On additive polynomials and certain maximal curves

Arnaldo Garcia*and Saeed Tafazolian
IMPA-Instituto Nacional de Matemática Pura e Aplicada,
Estrada Dona Castorina 110, Rio de Janeiro, Brazil
E-mail: garcia@impa.br and saeed@impa.br

Abstract

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

MSC: 11G20; 11T23; 14H25; 14H40

1 Introduction

By a curve we mean a smooth geometrically irreducible projective curve. Explicit curves (i.e., curves given by explicit equations) over finite fields with many rational points with respect to their genera have attracted a lot of attention, after Goppa discovered that they can be used to construct good linear error-correcting codes. For the number of $\mathbb{F}_q$-rational points on the curve $\mathcal{C}$ of genus $g(\mathcal{C})$ over $\mathbb{F}_q$ we have the following bound

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

which is well-known as the Hasse-Weil bound. This is a deep result due to Hasse for elliptic curves, and for general curves is due to A. Weil. When the cardinality of the finite field is square, a curve $\mathcal{C}$ over $\mathbb{F}_{q^2}$ is called maximal if it attains the Hasse-Weil bound, i.e., if we have the equality

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

From Ihara [9] we know that the genus of a maximal curve over $\mathbb{F}_{q^2}$ is bounded by

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

*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])

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

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

Remark 1.1. As J. P. Serre has shown, a subcover of a maximal curve is maximal (see [10]). So one way to construct explicit maximal curves is to find equations for Galois subcovers of the Hermitian curve (see [3] and [7]).

Let k be a field of positive characteristic p. An additive polynomial in $k[X]$ is a polynomial of the form

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

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

$$A(X) = F(Y) \tag{2}$$

where $A(X)$ is an additive and separable polynomial in $\mathbb{F}_{q^2}[X]$ and $F(Y) \in \mathbb{F}_{q^2}[Y]$ is a polynomial of degree m prime to the characteristic $p > 0$ of the finite field. The assumption that $F(Y)$ is a polynomial is not too restrictive (see Lemma 4.1 and Remark 4.2). The genus of the curve $\mathcal{C}$ is given by

$$2g(\mathcal{C}) = (degA - 1)(m - 1). \tag{3}$$

Maximal curves given by equations as in (2) above were already studied. In [1] they are classified under the assumption $m = q+1$ and a hypothesis on Weierstrass nongaps at a point; in [4] it is shown that if $A(X)$ has coefficients in the finite field $\mathbb{F}_q$ and $F(Y) = Y^{q+1}$, then the curve $\mathcal{C}$ is covered by the Hermitian curve ; and in [5] it is shown that if $\deg F(Y) = m = q + 1$, then the maximality of the curve $\mathcal{C}$ implies that the polynomial $A(X)$ has all roots in $\mathbb{F}_{q^2}$.

Here we generalize the above mentioned result from [5]; i.e., we show that a maximal curve $\mathcal{C}$ over $\mathbb{F}_{q^2}$ given by Equation (2) is such that all roots of $A(X)$ belong to $\mathbb{F}_{q^2}$ (see Theorem 4.3). The proof of this result uses ideas and arguments from [12] and [13].

Our main result in this work is the following theorem. For the proof we will use the p-adic Newton polygon of Artin-Schreier curves that is described in the next section (see Remark 2.5 here).

Theorem 1.2. *Let $\mathcal{C}$ be a maximal curve over $\mathbb{F}_{q^2}$ given by an equation of the form*

$$A(X) = Y^m \quad with \quad gcd(p, m) = 1, \tag{4}$$

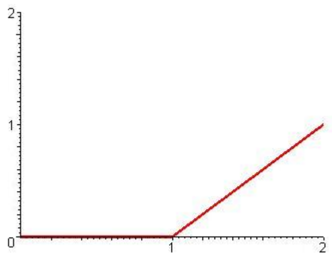
where $A(X) \in \mathbb{F}_{q^2}[X]$ is an additive and separable polynomial. Then we must have that m divides $q + 1$.

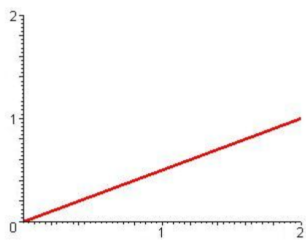
2 p-Adic Newton Polygons

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

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

Example 2.1. Let $\mathcal{C}$ be an elliptic curve over $\mathbb{F}_q$. There are only two possibilities for the Newton polygon of $\mathcal{C}$ as illustrated in the following pictures:





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

Remark 2.2. In the case of curves, we know that if L(t) is the numerator of the zeta function associated to the curve, then $f(t) = t^{2g} L(t^{-1})$ is the characteristic polynomial of the Frobenius action on the Jacobian of the curve. The Newton polygon of the curve is by definition the Newton polygon of the polynomial $f(t)$.

We recall the following fact about maximal curves (see [17] and [15, page 189]) :

Proposition 2.3. *Suppose q is square. For a smooth geometrically irreducible projective curve $\mathcal{C}$ of genus g, defined over $k = \mathbb{F}_q$, the following conditions are equivalent:*

- *$\mathcal{C}$ is maximal.*
- *$L(t) = (1 + \sqrt{q}t)^{2g}$, where $L(t)$ is the numerator of the associated zeta function.*
- *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.*

Now we can easily show that the following corollary holds, where we use the notation of Remark 2.2.

Corollary 2.4. *If the curve $\mathcal{C}$ is maximal, then all slopes of the Newton polygon of $\mathcal{C}$ are equal to $1/2$. In particular, its Hasse-Witt invariant is zero.*

Proof. Write $f(t) = \sum_{i=0}^{2g} b_i t^{2g-i}$. We have from Proposition 2.3 that $f(t) = (t+\sqrt{q})^{2g}$ and hence $b_i = \binom{2g}{i}(\sqrt{q})^i$. Thus $v_q(b_i) = v_q(\binom{2g}{i}) + \frac{i}{2} \geqslant \frac{i}{2}$, and this shows that all points $(i, v_q(b_i))$ are above or on the line $y = \frac{x}{2}$. Note that $b_{2g} = q^g$ and so $(2g, v_q(b_{2g})) = (2g, g)$ lies on the line $y = \frac{x}{2}$. ■

Remark 2.5. Consider the Artin-Schreier curve $\mathcal{C}$ given by $X^p - X = Y^d$, where $\gcd(d,p) = 1$ and $d \geq 3$. From Remark 1.4 of [19] we can describe the Newton polygon of $\mathcal{C}$ as below:

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

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

This Remark 2.5 will play a fundamental role in our proof of Theorem 4.10 and Lemma 4.11.

3 Additive Polynomials

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

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

Consider the equation

$$A(X) = 0. \tag{5}$$

We know that the roots of Equation (5) form a vector space of dimension n over $\mathbb{F}_p$. Hence there exists a basis

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

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

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

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

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

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

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

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

where

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

and

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

Hence

$$A_t(X) = A_{t-1}(X)A_{t-1}(X - \omega_t)\ldots A_{t-1}(X - (p-1)\omega_t). \tag{6}$$

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

The following lemma is crucial for us (see [13, Equation 11]):

Lemma 3.1. *Let $A(X) = \sum_{i=0}^{n} a_i X^{p^i}$ be an additive and separable polynomial. Then $A(X)$ is left divisible by $X^p - \alpha X$ if and only if α is a root of the equation*

$$a_n^{1/p^n} Y^{(p^n-1)/((p-1)p^{n-1})} + a_{n-1}^{1/p^{n-1}} Y^{(p^{n-1}-1)/((p-1)p^{n-2})} + \ldots + a_1^{1/p} Y + a_0 = 0. \tag{7}$$

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

$$a_n + a_{n-1}^p + a_{n-2}^{p^2} + ... + a_0^{p^n} = 0. \tag{8}$$

Corollary 3.2. *If the polynomial* $A(X) = \sum_{i=0}^{n} a_i X^{p^i}$ *has* $(*)-$*property, then* $A(X)$ *is left divisible by* $a(X) = X^p - X$.

Proof. The result follows from Lemma 3.1 with $\alpha = 1$. ■

Definition. For the additive and separable polynomial

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

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

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

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

Lemma 3.3. *If* $A(X) \in k[X]$ *is a monic additive and separable polynomial and* $\alpha^{-1} \in \bar{k}$ *is a root of the adjoint polynomial* $\bar{A}(X)$*, then* $\alpha^{-1} A(\alpha X)$ *has* $(*)-$*property.*

Proof. Write $A(X)$ as below

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

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

$$\alpha^{-1} A(\alpha X) = \alpha^{p^n - 1} X^{p^n} + a_{n-1} \alpha^{p^{n-1}-1} X^{p^{n-1}} + \ldots + a_1 \alpha^{p-1} X^p + a_0 X. \tag{9}$$

Now we verify that $\alpha^{-1} A(\alpha X)$ has $(*)-$property. This follows from the choice of α^{-1} as a root of the adjoint polynomial of $A(X)$. In fact we have

$$\begin{aligned} &\alpha^{p^n - 1} + (a_{n-1} \alpha^{p^{n-1}-1})^p + \ldots + (a_1 \alpha^{p-1})^{p^{n-1}} + (a_0)^{p^n} \\ &= \alpha^{p^n} . (\frac{1}{\alpha} + (\frac{a_{n-1}}{\alpha})^p + \ldots + (\frac{a_1}{\alpha})^{p^{n-1}} + (\frac{a_0}{\alpha})^{p^n}) \\ &= \alpha^{p^n} . \bar{A}(\alpha^{-1}) = 0. \ ■ \end{aligned} \tag{10}$$

Example 3.4. Consider the Hermitian curve $\mathcal{C}$ over $\mathbb{F}_{q^2}$ given by $X^q + X = Y^{q+1}$. Take $\alpha \in \mathbb{F}_{q^2}$ such that $\alpha^q + \alpha = 0$. Changing variable $X_1 := \alpha^{-1} X$ we have that the Hermitian curve can also be given as below:

$$Y^{q+1} = (\alpha X_1)^q + (\alpha X_1) = -\alpha (X_1^q - X_1). \tag{11}$$

With $A(X) = X^q + X$, we have $\alpha^{-1} A(\alpha X) = -(X_1^q - X_1)$; i.e., the additive polynomial $\alpha^{-1} A(\alpha X)$ has $(*)-$property.

The next lemma will be crucial in the proof of Theorem 4.3.

Lemma 3.5. *With notation as above, we have* $\mathcal{M}_A = \{\omega \in \bar{k} | A(\omega) = 0\} \subset k$ *if and only if* $\mathcal{M}_{\bar{A}} = \{\omega \in \bar{k} | \bar{A}(\omega) = 0\} \subset k$.

Proof. First we show that $\mathcal{M}_A \subset k$ implies $\mathcal{M}_{\bar{A}} \subset k$. Suppose $\omega_1, \omega_2, \ldots, \omega_n$ is a basis for $\mathcal{M}_A$. From the Equation (6) with $t = n$, we have

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

Hence we have

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

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

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

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

$$\begin{aligned}
\bar{\omega}_1 :=& (-1)^{n+1}\frac{\Delta(\omega_2, \omega_3, \ldots, \omega_n)}{\Delta(\omega_1, \omega_2, \ldots, \omega_n)} \\
\bar{\omega}_2 :=& (-1)^{n+2}\frac{\Delta(\omega_1, \omega_3, \ldots, \omega_n)}{\Delta(\omega_1, \omega_2, \ldots, \omega_n)} \\
&\vdots \\
\bar{\omega}_n :=& \frac{\Delta(\omega_1, \omega_2, \ldots, \omega_{n-1})}{\Delta(\omega_1, \omega_2, \ldots, \omega_n)},
\end{aligned} \tag{12}$$

then we have

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

Now according to Lemma 3.1, we can conclude that $\beta := (bA_{n-1}(\omega_n))^{p-1} = (b/\bar{\omega}_n)^{p-1}$ must be a root of Equation (7). Thus

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

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

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

We then conclude that

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

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

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

So $(\bar{\omega}_1/b)^p, (\bar{\omega}_2/b)^p, \ldots, (\bar{\omega}_n/b)^p$ are roots of $\bar{A}(X)$, and they form a basis over $\mathbb{F}_p$ for $\mathcal{M}_{\bar{A}}$. Hence we have shown that $\mathcal{M}_A \subset k$ implies $\mathcal{M}_{\bar{A}} \subset k$, since by Equation (12) we see that $(\bar{\omega}_1/b), \ldots, (\bar{\omega}_n/b)$ belong to k.

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

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

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

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

4 Certain Maximal Curves

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

$$A(X) = F(Y)$$

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

We start with a simple lemma:

Lemma 4.1. *With notation and hypotheses as above, if the curve $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$ then $F(Y)$ has only one pole which has order $m \leq q+1$.*

Proof. In [16] it was shown that the group of divisor classes of $\mathcal{C}$ of degree zero and order p has rank $\sigma = (\deg A - 1)(r-1)$ where r is the number of distinct poles of $F(Y)$ in $\bar{k} \cup \{\infty\}$. Hence $r = 1$, since according to Corollary 2.4 the Hasse-Witt invariant of a maximal curve is zero. By the genus formula we know

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

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

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

On the other hand one can observe that

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

Thus

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

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

Remark 4.2. Since $F(Y)$ is a rational function with coefficients in $\mathbb{F}_{q^2}$ and Lemma 4.1 shows that $F(Y)$ has a unique pole $\alpha \in \bar{\mathbb{F}}_q \cup \{\infty\}$, then this pole α lies in $\mathbb{F}_{q^2} \cup \{\infty\}$. If $\alpha \in \mathbb{F}_{q^2}$ then performing the substitution $Y \to 1/(Y - \alpha)$, we can assume that $F(Y)$ is a polynomial in $\mathbb{F}_{q^2}[Y]$.

The following theorem is similar to Theorem 1 in [12]:

Theorem 4.3. *Let $\mathcal{C}$ be a curve given by the equation $A(X) = F(Y)$, where $A(X) \in \mathbb{F}_{q^2}[X]$ is an additive and separable polynomial and $F(Y) \in \mathbb{F}_{q^2}[Y]$ is a polynomial of degree m relatively prime to the characteristic p. If the curve $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$, then all roots of $A(X)$ belong to $\mathbb{F}_{q^2}$.*

Proof. Let χ_1 denote the canonical additive character of $k = \mathbb{F}_{q^2}$. Denote by N the number of affine solutions of $A(X) = F(Y)$ over $\mathbb{F}_{q^2}$. The orthogonality relations of characters (see [11, page 189]) imply the equality

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

But we know from Theorem 5.34 in [11] that

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

So

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

We note that every affine point on the curve $\mathcal{C}$ over $\mathbb{F}_{q^2}$ is simple and $\mathcal{C}$ has exactly one infinite point. Hence the maximality of $\mathcal{C}$ and Weil's bound Theorem (see [11, Theorem 5.38]) imply that $\mathcal{M}_{\bar{A}} = \{c \in \bar{k} \mid \bar{A}(c) = 0\}$ is a subset of $\mathbb{F}_{q^2}$ and also that $\sum_{y \in k} \chi_1(-cF(y)) = (m-1)q$ for any $0 \neq c \in \mathcal{M}_{\bar{A}}$. So the desired result follows now from Lemma 3.5. ■

Remark 4.4. Let $\mathcal{C}$ be a curve over $\mathbb{F}_{q^2}$ given by an affine equation

$$G(X) = F(Y)$$

where $G(X)$ and $F(Y)$ are polynomials such that $G(X) - F(Y) \in \mathbb{F}_{q^2}[X, Y]$ is absolutely irreducible. Suppose that G and F are left divisible by g and f, respectively. Then the curve $\mathcal{C}_1$ given by

$$g(X) = f(Y),$$

is covered by the curve $\mathcal{C}$. In fact, write $G(X) = g(h_1(X))$ and $F(Y) = f(h_2(Y))$ and consider the surjective map from $\mathcal{C}$ to $\mathcal{C}_1$ given by $(x, y) \longmapsto (h_1(x), h_2(y))$.
Let $A(X)$ be an additive and separable polynomial with all roots in $\mathbb{F}_{q^2}$, that is left divisible by an additive polynomial $a(X)$. Then there exists an additive polynomial $u(X)$ such that

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

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

$$A(X) = F(Y) \qquad \text{and} \qquad a(X) = F(Y)$$

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

$$\sigma_\alpha(X) = X + \alpha \qquad \text{and} \qquad \sigma_\alpha(Y) = Y.$$

Lemma 4.5. *In the above situation, if the curve $\mathcal{C}$ given by $A(X) = aY^m + b$ is maximal over $k = \mathbb{F}_{q^2}$, then we must have that m is a divisor of $q^2 - 1$.*

Proof. Let d denote the $gcd(m, q^2 - 1)$. The curve $\mathcal{C}_1$ given by $A(X) = aZ^d + b$ is also maximal since it is covered by the curve $\mathcal{C}$ (indeed, just set $Z = Y^{\frac{m}{d}}$). We also have that $\{\alpha \in \mathbb{F}_{q^2} \mid \alpha \text{ is } m\text{-th power } \} = \{\alpha \in \mathbb{F}_{q^2} \mid \alpha \text{ is } d\text{-th power } \}$ and hence $\#\mathcal{C}(\mathbb{F}_{q^2}) = \#\mathcal{C}_1(\mathbb{F}_{q^2})$. Therefore $g(\mathcal{C}) = g(\mathcal{C}_1)$ and we then conclude from Equation (3) that $d = m$. ■

Lemma 4.6. *If $A(X) = F(Y)$ is maximal over $\mathbb{F}_{q^2}$, then there is a $\beta \in \mathbb{F}^*_{q^2}$ such that the curve $X^p - X = \beta F(Y)$ is also maximal.*

Proof. Since $A(X) = F(Y)$ is maximal over $\mathbb{F}_{q^2}$, Theorem 4.3 and Lemma 3.5 imply that $\bar{A}(X)$ has all roots in $\mathbb{F}_{q^2}$. Hence according to Lemma 3.3, there exists $\alpha \in \mathbb{F}^*_{q^2}$ such that $\alpha^{-1}A(\alpha X)$ has $(*)-$property. Take $\beta = \alpha^{-1}$. It then follows from Corollary 3.2 and Remark 4.4, that the curve $A(\alpha X) = F(Y)$ covers the curve $X^p - X = \beta F(Y)$. By Remark 1.1, the last curve is maximal. ■

Remark 4.7. Suppose m is a divisor of $q + 1$. It is well-known that $X^q - X = Y^m$ is maximal over $\mathbb{F}_{q^2}$ if and only if q is even or m divides $(q + 1)/2$. By Corollary 3.2 we have that $X^p - X = Y^m$ is also maximal.

Lemma 4.8. *Let β be an element of $\mathbb{F}^*_{q^2}$. If the curve $\mathcal{C}$ given by $X^p - X = \beta Y^m$ is maximal over $\mathbb{F}_{q^2}$ and $gcd(m, q + 1) = 1$, then m divides $(p - 1)$.*

Proof. Since m divides $q^2 - 1$ by Lemma 4.5 and $\gcd(m, q + 1) = 1$, then m is a divisor of $q - 1$. We denote by Tr the trace from $\mathbb{F}_{q^2}$ to $\mathbb{F}_p$. By Hilbert 90 Theorem, we know

$$\#\mathcal{C}(\mathbb{F}_{q^2}) = 1 + p + mpB, \tag{13}$$

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

$$\#\mathcal{C}(\mathbb{F}_{q^2}) = 1 + q^2 + (p - 1)(m - 1)q. \tag{14}$$

Comparing (13) and (14) gives

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

Hence

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

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

Remark 4.9. In Lemma 4.8, if the characteristic $p = 2$ then $m = p - 1 = 1$. The curve $\mathcal{C}$ is rational in this case. If $p = 3$ in Lemma 4.8, then again $m = 1$. The other possibility, $m = p - 1 = 2$ is discarded since we have $\gcd(m, q+1) = 1$.

Theorem 4.10. *Suppose that $m > 2$ is such that the characteristic p does not divide m and $gcd(m, q+1) = 1$. Then there is no maximal curve of the form $A(X) = Y^m$ over $\mathbb{F}_{q^2}$, where $A(X)$ is an additive and separable polynomial.*

Proof. If there is some maximal curve of this form, according to Lemma 4.6 and Lemma 4.8 there exists a nonzero element $\beta \in \mathbb{F}_{q^2}$ such that the curve $\mathcal{C}_1$ given by $X^p - X = \beta Y^m$ is also maximal and m must divide $p-1$. Now by using Remark 2.5, we know that the Newton polygon of $\mathcal{C}_1$ has slopes $1/m, 2/m, \ldots, (m-1)/m$. Therefore Corollary 2.4 implies that this curve is not maximal. ■

From the result above, we prove here Theorem 1.2 of Introduction.

Proof of Theorem 1.2. We consider two cases:

Case $p = 2$. In this case $\gcd(q+1, q-1) = 1$, and we know that m divides $q^2 - 1$ by Lemma 4.5. From Remark 1.1 we have that $A(X) = Y^d$ is also maximal for any prime divisor d of m. It now follows from Theorem 4.10 that this prime number d is a divisor of $q+1$. Since $\gcd(q+1, q-1) = 1$, we conclude that m divides $q+1$.

Case $p =$ odd. In this case $\gcd(q+1, q-1) = 2$. Reasoning as in the case $p = 2$, we get here that if d is an odd prime divisor of m then d is a divisor of $q+1$. The only situation still to be investigated is the following: $q + 1 = 2^r s$ with s an odd integer and $m = 2^{r_1} s_1$ with $r_1 > r$ and s_1 is a divisor of s. But according to Lemma 4.6 and the following lemma this case does not occur.

Lemma 4.11. *Assume that the characteristic p is odd and write $q + 1 = 2^r.s$ with s an odd integer. Denote by $m := 2^{r+1}$. Then there is no maximal curve over $\mathbb{F}_{q^2}$ of the form $X^p - X = \beta Y^m$ with $\beta \in \mathbb{F}_{q^2}^*$.*

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

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

$$\#\mathcal{C}(\mathbb{F}_{q^2}) = 1 + p + 4pB, \tag{15}$$

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

$$\#\mathcal{C}(\mathbb{F}_{q^2}) = 1 + q^2 + 3(p-1)q. \tag{16}$$

Comparing (15) and (16) gives

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

Hence

$$B = \frac{q/p - 1}{2}.\frac{q+1}{2} + \frac{q}{p}(p-1). \tag{17}$$

On the other hand, we have $\mathbb{F}_p^* \subset H$ since $(p-1)$ divides $(q^2-1)/4$. In fact since n is even we have that $p-1$ divides $(q-1)/2$. Therefore the multiplication by each element of $\mathbb{F}_p^*$ defines a map on S. This implies that $p-1$ is a divisor of B and so from Equation (17) we obtain that $p-1$ divides $(q/p-1)/2$. But this is impossible because n is even.

Case n is odd. We know the Newton polygon of a maximal curve over $\mathbb{F}_{q^2}$ is maximal, i.e. all slopes are $1/2$. Hence it is sufficient to show that the Newton polygon of the curve $\mathcal{C}$ is not maximal. As n is an odd number, the hypothesis $q+1 = 2^r.s$ implies $p+1 = 2^r.s_1$ with s_1 an odd integer. Hence $p \equiv 2^r - 1 \pmod{2^{r+1}}$ and $p(2^r-1) \equiv 1 \pmod{2^{r+1}}$. Now if we set $\theta := 2^r - 1$, with the notation of Remark 2.5, the permutation σ has the 2-cycle (1θ) in its standard representation with disjoint cycles. This 2-cycle (1θ) corresponds to the slope $\lambda = (\theta+1)/(2.2^{r+1}) = 1/4$ and this finishes the proof. ■■

We end up with some comments on known results and examples. Let $q = p^n$ and let t be a positive integer. Wolfmann [18] considered the number of rational points on the Artin-Schreier curve $\mathcal{C}$ defined over $\mathbb{F}_{q^{2t}}$ by the equation

$$X^q - X = aY^m + b$$

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

Here we only consider the case m divides $q^t + 1$. He showed that $\mathcal{C}$ is maximal over $\mathbb{F}_{q^{2t}}$ if and only if

1) $Tr(b) = 0$ where Tr denotes the trace of $\mathbb{F}_{q^{2t}}$ over $\mathbb{F}_q$.

2) $a^u = (-1)^v$ where $um = q^{2t} - 1$ and $vm = q^t + 1$.

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

$${X_1}^q - X_1 = aY^m \quad \text{with} \quad X_1 := X - \alpha.$$

Example 4.12. Suppose n is an odd number. The curve $\mathcal{C}$ given as follows

$$X^{p^2} - X = Y^m \quad \text{with} \quad m = (p^n+1)/(p+1), \tag{18}$$

is maximal over $\mathbb{F}_{p^{2n}}$ (see [6] for the case $n = 3$). Setting here $q = p^2$ then the curve $\mathcal{C}$ is maximal over $\mathbb{F}_{q^n}$ with n odd. Hence this maximal curve is not among the ones considered in [18].

In [8] it is proved that for $p = 2$ and $n = 3$ this curve in (18) is a Galois subcover of the Hermitian curve. In [6] it is shown that this curve for $p = 3$ and $n = 3$ is not a Galois subcover of the Hermitian curve.

Example 4.13. Suppose now that $n = 2k$ is an even number. The curve given by

$$X^{p^k} - X = \beta Y^m$$

with $\beta^{p^n-1} = -1$ and m a divisor of p^n+1 is a Galois subcover of the Hermitian curve. Hence it is also maximal over $\mathbb{F}_{p^{2n}}$. This follows from the equation (see Example 3.4)

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

Setting here $q = p^k$ then this curve $\mathcal{C}$ is maximal over $\mathbb{F}_{q^4}$. Hence this maximal curve is among the ones considered in [18].

Acknowledgment. We thank H. J. Zhu for helpful discussions on the p-adic Newton polygon.

References

[1] M. Abdon, A. Garcia, On a characterization of certain maximal curves, *Finite Fields Appl.* **10** (2004), 133-158.

[2] P. Berthelot, Slopes of Frobenius in crystalline cohomology, In: *Algebraic Geometry* (Arcata 1974), Proceedings of symposia in pure mathematics, **29**, 315-328.

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

[4] A. Garcia, M.Q. Kawakita, S. Miura, On certain subcovers of the Hermitian curve, *Comm. Algebra* **34** (2006), 973-982.

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

[6] A. Garcia, H. Stichtenoth, A maximal curve which is not a Galois subcover of the Hermitian curve, *Bull. Braz. Math. Soc.* (N.S.) **37** (2006), 139–152.

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

[8] A. Garcia, F. Torres, On unramified coverings of maximal curves, to appear in *Proceedings AGCT-10,* held at CIRM-Marseille in September 2005.

[9] Y. Ihara, Some remarks on the number of rational points of algebraic curves over finite fields, *J.Fac. Sci. Tokyo* **28** (1981), 721-724.

[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] R. Lidl, H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, 1997.

[12] M. Moisio, A construction of a class of maximal Kummer curves, *Finite Fields Appl.* **11** (2005), 667–673.

[13] O. Ore, On a special class of polynomials, *Trans.Amer.Math.Soc.* **35** (1933), 559-584.

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

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

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

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

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

[19] H.J. Zhu, p-adic variation of L functions of one variable exponential sums. I. *Amer. J. Math.* **125** (2003), 669-690.