Beiträge zur Algebra und Geometrie
Contributions to Algebra and Geometry
Volume 46 (2005), No. 1, 241-260.

On $\mathbf{F}_{q^2}$-maximal Curves of Genus $\frac{1}{6}(q-3)q$

Miriam Abdón **Fernando Torres***

Dep. Matemática, PUC-Rio
Marquês de S. Vicente 225, 22453-900, Rio de Janeiro, RJ, Brazil
e-mail: miriam@mat.puc-rio.br

IMECC-UNICAMP, Cx. P. 6065, Campinas, 13083-970-SP, Brazil
e-mail: ftorres@ime.unicamp.br

Abstract. We show that an $\mathbf{F}_{q^2}$-maximal curve of genus $\frac{1}{6}(q-3)q>0$ is either a non-reflexive space curve of degree $q+1$ whose tangent surface is also non-reflexive, or it is uniquely determined, up to isomorphism, by a plane model of Artin-Schreier type whenever $q \geq 27$.

MSC 2000: 11G20 (primary), 14G05, 14G10 (secondary)
Keywords: Finite field, maximal curve, non-reflexive variety, Artin-Schreier extension, additive polynomial

1. Introduction

Throughout, let $K=\mathbf{F}_{q^2}$ be the finite field of order q^2 where q is a power of a prime number, and $\bar{K}$ its algebraic closure. A projective, geometrically irreducible, non-singular algebraic curve defined over K (or simply, a curve over K) of genus $g>0$ is called *K-maximal*, if its number of K-rational points attains the Hasse-Weil upper bound

$$q^2+1+2qg.$$

Maximal curves are known to be very useful in coding theory [16], [37], correlations of shift register sequences [31], exponential sums [32], and finite geometry [24]. They have been

*The authors were partially supported respectively by FAPERJ and PRONEX-Cnpq (Brazil), and by Cnpq-Brazil (Proc. 300681/97-6)

intensively studied by several authors, and the following papers contain background and expository accounts: [36], [40], [15], [11], [10], [12], [7], [14], [28], [29].

The subject of this article is related with the following questions.

(I) Which are the positive integers that belong to the set

$$\mathbf{M} = \mathbf{M}(q^2) := \{g \in \mathbf{N} : g \text{ is the genus of a } K\text{-maximal curve}\}?$$

(II) For each $g \in \mathbf{M}$, how many non-isomorphic K-maximal curves of genus g do exist?

(III) For a K-maximal curve in a class of curves obtained from (II), write down an explicit plane model.

Ihara [27] pointed out that the number of rational points of a curve whose genus is bigger than the order of the base (finite) field cannot attain the Hasse-Weil upper bound. In particular, for $g \in \mathbf{M}$ (see Subsection 2.1):

$$g \le g_1 := \frac{1}{2}(q-1)q.$$

The following curve over K, which is the celebrated Hermitian curve, is a K-maximal curve of genus g_1

$$\mathcal{H}: \quad Y^qZ + YZ^q = X^{q+1}. \tag{1.1}$$

Rück and Stichtenoth [36] showed that this curve is the unique K-maximal curve, up to isomorphism, of genus g_1. Thus $g_1 \in \mathbf{M}$ and in this case the answer to both questions (II) and (III) are settled.

By a result of Serre, stated and proved in Lachaud's paper [30, Proposition 6], any curve covered by a K-maximal curve is also K-maximal. Thus a sufficient condition for a curve to be K-maximal is to be a quotient curve of $\mathcal{H}$ with respect to a subgroup of the automorphism group $PGU(3, K)$ of $\mathcal{H}$. In [13], [8], [9] genera of many quotient curves of $\mathcal{H}$ were computed and in several cases plane models were given. As noted in [7, Section 4], [1] two such curves may not be K-isomorphic even if they have the same genus, and hence the same number of K-rational points. This shows that it is hard to deal with the questions stated above; nevertheless, there exist further necessary conditions for $g \in \mathbf{M}$.

Let $g \in \mathbf{M}$, $g < g_1$; then from [40], [11],

$$g \le g_2 := \left\lfloor \frac{1}{4}(q-1)^2 \right\rfloor.$$

We have that $g_2 \in \mathbf{M}$ and it is only attained, up to isomorphism, by the non-singular model over K of the following plane curves (see [10], [2], [29]).

- $y^q + y = x^{\frac{1}{2}(q+1)}$, for $q > 1$ odd;
- $\sum_{i=0}^{t-1} y^{2^i} = x^{q+1}$, for $q = 2^t > 2$.

In particular, for $g = g_2$ the answer to both questions (II) and (III) stated above are determined. Now if $g \in \mathbf{M}$, $g < g_2$, then by [29]

$$g \le g_3 := \left\lfloor \frac{1}{6}(q^2 - q + 4) \right\rfloor.$$

It turns out that $g_3 \in \mathbf{M}$ since this number is realized by the non-singular model over K of the following plane curves (see [13], [8], [9, Theorem 2.1]).

- $y^{q+1} + x^{\frac{1}{3}(q+1)} + x^{\frac{2}{3}(q+1)} = 0$, for $q \equiv 2 \pmod 3$;
- $y^q - yx^{\frac{2}{3}(q-1)} + ax^{\frac{1}{3}(q-1)} = 0$, for $q \equiv 1 \pmod 3$, $q > 1$, and where $a \in K$ such that $a^{q-1} = -1$;
- $y^q + y + (\sum_{i=0}^{t-1} x^{3^i})^2 = 0$, for $q = 3^t > 1$.

In this case ($g = g_3$) the answer to question (II) is not known. By contrast, the fourth largest genus $g_4 \in \mathbf{M}$ might heavily depend on q. For example, let $g \in \mathbf{N}$ such that

$$\left\lfloor \frac{1}{6}(q-2)(q-1) \right\rfloor \leq g < g_3;$$

then in that interval only three values of $g \in \mathbf{M}$ are known to exist, namely:

(A) If $q \equiv 2 \pmod 3$, $q > 2$, there exists a K-maximal curve of genus $g_3 - 1$ (see [13], [9]) and thus $g_4 = g_3 - 1$; a plane model of such a curve can be found in [9]. Here the answer to question (II) is also open;

(B) If $q \equiv 2 \pmod 3$ and $q \geq 11$, then $\tilde{g} := \frac{1}{6}(q-2)(q-1) \in \mathbf{M}$ and the non-singular model over K of the plane curve $y^q + y = x^{\frac{1}{3}(q+1)}$ is the unique maximal curve, up to isomorphism, whose genus is $\tilde{g}$ (see [29]). Thus in this case all the questions above have been answered.

(C) If $q = 3^t > 3$, there exists a K-maximal curve of genus $g = \frac{1}{6}(q-3)q$, namely the non-singular model $\mathcal{X}$ over K of the plane curve $\mathcal{C} = \mathcal{C}_a$ defined by

$$\sum_{i=0}^{t-1} y^{3^i} = ax^{q+1}, \quad \text{with } a \in K \text{ such that } a^{q-1} = -1\,. \tag{1.2}$$

Let $a, b \in K$ such that $a^{q-1} = b^{q-1} = -1$; then the plane curves $\mathcal{C}_a$ and $\mathcal{C}_b$ are birational equivalent over K by means of the map $(x, y) \mapsto (\alpha x, y)$ with $\alpha^{q+1} = \frac{a}{b}$. Therefore the non-singular model $\mathcal{X}$ does not depend on the parameter a.

We also point out the following.

(D) If $q \equiv 1 \pmod 3$ and $q \geq 13$, then $g := \frac{1}{6}(q-2)(q-1) \notin \mathbf{M}$, see [29].

It is worthwhile to remark that each K-maximal curve mentioned above, is a quotient of the Hermitian curve $\mathcal{H}$ by a certain subgroup of $PGU(3, q^2)$ (see the respective reference quoted so far). At present, there is not known the existence of a K-maximal curve not covered by $\mathcal{H}$ (see Remark 4.2).

In this paper we are concerned about question (II) for the number $g = \frac{1}{6}(q-3)q > 0$ which, as we already pointed out, belongs to the set $\mathbf{M}$. Our main result is the following.

Theorem 1. *Let $\mathcal{X}$ be a K-maximal curve of genus $g = \frac{1}{6}(q-3)q > 0$. Then*

(1) *either $\mathcal{X}$ is a non-reflexive space curve of degree $q+1$ whose tangent surface is also non-reflexive, or*

(2) *$\mathcal{X}$ is the non-singular model over K of the plane curve defined by equation* (1.2) *whenever $q \geq 27$.*

Unfortunately this result is not satisfactory in the sense that we do not know of any example of a maximal curve satisfying assertion (1) and if so, how many non-isomorphic classes of such curves might exist? Nevertheless, its theoretical meaning provides some further connection between curves having many rational points with those having quite pathological behavior; cf. [23]. We remark that a similar result in characteristic two has been proved in [2] which then was improved in [29].

The first step to prove the theorem is to show that the curve $\mathcal{X}$ is embedded either in $\mathbf{P}^3(\bar{K})$, or in $\mathbf{P}^4(\bar{K})$ as a curve of degree $q+1$; see Lemma 3.1. This geometrical property for the former case, implies that both the curve and its tangent surfaces must be non-reflexive varieties by results of Homma [26] and Hefez-Kakuta [21]; we consider and survey this possibility in Section 4. In the later case, the curve is extremal in the sense of Subsection 2.4, and so a remarkable observation due to Accola [3] allows us the use of arithmetical properties of the Weierstrass semigroup at a certain point of the curve. In particular, we find that $\mathcal{X}$ admits a plane model over K defined by equation (5.1) and the proof of assertion (2) in the theorem is completed after we show that the plane curves in (5.1) and (1.2) are birational equivalent over K: this is done in Section 5.

The geometrical facts used in this paper, which are summarized in Section 2, are based on some properties of maximal curves from [10], [28], [29]; Stöhr-Voloch's paper [38] (which has to do with a geometric approach to the Hasse-Weil bound); Castelnuovo's genus bound [6] which can be extended to positive characteristic by Hartshorne [18, V, Theorem 6.4] and Rathmann results [35]; the extremely interesting Accola's paper [3] whose results are also valid in positive characteristic due to the aforementioned references. In Section 3 we state some specific results concerning K-maximal curves of genus $\frac{1}{6}(q-3)q$.

2. Background

2.1. Maximal curves

For a K-maximal curve $\mathcal{X}$ of genus $g>0$, the roots of $h(T) := T^{2g}L(T^{-1}) = (T+q)^{2g}$ are all equal to $-q$, where $L(T)$ is the enumerator of the Zeta function of $\mathcal{X}$ over K (see eg. [37, V.1]). It follows that (loc. cite)

$$q^2+1+2qg = \#\mathcal{X}(K) \le \#\mathcal{X}(\mathbf{F}_{q^4}) = q^4+1-2q^2g,$$

and whence we obtain the bound g_1 mentioned in the introduction. Furthermore, the polynomial $h(T)$ is the characteristic polynomial of the Frobenius morphism $\tilde{\Phi}$ over K on the Jacobian $\mathcal{J}$ of $\mathcal{X}$, which is induced by the Frobenius morphism Φ on $\mathcal{X}$. The morphism $\tilde{\Phi}$ is semi-simple (see [33]) and thus $\tilde{\Phi}+qI=0$ on $\mathcal{J}$. We can state this property by using divisors on $\mathcal{X}$; to do that we use the fact that $f\circ\Phi = \tilde{\Phi}\circ f$, where $f(P)=[P-P_0]$ is the natural morphism that sends P_0 to $0\in\mathcal{J}$ with P_0 being a K-rational point of $\mathcal{X}$. Therefore the following linear equivalence of divisors on $\mathcal{X}$ arises:

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

This equivalence allows us to investigate thoroughly arithmetical and geometrical properties of maximal curves by studying the complete liner series of degree $q+1$ on $\mathcal{X}$:

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

(see [29] and the references therein). The linear equivalence (2.1) implies that the definition of $\mathcal{D}$ is independent of the selection of the K-rational point P_0, and as well that $q+1$ belongs to the Weierstrass semigroup $H(P)$ at any K-rational point P. In particular, $\mathcal{D}$ is base-point-free.

2.2. Stöhr-Voloch theory

In this subsection, we consider some results of Stöhr-Voloch's paper [38] that have to do with Weierstrass points and Frobenius orders of linear series. Although these results can be stated for arbitrary linear series, we restrict ourselves to the case of the linear series $\mathcal{D}$ defined above.

Let N denote the (projective) dimension of $\mathcal{D}$, and for $P \in \mathcal{X}$ let $(n_i(P) : i = 0, 1, \dots)$ denote the strictly increasing sequence that enumerates the Weierstrass semigroup $H(P)$ at P. The linear equivalence (2.1) implies $N \geq 2$ and

$$0 = n_0(P) < n_1(P) < \cdots < n_{N-1}(P) \leq q < q+1 \leq n_N(P). \tag{2.2}$$

We already noticed that $n_N(P) = q+1$ if $P \in \mathcal{X}(K)$. From (2.1), one can easily deduce that $n_{N-1}(P) = q\ (*)$ provided that $P \in \mathcal{X} \setminus \mathcal{X}(\mathbf{F}_{q^4})$; the study of property $(*)$ for the remaining points is a non-trivial problem and indeed it is related with the very ampleness property of $\mathcal{D}$ (see Lemma 2.2 below).

For $P \in \mathcal{X}$ and i a non-negative integer, we introduce certain sub-sets of $\mathcal{D}$ that provide with geometric information about the curve $\mathcal{X}$. Let $\mathcal{D}_i = \mathcal{D}_i(P) := \{D \in \mathcal{D} : v_P(D) \geq i\}$ (here $D = \sum_P v_P(D)P$). Since $\deg(\mathcal{D}) = q+1$,

$$\mathcal{D} \supseteq \mathcal{D}_0 \supseteq \mathcal{D}_1 \supseteq \cdots \supseteq \mathcal{D}_q \supseteq \mathcal{D}_{q+1}.$$

We have that each $\mathcal{D}_i$ is a sub-linear series of $\mathcal{D}$, and the codimension of $\mathcal{D}_{i+1}$ in $\mathcal{D}_i$ is at most one. If $\mathcal{D}_i \supsetneq \mathcal{D}_{i+1}$, i is called a *$(\mathcal{D}, P)$-order*; thus by elementary Linear Algebra we have a sequence of $(N+1)$ $(\mathcal{D}, P)$-orders. This sequence will be denoted by $j_0 < j_1 < \cdots < j_N$, $(j_i = j_i(P))$; notice that $j_0 = 0$ as $\mathcal{D}$ is base-point-free. In addition, there is just one hyperplane $H_P \subseteq \mathbf{P}^N(\bar{K})$, say defined by $\sum_0^N a_i X_i = 0$, such that $\mathrm{div}(\sum_0^N a_i f_i) + (q+1)P_0 \in \mathcal{D}_{q+1}$ where $\pi = (f_0 : f_1 : \cdots : f_N)$ is a morphism associated to $\mathcal{D}$. The hyperplane H_P is the so-called *osculating hyperplane* at P. The left hand-side of the equation that defines the hyperplane is in fact the determinant $L = L(X_0, X_1, \dots, X_N)$ of the matrix whose rows are

$$(X_0, X_1, \dots, X_N)\,, \quad (D_t^{j_i} f_0(P), D_t^{j_i} f_1(P), \dots, D_t^{j_i} f_N(P))\,, \quad i = 0, 1, \dots, N-1, \tag{2.3}$$

(see [38, Corollary 1.3]). Here t is a local parameter at P and $D_t^{j_i}$'s are the Hasse derivatives on $\bar{K}(\mathcal{X})$ of order j_i with respect to t; see [20] for general properties on these operators. In the present work we only need Property 5.3 below.

It is a fundamental result the fact that the sequence of $(\mathcal{D}, P)$-orders is the same for all but finitely many points P [38, Theorem 1.5]. This constant sequence is called the *order sequence* of $\mathcal{D}$. It will be denoted by $0 = \epsilon_0 < \epsilon_1 < \cdots < \epsilon_N$. The finitely many points P, where exceptional $(\mathcal{D}, P)$-orders occur, are called the *$\mathcal{D}$-Weierstrass points.* There exists a divisor R, the *ramification divisor* of $\mathcal{D}$, whose support is exactly the set of $\mathcal{D}$-Weierstrass points:

$$R := \operatorname{div}(\det(D_t^{\epsilon_i} f_j)) + \operatorname{div}(dt)\sum_{i=0}^{N}\epsilon_i + (N+1)(q+1)P_0.$$

In particular, the number of $\mathcal{D}$-Weierstrass points (counted with multiplicity) is

$$\deg(R) = \sum_{i=0}^{N}\epsilon_i(2g-2) + (N+1)(q+1).$$

Associated to $\mathcal{D}$ we also have a divisor S, the so-called *Frobenius divisor over* K, which in some sense is closer related to the set of K-rational points of the curve. Let us assume that each coordinate f_i of π belongs to $K(\mathcal{X})$ (this can be done so since $\mathcal{X}$ is defined over K).

By (2.1), $\Phi(P) \in H_P$ for any point $P \in \mathcal{X}$; thus from (2.3), $L(\Phi(P)) = 0$ and so $L \circ \Phi = 0$. This suggests to study the following rational functions; for the sequence of non-negative integers $0 \le \nu_0 < \nu_1 < \cdots < \nu_{N-1}$, let $\tilde{L}$ be the determinant of the matrix whose rows are:

$$(f_0^{q^2}, f_1^{q^2}, \ldots, f_N^{q^2}), \quad (D_t^{\nu_i} f_0, D_t^{\nu_i} f_1, \ldots, D_t^{\nu_i} f_N), \quad i = 0, 1, \ldots, N-1. \tag{2.4}$$

There exist some sequences $\nu_0 < \nu_1 < \cdots < \nu_{N-1}$ such that $\tilde{L} \ne 0$ on $\mathcal{X}$. The minimal of such sequences with respect to the lexicographic order is called the *Frobenius order sequence over* K of the curve; as a matter of fact, such a sequence is a subsequence of the order sequence of $\mathcal{D}$ [38, Proposition 2.1]. There is a divisor associated to the Frobenius order sequence over K which is analogue to the ramification divisor, namely

$$S := \operatorname{div}(\tilde{L}) + \operatorname{div}(dt)\sum_{i=0}^{N-1}\nu_i + (q^2+N)(q+1)P_0;$$

we have that

$$\deg(S) = \sum_{i=0}^{N-1}\nu_i(2g-2) + (q^2+N)(q+1).$$

Properties concerning the divisors R and S (associated to $\mathcal{D}$) that play a role in the present work are collected below.

Lemma 2.1. (1) ([38, Proposition 1.4]) *$j_i(P) \ge \epsilon_i$ for each i and each $P \in \mathcal{X}$.*

(2) ([38, Theorem 1.5]) *$v_P(R) \ge \sum_{i=0}^{N}(j_i(P) - \epsilon_i)$, and the equality holds if and only if* $\det\left(\binom{j_i(P)}{\epsilon_j}\right) \not\equiv 0 \pmod p$.

(3) ([38, Corollary 2.6]) *$\nu_i \le j_{i+1}(P) - j_1(P)$ for each i and each $P \in \mathcal{X}(K)$.*

(4) ([38, Proposition 2.4]) *For $P \in \mathcal{X}(K)$, $v_P(S) \ge \sum_{i=0}^{N-1}(j_{i+1}(P) - \nu_i)$, and equality holds if and only if* $\det\left(\binom{j_{i+1}(P)}{\nu_j}\right) \not\equiv 0 \pmod p$. *For $P \notin \mathcal{X}(K)$, $v_P(S) \ge \sum_{i=0}^{N_1}(j_i(P) - \nu_i(P))$.*

(5) *From* (2.1), $\epsilon_N = \nu_{N-1} = q$.

(6) *From* (2.1), $j_N(P) = q+1$ *if* $P \in \mathcal{X}(K)$, *otherwise* $j_N(P) = q$.

(7) $j_1(P) = 1$ *for any* $P \in \mathcal{X}$: *if* $P \in \mathcal{X}(K)$ *the assertion follows from items* (3) *and* (6), *otherwise it follows from* (2.1). *In particular* $\epsilon_1 = 1$.

(8) ([10], [23, Theorem 1]) $N = 2$ *if and only if* $g = \frac{1}{2}(q-1)q$, *and* $\nu_1 = 1$ *if* $N \geq 3$.

(9) *If* $P \in \mathcal{X}(K)$, *from* (2.1) *and* (2.2) *the* $(\mathcal{D}, P)$*-orders are* $j_{N-i}(P) = n_N - n_i = q+1-n_i(P)$ $(i = 0, 1, \ldots, N)$; *in particular,* $n_{N-1}(P) = q$ *by item* (7). *For* P *non-rational, the elements* $n_{N-1}(P) - n_i(P)$, $(i = 0, \ldots, N-1,)$ *are* $(\mathcal{D}, P)$*-orders.*

We end this subsection mentioned the following key property of maximal curves.

Lemma 2.2. *For a* K*-maximal curve* $\mathcal{X}$, *the following statements hold.*

(1) ([28, Theorem 2.5]) *The linear series* $\mathcal{D}$ *is very ample; that is, every morphism* $\pi : \mathcal{X} \to \mathbf{P}^N(\bar{K})$ *associated to* $\mathcal{D}$ *is an embedding onto its image.*

(2) ([10, Proposition 1.9]) *Assertion* (1) *is equivalent to the fact that* $q \in H(P)$ *at any* $P \in \mathcal{X}$.

2.3. Castelnuovo's genus bound (for curves in projective spaces)

Let $\mathcal{X}$ be a curve of genus g and $\mathcal{E}$ a simple linear series on $\mathcal{X}$ meaning that $\mathcal{X}$ is birational to $\pi(\mathcal{X})$ for some morphism π associated to $\mathcal{E}$. Let d be the degree of $\mathcal{E}$ and r its (projective) dimension. Then the genus g is upper bounded by the so-called Castelnuovo's genus bound. We have that

$$g \leq c(d,r) := \frac{d-1-\epsilon}{2(r-1)}(d-r+\epsilon) \leq \begin{cases} \frac{(d-1-\frac{1}{2}(r-1))^2}{2(r-1)} & \text{if } r \text{ is odd,} \\ \frac{(d-1-\frac{1}{2}(r-1))^2-\frac{1}{4}}{2(r-1)} & \text{if } r \text{ is even,} \end{cases} \tag{2.5}$$

where ϵ is the unique integer such that $0 \leq \epsilon \leq r-2$ and $d-1 \equiv \epsilon \pmod{(r-1)}$. This result was known to be true in characteristic zero and proved first by Castelnuovo [6] (see also [4, p. 116]). As we already mentioned in the introduction, this result is also valid in positive characteristic by works of Hartshorne and Rathmann. We notice that one expects to obtain some information on the dimension r provided that g and d are known.

2.4. Extremal curves

We retain the setting and notation from the previous subsection. A curve $\mathcal{X}$ of genus g is called *extremal* (with respect to $\mathcal{E}$) if $g = c(d,r)$. The following result is implicitly contained in the proof of Castelnuovo's genus bound (2.5) taking into account the Riemann-Roch theorem. Our reference is Accola's paper [3, p. 351, Lemma 3.5] whose results are also valid in positive characteristic once again by Hartshorne's [18, Theorem 6.4] and Rathmann's [35, Corollary 2.8] works. Define the integer $\epsilon' \in \{2, \ldots, r\}$ by $d = m(r-1) + \epsilon'$.

Lemma 2.3. *Let* $\mathcal{X}$ *be an extremal curve with respect to the linear series* $\mathcal{E}$ *of degree* d *and dimension* r. *If* $m \geq 2$, *then*

(1) *the dimension of* $2\mathcal{E}$ *is* $3r-1$;

(2) *there exists a complete linear series* $\mathcal{E}'$ *of degree* $(\epsilon'-2)(m+1)$ *and dimension* $(\epsilon'-2)$ *such that* $(m-1)\mathcal{E} + \mathcal{E}'$ *is the canonical linear series on* $\mathcal{X}$.

3. K-maximal curves of genus $\frac{1}{6}(q-3)q$

Throughout, $\mathcal{X}$ denotes a K-maximal curve of genus $g = \frac{1}{6}(q-3)q > 0$. The results of this section have been summarized from the references [8] and [29]; we include the proofs for the sake of completeness. Let $\mathcal{D}$ be the linear series of degree $q+1$ and dimension N on $\mathcal{X}$ which was defined in Subsection 2.1.

Lemma 3.1. $N \in \{3, 4\}$.

Proof. The dimension N should be at least three by Lemma 2.1(8) and the hypothesis on g. By means of contradiction, suppose that $N \geq 5$. Then the Castelnuovo's genus bound (2.5) applied to $\mathcal{D}$ would imply

$$g = \frac{1}{6}(q-3)q \leq \frac{1}{8}(q-2)^2$$

so that $q \leq 3$, a contradiction. □

Next result takes into account basic facts for the case $N = 3$. Let $0 < 1 < j_2(P) < q+1$ be the $(\mathcal{D}, P)$-orders for $P \in \mathcal{X}(K)$, and $0 < 1 < \epsilon_2 < q$ (resp. $0 < 1 < q$) the order sequence (resp. Frobenius order sequence over K) of $\mathcal{D}$ (cf. Subsection 2.2).

Lemma 3.2. *If $N = 3$, the following statements hold.*

(1) $\epsilon_2 = 3$;
(2) $\dim(2\mathcal{D}) \geq 9$;
(3) *there exists a K-rational point P such that $n_1(P) = q-2$.*

Proof. (1) We claim that $\epsilon_2 \leq 3$, otherwise let S be the Frobenius divisor over K of $\mathcal{D}$; for $P \in \mathcal{X}(K)$ we have that $v_P(S) \geq 5$ by Lemma 2.1(4)(3)(1); thus

$$\deg(S) = (1+q)(2g-2) + (q^2+3)(q+1) \geq 5(q+1)^2(+5(2g-2).$$

It follows that $(q+1)(q^2-5q-2) \geq (2g-2)(4q-1)$; but $2g-2 = \frac{1}{3}(q^2-3q-6)$ and thus we would have $q^3 - q^2 - 12 \leq 0$ and so $q = 3$, a contradiction.

So far, we have shown that $\epsilon_2 \in \{2, 3\}$. Suppose that $\epsilon_2 = 2$. Let R be the ramification divisor of $\mathcal{D}$ and $P \in \mathcal{X}(K)$. Lemma 2.1(5)(6) gives $v_P(R) \geq 1$, and since $\deg(R) = (3+q)(2g-2) + 4(q+1)$ (cf. Subsection 2.2), the maximality of $\mathcal{X}$ gives

$$(3+q)(2g-2) + 4(q+1) \geq (q+1)^2 + q(2g-2)$$

so that $g \geq \frac{1}{6}(q^2-2q+3)$ and the result follows.
(2) In a similar way to the case $\mathcal{D}$, we can define the order sequence of the linear series $2\mathcal{D}$. We have that $\epsilon_i + \epsilon_j$ $(i, j = 0, 1, 2, 3)$ belong to the order sequence of $2\mathcal{D}$ and thus this sequence has at least nine elements, namely

$$0, 1, 2, 3, 4, 6, q, q+1, q+3, 2q.$$

(3) By Lemma 2.1(9) for any $P \in \mathcal{X}(K)$, the first non-negative Weierstrass non-gap at P satisfies $n_1(P) = q+1-j_2(P)$. We claim that $j_2(P) = 3$ for at least one K-rational point of

$\mathcal{X}$. Since $j_2(P) \geq \epsilon_2 = 3$ (see Lemma 2.1(1)), let us assume that $j_2(P) \geq 4$ for any K-rational point P. Then by Lemma 2.1(2) we would have

$$\deg(R) = (4+q)(2g-2) + 4(q+1) \geq 2(q+1)^2 + 2q(2g-2);$$

that is to say, $0 \geq (q-4)(2g-2) + (q+1)(2q-2) > 0$, a contradiction. □

Remark 3.3. Assertion (2) of the previous result will not be used in this paper. By applying Castelnuovo's genus bound to the linear series $2\mathcal{D}$, we have that $9 \leq \dim(2\mathcal{D}) \leq 11$.

Now we shall point out some results for the case $N = 4$. The first observation is that the curve is extremal with respect to $\mathcal{D}$. In fact, since $d-1 = q = 3(\frac{1}{3}q)$ and $r-1 = N-1 = 3$ it follows that $\epsilon = 0$, and hence $c(q+1, 4) = g = \frac{1}{6}(q-3)q$. For $P \in \mathcal{X}(K)$ and $P \in \mathcal{X} \setminus \mathcal{X}(K)$, let $0 < 1 < j_2 := j_2(P) < j_3 := j_3(P) < q+1$ and $0 < 1 < j_2 := j_2(P) < j_3 := j_3(P) < q$ be the $(\mathcal{D}, P)$-orders respectively. Let $0 < 1 < \epsilon_2 < \epsilon_3 < q$ and $0 < 1 < \nu_2 < q$ be the order sequence and the Frobenius order sequence over K of $\mathcal{D}$ respectively.

Lemma 3.4. *If $N = 4$, the following statements hold.*

(1) $\dim(2\mathcal{D}) = 11$;
(2) *there exists a complete linear series $\mathcal{D}'$ of degree $\frac{2}{3}q$ and dimension two such that $\frac{1}{3}(q-6)\mathcal{D} + \mathcal{D}'$ is the canonical linear series on $\mathcal{X}$;*
(3) *if $j_2 = 2$, then $j_3 = 3$;*
(4) *if $P \in \mathcal{X}(K)$ and $j_2 > 2$, then $j_2 = \frac{1}{3}(q+3)$, and $j_3 = \frac{1}{3}(2q+3)$. In particular, the Weierstrass semigroup at P is generated by $\frac{1}{3}q$ and $q+1$;*
(5) *if $q \geq 27$ and $P \notin \mathcal{X}(K)$, then $j_2 = 2$.*

Proof. (1)–(2) We already observed that $\mathcal{X}$ is an extremal curve with respect to $\mathcal{D}$; then assertions (1) and (2) follow from Lemma 2.3(1)(2) taking into account that $\epsilon' = 4$ and $m = \frac{1}{3}(q-1)$.
(3) Let $P \in \mathcal{X}(K)$. Then the following numbers are $(2\mathcal{D}, P)$-orders

$$0, 1, 2, 3, 4, j, j+1, j+2, 2j, q+1, q+2, q+3, q+j+1, 2q+2.$$

If $j > 4$, we would have the sequence $0 < 1 < 2 < 3 < 4 < j < j+1 < j+2 < q+3 < q+j+1 < 2q+2$ and whence $j = q$ by assertion (1). Therefore $n_1(P) = q+1-j_3$ (cf. Lemma 2.1(9)); that is $n_1(P) = 1$; this a contradiction since we have assumed that $g > 0$. If $j = 4$, then the following numbers would be $(2\mathcal{D}, P)$-orders:

$$0, 1, 2, 3, 4, 5, 6, 8, q+1, q+2, q+3, q+5, 2q+2;$$

which is again a contradiction by assertion (1). Now let $P \notin \mathcal{X}(K)$. Arguing as in the previous case we show that if $j \neq 4$, then $j = q-1$. Therefore the curve $\mathcal{X}$ is hyperelliptic by (2.1) so that

$$\#\mathcal{X}(K) = q^2 + 1 + 2qg \leq 2(q^2+1),$$

which gives $g \leq \frac{1}{2}(q-1)$, a contradiction.

(4) The elements of the following increasing sequence are $(2\mathcal{D}, P)$-orders:

$$0<1<2<j_2<j_3<j_3+1<q+1<q+2<q+1+j_2<q+1+j_3<2q+2.$$

(Here $j_3<q$, otherwise $n_1(P)=1$.) The numbers $j_2+1, 2j_2, j_2+j_3, 2j_3$ are also $(2\mathcal{D}, P)$-orders. (Notice that $j_2+1 \le j_3$.)

Case $j_2+1<j_3$. Hence in the above sequence we have 12 $(2\mathcal{D}, P)$-orders and by assertion (1), either $j_2+j_3=q+1$, or $j_2+j_3=q+2$; in particular, $2j_3=q+1+j_2$. In the former case, $2j_3=q+1+j_2$ and so $3j_2=q+1$, a contradiction; in the latter case, $j_3=2j_2-1$ so that $j_2=\frac{1}{3}(q+3)$ and $j_3=\frac{1}{3}(2q+3)/3$.

Case $j_2+1=j_3$. We show that this case cannot occur. If $q+2<j_2+j_3$, $2j_3=q+1+j_2$ which is not possible; if $q+2=j_2+j_3$ we would have that $\frac{1}{2}(q-1), \frac{1}{2}(q+1) \in H(P)$ by Lemma 2.1(9): thus $\frac{1}{2}(q-1), \frac{1}{2}(q+1), q-1, q, q+1 \in H(P)$ and so $N \ge 5$ by (2.2). Therefore, $j_2+j_3<q+2$. Since $j_2+j_3=q+1$ implies $2j_2=q$ and q is odd, in addition we have that $j_2+j_3<q+1$. Then $2j_2 \in \{j_3, j_3+1\}$ and hence $j_2 \le 2$, a contradiction.

Finally, $n_1(P)=\frac{1}{3}q \in H(P)$ by Lemma 2.1(9) so that $g=\#(\mathbf{N} \setminus H(P)) \le g_1 := \mathbf{N} \setminus H$, where H is the semigroup generated by $\frac{1}{3}q$ and $q+1$. By an elementary computation (see eg. [34]) it turns out that $g_1=g$, and so $H(P)=H$.

(5) By means of contradiction, suppose that there exists $P \notin \mathcal{X}(K)$ such that $j_2>2$. Arguing as in the proof of the previous assertion, we have to deal with the following two cases:

(5.1) Either $j_2=\frac{1}{3}q$ and $j_3=\frac{2}{3}q$, or

(5.2) $j_2=\frac{1}{2}(q-1)$ and $j_3=\frac{1}{2}(q+1)$.

In Case (5.1), $n_1 := n_1(P) \in \{\frac{2}{3}q, \frac{1}{3}q\}$ by Lemma 2.1(9); the $(\mathcal{D}, P)$-orders are $0<1<\frac{1}{3}q<\frac{2}{3}q<q$ and hence by assertion (1), the $(2\mathcal{D}, P)$-orders are $0<1<2<\frac{1}{3}q<\frac{1}{3}q+1<\frac{2}{3}q<\frac{2}{3}q+1<q<q+1<\frac{4}{3}q<\frac{5}{3}q<2q$. By applying Φ to (2.1) (cf. [18, IV, Example 26]), it turns out that these numbers are also the $(2\mathcal{D}, \Phi(P))$-orders. Now let $f \in \bar{K}(\mathcal{X})$ such that $\operatorname{div}(f-f(\Phi(P)))=D+e\Phi(P)-n_1P$, with $e \ge 1$ and $P, \Phi(P) \notin \operatorname{Supp}(D)$. If $n_1=\frac{2}{3}q$ (resp. $\frac{1}{3}q$), $3e+2$ (resp. $3e+1$) is a $(2\mathcal{D}, \Phi(P))$-order (resp. a $(\mathcal{D}, P)$-order) by (2.1). By the computations above concerning $(2\mathcal{D}, P)$-orders, we have a contradiction.

In Case (5.2), we apply assertion (2) and find that $2j_2+1 \notin H(P)$ whenever $2 \le \frac{1}{3}(q-6)$; that is, for $q \ge 27$. It follows then that $q \notin H(P)$ which is a contradiction according to Lemma 2.2. □

Corollary 3.5. *With the notation above,*

1. *for $q \ge 27$, there exists $P \in \mathcal{X}(K)$ such that $H(P)$ is generated by $\frac{1}{3}q$ and $q+1$;*
2. *let P be as in assertion (1), and $x \in K(\mathcal{X})$ such that $\operatorname{div}_\infty(x)=\frac{q}{3}P$. Then the morphism $x: \mathcal{X} \setminus \{P\} \to \mathbf{A}^1(\bar{K})$ is unramified, and $x^{-1}(\alpha) \subseteq \mathcal{X}(K)$ for any $\alpha \in K$;*
3. *the order sequence of $\mathcal{D}$ and the Frobenius order sequence over K of $\mathcal{D}$ are respectively $0,1,2,3,q$, and $0,1,2,q$.*

Proof. (1) By Lemma 3.4(4), it is enough to show that there exists $P \in \mathcal{X}(K)$ such that $j_2>2$. Suppose that $j_2=2$ for any $P \in \mathcal{X}(K)$. Then by Lemma 2.1(6) and Lemma

3.4(3)(5), the $(\mathcal{D}, P)$-orders at $P \in \mathcal{X}(K)$ and $P \notin \mathcal{X}(K)$ are respectively $0, 1, 2, 3, q+1$ and $0, 1, 2, 3, q$. Thus by Lemma 2.1(2) we would have

$$\deg(R) = (6+q)(2g-2) + 5(q+1) = \#\mathcal{X}(K) = (q+1)^2 + q(2g-2),$$

so that $2g-2 = \frac{1}{6}(q-4)(q+1)$; that is, $q^2 - 3q - 8 = 0$, a contradiction.

(2) For $\alpha \in K$, let $Q \in \mathcal{X}$ such that $x(Q) = \alpha$. Write $\operatorname{div}(x-\alpha) = eQ + D - \frac{q}{3}P$, $e \geq 1$, $P, Q \notin \operatorname{Supp}(D)$. We have to show that $e = 1$.

Case $Q \notin \mathcal{X}(K)$. From (2.1) follows that $0 < 1 \leq e < 2e < 3e \leq q$ are $(\mathcal{D}, Q)$-orders. If $e > 1$, $e = \frac{1}{3}q$ and so $qQ \sim qP$. We have then that $qQ + P \sim (q+1)P \sim qQ + \Phi(Q)$; that is to say, $P \sim \Phi(Q)$. Since $g > 0$, $P = \Phi(Q)$ which is a contradiction as Q is not rational.

Case $Q \in \mathcal{X}(K)$. Arguing as above we have that $0 < 1 \leq e < 2e < 3e < q+1$ are $(\mathcal{D}, Q)$-orders which clearly implies $e = 1$.

(3) From the proof above, we have that $0, 1, 2, 3$ belong to the $(\mathcal{D}, Q)$-orders at any point $Q \neq P$ of the curve. Then the result follows from Lemma 2.1(1)(3). □

Remark 3.6. For $q = 9$ we do not know whether or not there exists a K-rational point P such that $n_1 = 3$. The proof of this property for $q \geq 27$ is based on Lemma 3.4(5). The proof of this lemma does not work for $q = 9$; more precisely the case that we cannot eliminate is the existence of a point $P \notin \mathcal{X}(K)$ whose $(\mathcal{D}, P)$-orders are $0, 1, 4, 5, 9$, and such that $n_1 = 4$, $n_2 = 8$ and $n_3 = 9$. In this situation, $H(P)$ would contain the semigroup H generated by $4, 8, 9$, namely

$$\{0, 4, 8, 9, 12, 13, 16, 17, 18, 20, 21, 22, 24, 25, 26, 27, \ldots\}.$$

How can we compute $H(P) \setminus H$ (notice that $\mathbf{N} \setminus H(P) = g = 9$) ? The answer is obtained via Lemma 3.4(2): we have that there exists a complete linear series $\mathcal{E}$ of degree six and dimension two such that $\mathcal{D} + \mathcal{E}$ is the canonical linear series on $\mathcal{X}$. Then it is easy to see that $H(P) \setminus H = \{14, 19, 23\}$ since we have that $j + \ell + 1 \notin H(P)$ with j (resp. $\ell \leq 6$) being a $(\mathcal{D}, P)$-order (resp. a $(\mathcal{E}, P)$-order). The question is if a maximal curve of genus 9 defined over $\mathbf{F}_{81}$ with the property above might exist.

4. Genus $g = \frac{1}{6}(q-3)q$ with $N = 3$

Let $\mathcal{X}$ be a K-maximal curve of genus $g = \frac{1}{6}(q-3)q > 0$ with $N = 3$. By Lemmas 3.1(1) and 2.1(5) the orders of $\mathcal{D}$ are $0, 1, \epsilon_2 = 3, q$. What geometric phenomena does the invariant ϵ_2 reflect on $\mathcal{X}$? Several authors noticed that this invariant is related to the reflexivity or not of the curve $\mathcal{X}$ and its tangent surface $T(\mathcal{X})$ which is a property in the dual theory of curves. In our situation,

$$\text{both } \mathcal{X} \text{ and } T(\mathcal{X}) \text{ are non-reflexive varieties} \tag{4.1}$$

(which is in fact a geometric pathological behavior of a curve). In what follows we shall give an expository account concerning assertion (4.1). Background on dual theory of varieties can be found e.g. in [20], [22], [21], [25], [26], and [41].

Let us assume that $\mathcal{X} \subseteq \mathbf{P} := \mathbf{P}^3(\bar{K})$ (cf. Lemma 2.2) and denote by $\mathbf{P}^*$ the dual projective space of $\mathbf{P}$. The *conormal* variety $C(\mathcal{X})$ of $\mathcal{X}$ is the Zariski closure in $\mathbf{P} \times \mathbf{P}^*$ of the set

$$\{(P, H) \in (\mathcal{X}, \mathbf{P}^*) : I(P; \mathcal{X} \cdot H) > 1\},$$

where $I(P; \mathcal{X} \cdot H)$ denotes the intersection multiplicity of $\mathcal{X}$ and H at P. The dimension of this variety is $N - 1 = 2$ and we have two natural projections, namely $\pi : C(\mathcal{X}) \to \mathbf{P}$ and $\pi' : C(\mathcal{X}) \to \mathbf{P}^*$. The dual variety of $\mathcal{X}$ is the surface $\mathcal{X}' := \pi'(C(\mathcal{X}))$. The curve $\mathcal{X}$ is called *non-reflexive* if $C(\mathcal{X}) \neq C(\mathcal{X}')$ (here $C(\mathcal{X}')$ is defined in a similar way as in the case of a curve). We have that $\pi' : C(\mathcal{X}) \to \mathcal{X}'$ is a finite morphism; let i be the inseparable degree of this map. Hefez and Kakuta [21] (see also [19]) proved a generalization of the so called generic order of contact theorem of Hefez and Kleiman (see [22, Section 3.5]). In our case their result computes i as being the highest power of three that divides ϵ_2; that is to say, $i = 3$. Then for the aforementioned Hefez and Kleiman result, the inseparability of the morphism π' is equivalent to the non-reflexivity of $\mathcal{X}$.

Now let $T_P = T_P(\mathcal{X})$ denote the tangent line of $\mathcal{X}$ at P. The *tangent surface* $T(\mathcal{X})$ of $\mathcal{X}$ is the Zariski closure in $\mathbf{P}$ of the set $\cup_{P\in\mathcal{X}} T_P$. By using arithmetical properties of orders sequences, Homma [26, Proposition 1.2] (see also [19]) computed the orders sequences that space curves may have. In characteristic three we have four possibilities, namely either (i) $0, 1, 2, \tilde{q}$, or (ii) $0, 1, \tilde{q}, \tilde{q}+1$, or (iii) $0, 1, \tilde{q}, 2\tilde{q}$, or (iv) $0, 1, q', q'\tilde{q}$ (here q' and $\tilde{q}$ are powers of three). In our situation, case (iv) holds true with $q' = 3$ and $\tilde{q} = \frac{1}{3}q$. Homma also shows that each of these possibilities occur [26, p. 226]; however, his examples are all based on curves of genus zero. Then Homma's result Theorem 0.1 in [26](v) implies the non-reflexivity of the tangent surface $T(\mathcal{X})$ (as well of the curve $\mathcal{X}$).

It would be interesting to relate the maximality of $\mathcal{X}$ to the non-reflexivity of $T(\mathcal{X})$. For example a connection can be made by counting rational points; thus the matter is to find a tight upper bound for $\#T(\mathcal{X})(K)$. This could be done if one could extend Voloch's approach [39] concerning upper bounds on the number of rational points on surfaces over prime finite fields to surfaces defined in finite fields of arbitrary order. The generalized Voloch's result could also be used to establish insights on the existence of $\mathcal{X}$ as follows. Ballico [5] extended Harris' and Rathmanns results that have to do with space curves contained in surfaces of certain degree (see [17] and [35] respectively). For q large enough, Ballico's result implies that $\mathcal{X}$ is contained in a surface S of degree three or four. What numerical phenomena does the relation $\#\mathcal{X}(K) \leq \#S(K)$ reflect?

To finish this section, we point out a couple of remarks that might have to do with the existence of the curve $\mathcal{X}$.

Remark 4.1. (Related to Weierstrass semigroups) Let $P \in \mathcal{X}(K)$ such that $n_1(P) = q - 2$ (cf. Lemma 3.2(3)). Hence the Weierstrass semigroup at P, $H(P)$, contains the semigroup H generated by $q-2, q, q+1$, namely the semigroup

$$H = \{(q-2)i : i \in \mathbf{N}_0\} \cup_{i\in\mathbf{N}} \{(q-2)i + j : j = 2, \ldots, 3i\}.$$

We have that $\tilde{g} := \#(N \setminus H) = \frac{1}{6}(q^2 - q)$. Can we compute $H(P) \setminus H$? In order to do that we have to choose $\frac{1}{3}q$ elements from the set

$$\{qi - 2i + 1 : i = 1, \ldots, \frac{1}{3}q\} \cup_{i=1}^{\frac{1}{3}q-2} [(qi + i + 1, q(i+1) - 2i - 1] \cap \mathbf{N}.$$

Which geometrical or arithmetical phenomena do these computations give forth on the curve $\mathcal{X}$?

Remark 4.2. (Related with the existence of maximal curves covered by the Hermitian curve (1.1)). This remark shows that, under an additional hypothesis, the existence of a maximal curve $\mathcal{X}$ with $N=3$ of genus $g=\frac{1}{6}(q-3)q$ will provide us with a non-trivial example of a maximal curve. As we mention in the introduction, the existence of maximal curves not covered by the Hermitian curve is an open problem. Moreover, it is not known any example of a maximal curve which is covered by the Hermitian curve by a not Galois covering.

Suppose that the curve $\mathcal{X}$ is K-covered by the Hermitian curve, say via a covering π. We show that π cannot be Galois because of the hypothesis on N and g. If π were Galois from [9, Theorem 3.2] the degree of π has to be three; thus either $\mathcal{X}$ has a plane model as in (1.2) and thus $N=4$, or the genus of $\mathcal{X}$ would be $\frac{1}{6}(q-1)q$.

5. The genus $g=\frac{1}{6}(q-3)q$ with $N=4$

Throughout this section, $\mathcal{X}$ denotes a K-maximal curve of genus $g=\frac{1}{6}(q-3)q$, $q=3^t\geq 27$, with $N=\dim(\mathcal{D})=4$. We show that $\mathcal{X}$ is the non-singular model over K of a plane equation of type (1.2).

Let $P\in\mathcal{X}(K)$ be as in Corollary 3.5(1); that is to say, such that $H(P)$ is generated by $\frac{1}{3}q$ and $q+1$. We have that $\mathcal{D}=|(q+1)P|$ by (2.1). Let $x,y\in K(\mathcal{X})$ be such that $\mathrm{div}_\infty(x)=\frac{1}{3}qP$ and $\mathrm{div}_\infty(y)=(q+1)P$; then $\mathcal{D}$ is generated by the sections $1,x,x^2,x^3,y$. The Riemann-Roch space $\mathcal{L}(\frac{1}{3}q(q+1)P)$ is generated by the set

$$\{x^{q+1}\}\cup_{i=0}^{\frac{1}{3}q}\{x^jy^i : j=0,\dots,q-3i\},$$

which has $\frac{1}{6}(q^2+5q)+2$ elements. Now by the Riemann-Roch theorem, the K-dimension of $\mathcal{L}(\frac{1}{3}q(q+1)P)$ is $\frac{1}{6}(q^2+5q)+1$; on the other hand, $v(x^jy^i)\geq -\frac{1}{3}q(q+1)+1$ unless either $(j,i)=(q+1,0)$, or $(j,i)=(0,\frac{1}{3}q)$ (here v denotes the valuation at P) and therefore Property 5.1 below implies the following relation between the rational functions x and y:

$$x^{q+1}+\sum_{i=0}^{\frac{1}{3}q}A_i(x)y^i=0, \tag{5.1}$$

where each $A_i(x)\in K[x]$ with $\deg(A_i(x))\leq q-3i$, and $A_{\frac{1}{3}q}(x)=A_{\frac{1}{3}q}\in K^*$. Moreover, as $\gcd(\frac{1}{3}q,q+1)=1$, $K(\mathcal{X})=K(x,y)$ and thus equation (5.1) is in fact a plane model over K of $\mathcal{X}$.

Let $D^i:=D^i_x$ be the i-th Hasse derivative on $\bar{K}(\mathcal{X})$ with respect to the separating variable x (recall that $D^ix^j=\binom{j}{i}x^{j-i}$). In what follows we use the following properties on valuations and Hasse derivative operators (see e.g. [37, Lemma I.1.10] and [20, Lemma 3.11] respectively). Let $f_1,\dots,f_m\in\bar{K}(\mathcal{X})$.

Property 5.1.

If $f_1+\cdots+f_m=0$, then $\exists\, i\neq j$ such that $v(f_i)=v(f_j)=\min\{f_k : k=1,\dots,m\}$.

Property 5.2.

$$v(\sum_{i=1}^{m} f_i) = \min\{v(f_i) : i = 1, \dots , m\}, \textit{provided that } v(f_i) \neq v(f_j) \textit{ for } i \neq j.$$

Property 5.3.

For $f \in \bar{K}(\mathcal{X})$: $D^i f^{3^s} = (D^{\frac{i}{3^s}} f)^{3^s}$ if $3^s|i$, and $D^i f^{3^s} = 0$ otherwise.

Lemma 5.4. (1) $v(D^1 y) = -\frac{1}{3}q^2$.

(2) *Let $A_i(x)$ be as in* (5.1) *such that $A_i(x) \neq 0$; then either $i \equiv 0 \pmod 3$, or $i = 1$ and $A_1(x) = A_1 \in K^*$.*

(3) $v(D^3 y) = -q^2$.

Proof. (1) By Lemma 3.5(2), the morphism $x : \mathcal{X} \to \mathbf{P}^1(\bar{K})$ is totally ramified at P and unramified outside P; thus $\mathrm{div}(dx) = (2g-2)P$. Let t be a local parameter at P; then

$$v(D^1 y) = v(\frac{dy}{dt}) - v(\frac{dx}{dt}) = -q - 2 - (2g-2) = -\frac{1}{3}q^2.$$

(2) By applying D^1 to equation (5.1) we obtain:

$$x^q + F + GD^1 y = 0\,, \qquad \text{where}$$
$$F := \sum_{i=0}^{\frac{1}{3}q-1} y^i D^1 A_i(x)\,, \qquad G := \sum_{i=1}^{\frac{1}{3}q-1} i y^{i-1} A_i(x).$$

Let $i \in \{1, \dots , \frac{1}{3}(q-3)\}$ be such that $A_i(x) \neq 0$. Then $v(GD^1 y) < -\frac{1}{3}q^2$ whenever $i \not\equiv 0 \pmod 3$ and $i \geq 2$ (cf. assertion (1)). Thus from Properties 5.1 and 5.2, $v(F) = V(GD^1 y)$ $(*)$, and so there exist integers $0 \leq i_0 \leq \frac{1}{3}q - 1$, $1 \leq j_0 \leq \frac{1}{3}q - 1$ such that $v(y^{i_0} D^1 A_{i_0}(x)) = v(y^{j_0 - 1} A_{j_0}(x))$. Since $\gcd(\frac{1}{3}q, q+1) = 1$, this is not possible unless $i \equiv 0 \pmod 3$, or $i = 0$. Next we show that $A_1(x) \in K^*$. We have that $G = A_1(x)$ and that $(*)$ holds true provided that $v(G) > 0$; then the result follows.

(2) The Frobenius orders of $\mathcal{D}$ are $0, 1, 2, q$ by Corollary 3.5(3). Then the minimality of this sequence with respect to the lexicographic order implies the following relation between x and y:

$$y^{q^2} - y = (x^{q^2} - x)D^1 y + (x^{q^2} - x)^2 D^2 y + (x^{q^2} - x)^3 D^3 y\,. \tag{5.2}$$

Now from assertion (1) and Property 5.1, the above equation implies $v(D^2 y + (x^{q^2} - x)D^3 y) = -\frac{1}{3}q^3 - q^2$; so it is enough to show that

$$v(D^2 y) > -\frac{1}{3}q^3 - q^2\,. \tag{$**$}$$

By assertion (2), equation (5.1) can be written as:

$$x^{q+1} + A_1 y + \sum_{i=0}^{\frac{1}{9}q} A_{3i}(x) y^{3i} = 0.$$

Now apply D^2 to this equation; then by means of Property 5.3 we find that

$$D^2 A_0(x) + A_1 D^2 y + \sum_{i=1}^{\frac{1}{9}q} y^{3i} D^2 A_{3i}(x) = 0.$$

Then $(**)$ follows from Property 5.1 since $v(D^2 A_0(x)) \geq -\frac{1}{3}q^2 + \frac{2}{3}q$, and $v(\sum_{i=1}^{\frac{1}{9}q} y^{3i} D^2 A_{3i}(x)) \geq -\frac{5}{9}q^2 + \frac{1}{3}q$. □

Next we generalize Lemma 5.4(2).

Lemma 5.5. *With the notation above, let i, j be non-negative integers such that $i \geq 1$ and $3^j i \leq \frac{1}{3}q$. If $A_{3^j i}(x) \neq 0$, then either $i \equiv 0 \pmod 3$, or $i = 1$ and $A_{3^j}(x) = A_{3^j} \in K^*$.*

Proof. We apply induction on j. Lemma 5.4(2) takes care of the case $j = 0$. Inductive hypothesis reduces equation (5.1) to the equation:

$$x^{q+1} + A_0(x) + \sum_{k=0}^{j} A_{3^k} y^{3^k} + \sum_{k=1}^{\frac{q}{3^{j+2}}} A_{3^{j+1}k}(x) y^{3^{j+1}k} = 0.$$

By applying $D^{3^{j+1}}$ to this equation, taking into account that the $\mathcal{D}$-orders are $0, 1, 2, 3, q$ (cf. Corollary 3.5(3)), and by using Property 5.3 we obtain the following relation

$$A_{3^j}(D^3 y)^{3^j} + F + G(D^1 y)^{3^{j+1}} = 0\,, \qquad \text{where}$$

$$F := \sum_{k=0}^{\frac{q}{3^{j+2}}} y^{3^{j+1}k} D^{3^{j+1}} A_{3^{j+1}k}(x)\,, \qquad G := \sum_{k=1}^{\frac{q}{3^{j+2}}} k y^{3^{j+1}(k-1)} A_{3^{j+1}k}(x)\,.$$

Let $k \in \{1, \ldots, \frac{q}{3^{j+2}}\}$ be such that $A_{3^{j+1}k}(x) \neq 0$. Then Lemma 5.4(1)(3) implies $v(G(D^1 y)^{3^{j+1}}) < -q^2 3^j = v((D^3 y)^{3^j})$ whenever $k \geq 2$ and $k \not\equiv 0 \pmod 3$. Therefore from Property 5.1, $v(F) = v(G(D^1)^{3^{j+1}})\,(*)$; arguing as in the case $j = 0$ (see the proof of Lemma 5.4(2)) we find a contradiction unless $k = 1$ or $k \equiv 0 \pmod 3$. To show that $A_{3^{j+1}}(x) = A_{3^{j+1}} \in K^*$ notice that $(*)$ holds true whenever $v(G) < 0$; since $G = A_{3^{j+1}}(x)$, the result follows. □

Therefore Lemma 5.5 reduces equation (5.1) to the equation:

$$x^{q+1} + A_0(x) + \sum_{i=0}^{t-1} A_{3^i} y^{3^i} = 0\,, \tag{5.3}$$

where $A_0(x)$ is a polynomial in x of degree at most q, and each $A_{3^i} \in K^*$.

Set $A_0(x) := \sum_{i=0}^{q} a_i x^i$.

Lemma 5.6. *For an integer* $0 \le i \le t-1$,

(1) $a_i \neq 0$, *only if* $i=0$, *or* i *is a power or twice a power of* 3;

(2) $a_{2\cdot 3^i} = A_{3^i}\left(\frac{a_2}{A_1}\right)^{3^i}$.

Proof. (1) Let $4 \le j \le q-1$ be an integer; recall that $D^j y = 0$ (cf. Corollary 3.5(3)). Suppose that $3 \nmid j$; then by applying D^j to equation (5.3), $a_j = 0$ by Property 5.3. Suppose now that $3|j$ and write $j = 3^k\ell$ with $3 \nmid \ell$. Then $D^j y^{3^i} = (D^{\frac{3^k\ell}{3^i}} y)^{3^i} = 0$ for $k \ge i$ (cf. Property 5.3 again) and hence $a_j = 0$ for $\ell \ge 4$.
(2) By assertion (1), $A_0(x) = a_0 + \sum_{j=0}^{t-1} a_{3^j} x^{3^j} + \sum_{j=0}^{t-1} a_{2\cdot 3^j} x^{2\cdot 3^j}$. Let $i = 0, 1, \ldots, t-1$. By applying $D^{2\cdot 3^i}$ to equation (5.3), Property 5.3 implies that

$$D^{2\cdot 3^i} A_0(x) + A_{3^i}(D^2 y)^{3^i} = 0.$$

If $i = 0$, the definition of D^2 implies

$$D^2 y = -\frac{1}{A_1}\left(\sum_{j=0}^{q}\binom{j}{2} a_j x^{j-2}\right) = -\frac{a_2}{A_1}.$$

Let $i \ge 1$. Then $D^{2\cdot 3^i} A_0(x) = a_{2\cdot 3^i}$ and thus

$$a_{2\cdot 3^i} + A_{3^i}\left(-\frac{a_2}{A_1}\right)^{3^i} = 0.$$

□

This result reduces equation (5.3) to the following:

$$x^{q+1} + a_0 + \sum_{i=0}^{t} a_{3^i} x^{3^i} + \sum_{i=0}^{t-1} A_{3^i}\left(\frac{a_2}{A_1}x^2 + y\right)^{3^i},$$

and thus, by means of the change of coordinates $(x,y) \mapsto (x, \frac{a_2}{A_1}x^2 + y)$, the curve $\mathcal{X}$ admits a plane model over K given by

$$x^{q+1} + a_0 + \sum_{i=0}^{t} a_{3^i} x^{3^i} + \sum_{i=0}^{t-1} A_{3^i} y^{3^i} = 0\,. \tag{5.4}$$

We can assume $a_q = a_1 = a_0 = 0$. In fact, to obtain $a_q = 0$ we use the change of coordinates $(x,y) \mapsto (x - a_q, y)$; to obtain $a_1 = 0$ we use $(x,y) \mapsto (x, \frac{a}{A_1}x + y)$, where $a := a_q^q - a_1$; and to obtain $a_0 = 0$ we use $(x,y) \mapsto (x, y+\alpha)$, where $\alpha \in K$ such that $-\tilde{a} = \sum_0^{t-1} A_{3^i}\alpha^{3^i}$, with $\tilde{a} := a_0 - a_1 a_q - a_3 a_{q^3} - \cdots - a_{3^{t-1}} a_{q^{3^{t-1}}} + a_{q^{q+1}}$ (the existence of the element α is guaranteed by Corollary 3.5(2)).

Lemma 5.7. *For* $2 \le j \le t-1$ *an integer,*

(1) $A_{3^j} = \left(\frac{A_3}{A_1}\right)^{3^{j-1}} A_{3^{j-1}}$; *in particular,* $A_{3^j} = \left(\frac{A_3}{A_1^3}\right)^{\frac{1}{2}(3^j-1)} A_1^{3^j}$;

(2) $a_{3^j} = \left(\frac{a_3}{A_1}\right)^{3^{j-1}} A_{3^{j-1}}$.

Proof. In all the computations below we use the following facts: Property 5.3, equation (5.4) (with $a_1 = 0$), and that the orders of $\mathcal{D}$ are $0, 1, 2, 3, q$ (cf. Corollary 3.5(3)). We have $D^1 y = -\frac{1}{A_1} x^q$, and for $j = 1, \ldots, t-1$ (applying D^{3^j} to equation (5.4))

$$a_{3^j} + \sum_{i=0}^{j} A_{3^j} \left(D^{3^{j-i}} y\right)^{3^i} = 0\,, \qquad \text{that is}$$
$$a_{3^j} + A_{3^{j-1}} \left(D^3 y\right)^{3^{j-1}} + A_{3^j} (D^1 y)^{3^j} = 0\,.$$

The case $j=1$ gives $D^3 y = \frac{A_3}{A_1^4} x^{3q} - \frac{a_3}{A_1}$. Thus for $j \geq 2$ we find that

$$a_{3^j} + A_{3^{j-1}} \left(\frac{A_3}{A_1^4} x^{3q} - \frac{a_3}{A_1}\right)^{3^{j-1}} = A_{3^j} \left(\frac{1}{A_1} x^q\right)^{3^j}\,,$$

and the result follows by comparing coefficients. □

Corollary 5.8. *With the notation above,*

(1) $A_1^4 + A_3 (A_{\frac{1}{3}q})^3 q = 0$;

(2) $a_{3^j} = 0$ *for* $j = 1, \ldots, t-1$;

(3) $A_1^{q+3} + A_3 (A_{\frac{1}{3}q})^3 = 0$.

Proof. We have already seen that $D^1 y = -\frac{1}{A_1} x^q$ and $D^3 y = \frac{A_3}{A_1^4} x^{3q} - \frac{a_3}{A_1}$ (cf. proof of Lemma 5.7). By using these computations in equation (5.2), we have:

$$-(q+1)q^2 = v(y^{q^2} - y) = v((x^{q^2} - x^q)^3 (\frac{A_3}{A_1^4} x^{3q} - \frac{a_3}{A_1})) < v((x^{q^2} - x)\frac{x^q}{A_1})\,. \tag{5.5}$$

Now $v(y^{q^2}) = v(-\frac{x^{3q(q+1)}}{(A_{\frac{q}{3}})^{3q}})$ by equation (5.4); thus from (5.5) and Property 5.1 $-\frac{1}{(A_{\frac{1}{3}q})^{3q}} = \frac{A_3}{A_1^4}$.

(2) By Lemma 5.7(2), it is enough to show that $a_3 = 0$. Suppose that this is not the case; in particular, $a_{\frac{1}{3}q} \neq 0$ (loc. cite). Then if we rise equation (5.4) to the power $\frac{1}{3}q$, we can remove the terms of higher degree by assertion (1); we have then that the valuation at P of the left hand-side would be $v(a_{\frac{1}{3}q} x^{q^2}) = -\frac{1}{3}q^3$, while the valuation at P of the right hand-side, $v(x^{3q^2}) = -q^3$ which is a contradiction according to Property 5.1.

(3) Assertion (2) reduces equation (5.4) to the equation:

$$x^{q+1} + \sum_{i=0}^{t-1} A_{3^i} y^{3^i} = 0\,; \tag{5.6}$$

thus $D^2 y = 0$ (as follows from Property 5.3) and so equation (5.2) reads

$$y^{q^2} - y = (x^{q^2} - x) D^1 y + (x^{q^2} - x)^3 D^3 y\,.$$

After computing $x^{q^2}-x$ from equation (5.6) we replace it in the above equation and obtain an equality of polynomials in y. Looking at the coefficient of the monomial y^q, the result follows. $\square$

Now Lemma 5.7(1) makes it possible to re-write equation (5.6) as follows

$$x^{q+1}+\sum_{i=0}^{t-1}\left(\frac{A_3}{A_1^3}\right)^{\frac{1}{2}(3^i-1)}(A_1y)^{3^i}=0$$

and hence, by means of the change of coordinates $(x,y)\mapsto(x,-A_1y)$, the curve $\mathcal{X}$ admits the following plane model over K:

$$x^{q+1}=\sum_{i=0}^{t-1}\left(\frac{A_3}{A_1^3}\right)^{\frac{1}{2}(3^i-1)}y^{3^i}.$$

What can we say about the element $\frac{A_3}{A_1^3}\in K^*$? From Lemma 5.7(1) (with $j=t-1$) and Corollary 5.8(3), $\left(\frac{A_3}{A_1^3}\right)^{\frac{1}{2}(q-1)}=-1$ meaning that there exists $a\in K$ such that $\left(\frac{A_3}{A_1^3}\right)=a^2$ (notice that $a^{q-1}=-1$). Therefore by means of the change of coordinates $(x,y)\mapsto(x,ay)$ we conclude that the above equation is birational equivalent to the curve $\mathcal{C}$ in (1.2) and the proof of the theorem is complete.

References

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

[2] Abdón, M.; Torres, F.: *On maximal curves in characteristic two.* Manuscr. Math. **99** (1999), 39–53. Zbl 0931.11022

[3] Accola, R. D. M.: *On Castelnuovo's inequality for algebraic curves, I.* Trans. Am. Math. Soc. **251** (1979), 357–373. Zbl 0417.14021

[4] Arbarello, E.; Cornalba, M.; Griffiths, P. A.; Harris, J.: *Geometry of Algebraic Curves.* Vol. I, Springer-Verlag, New-York 1985. Zbl 0559.14017

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

[6] Castelnuovo, G.: *Ricerche di geometria sulle curve algebriche.* Atti. R. Acad. Sci. Torino **24** (1889), 346–373. JFM 21.0669.01

[7] Cossidente, A.; Hirschfeld, J. W. P.; Korchmáros, G.; Torres, F.: *On plane maximal curves.* Compos. Math. **121** (2000), 163–181. Zbl 0958.11048

[8] Cossidente, A.; Korchmáros, G.; Torres, F.: *On curves covered by the Hermitian curve.* J. Algebra **216** (1999), 56–76. Zbl pre01309249

[9] Cossidente, A.; Korchmáros, G.; Torres, F.: *Curves of large genus covered by the Hermitian curve.* Commun. Algebra **28**(10) (2000), 4707–4728. Zbl 0974.11031

[10] Fuhrmann, R.; Garcia, A.; Torres, F.: *On maximal curves.* J. Number Theory **67**(1) (1997), 29–51. Zbl 0914.11036

[11] Fuhrmann, R.; Torres, F.: *The genus of curves over finite fields with many rational points.* Manuscr. Math. **89** (1996), 103–106. Zbl 0857.11032

[12] Fuhrmann, R.; Torres, F.: *On Weierstrass points and optimal curves.* Rend. Circ. Mat. Palermo Suppl. **51** (1998), 25–46. Zbl pre01222881

[13] Garcia, A.; Stichtenoth, H.; Xing, C. P.: *On subfields of the Hermitian function field.* Compos. Math. **120** (2000), 137–170. Zbl 0990.11040

[14] Garcia, A.; Torres, F.: *On maximal curves having classical Weierstrass gaps.* Contemp. Math. **245** (1999), 49–59. Zbl 1044.11053

[15] van der Geer, G.; van der Vlugt, M.: *How to construct curves over finite fields with many points.* Arithmetic Geometry (Cortona 1994), F. Catanese (ed.), Cambridge Univ. Press, Sympos. Math. **37** (1997), 169–189. Zbl 0884.11027

[16] Goppa, V. D.: *Geometry and codes.* Mathematics and its applications **24**, Kluwer Academic Publisher, Dordrecht-Boston-London 1988.

[17] Harris, J.: *The genus of space curves.* Math. Ann. **249** (1980), 191–204. Zbl 0449.14006

[18] Hartshorne, R.: *Algebraic Geometry.* Graduate Texts in Mathematics **52**, Springer-Verlag, New York-Berlin 1977. Zbl 0367.14001

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

[20] Hefez, A.: *Non-reflexive curves.* Compos. Math. **69** (1989), 3–35. Zbl 0706.14024

[21] Hefez, A.; Kakuta, N.: *On the geometry of non-classical curves.* Bol. Soc. Bras. Mat. Nova Sér. **23**(1–2) (1992), 79–91. Zbl 0782.14024

[22] Hefez, A.; Kleiman, S.: *Notes on the duality of project varieties.* Geometry Today, Prog. Math. **60** (1985), 143–183.

[23] Hefez, A.; Voloch, J. F.: *Frobenius non-classical curves.* Arch. Math. **54** (1990), 263–273. Zbl 0662.14016

[24] Hirschfeld, J. W. P.: *Projective geometries over finite fields.* 2nd ed., Oxford Claredon Press, Oxford 1998. Zbl 0899.51002

[25] Homma, M.: *Reflexivity of tangent varieties associated with a curve.* Ann. Mat. Pura Appl. IV. Ser. **156** (1990), 195–210. Zbl 0722.14022

[26] Homma, M.: *Duality of spaces and their tangent surfaces in characteristic $p > 0$.* Ark. Mat. **29**(2) (1991), 221–235. Zbl 0766.14022

[27] Ihara, Y.: *Some remarks on the number of rational points of algebraic curves over finite fields.* J. Fac. Sci. Tokyo **28** (1981), 721–724. Zbl 0509.14019

[28] Korchmáros, G.; Torres, F.: *Embedding of a maximal curve in a Hermitian variety.* Compos. Math. **128** (2001), 95–113. Zbl 1024.11044

[29] Korchmáros, G.; Torres, F.: *On the genus of a maximal curve.* Math. Ann. **323**(3) (2002), 589–608. Zbl 1018.11029

[30] 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 (1987), 729–732. Zbl 0639.14013

[31] Lidl, R.; Niederreiter, H.: *Finite fields.* Encyclopedia Math. Appl. **20**, Adisson-Wesley, 1983. Zbl 0554.12010

[32] Moreno, C. J.: *Algebraic curves over finite fields.* Cambridge Univ. Press **97**, 1991. Zbl 0733.14025

[33] Mumford, D.: *Abelian varieties.* Tata Inst. Fund. Res., Oxford Univ. Press, Bombay 1985. Zbl 0583.14015

[34] Nijenhuis, A.; Wilf, H. S.: *Representations of integers by linear forms in non-negative integers.* J. Number Theory **4** (1972), 98–106. Zbl 0226.10057

[35] Rathmann, J.: *The uniform position principle for curves in characteristic* p. Math. Ann. **276** (1987), 565–579. Zbl 0595.14041

[36] Rück, H. G.; Stichtenoth, H.: *A characterization of Hermitian function fields over finite fields.* J. Reine Angew. Math. **457** (1994), 185–188. Zbl 0802.11053

[37] Stichtenoth, H.: *Algebraic function fields and codes.* Springer-Verlag, Berlin 1993. Zbl 0816.14011

[38] Stöhr, K. O.; Voloch, J. F.: *Weierstrass points and curves over finite fields.* Proc. Lond. Math. Soc. **52** (1986), 1–19. Zbl 0593.14020

[39] Voloch, J. F.: *Surfaces in* $\mathbf{P}^3$ *over finite fields.* Topics in algebraic and noncommutative geometry (Lumimy/Annapolis, MD, 2001), 219–226, Contemp. Math. **324** (2003), 219–226. Zbl 1040.11046

[40] Xing, C. P.; Stichtenoth, H.: *The genus of maximal function fields.* Manuscr. Math. **86** (1995), 217–224. Zbl 0826.11054

[41] Zak, F. L.: *Tangents and secants of algebraic varieties.* Transl. Math. Monogr. **127**, AMS (USA), 1993. Zbl 0795.14018

Received September 2, 2002; revised version February 15, 2004