ON THE SPECTRUM FOR THE GENERA OF MAXIMAL CURVES OVER SMALL FIELDS

NAZAR ARAKELIAN, SAEED TAFAZOLIAN, AND FERNANDO TORRES

Abstract. Motivated by previous computations in Garcia, Stichtenoth and Xing (2000) paper [9], we discuss the spectrum $M(q^2)$ for the genera of maximal curves over finite fields of order $q^2$ with $7 \leq q \leq 16$. In particular, by using a result in Kudo and Harashita (2016) paper [17], the set $M(7^2)$ is completely determined.

1. Introduction

Let $X$ be a (projective, nonsingular, geometrically irreducible, algebraic) curve of genus $g$ defined over a finite field $K = \mathbb{F}_\ell$ of order $\ell$. The following inequality is the so-called Hasse-Weil bound on the size $N$ of the set $X(K)$ of $K$-rational points of $X$:

$$|N - (\ell + 1)| \leq 2g \cdot \sqrt{\ell}. \quad (1.1)$$

In Coding Theory, Cryptography, or Finite Geometry one is often interested in curves with “many points”, namely those with $N$ as bigger as possible. In this paper, we work out over fields of square order, $\ell = q^2$, and deal with so-called maximal curves over $K$; that is to say, those curves attained the upper bound in (1.1), namely

$$N = q^2 + 1 + 2g \cdot q. \quad (1.2)$$

The subject matter of this note is in fact concerning the spectrum for the genera of maximal curves over $K$,

$$M(q^2) := \{g \in \mathbb{N}_0 : \text{there is a maximal curve over } K \text{ of genus } g\}. \quad (1.3)$$

In Section 2 we subsume basic facts on a maximal curve $X$ being the key property the existence of a very ample linear series $D$ on $X$ equipped with a nice property, namely (2.2). In particular, Castelnuovo’s genus bound (2.3) and Halphen’s theorem imply a nontrivial restriction on the genus $g$ of $X$, stated in (3.1) (see [15]) and thus $g \leq q(q-1)/2$ (Ihara’s bound [14]).

Let $r$ be the dimension of $D$. Then $r \geq 2$ by (2.2), and the condition $r = 2$ is equivalent to $g = q(q-1)/2$, or equivalent to $X$ being $K$-isomorphic to the Hermitian curve $y^{q+1} = x^q + x$ [24], [7]. Under certain conditions, we have a similar result for $r = 3$ in Corollary 2.3 and Proposition 3.1. In fact, in Section 3 we bound $g$ via Stöhr-Voloch theory [21]

Key words: finite field, Hasse-Weil bound, Stöhr-Voloch theory, maximal curve.

October 6, 2016.
applied to $D$ being the main results the aforementioned proposition and its Corollary 3.2. Finally, in Section 4 we apply all these results toward the computation of $M(q^2)$ for $q = 7, 8, 9, 11, 13, 16$. In fact, here we improve [9, Sect. 6] and, in particular, we can compute $M(7^2)$ (see Corollary 4.3) by using Corollary 3.2 and a result of Kudo and Harashita [17] which asserts that there is no maximal curve of genus 4 over $\mathbb{F}_{49}$.

We recall that the approach in this paper is quite different from Danisman and Ozdemir [3], where in particular the set $M(7^2)$ is missing.

Conventions. $\mathbb{P}^s$ is the $s$-dimensional projective space defined over the algebraic closure of the base field.

2. Basic Facts on Maximal curves

Throughout, let $X$ be a maximal curve over the field $K = \mathbb{F}_{q^2}$ of order $q^2$ of genus $g$. Let $\Phi : X \to X$ be the Frobenius morphism relative to $K$ (in particular, the set of fixed points of $\Phi$ coincides with $X(K)$). For a fixed point $P_0 \in X(K)$, let $j : X \to J, P \mapsto [P - P_0]$ be the embedding of $X$ into its Jacobian variety $J$. Then, in a natural way, $\Phi$ induces a morphism $\Phi : J \to J$ such that

$$(2.1) \quad j \circ \Phi = \Phi \circ j.$$ 

Now from (1.2) the enumerator of the Zeta Function of $X$ is given by the polynomial $L(t) = (1 + qt)^{2g}$. It turns out that $h(t) := t^{2g}L(t^{-1})$ is the characteristic polynomial of $\Phi$; i.e., $h(\Phi) = 0$ on $J$. As a matter of fact, since $\Phi$ is semisimple and the representation of endomorphisms of $J$ on the Tate module is faithful, from (2.1) it follows that

$$(2.2) \quad (q + 1)P_0 \sim qP + \Phi(P), \quad P \in X.$$ 

This suggests to study the Frobenius linear series on $X$, namely the complete linear series $D := |(q + 1)P_0|$ which is in fact a $K$-invariant of $X$ by (2.2); see [6], [12, Ch. 10] for further information.

Moreover, $D$ is a very ample linear series in the following sense. Let $r$ be the dimension of $D$, which we refer as the Frobenius dimension of $X$, and $\pi : X \to \mathbb{P}^r$ be a morphism related to $D$; we noticed above that $r \geq 2$ by (2.2). Then $\pi$ is an embedding [16, Thm. 2.5]. In particular, Castelnuovo’s genus bound applied to $\pi(X)$ gives the following constrain involving the genus $g$ and Castelnuovo numbers $c_0(r, q + 1)$:

$$(2.3) \quad g \leq c_0(r) = c_0(r, q + 1) := \begin{cases} \frac{(2q - (r - 1))^2 - 1}{8(r - 1)} & \text{if } r \text{ is even}, \\ \frac{(2q - (r - 1))^2}{8(r - 1)} & \text{if } r \text{ is odd}. \end{cases}$$ 

Remark 2.1. A direct computation shows that $c_0(r) \leq c_0(s)$ provided that $r \geq s$.

Since $c_0(r) \leq c_0(2) = q(q - 1)/2$, as $r \geq 2$, then $g \leq q(q - 1)/2$ which is a well-known fact on maximal curves over $K$ due to Ihara [14]. In addition, $c_0(r) \leq c_0(3) = (q - 1)^2/4$ for
$r \geq 3$, so that the genus $g$ of a maximal curve over $K$ does satisfy the following condition (see [7])

\[(2.4) \quad g \leq c_0(3) = (q - 1)^2/4 \quad \text{or} \quad g = c_0(2) = q(q - 1)/2.\]

As a matter of fact, the following sentences are equivalent.

**Lemma 2.2.** ([19], [7])

1. $g = c_0(2) = q(q - 1)/2$;
2. $(q - 1)^2/4 < g \leq q(q - 1)/2$;
3. $r = 2$;
4. $\mathcal{X}$ is $K$-isomorphic to the Hermitian curve $\mathcal{H} : y^{q+1} = x^q + x$.

**Corollary 2.3.** Let $\mathcal{X}$ be a maximal curve over $K$ of genus $g$ and Frobenius dimension $r$. Suppose that

\[c_0(4) = (q - 1)(q - 2)/6 < g \leq c_0(3) = (q - 1)^2/4.\]

Then $r = 3$.

**Proof.** If $r \geq 4$, then $g \leq (q - 1)(q - 2)/6$ by (2.3); so $r = 2$ or $r = 3$. Thus $r = 3$ by Lemma 2.2 and hypothesis on $g$. \qed

Under certain conditions, this result will be improved in Proposition 3.1.

The following important remark is commonly attributed to J.P. Serre.

**Remark 2.4.** Any curve (nontrivially) $K$-covered by a maximal curve over $K$ is also maximal over $K$. In particular, any subcover over $K$ of the Hermitian curve is so; see e.g. [9], [2].

**Remark 2.5.** We do point out that there are maximal curves over $K$ which cannot be (nontrivially) $K$-covered by the Hermitian curve $\mathcal{H}$, see [11], [22], [10].

We also notice that there are maximal curves over $K$ that cannot be Galois covered by the Hermitian curve $\mathcal{H}$, [8], [4], [22], [10].

We also observe that all the examples occurring in this remark are defined over fields of order $q^2 = \ell^6$ with $\ell > 2$.

### 3. The set $M(q^2)$

In this section we investigate the spectrum $M(q^2)$ for the genera of maximal curves defined in (1.3). By using Remark 2.4 this set has already been computed for $q \leq 5$ [9, Sect. 6]. As a matter of fact, $M(2^2) = \{0, 1\}$, $M(3^2) = \{0, 1, 3\}$, $M(4^2) = \{0, 1, 2, 6\}$, and $M(5^2) = \{0, 1, 2, 3, 4, 10\}$. Thus from now on we assume $q \geq 7$.

Let $c_0(r)$ be the Castelnuovo’s number in (2.3) and $g \in M(q^2)$. It is known that $g = \lfloor c_0(3) \rfloor$ if and only if $\mathcal{X}$ is the quotient of the Hermitian curve $\mathcal{H}$ by certain involution [6],
[1], [15]. Indeed, \( \mathcal{X} \) is uniquely determined by plane models of type: \( y^{(q+1)/2} = x^q + x \) if \( q \) is odd, and \( y^{q+1} = x^{q/2} + \ldots + x \) otherwise.

Let us consider next an improvement on (2.4). If \( r \geq 4 \), from (2.3), \( g \leq c_0(4) = (q - 1)(q - 2)/6 \). Let \( r = 3 \) and suppose that
\[
c_1(3) = c_1(q^2, 3) := (q^2 - q + 4)/6 < g \leq c_0(3).
\]
Here Halphen’s theorem implies that \( \mathcal{X} \) is contained in a quadric surface and so \( g = c_0(3) \) (see [15]). In particular, (2.4) improves to
\[
(3.1) \quad g \leq c_1(3), \quad \text{or} \quad g = \lfloor c_0(3) \rfloor, \quad \text{or} \quad g = c_0(2). 
\]
Next we complement Corollary 2.3 under certain extra conditions.

**Proposition 3.1.** Let \( \mathcal{X} \) be a maximal curve over \( K \), \( q \not\equiv 0 \pmod{3} \), of genus \( g \) with Frobenius dimension \( r = 3 \) such that \( (4q - 1)(2g - 2) > (q + 1)(q^2 - 5q - 2) \). Then
\[
g \geq c_0(4) + (q + 1)/6 = (q^2 - 2q + 3)/6.
\]

**Proof.** We shall apply Stöhr-Voloch theory [21] to \( D = \{|(q + 1)|P_0| \}. \) Let \( R = \sum_P v_P(R)P \) and \( S = \sum_P v_P(S)P \) denote respectively the ramification and Frobenius divisor of \( D \). Associated to each point \( P \in \mathcal{X} \), there is a sequence of the possible intersection multiplicities of \( \mathcal{X} \) with hyperplanes in \( \mathbb{P}^3 \), namely \( \mathcal{R}(P) = 0 = j_0(P) < 1 = j_1(P) < j_2(P) < j_3(P). \)
From (2.2), \( j_3(P) = q + 1 \) (resp. \( j_3(P) = q \)) if \( P \in \mathcal{X}(K) \) (resp. \( P \not\in \mathcal{X}(K) \)). Moreover, the sequence \( \mathcal{R}(P) \) is the same for all but a finitely number of points (the so-called \( D \)-Weierstrass points of \( \mathcal{X} \)); such a sequence (the orders of \( D \)) will be denoted by \( E : 0 = \epsilon_0 < 1 = \epsilon_1 < \epsilon_2 < \epsilon_3 = q. \) One can show that the numbers \( 1 = \nu_1 < q = \nu_2 \) (the \( K \)-Frobenius orders of \( D \)) satisfy the very basic properties (5) and (6) below (cf. [21]):

1. \( j_i(P) \geq \epsilon_i \) for any \( i \) and \( P \in \mathcal{X} \);
2. \( v_P(R) \geq 1 \) for \( P \in \mathcal{X}(K) \);
3. \( \deg(R) = (\epsilon_3 + \epsilon_2 + 1)(2g - 2) + (r + 1)(q + 1) \);
4. \( (p \text{-adic criterion}) \) If \( \epsilon \) is an order and \( (\eta^t) \not\equiv 0 \pmod{p} \), then \( \eta \) is also an order;
5. \( v_P(S) \geq j_2(P) + (j_3(P) - \nu_2) = j_2(P) + 1 \) for \( P \in \mathcal{X}(K) \);
6. \( \deg(S) = (\nu_1 + \nu_2)(2g - 2) + (q + 2 + r)(q + 1) \).

**Claim** \( \epsilon_2 = 2. \) Suppose that \( \epsilon_2 \geq 3; \) then \( \epsilon_2 \geq 4 \) by the \( p \)-adic criterion. Then the maximality of \( \mathcal{X} \) gives
\[
\deg(S) = (1 + q)(2g - 2) + (q^2 + 3)(q + 1) \geq 5(q + 1)^2 + 5q(2g - 2)
\]
so that
\[
(q + 1)(q^2 - 5q - 2) \geq (4q - 1)(2g - 2),
\]
a contradiction and the proof of the claim follows.

Finally, we use the ramification divisor \( R \) of \( D \); we have
\[
\deg(R) = (q + 2 + 1)(2g - 2) + 4(q + 1) \geq (q + 1)^2 + q(2g - 2)
\]
and thus \( g \geq (q^2 - 2q + 3)/6 \).

**Corollary 3.2.** Let \( X \) be a maximal curve over \( K \), of genus \( g \), where \( q \not\equiv 0 \pmod{3} \). Then

\[
g \geq (q^2 - 2q + 3)/6 \quad \text{provided that } g > (q - 1)(q - 2)/6.
\]

**Proof.** Let \( D \) be the Frobenius linear series of \( X \) and \( r \) the Frobenius dimension. By (2.3) and Lemma 2.2, we can assume \( r = 3 \). Now the hypothesis on \( g \) is equivalent to

\[
(2g - 2) > (q + 1)(q - 4)/3;
\]

thus

\[
(4q - 1)(2q - 2) > (4q - 1)(q + 1)(q - 4)/3 > (q + 1)(q^2 - 5q - 2),
\]

and the result follows from Proposition 3.1. \( \square \)

4. \( M(q^2) \) for \( 7 \leq q \leq 16 \)

In this section we shall improve on the following computations which follow from [9, Remark 6.1] and (3.1).

**Proposition 4.1.**

(1) \( \{0, 1, 2, 3, 5, 7, 9, 21\} \subseteq M(7^2) \subseteq [0, 7] \cup \{9\} \cup \{21\}; \)

(2) \( \{0, 1, 2, 3, 4, 6, 7, 9, 10, 12, 28\} \subseteq M(8^2) \subseteq [0, 10] \cup \{12\} \cup \{28\}; \)

(3) \( \{0, 1, 2, 3, 4, 6, 8, 9, 12, 16, 36\} \subseteq M(9^2) \subseteq [0, 12] \cup \{16\} \cup \{36\}; \)

(4) \( \{0, 1, 2, 3, 4, 5, 7, 9, 10, 11, 13, 15, 18, 19, 25, 55\} \subseteq M(11^2) \subseteq [0, 19] \cup \{25\} \cup \{55\}; \)

(5) \( \{0, 2, 3, 6, 9, 12, 15, 18, 26, 36, 78\} \subseteq M(13^2) \subseteq [0, 26] \cup \{36\} \cup \{78\}; \)

(6) \( \{0, 1, 2, 4, 6, 8, 12, 24, 28, 40, 56, 120\} \subseteq M(16^2) \subseteq [0, 40] \cup \{56\} \cup \{120\}. \)

**Proposition 4.2.** Let \( M(q^2) \) be the spectrum for the genera of maximal curves over \( K \). Then

(1) \( 6 \not\in M(7^2); \)

(2) \( 8 \not\in M(8^2); \)

(3) \( 16 \not\in M(11^2); \)

(4) \( 23, 24 \not\in M(13^2); \)

(5) \( 36, 37 \not\in M(16^2). \)

**Proof.** Let \( q = 7 \). By Corollary 3.2, \( g = 6 \not\in M(7^2). \) The other cases are handle in a similar way. \( \square \)

**Corollary 4.3.** We have

\[
M(7^2) = \{0, 1, 2, 3, 5, 7, 9, 21\}.
\]

**Proof.** By the above Propositions, it is enough to show that \( 4 \not\in M(7^2). \) Indeed, this is the case as follows from a result in Kudo and Harashita paper [17, Thm. B] concerning superspecial curves. \( \square \)
Remark 4.4. To compute $M(q^2)$ for $q = 8, 9, 11, 13, 16$ we need to answer the following questions:

1. Is $5 \in M(8^2)$?
2. Are $5, 7, 10, 11 \in M(9^2)$?
3. Are $8, 12, 14, 17 \in M(11^2)$?
4. Are $1, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 21, 22 \in M(13^2)$?
5. Are $3, 5, 7, 9, 10, 11, 13, 14, \ldots, 22, 23, 25, 26, 27, 29, 30, 31, 32, 33, 34, 35, 38, 39 \in M(16^2)$?

Example 4.5. Here, for the sake of completeness, we provide an example of a maximal curve of genus $g$ for each $g \in M(7^2)$; cf. [18], [23].

1. ($g = 0$) The rational curve;
2. ($g = 1$) $y^2 = x^3 + x$;
3. ($g = 2$) $y^2 = x^5 + x$;
4. ($g = 3$) $y^2 = x^7 + x$;
5. ($g = 5$) $y^8 = x^4 - x^2$;
6. ($g = 7$) $y^{16} = x^9 - x^{10}$;
7. ($g = 9$) $y^4 = x^7 + x$;
8. ($g = 21$) $y^8 = x^7 + x$.

Remark 4.6. The curves in (6), (7), and (8) above are unique up to $\mathbb{F}_{19}$-isomorphism; see respectively [5], [6], and [19].

Acknowledgment. The first author was partially supported by FAPESP, grant 2013/00564-1. The second author was in part supported by a grant from IPM (No. 93140117). The third author was partially supported by CNPq (Grant 308326/2014-8).

References


[18] www.manypoints.org, “manYPoints-Table of Curves with Many Points”.


CMCC/Universidade Federal do ABC, Avenida dos Estados 5001, 09210-580, Santo André, SP-Brasil

E-mail address: n.arakelian@ufabc.edu.br

School of Mathematics, Institute for Research in Fundamental Science (IPM), P.O. Box 19395-5746, Tehran, Iran, Dept. of Mathematics and Computer Science, Amirkabir University of Technology, 424 Hafez Ave, Tel: +98 (21) 64540 P.O. Box: 15875-4413, Tehran, Iran

E-mail address: saeed@gmail.com

IMECC/UNICAMP, R. Sérgio Buarque de Holanda 651, Cidade Universitária “Zeférrino Vaz”, 13083-859, Campinas, SP, Brazil

E-mail address: ftorres@ime.unicamp.br