Definition 2.27. The power series

$$Z(t) := Z_F(t) := \sum_{n=0}^{\infty} A_n t^n \ \in \ \mathbb{C}[[t]]$$

is called the *zeta function* of F/k.

Observe that we regard t here as a complex variable, and $Z(t)$ is a power series over the field of complex numbers. It is remarkable that this power series is convergent for $|t| < q^{-1}$. In the following we present some properties of the zeta function:

Proposition 2.28 ([43], Proposition V.1.8)**.** *For $|t| < q^{-1}$, the zeta function can be represented as an absolutely convergent product*

$$Z(t) = \prod_{P \in \mathbb{P}_F} (1 - t^{deg\ P})^{-1}.$$

In particular, $Z(t) \neq 0$ for $|t| < q^{-1}$.

The zeta function $Z(t)$ can be extended to a meromorphic function on the whole complex plane; actually $Z(t)$ can be extended to an element $Z(t) \in \mathbb{C}(T)$.

Proposition 2.29 ([43], Proposition V.1.13)**.** *The zeta function of F/k satisfies the functional equation*

$$Z(t) = q^{g-1} t^{2g-2} Z(\frac{1}{qt}).$$

Definition 2.30. The polynomial $L(t) := L_F(t) := (1-t)(1-qt)Z(t)$ is called the *$L-$polynomial* of F/k.

It is easy to show that $L(t)$ is a polynomial of degree$= 2g$. Observe that $L(t)$ contains information about all the numbers A_n $(n \geq 0)$.

Theorem 2.31 ([43], Theorem V.1.15)**.** *(a) The polynomial $L(t)$ belongs to $\mathbb{Z}[t]$.*

(b) We write $L(t) = a_0 + a_1 t + \ldots + a_{2g} t^{2g}$. Then the following holds:

(1) $a_0 = 1$ and $a_{2g} = q^g$.

(2) $a_{2g-i} = q^{g-i} a_i$, for $0 \leq i \leq g$.

(3) $a_1 = N - (q+1)$ where N is the number of places of degree one.

(4) The polynomial $L(t)$ factors in $\mathbb{C}[t]$ in the form

$$L(t) = \prod_{i=1}^{2g} (1 - \alpha_i t), \tag{2.5}$$

where the complex numbers $\alpha_1, \ldots, \alpha_{2g}$ are algebraic integers, and they can be arranged in such a way that $\alpha_i \alpha_{g+i} = q$ holds, for $i = 1, \ldots, g$.

(c) If $L_r(t) := (1-t)(1-q^r t) Z_r(t)$ denotes the $L-$polynomial of the constant field extension $F_r = F\mathbb{F}_{q^r}$, then we have

$$L_r(t) = \prod_{i=1}^{2g} (1 - \alpha_i^r t).$$

The above theorem shows that the number

$$N(F) := N = |\{P \in \mathbb{P}_F; deg\ P = 1\}|$$

can be easily calculated if the $L-$polynomial $L_F(t)$ of $F/\mathbb{F}_q$ is known. More generally, we consider for $r \geq 1$ the number

$$N(F_r) := N_r = |\{P \in \mathbb{P}_{F_r}; deg\ P = 1\}| \tag{2.6}$$

where $F_r = F\mathbb{F}_{q^r}$ is the constant field extension of $F/\mathbb{F}_q$ of degree r. Hence we have

from item 3) of Theorem 2.31:

Corollary 2.32. *For any $r \geq 1$, we have*

$$N_r = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r.$$

In particular, $N = q + 1 - \sum_{i=1}^{2g} \alpha_i$.

The next theorem is a very deep result. It is the main ingredient in the proof of the Hasse-Weil bound.

Theorem 2.33 ([43], Theorem V.2.1)**.** *The reciprocals of the roots of $L_F(t)$ satisfy*

$$|\alpha_i| = q^{1/2} \qquad \text{for } i = 1, \ldots, 2g.$$

As an important conclusion we have:

Theorem 2.34 (Hasse-Weil Bound)**.** *The number $N = N(F)$ of places of $F/\mathbb{F}_q$ of degree one can be estimated by*

$$|N - q + 1| \leq 2g\sqrt{q}.$$

There are however situations in which the bound can be improved. For instance, if q is not a square there is a non-trivial improvement due to Serre:

$$q + 1 - g[2\sqrt{q}] \leq N \leq q + 1 + g[2\sqrt{q}],$$

where $[a]$ denote the integer part of the real number a.

Remark 2.35. Let F/k be a function field with constant field $k = \mathbb{F}_q$ (i.e., $\mathbb{F}_q$ is algebraically closed in F). To the field F there is an associated projective nonsingular and geometrically irreducible curve $\mathcal{C}$ defined over $k = \mathbb{F}_q$. The places of F of degree

one correspond to $\mathbb{F}_q$-rational points on the curve $\mathcal{C}$; i.e., we have

$$N(F) = \#\mathcal{C}(\mathbb{F}_q).$$

The field F is the field of rational functions (defined over $k = \mathbb{F}_q$) on the associated curve $\mathcal{C}$.

2.2 The Weil Conjectures

In 1949, André Weil made a series of very general conjectures concerning the number of points on varieties defined over finite fields.

Let k be a field with q elements and for each integer $n \geq 1$, let k_n be the extension of k of degree n, so $\#k_n = q^n$. Let $\mathcal{V}/k$ be a projective nonsingular variety of dimension d, so $\mathcal{V}$ is the set of zeros

$$f_1(x_0, \ldots, x_s) = \ldots = f_m(x_0, \ldots, x_s) = 0,$$

of a collection of homogeneous polynomials with coefficients in k. Then $\mathcal{V}(k_n)$ is the set of points of $\mathcal{V}$ with coordinates in k_n. We put the number of such points into a generating function.

Definition 2.36. The zeta function of $\mathcal{V}/k$ is the power series

$$Z(\mathcal{V}/k; t) = \exp(\sum_{n=1}^{\infty} (\#\mathcal{V}(k_n)) \frac{t^n}{n}).$$

Here if $F(t) \in \mathbb{Q}[[t]]$ is a power series with no constant term, then exp(F(t)) is the power series $\sum_{i=0}^{\infty} F(t)^i/i!$.

Theorem 2.37. ***(Weil conjectures)*** *Let k be a field with q elements and $\mathcal{V}/k$ a smooth projective variety of dimension n.*

(a) Rationality

$$Z(V/k;t) \in \mathbb{Q}(t).$$

(b) Functional Equation

There is an integer ϵ (the Euler characteristic of $\mathcal{V}$) so that

$$Z(\mathcal{V}/k;1/q^n t) = \pm q^{n\epsilon/2} t^{\epsilon} Z(\mathcal{V}/k;t).$$

(c) Riemann Hypothesis

There is a factorization

$$Z(\mathcal{V}/k;t) = \frac{P_1(t)\dots P_{2n-1}(t)}{P_0(t)P_2(t)\dots P_{2n}(t)}$$

with each $P_i(t) \in \mathbb{Z}[t]$. Further $P_0(t) = 1-t$, $P_{2n}(t) = 1-q^n t$, and for each $1 \le i \le 2n-1$, the polynomial $P_i(t)$ factors (over $\mathbb{C}$) as

$$P_i(t) = \prod_j (1-\alpha_{ij}t) \text{ with } |\alpha_{ij}| = q^{i/2}.$$

This conjecture was proposed by Weil in 1949, and proven by him for curves and abelian varieties. Weil also observed that most of these properties would follow formally for general varieties $\mathcal{V}$ from the existence of a good cohomology theory, what is now called Weil cohomology theory. In fact the Lefschetz fixed point theorem suggests why these conjectures are true.

Let q be the order of k; and $\mathscr{F}$ be the endomorphism on the l-adic *étale* cohomology groups $H^i_{et}(\bar{\mathcal{V}}, \mathbb{Q}_l)$ of $\mathcal{V}$ (for some prime l different from the characteristic of k and $\bar{\mathcal{V}}$ a geometric model of $\mathcal{V}$) induced by the endomorphism of $\bar{\mathcal{V}}$ given by $x \mapsto x^q$: The Grothendieck-Lefschetz formula expresses this zeta function as a rational fraction in

terms of the (reciprocal) characteristic polynomials of $\mathscr{F}$ on the H^i_{et}' s

$$\#\mathcal{V}(k) = \sum_{r=0}^{2n}(-1)^r Tr(\mathscr{F}|H^r_{et}(\bar{\mathcal{V}}, \mathbb{Q}_l)). \tag{2.7}$$

Hence

$$Z(\mathcal{V}/k;t) = \frac{P_1(t)\dots P_{2n-1}(t)}{P_0(t)P_2(t)\dots P_{2n}(t)},$$

where

$$P_i(t) = \det(1 - \mathscr{F}t|H^i_{et}(\bar{\mathcal{V}}, \mathbb{Q}_l)). \tag{2.8}$$

However the rationality of the zeta function in general was established by Dwork in 1960 using techniques of $p-$adic functional analysis. In 1962 the $l-$adic cohomology theory developed by Grothendieck and others gave another proof of the rationality and of the functional equation. Then in 1973 Deligne proved the Riemann hypothesis.

We now recall the Weil conjectures for curves (Hasse-Weil Theorem). Let $\mathcal{C}$ be a projective nonsingular geometrically irreducible curve of genus g defined over k, then

$$Z(\mathcal{C}/k;t) = \frac{L(t)}{(1-t)(1-qt)},$$

where $L(t)$ is a polynomial in $\mathbb{Z}[t]$ of degree $2g$ such that

$$L(t) = \prod_{i=1}^{2g}(1 - \alpha_i t),$$

where $\alpha_i \in \mathbb{C}$ with $|\alpha_i| = q^{1/2}$ for any $1 \leq i \leq 2g$. Using this zeta function for the curve $\mathcal{C}$ we have that $\#\mathcal{C}(\mathbb{F}_q) = 1 + q - \sum_{i=1}^{2g}\alpha_i$. One can show that this is equivalent to the bound below:

$$|\#\mathcal{C}(\mathbb{F}_q) - (1+q)| \leq 2gq^{1/2}.$$

The following theorem is due to Rosenlicht and it is crucial for us:

Theorem 2.38 ([42], VII, Theorem 9)**.** *Let $\mathcal{C}$ be a curve with Jacobian $\mathcal{J}$. Then the canonical map $\mathcal{C} \to \mathcal{J}$ induces the following isomorphism:*

$$H^1(\mathcal{C}, \mathscr{O}_{\mathcal{C}}) \simeq H^1(\mathcal{J}, \mathscr{O}_{\mathcal{J}}).$$

Remark 2.39. There is a similar result for the étale cohomology (see [6], Corollary 9.6). In fact we have

$$H^1_{et}(\mathcal{C}, \mathbb{Z}_l) \simeq H^1_{et}(\mathcal{J}, \mathbb{Z}_l) \simeq T_l\mathcal{J},$$

where $T_l\mathcal{J} := \lim_{\leftarrow} \mathcal{J}[l^m]$.

Corollary 2.40. *If $L(t)$ is the numerator of the zeta function associated to the curve $\mathcal{C}$, then $h(t) = t^{2g}L(t^{-1})$ is the characteristic polynomial of the Frobenius action on the Jacobian $\mathcal{J}$ of $\mathcal{C}$.*

Proof. From Equation (2.8) we have

$$\begin{aligned} L(t) &= \det(1 - \mathscr{F}t | H^1_{et}(\mathcal{C}, \mathbb{Q}_l)) \\ &= \det(1 - \mathscr{F}t | H^1_{et}(\mathcal{J}, \mathbb{Q}_l)) \\ &= t^{2g}h(t^{-1}). \end{aligned}$$

■

2.3 Algebraic Curves

2.3.1 Maximal Curves

One is often interested in curves $\mathcal{C}$ which have many points; i.e., curves $\mathcal{C}$ such that $N = \#\mathcal{C}(\mathbb{F}_q)$ is a big number. So we introduce the following notion:

Definition 2.41. A curve $\mathcal{C}$ of genus $g \neq 0$ defined over $\mathbb{F}_q$ is said to be *maximal* (resp. *minimal*) if $N = q + 1 + 2gq^{1/2}$ (resp. if $N = q + 1 - 2gq^{1/2}$).

Obviously, maximal (or minimal) curves over $\mathbb{F}_q$ with genus $g \neq 0$ can exist only if q is a square.

Lemma 2.42. *The curve $\mathcal{C}$ is maximal (resp. minimal) over $\mathbb{F}_{q^2}$ if and only if we have that*

$$\alpha_i = -q \ (resp.\ \alpha_i = q) \ \ for\ i = 1, \ldots, 2g. \tag{2.9}$$

Proof. Suppose $\mathcal{C}$ is a maximal curve over $\mathbb{F}_{q^2}$. Let $\alpha_1, \ldots, \alpha_{2g}$ be the reciprocals of the roots of $L(t)$. Since

$$N = q + 1 - \sum_{i=1}^{2g} \alpha_i \text{ and } |\alpha_i| = q,$$

the assumption $N = q + 1 + 2gq$ implies that

$$\alpha_i = -q \text{ for } i = 1, \ldots, 2g.$$

The result for minimal curves follows similarly. ■

Corollary 2.43. *Let $\mathcal{C}$ be a maximal curve over $\mathbb{F}_{q^2}$. Then the curve $\mathcal{C}$ is minimal (resp. maximal) over $\mathbb{F}_{q^{2n}}$ for n even (resp. odd).*

Corollary 2.44. *Let $\mathcal{C}$ be a maximal (resp. minimal) curve over $\mathbb{F}_{q^2}$. Then*

$$L(t) = (1 + qt)^{2g} \ (resp.\ L(t) = (1 - qt)^{2g}). \tag{2.10}$$

We recall the following fact about maximal curves (see [49] and [43]):

Proposition 2.45. *Suppose q is square. For a smooth projective curve $\mathcal{C}$ of genus g, defined over $k = \mathbb{F}_q$, the following conditions are equivalent:*

- *$\mathcal{C}$ is maximal.*

- *Jacobian of $\mathcal{C}$ is $k-$isogenous to the g-th power of a supersingular elliptic curve, all of whose endomorphisms are defined over k.*

Our next result due to Ihara shows that $\mathcal{C}$ over $\mathbb{F}_{q^2}$ can not be maximal if the genus is large with respect to q.

Proposition 2.46 ([27])**.** *Suppose that $\mathcal{C}$ over $\mathbb{F}_{q^2}$ is maximal. Then*

$$g(\mathcal{C}) \leq \frac{q(q-1)}{2}.$$

Proof. We consider the number N_2 of rational points on the curve $\mathcal{C}$ over $\mathbb{F}_{q^4}$. We have from Corollary 2.43:

$$N_2 = q^4 + 1 - \sum_{i=1}^{2g} \alpha_i^2 = q^4 + 1 - 2gq^2.$$

Hence we get the inequality below since $N_2 \geq N = \#\mathcal{C}(\mathbb{F}_{q^2})$:

$$q^2 + 1 + 2gq \leq q^4 + 1 - 2gq^2.$$

The inequality $g \leq q(q-1)/2$ follows immediately. ■

There is a unique maximal curve over $\mathbb{F}_{q^2}$ which attains the above genus bound, and it can be given by the affine equation (see [39])

$$y^q + y = x^{q+1}. \tag{2.11}$$

This is the so-called *Hermitian curve* over $\mathbb{F}_{q^2}$.

Remark 2.47. As J. P. Serre has pointed out, if there is a morphism defined over the field k between two curves $f : \mathcal{C} \longrightarrow \mathcal{D}$, then the $L-$polynomial of $\mathcal{D}$ divides the one of $\mathcal{C}$. Hence a subcover $\mathcal{D}$ of a maximal curve $\mathcal{C}$ is also maximal (see Proposition 6 of [31]). So one way to construct explicit maximal curves over $\mathbb{F}_{q^2}$ is to find equations

for subcovers of the Hermitian curve (see [1] and [15]). On the other hand, it was a conjecture that every maximal curve over $\mathbb{F}_{q^2}$ is a subcover of the Hermitian curve given by Equation 2.11. Recently this conjecture was disproved (see [19]).

2.3.2 The Hasse-Witt Matrix

Let k be a field of characteristic $p > 0$ and $\mathcal{C}$ a curve defined over k of genus $g > 0$, with function field $F = k(\mathcal{C})$. We suppose that there is on the curve $\mathcal{C}$ a set $P_1, \ \ldots \ P_g$ of distinct $k-$rational points such that the divisor $D = \sum_{i=1}^{g} P_i$ is nonspecial. For each P_i we choose a local uniformizer t_i and define adeles $\alpha_i = (\alpha_{i,P})$ for $0 \leq i \leq g$ as below:

$$\alpha_{i,P} = \begin{cases} 0 & \text{if} \quad P \neq P_i, \\ \frac{1}{t_i} & \text{if} \quad P = P_i, \end{cases}$$

Then $\alpha_1, \ \ldots \ \alpha_g$ form a basis of

$$\mathscr{A}_F/(\mathscr{A}_F(0) + F),$$

since the divisor $\sum_{i=1}^{g} P_i$ was chosen nonspecial. In particular, there is a congruence relation as below

$$\alpha_j^p \equiv \sum_{i=1}^{g} a_{ij}\alpha_i \bmod (\mathscr{A}_F(0) + F), \quad \text{with } a_{ij} \in k.$$

Definition 2.48. The matrix $\mathscr{H} = (a_{ij})$ is called the *Hasse-Witt matrix* of of the curve $\mathcal{C}$.

It was first introduced by Hasse and Witt in [26] in the way just described, and there they established two basic properties:

1) If the nonspecial system P_i of g points is replaced by g others, then $\mathscr{H}$ is

transformed according to the law

$$\mathscr{H} \to S^{-1}\mathscr{H}S^{(p)}$$

where S is a nonsingular $g \times g$ matrix with entries in k and $S^{(p)}$ is obtained from S by raising each of its entries to the p-th power.

2) If k is algebraically closed, the cyclic unramified extensions of $\mathcal{C}$ of degree p are in one-to-one correspondence with equivalence classes of column vectors $\bar{c} \in k^g$ modulo multiplication by elements of the prime field satisfying

$$\mathscr{H}\bar{c}^{(p)} = \bar{c}.$$

The $\bar{c}'$s form a linear space whose dimension s is the rank of the matrix

$$\mathscr{H}\mathscr{H}^{(p)} \dots \mathscr{H}^{(p^{g-1})}. \tag{2.12}$$

Now according to (2.3), we can interpret the Hasse-Witt matrix of the curve $\mathcal{C}$ as the matrix of the semi-linear Frobenius operator

$$\mathscr{F} : H^1(\mathcal{C}, \mathscr{O}) \to H^1(\mathcal{C}, \mathscr{O}), \tag{2.13}$$

for a suitable basis of $H^1(\mathcal{C}, \mathscr{O})$.

In the following we recall some facts from [26]:

In general case , let ψ be a $p-$linear endomorphism of the vector space V, of finite dimension, over a algebraically closed field k of characteristic $p > 0$. Then we can find a canonical decomposition

$$V = V_s \oplus V_\sigma, \tag{2.14}$$

where V_s and V_σ are stable under the endomorphism ψ. Moreover ψ is nilpotent

on V_σ and surjective on V_s. Dimensions of V_s and V_σ are denoted by $s(V)$ and $\sigma(V)$ respectively. It is shown moreover that V_s contains a basis $e_1, \ldots, e_s$ such that $\psi(e_i) = e_i$ for all i. Let $v \in V$ be such that $\psi(v) = v$, then v is a linear combination of $e_1, \ldots, e_s$ with integer coefficients mod p, and therefore such fixed elements v form the finite group V^ψ of order $p^{s(V)}$.

Let V' be the dual space of V. The transpose ψ' of ψ is the endomorphism p^{-1}-linear on V' defined by the formula:

$$< \psi v,\ v' >=< v,\ \psi' v' >^p \ \text{ for } v \in V \text{ and } v' \in V'. \tag{2.15}$$

To the decomposition (2.14) corresponds the dual decomposition:

$$V' = V'_s \oplus V'_\sigma. \tag{2.16}$$

With the above notation, set $V = H^1(\mathcal{C}, \mathscr{O})$ and the endomorphism $\psi = \mathscr{F}$ such as (2.13). From Serre duality we know that $V' = H^0(\mathcal{C}, \Omega^1)$. In fact if we identify $\mathscr{A}_F/(\mathscr{A}_F(0) + F)$ with $H^1(\mathcal{C}, \mathscr{O})$, it is well-known that the space $\mathscr{A}_F/(\mathscr{A}_F(0) + F)$ is the dual of $H^0(\mathcal{C}, \Omega^1)$. The duality comes from the following bilinear form:

$$< \alpha, \omega >= \sum_{P \in \mathcal{C}} \mathrm{res}_P(\alpha_P \omega), \tag{2.17}$$

where α is an adele and ω is a differential form .

The dual of $\mathscr{F}$ is very interesting and will be described in the next section.

2.3.3 Cartier Operator

Let k be a perfect field of characteristic $p > 0$. If F is a function field in one variable over k, then F has a unique purely inseparable subextension of degree p. If x is an element of F such that x is not in F^p, then $F = F^p(x)$.

Any arbitrary differential form ω of F can be written as $\omega = ydx$ for some $y \in F$, or in other words

$$\omega = (y_0^p + y_1^p x + \ldots + y_{p-1}^p x^{p-1})dx \text{ where } y_i \in F.$$

We define the *Cartier operator* $\mathscr{C}$ on differential forms by letting

$$\mathscr{C}\omega = y_{p-1}dx.$$

Remark 2.49. On can show that this value $\mathscr{C}\omega$ is independent of the representation of the differential form, i.e., we get the same value if we write the form as $\omega = zdt$ for some $z \in F$ and $t \in F \setminus F^p$ (see [33, Appendix 2]).

The Cartier operator is obviously additive, and it is linear with respect to the prime field. Let $\mathcal{C}$ be a curve defined over an algebraically closed field k of characteristic $p > 0$. Let $F = k(\mathcal{C})$ be the field of $k-$rational functions on $\mathcal{C}$. We have the following properties:

(i) $\mathscr{C}$ is $1/p-$linear; i.e., $\mathscr{C}$ is additive and $\mathscr{C}(z^p\omega) = z\,\mathscr{C}(\omega)$,

(ii) $\mathscr{C}$ vanishes on exact differentials; i.e., $\mathscr{C}\omega = 0$ if and only if $\omega = (dh)$ for some $h \in F$,

(iii) $\mathscr{C}(z^{p-1}dz) = dz$,

(iv) a differential $\omega \in H^0(\mathcal{C}, \Omega^1)$ is logarithmic (i.e., there exists $z \neq 0$ such that $\omega = dz/z$) if and only if ω is closed and $\mathscr{C}(\omega) = \omega$,

(v) $\mathscr{C}(z^{n-1}dz) = 0$ if $\gcd(n, p) = 1$.

It is useful to decompose a differential form $\omega = ydx$ as a sum

$$\omega = df + g^p\frac{dx}{x}, \quad \text{with some elements} \quad f, g \in F.$$

The existence of such a decomposition is obvious since the terms $y_i^p x^i$ with $0 \leq i \leq p-2$ can be integrated. The uniqueness is equally clear. When ω is so written, then it holds:

$$\mathscr{C}(\omega) = g\frac{dx}{x}.$$

We have also the following properties of the Cartier operator:

(vi) If ω is regular at a place of F over k, then $\mathscr{C}(\omega)$ is also regular at this place.

(vii) Let P be a place of F over k, then $\mathrm{res}_P \mathscr{C}\omega = (\mathrm{res}_P \omega)^{1/p}$.

Hence we can define the Cartier operator as below:

Let $\mathcal{C}$ be a curve defined over a perfect field k of characteristic $p > 0$, then there is the operator

$$\mathscr{C} : H^0(\mathcal{C}, \Omega^1) \to H^0(\mathcal{C}, \Omega^1) \tag{2.18}$$

satisfying the above properties.

Proposition 2.50. *The homomorphism $\mathscr{C} : H^0(\mathcal{C}, \Omega^1) \to H^0(\mathcal{C}, \Omega^1)$ is coincident with the dual $\mathscr{F}'$ of $\mathscr{F} : H^1(\mathcal{C}, \mathscr{O}) \to H^1(\mathcal{C}, \mathscr{O})$.*

Proof. From (2.15) it is sufficient to show that if ω is a differential form and α is an adele, one has the equality:

$$< \alpha^p, \omega > = < \alpha, \mathscr{C}\omega >^p .$$

But this equality follows from Property (vii) and Equation (2.17). ■

Definition 2.51. For a basis $\omega_1, \ldots, \omega_g$ of $H^0(\mathcal{C}, \Omega^1)$ we let (a_{ij}) denote the associated matrix of the Cartier operator $\mathscr{C}$; i.e., we have

$$\mathscr{C}(\omega_j) = \sum_{i=1}^{g} a_{ij}\omega_i.$$

The corresponding *Hasse-Witt matrix* $\mathscr{H}$ is obtained by taking $p-$th powers, i.e., we have

$$\mathscr{H} = (a_{ij}^p).$$

Because of $1/p$-linearity, the iterated operator $\mathscr{C}^n$ is represented with respect to the basis $\omega_1, \ldots, \omega_g$ by the product of matrices below:

$$(a_{ij}^{1/p^{n-1}}).\ldots.(a_{ij}^{1/p}).(a_{ij}).$$

By raising the coefficients to p^n-th powers we get the matrix

$$\mathscr{H}^{[n]} = (a_{ij}^p).(a_{ij}^{p^2}).\ldots.(a_{ij}^{p^n}).$$

It is remarkable that if $n \geq g$ then the rank of the matrix $\mathscr{H}^{[n]}$ does not depend on n and it is equal to Hasse-Witt invariant of $\mathcal{C}$.

Remark 2.52. For a given natural number n, one can show:

$$\mathscr{C}^n(x^j dx) = \begin{cases} 0 & \text{if} \quad p^n \nmid j+1 \\ x^{s-1}dx & \text{if} \quad j+1 = p^n s. \end{cases}$$

2.3.4 Hasse-Witt Invariant

Definition 2.53. The *$p-$rank* of an abelian variety $\mathcal{A}/k$ is denoted by $\sigma(\mathcal{A})$; it means that there are exactly $\sigma(\mathcal{A})$ copies of $\mathbb{Z}/p\mathbb{Z}$ in the group of points of order p in $\mathcal{A}(\bar{k})$. The $p-$rank $\sigma(\mathcal{C})$ of a curve $\mathcal{C}/k$ is the $p-$rank of its Jacobian. We call it also the *Hasse-Witt invariant* of the curve.

If we have the $L-$polynomial of a curve $\mathcal{C}$, we can use the following result to determine its Hasse-Witt invariant (see [44, Satz1]):

Proposition 2.54. *Let $\mathcal{C}$ be a curve defined over a finite field $k = \mathbb{F}_q$. If we have*

$L(t) = 1 + a_1 t + \ldots + a_{2g-1} t^{2g-1} + q^g t^{2g}$, *then*

$$\sigma(\mathcal{C}) = max\ \{i \mid a_i \not\equiv 0 (mod\ p)\}.$$

Remark 2.55. From Theorem 2.31 we know that $a_{2g-i} = q^{g-i} a_i$, for $0 \leq i \leq g$. Hence according to the above proposition, we have $0 \leq \sigma(\mathcal{C}) \leq g$.

Let $\mathcal{C}$ be a curve defined over the field k. The set $\mathcal{D}^0(\mathcal{C}) := \{A \in \mathcal{D}(\mathcal{C}) | \deg A = 0\}$ which is obviously a subgroup of the divisor group $\mathcal{D}(\mathcal{C})$, is called the group of divisors of degree zero, and

$$\mathcal{C}\ell^0(\mathcal{C}) := \{[A] \in \mathcal{C}\ell(\mathcal{C}) | \deg [A] = 0\}$$

is the group of divisor classes of degree zero. Let G_p denotes the subgroup of elements $d \in \mathcal{C}\ell^0(\mathcal{C})$, such that $pd = 0$. As before we denote by F the field of $k-$rational functions on the curve $\mathcal{C}$.

Proposition 2.56 ([40])**.** *The group G_p is canonically isomorphic to the additive group of differential forms of $H^0(\mathcal{C}, \Omega^1)$ such that $\mathscr{C}\omega = \omega$.*

Proof. We define the morphism $\theta : G_p \to H^0(\mathcal{C}, \Omega^1)$ as follows: consider $d \in G_p$, and a divisor D that represents d; there is a function $f \neq 0$ such that $pD = div(f)$. We define $\theta(d) = df/f$. First we show that θ is well-defined. In fact if $d = \overline{D} = \overline{D + div(g)}$ for some function $g \neq 0$, then $pD + pdiv(g) = div(fg^p)$. But $d(fg^p)/fg^p = df/f = \theta(d)$. On the other hand, if $P \in \mathcal{C}$ then $f = t^p u$ where $t \in F$ and u is a unit in $\mathcal{O}_P$. Thus $df/f = du/u$ and this means df/f does not have a pole at P. Hence $\theta(d)$ is a holomorphic form. As $\mathscr{C}(df/f) = df/f$, we need only to show that θ is surjective. Suppose $\omega = df/f$. Since $\omega \in H^0(\mathcal{C}, \Omega^1)$ is holomorphic, the order of the function $f \in F$ at any point $P \in \mathcal{C}$ is divisible by p. Hence $div(f) = pD$ and so $\theta(d = \bar{D}) = \omega$. This complete the proof. ■

Applying the above proposition to the Cartier operator on Ω_{reg}, we get the fol-

lowing decomposition for the vector space $\Omega_{\text{reg}} = H^0(\mathcal{C}, \Omega^1)$:

$$\Omega_{\text{reg}} = \Omega^s_{\text{reg}} \oplus \Omega^\sigma_{\text{reg}}$$

where

(i) $\Omega^s_{\text{reg}} = k -$ space of logarithmic differentials,

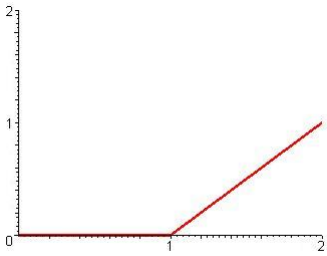
(ii) The p-rank of $\mathcal{C}$ is dim Ω^s_{reg} .

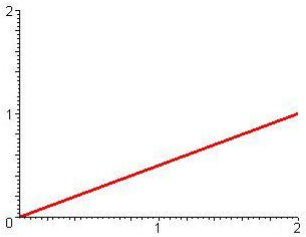
2.3.5 p-adic Newton Polygon

Let $P(t) = \sum a_i t^{d-i} \in \mathbb{Q}_p[t]$ be a monic polynomial of degree d. We are interested in the p-adic values of its zeros (in an algebraic closure of $\mathbb{Q}_p$). These can be computed by the (p-adic) Newton polygon of this polynomial.
The *Newton polygon* is defined as the lower convex hull of the points $(i, v_q(a_i))$, $i = 0, \ldots, d$, where v_q is the p-adic valuation normalized so that $v_q(q) = 1$.

Let $\mathcal{A}$ be an abelian variety over $\mathbb{F}_q$, then the geometric Frobenius $\mathscr{F}_\mathcal{A} \in End(\mathcal{A})$ has a characteristic polynomial $f_\mathcal{A}(t) = \sum b_i t^{2g-i} \in \mathbb{Z}[t] \subset \mathbb{Q}_p[t]$. By definition the *Newton polygon* of $\mathcal{A}$ is the Newton polygon of $f_\mathcal{A}(t)$. Note that $(0, v_q(b_0)) = (0, 0)$ because the polynomial is monic, and $(2g, v_q(b_{2g})) = (2g, g)$ because $b_{2g} = q^g$. Moreover for the slope λ of every side of this polygon we have $0 \leq \lambda \leq 1$. In fact ordinary abelian varieties are characterized by the fact that the Newton polygon has g slopes equal to 0, and g slopes equal to 1. Supersingular abelian varieties turn out to be characterized by the fact that all $2g$ slopes are equal to $\frac{1}{2}$. The $p-$rank is exactly equal to the length of the slope zero segment of its Newton polygon.

Example 2.57. Let $\mathcal{C}$ be an elliptic curve over $\mathbb{F}_q$. There are only two possibilities for the Newton polygon of $\mathcal{C}$ as illustrated in the following pictures:





The first case occurs if and only if $\mathcal{C}$ is an ordinary elliptic curve, and the second one is the Newton polygon of supersingular elliptic curves.

Remark 2.58. In the case of curves, over finite fields, from Corollary 2.40 we know that if $L(t)$ is the numerator of the zeta function associated to the curve, then $f(t) = t^{2g}L(t^{-1})$ is the characteristic polynomial of the Frobenius action on the Jacobian of the curve. The Newton polygon of the curve is by definition the *Newton polygon* of the polynomial $f(t)$. In fact if the curve $\mathcal{C}$ is defined over $\mathbb{F}_q$, $q = p^v$ for some integer v, and the $L-$polynomial is given by $L(t) = 1 + \sum_{l=1}^{2g} a_l t^l \in 1 + t\mathbb{Z}[t]$, consider the sequence of points in $\mathbb{R}^2$ (If $b_i = 0$, define $\mathrm{ord}_p b_i = \infty$):

$$(0,0), (1, \frac{\mathrm{ord}_p a_1}{v}), (2, \frac{\mathrm{ord}_p a_2}{v}), \ldots, (2g, \frac{\mathrm{ord}_p a_{2g}}{v}),$$

where ord_p denotes the $p-$adic valuation. The normalized p-adic Newton polygon is defined to be the lower convex hull of this sequence of points.

Now we can easily show that the following corollary holds, where we use the notation of Remark 2.58.

Corollary 2.59. *If the curve $\mathcal{C}$ is maximal, then all slopes of the Newton polygon of $\mathcal{C}$ are equal to* $1/2$. *In particular, its Hasse-Witt invariant is zero.*

Proof. Write $f(t) = \sum_{i=0}^{2g} b_i t^{2g-i}$. We have from Corollary 2.44 that $f(t) = (t+\sqrt{q})^{2g}$ and hence $b_i = \binom{2g}{i}(\sqrt{q})^i$. Thus $v_q(b_i) = v_q(\binom{2g}{i}) + \frac{i}{2} \geqslant \frac{i}{2}$, and this shows that all points $(i, v_q(b_i))$ are above or on the line $y = \frac{x}{2}$. Note that $b_{2g} = q^g$ and so

$(2g, v_q(b_{2g})) = (2g, g)$ lies on the line $y = \frac{x}{2}$. ■

Definition 2.60. Let $\mathcal{C}$ be a curve of genus g defined over a field k of characteristic $p > 0$. The curve $\mathcal{C}$ is called *supersingular* if and only if its Newton polygon is maximal, i.e., all the slopes are equal to 1/2. The curve $\mathcal{C}$ is called *ordinary* if and only if its Newton polygon has g slopes equal to zero.

Here we can characterize all curves with maximal Newton polygon defined over a finite field k as below:

Theorem 2.61 ([45], Proposition 1)**.** *Let $\mathcal{C}$ be a curve defined over a finite field k. Then $\mathcal{C}$ is supersingular if and only if $\mathcal{C}$ is minimal over some extension of k.*

Proof. Set $q = \#k$. Suppose $L(t) = 1+a_1t+\ldots+a_{2g-1}t^{2g-1}+q^gt^{2g} = \prod_{i=1}^{2g}(1-\alpha_i t)$. If $\mathcal{C}$ is minimal over $k_n = \mathbb{F}_{q^n}$, then $\alpha_i^n = q^{n/2}$ for $i = 1, 2, ..., 2g$. Hence the characteristic polynomial $h_n(t)$ of the Frobenius relative to k_n is given by $h_n(t) = (t - q^{n/2})^{2g}$. The same arguments show that $\mathcal{C}$ is maximal over k_n if and only if $h_n(t) = (t + q^{n/2})^{2g}$. Therefore all roots of $L(t/\sqrt{q})$ are roots of unity if and only if $\mathcal{C}$ is minimal over some extension k_n. Now we must show that all roots of $L(t/\sqrt{q})$ are roots of unity if and only if it holds for $i = 0, 1, \ldots, 2g$ that

$$\mathrm{ord}_p(a_i) \geq \frac{i}{2}\mathrm{ord}_p(q),$$

where p is the characteristic of k.

"Only if" part: Let $\Omega = \mathbb{Q}(\alpha_1, \ldots, \alpha_{2g})$ and $\mathbf{p}$ be a prime above p in Ω. There exists a positive integer m such that $\alpha_i^m = q^{m/2}$ for $i = 1, \ldots, 2g$, hence $m\upsilon_{\mathbf{p}}(\alpha_i) = \upsilon_{\mathbf{p}}(q^{m/2}) = \frac{m}{2}e(\mathbf{p}|p)\mathrm{ord}_p(q)$, i.e., $\upsilon_{\mathbf{p}}(\alpha_i) = e(\mathbf{p}|p)\mathrm{ord}_p(q)/2$. Therefore

$$\mathrm{ord}_p(a_i) = \frac{1}{e(\mathbf{p}|p)}\upsilon_{\mathbf{p}}(\sum(-1)^i\alpha_{j_1}\ldots\alpha_{j_i}) \geq \frac{i}{2}\mathrm{ord}_p(q).$$

"if" part: (i) If q is a square; i.e., if $\sqrt{q} \in \mathbb{N}$ then we have that the polynomial

$$L(\frac{t}{\sqrt{q}}) = 1 + \sum_{i=1}^{2g-1} \frac{a_i}{(\sqrt{q})^i} t^i + t^{2g}$$

has integer coefficients $a_i/(\sqrt{q})^i \in \mathbb{Z}$; in fact this follows from the hypothesis

$$ord_p(a_i) \geq \frac{i}{2} ord_p(q).$$

The roots of $L(t/\sqrt{q})$ are exactly the elements $\sqrt{q}/\alpha_i$ for $i = 1, 2, \ldots, 2g$; hence the elements $\sqrt{q}/\alpha_i$ are algebraic integers with all conjugates having norm one. It now follows from [51, Lemma 1.6] that all roots of $L(t/\sqrt{q})$ are roots of unity.

(ii) If q is not a square, we consider the polynomial $L_2(t)$ which is the $L-$polynomial of the curve $\mathcal{C}$ considered over $\mathbb{F}_{q^2}$:

$$L_2(t) = \prod_{i=1}^{2g} (1 - \alpha_i^2 t) := 1 + b_1 t + \ldots + b_{2g-1} t^{2g-1} + q^{2g} t^{2g}.$$

Since b_j is a symmetric function on $\alpha_1, \ldots, \alpha_{2g}$ of degree $2j$ we have that b_j is a polynomial in $a_1, \ldots, a_{2j}$ of the form

$$b_j = \sum c_{i_1 \ldots i_r} a_{i_1}^{e_1} \ldots a_{i_r}^{e_r}$$

where $c_{i_1 \ldots i_r} \in \mathbb{Z}$, and $\sum_{\ell=1}^{r} e_\ell i_\ell = 2j$. Hence

$$\text{ord}_p(b_j) \geq \min\{\text{ord}_p(a_{i_1}^{e_1} \ldots a_{i_r}^{e_r})\} \geq \sum_{\ell=1}^{r} e_\ell (\frac{i_\ell}{2} \text{ord}_p(q)) = \frac{j}{2} \text{ord}_p(q^2).$$

From (i) it follows that all roots of $L_2(t/q)$ are roots of unity. These roots are the elements $(\sqrt{q}/\alpha_i)^2$ and hence we have that $\sqrt{q}/\alpha_i$ is a root of unity; i.e., all roots of $L(t/\sqrt{q})$ are roots of unity. ■

2.4 Characters

Let G be a finite abelian group of order $|G|$ with identity element 1_G. A *character* χ of G is a homomorphism from G into the multiplicative group U of complex numbers of absolute value 1. More precisely,

$$\chi : G \to U = \{x \in \mathbb{C} || x| = 1\},$$

$$\chi(g_1 + g_2) = \chi(g_1)\chi(g_2).$$

Let $\hat{G}$ denote the group of characters of the group G. The trivial character is by definition such that $\chi(g) = 1$ for each $g \in G$.

Theorem 2.62 ([34], Theorem 5.4)**.** *(a) If χ is a nontrivial character of the finite abelian group G, then*

$$\sum_{g \in G} \chi(g) = 0.$$

(b) If $g \in G$ with $g \neq 1_G$, then

$$\sum_{\chi \in \hat{G}} \chi(g) = 0.$$

Corollary 2.63. *The number of characters of a finite abelian group G is equal to $|G|$.*

Proof. This follows from

$$|\hat{G}| = \sum_{g \in G} \sum_{\chi \in \hat{G}} \chi(g) = \sum_{\chi \in \hat{G}} \sum_{g \in G} \chi(g) = |G|. \ \blacksquare$$

In a finite field $\mathbb{F}_q$ there are two finite abelian groups that are of significance; namely, the additive group and the multiplicative group of the field. Therefore we will have to make an important distinction between the characters pertaining to these two group structures:

(a) Let $G = (\mathbb{F}_q, +)$. Let p be the characteristic of $\mathbb{F}_q$. Let $Tr : \mathbb{F}_q \to \mathbb{F}_p$ be the trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$. Then the function χ_1 defined by

$$\chi_1(c) = e^{2\pi i Tr(c)/p} \text{ for all } c \in \mathbb{F}_q$$

is a character of the additive group of $\mathbb{F}_q$. The character χ_1 will be called the *canonical additive character* of $\mathbb{F}_q$.

Theorem 2.64 ([34], Theorem 5.7)**.** *For $b \in \mathbb{F}_q$, the function χ_b defined by $\chi_b(c) = \chi_1(bc)$ for all $c \in \mathbb{F}_q$ is an additive character of $\mathbb{F}_q$, and every additive character of $\mathbb{F}_q$ is obtained in this way.*

(b) Let $G = (\mathbb{F}_q^*, \times)$. Since G is a cyclic group of order $q-1$, its characters can be easily determined. Let g be a generator of G, and for a fixed integer j, with $0 \leq j \leq q-2$, the function

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

defines a character of G. On the other hand, if χ is any character of G, then $\chi(g)$ must be a $(q-1)-$th root of unity, say $\chi(g) = e^{2\pi ij/(q-1)}$ for some $0 \leq j \leq q-2$, and it follows that $\chi = \chi_j$. Therefore, $\hat{G}$ consists exactly of the characters $\chi_0, \ldots, \chi_{(q-2)}$.

Definition 2.65. Let ψ be a multiplicative and χ an additive character of $\mathbb{F}_q$. Then the *Gauss sum* $G(\psi, \chi)$ is defined by

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

The absolute value of $G(\psi, \chi)$ can obviously be at most $q-1$, but it is in general much smaller (see [34, Theorem 5.11]). In Section 3.1 we explain how the zeta function of Artin-Schreier curves over $\mathbb{F}_q$ is connected with the Gauss sum $G(\psi, \chi)$.

Definition 2.66. Let λ_1, λ_2 be two multiplicative characters of $\mathbb{F}_q$. Then the sum

$$J(\lambda_1, \lambda_2) = \sum_{c \in \mathbb{F}_q^*} \lambda_1(c)\lambda_2(1-c),$$

is called a *Jacobi sum* in $\mathbb{F}_q$.

Just as Artin-Schreier curves are connected with Gauss sums, the Fermat curves are connected with Jacobi sums (see Section (4.2.1)).

Let ψ_1, ψ_2 be two nontrivial multiplicative characters of $\mathbb{F}_q$, and χ be a not trivial additive character of $\mathbb{F}_q$. Then if $\psi_1\psi_2$ is nontrivial, the Gauss and Jacobi sums are related by the following equation:

$$J(\psi_1, \psi_2) = \frac{G(\psi_1, \chi)\ G(\psi_2, \chi)}{G(\psi_1\ \psi_2, \chi)}$$

The statements of Theorem 2.62 and Corollary 2.63 can be combined into the *orthogonality relations for characters*. Let χ and ψ be characters of a finite abelian group G. Then

$$\frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\psi(g)} = \begin{cases} 0 & \text{for} \quad \chi \neq \psi \\ 1 & \text{for} \quad \chi = \psi, \end{cases}$$

where $\overline{\psi(g)}$ denotes complex conjugation.

Furthermore, if g and h are elements of G, then

$$\frac{1}{|G|} \sum_{\chi \in \hat{G}} \chi(g)\overline{\chi(h)} = \begin{cases} 0 & \text{for} \quad g \neq h \\ 1 & \text{for} \quad g = h. \end{cases}$$

Character theory is often used to obtain expressions for the number of solutions of equations in a finite abelian group G.

Corollary 2.67. *Let f be an arbitrary map from G into G. Then for a fixed $h \in G$,*

the number $N(h)$ of elements $g \in G$ with $f(g) = h$ is given by

$$N(h) = \frac{1}{|G|} \sum_{g \in G} \sum_{\chi \in \hat{G}} \chi(f(g)) \overline{\chi(h)}.$$

We end this section with a deep result of Weil that is crucial for us.

Theorem 2.68 ([34], Theorem 5.38)**.** *Let $f \in \mathbb{F}_q[X]$ be a polynomial of degree $n \geq 1$ with $gcd(n, q) = 1$ and let χ be a nontrivial additive character of $\mathbb{F}_q$. Then*

$$|\sum_{c \in \mathbb{F}_q} \chi(f(c))| \leq (n-1)q^{1/2}.$$

Chapter 3

Additive Polynomials and Certain Maximal Curves

In this section we show that a maximal curve over $\mathbb{F}_{q^2}$ given by an equation $A(x) = F(y)$, where $A(x) \in \mathbb{F}_{q^2}[x]$ is additive and separable and where $F(y) \in \mathbb{F}_{q^2}[y]$ has degree m prime to the characteristic p, is such that all roots of $A(x)$ belong to $\mathbb{F}_{q^2}$. In the particular case where $F(y) = y^m$, we show that the degree m is a divisor of $q+1$.

We start by giving the definition of p-cyclic extensions of $\mathbb{P}^1$. Using the Newton polygon of Artin-Schreier curves, we characterize maximal curves given by the equation $x^p - x = \alpha y^m$ over $\mathbb{F}_{q^2}$ with $\gcd(m,p) = 1$, and we show that they have the following form:

$$x^p + x = y^m \qquad \text{where } m \mid q+1. \tag{3.1}$$

Then we study the additive polynomials, and using orthogonality relations for characters we generalize this result for any additive and separable polynomial $A(x)$ instead of $x^p - x$.

3.1 p-Cyclic Extensions of $\mathbb{P}^1$

Let k be an algebraically closed field of characteristic $p > 0$. If F is any field of characteristic $p \neq 0$, a cyclic extension of degree p is of the form $L = F(x)$ where $x^p - x = g(y)$ for some $g(y) \in F$. Moreover we can assume that $g(y)$ satisfies the following conditions:

$$g(y) = \frac{g_1(y)}{(y-\alpha_1)^{e_1} \dots (y-\alpha_n)^{e_n}}$$

where

(1) $g_1(y)$ is a polynomial in $k[y]$.

(2) e_i' s are positive integers prime to p.

(3) $\alpha_i \neq \alpha_j$ and $g_1(\alpha_i) \neq 0$ for $i = 1, \dots, n$.

(4) deg $g_1(y) - (e_1 + \dots + e_n)$ is a positive integer relatively prime to p.

Let $\pi : \mathcal{C} \to \mathcal{D}$ be a $p-$cyclic covering of complete non-singular curves over k. Then the Deuring-Shafarevich formula gives a the following relation between the Hasse-Witt invariants of $\mathcal{C}$ and $\mathcal{D}$:

$$\sigma(\mathcal{C}) - 1 + r = p(\sigma(\mathcal{D}) - 1 + r),$$

where r is the number of the ramification points with respect to π.

Here we consider p-cyclic extension of the rational function field $k(y)$. Let $\mathcal{C}$ be a projective geometrically irreducible non-singular curve defined over a finite field such that

$$\mathcal{C} \to \mathbb{P}^1$$

is a cyclic covering of degree p. If $\sigma(\mathcal{C}) = 0$, then in the Deuring-Shafarevich formula we must have $r = 1$ and so we can put this unique ramification point in infinity. This

implies that for the curve $\mathcal{C}$ with $\sigma(\mathcal{C}) = 0$ we can assume $g(y)$ is a polynomial (see also Remark 4.27).

When $g(y)$ is a monomial we have the classical Artin-Schreier curve $\mathcal{C}$ that given by

$$x^p - x = y^m \quad \gcd(m, p) = 1. \tag{3.2}$$

In this case, over a finite field of characteristic p containing μ_m, the set of m-th roots of unity, the curve $\mathcal{C}$ has two types of automorphism:

$$y \mapsto \xi y,\ x \mapsto x \qquad \text{with } \xi \in \mu_m \tag{3.3}$$

and

$$y \mapsto y,\ x \mapsto x + \alpha \qquad \text{with } \alpha \in \mathbb{F}_p. \tag{3.4}$$

We shall see that the first type corresponds to the multiplicative character ψ and the second type to the additive character χ in the Gauss sum. Set $\hat{G} := \hat{\mu}_m \times \hat{\mathbb{F}}_p$ and

$$S := \{(\psi, \chi) \in \hat{G} | \psi \neq 1, \chi \neq 1\}.$$

Then the nominator of the zeta function of the curve $\mathcal{C}$ over a field $\mathbb{F}_l$, where l is a power of p and $l \equiv 1 \pmod{m}$, is equal to

$$L_{\mathcal{C}}(t) = \Pi_{(\psi,\chi)\in S}(1 + G(\psi, \chi \circ tr)t), \tag{3.5}$$

where tr denotes the trace function over $\mathbb{F}_l$ to $\mathbb{F}_p$ (see [8]).

Remark 3.1. Consider the Artin-Schreier curve $\mathcal{C}$ given by $x^p - x = y^m$, where $\gcd(m, p) = 1$ and $d \geq 3$. From Remark 1.4 of [57] we can describe the Newton polygon of $\mathcal{C}$ as below:

Let σ be the permutation in the symmetric group S_{m-1} such that for every $1 \leq$

$n \leq m-1$ we set $\sigma(n)$ the least positive residue of pn mod m. Write σ as a product of disjoint cycles (including 1-cycles). For a cycle $\tau = (a_1 a_2 \dots a_t)$ in S_{m-1} we define $N(\tau) := a_1 + a_2 + \ldots + a_t$. Let σ_i be a l_i-cycle in σ. Let $\lambda_i := N(\sigma_i)/(ml_i)$. Arrange σ_i in an order such that $\lambda_1 \leq \lambda_2 \leq \ldots$. For every cycle σ_i in σ let the pair $(\lambda_i, l_i(p-1))$ represent the line segment of (horizontal) length $l_i(p-1)$ and of slope λ_i. The joint of the line segments $(\lambda_i, l_i(p-1))$ is the lower convex hull consisting of the line segments $(\lambda_i, l_i(p-1))$ connected at their endpoints, and this is the Newton polygon of the curve $\mathcal{C}$. Note that this Newton polygon only depends on the residue class of p mod m. For example if $p \equiv 1 \pmod{m}$, then σ is the identity of S_{m-1} and so it is a product of 1-cycles. We then get the Newton polygon from the following line segments:

$$(\frac{1}{m}, p-1), (\frac{2}{m}, p-1), \ldots, (\frac{m-1}{m}, p-1).$$

Here we want to give a characterization for maximal Artin-Schreier curve defined over a finite field. We begin with a simple lemma:

Lemma 3.2. *If the curve $\mathcal{C}$ given by $x^p - x = ay^m + b \in \mathbb{F}_{q^2}$ is maximal over $k = \mathbb{F}_{q^2}$, then we must have that m is a divisor of $q^2 - 1$.*

Proof. Let d denote the $gcd(m, q^2-1)$. The curve $\mathcal{C}_1$ given by $x^p - x = az^d + b$ is also maximal since it is covered by the curve $\mathcal{C}$ (indeed, just set $z = y^{\frac{m}{d}}$). We also have that $\{\alpha \in \mathbb{F}_{q^2} \mid \alpha \text{ is } m\text{-th power }\} = \{\alpha \in \mathbb{F}_{q^2} \mid \alpha \text{ is } d\text{-th power }\}$ and hence $\#\mathcal{C}(\mathbb{F}_{q^2}) = \#\mathcal{C}_1(\mathbb{F}_{q^2})$. Therefore $g(\mathcal{C}) = g(\mathcal{C}_1)$ and we then conclude from Equation (1.4) that $d = m$. ■

Lemma 3.3. *Let β be an element of $\mathbb{F}_{q^2}^*$. If the curve $\mathcal{C}$ given by $x^p - x = \beta y^m$ is maximal over $\mathbb{F}_{q^2}$ and $gcd(m, q+1) = 1$, then m divides $(p-1)$.*

Proof. Since m divides $q^2 - 1$ by Lemma 3.2 and $\gcd(m, q+1) = 1$, then m is a divisor of $q - 1$. We denote by Tr the trace from $\mathbb{F}_{q^2}$ to $\mathbb{F}_p$. By Hilbert 90 Theorem,

we know

$$\#\mathcal{C}(\mathbb{F}_{q^2}) = 1 + p + mpB, \tag{3.6}$$

where $B := \#\{\alpha \in H \mid Tr(\beta\alpha) = 0\}$ and H denotes the subgroup of $\mathbb{F}_{q^2}^*$ with $(q^2-1)/m$ elements. In fact, $\mathcal{C}$ has one infinite point, p points which correspond to $y = 0$ and some mpB other points. The existence of the latter points follows from Hilbert 90 Theorem. Since the genus of this curve is $g(\mathcal{C}) = (m-1)(p-1)/2$ and the curve $\mathcal{C}$ is maximal, then

$$\#\mathcal{C}(\mathbb{F}_{q^2}) = 1 + q^2 + (p-1)(m-1)q. \tag{3.7}$$

Comparing (3.6) and (3.7) gives

$$1 + q^2 + (p-1)(m-1)q = 1 + p + mpB.$$

Hence

$$(q^2 - p) + (p-1)(m-1)q = mpB$$

or $(q^2/p - 1) + (1-p)q/p + m(p-1)q/p = mB$. Thus m divides $(q/p - 1)(q+1)$. On the other hand we have $\gcd(m, q+1) = 1$. Therefore m divides $(q-p)$, and the result follows from the fact that m is a divisor of $q-1$. ■

Remark 3.4. In Lemma 3.3, if the characteristic $p = 2$ then $m = p - 1 = 1$. The curve $\mathcal{C}$ is rational in this case. If $p = 3$ in Lemma 3.3, then again $m = 1$. The other possibility, $m = p - 1 = 2$ is discarded since we have $\gcd(m, q+1) = 1$.

Proposition 3.5. *Suppose that $m > 2$ is such that the characteristic p does not divide m and $gcd(m, q+1) = 1$. Then there is no maximal curve of the form $x^p - x = ay^m$ over $\mathbb{F}_{q^2}$, for any $a \in \mathbb{F}_{q^2}$.*

Proof. If there is some maximal curve of this form, according to Lemma 3.3 m must divide $p-1$. Now by using Remark 3.1, we know that the Newton polygon of $\mathcal{C}_1$ has

slopes $1/m, 2/m, \ldots, (m-1)/m$. Therefore Corollary 2.59 implies that this curve is not maximal. ■

Theorem 3.6. *Let $\mathcal{C}$ be a curve defined over $\mathbb{F}_{q^2}$ given by the equation*

$$x^p - x = ay^m,$$

where $gcd(m, p) = 1$. If $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$, then m is a divisor of $q + 1$.

We consider two cases:

Case $p = 2$. In this case $\gcd(q+1, q-1) = 1$, and we know that m divides $q^2 - 1$ by Lemma 3.2. From Remark 2.47 we have that $x^p - x = ay^d$ is also maximal for any prime divisor d of m. It now follows from Proposition 3.5 that this prime number d is a divisor of $q + 1$. Since $\gcd(q + 1, q - 1) = 1$, we conclude that m divides $q + 1$.

Case $p = odd$. In this case $\gcd(q + 1, q - 1) = 2$. Reasoning as in the case $p = 2$, we get here that if d is an odd prime divisor of m then d is a divisor of $q+1$. The only situation still to be investigated is the following: $q + 1 = 2^r s$ with s an odd integer and $m = 2^{r_1} s_1$ with $r_1 > r$ and s_1 is a divisor of s. But according to Remark 2.47 and the following lemma this case does not occur.

Lemma 3.7. *Assume that the characteristic p is odd and write $q + 1 = 2^r.s$ with s an odd integer. Denote by $m := 2^{r+1}$. Then there is no maximal curve over $\mathbb{F}_{q^2}$ of the form $x^p - x = \beta y^m$ with $\beta \in \mathbb{F}_{q^2}^*$.*

Proof. Writing $q = p^n$ we consider two cases:

Case n is even. Clearly in this case we have $q + 1 = 2s$ with s an odd integer. So we must show that there is no maximal curve $\mathcal{C}$ of the form $x^p - x = \beta y^4$. We denote by Tr the trace from $\mathbb{F}_{q^2}$ to $\mathbb{F}_p$. By Hilbert 90 Theorem, we know

$$\#\mathcal{C}(\mathbb{F}_{q^2}) = 1 + p + 4pB, \tag{3.8}$$

where $B := \#S$, with $S := \{\alpha \in H \mid Tr(\beta\alpha) = 0\}$ and H denotes the subgroup of $\mathbb{F}_{q^2}^*$ with $(q^2-1)/4$ elements. Since the genus of this curve is $g(\mathcal{C}) = 3(p-1)/2$ and the curve $\mathcal{C}$ is maximal, then

$$\#\mathcal{C}(\mathbb{F}_{q^2}) = 1 + q^2 + 3(p-1)q. \tag{3.9}$$

Comparing (3.8) and (3.9) gives

$$1 + q^2 + 3(p-1)q = 1 + p + 4pB.$$

Hence

$$B = \frac{q/p-1}{2}.\frac{q+1}{2} + \frac{q}{p}(p-1). \tag{3.10}$$

On the other hand, we have $\mathbb{F}_p^* \subset H$ since $(p-1)$ divides $(q^2-1)/4$. In fact since n is even we have that $p-1$ divides $(q-1)/2$. Therefore the multiplication by each element of $\mathbb{F}_p^*$ defines a map on S. This implies that $p-1$ is a divisor of B and so from Equation (3.10) we obtain that $p-1$ divides $(q/p-1)/2$. But this is impossible because n is even.

Case n is odd. We know the Newton polygon of a maximal curve over $\mathbb{F}_{q^2}$ is maximal, i.e., all slopes are $1/2$. Hence it is sufficient to show that the Newton polygon of the curve $\mathcal{C}$ is not maximal. As n is an odd number, the hypothesis $q+1 = 2^r.s$ implies $p+1 = 2^r.s_1$ with s_1 an odd integer. Hence $p \equiv 2^r - 1 \pmod{2^{r+1}}$ and $p(2^r-1) \equiv 1 \pmod{2^{r+1}}$. Now if we set $\theta := 2^r - 1$, with the notation of Remark 3.1, the permutation σ has the 2-cycle (1θ) in its standard representation with disjoint cycles. This 2-cycle (1θ) corresponds to the slope $\lambda = (\theta+1)/(2.2^{r+1}) = 1/4$ and this finishes the proof. ■■

3.2 Additive Polynomials

Let k be a perfect field of characteristic $p > 0$ (e.g. $k = \mathbb{F}_q$) and let $\bar{k}$ be the algebraic closure of k. Let $A(x)$ be an additive and separable polynomial in $k[x]$:

$$A(x) = \sum_{i=0}^{n} a_i x^{p^i} \quad \text{where} \quad a_0 a_n \neq 0.$$

Consider the equation

$$A(x) = 0. \tag{3.11}$$

We know that the roots of Equation (3.11) form a vector space of dimension n over $\mathbb{F}_p$. Hence there exists a basis

$$\omega_1, \omega_2, \ldots, \omega_n$$

for $\mathcal{M}_A := \{\omega \in \bar{k} | A(\omega) = 0\}$. Every root is uniquely representable in the form

$$\omega = k_1\omega_1 + \ldots + k_n\omega_n \qquad \text{where} \quad k_i \quad \text{belongs to} \quad \mathbb{F}_p.$$

On the other hand given a $\mathbb{F}_p-$space $\mathcal{M}$ of dimension n, with $\mathcal{M} \subseteq \bar{k}$, we can associate a monic additive polynomial $A(x) \in \bar{k}[x]$ of degree p^n having the elements of $\mathcal{M}$ for roots.

Let $\omega_1, \omega_2, \ldots, \omega_n$ be a basis for $\mathcal{M}$. Let $A_t(x)$ $(1 \leq t \leq n)$ be the monic additive and separable polynomial in $\bar{k}[x]$ having the roots ω below:

$$\omega = k_1\omega_1 + \ldots + k_t\omega_t \qquad \text{where} \quad k_i \quad \text{belongs to} \quad \mathbb{F}_p.$$

Then we have the following description of the monic additive polynomial $A_t(x)$

$$A_t(x) = \frac{\Delta(\omega_1, \omega_2, \ldots, \omega_t, x)}{\Delta(\omega_1, \omega_2, \ldots, \omega_t)},$$

where

$$\Delta(\omega_1, \omega_2, \ldots, \omega_t) = det \begin{vmatrix} \omega_1 & \omega_2 & \ldots & \omega_t \\ \omega_1^p & \omega_2^p & \ldots & \omega_t^p \\ \vdots & \ldots & \ldots & \vdots \\ \omega_1^{p^{t-1}} & \omega_2^{p^{t-1}} & \ldots & \omega_t^{p^{t-1}} \end{vmatrix}$$

and

$$\Delta(\omega_1, \omega_2, \ldots, \omega_t, x) = det \begin{vmatrix} \omega_1 & \omega_2 & \ldots & \omega_t & x \\ \omega_1^p & \omega_2^p & \ldots & \omega_t^p & x^p \\ \vdots & \ldots & \ldots & \vdots & \vdots \\ \omega_1^{p^t} & \omega_2^{p^t} & \ldots & \omega_t^{p^t} & x^{p^t} \end{vmatrix}.$$

Hence

$$A_t(x) = A_{t-1}(X)A_{t-1}(x - \omega_t) \ldots A_{t-1}(x - (p-1)\omega_t). \tag{3.12}$$

Let $G(x)$ be a polynomial in $k[x]$. If there exist polynomials $g(x)$ and $h(x)$ in $k[x]$ such that $G(x) = g(h(x))$, then we say that $G(x)$ is left divisible by $g(x)$.

The following lemma is crucial for us (see [38, Equation 11]):

Lemma 3.8. *Let $A(x) = \sum_{i=0}^{n} a_i x^{p^i}$ be an additive and separable polynomial. Then $A(x)$ is left divisible by $x^p - \alpha x$ if and only if α is a root of the equation*

$$a_n^{1/p^n} y^{(p^n-1)/((p-1)p^{n-1})} + a_{n-1}^{1/p^{n-1}} y^{(p^{n-1}-1)/((p-1)p^{n-2})} + \ldots + a_1^{1/p} y + a_0 = 0. \tag{3.13}$$

Definition. We say that an additive and separable polynomial $A(x) = \sum_{i=0}^{n} a_i x^{p^i}$ has $(*)-$property if its coefficients satisfy the following equality:

$$a_n + a_{n-1}^p + a_{n-2}^{p^2} + ... + a_0^{p^n} = 0. \tag{3.14}$$

Corollary 3.9. *If the polynomial* $A(x) = \sum_{i=0}^{n} a_i x^{p^i}$ *has* $(*)-$*property, then* $A(x)$ *is left divisible by* $a(x) = x^p - x$.

Proof. The result follows from Lemma 3.8 with $\alpha = 1$. ■

Definition. For the additive and separable polynomial

$$A(x) = a_n x^{p^n} + a_{n-1} x^{p^{n-1}} + \ldots + a_1 x^p + a_0 x,$$

we define another additive polynomial $\bar{A}(x)$ as follows

$$\bar{A}(x) = (a_0 x)^{p^n} + (a_1 x)^{p^{n-1}} + \ldots + (a_{n-1} x)^p + a_n x,$$

which is the so-called *adjoint polynomial* of $A(X)$.

Lemma 3.10. *If* $A(x) \in k[x]$ *is a monic additive and separable polynomial and* $\alpha^{-1} \in \bar{k}$ *is a root of the adjoint polynomial* $\bar{A}(x)$*, then* $\alpha^{-1} A(\alpha x)$ *has* $(*)-$*property.*

Proof. Write $A(x)$ as below

$$A(x) = x^{p^n} + a_{n-1} x^{p^{n-1}} + ... + a_1 x^p + a_0 x.$$

Take $\alpha \in \bar{k}$ such that α^{-1} is a root of $\bar{A}(x)$. Clearly, we have

$$\alpha^{-1} A(\alpha x) = \alpha^{p^n - 1} x^{p^n} + a_{n-1} \alpha^{p^{n-1} - 1} x^{p^{n-1}} + ... + a_1 \alpha^{p-1} x^p + a_0 x. \tag{3.15}$$

Now we verify that $\alpha^{-1} A(\alpha x)$ has $(*)-$property. This follows from the choice of α^{-1}

as a root of the adjoint polynomial of $A(x)$. In fact we have

$$\begin{aligned}
&\alpha^{p^n-1} + (a_{n-1}\alpha^{p^{n-1}-1})^p + ... + (a_1\alpha^{p-1})^{p^{n-1}} + (a_0)^{p^n} \\
&= \alpha^{p^n}.(\frac{1}{\alpha} + (\frac{a_{n-1}}{\alpha})^p + ... + (\frac{a_1}{\alpha})^{p^{n-1}} + (\frac{a_0}{\alpha})^{p^n}) \\
&= \alpha^{p^n}.\bar{A}(\alpha^{-1}) = 0. \ \blacksquare
\end{aligned} \tag{3.16}$$

Example 3.11. Consider the Hermitian curve $\mathcal{C}$ over $\mathbb{F}_{q^2}$ given by $x^q + x = y^{q+1}$. Take $\alpha \in \mathbb{F}_{q^2}$ such that $\alpha^q + \alpha = 0$. Changing variable $x_1 := \alpha^{-1}x$ we have that the Hermitian curve can also be given as below:

$$y^{q+1} = (\alpha x_1)^q + (\alpha x_1) = -\alpha(x_1^q - x_1). \tag{3.17}$$

With $A(x) = x^q + x$, we have $\alpha^{-1}A(\alpha x) = -(x_1^q - x_1)$; i.e., the additive polynomial $\alpha^{-1}A(\alpha x)$ has $(*)-$property.

The next lemma will be crucial in the proof of Theorem 3.15.

Lemma 3.12. *With notation as above, we have* $\mathcal{M}_A = \{\omega \in \bar{k} | A(\omega) = 0\} \subset k$ *if and only if* $\mathcal{M}_{\bar{A}} = \{\omega \in \bar{k} | \bar{A}(\omega) = 0\} \subset k$.

Proof. First we show that $\mathcal{M}_A \subset k$ implies $\mathcal{M}_{\bar{A}} \subset k$. Suppose $\omega_1, \omega_2, \ldots, \omega_n$ is a basis for $\mathcal{M}_A$. From the Equation (3.12) with $t = n$, we have

$$A_n(x) = A_{n-1}(x)A_{n-1}(x - \omega_n) \ldots A_{n-1}(x - (p-1)\omega_n).$$

Hence we have

$$A(x) = a_n A_n(x) = a_n(A_{n-1}(x)^p - A_{n-1}(\omega_n)^{p-1}A_{n-1}(x)).$$

If we set $a_n = b^p$ for some $b \in k$, which is possible since k is perfect, then

$$A(x) = (bA_{n-1}(x))^p - (bA_{n-1}(\omega_n))^{p-1}(bA_{n-1}(x)).$$

This shows that $A(x)$ is left divisible by $x^p - (bA_{n-1}(\omega_n))^{p-1}x$. On the other hand, if we define

$$\begin{aligned}
\bar{\omega}_1 :=& (-1)^{n+1}\frac{\Delta(\omega_2, \omega_3, \ldots, \omega_n)}{\Delta(\omega_1, \omega_2, \ldots, \omega_n)} \\
\bar{\omega}_2 :=& (-1)^{n+2}\frac{\Delta(\omega_1, \omega_3, \ldots, \omega_n)}{\Delta(\omega_1, \omega_2, \ldots, \omega_n)} \\
&\vdots \\
\bar{\omega}_n :=& \frac{\Delta(\omega_1, \omega_2, \ldots, \omega_{n-1})}{\Delta(\omega_1, \omega_2, \ldots, \omega_n)},
\end{aligned} \tag{3.18}$$

then we have

$$A_{n-1}(\omega_n) = \frac{\Delta(\omega_1, \omega_2, \ldots, \omega_n)}{\Delta(\omega_1, \omega_2, \ldots, \omega_{n-1})} = \frac{1}{\bar{\omega}_n}.$$

Now according to Lemma 3.8, we can conclude that $\beta := (bA_{n-1}(\omega_n))^{p-1} = (b/\bar{\omega}_n)^{p-1}$ must be a root of Equation (3.13). Thus

$$a_n^{1/p^n}\beta^{(p^n-1)/((p-1)p^{n-1})} + a_{n-1}^{1/p^{n-1}}\beta^{(p^{n-1}-1)/((p-1)p^{n-2})} + \ldots + a_2^{1/p^2}\beta^{(p+1)/p} + a_1^{1/p}\beta + a_0 = 0.$$

Hence if we set $\lambda = b/\bar{\omega}_n$, then

$$a_n(\frac{1}{\lambda^p})^{(1-p^n)} + a_{n-1}^p(\frac{1}{\lambda^p})^{(p-p^n)} + \ldots + a_2^{p^{n-2}}(\frac{1}{\lambda^p})^{(p^{n-2}-p^n)} + a_1^{p^{n-1}}(\frac{1}{\lambda^p})^{(p^{n-1}-p^n)} + a_0^{p^n} = 0.$$

We then conclude that

$$a_n(\frac{1}{\lambda^p}) + a_{n-1}^p(\frac{1}{\lambda^p})^p + \ldots + a_2^{p^{n-2}}(\frac{1}{\lambda^p})^{p^{n-2}} + a_1^{p^{n-1}}(\frac{1}{\lambda^p})^{p^{n-1}} + a_0^{p^n}(\frac{1}{\lambda^p})^{p^n} = 0.$$

This means that $(\bar{\omega}_n/b)^p$ is a root of $\bar{A}(x)$. By changing the order of the basis elements ω_i of $\mathcal{M}_A$, one can deduce in the same way that $A(x)$ is left divisible by

$$x^p - (b/\bar{\omega}_i)^{p-1}x \qquad \text{for} \quad i = 1, 2, \ldots, n.$$

So $(\bar{\omega}_1/b)^p, (\bar{\omega}_2/b)^p, \ldots, (\bar{\omega}_n/b)^p$ are roots of $\bar{A}(x)$, and they form a basis over $\mathbb{F}_p$ for $\mathcal{M}_{\bar{A}}$. Hence we have shown that $\mathcal{M}_A \subset k$ implies $\mathcal{M}_{\bar{A}} \subset k$, since by Equation (3.18) we see that $(\bar{\omega}_1/b), \ldots, (\bar{\omega}_n/b)$ belong to k.

Conversely, consider $\bar{\bar{A}}(x)$ the adjoint polynomial of $\bar{A}(x)$. Then

$$\bar{\bar{A}}(x) = a_n^{p^n} x^{p^n} + a_{n-1}^{p^n} x^{p^{n-1}} + \ldots + a_1^{p^n} x^p + a_0^{p^n} x.$$

Now one can verify that $\omega_1^{p^n}, \omega_2^{p^n}, \ldots, \omega_n^{p^n}$ form a basis for $\mathcal{M}_{\bar{\bar{A}}}$.

Assume $\mathcal{M}_{\bar{A}} \subset k$. Then we have already shown that $\mathcal{M}_{\bar{\bar{A}}} \subset k$. Therefore the elements $\omega_1^{p^n}, \omega_2^{p^n}, \ldots, \omega_n^{p^n}$ belong to k and this shows that $\omega_1, \omega_2, \ldots, \omega_n$ belong to k, since k is a perfect field. It yields $\mathcal{M}_A \subset k$. ■

3.3 Certain Maximal Curves

In this section we consider curves $\mathcal{C}$ over $k = \mathbb{F}_{q^2}$ given by an affine equation

$$A(x) = F(y)$$

where $A(x)$ is an additive and separable polynomial in $\mathbb{F}_{q^2}[x]$ and $F(y)$ is a rational function in $k(y)$ such that every pole of $F(y)$ in $\bar{k}(y)$ occurs with a multiplicity relatively prime to the characteristic p.

We start with a simple lemma:

Lemma 3.13. *With notation and hypotheses as above, if the curve $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$ then $F(y)$ has only one pole which has order $m \leq q+1$.*

Proof. In [48] it was shown that the group of divisor classes of $\mathcal{C}$ of degree zero and order p has rank $\sigma = (\deg A - 1)(r-1)$ where r is the number of distinct poles of $F(y)$ in $\bar{k} \cup \{\infty\}$. Hence $r = 1$, since according to Corollary 2.59 the Hasse-Witt invariant of a maximal curve is zero. By the genus formula we know

$$2g(\mathcal{C}) = (\deg \mathrm{A} - 1)(m-1).$$

Now if $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$, then

$$\#\mathcal{C}(\mathbb{F}_{q^2}) = 1 + q^2 + 2g(\mathcal{C})q.$$

On the other hand one can observe that

$$\#\mathcal{C}(\mathbb{F}_{q^2}) \leq (q^2+1)\deg A.$$

Thus

$$2g(\mathcal{C})q \leq (q^2+1)(\deg A - 1).$$

Using the genus formula we obtain $(m-1)q \leq q^2+1$. Hence $m \leq q+1$. ■

Remark 3.14. Since $F(y)$ is a rational function with coefficients in $\mathbb{F}_{q^2}$ and Lemma 3.13 shows that $F(y)$ has a unique pole $\alpha \in \bar{\mathbb{F}}_q \cup \{\infty\}$, then this pole α lies in $\mathbb{F}_{q^2} \cup \{\infty\}$. If $\alpha \in \mathbb{F}_{q^2}$ then performing the substitution $y \to 1/(y-\alpha)$, we can assume that $F(y)$ is a polynomial in $\mathbb{F}_{q^2}[y]$.

The following theorem is similar to Theorem 1 in [35]:

Theorem 3.15. *Let $\mathcal{C}$ be a curve given by the equation $A(x) = F(y)$, where $A(x) \in \mathbb{F}_{q^2}[x]$ is an additive and separable polynomial and $F(y) \in \mathbb{F}_{q^2}[y]$ is a polynomial of degree m relatively prime to the characteristic p. If the curve $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$, then all roots of $A(x)$ belong to $\mathbb{F}_{q^2}$.*

Proof. Let χ_1 denote the canonical additive character of $k = \mathbb{F}_{q^2}$. Denote by N the number of affine solutions of $A(x) = F(y)$ over $\mathbb{F}_{q^2}$. The orthogonality relations of characters (see Corollary 2.67) imply the equality

$$q^2 N = \sum_{c \in k} (\sum_{y \in k} \chi_1(-cF(y)))(\sum_{x \in k} \chi_1(cA(x))).$$

But we know from Theorem 5.34 in [34] that

$$\sum_{x \in k} \chi_1(cA(x)) = \begin{cases} 0 & \text{if} \quad \bar{A}(c) \neq 0 \\ q^2 & \text{if} \quad \bar{A}(c) = 0. \end{cases}$$

So

$$N = q^2 + \sum_{\substack{c \in k^* \\ \bar{A}(c) = 0}} (\sum_{y \in k} \chi_1(-cF(y))).$$

We note that every affine point on the curve $\mathcal{C}$ over $\mathbb{F}_{q^2}$ is simple and $\mathcal{C}$ has exactly one infinite point. Hence the maximality of $\mathcal{C}$ and Weil's bound Theorem 2.68 imply that $\mathcal{M}_{\bar{A}} = \{c \in \bar{k} \mid \bar{A}(c) = 0\}$ is a subset of $\mathbb{F}_{q^2}$ and also that $\sum_{y \in k} \chi_1(-cF(y)) = (m-1)q$ for any $0 \neq c \in \mathcal{M}_{\bar{A}}$. So the desired result follows now from Lemma 3.12. ■

Remark 3.16. Let $\mathcal{C}$ be a curve over $\mathbb{F}_{q^2}$ given by an affine equation

$$G(x) = F(y)$$

where $G(x)$ and $F(y)$ are polynomials such that $G(x) - F(y) \in \mathbb{F}_{q^2}[x, y]$ is absolutely

irreducible. Suppose that G and F are left divisible by g and f, respectively. Then the curve $\mathcal{C}_1$ given by

$$g(x) = f(y),$$

is covered by the curve $\mathcal{C}$. In fact, write $G(x) = g(h_1(x))$ and $F(y) = f(h_2(y))$ and consider the surjective map from $\mathcal{C}$ to $\mathcal{C}_1$ given by $(x, y) \longmapsto (h_1(x), h_2(y))$.

Let $A(x)$ be an additive and separable polynomial with all roots in $\mathbb{F}_{q^2}$, that is left divisible by an additive polynomial $a(x)$. Then there exists an additive polynomial $u(x)$ such that

$$A(x) = a(u(x)).$$

Let $U := \{\alpha \in \mathbb{F}_{q^2} \mid u(\alpha) = 0\}$. For a polynomial $F(y) \in \mathbb{F}_{q^2}[y]$ with degree m prime to the characteristic p, the algebraic curves $\mathcal{C}$ and $\mathcal{C}_1$ over $\mathbb{F}_{q^2}$ defined respectively by

$$A(x) = F(y) \qquad \text{and} \qquad a(x) = F(y)$$

with the additive polynomial $u(x)$ such that $A(x) = a(u(x))$ as above, are such that the first curve $\mathcal{C}$ is a Galois cover of the second $\mathcal{C}_1$ with a Galois group isomorphic to U. In fact, for each element $\alpha \in U$ consider the automorphism of the first curve given by

$$\sigma_\alpha(x) = x + \alpha \qquad \text{and} \qquad \sigma_\alpha(y) = y.$$

Lemma 3.17. *If $A(x) = F(y)$ is maximal over $\mathbb{F}_{q^2}$, then there is a $\beta \in \mathbb{F}_{q^2}^*$ such that the curve $x^p - x = \beta F(y)$ is also maximal.*

Proof. Since $A(x) = F(y)$ is maximal over $\mathbb{F}_{q^2}$, Theorem 3.15 and Lemma 3.12 imply that $\bar{A}(x)$ has all roots in $\mathbb{F}_{q^2}$. Hence according to Lemma 3.10, there exists $\alpha \in \mathbb{F}_{q^2}^*$ such that $\alpha^{-1}A(\alpha x)$ has $(*)-$property. Take $\beta = \alpha^{-1}$. It then follows from Corollary 3.9 and Remark 3.16, that the curve $A(\alpha x) = F(y)$ covers the curve $x^p - x = \beta F(y)$. By Remark 2.47, the last curve is maximal. ■

As a corollary of Lemma 3.17 and Theorem 3.6 we have:

Theorem 3.18. *Let $\mathcal{C}$ be a maximal curve over $\mathbb{F}_{q^2}$ given by an equation of the form*

$$A(x) = y^m \quad with \quad gcd(p, m) = 1, \tag{3.19}$$

where $A(x) \in \mathbb{F}_{q^2}[x]$ is an additive and separable polynomial. Then we must have that m divides $q + 1$.

We end up with some comments on known results and examples. Let $q = p^n$ and let t be a positive integer. Wolfmann [54] considered the number of rational points on the Artin-Schreier curve $\mathcal{C}$ defined over $\mathbb{F}_{q^{2t}}$ by the equation

$$x^q - x = ay^m + b$$

where $a, b \in \mathbb{F}_{q^{2t}}$, $a \neq 0$ and m is any positive integer relatively prime to the characteristic p.

Proposition 3.19 ([54], Theorem 1)**.** *Let $\mathcal{C}$ be a curve defined over $\mathbb{F}_{q^2}$ by the equation*

$$x^q - x = ay^m + b$$

where $a, b \in \mathbb{F}_{q^2}$, $a \neq 0$ and m is any positive integer relatively prime to the characteristic p. Suppose m dividing $q + 1$ and $nm = q^2 - 1$ and $um = q + 1$. Then if $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$, then $tr(b) = 0$ and $a^n = (-1)^u$.

We note here that the condition $tr(b) = 0$, means that $\alpha^q - \alpha = b$ for some element $\alpha \in \mathbb{F}_{q^{2t}}$ by Hilbert 90 Theorem. So the curve $\mathcal{C}$ can be given by

$${x_1}^q - x_1 = ay^m \quad \text{with} \quad x_1 := x - \alpha.$$

Example 3.20. Suppose n is an odd number. The curve $\mathcal{C}$ given as follows

$$x^{p^2} - x = y^m \quad \text{with} \quad m = (p^n + 1)/(p + 1), \tag{3.20}$$

is maximal over $\mathbb{F}_{p^{2n}}$ (see [14] for the case $n = 3$). Setting here $q = p^2$ then the curve $\mathcal{C}$ is maximal over $\mathbb{F}_{q^n}$ with n odd. Hence this maximal curve is not among the ones considered in [54].

In [18] it is proved that for $p = 2$ and $n = 3$ this curve in (3.20) is a Galois subcover of the Hermitian curve. In [14] it is shown that this curve for $p = 3$ and $n = 3$ is not a Galois subcover of the Hermitian curve.

Example 3.21. Suppose now that $n = 2k$ is an even number. The curve given by

$$x^{p^k} - x = \beta y^m$$

with $\beta^{p^n-1} = -1$ and m a divisor of p^n+1 is a Galois subcover of the Hermitian curve. Hence it is also maximal over $\mathbb{F}_{p^{2n}}$. This follows from the equation (see Example 3.11)

$$x^{p^n} - x = (x^{p^k} + x)^{p^k} - (x^{p^k} + x).$$

Setting here $q = p^k$ then this curve $\mathcal{C}$ is maximal over $\mathbb{F}_{q^4}$. Hence this maximal curve is among the ones considered in [54].

Chapter 4

Some Characterization of Maximal Curves

In this chapter, we consider maximal and minimal curves over a finite field with q^2 elements. In the first section we study acting the Cartier operator $\mathscr{C}$ on the space of regular differential forms of a maximal curve and we show that

Theorem 4.1. *Let $\mathcal{C}$ be a curve defined over a finite field with q^2 elements, where $q = p^n$ for some $n \in \mathbb{N}$. If $\mathcal{C}$ is maximal (or minimal) over $\mathbb{F}_{q^2}$, then $\mathscr{C}^n = 0$.*

In next sections, we use this property to find some characterizations for maximal and minimal curves; first in Section 4.2.1 we characterize maximal Fermat curves (see Theorem 4.21); second we derive explicit equations for maximal and minimal Artin-Schreier curves over $\mathbb{F}_{q^2}$ given by the relation $y^q - y = f(x)$, where $f(x)$ is a rational function with coefficients in $\mathbb{F}_{q^2}$ (see Theorem 4.30 and Theorem 4.32); in third we classify maximal and minimal hyperelliptic curves over $\mathbb{F}_{q^2}$ such that attain the upper genus bound (see Theorem 4.36 and Remark 4.38); in the last section we find some properties of Artin-Schreier curves that attain the upper Serre bound (SW-maximal). We also show all of maximal curves of these types are subcovers of the Hermitian curve.

4.1 The Hasse-Witt matrix of Maximal Curves

In this section we recall the following basic result concerning Jacobians. Let $\mathcal{C}$ be a curve, $\mathscr{F}$ denotes the Frobenius endomorphism (relative to the base field) of the Jacobian $\mathcal{J}$ of $\mathcal{C}$, and let $h(t)$ be the characteristic polynomial of $\mathscr{F}$. Let $h(t) = \prod_{i=1}^{T} h_i(t)^{r_i}$ be the irreducible factorization of $h(t)$ over $\mathbb{Z}[t]$. Then

$$\prod_{i=1}^{T} h_i(\mathscr{F}) = 0 \quad \text{on} \quad \mathcal{J}. \tag{4.1}$$

This follows from the semisimplicity of $\mathscr{F}$ and the fact that the representation of endomorphisms of $\mathcal{J}$ on the Tate module is faithful (cf. [49, Theorem 2] and [32, VI, Section 3]) (See [10] for more details and some applications). In the case of a maximal curve over $\mathbb{F}_{q^2}$, we have $h(t) = (t+q)^{2g}$. Therefore from (4.1) we obtain the following result, which is contained in the proof of [39, Lemma 1].

Lemma 4.2. *The Frobenius map $\mathscr{F}$ (relative to $\mathbb{F}_{q^2}$) of the Jacobian $\mathcal{J}$ of a maximal (resp. minimal) curve over $\mathbb{F}_{q^2}$ acts as multiplication by $-q$ (resp. by $+q$).*

Remark 4.3. Let $\mathcal{A}$ be an abelian variety defined over $\mathbb{F}_{q^2}$, of dimension g. Then we have

$$(q-1)^{2g} \leq \#\mathcal{A}(\mathbb{F}_{q^2}) \leq (q+1)^{2g}.$$

But if $\mathcal{C}$ is a maximal (resp. minimal) curve over $\mathbb{F}_{q^2}$, by the above lemma we have $\mathcal{J}(\mathbb{F}_{q^2}) = (\mathbb{Z}/(q+1)\mathbb{Z})^{2g}$ (resp. $\mathcal{J}(\mathbb{F}_{q^2}) = (\mathbb{Z}/(q-1)\mathbb{Z})^{2g}$). So the Jacobian of a maximal (resp. minimal) curve is maximal (resp. minimal) in the sense of the above bounds.

Let $\mathcal{C}$ be a maximal or minimal curve. Applying Proposition 2.56 to the Cartier operation on $V = \Omega_{reg}$ of the curve $\mathcal{C}$, we get $\mathscr{C}^r = 0$ for some integer r. In fact the subgroup $G_p(\mathcal{C})$ of elements of $C^0(F_{\mathcal{C}})$ of order p is isomorphic to the additive group of differentials of $H^0(\Omega^1_{\mathcal{C}})$ such that $\mathscr{C}(\omega) = \omega$. But if $\mathcal{C}$ is maximal or minimal,

Corollary 2.59 implies $G_p(\mathcal{C}) = 0$. Here we want to show the following theorem:

Theorem 4.4. *Let $\mathcal{C}$ be a curve defined over a finite field with q^2 elements, where $q = p^n$ for some $n \in \mathbb{N}$. If $\mathcal{C}$ is maximal (or minimal) over $\mathbb{F}_{q^2}$, then $\mathscr{C}^n = 0$.*

To proof the above theorem we use Witt cohomology. So we need some properties of Witt cohomology introduced by Serre as a p-adic cohomology(see [40]). In fact if k is a perfect field of characteristic p, a classical construction yields a canonical lifting of k to a discrete valuation ring

$$\mathcal{W}(k) = \lim_{\leftarrow} \mathcal{W}_r(k).$$

Serre generalized this to $\mathcal{W}(\mathrm{R})$ for any ring R of characteristic $p > 0$, obtained a sheaf of rings $\mathcal{W}_r = \mathcal{W}(\mathscr{O}_{\mathcal{X}})$ for any variety $\mathcal{X}$. Here we recall briefly some definition and some properties and for a more comprehensive approach we refer the reader to [21] and [40].

Let p be a fixed prime and R a commutative ring with unit of characteristic p. We denote by $\mathcal{W}_r(\mathrm{R})$ the ring of Witt vectors of length r with components in R. The composition laws of commutative ring $\mathcal{W}_r(\mathrm{R})$ are given by certain polynomials with coefficients in the prime field. The rings $\mathcal{W}_r(\mathrm{R})$ are mapped onto one another by the following equations:

(a) *The Frobenius endomorphism* $\mathscr{F}_p : \mathcal{W}_r(\mathrm{R}) \to \mathcal{W}_r(\mathrm{R})$. By definition

$$\mathscr{F}_p(a_0, \ldots, a_{r-1}) = (a_0^p, \ldots, a_{r-1}^p).$$

This is a ring homomorphism.

(b) *The shift* $\mathcal{V} : \mathcal{W}_r(\mathrm{R}) \to \mathcal{W}_{r+1}(\mathrm{R})$. By definition

$$\mathcal{V}(a_0, \ldots, a_{r-1}) = (0, a_0, \ldots, a_{r-1}).$$

This is an additive operator. If R is a $k-$algebra, where k is a perfect field of characteristic p, then $\mathcal{V}$ is an p^{-1}-linear transformation of the structure of $\mathcal{W}_r(\mathrm{R})$ as $\mathcal{W}_r(k)$-module.

(c) *The restriction* $\mathscr{R} : \mathcal{W}_{r+1}(\mathrm{R}) \to \mathcal{W}_r(\mathrm{R})$. By definition

$$\mathscr{R}(a_0, \ldots, a_r) = (a_0, \ldots, a_{r-1}).$$

This is a ring homomorphism and commutes with the Frobenius endomorphism. Further, we have

$$\mathscr{R}\mathcal{V}\mathscr{F}_p = \mathscr{F}_p\mathscr{R}\mathcal{V} = \mathscr{R}\mathscr{F}_p\mathcal{V} = p$$

(multiplication by p.)

The projective limit of the system $\mathcal{W}_r(\mathrm{R})$ of rings with respect to restriction is denoted by $\mathcal{W}(\mathrm{R})$. It is a ring of characteristic zero on which the operators $\mathscr{F}_p$ and $\mathcal{V}$ are defined and satisfy the relation $\mathcal{V}\mathscr{F}_p = \mathscr{F}_p\mathcal{V} = p$.

If $\mathrm{R} = k$ is a perfect field of characteristic p, then $\mathcal{W}(k)$ is a complete discrete normed ring with the unique maximal ideal $p\mathcal{W}(k)$. In this case

$$\mathcal{W}_r(k) = \mathcal{W}(k)/p^r\mathcal{W}(k).$$

If $k = \mathbb{F}_p$ is the prime field, then $\mathcal{W}(k)$ is isomorphic to the ring $\mathbb{Z}_p$ of $p-$adic integers, $\mathscr{F}_p$ is the identical isomorphism and $\mathcal{V}w = pw$ for every $w \in \mathcal{W}(k)$.

Cohomology with coefficients in a sheaf of Witt vectors. Let $\mathcal{X}$ be an algebraic $k-$variety, where k is any algebraically closed field of characteristic p, and let $\mathscr{O}$ be the sheaf of local rings on $\mathcal{X}$. Each fibre $\mathscr{O}_x$ is a ring of characteristic p. The union of the rings $\mathcal{W}_r(\mathscr{O}_x)$ for each $x \in \mathcal{X}$ has a natural structure as a sheaf of rings over $\mathcal{X}$, which we shall denote by $\mathscr{W}_r$. The operations $\mathscr{F}_p, \mathcal{V}$ and $\mathscr{R}$ extend to $\mathscr{W}_r$. The sheaves $\mathscr{W}_r$ are sheaves of $\mathcal{W}(k)$-modules, which annihilated by ideas $p^r\mathcal{W}(k)$.

Following Serre we define cohomology groups $H^m(\mathcal{X}, \mathscr{W}_r)$ which can be operated on by $\mathscr{F}_p, \mathcal{V}$ and $\mathscr{R}$. For any $m \geq 0$, $\mathcal{W}(k)$-modules $H^m(\mathcal{X}, \mathscr{W}_r)$ and homomorphisms $R : H^m(\mathcal{X}, \mathscr{W}_{r+1}) \longrightarrow H^m(\mathcal{X}, \mathscr{W}_r)$ form a projective system. The projective limit, which we denote by $H^m(\mathcal{X}, \mathscr{W})$, is also a $\mathcal{W}(k)$-module and admits the operators $\mathscr{F}_p$, and $\mathcal{V}$. The exact sequence

$$0 \to \mathscr{W}_N \xrightarrow{\mathcal{V}^r} \mathscr{W}_{N+r} \xrightarrow{\mathscr{R}^r} \mathscr{W}_r \to 0$$

of sheaves gives rise to the exact cohomology sequence

$$\ldots \to H^m(\mathcal{X}, \mathscr{W}_N) \xrightarrow{\mathcal{V}^r} H^m(\mathcal{X}, \mathscr{W}_{N+r}) \xrightarrow{\mathscr{R}^r} H^m(\mathcal{X}, \mathscr{W}_r) \xrightarrow{\delta_r^m} H^{m+1}(\mathcal{X}, \mathscr{W}_N) \to \ldots$$

and so, on going the projective limit as $N \to \infty$, we obtain the exact sequence

$$\ldots \to H^m(\mathcal{X}, \mathscr{W}) \xrightarrow{\mathcal{V}^r} H^m(\mathcal{X}, \mathscr{W}) \xrightarrow{p^r} H^m(\mathcal{X}, \mathscr{W}_r) \xrightarrow{\delta_r^m} H^{m+1}(\mathcal{X}, \mathscr{W}) \to \ldots \tag{4.2}$$

Lemma 4.5 ([41])**.** *As notation above, if $\mathcal{X}$ be a abelian variety, then the coboundary operators δ_r^m are identically zero.*

Now we can give a proof for Theorem 4.4

Proof of Theorem 4.4. Let $\mathcal{C}$ be a maximal (or minimal) curve over $\mathbb{F}_{q^2}$, $q = p^n$ for some integer n, with Jacobian $\mathcal{J}$. Then by Lemma 4.5 and Exact sequence (4.2) for $r = 1$, we have an exact sequence

$$H^1(\mathcal{J}, \mathscr{W}) \xrightarrow{\mathcal{V}} H^1(\mathcal{J}, \mathscr{W}) \xrightarrow{p} H^1(\mathcal{J}, \mathscr{O}_{\mathcal{J}}) \to 0. \tag{4.3}$$

Now if we let $\mathscr{F}_{q^2}$ denote the Frobenius with respect to $\mathbb{F}_{q^2}$ and $\mathscr{F}_p$ the absolute Frobenius, then ${\mathscr{F}_p}^{2n} = \mathscr{F}_{q^2}$ on $H^1(\mathcal{J}, \mathscr{W})$. According to Lemma 4.2 we know the Frobenius acting on the Jacobian of $\mathcal{C}$ acts as the multiplication by $\pm q$, hence ${\mathscr{F}_p}^{2n} =$

$\pm p^n$. Now $p^n = \mathscr{F}_p{}^n \mathcal{V}^n$ and $\mathscr{F}_p$ is injective on $H^1(\mathcal{J}, \mathscr{W})$ so $\mathscr{F}_p{}^n = \pm \mathcal{V}^n$. This implies $\mathscr{F}_p{}^n = 0$ on $H^1(\mathcal{J}, \mathscr{O}_\mathcal{J})$ (see also [9, Proposition 1.2]). In fact, Exact sequence (4.3) implies

$$H^1(\mathcal{J}, \mathscr{O}_\mathcal{J}) = H^1(\mathcal{J}, \mathscr{W})/\mathcal{V}H^1(\mathcal{J}, \mathscr{W}).$$

Then from Rosenlicht Theorem 2.38 we have that the Frobenius $\mathscr{F}_p$ acting on the $H^1(\mathcal{C}, \mathscr{O}_\mathcal{C})$ satisfies $\mathscr{F}_p{}^n = 0$. Finally, by Proposition 2.50 the Cartier operator acting on $H^0(\Omega_\mathcal{C})$ and the Frobenius acting an $H^1(\mathcal{C}, \mathscr{O}_\mathcal{C})$ are dual to each, so we have $\mathscr{C}^n = 0$. ■

The next result relates the Hasse-Witt matrix and the Weierstrass gap sequence at a rational point.

Proposition 4.6 ([46], Corollary 2.7)**.** *Let $\mathcal{C}$ be a curve defined over a perfect field and $n \in \mathbb{N}$. Let $\mathscr{H}$ denote the Hasse-Witt matrix of the curve $\mathcal{C}$. If P is a rational point on $\mathcal{C}$, then the rank of $\mathscr{H}^{[n]}$ is larger than or equal to the number of gaps at P divisible by p^n.*

Corollary 4.7. *Let $\mathcal{C}$ be a curve defined over $\mathbb{F}_{q^2}$. Let P be a rational point on the curve $\mathcal{C}$. If $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$ then q is not a gap number of P.*

Proof. Writing $q = p^n$ for some integer n, if $\mathcal{C}$ is a maximal curve over $\mathbb{F}_{q^2}$ then by Theorem 4.1 we have $\mathscr{H}^{[n]} = 0$. Thus the result follows from Proposition 4.6. ■

Corollary 4.8. *Let $\mathcal{C}$ be a hyperelliptic curve over $\mathbb{F}_{q^2}$ where $q = p^n$ and $p > 2$. If $\mathscr{C}^n = 0$, then*

$$g(\mathcal{C}) \leq \frac{q-1}{2}.$$

Proof. As the genus is fixed under a constant field extension, we can suppose that k is algebraically closed. We know that a Weierstrass point on a hyperelliptic curve has the gap sequence $1, 3, 5, \ldots, 2g-1$, so the result follows from Proposition 4.6. ■

Remark 4.9. If $\mathcal{C}$ is maximal over $\mathbb{F}_{p^2}$ then $\mathscr{C} = 0$. On the other hand we know that the Cartier operator on a curve is zero if and only if the Jacobian of the curve is the product of supersingular elliptic curves (see [37, Theorem 4.1]). Now by Theorem 1.1 of [9] we will have also

- $g(\mathcal{C}) \leqslant (p^2 - p)/2$
- $g(\mathcal{C}) \leqslant (p-1)/2$ if $\mathcal{C}$ is hyperelliptic and $(p, g) \neq (2, 1)$.

Here we give an example of a supersingular non-singular curve $\mathcal{X}$ defined over a finite field $\mathbb{F}_{p^2}$ such that its Hasse-Witt matrix is zero but $\mathcal{X}$ is not maximal or minimal over $\mathbb{F}_{p^2}$.

Example 4.10. Let $\mathcal{X}(n)$ be the Hurwitz curve of degree $n+1$, i.e., the non-singular plane curve given by equation

$$x^n y + y^n z + z^n x = 0,$$

where $p = char(\mathbb{F}_{q^2})$ does not $d := n^2 - n + 1$. According to [1, Theorem 3.1] we know that $\mathcal{X}(n)$ is maximal over $\mathbb{F}_{q^2}$ if and only if $d := n^2 - n + 1$ divides $q + 1$. Hence the curve $\mathcal{X}(p)$ is not maximal over $\mathbb{F}_{p^2}$. On the other hand the curve $\mathcal{X}(p)$ is not minimal over $\mathbb{F}_{q^2}$ since it is maximal over $\mathbb{F}_{p^6}$ (see Corollary 2.43). Now we can show that the Hasse-Witt matrix of $\mathcal{X}(p)$ is identically zero, i.e., the action of Frobenius on $H^1(\mathcal{X}(p), \mathscr{O}_{\mathcal{X}(p)})$ is 0. Here we recall the proof of this fact for $p = 3$, due to Hartshorne [23]:

Let k be an algebraically closed field of characteristic 3. Consider the curve $\mathcal{X} := \mathcal{X}(3)$ given by the equation $g := x^3y + y^3z + z^3x$ as a plane curve in $P := \mathbb{P}^2(k)$. $\mathcal{X}$ is a plane curve of degree 4, it has genus 3. Then we have an exact sequence

$$0 \to \mathscr{O}_P(-4) \xrightarrow{g} \mathscr{O}_P \to \mathscr{O}_{\mathcal{X}} \to 0,$$

which gives rise to an isomorphism

$$H^1(\mathcal{X}, \mathscr{O}_{\mathcal{X}}) \stackrel{\cong}{\to} H^2(P, \mathscr{O}_P(-4)).$$

This latter vector space, according to the explicit calculations of cohomology on projective space (see Theorem 5.1 Chapter III of [24]), has a basis consisting of the negative monomials of degree 4, namely

$$\frac{1}{x^2yz}, \ \frac{1}{xy^2z}, \ \frac{1}{xyz^2}.$$

Under the above isomorphism, the action of Frobenius on $H^1(\mathcal{X}, \mathscr{O}_{\mathcal{X}})$ becomes the composition

$$H^2(P, \mathscr{O}_P(-4)) \stackrel{f^*}{\to} H^2(P, \mathscr{O}_P(-12)) \stackrel{g^2}{\to} H^2(P, \mathscr{O}_P(-4))$$

of Frobenius on $\mathbb{P}^2$ with multiplication by g^2. Now Frobenius takes our there monomials into their cubes,

$$\frac{1}{x^6y^3z^3}, \ \frac{1}{x^3y^6z^3}, \ \frac{1}{x^3y^3z^6}.$$

Every monomial of g^2 contains either x^6 or y^3 or z^3. Hence $g^2/x^6y^3z^3 = 0$ in $H^2(P, \mathscr{O}_P(-4))$. ■

4.2 Applications

In this section we give some classifications of maximal curves as applications of Theorem 4.4.

4.2.1 Fermat Curves

In this section we introduce a characterization for maximal Fermat curves. First we review some known result of Fermat curves.

Let k be a field, $\bar{k} \supseteq k$ be its algebraic closure. The *Fermat curve of exponent m over k* is the projective plane curve $\mathcal{C}(m) \subseteq \mathbb{P}^2(k)$ defined by the homogeneous equation

$$x^m + y^m = z^m. \tag{4.4}$$

In case $k = \mathbb{Q}$, Fermat curves are intimately related to Fermat's last theorem, and there is no further need to give reasons why one should study these curves.

If k has positive characteristic $p > 0$ and $m = rp$ is a multiple of p, then Equation (4.4) can be written as $(x^r + y^r = z^r)^p$ and is therefore reducible. If however the characteristic of k is relatively prime to m, then the Equation (4.4) is absolutely irreducible. In this case the Fermat curve $\mathcal{C}(m)$ over k is easily seen to be non-singular, and therefore its genus is

$$g(\mathcal{C}(m)) = (m-1)(m-2)/2.$$

Let us consider the automorphisms of the Fermat curve $\mathcal{C}(m)$ over $k = \bar{k}$ (as always we assume that m is relatively prime to the characteristic of k). For all $m \geq 4$, the group of $Aut(\mathcal{C}(m))$ is finite, as follows from Hurwitz theorem. There are some obvious automorphism $f \in Aut(\mathcal{C}(m))$:

(i) $(a:b:c) \mapsto (\zeta a : \xi b : c)$ with $\zeta^m = \xi^m = 1$.

Here we denote by $(a:b:c) \in \mathbb{P}^2(k)$ a point of $\mathcal{C}(m)$, hence $a^m + b^m = c^m$.

(ii) The permutations of 3 coordinates of $\mathbb{P}^2(k)$ yield automorphisms of $\mathcal{C}(m)$.

There are m^2 automorphism of type (i) and 6 automorphism of type (ii); altogether they generate a subgroup

$$G \subseteq Aut(\mathcal{C}(m)) \text{ with } ord(G) = 6m^2.$$

For most values of m, the group G above is the full automorphism group of $\mathcal{C}(m)$.

If k is a finite field with l elements, Just as the Artin-Schreier curve is connected with Gauss sums, similarly the Fermat curve $\mathcal{C}(m)$ with $l \equiv 1 \pmod{m}$, is connected with Jacobi sums. In fact as Weil explain in his famous paper in [53] we have the following equation for L-polynomial of Fermat curve $\mathcal{C}(m)$:

$$L(t) = \prod_{\substack{1 \le r,s \le m \\ r+s \neq m}} (1 - J(\widetilde{\psi}_r, \widetilde{\psi}_s)t), \tag{4.5}$$

where $(\psi_r, \psi_s) \in \hat{\mu}_m \times \hat{\mu}_m$ and $\widetilde{\psi}(x) := \psi(x^{(l-1)/m})$.

Here we are interested to characterize maximal curves. For this we begin with a simple lemma:

Lemma 4.11. *With notation and hypotheses as above, If $\mathcal{C}(m)$ is maximal over $\mathbb{F}_{q^2}$, then $m \le q+1$.*

Proof. Since the genus is $g = (m-1)(m-2)/2$ and the curve $\mathcal{C}(m)$ is maximal over $\mathbb{F}_{q^2}$, then

$$\#\mathcal{C}(m)(\mathbb{F}_{q^2}) = 1 + q^2 + (m-1)(m-2)q. \tag{4.6}$$

Looking at the function field extension $\mathbb{F}_{q^2}(x,y)/\mathbb{F}_{q^2}(x)$, where it holds that $y^m = 1-x^m$, the points with $x^m = 1$ are totally ramified. Hence we also have the following inequality

$$\#\mathcal{C}(m)(\mathbb{F}_{q^2}) \leqslant m + (q^2+1-m)m. \tag{4.7}$$

Using (4.6) and (4.7) we conclude that $m \leqslant q+1$. ■

Remark 4.12. If $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$, then m divides q^2-1 (see the proof of Lemma 3.2).

We will now show that specific Fermat curves are maximal: let $l = q^2$ be a square, and consider the Hermitian curve $\mathcal{H} = \mathcal{C}(q+1)$ over $\mathbb{F}_l$. We determine the points $P = (a:b:c) \in \mathcal{H}(\mathbb{F}_l)$.

(i) $c = 1$, so $P = (a:b:1)$. We can choose $b \in \mathbb{F}_l$ arbitrary; then a must satisfy the equation

$$a^{q+1} = -1 - b^{q+1}. \tag{4.8}$$

If $b^{q+1} = -1$, then $a = 0$ and

$$P = (0:b:1) \in \mathcal{H}(\mathbb{F}_l) \tag{4.9}$$

If $b^{q+1} \neq -1$, then $-1-b^{q+1}$ is a non-zero element in $\mathbb{F}_q$, and equation (4.8) has $q+1$ distinct roots $a \in \mathbb{F}_l$. Hence we find for any $b \in \mathbb{F}_l$ with $b^{q+1} \neq -1$ exactly $q+1$ points

$$P = (a:b:1) \in \mathcal{H}(\mathbb{F}_l). \tag{4.10}$$

Note that $b^{q+1} \neq -1$ holds for exactly $q^2-(q+1)$ elements $b \in \mathbb{F}_l$.

(ii) $c = 0$, so $P = (a:1:0)$. Since $a^{q+1}+1 = 0$ has $q+1$ roots $a \in \mathbb{F}_l$, we find

exactly $q+1$ points of the form

$$P = (a : 1 : 0) \in \mathcal{H}(\mathbb{F}_l). \tag{4.11}$$

Counting all points $P \in \mathcal{H}(\mathbb{F}_l)$ as given by (4.9), (4.10) and (4.11) we find that

$$\begin{aligned} \#\mathcal{H}(\mathbb{F}_{q^2}) &= (q+1) + (q^2 - (q+1))(q+1) + (q+1) \\ &= (q+1)(q^2 - q + 1) = q^3 + 1. \end{aligned}$$

Hence the Hermitian curve $\mathcal{H} = \mathcal{C}(q+1)$ is maximal over $\mathbb{F}_{q^2}$ of genus $g(\mathcal{H}) = q(q-1)/2$. Hermitian curves are not the only examples of maximal curves among the Fermat curves. In fact if m divides $q+1$, i.e., $q+1 = mr$ for some integer r, then we can define the following morphism

$$\begin{cases} \mathcal{C}(q+1) & \to & \mathcal{C}(m) \\ (x, y) & \mapsto & (x^r, y^r). \end{cases}$$

Hence $\mathcal{C}(m)$ is covered by $\mathcal{C}(q+1)$. Thus by Remark 2.47 if m divides $q+1$, then $\mathcal{C}(m)$ is maximal. Here we want to show they are all of maximal Fermat curves, indeed we show that the degree of any maximal Fermat curve over $\mathbb{F}_{q^2}$ is a divisor of $q+1$. Before giving the proof, we review some known result of the Hasse-Witt matrix of the Fermat curves from [30]:

Let k be a perfect field of characteristic $p > 0$, and the curve $\mathcal{C}(m)$ defined over k. We study the $H^0(\mathcal{C}(m), \Omega^1)$, k-module of holomorphic differentials in $\mathcal{C}(m)$. For given pair $[\ell, i]$ of integers satisfying $0 \leq \ell \leq m-3$ and $0 \leq i \leq \ell$, we put

$$\omega_{\ell,i} = x^i y^{\ell - i} dx / y^{m-1}.$$

It is well known that

$$\omega_{0,0},\quad \omega_{1,1},\quad \omega_{1,0},\ldots,\quad \omega_{m-3,m-3},\quad \omega_{m-3,m-2},\ldots,\quad \omega_{m-3,0},$$

is a basis of $H^0(\mathcal{C}(m),\Omega^1)$. Such a basis is said to be canonical.

Because of gcd(m,p)=1, it is easy to prove the following lemma:

Lemma 4.13. *For a given integer r and pair $[\ell,i]$ of integers satisfying $0\le\ell\le m-3$ and $0\le i\le\ell$, there exists one and only one pair $[u,v]$ of integers such that*

$$(E(m,p^r;\ell,i))\qquad \begin{cases} p^r u+mv=(p^r-1)(m-1)+\ell-i, \\ 0\le u\le m-2 \ \ \textit{and} \ \ 0\le v\le p^r-1. \end{cases}$$

The notation being as in Lemma 4.13, we get

$$\begin{aligned} \omega_{\ell,i} &= x^i y^{\ell-i}dx/y^{m-1} \\ &= x^i y^{(p^r-1)(m-1)+\ell-i}dx/y^{p^r(m-1)} \\ &= x^i(1-x^m)^v y^{p^r u}dx/y^{p^r(m-1)} \\ &= (y^u/y^{m-1})^{p^r}\sum_{0\le j\le v}(-1)^j\binom{v}{j}x^{mj+i}dx., \end{aligned} \tag{4.12}$$

The following lemma is also easily proved:

Lemma 4.14. *For a given integer r and pairs $[\ell,i]$ and $[u,v]$ as in Lemma 4.13,*

(i) there exists one and only one pair $[j,s]$ of integers such that

$$(E(m,p^r;\ell,i;u,v))\qquad \begin{cases} mj+i=p^r(s+1)-1, \\ 0\le j\le p^r-1 \ \ \textit{and} \ \ 0\le s\le m-2. \end{cases}$$

(ii) In this case, if $j\le v$ then $u+s\le m-3$, and if $j>v$ then $u+s\ge m-1$.

Thus, the rotations being as in Lemma 4.14, we obtain

Theorem 4.15. *For a given integer r and pair $[\ell, i]$ of integers satisfying $0 \leq \ell \leq m-3$ and $0 \leq i \leq \ell$, let $[u, v]$ be the solution of $E(m, p^r; \ell, i)$ and $[j, s]$ the solution of $E(m, p^r; \ell, i; u, v)$. Then*

$$\mathscr{C}^r(\omega_{\ell,i}) = \begin{cases} (-1)^j \binom{v}{j} x^s y^u dx/y^{m-1} & \text{if} \quad j \leq v, \\ 0 & \text{if} \quad j > v. \end{cases}$$

We will now put $I(\ell, i) = \ell - i + l + \ell(\ell+1)/2$ and $\omega_{I(\ell,i)} = \omega_{\ell,i}$ for $0 \leq \ell \leq m-3$ and $0 \leq i \leq \ell$. Then $\omega_1, \omega_2, \ldots, \omega_g$ means the canonical basis of $H^0(\mathcal{C}(m), \Omega^1)$, where $g = (m-1)(m-2)/2$.

We denote by $\mathscr{H}$ the Hasse-Witt matrix of curve $\mathcal{C}(m)$ with respect to the canonical basis $\omega_1, \omega_2, \ldots, \omega_g$.

Corollary 4.16 ([30], Corollary of Theorem 1)**.** *$\mathscr{H}$ has at most one non-zero element in each row and in each column.*

Proof. From Theorem 4.15, it is clear that $\mathscr{H}$ has at most one non-zero element in each row. Next, for given pairs $[\ell, i]$ and $[\ell', i']$ satisfying $0 \leq \ell \leq m-3$, $0 \leq i \leq \ell$, $0 \leq \ell' \leq m-3$ and $0 \leq i' \leq k'$, let $[u, v]$ and $[u', v']$ be solutions of $E(m, p; \ell, i)$ and $E(m, p; \ell', i')$ respectively.

Assume that $[u+s, s] = [u'+s', s']$. Then $E(m, p; \ell, i; u, v)$ and $E(m, p; \ell', i'; u', v')$ lead to $i \equiv i' \bmod m$ and so $i = i'$. Thus $E(m, p; \ell, i)$ and $E(m, p; \ell', i')$ lead to $\ell \equiv \ell' \bmod m$ and so $\ell = \ell'$. This shows that $\mathscr{H}$ has at most one non-zero element in each column. ■

Theorem 4.17 ([30], Theorem 2)**.**

$$p \equiv 1 \ (mod\ m) \qquad \text{if and only if} \quad \text{rank } \mathscr{H} = g.$$

Proof. Let $p \equiv 1 \ (mod\ m)$. Then, for each pair $[\ell, i]$ ($0 \leq \ell \leq m-3$ *and* $0 \leq i \leq \ell$), let $[u, v]$ be the solution of $E(m, p; \ell, i)$ and $[j, s]$ the solution of $E(m, p; \ell, i; u, v)$.

Evidently

$$u = \ell - i, \qquad v = (p-1)(i+m-\ell-1)/m,$$

$$j = (p-1)(i+1)/m, \qquad s = i.$$

Since $j < v$ and $u + s = \ell$, it is clear that

$$\mathscr{C}(\omega_{\ell,i}) = (-1)^j \binom{v}{j} \omega_{\ell,i},$$

we see that $\mathscr{H}$ is diagonal and rank $\mathscr{H} = g$.

Conversely, assume rank $\mathscr{H} = g$. Then let $[u_\ell, v_\ell]$ be the solution of $E(m, p; \ell, \ell)$ for $\ell = 0, 1, \ldots, m-3$. Clearly

$$u_0 = u_1 = \ldots = u_{m-3} \text{ and } v_0 = v_1 = \ldots = v_{m-3}$$

Moreover, let $[j_\ell, s_\ell]$ be the solution of $E(m, p; \ell, \ell; u_\ell, v_\ell)$ for $\ell = 0, 1, \ldots, m-3$. Then it is easy that

$$\{s_0, s_1, \ldots, s_{m-3}\} = \{0, 1, \ldots, m-3\}.$$

Therefore, from $\ell + 1 \equiv p(s_\ell + 1) \pmod{m}$ for $\ell = 0, 1, \ldots, m-3$, summing both sides over k yields

$$(m-1)(m-2)/2 \equiv p(m-1)(m-2)/2 \pmod{m}$$

and so we get $p-1+m(p-1)(m-3)/2 \equiv 0 \pmod{m}$. Thus, because of $2 \mid (p-1)(m-3)$, we have $p \equiv 1 \pmod{m}$. ■

Now we will give the rank relation between the Hasse-Witt matrices of two Fermat curves and gives its simple application.

As before, let m be an integer having $m \geq 3$. Denote by p and p' primes numbers such that $\gcd(m, p) = 1$ and $\gcd(m, p') = 1$. And let k and k' be perfects fields of

characteristic p and $p^{'}$ respectively. Moreover let $\mathcal{C}(m)$ and $\mathcal{C}'(m)$ be algebraic curves over k and $k^{'}$ respectively.

Put $g = (m-1)(m-2)/2$ and denote by $\mathscr{H}$ and $\mathscr{H}'$ the Hasse-Witt matrices of $\mathcal{C}(m)$ and $\mathcal{C}'(m)$ with respect to the canonical bases of holomorphic differentials respectively.

Theorem 4.18 ([30], Theorem 3)**.** *If* $p + p^{'} \equiv 0$ (mod) m, *then*

$$rank\ \mathscr{H}\ +\ rank\ \mathscr{H}' = g.$$

Proof. For a given pair $[\ell, i]$ of integers satisfying $0 \leq \ell \leq m-3$ and $0 \leq i \leq \ell$, let $[u, v]$ and $[u^{'}, v^{'}]$ be the solutions of $E(m, p; \ell, i)$ and $E(m, p^{'}; \ell, i)$ and let $[j, s]$ and $[j^{'}, s^{'}]$ be the solution of $E(m, p; \ell, i; u, v)$ and $E(m, p^{'}; \ell, i; u^{'}, v^{'})$ respectively.

Then $E(m, p; \ell, i)$ and $E(m, p^{'}; \ell, i)$ lead to $p(u+1) \equiv p^{'}(u^{'}+1) \pmod{m}$ and so $u + u^{'} + 2 = m$. Moreover $E(m, p; \ell, i; u, v)$ and $E(m, p^{'}; \ell, i; u^{'}, v^{'})$ lead to $p(s+1) \equiv p^{'}(s^{'}+1) \pmod{m}$ and so we get $s + s^{'} + 2 = m$.

Thus, in view of Lemma 4.14 (ii) and of $u + s + u^{'} + s^{'} = 2(m-2)$, we see that $j \leq v$ if and only if $j^{'} \geq v^{'}$. So, by making use of Theorem 4.15, we obtain that $\mathscr{C}(\omega_{\ell,i}) \neq 0$ if and only if $\mathscr{C}'(\omega'_{\ell,i}) = 0$, where $\omega_{\ell,i}$ and $\omega'_{\ell,i}$ mean the canonical bases of holomorphic differentials of $\mathcal{C}(m)$ and $\mathcal{C}'(m)$. Therefore the required formula follows immediately from Corollary 4.16. ■

Corollary 4.19 ([30], Corollary 1 of Theorem 3)**.**

$$p \equiv -1\ (mod\ m) \qquad if\ and\ only\ if \quad rank\ \mathscr{H} = 0.$$

Proof. As $\gcd(m, p) = 1$ using Drichlet Theorem (see [2]) we can find a prime number $p^{'}$ such that $p + p^{'} \equiv 0 \pmod{m}$. Hence the result follows from combining Theorem 4.17 and Theorem 4.18. ■

Remark 4.20. Let $\mathcal{C}(m)$ be a maximal curve defined over $k = \mathbb{F}_{p^2}$ where p is the characteristic of k. Hence from Theorem 4.4, we know $\mathscr{C} = 0$. Hence by the above corollary m is a divisor of $p + 1$.

Considerations such as the above led us to obtain the following result:

Theorem 4.21. *Let $\mathcal{C}(m)$ be a Fermat curve of degree m prime to the characteristic p defined over $\mathbb{F}_{q^2}$. Then $\mathcal{C}(m)$ is maximal over $\mathbb{F}_{q^2}$ if and only if m divides $q + 1$.*

Proof. If m divides $q + 1$, from the above discussion we have that the curve $\mathcal{C}(m)$ is maximal over $\mathbb{F}_{q^2}$. Now we must show the converse statement. Consider then the maximal curve $\mathcal{C}(m)$ over $\mathbb{F}_{q^2}$. By Remark 4.12 we have that m divides $q^2 - 1$. As in the proof of Lemma 4.11, looking at the function field extension $\mathbb{F}_{q^2}(x, y)/\mathbb{F}_{q^2}(x)$ we have:

$$\#\mathcal{C}(m)(\mathbb{F}_{q^2}) = m + \lambda m \qquad \text{for some integer } \lambda. \tag{4.13}$$

In fact $\mathcal{C}(m)$ has m rational points which correspond to the totally ramified points with $x^m = 1$ and some others that are completely splitting. On the other hand from the maximality of $\mathcal{C}(m)$, we have

$$\#\mathcal{C}(m)(\mathbb{F}_{q^2}) = 1 + q^2 + (m - 1)(m - 2)q. \tag{4.14}$$

Comparing (4.13) and (4.14) we obtain that m divides $(q + 1)^2$. Hence m divides $2(q + 1)$, since m is a divisor of $q^2 - 1$. Now we have two cases:

Case $p = 2$. In this case since $\gcd(m, p) = 1$, we have that m is odd and hence it divides $q + 1$, since it divides $2(q + 1)$.

Case $p =$ odd. In this case we have $\gcd(q + 1, q - 1) = 2$. Reasoning as in the case $p = 2$, we get here that if d is an odd divisor of m, then d is a divisor of $q + 1$. The only situation still to be investigated is the following: $q + 1 = 2^r s$ with s an odd integer and $m = 2^{r+1} s_1$ with s_1 a divisor of s. But according to Remark 2.47 and the following lemma, this situation does not occur.

Lemma 4.22. *Assume that the characteristic p is odd and write $q+1 = 2^r.s$ with s an odd integer. Denote by $m := 2^{r+1}$. Then the Fermat curve $\mathcal{C}(m)$ is not maximal over $\mathbb{F}_{q^2}$.*

Proof. Writing $q = p^n$ we consider three cases:

Case $p \equiv 1$ (mod 4). In this case we have $q+1 = 2.s$ with s an odd integer. So we must show that the curve $\mathcal{C}(4)$ is not maximal over $\mathbb{F}_{q^2}$. But it follows from Theorem 4.17 that the curve $\mathcal{C}(4)$ with $p \equiv 1 \pmod 4$ is ordinary and so it is not maximal.

Case $p \equiv 3$ (mod 4) and n even. In this case we have again $q+1 = 2.s$ with s an odd integer and we must show that the curve $\mathcal{C}(4)$ is not maximal over $\mathbb{F}_{q^2}$. Since 4 is a divisor of $p+1$, the curve $\mathcal{C}(4)$ is maximal over $\mathbb{F}_{p^2}$. Hence $\mathcal{C}(4)$ is minimal over $\mathbb{F}_{q^2}$ because n is even.

Case $p \equiv 3$ (mod 4) and n odd. As n is odd then we have $q+1 = 2^r s$ with $r \geqslant 2$ and s odd. Here we can assume that $r \geq 3$. In fact for $r = 2$ according to [29, page 204], the curve $\mathcal{C}(8)$ is not supersingular and hence $\mathcal{C}(8)$ cannot be maximal. Note that $r = 2$ implies $p \equiv 3 \pmod 8$.

Consider now the curve $\mathcal{C}(m)$ with $m = 2^{r+1}$ and $r \geq 3$. As $m = 2^{r+1}$ is the biggest power of 2 that divides $q^2 - 1$, so (-1) is not a m-th power in $\mathbb{F}_{q^2}^*$. Hence the points at infinity on $y^m = 1 - x^m$ are not rational. In this case, as μ_m acts on $\mathcal{C}(m)$ we have:

$$\#\mathcal{C}(m)(\mathbb{F}_{q^2}) = m + \lambda_1 m^2 \qquad \text{for some integer } \lambda_1. \tag{4.15}$$

Then from (4.14) and (4.15) we get

$$q^2 + 1 + 2q - 3mq - m \equiv 0 \pmod{m^2}.$$

Hence $(q+1)^2 - m(2q+2) - m(q-1) \equiv 0 \pmod{m^2}$. Since m divides $2q+2$, we obtain that $4(q+1)^2 - 4m(q-1) \equiv 0 \pmod{4m^2}$. This implies that m divides $4(q-1)$ and this is impossible as $r \geqslant 3$ and $4(q-1) = 8s_1$ with s_1 odd. This completes the

proofs of Lemma 4.22 and of Theorem 4.21 ■■

Remark 4.23. The particular case of Theorem 4.21 when m is of the form $m = t^2 - t + 1$ with $t \in \mathbb{N}$, was proved in Corollary 3.5 of [1].

Remark 4.24. In the following we give another proof for our classification of maximal Fermat curves; Consider Fermat curve $\mathcal{C}(m)$ given by

$$Y^m + X^m = 1.$$

Let $k = \mathbb{F}_{p^f}$ be a finite field of characteristic $p > 0$, where f is the smallest positive integer such that

$$p^f \equiv 1 \pmod{m}.$$

Then we have the following theorem:

Theorem 4.25 ([56], Theorem 3.5)**.** *By the above situation, the Jacobian of the curve $\mathcal{C}(m)$ is supersingular if and only if f is even and m divides $p^{f/2} + 1$.*

Corollary 4.26. *Let $\mathcal{C}(m)$ be the Fermat curve of degree m prime to the characteristic p defined over $\mathbb{F}_{q^2}$ with $q = p^n$. Then*

1) $\mathcal{C}(m)$ is maximal over $\mathbb{F}_{q^2}$ if and only if m divides $q + 1$.

2) If $\mathcal{C}(m)$ is minimal over $\mathbb{F}_{q^2}$ then n is even and m divides $p^n - 1$. In the other word, minimal Fermat curves are maximal over some constant subfield.

Proof. 1) If $\mathcal{C}(m)$ is maximal over $\mathbb{F}_{q^2}$, $q = p^n$, we know that

$$p^{2n} \equiv 1 \pmod{m}.$$

As f is smallest with this property, one can show that f divides $2n$, set $2n = fh$. As maximal (or minimal) curves are supersingular, by the above theorem we have f is

even and m divides $p^{f/2}+1$. Hence $\mathcal{C}(m)$ is also maximal over $\mathbb{F}_{p^f}$ and maximality over $\mathbb{F}_{q^2}$ implies that h is odd. Hence m divides $q+1$.

2) If $\mathcal{C}(m)$ is minimal over $\mathbb{F}_{q^2}$, then is supersingular. By the proof of the first part we know that f divides $2n$. Now if $2n = f$ then $\mathcal{C}(m)$ is maximal, so we can assume $f < 2n,\ 2n = fh$, and $h > 1$. Furthermore h is even since $\mathcal{C}(m)$ is maximal over $\mathbb{F}_{p^f}$. ■

4.2.2 Artin-Schreier Curves

In this section we consider curves $\mathcal{C}$ over $k = \mathbb{F}_{q^2}$ given by an affine equation

$$y^q - y = f(x), \tag{4.16}$$

where $f(x)$ is an *admissible* rational function in $k(x)$; i.e., a rational function such that every pole of $f(x)$ in the algebraic closure $\bar{k}$ occurs with a multiplicity relatively prime to the characteristic p. If $\mathcal{C}$ is a maximal curve over $\mathbb{F}_{q^2}$, from [18, Remark 4.2] we can assume that $f(x)$ is a polynomial of degree $\leq q+1$. In the following we apply results introduced in the preceding sections to characterize maximal curves given as in Equation (4.16).

The following remark is due to Stichtenoth:

Remark 4.27. Suppose that $q = p$ in Equation (4.16) considered over a perfect field k. Then we can change variables to assume that the curve $\mathcal{C}$ is given by Equation (4.16) with an admissible rational function. This follows from the partial fraction decomposition and from arguments similar to the proof of [43, Lemma III.7.7]. In fact let $u(x)$ in $k[x]$ be an irreducible polynomial and suppose that the rational function $f(x)$ involves a partial fraction of the form $c(x) = u(x)^{rp}$, with $c(x)$ a polynomial in $k[x]$ prime to $u(x)$ and with r a natural number. Since the quotient field $k[x]/(u(x))$ is perfect, we can find polynomials $a(x)$ and $b(x)$ in $k[x]$ such that $c(x) = a(x)^p +$

$b(x)/u(x)$. Denoting by $z = a(x) = u(x)^r$ we get:

$$c(x) = u(x)^{rp} - (z^p - z) = z + b(x) = u(x)^{rp-1}.$$

Performing the substitution $y \to y - z$ and repeating the arguments above we get the desired result.

Denote by tr the trace of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. We have that (see [54]):

Proposition 4.28. *Let $\mathcal{C}$ be a curve defined over $\mathbb{F}_{q^2}$ by the equation*

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

where $a, b \in \mathbb{F}_{q^2}$, $a \neq 0$ and d is any positive integer relatively prime to the characteristic p. Suppose d divides $q+1$ and define v and u by $vd = q^2-1$ and $ud = q+1$. Then

1) If $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$, then $tr(b) = 0$ and $a^v = (-1)^u$.

2) If $\mathcal{C}$ is minimal over $\mathbb{F}_{q^2}$ and $q \neq 2$, then $d = 2$, $tr(b) = 0$ and $a^v \neq (-1)^u$.

Remark 4.29. Let $q = 2$ and $b \in \mathbb{F}_4 \setminus \mathbb{F}_2$; apart from the curves listed in item 2) of the above proposition, we have another minimal one of the form as in Equation (4.16): the minimal elliptic curve over $\mathbb{F}_4$ given by the affine equation $y^2 + y = x^3 + b$.

Suppose $q = p$ is a prime. Then a curve given by Equation (4.16) is a $p-$cyclic extension of $\mathbb{P}^1$. In [28] we have a characterization of such curves, defined over an algebraically closed field, with zero Hasse-Witt matrix. Here we generalize their argument, and we characterize such curves in the general case $q = p^n$ with nilpotent Cartier operator $\mathscr{C}^n = 0$.

We now state the main result of this section:

Theorem 4.30. *Let $\mathcal{C}$ be a curve defined by the equation $y^q - y = f(x)$, where $f(x) \in \mathbb{F}_{q^2}[x]$ is a polynomial of degree d prime to p. If the curve $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$, then $\mathcal{C}$ is isomorphic to the projective curve defined over $\mathbb{F}_{q^2}$ by the following affine equation*

$$y^q + y = x^d \qquad \text{with} \quad d \text{ a divisor of } q+1.$$

Proof. Write $q = p^n$. As the curve $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$, from Theorem 4.1 we know that $\mathscr{C}^n = 0$.

A basis $\mathcal{B}$ for $H^0(\mathcal{C}, \Omega^1)$ is as bellow :

$$\mathcal{B} = \{y^r x^a dx \mid 0 \leq a, r \text{ and } ap^n + rd \leq (p^n - 1)(d-1) - 2\}. \tag{4.17}$$

Since $y = y^q - f(x)$ we have

$$\mathscr{C}^n(y^r x^a dx) = \mathscr{C}^n((y^q - f)^r x^a dx).$$

From Remark 2.52 we get

$$\mathscr{C}^n(y^r x^a dx) = \sum_{h=0}^{r} \binom{r}{h} (-1)^h y^{r-h} \mathscr{C}^n(f^h x^a dx). \tag{4.18}$$

Hence we have

$$\mathscr{C}^n(f^h x^a dx) = 0 \tag{4.19}$$

for all h, r and a satisfying $0 \leq h \leq r$, $\binom{r}{h}$ is prime to p and

$$ap^n + rd \leq (p^n - 1)(d-1) - 2. \tag{4.20}$$

First we show again that the degree of $f(x)$ is not bigger than $q+1$. In fact if

$d = \deg(f(x) \geq q+2$, then $x^{q-1}dx$ is a element of $\mathcal{B}$, because

$$q(q-1) \leq (q-1)(q+1) - 2.$$

From Remark 2.52 we get $\mathscr{C}^n(x^{p^n-1}dx) = dx$ and this contradicts $\mathscr{C}^n = 0$.

Now if $d = q+1$, then the genus of the curve $\mathcal{C}$ is $g = q(q-1)/2$. Hence according to [39] the curve $\mathcal{C}$ is the Hermitian curve given by:

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

Hence we can assume $d \leq q$, and so $d \leq q-1$. Then there exists $\ell \geq 1$ such that

$$\ell d + 1 \leq q < (\ell+1)d + 1.$$

Again by $\gcd(p, d) = 1$, we have

$$\ell d + 1 \leq q \leq (\ell+1)d - 1. \tag{4.21}$$

For a natural number $r \in \mathbb{N}$ satisfying

$$(q-1-r)d \geq q+1$$

we define

$$a(r) := [d - 1 - \frac{(r+1)d+1}{q}].$$

This number $a(r)$ is the biggest possible number $a \in \mathbb{N}$ satisfying (4.20).

From (4.21) and $d \leq q-1$, we get that $a(\ell) = d-3$ and therefore

$$deg(f^\ell x^{a(\ell)}) = \ell d + a(\ell) = (\ell+1)d - 3. \tag{4.22}$$

Suppose that $q-1=\ell d+a$ with $0\leq a\leq a(\ell)$. Then the polynomial $f^{\ell}x^{a}$ has degree $q-1$ and it follows from Remark 2.52 that

$$\mathscr{C}^{n}(f^{\ell}x^{a}.dx)={a_{d}}^{\ell/q}.dx$$

where a_d denotes the leading coefficient of $f(x)$. But this is in contradiction with (4.19) where we take $r=h=\ell$.

Therefore we now get from (4.22) that

$$q-1\geq \ell d+a(\ell)+1=(\ell+1)d-2. \tag{4.23}$$

By (4.21) and (4.23), we have

$$q+1=sd \qquad \text{with } s:=\ell+1\geq 2. \tag{4.24}$$

Since $\gcd(p,d)=1$, we can change the variable x by $x\mapsto x+\alpha$, for a suitable $\alpha\in\mathbb{F}_{q^2}$, such that

$$f(x)=a_{d}x^{d}+a_{i}x^{i}+...+a_{0} \text{ with } i\leq d-2.$$

Therefore

$$f(x)^{s}=a_{d}^{s}x^{sd}+sa_{d}^{s-1}a_{i}x^{i+(s-1)d}+...+a_{0}^{s}.$$

Suppose $d\geq 3$. In this case if $1\leq i\leq d-2$, then

$$0\leq d-i-2\leq d-3=a(s).$$

We stress here that it holds $a(\ell)=a(\ell+1)=d-3$.

Therefore

$$i + (s-1)d + d - i - 2 = sd - 2 = q - 1,$$

and we get

$$\mathscr{C}^n(f^s x^{d-i-2} dx) = s(a_d^{s-1} a_i)^{1/q} dx = 0.$$

This implies $a_i = 0$ since s is prime to p by (4.24). Hence $f(x)$ must be of the form (the case $d = 2$ is trivial)

$$f(x) = ax^d + b \qquad \text{with } d \text{ a divisor of } q+1.$$

Now if the curve is maximal, from Proposition 4.28 we know that $tr(b) = 0$ and $a^v = (-1)^u$ where $u = (q+1)/d$ and $v = (q^2-1)/d$. By Hilbert's 90 Theorem, there exists $\gamma \in \mathbb{F}_{q^2}$ such that $\gamma^q - \gamma = b$ and by changing variable $y \to y + \gamma$ we can assume $b = 0$.

Now we have two cases:

Case u is even. In this case $a^v = 1$ and hence $a = c^d$ for some $c \in \mathbb{F}_{q^2}^*$. Changing variable $x \to c^{-1}x$ we have

$$y^q - y = x^d \quad \text{with} \quad d \mid q+1.$$

Take $\alpha \in \mathbb{F}_{q^2}$ with $\alpha^{q-1} = -1$. Substituting $y \to \alpha^{-1}.y$ we have $y^q + y = \alpha x^d$. Again here $\alpha^v = \alpha^{(q-1)u} = (-1)^u = 1$ and hence $\alpha = \theta^d$ for some element $\theta \in \mathbb{F}_{q^2}^*$ and we conclude that the curve is isomorphic to $y^q + y = x^d$.

Case u is odd. In this case $a^v = -1$ and hence $(-a^{q-1})^u = 1$. So $-a^{q-1} = \beta^{d(q-1)}$ for some $\beta \in \mathbb{F}_{q^2}^*$. Set $\mu := a\beta^{-d}$, then $\mu^{q-1} = -1$. Now by changing variables $x \to \beta^{-1}x$ and $y \to -\mu y$ we have that the curve $\mathcal{C}$ is equivalent to

$$y^q + y = x^d \quad \text{with} \quad d \mid q+1. \ \blacksquare$$

degree q and where f(x) is an admissible rational function in

Remark 4.31. Most of the arguments in the proof above just uses the property $\mathscr{C}^n = 0$. We then have that the hypothesis that d divides $q+1$ in Proposition 4.28 is superfluous. We also get that all maximal curves over $\mathbb{F}_{q^2}$ given by $y^q - y = f(x)$ as in Theorem 4.30 are covered by the Hermitian curve.

We can also classify minimal Artin-Schreier curves over $\mathbb{F}_{q^2}$ as bellow:

Theorem 4.32. *Let $\mathcal{C}$ be a curve defined by the equation $y^q - y = f(x)$, where $f(x) \in \mathbb{F}_{q^2}[x]$ has degree prime to p and $p \neq 2$. If $\mathcal{C}$ is minimal over $\mathbb{F}_{q^2}$ and $g(\mathcal{C}) \neq 0$, then $\mathcal{C}$ is equivalent to the projective curve defined by the equation*

$$y^q - y = ax^2 \quad \textit{where} \quad a \in \mathbb{F}_{q^2},\ a \neq 0, \quad \textit{and it satisfies} \quad a^{\frac{q^2-1}{2}} \neq (-1)^{\frac{q+1}{2}}.$$

Proof. We know that if a curve is minimal over $\mathbb{F}_{q^2}$, with $q = p^n$, then again the operator $\mathscr{C}^n$ is zero. So by the proof of the above theorem, the curve can be defined by $y^q - y = ax^d + b$ where d is a divisor of $q+1$. Now we can use again Proposition 4.28; it yields $d = 2$, $tr(b) = 0$ and $a^{\frac{q^2-1}{2}} \neq (-1)^{\frac{q+1}{2}}$. ■

Remark 4.33. Consider a maximal curve over $k = \mathbb{F}_{q^2}$ given by $A(y) = f(x)$, where $A(y)$ is an additive separable polynomial in $k[y]$ of degree q and where $f(x)$ is an admissible rational function in $k(x)$. From Remark 3.14 we can assume that $f(x)$ is a polynomial in $k[x]$ and from Theorem 3.15 we have that all roots of $A(y)$ belong to k. As now follows from Proposition 1.1 of [13], we can assume that $A(y) = y^q - y$. Hence we are in the situation of Theorem 4.30.

Remark 4.34. In the above theorem, if $q \equiv 1 \pmod 4$, then changing variable $x \to \alpha^{-1}x$, where $a = \alpha^2$, the minimal curve $\mathcal{C}$ is equivalent to

$$y^q - y = x^2.$$

Clearly, this last curve is maximal over $\mathbb{F}_{q^2}$ if $q \equiv 3 \pmod 4$.

Let $\pi : \mathcal{C} \to \mathcal{D}$ be a $p-$cyclic covering of projective nonsingular curves over the algebraic closure $\bar{k}$. Then we have the so-called Deuring-Shafarevich formula:

$$\sigma(\mathcal{C}) - 1 + r = p(\sigma(\mathcal{D}) - 1 + r), \tag{4.25}$$

where r is the number of ramification points of the covering π.

Corollary 4.35. *Let $\mathcal{C}$ be a curve defined over $k = \mathbb{F}_{p^2}$ such that there exists*

$$\mathcal{C} \to \mathbb{P}^1$$

a cyclic covering of degree p which also defined over k. If the curve $\mathcal{C}$ is maximal over $\mathbb{F}_{p^2}$, then $\mathcal{C}$ is isomorphic to the curve given by the affine equation $y^p + y = x^d$, where d divides $p + 1$.

Proof. From Remark 4.27 we can assume that the curve $\mathcal{C}$ is given by :

$$y^p - y = f(x),$$

where every pole of $f(x)$ in $\bar{k}$ occurs with a multiplicity relatively prime to the characteristic p. Now if the curve $\mathcal{C}$ is maximal, then according to Corollary 2.59 we know that $\sigma(\mathcal{C}) = 0$. Note that from Formula (4.25) we must have $r = 1$ and we can put this unique ramification point at infinity, and hence we can assume that $f(x)$ is a polynomial. The result now follows from Theorem 4.30. ■

4.2.3 Hyperelliptic Curves

Let $k = \mathbb{F}_{q^2}$ be a finite field of characteristic $p > 2$. Let $\mathcal{C}$ be a projective nonsingular hyperelliptic curve over k of genus g. Then $\mathcal{C}$ can be defined by an affine equation of

the form

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

where $f(x)$ is a polynomial over k of degree $2g+1$, without multiple roots. If $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$ then by Corollary 4.8 we have an upper bound on the genus, namely

$$g(\mathcal{C}) \leq \frac{q-1}{2}.$$

In the following theorem we establish a characterization of maximal hyperelliptic curves that attain this upper bound.

Theorem 4.36. *There is a unique maximal hyperelliptic curve over $\mathbb{F}_{q^2}$ with genus $g = (q-1)/2$. It can be given by the affine equation*

$$y^2 = x^q + x.$$

Before proving this theorem, we need to explain how the matrix associated to $\mathscr{C}^n$, where $q = p^n$, is determined from $f(x)$. It is remarkable that the Hasse-Witt matrix of hyperelliptic curves determined completely in [55].

The differential 1-forms of the first kind on $\mathcal{C}$ form a $k-$vector space $H^0(\mathcal{C}, \Omega^1)$ of dimension g with basis

$$\mathcal{B} = \{\omega_i = \frac{x^{i-1}dx}{y}, \;\; i = 1, \ldots, g\}.$$

The images under the operator $\mathscr{C}^n$ are determined in the following way. Rewrite

$$\omega_i = \frac{x^{i-1}dx}{y} = x^{i-1}y^{-q}y^{q-1}dx = y^{-q}x^{i-1}\sum_{j=0}^{N} c_j x^j dx,$$

where the coefficients $c_j \in k$ are obtained from the expansion

$$y^{q-1} = f(x)^{(q-1)/2} = \sum_{j=0}^{N} c_j x^j \qquad \text{with } N = \frac{q-1}{2}(2g+1).$$

Then we get for $i = 1, \ldots, g$,

$$\omega_i = y^{-q}\Big(\sum_{\substack{j \\ i+j \neq 0 \ mod \ q}} c_j x^{i+j-1} dx \Big) + \sum_{l} c_{(l+1)q-i} \ \frac{x^{(l+1)q}}{y^q} \frac{dx}{x}.$$

Note here that $0 \leq l \leq \frac{N+i}{q} - 1 < g - \frac{1}{2}$. On the other hand, we know from Remark 2.52 that if $\mathscr{C}^n(x^{r-1}dx) \neq 0$ then $r \equiv 0 \pmod{q}$. Thus we have

$$\mathscr{C}^n(\omega_i) = \sum_{l=0}^{g-1} \left(c_{(l+1)q-i}\right)^{1/q} . \frac{x^l}{y} dx.$$

If we write $\omega = (\omega_1, \ldots, \omega_g)$ as a row vector we have

$$\mathscr{C}^n(\omega) = \omega A^{(1/q)},$$

where A is the $(g \times g)$ matrix with elements in k given as

$$A = \begin{pmatrix} c_{q-1} & c_{q-2} & \cdots & c_{q-g} \\ c_{2q-1} & c_{2q-2} & \cdots & c_{2q-g} \\ \vdots & \cdots & \cdots & \vdots \\ c_{gq-1} & c_{gq-2} & \cdots & c_{gq-g} \end{pmatrix}.$$

Remark 4.37. In [50] the author find a characterization for hyperelliptic curves defined over an algebraically closed field whose Hasse-Witt matrix is zero. Here we use his idea to find hyperelliptic curves with nilpotent Cartier operator.

Proof of Theorem 6.1. Let $\mathcal{C}$ be a hyperelliptic curve of genus given by $g =$

$(q-1)/2$. Then the curve $\mathcal{C}$ can be defined by the equation $y^2 = f(x)$, with a square-free polynomial

$$f(x) = a_q x^q + a_{q-1}x^{q-1} + \ldots + a_1 x + a_0 \in \mathbb{F}_{q^2}[x] \text{ and } a_q \neq 0.$$

As $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$, then $\mathcal{C}$ has $1 + q^2 + q(q-1)$ rational points. On the other hand if we consider $\mathcal{C}$ as a double cover of $\mathbb{P}^1$, the ramification points are the roots of $f(x)$ and the point at infinity. As the point at infinity is a rational point and $1 + q^2 + q(q-1)$ is an even number, we have that $f(x)$ must have an odd number of rational roots. Hence $f(x)$ has at least one rational root in $\mathbb{F}_{q^2}$, denote it by θ. Now by substituting $x + \theta$ for x, we can assume that $\mathcal{C}$ is defined by the equation $y^2 = f(x)$ with $f(0) = 0$. We then write

$$f(x) = a_q x^q + a_{q-1}x^{q-1} + \ldots + a_1 x \in \mathbb{F}_{q^2}[x] \text{ and } a_1 a_q \neq 0.$$

Now as the curve $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$, with $q = p^n$ for some integer n, then $\mathscr{C}^n = 0$. So the above matrix A is the zero matrix. Hence looking at the last row of A, we have

$$c_{gq-1} = c_{gq-2} = \ldots = c_{gq-g} = 0.$$

We will show by induction that this means

$$a_{q-1} = a_{q-2} = \ldots = a_{q-g} = 0.$$

First we observe that

$$c_{gq-1} = g.{a_q}^{g-1} a_{q-1}.$$

So $c_{gq-1} = 0$ implies $a_{q-1} = 0$. Now assume $a_{q-i} = 0$, for all $1 \leq i < m \leq g$. We want to show then that $a_{q-m} = 0$. Under the assumption above, we have that $f(x)$ reduces

to

$$f(x) = a_q x^q + a_{q-m} x^{q-m} + \ldots + a_1 x.$$

We will then have that $c_{gq-m} = g.a_q^{g-1} a_{q-m}$. So $c_{gq-m} = 0$ implies that $a_{q-m} = 0$. By induction, we have shown that the polynomial $f(x)$ reduces to

$$f(x) = a_q x^q + a_g x^g + \ldots + a_2 x^2 + a_1 x.$$

Now we want to show that $a_t = 0$ for all $2 \leq t \leq g$. Looking at the first row of the matrix A, we have

$$c_{q-1} = c_{q-2} = \ldots = c_{g+1} = 0.$$

By induction we can show that this means

$$a_2 = a_3 = \ldots = a_g = 0.$$

In fact, we first observe that $c_{g+1} = g{a_1}^{g-1} a_2$. Because $a_1 \neq 0$, $c_{g+1} = 0$ implies $a_2 = 0$. Now assume that $a_i = 0$ for all i with $2 \leq i < m \leq g$. We want to show that $a_m = 0$. Under this assumption, we have that $f(x)$ is :

$$f(x) = a_q x^q + a_g x^g + \ldots + a_m x^m + a_1 x.$$

We will then have that $c_{g-1+m} = g.{a_1}^{g-1} a_m$. Again because $a_1 \neq 0$, we have that $c_{g-1+m} = 0$ implies $a_m = 0$. Thus by induction we have shown that the polynomial $f(x)$ must be of the form

$$f(x) = a_q x^q + a_1 x \qquad \text{with } a_1.a_q \neq 0.$$

Now we can write the equation of the curve $\mathcal{C}$ as below:

$$x^q + \mu x = \lambda y^2 \quad \text{for some} \quad \mu, \lambda \in \mathbb{F}_{q^2}^*.$$

As the curve $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$, one can show easily that the additive polynomial $A(x) := x^q + \mu x$ has at least a nonzero root $\beta \in \mathbb{F}_{q^2}^*$. In fact more holds; it follows from [18, Theorem 4.3] that all roots of $A(x)$ belong to $\mathbb{F}_{q^2}$.

Set $\alpha := \beta^q$ and $x_1 = \alpha x$, then

$$A(x) = \alpha^{-q}(\alpha x)^q + (\mu\alpha^{-1})(\alpha x).$$

Hence

$$A(x) = \alpha^{-q}((x_1)^q + \mu\alpha^{q-1}x_1)$$

has the root $x_1 = \alpha\beta = \beta^{q+1} \in \mathbb{F}_q^*$. So $\mu\alpha^{q-1} = -1$, and this means that the curve $\mathcal{C}$ is equivalent to the curve given by the equation

$$x_1^q - x_1 = ay^2, \quad \text{where} \quad a := \alpha^q\lambda.$$

Now as we have seen at the end of the proof of Theorem 4.30, this curve is isomorphic to the curve given by the equation

$$y^2 = x^q + x. \ \blacksquare$$

Remark 4.38. Suppose that $y^2 = f(x)$, with $f(x) \in \mathbb{F}_{q^2}[x]$ a square-free polynomial having $\deg f(x) = q = p^n$ and with p an odd prime, is the equation of a minimal curve $\mathcal{C}$ over $\mathbb{F}_{q^2}$. Then we have

$$\#\mathcal{C}(\mathbb{F}_{q^2}) = q^2 + 1 - (q-1)q = q + 1$$

and in particular $\#\mathcal{C}(\mathbb{F}_{q^2})$ is an even natural number. As in the proof of Theorem 4.36 we can assume that $f(0) = 0$, and from $\mathscr{C}^n = 0$ we then conclude that it holds

$$f(x) = a_q x^q + a_1 x \qquad \text{with} \quad a_1 a_q \neq 0.$$

Hence the minimal curve $\mathcal{C}$ can be defined by

$$x^q + \mu x = \lambda y^2, \qquad \text{for some} \quad \mu, \lambda \in \mathbb{F}_{q^2}^*.$$

The polynomial $A(x) = x^q + \mu x$ must have a nonzero root in $\mathbb{F}_{q^2}$; otherwise the map sending x to $A(x)$ would be an additive automorphism of $\mathbb{F}_{q^2}$ and hence the cardinality of rational points would satisfy

$$\#\mathcal{C}(\mathbb{F}_{q^2}) = 1 + q^2.$$

We then conclude, as in the proof of Theorem 4.36, that the curve $\mathcal{C}$ can be given by the equation

$$x_1^q - x_1 = a y^2, \qquad \text{with} \quad a \in \mathbb{F}_{q^2}^*.$$

It now follows from Proposition 4.28 that

$$a^v \neq (-1)^u \qquad \text{with } u = \frac{q+1}{2} \text{ and } v = \frac{q^2-1}{2}.$$

Remark 4.39. An analogous result to Theorem 4.36 holds in the case of characteristic $p = 2$; i.e., if $p = 2$ then the curve given by $y2 + y = x^{q+1}$ is the unique maximal hyperelliptic curve over $k = \mathbb{F}_{q^2}$ with genus $g = q/2$. In fact with arguments as in the proof of Corollary 4.35, we get that the curve can be given by $y^2 + y = f(x)$ with $f(x)$ a polynomial in $k[x]$ of degree $q + 1$. The result now follows from Theorem 2.3 of [12].

4.2.4 Serre Maximal Curves

In this section we consider curves $\mathcal{C}$ that attain the Serre upper bound and we call them *SW− maximal curves*; i.e., it holds that

$$\#\mathcal{C}(\mathbb{F}_q) = q + 1 + [2\sqrt{q}].g(\mathcal{C}).$$

Proposition 4.40. *Let k be a field with q elements and denote by $m = [2\sqrt{q}]$. For a smooth projective curve $\mathcal{C}$ of genus g defined over $k = \mathbb{F}_q$, the following conditions are equivalent:*

- *The curve $\mathcal{C}$ is SW−maximal.*
- *The L− polynomial of $\mathcal{C}$ satisfies $L(t) = (1 + mt + qt^2)^g$.*

Proof. See [31] and [43, page 180]. ■

Corollary 4.41. *Let $\mathcal{C}$ be a smooth projective curve of genus g defined over $k = \mathbb{F}_q$ which attains the Serre bound. Then its Hasse-Witt invariant satisfies*

$$\sigma(\mathcal{C}) = \begin{cases} g & \text{if} \quad gcd(p, m) = 1 \\ 0 & \text{if} \quad p \mid m \end{cases}$$

Proof. Since $\mathcal{C}$ is SW-maximal, from Proposition 4.40 we have

$$\begin{aligned} L(t) &= (1 + mt + qt^2)^g \\ &= 1 + \textstyle\sum_{i=1}^{g} \binom{g}{i} t^i (m + qt)^i \\ &= 1 + \textstyle\sum_{i=1}^{g} \binom{g}{i} t^i (\sum_{j=0}^{i} \binom{i}{j} m^{i-j} q^j t^j). \end{aligned}$$

If p divides m, then it is clear from Proposition 2.54 that $\sigma(\mathcal{C}) = 0$. Now suppose that $\gcd(p, m) = 1$. We have to show that the coefficient of t^g in the L-polynomial $L(t)$ is not divisible by p. Denote it by a_g.

From the last equality above, we then obtain

$$a_g \equiv m^g \pmod{p}. \blacksquare$$

We recall that an admissible rational function $f(x) \in k(x)$ is such that every pole of $f(x)$ in the algebraic closure $\bar{k}$ occurs with a multiplicity prime to the characteristic p. We then have:

Theorem 4.42. *Let $\mathcal{C}$ be a SW-maximal curve over $\mathbb{F}_q$ given by an affine equation of the form*

$$A(y) = f(x), \tag{4.26}$$

where $A(y) \in \mathbb{F}_q[y]$ is an additive and separable polynomial and where $f(x)$ is an admissible rational function. Denote by $m = [2\sqrt{q}]$ and suppose that $gcd(p, m) = 1$. Then all poles of $f(x)$ are simple poles.

Proof. We know that a curve $\mathcal{C}$ given by (4.26) is ordinary if and only if the rational function $f(x)$ has only simple poles (see [48, Corollary 1]). Thus Theorem 4.42 follows directly from Corollary 4.41 . $\blacksquare$

Corollary 4.43. *Let $\mathcal{C}$ be a SW-maximal curve as in the above theorem. Then $g(\mathcal{C}) = (degA - 1)(s - 1)$ where s denotes the number of poles of $f(x)$.*

We finish with two examples of SW-maximal Artin-Schreier curves:

Example 4.44. Let $k = \mathbb{F}_2$. So $m = [2\sqrt{2}] = 2$ and p divides m. Let $\mathcal{C}$ be the elliptic curve over $\mathbb{F}_2$, given by the affine equation

$$y^2 + y = x^3 + x.$$

One can see easily that $\mathcal{C}$ has five $k-$rational points which means that $\mathcal{C}$ is SW-maximal over k. Note that $f(x) = x^3 + x$ has a pole of order 3 at infinity.

Example 4.45. Let $k = \mathbb{F}_8$. So $m = [2\sqrt{8}] = 5$ and $\gcd(p, m) = 1$. Let $\mathcal{C}$ be the elliptic curve over $\mathbb{F}_8$, given by the affine equation

$$y^2 + y = \frac{x^2 + x + 1}{x}.$$

Then the curve $\mathcal{C}$ is SW-maximal since $\mathcal{C}$ has 14 $k-$rational points. In fact the two simple poles of $(x^2 + x + 1)/x$ are totally ramified in the extension $k(x, y)/k(x)$ and they correspond to two $k-$rational points on $\mathcal{C}$. By Hilbert 90 Theorem, we have

$$\#\mathcal{C}(\mathbb{F}_8) = 2 + 2B,$$

where $B := \#\{\alpha \in \mathbb{F}_8 \mid tr_{\mathbb{F}_8|\mathbb{F}_2}(\frac{\alpha^2+\alpha+1}{\alpha}) = 0\}$. But one can show that $B = 6$; in fact the points $x = \alpha \in \mathbb{F}_8 \setminus \mathbb{F}_2$ are completely splitting in $k(x, y)/k(x)$.

Bibliography

[1] A. Aguglia, G. Korchmáros and F. Torres, Plane maximal curves, *Acta Arith.* **98** (2001), 165-179.

[2] T. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag.

[3] M. Abdón, A. Garcia, On a characterization of certain maximal curves, *Finite Fields Appl.* **10** (2004), 133-158.

[4] Y. Aubry, M. Perret, Divisibility of zeta functions of curves in a covering. *Arch. Math.***82** (2004), 205-213.

[5] P. Berthelot, Slopes of Frobenius in crystalline cohomology, In: *Algebraic Geometry* (Arcata 1974), Proceedings of symposia in pure mathematics, **29**, 315-328.

[6] G. Cornell, J. H. Silverman, *Arithmetic Geometry*, Springer-Verlag, 1985.

[7] A. Cossidente, G. Korchmáros, F. Torres, Curves of large genus covered by the Hermitian curve, *Comm. Algebra* **28** (2000), 4707–4728.

[8] H. Davenport, H. Hasse, Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen, *J. Reine Angew. Math.* **172** (1934), 151-182.

[9] T. Ekedahl, On supersingular curves and abelian varieties, *Math. Scand.* **60**(1987), 151-178.

[10] R. Fuhrmann, F. Torres, On Weierstrass points and optimal curves. *Rend. Circ. Mat. Palermo* Suppl. **51** (1998), 25-46.

[11] A. Garcia, M.Q. Kawakita, S. Miura, On certain subcovers of the Hermitian curve, *Comm. Algebra* **34** (2006), 973-982.

[12] A. Garcia, F. Özbudak, Some maximal function fields and additive polynomials, *Comm. Algebra* **35** (2007), 1553-1566.

[13] A. Garcia, H. Stichtenoth, Elementary abelian p-extensions of algebraic function fields, *Manuscripta Math.* **72** (1991), 67-79.

[14] A. Garcia, H. Stichtenoth, A maximal curve which is not a Galois subcover of the Hermitian curve, *Bull. Braz. Math. Soc.* (N.S.) **37** (2006), 139–152.

[15] A. Garcia, H. Stichtenoth, C.P. Xing, On subfields of Hermitian function fields, *Composito Math.* **120** (2000), 137-170.

[16] A. Garcia, S. Tafazolian, On additive polynomial and certain maximal curves, Preprint, available at www.impa.br .

[17] A. Garcia, S. Tafazolian, Certain maximal curves and Cartier operator, Preprint, available at www.impa.br .

[18] A. Garcia, F. Torres, On unramified coverings of maximal curves, to appear in *Proceedings AGCT-10,* held at CIRM-Marseille in September 2005.

[19] M. Giulietti, G. Korchmáros, A new family of maximal curves over a finite field, Preprint, 2007.

[20] V. D. Goppa, *Geometry and Codes*, Mathematics and its applications, 24, Kluwer Academic Publishers, Dordrecht-Boston-London (1988).

[21] M. J. Greenberg, *Lectures on Forms in Many Variables*, W. A. Benjamin, Inc., New York-Amsterdam 1969.

[22] A. Grothendieck, Sur une note de Mattuck-Tate, *J. Reine Angew. Math.* **200** (1958), 208-215.

[23] R. Hartshorne, Ample vector bundles on curves, *Nagoya Math. J.* **43** (1943), 73-89.

[24] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, Berlin, 1977.

[25] H. Hasse, Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper, *J. Reine Angew. Math.* **172** (1934), 37-54.

[26] H. Hasse, E. Witt, Zyklische unverzweigte Erweiterungskörper vom Primzahlgrade p über einen algebraischen Funktionenkörper der Charakteristik p, *Monatsh. Math.* **43** (1936), 477-492.

[27] Y. Ihara, Some remarks on the number of rational points of algebraic curves over finite fields, *J.Fac. Sci. Tokyo* **28** (1981), 721-724.

[28] P. Irokawo, R. Sasaki, A remark on Artin-Schreier curves whose Hass-Witt maps are the zero maps, *Tsubuka J. Math.* **1** (1991), 185-192.

[29] N. Koblitz, p-adic variation of the zeta-function over families of varieties defined over finite fields, *Compositio Math.* **31** (1975), 119–218.

[30] T. Kodama, T. Washio, Hasse-Witt Matrices of Fermat curves. *Manuscripta Math.* **60**, (1988) 185-195.

[31] G. Lachaud, Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis, *C.R. Acad. Sci.Paris* **305** (1987), 729-732.

[32] S. Lang, *Abelian Varieties*, Interscience, New York, 1959.

[33] S. Lang, *Elliptic Functions*, Addision-Wesley Publishing Company, 1973.

[34] R. Lidl, H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, 1997.

[35] M. Moisio, A construction of a class of maximal Kummer curves, *Finite Fields Appl.* **11** (2005), 667–673.

[36] P. Morandli, *Fields and Galois Theory*, Graduate Texts in Mathematics, **167**. Springer-Verlag, New York (1996).

[37] N.O. Nygaard, Slopes of powers of Frobenius on crystalline cohomology, *Ann. Sci. cole Norm. Sup.* **14** (1981), 369-401 (1982).

[38] O. Ore, On a special class of polynomials, *Trans. Amer. Math. Soc.* **35** (1933), 559-584.

[39] H-G. Rück, H. Stichtenoth, A characterization of Hermitian function fields over finite fields, *J. Reine Angew. Math.* **457** (1994), 185-188.

[40] J.P. Serre, Sur la topologie des varits algbriques en caractristique p, Symposium internacional de topologa algebraica International symposium on algebraic topology (1958), 24-53.

[41] J.P. Serre, Qualques propriétés des Variétés abéliénnes en caracteristique p, *Amer. J. Math.* **80** (1958), 715-739.

[42] J.P. Serre, *Algebraic Groups and Class Fields*, Springer, 1997.

[43] H. Stichtenoth, *Algebraic function fields and codes*, Springer-Verlag, Berlin, 1993.

[44] H. Stichtenoth, Die Hasse-Witt-Invariante eines Kongruenzfunktionenkörpers. *Arch. Math.* **33**(1979/80), 357-360.

[45] H. Stichtenoth, C. Xing, On the structure of the divisor class group of a class of curves over finite fields, *Arch. Math.* **65** (1995), 141-150.

[46] K.O. Stöhr, P. Viana, A study of Hasse-Witt matrices by local methods, *Math. Z.* **200** (1989), 397-407.

[47] D. Subrao, The p-rank of Artin-Schreier curves, *Manuscripta Math.* **16** (1975), 169-193.

[48] F.J. Sullivan, p-torsion in the class group of curves with too many automorphisms, *Arch. Math.* **26** (1975), 253-261.

[49] J. Tate, Endomorphisms of abelian varieties over finite fields, *Invent. Math.* **2** (1966), 134-144.

[50] R.C. Valentini, Hyperelliptic curves with zero Hasse-Witt matrix, *Manuscripta Math.* **86** (1995), 185-194.

[51] L. C. Washington, *Introduction to cyclotomic fields*, Springer-Verlag, Berlin-Heidelberg-New York, 1982.

[52] A. Weil, *Courbes algébriques et variétés abeliennes*, Hermann, Paris, (1971).

[53] A. Weil, Number of solutions of equations in finite fields, *Bull. A. M. S.* **55** (1949), 497-508.

[54] J. Wolfmann, The number of points on certain algebraic curves over finite fields, *Comm. Algebra* **17** (1989), 2055–2060.

[55] N. Yui, On the Jacobian varieties of hyperelliptic curves over fields of characteristic $p > 2$, *J. Algebra* **52** (1978), 378-410.

[56] N. Yui, On the Jacobian variety of the Fermat curve, *J. Algebra* **65** (1980), 1-35.

[57] H.J. Zhu, p-adic variation of L functions of one variable exponential sums. I, *Amer. J. Math.* **125** (2003), 669-690.