ON THE CURVE $Y^n = X^\ell(X^m+1)$ OVER FINITE FIELDS II

SAEED TAFAZOLIAN AND FERNANDO TORRES

Abstract. Let $\mathbb{F}$ be the finite field of order $q^2$. In this paper we continue the study in [20], [19], [18] of $\mathbb{F}$-maximal curves defined by equations of type $y^n = x^\ell(x^m+1)$. For example new results are obtained via certain subcovers of the nonsingular model of $v^N = u^{t^\alpha} - u$ where $q = t^\alpha$, $\alpha \geq 3$ odd and $N = (t^\alpha+1)/(t+1)$. We do observe that the case $\alpha = 3$ is closely related to the Giulietti-Korchmáros curve.

1. Introduction

Let $\mathcal{X}$ be a (projective, geometrically irreducible, nonsingular, algebraic) curve of genus $g = g(\mathcal{X})$ defined over the finite field $\mathbb{F} := \mathbb{F}_{q^2}$ of order $q^2$. We are interested in $\mathbb{F}$-maximal curves; that is, in those curves $\mathcal{X}$ such that its number $\#\mathcal{X}(\mathbb{F})$ of $\mathbb{F}$-rational points attains the Hasse-Weil upper bound $q^2 + 1 + 2q \cdot g$. Apart from their intrinsic interest, these curves are usually the building block of outstanding applications in Coding Theory, Cryptography, Finite Geometry and related areas; see for example [17], [10], [11]. Many results on maximal curves can be seen in [4], [10, Ch. 10] and their references.

As a side remark, a challenging problem arises, namely to find $\mathbb{F}$-maximal curves having a friendly plane model. This led to consider certain Kummer extensions of $\mathbb{P}^1$ (the projective line over the algebraic closure of $\mathbb{F}$)

(1.1) $y^n = f(x),$

where $n \geq 2$ is an integer and $f(x) \in \mathbb{F}[x]$ is a polynomial such that $y^n - f(x)$ is absolutely irreducible. These curves subsume several classical examples of curves over finite fields as we can see for example in [11], [13], [15]. Without loss of generality we assume throughout this paper that $q^2 \equiv 1 \pmod{n}$ (see [15, p. 51]).

In general, the genus of an $\mathbb{F}$-maximal curve $\mathcal{X}$ satisfies the so-called Ihara’s bound: $g(\mathcal{X}) \leq g_0 := q(q-1)/2$ (see e.g. [17, Prop. 5.3.3]); we have equality if and only if $\mathcal{X}$ is $\mathbb{F}$-isomorphic to the Hermitian curve $\mathcal{H}$ over $\mathbb{F}$ which can be defined by the plane curve $v^{q+1} = u^{q+1} + 1$ (see [14]). In particular, $\mathcal{H}$ is defined by a curve of type (1.1) and many other examples arise (see e.g. [5], [8]) by taking into consideration a result commonly attributed to J.P. Serre, namely that any curve $\mathbb{F}$-dominated by $\mathcal{H}$ is also $\mathbb{F}$-maximal [12].


Keywords: finite field, maximal curve, Kummer extension.

September 14, 2019.
Prop. 6. We do point out that the converse is not true, being the first counterexample described by Giulietti and Korchmáros [9]; as a matter of fact, they constructed an F-maximal curve which cannot be F-dominated by \( \mathcal{H} \) provided that \( q = t^3 > 8 \) (nowadays such a curve is simply called the GK-curve).

In [20], [19], [18] we basically considered F-maximal curves \( \mathcal{X}(n, \ell, m) \) with plane models of type (1.1) with \( f(x) = x^\ell(x^m + 1) \), where any of the following conditions hold true:

(a) \( \ell = 0 \) and both \( n \) and \( m \) divide \( q + 1 \);
(b) \( \ell = 1: \) \( nm \) divide \( q + 1 \), or \( m \equiv -2 \pmod{n} \) and \( q \equiv m + 1 \pmod{nm} \);
(c) \( \ell > 1 \) and \( nm \) divide \( q + 1 \).

In this paper we consider such curves \( \mathcal{X}(n, \ell, m) \) subject to any of the following complementary conditions:

(A) (See Section 2) Both \( n \) and \( m \) divide \( q + 1 \), and \( \ell = sm \) with \( s \geq 1 \) an integer;
(B) (See Section 3) \( n, \ell, m \) are positive integers such that \( n \) divides \( q + 1 \), \( m \) divides \( q - 1 \), and \( n \) divides \( \frac{\ell(q - 1)}{m} - 1 \);
(C) (See Section 4) We let \( q = t^\alpha \) with an integer \( \alpha \geq 3 \) odd, \( N = (t^\alpha + 1)/(t + 1) \). Thus \( \mathcal{X}(n, \ell, m) \) will be certain curves F-dominated by the non-singular model of \( v^N = u^{t^2} - u \) which in fact it is F-maximal; see [1]. We notice that the case \( \alpha = 3 \) is closely related to the aforementioned GK-curve; see [7].

Remark 1.1. Let \( q \) be as above. If \( m = n \), \( n \) divides \( q + 1 \) and \( \ell = sm \), then \( \mathcal{X}(n, \ell, m) \) is F-isomorphic to \( \mathcal{X}(n, 0, n) \) and this is Case (a) above. Thus we shall consider \( m \neq n \) in Case (A).

Remark 1.2. Let us recall that the genus of the curve \( \mathcal{X}(n, \ell, m) \) defined by (1.1) with \( f(x) = x^\ell(x^m + 1) \), where we always assume gcd\((q, nm)\) = 1, satisfies (see [20, Lemma 2.1])

\[
2g(\mathcal{X}) = (n - 1)m + 2 - \gcd(n, \ell) - \gcd(n, \ell + m).
\]

Moreover, without loss of generality, we can assume \( n > \ell \) since otherwise for \( \ell \equiv r \pmod{n} \) with \( 0 \leq r < n \), the curve \( \mathcal{X}(n, \ell, m) \) is F-isomorphic to \( \mathcal{X}(n, r, m) \); see [20, Remark 2.2].

2. Case (A)

In this section we consider the complementary Case (A) above.

**Proposition 2.1.** Suppose that \( n, m, s \) are positive integers such that both \( n \) and \( m \) divide \( q + 1 \). Let \( \ell = sm \). Then \( \mathcal{X}(n, \ell, m) \) is an F-maximal curve.

**Proof.** We show that \( \mathcal{X} \) is F-dominated by the Hermitian curve \( \mathcal{H} : v^{q+1} = u^{q+1} + 1 \). Indeed, set \( j := \frac{q + 1}{n} \) and \( k := \frac{q + 1}{m} \). Consider the following morphism

\[
\pi : \mathcal{H} \rightarrow \mathbf{P}^2, \quad (u, v, 1) \mapsto (x, y, 1) := (u^k, u^{sj} v^j, 1)
\]
which corresponds to the field extension $F(u, v)|F(x, y)$. Then $y^n = x^m(x^m + 1)$ is the plane model of $\pi(H)$ and hence $X'(n, \ell, m)$ is an $F$-maximal curve.

\[ (*) \]

**Example 2.2.** Let $q, m, s$ be as in Proposition 2.1. Suppose that $n = q + 1$, set $m = (q + 1)/b$ with $b = (q + 1)/m > s \geq 1$. Then by (1.2) the genus $g$ of the curve $X'(n, \ell, m)$, where $\ell = sm$, satisfies

\[
2g = mq + 2 - m \gcd((q + 1)/m, s) - m \gcd((q + 1)/m, s + 1); \quad \text{i.e.,}
\]

\[
2g = mq + 2 - m \gcd(b, s) - m \gcd(b, s + 1). \tag{2.1}
\]

Thus $g$ is of the form $Aq + B$ where $A, B$ are rational numbers. Recall that the spectrum for the genera of maximal curves over $F$ is the set

\[
M(q^2) := \{ g \in \mathbb{N}_0 : \text{there is an $F$-maximal curve of genus $g$} \}.
\]

A basic problem in Curve Theory over Finite Fields concerns the computation of $M(q^2)$; although its calculation is currently out of reach, in general we have

\[
\{ g_2, g_1, g_0 \} \subseteq M(q^2) \subseteq [0, g_2] \cup \{ g_1, g_0 \},
\]

where $g_2 := [(q^2 - q + 4)/6]$, $g_1 := [(q - 1)^2/4]$, and $g_0 = q(q - 1)/2$ is the aforementioned Ihara’s bound (see [10, §10.5]). Calculations for $q \leq 16$ can be found in [2].

By using formula (2.1) let us work out next some concrete examples.

(I) Let $s = 1$. If $b = (q + 1)/m > 1$ is even (resp. odd), then $2g = mq + 2 - m \gcd((q + 1)/m, s) - m \gcd((q + 1)/m, s + 1); \quad \text{i.e.,}$

\[
2g = mq + 2 - m \gcd(b, s) - m \gcd(b, s + 1). \tag{2.1}
\]

(a) Let $m = 1$. Thus if $q$ odd (resp. $q$ even), then $g = (q - 1)/2 \in M(q^2)$ (resp. $g = q/2 \in M(q^2)$). These values correspond to the biggest genus that an $F$-maximal hyperelliptic curve can have since in this case, the number of $F$-rational points is upper bounded by $2(q^2 + 1)$.

(b) Let $m = 2$. Then $b = (q + 1)/2 > 1$ is even (resp. odd) if and only if $q \equiv 3 \pmod{4}$ (resp. $q \equiv 1 \pmod{4}$) and so $g = q - 2 \in M(q^2)$ (resp. $g = q - 1 \in M(q^2)$).

(c) Let $m = 3$. Then $b = (q + 1)/3 > 1$ is even if and only if $q \equiv 5 \pmod{6}$ and so $g = (3q - 7)/2 \in M(q^2)$.

(d) Let $m = 4$. Then $b = (q + 1)/4 > 1$ is even (resp. odd) if and only if $q \equiv 7 \pmod{8}$ (resp. $q \equiv 3 \pmod{8}$, $q > 3$) and so $g = 2q - 5 \in M(q^2)$ (resp. $g = 2q - 3 \notin M(q^2)$).

(II) Let $s = 2$ and $b = (q + 1)/m > 2$. If $b \equiv 1, 5 \pmod{6}$ (resp. $b \equiv 2, 4 \pmod{6}$) (resp. $b \equiv 3 \pmod{6}$) (resp. $b \equiv 0 \pmod{6}$), then $2g = mq + 2 - m \gcd((q + 1)/m, s) - m \gcd((q + 1)/m, s + 1); \quad \text{i.e.,}$

\[
2g = mq + 2 - m \gcd(b, s) - m \gcd(b, s + 1). \tag{2.1}
\]

(a) In particular, for $m = 1$ and $q \equiv 5 \pmod{6}$, $g = (q - 3)/2 \in M(q^2)$.

(b) Let $m = 2$. Then $b = (q + 1)/2 \equiv 4 \pmod{6}$ if and only if $q \equiv 7 \pmod{12}$ and so $g = q - 2 \in M(q^2)$; $b = (q + 1)/2 \equiv 3 \pmod{6}$ if and only if $q \equiv 5 \pmod{6}$.
(mod 12) and so \( g = q - 3 \in \mathbf{M}(q^2) \); finally, we have that \( b = (q + 1)/2 \equiv 0 \) (mod 6) if and only if \( q \equiv 11 \) (mod 12) and so \( g = q - 4 \in \mathbf{M}(q^2) \).

3. Case (B)

In this section we consider the complementary Case (B) stated in the introduction.

**Proposition 3.1.** Let \( n, \ell, m \) be positive integers such that \( n \) divides \( q + 1 \), \( m \) divides \( q - 1 \) and \( n \) divides also \( \ell \frac{q-1}{m} - 1 \). Then the curve \( X(n, \ell, m) \) is \( F \)-maximal.

**Proof.** The Hermitian curve \( H \) over \( F \) is also defined by \( v^q + 1 = u^q + u \) \cite[Lemma 6.4.4]{17}. Set \( j := \frac{q+1}{n}, k := \frac{q-1}{m} \) and \( i := \frac{\ell k - 1}{n} \). Consider the following morphism

\[
\pi : H \to \mathbf{P}^2, \quad (u, v, 1) \mapsto (x, y, 1) := (u^k, u^i v^j, 1).
\]

Then, after some computations, we find that \( X(n, \ell, m) \) defines \( \pi(H) \) and the result follows. \( \square \)

**Example 3.2.** Let \( q \equiv 3 \) (mod 4) and consider \( n = q + 1, m = 2 \) and \( \ell = (q - 1)/2 \). Then the curve \( X = X(n, \ell, m) \) is \( F \)-maximal by Proposition 3.1 and \( g(X) = q \) by relation (1.2) above; i.e., \( q \) is in the spectrum set \( \mathbf{M}(q^2) \) defined in Example 2.2 (compare with \cite[Remark 6.2]{5}).

In this case we observe also that \( \gcd(n, \ell + m) = 1 \) and hence there is just one point \( P \) over \( x = \infty \). Then we can compute the Weierstrass semigroup at \( P \), cf. \cite[Remark 2.8]{20}, and therefore one-point AG-codes having good parameters can be constructed; cf. \cite{16}.

**Example 3.3.** Let \( q \equiv 11 \) (mod 12). Then by Examples 2.2, 3.2

\[
\{(q - 3)/2, (q - 1)/2, q - 4, q - 2, q\} \subseteq \mathbf{M}(q^2).
\]

This led to the following natural problem.

**Problem 3.4.** For a given prime power \( q \) find an integer \( I = I(q^2) \) such that \([0, I] \subseteq \mathbf{M}(q^2)\) but \( I + 1 \not\in \mathbf{M}(q^2)\).

According to the results in \cite{2} for \( q \leq 7, I(q^2) = \lfloor q/2 \rfloor \).

4. Case (C)

Here we deal with the complementary Case (C) stated in the introduction. Throughout this section, we fix the following notation.

- \( t \) is a prime power and \( \alpha \geq 1 \) is an integer. We set \( q := t^\alpha \) and so \( q^2 - 1 = (t^2 - 1)A(t, \alpha) \) with \( A(t, \alpha) := \sum_{i=0}^{\alpha-1} t^{2i} \).
- As above \( F \) stands for the finite field with \( q^2 = t^{2\alpha} \) elements.
- \( n, \ell, m \) are positive integers.
Proposition 4.1. Notation as above. Suppose in addition that $\alpha \geq 3$ is odd, set $N := (t^\alpha + 1)/(t + 1)$. Suppose that $m$ divides $t^2 - 1$, $n$ divides both $N$ and $\ell(t^2 - 1)/m - 1$. Then the curve $\mathcal{Y}(n, \ell, m)$ defined by $y^n = x^\ell(x^m - 1)$ is $\mathbb{F}$-maximal.

Proof. From [1] we know that the non-singular model $\mathcal{Z} = \mathbb{Z}_\alpha$ of the plane curve $v^N = u^2 - u$ is $\mathbb{F}$-maximal. Set $a := \frac{N}{n}$, $b := \frac{t^2 - 1}{m}$ and $c := \frac{\ell - 1}{n}$. Consider the following morphism on the function field $\mathbb{F}(u, v)$ of $\mathcal{Z}$

$$\pi : (u, v) \mapsto (x, y) := (u^b, u^c v^a).$$

After some computations we find that $\mathcal{Y}(n, \ell, m)$ defines a plane model for the covered function field $\pi(\mathbb{F}(u, u))$ and we are done. \qed

Remark 4.2. Notation as above. Suppose that the two conditions below hold true.

(A) $m$ divides $t^2 - 1$

(B) $nm/\gcd(\ell, m)$ divides $q^2 - 1$.

We shall state sufficient arithmetical conditions on the parameters $n, \ell, m$ and $t$ in order that the curves $\mathcal{X}(n, \ell, m)$ and $\mathcal{Y}(n, \ell, m)$ defined respectively by $y^n = x^\ell(x^m + 1)$ and $y^n = x^\ell(x^m - 1)$ be indeed $\mathbb{F}$-isomorphic.

There is $\delta \in \mathbb{F}$ such that $\delta^m = -1$ if

$$\frac{t^2 - 1}{m} \text{ is even.}$$

Then via $x \mapsto \delta x$ the curve $\mathcal{Y}(n, \ell, m)$ can be defined by $y^n = -\delta^\ell x^\ell(x^m + 1)$. Now we look for $\eta \in \mathbb{F}$ such that

$$\eta^n = -\delta^\ell;$$

we must have thus an equation of type

$$\eta^{nm/\gcd(\ell, m)} = (-1)^{m/\gcd(\ell, m)}(-1)^{\ell/\gcd(\ell, m)}.$$

Hence $\eta \in \mathbb{F}$ if any of the following conditions hold true.

(4.2) $m/\gcd(\ell, m)$ and $\ell/\gcd(\ell, m)$ have the same parity.

(4.3) $m/\gcd(\ell, m)$ and $\ell/\gcd(\ell, m)$ have different parity but $(q^2 - 1)\gcd(\ell, m)/nm$ is even.

Therefore if either (4.1) and (4.2), or (4.1) and (4.3) hold true then $\mathcal{X}(n, \ell, m)$ and $\mathcal{Y}(n, \ell, m)$ are $\mathbb{F}$-isomorphic via the morphism $(x, y) \mapsto (\delta x, \eta y)$.

Notice that $(q^2 - 1)\gcd(\ell, m)/nm$ is already even if $n$ divides $A(t, \alpha)$ and (4.1) holds.

Example 4.3. Notation as above. We let $\alpha \geq 3$ be odd. We claim that the curve $\mathcal{X} := \mathcal{X}(n, \ell, m)$ is $\mathbb{F}$-maximal whenever:

(1) $m$ divides $t^2 - 1$ and $(t^2 - 1)/m$ is even;

(2) $n$ divides both $N = (t^\alpha + 1)/(t + 1)$ and $\ell(t^2 - 1)/m - 1$. 
Indeed, clearly (4.1) above is true and \( nm \) divides \( q^2 - 1 = (t^2 - 1)A(t, \alpha) \) since \( N \) divides \( A(t, \alpha) \); hence either (4.2) or (4.3) is satisfied. Thus by Remark 4.2 \( X \) is \( F \)-isomorphic to \( \mathcal{Y}(n, \ell, m) \) and \( X \) is \( F \)-maximal by Proposition 4.1.

For instance to compute the genus of \( X = X(n, \ell, m) \) in case \( n = 2\ell - 1, m = (t^2 - 1)/2 \) with \( t \) odd, we use (1.2) by observing that \( \ell + m = (n + t^2)/2 \); hence \( \gcd(n, \ell) = 1 \) and \( \gcd(n, \ell + m) = 1 \) and so \( g(X) = (\ell - 1)(t^2 - 1)/2 \).

**Example 4.4.** In example 4.3 above let \( \ell = 4, n = 7, m = (t^2 - 1)/2 \). The hypotheses \( t \) odd and \( t \) divides \( N = (t^3+1)/(t+1) = t^2 - t + 1 \) \( (\alpha = 3) \) are fulfilled if and only if \( t \equiv 3, 5 \pmod{14} \). Hence the curve \( X = X(7, 4, (t^2 - 1)/2) \) defined by \( y^7 = x^4(x^{(t^2-1)/2} + 1) \) is \( F \)-maximal of genus \( g(X) = 3(t^2 - 1)/2 \). We recall that \( \#F = t^6 \).

By construction (proof of Proposition 4.1) \( X \) is \( F \)-covered by \( Z_3 \) given by \( v^{t^2-t+1} = u^2 - u \) whose genus is \( g(Z_3) = (t^2 - 1)(t^2 - t)/2 \) as follows from (1.2). Now for \( t = 3 \), \( Z_3 \) is the curve \( v^7 = u^9 - v^3 \) of genus 24 which is the first known example, discovered by Garcia and Stichtenoth, of an \( F \)-maximal curve that cannot be Galois-covered by the corresponding Hermitian curve \( \mathcal{H} : y^{28} = x^{27} + x \); see [6].

For \( t = 3 \), \( X = X(7, 4, 4) \) is \( F \)-maximal of genus \( g(X) = 12 \). Thus we are naturally led to the following.

**Question 4.5.** Let \( F \) be the finite field with \( 3^6 \) elements. Is the curve \( X = X(7, 4, 4) \) above \( F \)-Galois covered by the Hermitian curve over \( F \)?

Unfortunately the method in [3, Prop. 5.1] (or in [6]) cannot be applied here.

**Remark 4.6.** For an AG-code \( C \) with parameters \( [n(C), k(C), d(C)] \) built on a curve \( X \) over \( F \) (the finite field of order \( q^2 \)) with many points, we have

\[
  k(C) + d(C) \geq n(C) + 1 - g(X);
\]

see e.g. [Cor. 2.2.3]Sti. Thus the performance of \( C \) is better whenever \( n(C) \) is large compare with \( g(X) \). In particular, if the curve is \( F \) maximal and \( C \) is a one-point AG-code, the performance of \( C \) is better if \( q^2 \) is large compare with \( g \). Therefore, the curves in Example 4.4 are of higher interest in Coding Theory.

**Acknowledgments.** The authors were in part supported respectively by FAPESP/SP-Brazil (Grant 2017/19190-5) and by CNPq-Brazil (Grant 310623/2017-0). The second author thanks P. Chacón for her constant support and friendship.

**References**


THE CURVE $Y^n = X^r(X^m + 1)$ OVER FINITE FIELDS


IMECC-UNICAMP, R. SÉRGIO BUARQUE DE HOLANDA, 651, CIDADE UNIVERSITÁRIA “ZEFERINO VAZ”, 13083-859, CAMPINAS, SP, BRAZIL.

Email address: tafazolian@ime.unicamp.br

Email address: ftorres@ime.unicamp.br