A NOTE ON CERTAIN MAXIMAL CURVES

SAEED TAFAZOLIAN AND FERNANDO TORRES

Abstract. We characterize certain maximal curves over finite fields whose plane models are of Hurwitz type, namely $x^m y^a + y^n + x^b = 0$. We also consider maximal hyperelliptic curves of maximal genus. Finally, we discuss maximal curves of type $y^q + y = x^m$ via class field theory.

1. Introduction

Let $\mathcal{C}$ be a projective, nonsingular, geometrically irreducible, algebraic curve defined over $\mathbb{F}_{q^2}$, the finite field of order q^2. We say that $\mathcal{C}$ is *maximal over* $\mathbb{F}_{q^2}$ if the number of its $\mathbb{F}_{q^2}$-rational points attains the Hasse-Weil upper bound; that is, whenever

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

where $g = g(\mathcal{C})$ is the genus of $\mathcal{C}$. These curves are interesting mathematical objects by their own and they have been intensively studied in connection with coding theory [12], finite geometry [10], [11], supersingular curves [14], [18], and exponential sums over finite fields [17].

Ihara [23, Prop. 5.3.3] noticed that the genus g of a maximal curve over $\mathbb{F}_{q^2}$ does satisfy the inequality

$$g \le q(q-1)/2\,. \tag{1.1}$$

Rück and Stichtenoth [19] showed that, up to $\mathbb{F}_{q^2}$-isomorphism, there is just one maximal curve over $\mathbb{F}_{q^2}$ of genus $q(q-1)/2$, namely the so-called Hermitian curve over $\mathbb{F}_{q^2}$ which can be defined by the affine equation

$$u^{q+1} + v^{q+1} + 1 = 0\,. \tag{1.2}$$

Remark 1.1. It is commonly attributed to J.P. Serre the important fact that any curve over $\mathbb{F}_{q^2}$ which is nontrivially $\mathbb{F}_{q^2}$-covered by a maximal curve over $\mathbb{F}_{q^2}$ is also maximal over $\mathbb{F}_{q^2}$; cf. [27], [16], [14, Prop. 2.3]. Thus one way to construct maximal curves is by finding subcovers of the Hermitian curve; see for example [1], [3], [7].

We do observe that not all maximal curves arise as in the above remark [9], [24]; see also [6], [4]. Further facts on maximal curves can be found in [5] and [11, Ch. 10].

2010 MSC: 11G20, 11M38, 14G15, 14H25.
Key words: finite field, maximal curve, Hurwitz curve, hyperelliptic curve, Galois abelian covering.

The objective of this paper is to provide with a characterization of three oustanding classes of maximal curves over $\mathbb{F}_{q^2}$ which are usually related to very basic matters in curve theory over finite fields.

I. In Section 2 we deal with curves over $\mathbb{F}_{q^2}$ of Hurwitz type, namely nonsingular models $\mathcal{C} = \mathcal{C}_{a,b,m,n}$ over $\mathbb{F}_{q^2}$ of equations of type $x^m y^a + y^n + x^b = 0$ where a, b, m, n are nonnegative integers such that $\delta := ab - bn + mn \geq 1$ is coprime with q. A very basic property here is that $\mathcal{C}$ is $\mathbb{F}_{q^2}$-covered by the Fermat curve $u^\delta + v^\delta + 1 = 0$ and thus the arithmetical condition

$$q + 1 \equiv 0 \pmod{\delta} \tag{1.3}$$

provide us with a sufficient condition for the maximality over $\mathbb{F}_{q^2}$ of $\mathcal{C}$. The main result in this section is Theorem 2.9 where in fact it is shown that (1.3) characterizes the maximality of $\mathcal{C}$ over $\mathbb{F}_{q^2}$, whenever $a = 1$, $n \geq 2$, $\gcd(m, n-1) = 1$ and $b \equiv 1 \pmod{n}$. This result generalizes the case of Hurwitz curves ($a = b = 1$, $n = m$) which was already investigated in [1]. See also Proposition 2.10 for a related result when a, m, n are as above but with $b \equiv 0 \pmod{n}$.

The approach in Section 2 follows closely [1] where the key tool is a property concerning Weierstrass semigroups at $\mathbb{F}_{q^2}$-rational points of maximal curves over $\mathbb{F}_{q^2}$, namely Lemma 2.6 below. This property also plays a key role in handling maximal curves of either Fermat type [25] or Picard type [26].

II. In Section 3 we investigate hyperelliptic maximal curves $\mathcal{C}$ over $\mathbb{F}_{q^2}$ of maximal genus with an additional hypothesis involving Weierstrass points and $\mathbb{F}_{q^2}$-rational points. Let g be the genus of $\mathcal{C}$. In this case Ihara's bound (1.2) becomes $g \leq q/2$ (see Lemma 3.1). We characterize such curves $\mathcal{C}$ whose genus equals $\lfloor \frac{q}{2} \rfloor$; see Theorem 3.3. As in the case of Hurwitz type curves, the main tool employed here is also Weierstrass point theory. In fact the case q odd follows from a general result in [5] while the even case use the Fundamental Equivalence of divisors (2.2) on maximal curves.

We do remark that Theorem 3.3 was already fixed by Garcia and Tafazolian in [8] where the key tool is the use of Cartier operators.

III. About thirty years ago, Serre indicated his method for using class field theory to construct curves over finite fields with many rational points [21]. Given a finite Galois abelian extension $\mathbf{F}|\mathbf{K}$ of function fields over $\mathbb{F}_{q^2}$ the method depends on the structure of the conductor of such an extension as well as the number of places of degree one of $\mathbf{K}$ that can be splited completely in $\mathbf{F}$. In this way Lauter [13] characterized the Hermitian Function Field related to (1.2) (as well as the Suzuki and Ree function fields). Here we prove a similar result for the function field $\mathbb{F}_{q^2}(x, y)$ with $y^q + y = x^m$, m being a divisor of $q+1$. Indeed, $\mathbb{F}_{q^2}(x,y)$ is the larguest Galois abelian extension of $\mathbb{F}_{q^2}(x)$ satisfying the following properties (see Theorem 4.5):

(III.1) The conductor is $(m+1)\mathbf{p}$ with $\mathbf{p}$ being the place in $\mathbb{F}_{q^2}(x)$ corresponding to the point $x=\infty\in\mathbb{P}^1$;

(III.2) There are at least $m(q-1)+1$ degree one places in $\mathbb{F}_{q^2}(x)$ which split completely in $\mathbb{F}_{q^2}(x,y)$.

We do point out that all the curves considered above are $\mathbb{F}_{q^2}$-covered by the Hermitian curve over $\mathbb{F}_{q^2}$. There are no overlapping between the plane models arising in (I), (II), (III) above except the case $m=2$ and q odd which clearly arises in both cases (II) and (III).

Convention. In this paper, unless otherwise stated, by a *curve* we shall mean a projective, nonsingular, geometrically irreducible, algebraic curve. By $\mathbb{P}^r$ we denote the r-dimensional projective space over the algebraic closure of the corresponding base field.

2. On maximal curves defined by $x^my^a+y^n+x^b=0$

Throughout this section we let a,b,m,n be nonnegative integers such that

$$\delta=\delta(a,b,m,n):=ab-bn+mn\geq 1\,.$$

Let q be a prime power such that $\gcd(q,\delta)=1$ and let $\mathbf{F}_\delta$ be the Fermat curve given by the affine equation

$$u^\delta+v^\delta+1=0\,.$$

In particular, $\mathbf{F}_\delta$ is a nonsingular plane curve defined over $\mathbb{F}_{q^2}$ of degree δ. Next we consider the morphism

$$\varphi=\varphi_{a,b,m,n}:\mathbf{F}_\delta\to\mathbb{P}^2\,,\quad (u,v,1)\mapsto(x,y,1):=(u^nv^{-a},u^bv^{m-b},1)$$

which corresponds to the field extension $\mathbb{F}_{q^2}(u,v)|\mathbb{F}_{q^2}(x,y)$, where u,v,x,y are as above.

Definition 2.1. *We let $\mathcal{C}=\mathcal{C}_{a,b,m,n}$ be the nonsingular model over $\mathbb{F}_{q^2}$ of the (possible singular) plane curve $\varphi(\mathbf{F}_\delta)\subseteq\mathbb{P}^2$.*

We notice that the coordinates x and y of φ satisfy the relation

$$x^my^a+y^n+x^b=u^{bn}v^{-ab}(u^\delta+v^\delta+1)$$

and so a plane model for $\mathcal{C}$ is given by

$$x^my^a+y^n+x^b=0\,. \tag{2.1}$$

Remark 2.2. We always assume $a\leq m$ since the curves $\mathcal{C}(a,b,m,n)$ and $\mathcal{C}(m,n,a,b)$ are $\mathbb{F}_{q^2}$-isomorphic.

In this section we are interested in the maximality over $\mathbb{F}_{q^2}$ of the curve $\mathcal{C}_{a,b,m,n}$. The following result, which is well-known for particular values of a, b, m, n (see Remark 2.5 below), is the starting point of our research.

Proposition 2.3. *Let a, b, m, n, δ be as above and let q a prime power. Then the curve $\mathcal{C} = \mathcal{C}_{a,b,m,n}$ is maximal over $\mathbb{F}_{q^2}$ provided that the congruence (1.3) holds true.*

Proof. By definition $\mathcal{C}$ is covered by the Fermat curve $\mathbf{F}_\delta$ and consequently it is $\mathbb{F}_{q^2}$-covered by the Hermitian curve (1.2) as δ divides $q+1$. Then $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$ by Remark 1.1. □

Question 2.4. *Does condition (1.3) characterize the maximality of the curve $\mathcal{C}_{a,b,m,n}$ over $\mathbb{F}_{q^2}$?*

Remark 2.5. Notations as above. Suppose that $a = b$ and $m = n$ and set $\delta_{a,m} := \delta_{a,a,m,m} = a^2 - am + m^2 \geq 1$. Let q be a prime power such that $\gcd(q, \delta_{a,m}) = 1$.

(1) The curve $\mathcal{C}_m := \mathcal{C}_{1,1,m,m}$ with plane model $x^m y + y^m + x = 0$ is the so-called *Hurwitz curve* over $\mathbb{F}_{q^2}$. Indeed this plane model is nonsingular. (The case $m = 3$ defines the well-studied quartic Klein curve). Here (1.3) characterizes the maximality of $\mathcal{C}_m$ over $\mathbb{F}_{q^2}$; see [1, Thm. 3.1].

(2) Let $a > 1$. The curve $\mathcal{C}_{a,m} = \mathcal{C}_{a,a,m,m}$ with plane model $x^m y^a + y^m + x^a = 0$ is the so-called *generalized Hurwitz curve* over $\mathbb{F}_{q^2}$; see [2] and the references therein. Here (1.3) characterizes the maximality of $\mathcal{C}_{a,m}$ over $\mathbb{F}_{q^2}$ whenever $\delta_{a,m}$ is a prime number; see [1, Thm. 4.5].

To study Question 2.4 above we follow the approach in [1] and hence we begin by recalling an important result on Weierstrass semigroups at rational points on maximal curves (Lemma 2.6 below).

Let $\mathcal{X}$ be a maximal curve over $\mathbb{F}_{q^2}$. Let $\Phi : \mathcal{X} \to \mathcal{X}$ be the Frobenius morphism on $\mathcal{X}$ relative to $\mathbb{F}_{q^2}$. Then for a rational point $P \in \mathcal{X}(\mathbb{F}_{q^2})$ and an arbitrary point $Q \in \mathcal{X}$, the following linear equivalence of divisors holds true [5, Cor. 1.2]

$$(q+1)P \sim qQ + \Phi(Q)\,. \tag{2.2}$$

In particular, for any $P, Q \in \mathcal{X}(\mathbb{F}_{q^2})$, $(q+1)Q \sim (q+1)P$ [19, Lemma 1], so that $q+1$ belongs to the Weierstrass semigroup at any $\mathbb{F}_{q^2}$-rational point of $\mathcal{X}$. Therefore the following holds true.

Lemma 2.6. ([25, Lemma 3]) *Let $\mathcal{X}$ be a maximal curve over $\mathbb{F}_{q^2}$, and let P and Q be two distinct $\mathbb{F}_{q^2}$-rational points. Suppose that there exists a natural number h such that $hP \sim hQ$. Then $t := \gcd(h, q+1)$ is also a non-gap at P (or at Q).*

From now on we investigate the maximality over $\mathbb{F}_{q^2}$ of the curve $\mathcal{C} = \mathcal{C}_{1,b,m,n}$ with $b \equiv 0, 1 \pmod{n}$. Recall that $m \geq 1$ and $\gcd(q, \delta) = 1$ with $\delta = b - bn + mn \geq 1$. We further assume:

- $n \geq 2$ and $\gcd(m, n-1) = 1$.

After multiplying (2.1) by $x^{\delta-b}$ and setting $z := x^{m-b}y$ we obtain an alternative plane model for $\mathcal{C}$, namely

$$x^\delta = -\frac{z^n}{z+1}\,. \tag{2.3}$$

Next we compute the divisors of z and x. Since $\gcd(\delta, n-1) = \gcd(m, n-1) = 1$ there is just one point $P_\infty \in \mathcal{C}$ over $z = \infty$. Let $P_{-1} \in \mathcal{C}$ be the unique point over $z = -1$. Therefore

$$\operatorname{div}(z) = \frac{\delta}{\gcd(\delta, n)} D - \delta P_\infty \quad \text{and} \quad \operatorname{div}(x) = \frac{n}{\gcd(\delta, n)} D - P_{-1} - (n-1)P_\infty\,, \tag{2.4}$$

where D is a positive divisor of degree $\gcd(\delta, n)$ related to the zero divisor of x. In particular, the genus $g(\mathcal{C})$ of $\mathcal{C}$ can be easily computed via the Riemann-Hurwitz relation applied to the Galois abelian morphism $z : \mathcal{C} \to \mathbb{P}^1$. We have

$$2g(\mathcal{C}) = \delta + 1 - \gcd(\delta, n) - \gcd(\delta, n-1) = \delta - \gcd(b, n)\,. \tag{2.5}$$

We shall need the following result on numerical semigroups.

Lemma 2.7. ([20, p. 6]) *Let $i, d \geq 1$, k be integers such that $\gcd(i, d) = 1$ and $2 \leq k \leq i$. Let H_S be the numerical semigroup generated by the set $S := \{i + sd : s = 0, \ldots, k-1\}$. Then the genus $g_S = \#(\mathbb{N}_0 \setminus H_S)$ of H_S satisfies $2g_S = (i-1)(\alpha + d) + \beta(\alpha + 1)$, where $i - 1 = \alpha(k-1) + \beta$ with $0 \leq \beta < k-1$. In particular, if $i = k$, then*

$$2g_S = (i-1)(d+1)\,.$$

We now compute the Weierstrass semigroup $H(P_\infty)$ of $\mathcal{C}$ at P_∞.

Lemma 2.8. *Notations and assumptions as above. Let $\Delta := \lfloor \frac{\delta}{n} \rfloor$ and $i := \delta - \Delta(n-1)$. Let $I = 0$ if $b \equiv 1 \pmod{n}$, and $I = 1$ if $b \equiv 0 \pmod{n}$. Suppose that $\gcd(i, n-1) = 1$ and $k := \Delta - I + 1 \geq 2$.*

Then $H(P_\infty) = H_S$, the semigroup generated by the set

$$S = \{i + s(n-1) : s = 0, \ldots, k-1\}\,.$$

Proof. Let $s \geq 0$ be an integer. From (2.4) we have

$$\operatorname{div}(\frac{z}{x^s}) = \frac{\delta - sn}{\gcd(\delta, n)}\, D + sP_{-1} - (\delta - s(n-1))\, P_\infty \tag{2.6}$$

so that $\delta - s(n-1) = i + (\Delta - s)(n-1) \in H(P_\infty)$ if $s \le \Delta$; thus $H(P_\infty) \supseteq H_S$. Let $d = n-1$. Notice that $\delta \equiv b \pmod n$

(1) If $b \equiv 1 \pmod n$, then $k = \Delta + 1 = i = \min(S)$. Hence by Lemma 2.7

$$g(\mathcal{C}) = g(H(P_\infty)) \le g_S = (i-1)(d+1)/2\,.$$

Since $(i-1)(d+1) = \delta - 1$, then $H(P_\infty) = H_S$ by (2.5).

(2) Let $b \equiv 0 \pmod n$. Here $k = \Delta = \min(S)$ and hence by arguing as in (1) $g(\mathcal{C}) \le g_S = (\delta - n)/2$; the result follows again from (2.5). □

Now we state a positive answer to Question 2.4 for certain maximal curves of type $\mathcal{C}_{1,b,m,n}$.

Theorem 2.9. *Let $b, m \ge 0$, $n \ge 2$ be integers with $b \equiv 1 \pmod n$. Let $\delta = b - bn + mn \ge 2$, $\Delta = \lfloor \frac{\delta}{n} \rfloor \ge 1$, and suppose that $\gcd(\Delta + 1, n-1) = 1$. Let $\mathcal{C} = \mathcal{C}_{1,b,m,n}$ be the curve in Definition 2.1 over $\mathbb{F}_{q^2}$ where $\gcd(q, \delta) = 1$. Then the following statements are equivalent:*

1. *The Fermat curve $\mathbf{F}_\delta : u^\delta + v^\delta + 1 = 0$ is maximal over $\mathbb{F}_{q^2}$;*
2. *The curve $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$;*
3. *$q + 1 \equiv 0 \pmod \delta$.*

Proof. In view of Remark 1.1 and Proposition 2.3, we just have to show that (3) is a necessary condition for the maximality of $\mathcal{C}$ over $\mathbb{F}_{q^2}$. We look at the plane model (2.3). Since $\gcd(\delta, n) = \gcd(b, n) = 1$ by hypothesis, there is just one point $P_0 \in \mathcal{C}$ over $z = 0$; moreover P_0 is $\mathbb{F}_{q^2}$-rational. Then from (2.6) we obtain the equivalence of divisors $\delta P_0 \sim \delta P_\infty$ and so $t := \gcd(\delta, q+1) \in H(P_\infty)$ by Lemma 2.6. We have $t > 1$ by (2.5) and set $\delta = rt$ for some integer r. Let $i := \delta - \Delta d = \Delta + 1$ with $d = n - 1$. By Lemma 2.8 there exist $A, B \in \mathbb{N}_0$ such that $\delta = i + (i-1)d = rAi + rBd$. By taking module i and since $\gcd(i, d) = 1$ we find that $r = A = 1$ and $B = i - 1$. This implies $t = \delta$ and we get (3). □

For the case $b \equiv 0 \pmod n$ we obtain the following weak answer to Question 2.4.

Proposition 2.10. *Let $b, m \ge 0$, $n \ge 2$ be integers with $b \equiv 0 \pmod n$. Let $\delta = b - bn + mn$, $\Delta = \frac{\delta}{n} \ge 2$, and suppose that $\gcd(\Delta, n-1) = 1$. Let $\mathcal{C} = \mathcal{C}_{1,b,m,n}$ be the curve in Definition 2.1 over $\mathbb{F}_{q^2}$ with $\gcd(q, \delta) = 1$. Then*

1. *If $q + 1 \equiv 0 \pmod \delta$, then $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$;*
2. *Conversely, if $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$, then $q + 1 \equiv 0 \pmod{\frac{\delta}{n}}$.*

Proof. (1) follows from Proposition 2.3. The proof of (2) is quite similar to the proof of Theorem 2.9. With $s = \delta/n$, (2.6) gives the linear equivalence $\frac{\delta}{n}P_{-1} \sim \frac{\delta}{n}P_\infty$ where P_{-1} is also $\mathbb{F}_{q^2}$- rational. Thus $t := \gcd(\frac{\delta}{n}, q+1)$ which belongs to $H(P_\infty)$ by Lemma 2.6. We have that $t > 1$ by (2.5) and by Lemma 2.8 $t = \frac{\delta}{n}$ since $H(P_\infty)$ is generated by a set S with $\min(S) = \frac{\delta}{n}$. □

Example 2.11. Notation as above. Let $a = b = 1$, $n = 2$ and $m \geq 1$ be an integer. Let $\mathcal{C}_m$ be the curve $\mathcal{C}_{1,1,m+1,2}$ which is hyperelliptic by (2.4). Here $\delta(1, 1, m+1, 2) = 2m+1$ and thus the genus of $\mathcal{C}_m$ equals m by (2.5). In particular, $\mathcal{C}_m$ is an explicit example of a hyperelliptic maximal curve over $\mathbb{F}_{q^2}$ of genus m, where $q \equiv -1 \pmod{2m+1}$. In a similar way, the curve $\mathcal{C}_{1,2,m+2,2}$, with $\delta(1, 2, m+2, 2) = 2m+2$ is a hyperelliptic curve over $\mathbb{F}_{q^2}$ of genus m, where $q \equiv -1 \pmod{2m+2}$.

Example 2.12. A genus 3 hyperelliptic maximal curve over $\mathbb{F}_{q^2}$ can only exist if $q \geq 7$ by Lemma 3.1 and in fact the curve $y^2 = x^7 + x$ is of this type over $\mathbf{F}_{49}$. Indeed, Example 2.11 provide us with such curves whenever $q \equiv -1 \pmod 7$ or $q \equiv -1 \pmod 8$; cf. [15] and the references therein.

3. On maximal hyperelliptic curves of maximal genus

Let q be a prime power. In this section we investigate certain maximal curves $\mathcal{C}$ over $\mathbb{F}_{q^2}$ of genus $g \geq 1$ equipped with a morphism $\pi : \mathcal{C} \to \mathbb{P}^1$ over $\mathbb{F}_{q^2}$ of degree two; that is to say, we deal with certain maximal hyperelliptic curves over $\mathbb{F}_{q^2}$. To start with we rewrite Ihara's bound (1.1) in this case.

Lemma 3.1. *The genus of a hyperelliptic maximal curve over $\mathbb{F}_{q^2}$ is upper bounded by $q/2$.*

Proof. Let g be the genus of the curve. By counting rational points via the morphism $\pi : \mathcal{C} \to \mathbb{P}^1$ over $\mathbb{F}_{q^2}$ of degree two we have

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

and the result follows. □

Remark 3.2. Lemma 3.1 is sharp. To see this let us recall [23, Ex. 6.4.3] that the Hermitian curve (1.2) can also be described by the equation

$$v^{q+1} = u^q + u\,. \tag{3.1}$$

Then we consider two cases according to the parity of q.

(1) If q is odd, the hyperellipic curve $y^2 = x^q + x$ of genus $(q-1)/2$ is maximal over $\mathbb{F}_{q^2}$ since it is covered by (3.1) via $(u, v) \mapsto (x, y) := (u, v^{(q+1)/2})$.

(2) If q is even, the hyperelliptic curve $y^2 + y = x^{q+1}$ of genus $q/2$ is maximal over $\mathbb{F}_{q^2}$ since it is covered by (3.1) via $(u, v) \mapsto (x, y) := (u^{q/2} + \ldots + u, v)$.

The main result in this section is concerning the uniqueness of hyperelliptic maximal curves over $\mathbb{F}_{q^2}$ of maximal genus under an additional hypothesis involving Weierstrass points and $\mathbb{F}_{q^2}$-rational points.

Theorem 3.3. *Let $\mathcal{C}$ be a hyperelliptic maximal curve over $\mathbb{F}_{q^2}$ of genus $g = \lfloor \frac{q}{2} \rfloor$. Assume that there is a Weierstrass point P_0 of $\mathcal{C}$ which is also a $\mathbb{F}_{q^2}$-rational point.*

(1) *If q is odd, then $\mathcal{C}$ is given by $y^2 = x^q + x$;*
(2) *If q is even, then $\mathcal{C}$ is given by $y^2 + y = x^{q+1}$*

Proof. We know that the Weierstrass semigroup of $\mathcal{C}$ at P_0 is generated by 2 and $2g + 1$. Let x, y be rational functions on $\mathcal{C}$ such that $\mathrm{div}_\infty(x) = 2P_0$ and $\mathrm{div}_\infty(y) = (2g + 1)P_0$. By considering the Riemann-Roch space $L(2(2g+1)P_0)$ over $\mathbb{F}_{q^2}$, $\mathcal{C}$ is then defined by an equation over $\mathbb{F}_{q^2}$ of type

$$y^2 + A(x)y + B(x) = 0\,, \tag{3.2}$$

where $A(x), B(x)$ are polynomials in $\mathbb{F}_{q^2}[x]$ with $\deg(A(x)) \le g$ and $\deg(B(x)) = 2g + 1$.

(1) Let q be odd and so $2g + 1 = q$. Here (3.2) can be rewritten as an equation of type $y^2 = f(x)$ with $f(x)$ being a polynomial of degree $2g + 1$. Now we can apply Weierstrass Point Theory as in [5]. Let $\mathcal{D} = |(q + 1)P_0|$ be the Frobenius linear system on $\mathcal{C}$. Clearly its projective dimension is $N = g + 2$ so that $N - 1 = g + 1 = (q + 1)/2$ and the result follows directly from [5, Thm. 2.3].

(2) Let q be even and so $2g = q$. The following result is [5, Prop. 1.7(ii)]. For the sake of completeness we write a proof.

Claim. The point P_0 is the unique Weierstrass point of $\mathcal{C}$.

Proof of the Claim. Let P and Q be Weierstrass points of $\mathcal{C}$. From $2P \sim 2Q$ we have $qP \sim qQ$ so that $qP + \Phi(P) \sim qQ + \Phi(P)$ and so $P = Q$ by (2.2) and since $g > 0$.

Then in (3.2) we have $A(x) = A \in \mathbb{F}_{q^2} \setminus \{0\}$. Moreover, since $\mathcal{C}$ is maximal of genus $g = q/2$, $\#\mathcal{C}(\mathbb{F}_{q^2}) = 2q^2 + 1$ and thus in (3.2) we also have that $B(x) = Bx^{q+1}$. Now by using the map $y \mapsto Ay$, we see that the curve $\mathcal{C}$ is in fact defined by $y^2 + y = Cx^{q+1}$ with $C = A^{-1}B$, where in addition $C^{q-1} = 1$ (see [28, p. 2056]). In particular, $C \in \mathbb{F}_q$ and so there exists $D \in \mathbb{F}_{q^2}$ such that $C = D^{q+1}$; therefore by using the map $x \mapsto D^{-1}x$ the proof follows. □

Remark 3.4. As was mention in the introduction, Theorem 3.3 was already noticed by Garcia and Tafazolian in [8] where the key tool for the proof was the use of Cartier operators.

4. On maximal curves via Class Field Theory

Let q be a prime power. For m a divisor of $q+1$ let $\mathcal{H}_m$ be the nonsingular model over $\mathbb{F}_{q^2}$ of the plane curve

$$y^q + y = x^m\,. \tag{4.1}$$

We observe that $\mathcal{H}_{q+1}$ is the Hermitian curve (3.1) and that $\mathcal{H}_m$ is $\mathbb{F}_{q^2}$-covered by this curve; thus the curve $\mathcal{H}_m$ is also maximal over $\mathbb{F}_{q^2}$ according to Remark 1.1. It generalizes the curve in odd characteristic investigated in Theorem 3.3; in addition, the map $x : \mathcal{H}_m \to \mathbb{P}^1$ is a degree q Galois abelian morphism defined over $\mathbb{F}_{q^2}$. As a matter of fact, these properties characterize $\mathcal{H}_m$ as follows:

Theorem 4.1. ([8, Thm. 5.2]) *Let $\mathcal{C}$ be a maximal curve over $\mathbb{F}_{q^2}$ equipped with a Galois abelian morphism defined over $\mathbb{F}_{q^2}$ of degree q. Then there is a divisor m of $q+1$ such that $\mathcal{C}$ is $\mathbb{F}_{q^2}$-isomorphic to $\mathcal{H}_m$.*

On the other hand, from (4.1) it follows that the polar divisors of the functions x and y are respectively

$$\mathrm{div}_\infty(x) = qP_\infty \quad \text{and} \quad \mathrm{div}_\infty(y) = mP_\infty\,, \tag{4.2}$$

where $P_\infty \in \mathcal{H}_m$ is the unique point in $\mathcal{H}_m$ over $x = \infty$. Then another characterization of $\mathcal{H}_m$ is available, namely:

Theorem 4.2. ([5, Thm. 2.3]) *Let $\mathcal{C}$ be maximal curve over $\mathbb{F}_{q^2}$ and $P_\infty \in \mathcal{C}(\mathbb{F}_{q^2})$. Suppose that there is a non-gap m at P_∞ which is a divisor of $q+1$. Then $\mathcal{C}$ is $\mathbb{F}_{q^2}$-isomorphic to $\mathcal{H}_m$.*

Remark 4.3. While the proof of Theorem 4.1 has been carry on via the use of Cartier operators (cf. [8]), the proof of Theorem 4.2 is based on Weierstrass Point Theory (cf. [5]).

The objective of this section is to establish a further characterization of $\mathcal{H}_m$ by using rudiments of class field theory applied to the morphism $x : \mathcal{H}_m \to \mathbb{P}^1$ $(*)$. As a matter of fact, since we are now looking from the field theoretical point of view we investigate $(*)$ via the corresponding degree q Galois abelian extension of function fields over $\mathbb{F}_{q^2}$, namely

$$\mathbb{F}_{q^2}(x,y)|\mathbb{F}_{q^2}(x)\,, \tag{4.3}$$

with x, y satisfying (4.1). Let G be the Galois group of this extension. Then the elements of G are those σ such that $\sigma(x) = x$ and $\sigma(y) = y + b$ with $b \in \mathbb{F}_{q^2}$ such that $b^q + b = 0$. Let $\mathcal{P}$ and $\mathbf{p}$ be the places of $\mathbb{F}_{q^2}(x,y)$ and $\mathbb{F}_{q^2}(x)$ corresponding respectively to the points P_∞ (the common pole of x and y in (4.2)) and $p = x(P_\infty)$. Let $\nu = \nu_{P_\infty}$, $\mathcal{O} = \mathcal{O}_{P_\infty}$ and

$t = t_{P_\infty}$ be the valuation, the local ring and a local parameter at P_∞, respectively. We observe that we can choose $t = xy^{-n}$ by (4.2), where $mn = q+1$.

Lemma 4.4. *Notations and assumptions as above.*

1. *The conductor of the extension (4.3) is the divisor* $\mathbf{f} = (m+1)\mathbf{p}$;
2. *There is at least* $(q-1)m+1$ *places of degree one of* $\mathbb{F}_{q^2}(x)$ *which split completely in* $\mathbb{F}_{q^2}(x,y)$.

Proof. (1) From (4.1) it follows that $\mathbf{p}$ is the only place of $\mathbb{F}_{q^2}(x)$ which ramifies in $\mathbb{F}_{q^2}(x,y)$; indeed, it is totally ramified and hence the conductor $\mathbf{f}$ is a multiple of $\mathbf{p}$ [22, Prop. 24, p. 150]). Let $k \geq 1$ be the integer such that $\mathbf{f} = k\mathbf{p}$. To compute k we use the ramification theory of abelian coverings as in [23, Sect. 3.8]. For each integer $i \geq -1$, the i-th ramification group of the extension $\mathcal{P}|\mathbf{p}$ is given by

$$G_i = \{\sigma \in G : \nu(\sigma(z) - z) \geq i+1\,, \forall z \in \mathcal{O}\}\,.$$

For $i \geq 0$, $\sigma \in G_i$ if and only if $\nu(\sigma(t) - t) \geq i+1$ [23, Prop. 3.8.6(c)]. Let $\sigma(x) = x$ and $\sigma(y) = y + b$ with $b^q + b = 0$, $b \neq 0$. We have

$$\sigma(t) - t = x(y+b)^{-n}y^{-n}[(y^n - (y+b)^n]$$

and hence $\nu(\sigma(t) - t) = m+1$. Thus we have the following flag of ramification groups corresponding to $\mathcal{P}|\mathbf{p}$:

$$G_0 = G_1 = \ldots = G_m \neq G_{m+1} = 1\,,$$

where $\#G_i = q$ for $i \leq m$. Then as from (cf. [13, p. 89], [22, Ex. 2, p. 124]) we know that

$$k = \frac{1}{q}(\#G_1 + \ldots + \#G_m) + 1\,,$$

the proof follows.

(2) Since $\mathcal{H}_m$ is maximal over $\mathbb{F}_{q^2}$, the corresponding function field will have $q^2 + 1 + 2gq$ degree one places, where $g = (q-1)(m-1)/2$ is the genus of $\mathcal{H}_m$. Thus from (4.1) there are at least $q + (q-1)(m-1) = (q-1)m+1$ degree one places in $\mathbb{F}_{q^2}(x)$ which split completely in $\mathbb{F}_{q^2}(x,y)$. □

The main result of this section is the following theorem which was first noticed by Lauter for the Hermitian curve [13, Thm. 2]. We follow closely her arguments.

Theorem 4.5. *Notations as above. Let q be a prime power and m be a divisor of $q+1$. Let $\mathbf{F}$ be the largest abelian extension of $\mathbb{F}_{q^2}(x)$ which has conductor $\mathbf{f} = (m+1)\mathbf{p}$, and in which at least $(q-1)m+1$ degree one places of $\mathbb{F}_{q^2}(x)$ split completely. Then $\mathbf{F} = \mathbb{F}_{q^2}(x,y)$ with x, y fulfilling (4.1).*

Proof. As we already mentioned, the case $m = q+1$ was fixed in [13, Thm. 2]. Let $m < q+1$. We have $\mathbf{F} \supseteq \mathbf{F}_1 := \mathbb{F}_{q^2}(x,y) \supseteq \mathbb{F}_{q^2}(x)$ and so we have to show that $d := [\mathbf{F} : \mathbf{F}_1] = 1$. Let us work out first some estimatives involving degree one places. By hypothesis on the conductor, the place $\mathbf{p}$ of $\mathbb{F}_{q^2}(x)$ is the only one that ramifies in $\mathbf{F}$. Indeed, it is totally ramified. To see this property let $\mathcal{P}'$ be a place of $\mathbf{F}$ over $\mathbf{p}$; let T be its inercia field. Then $T = \mathbb{F}_{q^2}(x)$ by [23, Thm. 3.8.2(d)] which implies the aforementioned property; moreover, this also shows that $\mathbf{F}$ is a function field over $\mathbb{F}_{q^2}$. Let g be the genus of $\mathbf{F}$. Hence by the Hasse-Weil bound

$$1 + dq((q-1)m+1) \leq (q+1)^2 + q(2g-2)\,, \tag{4.4}$$

where $2g-2 = dq(-2)+\delta$ by the Riemann-Hurwitz formula with δ being the degree of the discriminant of $\mathbf{F}|\mathbb{F}_{q^2}(x)$. We evaluate δ by using the so-called conductor-discriminant formula (see e.g. [22, Ch. VI]); that is to say,

$$\delta = \sum_{\chi} f(\chi)$$

where the sum is taken over all irreducible characters χ of the Galois group of $\mathbf{F}|\mathbb{F}_{q^2}(x)$, $f(\chi)$ being the degree of the conductor of χ. Clearly $f(\chi) \leq m+1$ with $f(1) = 0$; hence $\delta \leq (dq-1)(m+1)$ so that

$$2g-2 \leq dq(-2) + (dq-1)(m+1)\,. \tag{4.5}$$

From (4.4) and (4.5) we have $d(q+1-m) \leq q+1-m$ and so $d \leq 1$ as $m < q+1$. This completes the proof of the theorem. ☐

Acknowledgments. The first author was supported by FAPESP/SP-Brazil (grant 2012/02255-3), and the second author was partially supported by CNPq-Brazil (grant 306324/2011-3).

References

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

[2] H. Bennama et P. Carbonne, Courbes $X^mY^n + Y^mZ^n + Z^mX^n = 0$ et Décomposition de la Jacobienne, *J. Algebra* **188** (1997), 409–417.

[3] A. Cossidente, G. Korchmáros and F. Torres, Curves of large genus covered by the Hermitian curve, *Comm. Algebra* **28** (2000), 4707–4728.

[4] Y. Duursma and K.H. Mak, On maximal curves which are not Galois subcovers of the Hermitian curve, *Bull. Braz. Math. Soc. New Series* **43**(3) (2012), 453–465.

[5] R. Fuhrmann, A. Garcia and F. Torres, On maximal curves, *J. Number Theory* **67** (1997), 29–51.

[6] A. Garcia, Güneri and H. Stichtenoth, A maximal curve which is not Galois covered by the Hermitian curve, *Bull. Braz. Math. Soc. New Series* **37**(1) (2006), 139–152.

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

[8] A. Garcia and S. Tafazolian, Certain maximal curves and Cartier operators, *Acta Arith.* **135** (2008), 199–218.

[9] M. Giulietti and G. Korchmáros, A new family of maximal curves over a finite field, *Math. Ann.* **343** (2000), 229–245.
[10] J.W.P. Hirschfeld, "Projective geometries over finite fields", second edition, Oxford University Press, Oxford, 1998.
[11] J. W.P, Hirschfeld, G. Korchmáros and F. Torres, "Algebraic curves over a finite field", Princeton Univ. Press, 2008.
[12] N.E. Hurt, "Many Rational Points: Coding Theory and Algebraic Geometry", Kluwer Academic Publishers, 2003.
[13] K. Lauter, Deligne-Lusztig curves as ray class fields, *Manuscripta Math.* **98** (1999), 87–96.
[14] A. Kazemifard, A. R. Naghipour and S. Tafazolian, A note on superspecial and maximal curves, *Bull. Iranian Math. Soc.* **39** (2013), 405–413.
[15] T. Kodama, J. Tap and T. Washio, Maximal hyperelliptic curves of genus three, *Finite Fields Appl.* **15** (2009), 392–403.
[16] G. Lachaud, Sommes d'Eisenstein et nombres de points de certaines courbes algébriques sur les corps finis, *C.R. Acad. Sci. Paris Sér. I Math.* **305** (1987), 729–732.
[17] C.J. Moreno, "Algebraic curves over finite fields", Cambridge University Press, Vol. 97, 1991.
[18] R. Re, Supersingular quotients of Fermat curves, *Finite Fields Appl.* **15** (2009), 450–467.
[19] H-G. Rück and H. Stichtenoth, A characterization of Hermitian function fields over finite fields, *J. Reine Angew. Math.* **457** (1994), 185–188.
[20] E.S. Selmer, On the linear diophantine problem of Frobenius, *J. Reine. Angew. Math.* **293/294** (1977), 1–17.
[21] J.-P. Serre, Sur le nombre des points rationnels d'une courbe algérique sur un corps fini, *C.R. Acad. Sci Paris Sér. I Math.* **296** (1983), 397–402.
[22] J.-P. Serre, "Algebraic groups and class fields", Grad. Texts in Math., vol. 117, Springer–Verlag, 1988.
[23] H. Stichtenoth, "Algebraic function fields and codes", second ed., Grad. Texts in Math., vol. 254, Springer–Verlag, 2009.
[24] S. Tafazolian, A. Teherán-Herrera and F. Torres, *Further examples of maximal curves which cannot be covered by the Hermitian curve*, preprint, 2014.
[25] S. Tafazolian and F. Torres, On maximal curves of Fermat type, *Adv. Geom.* **13** (2013), 613-617.
[26] S. Tafazolian and F. Torres, On the curve $y^n = x^m + x$ over finite fields, *J. Number Theory*, **145** (2014), 51–66.
[27] J. Tate, Endomorphisms of Abelian Varieties over Finite Fields, *Invent. Math.* **2** (1996), 134–144.
[28] J. Wolfmann, The number of points on certain algebraic curves over finite fields, *Comm. Algebra* **17** (1989), 2055–2060.

IMECC-UNICAMP, R. Sérgio Buarque de Holanda, 651, Cidade Universitária "Zeferino Vaz", 13083-859, Campinas, SP, Brazil
E-mail address: tafazolian@ime.unicamp.br
E-mail address: ftorres@ime.unicamp.br