Revista Colombiana de Matemáticas
Volumen 53(2019) páginas 223-235

On space maximal curves

Sobre curvas maximales en el espacio

Paulo César Oliveira[1,✉], Fernando Torres[2]

[1]Universidade Regional do Cariri, Juazeiro do Norte, Brazil

[2]Universidade Estadual de Campinas, Campinas, Brazil

Abstract. Any maximal curve $\mathcal{X}$ is equipped with an intrinsic embedding $\pi : \mathcal{X} \to \mathbb{P}^r$ which reveal outstanding properties of the curve. By dealing with the contact divisors of the curve $\pi(\mathcal{X})$ and tangent lines, in this paper we investigate the first positive element that the Weierstrass semigroup at rational points can have whenever $r = 3$ and $\pi(\mathcal{X})$ is contained in a cubic surface.

Key words and phrases. finite fields, Stöhr-Voloch theory, Hasse-Weil bound, maximal curve.

2010 Mathematics Subject Classification. 53C21, 53C42.

Resumen. Toda curva maximal $\mathcal{X}$ está intrínsicamente dotada de un mergullo $\pi : \mathcal{X} \to \mathbb{P}^r$ el cual vislumbra propiedades cruciales de la curva. Para $r = 3$, considerando los divisores de contacto de la curva $\pi(\mathcal{X})$ y rectas tangentes, investigamos el posible primer elemento positivo que un semigrupo de Weierstrass en un punto racional puede tener en el caso que $\pi(\mathcal{X})$ esté contenida en una superficie cúbica.

Palabras y frases clave. cuerpos finitos, teoría de Stöhr-Voloch, cota de Hasse-Weil, curva maximal.

1. Introduction

Throughout this paper, $\mathbf{F}$ stands for the finite field $\mathbb{F}_{q^2}$ of order q^2. A projective, geometrically irreducible, non-singular algebraic curve $\mathcal{X}$ defined over $\mathbf{F}$ of genus $g = g(\mathcal{X})$ is said to be $\mathbf{F}$-*maximal* if the number of its $\mathbf{F}$-rational points attains the Hasse-Weil upper bound; that is,

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

Apart from being interesting mathematical objects by their own, these curves have been extensively studied as they are of great interest in Coding Theory, Cryptography and related areas; see for example the books [24], [16], [14].

Let $\mathcal{X}$ be an $\mathbf{F}$-maximal curve of genus g. Then the numerator of the Zeta function of $\mathcal{X}$ is the polynomial $L(t) = (1+qt)^{2g}$ and hence $h(t) = t^{2g}L(t^{-1}) = (t+q)^{2g}$ is the characteristic polynomial of certain endomorphism $\tilde{\mathbf{\Phi}}$ on the Jacobian $\mathcal{J}$ of $\mathcal{X}$. This map is uniquely determined by the $\mathbf{F}$-Frobenius morphism $\mathbf{\Phi} : \mathcal{X} \to \mathcal{X}$ in such a way that $\iota \circ \mathbf{\Phi} = \tilde{\mathbf{\Phi}} \circ \iota$, where $\iota : \mathcal{X} \to \mathcal{J}$ is the natural embedding given by $P \mapsto [P - P_0]$ with $P_0 \in \mathcal{X}(\mathbf{F})$. It turns out that $\tilde{\mathbf{\Phi}}$ is semisimple and so the following linear equivalence (sometimes called the *fundamental equivalence*) on $\mathcal{X}$ arises (see [16, Thm. 10.1, Thm. 9.79]):

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

This suggests the study of the (complete) linear series $\mathcal{D}_{\mathcal{X}} := |(q+1)P_0|$ (sometimes called the *Frobenius linear series* of $\mathcal{X}$) whose definition clearly does not depend on the choice of the $\mathbf{F}$-rational point P_0. As a matter of fact, several arithmetical and geometrical properties of maximal curves are revealed through this linear series (loc. cit.). In particular, $\mathcal{D}_{\mathcal{X}}$ is very ample [7, Prop. 1.9], [18, Thm. 2.5] which means that the morphism associated to $\mathcal{D}_{\mathcal{X}}$

$$\pi_{\mathcal{D}_{\mathcal{X}}} : \mathcal{X} \to \mathbf{P}^r \tag{2}$$

is an embedding, where $r = r(\mathcal{X}) \geq 2$ is the projective dimension of $\mathcal{D}_{\mathcal{X}}$ (sometimes called the *Frobenius dimension* of $\mathcal{X}$), and $\mathbf{P}^r$ is the projective r-space over the algebraic closure of $\mathbf{F}$.

It is well-known that the Hermitian curve $\mathcal{H}$ defined by $v^{q+1} = u^{q+1} + 1$ is $\mathbf{F}$-maximal of genus $g(\mathcal{H}) = g_0 := q(q-1)/2$; see [24, Ex. 6.3.6]. Indeed, among $\mathbf{F}$-maximal curves, the curve $\mathcal{H}$ admits the following characterization.

Proposition 1.1. ([23], [27], [9]) *If $\mathcal{X}$ is $\mathbf{F}$-maximal, the following sentences are equivalent:*

(1) $\mathcal{X}$ is $\mathbf{F}$-isomorphic to the Hermitian curve $\mathcal{H}$;

(2) $g(\mathcal{X}) = g_0$;

(3) $g(\mathcal{X}) > (q-1)^2/4$;

(4) $r(\mathcal{X}) = 2$;

(5) There exists $P \in \mathcal{X}(\mathbf{F})$ such that the first positive element of $H(P)$, the Weierstrass semigroup at P, equals q.

From (2) any $\mathbf{F}$-maximal curve $\mathcal{X}$ is $\mathbf{F}$-isomorphic to a non-degenerate curve of degree $q+1$ in $\mathbf{P}^r$, $r = r(\mathcal{X})$. Thus the classical Castelnuovo's genus bound can be used to explain partially Proposition 1.1 as it gives the first general constrain between $g(\mathcal{X})$ and the pair (q, r) (see [16, Cor. 10.25]):

$$g(\mathcal{X}) \leq F(q,r) := \begin{cases} [(q-(r-1)/2)^2 - 1/4]/2(r-1)\,, & \text{if } r \text{ is even}\,, \\ [(q-(r-1)/2)^2]/2(r-1)\,, & \text{if } r \text{ is odd}\,. \end{cases} \tag{3}$$

Notice that the function $F(q, r)$ satisfies $F(q, r) \leq F(q, s)$ for $r \geq s$; in particular, $g(\mathcal{X}) \leq F(q, 3) = (q-1)^2/4$ provided that $r(\mathcal{X}) \geq 3$. Then, with $g_1 := \lfloor (q-1)^2/4 \rfloor$, by Proposition 1.1 the *spectrum for the genera* of $\mathbf{F}$-maximal curves, namely the set

$$\mathbf{M}(q^2) := \{g \in \mathbb{N}_0 : \text{there is an } \mathbf{F}\text{-maximal curve of genus } g\}\,,$$

satisfies

$$\mathbf{M}(q^2) \subseteq [0, g_1] \cup \{g_0\}\,. \tag{4}$$

We recall that g_0 is the well-known Ihara's bound on the genus of $\mathbf{F}$-maximal curves [15]. One of the main problems in Curve Theory Over Finite Fields is the computation of $\mathbf{M}(q^2)$; in general one cannot expect to give a full answer to this matter but improvements on (4) can be expected as far as improvements on Castelnuovo's genus bound of curves in $\mathbf{P}^r$ are known.

In view of Proposition 1.1 it is natural to investigate *space* $\mathbf{F}$*-maximal curves* with respect to $\mathcal{D}_{\mathcal{X}}$; that is, those with $r(\mathcal{X}) = 3$. Here a natural way of bounding $g(\mathcal{X})$, which generalizes Castelnuovo's method, is by looking at the degree $d \geq 2$ of surfaces $S \subseteq \mathbf{P}^3$ such that $\pi(\mathcal{X}) \subseteq S$ where $\pi = \pi_{\mathcal{X}}$ is as in (2); cf. [12], [21]. We have the following Halphen-Ballico result (see [3]) which deals with the case of quadrics. Let g_1 be as in (4) and set $g_2 := \lfloor (q^2 - q + 4)/6 \rfloor$; then

$$\pi(\mathcal{X}) \text{ is contained in a quadric in } \mathbf{P}^3 \text{ provided that } g_2 < g(\mathcal{X}) \leq g_1\,. \tag{5}$$

Now the $\mathbf{F}$-maximal property of $\mathcal{X}$ implies certain constrains on the first positive element $m_1(P)$ of the Weierstrass semigroup $H(P)$ at some $P \in \mathcal{X}(\mathbf{F})$, and (4) admits the folloing improvement [18]:

$$\mathbf{M}(q^2) \subseteq [0, g_2] \cup \{g_1\} \cup \{g_0\}\,. \tag{6}$$

An analogue of Proposition 1.1 emerges, namely

Proposition 1.2. ([7], [1], [17], [18]) *Let $\mathcal{X}$ be an $\mathbf{F}$-maximal curve. The following sentences are equivalent:*

(1) $\mathcal{X}$ is isomorphic to a quotient of $\mathcal{H}$ by certain involution;

(2) $g(\mathcal{X}) = g_1$;

(3) $\pi(\mathcal{X})$ *is contained in a quadric;*

(4) There exists $P \in \mathcal{X}(\mathbf{F})$ *such that the first positive element of* $H(P)$*, the Weierstrass semigroup at* P*, equals* $\lfloor (q+1)/2 \rfloor$.

The starting points of our result are in fact Propositions 1.1, 1.2 above. Under condition (7) below, the main result in this paper is Corollary 2.6, where a hypothesis on a cubic surface is considered; in this way a weak version of the aforementioned propositions is obtained. We always assume $q > 7$; cf. [2].

We do point out that our approach follows closely the works by Cossidente-Korchmáros-Torres [4, Sect. 3], [5, Sect. 5], Korchmáros-Torres [18], Fanali-Giulietti [6] and Arakelian-Tafazolian-Torres [2].

Conventions. $\mathbf{P}^s$ stands for the projective s-space over the algebraic closure of the base field. For a point P in a curve, $H(P)$ denotes the Weierstrass semigroup at P; $m_1(P)$ is the first positive element of $H(P)$.

2. Maximal curves and cubic surfaces

Let $\mathcal{X}$ be an $\mathbf{F}$-maximal curve, $P_0 \in \mathcal{X}(\mathbf{F})$ and $\mathcal{D} = \mathcal{D}_{\mathcal{X}} = |(q+1)P_0|$ the liner series introduced in Section 1; i.e., it is the set of effective divisors on $\mathcal{X}$ which are linearly equivalent to the divisor $(q+1)P_0$. We always assume $g(\mathcal{X}) > 0$; taking into consideration (6) and Propositions 1.1, 1.2 above, we also assume:

$$r(\mathcal{X}) = 3 \qquad \text{and} \qquad g(\mathcal{X}) \le g_2 = \lfloor (q^2 - q + 4)/6 \rfloor \,. \tag{7}$$

***Remark* 2.1.** Let $\mathcal{X}$ be an $\mathbf{F}$-maximal curve. From (3) and Proposition 1.1, a sufficient condition to have $r(\mathcal{X}) = 3$ is that $(q-1)(q-2)/6 < g(\mathcal{X}) \le g_1 = \lfloor (q-1)^2/4 \rfloor$.

Let $\pi = \pi_{\mathcal{D}} : \mathcal{X} \to \mathbf{P}^3$ be the morphism associated to $\mathcal{D}$.

Definition 2.2. For $P \in \mathcal{X}$, a non-negative integer j is called an $(\mathcal{D}, P)$-order if there is $D \in \mathcal{D}$ such that the coefficient $v_P(D)$ of P in D equals j.

Now let $P \in \mathcal{X}(\mathbf{F})$. Relation (1) implies the following behaviour for elements of $H(P)$:

$$m_0(P) = 0 < m_1(P) < m_2(P) < m_3(P) = q+1\,.$$

Thus for each $i = 0,1,2,3$ there are rational functions on $\mathcal{X}$, $h_i : \mathcal{X} \to \mathbf{P}^1$ such that $\mathrm{div}(h_i) = D_i - m_i(P)P$, $P \notin \mathrm{supp}(D_i)$ with $\mathrm{div}(h_3) = (q+1)P - (q+1)P_0$, $P \ne P_0$. For $P = P_0$ we put $h_3 = 1$. Then

$$\mathrm{div}(h_i h_3) + (q+1)P_0 = D_i + (q+1-m_i(P))P \in \mathcal{D}$$

and the $(\mathcal{D}, P)$-orders do satisfy (cf. [7, Prop. 1.5(iii)])

$$j_i(P) = q + 1 - m_{3-i}(P)\,, \quad i = 0,1,2,3\,; \tag{8}$$

therefore at $P \in \mathcal{X}(\mathbf{F})$, $j_3(P) = q+1$ and the first positive element $m_1(P)$ of $H(P)$ and $j_2(P)$ are related to each other by the equation

$$m_1(P) = q + 1 - j_2(P)\,. \tag{9}$$

***Remark* 2.3.** For the linear system $\mathcal{D}$ above and any $P \in \mathcal{X}$, the $(\mathcal{D}, P)$ orders can be ordered as a sequence $j_0(P) < j_1(P) < j_2(P) < j_3(P) \leq q+1$ with $j_0(P) = 0$ as $\mathcal{D}$ is base-point-free. Relation (1) shows that 1 and q are $(\mathcal{D}, P)$-orders for $P \notin \mathcal{X}(\mathbf{F})$. Thus for such points $j_1(P) = 1$ and $j_3(P) = q$ (as $g(\mathcal{X}) > 0$).

Now $j_3(P)$ is the intersection multiplicity of the curve $\pi(\mathcal{X}) \subseteq \mathbf{P}^3$ and the osculating hyperplane at $\pi(P)$ (cf. [25]); in addition, (1) also shows that $\pi(\mathbf{\Phi}(P))$ belongs to this hyperplane and we have the following key observation due to Stöhr and Voloch [25, Cor. 2.6]: Let $\nu_2 := q$ and $P \in \mathcal{X}(\mathbf{F})$. Then $j_3(P) - j_1(P) \geq \nu_2$; in particular, for $P \in \mathcal{X}(\mathbf{F})$, $j_1(P) = 1$, and so $m_2(P) = q$ by (8).

Lemma 2.4. *Let $\mathcal{X}$ be an $\mathbf{F}$-maximal curve satisfying (7) and let $P \in \mathcal{X}(\mathbf{F})$.*

(1) If $q > 3$, then $j_2(P) \notin \{(q+3)/2, (2q+3)/3, (2q+2)/3, q-1, q\}$;

(2) $j_2(P) \notin \{(q+1)/2, (q+2)/2\}$.

(3) If q is even and $j_2(P) = q/2$, then $g(\mathcal{X}) \leq q^2/8$.

***Proof*.** We have $m_1(P) = q+1-j_2(P)$; see (9).

(1) Since $2m_1(P) \geq m_2(P)$ and $m_2 = q$ by Remark 2.3, then $j_2(P) \leq (q+2)/2$. If any of the values in (1) were allowed, then $q \leq 3$.

(2) Suppose $j_2 = (q+1)/2$ (resp. $j_2 = (q+2)/2$). Then $m_1(P) = (q+1)/2$ (resp. $m_1(P) = q/2$) and hence $g(\mathcal{X}) = \lfloor (q-1)^2/4 \rfloor$ by [18, Thm. 1].

(3) If $j_2(P) = q/2$, $m_1(P) = (q+2)/2$ by Remark 2.3; then $g(\mathcal{X}) \leq g(H)$ where H is the semigroup generated by $(q+2)/2, q, q+1$ and $g(H) = \#(\mathbb{N}_0 \setminus S)$ is the genus of H. This number can be computed by the method of Rosales and Garcí a-Sánchez in [22]; i.e., $g(H) = q^2/8$ and the result follows. ☑

Theorem 2.5. *Let $\mathcal{X}$ be an $\mathbf{F}$-maximal curve satisfying (7). Suppose that $\pi(\mathcal{X})$ is contained in a cubic surface S.*

(1) For $P \in \mathcal{X}(\mathbf{F})$, $j_2(P) \in \{2, 3, q/2, (q+1)/3, (q+2)/3, (q+3)/3\}$;

(2) If q is even and $g(\mathcal{X}) > q^2/8$, then $j_2(P) \neq q/2$.

***Proof*.** Let $j_0 = 0 < j_1 = 1 < j_2 < j_3 = q+1$ be the $(\mathcal{D}, P)$-orders with $j_2 = j_2(P)$ and $v = v_P$ the valuation at P. Then π can be defined by $(f_0 : f_1 : f_2 : f_3)$ such that $v(f_i) = j_i$; in particular, $\pi(P) = (1:0:0:0)$ and throughout we assume $f_0 = 1$. Let the cubic surface S be defined by

$$\begin{aligned} F(X_0,X_1,X_2,X_3) = {} & a_{000}X_0^3 + a_{001}X_0^2X_1 + a_{002}X_0^2X_2 + a_{003}X_0^2X_3 + a_{111}X_1^3 \\ & + a_{110}X_1^2X_0 + a_{112}X_1^2X_2 + a_{113}X_1^2X_3 + a_{222}X_2^3 + a_{220}X_2^2X_0 \\ & + a_{221}X_2^2X_1 + a_{223}X_2^2X_3 + a_{333}X_3^3 + a_{330}X_3^2X_0 + a_{331}X_3^2X_1 \\ & + a_{332}X_3^2X_2 + a_{012}X_0X_1X_2 + a_{013}X_0X_1X_3 + a_{023}X_0X_2X_3 \\ & + a_{123}X_1X_2X_3. \end{aligned}$$

Then $F(1,f_1,f_2,f_3)=0$ and $a_{000}=0$. Now the valuation at P of the functions

$$\begin{gathered} f_1, f_2, f_3, f_1^3, f_1^2, f_1^2f_2, f_1^2f_3, f_2^3, f_2^2, f_2^2f_1, f_2^2f_3, f_3^3, \\ f_3^2, f_3^2f_1, f_3^2f_2, f_1f_2, f_1f_3, f_2f_3, f_1f_2f_3 \end{gathered}$$

are respectively

$$\begin{gathered} 1, j_2, j_3, 3, 2, 2+j_2, 2+j_3, 3j_2, 2j_2, 1+2j_2, 2j_2+j_3, 3j_3, \\ 2j_3, 1+2j_3, j_2+2j_3, 1+j_2, 1+j_3, j_2+j_3, 1+j_2+j_3\,. \end{gathered}$$

Then the valuation property of v implies $a_{001}=0$. Let $j_2>3$ so that $a_{111}=a_{110}=0$ (recall that $q>7$). We have $j_2+2<j_3$, otherwise $j_2\in\{q,q-1\}$ which is not possible by Lemma 2.4. Thus

$$\begin{aligned} j_2 < j_2+1 < j_2+2 < j_3 < j_3+1 < j_3+2 < j_3+j_2 < j_3+j_2+1 < 2j_3 < \\ 2j_3+1 < 2j_3+j_2 < 3j_3\,. \end{aligned}$$

Since $2j_2<2j_2+1<3j_2<2j_2+j_3$, the valuation property of v implies the following cases:

(1) Either $2j_2\in\{j_3,j_3+1,j_3+2\}$, or

(2) $2j_2+1=j_3$, or

(3) $3j_2\in\{j_3,j_3+1,j_3+2,2j_3,2j_3+1\}$.

By Lemma 2.4, $2j_2\neq j_3,j_3+1,j_3+2$, $3j_2\neq 2j_3$, $3j_2\neq 2j_3+1$, and $2j_2+1\neq j_3$ whenever $g>q^2/8$.

Therefore $j_2\in\{2,3,(q+1)/3,(q+2)/3,(q+1)/3\}$ and the proof follows. ☑

Now we can state the main result in this paper.

Corollary 2.6. *Let $\mathcal{X}$ be an $\mathbf{F}$-maximal curve as in Theorem 2.5. Then the multiplicity $m_1(P)$ of the Weierstrass semigroup $H(P)$ at $P\in\mathcal{X}(\mathbf{F})$ do satisfy*

$$m_1(P)\in\{(q+2)/2,(2q+2)/3,(2q+1)/3,2q/3,q-2,q-1\}\,.$$

In addition, if q is even and $g(\mathcal{X})>q^2/8$, then $m_1(P)\neq(q+2)/2$.

Proof. It follows from (9) and the theorem above. ☑

***Remark* 2.7.** Notation as in Remark 2.3. For the linear series $\mathcal{D}$, a basic result is that for almost $P \in \mathcal{X}$, the sequence $j_0(P < j_1(P) < j_2(P) < j_3(P)$ is constant (so called *order sequence of* $\mathcal{D}$) cf. [25, p. 5]). In Remark 2.3 we noticed that $j_0(P) = 0$, $j_1(P) = 1$, $j_3(P) = q$ for $P \notin \mathcal{X}(\mathbf{F})$ and thus the order sequence of $\mathcal{D}$ is of type $0 < 1 < \epsilon_2 < q$.

By the proof of [2, Prop. 3.1], $\epsilon_2 = 2$ provided that

$$g(\mathcal{X}) > \begin{cases} (q^2+1)(q-4)/2(4q-1)\,, & \text{whenever } q \not\equiv 0 \pmod 3\,, \\ g > (q^2+1)(q-3)/2(3q-1)\,, & \text{otherwise}\,. \end{cases}$$

This forces $g(\mathcal{X}) \geq (q^2 - 2q + 3)/6\,(*)$ (see [4, Remark 3.3], [2, Prop. 3.1]).

Now for $P \in \mathcal{X}(\mathbf{F})$ the Weierstrass semigroup $H(P)$ contains the semigroup generated by $m, q, q+1$, where $m = m_1(P) = q + 1 - j_2(P)$ (cf. 9); hence $g(\mathcal{X}) \leq g(H)$ (the genus of H). Then by using heavy arithmetical computations from [8, Sect. 2] and by taking into consideration restriction $(*)$ above, Corollary 2.6 was already proved in [4, Cor. 3.5] whithout the hypothesis regarding the cubic surface.

***Remark* 2.8.** Let $\mathcal{X}$ be an $\mathbf{F}$-maximal curve such that (7) holds; in particular, we identify $\mathcal{X}$ with a non-degenerate projective curve in $\mathbf{P}^3$ and we can apply the aforementioned Castelnuovo and Halphen-Ballico results as they are true in positive characteristic [3]. We look forward a result of type: There exists a polynomial (of one indeterminate) $A(x) \in \mathbb{Q}[x]$ such that

$$g(\mathcal{X}) > A(q+1) \quad \text{implies} \quad \pi(\mathcal{X}) \subseteq S\,, \tag{10}$$

where S is a surface of degree $d \leq 3$ (Then we shall assume $d = 3$ by Propositions 1.1, 1.2.)

***Remark* 2.9.** In the literature, for a non-degenerate projective space curve $\mathcal{C}$ of degree $q+1$ over the complex numbers, there are available results of type (10) which in fact appear as particular cases of a vast theory that generalize the aforementioned Castelnuovo and Halphen results; see Eisenbud-Harris book [12, Thm. 3.22, p. 117].

Let q be large, says $q \geq 107$. If

$$g(\mathcal{C}) > A(q+1) := \begin{cases} \dfrac{q(q+2)}{8}, & \text{if} \quad q \equiv 0, 2 \pmod 4\,, \\ \dfrac{q^2+2q-3}{8}, & \text{if} \quad q \equiv 1 \pmod 4\,, \\ \dfrac{q^2+2q+9}{8}, & \text{otherwise}\,, \end{cases}$$

then there exists a surface S of degree 2 or 3 such that $\mathcal{C} \subseteq S$.

Question 2.10. Is Remark 2.9 true in positive characteristic?

3. Examples

In this section we illustrate Corollary 2.6. Notation as above; in particular, $\mathcal{H}$ is the Hermitian curve over $\mathbf{F} = \mathbf{F}_{q^2}$ defined by $v^{q+1} = u^{q+1} + 1$. Let $\pi : \mathcal{H} \to \mathbf{P}^2$ be a non-trivial morphism over $\mathbf{F}$ and $\mathcal{X}$ the non-singular model of the plane curve $\pi(\mathcal{H})$; then π can be lifted to a morphism $\mathcal{H} \to \mathcal{X}$, which we still denote by π. In this case, the curve $\mathcal{X}$ is also $\mathbf{F}$-maximal (see e.g. [19]).

Example 3.1. (cf. [6, Sect. 5]) Let $q \equiv 2 \pmod 3$ and $\pi : \mathcal{H} \to \mathbf{P}^2$ be the morphism given by $\pi = (x : y : 1) := (u^3 : uv : 1)$. Then the plane curve $\pi(\mathcal{H})$ is defined by

$$y^{q+1} = x^{(q+1)/3}(x^{(q+1)/3} + 1)\,,$$

and by applying the Riemann-Hurwitz formula to the function $x : \mathcal{X} \to \mathbf{P}^1$, where $\mathcal{X}$ is the non-singular model of $\pi(\mathcal{H})$, we find that $\mathcal{X}$ is $\mathbf{F}$-maximal of genus $g(\mathcal{X}) = g_2 = (q^2 - q + 4)/6$ (cf. [10], [5, Prop. 2.1]). We notice that $r(\mathcal{X}) = 3$ by Remark 2.1 above.

Next we shall compute the Weierstrass semigroup $H(P)$ at certain points of $\mathcal{X}$; we start by computing some principal divisors on $\mathcal{X}$ via tools from [24].

(a) There are $(q+1)/3$ points in $x^{-1}(\infty)$, say P_i, $i = 1, \ldots, (q+1)/3$.
Set $D_\infty := P_1 + \ldots + P_{(q+1)/3}$.

(b) There are $(q+1)/3$ points in $x^{-1}(0)$, say Q_i, $i = 1, \ldots, (q+1)/3$.
Set $D_0 := Q_1 + \ldots + Q_{(q+1)/3}$. Then $\mathrm{div}(x) = 3D_0 - 3D_\infty$.

(c) Let $a \in \mathbf{F}$ such that $a^{(q+1)/3} = -1\,(*)$. There is just point R_a over $x^{-1}(a)$ and
$\mathrm{div}(x-a) = (q+1)R_a - 3D_\infty$. Set $D := \sum_{i/i^{(q+1)/3}=-1} R_i$.
Then $\mathrm{div}(x^{(q+1)/3} + 1) = (q+1)D - (q+1)D_\infty$.

From (a), (b), (c), $\mathrm{div}(y) = D_0 + D - 2D_\infty$, and for $a \in \mathbf{F}$ as in $(*)$ above

$$\mathrm{div}((x-a)^{-1}) = 3D_\infty - (q+1)R_a\,, \quad \mathrm{div}(y(x-a)^{-1}) = D_0 + D' + D_\infty - qR_a \quad \text{and}$$

$$\mathrm{div}(y^3x^{-1}(x-a)^{-1}) = 3D' - (q-2)R_a\,,$$

where $D' = D - R_a$. It follows that $H(R_a) \supseteq H := \langle q-2, q, q+1\rangle$ so that $g(\mathcal{X}) \le g(H)$. We have that the sequence $q-2, q+1, q$ is telescopic and so $g(H) = (q^2 - q + 4)/6$ (see e.g. [13, Prop. 5.35]). Therefore

Claim. $H(R_a) = H$ and $m_1(R_a) = q-2$ (this also shows that $r(\mathcal{X}) = 3$).

Moreover by Remark 2.7 the order sequence of $\mathcal{X}$ is $0 < 1 < 2 < q$ and thus there is also a point $P \in \mathcal{X}(\mathbf{F})$ with $m_1(P) = q-1$ (see [4, Lemma 3.7]).

***Remark* 3.2.** We can construct explicit and outstanding AG one-point codes based on the curve in Example 3.1 by taking into consideration the telescopic property of $H(R_a)$; cf. [13, Sect. 5], [26, Sect. 5].

Example 3.3. Let $q \equiv 2 \pmod 3$. Here we point out properties of an arbitrary $\mathbf{F}$-maximal curve $\mathcal{X}$ of genus $g(\mathcal{X}) = g_2 = (q^2 - q + 4)/6$. We have $r(\mathcal{X}) = 3$ by Remark 2.1, and that $0 < 1 < 2 < q$ is the order sequence of $\mathcal{D} = \mathcal{D}_{\mathcal{X}}$ by Remark 2.7. Then by [4, Lemma 3.7] there is $\bar{P} \in \mathcal{X}(\mathbf{F})$ with $m_1(\bar{P}) = q - 1$, or $j_2(\bar{P}) = 2$ by (9).

Claim. There is $P \in \mathcal{X}(\mathbf{F})$ such that $j_2(P) > 2$.

Indeed, otherwise [18, Lemma 7] would imply $g = (q^2 - 2q + 3)/6$, a contradiction.

Let $\pi : \mathcal{X} \to \mathbf{P}^3$ be the morphism associated to $\mathcal{D}$. We are led to the following questions.

(A) Is $\pi(\mathcal{X})$ contained in a cubic surface? (This would be true if the answer to Question 2.10 is affirmative)

(B) Let $\mathcal{X}$ be an $\mathbf{F}$-maximal curve. Then $g(\mathcal{X}) = g_2$ if and only if $\pi(\mathcal{X})$ is contained in a cubic surface and there is $\bar{P} \in \mathcal{X}(\mathbf{F})$ with $j_2(\bar{P}) > 2$?

Question (B) above is related to the following result which is a consequence of the proof of [18, Thm. 1] and [18, Lemma 7].

***Remark* 3.4.** With g_1 as in (4), for an $\mathbf{F}$-maximal curve $\mathcal{X}$ we have that $g(\mathcal{X}) = g_1$ if and only if $\pi(\mathcal{X})$ is contained in a quadric and there is $\bar{P} \in \mathcal{X}(\mathbf{F})$ with $j_2(\bar{P}) > 2$.

Example 3.5. Let $q \equiv 2 \pmod 3$. We investigate $\mathbf{F}$-maximal curves of genus $g(\mathcal{X}) = g_3 = g_2 - 1 = (q^2 - q - 2)/6$ which were constructed in [4]. To start with, $r(\mathcal{X}) = 3$ by Remark 2.1 and the order seqeunce of $\mathcal{D}$ is $0 < 1 < 2 < q$ by Remark 2.7. In particular, there is $P \in \mathcal{X}(\mathbf{F})$ such that $m_1(P) = q - 1$ by [4, Lemma 3.7].

We further assume the following properties:

(a) $\pi(\mathcal{X})$ is contained in a cubic surface;

(b) $\pi : \mathcal{H} \to \mathcal{X}$ is Galois of degree three.

(The aforementioned curves in [4] satisfy these properties)

Claim. There is $\bar{P} \in \mathcal{X}(\mathbf{F})$ with $m_1(\bar{P}) = (2q + 2)/3$.

Proof of the Claim. By the Riemann-Hurwitz relation there is $\bar{P} \in \mathcal{X}(\mathbf{F})$ which is totally ramified for π. Let $Q = \pi^{-1}(\bar{P}) \in \mathcal{H}$. The first six positive elements of the Weierstrass semigroup at Q are $q, q + 1, 2q, 2q + 1, 2q + 2, 3q$.

Now let $m = m_1(\bar{P}) < q < q+1$ be the first three positive elements of $H(\bar{P})$. Then $3m \in \{q, q+1, 2q, 2q+1, 2q+2\}$ and so $m \in \{(q+1)/3, (2q+2)/3$. We eliminate the case $m = (q+1)/3$ by Corollary 2.6 and the Claim follows.

Example 3.6. Let $q \not\equiv 2 \pmod 3$ and $\mathcal{X}$ be an $\mathbf{F}$-maximal curve of genus $g(\mathcal{X}) = g_2 = (q^2 - q)/6$; hence $r(\mathcal{X}) = 3$ by Remark 2.1 and the order sequence of $\mathcal{D}$ is $0 < 1 < 2 < q$ by Remark 2.7. by Remark 2.7. In particular, there is $P \in \mathcal{X}(\mathbf{F})$ such that $m_1(P) = q-1$ by [4, Lemma 3.7]. We notice that examples of such curves do exist: see e.g. [10], [5, Prop. 2.1].

Let us assume properties (a) and (b) in Example 3.5 (indeed, the aforementioned examples satisfy these hypotheses).

Claim. If $q \equiv 1 \pmod 3$ (resp. $q \equiv 0 \pmod 3$), then there exists $\bar{P} \in \mathcal{X}(\mathbf{F})$ with $m_1(\bar{P}) = (2q+1)/3$ (resp. $m_1(\bar{P}) = 2q/3$).

Arguing as in Example 3.5 there is $\bar{P} \in \mathcal{X}(\mathbf{F})$ such that $3m \in \{q, q+1, 2q, 2q+1, 2q+2\}$ with $m = m_1(\bar{P})$.

If $q \equiv 1 \pmod 3$, $m = (2q+1)/3$.

If $q \equiv 0 \pmod 3$, either $m = q/3$ or $m = 2q/3$. The former case is eliminated by Corollary 2.6.

Example 3.7. Here we present an $\mathbf{F}$-maximal curve $\mathcal{X}$ with $r(\mathcal{X}) = 3$ such that $\pi(\mathcal{X})$ cannot be contained in a cubic surface, where π is the morphism associated to $\mathcal{D}$. Indeed, we consider the so-called GK-curve [11] whose Weierstrass semigroups at rational points were computed in [6]. This curve is defined over $\mathbf{F} = \mathbb{F}_{q^2}$ with $q = \ell^3$. For $\ell > 2$ this is the first example of an $\mathbf{F}$-maximal curve that cannot be dominated by $\mathcal{H}$ (loc. cit.)

On this curve there is $\bar{P} \in \mathcal{X}(\mathbf{F})$ such that $m_1(\bar{P}) = \ell^3 - \ell^2 + \ell$ [11, Sect. 4], and therefore, according to Corollary 2.6, $\pi(\mathcal{X})$ cannot be contained in a cubic. We notice that the genus of $\mathcal{X}$ is $g(\mathcal{X}) = \frac{1}{2}(\ell^5 - 2\ell^3 + \ell^2)/2$ and so it does not satisfies Remark 2.9. Further examples can be found in [26].

We end this paper with the following:

Question 3.8. Let $\mathcal{X}$ be an $\mathbf{F}$-maximal curve with $r(\mathcal{X}) = 3$. Suppose that $\pi(\mathcal{X}) \subseteq S$, where S is a surface of degree $d \geq 2$. Let $P \in \mathcal{X}(\mathbf{F})$ and suppose $g(\mathcal{X})$ large enough. Then $m_1(P) = (q+1) - \frac{q+i}{d}$ or $m_1(P) = q - j$ for some $i = 1, \ldots, d$, $j = 2, \ldots, d$. Are all these cases possible?

Acknowledgment. This paper is based on the Ph.D. dissertation [20] done at IMECC-UNICAMP. The second author was partially supported by CNPq (Grant 310623/2017-0). We also gratefully thank James W.P. Hirschfeld for useful comments.

References

[1] M. Abdón and F. Torres, *Maximal curves in charateristic two*, Manuscripta Math. **99** (1999), 39–53.

[2] N. Arakelian, S. Tafazolian, and F. Torres, *On the spectrum for the genera of maximal curves over small fields*, Adv. Math. Commun. **12** (2018), 143–149.

[3] E. Ballico, *Space curves not contained in low degree surfaces in positive characteristic*, Noti di Matematica **20** (2000/2001), no. 2, 27–33.

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

[5] ———, *Curves of large genus covered by the hermitian curve*, Comm. Algebra **28** (2000), 4707–4728.

[6] S. Fanali and M. Giulietti, *On some open problems on maximal curves*, Des. Codes Cryptogr. **56** (2010), 131–139.

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

[8] R. Fuhrmann, *Algebraische funktionenkörper über endlichen körpern mit maximaler anzahl rationaler stellen*, Ph.d dissertation, Universität GH Essen, 1995.

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

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

[11] M. Giulietti and G. Korchmáros, *A new family of maximal curves over a finite fiel*, Math. Annalen **343** (2009), 229–245.

[12] J. Harris, *Curves in projective space*, Université de Montréal, 1982.

[13] T. Hoholdt, J. H. van Lint, and R. Pellikaan, *Algebraic geometry codes*, vol. 1, Elsevier, 1998.

[14] N. E. Hurt, *Many rational points, coding theory and algebraic geometry*, Kluwer Acad. Publishers, 2003.

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

[16] Hirschfeld J. W. P., G. Korchmáros, and F. Torres, *Algebraic curves over a finite field*, Princeton Univ. Press, 2008.

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

[18] ______, *On the genus of a maximal curve*, Math. Annalen **323** (2002), 589–608.

[19] G. Lachaud, *Sommes d'eisenstein et nombre de points de certains courbes algébriques sur les corps finis*, C.R. Acad. Sci. Paris Sér. I Math **305** (1987), 729–732.

[20] P. C. Oliveira, *Sobre curvas maximais em superfícies cúbicas*, Tesis doctoral, Universidade Estadual de Campinas, 2016.

[21] J. Rathmann, *The uniform position principle for curves in charateristic p*, Math. Annalen **276** (1987), 565–579.

[22] J. C. Rosales and P. A. García-Sanchez, *Numerical semigroups with embedding dimension three*, Arch. Math. **83** (2004), 488–496.

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

[24] H. Stichtenoth, *Algebraic function fields and codes*, Springer-Verlag, 2009.

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

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

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

(Recibido en de 2018. Aceptado en de 2018)

Departamento de Matemática Pura e Aplicada
Universidade Regional do Cariri
Centro de Ciências e Tecnologia
Av. Leão Sampaio, 107, Triângulo, 63.040-000
Juazeiro do Norte, CE, Brazil
e-mail: paulocesar.oliveira@urca.br

IMECC - UNICAMP
Rua Sérgio Buarque de Holanda, 651,
Cidade Universitária Zeferino Vaz, 13.083-859,
Campinas, SP, Brazil
e-mail: ftorres@ime.unicamp.br