Certain maximal curves and Cartier operators *

by

Arnaldo Garcia[†]**and Saeed Tafazolian**

(IMPA at Rio de Janeiro)

1 Introduction

More than half a century ago, André Weil proved a formula for the number $N = \#\mathcal{C}(\mathbb{F}_q)$ of rational points on a smooth geometrically irreducible projective curve $\mathcal{C}$ of genus g defined over a finite field $\mathbb{F}_q$. This formula provides upper and lower bounds on the number of rational points possible. It states that:

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

In general, this bound is sharp. In fact if q is a square, there exist several curves that attain the above upper bound (see [4], [5], [14] and [23]). We say a curve is *maximal* (resp. *minimal*) if it attains the above upper (resp. lower) bound.

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 (see [17, Section V.3]):

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

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

Ihara showed that if a curve $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$ then its genus satisfies

$$g \leq \frac{q^2 - q}{2}. \tag{1.1}$$

---

* *2000 Mathematics Subject Classification*: 11G20, 11M38, 14G15, 14H25. ***Keywords:*** finite fields, maximal curves, genus, Hasse-Witt invariant, Cartier operator, Fermat curves, Artin-Schreier curves, hyperelliptic curves.

[†] A. Garcia was partially supported by a grant from CNPq-Brazil (# 307569/2006-3).

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 [14])

$$y^q + y = x^{q+1}. \tag{1.2}$$

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

In this paper, we consider maximal (and also minimal) curves over a finite field with q^2 elements. We give a characterization of certain maximal and minimal curves of types: Fermat, Artin-Schreier or hyperelliptic. The main tool is the Cartier operator, which is a nilpotent operator in the case of maximal (or minimal) curves over finite fields. We give generalizations of results from [1], [7], [9], [22] and [23].

In Section 2 we review some important properties of these curves. Of special interest is Proposition 2.9 which is used to prove in Section 3 that $\mathscr{C}^n = 0$ for a maximal or a minimal curve over $\mathbb{F}_{q^2}$ with $q = p^n$, where $\mathscr{C}$ denotes the Cartier operator (see Theorem 3.3). In Section 4 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 [9, Corollary 1] which deals with the case $q = p$ prime (see Remark 4.3).

In Section 5 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 5.4). In particular this result shows that the hypothesis d is a divisor of $q+1$ in Proposition 5.2 is superfluous and that the maximal curves $\mathcal{C}$ in Theorem 5.4 are covered by the Hermitian curve over $\mathbb{F}_{q^2}$ given by Equation (1.2) (see Remark 5.5). The main ideas here come from [7] which deals with the case $q = p$ prime. In Section 6 we deal with maximal 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 we 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 given by $g = (q-1)/2$ (see Theorem 6.1). The main ideas here come from [22] which deals with hyperelliptic curves with zero Hasse-Witt matrix (see Remark 6.2).

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

2 Maximal curves

In this section we review some well-known properties of maximal curves.

Let $\mathcal{C}$ be a curve of genus $g > 0$ over the finite field $k = \mathbb{F}_q$ with q elements. The *zeta function* of $\mathcal{C}$ is a rational function of the form

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

where $L(t) \in \mathbb{Z}[t]$ is a polynomial of degree $2g$ with integral coefficients. We call this polynomial the $L-$*polynomial* of $\mathcal{C}$ over k.

Let K/k be the function field of $\mathcal{C}$ over k. Then the divisor class group $C^0(K)$ is finite and it is isomorphic to the group of $k-$rational points of the Jacobian $\mathcal{J}$ of $\mathcal{C}$,

$$C^0(K) = \mathcal{J}(k).$$

It is well-known that the class number $h = \text{ord}\ (C^0(K))$ of K/k is given by $h = L(1)$. We have that

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

where $a_{2g-i} = q^{g-i}a_i$, for $i = 1, \ldots, g$, and moreover the α_i's are complex numbers with absolute value $\mid \alpha_i \mid = \sqrt{q}$ for $1 \leqslant i \leqslant 2g$.

We recall the following fact about maximal curves (see [21]):

Proposition 2.1. *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(minimal, respectively)*
- $L(t) = (1+\sqrt{q}t)^{2g}$ ($L(t) = (1-\sqrt{q}t)^{2g}$, *respectively)*
- *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.*

Remark 2.2. As J. P. Serre has shown, 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 [10]). So one way to construct explicit maximal curves is to find equations for subcovers of the Hermitian curve (see [1] and [4]).

Let $h(t) = t^{2g}L(t^{-1})$. Then $h(t)$ is the *characteristic polynomial* of the Frobenius action on the Jacobian variety $\mathcal{J}/k$.

Definition. 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 [16]):

Proposition 2.3. *Let $\mathcal{C}$ be a curve defined over $k = \mathbb{F}_q$. If $L-$polynomial is $L = 1 + a_1t + \ldots + a_{2g-1}t^{2g-1} + q^g t^{2g}$, then the Hasse-Witt invariant satisfies*

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

Remark 2.4. Since $a_{2g-i} = q^{g-i}a_i,\ i = 0, 1, \ldots, g$, then $0 \leq \sigma(\mathcal{C}) \leq g$. If $\sigma(\mathcal{C}) = g$ the curve is called *ordinary.*

Corollary 2.5. *If a curve $\mathcal{C}$ is maximal (or minimal) over a finite field, then the Hasse-Witt invariant satisfies $\sigma(\mathcal{C}) = 0$.*

Proof. It follows from the above proposition and Proposition 2.1. ■

Remark 2.6. In fact, the p-rank of an abelian variety is equal to the number of zero slopes in its $p-$adic Newton polygon and this number is not bigger than the dimension. So in general we have $0 \leqslant \sigma(\mathcal{C}) \leqslant g(\mathcal{C})$. From Proposition 2.1 a maximal (or minimal) curve $\mathcal{C}$ is supersingular, so all slopes of its Newton polygon are equal to 1/2. On the other hand if a curve $\mathcal{C}$ defined over a finite field $k = \mathbb{F}_q$ is supersingular, then $\mathcal{C}$ is minimal over some finite extension of k (see [18, Proposition 1]). For additional information about Newton polygon, see [12].

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

$$\prod_{i=1}^{T} h_i(\mathscr{F}) = 0 \quad \text{on} \quad \mathcal{J}. \tag{2.1}$$

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. [21, Theorem 2] and [11, VI, Section 3]). In the case of a maximal curve over $\mathbb{F}_{q^2}$, we have $h(t) = (t + q)^{2g}$. Therefore from (2.1) we obtain the following result, which is contained in the proof of [14, Lemma 1].

Lemma 2.7. *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 2.8. 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.

The following proposition is crucial for us (see [2, Proposition 1.2]):

Proposition 2.9. *Let $\mathcal{A}$ be an abelian variety defined over $\mathbb{F}_{q^2}$, where $q = p^n$. If the Frobenius $\mathscr{F}$ relative to $\mathbb{F}_{q^2}$ acts on the abelian variety $\mathcal{A}$ as multiplication by $\pm q$, then we have that $\mathscr{F}^n = 0$.*

3 Cartier Operator

Let $\mathcal{C}$ be a curve defined over a perfect field k of characteristic $p > 0$. Let Ω^1 be the sheaf of differential 1-forms on $\mathcal{C}$. Then there exists a unique operation,

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

the so-called *Cartier operator*, such that

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

(ii) $\mathscr{C}$ vanishes on exact differentials; i.e., $\mathscr{C}(df) = 0$,

(iii) $\mathscr{C}(f^{p-1}df) = df$,

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

Remark 3.1. Moreover for a given natural number n, one can easily show that

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

We mention here the following theorem of Hasse-Witt ([6]):

Theorem 3.2. *Let V be a finite dimensional vector space over an algebraically closed field of characteristic $p > 0$. Let $\psi : V \to V$ be a $1/p-$linear map. Then there are two subspaces V^s and V^0 satisfying the following conditions:*

- *V^s is spanned by ψ invariant elements.*
- *Each y in V^0 is killed by an iterate of ψ.*
- *$V = V^s \oplus V^0$.*

Definition. For a basis $\omega_1, \ldots, \omega_g$ of $H^0(\mathcal{C}, \Omega^1)$ 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* $\mathscr{A}(\mathcal{C})$ is obtained by taking $p-$th roots, i.e., we have

$$\mathscr{A}(\mathcal{C}) = (a_{ij}^{1/p}).$$

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

$$(a_{ij}^{1/p^{n-1}}). \ldots .(a_{ij}^{1/p^2}).(a_{ij}^{1/p}).(a_{ij}).$$

We denote by $\mathscr{A}(\mathcal{C})^{[n]}$ the $p-$th root of the matrix above that represents the iterated Cartier operator $\mathscr{C}^n$.

Theorem 3.3. *Let $\mathcal{C}$ be an algebraic curve defined over a finite field with q^2 elements, where $q = p^n$ for some $n \in \mathbb{N}$. If the curve $\mathcal{C}$ is maximal (or minimal) over $\mathbb{F}_{q^2}$, then we have that $\mathscr{C}^n = 0$.*

Proof. From Lemma 2.7 we know that the Frobenius acting on the Tate module of the Jacobian of $\mathcal{C}$ acts as the multiplication by $\pm q$. Then one may apply Proposition 2.9 to conclude that $\mathscr{F}^n = 0$. Finally, since the Cartier operator acting on $H^0(\mathcal{C}, \Omega^1)$ is dual to the Frobenius acting on $H^1(\mathcal{C}, \mathscr{O}_\mathcal{C})$ by the Serre duality, one obtains also that $\mathscr{C}^n = 0$. ■

The next result (see [19, Corollary 2.7]) relates the Hasse-Witt matrix and the Weierstrass gap sequence at a rational point.

Proposition 3.4. *Let $\mathcal{C}$ be a curve defined over a perfect field and $n \in \mathbb{N}$. Let $\mathscr{A}(\mathcal{C})$ denote the Hasse-Witt matrix of the curve $\mathcal{C}$. If P is a rational point on $\mathcal{C}$, then the rank of $\mathscr{A}(\mathcal{C})^{[n]}$ is larger than or equal to the number of gaps at P divisible by p^n.*

Corollary 3.5. *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 3.3 we have $\mathscr{A}(\mathcal{C})^{[n]} = 0$. Thus the result follows from Proposition 3.4. ■

Corollary 3.6. *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 3.4. ■

Remark 3.7. 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 [13, Theorem 4.1]). Now by Theorem 1.1 of [2] 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 $(p, g) \neq (2, 1)$.

4 Fermat curves

In this section we give a characterization of maximal Fermat curves.

Let k be a finite field with q^2 elements, where $q = p^n$ for some integer n. Let $\mathcal{C}(m)$ be the Fermat curve defined over k by

$$x^m + y^m = z^m,$$

where m is an integer such that $m \geq 3$ and $\gcd(m, p) = 1$.

As is well-known, the genus g of $\mathcal{C}(m)$ is $g = (m-1)(m-2)/2$. The affine model of the curve $\mathcal{C}(m)$ is given by $x_1^m + y_1^m = 1$, $(x_1 = x/z,\ y_1 = y/z)$. Let μ_m denote the set of $m-$th roots of unity. If m divides $q^2 - 1$, then the group $\mu_m \times \mu_m$ operates on rational points of $\mathcal{C}(m)$ by

$$(\xi, \zeta)(x_1, y_1) = (\xi x_1, \zeta y_1) \quad \text{with } \xi, \zeta \in \mu_m. \tag{4.1}$$

Remark 4.1. If $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$, then m divides q^2-1 (see the proof of Lemma 4.5 in [5]).

Lemma 4.2. *With notation and hypotheses as above. If $\mathcal{C}(m)$ is maximal over $\mathbb{F}_{q^2}$, then $m \leq q+1$.*

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

$$\#\mathcal{C}(m)(\mathbb{F}_{q^2}) = 1 + q^2 + (m-1)(m-2)q. \tag{4.2}$$

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

$$\#\mathcal{C}(m)(\mathbb{F}_{q^2}) \leqslant m + (q^2 + 1 - m)m. \tag{4.3}$$

Using (4.2) and (4.3) we conclude that $m \leqslant q+1$. ■

If $m = q+1$ then $\mathcal{C}(q+1)$ is the Hermitian curve over $\mathbb{F}_{q^2}$. Suppose m divides $q+1$; i.e., $q+1 = mr$ for some integer r. Then we can define the following morphism

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

Hence $\mathcal{C}(m)$ is covered by $\mathcal{C}(q+1)$. Thus by Remark 2.2 if m divides $q+1$, then $\mathcal{C}(m)$ is maximal over $\mathbb{F}_{q^2}$. Now we want to show the converse of it. We start with a remark:

Remark 4.3. Assume $q = p$ is a prime number. If the curve $\mathcal{C}(m)$ is maximal over $\mathbb{F}_{p^2}$, then Theorem 3.3 implies that the Hasse-Witt matrix of $\mathcal{C}(m)$ is zero. Hence from [9, Corollary 1] we get that m is a divisor of $p+1$. The next theorem generalizes this result.

Theorem 4.4. *Let $\mathcal{C}(m)$ be the 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 4.1 we have that m divides q^2-1. As in the proof of the lemma above, looking at the function field extension $\mathbb{F}_{q^2}(x,y)/\mathbb{F}_{q^2}(x)$ we have:

$$\#\mathcal{C}(m)(\mathbb{F}_{q^2}) = m + \lambda m \qquad \text{for some integer } \lambda. \tag{4.4}$$

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

$$\#\mathcal{C}(m)(\mathbb{F}_{q^2}) = 1 + q^2 + (m-1)(m-2)q. \tag{4.5}$$

Comparing (4.4) and (4.5) 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 2.2 and the following lemma, this situation does not occur.

Lemma 4.5. *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 [9, Theorem 2] 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 [8, 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. This implies that (see (4.1)) :

$$\#\mathcal{C}(m)(\mathbb{F}_{q^2}) = m + \lambda_1 m^2 \qquad \text{for some integer } \lambda_1. \tag{4.6}$$

Then from (4.5) and (4.6) 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 4.5 and of Theorem 4.4. ■■

Remark 4.6. The particular case of Theorem 4.4 when m is of the form $m = t^2 - t + 1$ with $t \in \mathbb{N}$, was proved in Corollary 3.5 of [1].

5 Artin-Schreier curves

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

$$y^q - y = f(x), \tag{5.1}$$

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 [5, 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 (5.1).

The following remark is due to Stichtenoth:

Remark 5.1. Suppose that $q = p$ in Equation (5.1) considered over a perfect field k. Then we can change variables to assume that the curve $\mathcal{C}$ is given by Equation (5.1) with an admissible rational function. This follows from the partial fraction decomposition and from arguments similar to the proof of [17, 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 $c(x)/u(x)^{lp}$, with $c(x)$ a polynomial in $k[x]$ prime to $u(x)$ and with l 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 $z = a(x)/u(x)^l$ we get:

$$c(x)/u(x)^{lp} - (z^p - z) = z + b(x)/u(x)^{lp-1}.$$

Performing the substitution $y \to y - z$ and repeating this argument as in the proof of [17, Lemma III.7.7], we get the desired result.

Denote by tr the trace of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. We have that (see [23]):

Proposition 5.2. *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 5.3. 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 (5.1): 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 (5.1) is a $p-$cyclic extension of $\mathbb{P}^1$. In [7] 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 5.4. *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 3.3 we know that $\mathscr{C}^n = 0$.

A basis $\mathcal{B}$ for $H^0(\mathcal{C}, \Omega^1)$ is as bellow :

$$\mathcal{B} = \{y^r x^a dx \,|0 \leq a, r \ \text{ and } \ ap^n + rd \leq (p^n - 1)(d-1) - 2\}. \tag{5.2}$$

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 3.1 we get

$$\mathscr{C}^n(y^r x^a dx) = \sum_{h=0}^{r} \binom{r}{h} (-1)^h y^{r-h} \mathscr{C}^n(f^h x^a dx). \tag{5.3}$$

Hence we have

$$\mathscr{C}^n(f^h x^a dx) = 0 \tag{5.4}$$

for all h, r and a satisfying $0 \le h \le r$, $\binom{r}{h}$ is prime to p and

$$ap^n + rd \le (p^n - 1)(d-1) - 2. \tag{5.5}$$

First we show again that the degree of $f(x)$ is not bigger than $q+1$. In fact if $d = \deg(f(x) \ge q+2$, then $x^{q-1}dx$ is a element of $\mathcal{B}$, because

$$q(q-1) \le (q-1)(q+1) - 2.$$

From Remark 3.1 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 [14] the curve $\mathcal{C}$ is the Hermitian curve given by:

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

Hence we can assume $d \le q$, and so $d \le q-1$. Then there exists $\ell \ge 1$ such that

$$\ell d + 1 \le q < (\ell+1)d + 1.$$

Again by $\gcd(p,d) = 1$, we have

$$\ell d + 1 \le q \le (\ell+1)d - 1. \tag{5.6}$$

For a natural number $r \in \mathbb{N}$ satisfying

$$(q-1-r)d \ge q+1$$

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 (5.5).

From (5.6) and $d \le q-1$, we get that $a(\ell) = d-3$ and therefore

$$deg(f^\ell x^{a(\ell)}) = \ell d + a(\ell) = (\ell+1)d - 3. \tag{5.7}$$

Suppose that $q-1 = \ell d + a$ with $0 \le a \le a(\ell)$. Then the polynomial $f^\ell x^a$ has degree $q-1$ and it follows from Remark 3.1 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 (5.4) where we take $r = h = \ell$.

Therefore we now get from (5.7) that

$$q - 1 \geq \ell d + a(\ell) + 1 = (\ell + 1)d - 2. \tag{5.8}$$

By (5.6) and (5.8), we have

$$q + 1 = sd \qquad \text{with } s := \ell + 1 \geq 2. \tag{5.9}$$

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

$$f(x)^s = a_d^s x^{sd} + s a_d^{s-1} a_i x^{i+(s-1)d} + ... + a_0^s.$$

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 (5.9). 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 5.2 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

$$y^q + y = x^d \quad \text{with} \quad d \mid q+1. \ \blacksquare$$

Remark 5.5. 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 5.2 is superfluous. We also get that all maximal curves over $\mathbb{F}_{q^2}$ given by $y^q - y = f(x)$ as in Theorem 5.4 are covered by the Hermitian curve.

We can also classify minimal Artin-Schreier curves over $\mathbb{F}_{q^2}$ as below:

Theorem 5.6. *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*

$$y^q - y = ax^2 \quad \text{where} \quad a \in \mathbb{F}_{q^2},\ a \neq 0, \quad \text{and it satisfies} \quad a^{\frac{q^2-1}{2}} \neq (-1)^{\frac{q+1}{2}}.$$

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 5.2; it yields $d = 2$, $tr(b) = 0$ and $a^{\frac{q^2-1}{2}} \neq (-1)^{\frac{q+1}{2}}$. $\blacksquare$

Remark 5.7. 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:

$$\sigma(\mathcal{C}) - 1 + r = p(\sigma(\mathcal{D}) - 1 + r), \tag{5.10}$$

where r is the number of ramification points of the covering π.

Corollary 5.8. *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 is 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 5.1 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 2.5 we know that $\sigma(\mathcal{C}) = 0$. Note that from Formula (5.10) 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 in $k[x]$. Note here that the unique ramification point is a k-rational point. The result now follows from Theorem 5.4. ■

6 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 3.6 we have an upper bound on the genus, namely

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

In the next theorem we establish a characterization of maximal hyperelliptic curves in characteristic $p > 2$ that attain this genus upper bound.

Theorem 6.1. *Suppose that $p > 2$. 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 $f(x)$.

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 3.1 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

$$\mathscr{C}^n(\omega) = \omega M^{(1/q)},$$

where M is the $(g \times g)$ matrix with elements in k given as

$$M = \begin{pmatrix} c_{q-1} & c_{q-2} & \cdots & c_{q-g} \\ c_{2q-1} & c_{2q-2} & \cdots & c_{2q-g} \\ \vdots & \cdots & \cdots & \vdots \\ c_{gq-1} & c_{gq-2} & \cdots & c_{gq-g} \end{pmatrix}.$$

Remark 6.2. In [22] the author find a characterization for hyperelliptic curves defined over an algebraically closed field whose Hasse-Witt matrix is zero. In the proof below we use his ideas to classify hyperelliptic curves with a 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 M is the zero matrix. Hence looking at the last row of M, 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 M, 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 [5, 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 5.4, this curve is isomorphic to the curve given by the equation

$$y^2 = x^q + x. \ \blacksquare$$

In the next theorem we classify also minimal hyperelliptic curves over $\mathbb{F}_{q^2}$ in characteristic $p > 2$ with genus satisfying $g = (q-1)/2$:

Theorem 6.3. *Suppose that $p > 2$. There is a unique curve $\mathcal{C}$ which is a minimal hyperelliptic curve over $\mathbb{F}_{q^2}$ with genus $g = (q-1)/2$; it can be given by the affine equation*

$$a.y^2 = x^q - x, \quad \textit{with} \quad a \in \mathbb{F}_{q^2}^* \quad \textit{such that} \quad a^{(q^2-1)/2} \neq (-1)^{(q+1)/2}.$$

Proof. The curve $\mathcal{C}$ can be given by $y^2 = f(x)$, with $f(x)$ a square-free polynomial in $\mathbb{F}_{q^2}[x]$ of degree $deg(f(x)) = q = p^n$. 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 6.1 we can assume that $f(0) = 0$, and from $\mathscr{C}^n = 0$ we then conclude that it holds

$$f(x) = a_q x^q + a_1 x \qquad \text{with } \ a_1 a_q \neq 0.$$

Hence the minimal curve $\mathcal{C}$ can be defined by

$$x^q + \mu x = \lambda y^2, \qquad \text{for some } \ \mu, \lambda \in \mathbb{F}^*_{q^2}.$$

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

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

From this nonzero root $\beta \in \mathbb{F}^*_{q^2}$, we conclude as in the proof of Theorem 6.1 that the curve $\mathcal{C}$ can be given by the equation

$$x_1^q - x_1 = a.y^2, \qquad \text{with } \ a \in \mathbb{F}^*_{q^2}.$$

It now follows from Proposition 5.2 that

$$a^v \neq (-1)^u \qquad \text{with } u = \frac{q+1}{2} \text{ and } v = \frac{q^2-1}{2}.$$

For an element $a \in \mathbb{F}^*_{q^2}$ we have $a^v = \pm 1$. Consider two curves over $\mathbb{F}_{q^2}$ given by $a_1.y^2 = x^q - x$ and by $a_2.y^2 = x^q - x$ respectively, with $a_1^v \neq (-1)^u$ and with $a_2^v \neq (-1)^u$. Hence it holds that $a_1^v = a_2^v$ and we have $a_2 = a_1.c^2$, for some element $c \in \mathbb{F}^*_{q^2}$. The substitution $y \to cy$ shows that the two curves above are isomorphic to each other. ■

The theorem below is the analogous to Theorem 6.1 in case of characteristic $p = 2$:

Theorem 6.4. *Suppose that $p = 2$. There exists a unique maximal hyperelliptic curve over $\mathbb{F}_{q^2}$ with genus $g = q/2$. It can be given by the affine equation*

$$y^2 + y = x^{q+1}.$$

Proof. With arguments as in the proof of Corollary 5.8, we get that the curve can be given by $y^2 + y = f(x)$ with $f(x)$ a polynomial in $\mathbb{F}_{q^2}[x]$ of degree $q + 1$. The result now follows from item 3) of Theorem 2.3 of [3]. ■

7 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., curves $\mathcal{C}$ defined over $\mathbb{F}_q$ such that

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

Proposition 7.1. *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 [10] and [17, page 180]. ■

Corollary 7.2. *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 7.1 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 2.3 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 7.3. *Let $\mathcal{C}$ be a SW-maximal curve over $\mathbb{F}_q$ given by an affine equation of the form*

$$A(y) = f(x), \tag{7.1}$$

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 (7.1) is ordinary if and only if the rational function $f(x)$ has only simple poles (see [20, Corollary 1]). Thus Theorem 7.3 follows directly from Corollary 7.2 . ■

Corollary 7.4. *Let $\mathcal{C}$ be a SW-maximal curve as in the above theorem with $gcd(p,m) = 1$. Then the genus satisfies $g(\mathcal{C}) = (degA - 1)(s - 1)$, where s denotes the number of poles of $f(x)$.*

We finish with two examples of SW-maximal Artin-Schreier curves. In the first example we have that p divides m and the rational function $f(x)$ has a nonsimple pole; in the second, we have that $\gcd(p,m) = 1$ and the rational function $f(x)$ has only simple poles, as follows from Theorem 7.3.

Example 7.5. 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 7.6. 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 $k(x,y)/k(x)$.

References

[1] A. Aguglia, G. Korchmáros and F. Torres, *Plane maximal curves*, Acta Arith. 98 (2001), 165-179.

[2] T. Ekedahl, *On supersingular curves and abelian varieties*, Math. Scand. 60 (1987), 151-178.

[3] A. Garcia and F. Özbudak, *Some maximal function fields and additive polynomials*, Comm. in Algebra 35 (2007), 1553-1566.

[4] A. Garcia, H. Stichtenoth and C. P. Xing, *On subfields of Hermitian function fields*, Composito Math. 120 (2000), 137-170.

[5] A. Garcia and S. Tafazolian, *On additive polynomials and certain maximal curves*, preprint available at www.preprint.impa.br .

[6] H. Hasse and E. Witt, *Zyklische unverzweigte Erweiterungskörper vom Primzahlgrade p über einen algebraischen Funktionenkörper der Characteristic p*, Monatsh. Math. 43 (1936), 477-492.

[7] S. Irokawo and R. Sasaki, *A remark on Artin-Schreier curves whose Hasse-Witt maps are the zero maps*, Tsubuka J. Math. 1 (1991), 185-192.

[8] N. Koblitz, *p-adic variation of the zeta-function over families of varieties defined over finite fields*, Compositio Math. 31 (1975), 119-218.

[9] T. Kodama and T. Washio, *Hasse-Witt Matrices of Fermat curves*, Manuscripta Math. 60 (1988) 185-195.

[10] 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.

[11] S. Lang, *Abelian Varieties*, Interscience, New York, 1959.

[12] J. I. Manin, *Theory of commutative formal groups over fields of finite characteristic*, (Russian) Uspehi Mat. Nauk 18 (1963), 3-90.

[13] N.O. Nygaard, *Slopes of powers of Frobenius on crystalline cohomology*, Ann. Sci. École Norm. Sup. 14 (1981), 369-401.

[14] H.G. Rück and H. Stichtenoth, *A characterization of Hermitian function fields over finite fields*, J. Reine Angew. Math. 457 (1994), 185-188.

[15] J. P. Serre, *Sur la topologie des variétiés algébriques en caractéristique p*, Symposium internacional de topología algebraica (International symposium on algebraic topology). (1958), 24-53.

[16] H. Stichtenoth, *Die Hasse-Witt Invariante eines Kongruenzfunktionenkörpers*, Arch. Math. 33 (1979/80), 357-360.

[17] H. Stichtenoth, *Algebraic function fields and codes*, Universitext, Springer-Verlag, Berlin- Heidelberg, 1993.

[18] H. Stichtenoth and C. P. Xing, *On the structure of the divisor class group of curves over finite fields*, Arch. Math. 65 (1995), 141-150.

[19] K. O. Stöhr and P. Viana, *A study of Hasse-Witt matrices by local methods*, Math. Z. 200 (1989), 397-407.

[20] F. J. Sullivan, *p-torsion in the class group of curves with too many automorphisms*, Arch. Math. 26 (1975), 253-261.

[21] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. 2 (1966), 134-144.

[22] R. C. Valentini, *Hyperelliptic curves with zero Hasse-Witt matrix*, Manuscripta Math. 86 (1995), 185-194.

[23] J. Wolfmann, *The number of points on certain algebraic curves over finite fields*, Comm. Algebra 17 (1989), 2055-2060.

ARNALDO GARCIA and SAEED TAFAZOLIAN
IMPA-Instituto Nacional de Matemática Pura e Aplicada,
Estrada Dona Castorina 110, Jardim Botanico,
22460-320, Rio de Janeiro, Brazil
E-mail: garcia@impa.br and saeed@impa.br