ON A $\mathbf{F}_{q^2}$-MAXIMAL CURVE OF GENUS $q(q-3)/6$

MIRIAM ABDÓN AND FERNANDO TORRES

Abstract. We show that a $\mathbf{F}_{q^2}$-maximal curve of genus $q(q-3)/6$ in characteristic three is unique up to $\mathbf{F}_{q^2}$-isomorphism unless an unexpected situation occurs.

1. Introduction

Let $\mathcal{X}$ be a projective, geometrically irreducible, non-singular algebraic curve of genus g defined over the finite field $\mathbf{F}_{q^2}$ of order q^2. The curve $\mathcal{X}$ is called $\mathbf{F}_{q^2}$-*maximal* if it attains the Hasse-Weil upper bound on the number of $\mathbf{F}_{q^2}$-rational points; i.e., if one has

$$\#\mathcal{X}(\mathbf{F}_{q^2}) = (q+1)^2 + q(2g-2)\,.$$

Maximal curves are known to be very useful in Coding Theory [18] and they have been intensively studied by several authors: see e.g. [34], [17], [12], [13], [14], [16], [15], [28], [29]. The subject of this paper is related to the following basic questions:

- For a given power q of a prime, which is the spectrum of the genera g of $\mathbf{F}_{q^2}$-maximal curves?
- For each g in the previous item, how many non-isomorphic $\mathbf{F}_{q^2}$-maximal curves of genus g do exist?
- Write down an explicit $\mathbf{F}_{q^2}$-plane model for each of the curves in the previous item.

Ihara [26] observed that g cannot be large enough compared with q^2. More precisely,

$$g \le g_1 = g_1(q^2) := q(q-1)/2\,.$$

Rück and Stichtenoth [32] showed that (up to $\mathbf{F}_{q^2}$-isomorphism) there is just one $\mathbf{F}_{q^2}$-maximal curve of genus g_1, namely the Hermitian curve of equation

$$Y^qZ + YZ^q = X^{q+1}\,. \tag{1.1}$$

Conversely, if $g < g_1$, then

$$g \le g_2 = g_2(q^2) := \lfloor (q-1)^2/4 \rfloor$$

2000 Math. Subj. Class.: Primary 11G20, Secondary 14G05, 14G10.

Key words.: Finite field, Maximal curve, Artin-Schreier extension, Additive polynomial.

Abdón was partially supported by FAPERJ and PRONEX-Cnpq (Brazil) while Torres acknowledges support by Cnpq-Brazil, Proc. 300681/97-6.

(see [34], [13]) and, up to $\mathbf{F}_{q^2}$-isomorphism, there is just one $\mathbf{F}_{q^2}$-maximal curve of genus g_2 which is obtained as the quotient of the Hermitian curve by a certain involution (see [12, Thm. 3.1], [4], [29, Thm. 3.1]). Now if $g < g_2$, then (see [29])

$$g \le g_3 = g_3(q^2) := \lfloor (q^2 - q + 4)/6 \rfloor \,,$$

being this bound sharp as examples in [15], [28], and [11] show. These examples arise as quotient curves of the Hermitian curve by certain automorphism of order three; however it is not known whether or not such curves are $\mathbf{F}_{q^2}$-unique. In view of the results stated above and taking into consideration the examples in [10], [11] and [15], it is reasonable to expect that only few (non-isomorphism) $\mathbf{F}_{q^2}$-maximal curves do exist having genus g close to the upper limit g_1 provided that q is fixed. As a matter of fact, in the range

$$\lfloor (q-1)(q-2)/6 \rfloor \le g < g_3 \,,$$

the following statements hold:

(I) If $q \equiv 2 \pmod 3$, there exists an $\mathbf{F}_{q^2}$-maximal curve of genus $g = g_3 - 1$; see [10, Thm. 6.2] and [15, Thm. 5.1]. Such a curve is also the quotient of the Hermitian curve by a certain automorphism of order three and it is also not known whether this curve is unique or not;

(II) If $q \equiv 2 \pmod 3$ and $q \ge 11$, there is just one $\mathbf{F}_{q^2}$-maximal curve (up to $\mathbf{F}_{q^2}$-isomorphism) of genus $(q-1)(q-2)/6$, namely the non-singular model of the affine plane curve $y^q + y = x^{(q+1)/3}$, see [29, Thm. 4.5];

(III) If $q \equiv 1 \pmod 3$ with $q \ge 13$, there is no $\mathbf{F}_{q^2}$-maximal curve of genus $(q-1)(q-2)/6$, loc. cit.;

(IV) If $q = 3^t$, $t \ge 1$, there exists an $\mathbf{F}_{q^2}$-maximal curve of genus $g = q(q-3)/6$, namely the non-singular model over $\mathbf{F}_{q^2}$ of the affine plane curve

$$\sum_{i=1}^{t} y^{q/3^i} = x^{q+1} \,. \tag{1.2}$$

The objective of this paper is to investigate the uniqueness (up to $\mathbf{F}_{q^2}$-isomorphism) of the $\mathbf{F}_{q^2}$-maximal curve in statement (IV) above. Our main result is Theorem 4.1, where we show that if such a curve is not uniquely defined by (1.2), then an unexpected situation might occur; unfortunately, we we do not know whether or not such a circumstance can be eliminated (see Remarks in Section 3). We point out that several examples of non-isomorphic $\mathbf{F}_{q^2}$-maximal curves of genus $g \approx q^2/8$ are known; see [9, Remark 4.1], [1], [3].

As in previous research (see e.g. [12], [29] and the reference therein), the essential tool used here is Stöhr-Voloch's approach [35] to the Hasse-Weil bound applied to the complete base-point-free linear series $\mathcal{D} := |(q+1)P_0|$ defined on maximal curves which was introduced in [13]. In Section 2 we review some properties of $\mathcal{D}$; in particular, for $g = (q-3)q/6$ and

$q \geq 9$ we find that the dimension of $\mathcal{D}$ is either three or four. The later case is handle as in [4] although here we simplify some computations.

2. Preliminaries

Throughout the paper we assume $q \geq 9$ since the case $q = 3$ is trivial. As it is known from [13], any $\mathbf{F}_{q^2}$-maximal curve $\mathcal{X}$ is equipped with its $\mathbf{F}_{q^2}$-canonical linear series; namely, the complete simple base-point-free linear series

$$\mathcal{D} = \mathcal{D}_{\mathcal{X}} := |(q+1)P_0|\,,$$

where P_0 is an arbitrary $\mathbf{F}_{q^2}$-rational point of $\mathcal{X}$. The key property of $\mathcal{D}$ is the following linear equivalence of divisors [12, Cor. 1.2]:

$$qP + \mathbf{\Phi}(P) \sim (q+1)P_0\,, \qquad \forall P \in \mathcal{X}\,, \tag{2.1}$$

where $\mathbf{\Phi} = \mathbf{\Phi}_{q^2}$ is the Frobenius morphism on $\mathcal{X}$ relative to $\mathbf{F}_{q^2}$. In particular, this allows us to fix a $\mathbf{F}_{q^2}$-rational point P_0 for the rest of the paper. To deal with the dimension N of $\mathcal{D}$ we use the Castelnuovo's genus bound (for curves in projective spaces) which, for a simple linear series g^r_d on $\mathcal{X}$, upper bounds the genus g of the curve by means of the Castelnuovo's number $c(d,r)$; i.e., one has

$$g \leq c(d,r) := \frac{d-1-\epsilon}{2(r-1)}(d-r+\epsilon)\,, \tag{2.2}$$

being ϵ the unique integer with $0 \leq \epsilon \leq r-2$ and $d-1 \equiv \epsilon \pmod{r-1}$; see [8], [6, p. 116], [20, IV, Thm 6.4], [31, Cor. 2.8].

Lemma 2.1. *For a $\mathbf{F}_{q^2}$-maximal curve of genus $g = q(q-3)/6$, $N \in \{3,4\}$.*

Proof. We have that $N \geq 2$ and that $N = 2$ if and only if $\mathcal{X}$ is the Hermitian curve whose genus is $g = q(q-1)/2$ (see [14, Thm. 2.4]). Therefore $N \geq 3$. If $N \geq 5$, from (2.2) and the hypothesis on g we would have $q(q-3)/6 \leq (q-2)^2/8$; so $q^2 \leq 12$, a contradiction. □

Next based on Stöhr-Voloch's Theory [35], we summarize some properties on Weierstrass Point Theory and Frobenius Orders with respect to the linear series $\mathcal{D}$. Let $\epsilon_0 = 0 < \epsilon_1 = 1 < \ldots < \epsilon_N$ and $\nu_0 = 0 < \nu_1 < \ldots < \nu_{N-1}$ denote respectively the $\mathcal{D}$-orders and $\mathbf{F}_{q^2}$-Frobenius orders of $\mathcal{D}$. For $P \in \mathcal{X}$, let $j_0(P) = 0 < j_1(P) < \ldots < j_N(P)$ be the $(\mathcal{D},P)$-orders of $\mathcal{D}$, and $(n_i(P) : i = 0,1,\ldots)$ the strictly increasing sequence that enumerates the Weierstrass semigroup $H(P)$ at P. We have

$$0 < n_1(P) < \ldots < n_{N-1}(P) \leq q < q+1 \leq n_N(P)\,,$$

and $n_N(P) = q+1$ for $P \in \mathcal{X}(\mathbf{F}_{q^2})$ by (2.1); furthermore, $n_{N-1}(P) = q$ for any $P \in \mathcal{X}$ ([12, Prop. 1.9], [29, Thm. 2.5]). We also have the following facts from [12, Thm. 1.4, Prop. 1.5]:

Lemma 2.2. (1) $\epsilon_N = \nu_{N-1} = q$;

(2) $\nu_1 = 1$ *if* $N \geq 3$;
(3) $j_1(P) = 1$ *for any* P;
(4) $j_N(P) = q+1$ *if* $P \in \mathcal{X}(\mathbf{F}_{q^2})$, *otherwise* $j_N(P) = q$;
(5) *If* $P \in \mathcal{X}(\mathbf{F}_{q^2})$, *then the* $(\mathcal{D}, P)$*-orders are* $n_N(P) - n_i(P)$, $i = 0, 1, \ldots, N$;
(6) *If* $P \notin \mathcal{X}(\mathbf{F}_{q^2})$, *then the elements* $n_{N-1}(P) - n_i(P)$, $i = 0, \ldots, N-1$, *are* $(\mathcal{D}, P)$*-orders.*

3. Case $N = 3$

Let $\mathcal{X}$ be a $\mathbf{F}_{q^2}$-maximal curve of genus $g = q(q-3)/6$ and let us keep the notation in Section 2. Then, as we saw in Lemma 2.1, the dimension N of $\mathcal{D} = \mathcal{D}_{\mathcal{X}}$ is either 3 or 4. In this section we point out some consequences of former possibility.

Lemma 3.1. *If* $N = 3$, *then* $\epsilon_2 = 3$.

Proof. Let S be the $\mathbf{F}_{q^2}$-Frobenius divisor associated to $\mathcal{D}$ (cf. [35]). Then $\deg(S) = (\nu_1 + \nu_2)(2g-2) + (q^2+3)(q+1)$, where $\nu_1 = 1$ and $\nu_2 = q$ by Lemma 2.2. For $P \in \mathcal{X}(\mathbf{F}_{q^2})$ it is known that (loc. cit.)

$$v_P(S) \geq j_1(P) + (j_2(P) - \nu_1) + (j_3(P) - \nu_2) = j_2(P) + 1\,.$$

Moreover, as $j_2(P) \geq \epsilon_2$, the maximality of $\mathcal{X}$ implies $\deg(S) \geq (\epsilon_2+1)((q+1)^2 + q(2g-2))$. Now, suppose that $\epsilon_2 \geq 4$. Then the above inequality becomes

$$(q+1)(q^2 - 5q - 2) \geq (2g-2)(4q-1)\,,$$

which is a contradiction with the hypothesis on g. Thus we have shown that $\epsilon_2 \in \{2, 3\}$. If ϵ_2 were 2, from [10, Remark 3.3(1)] we would have $g \geq (q^2 - 2q + 3)/6$, which is again a contradiction with respect to g. □

Corollary 3.2. *If* $N = 3$, *then* $\dim(2\mathcal{D}) \geq 9$.

Proof. Since $0, 1, 3, q$ are $\mathcal{D}$-orders (Lemma 2.2), then it is easy to see that $0, 1, 2, 3, 4, 6, q, q+1, q+3, 2q$ are $2\mathcal{D}$-orders and the result follows. □

Corollary 3.3. ([10, Lemma 3.7]) *If* $N = 3$, *then there exists a* $\mathbf{F}_{q^2}$*-rational point* P *such that* $n_1(P) = q-2$.

This section is close with some feelings about the possibility $N = 3$.

Remark 3.4. (Related with Weierstrass semigroups) From Lemma 2.2 and Corollary 3.3 there exists $P \in \mathcal{X}(\mathbf{F}_{q^2})$ such that $n_1(P) = q-2$, $n_2(P) = q$, $n_3(P) = q+1$; i.e., the Weierstrass semigroup $H(P)$ contains the semigroup

$$H := \langle q-2, q, q+1 \rangle = \{(q-2)i : i \in \mathbf{N}\} \cup \{qi - 2(i-1) : i \in \mathbf{Z}^+\}$$

whose genus (i.e; $\#(\mathbf{N}\setminus H)$) is equal to $(q^2-q)/6$ (see e.g. [10, Lemma 3.4]). How can we complete H in order to get $H(P)$? We have to choose $q/3$ elements from $\mathbf{N}\setminus H$, and it is easy to see that such elements must belong to the set

$$\{(i(q-1) : i = 2,\ldots,q/3-1\} \cup \{q^2-5q/3-1, q^2-5q, q^2-5q/3+1\}\,.$$

This set contains $q/3+2$ elements, so we have to exclude two elements from it. Hence we arrive to the following seven possibilities:

(i) $q-1, 2q-2 \notin H(P)$;
(ii) $q-1 \notin H(P)$ but $2q-2 \in H(P)$; in this case we have to eliminate one element from the set $\{q^2-5q/3-1, q^2-5q/3, q^2-5q/3+1\}$;
(iii) $q-1, 2q-2 \in H(P)$; in this case we have to eliminate two elements from the set $\{q^2-5q/3-1, q^2-5q/3, q^2-5q/3+1\}$.

So far, we do not know how an obstruction (for N being equal to 3) might arise from some of the possibilities above.

Remark 3.5. (Related with the Hermitian curve (1.1)) Suppose that $\mathcal{X}$ is $\mathbf{F}_{q^2}$-covered by the Hermitian curve. Then the covering cannot be Galois; otherwise by [11, Prop. 5.6] the curve would be $\mathbf{F}_{q^2}$-isomorphic to the non-singular model of (1.2) and thus $N=4$. We recall that there is not known any example of a $\mathbf{F}_{q^2}$-maximal curve $\mathbf{F}_{q^2}$-covered by the Hermitian curve by a non-Galois covering.

Remark 3.6. (Reflexivity, Duality and the Surface Tangent) Recall that we can assume our curve $\mathcal{X}$ as being embedded in $\mathbf{P}^3(\bar{\mathbf{F}}_{q^2})$ by [28, Thm. 2.5]. Hefez [21] noticed that four cases for the generic contact orders for space curves can occur. Homma [25] realized that all the four aforementioned cases occur and characterized each of them by means of the reflexivity of either the curve $\mathcal{X}$, or the tangent surface $\mathrm{Tan}(\mathcal{X})$ associated to it (see also [24]). In our situation ($\epsilon_2 = 3$ and $\epsilon_3 = q$), the curve is non-reflexive by Hefez-Kleiman Generic Order of Contact Theorem [23]. Thus, by Homma's result, it holds that $N=3$ if and only $\mathrm{Tan}(\mathcal{X})$ is non-reflexive. So far we do not know how to relate the maximality of $\mathcal{X}$ to the non-reflexivity of its tangent surface. We mention that techniques analogous to those of [35] that work on certain surfaces in $\mathbf{P}^3$ over prime fields is now available thanks to a recent paper by Voloch [36].

Remark 3.7. (Related to Halphen's theorem) Ballico [7] extended Harris [19] and Rathmann [31] results concerning space curves contained in surfaces of certain degree. For a $\mathbf{F}_{q^2}$-maximal curve $\mathcal{X}$ of genus $q(q-3)/6$, with q large enough, Ballico's result implies that $\mathcal{X}$ is contained in a surface of degree 3 or 4. On the other hand, suppose that Voloch's approach [36] can be extended to cover the case of surfaces over arbitrary finite fields. Then a conjunction of Ballico and Voloch's result would provide with further insights of the curves studied here.

4. Main Result

Theorem 4.1. *Let $\mathcal{X}$ be a $\mathbf{F}_{q^2}$-maximal curve of genus $g = q(q-3)/6$. Then either*

(1) *$\mathcal{X}$ is $\mathbf{F}_{q^2}$-isomorphic to the non-singular model of the plane curve (1.2); or*
(2) *$N := \dim(\mathcal{D}_{\mathcal{X}}) = 3$ and $\epsilon_2 = 3$.*

Remark 4.2. In Case (1), the curve is $\mathbf{F}_{q^2}$-covered by the Hermitian curve (1.1).

To give the proof of the theorem we need some auxiliary results. First of all, by Lemmas 2.1 and 3.1, we can assume $N = 4$. In particular, we notice that g is equal to Castelnuovo's number $c(q+1, 4)$ and hence from Accola's paper [5, p. 36 and Lemma 3.5] the following holds:

Lemma 4.3. (1) $\dim(2\mathcal{D}) = 11$;
(2) *There exists a base-point-free 2-dimensional complete linear series $\mathcal{D}'$ of degree $2q/3$ such that $\frac{q-6}{3}\mathcal{D} + \mathcal{D}'$ is the canonical linear series of $\mathcal{X}$.*

Part (1) of this lemma implies Lemmas 4.2 and 4.4 in [29]:

Corollary 4.4. (1) *If $j_2(P) = 2$, then $j_3(P) = 3$;*
(2) *If $P \in \mathcal{X}(\mathbf{F}_{q^2})$ and $j_2(P) > 2$, then $j_2(P) = (q+3)/3$, $j_3(P) = (2q+3)/3$;*
(3) *If $P \notin \mathcal{X}(\mathbf{F}_{q^2})$ and $j_2(P) > 2$, then either $j_2(P) = q/3$, $j_3(P) = 2q/3$; or $j_2(P) = (q-1)/2)$, $j_3(P) = (q+1)/2$.*

Lemma 4.5. *For $q = 9$, $n_1(P) = 3$ for any $P \in \mathcal{X}(\mathbf{F}_{q^2})$.*

Proof. Let P be a $\mathbf{F}_{q^2}$-rational and set $n_i := n_i(P)$. Lemma 2.2 implies that $0, 1, j_2 = 10 - n_2, j_3 = 10 - n_1, 10$ are the $\mathcal{D}$-orders at the point. Then the set of $2\mathcal{D}$-orders at P must contain the set $\{0, 1, 2, j_2, j_2+1, 2j_2, j_3, j_3+1, j_2+j_3, 2j_3, 10, 11, j_2+10, j_3+10, 20\}$ and hence, as $\dim(2\mathcal{D}) = 11$ by Lemma 4.3, the result follows. □

From now on let us assume $q \geq 27$.

Lemma 4.6. (1) *The case (3) in Corollary 4.4 cannot occur;*
(2) *There exists $P_1 \in \mathcal{X}(\mathbf{F}_{q^2})$ such that $j_2(P_1) > 2$; in this case, $n_1(P_1) = q/3$;*
(3) *Let P_1 be as in (2) and $x \in \mathbf{F}_{q^2}(\mathcal{X})$ such that $\mathrm{div}_\infty(x) = \frac{q}{3}P_1$. Then the morphism $x : \mathcal{X} \setminus \{P_1\} \to \mathbf{A}^1(\bar{\mathbf{F}}_{q^2})$ is unramified.*
(4) *The $\mathcal{D}$-orders and $\mathbf{F}_{q^2}$-Frobenius orders of $\mathcal{D}$ are respectively $0, 1, 2, 3, q$ and $0, 1, 2, q$.*

Proof. For $P \in \mathcal{X}$, set $j_i = j_i(P)$ and $n_i = n_i(P)$.

(1) We have that $\{q - n_2, q - n_1\} \subseteq \{1, j_2, j_3\}$ by Lemma 2.2(6). Suppose that Case (3) in Cor. 4.4 occurs.

Case $j_2 = q/3$, $j_3 = 2q/3$. Here $n_1 \in \{2q/3, q/3\}$; let $f \in \bar{\mathbf{F}}_{q^2}(\mathcal{X})$ such that $\mathrm{div}(f - f(\mathbf{\Phi}(P))) = D + e\mathbf{\Phi}(P) - n_1 P$, where $e \geq 1$ and $P \notin \mathrm{Supp}(D)$. If $n_1 = 2q/3$, then $3e+2$ is an $(2\mathcal{D}, \mathbf{\Phi}(P))$-order by (2.1). However, as $\dim(2\mathcal{D}) = 11$, the sequence of $(2\mathcal{D}, \mathbf{\Phi}(P))$-orders is $0, 1, 2, q/3, q/3+1, 2q/3, 2q/3+1, q, q+1, 4q/3, 5q/3, 2q$ and thus $n_1 = q/3$. In this case, arguing as above, $3e+1$ is an $(\mathcal{D}, \mathbf{\Phi}(P))$-order which is a contradiction.

Case $j_2 = (q-1)/2$, $j_3 = (q+1)/2$. From Lemma 4.3(2) and the hypothesis $q \geq 27$, we have that $2j_2 + 1 = q$ is a Weierstrass gap at P (i.e.; $q \notin H(P)$), a contradiction with $n_3 = q$.

(2) If we show that there exists $P_1 \in \mathcal{X}$ such that $j_2(P_1) > 2$, then the point P_1 will be $\mathbf{F}_{q^2}$-rational by (1). So, suppose that $j_2(P) = 2$ for any $P \in \mathcal{X}$. Let R denote the ramification divisor associated to $\mathcal{D}$ (cf. [35]). Then the $\mathcal{D}$-Weierstrass points coincide with the set of $\mathbf{F}_{q^2}$-rational points and $v_P(R) = 1$ for $P \in \mathcal{X}(\mathbf{F}_{q^2})$ (cf. Lemma 2.2). Therefore

$$\deg(R) = (q+6)(2g-2) + 5(q+1) = (q+1)^2 + q(2g-2)\,,$$

so that $2g - 2 = (q-1)(q-4)/6$, a contradiction. That $n_1 = q/3$ follows immediately from Cor. 4.4(2) and Lemma 2.2(5).

(3)-(4) Let $y \in \mathbf{F}_{q^2}(\mathcal{X})$ be such that $\mathrm{div}_\infty(y) = (q+1)P_0$. Then the sections of $\mathcal{D}$ are generated by $1, x, x^2, x^3, y$. Now, if we show that there exists $P \in \mathcal{X}(\mathbf{F}_{q^2})$ such that $j_2(P) = 2$ and $j_3(P) = 3$, then (4) follows since $\epsilon_i \leq j_i(P)$ and $\nu_{i-i} \leq j_i(P) - j_1(P)$ (cf. [35]). To see that such a point P do exist, we proceed as in [14, p. 38]. For $P \in \mathcal{X} \setminus \{P_0\}$, write $\mathrm{div}(x - x(P)) = eP + D - n_1 P_0$ with $e \geq 1$ and $P, P_0 \notin \mathrm{Supp}(D)$. Then $e, 2e, 3e$ are $(\mathcal{D}, P)$-orders and if $e > 1$, $3e = q+1$, a contradiction as $q \equiv 0 \pmod 3$. Thus the proof is complete. □

Let $v = v_{P_0}$ be the valuation at P_0, and $D^i := D^i_x$ the i-th Hasse differential operator on $\bar{\mathbf{F}}_{q^2}(\mathcal{X})$ with respect to x (see e.g. [22, §3]). We set $D := D^1$.

Corollary 4.7. $v(Dy) = -q^2/3$.

Proof. (cf. [4, p. 47]) Let t be a local parameter at P_0; then

$$v(Dy) = v(dy/dt) - v(dx/dt) = -q - 2 - 2g - 2 = -q^2/3,$$

since by the previous lemma the morphism $x : \mathcal{X} \to \mathbf{P}^1(\bar{\mathbf{F}}_{q^2})$ is totally ramified at P_0 and unramified outside P_0, and since a canonical divisor has degree $2g-2$. □

Proof of Theorem 4.1. Let x and y be as above; they are related to each other by an equation over $\mathbf{F}_{q^2}$ of type (see e.g. [27])

$$x^{q+1} + ay^{q/3} + \sum_{i=0}^{q/3-1} A_i(x)y^i = 0\,, \tag{4.1}$$

where $a \neq 0$, and the $A_i(x)$'s are polynomials in x such that $\deg(A_i(x)) \leq q - 3i$. Now by Lemma 4.6(3) we have a relation of type (cf. [35, Prop. 2.1]):

$$y^{q^2} - y = (x^{q^2} - x)Dy + (x^{q^2} - x)^2 D^2 y + (x^{q^2} - x)^3 D^3 y \tag{4.2}$$

Claim 4.8. (1) $A_i(x) = 0$ for i not a power of 3, $i \geq 2$;
(2) $A_{3^j}(x) \in \mathbf{F}_{q^2}$ for $j = 0, 1, \ldots, t-2$.

Proof. First we show that $A_i(x) = 0$ if $i \geq 2$ and $i \not\equiv 0 \pmod 3$. To do that, let apply D to Eq. 4.1; so

$$0 = x^q + \sum_{i=0}^{q/3-1} DA_i(x)y^i + (\sum_{i=1}^{q/3-1} A_i(x)iy^{i-1})Dy\,.$$

Suppose that $A_i(x) \neq 0$ for some $i \geq 2$, $i \not\equiv 0 \pmod 3$. Then, as

$$v(\sum_{i=1}^{q/3-1} A_i(x)iy^{i-1}Dy) < v(x^q)\,,$$

by Cor. 4.7, we must have that

$$v(\sum_{i=1}^{q/3-1} A_i(x)iy^{q-1}Dy) = v(\sum_{i=0}^{q/3-1} DA_i(x)y^i)\,,$$

so that there exists integers $2 \leq i_0 \leq q/3 - 1$, $i_0 \not\equiv 0 \pmod 3$ and $1 \leq j_0 \leq q/3 - 1$ such that $v(A_{i_0}(x)y^{i_0-1} = v(DA_{j_0}(x)y^{j_0})$ and then $-q/3(deg(DA_{j_0} - deg(A_{i_0}) = -(q+1)(i_0 - 1 - j_0) - q^2/3$ and it gives us a contradiction.

Then Eq. 4.1 is reduced to

$$x^{q+1} + ay^{q/3} + A_0(x) + a_1(x)y + \sum_{i=1}^{q/9-1} A_{3i}(x)y^{3i} = 0\,. \tag{4.3}$$

Now we can conclude that $A_1 \in \mathbf{F}_{q^2}$. Indeed, applying D to Eq. 4.3 we have that $0 = x^q + DA_0(x) + D(A_1(x)y) + \sum_{i=1}^{q/9-1} DA_{3i}(x)y^{3i}$, and then from Cor 4.7 the claim follows.

Next we show that $A_{3i}(x) = 0$ for $i \geq 2$ and $i \not\equiv 0 \pmod 3$. In order to do that we need to compute $v(D^3y)$. From Eq. 4.2 we have that $v(D^2y - (x^{q^2} - x)D^3y) = -q^3/3 - q^2$. Then it is enough to show that $v(D^2y) > -q^3/3 - q^2$. This follows by applying D^2 to Eq. 4.3 and comparing valuations. Thus $v(D^3y) = -q^2$.

Finally, we use induction via D^{3^i} applied to Eq. 4.3 ($i = 1, \ldots,\ t-2$) together with properties of the valuation v. □

Thus Eq. 4.1 becomes

$$ay^{q/3}+x^{q+1}+A_0(x)+\sum_{i=0}^{t-2}A_{3^i}y^{3^i}=0\,,$$

with each $A_i\in\mathbf{F}_{q^2}$. Notice that $A_1\neq 0$ since the extension $\bar{\mathbf{F}}_{q^2}(x,y)|\bar{\mathbf{F}}_{q^2}(x)$ is separable. Finally the proof of Theorem 4.1 follows from [2, Sect. 5]; here we just point out the main ideas from that reference for the case $p=3$:

(i) By using the orders of the linear series $\mathcal{D}$ (Lemma 4.6), we have that

$$A_0(x)=b_0+b_1x+b_2x^2+\sum_{i=1}^{t-1}b_{3^i}x^{3^i}+\sum_{i=1}^{t-1}b_{23^i}x^{23^i}\,.$$

(ii) From the previous item and Eq. 4.2 we find that

$$b_{i3^j}=a_jb_i^{3^j}\,,\qquad i=1,2; j=1,\ldots,t-1\,.$$

Similarly, $A_j=A_1^{(3^{t-j}-1)/2}$.

(iii) Next the polynomial $A_0(x)$ can be reduced to an additive polynomial: $A_0(x)=\sum_{i=0}^{t-1}b_{3^i}x^{3^i}+b_0$ since $b_2=0$ which follows from the previous item.

(iv) Finally, the previous reduction on $A_0(x)$ and the relations for its coefficients in Item (ii) implies the theorem via a $\mathbf{F}_{q^2}$-change of coordinates, namely $x\mapsto dx$, $y\mapsto y+b_1x+e$, where $d^{q+1}=c$ with c such that $c^2=A_1$, and where e is a solution of the equation in Z: $\sum_{i=0}^{t-1}A_iZ^{3^i}=b_0$.

References

[1] M. Abdón, "On maximal curves in characteristic two", Ph.D. dissertation, Série F-121/2000, IMPA, Rio de Janeiro, Brazil, 2000.

[2] M. Abdón and A. Garcia, "On a characterization of certain maximal curves" (provisory title), work in progress.

[3] M. Abdón, H. Stichtenoth and F. Torres, *On maximal curves and Artin Schreier extensions* (provisory title), work in progress.

[4] M. Abdón and F. Torres, *On maximal curves in characteristic two*, Manuscripta Math. **99** (1999), 39–53.

[5] R.D.M. Accola, *On Castelnuovo's inequality for algebraic curves, I*, Trans. Amer. Math. Soc. **251** (1979), 357–373.

[6] E. Arbarello, M. Cornalba, P.A. Griffiths, and J. Harris, "Geometry of Algebraic Curves," Vol. I, Springer-Verlag, New-York, 1985.

[7] E. Ballico, *Space curves not contained in low degree surfaces in positive characteristic*, Preprint May 2000.

[8] G. Castelnuovo, *Ricerche di geometria sulle curve algebriche*, Atti. R. Acad. Sci. Torino **24** (1889), 196–223.

[9] A. Cossidente, J.W.P. Hirschfeld, G. Korchmáros and F. Torres, *On plane maximal curves*, Compositio Math. **121** (2000), 163–181.

[10] A. Cossidente, G. Korchmáros and F. Torres, *On curves covered by the Hermitian curve*, J. Algebra **216** (1999), 56–76.

[11] A. Cossidente, G. Korchmáros and F. Torres, *Curves of large genus covered by the Hermitian curve*, Comm. Algebra **28**(10) (2000), 4707–4728.

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

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

[14] R. Fuhrmann and F. Torres, *On Weierstrass points and optimal curves*, Rend. Circ. Mat. Palermo Suppl. **51** (1998), 25–46.

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

[16] A. Garcia and F. Torres, *On maximal curves having classical Weierstrass gaps*, Contemp. Math. **245** Amer. Math. Soc. (1999), 49–59.

[17] G. van der Geer and M. van der Vlugt, How to construct curves over finite fields with many points, *Arithmetic Geometry* (Cortona 1994), F. Catanese Ed., Cambridge Univ. Press, Cambridge, 169–189, 1997.

[18] V.D. Goppa, "Geometry and codes", Mathematics and its applications, Vol. 24. Kluwer Academic Publisher, Dordrechet-Boston-London, 1988.

[19] J. Harris, *The genus of space curves*, Math. Ann. **249** (1980), 191–204.

[20] R. Hartshorne, "Algebraic Geometry", Grad. Texts in Math., Vol. 52, Springer-Verlag, New York-Berlin, 1977.

[21] A. Hefez, *Non classical curves*, Atas 16 Coloquio Bras. de Matem. (1988), 33–37.

[22] A. Hefez, *Non-reflexive curves*, Compositio Math. **69** (1989), 3–35.

[23] A. Hefez and S. Kleiman, Notes on the duality of project varieties, "Geometry Today", 143–183, Birkhäuser, 1985.

[24] M. Homma, *Reflexivity of tangent varieties associated with a curve*, Ann. Mat. Pura Appl. (4) **156** (1990), 195–210.

[25] M. Homma, *Duality of spaces and their tangent surfaces in characteristic $p > 0$*, Ark. Math. **28**(2) (1991), 221–235.

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

[27] T. Kato, *On Weierstrass points whose first non-gaps are three*, J. Reine Angew. Math. **316** (1979), 99–109.

[28] G. Korchmáros and F. Torres, *Embedding of a maximal curve in a Hermitian variety*, Composition Math., to appear.

[29] G. Korchmáros and F. Torres, *On the genus of a maximal curve*, arXiv: math.AG/000802.

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

[31] J. Rathmann, *The uniform position principle for curves in characteristic p*, Math. Ann. **276** (1987), 565–579.

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

[33] H. Stichtenoth, "Algebraic function fields and codes", Springer-Verlag, Berlin, 1993.

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

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

[36] J.F. Voloch, *Surfaces in $\mathbf{P}^3$ over finite fields*, preprint available at the location http://www.ma.utexas.edu/users/voloch.

Instituto de Matemática (GAN) - UFF, Rua Mário Santos Braga, s/n, Campus do Valonguinho, Niteroi, 24.020-140-RJ, Brazil

E-mail address: miriam@mat.uff.br

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

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

Current Address: Departamento de Matemática, Universidad de Valladolid, Spain