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 $\mathbf{M}(q^2)$ for the genera of maximal curves over finite fields of order q^2 with $7 \le q \le 16$. In particular, by using a result in Kudo and Harashita (2016) paper [17], the set $\mathbf{M}(7^2)$ is completely determined.

1. Introduction

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

$$|N - (\ell + 1)| \le 2g \cdot \sqrt{\ell}\,. \tag{1.1}$$

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* $\mathbf{K}$; that is to say, those curves attained the upper bound in (1.1), namely

$$N = q^2 + 1 + 2g \cdot q\,. \tag{1.2}$$

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

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

In Section 2 we subsume basic facts on a maximal curve $\mathcal{X}$ being the key property the existence of a very ample linear series $\mathcal{D}$ on $\mathcal{X}$ 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 $\mathcal{X}$, stated in (3.1) (see [15]) and thus $g \le q(q-1)/2$ (Ihara's bound [14]).

Let r be the dimension of $\mathcal{D}$. Then $r \ge 2$ by (2.2), and the condition $r = 2$ is equivalent to $g = q(q-1)/2$, or equivalent to $\mathcal{X}$ being $\mathbf{K}$-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 $\mathcal{D}$ 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 $\mathbf{M}(q^2)$ for $q = 7, 8, 9, 11, 13, 16$. In fact, here we improve [9, Sect. 6] and, in particular, we can compute $\mathbf{M}(7^2)$ (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 $\mathbf{M}(7^2)$ 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 $\mathcal{X}$ be a maximal curve over the field $\mathbf{K} = \mathbb{F}_{q^2}$ of order q^2 of genus g. Let $\Phi : \mathcal{X} \to \mathcal{X}$ be the Frobenius morphism relative to $\mathbf{K}$ (in particular, the set of fixed points of Φ coincides with $\mathcal{X}(\mathbf{K})$). For a fixed point $P_0 \in \mathcal{X}(\mathbf{K})$, let $j : \mathcal{X} \to \mathcal{J}, P \mapsto [P - P_0]$ be the embedding of $\mathcal{X}$ into its Jacobian variety $\mathcal{J}$. Then, in a natural way, Φ induces a morphism $\tilde{\Phi} : \mathcal{J} \to \mathcal{J}$ such that

$$j \circ \tilde{\Phi} = \tilde{\Phi} \circ j \,. \tag{2.1}$$

Now from (1.2) the enumerator of the Zeta Function of $\mathcal{X}$ 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 $\tilde{\Phi}$; i.e., $h(\tilde{\Phi}) = 0$ on $\mathcal{J}$. As a matter of fact, since $\tilde{\Phi}$ is semisimple and the representation of endomorphisms of $\mathcal{J}$ on the Tate module is faithful, from (2.1) it follows that

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

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

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

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

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 $\mathbf{K}$ 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 $\mathbf{K}$ does satisfy the following condition (see [7])

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

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 $\mathbf{K}$-isomorphic to the Hermitian curve $\mathcal{H}: y^{q+1} = x^q + x$.*

Corollary 2.3. *Let $\mathcal{X}$ be a maximal curve over $\mathbf{K}$ 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. □

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) $\mathbf{K}$-covered by a maximal curve over $\mathbf{K}$ is also maximal over $\mathbf{K}$. In particular, any subcover over $\mathbf{K}$ of the Hermitian curve is so; see e.g. [9], [2].

Remark 2.5. We do point out that there are maximal curves over $\mathbf{K}$ which cannot be (nontrivially) $\mathbf{K}$-covered by the Hermitian curve $\mathcal{H}$, see [11], [22], [10].
We also notice that there are maximal curves over $\mathbf{K}$ that cannot be Galois covered by the Hermitian curve [8], [4], [22], [10].
We also observe that all the examples occuring in this remark are defined over fields of order $q^2 = \ell^6$ with $\ell > 2$.

3. The set $\mathbf{M}(q^2)$

In this section we investigate the spectrum $\mathbf{M}(q^2)$ 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, $\mathbf{M}(2^2) = \{0, 1\}$, $\mathbf{M}(3^2) = \{0, 1, 3\}$, $\mathbf{M}(4^2) = \{0, 1, 2, 6\}$, and $\mathbf{M}(5^2) = \{0, 1, 2, 3, 4, 10\}$. Thus from now on we assume $q \geq 7$.

Let $c_0(r)$ be the Castelnuovo's number in (2.3) and $g \in \mathbf{M}(q^2)$. 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

$$g \leq c_1(3)\,, \quad \text{or} \quad g = \lfloor c_0(3) \rfloor\,, \quad \text{or} \quad g = c_0(2)\,. \tag{3.1}$$

Next we complement Corollary 2.3 under certain extra conditions.

Proposition 3.1. *Let $\mathcal{X}$ be a maximal curve over $\mathbf{K}$, $q \not\equiv 0 \pmod 3$, 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 $\mathcal{D} = |(q+1)P_0|$. Let $R = \sum_P v_P(R)P$ and $S = \sum_P v_P(S)P$ denote respectively the ramification and Frobenius divisor of $\mathcal{D}$. 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 $P \in \mathcal{X}(\mathbf{K})$ (resp. $P \notin \mathcal{X}(\mathbf{K})$). Moreover, the sequence $\mathcal{R}(P)$ is the same for all but a finitely number of points (the so-called $\mathcal{D}$-Weierstrass points of $\mathcal{X}$); such a sequence (the *orders* of $\mathcal{D}$) will be denoted by $\mathcal{E} : 0 = \epsilon_0 < 1 = \epsilon_1 < \epsilon_2 < \epsilon_3 = q$. One can show that the numbers $1 = \nu_1 < q = \nu_2$ (the $\mathbf{K}$-*Frobenius orders* of $\mathcal{D}$) 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 $P \in \mathcal{X}(\mathbf{K})$;
(3) $\deg(R) = (\epsilon_3 + \epsilon_2 + 1)(2g-2) + (r+1)(q+1)$;
(4) (p-adic criterion) If ϵ is an order and $\binom{\epsilon}{\eta} \not\equiv 0 \pmod p$, then η is also an order;
(5) $v_P(S) \geq j_2(P) + (j_3(P) - \nu_2) = j_2(P) + 1$ for $P \in \mathcal{X}(\mathbf{K})$;
(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 $\mathcal{D}$; 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 $\mathcal{X}$ be a maximal curve over $\mathbf{K}$, of genus g, where $q \not\equiv 0 \pmod 3$. Then*

$$g \geq (q^2-2q+3)/6 \quad \textit{provided that } g > (q-1)(q-2)/6\,.$$

Proof. Let $\mathcal{D}$ be the Frobenius linar series of $\mathcal{X}$ 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

$$(4q-1)(2g-2) > (4q-1)(q+1)(q-4)/3 > (q+1)(q^2-5q-2)\,,$$

and the result follows from Proposition 3.1. □

4. $\mathbf{M}(q^2)$ 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. $\{0,1,2,3,5,7,9,21\} \subseteq \mathbf{M}(7^2) \subseteq [0,7] \cup \{9\} \cup \{21\}$;
2. $\{0,1,2,3,4,6,7,9,10,12,28\} \subseteq \mathbf{M}(8^2) \subseteq [0,10] \cup \{12\} \cup \{28\}$;
3. $\{0,1,2,3,4,6,8,9,12,16,36\} \subseteq \mathbf{M}(9^2) \subseteq [0,12] \cup \{16\} \cup \{36\}$;
4. $\{0,1,2,3,4,5,7,9,10,11,13,15,18,19,25,55\} \subseteq \mathbf{M}(11^2) \subseteq [0,19] \cup \{25\} \cup \{55\}$;
5. $\{0,2,3,6,9,12,15,18,26,36,78\} \subseteq \mathbf{M}(13^2) \subseteq [0,26] \cup \{36\} \cup \{78\}$;
6. $\{0,1,2,4,6,8,12,24,28,40,56,120\} \subseteq \mathbf{M}(16^2) \subseteq [0,40] \cup \{56\} \cup \{120\}$.

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

1. $6 \notin \mathbf{M}(7^2)$;
2. $8 \notin \mathbf{M}(8^2)$;
3. $16 \notin \mathbf{M}(11^2)$;
4. $23, 24 \notin \mathbf{M}(13^2)$;
5. $36, 37 \notin \mathbf{M}(16^2)$.

Proof. Let $q=7$. By Corollary 3.2, $g=6 \notin \mathbf{M}(7^2)$. The other cases are handle in a similar way. □

Corollary 4.3. *We have*

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

Proof. By the above Propositions, it is enough to show that $4 \notin \mathbf{M}(7^2)$. Indeed, this is the case as follows from a result in Kudo and Harashita paper [17, Thm. B] concerning superspecial curves. □

Remark 4.4. To compute $\mathbf{M}(q^2)$ for $q = 8, 9, 11, 13, 16$ we need to answer the following questions:

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

Example 4.5. Here, for the sake of completeness, we provide an example of a maximal curve of genus g for each $g \in \mathbf{M}(7^2)$; 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 $\mathbb{F}_{49}$-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

[1] M. Abdón and F. Torres, *Maximal curves in characteristic two*, Manuscripta Math. **99** (1999), 39–53.
[2] A. Cossidente, G. Korchmáros and F. Torres, *On curves covered by the Hermitian curve*, J. Algebra **216** (1999), 56–76.
[3] Y. Danisman and M. Ozdemir, *On the genus spectrum of maximal curves over finite fields*, Journal of Discrete Mathematical Sciences and Cryptography **18**(5) (2015), 513–529.
[4] 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.
[5] S. Fanali, M. Giulietti and I. Platoni, *On maximal curves over finite fields of small order*, Adv. Math. Commun. **6**(1) (2012), 107–120.
[6] R. Fuhrmann, A. Garcia and F. Torres, *On maximal curves*, J. Number Theory **67**(1) (1997), 29–51.
[7] R. Fuhrmann and F. Torres, *The genus of curves over finite fields with many rational points*, Manuscripta Math. **89** (1996), 103–106.
[8] A. Garcia and H. Stichtenoth, *A maximal curve which is not a Galois subcover of the Hermitian curve*, Bulletin Braz. Math. Soc. **37** (2006), 1–14.

[9] A. Garcia, H. Stichtenoth, and C.P. Xing, *On subfields of the Hermitian function field*, Compositio Math. **120** (2000), 137–170.

[10] M. Giulietti, L. Quoos and G. Zini, *Maximal curves from subcovers of the GK-curve*, preprint, February, 2015.

[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 Finite Fields", Princenton University Press, USA, 2008.

[13] N.E. Hurt, "Many Rational Points, Coding Theory and Algebraic Geometry", Kluwer Academic Publishers, The Netherlands, 2003.

[14] I. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Tokyo, Sec. Ia, **28**(3) (1981), 721–724.

[15] G. Korchmáros and F. Torres, *On the genus of a maximal curve*, Math. Ann. **323** (2002), 589–608.

[16] G. Korchmáros and F. Torres, *Embedding of a maximal curve in a Hermitian variety*, Compositio Mathematica **128** (2001), 95–113.

[17] M. Kudo and S. Harashita, *Superspecial curves of genus 4 in small characteristic*, arXiv: 1607.01114v1.

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

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

[20] H. Stichtenoth, "Algebraic Function Fields and Codes", Springer-Verlag, New York, Second Edition, 2009.

[21] K.O. Stöhr and J.F. Voloch, *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. **52** (1986), 1-19.

[22] S. Tafazolian, A. Teherán-Herrera, F. Torres, *Further examples of maximal curves which cannot be covered by the Hermitian curve*, J. Pure Appl. Algebra **220**(3) (2016), 1122–1132..

[23] S. Tafazolian and F. Torres, *On the curve $y^n = x^m + x$ over finite fields*, J. Number Theory **145** (2014), 51–66.

[24] C.P. Xing and H. Stichtenoth, *The genus of maximal functions fields*, Manuscripta Math. **86** (1995), 217–224.

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 Scinence, 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 "Zeferino Vaz", 13083-859, Campinas, SP, Brazil

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