On maximal curves of Fermat type

Saeed Tafazolian* and Fernando Torres†

July 31, 2014

Abstract

The aim of this paper is to give a characterization of a maximal curve given by the equation $x^n + y^m = 1$ over a finite field $\mathbb{F}_{q^2}$.


By a curve over a field $k$ we mean a projective, non-singular, algebraic curve defined over $k$ and irreducible over the algebraic closure $\overline{k}$ of $k$. A curve $C$ of genus $g = g(C)$ defined over a finite field $\mathbb{F}_{q^2}$ with $q^2$ elements is called maximal over $\mathbb{F}_{q^2}$ if the cardinality of the set $C(\mathbb{F}_{q^2})$ of its $\mathbb{F}_{q^2}$-rational points attains the Hasse-Weil upper bound, that is,

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

Ihara (see [11, Proposition 5.3.3]) showed that if a curve $C$ is maximal over $\mathbb{F}_{q^2}$, then

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

Maximal curves with genus $(q - 1)q/2$ have been characterized, see [10]. Up to $\mathbb{F}_{q^2}$-isomorphism, there is just one maximal curve over $\mathbb{F}_{q^2}$ with this genus, the so-called Hermitian curve $H$ which can be given by the equation

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

Remark 1. As J. P. Serre has pointed out (see e.g. [8, Proposition 2.3]), if there is a morphism defined over the field $k$ between two curves $f : C \rightarrow D$, then the $L$-polynomial of $D$ divides the one of $C$. Hence a subcover $D$ of a maximal curve $C$ is also maximal. So one way to construct explicit maximal curves is to find equations for subcovers of the Hermitian curve (see e.g. [1], [4], [2]).

*The first author was supported by FAPESP/SP-Brazil grant 2012/02255-3.
†The second author was supported by CNPq-Brazil grant 306324/2011-3.
General facts on maximal curves can be seen in [3], [7, Chapter 10].
In this paper, we consider maximal curves $C(n, m)$ given by the equation
\[ x^n + y^m = 1 \]
on a finite field with $q^2$ elements. From [11, Example 6.3.3] it follows that
\[ g(C(n, m)) = 1/2[(n - 1)(m - 1) - \gcd(n, m) + 1]. \]
In the particular case, when $n = m$, it has been proved that the Fermat curve $C(m): x^m + y^m = 1$ is maximal over $\mathbb{F}_{q^2}$ if and only if $m$ divides $q + 1$; see [6, Theorem 4.4]
and also Theorem 4 here.

From Lemma 1 in [10] we have that:

**Proposition 2.** Let $C$ be a maximal curve over $\mathbb{F}_{q^2}$, and let $P_0$ and $P_1$ be two rational points. Then
\[ (q + 1)P_0 \sim (q + 1)P_1. \]
This result says that the linear system $|(q + 1)P_0|$, $P_0$ a rational point, is an $\mathbb{F}_{q^2}$-invariant of the curve. In particular, we have that $q + 1 \in H(P_0)$, the Weierstrass semigroup at $P_0$, i.e., $(q + 1)$ is a pole number at any rational point.

In [1] the authors use Lemma 3 below to characterize maximal Hurwitz curves, i.e., plane curves of type $x^my + y^m + x = 0$. Here we state some other applications of this lemma; for the sake of completeness we write a proof of such a result.

**Lemma 3.** Let $C$ be a maximal curve over $\mathbb{F}_{q^2}$, and let $P_0$ and $P_1$ be two rational points. Suppose that there exists a natural number $m$ such that $mP_0 \sim mP_1$. If $d := \gcd(m, q + 1)$, then $d$ is a pole number at $P_0$.

**Proof.** We can find two integers $r$ and $s$ such that $d = rm + s(q + 1)$. As we have $mP_0 \sim mP_1$, then $rmP_0 \sim rmP_1$. And also according to Proposition 2, we get $s(q + 1)P_0 \sim s(q + 1)P_1$. Hence we obtain
\[ dP_0 \sim dP_1 \]
and so the result follows. \qed

Now we are able to prove the main result of this paper, namely Theorem 5 below. First we give a simple proof of [6, Theorem 4.4].

**Theorem 4.** Let $C(m): x^m + y^m = 1$ be the Fermat curve of degree $m$ defined over $\mathbb{F}_{q^2}$. Then $C(m)$ is maximal over $\mathbb{F}_{q^2}$ if and only if $m$ divides $q + 1$. 

\[ 2 \]
Proof. (cf. [12, Theorem 5]) Suppose \( C(m) \) is maximal over \( \mathbb{F}_{q^2} \). We first show that

\[
q^2 \equiv 1 \pmod{m}.
\]

In fact, let \( f = \gcd(m, q^2 - 1) \). If \( C(m) \) is maximal over \( \mathbb{F}_{q^2} \), then the curve \( C_1 \) given by the equation \( y^f = 1 - x^m \) is also maximal since it is covered by the curve \( C(m) \). We also have

\[
\{ \alpha \in \mathbb{F}_{q^2} \mid \alpha \text{ is } m\text{-th power} \} = \{ \alpha \in \mathbb{F}_{q^2} \mid \alpha \text{ is } f\text{-th power} \}.
\]

The plane curve \( C_1 \) possesses just one infinite point, which is the center of \( f \) places of degree 1 in the function field \( \mathbb{F}_{q^2}(C_1) \), and that \( f \) is just the number of places of degree 1 centered at infinite points of \( C(m) \). Hence \( \#C(m)(\mathbb{F}_{q^2}) = \#C_1(\mathbb{F}_{q^2}) \). Therefore \( g(C(m)) = g(C_1) \) and we conclude that \( f = m \).

Consider now the affine equation of the curve: \( x^n + y^m = 1 \). For \( \alpha^m = \beta^m = 1 \) let \( P_\alpha = (0, \alpha) \) and \( P_\beta = (0, \beta) \). Hence \( P_\alpha \) and \( P_\beta \) are rational points because \( m \) divides \( q^2 - 1 \). Then \( \text{div}(y - \alpha) = mP_\alpha - D_1 \) and \( \text{div}(y - \beta) = mP_\beta - D_1 \), for some divisor \( D_1 \). Thus

\[
mP_\alpha \sim mP_\beta.
\]

We also have \( \text{div}(y) = \sum_\alpha P_\alpha - D_1 \); and so the Weierstrass semigroup at \( P_\alpha \) is generated by \( m - 1 \) and \( m \). If \( d := \gcd(m, q + 1) \), then by Lemma 3 \( d \in H(P_\alpha) \). Thus \( d = a(m - 1) + bm \) with \( a, b \geq 0 \), and \( m = cd = ca(m - 1) + bm \). It follows that \( d = m \). Conversely if \( m \) divides \( q + 1 \), then the curve \( C(m) \) is covered by the Hermitian curve \( H \) and so is maximal over \( \mathbb{F}_{q^2} \). This completes the proof. \( \square \)

Now we can generalize this result as follows:

**Theorem 5.** Suppose \( q \) is a power of a prime number \( p \) and let \( m > 1 \) and \( n > 1 \) be integers such that \( \gcd(p, m) = \gcd(p, n) = 1 \). Then the smooth complete curve \( C(n, m) \) corresponding to \( x^n + y^m = 1 \) is maximal over \( \mathbb{F}_{q^2} \) if and only if both integers \( n \) and \( m \) divide \( q + 1 \).

**Proof.** Suppose \( m \) and \( n \) divide \( q + 1 \). Let \( q + 1 = na = mb \) and consider the following morphism

\[
\begin{align*}
\mathcal{H} & \rightarrow C(n, m) \\
(x, y) & \mapsto (x^n, y^m).
\end{align*}
\]

Hence \( C(n, m) \) is covered by the Hermitian curve and Remark 1 implies that \( C(n, m) \) is maximal over \( \mathbb{F}_{q^2} \).

Consider now the affine equation of the curve: \( x^n + y^m = 1 \). If the curve \( C(n, m) \) is maximal over \( \mathbb{F}_{q^2} \) then as in the proof of Theorem 4 we can show that both \( n \) and \( m \) divide \( q^2 - 1 \). Now as \( m > 1 \) and \( n > 1 \) we have non-trivial factorization in prime
numbers, \( m = p_1^{r_1} \ldots p_t^{r_t} \) and \( n = p_1^{s_1} \ldots p_t^{s_t} \). Set \( w_i = \max\{r_i, s_i\} \). Then we shall show that \( p_i^{w_i} \) divides \( q + 1 \) for all \( 1 \leq i \leq t \). By Remark 1, the curve

\[
x^{p_i^{w_i}} + y^{p_j^{s_j}} = 1
\]

is maximal over \( \mathbb{F}_{q^2} \). Two cases might arise,

**Case** \( p_i = p_j \). Here again by Remark 1 the curve \( x^{p_i} + y^{p_i} = 1 \) is maximal over \( \mathbb{F}_{q^2} \) so that \( p_i \) divides \( q + 1 \) by Theorem 4. Let \( w_i \geq 2 \). If \( p_i > 2 \), then \( p_i^{w_i} \) divides \( q + 1 \) since \( m \) and \( n \) divide \( q^2 - 1 \) and \( \gcd(q + 1, q - 1) = 2 \). Let \( p_i = 2 \). We are led to a maximal curve over \( \mathbb{F}_{q^2} \) defined by an equation of type \( x^{2r+1} + y^2 = 1 \), where \( q + 1 = 2^s \) with \( s \) an odd integer. It has been shown that the Hasse-Witt invariant of this curve is not zero [13, Lemma 10] so that it cannot be maximal; this rule out the case \( p_i = 2 \).

**Case** \( p_i \neq p_j \). In this case, we can assume \( m = p_i^{r_i} \) and \( n = p_j^{s_j} \) so that \( \gcd(n, m) = 1 \). Due to similarity, we only show that \( m \) divides \( q + 1 \). For \( \alpha^n = \beta^n = 1 \), let \( P_\alpha = (\alpha, 0) \) and \( P_\beta = (\beta, 0) \). Hence \( P_\alpha \) and \( P_\beta \) are \( \mathbb{F}_{q^2} \)-rational points of \( \mathcal{C}(n, m) \). Thus we obtain that \( \text{div}(x - \alpha) = mP_\alpha - D_1 \) and \( \text{div}(x - \beta) = mP_\beta - D_1 \) for some positive divisor \( D_1 \). Thus

\[
mP_\alpha \sim mP_\beta
\]

and from from Lemma 3 we get that \( d := \gcd(m, q + 1) \) belongs to the Weierstrass semigroup \( H(P_\alpha) \) at \( P_\alpha \).

On the other hand, from [9, p. 115] it is known that \( H(P_\alpha) \) is given by

\[
H(P_\alpha) = \mathbb{N} - \{im + j + 1 \mid i, j \geq 0 \text{ and } 2g - 2 - (im + jn) \geq 0\}.
\]

Thus, as \( d = 0m + (d - 1) + 1 \), then \( 2g - 2 - [0m + (d - 1)n] < 0 \) since \( d \in H(P_\alpha) \). This means that \( dn > nm - m - 1 \). If \( n > 2 \), then it is clear that \( d > m/2 \). If \( n = 2 \), then we have \( 2d > m - 1 \). So \( 2d > m \) since \( \gcd(n, m) = 1 \). Hence we conclude that \( d = m \).

**Remark 6.** Let \( m \) be a positive integer number. Then the curve

\[
\mathcal{C}(1, m) : x + y^m = 1
\]

is clearly maximal over \( \mathbb{F}_{q^2} \) for any \( q \). In particular, not necessarily \( m \) divides \( q + 1 \).

**Remark 7.** Suppose \( \text{char}(k) = p > 2 \). In [13] the author has shown that the hyperelliptic curve given by the equation \( y^2 = x^m + 1 \) is maximal over \( \mathbb{F}_{q^2} \) if and only if \( m \) divides \( q + 1 \); Theorem 5 generalizes this result.

**Remark 8.** For \( n, m > 1 \) integers, Theorem 5 shows that the curve \( x^n + y^m = 1 \) is maximal over \( \mathbb{F}_{q^2} \) if and only if it is covered by the Hermitian curve \( \mathcal{H} \) over \( \mathbb{F}_{q^2} \).
We finish this note by giving another application of Lemma 3 above. In particular, we give a simple proof of [5, Theorem 1.2].

**Theorem 9.** Let \( C \) be a maximal curve over \( \mathbb{F}_{q^2} \), \( q \) a power of \( p \), given by an equation of the form
\[
A(x) = y^m \quad \text{with} \quad \gcd(p, m) = 1,
\]
where \( A(x) \in \mathbb{F}_{q^2}[x] \) is an additive and separable polynomial with \( \deg(A(x)) > 1 \). Then we must have that \( m \) divides \( q + 1 \).

**Proof.** Suppose \( \deg(A(x)) = p^t \). Let \( P_0 \) and \( P_\infty \) be the \( \mathbb{F}_{q^2} \)-rational points over \( x = 0 \) and \( x = \infty \), respectively. Then \( mP_0 \sim mP_\infty \) and hence by using Lemma 3, \( d := \gcd(m, q + 1) \in H(P_\infty) \). One can show that \( p^t \) and \( m \) are both pole numbers at \( P_\infty \) and thus the Weierstrass semigroup \( H(P_\infty) \) is generated by \( p^t \) and \( m \) as \( g(C) = (p^t - 1)(m - 1)/2 \) (loc. cit.). This implies \( d = m \). \( \Box \)

**Acknowledgment.** We are grateful to H. Stichtenoth who suggested us to write some applications of Lemma 3. We also thank the referee for pointing out Remark 6 and for valuable comments and suggestions which led to improve the exposition of the paper. We also want to thank H. Borges for point out to us a mistake in the proof of Theorem 9.

**References**


UNICAMP/IMECC
Rua Sérgio Buarque de Holanda, 651
Cidade Universitária, 13083 - 859
Campinas, SP, Brazil.
E-mail: tafazolian@ime.unicamp.br, fتورres@ime.unicamp.br