ACTA ARITHMETICA
XCVIII.2 (2001)

Plane maximal curves

by

Angela Aguglia (Napoli), Gábor Korchmáros (Potenza)
and Fernando Torres (Campinas)

1. Introduction. An $\mathbb{F}_{q^2}$-*maximal curve* of genus g is a projective, geometrically irreducible, non-singular, algebraic curve defined over a finite field $\mathbb{F}_{q^2}$ of order q^2 such that the number of its $\mathbb{F}_{q^2}$-rational points attains the Hasse–Weil upper bound

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

Maximal curves, especially those having large genus with respect to q, are known to be very useful in coding theory [19]. Also, there are various ways of employing them in cryptography, and it is expected that this interesting connection will be explored more fully; see [34, Chapter 8]. Another motivation for the study of maximal curves comes from correlations of shift register sequences [28], exponential sums over finite fields [29], and finite geometry [22]. Recent papers on maximal curves which also contain background and expository accounts are [32], [35], [10], [9], [18], [11], [7], [14], [6], [1], [8], and [26].

A relevant result on $\mathbb{F}_{q^2}$-maximal curves $\mathcal{X}$ with genus g states that either $g = q(q-1)/2$ and $\mathcal{X}$ is $\mathbb{F}_{q^2}$-isomorphic to the Hermitian curve $\mathcal{H}$ of equation

$$X^{q+1} + Y^{q+1} + Z^{q+1} = 0, \tag{1.1}$$

or $g \le (q-1)^2/4$; see [25], [35], and [10]. One expects that the bound $(q-1)^2/4$ can be substantially lowered apart from a certain number of exceptional values of g. Finding such values is one of the problems of current interest in the study of maximal curves; see [9, Section 3], [11, Proposition 2.5], [7, Section 3], and [1].

2000 *Mathematics Subject Classification*: Primary 11G20; Secondary 14G15.

This research was carried out within the project "Progetto e Realizzazione di un Criptosistema per Telecomunicazioni", POP FESR 1994/99 – II Triennio. The third author was partially supported by Cnpq-Brazil, Proc. 300681/97-6.

In this paper we investigate (non-singular) plane maximal curves. In Section 2 we prove the non-existence of a plane $\mathbb{F}_{q^2}$-maximal curve whose genus belongs to the interval $(q(q-2)/8, q(q-2)/4]$ for q even, while $((q-1)(q-3)/8, (q-1)^2/4]$ for q odd; see Corollary 2.3. The curves studied in Section 3 show that these bounds are sharp in some cases. In contrast, a few examples of (non-planar) $\mathbb{F}_{q^2}$-maximal curves with genera in these intervals are known to exist; see [9, Section 3], [7, pp. 74–75], [1], [13], and [8, Theorem 2.1].

In the course of our investigation we point out that the Hermitian curve $\mathcal{H}$ is the unique $\mathbb{F}_{q^2}$-maximal curve (up to $\mathbb{F}_{q^2}$-isomorphism) which is $\mathbb{F}_{q^2}$-Frobenius non-classical with respect to the linear series Σ_1 cut out by lines; see Proposition 2.2. Also, the order of contact ε_2 of a non-classical (with respect to Σ_1) $\mathbb{F}_{q^2}$-maximal curve with the tangent at a general point satisfies $\varepsilon_2^2 \le q/p$, where $p := \mathrm{char}(\mathbb{F}_{q^2})$; see Corollary 2.8. In particular, plane $\mathbb{F}_{q^2}$-maximal curves with $q = p$ and $q = p^2$ are classical with respect to Σ_1.

According to [27, Prop. 6], every curve which is $\mathbb{F}_{q^2}$-covered by the Hermitian curve is $\mathbb{F}_{q^2}$-maximal. An open problem of considerable interest is to decide whether the converse of this statement also holds. In Section 3 we solve this problem for the family of the so-called Hurwitz curves. Recall that a Hurwitz curve of degree $n+1$ is defined as a non-singular plane curve of equation

$$X^nY + Y^nZ + Z^nX = 0, \tag{1.2}$$

where $p = \mathrm{char}(\mathbb{F}_{q^2})$ does not divide $n^2 - n + 1$. Theorem 3.1 together with Corollary 3.3 states indeed that the Hurwitz curve is $\mathbb{F}_{q^2}$-covered by the Hermitian curve if and only if

$$q + 1 \equiv 0 \pmod{(n^2 - n + 1)}. \tag{1.3}$$

It should be noted on the other hand that for certain n and p, the Hurwitz curve is not $\mathbb{F}_{q^2}$-maximal for any power q of p; this occurs, for instance, for $n = 3$ and $p \equiv 1 \pmod 7$. One can then ask for conditions in terms of n and p which assure that the Hurwitz curve is $\mathbb{F}_{q^2}$-maximal for some power q of p. Our results in this direction are given in Remarks 3.6 and 3.10, and Corollaries 3.7 and 3.8. They generalize some previous results obtained in [4, Lemmes 3.3, 3.6]. Another feature of the Hurwitz curve is that it is non-classical provided that p^e divides n with $p^e \ge 3$; see Remark 3.11. So if both (1.3) and $p^e \mid n$ hold then the Hurwitz curve turns out to be a non-classical plane $\mathbb{F}_{q^2}$-maximal curve. Examples are given in Corollary 3.8. As far as we know, these Hurwitz curves together with the Hermitian curves and the Fermat curves of degree $n^2 - n + 1$ (see Corollary 3.3) are the only known examples of non-classical plane $\mathbb{F}_{q^2}$-maximal curves. As mentioned before, these curves show the sharpness of some of the results obtained in Section 2.

Hurwitz curves as well as their generalizations have been investigated for several reasons by many authors; see [3, Section 1] and [31]. This gives a motivation to the final Section 4 where we show that the main results of Section 3 extend to (the non-singular model of) the curve with equation

$$X^nY^l + Y^nZ^l + Z^nX^l = 0,$$

where $n \geq l \geq 2$ and $p = \mathrm{char}(\mathbb{F}_{q^2})$ does not divide $Q(n,l) := n^2 - nl + l^2$.

Our investigation uses some concepts, such as non-classicity, from Stöhr–Voloch's paper [36] where an alternative proof to the Hasse–Weil bound was given among other things. We also refer to that paper for terminology and background results on orders and Frobenius orders of linear series on curves.

2. The degree of a plane maximal curve. Let $\mathcal{X}$ be a plane $\mathbb{F}_{q^2}$-maximal curve of degree $d \geq 2$. Since the genus of $\mathcal{X}$ is $(d-1)(d-2)/2$, the upper bound for g quoted in Section 1 can be rephrased in terms of d:

$$d \leq d_1(q) := \frac{3 + \sqrt{2(q-3)(q+1)+9}}{2} \quad \text{or} \quad d = q+1. \tag{2.1}$$

The main result in this section is the improvement of (2.1) given in Theorem 2.12: Apart from small q's, either $d = q+1$, or $d = \lfloor (q+2)/2 \rfloor$, or d is upper bounded by a certain function $d_5(q)$ such that $d_5(q)/q \approx 2/5$. Our first step consists in lowering $d_1(q)$ to $d_2(q)$ with $d_2(q)/q \approx 1/2$.

Let Σ_1 be the linear series cut out by lines of $\mathbb{P}^2(\overline{\mathbb{F}}_{q^2})$ on $\mathcal{X}$. For $P \in \mathcal{X}$, let $j_0(P) = 0 < j_1(P) = 1 < j_2(P)$ be the (Σ_1, P)-orders, and $\varepsilon_0 = 0 < \varepsilon_1 = 1 < \varepsilon_2$ the orders of Σ_1. Also, let $\nu_0 = 0 < \nu_1$ be $\mathbb{F}_{q^2}$-Frobenius orders of Σ_1. Finally, p will denote the characteristic of $\mathbb{F}_{q^2}$.

LEMMA 2.1. (1) $\nu_1 \in \{1, \varepsilon_2\}$;
(2) $\varepsilon_2 \leq q$;
(3) ε_2 *is a power of* p *whenever* $\varepsilon_2 > 2$.

Proof. For (1), see [36, Prop. 2.1]. For (2), suppose that $\varepsilon_2 > q$; then $\varepsilon_2 = q+1$ as $\varepsilon_2 \leq d$ and $d \leq q+1$ by (2.1). Then, by the p-adic criterion [36, Cor. 1.9], q would be a Σ_1-order, a contradiction. For (3), see [16, Prop. 2]. ∎

The following result is a complement to [30, Prop. 3.7], [23, Thm. 6.1], and [21, Prop. 6].

PROPOSITION 2.2. *For a plane* $\mathbb{F}_{q^2}$*-maximal curve* $\mathcal{X}$ *of degree* $d \geq 3$, *the following conditions are equivalent*:

(1) $d = q+1$;
(2) $\mathcal{X}$ *is* $\mathbb{F}_{q^2}$*-isomorphic to the Hermitian curve of equation* (1.1);
(3) $\varepsilon_2 = q$;
(4) $\nu_1 = q$;
(5) $j_2(P) = q+1$ *for each* $P \in \mathcal{X}(\mathbb{F}_{q^2})$;
(6) $\nu_1 > 1$; *i.e.* Σ_1 *is* $\mathbb{F}_{q^2}$*-Frobenius non-classical.*

Proof. (1)⇒(2). Since the genus of a non-singular plane curve of degree d is $q(q-1)/2$, part (2) follows from [32].

(2)⇒(3). This is well known property of the Hermitian curve; see e.g. [10, p. 105] or [15].

(3)⇒(4). If $q=2$, then from $d \geq \varepsilon_2 = q$ and (2.1), either $d=2$ or $d=3$. By hypothesis, $d=3$ can only occur, and so, by parts (1) and (2), $\mathcal{X}$ is $\mathbb{F}_4$-isomorphic to the Hermitian curve $X^3+Y^3+Z^3=0$. Then $\nu_1 = \varepsilon_2 = 2$; see loc. cit.

Let $q \geq 3$. By Lemma 2.1(1), $\nu_1 \in \{1, q\}$. Suppose that $\nu_1 = 1$ and let S_1 be the $\mathbb{F}_{q^2}$-Frobenius divisor associated with Σ_1. Then, by [36, Thm. 2.13],

$$\deg(S_1) = (2g-2) + (q^2+2)d \geq 2\#\mathcal{X}(\mathbb{F}_{q^2}) = 2(q+1)^2 + 2q(2g-2)$$

so that $((2q-1)d - (q^2+2q+1))(d-2) \leq 0$, and hence

$$d \leq F(q) := (q^2+2q+1)/(2q-1). \tag{2.2}$$

Thus, as $d \geq \varepsilon_2 = q$, we would have $q^2-3q-1 \leq 0$ and hence $q \leq 3$. If $q=3$, from (2.2) we have $d=3$; this contradicts [30, Cor. 2.2] (cf. Remark 2.5(ii)).

(4)⇒(5). By [36, Cor. 2.6], $\nu_1 \leq j_2(P) - 1$ for any $P \in \mathcal{X}(\mathbb{F}_{q^2})$. Then part (5) follows as $j_2(P) \leq d$ and $d \leq q+1$ by (2.1).

(5)⇒(6). Suppose that $\nu_1 = 1$. Then, by [36, Prop. 2.4(a)], $v_P(S_1) \geq q+1$ for any $P \in \mathcal{X}(\mathbb{F}_{q^2})$. Therefore

$$\deg(S_1) = (2g-2)+(q^2+2)d \geq (q+1)\#\mathcal{X}(\mathbb{F}_{q^2}) = (q+1)^3+(q+1)q(2g-2),$$

a contradiction as $3 \leq d \leq q+1$.

(6)⇒(1). From [21, Thm. 1] and the $\mathbb{F}_{q^2}$-maximality of $\mathcal{X}$ we have

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

Since $2g-2 = d(d-3)$ and $d > 1$, part (1) follows. ∎

Corollary 2.3. *Let $d \geq 3$ be the degree of a plane $\mathbb{F}_{q^2}$-maximal curve. Then either $d = q+1$ or*

$$d \leq d_2(q) := \begin{cases} \lfloor (q+2)/2 \rfloor & \text{if } q \geq 4 \text{ and } q \neq 3,5, \\ 3 & \text{if } q = 3, \\ 4 & \text{if } q = 5. \end{cases}$$

In particular, for $q \neq 3,5$, an $\mathbb{F}_{q^2}$-maximal curve has no non-singular plane model if its genus belongs to the interval $(q(q-2)/8, q(q-2)/4]$, for q even, and $((q-1)(q-3)/8, (q-1)^2/4]$, for q odd.

Proof. The statement on the genus follows immediately from the upper bound on d. By (2.1) we have $d \leq q+1$. If $d < q+1$, then $q \geq 3$ and from Proposition 2.2, Σ_1 is $\mathbb{F}_{q^2}$-Frobenius classical. In particular, (2.2) holds true: $d \leq F(q)$. It is easy to see that $F(q) < (q+3)/2$ for $q > 5$ and $F(4) = 25/7$. Moreover, $F(3) = 16/5$ and $F(5) = 4$, and the result follows. ∎

REMARK 2.4. Let d be the degree of a plane $\mathbb{F}_{q^2}$-maximal curve of degree d and assume that $3 \le d \le d_2(q)$.

(i) If q is odd, then the $\mathbb{F}_{q^2}$-maximal curve of equation

$$X^{(q+1)/2} + Y^{(q+1)/2} + Z^{(q+1)/2} = 0$$

shows that the upper bound $d_2(q) = (q+1)/2$ in Corollary 2.3 is the best possible as far as $q \neq 3, 5$. We notice that this curve is the unique $\mathbb{F}_{q^2}$-maximal plane curve (up to $\mathbb{F}_{q^2}$-isomorphism) of degree $(q+1)/2$ provided that $q \ge 11$; see [6].

(ii) From results of Deuring, Tate and Waterhouse (see e.g. [37, Thm. 4]), there exist elliptic $\mathbb{F}_{q^2}$-maximal curves for any q. In particular, $d_2(q) = 3$ is sharp for $q = 3$.

(iii) From [33, Sec. 4], there exists a plane quartic $\mathbb{F}_{25}$-maximal curve, so $d_2(q) = 4$ is sharp for $q = 5$.

(iv) By part (ii), $d_2(q) = 3$ is sharp for $q = 4$. For $q \ge 8$, q even, no information is currently available to assess how good the bound $d_2(q) = (q+2)/2$ is.

We go on to look for an upper bound for the degree d of an $\mathbb{F}_{q^2}$-maximal curve satisfying the condition $d < \lfloor (q+2)/2 \rfloor$. Our approach is inspired by [6, Sec. 3] where the $\mathbb{F}_{q^2}$-Frobenius divisor S_2 associated with the linear series Σ_2 cut out on $\mathcal{X}$ by conics was employed to obtain upper bounds for the number of $\mathbb{F}_{q^2}$-rational points of plane curves. In fact, if we use Σ_2 instead of Σ_1, we can get better results for values for d ranging in certain intervals depending on q. This was pointed out for the first time in [17].

In order to compute the Σ_2-orders of a plane $\mathbb{F}_{q^2}$-maximal curve $\mathcal{X}$, one needs to know whether $\mathcal{X}$ is classical or not with respect to Σ_1. This gives the motivation to Proposition 2.6. The following remark will be useful in the proof.

REMARK 2.5. (i) If a projective, geometrically irreducible, non-singular, algebraic curve defined over a field of characteristic $p > 0$ admits a linear series Σ of degree D, then Σ is classical provided that $p > D$; see [36, Cor. 1.8].

(ii) If a non-singular plane curve of degree D defined over a field of characteristic $p > 0$ is non-classical with respect to the linear series cut out by lines, then $D \equiv 1 \pmod{p}$; see [30, Cor. 2.2], and [24, Cor. 2.4].

PROPOSITION 2.6. *Let $\mathcal{X}$ be a plane $\mathbb{F}_{q^2}$-maximal curve of degree d such that $3 \le d \le d_2(q)$, where $d_2(q)$ is as in Corollary* 2.3. *Then the linear series Σ_1 on $\mathcal{X}$ is classical provided that one of the following conditions holds*:

(i) $p > d$ *or* $d \not\equiv 1 \pmod{p}$;
(ii) $q = 4, 8, 16, 32$;

(iii) $p \geq 3$ *and either* $q = p$ *or* $q = p^2$;

(iv) $p = 2$, $q \geq 64$, *and either* $d \leq 4$, *or* $d \geq d_3(q) := q/4 - 1$ *for* $q = 64, 128, 256$, *or* $d \geq d_3(q) := q/4$ *for* $q \geq 512$;

(v) $p \geq 3$, $q = p^v$ *with* $v \geq 3$, *and* $d \geq d_3(q) := q/p - p + 2$.

Proof. If (i) holds, then Σ_1 is classical by Remark 2.5. For $q = p$, the hypothesis on d yields $p \geq 3$ and hence $d \leq (p+1)/2 < p$. Thus Σ_1 is classical by Remark 2.5(i). Note that the following computations will provide another proof of this fact.

For the rest of the proof we assume Σ_1 to be non-classical, and we show that no one of the conditions (i)–(v) holds. From Lemma 2.1(3), $\varepsilon_2 \geq M$, where $M = 4$ for $p = 2$, and $M = p$ for $p \geq 3$. Also, $\nu_1 = 1$ by Proposition 2.2. Therefore, as $j_2(P) \geq \varepsilon_2$ for each $P \in \mathcal{X}$ [36, p. 5], from [36, Prop. 2.4(a)] we deduce that $v_P(S_1) \geq M$ for each $P \in \mathcal{X}(\mathbb{F}_{q^2})$, where as before S_1 denotes the $\mathbb{F}_{q^2}$-Frobenius divisor associated with Σ_1. Thus,

$$\deg(S_1) = (2g-2) + (q^2+2)d \geq M\#\mathcal{X}(\mathbb{F}_{q^2}) = M(q+1)^2 + Mq(2g-2),$$

or, equivalently,

$$(Mq-1)d^2 - (q^2 + 3Mq - 1)d + M(q+1)^2 \leq 0.$$

On the other hand, the discriminant of the above quadratic polynomial in d is

$$\Delta_M(q) := q^4 - (4M^2 - 6M)q^3 + (M^2 + 4M - 2)q^2 - (4M^2 - 2M)q + 4M + 1,$$

and hence $\Delta_M(q) < 0$ if and only if either $q = 4, 8, 16, 32$ and $M = 4$, or $q = p, p^2$ and $M = p \geq 3$. For these q's, the above inequality cannot actually hold, and hence Σ_1 must be classical. Furthermore, if $\Delta_M(q) \geq 0$, then

$$F'(M,q) := \frac{q^2 + 3Mq - 1 - \sqrt{\Delta_M(q)}}{2(Mq-1)} \leq d \leq F(M,q) := \frac{q^2 + 3Mq - 1 + \sqrt{\Delta_M(q)}}{2(Mq-1)}.$$

It is easy to check that $F'(4,q) > 4$, $F(4,q) < q/4 - 1$ for $q = 64, 128, 256$, and that $F(4,q) < q/4$ for $q \geq 512$; hence if (iv) holds, then Σ_1 must be classical. Let $p \geq 3$. If $q/p - p + 2 \leq d \leq q/p$, then Σ_1 must be classical by (i). So we can suppose that $d \geq q/p + 1$. It turns out that $F(p,q) < q/p + 1$ and hence the result follows when (v) is assumed to be true. ∎

Remark 2.7. For $q = p^3$, $p \geq 3$, the bound $d_3(q)$ in Proposition 2.6 is sharp. Indeed, there exists a plane $\mathbb{F}_{p^6}$-maximal curve of degree $p^2 - p + 1$ which is non-classical for Σ_1 (see Corollary 3.3 and Remark 3.11).

Corollary 2.8. *Let* $\mathcal{X}$ *be a plane* $\mathbb{F}_{q^2}$*-maximal curve of degree* d *as in Proposition* 2.6. *Assume that* $\mathcal{X}$ *is non-classical for* Σ_1 *and let* ε_2 *be the*

order of contact of $\mathcal{X}$ with the tangent at a general point. Then

(1) $q \geq 64$ *if* $p = 2$, *and* $q \geq p^3$ *for* $p \geq 3$;
(2) $\varepsilon_2^2 \leq q/p$.

Proof. Part (1) follows from Proposition 2.6(ii)(iii). To prove (2), we first note that $\varepsilon_2 < q$ (cf. Proposition 2.2), and that ε_2 is a power of p (see Lemma 2.1(3)). Now, with the same notation as in the proof of the previous proposition, we get $d \leq F(M, q)$ with $M = \varepsilon_2$. So $d \leq q/\varepsilon_2$. Furthermore, $d \geq \varepsilon_2$ and so $d \geq \varepsilon_2 + 1$ by Remark 2.5(ii). Hence $\varepsilon_2 + 1 \leq q/\varepsilon_2$ and part (2) follows. ∎

REMARK 2.9. The example in Remark 2.7 shows that Corollary 2.8(1) is sharp for $p \geq 3$.

Our next step is to show that every plane $\mathbb{F}_{q^2}$-maximal curve which is classical for Σ_1 contains an $\mathbb{F}_{q^2}$-rational point different from its inflexions.

LEMMA 2.10. *Let $\mathcal{X}$ be an $\mathbb{F}_{q^2}$-maximal curve of degree $d \geq 3$ which is classical with respect to Σ_1. Then there exists $P_0 \in \mathcal{X}(\mathbb{F}_{q^2})$ whose (Σ_1, P_0)-orders are $0, 1, 2$.*

Proof. Let R_1 be the ramification divisor associated with Σ_1 and suppose that $j_2(P) \geq 3$ for each $P \in \mathcal{X}(\mathbb{F}_{q^2})$. Then from [36, p. 12],

$$\deg(R_1) = 3(2g-2) + 3d \geq \#\mathcal{X}(\mathbb{F}_{q^2}) = (q+1)^2 + q(2g-2)$$

which is a contradiction as $g \geq 1$ and $3 \leq d < q + 1$. ∎

It should be noticed that Lemma 2.10 improves a previous result (see [6, Cor. 3.2]).

We are in a position to establish some useful properties of the linear series Σ_2 cut out by conics of $\mathbb{P}^2(\overline{\mathbb{F}}_{q^2})$ on the plane $\mathbb{F}_{q^2}$-maximal curve $\mathcal{X}$ of degree $d \geq 3$. Since $\mathcal{X}$ is non-singular, $\Sigma_2 = 2\Sigma_1$. Taking into account $d \geq 3$, we see that Σ_2 is a 5-dimensional linear series of degree $2d$.

LEMMA 2.11. *Let d be the degree of a plane $\mathbb{F}_{q^2}$-maximal curve $\mathcal{X}$. Let $q = 8$ or $q \geq 11$, and suppose that*

$$d_4(q) := \frac{2q^2 + 15q - 20 + \sqrt{4q^4 - 40q^3 + 145q^2 - 300q + 600}}{10(q-2)} < d \leq d_2(q),$$

where $d_2(q)$ is as in Corollary 2.3. Then the orders of Σ_2 (resp. $\mathbb{F}_{q^2}$-Frobenius orders) of Σ_2 are $0, 1, 2, 3, 4, \varepsilon$ (resp. $0, 1, 2, 3, \varepsilon$) with $5 \leq \varepsilon \leq q$. Furthermore, p divides ε.

Proof. By some computations we find that $d_4(q)$ is greater than the $d_3(q)$ of Proposition 2.6. So the curve $\mathcal{X}$ is classical for Σ_1. Let $P_0 \in \mathcal{X}(\mathbb{F}_{q^2})$ be as in Lemma 2.10. Then the (Σ_2, P_0)-orders are $0, 1, 2, 3, 4$ and j_0 with $5 \leq j_0 \leq 2d$ (cf. [16, p. 464]). Therefore, the Σ_2-orders are $0, 1, 2, 3, 4$ and

ε with $5 \le \varepsilon \le j_0$. Since $j_0 \le 2d$, from Corollary 2.3, $\varepsilon \le q+2$, and hence $\varepsilon \le q$ by the p-adic criterion [36, Cor. 1.9]. Also, the $\mathbb{F}_{q^2}$-Frobenius orders of Σ_2 are $0, 1, 2, 3$ and ν with $\nu \in \{4, \varepsilon\}$; see [36, Prop. 2.1, Cor. 2.6]. Suppose that $\nu = 4$ and let S_2 denote the $\mathbb{F}_{q^2}$-Frobenius divisor associated with Σ_2. Then from [36, Thm. 2.13],

$$\deg(S_2) = 10(2g-2) + (q^2+5)2d \ge 5\#\mathcal{X}(\mathbb{F}_{q^2}) = 5(q+1)^2 + 5q(2g-2)$$

or equivalently

$$(5q-10)d^2 - (2q^2+15q-20)d + 5(q+1)^2 \le 0.$$

The discriminant of this equation is $4q^4 - 40q^3 + 145q^2 - 300q + 600$ and it is positive for any q. Since $d_4(q)$ is the greatest root of the quadratic polynomial in d above, $d \le d_4(q)$, a contradiction. Finally, p divides ε by [12, Cor. 3]. ∎

Let $d_4(q)$ be as in Lemma 2.11. Note that $d_4(q)/q \approx 2/5$. For $q = p^v$, $v \ge 2$, set

$$d_4(p,q) = \frac{2q^2 + 3\big(5 - \frac{1}{p}\big)q - 8}{2\big(5 - \frac{1}{p}\big)q - 12} + \frac{\sqrt{4q^4 - 8\big(5 - \frac{1}{p}\big)q^3 + \big(113 - \frac{50}{p} + \frac{9}{p^2}\big)q^2 - 4\big(25 - \frac{17}{p}\big)q + 184}}{2\big(5 - \frac{1}{p}\big)q - 12}.$$

THEOREM 2.12. *Let d be the degree of a plane $\mathbb{F}_{q^2}$-maximal curve $\mathcal{X}$. Suppose that $3 \le d < q+1$ and that $q = 8$ or $q \ge 11$. Then*

$$d \le d_5(q) := \begin{cases} d_4(q) & \text{if } q = p, \\ d_4(p,q) & \text{if } q = p^v,\ v \ge 2, \end{cases} \quad \text{or} \quad d = \lfloor (q+2)/2 \rfloor.$$

Proof. Suppose that $d > d_5(q)$. By means of some computations, $d_4(p,q) > d_4(q)$ and hence Lemma 2.11 holds true. With the same notation as in the proof of that lemma, we can then use the following two facts: $\varepsilon = \nu \le q$, and $p \,|\, \varepsilon$. Actually, we will improve the latter.

CLAIM 1. *ε is a power of p.*

Indeed, by $p \,|\, \varepsilon$ and the p-adic criterion [36, Cor. 1.9], a necessary and sufficient condition for ε not to be a power of p is that $p \in \{2, 3\}$ and $\varepsilon = 6$. If this occurs, one can argue as in the previous proof to obtain

$$(5q-2)d^2 - (q^2+15q-31)d + 5(q+1)^2 \le 0.$$

From this,

$$d \le G(q) := \frac{q^2 + 15q - 31 + \sqrt{q^4 - 70q^3 + 203q^2 - 550q + 1201}}{2(5q-12)},$$

which is a contradiction as $G(q) < d_5(q)$.

CLAIM 2. $\varepsilon = q$.

The claim is certainly true for $q = p$. So, $q = p^v$, with $v \geq 2$. If $\varepsilon < q$, by Claim 1 we have $\varepsilon \leq q/p$. Together with

$$\deg(S_2) = (6+\nu)(2g-2) + (q^2+5)2d \geq 5\#\mathcal{X}(\mathbb{F}_{q^2}) = 5(q+1)^2 + 5q(2g-2),$$

this would yield

$$(5q - q/p - 6)d^2 - (2q^2 + 15q - 3q/p - 8)d + 5(q+1)^2 \leq 0,$$

and hence $d \leq d_4(p,q)$, a contradiction.

Now from Claim 2 and [36, Cor. 2.6], we have

$$q = \varepsilon = \nu \leq j_5(P_0) - 1 \leq 2d - 1,$$

and Theorem 2.12 follows from Corollary 2.3. ∎

REMARK 2.13. The referee asked about the existence of plane $\mathbb{F}_{q^2}$-maximal curves of degree d such that $(q+1)/3 < d < (q+1)/2$, q odd and large enough. According to Theorem 2.12, we have $d_5(q) \approx 2q/5$ for q large enough. For the existence problem of plane $\mathbb{F}_{q^2}$-maximal curves of degree d with $(q+1)/3 < d < d_5(q)$ for q large enough, the arguments in the previous two proofs show that such a curve $\mathcal{X}$ is Frobenius non-classical with respect to $\Sigma_3 = 3\Sigma_1$. In fact, if S_3 denotes the $\mathbb{F}_{q^2}$-Frobenius divisor associated with Σ_3 and $\mathcal{X}$ is assumed to be $\mathbb{F}_{q^2}$-Frobenius classical, from [36, Thm. 2.13] we have

$$\deg(S_3) = 36(2g-2) + (q^2+9)3d \geq \#\mathcal{X}(\mathbb{F}_{q^2}) = 9(q+1)^2 + 9q(2g-2),$$

whence $d \approx q/3$ for q large enough. In contrast, if $\mathcal{X}$ is an $\mathbb{F}_{q^2}$-Frobenius non-classical curve with respect to Σ_3, then the coefficient 36 must be replaced by a term depending on d, and the previous result $d \approx q/3$ does not follow any longer. To work out properly what happens in this situation, one should apply an estimate better than [36, Thm. 2.13]. Unfortunately, no such estimate is currently available in the literature.

3. Maximal Hurwitz's curves. In this section we give a necessary and sufficient condition for q in order that the Hurwitz curve $\mathcal{X}_n$ defined by (1.2) be $\mathbb{F}_{q^2}$-maximal.

THEOREM 3.1. *The curve $\mathcal{X}_n$ is $\mathbb{F}_{q^2}$-maximal if and only if* (1.3) *holds.*

We first prove two lemmas.

LEMMA 3.2 ([4, p. 210]). *The Hurwitz curve $\mathcal{X}_n$ is $\mathbb{F}_p$-covered by the Fermat curve*

$$\mathcal{F}_{n^2-n+1}: \quad U^{n^2-n+1} + V^{n^2-n+1} + W^{n^2-n+1} = 0.$$

Proof. Let $u = U/W$ and $v := V/W$. Then the image of the morphism $(u : v : 1) \to (x : y : 1) = (u^n v^{-1} : uv^{n-1} : 1)$ is the curve defined by $x^n y + y^n + x = 0$. This proves the lemma. ∎

COROLLARY 3.3. *Suppose that* (1.3) *holds. Then both curves* $\mathcal{X}_n$ *and* $\mathcal{F}_{n^2-n+1}$ *are* $\mathbb{F}_{q^2}$*-covered by the Hermitian curve of equation* (1.1)*. In particular, both are* $\mathbb{F}_{q^2}$*-maximal.*

Proof. If (1.3) holds, it is clear that $\mathcal{F}_{n^2-n+1}$ is $\mathbb{F}_{q^2}$-covered by the Hermitian curve. This property extends to $\mathcal{X}_n$ via the previous lemma. For both curves, the $\mathbb{F}_{q^2}$-maximality now follows from [27, Prop. 6]. ∎

LEMMA 3.4 ([5, p. 5249]). *The Weierstrass semigroup of* $\mathcal{X}_n$ *at the point* $(0 : 1 : 0)$ *is generated by the set* $S := \{s(n-1)+1 : s = 1, \dots, n\}$.

Proof. Let $P_0 := (1 : 0 : 0)$, $P_1 = (0 : 1 : 0)$, and $P_2 = (0 : 0 : 1)$. Then

$$\operatorname{div}(x) = nP_2 - (n-1)P_1 - P_0 \quad \text{and} \quad \operatorname{div}(y) = (n-1)P_0 + P_2 - nP_1$$

so that

$$\operatorname{div}(x^{s-1}y) = (n(s-1)+1)P_2 + (n-s)P_0 - (s(n-1)+1)P_1.$$

This shows that S is contained in the Weierstrass semigroup $H(P_1)$ at P_1. In particular, $H(P_1) \supseteq \langle S \rangle$. Since $\#(\mathbb{N}_0 \setminus \langle S \rangle) = n(n-1)/2$ (see [20]), the result follows. ∎

Proof of Theorem 3.1. If (1.3) holds, then $\mathcal{X}_n$ is $\mathbb{F}_{q^2}$-maximal by Corollary 3.3. Conversely, assume that $\mathcal{X}_n$ is $\mathbb{F}_{q^2}$-maximal. Then $(q+1)P_1 \sim (q+1)P_2$ [32, Lemma 1], and the case $s = n$ in the proof of Lemma 3.4 gives $(n^2-n+1)P_1 \sim (n^2-n+1)P_2$. Therefore $d := \gcd(n^2-n+1, q+1)$ belongs to $H(P_1)$. According to Lemma 3.4 we have $d = A(n-1)+B$ with $A \geq B \geq 1$. Now, there exists $C \geq 1$ such that $(A(n-1)+B)C = n^2 - n + 1$ and so $BC = D(n-1)+1$ for some $D \geq 0$. Therefore, $AD(n-1) + A + BD = Bn$. We claim that $D = 0$, otherwise the left side of the last equality would be greater than Bn. Then $B = C = 1$ and so $A = n$; i.e., $d = n^2 - n + 1$ and the proof is complete.

COROLLARY 3.5. *The curve* $\mathcal{F}_{n^2-n+1}$ *in Lemma* 3.2 *is* $\mathbb{F}_{q^2}$*-maximal if and only if* (1.3) *holds.*

Proof. If (1.3) is satisfied, the result follows from Corollary 3.3. Now if $\mathcal{F}_{n^2-n+1}$ is $\mathbb{F}_{q^2}$-maximal, then $\mathcal{X}_n$ is also $\mathbb{F}_{q^2}$-maximal by Lemma 3.2 and [27, Prop. 6]. Then the corollary follows from Theorem 3.1. ∎

REMARK 3.6. For a given positive integer n, we are led to look for a power q of a prime p such that $q+1 \equiv 0 \pmod{m}$ with $m = n^2-n+1$. Since $m \not\equiv 0 \pmod{p}$, and $p \not\equiv 0 \pmod{m}$, a necessary and sufficient condition for q to have the required property (1.3) is $p \equiv x \pmod{m}$, where x is a solution

of the congruence $X^w + 1 \equiv 0 \pmod m$, and w is defined by $q = p^{\phi(m)v+w}$, $w \in \{1, \dots, \phi(m) - 1\}$; here ϕ denotes the Euler function.

Regarding specific examples, we notice that Carbonne and Hénocq [4, Lemmes 3.3, 3.6] pointed out that $\mathcal{X}_n$ is $\mathbb{F}_{q^2}$-maximal in the following cases:

(1) $n = 3$, $q = p^{6v+3}$ and $p \equiv 3, 5 \pmod 7$;
(2) $n = 4$, $q = p^{12v+6}$ and $p \equiv 2, 6, 7, 11 \pmod{13}$.

By using Theorem 3.1 and Remark 3.6 we have the following result.

COROLLARY 3.7. (1) *The curve $\mathcal{X}_2$ is $\mathbb{F}_{q^2}$-maximal if and only if $q = p^{2v+1}$ and $p \equiv 2 \pmod 3$.*

(2) *The curve $\mathcal{X}_3$ is $\mathbb{F}_{q^2}$-maximal if and only if either $q = p^{6v+1}$ and $p \equiv 6 \pmod 7$, or $q = p^{6v+3}$ and $p \equiv 3, 5, 6 \pmod 7$, or $q = p^{6v+5}$ and $p \equiv 6 \pmod 7$.*

(3) *The curve $\mathcal{X}_4$ is $\mathbb{F}_{q^2}$-maximal if and only if either $q = p^{12v+1}$ and $p \equiv 12 \pmod{13}$, or $q = p^{12v+2}$ and $p \equiv 5, 8 \pmod{13}$, or $q = p^{12v+3}$ and $p \equiv 4, 10, 12 \pmod{13}$, or $q = p^{12v+5}$ and $p \equiv 12 \pmod{13}$, or $q = p^{12v+6}$ and $p \equiv 2, 5, 6, 7, 8, 11 \pmod{13}$, or $q = p^{12v+7}$ and $p \equiv 12 \pmod{13}$, or $q = p^{12v+9}$ and $p \equiv 4, 10, 12 \pmod{13}$, or $q = p^{12v+11}$ and $p \equiv 12 \pmod{13}$.*

COROLLARY 3.8. *Let n be a positive integer, $m := n^2 - n + 1$ and p a prime.*

(1) *If $n = p^e$ with $e \geq 1$, then the curve $\mathcal{X}_n$ is $\mathbb{F}_{q^2}$-maximal with $q = p^{\phi(m)v+3e}$.*

(2) *Let $p \equiv 3 \pmod 4$ and $n \equiv 0, 1 \pmod p$ be such that m is prime and $m \equiv 3 \pmod 4$. Then $\mathcal{X}_n$ is $\mathbb{F}_{q^2}$-maximal with $q = p^{(m-1)v+(m-1)/2}$.*

Proof. Part (1) follows from the identity $p^{3e} + 1 = (p^e + 1)(p^{2e} - p^e + 1)$ and Theorem 3.1.

To show (2), it is enough to check that $p^{(m-1)/2} + 1 \equiv 0 \pmod m$. Recall that the Legendre symbol (a/p) is defined by

$$(a/p) = \begin{cases} 1 & \text{if } x^2 \equiv a \pmod p \text{ has two solutions in } \mathbb{Z}_p, \\ -1 & \text{if } x^2 \equiv a \pmod p \text{ has no solution in } \mathbb{Z}_p. \end{cases}$$

In our case, since $m \equiv 1 \pmod p$, we have $(m/p) = 1$. By the quadratic reciprocity law

$$(m/p)(p/m) = (-1)^{((m-1)/2)((p-1)/2)},$$

from $(m/p) = 1$ and $m \equiv 3 \pmod 4$ we get $(p/m) = (-1)^{(p-1)/2}$. Now, as $p \equiv 3 \pmod 4$, we have $(p/m) = -1$. In other words, p viewed as an element in $\mathbb{F}_m$ is a non-square in $\mathbb{F}_m$. Since -1 is also a non-square in $\mathbb{F}_m$, it follows that $p \equiv (-1)u^2 \pmod m$ with $u \in \mathbb{Z}$ such that $u \not\equiv 0 \pmod m$. Hence $p^{(m-1)/2} \equiv (-1) \pmod m$ because, in particular, m is odd and $u^{m-1} \equiv 1 \pmod m$. ∎

REMARK 3.9. The hypothesis $m \equiv 3 \pmod 4$ in the above corollary cannot be relaxed. In fact, for $n = 4$ we have $m = 13$ but, according to Corollary 3.7, $\mathcal{X}_4$ is not $\mathbb{F}_{3^6}$-maximal.

REMARK 3.10. Let us assume the hypothesis in Corollary 3.8(2) with m not necessarily prime. In this case, to study the congruence in (1.3) we have to consider the multiplicative group Φ_m of units in $\mathbb{Z}_m$. This group has order $\phi(m)$, and $p \in \Phi_m$ since $m \equiv 1 \pmod p$. Now suppose that p, as an element of Φ_m, has even order $2i$. Then $p^{2i} \equiv 1 \pmod m$ and hence $(p^i + 1)(p^i - 1) \equiv 0 \pmod m$. Since p has order greater than i, we have $p^i - 1 \not\equiv 0 \pmod m$ unless both $p^i + 1$ and $p^i - 1$ are zero divisors in $\mathbb{Z}_m$. If we assume that this does not happen, then equivalence (1.3) follows for $q = p^{\phi(m)v+i}$.

REMARK 3.11. Let p be a prime, $n := p^e u$ with $e \geq 1$ and $\gcd(p, u) = 1$. Assume $e \geq 2$ if $p = 2$. Then the Hurwitz curve $\mathcal{X}_n$ as well as the curve $\mathcal{F}_{n^2-n+1}$ are non-classical with respect to Σ_1. It is easy to see that $0, 1$ and p^e are their Σ_1-orders.

4. On the maximality of generalized Hurwitz curves. In this section we investigate the $\mathbb{F}_{q^2}$-maximality of the non-singular model of the so-called generalized Hurwitz curve $\mathcal{X}_{n,l}$ of equation

$$X^n Y^l + Y^n Z^l + Z^n X^l = 0,$$

where $n \geq l \geq 2$ and $p = \mathrm{char}(\mathbb{F}_{q^2})$ does not divide $Q(n, l) := n^2 - nl + l^2$. The singular points of $\mathcal{X}_{n,l}$ are $P_0 := (1 : 0 : 0)$, $P_1 = (0 : 1 : 0)$, and $P_2 = (0 : 0 : 1)$; each of them is unibranched with δ-invariant equal to $(nl - n - l + \gcd(n, l))/2$. Therefore its genus g (cf. [3, Sec. 4] and [2, Example 4.5]) is equal to

$$g = \frac{n^2 - nl + l^2 + 2 - 3\gcd(n, l)}{2}.$$

First we generalize Lemma 3.2.

LEMMA 4.1. *The curve $\mathcal{X}_{n,l}$ is $\mathbb{F}_{q^2}$-covered by the Fermat curve*

$$\mathcal{F}_{n^2-nl+l^2} : \quad U^{n^2-nl+l^2} + V^{n^2-nl+l^2} + W^{n^2-nl+l^2} = 0.$$

Proof. The curve $\mathcal{X}_{n,l}$ is $\mathbb{F}_{q^2}$-covered by $\mathcal{F}_{n^2-nl+l^2}$ via the morphism $(u : v : 1) \to (x : y : 1) := (u^n v^{-m} : u^m v^{n-m} : 1)$, where $u := U/W$ and $v := V/W$. ∎

From this lemma and [27, Prop. 6] we have the following.

COROLLARY 4.2. *The curve $\mathcal{F}_{n^2-nl+l^2}$ in the above lemma and the $\mathbb{F}_{q^2}$-non-singular model of $\mathcal{X}_{n,l}$ are $\mathbb{F}_{q^2}$-maximal provided that*

$$n^2 - nl + l^2 \equiv 0 \pmod{(q + 1)}. \tag{4.1}$$

Now, we generalize Lemma 3.4 for any two coprime n and l. For $0 \le i \le 2$, let Q_i be the unique point in the non-singular model of $\mathcal{X}_{n,l}$ lying over P_i.

LEMMA 4.3. *Suppose that* $\gcd(n,l) = 1$. *Then the Weierstrass semigroup* $H(Q_1)$ *at* Q_1 *is given by*

$$\left\{(n-l)s + nt : s,t \in \mathbb{Z};\ t \ge 0 - \frac{l}{n}t \le s \le \frac{n-l}{l}t\right\}. \tag{4.2}$$

Proof. Let $x := X/Z, y := Y/Z$. It is not difficult to see that $\mathrm{div}(x) = nQ_2 - (n-l)Q_1 - lQ_0$ and $\mathrm{div}(y) = (n-l)Q_0 + lQ_2 - nQ_1$. Hence, for $s,t \in \mathbb{Z}$,

$$\mathrm{div}(x^s y^t) = (ns+lt)Q_2 + (-ls+(n-l)t)Q_0 - ((n-l)s+nt)Q_1,$$

and hence $(n-l)s+nt \in H(Q_1)$ provided that $ns+lt \ge 0$ and $-ls+(n-l)t \ge 0$. Let H denote the set introduced in (4.2). Then $H \subseteq H(Q_1)$, and it is easily checked that H is a semigroup. By means of some computations we see that $\#(\mathbb{N} \setminus H) = (n^2 - nl + l^2 - 1)/2$, whence $H = H(Q_1)$ follows. ∎

REMARK 4.4. The above Weierstrass semigroup $H(Q_1)$ was computed for $l = n-1$, and $(n,l) = (5,2)$ in [3].

We are able to generalize Theorem 3.1 for certain curves $\mathcal{X}_{n,l}$.

THEOREM 4.5. *Assume that* $\gcd(n,l) = 1$ *and* $Q := Q(n,l) = n^2 - nl + l^2$ *is prime. Then* $\mathcal{X}_{n,l}$ *is* $\mathbb{F}_{q^2}$*-maximal if and only if* (4.1) *holds.*

Proof. The "if" part follows from Corollary 4.2 and here we do not use the hypothesis that Q is prime. For the "only if" part, we first notice that each Q_i is $\mathbb{F}_{q^2}$-rational. Now the case $s = n-m$ and $t = m$ in the proof of Lemma 4.3 gives $QQ_2 \sim QQ_1$. Therefore $d = \gcd(Q, q+1) \in H(Q_1)$ because $(q+1)Q_1 \sim (q+1)Q_2$ [32, Lemma 1]. As $1 \notin H(Q_1)$ and Q is prime, the result follows. ∎

COROLLARY 4.6. *Let* n, l *and* Q *be as in Theorem* 4.5. *Then the curve* $\mathcal{F}_{n^2-nl+l^2}$ *in Lemma* 4.1 *is* $\mathbb{F}_{q^2}$*-maximal if and only if* (4.1) *holds.*

Proof. Similar to the proof of Corollary 3.5. ∎

REMARK 4.7. There are infinitely many n, l with $n > l \ge 1$ such that $Q(n,l)$ is prime. In fact, for a prime p' such that $p' \equiv 1 \pmod 6$, there exist such n and l so that $p' = Q(n,l)$ (see [3, Remarque 4]).

References

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

[2] P. Beelen and R. Pellikaan, *The Newton polygon of plane curves with many rational points*, Des. Codes Cryptogr. 21 (2000), 41–67.

[3] H. Bennama et P. Carbonne, *Courbes $X^mY^n+Y^mZ^n+Z^mX^n = 0$ et décomposition de la Jacobienne*, J. Algebra 188 (1997), 409–417.

[4] P. Carbonne et T. Hénocq, *Décomposition de la Jacobienne sur les corps finis*, Bull. Polish Acad. Sci. Math. 42 (1994), 207–215.

[5] P. Carbonne, T. Hénocq et F. Rigal, *Points de Weierstrass de deux familles de courbes*, Comm. Algebra 27 (1999), 5235–5254.

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

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

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

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

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

[11] —, —, *On Weierstrass points and optimal curves*, Rend. Circ. Mat. Palermo Suppl. 51 (1998), 25–46.

[12] A. Garcia and M. Homma, *Frobenius order-sequences of curves*, in: Algebra and Number Theory, G. Frey and J. Ritter (eds.), de Gruyter, Berlin, 1994, 27–41.

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

[14] A. Garcia and F. Torres, *On maximal curves having classical Weierstrass gaps*, in: Applications of Curves over Finite Fields, M. D. Fried (ed.), Contemp. Math. 245, Amer. Math. Soc., 1999, 49–59.

[15] A. Garcia and P. Viana, *Weierstrass points on certain non-classical curves*, Arch. Math. (Basel) 46 (1986), 315–322.

[16] A. Garcia and J. F. Voloch, *Wronskians and linear independence in fields of prime characteristic*, Manuscripta Math. 59 (1987), 457–469.

[17] —, —, *Fermat curves over finite fields*, J. Number Theory 30 (1988), 345–356.

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

[19] V. D. Goppa, *Geometry and Codes*, Math. Appl. 24, Kluwer, Dordrecht, 1988.

[20] D. D. Grant, *On linear forms whose coefficients are in arithmetical progression*, Israel J. Math. 15 (1973), 204–209.

[21] A. Hefez and J. F. Voloch, *Frobenius non classical curves*, Arch. Math. (Basel) 54 (1990), 263–273.

[22] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, 2nd ed., Oxford Univ. Press, Oxford, 1998.

[23] M. Homma, *Funny plane curves in characteristic $p > 0$*, Comm. Algebra 15 (1987), 1469–1501.

[24] —, *A souped-up version of Pardini's theorem and its applications to funny curves*, Compositio Math. 71 (1989), 295–302.

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

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

[27] G. Lachaud, *Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis*, C. R. Acad. Sci. Paris Sér. I 305 (1987), 729–732.
[28] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl. 20, Adisson-Wesley, 1983.
[29] C. J. Moreno, *Algebraic Curves over Finite Fields*, Cambridge Univ. Press, Vol. 97, 1991.
[30] R. Pardini, *Some remarks on plane curves over fields of finite characteristic*, Compositio Math. 60 (1986), 3–17.
[31] R. Pellikaan, *The Klein quartic, the Fano plane and curves representing designs*, in: Codes, Curves and Signals: Common Threads in Communications, A. Vardy (ed.), Kluwer, Dordrecht, 1998, 9–20.
[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] J. P. Serre, *Résumé des cours de 1983–1984*, Ann. Collège France 79–83 (1984); reprinted in Œuvres III, 701–705.
[34] I. E. Shparlinski, *Finite Fields*: *Theory and Computation*, Dordrecht, 1999.
[35] H. Stichtenoth and C. Xing, *The genus of maximal function fields*, Manuscripta Math. 86 (1995), 217–224.
[36] K. O. Stöhr and J. F. Voloch, *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. 52 (1986), 1–19.
[37] E. Ughi, *On the number of points of elliptic curves over a finite field and a problem of B. Segre*, European J. Combin. 4 (1983), 263–270.

Dipartimento di Matematica
e Applicazioni "R. Caccioppoli"
Università di Napoli "Federico II"
80126 Napoli, Italy
E-mail: aguglia@matna2.dma.unina.it

Dipartimento di Matematica
Università di Basilicata
Via N. Sauro 85
85100 Potenza, Italy
E-mail: korchmaros@unibas.it

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

Received on 10.4.2000
and in revised form on 28.6.2000 (3801)