ON THE CURVE $Y^n = X^m + X$ OVER FINITE FIELDS

SAEED TAFAZOLIAN AND FERNANDO TORRES

ABSTRACT. We show that a maximal curve over $\mathbb{F}_{q^2}$ defined by the affine equation $y^n = f(x)$, where $f(x) \in \mathbb{F}_{q^2}[x]$ has degree coprime to n, is such that n is a divisor of $q+1$ if and only if $f(x)$ has a root in $\mathbb{F}_{q^2}$. In this case, all the roots of $f(x)$ belong to $\mathbb{F}_{q^2}$; cf. Thm. 1.2, Thm. 4.3 in [J. Pure Appl. Algebra **212** (2008), 2513–2521]. In particular, we characterize certain maximal curves defined by equations of type $y^n = x^m + x$ over finite fields.

1. INTRODUCTION

Let $\mathcal{C}$ be a (projective, non-singular, geometrically irreducible, algebraic) curve defined over the finite field $\mathbb{F}_\ell$ of order ℓ. Let $\mathcal{C}(\mathbb{F}_\ell)$ denote the set of $\mathbb{F}_\ell$-rational points of $\mathcal{C}$. In the study of curves over finite fields, a fundamental problem is on the size of $\mathcal{C}(\mathbb{F}_\ell)$. The very basic result here is the Hasse-Weil bound (see [16, Thm. 5.2.3], [12, Thm. 9.18]) which asserts that

$$|\#\mathcal{C}(\mathbb{F}_\ell) - (\ell + 1)| \leq 2g\sqrt{\ell}\,,$$

where g is the genus of $\mathcal{C}$. The curve $\mathcal{C}$ is called *maximal over* $\mathbb{F}_\ell$ if the number of elements of $\mathcal{C}(\mathbb{F}_\ell)$ satisfies

$$\#\mathcal{C}(\mathbb{F}_\ell) = \ell + 1 + 2g\sqrt{\ell}\,.$$

We only consider maximal curves of positive genus and hence ℓ will always be a square, says $\ell = q^2$. Not all the curves over $\mathbb{F}_{q^2}$ can be maximal. As a matter of fact, a necessary condition is a result pointed out by Ihara (see, [16, Prop. 5.3.3]), namely that the genus g of a maximal curve over $\mathbb{F}_{q^2}$ do satisfy the inequality

$$g \leq q(q-1)/2\,.$$

Up to $\mathbb{F}_{q^2}$-isomorphism, there is just one maximal curve over $\mathbb{F}_{q^2}$ of genus $g = q(q-1)/2$, the so-called Hermitian curve over $\mathbb{F}_{q^2}$ (see [15]) which can be defined by the affine equation

$$v^{q+1} = u^{q+1} + 1$$

or birationally equivalently, it is given by $v^{q+1} = u^q + u$ (see [16, Example 6.4.3]).

By a result due to Serre (see, for example, [13, Prop. 2.3]), any curve which is $\mathbb{F}_{q^2}$-covered by a maximal curve over $\mathbb{F}_{q^2}$ is also maximal over $\mathbb{F}_{q^2}$. Thus we obtain several explicit examples of maximal curves by taking advantage of the fact that the automorphism group

2010 MSC: 11G20, 11M38, 14G15, 14H25.

Keywords: finite fields, maximal curves, Weierstrass semigroups, Picard curves, Fermat curves.

of the Hermitian curve is very huge; see, for example, [7], [1], [10]. We stress that not every maximal curve can be obtained in this way [11]; see also [6], [2].

In several instances, for example in applications to Coding Theory, Finite Geometry, or Cryptography it is desirable to work out with explicit plane models of maximal curves over $\mathbb{F}_{q^2}$. Let $n, m \geq 2$ be integers and let $\mathcal{C}(n,m)$ be the $\mathbb{F}_{q^2}$-nonsingular model of the plane affine curve

$$y^n = x^m + x\,.$$

The goal of this paper is to study the characterization of the maximality over $\mathbb{F}_{q^2}$ of curves of type $\mathcal{C}(n,m)$. This curve is a particular case of a curve $\mathcal{C}$ defined by $y^n = f(x)$ with $f(x)$ being a separable polynomial of degree m such that $\gcd(n,m) = 1$. Here we show that if $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$, then n divides $q+1$ if and only if $f(x)$ has a root in $\mathbb{F}_{q^2}$; in this case all the roots belong to $\mathbb{F}_{q^2}$, see Theorem 3.2. Indeed, we generalize the main result in [9].

Remark 1.1. Note that $\mathcal{C}(q+1,q)$ is the Hermitian curve over $\mathbb{F}_{q^2}$.

In order to study the maximaity of the curve $\mathcal{C}(n,m)$, we mainly use the Serre property via coverings of curves, a property of non-gaps at maximal cuves (Lemma 2.1) as well as certain property of a Cartier operator on maximal curves (Lemma 2.2). Our starting point is the existence of a natural covering of curves

$$(u,v) \in \mathcal{F}(s) \to (x,y) := (u^n, uv^{m-1}) \in \mathcal{C}(n,m)\,,$$

where $\mathcal{F}(s)$ is the Fermat curve defined by $v^s = u^s + 1$ of degree $s := n(m-1)$. This provides us with our first sufficient condition (Proposition 4.10), namely

$$q \equiv -1 \pmod{s}\,,$$

in order that $\mathcal{C}(n,m)$ be maximal over $\mathbb{F}_{q^2}$ (by means of the already mentioned Serre property).

Let $q = p^a$. In the case $m = p^b$, we show that the curve $\mathcal{C}(n,p^b)$ is maximal over $\mathbb{F}_{q^2}$ if and only if n divides $q+1$, says $q+1 = tn$, and b divides a, says $a = cb$, such that c is odd provided that t is so; see Theorem 4.7.

Let $\gcd(q,m) = 1$. Let $\gcd(n,m) = 1$ and q be such that $\gcd(q,s) = 1$. We consider two possibilities:

(A) If $m \equiv -1 \pmod{n}$, then $\mathcal{C}(n,m)$ is maximal over $\mathbb{F}_{q^2}$ if and only if $q \equiv -1, m \pmod{s}$?
(B) If $m \not\equiv -1 \pmod{n}$, then $\mathcal{C}(n,m)$ is maximal over $\mathbb{F}_{q^2}$ if and only if $q \equiv -1 \pmod{s}$?

In several cases we have that (A) and (B) occur. For example, the Picard curve $\mathcal{C}(3,4)$, the hyperelliptic curve $\mathcal{C}(2,2g+1)$ provide positive evidence for (A) and (B), respectively

(see Proposition 4.2 and Proposition 4.3). See also Proposition 4.13, Theorem 4.18 and Examples 4.17, 4.19.

2. Two properties of maximal curves

Let $\mathcal{C}$ be a maximal curve over $\mathbb{F}_{q^2}$ of genus g. In this secion we first recall a property of non-gaps at $\mathbb{F}_{q^2}$-rational points of $\mathcal{C}$ (Lemma 2.1) which is a consequence of the particular fashion of the enumerator of the Zeta function of $\mathcal{C}$ over $\mathbb{F}_{q^2}$, namely $L(t) = (t+q)^{2g}$ [12, Thm. 10.1]; then we also recall a property of the Cartier operators on $\mathcal{C}$ (Lemma 2.2). For $P \in \mathcal{C}(\mathbb{F}_{q^2})$ and $Q \in \mathcal{C}$ an arbitrary point of $\mathcal{C}$, the following equivalence of divisors hold true [3, Cor. 1.2]

$$(q+1)P \sim qQ + \mathbf{\Phi}(Q)\,, \tag{2.1}$$

where $\mathbf{\Phi} : \mathcal{C} \to \mathcal{C}$ is the Frobenious morphism relative to $\mathbb{F}_{q^2}$. Thus an interesting and quite useful consequence is the following result on non-gaps ([1, Proof of Thm. 3.1], [19, Lemma 3]).

Lemma 2.1. *Let $\mathcal{C}$ be a maximal curve over $\mathbb{F}_{q^2}$ and $P, Q \in \mathcal{C}(\mathbb{F}_{q^2})$. Let $t \geq 0$ be an integer such that $tP \sim tQ$. Then $d = \gcd(t, q+1)$ is also a non-gap at P (or at Q).*

Now let Ω^1 be the sheaf of regular 1-forms on the curve $\mathcal{C}$. There exists a canonical $1/p$-linear operator $\mathfrak{C} : \Omega^1 \to \Omega^1$, the so-called *Cartier operator* on $\mathcal{C}$, such that

(i) $\mathfrak{C}$ is $1/p-$linear; i.e., $\mathfrak{C}$ is additive and $\mathfrak{C}(f^p\omega) = f\ \mathfrak{C}(\omega)$,
(ii) $\mathfrak{C}$ vanishes on exact differentials; i.e., $\mathfrak{C}(df) = 0$,
(iii) $\mathfrak{C}(f^{p-1}df) = df$,
(iv) a differential $\omega \in \Omega^1$ is logarithmic if and only if ω is closed and $\mathfrak{C}(\omega) = \omega$.

The following result is crucial for us (see [8, Thm. 3.3]):

Lemma 2.2. *Let $\mathcal{C}$ be a maximal curve over $\mathbb{F}_{q^2}$, $q = p^a$ with $p \geq 2$ a prime and $a \in \mathbb{N}$. Then $\mathfrak{C}^a = 0$ on $H^0(\mathcal{C}, \Omega^1)$, where $\mathfrak{C}$ is the Cartier operator on $\mathcal{C}$.*

Remark 2.3. Moreover, one can easily show that

$$\mathfrak{C}^a(x^j dx) = \begin{cases} 0 & \text{if } p^a \nmid j+1 \\ x^{c-1}dx & \text{if } j+1 = p^a c. \end{cases}$$

Further information on maximal curves can be seen in [3] and [12, Ch. 10].

3. The curve $y^n = f(x)$

Let q be a power of a prime $p \geq 2$ and $n, m \geq 2$ be integers. The most popular curve of type $y^n = f(x)$ is the the so-called Fermat type $\mathcal{F}(n,m)$ which by definition is the non-singular model over $\mathbb{F}_{q^2}$ of the plane curve of Fermat type

$$v^n = u^m + 1\,.$$

If $n = m$ we just write $\mathcal{F}(n) = \mathcal{F}(n,n)$. The problem regarding the number of rational points of $\mathcal{F}(n,m)$ over finite fields was investigated by several authors; see e.g. [8, Thm. 4.4], [19] and the references therein. Concerning maximal curves of Fermat type, the basic result is the following.

Proposition 3.1. *Let* $\gcd(q, nm) = 1$. *The curve* $\mathcal{F}(n,m)$ *is* $\mathbb{F}_{q^2}$*-maximal if and only if both* n *and* m *divides* $q+1$. *In this case,* $\mathcal{F}(n,m)$ *is* $\mathbb{F}_{q^2}$*-covered by the Hermitian curve.*

The following result subsumes a partial generalization of Proposition 3.1, it generalizes Thms. 1.2 and 4.3 of [9] and is very much related to the results in [4].

Theorem 3.2. *Let* q *be a prime power,* $n \geq 2$ *an integer, and* $f(x)$ *be a separable polynomial in* $\mathbb{F}_{q^2}[x]$ *of degree* $m \geq 2$ *with* $\gcd(n,m) = 1$ *and* $\gcd(q,n) = 1$. *Let* $\mathcal{C}$ *be the non-singular model over* $\mathbb{F}_{q^2}$ *of the plane curve defined by* $y^n = f(x)$. *Suppose that* $\mathcal{C}$ *is maximal over* $\mathbb{F}_{q^2}$. *Then* $f(x)$ *has a root in* $\mathbb{F}_{q^2}$ *if and only if* n *divides* $q+1$. *In this case, all the roots of* $f(x)$ *belong to* $\mathbb{F}_{q^2}$.

Proof. We first show that n divides $q+1$ provided that $f(x)$ has a root $\alpha \in \mathbb{F}_{q^2}$. Let $r^a > 1$ be a prime power with $r^a \mid n$. Then the non-singular model $\mathcal{C}_1$ over $\mathbb{F}_{q^2}$ of the curve defined by $y^{r^a} = f(x)$ is also maximal over $\mathbb{F}_{q^2}$ whose genus is $g_1 = (r^a-1)(m-1)/2$. Let $Q, P \in \mathcal{C}_1(\mathbb{F}_{q^2})$ be the points over $x = \alpha$ and over $x = \infty$, respectively. Then $r^a P \sim r^a Q$ and thus $d = \gcd(r^a, q+1)$ is a non-gap at P by Lemma 2.1. Since $g_1 > 0$, we have that d is a power of r with $1 < d \leq r^a$. Now the Weierstrass semigroup at P is generated by r^a and m so that there exist $\beta, \gamma \geq 0$ integers such that $d = \beta r^a + \gamma m$. Then, as $\gcd(n,m) = 1$, $d = r^a$ and thus $q \equiv -1 \pmod{n}$. Conversely, suppose that $f(\alpha) \neq 0$ for any $\alpha \in \mathbb{F}_{q^2}$. Thus by the maximality of $\mathcal{C}$ over $\mathbb{F}_{q^2}$, and by counting rational points via the morphism $y : \mathcal{C} \to \mathbb{P}^1$ we find that

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

where $2g = (n-1)(m-1)$ and e is a certain integer. We know that $q^2 \equiv 1 \pmod{n}$ by [17, Thm. 5]. We claim that $q \not\equiv -1 \pmod{n}$. Otherwise, by applying module n in $(*)$ we would have $m \equiv 0 \pmod{n}$ which is not possivel by hypothesis. Next we show the last part of the proposition. Let $R \in \mathcal{C}$ such that $nR \sim nQ$ where Q is as above. Therefore $(q+1)R \sim (q+1)Q \sim qR + \mathbf{\Phi}(R)$ by (2.1) so that $R \in \mathcal{C}(\mathbb{F}_{q^2})$. $\square$

Remark 3.3. In general, if $y^n = f(x)$ defines a maximal curve over $\mathbb{F}_{q^2}$, then, as we already noticed in the proof of Theorem 3.2, n must be a divisor of $q^2 - 1$ (cf. [17, Thm. 5]). For example, the Hermitian curve admits a plane model of type $y^{q^2-1} = x(x+1)^{q-1}$ and thus for any divisor n of $q^2 - 1$, the curve $y^n = x(x+1)^{q-1}$ is maximal $\mathbb{F}_{q^2}$ as well; cf. [7, Example 6.3]. Thus the hypothesis of $f(x)$ being separable in Theorem 3.2 cannot be relaxed.

4. The case $y^n = f(x) = x^m + x$

Let q be a power of a prime $p \geq 2$ and $n, m \geq 2$ be integers. In this section we study the non-singular model $\mathcal{C}(n, m)$ over $\mathbb{F}_{q^2}$ of the plane curve

$$y^n = x^m + x\,.$$

First we notice that in some cases the curve $\mathcal{C}(n, m)$ is $\mathbb{F}_{q^2}$-isomorphic to the Fermat type curve $\mathcal{F}(n, m-1)$ which was already been considered in the previous section.

Proposition 4.1. *Let q, n, m be as above with $\gcd(q, s) = 1$, where $s := n(m-1)$. Suppose that n divides m. Then the curve $\mathcal{C} = \mathcal{C}(n, m)$ is maximal over $\mathbb{F}_{q^2}$ if and only if $q \equiv -1 \pmod{s}$. In this case, the curve $\mathcal{C}$ is $\mathbb{F}_{q^2}$-covered by the Hermitian curve $v^{q+1} = u^q + u$.*

Proof. We notice that $\mathcal{C}$ is $\mathbb{F}_{q^2}$-isomorphic to the Fermat curve type $\mathcal{F}(n, m-1)$ by means of the automorphism $(u, v) \mapsto (x, y) := (1/u, v/u^t)$, where $m = tn$. Thus the proof follows from Proposition 3.1 and the fact that $\gcd(n, m-1) = 1$. □

We observe now that $\mathcal{C}(3, 4)$ is a so-called Picard curve type over $\mathbb{F}_{q^2}$ and it has been already investigated by several authors; For example Kazemifard and Tafazolian [14] (see also the references therein) among other things proved the following.

Proposition 4.2. *Let q be a power of a prime different from 3. Then the curve $\mathcal{C}(3, 4)$ is maximal over $\mathbb{F}_{q^2}$ if and only if $q \equiv -1 \pmod{9}$. In this case, $\mathcal{C}(3, 4)$ is $\mathbb{F}_{q^2}$-covered by the Hermitian curve.*

In particular, we notice that the Picard curves $\mathcal{F}(3, 4)$ and $\mathcal{C}(3, 4)$ (both of genus 3) are not $\mathbb{F}_{q^2}$-isomorphic for infinitely many value of q. We also have the following result [18, Thm. 1].

Proposition 4.3. *Let q be a prime power and $g \geq 1$ an integer with $\gcd(q, 2g) = 1$. Then the hyperelliptic curve $\mathcal{C}(2, 2g+1)$ is maximal over $\mathbb{F}_{q^2}$ if and only if $q \equiv -1, 2g+1 \pmod{4g}$. In both cases, the curve is $\mathbb{F}_{q^2}$-covered by the Hermitian curve.*

In the particular case of the curve $\mathcal{C}(n, m)$, Theorem 3.2 becomes.

Proposition 4.4. *Let $n, m \geq 2$ be integers with $\gcd(n, m) = 1$, set $s := n(m-1)$, and suppose that $\gcd(q, s) = 1$. If the curve $\mathcal{C}(n, m)$ is maximal over $\mathbb{F}_{q^2}$, then n divides $q+1$. Moreover, $m-1$ divides $q^2 - 1$.*

Proof. We apply Theorem 3.2 and hence we only need to show the second assertion. Fix a root $\alpha \in \mathbb{F}_{q^2}$ of $x^{m-1} = -1$. Then the set $\{\alpha x : x^{m-1} = -1\}$ is the set of the $m-1$ distinct roots of the equation $y^{m-1} = 1$ and we are done. □

Remark 4.5. Given $n, m \geq 2$ integers, the solution for the congruences $q \equiv -1 \pmod{n}$ and $q^2 \equiv 1 \pmod{m-1}$ is of type $q \equiv -1 + ni \pmod{s}$ with $s = n(m-1)$ and $i \in \{0, \ldots, m-2\}$ such that $ni(ni-2) \equiv 0 \pmod{m-1}$.

To deal with the case m a power of the characteristic of the base field, the following result due to Wolfmann [20] is required.

Proposition 4.6. *Let $\mathcal{C}$ be the non-singular model over $\mathbb{F}_{q^2}$ of the curve defined by*

$$\alpha y^n = x^{p^b} - x\,,$$

where $q = p^{cb}$, $\alpha \in \mathbb{F}_{q^2}^*$ and n is a positive divisor of $q+1$. Define t and r by $tn = q+1$ and $rn = q^2 - 1$. Then the curve $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$ if and only if $\alpha^r = (-1)^t$.

We apply this result to deal with the maximality over $\mathbb{F}_{q^2}$, $q = p^a$, of the curve $\mathcal{C}(n, m)$ with $m = p^b$ being $p > 2$. Suppose that such a curve is maximal over $\mathbb{F}_{q^2}$. We claim that $n|(q+1)$ and $b|a$. In fact, Proposition 4.4 implies the first assertion and that $b|(2a)$ as $(p^b - 1)|(p^{2a} - 1)$. Let $2a = hb$ and so we have to show that h is even. Now Theorem 3.2 implies that each root α of $x^{p^b} + x$ belongs to $\mathbb{F}_{q^2}$; hence for $\alpha \neq 0$ we obtain

$$1 = \alpha^{(q^2-1)} = \alpha^{(p^b-1)(p^{b^{h-1}}+\cdots+1)} = (-1)^{(p^{b^{h-1}}+\cdots+1)} = (-1)^h$$

and hence h is even as $p > 2$. Therefore we have shown the first part of the following.

Theorem 4.7. *Let $q = p^a$ be a power of a prime $p > 2$. Let $\mathcal{C} := \mathcal{C}(n, p^b)$ be the curve over $\mathbb{F}_{q^2}$ defined by the equation $y^n = x^{p^b} + x$ with $\gcd(p, n) = 1$. Then $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$ if and only if n divides $q+1$, says $q+1 = tn$, and b divides a, says $a = cb$, such that c is odd provided that t is so. In this case, the curve is $\mathbb{F}_{q^2}$-covered by the Hermitian curve $v^{q+1} = u^q + u$.*

Proof. Let us show first that t is odd implies that c is so. By performing the substitution $x \mapsto -\alpha^{-1}x$ in the equation that defines $\mathcal{C}$, being α a non-zero root of $x^{p^b} + x = 0$, we can assume that the curve $\mathcal{C}$ can also be defined by the equation $\alpha y^n = x^{p^b} - x$. Now since $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$, Proposition 4.6 implies

$$(-1)^t = \alpha^{t(q-1)} = \alpha^{t(p^b-1)(p^{b^{c-1}}+\cdots+1)} = (-1)^{t(p^{b^{c-1}}+\cdots+1)} = (-1)^{tc}$$

and hence, as $p > 2$, c is odd if t is so. Conversely, we have two cases; let $q+1 = tn$ with t odd so that c is odd. Let us define the polynomial

$$Q(u) := u^{p^{a-b}} - \cdots + u^{p^{a-cb}}\,.$$

We have that $Q(u)^{p^b} + Q(u) = u^q + u$ and hence $\mathcal{C}$ is covered by the Hermitian curve via $(u, v) \mapsto (x, y) = (Q(u), v^t)$. Now let t be even. Let α be as above and β such that $\beta^n =$

α^{-1}; thus $\beta \in \mathbb{F}_{q^2}$. Then via $(x, y) \mapsto (x, \beta y)$ the curve $\mathcal{C}$ is also described by $y^n = x^{p^b} - x$ Finally we cover $\mathcal{C}$ from the Hermitian curve via $(u, v) \mapsto (x, y) = (u^{p^{a-b}} + \cdots + u, \gamma v^t)$, where γ^n is a non-zero root of $x^q + x = 0$. □

The following result is related with the type of curves considered in [5].

Theorem 4.8. *Let $q = p^a$ be a power of a prime $p \geq 2$, and $f(x)$ a polynomial in $\mathbb{F}_{q^2}[x]$ of degree $m \geq 2$ with $\gcd(q + 1, m) = 1$. If $y^{q+1} = f(x)$ defines a maximal curve $\mathcal{C}$ over $\mathbb{F}_{q^2}$, then m is a power of p with $2 \leq m \leq q$. In the case where $f(x) = x^m + x$, the curve $\mathcal{C} = \mathcal{C}(q + 1, m)$ is maximal over $\mathbb{F}_{q^2}$ if and only if $m = p^b$, with $a = cb$ and c odd. Moreover, $\mathcal{C}$ is $\mathbb{F}_{q^2}$-covered by the Hermitian curve.*

Proof. The Weierstrass semigroup at the unique $\mathbb{F}_{q^2}$-rational point P over $x = \infty$ is generated by $q + 1$ and m. Suppose that $\mathcal{C}$ is a maximal curve over $\mathbb{F}_{q^2}$; then q is a non-gap at P by [3, Prop. 1.5(iv)] and thus $m = p^b$ with $1 \leq b \leq a$. Let $\mathcal{C} = \mathcal{C}(q + 1, p^b)$. If $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$, then by Lemma 6 and the proof of Theorem 7 in [5] there exists a separable additive polynomial $Q(x) \in \mathbb{F}_{q^2}[x]$ such that

$$f(Q(x)) = Q(x)^{p^b} + Q(x) = x^{p^a} + x\,. \quad (*)$$

It turns out that $Q(x)$ is of type $Q(x) = x^{p^{a-b}} - x^{p^{a-2b}} + \ldots$ $(*_1)$ and hence there is an odd integer c such that $a = cb$ $(*_2)$. Conversely, if $(*_2)$ holds true then the polynomial $Q(x)$ in $(*_1)$ satisfies $(*)$; thus the morphism $(u, v) \mapsto (x, y) = (Q(u), v)$ is a $\mathbb{F}_{q^2}$-covering from the Hermitian curve $u^{q+1} = v^q + v$ to the curve $\mathcal{C}$, and we are done. □

Theorem 4.9. *Let $q = p^a$ be a power of a prime $p > 3$. Let $m \geq 2$ be an integer such that $\gcd(\frac{q+1}{2}, m) = 1$. The curve $\mathcal{C} = \mathcal{C}(\frac{q+1}{2}, m)$ given by the equation $y^{(q+1)/2} = x^m + x$ is maximal over $\mathbb{F}_{q^2}$ if and only if $m = 2, 3$ or $m = p^b$ where b divides a. In any case above, $\mathcal{C}$ is $\mathbb{F}_{q^2}$-covered by the Hermitian curve.*

Proof. Let $\mathcal{C}$ be maximal over $\mathbb{F}_{q^2}$. Let P be the unique point over $x = \infty$. Then the Weierstrass semigruop $H(P)$ at P is generated by $(q + 1)/2$ and m, where $m \leq q$ since the genus of $\mathcal{C}$ is at most $q(q - 1)/2$. As q belongs to $H(P)$ [3, Prop. 1.5(iv)] we can find a pair of non-negative integers α, β such that $\alpha m + \beta\frac{q+1}{2} = q$. Clearly, $\beta < 2$ and if $\beta = 0$, m divides q and $m = p^b$. In this case, from Theorem 4.7 the maximal curve $\mathcal{C}$ is $\mathbb{F}_{q^2}$-covered by the Hermitian curve. But if $\beta = 1$, then m divides $(q - 1)/2$. In the later case, if $m = 2$ (resp. $m = 3$), then $s = \frac{q+1}{2}(2 - 1) = \frac{q+1}{2}$ (resp $s = \frac{q+1}{2}(3 - 1) = q + 1$) divides $q + 1$ and so the curve is maximal because it is covered by the Hermitian curve; cf. Proposition 4.10.

Now suppose $m > 3$. In this case we show that $\mathcal{C}$ is not maximal. In fact, we know that $\alpha m = \frac{q-1}{2}$, or equivalently $q - 1 = 2\alpha m$. It follows that

$$2q - 1 = 4\alpha m + 1 = 4\alpha(m - 1) + (4\alpha + 1)\,.$$

We have the following basis for regular 1-forms of $\mathcal{C}$

$$\mathfrak{B} = \{\omega_{i,j} := x^i y^j dx/y^{(q-1)/2} \text{ with } (2g-2) - \frac{q+1}{2}i - mj \geq 0\},$$

where by [16, Example 6.3.3] the genus g of $\mathcal{C}$ satisfies

$$g = 1/2[\frac{q-1}{2}(m-1) - \gcd(\frac{q+1}{2}, m) + 1].$$

Since for any j, $j - \frac{q-1}{2} = -(j+1)q + (2j+1)\frac{q+1}{2}$, we get

$$\mathfrak{C}^a(\omega_{i,j}) = \mathfrak{C}^a(x^i y^j dx/y^{(q-1)/2}) = \mathfrak{C}^a(y^{-(j+1)q} y^{(2j+1)(q+1)/2} x^i dx) =$$
$$y^{-(j+1)}\mathfrak{C}^a((x^m+x)^{(2j+1)} x^i dx) = y^{-(j+1)}\Sigma_{\ell=0}^{(2j+1)} b_\ell \mathfrak{C}^a(x^{(m-1)\ell+(2j+1)+i} dx).$$

Wee consider two cases: if p does not divide $4\alpha+1$, then

$$\mathfrak{C}^a(\omega_{0,2\alpha}) = b_{4\alpha}\omega_{1,(m-2)\alpha-1} = (4\alpha+1)\omega_{1,(m-2)\alpha-1} \neq 0.$$

Note that as $m > 3$, the regular 1-forms $\omega_{1,(m-2)\alpha-1}$, $\omega_{2,(m-3)\alpha-1}$ and $\omega_{0,2\alpha}$ belong to $\mathfrak{B}$ and so are well defined. Otherwise, if p divides $4\alpha+1$, then p does not divide $6\alpha+1$ and so we get

$$\mathfrak{C}^a(\omega_{1,3\alpha}) = b_{6\alpha}\omega_{2,(m-3)\alpha-1} = (6\alpha+1)\omega_{2,(m-3)\alpha-1} \neq 0.$$

Observe that here we need $m > 5$, since then we have $\omega_{1,3\alpha} \in \mathfrak{B}$. Now clearly if p divides $4\alpha+1$, then $m > 4$ and if $m = 5$ we can show that $p = 3$.

Therefore we conclude that the curve $\mathcal{C}((q+1)/2, m)$ for $m > 3$ is not maximal, because $\mathfrak{C}^a \neq 0$ (cf. Lemma 2.2). □

The following result was already stated in the introduction.

Proposition 4.10. *Let $n, m \geq 2$ be integers, $s = n(m-1)$, and q a power of a prime. Then $\mathcal{C}(n,m)$ is maximal over $\mathbb{F}_{q^2}$ provided that $q \equiv -1 \pmod{s}$.*

Remark 4.11. Let q be a prime power and t a divisor of $q+1$. Then the curve $\mathcal{C}(\frac{q+1}{t}, t+1)$ is maximal over $\mathbb{F}_{q^2}$ by Proposition 4.10. In particular, $\mathcal{C}(q+1, 2)$ is maximal over $\mathbb{F}_{q^2}$ and $\gcd(q+1, 2) = 2$ if q is odd. Thus the condition $\gcd(q+1, m) = 1$ in Theorem 4.8 cannot be avoided.

Next we point out another sufficient condition in order that $\mathcal{C}(n,m)$ be maximal over $\mathbb{F}_{q^2}$.

Proposition 4.12. *Let $n, m \geq 2$ be integers with $m \equiv -1 \pmod{n}$, $s = n(m-1)$ and q a power of a prime. Then the curve $\mathcal{C}(n,m)$ is maximal over $\mathbb{F}_{q^2}$ provided that $q \equiv m \pmod{s}$.*

Proof. From the congruences, we deduce that $q \equiv -1 \pmod{n}$. We shall show that $\mathcal{C}(n,m)$ is $\mathbb{F}_{q^2}$-covered by the Hermitian curve; let us recall that this curve can also be described over $\mathbb{F}_{q^2}$ by the equation $v^{q+1} = u^q + u$ (see [16, Example VI.4.3]). Write $q+1 = an$ and $q = bn(m-1)+m$. Then the image of the morphism $(u,v) \mapsto (x,y) := (u^{bn+1}, u^b v^a)$ defines $\mathcal{C}(n,m)$, and we are done. □

For $m \geq 2$ an integer let q be a power of an odd prime such that

$$q^2 \equiv 1 \pmod{m-1} \quad \text{implies} \quad q \equiv -1, 1 \pmod{m-1}. \qquad (*)$$

This can be occur, for example when $m-1 = \ell^t$ or $m-1 = 2\ell^t$ with $\ell > 2$ being a prime and $t \geq 1$ an integer.

Proposition 4.13. *Let $n, m \geq 2$ be integers such that n is odd and such that $(*)$ holds true. In addition, assume $\gcd(n, m) = 1$, $\gcd(n, m-1) = 1$, and that $m \equiv -1 \pmod{n}$. Set $s := n(m-1)$. Let q be a prime power with $\gcd(q, s) = 1$. Then the curve $\mathcal{C} = \mathcal{C}(n, m)$ is maximal over $\mathbb{F}_{q^2}$ if and only if $q \equiv -1, m \pmod{s}$.*

Proof. By Propositions 4.10 and 4.12, $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$ provided that $q \equiv -1, m \pmod{s}$. Conversely, let $\mathcal{C}$ be maximal over $\mathbb{F}_{q^2}$. From Proposition 4.4 and $(*)$ we have two cases:

1. $q \equiv -1 \pmod{m-1}$. Here we conclude that $s = n(m-1)$ divides $q+1$ because n is a divisor of $q+1$ and $\gcd(n, m-1) = 1$.

2. $q \equiv 1 \pmod{m-1}$. In this case we have $q = (m-1)t + 1$ for some integer $t \geq 1$. Set $t = hn + r$ for some integers $h \geq 0$ and $0 \leq r \leq n-1$. Thus we have $q = (m-1)(hn+r)+1 = n(m-1)h + r(m+1) - 2r + 1$. This implies that n divides $2r-2$. Therefore, as n is odd, we obtain $r = 1$ so that $q \equiv m \pmod{s}$. This completes the proof. □

Remark 4.14. The restrictions $\gcd(n, m) = 1$, $\gcd(n, m-1) = 1$, and $m \equiv -1 \pmod{n}$ in Proposition 4.13 cannot be relaxed as one can see by considering the curves $\mathcal{C}(n, n)$ and $\mathcal{C}(3, 4)$ in Proposition 4.1 and Proposition 4.2, respectively.

Next we generalize the Picard curve type $\mathcal{C}(3, 4)$ (Proposition 4.2) over $\mathbb{F}_{p^2}$ by considering the curve $\mathcal{C} = \mathcal{C}(3, m)$ defined by the equation $y^3 = x^m + x$. The following set contains a basis for regular 1-forms of $\mathcal{C}$

$$\{\omega_{i,j} := x^i y^j dx/y^2 \text{ with } (2g-2) - 3i - mj \geq 0\},$$

where g is the genus of $\mathcal{C}$.

Theorem 4.15. *Let $m \geq 2$ be an integer. Set $s := 3(m-1)$ and let p be a prime with $\gcd(p, s) = 1$. The curve $\mathcal{C} := \mathcal{C}(3, m)$ given by the equation $y^3 = x^m + x$ is maximal over $\mathbb{F}_{p^2}$ if and only if*

(1) $m \equiv 0 \pmod{3}$ *and* $p \equiv -1 \pmod{s}$;
(2) $m \equiv 1 \pmod{3}$ *and* $p \equiv -1 \pmod{s}$;
(3) $m \equiv 2 \pmod{3}$ *and* $p \equiv -1, m \pmod{s}$.

Proof. If (1), (2) or (3) hold true, then $\mathcal{C}$ is maximal over $\mathbb{F}_{p^2}$ by Propositions 4.10 and 4.12. Let $\mathcal{C}$ be maximal over $\mathbb{F}_{p^2}$. Here we have $g = m-2$ (resp. $m-1$) if $m \equiv 0 \pmod{3}$ (resp. $m \not\equiv 0 \pmod{3}$).

(1) If $m \equiv 0 \pmod 3$, the result follows from Proposition 4.1.

(2) Let $m \equiv 1 \pmod 3$, then we set $p = 3gh + 3r + 2$ since 3 divides $p+1$. By the above conditions, we have $0 \leq r \leq g-1$. If $r = g-1$, then we get $3r+2 = 3g-1$ and we conclude that the curve $\mathcal{C}(3,m)$ is covered by the Hermitian curve and so is $\mathbb{F}_{p^2}$-maximal. We show that for any other cases this curve can not be maximal. In fact, we show that for any r such that $0 \leq r \leq g-2$ there exist a regular 1-form ω which $\mathfrak{C}(\omega) \neq 0$.

Let $p = 3gh + 3r + 2$. So $p - 2 = 3gh + 3r$ or $(p-2)/3 = gh + r$. For any $0 \leq i \leq \frac{(2g-2)}{3}$ we obtain

$$\mathfrak{C}(\omega_{i,0}) = \mathfrak{C}(x^i dx/y^2) = \mathfrak{C}(y^{q-2}y^{-p}x^i dx) =$$
$$y^{-1}\mathfrak{C}((x^{g+1}+x)^{gh+r}x^i dx) = y^{-1}\Sigma_{\ell=0}^{gh+r} b_\ell \mathfrak{C}(x^{gh+r+i+\ell g}dx)\,.$$

Set $g = m-1 = 3t$. In the following we show that for any r such that $0 \leq r \leq g-2 = 3t-2$ we can find an integer b such that $gh + r + i + \ell g = bp - 1$ or equivalently,

$$i + \ell g = (3b-1)gh + (3b-1)r + (2b-1) \text{ with } 0 \leq \ell \leq gh + r\,, \tag{4.1}$$

and so we obtain $\mathfrak{C}(\omega_{i,0}) = \omega_{b-1,1} \neq 0$.

For $0 \leq r \leq t-1$: it is sufficient to put $b = 1$ and $\ell = 2h$ since $0 \leq i \leq \frac{(2g-2)}{3} \leq 2t-1$.

For $r = t > 1$: in this case we have $p = 3gh + 3t + 2$ and so $m - 1 = g = 3t$ does not divide $p^2 - 1 = (3gh + 3t + 3)(3gh + 3t + 1)$. Thus the curve is not maximal over $\mathbb{F}_{p^2}$.

In the case $t = 1$ the curve is the Picard curve and we know the result.

For $t < r < 2.5t$: it is sufficient to find a suitable $1 < b$ and set $\ell = (3b-1)h + b$. Indeed from Equation (4.1) we get

$$i + \ell g = i + ((3b-1)h + b)g = (3b-1)gh + (3b-1)r + (2b-1)$$

which means that $(3b-1)r = i + 3bt - (2b-1)$. As $0 \leq i \leq 2t-1$,

$$\frac{3b}{3b-1}t < r < \frac{3b+2}{3b-1}t$$

or equivalently we get

$$t + \frac{1}{3b-1}t < r < t + \frac{3}{3b-1}t\,.$$

For $2.4t < r < 3t-2$: it is sufficient to find a suitable $2 \leq b$ and set $\ell = (3b-1)h + 3b - 2$. Indeed from Equation (4.1) we get

$$i + \ell g = i + ((3b-1)h + 3b - 2)g = (3b-1)gh + (3b-1)r + (2b-1)$$

which means that $(3b-1)r = i + 9bt - 6t - (2b-1)$. As $0 \leq i \leq 2t-1$,

$$\frac{9b-6}{3b-1}t < r < \frac{9b-4}{3b-1}t$$

or equivalently we get

$$2t + \frac{3b-4}{3b-1}t < r < 2t + \frac{3b-2}{3b-1}t\,.$$

(3) Similarly we can prove the result for the case $m \equiv 2 \pmod 3$. In this case, if $r = g-1$ (resp. $r = (g-1)/3$), then we get $3r+2 = 3g-1$ (resp. $3r+2 = g+1 = m$) and we conclude that the curve $\mathcal{C}(3,m)$ is covered by the Hermitian curve and so it is maximal.

We show that for any other cases this curve can not be maximal. In fact, we show that for any r such that $0 \leq r \leq g-2$ there exist a regular 1-form ω which $\mathfrak{C}(\omega) \neq 0$. To respect the proof of the above case: if we set $g = 3t+1$, then the case $r = t$ is equivalent to $r = (g-1)/3$. Other cases are similar. □

Remark 4.16. Theorem 4.15 might be true for curves $\mathcal{C}(3,m)$ over $\mathbb{F}_{q^2}$ being q an arbitrary power of a prime. See the following example.

Example 4.17. Let q be a power of a prime bigger than 3. Then the curve $\mathcal{C} := \mathcal{C}(3,7)$ is maximal over $\mathbb{F}_{q^2}$ if and only if $q \equiv -1 \pmod{18}$. Here we have $s = 3 \times 6 = 18$. Thus according to Proposition 4.10, $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$ if $q \equiv -1 \pmod{18}$. Conversely, if $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$, then 3 divides $q+1$. Thus we conclude that 3 divides $p+1$ and a is odd, where $q = p^a$. Thus the following cases $p \equiv 5, 11, 17 \pmod{18}$ might occur. If $p \equiv 17 \pmod{18}$, then we get $q \equiv 17 \pmod{18}$ since a is odd. In the cases $p \equiv 5, 11 \pmod{18}$, we obtain that $p^3 \equiv -1 \pmod{18}$ and so $\mathcal{C}$ is maximal over $\mathbb{F}_{p^6}$. Now if 3 divides a, then $q \equiv -1 \pmod{18}$ and the result follows. Otherwise, if 3 does not divide a, as $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$ and $\mathbb{F}_{p^6}$, we conclude that the curve $\mathcal{C}$ is maximal also over $\mathbb{F}_{p^2}$ (see the proof of Theorem 18 in [14]). But this is impossible by Theorem 4.15.

Theorem 4.18. *Let $q = p^a$ be a power of a prime p. Let $n \geq 4$ be an integer. Then the curve $\mathcal{C}(n,3)$ given by the equation $y^n = x^3 + x$ is maximal over $\mathbb{F}_{q^2}$ if and only if either $n = 4$ and $q \equiv -1, 3 \pmod 8$, or $n > 4$ and $q \equiv -1 \pmod{2n}$. In any case, the curve $\mathcal{C}(n,3)$ is $\mathbb{F}_{q^2}$-covered by the Hermitian curve.*

Proof. First we consider the case $n = 4$ and $m = 3$. Here $s = 4 \times 2 = 8$ and the result follows from Propositions 4.10, 4.12, and Remark 4.5. Let $n > 4$ and thus $s = n \times 2$. If $q \equiv -1 \pmod{2n}$, the curve $\mathcal{C}(n,3)$ is maximal over $\mathbb{F}_{q^2}$ by Proposition 4.10. Conversely, suppose that $\mathcal{C}(n,3)$ is maximal over $\mathbb{F}_{q^2}$. Then by Proposition 4.4, n is a divisor of $q+1$. We want to show that $2n$ divides $q+1$. The only situation to be investigated is the following:

$q+1 = 2^r t_1$ with t_1 an odd integer and $n = 2^r t_2$ with t_2 a divisor of t_1. But this case does not occur. In fact, below we show that the curve $\mathcal{C}(2^r, 3)$ is not maximal over $\mathbb{F}_{q^2}$. Two cases arise:

1. a is even. Here we have $q+1 = 2t_1$ where t_1 is odd. If the hyperelliptic curve $y^2 = x^3 + x$ of genus $g = 1$ is maximal over $\mathbb{F}_{q^2}$, then from Proposition 4.3 we conclude that 4 divides $q+1$ which is a contradiction.

2. a is odd. In this case, if $q+1 = 2^r t_1$ with t_1 odd, then we also have $p+1 = 2^r t$ with t odd. Here we can assume $r \geq 3$. Next as the genus of $\mathcal{C}$ is $g = 2^r - 1$ we fix the following

basis for regular 1-forms

$$\mathfrak{B} = \{\omega_{i,j} := x^i y^j dx/y^{(2^r-1)} \text{ with } 2^{r+1} - 4 - 2^r i - 3j \geq 0\}\,.$$

Now as for any j we can write $j-(2^r-1) = -(j+1)p + [(j+1)t-1]2^r$, we get

$$\mathfrak{C}(\omega_{0,j}) = \mathfrak{C}(y^j dx/y^{2^r-1}) = \mathfrak{C}(y^{-(j+1)p} y^{[(j+1)t-1]2^r} dx) =$$
$$y^{-(j+1)}\mathfrak{C}((x^3+x)^{(j+1)t-1}dx) = y^{-(j+1)}\Sigma_{\ell=0}^{(2j+1)} b_\ell \mathfrak{C}(x^{2\ell+(j+1)t-1}dx)\,.$$

Now if we set $j = 2^{r-1}$ and $\ell_1 = (2^{r-1}t - t - 1)/2$ we obtain

$$\mathfrak{C}(\omega_{0,2^{r-1}}) = b_{\ell_1}\omega_{0,2^{r-1}-2} \neq 0\,.$$

And if we set $j = 2^{r-1}-2$ and $\ell_2 = (2^{r-1}t + t - 1)/2$ we obtain

$$\mathfrak{C}(\omega_{0,2^{r-1}-2}) = b_{\ell_2}\omega_{0,2^{r-1}} \neq 0\,.$$

From Lemma 2.2 this is a contradiction because $\mathfrak{C}^a(\omega_{0,2^{r-1}})$ is not zero. Thus we conclude that the curve $\mathcal{C}(2^r, 3)$ is not maximal. □

We end up this paper by characterizing maximal curves of type $\mathcal{C}(4,7)$.

Example 4.19. Let q be a power of a prime bigger than 3. The curve $\mathcal{C}(4,7)$ given by the equation $y^4 = x^7 + x$ is maximal over $\mathbb{F}_{q^2}$ if and only if $q \equiv -1, 7 \pmod{24}$. In particular, this curve is covered by the Hermitian curve.

We have that $\mathcal{C}(4,7)$ is maximal over $\mathbb{F}_{q^2}$ provided that $q \equiv -1, 7$ by Propositions 4.10 and 4.13. Conversely, if the curve $\mathcal{C}(4,7)$ is maximal over $\mathbb{F}_{q^2}$, then Remark 4.5 implies $q \equiv -1, 7, 11, 19 \pmod{24}$. Let $q = p^a$ and assume that $q \equiv 11, 19 \pmod{24}$. From $q \equiv -1 \pmod 4$ it follows that $p \equiv 11, 19 \pmod{24}$ and a is odd. In these cases, we show that $\mathfrak{C}(\omega_1) = \omega_7$ and $\mathfrak{C}(\omega_7) = \omega_1$ which means that $\mathfrak{C}^d \neq 0$ for any $d > 0$. But we know that if the curve $\mathcal{C}(4,7)$ is maximal over $\mathbb{F}_{q^2}$, then $\mathfrak{C}^a = 0$ where $q = p^a$ by Lemma 2.2.

Let $p \equiv 11 \pmod{24}$ and set $p = 24t + 11$. So $3p - 1 = 4(18t+8)$ or $(3p-1)/4 = 18t + 8$.

$$\mathfrak{C}(\omega_1) = \mathfrak{C}(dx/y) = \mathfrak{C}(y^{3p-1}y^{-3p}dx) = y^{-3}\mathfrak{C}((x^7+x)^{18t+8}dx)$$
$$= y^{-3}\Sigma_{i=0}^{18t+8} b_i \mathfrak{C}(x^{6i+18t+8}dx) = x^2 dx/y^3 = \omega_7,$$

since for $i = 9t + 4$ we get $3p - 1 = 72t + 32 = 6(9t+4) + 18t + 8$.

Let $p \equiv 11 \pmod{24}$ and set $p = 24t + 11$. So $p - 3 = 4(6t+2)$ or $(p-3)/4 = 6t + 2$. Thus

$$\mathfrak{C}(\omega_7) = \mathfrak{C}(x^2 dx/y^3) = \mathfrak{C}(y^{p-3}y^{-p}dx) = y^{-1}\mathfrak{C}((x^7+x)^{6t+2}x^2 dx)$$
$$y^{-1}\Sigma_{i=0}^{6t+2} b_i \mathfrak{C}(x^{6i+6t+4}dx) = dx/y = \omega_1,$$

since for $i = 3t + 1$ we get $p - 1 = 24t + 10 = 6(3t+1) + 6t + 4$.

Let $p \equiv 19 \pmod{24}$ and set $p = 24t+19$. So $3p-1 = 4(18t+14)$ or $(3p-1)/4 = 18t+14$. Thus

$$\mathfrak{C}(\omega_1) = \mathfrak{C}(dx/y) = \mathfrak{C}(y^{3p-1}y^{-3p}dx) = y^{-3}\mathfrak{C}((x^7+x)^{18t+14}dx)$$

$$= y^{-3}\Sigma_{i=0}^{18t+14} b_i \mathfrak{C}(x^{6i+18t+14}dx) = x^2dx/y^3 = \omega_7,$$

since for $i = 9t + 7$ we get $3p - 1 = 72t + 56 = 6(9t + 7) + 18t + 14$.

Let $p \equiv 19 \pmod{24}$ and set $p = 24t + 19$. So $p - 3 = 4(6t + 4)$ or $(p - 3)/4 = 6t + 4$. Thus

$$\mathfrak{C}(\omega_7) = \mathfrak{C}(x^2dx/y^3) = \mathfrak{C}(y^{p-3}y^{-p}dx) = y^{-1}\mathfrak{C}((x^7 + x)^{6t+4}x^2dx)$$

$$= y^{-1}\Sigma_{i=0}^{6t+4} b_i \mathfrak{C}(x^{6i+6t+6}dx) = dx/y = \omega_1,$$

since for $i = 3t + 2$ we get $p - 1 = 24t + 18 = 6(3t + 2) + 6t + 6$.

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] I. 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.

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

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

[5] A. Garcia, M.K. Kawakita and S. Miura, *On certain subcovers of the Hermitian curve*, Comm. Algebra **34** (2006), 973–982.

[6] A. Garcia and H. Stichtenoth, *A maximal curve which is not a Galois subcover of 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] A. Garcia and S. Tafazolian, *On additive polynomials and certain maximal curves*, J. Pure Appl. Algebra **212** (2008), 2513–2521.

[10] M. Giulietti, J.W.P. Hirschfeld, G. Korchmáros and F. Torres, *Curves covered by the Hermitian curve*, Finite
Fields Appl. **12** (2006), 539–564.

[11] M. Giulietti and G. Korchmáros, *A new family of maximal curves over a finite field*, Math. Ann. **343** (2009), 229–245.

[12] J. W.P, Hirschfeld, G. Korchmáros and F. Torres, "Algebraic curves over a finite field", Princeton Univ. Press, 2008.

[13] A. Kazemifard, A. R. Naghipour and S. Tafazolian, *A note on superspecial and maximal curves*, Bull. Iranian Math. Soc. **39** (2013), 405–413.

[14] A. Kazemifard and S. Tafazolian, *A note on some Picard curves over finite fields*, preprint.

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

[16] H. Stichtenoth, "Algebraic function fields and codes", second ed., Grad. Texts in Math., vol. 254, Springer–Verlag, 2009.

[17] S. Tafazolian, *A characterization of maximal and minimal Fermat curves*, Finite Fields Appl. **16** (2010), 1–3.
[18] S. Tafazolian, *A family of maximal hyperelliptic curves*, J. Pure Appl. Algebra **216** (2012), 1528–1532.
[19] S. Tafazolian and F. Torres, *On maximal curves of Fermat type*, Adv. Geom., **13** (2013), 613–617.
[20] 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