ON THE GENUS OF A MAXIMAL CURVE

GÁBOR KORCHMÁROS AND FERNANDO TORRES

ABSTRACT. Previous results on genera g of $\mathbf{F}_{q^2}$-maximal curves are improved:

(1) Either $g \le \lfloor (q^2-q+4)/6 \rfloor$, or $g = \lfloor (q-1)^2/4 \rfloor$, or $g = q(q-1)/2$.
(2) The hypothesis on the existence of a particular Weierstrass point in [2] is proved.
(3) For $q \equiv 1 \pmod 3$, $q \ge 13$, no $\mathbf{F}_{q^2}$-maximal curve of genus $(q-1)(q-2)/6$ exists.
(4) For $q \equiv 2 \pmod 3$, $q \ge 11$, the non-singular $\mathbf{F}_{q^2}$-model of the plane curve of equation $y^q + y = x^{(q+1)/3}$ is the unique $\mathbf{F}_{q^2}$-maximal curve of genus $g = (q-1)(q-2)/6$.
(5) Assume $\dim(\mathcal{D}_{\mathcal{X}}) = 5$, and $\mathrm{char}(\mathbf{F}_{q^2}) \ge 5$. For $q \equiv 1 \pmod 4$, $q \ge 17$, the Fermat curve of equation $x^{(q+1)/2} + y^{(q+1)/2} + 1 = 0$ is the unique $\mathbf{F}_{q^2}$-maximal curve of genus $g = (q-1)(q-3)/8$. For $q \equiv 3 \pmod 4$, $q \ge 19$, there are exactly two $\mathbf{F}_{q^2}$-maximal curves of genus $g = (q-1)(q-3)/8$, namely the above Fermat curve and the non-singular $\mathbf{F}_{q^2}$-model of the plane curve of equation $y^q + y = x^{(q+1)/4}$.

The above results provide some new evidences on maximal curves in connection with Castelnuovo's bound and Halphen's theorem, especially with extremal curves; see for instance the conjecture stated in Introduction.

1. INTRODUCTION

An $\mathbf{F}_{q^2}$-*maximal curve* $\mathcal{X}$ of genus g is defined to be a projective, geometrically irreducible, non-singular algebraic curve defined over $\mathbf{F}_{q^2}$ such that the number of its $\mathbf{F}_{q^2}$-rational points attains the Hasse-Weil upper bound, namely

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

$\mathbf{F}_{q^2}$-maximal curves especially those with large genus are currently investigated also in connection with coding theory and cryptography based on Goppa's method [30, Ch. 4, Sect. 7]. It is well known that $g \le q(q-1)/2$, see [36], and that g reaches this upper limit if and only if $\mathcal{X}$ is $\mathbf{F}_{q^2}$-isomorphic to the Hermitian curve, see [39]. In [16] it is proven that

$$\text{either} \qquad g \le \lfloor (q-1)^2/4 \rfloor\,, \qquad \text{or} \qquad g = q(q-1)/2\,. \tag{1.1}$$

Mathematics Subject Classification (2000): Primary 11G; Secondary 14G.

Key words: Maximal Curves, Linear Series, Castelnuovo's Theorem, Halphen's Theorem.

This research was carried out within the project "Progetto e Realizzazione di un Criptosistema per Telecomunicazioni", POP FESR 1994/99 - II Triennio. The second author was partially support by Cnpq-Brazil, Proc. 300681/97-6. We are indebted to E. Ballico for sending us his paper [5].

For q odd, $g=(q-1)^2/4$ occurs if and only if $\mathcal{X}$ is $\mathbf{F}_{q^2}$-isomorphic to the non-singular model of the plane curve of equation $y^q+y=x^{(q+1)/2}$, see [15, Thm. 3.1]. For q even, a similar result is obtained in [2] under an extra-condition that $\mathcal{X}$ has a particular Weierstrass point: $g=\lfloor (q-1)^2/4\rfloor = q(q-2)/4$ if and only if $\mathcal{X}$ is $\mathbf{F}_{q^2}$-isomorphic to the non-singular model of the plane curve of equation $y^{q/2}+\ldots+y^2+y=x^{q+1}$. These results together with some evidences coming from [12], [13], [21] make it plausible that only few $\mathbf{F}_{q^2}$-maximal curves can have genus close to the upper limit. As a matter of fact, in the range

$$\lfloor (q-1)(q-3)/8\rfloor \le g < \lfloor (q-1)^2/4\rfloor ,$$

only twelve examples up to $\mathbf{F}_{q^2}$-isomorphisms are known to exist and the spectrum of their genera is listed below:

(I) $g=\lfloor (q^2-q+4)/6\rfloor$ for $q\equiv 0,1,2 \pmod 3$, see Remark 3.4;
(II) $g=(q^2-q-2)/6$ for $q\equiv 2 \pmod 3$, see [12, Thm. 6.2] or [21, Thm. 5.1];
(III) $g=\lfloor ((q-1)(q-2)/6\rfloor$ for $q\equiv 0,2 \pmod 3$, see the case $N=4$ in (2.8), and Sect. 4.1;
(IV) $g=\lfloor (q^2-2q+5)/8\rfloor$ for $q\equiv 0,1,3 \pmod 4$, see Remark 4.10;
(V) $g=\lfloor (q-1)(q-3)/8\rfloor$ for $q\equiv 0,1,3 \pmod 4$, see the case $N=5$ in (2.8), and Sect. 4.2.

Theorem 3.1 in this paper together with (1.1) prove the following result, see Corollary 3.3:

(1.2) either $g\le \lfloor (q^2-q+4)/6\rfloor$, or $g=\lfloor (q-1)^2/4\rfloor$, or $g=q(q-1)/2$.

This result is the best possible since the upper bound in (1.2) cannot be improved as it is attained by the curves cited in (I) for every q. In other words the third largest genus of an $\mathbf{F}_{q^2}$-maximal curve equals $g=\lfloor (q^2-q+4)/6\rfloor$ independently of q; by contrast, the fourth largest genus might heavily depend on q. The above examples also show that the gap between the first and second as well as the second and third largest genus is approximately constant times q^2, while the gap between the third and forth is only 1 for $q\equiv 2 \pmod 3$, and at most constant times q for $q\equiv 0 \pmod 3$.

The essential idea of the proof of Theorem 3.1 is to show that every $\mathbf{F}_{q^2}$-maximal curve of genus $g>\lfloor (q^2-q+4)/6\rfloor$ has a non-singular model $\mathcal{X}$ over $\mathbf{F}_{q^2}$ embedded in $\mathbf{P}^3(\bar{\mathbf{F}}_{q^2})$ such that $\mathcal{X}$ has degree $q+1$ and lies on an $\mathbf{F}_{q^2}$-rational quadratic cone $\mathcal{Q}$ whose vertex V belongs to $\mathcal{X}$. This idea will be worked out using the "natural embedding theorem", see [37, Thm. 2.5], together with Weierstrass point theory, Castelnuovo's genus bound, Halphen's theorem and some other tools. Actually, for q even the vertex V is a particular $\mathbf{F}_{q^2}$-rational Weierstrass point of $\mathcal{X}$, since the order-sequence of $\mathcal{X}$ at V (i.e. the possible intersection numbers of $\mathcal{X}$ with hyperplanes at V) turns out to be $(0,1,(q+2)/2,q+1)$. Similarly for q odd, an $\mathbf{F}_{q^2}$-rational Weierstrass point with order-sequence $(0,1,(q+1)/2,q+1)$ is shown to exist. An $\mathbf{F}_{q^2}$-rational point of $\mathcal{X}$

with such a particular order-sequence forces $\mathcal{X}$ to have genus $\lfloor (q-1)^2/4 \rfloor$ as noticed in [37, Remark 2.6(1)]. Then, the already quoted characterization theorems from [15], and [2] will be applied to complete the proof of Theorem 3.1. It should be noted that Theorem 3.1 improves both [17, Prop. 2.5] and the main result in [2].

Curves with genera as in (III) and (V) above turn out be *extremal* in $\mathbf{P}^4(\bar{\mathbf{F}}_{q^2})$ and in $\mathbf{P}^5(\bar{\mathbf{F}}_{q^2})$ respectively, as such genera are Castelnuovo's numbers $c_0(q+1,r)$, $r=4,5$, see (2.1). Extremal curves in zero characteristic have been widely investigated, see, for instance, [4] and the references therein. Several relevant properties of extremal curves are known to hold true in positive characteristic thanks to Rathmann's work [38] (see also [6]). For the present purpose, the key result on extremal curves is Lemma 2.3 stated in Sect. 2.1. Indeed, this lemma together with other results will give both the non-existence of $\mathbf{F}_{q^2}$-maximal curves of genus $(q-1)(q-2)/3$ for $q \equiv 1 \pmod 3$, and a characterization of a $\mathbf{F}_{q^2}$-maximal curve with such a genus for $q \equiv 2 \pmod 3$, $q \geq 11$; see Theorem 4.5. Under two additional hypotheses, namely the curve is naturally embedded in $\mathbf{P}^5(\bar{\mathbf{F}}_{q^2})$ and $\mathrm{char}(\mathbf{F}_{q^2}) \geq 5$, the aforementioned key result will also be an essential ingredient in characterizing $\mathbf{F}_{q^2}$-maximal curves of genus $(q-1)(q-3)/8$ for $q \equiv 1,3 \pmod 4$, $q \geq 11$; see Theorem 4.9. This theorem is related to a previous characterization of plane $\mathbf{F}_{q^2}$-maximal curves of degree $(q+1)/2$ stated in [11]. Also, in view of the results in Sect. 4.1 and [2, Proof of Prop. 2.4], it seems plausible that any two $\mathbf{F}_{q^2}$-maximal curves of genus $q(q-3)/6$ for $q \equiv 0 \pmod 3$ are $\mathbf{F}_{q^2}$-isomorphic. On the contrary, due to the examples in [1, Sect. 5], no similar result for curves of genus $q(q-4)/8$, $q \equiv 0 \pmod 4$ can hold. For a further interesting question related to these matters, see Remark 2.14.

The genera in (I) and (IV) above coincide with Halphen's number $c_1(q+1,r)$, $r=3,4$, see (2.2). Extensions of results around Halphen's theorem from zero characteristic to positive characteristic are also possible again by Rathmann's work [38] and Ballico's paper [5]. Unfortunately, we do not have so far a classification theorem for $\mathbf{F}_{q^2}$-maximal curves with such genera. What we currently know in this direction is that extremal curves lie on special surfaces such as scrolls, see e.g. [4, Ch. III, Thm. 2.5], and that curves with enough large degree and genus equal to Halphen's number are Cohen-Macaulay curves lying on Castelnuovo surfaces, see the main theorem in [10]. These facts together with the general form of the above mentioned "natural embedding theorem" stating that every $\mathbf{F}_{q^2}$-maximal curve is naturally embedded in a high-dimensional projective space over $\mathbf{F}_{q^2}$ as a curve of degree $q+1$ contained in a Hermitian variety of degree $q+1$, see [37, Thm. 3.4], seem to be a good starting point of a classification project for such $\mathbf{F}_{q^2}$-maximal curves.

Finally, we stress that (1.2) provides evidence for the following conjecture.

Conjecture. With notation as in (2.1) and (2.2), there is no $\mathbf{F}_{q^2}$-maximal curve of genus g such that

$$c_1(q+1,r) < g < c_0(q+1,r)\,.$$

2. Background

Our purpose in this section is to recall some results concerning upper bounds on the genus of curves, Weierstrass Point Theory and Frobenius orders as well as some results on maximal curves.

Convention. The word *curve* will mean a projective, geometrically irreducible, non-singular algebraic curve.

2.1. Castelnuovo's genus bound and Halphen's theorem. Throughout this sub-section, $\mathcal{X}$ denotes a curve defined over an algebraically closed field $\mathbf{F}$. Let $\mathcal{D}$ be an r-dimensional, $r \geq 2$, base-point-free linear series of degree d defined on $\mathcal{X}$; $\mathcal{D}$ is assumed to be simple, that is $\mathcal{X}$ is birational to $\pi(\mathcal{X})$, where π denotes a morphism associated to $\mathcal{D}$. Castelnuovo showed that the genus g of $\mathcal{X}$ is upper bounded by a function depending on r and d. More precisely, let ϵ be the unique integer with $0 \leq \epsilon \leq r-2$ and $d-1 \equiv \epsilon \pmod{(r-1)}$, and define Castelnuovo's number $c_0(d,r)$ by

$$c_0(d,r) := \frac{d-1-\epsilon}{2(r-1)}(d-r+\epsilon)\,. \tag{2.1}$$

Lemma 2.1. (Castelnuovo's genus bound for curves in projective spaces, [8], [4, p. 116], [33, IV, Thm. 6.4], [3, Thm. 3.3], [38, Cor. 2.8])

$$g \leq c_0(d,r,\epsilon)\,.$$

Remark 2.2.

$$c_0(d,r,\epsilon) \leq \begin{cases} (d-1-(r-1)/2)^2/2(r-1) & \text{for } r \text{ odd,} \\ (d-1-(r-1)/2)^2 - 1/4)/2(r-1) & \text{for } r \text{ even.} \end{cases}$$

Curves with genus equal to Castelnuovo's number have several remarkable properties; see e.g. [3], [14, Ch. 3], [4, Ch. 3, Sect. 2]. We will use the following one, which is in fact implicitly contained in the proof of Castelnuovo's genus bound taking into account the Riemann-Roch theorem; see e.g. [3, p. 361 and Lemma 3.5].

Lemma 2.3. *Assume $g = c_0(d,r)$, and define ϵ' by $d = m(r-1)+\epsilon'$ with $\epsilon' \in \{2,\ldots,r\}$. If $m \geq 2$., then:*

1. *the dimension of the linear series $2\mathcal{D}$ is $3r-1$;*
2. *there exists a base-point-free $(\epsilon'-2)$-dimensional complete linear series $\mathcal{D}'$ of degree $(\epsilon'-2)(m+1)$ such that $(m-1)\mathcal{D}+\mathcal{D}'$ is the canonical linear series.*

The following theorem going back to Halphen improves Castelnuovo's genus bound for certain curves in $\mathbf{P}^3(\mathbf{F})$.

Lemma 2.4. (Halphen's theorem, [31, Thm. 3.1], [14, Thm. 3.13], [5]) *Assume $d \geq 7$, and $d = 17$ or $d \geq 25$ when $\mathrm{char}(\mathbf{F}) > 0$. If $\mathcal{X}$ is embedded in $\mathbf{P}^3(\mathbf{F})$, then $\mathcal{X}$ lies on a quadric surface provided that*

$$g > c_1(d,3) := \lfloor (d^2 - 3d + 6)/6 \rfloor .$$

Remark 2.5. For a historical account of Halphen's theorem, see [33, p. 349] or Introduction in [31] and [32]. The proof in characteristic 0 due to Eisenbud and Harris [14, Thm. 3.13] depends on the Uniform Position Principle applied to the generic hyperplane section of $\mathcal{X}$, and it still works verbatim in positive characteristic.

Halphen's theorem extends to certain curves in $\mathbf{P}^r(\mathbf{F})$ for $r \geq 4$, and it turns out to be very useful when one looks for a bound $c_\alpha(d,r)$ for the genus of a curve of degree d in $\mathbf{P}^r(\mathbf{F})$ not lying on any irreducible surface of degree less than $r + \alpha - 1$. For our purpose, the smallest case $\alpha = 1$ is needed:

Lemma 2.6. ([14, Thm. 3.22], [38, Cor. 2.8]) *Suppose that $\mathcal{X}$ is a curve in $\mathbf{P}^r(\mathbf{F})$ of degree d and genus g. Assume*

$$d \geq \begin{cases} 36r & \text{if } r \leq 6, \\ 288 & \text{if } r = 7, \\ 2^{r+1} & \text{if } r \geq 8. \end{cases}$$

Then $\mathcal{X}$ lies on a surface of degree less than or equal to $r-1$ provided that

$$g > c_1(d,r) := \frac{d-1-\epsilon_1}{2r}(d - r + \epsilon_1 + 1) + \begin{cases} 0 & \text{if } \epsilon_1 \leq r-2 \\ 1 & \text{if } \epsilon_1 = r-1 \end{cases}, \tag{2.2}$$

where ϵ_1 is the unique integer such that $0 \leq \epsilon_1 \leq r-1$ and $d - 1 \equiv \epsilon_1 \pmod{r}$.

Notice that (2.2) for $r = 3$ coincides with the formula in Lemma 2.4. A full account of results related to Halphen's theorem is found in the already mentioned [14], [31], as well as in [10] and [9].

2.2. Weierstrass Point Theory and Frobenius orders. Our reference in this sub-section is Stöhr-Voloch's paper [41]. Let $\mathcal{X}$ be a curve defined over an algebraically closed field $\mathbf{F}$ of characteristic p, g its genus, and $\mathcal{D}$ an r-dimensional, $r \geq 1$, simple base-point-free linear series of degree d defined on $\mathcal{X}$. The *$(\mathcal{D},P)$-order sequence* of $P \in \mathcal{X}$ is the strictly increasing sequence $j_0(P) = 0 < j_1(P) < \ldots < j_r(P)$ enumerating the set $\{v_P(D) : D \in \mathcal{D}\}$, with $v_P(D)$ being the weight of the divisor D at P, see [41, p. 3]. If π is a morphism associated to $\mathcal{D}$, then

$$\mathcal{D} = \{\pi^*(H) : H \text{ hyperplane in } \mathbf{P}^r(\mathbf{F})\} ,$$

and the $(\mathcal{D}, P)$-order sequence consists of all possible intersection numbers of $\mathcal{X}$ with hyperplanes at P in the usual order whenever $\mathcal{X} \subseteq \mathbf{P}^r(\mathbf{F})$. Furthermore, the $(\mathcal{D}, P)$-order sequence is the same for all but finitely many points [41, pp. 4-6]. and each of the exceptional points is called a $\mathcal{D}$-*Weierstrass point* of $\mathcal{X}$. According to [41, p. 6], there exists a divisor $R = R_{\mathcal{D}}$ on $\mathcal{X}$, the so-called *ramification divisor*, with support consisting of all $\mathcal{D}$-Weierstrass points of $\mathcal{X}$ and degree

$$\deg(R) = \sum_{i=0}^{r} \epsilon_i(2g-2) + (r+1)d\,, \tag{2.3}$$

where $\epsilon_0 = 0 < \epsilon_1 = 1 < \ldots < \epsilon_r$ is the $\mathcal{D}$-*order sequence* of $\mathcal{X}$, that is the $(\mathcal{D}, P)$-order sequence at a general (i.e. a non $\mathcal{D}$-Weierstrass) point $P \in \mathcal{X}$. It should be noted that the well known *Weierstrass points of* $\mathcal{X}$ appear in this context as the Weierstrass points of the canonical linear series on $\mathcal{X}$ in which case

$$H(P) := \mathbf{N}_0 \setminus \{j_i(P) + 1 : i = 0, \ldots, g-1\}$$

is a numerical semigroup whose elements are called *Weierstrass non-gaps* at P. The strictly increasing sequence enumerating $H(P)$ is usually denoted by $(m_i(P) : i = 0, 1, \ldots)$.

A general rule to compute the $(\mathcal{D}, P)$-orders and $v_P(R)$ is given by the following lemma.

Lemma 2.7. ([41, p. 5, Thm. 1.5])

(1) $j_i(P) \geq \epsilon_i$ *for each* P *and each* i;
(2) $v_P(R) \geq \sum_{i=0}^{r}(j_i(P) - \epsilon_i)$, *and equality holds if and only if* $\det(\binom{j_i(P)}{\epsilon_k}) \not\equiv 0 \pmod{p}$.

To every point $P \in \mathcal{X}$ there is attached the flag of osculating subspaces of $\mathbf{P}^r(\mathbf{F})$ relative to a morphism π associated to $\mathcal{D}$. For each i, $0 \leq i \leq r-1$, the *ith osculating space* $L_i(P)$ of $\mathcal{X}$ at P (with respect to π) is the i-dimensional subspace in $\mathbf{P}^r(\mathbf{F})$ defined as the intersection of all hyperplanes H in $\mathbf{P}^r(\mathbf{F})$ satisfying $v_P(\pi^*(H)) \geq j_{i+1}(P)$. Clearly, $L_0(P) = \{\pi(P)\} \subseteq L_1(P) \subseteq \ldots \subseteq L_{r-1}(P)$. Also, $L_i(P)$ is uniquely determined by $\mathcal{D}$ up to projective equivalence because any two morphisms associated to $\mathcal{D}$ are projectively equivalent. We will refer to $L_1(P)$ and $L_{r-1}(P)$ as the *tangent line* and *osculating hyperplane* of $\mathcal{X}$ at P, respectively.

Lemma 2.8. ([41, Proof of Thm. 1.1]) *Let* H *be a hyperplane in* $\mathbf{P}^r(\mathbf{F})$, *and* $i \in \{0, \ldots, r-1\}$. *Then* $H \supseteq L_i(P)$ *if and only if* $v_P(\pi^*(H)) \geq j_{i+1}(P)$.

In the case where $\mathbf{F}$ is the algebraic closure of a finite field $\mathbf{F}_\ell$ with ℓ elements, and both $\mathcal{X}$ and $\mathcal{D}$ are defined over $\mathbf{F}_\ell$, one can also define the so-called $\mathbf{F}_\ell$-*Frobenius divisor* $S = S_{\mathcal{D},\ell}$ associated do $\mathcal{D}$, see [41, p. 9], whose degree is given by

$$\deg(S) = \sum_{i=0}^{r-1} \nu_i(2g-2) + (\ell + r)d\,, \tag{2.4}$$

where $\nu = 0 < \ldots < \nu_{r-1}$ is a suitable subsequence of the $\mathcal{D}$-order sequence [41, Prop. 2.1].

Lemma 2.9. ([41, Prop. 2.4(a), Cor. 2.6])

$$v_P(S) \geq \sum_{i=1}^{r} (j_i(P) - \nu_{i-1})$$

provided that $P \in \mathcal{X}(\mathbf{F}_\ell)$. *In particular* $\mathcal{X}(\mathbf{F}_\ell) \subseteq \mathrm{Supp}(S)$.

2.3. $\mathbf{F}_{q^2}$-maximal curves. Throughout this sub-section, $\mathcal{X}$ denotes an $\mathbf{F}_{q^2}$-maximal curve of genus g. Whenever concepts and results apply from previous sub-sections, the field $\mathbf{F}$ will be the algebraic closure $\bar{\mathbf{F}}_{q^2}$ of $\mathbf{F}_{q^2}$. A deep result depending on the zeta function is the so-called Fundamental Equivalence on divisors [15, Cor.1.2]:

$$qP + \mathbf{Fr}_{\mathcal{X}}(P) \sim (q+1)Q\,, \qquad P \in \mathcal{X}\,, \quad Q \in \mathcal{X}(\mathbf{F}_{q^2})\,, \tag{2.5}$$

where $\mathbf{Fr}_{\mathcal{X}}$ denotes the Frobenius morphism on $\mathcal{X}$ relative to $\mathbf{F}_{q^2}$. As a consequence, $\mathcal{X}$ is equipped with the base-point-free linear series

$$\mathcal{D}_{\mathcal{X}} := |(q+1)P_0|\,, \qquad P_0 \in \mathcal{X}(\mathbf{F}_{q^2}),$$

which is independent of the choice of the point P_0 in $\mathcal{X}(\mathbf{F}_{q^2})$, and has projective dimension $\dim(\mathcal{D}_{\mathcal{X}})$ at least 2. Note that (2.5) is equivalent to

$$\pi^*(L_{r-1}(P)) = qP + \mathbf{Fr}_{\mathcal{X}}(P)\,, \tag{2.6}$$

π being a morphism associated to $\mathcal{D}_{\mathcal{X}}$. Set $N := \dim(\mathcal{D}_{\mathcal{X}})$. The following result shows that $\mathcal{X}$ has a non-singular model over $\mathbf{F}_{q^2}$ given by a curve in $\mathbf{P}^N(\bar{\mathbf{F}}_{q^2})$ of degree $q+1$.

Lemma 2.10. (Natural embedding theorem, [37, Thm. 2.5], [15, Prop. 1.9]) *The linear series* $\mathcal{D}_{\mathcal{X}}$ *is very ample; i.e. any morphism associated to* $\mathcal{D}_{\mathcal{X}}$ *is a close embedding. Equivalently,* q *is a Weierstrass non-gap at any point of* $\mathcal{X}$.

The natural embedding theorem together with Castelnuovo's genus bound (Lemma 2.1) and its corollary stated in Remark 2.2 provide a very useful upper bound on the genus g of $\mathbf{F}_{q^2}$-maximal curves, namely

$$g \leq \begin{cases} (q-(N-1)/2)^2/2(N-1) & \text{for odd } N, \\ (q-(N-1)/2)^2 - 1/4)/2(N-1) & \text{for even } N. \end{cases} \tag{2.7}$$

Corollary 2.11. (1) ([36]) $g \leq q(q-1)/2$;
(2) ([40, Prop. 3]) *If* $\dim(\mathcal{D}_{\mathcal{X}}) \geq 3$, *then* $g \leq (q-1)^2/4$;

We point out that Lemma 2.10 together with Corollary 2.11 yields the following lemma that strengthens the Rück-Stichtenoth's characterization of the Hermitian curve [39]

Lemma 2.12. ([17, Thm. 2.4]) *For a $\mathbf{F}_{q^2}$-maximal curve $\mathcal{X}$ of genus g, the following statements are equivalent:*

(1) $g > (q-1)^2/4$;
(2) $\dim(\mathcal{D}_{\mathcal{X}}) = 2$;
(3) $\mathcal{X}$ *is* $\mathbf{F}_{q^2}$*-isomorphic to the Hermitian curve of equation* $Y^qZ + YZ^q = X^{q+1}$;
(4) $g = q(q-1)/2$.

As a consequence, we have the following result

Corollary 2.13. ([16]) *The genus g of a $\mathbf{F}_{q^2}$-maximal curve satisfies either*

$$g \le \lfloor (q-1)^2/4 \rfloor \qquad or \qquad g = q(q-1)/2\,.$$

Remark 2.14. Castelnuovo's number $c_0(q+1,N)$ in (2.1) is attained by an $\mathbf{F}_{q^2}$-maximal curve in the cases $q \equiv N-2, 0 \pmod{(N-1)}$. The existence of such a curve $\mathcal{X}$ is strongly related to the existence of a point $P_1 \in \mathcal{X}(\mathbf{F}_{q^2})$ such that m is a Weierstrass non-gap at P_1 satisfying $m(N-1) \le q+1$ $(*)$. Since $m_N(P_1) = q+1$ and $m_{N-1}(P_1) = q$ by Lemma 2.15(2), if m is a Weierstrass non-gap at P_1, then m must satisfy $m(N-1) \ge q$. Hence, property $(*)$ occurs when either $m(N-1) = q+1$ $(*_1)$ or $m(N-1) = q$ $(*_2)$. The smallest possibilities for N are investigated in the sequel, namely $N = 3$ in Sect. 3 while $N \in \{4,5\}$ in Sect. 4.

In case $(*_1)$, $g = c_0(q+1,N) = (q-1)((q+1)/(N-1)-1)/2$ by [37, Remark 2.6(1)]. There exists just one $\mathbf{F}_{q^2}$-maximal curve (up to $\mathbf{F}_{q^2}$-isomorphism) satisfying $(*_1)$, namely the non-singular $\mathbf{F}_{q^2}$-model of the plane curve of equation $y^q + y = x^{(q+1)/(N-1)}$ [15, Thm. 2.3].

In case $(*_2)$, $g = c_0(q+1,N) = q(q-(N-1))/2(N-1)$ by [37, Remark 2.6(1)]. van der Geer and van der Vlugt, see [26, Thm. 3.1] and [27, Remark 5.2], by means of fibre product of certain Artin-Schreier p-extensions of the projective line showed that such curves do exist. Garcia and Stichtenoth, see [20, Sect. V, Ex. E], noticed that such curves admit a plane model of type

$$F(y) = f(x)\,, \tag{2.8}$$

where $F \in \mathbf{F}_{q^2}[Y]$ is a p-linear polynomial of degree $q/(N-1)$ whose linear coefficient is different from zero, and where $f \in \mathbf{F}_{q^2}[X]$ is a polynomial of degree $q+1$. Here P_1 is the unique point over $x = \infty$. For $N-1 = p$, see also [18, Ex. 1.2] and [28, Prop. 3.5]. Unlike the previous case, several pairwise non $\mathbf{F}_{q^2}$-isomorphic $\mathbf{F}_{q^2}$-maximal curves satisfying $(*_2)$ are known to exist; see [1, Sect. 5]. It has been conjectured [15, p. 46] that a plane $\mathbf{F}_{q^2}$-model for a $\mathbf{F}_{q^2}$-maximal curve satisfying $(*_2)$ has equation of type (2.8) with $f(x) = x^{q+1}$. Conversely, the following question arises: Determine the polynomials F and f such that such that the plane curve of equation (2.8) has an $\mathbf{F}_{q^2}$-maximal non-singular model. Examples of such curves arise for instance in [23],

[24], and [28]. Examples of $\mathbf{F}_{q^2}$-maximal curves defined by (2.8), where either F or f are $\mathbf{F}_{q^2}$-rational functions, can be found in [28] and [18].

Finally, some results on Weierstrass Point Theory and Frobenius orders with respect to the linear series $\mathcal{D}_{\mathcal{X}}$. With the same notation as in Sect. 2.2, Lemma 2.10 together with (2.5) forces the first N non-gaps at $P \in \mathcal{X}$ to have the following behaviour:

$$m_1(P) < \ldots < m_{N-1}(P) = q < m_N(P)\,. \tag{2.9}$$

Furthermore,

Lemma 2.15. ([15, Thm. 1.4, Prop. 1.5(ii)(iii)])

(1) $j_1(P) = 1$ *for any* P; $j_N(P) = q+1$ *if* $P \in \mathcal{X}(\mathbf{F}_{q^2})$, *and* $j_N(P) = q$ *otherwise*;
(2) $j_{N-i}(P) + m_i(P) = q+1$ *for* $i = 0, \ldots, N$, *provided that* $P \in \mathcal{X}(\mathbf{F}_{q^2})$;
(3) $q - m_i(P)$ *is a* $(\mathcal{D}_{\mathcal{X}}, P)$*-order for* $i = 0, \ldots, N-1$, *provided that* $P \notin \mathcal{X}(\mathbf{F}_{q^2})$;
(4) $\epsilon_N = \nu_{N-1} = q$;
(5) $\nu_1 = 1$ *if* $N \geq 3$.

Then, we have one of the main features of the linear series $\mathcal{D}_{\mathcal{X}}$, namely

$$\mathcal{X}(\mathbf{F}_{q^2}) \subseteq \mathrm{Supp}(R_{\mathcal{D}_{\mathcal{X}}})\,.$$

Lemma 2.16. *Let* $\mathcal{X}$ *be a* $\mathbf{F}_{q^2}$*-maximal curve of genus* g. *Set* $N := \dim(\mathcal{D}_{\mathcal{X}})$.

(1) *If* $\mathcal{X}$ *is hyperelliptic, then* $q \leq 2N-2$.
(2) *The curve* $\mathcal{X}$ *is hyperelliptic provided that either* $j_{N-1}(P) = j_N(P) - 2$ *for* $P \in \mathcal{X}(\mathbf{F}_{q^2})$, *or* $j_{N-1}(P) = j_N(P) - 1$ *otherwise.*
(3) *If there exists* $P \in \mathcal{X}(\mathbf{F}_{q^2})$ *with* $j_{N-1}(P) = j_N(P) - 1$, *then* $q = N-1$.

Proof. If $\mathcal{X}$ is hyperelliptic, $m_1(P) = g+1$ at a general point P. Then from (2.9), $m_{N-1}(P) = g+N-1 = q$ and so $g = q-N+1$. On the other hand $\#\mathcal{X}(\mathbf{F}_{q^2}) \leq 2(q^2+1)$ and maximality of $\mathcal{X}$ yields $2g \leq q$. From these computations (1) follows. Let $P \in \mathcal{X}(\mathbf{F}_{q^2})$ such that $j_{N-1}(P) \in \{q-1, q\}$. Then from Lemma 2.15(2) we have $m_1(P) \in \{2, 1\}$ and so either $\mathcal{X}$ is hyperelliptic or $m_N = N = q+1$. Finally, let $P \notin \mathcal{X}(\mathbf{F}_{q^2})$ such that $j_{N-1}(P) = q-1$. Then from (2.5), $(q-1)P + D \sim qP + \mathbf{Fr}_{\mathcal{X}}(P)$ with $P \notin \mathrm{Supp}(D)$, so that $D \sim P + \mathbf{Fr}_{\mathcal{X}}(P)$; i.e. $\mathcal{X}$ is hyperelliptic. □

Lemma 2.17. *Let* $\mathcal{X}$ *be a* $\mathbf{F}_{q^2}$*-maximal curve so that* $j_{N-1}(P) = N-1$ *for every point* $P \in \mathcal{X}$, *where* $N = \dim(\mathcal{D}_{\mathcal{X}})$. *Then*

$$(N-1)N(g-1) = (q+1)(q-N)\,.$$

Proof. The set of $\mathcal{D}_{\mathcal{X}}$-Weierstrass points of $\mathcal{X}$ coincides with the set of $\mathbf{F}_{q^2}$-rational points, and $v_P(R_{\mathcal{D}_{\mathcal{X}}}) = 1$ for $P \in \mathcal{X}(\mathbf{F}_{q^2})$; cf. Lemmas 2.15(1), 2.7. Hence the result follows from (2.3) taking into account the maximality of $\mathcal{X}$. □

3. On maximal curves embedded in a quadric surface

The Rück-Stichtenoth theorem together with [17, Thm. 2.4], stated in the previous section as Lemma 2.12, gives a complete classification of $\mathbf{F}_{q^2}$-maximal curves of genus $g > (q-1)^2/4$. The objective of this section is to obtain a similar theorem valid for $(q^2-q+4)/6 < g \le (q-1)^2/4$. Notation and terminology are the same as in Sect. 2.

Theorem 3.1. *Let $\mathcal{X}$ be a $\mathbf{F}_{q^2}$-maximal curve of genus g, and π a $\mathbf{F}_{q^2}$-morphism associated to $\mathcal{D}_{\mathcal{X}}$. Assume $q \ge 7$. Then the following conditons are equivalent:*

(1) $\lfloor (q^2-q+4)/6 \rfloor < g \le \lfloor (q-1)^2/4 \rfloor$;
(2) $\dim(\mathcal{D}_{\mathcal{X}}) = 3$, *$\pi(\mathcal{X})$ lies on a quadric surface in $\mathbf{P}^3$, and $g \ne (q^2-2q+3)/6$ whenever $q \equiv 3,5 \pmod 6$*;
(3) $\dim(\mathcal{D}_{\mathcal{X}}) = 3, \dim(2\mathcal{D}_{\mathcal{X}}) = 8$, *and $g \ne (q^2-2q+3)/6$ whenever $q \equiv 3,5 \pmod 6$*;
(4) $\dim(\mathcal{D}_{\mathcal{X}}) = 3$ *and there exists $P \in \mathcal{X}(\mathbf{F}_{q^2})$ such that $j_2(P) = (q+1)/2$ if q is odd, or $j_2(P) = (q+2)/2$ otherwise*;
(5) *$\mathcal{X}$ is $\mathbf{F}_{q^2}$-isomorphic to the non-singular $\mathbf{F}_{q^2}$-model of either $y^q + y = x^{(q+1)/2}$ if q is odd, or $y^{q/2} + y^{q/4} + \ldots + y^2 + y = x^{q+1}$ otherwise.*
(6) *$g = (q-1)^2/4$ if q is odd or $g = q(q-2)/4$ otherwise. In particular the genus g equals Castelnuovo's number $c_0(q+1,3)$.*

Under stronger hypotheses, this theorem was partially proved in [17, Prop. 2.5] for q odd, and in [2] for q even.

Remark 3.2. For $q = 2,3,4,5$ the spectrum of the genera of $\mathbf{F}_{q^2}$-maximal curves is $\{0,1\}, \{0,1,3\}, \{0,1,2,6\}, \{0,1,2,3,4,10\}$, respectively; see [21, Remark 6.1].

From Theorem 3.1 and Remark 3.2, Corollary 2.13 can be strengthen as follows:

Corollary 3.3. *The genus g of a $\mathbf{F}_{q^2}$-maximal curve satisfies either*

$$g \le \lfloor (q^2-q+4)/6 \rfloor \qquad or \qquad g = \lfloor \tfrac{(q-1)^2}{4} \rfloor \qquad or \qquad g = (q-1)q/2\,.$$

Remark 3.4. $\mathbf{F}_{q^2}$-maximal curves of genus $\lfloor (q^2-q+4)/6 \rfloor$ do exist as the following examples show, see [21], [13, Thm. 2.1]:

(i) If $q \equiv 2 \pmod 3$, the non-singular $\mathbf{F}_{q^2}$-model of $x^{(q+1)/3)} + x^{2(q+1)/3} + y^{q+1} = 0$ is $\mathbf{F}_{q^2}$-maximal and has genus $(q^2-q+4)/6$.
(ii) If $q \equiv 1 \pmod 3$, the non-singular $\mathbf{F}_{q^2}$-model of $y^q - yx^{2(q-1)/3} + x^{(q-1)/3} = 0$ is $\mathbf{F}_{q^2}$-maximal and has genus $(q^2-q)/6$.
(iii) If $q = p^t \equiv 0 \pmod 3$, the non-singular $\mathbf{F}_{q^2}$-model of $y^q + y + (\sum_{i=1}^{t} x^{q/p^i})^2 = 0$ is $\mathbf{F}_{q^2}$-maximal and has genus $(q^2-q)/6$.

It may be that no further infinite family exists. Also, each of the above curves is $\mathbf{F}_{q^2}$-covered by the Hermitian curve via a suitable morphism of degree 3, and it would be of interest to prove or disprove uniqueness of some (perhaps all) of these examples.

Remark 3.5. In searching quantitative results for the number of $\mathbf{F}_\ell$-rational points of a curve of genus g, the maximum number $N_\ell(g)$ of $\mathbf{F}_\ell$-rational points on such curves play an important role; see e.g. [26]. Corollary 3.3 excludes certain values for $N_{q^2}(g)$ whenever $(q^2-q+4)/6 < g < (q-1)^2/4$ or $(q-1)^2/4 < g < q(q-1)/2$. More precisely, for such values of g, we have $N_{q^2}(g) < q^2+1+2qg$. A similar resuly follows from Theorem 4.5(a). Hence from deeper results due to J.P. Serre and K. Lauter one can deduce $N_{q^2}(g) \le q^2+1+2qg-m$, where $m \in \{1,2,3\}$, cf. [29]. One can also obtain improvements on some entries in the tables of loc. cit. For instance, we have $N_{64}(11) \le 238$, $N_{81}(13) \le 314$, $N_{81}(15) \le 350$, while the upper bounds in the tables are respectively 241, 316, 352. It should be noted that the above considerations will extend to a more general case, once the conjecture stated in the introduction has been proved.

In proving Theorem 3.1, we will need some technical results concerning $\mathbf{F}_{q^2}$-maximal $\mathcal{X}$ with $\dim(\mathcal{D}_\mathcal{X}) = 3$.

Lemma 3.6. *Let $\mathcal{X}$ be a $\mathbf{F}_{q^2}$-maximal curve with $\dim(\mathcal{D}_\mathcal{X}) = 3$, and π a $\mathbf{F}_{q^2}$-morphism associated to $\mathcal{D}_\mathcal{X}$. Assume $q \ge 4$.*

(1) $\dim(2\mathcal{D}_\mathcal{X}) \ge 8$.
(2) *If $\dim(2\mathcal{D}_\mathcal{X}) = 8$, then $\pi(\mathcal{X})$ lies on a quadric surface in $\mathbf{P}^3(\bar{\mathbf{F}}_{q^2})$.*
(3) *The quadric surface $\mathcal{Q}$ in part (2) is uniquely determinated by the property $\pi(\mathcal{X}) \subseteq \mathcal{Q}$, and it is defined over $\mathbf{F}_{q^2}$.*

Proof. (1) Let $P \in \mathcal{X}(\mathbf{F}_{q^2})$ and set $m_i := m_i(P)$. From Lemma 2.15(2), $m_2 = q$ and $m_3 = q+1$. Then, as $2m_1 \ge m_2 = q$ and $q \ge 4$, it is easy to see that there are at least 8 positive Weierstrass non-gaps in $[m_1, 2m_3]$ and so $\dim(2\mathcal{D}_\mathcal{X}) \ge 8$.

(2) See [33, p. 352].

(3) If $\pi(\mathcal{X})$ lies on $\mathcal{Q}$, then $\pi(\mathcal{X})$ also lies on $\mathbf{F}r(\mathcal{Q})$, where $\mathbf{F}r$ is the Frobenius collination on $\mathbf{P}^3(\bar{\mathbf{F}}_{q^2})$ relative to $\mathbf{F}_{q^2}$. Clearly $\mathcal{Q} = \mathbf{F}r(\mathcal{Q})$ if and only if $\mathcal{Q}$ is defined over $\mathbf{F}_{q^2}$. It this were not the case in our situation, then $\mathcal{X}$ would be contained in the intersection of two distinct quadrics, contradicting the hypothesis $q+1 = \deg(\pi(\mathcal{X})) \le 4$ by the Bézout theorem. □

Lemma 3.7. *Let $\mathcal{X}$ be a $\mathbf{F}_{q^2}$-maximal curve with $\dim(\mathcal{D}_\mathcal{X}) = 3$, π a morphism associated to $\mathcal{D}_\mathcal{X}$, and $P \in \mathcal{X}$. Suppose that $\pi(\mathcal{X})$ lies on a quadric surface $\mathcal{Q}$ in $\mathbf{P}^3(\bar{\mathbf{F}}_{q^2})$, and that $q \ge 5$. Then*

(1) $j_2(P) \in \{2, j_3(P)/2, (j_3(P)+1)/2\}$;
(2) *$j_2(P) > 2$ if and only if the tangent line $L_1(P)$ of $\mathcal{X}$ at P lies on $\mathcal{Q}$;*
(3) *either q is even, $j_2(P) = q/2$ and $P \notin \mathcal{X}(\mathbf{F}_{q^2})$ or q is odd, $j_2(P) = (q+1)/2$ and $P \in \mathcal{X}(\mathbf{F}_{q^2})$ provided that $j_2(P) > 2$ and that $\mathcal{Q}$ is non-singular at $\pi(P)$.*

Proof. Set $j_i := j_i(P)$, $i = 0, \ldots, 3$. Let $x_0 = 1, x_1, x_2, x_3$ be $\mathbf{F}_{q^2}$-rational functions on $\mathcal{X}$, such that $v_P(x_i) = j_i$. Up to a projective collineation in $\mathbf{P}^3(\bar{\mathbf{F}}_{q^2})$, we can assume $\pi = (x_0 : x_1 : x_2 : x_3)$. Let $(X_0, \ldots, X_3)$ be coordinates in $\mathbf{P}^3(\bar{\mathbf{F}}_{q^2})$ such that each x_i is the pull-back via π of X_i/X_0 restricted to $\pi(\mathcal{X})$. Then $\pi(P) = (1 : 0 : 0 : 0)$ and $L_1(P)$ is given by $X_2 = X_3 = 0$; see [41, proof of Thm. 1.1]. Let the quadric $\mathcal{Q}$ have homogeneous equation

$$F(X_0, X_1, X_2, X_3) = a_{00}X_0^2 + a_{01}X_0X_1 + a_{02}X_0X_2 + a_{03}X_0X_3 + a_{11}X_1^2 + a_{12}X_1X_2 + a_{13}X_1X_3 + a_{22}X_2^2 + a_{23}X_2X_3 + a_{33}X_3^2 .$$

Then $a_{00} = 0$ because of $F(\pi(P)) = 0$. Furthermore, x_1, x_2 and x_3 are related in the function field over $\bar{\mathbf{F}}_{q^2}$ of $\mathcal{X}$ by $F(1, x_1, x_2, x_3) = 0$. In addition, the valuation at P of the functions $x_1, x_2, x_3, x_1^2, x_1x_2, x_1x_3, x_2^2, x_2x_3, x_3^2$ are respectively

$$1, j_2, j_3, 2, j_2 + 1, j_3 + 1, 2j_2, j_3 + j_2, 2j_3 . \tag{3.1}$$

Hence, $a_{01} = 0$.

(1) $j_2 + 1 < j_3$ by Lemma 2.16 and the hypothesis $q \geq 5$. So from the inequalities

$$2 \leq j_2 < j_2 + 1 < j_3 < j_3 + 1 < j_3 + j_2 < 2j_3$$

and (3.1) we obtain part (1).

(2) We have from (3.1) that $j_2 > 2$ if and only if $a_{11} = 0$. Now, as $F(X_0, X_1, 0, 0) = a_{11}X_1^2$, the last condition is equivalent to $L_1(P) \subseteq \mathcal{Q}$ and the result follows.

(3) If $j_2 > 2$, from the proof of part (1) we get $a_{11} = a_{02} = a_{12} = 0$. An easy computation shows then that $\mathcal{Q}$ is non-singular at $\pi(P)$ if and only if $a_{03} \neq 0$. Therefore $2j_2 = j_3$, and the result follows from Lemma 2.15(1). □

Proposition 3.8. *Let $\mathcal{X}$ be a $\mathbf{F}_{q^2}$-maximal curve and π a $\mathbf{F}_{q^2}$-morphism associated to $\mathcal{D}_{\mathcal{X}}$. Suppose that q is even, $q > 4$, and that $\pi(\mathcal{X})$ lies on a quadric $\mathcal{Q}$ in $\mathbf{P}^3(\bar{\mathbf{F}}_{q^2})$. Then*

(1) *$\mathcal{Q}$ is a cone;*
(2) *the vertex V of $\mathcal{Q}$ belongs to $\pi(\mathcal{X})$; if $V = \pi(\tilde{V})$, then $\tilde{V} \in \mathcal{X}(\mathbf{F}_{q^2})$ and $j_2(\tilde{V}) = (q + 2)/2$.*

Proof. General properties of quadrics of a 3-dimensional projective space over a finite field can be found in [35]. Here we will use the following properties: Let $P \in \mathcal{Q}$ be a non-singular point of $\mathcal{Q}$ and denote by $T_P\mathcal{Q}$ the tangent plane of $\mathcal{Q}$ at P.

- If $P \in \pi(\mathcal{X})$, then $T_P\mathcal{Q} \supseteq L_1(P)$;
- Let ℓ and ℓ_1 be lines such that $P \in \ell \subseteq \mathcal{Q}$, and $\ell_1 \subseteq T_P\mathcal{Q}$. If $\ell \neq \ell_1$, then $T_P\mathcal{Q}$ is generated by ℓ and ℓ_1;
- There exist lines ℓ and ℓ_1 such that $P \in \ell \cap \ell_1$, and $\mathcal{Q} \cap T_P\mathcal{Q} = \ell \cup \ell_1$;

If $\mathcal{Q}$ is non-singular, then

- No two tangent hyperplanes of $\mathcal{Q}$ at different points coincide.

To simplify our notation we shall identify $\mathcal{X}$ and $\pi(\mathcal{X})$, according to Lemma 2.10.

(1) Since $\mathcal{X}$ is non-degenerate, $\mathcal{Q}$ is irreducible. Then $\mathcal{Q}$ is a cone if and only if $\mathcal{Q}$ is singular, as this case can only occur when $\mathcal{Q}$ has just one singular point.

Suppose that $\mathcal{Q}$ is non-singular. Then from Lemma 3.7(3), $j_2(Q) = 2$ for each $Q \in \mathcal{X}(\mathbf{F}_{q^2})$. Note that there exists $P \in \mathcal{X} \setminus \mathcal{X}(\mathbf{F}_{q^2})$ such that $j_2(P) > 2$; in fact, otherwise Lemma 2.17 would yield $6(g-1) = (q+1)(q-3)$; but then q would be odd, a contradiction. Hence $j_2(P) = q/2$ by Lemma 3.7(3). Let $Q_1 \in \mathcal{X}(\mathbf{F}_{q^2})$. We have $Q_1 \notin L_1(P)$, as $\mathcal{X} \cap L_1(P) \subseteq \mathcal{X} \cap L_2(P) = \{P, \mathbf{Fr}_{\mathcal{X}}(P)\}$ (cf. (2.6)), and hence the plane $H = H_{Q_1}$ generated by $L_1(P)$ and Q_1 is well defined. Then $H \neq L_2(P)$, and the intersection divisor of $\mathcal{X}$ and H becomes

$$\mathcal{X} \cdot H = \frac{q}{2}P + D\,, \tag{3.2}$$

where $D = D_{Q_1}$ is a divisor on $\mathcal{X}$ of degree $(q+2)/2$ with $Q_1 \in \mathrm{Supp}(D)$, and $P \notin \mathrm{Supp}(D)$. In addition, Lemma 3.7(2) assures the existence of a line $\ell = \ell_{Q_1}$ such that

$$\mathcal{Q} \cap H = L_1(P) \cup \ell\,. \tag{3.3}$$

Actually, the line ℓ is defined over $\mathbf{F}_{q^2}$. In fact, $\mathcal{Q}$ is defined over $\mathbf{F}_{q^2}$ by Lemma 3.6(3), and $Q_1 \in \mathcal{X}(\mathbf{F}_{q^2}) \setminus L_1(P)$ implies that $Q_1 \in \ell$.

Claim 1. $\mathcal{X} \cap \ell \subseteq \mathcal{X}(\mathbf{F}_{q^2})$.

Proof of Claim 1. If there exists $Q \in \mathcal{X} \cap \ell \setminus \mathcal{X}(\mathbf{F}_{q^2})$, then $\mathbf{Fr}_{\mathcal{X}}(Q) \in \ell$ as ℓ is defined over $\mathbf{F}_{q^2}$. Thus $\ell \subseteq L_2(Q)$, and hence $\ell \cap \mathcal{X} \subseteq \{Q, \mathbf{Fr}_{\mathcal{X}}(Q)\}$. It follows $Q_1 \notin \ell$, but this is a contradiction.

Claim 2. If $Q \in \mathrm{Supp}(D) \setminus \{\mathbf{Fr}_{\mathcal{X}}(P)\}$, then $Q \in \mathcal{X}(\mathbf{F}_{q^2})$ and $v_Q(D) = 1$.

Proof of Claim 2. Since $\mathrm{Supp}(D) \setminus \{\mathbf{Fr}_{\mathcal{X}}(P)\} \subseteq \ell \cap \mathcal{X}$, we have $Q \in \mathcal{X}(\mathbf{F}_{q^2})$ by Claim 1. Now if $v_Q(D) \geq 2$, then $H \supseteq L_1(Q)$ by $j_2(Q) = 2$ and Lemma 2.8. Also, $\ell \neq L_1(Q)$ because $L_1(Q) \not\subseteq \mathcal{Q}$ by Lemma 3.7(2). Therefore the plane H is generated by the lines ℓ and $L_1(Q)$, and hence $H = T_{Q_1}\mathcal{Q}$. Let ℓ_1 be the line defined by $Q_1 \in \ell_1$, and $\mathcal{Q} \cap T_{Q_1}\mathcal{Q} = \ell \cap \ell_1$. From (3.3), we infer that $L_1(P) = \ell_1$ and so $Q_1 \in L_1(P)$, but this is a contradiction.

Claim 3. $\mathbf{Fr}_{\mathcal{X}}(P) \notin \mathrm{Supp}(D)$.

Proof of Claim 3. Suppose on the contrary that $\mathbf{Fr}_{\mathcal{X}}(P) \in \mathrm{Supp}(D)$. Equivalently, $\mathbf{Fr}_{\mathcal{X}}(P) \in L_1(P)$ by Claim 1. Then $v_{\mathbf{Fr}_{\mathcal{X}}(P)}(D) = 1$. In fact, using a similar argument to that in the proof the previous claim, one can show that $v_{\mathbf{Fr}_{\mathcal{X}}(P)}(D) \neq 1$ together with $L_1(P) \neq L_1(\mathbf{Fr}_{\mathcal{X}}(P))$ implies $H = T_{\mathbf{Fr}_{\mathcal{X}}(P)}\mathcal{Q}$ in contradiction with (2.6). Hence, for

each $Q \in \mathcal{X}(\mathbf{F}_{q^2})$, the divisor D in (3.2) may also be written as $D = D_Q = \mathbf{Fr}_{\mathcal{X}}(P)+D'_Q$ in such a way that (3.3) holds true, $\mathrm{Supp}(D'_Q) \subseteq \mathcal{X}(\mathbf{F}_{q^2})$, and $\deg(D'_Q) = q/2$. Notice that H_Q is generated by $L_1(P)$ and Q' $(*)$ where Q' is any point of $\mathrm{Supp}(D'_Q)$. Now let $Q_1, Q_2 \in \mathcal{X}(\mathbf{F}_{q^2})$ such that $Q_2 \notin \mathrm{Supp}(D'_{Q_1})$. Then $\mathrm{Supp}(D'_{Q_1}) \cap \mathrm{Supp}(D'_{Q_2}) = \emptyset$, otherwise $H_{Q_1} = H_{Q_2}$ by $(*)$. This yields that $q/2$ must divide the number of $\mathbf{F}_{q^2}$-rational points of $\mathcal{X}$, which is a contradiction because $\#\mathcal{X}(\mathbf{F}_{q^2}) = q^2 + 1 + 2gq$ is an odd number.

So far we have shown that each $Q_1 \in \mathcal{X}(\mathbf{F}_{q^2})$ gives rise to a plane H_{Q_1}, to a line $\ell = \ell_{Q_1}$, and to a divisor $D = D_{Q_1}$ such that (3.2) and (3.3) hold with $D = Q_1+Q_2+\ldots+Q_{(q+2)/2}$ being the sum of $(q+2)/2$ $\mathbf{F}_{q^2}$-rational points. Notice that $\mathrm{Supp}(D) = \mathcal{X} \cap \ell$. Let ℓ_1 be chosen in such a way that $Q_1 \in \ell_1$ and that

$$\mathcal{Q} \cap T_{Q_1}\mathcal{Q} = \ell \cup \ell_1 \,. \tag{3.4}$$

Clearly, ℓ_1 is $\mathbf{F}_{q^2}$-rational, and thus $\mathcal{X} \cap \ell_1 \subseteq \mathcal{X}(\mathbf{F}_{q^2})$ as in the proof of Claim 1. Therefore

$$\mathcal{X} \cdot T_{Q_1}\mathcal{Q} = 2Q_1 + Q_2 + \ldots + Q_{(q+2)/2} + D' \,, \tag{3.5}$$

where D' is a divisor on $\mathcal{X}$ of degree $(q-2)/2$ such that $Q_1 \notin \mathrm{Supp}(D') \subseteq \mathcal{X}(\mathbf{F}_{q^2})$.

Claim 4. $\mathrm{Supp}(D) \cap \mathrm{Supp}(D') = \emptyset$, and $v_S(D') = 1$ for each $S \in \mathrm{Supp}(D')$.

Proof of Claim 4. Let $S \in \mathrm{Supp}(D')$. Suppose on the contrary that $S = Q_i$ for some i. Then $T_{Q_1}\mathcal{Q}$ contains $L_1(Q_i)$ which is different from ℓ as $j_2(Q_i) = 2$. Hence $T_{Q_1}\mathcal{Q}$ is generated by $L_1(Q_i)$ and ℓ. These lines also generate $T_{Q_i}\mathcal{Q}$ and so $i = 1$ contradicting $Q_1 \notin \mathrm{Supp}(D')$.

Finally suppose on the contrary that $v_S(D_2) \geq 2$. Replacing ℓ by ℓ_1, the above argument shows that $T_S\mathcal{Q} = T_{Q_1}\mathcal{Q}$, whence $S = Q_1$ follows, again a contradiction.

Therefore, to each Q_1 we have associated two lines ℓ and ℓ_1 such that both (3.4) and (3.5) hold where D' is a divisor of degree $(q-2)/2$, $\mathrm{Supp}(D') \subseteq \mathcal{X}(\mathbf{F}_{q^2})$, and $\mathrm{Supp}(D) \cap \mathrm{Supp}(D') = \{Q_1\}$. As it is well-known, $\mathcal{Q}$ has just two families of lines contained in $\mathcal{Q}$ and any two lines of the same family are disjoint. This implies again that $\#\mathcal{X}(\mathbf{F}_{q^2})$ must be a multiple of $q/2$, contradicting the $\mathbf{F}_{q^2}$-maximality of $\mathcal{X}$.

(2) As q is even, from Lemma 2.17 there exists $P \in \mathcal{X}$ such that $j_2(P) > 2$. Suppose that $P \notin \mathcal{X}(\mathbf{F}_{q^2})$. From $j_2(P)P+D \sim (q+1)P_0$, we find that $j_2(P)\mathbf{Fr}_{\mathcal{X}}(P)+\mathbf{Fr}_{\mathcal{X}}(D) \sim (q+1)P_0$ and so $j_2(\mathbf{Fr}_{\mathcal{X}}(P)) = j_2(P) > 2$. Therefore $L_1(P) \cup L_1(\mathbf{Fr}_{\mathcal{X}}(P) \subseteq \mathcal{Q}$ by Lemma 3.7(2), and hence $V \in L_1(P) \cap L_1(\mathbf{Fr}_{\mathcal{X}}(P))$. Now, since V is $\mathbf{F}_{q^2}$-rational by Lemma 3.6(3), we have $\mathbf{Fr}_{\mathcal{X}}(P) \neq V$, and hence $L_1(\mathbf{Fr}_{\mathcal{X}}(P))$ is generated by $\mathbf{Fr}_{\mathcal{X}}(P)$ and V; in particular $L_1(\mathbf{Fr}_{\mathcal{X}}(P)) \subseteq L_2(P)$ and thus $1 = v_{\mathbf{Fr}_{\mathcal{X}}(P)}(\mathcal{X} \cdot L_2(P)) \geq j_2(\mathbf{Fr}_{\mathcal{X}}(P))$ by Lemma 2.8, a contradiction.

Therefore P must be $\mathbf{F}_{q^2}$-rational and hence $\mathcal{Q}$ must have a singularity at P by Lemma 3.7(3). Then $P = V$ and $j_2(P) = (q+2)/2$ by Lemma 3.7(1) and the assumption of q being even. □

Proof of Theorem 3.1. (1)⇒(2) : From the hypothesis on g, $\dim(\mathcal{D}_\mathcal{X}) = 3$ follows by (2.7) and Lemma 2.12. Since $c_1(q+1,3)$ in Lemma 2.4 is equal to $\lfloor (q^2-q+4)/6 \rfloor$, that lemma together with Lemma 2.10 shows that $\pi(\mathcal{X})$ lies on a quadric provided that $q \notin \{7,8,9,11,13,17,19,23\}$.

Assume $q = 8$. Then $g > (q^2-q+4)/6 = 10$. By virtue of Lemma 3.6(1)(2), it is enough to show that $\dim(2\mathcal{D}_\mathcal{X}) \leq 8$. Suppose on the contrary that $\dim(2\mathcal{D}_\mathcal{X}) \geq 9$. Then from Lemma 2.1 and Remark 2.2, $g \leq (q-1)(q-2)/4 = 10.5$ follows, a contradiction.

Now, let q be odd, $q \geq 7$. Our goal is to show that the second positive $\mathcal{D}_\mathcal{X}$-order ϵ_2 (see sections 2.2, 2.3) is equal to two. In fact, if this is the case, then the Generic Order of Contact Theorem [34, Thm. 3.5] yields that the curve $\mathcal{X}$ (that is $\pi(\mathcal{X})$ by previous identification) is reflexive. Reflexivity forces the monodromy group of $\mathcal{X}$ to be isomorphic to the symmetric group S_{q+1}, see ([7, p. 264], [38, Cor. 2.2]). Hence the points of a general hyperplane section of $\mathcal{X}$ lie in uniform position [38, Cor. 1.8]. Then Lemma 2.4 holds true; see Remark 2.5.

Suppose on the contrary that $\epsilon_2 > 2$. Let S be the $\mathbf{F}_{q^2}$-Frobenius divisor associated to $\mathcal{D}_\mathcal{X}$. From Lemmas 2.9, 2.7(1), 2.15(4)(5), $v_P(S) \geq \epsilon_2 + 1 \geq 4$ for any $P \in \mathcal{X}(\mathbf{F}_{q^2})$. Then by (2.4) and the $\mathbf{F}_{q^2}$-maximality of $\mathcal{X}$, $(3q-1)(2g-2) \leq (q+1)(q^2-4q-1)$. On the other hand, $2g-2 > (q+1)(q-2)/3$ by hypothesis, and thus $5q+5 < 0$, a contradiction.

(3)⇒(2) : This follows from Lemma 3.6(2).

(2)⇒(4) : Let q be odd. There exists $P \in \mathcal{X}$ such that $j_2(P) > 2$, otherwise g would be equal to $(q^2-2q+3)/6$ by Lemma 2.17. If such a point $P \in \mathcal{X}$ should not be in $\mathcal{X}(\mathbf{F}_{q^2})$, then by Lemma 3.7(3) both P and $\mathbf{Fr}_\mathcal{X}(P)$ would be singular points of the quadric, a contradiction. Therefore $P \in \mathcal{X}(\mathbf{F}_{q^2})$ and hence $j_2(P) = (q+1)/2$ by Lemma 3.7(1). If q is even, the result follows from Proposition 3.8(2).

(4)⇒(5) : From Lemma 2.15(2) and the hypothesis, $m_1(P) = (q+1)/2$ for q is odd, and $m_1(P) = q/2$ for q even. In the odd case, $(\dim(\mathcal{D}_\mathcal{X}) - 1)m_1(P) = q+1$, and (5) follows from [15, Thm. 2.3]. In the even case, $(\dim(\mathcal{D}_\mathcal{X}) - 1)m_1(P) = q$, and hence $g = q(q-2)/4$ by [37, Remark 2.6(1)]. Then (5) follows from the main result in [2].

The implications (5)⇒(6), (6)⇒(1), and (5)⇒(3) are trivial.

4. On $\mathbf{F}_{q^2}$-maximal curves whose genus equals Castelnuovo's number

In this section we investigate certain $\mathbf{F}_{q^2}$-maximal curves whose genus equals Castelnuovo's number $c_0(q+1,N)$ for $N \in \{4,5\}$.

4.1. The case $q \equiv 1, 2 \pmod 3$. The main result is Theorem 4.5 which provides a complete description of $\mathbf{F}_{q^2}$-maximal curves of genus $g = (q-1)(q-2)/6$, $q \equiv 1, 2 \pmod 3$, $q \geq 11$: Such $\mathbf{F}_{q^2}$-maximal curves can only exist for $q \equiv 2 \pmod 3$, and they are $\mathbf{F}_{q^2}$-isomorphic to the non-singular $\mathbf{F}_{q^2}$-model of the plane curve of equation

$$y^q + y = x^{(q+1)/3}\,. \tag{4.1}$$

To do this let $\mathcal{X}$ denote an $\mathbf{F}_{q^2}$-maximal curve of genus $g = (q-1)(q-2)/6$ with $q \equiv 1, 2 \pmod 3$, equipped with the linear series $\mathcal{D}_{\mathcal{X}}$ as defined before. The first step is to compute the dimension of $\mathcal{D}_{\mathcal{X}}$.

Lemma 4.1. $\dim(\mathcal{D}_{\mathcal{X}}) = 4$. *In particular,* $g = c_0(q+1, 4)$.

Proof. From (2.7) and Lemma 2.12, $\dim(\mathcal{D}_{\mathcal{X}}) \in \{3, 4\}$. Suppose on the contrary that $\dim(\mathcal{D}_{\mathcal{X}}) = 3$. If $\epsilon_2 = 2$, (2.3) becomes $\deg(R) = (3+q)(2g-2) + 4(q+1)$, while $\mathbf{F}_{q^2}$-maximality of $\mathcal{X}$ implies $\deg(R) \geq q^2 + 1 + 2gq$ as $v_P(R) \geq 1$ for every $P \in \mathbf{F}_{q^2}(\mathcal{X})$. But then $g \geq (q^2 - 2q + 3)/6$ contradicting the hypothesis on g. If $\epsilon_2 > 2$, then $\epsilon_2 \geq 5$ by the p-adic criteriom [41, Cor. 1.9] and $q \not\equiv 0 \pmod 3$. Replacing the ramification divisor R by the Frobenius divisor S in the previous argument yields again a contradiction. In fact, (2.4) reads currently $\deg(S) = (1+q)(2g-2) + (q^2+3)(q+1)$, while $\deg(S) \geq (q^2 + 1 + 2gq)(\epsilon_2 + 1)$ by the $\mathbf{F}_{q^2}$-maximality of $\mathcal{X}$ and the lower bound $v_P(S) \geq \epsilon_2 + 1$ for $P \in \mathbf{F}_{q^2}(\mathcal{X})$ which has been shown in the proof of Theorem 3.1. Taking $\epsilon_2 \geq 5$ into account, this gives $(5q-1)(2g-2) \leq (q+1)(q^2 - 6q - 3)$, whence $2q^2 - 3q + 13 \leq 0$ follows for $g = (q-1)(q-2)/6$; a contradiction. □

We take advantage of the current hypothesis that the genus of $\mathcal{X}$ is equal to Castelnuovo's number $c_0(q+1, 4)$ by means of Lemma 2.3(1). Indeed, this lemma implies that $\dim(2\mathcal{D}_{\mathcal{X}}) = 11$ which allows to compute the possibilities for $(\mathcal{D}_{\mathcal{X}}, P)$-orders. To show how to do this, set $j_i = j_i(P)$ and denote by Σ_P the set of $(2\mathcal{D}_{\mathcal{X}}, P)$-orders. Then Σ_P contains both the following sets Σ_1 and Σ_2:

$$\begin{aligned} \Sigma_1 &:= \{0, 1, 2, j_3, j_4, j_4+1, j_4+j_2, j_4+j_3, 2j_4\} \\ \Sigma_2 &:= \{j_2, j_2+1, j_3+1, 2j_2, j_3+j_2, 2j_3\}\,, \end{aligned} \tag{4.2}$$

where $j_4 = q+1$ for $P \in \mathcal{X}(\mathbf{F}_{q^2})$, and $j_4 = q$ otherwise (cf. Lemma 2.15(1)).

Lemma 4.2. *Let $\mathcal{X}$ be a $\mathbf{F}_{q^2}$-maximal curve and $P \in \mathcal{X}$ a point with $j_2(P) = 2$. If $\dim(\mathcal{D}_{\mathcal{X}}) = 4$, $\dim(2\mathcal{D}_{\mathcal{X}}) = 11$, and $q \geq 9$, then $j_3(P) = 3$.*

Proof. The hypothesis on q together with Lemma 2.16 implies that

$$j_3 < j_4 - 2 \text{ for } P \in \mathcal{X}(\mathbf{F}_{q^2}) \quad \text{and} \quad j_3 < j_4 - 1 \text{ otherwise}\,. \tag{4.3}$$

Suppose $j_3 > 3$. If $P \in \mathcal{X}(\mathbf{F}_{q^2})$, from (4.2) and (4.3)

$$\Sigma_P = \Sigma_1 \cup \{3, j_3+1, j_3+2\}\,,$$

and $2j_2, 2j_3 \in \Sigma_P$. Thus $j_3 = 2j_2 = 4$ so that $2j_3 = 8 = j_4 = q+1$; i.e. $q = 7$. If $P \notin \mathcal{X}(\mathbf{F}_{q^2})$ and $j_3 > 4$, from (4.2) and (4.3) we have

$$\Sigma_P = \Sigma_1 \cup \{3, 4, j_3 + 1\},$$

and $(j_3 + 2, 2j_3) \in \{(q, q+1), (q, q+2), (q+1, q+2)$. Then $j_3 \leq 4$, a contradiction. Finally, if $P \notin \mathcal{X}(\mathbf{F}_{q^2})$ and $j_3 = 4$, then (4.2) together with (4.3) gives

$$\Sigma_P = \Sigma_1 \cup \{3, 5, 6, 8\}.$$

Hence $j_4 = q = 8$, and this completes the proof. □

The previous lemma together with Lemma 2.17 gives the following result.

Corollary 4.3. *Let $\mathcal{X}$ be a $\mathbf{F}_{q^2}$-maximal curve such that $\dim(\mathcal{D}_\mathcal{X}) = 4$ and $\dim(2\mathcal{D}_\mathcal{X}) = 11$. Assume $q \geq 9$. If $j_2(P) = 2$ for any $P \in \mathcal{X}$, then $q \equiv 1, 2 \pmod 3$ and $g = (q^2 - 3q + 8)/12$.*

Now, we investigate the case $j_2(P) > 2$ for some $P \in \mathcal{X}$.

Lemma 4.4. *Let $\mathcal{X}$ be a $\mathbf{F}_{q^2}$-maximal curve and $P \in \mathcal{X}$ a point with $j_2(P) > 2$. Suppose that $\dim(\mathcal{D}_\mathcal{X}) = 4$, $\dim(2\mathcal{D}_\mathcal{X}) = 11$, and that $q \geq 7$.*

(1) *If $P \in \mathcal{X}(\mathbf{F}_{q^2})$ and $g > (q-2)q/8$ for q even, then either $q \equiv 2 \pmod 3$, $j_2(P) = (q+1)/3, j_3(P) = (2q+2)/3$; or $q \equiv 0 \pmod 3$, $j_2(P) = (q+3)/3, j_3(P) = (2q+3)/3$;*
(2) *If $P \notin \mathcal{X}(\mathbf{F}_{q^2})$, then either $q \equiv 1 \pmod 3$, $j_2(P) = (q+2)/3, j_3(P) = (2q+1)/3$; or $q \equiv 0 \pmod 3$, $j_2(P) = q/3, j_3(P) = 2q/3$; or q is odd, $j_2(P) = (q-1)/2$, $j_3(P) = (q+1)/2$; or q is even, $j_2(P) = q/2, j_3(P) = (q+2)/2$.*

Proof. Suppose first that $j_3 > j_2 + 1$. According to (4.2) and (4.3) we have only three possibilities, namely

$$\Sigma_P = \Sigma_1 \cup \{j_2, j_2 + 1, j_3 + 1\},$$

and $(j_3 + j_2, 2j_3) \in \{(j_4, j_4 + 1), (j_4, j_4 + j_2), (j_4 + 1, j_4 + j_2)\}$. The first one cannot actually occur by $j_3 \neq j_2 + 1$; from the second one $j_4 \equiv 0 \pmod 3$, $j_2 = j_4/3$, $j_3 = 2j_4/3$ follow, while the third one gives $j_4 \equiv 1 \pmod 3$, $j_2 = (j_4 + 2)/3$, and $j_3 = (2j_4 + 1)/3$.

Suppose next that $j_3 = j_2 + 1$. Then $2j_2 \notin \{j_3, j_3 + 1\}$ by $j_2 > 2$. Moreover, $2j_2 \neq j_4 + 1$; otherwise $j_2 = (j_4 + 1)/2, j_3 = (j_4 + 3)/2$ and from (4.2) and (4.3) we would have

$$\Sigma_P = \Sigma_1 \cup \{j_2, j_3 + 1, j_4 + 2, j_4 + 3\}$$

which implies $j_4 + j_2 = j_4 + 3$; whence $j_4 = 5$ and so $q \leq 5$. If $2j_2 = j_4$, then $P \notin \mathcal{X}(\mathbf{F}_{q^2})$; otherwise $j_3 = (q+3)/2$ and hence $m_1 = (q-1)/2$ by Lemma 2.15(2), and this would imply $\dim(\mathcal{D}_\mathcal{X}) \geq 5$. Finally, assume that $2j_2 \notin \{j_3, j_3 + 1, j_4, j_4 + 1\}$. Then from (4.2) and (4.3)

$$\Sigma_P = \{j_2, j_3 + 1, 2j_2\},$$

and $j_3 + j_2 \in \{j_4, j_4 + 1\}$. If $j_3 + j_2 = j_4 + 1$, then $2j_2 = j_4$, whence $j_3 + j_2 = j_4$. Then $j_2 = (j_4 - 1)/2$ and $j_3 = (j_4 + 1)/2$. We claim that $P \notin \mathcal{X}(\mathbf{F}_{q^2})$. In fact, otherwise $j_2 = q/2$, $j_3 = (q+2)/2$ and hence $m_1 = q/2$, $m_2 = (q+2)/2$ by Lemma 2.15(2) which yields $g \leq (q-2)q/8$, a contradiction. □

Theorem 4.5. *Assume $q \geq 11$.*

(1) *If $q \equiv 1 \pmod 3$, there is no $\mathbf{F}_{q^2}$-maximal curve of genus $(q-1)(q-2)/6$.*
(2) *If $q \equiv 2 \pmod 3$, the following statements are equivalent for a $\mathbf{F}_{q^2}$-maximal curve $\mathcal{X}$ of genus g:*
   (a) $g = (q-1)(q-2)/6$;
   (b) $\exists P \in \mathcal{X}(\mathbf{F}_{q^2}), \exists m \in H(P)$ such that $3m = q+1$;
   (c) $\mathcal{X}$ is $\mathbf{F}_{q^2}$-isomorphic to the non-singular $\mathbf{F}_{q^2}$-model of the curve (4.1).

Proof. (1) Suppose on the contrary that $\mathcal{X}$ is an $\mathbf{F}_{q^2}$-maximal curve of genus $g = (q-1)(q-2)/3$ with $q \equiv 1 \pmod 3$. Since $q+1 = \frac{q-1}{3} \cdot 3 + 2$, we have $g = c_0(q+1, 3)$ by Lemma 4.1. Hence, Lemma 2.3 implies that $\dim(2\mathcal{D}_{\mathcal{X}}) = 11$ and that $\frac{q-4}{3}\mathcal{D}_{\mathcal{X}}$ is the canonical linear series on $\mathcal{X}$. Then

$$a_1 i_1 + \ldots + a_{(q-4)/3} i_{(q-4)/3} + 1 \notin H(P)\,, \tag{4.4}$$

where the i_j's are $(\mathcal{D}_{\mathcal{X}}, P)$-orders, and the a_j's are non-negative integers such that $\sum_j a_j \leq (q-4)/3$. We choose then $P \in \mathcal{X}$ with $j_2(P) > 2$ according to Corollary 4.3. By Lemma 4.4, $P \notin \mathcal{X}(\mathbf{F}_{q^2})$. Thus, we have to analyze three cases. As before, $m_i = m_i(P)$ stands for the ith Weierstrass non-gap at P. Recall that $m_3 = q$ by (2.9)).

Case 1: $j_2(P) = (q+2)/3, j_3(P) = (2q+1)/3$. From Lemma 2.15(3), $\{q - m_2, q - m_1\} \subseteq \{1, (q+2)/3, (2q+1)/3\}$. We have that $q - m_1 = (q+2)/3$, since otherwise $m_1 = (q-1)/3$ and hence $q \geq m_4$, a contradiction. Thus $m_1 = (2q-2)/3$. However this leads again to a contradiction since, by (4.4), $(q-7)/3 + (q+2)/3 + 1 = (2q-2)/3$ does not belong to $H(P)$.

Case 2: q odd, $j_2(P) = (q-1)/2, j_3(P) = (q+1)/2$. From (4.4), $2j_2(P) + 1 = q$ does not belong to $H(P)$, a contradiction.

Case 3: q even, $j_2(P) = q/2, j_3(P) = (q+2)/2$. Arguing as in Case 1 we have either $m_1 = q/2 - 1$ or $m_1 = q/2$. In the former case, $q - 2 \in H(P)$ and thus Lemma 2.15(3) implies $j_2(P) = 2$. Since this is not admitted currently, the latter case can only occur. Then $m_1 = q/2$ and $m_2 = q - 1$. Now, as $\dim(2\mathcal{D}_{\mathcal{X}}) = 11$, from (2.5) $m_9 = 2q$ follows. Since a similar result to Lemma 2.15(3) holds, namely $2q - m_i$ is a $(2\mathcal{D}_{\mathcal{X}}, P)$-order for $i = 0, \ldots, 9$, and the set of $(2\mathcal{D}_{\mathcal{X}}, P)$-orders is

$$\{0, 1, 2, q/2, (q+2)/2, (q+4)/2, q, q+1, q+2, 3q/2, 3q/2, 2q\}\,,$$

we conclude that $2q - m_4 = q/2 + 2$; whence $m_4 = 3q/2 - 2$. Finally from (4.4), $\ell := \frac{q-4}{3}(q/2+1) + 1 \notin H(P)$. On the other hand, $\ell = m_4 + \frac{q-10}{6} m_2 \in H(P)$, a contradiction.

(2) (a)⇒(b) : In virtue of Lemma 4.1, we have $g = c_0(q+1, 4)$. By $q+1 = \frac{q-2}{3} \cdot 3 + 3$, Lemma 2.3 shows that $\dim(2\mathcal{D}_{\mathcal{X}}) = 11$ and that $\frac{q-5}{3}\mathcal{D}_{\mathcal{X}} + \mathcal{D}'$ is the canonical linear series, where $\mathcal{D}'$ is a base-point-free 1-dimensional linear series of degree $(q+1)/3$. Let $P \in \mathcal{X}$ and assume $j_2(P) > 2$ according to Corollary 4.3. If $P \in \mathcal{X}(\mathbf{F}_{q^2})$, from Lemma 4.4(1) the result follows. Otherwise, $P \notin \mathcal{X}(\mathbf{F}_{q^2})$, and we have two possibilities according as q is odd or even (Lemma 4.4(2)).

Case 1: q is odd $j_2(P) = (q-1)/2$, $j_3(P) = (q+1)/2$. A similar property to (4.4) holds, namely $\delta + 1 \notin H(P)$ for any $(\frac{q-5}{3}\mathcal{D}_{\mathcal{X}}, P)$-order δ. Hence $2j_2(P) = 1 = q$ is not in $H(P)$, a contradiction.

Case 2: q is even, $j_2(P) = q/2$, $j_3(P) = (q+2)/2$. From the Case 3 in the proof of part (1), we have $m_1 = q/2$. Notice that the degree $(q+1)/3$ of the above linear series $\mathcal{D}'$ is coprime to m_1. Then by the well known Riemann's inequality for the genus g applied to $\mathcal{D}'$ and the linear series corresponding to m_1 we obtain $g \le (q-2)^2/6$, a contradiction.

The implication (b)⇒(c) is a special case of [15, Thm. 2.3] while (c)⇒(a) is trivial. □

4.2. The case of $(q-1)(q-3)/8$, q odd. The main result is Theorem 4.9 which is analogous to Theorem 4.5. It states that for $p \ge 5$ and q large enough, the non-singular $\mathbf{F}_{q^2}$-model of the curve of equation

$$y^q + y = x^{(q+1)/4}, \qquad q \equiv 3 \pmod 4, \tag{4.5}$$

together with the Fermat curve of degree $(q+1)/2$

$$x^{(q+1)/2} + y^{(q+1)/2} + 1 = 0. \tag{4.6}$$

are the unique $\mathbf{F}_{q^2}$-maximal curves of genus $g = (q-1)(q-3)/8$ provided that $\dim(\mathcal{D}_{\mathcal{X}}) = 5$ holds. The extra-condition on $\dim(\mathcal{D}_{\mathcal{X}})$ is assumed since the argument in Lemma 4.1 only proves that $\dim(\mathcal{D}_{\mathcal{X}}) \in \{4, 5\}$. Then $g = c_0(q+1, 5)$, and once again we take advantage of the hypothesis on the genus by means of Lemma 2.3.

The above two curves are in fact not isomorphic even over $\bar{\mathbf{F}}_{q^2}$; see [11, Remark 4.1]. The curve in (4.6) was characterized in [11] as the unique (up to $\mathbf{F}_{q^2}$-isomorphism) plane $\mathbf{F}_{q^2}$-maximal curve of degree $(q+1)/2$ provided that q is odd and $q \ge 11$.

As $\dim(2\mathcal{D}_{\mathcal{X}}) = 14$ by Lemma 2.3(1), we are able again to compute the possibilities for the sequence of $(\mathcal{D}_{\mathcal{X}}, P)$-orders for $P \in \mathcal{X}$. The proofs of the following two results will be omited since they are similar to those of Lemmas 4.2, 4.4, and Corollary 4.3. By Lemma 2.15(1) $j_1(P) = 1$ and either $j_5(P) = q+1$ if $P \in \mathcal{X}(\mathbf{F}_{q^2})$, or $j_5(P) = q$ otherwise.

Lemma 4.6. *Let $\mathcal{X}$ be a $\mathbf{F}_{q^2}$-maximal curve and $P \in \mathcal{X}$. Assume that $\dim(\mathcal{D}_{\mathcal{X}}) = 5, \dim(2\mathcal{D}_{\mathcal{X}}) = 14$, and that $q \ge 11$.*

(1) *If* $j_3(P) = 3$, *then* $j_4(P) = 4$.
(2) *Let* $j_2(P) = 2$ *but* $j_3(P) > 3$. *If* $P \in \mathcal{X}(\mathbf{F}_{q^2})$, *then* q *is odd,* $j_3(P) = (q+1)/2$, *and* $j_4(P) = (q+3)/2$. *If* $P \notin \mathcal{X}(\mathbf{F}_{q^2})$, *then* q *is even,* $j_3(P) = q/2$, *and* $j_4(P) = (q+2)/2$.
(3) *Let* $P \in \mathcal{X}(\mathbf{F}_{q^2})$ *and* $j_2(P) > 2$. *Assume* $g > (q-2)^2/9$ *if* $q \equiv 2 \pmod 3$ *and* $g > (q-3)q/9$ *if* $q \equiv 0 \pmod 3$. *Then either* $q \equiv 3 \pmod 4, j_2(P) = (q+1)/4, j_3(P) = 2(q+1)/4, j_4(P) = 3(q+1)/4$, *or* $q \equiv 0 \pmod 4, j_2(P) = (q+4)/4, j_3(P) = (2q+4)/4, j_4(P) = (3q+4)/4$.
(4) *Let* $P \notin \mathcal{X}(\mathbf{F}_{q^2})$ *and* $j_2(P) > 2$. *Then either* $q \equiv 1 \pmod 4, j_2(P) = (q+3)/4$, $j_3(P) = (2q+2)/4, j_4(P) = (3q+1)/4$, *or* $q \equiv 0 \pmod 4$, $j_2(P) = q/4$, $j_3(P) = 2q/4$, $j_4(P) = 3q/4$, *or* $q \equiv 1 \pmod 3$, $j_2(P) = (q-1)/3$, $j_3(P) = (q+2)/3$, $j_4(P) = (2q+1)/3$, *or* $q \equiv 0 \pmod 3, j_2(P) = q/3, j_3(P) = (q+3)/3, 2q/3$.

Corollary 4.7. *Let* $\mathcal{X}$ *be a* $\mathbf{F}_{q^2}$*-maximal curve of genus* g. *Assume that* $\dim(\mathcal{D}_\mathcal{X}) = 5$, $\dim(2\mathcal{D}_\mathcal{X}) = 14$, *and that* $q \geq 11$. *If* $j_3(P) = 3$ *for every* $P \in \mathcal{X}$, *then* $q \equiv 0, 4 \pmod 5$ *and* $g = (q^2 - 4q + 15)/20$.

Corollary 4.8. *Let* $\mathcal{X}$ *be a* $\mathbf{F}_{q^2}$*-maximal curve of genus* $(q-1)(q-3)/8$ *with* q *odd. Assume* $\dim(\mathcal{D}_\mathcal{X}) = 5$ *and* $q \geq 11$. *Then:*

(1) $\mathcal{X}$ *is* $\mathbf{F}_{q^2}$*-isomorphic to the non-singular* $\mathbf{F}_{q^2}$*-model of (4.5) if and only if there exists* $P \in \mathcal{X}(\mathbf{F}_{q^2})$ *with* $j_2(P) > 2$;
(2) $\mathcal{X}$ *is* $\mathbf{F}_{q^2}$*-isomorphic to (4.6) if and only if there exists* $P \in \mathcal{X}(\mathbf{F}_{q^2})$ *with* $j_2(P) = 2$, *and* $j_3(P) > 3$.

Proof. (1) Let P be the unique point over $x = \infty$. It is straightforward to check that $m_3(P) = 3(q+1)/4$. Hence $j_2(P) = (q+1)/4$ by Lemma 2.15(2). Conversely, from Lemma 4.6(3) we have $j_4(P) = 3(q+1)/4$ and so $m_1(P) = (q+1)/4$ by Lemma 2.15(3). Now, the result follows from [15, Thm. 2.3].

(2) We have $\mathcal{D}_\mathcal{X} = 2\mathcal{D}$, where $\mathcal{D}$ is the linear series cut out by lines on $\mathcal{X}$ ([11, Thm. 3.5]) and hence every $\mathbf{F}_{q^2}$-rational inflexion point P ([11, Lemma 3.6]) satisfies both $j_2(P) = 2$ and $j_3(P) > 3$. Conversely, from Lemmas 4.6(2), 2.15(2) we obtain both $m_1(P) = (q-1)/2$ and $m_2(P) = (q+1)/2$. Hence the result from [11, Thm. 1.1]. □

Theorem 4.9. *Let* $\mathcal{X}$ *be a* $\mathbf{F}_{q^2}$*-maximal curve of genus* $g = (q-1)(q-3)/8$ *with* q *odd. Assume* $\dim(\mathcal{D}_\mathcal{X}) = 5$, *and* $p \geq 5$.

(1) *If* $q \equiv 1 \pmod 4$ *and* $q \geq 17$, *then* $\mathcal{X}$ *is* $\mathbf{F}_{q^2}$*-isomorphic to the Fermat curve (4.6).*
(2) *If* $q \equiv 3 \pmod 4$ *and* $q \geq 19$, *then* $\mathcal{X}$ *is* $\mathbf{F}_{q^2}$*-isomorphic to either (4.6) or the non-singular* $\mathbf{F}_{q^2}$*-model of(4.5).*

Proof. We have already observed that $g = c_0(q+1, 5)$ and thus $\dim(2\mathcal{D}_\mathcal{X}) = 14$. In particular, by Corollary 4.7 there exists $P \in \mathcal{X}$ with $j_3(P) > 3$.

(1) Let $q \equiv 1 \pmod 4$. If $P \in \mathcal{X}(\mathbf{F}_{q^2})$, then Lemma 4.6(2)(3) yields $j_2(P) = 2$ and the result follows from Corollary 4.8(2). To show that this is actually the only possible case, assume on the contrary that $P \notin \mathcal{X}(\mathbf{F}_{q^2})$. Note that $\mathcal{K} := \frac{q-5}{4}\mathcal{D}_{\mathcal{X}}$ is the canonical linear series by Lemma 2.3(2), and hence that $\delta + 1 \notin H(P)$ for any $(\mathcal{K}, P)$-order δ. Recall that $m_4 = q$ by (2.9). Now, Lemma 4.6 together with $p \geq 5$ leads to the following two cases.

Case 1: $j_2(P) = (q+3)/4, j_3(P) = (2q+2)/4, j_4(P) = (3q+1)/4$. Here, $\{q - m_3, q - m_2, q - m_1\} \subseteq \{1, (q+3)/4, (2q+2)/4, (3q+1)/4\}$ by Lemma 2.15(3). Thus $m_1 = (2q-2)/4, m_2 = (3q-3), m_3 = q-1$. Now, $\delta = (q-9)/4 + (3q+1)/4 = q-2$ is a $(\mathcal{K}, P)$-order and hence $q - 1 \notin H(P)$, a contradiction.

Case 2: $q \equiv 1 \pmod 3, j_2(P) = (q-1)/3, j_3(P) = (q+2)/3, j_4(P) = (2q+1)/3$. Here, $\delta = 3j_2(P)$ is a $(\mathcal{K}, P)$-order (as $(q-5)/4 \geq 3$) and so q cannot belong to $H(P)$, a contradiction.

(2) $q \equiv 3 \pmod 4$. As above, if we show that $P \in \mathcal{X}(\mathbf{F}_{q^2})$, the result will follow from Corollary 4.8. If $P \notin \mathcal{X}(\mathbf{F}_{q^2})$, Lemma 4.6(2)(4) together with $p \geq 5$ yields $j_2(P) = (q-1)/3$. Now, Lemma 2.3(2) implies that $\delta + 1 \notin H(P)$ for every $(\frac{q-7}{4}\mathcal{D}_{\mathcal{X}}, P)$-order δ. On the other hand, as $(q-7)/4 \geq 3$, $3j_2(P) + 1 = q \in H(P)$, a contradiction. □

Remark 4.10. As pointed out in Introduction, $\mathbf{F}_{q^2}$-maximal curves of genus $g = \lfloor (q^2 - 2q + 5)/8 \rfloor$ do exist. This genus equals Halphen's number $c_1(4, q+1)$, cf. (2.2). So far, the following examples are known:

(i) For $q \equiv 0 \pmod 4$, curves of genus $(q^2 - 2q)/8$ belong to a family of $\mathbf{F}_{q^2}$-maximal curves constructed by van der Geer and van der Vlugt, see [25, Prop. 5.2(ii)], via fibre products of certain Artin-Schreier p-extensions of the projective line. See also [21, Thm. 3.3]. It seems plausible that a plane model for such a curve may be obtained from the proof of [19, Prop. 1.1].

(ii) For $q \equiv 1 \pmod 4$, curves of genus $(q-1)^2/8$ have been constructed as a quotient of the Hermitian curve $\mathcal{H}$ by a subgroup of the automorphism group of $\mathcal{H}$; see [13, Prop. 3.3(3)].

(iii) For $q \equiv 3 \pmod 4$, curves of genus $(q^2 - 2q + 5)/8$ have been constructed in a similar way as in (II) above; see [13, Prop. 3.3(3)(1)] or [21, Ex. 5.10].

For the curves mentioned in (ii) and (iii), no plane model seems to be available in the literature.

References

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

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

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

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

[5] E. Ballico, *Space curves not contained in low degree surfaces in positive characteristic*, preprint.

[6] E. Ballico and A. Cossidente, *On the generic hyperplane section of curves in positive characteristic*, J. Pure and Applied Algebra **102** (1995) 243-250.

[7] E. Ballico and A. Hefez, *On the Galois group associated to a generically etale morphism*, Comm. Algebra **14**(5) (1986), 899–909.

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

[9] L. Chiantini and C. Ciliberto, *Towards a Halphen theory of linera series on curves*, Trans. Amer. Math. Soc. **351**(6) (1999), 2197–2212.

[10] L. Chiantini, C. Ciliberto and V. Di Gennaro, *The genus of projective curves*, Duke Math. J. **70**(2) (1993), 229–245.

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

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

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

[14] D. Eisenbud and J. Harris, "Curves in projective space", Les Presses de l'Université de Montréal, Montréal, 1982.

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

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

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

[18] A. Garcia and L. Quoos, *A construction of curves over finite fields*, preprint May 2000.

[19] A. Garcia and H. Stichtenoth, *Elementary abelian p-extensions of algebraic function fields*, Manuscripta Math. **72** (1991), 67–79.

[20] A. Garcia and H. Stichtenoth, *Algebraic functions fields over finite fields with many places*, IEEE Trans. Inform. Theory **41**(6) (1995), 1548–1563.

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

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

[23] G. van der Geer and M. van der Vlugt, *Weight distribution for a certain class and maximal curves*, Discr. Math. **106/107** (1992), 209–218.

[24] G. van der Geer and M. van der Vlugt, *Fibre products of Artin-Schreier curves and generalized Hamming weights of codes*, J. Comb. Theory, ser. A **70** (1995), 337–348.

[25] G. van der Geer and M. van der Vlugt, *Quadratic forms, generalized Hamming weights of codes and curves with many points*, J. Number Theory **59** (1996), 20–36.

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

[27] G. van der Geer and M. van der Vlugt, *Generalized Reed-Müller codes and curves with many points*, Report W97-22, Mathematical Institute, University of Leiden, The Netherlands (alg-geom/9710016).
[28] G. van der Geer and M. van der Vlugt, *Kummer curves with many points*, preprint math.AG/9909037.
[29] G. van der Geer and M. van der Geer, *Tables of curves with many points*, July 2000, http://www.wins.uva.nl/~ geer.
[30] V.D. Goppa, "Geometry and Codes", Math. Appl., Kluwer Acad. Publ., Dordrecht, 1988.
[31] L. Gruson and C. Peskine, Genre des courbes de l'espace projetif, "Algebraic Geometry", Proc. Tromso, Norway", Lect. Notes in Math. Vol. 657, Springer-Verlag, Berlin, 1977.
[32] J. Harris, *The genus of space curves*, Math. Ann. **249**, (1980), 192–204.
[33] R. Hartshorne, "Algebraic Geometry", Grad. Texts in Math., Vol. 52, Springer-Verlag, New York/Berlin, 1977.
[34] A. Hefez and S. Kleiman, Notes on the duality of projective varieties, "Geometry Today", 143–183, Birkhäuser, 1985.
[35] J.W.P. Hirschfeld, "Projective Geometries over Finite Fields", second edition, Oxford University Press, Oxford, 1998.
[36] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Tokyo **28** (1981), 721–724.
[37] G. Korchmáros and F.Torres, Embedding of a maximal curve in a Hermitian variety, to appear in Compositio Math.
[38] J. Rathmann, *The uniform position principle for curves in characteristic p*, Math. Ann. **276** (1987), 565-579.
[39] H.G. Rück and H. Stichtenoth, *A characterization of Hermitian function fields over finite fields*, J. Reine Angew. Math. **457** (1994), 185–188.
[40] H. Stichtenoth and C. Xing, *The genus of maximal functions fields*, Manuscripta Math. **86** (1995), 217–224.
[41] K.O. Stöhr and J.F. Voloch, *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. **52** (1986), 1-19.

Dipartimento di Matematica, Universitá della Basilicata, via N. Sauro 85,, 85100 Potenza, Italy

E-mail address: korchmaros@unibas.it

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

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