ON MAXIMAL CURVES HAVING CLASSICAL WEIERSTRASS GAPS

ARNALDO GARCIA AND FERNANDO TORRES

ABSTRACT. We study geometrical properties of maximal curves over the finite field $\mathbb{F}_{q^2}$ with q^2 elements having classical Weierstrass gaps. We obtain in particular that the support of the Frobenius divisor associated to the linear system $|(q+1)P|$, P being a $\mathbb{F}_{q^2}$-rational point, is equal to the union of the set of Weierstrass points (for the canonical divisor) with the set of $\mathbb{F}_{q^2}$-rational points of the curve.

1. INTRODUCTION

The theory of equations over finite fields (or the theory of congruences) is the basis for classical number theory. Its foundations were done, among others, by mathematicians like Fermat, Euler, Lagrange, Gauss, and Galois, see Dickson's book [D]. Historically, the object of the first investigations in this theory were the congruences of the special form

$$y^2 \equiv f(x) \quad (\text{modulo a prime number}), \tag{1.1}$$

where $f(x)$ is a polynomial (or rational function) with integer coefficients. Such congruences were used to get results such as the representability of integers as sum of four squares, or the distribution of pairs of quadratic residues, or even the estimation of the sum of Legendre's quadratic residues symbols.

Poincaré suggested that the study of congruences in two variables should use the methods of the theory of algebraic functions. E. Artin then constructed a theory of quadratic extensions of the field $\mathbb{F}_p(x)$, p a prime, by adjoining the roots of congruence (1.1) and introduced a zeta-function for this field in analogy with Dedekind's zeta-function for quadratic extensions of the field of rational numbers. Assuming that Riemann's hypothesis was valid for his zeta-function, Artin conjectured an upper bound for the number of solutions of congruences such as in (1.1) above. Artin's conjecture was then proved by Hasse for polynomials $f(x)$ of degrees 3 and 4 over arbitrary finite fields, and widely generalized by A. Weil as follows. Let X be a projective geometrically irreducible nonsingular algebraic curve of genus g, defined over a finite field $\mathbb{F}_\ell$ with ℓ

1991 Math. Subj. Class.: Primary 11G, Secondary 14G.

Both authors were partially supported by Cnpq-Brazil and by PRONEX # 41.96.0883.00.

elements. Then,

$$|\#X(\mathbb{F}_\ell) - (\ell+1)| \le 2g\sqrt{\ell}\,, \tag{1.2}$$

where $X(\mathbb{F}_\ell)$ denotes the set of $\mathbb{F}_\ell$-rational points of the curve X. Inequality (1.2) is equivalent to the validity of Riemann's hypothesis for the zeta-function associated to the curve X. Bombieri [B] gave an elementary proof of (1.2) following ideas of Stepanov, Postnikov and Manin that were used to treat the special case of hyperelliptic curves; see [Ste, Chapter 5].

The interest on curves over finite fields with many rational points was renewed after Goppa's construction of codes with good parameters from such curves, see [Go]. Number of solutions of congruences in two variables has other applications such as estimates of exponential sums over finite fields [Mo], finite geometries [H], correlations of shift register sequences [L-N].

Here we will be interested in *maximal curves over* $\mathbb{F}_\ell$ with $\ell = q^2$, that is curves X attaining Hasse-Weil's upper bound:

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

It is often the case that maximal curves are special (and interesting) from other points of view. For example, it is often the case that they have large automorphism groups, see [K] and [Sti], and that they are nonclassical for the canonical linear series [FGT]. A central problem is the classification of maximal curves over $\mathbb{F}_{q^2}$ of a given genus. Besides the action of the Frobenius morphism on the Jacobian of a maximal curve [FGT, Corollary 1.2], a central role in the classification problem is played by Stöhr-Voloch's approach [SV] to the Hasse-Weil's bound (1.2). Roughly speaking, instead of bounding the number of fixed points of the Frobenius morphism on the curve, Stöhr-Voloch's approach bounds the number of points whose image under the Frobenius morphism lies on the osculating hyperplane at the point. Their theory of Frobenius orders is quite similar to Weierstrass point theory in prime characteristic, as introduced by F.K. Schmidt [Sch].

The genus of a maximal curve over $\mathbb{F}_{q^2}$ satisfies [Ih], [Sti-X], [FT1]

$$g \le (q-1)^2/4 \qquad \text{or} \qquad g = (q-1)q/2\,.$$

Maximal curves with genus $(q-1)q/2$ have been characterized, see [R-Sti]. 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 which can be given by the affine equation $y^q + y = x^{q+1}$. Maximal curves with the next highest genus $(q-1)^2/4$, q odd, have also been characterized; see [FGT, Theorem 3.1]. Again, up to $\mathbb{F}_{q^2}$-isomorphism, there is just one maximal curve with this genus and it can be given by $y^q + y = x^{(q+1)/2}$. In the latter case, the proof of the uniqueness involves the study of the interplay between the canonical divisor and the divisor $\mathcal{D} := |(q+1)P_0|$ on the curve, P_0 being a $\mathbb{F}_{q^2}$-rational point, via Stöhr-Voloch's

approach to the Hasse-Weil bound. Here we study further the interplay between these divisors and we prove that the support of the $\mathbb{F}_{q^2}$-Frobenius divisor associated to $\mathcal{D}$ is contained in the union of the set of $\mathbb{F}_{q^2}$-rational points and the set of Weierstrass points of the curve (see Theorem 2.1). This inclusion turned out to be an equality (Theorem 3.7) in the case of maximal curves having classical Weierstrass gaps. This answers the following interesting question at the set-theoretical level,

Question 1.1. For a maximal curve X over $\mathbb{F}_{q^2}$ with classical Weierstrass gaps, holds it that

$$S^{\mathcal{D}} = (n+1) \sum_{P \in X(\mathbb{F}_{q^2})} P + R^{\mathcal{K}_X} \ ?$$

Above $S^{\mathcal{D}}$ is the $\mathbb{F}_{q^2}$-Frobenius divisor associated to the linear system $\mathcal{D}$ (see [SV]), and $R^{\mathcal{K}_X}$ is the ramification divisor associated to the canonical linear system $\mathcal{K}_X$ of X (whose support consists of exactly the Weierstrass points of X). Remark 2.3 gives computational evidence and Theorem 2.1 gives set-theoretical evidence to the question. Moreover, Examples 2.4 and 3.8 give a positive answer to the question for a class of hyperelliptic maximal curves.

We recall that the genus g of a maximal curve over $\mathbb{F}_{q^2}$ satisfies $g \geq q - n$, $n+1$ being the projective dimension of the linear system $\mathcal{D}$, and $g = q - n$ if the curve has classical Weierstrass gaps [FGT, Proposition 1.7(i)]. So while in [FGT] we were interested in maximal curves with high genus, here on the contrary we are mainly interested on maximal curves with the smallest possible genus.

We end up the paper by giving examples of maximal curves with classical Weierstrass gaps and with Remark 4.1 which suggests the investigation of maximal curves in a more restricted class.

2. Maximal curves

We use the following terminology and notations:

- A curve over $\mathbb{F}_{q^2}$ is a projective geometrically irreducible nonsingular algebraic curve defined over $\mathbb{F}_{q^2}$.
- For X a maximal curve over $\mathbb{F}_{q^2}$ and $P_0 \in X(\mathbb{F}_{q^2})$ we set
$$\mathcal{D} := |(q+1)P_0|, \qquad n+1 := \dim(\mathcal{D}).$$
- For a $\mathbb{F}_{q^2}$-linear system $\mathcal{L}$ on $X \,|\, \mathbb{F}_{q^2}$ we denote by $R^{\mathcal{L}}$ (resp. $S^{\mathcal{L}} = S^{(\mathcal{L},q^2)}$) the ramification divisor (resp. the $\mathbb{F}_{q^2}$-Frobenius divisor) associated to $\mathcal{L}$; the notation $j_i(P)$ (resp. $L_i(P)$) stands for the ith $(\mathcal{D}, P)$-order (resp. ith $\mathcal{D}$-osculating space at P); see [SV].
- We denote by $\mathcal{K} = \mathcal{K}_X$ the canonical linear system on X. Recall that $\mathcal{W}_X := \mathrm{Supp}(R^{\mathcal{K}})$ is the set of Weierstrass points of X.

- For $P \in X$, $m_i = m_i(P)$ denotes the ith non-gap at P, with $m_0(P) := 0$, and $H(P)$ the Weierstrass semigroup at P. Recall that a curve X is classical iff $m_1(P) = g + 1$ for each $P \notin \mathcal{W}_X$, g being the genus of X.
- Fr_X denotes the Frobenius morphism on X relative to $\mathbb{F}_{q^2}$.

Fundamental Linear Equivalence (FGT, Corollary 1.2)**.** *For $X \mid \mathbb{F}_{q^2}$ a maximal curve, $P_0 \in X(\mathbb{F}_{q^2})$ and $P \in X$, we have the following linear equivalence:*

$$qP + \mathrm{Fr}_X(P) \sim (q+1)P_0 \,.$$

It follows that $n+1$ is independent of $P_0 \in X(\mathbb{F}_{q^2})$, that $m_{n+1}(P) = q+1$ for each $P \in X(\mathbb{F}_{q^2})$, and that

$$m_0(P) = 0 < \ldots < m_n(P) \le q < m_{n+1}(P) \qquad \text{for each } P \in X \,. \tag{2.1}$$

Therefore the following numbers are $(\mathcal{D}, P)$-orders for $P \notin X(\mathbb{F}_{q^2})$ [FGT, Prop. 1.5(ii)]:

$$q - m_i(P) \qquad \text{for} \qquad i = 0, 1, \ldots, n \,. \tag{2.2}$$

In addition, $m_n(P) = q$ for each $P \in X(\mathbb{F}_{q^2}) \cup (X \setminus X(\mathbb{F}_{q^4}))$ [FGT, Prop. 1.5(v)].

Theorem 2.1. *For $X \,|\, \mathbb{F}_{q^2}$ a maximal curve, we have*

$$\mathrm{Supp}(S^{\mathcal{D}}) \subseteq \mathcal{W}_X \cup X(\mathbb{F}_{q^2}) \,.$$

Proof. Let $P \notin \mathcal{W}_X \cup X(\mathbb{F}_{q^2})$. Then $m_i(P)$ is independent of P and $\nu_i := q - m_{n-i}(P)$ $(i = 0, \ldots, n)$ are the $\mathbb{F}_{q^2}$-Frobenius orders of $\mathcal{D}$ [FT2, §2.2]. Furthermore, by (2.2), there exists $I = I(P) \in \mathbb{Z}^+$ such that

$$\nu_0 < \ldots < \nu_{I-1} < j_I(P) < \nu_I < \ldots < \nu_n \tag{$*$}$$

are the $(\mathcal{D}, P)$-orders.

Claim. $\mathrm{Fr}_X(P) \in L_I(P) \setminus L_{I-1}(P)$.

Proof. (*Claim*) For $i = 0, 1, \ldots, n$ let $u_{n-i} \in \bar{\mathbb{F}}_{q^2}(X)$, where $\bar{\mathbb{F}}_{q^2}$ stands for the algebraic closure of $\mathbb{F}_{q^2}$, be such that $\mathrm{div}(u_{n-i}) = D_i - m_i(P)P$, with $D_i \succeq 0$, $P \notin \mathrm{Supp}(D_i)$ and let $u \in \bar{\mathbb{F}}_{q^2}(X)$ be such that $\mathrm{div}(u) = qP + \mathrm{Fr}_X(P) - (q+1)P_0$ (cf. the Fundamental Linear Equivalence). Then

$$\mathrm{div}(uu_{n-i}) + (q+1)P_0 = (q - m_i(P))P + \mathrm{Fr}_X(P) + D_i \,. \tag{$**$}$$

By considering the morphism π with homogeneous coordinates v and uu_{n-i}, $i = 0, 1, \ldots, n$, where $v \in \bar{\mathbb{F}}_{q^2}(X)$ is such that $\mathrm{div}(v) + (q+1)P_0 = j_I(P)P + D_v$, with $D_v \succeq 0$, $P \notin \mathrm{Supp}(D_v)$, we see from [SV, Proof of Thm. 1.1] and $(**)$ that $\mathrm{Fr}_X(P) \in L_I(P)$. Now (loc. cit.) if $\mathrm{Fr}_X(P) \in L_{I-1}(P)$, then $\mathrm{Fr}_X(P) \in \mathrm{Supp}(D_v)$ and by the Fundamental Linear Equivalence we would have $q - j_I(P) = m_i(P)$ for some $i = 0, 1, \ldots, n$, a contradiction. □

To finish the proof of the theorem, notice that the claim and $(*)$ imply the following linear relation

$$(***) \qquad D^{j_I(P)}\pi(P) = a\pi(\mathrm{Fr}_X(P)) + \sum_{i=0}^{I-1} a_i D^{\nu_i}\pi(P)\,,$$

where $a \neq 0, a_i \in \bar{\mathbb{F}}_{q^2}$ and $D^j\pi(P)$ is the vector whose coordinates are evaluations at P of the Hasse derivatives (with respect to a local parameter at P) of the homogeneous coordinates of the morphism π defined above. Now suppose that $P \in \mathrm{Supp}(S^{\mathcal{D}})$. Then, the following vectors would be linearly dependent

$$\pi(\mathrm{Fr}_X(P)), D^{\nu_0}\pi(P), D^{\nu_1}\pi(P), \ldots, D^{\nu_n}\pi(P)\,.$$

From the linear relation in $(***)$ we then conclude that the following vectors would be linearly dependent

$$D^{j_I(P)}\pi(P), D^{\nu_0}\pi(P), D^{\nu_1}\pi(P), \ldots, D^{\nu_n}\pi(P)$$

and this contradicts the fact that the elements in $(*)$ are the $(\mathcal{D}, P)$-orders. □

Remark 2.2. Recall that $X(\mathbb{F}_{q^2}) \subseteq \mathrm{Supp}(R^{\mathcal{D}})$ [FGT, Thm 1.4] and that these sets may be different from each other [FGT, Example 1.6]. So in general we have that

$$\mathrm{Supp}(S^{\mathcal{D}}) \subseteq \mathcal{W}_X \cup X(\mathbb{F}_{q^2}) \subseteq \mathcal{W}_X \cup \mathrm{Supp}(R^{\mathcal{D}}),$$

where the last inclusion may be proper.

Remark 2.3. Suppose that X is both maximal and classical. Then, by considering $P \notin \mathcal{W}_X$, from (2.1) we have that $g = q - n$ and that the $\mathcal{D}$-orders are $0, \ldots, n-1, \epsilon_n \geq n$ and q (cf. [FGT, Prop. 1.5(ii), Prop. 1.7]). We also have that the $\mathbb{F}_{q^2}$-Frobenius orders of $\mathcal{D}$ are $0, \ldots, n-1, q$ ([FT2, §2.2]). Since [SV, p. 9]

$$\deg(S^{\mathcal{D}}) = \sum_{i=0}^{n} \nu_i(2g-2) + (q^2+n+1)(q+1)\,,$$

after some computations we find that

$$(2.3) \qquad \deg(S^{\mathcal{D}}) = (n+1)\#X(\mathbb{F}_{q^2}) + \deg(R^{\mathcal{K}_X})\,.$$

This together with Theorem 2.1 suggest Question 1.1 in the introduction.

Example 2.4. Here we are going to show that the equality in Question 1.1 holds for certain hyperelliptic maximal curves. Let $X \,|\, \mathbb{F}_{q^2}$ be such a curve of genus $g > 1$. By considering the unique linear system g^1_2 on X and the maximality of X we see that $q \geq 2g$; furthermore, it is well known that X is classical. We set $\mathcal{W} := \mathcal{W}_X$ and we restrict our attention to the case where one has

$$\mathcal{W} \subseteq X(\mathbb{F}_{q^2}) \qquad \text{and} \qquad q \text{ odd}\,.$$

(The case q even will we considered in Example 3.8.) There are two types of $\mathbb{F}_{q^2}$-rational points: either $P \in \mathcal{W}$ or $P \notin \mathcal{W}$.

Let $P \in \mathcal{W}$. Setting $t := q-2g$, the first $(n+2)$-non-gaps of X at P are $0, 2, \ldots, 2g, 2g+1, \ldots, 2g+t, 2g+t+1$ and hence, by [FGT, Prop. 1.5(iii)], the $(\mathcal{D}, P)$-orders are $0, 1, \ldots, t+1, t+3, \ldots, 2g+t-1, 2g+t+1$. So [SV, Prop. 2.4(a)] implies $v_P(S^{\mathcal{D}}) \geq q + (g-1)(g-2)/2$.

Let $P \in X(\mathbb{F}_{q^2}) \setminus \mathcal{W}$. As in the previous case, here we find that $v_P(S^{\mathcal{D}}) \geq n+1 = q-g+1$.

Since $\#\mathcal{W} = 2g+2$ (here we use q odd), then after some computations we have that

$$\sum_{P \in X(\mathbb{F}_{q^2})} v_P(S^{\mathcal{D}}) \geq \deg(S^{\mathcal{D}}) = (2g-2)(\frac{(n-1)n}{2} + q) + (q^2+n+1)(q+1)\,,$$

hence that

$$S^{\mathcal{D}} = \sum_{P \in \mathcal{W}} (q + \frac{(g-1)(g-2)}{2})P + \sum_{P \in X(\mathbb{F}_{q^2}) \setminus \mathcal{W}} (n+1)P\,.$$

From this one concludes that the equality in Question 1.1 holds by using the fact that the multiplicity of a Weierstrass point in the divisor $R^{\mathcal{K}}$ is $g(g-1)/2$.

3. Certain maximal curves

The curves we have in mind in this section are maximal curves having classical Weierstrass gaps, however we will consider a more general setting. For a maximal curve $X \,|\, \mathbb{F}_{q^2}$ let us consider the following conditions:

(I) For $Q_1, Q_2 \notin X(\mathbb{F}_{q^2})$, $H(Q_1) \cap [0,q] = H(Q_2) \cap [0,q] \Rightarrow H(Q_1) = H(Q_2)$.
(II) For $Q \notin \mathcal{W}_X$, $m_i(Q) = q-n+i$, $i = 1, \ldots, n$.

By (2.1) each maximal curve with $g = q-n$ (e.g. a classical maximal curve) satisfies Condition (I). Other examples are provided by maximal curves $X \,|\, \mathbb{F}_{q^2}$ with $\mathcal{W}_X \subseteq X(\mathbb{F}_{q^2})$; in this case $\mathcal{W}_X = X(\mathbb{F}_{q^2})$ whenever $g > q-n$ [FT2, Corollary 2.3].

Condition (II) is satisfied by classical maximal curves, by the Hermitian curve and by some curves covered by this curve (see [G-Vi]).

For $X \,|\, \mathbb{F}_{q^2}$ a maximal curve, denote by $\tilde{m}_i$ the ith non-gap at $P \notin \mathcal{W}_X$. If X satisfies Condition (II), then, by (2.2) and [FGT, Thm. 1.4(i)], the $\mathcal{D}$-orders are $0, \ldots, n-1, \epsilon_n \geq n$ and $\epsilon_{n+1} = q$; furthermore, by [FT2, §2.2], the $\mathbb{F}_{q^2}$-Frobenius orders are $0, \ldots, n-1$ and q.

Proposition 3.1. *For a maximal curve $X \,|\, \mathbb{F}_{q^2}$ satisfying Condition (I), one has*

$$\mathcal{W}_X \setminus \mathrm{Supp}(R^{\mathcal{D}}) \subseteq \mathrm{Supp}(S^{\mathcal{D}})\,.$$

Proof. We first notice that, for $Q \notin X(\mathbb{F}_{q^2})$, Condition (I) implies

$$Q \in \mathcal{W}_X \quad \Leftrightarrow \quad \{m_1(Q), \dots, m_n(Q)\} \neq \{\tilde{m}_1, \dots, \tilde{m}_n\};$$

we also notice that $m_i(Q) \leq \tilde{m}_i$ for each i. Now let $Q \in \mathcal{W}_X \setminus \mathrm{Supp}(R^{\mathcal{D}})$ and let $k \in [1, n-1]$ be such that $m_i(Q) = \tilde{m}_i$ for $1 \leq i < k$ and $m_k(Q) < \tilde{m}_k$. Then, by (2.2), the $\mathcal{D}$-orders (which are also the $(\mathcal{D}, Q)$-orders since $Q \notin \mathrm{Supp}(R^{\mathcal{D}})$) are

$$\epsilon_0 = 0 = q - \tilde{m}_n < \epsilon_1 = 1 = q - \tilde{m}_{n-1} \dots < \epsilon_{n-k} = q - \tilde{m}_k <$$
$$\epsilon_{n-k+1} = q - m_k(Q) < \epsilon_{n-k+2} = q - \tilde{m}_{k-1} < \dots < \epsilon_{n+1} = q = q - \tilde{m}_0$$

so that $m_i(Q) = \tilde{m}_i$ for $k+1 \leq i \leq n$. As in the proof of the claim in Theorem 2.1, we conclude that (for $J = n - k$)

$$\mathrm{Fr}_X(Q) \in L_J(Q) \setminus L_{J-1}(Q).$$

We note also that ϵ_{J+1} is the $\mathcal{D}$-order one should take out to get the $\mathbb{F}_{q^2}$-Frobenius orders of $\mathcal{D}$, hence $\nu_i = \epsilon_i$ for $i \leq J$. We then conclude that the vectors

$$\pi(\mathrm{Fr}_X(Q)), D^{\nu_0}\pi(Q), \dots, D^{\nu_J}\pi(Q)$$

are linearly dependent and this finishes the proof. □

Lemma 3.2. *Let $X \,|\, \mathbb{F}_{q^2}$ be a maximal curve satisfying both Conditions (I) and (II) and let $P \in \mathcal{W}_X \setminus X(\mathbb{F}_{q^2})$ with $j_{n-1}(P) = n-1$. Then $m_1(P) = q - j_n(P)$.*

Proof. By (2.2) we have that $q - m_1(P)$ is a $(\mathcal{D}, P)$-order with $q - m_1(P) \leq j_n(P)$. If $q - m_1(P) < j_n(P)$ we would have $q - m_1(P) \leq n-1$ so that $m_i(P) = q - n + i$ for $i = 1, \dots, n$ (see (2.1)). Consequently by Condition (II), $H(P) \cap [0, q] = H(Q) \cap [0, q]$, for $Q \notin \mathcal{W}_X$ and hence $H(P) = H(Q)$ by Condition (I), i.e. P is not a Weierstrass point, a contradiction. □

Remark 3.3. Suppose that X satisfies both Conditions (I) and (II). Let $P \in \mathcal{W}_X \setminus \mathrm{Supp}(R^{\mathcal{D}})$. Then Lemma 3.2 implies $m_1(P) = q - \epsilon_n$ and from the proof of Proposition 3.1, we have $m_i(P) = q - n + i$, $i = 2, \dots, n$. Then

$$n \leq \epsilon_n \leq \frac{q + n - 2}{2},$$

where the last inequality follows from the fact that $2m_1(P) \geq m_2(P)$. Next we state a criterion to ensure that $\epsilon_n = n$, namely

$$\mathcal{W}_X \setminus \mathrm{Supp}(R^{\mathcal{D}}) \neq \emptyset \quad \text{and} \quad p := \mathrm{char}(\mathbb{F}_{q^2}) \geq g \qquad \Rightarrow \qquad \epsilon_n = n.$$

Indeed if $\epsilon_n > n$, by the p-adic criterion [SV, Corollary 1.9], we would have $\epsilon_n \leq q - p$ so that $\epsilon_n \leq n + g - p$ (see (2.1)), i.e. $\epsilon_n = n$, a contradiction.

Lemma 3.4. *Let $X \,|\, \mathbb{F}_{q^2}$ be a maximal curve satisfying both Conditions (I) and (II) and let $P \in X \setminus X(\mathbb{F}_{q^2})$ with $j_{n-1}(P) = n-1$. Then the following statements are equivalent:*

1. $q - j_n(P) \in H(P)$.
2. $P \in \mathrm{Supp}(S^{\mathcal{D}})$.

Proof. (1) $\Rightarrow$ (2) : If $q - j_n(P) \in H(P)$, then as in the proof of the claim in Theorem 2.1 we have $\mathrm{Fr}_X(P) \in L_{n-1}(P)$ and hence it belongs to $\mathrm{Supp}(S^{\mathcal{D}})$ since $0, \ldots, n-1$ are the $\mathbb{F}_{q^2}$-Frobenius orders of $\mathcal{D}$ and $j_{n-1}(P) = n-1$.

(2) $\Rightarrow$ (1) By Theorem 2.1 we have that $P \in \mathcal{W}_X$ and the result follows from Lemma 3.2. □

Corollary 3.5. *Let $X\,|\,\mathbb{F}_{q^2}$ be a maximal curve satisfying both Conditions (I) and (II). For $P \in X$ the following statements are equivalent:*

1. $P \notin \mathrm{Supp}(S^{\mathcal{D}})$.
2. *The $(\mathcal{D}, P)$-orders are $0, 1, \ldots, n-1, j_n$ and $j_{n+1} = q$ with $q - j_n \notin H(P)$.*

Proof. By Lemma 3.4 we just need to show that (1) $\Rightarrow$ (2). Since $0, \ldots, n-1$ are $\mathbb{F}_{q^2}$-Frobenius orders and in view of [FGT, Thm. 1.4(ii)], we see that $j_{n-1}(P) > n-1$ or $j_{n+1}(P) = q+1$ imply that $P \in \mathrm{Supp}(S^{\mathcal{D}})$. So the $(\mathcal{D}, P)$-orders are as stated in (2) and the result follows again from Lemma 3.4 □

From Theorem 2.1, Lemma 3.2 and Lemma 3.4, we obtain

Corollary 3.6. *Let $X\,|\,\mathbb{F}_{q^2}$ be a maximal curve satisfying both Conditions (I) and (II) and $P \in X \setminus X(\mathbb{F}_{q^2})$ with $j_{n-1}(P) = n-1$. The following statements are equivalent:*

1. $P \in \mathrm{Supp}(S^{\mathcal{D}})$.
2. $P \in \mathcal{W}_X$.
3. $m_1(P) = q - j_n(P)$.
4. $q - j_n(P) \in H(P)$.

Now we can state the main result of this section:

Theorem 3.7. *For a maximal curve satisfying both Conditions (I) and (II), we have*

$$\mathrm{Supp}(S^{\mathcal{D}}) = \mathcal{W}_X \cup X(\mathbb{F}_{q^2})\,.$$

Proof. From Theorem 2.1 and the fact that $X(\mathbb{F}_{q^2}) \subseteq \mathrm{Supp}(S^{\mathcal{D}})$ it is enough to show that

$$P \in \mathcal{W}_X \setminus X(\mathbb{F}_{q^2}) \quad \Rightarrow \quad P \in \mathrm{Supp}(S^{\mathcal{D}})\,.$$

If $j_{n-1}(P) > n-1$, then $P \in \mathrm{Supp}(S^{\mathcal{D}})$ (see the proof of Corollary 3.5). So let now $j_{n-1}(P) = n-1$. Then again $P \in \mathrm{Supp}(S^{\mathcal{D}})$ as follows from Corollary 3.6. □

Example 3.8. We complement Example 2.4 by considering hyperelliptic maximal curves of genus bigger than 1 over $\mathbb{F}_{q^2}$ with q even. We are going to show that these curves also satisfy the equality in Question 1.1. So let X be a such curve. By [FGT, Proposition 1.7(ii)], $\#\mathcal{W}_X = 1$; say $\mathcal{W}_X = \{Q\}$. Then for at least $(\#X(\mathbb{F}_{q^2}) - 1)$ $\mathbb{F}_{q^2}$-rational points $P \in X$ we have $v_P(S^{\mathcal{D}}) = n + 1$, as follows from the computations in Example 2.4 and [SV, Proposition 2.4(a)]. Furthermore $\mathrm{Supp}(S^{\mathcal{D}}) = \{Q\} \cup X(\mathbb{F}_{q^2})$ by Theorem 3.7. Next we compute $v_Q(S^{\mathcal{D}})$ by using Eq. (2.3). We consider two cases according Q is $\mathbb{F}_{q^2}$-rational or not.

If $Q \in X(\mathbb{F}_{q^2})$, from (2.3) we have

$$v_Q(S^{\mathcal{D}}) = \deg(S^{\mathcal{D}}) - (n+1)(\#X(\mathbb{F}_{q^2}) - 1) = \deg(R_X^{\mathcal{W}}) + n + 1\,.$$

If $Q \notin X(\mathbb{F}_{q^2})$, from (2.3) we have

$$v_Q(S^{\mathcal{D}}) = \deg(S^{\mathcal{D}}) - (n+1)\#X(\mathbb{F}_{q^2}) = \deg(R_X^{\mathcal{W}})\,.$$

From these computations follow the equality in Question 1.1 for hyperelliptic maximal curves over $\mathbb{F}_{q^2}$ with q even.

4. Examples

From [R-Sti], the unique maximal curve over $\mathbb{F}_{q^2}$ of genus $q(q-1)/2$ is the Hermitian curve in $\mathbb{P}^2(\bar{\mathbb{F}}_{q^2})$ defined by

$$Y(Y^{q-1} + 1) = X^{q+1}\,.$$

Let $\pi : \mathbb{P}^2(\bar{\mathbb{F}}_{q^2}) \to \mathbb{P}^2(\bar{\mathbb{F}}_{q^2})$ be the morphism over $\mathbb{F}_{q^2}$ given by $(x : y : 1) \to (y^{q-1} : x^{(q^2-1)/m} : 1)$ with m a divisor of $(q^2 - 1)$. Then the nonsingular model of $\pi(X)$ is a maximal curve over $\mathbb{F}_{q^2}$ [La, Proposition 6] and $\pi(X)$ is defined by

$$W^m = Z(Z+1)^{q-1}\,. \tag{4.1}$$

By the Riemann-Hurwitz relation, the genus g of this curve satisfies

$$g = \frac{m - \delta}{2}, \qquad \text{where } \delta = \gcd(m, q-1)\,.$$

These examples are the ones in [G-Sti-X, Corollary 4.9] (see also Lang's [L, Ch. I,§7] and the references therein). Suppose one is interested in genus 4 maximal curves of the type above. So $m - \delta = 8$ and since δ divides m, we have that $\delta = 1, 2, 4$ or 8. As an example, let $\delta = 1$ and hence $m = 9$. Since $m = 9$ divides $(q^2 - 1)$ and moreover $\delta = 1 = \gcd(m, q-1)$, we must have that m divides $(q+1)$. So the prime power q must be chosen in the following congruence class:

$$q \equiv -1 \pmod 9\,.$$

With the above reasoning one obtains the following table which gives for a fixed genus g $(1 \le g \le 7)$ maximal curves over $\mathbb{F}_{q^2}$ arising from curves of type (4.1).

Genus	m	q	Genus	m	q
$g=1$	3	$q\equiv -1 \pmod 3$	$g=5$	11	$q\equiv -1 \pmod{11}$
$g=1$	4	$q\equiv -1 \pmod 4$	$g=5$	12	$q\equiv -1 \pmod{12}$
$g=2$	5	$q\equiv -1 \pmod 5$	$g=5$	15	$q\equiv -4 \pmod{15}$
$g=2$	6	$q\equiv -1 \pmod 6$	$g=5$	20	$q\equiv 11 \pmod{20}$
$g=2$	8	$q\equiv 5 \pmod 8$	$g=6$	13	$q\equiv -1 \pmod{13}$
$g=3$	7	$q\equiv -1 \pmod 7$	$g=6$	14	$q\equiv -1 \pmod{14}$
$g=3$	8	$q\equiv -1 \pmod 4$	$g=6$	15	$q\equiv 4 \pmod{15}$
$g=3$	12	$q\equiv 7 \pmod{12}$	$g=6$	24	$q\equiv 13 \pmod{24}$
$g=4$	9	$q\equiv -1 \pmod 9$	$g=7$	15	$q\equiv -1 \pmod{15}$
$g=4$	10	$q\equiv -1 \pmod{10}$	$g=7$	16	$q\equiv -1 \pmod 8$
$g=4$	12	$q\equiv 5 \pmod{12}$	$g=7$	21	$q\equiv 8 \pmod{21}$
$g=4$	16	$q\equiv 9 \pmod{16}$	$g=7$	28	$q\equiv 15 \pmod{28}$

By the Dirichlet theorem there are infinitely many prime numbers in each of the congruence classes above. Notice that the classicality of the curve is assured as soon as $\mathrm{char}(\mathbb{F}_{q^2}) > 2g-2$.

Remark 4.1. We finish this section with a more restricted class of classical maximal curves . We consider maximal curves over $\mathbb{F}_{q^2}$ where each rational point is not a Weierstrass point, so that $v_P(R^{\mathcal{D}})=1$ for each $P\in X(\mathbb{F}_{q^2})$, and where

$$X(\mathbb{F}_{q^2}) = \mathrm{Supp}(R^{\mathcal{D}})\,.$$

Then from

$$\deg(R^{\mathcal{D}}) = (\frac{n(n+1)}{2}+q)(2g-2)+(n+2)(q+1) = \#X(\mathbb{F}_{q^2}) = (q+1)^2+q(2g-2)$$

we have that $n(n+1)(g-1)=(q+1)(g-1)$ and hence

$$g=1 \qquad \text{or} \qquad q=n^2+n-1\,.$$

The only example we know of a curve with $g>1$ in this restricted class of maximal curves is the one over $\mathbb{F}_{25}$ of genus 3 listed by Serre in [Se, Section 4]; in this example $n=2$ (cf. [FGT, Example 2.4(i)]).

References

[B] Bombieri, E.: *Hilbert's 8th problem: An analogue*, Proc. Symp. Pure Math. **28**, 269–274 (1976).

[D] Dickson, L.E.: *History of the theory of numbers*, Vol. II, Chelsea Publ. Comp., New York, 1971.

[FGT] Fuhrmann, R.; Garcia, A.; Torres, F.: *On maximal curves*, J. Number Theory **67**(1), 29–51 (1997).

[FT1] Fuhrmann, R.; Torres, F.: *The genus of curves over finite fields with many rational points*, Manuscripta Math. **89**, 103–106 (1996).

[FT2] Fuhrmann, R.; Torres, F.: *On Weierstrass points and optimal curves*, to appear in Rend. Circ. Mat. Palermo.

[G-Sti-X] Garcia, A.; Stichtenoth, H.; Xing, C.: *On subfields of the Hermitian function field*, Compositio Math., to appear.

[G-Vi] Garcia, A.; Viana, P.: *Weierstrass points on certain non-classical curves*, Arch. Math. **46**, 315–322 (1986).

[Go] Goppa, V.D.: *Geometry and Codes*, Mathematics and its applications, 24, Kluwer Academic Publishers, Dordrecht-Boston-London, 1988.

[H] Hirschfeld, J.W.P.: *Projective Geometries over Finite Fields*, second edition, Oxford University Press, Oxford, 1998.

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

[K] Kontogeorgis, A.I.: *The group of automorphisms of function fields of the curve* $x^n+y^m+1=0$, J. Number Theory **72**, 110–136 (1998).

[L] Lang, S.: *Complex Multiplication*, Grundlehren der mathematischen Wissenschaften 255, Springer-Verlag, 1983.

[La] Lachaud, G.: *Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis*, C.R. Acad. Sci. Paris, **305**, Série I, 729–732 (1987).

[L-N] Lidl, R.; Niederreiter, H.: *Finite Fields*, Encyclopedia of mathematics and its applications, vol. 20, Addison-Wesley, 1983.

[Mo] Moreno, C.J.: *Algebraic Curves over Finite Fields*, Cambridge University Press, Vol. 97, 1991.

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

[Sch] Schmidt, F.K.: *Zur arithmetischen Theorie der algebraischen Funktionen II. Allgemeine Theorie der Weierstrasspunkte*, Math. Z. **45**, 75–96 (1939).

[Se] Serre, J.P.: *Résumé des cours de 1983-1984*, Annu. Collegue France **79**–**83** (1984).

[Ste] Stepanov, S.A.: *Arithmetic of algebraic curves*, Monographs in contemporary mathematics, Consultants Bureau, New York - London, 1994.

[Sti] Stichtenoth, H.: *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharacteristic*, Arch. Math. **24**, 527–544 and 615–631 (1973).

[Sti-X] Stichtenoth, H.; Xing, C.: *The genus of maximal functions fields*, Manuscripta Math. **86**, 217–224 (1995).

[SV] Stöhr, K.O.; Voloch, J.F.: *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. (3) **52**, 1–19 (1986).

[W] Weil, A.: *Courbes algébriques et variétés abeliennes*, Hermann, Paris, 1971.

IMPA, Est. Dona Castorina 110, Rio de Janeiro, 22460-320-RJ, Brazil

E-mail address: garcia@impa.br

IMECC-UNICAMP, Cx. P. 6065, Campinas, 13083-970-SP, Brazil

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