Compositio Mathematica **121:** 163–181, 2000.

On Plane Maximal Curves

A. COSSIDENTE[1], J. W. P. HIRSCHFELD[2], G. KORCHMÁROS[1]
AND F. TORRES[3]
[1]*Dipartimento de Matematica, Università della Basilicata, Potenza, 85100, Italy.*
e-mail: {cossidente, korchmaros}@unibas.it
[2]*School of Mathematical Sciences, University of Sussex, Brighton BN1 9QH, United Kingdom.*
e-mail: jwph@sussex.ac.uk
[3]*IMECC-UNICAMP, Cx. P. 6065, Campinas, 13083-970-SP, Brazil.*
e-mail: ftorres@ime.unicamp.br

(Received: 3 March 1998; in final form: 4 December 1998)

Abstract. The number N of rational points on an algebraic curve of genus g overa finite field $\mathbb{F}_q$ satisfies the Hasse–Weil bound $N \leqslant q+1+2g\sqrt{q}$. A curve that attains this bound is called maximal. With $g_0 = \frac{1}{2}(q-\sqrt{q})$ and $g_1 = \frac{1}{4}(\sqrt{q}-1)^2$, it is known that maximalcurves have $g = g_0$ or $g \leqslant g_1$. Maximal curves with $g = g_0$ or g_1 have been characterized up to isomorphism. A natural genus to be studied is $g_2 = \frac{1}{8}(\sqrt{q}-1)(\sqrt{q}-3)$, and for this genus there are two non-isomorphic maximal curves known when $\sqrt{q} \equiv 3 \pmod 4$. Here, a maximal curve with genus g_2 and a non-singular plane model is characterized as a Fermat curve of degree $\frac{1}{2}(\sqrt{q}+1)$.

Mathematics Subject Classifications (2000): Primary 11Gxx, Secondary 14Gxx.

Key words: finite field, maximal curve, linear series.

1. Introduction

For a non-singular model of a projective, geometrically irreducible, algebraic curve $\mathcal{X}$ defined over a finite field $\mathbb{F}_q$ with q elements, the number N of its $\mathbb{F}_q$-rational points satisfies the Hasse–Weil bound, namely (see [We], [Sti, §V.2])

$$|N-(q+1)| \leqslant 2g\sqrt{q}\,.$$

If $\mathcal{X}$ is plane of degree d, then this bound implies that

$$|N-(q+1)| \leqslant (d-1)(d-2)\sqrt{q}\,. \tag{1.1}$$

These bounds are important for applications in Coding theory (see, for example, [Sti]) and in finite geometry (see [H, Ch. 10]). In these subjects, one is often interested in curves with *many* $\mathbb{F}_q$-rational points and, in particular, *maximal curves*, that is, curves where N reaches the upper Hasse–Weil bound.

The approach of Stöhr and Voloch [SV] to the Hasse–Weil bound shows that an upper bound for N can be obtained via $\mathbb{F}_q$-linear series. This upper bound depends

https://doi.org/10.1023/A:1001826520682 Published online by Cambridge University Press

not only on q and g, as does the Hasse–Weil bound, but also on the dimension and the degree of the linear series.

In [HK1] an upper bound for N was found in the case that $\mathcal{X}$ is a plane curve. It turns out that this bound is better than the upper bound from (1.1) under certain conditions on d and q. The bound in [HK1] is not symmetrical in the different types of points that a non-singular plane curve has. In fact, two types of $\mathbb{F}_q$-rational points of $\mathcal{X}$ are distinguished: (a) regular points (non-inflexion points), and (b) inflexion points. Let M_q and M'_q be the numbers of type (a) and (b) respectively. If d and q satisfy certain restrictions, then

$$2M_q + M'_q \leqslant d(q - \sqrt{q} + 1), \tag{1.2}$$

and equality holds if and only if $\mathcal{X}$ is a non-singular plane maximal curve over $\mathbb{F}_q$ of degree $d = \frac{1}{2}(\sqrt{q} + 1)$. Actually, (1.2) holds true for any (possible singular) irreducible plane curve $\mathcal{C}$ defined over $\mathbb{F}_q$ provided that M_q and M'_q are introduced in the following way. Let $\mathcal{X}$ be the normalization of $\mathcal{C}$, and let g^2_d be the linear series associated to the morphism $\pi\colon \mathcal{X} \to \mathcal{C}$. For a point P of X let (j_0, j_1, j_2) be the order sequence of $\mathcal{X}$ at P with respect to g^2_d. If $\pi(P)$ is centred at an $\mathbb{F}_q$-rational point, then P is of type (a) or (b) according as $j_2 = 2j_1$ or not. In [HK1] the result was also phrased in terms of branches (or places), in the same terminology as [Wa, Chapter IV]; a branch $\pi(P)$ has order α and class β if $(0, \alpha, \alpha + \beta)$ is the order sequence of $\mathcal{X}$ at P with respect to g^2_d. The result given by (1.2) is the starting point of our research.

An example of a curve attaining the equality in (1.2) is provided by the Fermat curve $\mathcal{F}$ (see Section 3) with equation, in homogeneous coordinates (U, V, W),

$$U^{(\sqrt{q}+1)/2} + V^{(\sqrt{q}+1)/2} + W^{(\sqrt{q}+1)/2} = 0. \tag{1.3}$$

The main result of the paper is to show the following converse (see Section 5).

THEOREM 1.1. *If $\mathcal{X}$ is a non-singular plane maximal curve over $\mathbb{F}_q$ of degree $\frac{1}{2}(\sqrt{q} + 1)$, then it is $\mathbb{F}_q$-isomorphic to $\mathcal{F}$ when $q \geqslant 121$.*

This result is connected to recent investigations on the genus of maximal curves [FT], [FGT], [FT1]. The genus g of a maximal curve $\mathcal{X}$ over $\mathbb{F}_q$ is at most $\frac{1}{2}\sqrt{q}(\sqrt{q} - 1)$ [Ih], [Sti, §V.2] with equality holding if and only if $\mathcal{X}$ is $\mathbb{F}_q$-isomorphic to the Hermitian curve with equation

$$u^{\sqrt{q}+1} + v^{\sqrt{q}+1} + w^{\sqrt{q}+1} = 0,$$

[R-Sti]. In [FT] it was observed that

$$g \leqslant \tfrac{1}{4}(\sqrt{q} - 1)^2 \quad \text{if} \quad g < \tfrac{1}{2}\sqrt{q}(\sqrt{q} - 1),$$

https://doi.org/10.1023/A:1001826520682 Published online by Cambridge University Press

a result conjectured in [Sti-X]. Also, if q is odd and

$$\tfrac{1}{4}(\sqrt{q}-1)(\sqrt{q}-2) < g \leqslant \tfrac{1}{4}(\sqrt{q}-1)^2\,,$$

then $g = \frac{1}{4}(\sqrt{q}-1)^2$ and $\mathcal{X}$ is $\mathbb{F}_q$-isomorphic to the non-singular model of the curve with affine equation $y^q + y = x^{(\sqrt{q}+1)/2}$ [FGT, Thm. 3.1], [FT1, Prop. 2.5]. In general, the situation for either q odd and $g \leqslant \frac{1}{4}(\sqrt{q}-1)(\sqrt{q}-2)$ or q even and $g \leqslant \frac{1}{4}\sqrt{q}(\sqrt{q}-2)$ is unknown. In the latter case, an example where equality holds is provided by the non-singular model of the curve with affine equation

$$\sum_{i=1}^{t} y^{\sqrt{q}/2^i} = x^{q+1}\,, \qquad \sqrt{q} = 2^t\,,$$

and it seems that this example may be the only one up to $\mathbb{F}_q$-isomorphism [AT].

In [FGT, §2] the maximal curves obtained from the affine equation $y^{\sqrt{q}} + y = x^m$, where m is a divisor of $(\sqrt{q}+1)$, are characterized by means of Weierstrass semigroups at an $\mathbb{F}_q$-rational point; the genera of these curves are given by $g = \frac{1}{2}(\sqrt{q}-1)(m-1)$. If $m = \frac{1}{4}(\sqrt{q}+1)$ and $\sqrt{q} \equiv 3 \pmod 4$, we find two curves of genus $\frac{1}{8}(\sqrt{q}-1)(\sqrt{q}-3)$, namely the curve with affine equation $y^{\sqrt{q}} + y = x^{(\sqrt{q}+1)/4}$ and the curve $\mathcal{F}$ of our main result. It turns out that these curves are not $\bar{\mathbb{F}}_q$-isomorphic (see Remark 4.1(ii)). As far as we know, this is the first example of two maximal curves of a given genus that are not $\mathbb{F}_q$-isomorphic for infinitely many values of q. It is an interesting open problem to decide if the two examples of maximal curves with genus g_2 are the only ones.

As in [HK], [HK1], [FT], [FGT], [FT1], the key tool used to carry out the research here is the approach of Stöhr and Voloch [SV] to the Hasse–Weil bound applied to suitable $\mathbb{F}_q$-linear series on the curve.

Convention. From now on, the word *curve* means a projective, geometrically irreducible, non-singular, algebraic curve.

2. Background

In this section we summarize background material concerning Weierstrass points and Frobenius orders from [SV, §§1–2].

Let $\mathcal{X}$ be a curve of genus g defined over $\bar{\mathbb{F}}_q$ equipped with the action of the Frobenius morphism $\Phi_{\mathcal{X}}$ over $\mathbb{F}_q$. Let $\mathcal{D}$ be a g^r_d on $\mathcal{X}$ and suppose that it is defined over $\mathbb{F}_q$. Then associated to $\mathcal{D}$ there exist two divisors on $\mathcal{X}$, namely the *ramification divisor*, denoted by $R = R^{\mathcal{D}}$, and the $\mathbb{F}_q$-*Frobenius divisor*, denoted by $S = S^{\mathcal{D}} = S^{(\mathcal{D},q)}$. Both divisors describe the geometrical and arithmetical properties of $\mathcal{X}$; in particular, the divisor S provides information on the number $\#\mathcal{X}(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points of $\mathcal{X}$.

https://doi.org/10.1023/A:1001826520682 Published online by Cambridge University Press

For $P \in \mathcal{X}$, let $j_i(P)$ be the ith $(\mathcal{D}, P)$-order, $\varepsilon_i = \varepsilon_i^{\mathcal{D}}$ be the ith $\mathcal{D}$-order $(i = 0, \ldots, r)$, and $\nu_i = \nu_i^{(\mathcal{D},q)}$ be the ith $\mathbb{F}_q$-Frobenius order of $\mathcal{D}$ $(i = 0, \ldots, r-1)$. The curve $\mathcal{X}$ is *$\mathcal{D}$-classical*, or $\mathcal{D}$ is *classical*, if $(\varepsilon_0, \ldots, \varepsilon_r) = (0, \ldots, r)$. Similarly, $\mathcal{X}$ is *$\mathcal{D}$-Frobenius classical*, or $\mathcal{D}$ is *Frobenius classical*, if $(\nu_0, \ldots, \nu_{r-1}) = (0, \ldots, r-1)$. Then the following properties hold:

(1) $\deg(R) = (2g-2)\sum_{i=0}^{r} \varepsilon_i + (r+1)d$;
(2) $j_i(P) \geqslant \varepsilon_i$ for each i and each P;
(3) $v_P(R) \geqslant \sum_{i=0}^{r}(j_i(P) - \varepsilon_i)$ and equality holds if and only if $\det(\binom{j_i(P)}{\varepsilon_j}) \not\equiv 0 \pmod{p}$;
(4) (ν_i) is a subsequence of (ε_i);
(5) $\deg(S) = (2g-2)\sum_{i=0}^{r-1} \nu_i + (q+r)d$;
(6) $\nu_i \leqslant j_{i+1}(P) - j_1(P)$, for each i and each $P \in \mathcal{X}(\mathbb{F}_q)$;
(7) $v_P(S) \geqslant \sum_{i=0}^{r-1}(j_{i+1}(P) - \nu_i)$, for each $P \in \mathcal{X}(\mathbb{F}_q)$, and equality holds if and only if $\det(\binom{j_{i+1}(P)}{\nu_j}) \not\equiv 0 \pmod{p}$.

Therefore, if $P \in \mathcal{X}(\mathbb{F}_q)$, properties (6) and (7) imply

(8) $v_P(S) \geqslant r j_1(P)$.

Consequently, from (5) and (8), we obtain the main result of [SV], namely,

(9) $\#\mathcal{X}(\mathbb{F}_q) \leqslant \deg(S)/r$.

3. Plane Maximal Curves of Degree $(\sqrt{q}+1)/2$

Throughout this section we use the following notation:

(a) Σ_1 is the linear series on a plane curve over $\mathbb{F}_q$ obtained from lines of $\mathbb{P}^2(\mathbb{F}_q)$, and Σ_2 is the series obtained from conics;
(b) for $i = 1, 2$, the divisor R_i is the ramification divisor and S_i is the $\mathbb{F}_q$-Frobenius divisor associated to Σ_i;
(c) $j_n^i(P)$ is the nth (Σ_i, P)-order;
(d) $\varepsilon_n^i = \varepsilon_n^{\Sigma_i}$ and $\nu_n^i = \nu_n^{(\Sigma_i,q)}$;
(e) $p = \operatorname{char}(\mathbb{F}_q)$.

LEMMA 3.1. *Let $\mathcal{X}$ be a plane non-singular curve over $\mathbb{F}_q$ of degree d. If $d \not\equiv 1 \pmod{p}$, then $\mathcal{X}$ is classical for Σ_1.*

Proof. See [Par, Corollary 2.2] for $p > 2$ and [Ho, Corollary 2.4] for $p \geqslant 2$.

https://doi.org/10.1023/A:1001826520682 Published online by Cambridge University Press

COROLLARY 3.2. *Let $\mathcal{X}$ be a plane non-singular maximal curve over $\mathbb{F}_q$ of degree d with $d \not\equiv 1 \pmod{p}$ and $2 < d \leqslant (\sqrt{q}+1)^2/3$. Then there exists $P_0 \in \mathcal{X}(\mathbb{F}_q)$ whose (Σ_1, P_0)-orders are* $0, 1, 2$.

Proof. Suppose that $j_2^1(P) > 2$ for each $P \in \mathcal{X}(\mathbb{F}_q)$. Then by Section 2(3) and the previous lemma we would have $v_P(R_1) \geqslant 1$ for such points P. Consequently, by Section 2(1) and the maximality of $\mathcal{X}$, it follows that

$$\deg(R_1) = 3(2g-2) + 3d \geqslant \#\mathcal{X}(\mathbb{F}_q) = (\sqrt{q}+1)^2 + \sqrt{q}(2g-2),$$

so that

$$0 \geqslant (\sqrt{q}+1)\left(\sqrt{q}+1-\frac{3d}{\sqrt{q}+1}\right) + (2g-2)(\sqrt{q}-3)\,,$$

a contradiction.

Note that the hypothesis on d rules out the possibility $q = 4$.

Throughout the remainder of the paper, let $\mathcal{X}$ be a plane non-singular maximal curve of degree d. We have the following relation between (Σ_1, P)-orders and (Σ_2, P)-orders for $P \in \mathcal{X}$.

Remark 3.3 [GV, p. 464]. For $P \in \mathcal{X}$, the set

$$\{j_1^1(P), j_2^1(P), 2j_1^1(P), j_1^1(P) + j_2^1(P), 2j_2^1(P)\}$$

is contained in the set of (Σ_2, P)-orders.

Now suppose that d satisfies the hypotheses in Corollary 3.2 and let $P_0 \in \mathcal{X}(\mathbb{F}_q)$ be as in this corollary. Then, by Remark 3.3 and the fact that $\dim(\Sigma_2) = 5$, the (Σ_2, P_0)-orders are $0, 1, 2, 3, 4$ and $j := j_5^2(P_0)$ with $5 \leqslant j \leqslant 2d$. Therefore, by Section 2(2), (6), (4),

(a) the Σ_2-orders are $0, 1, 2, 3, 4$ and $\varepsilon := \varepsilon_5^2$ with $5 \leqslant \varepsilon \leqslant j$;
(b) the $\mathbb{F}_q$-Frobenius orders are $0, 1, 2, 3$ and $v := v_4^2$ with $v \in \{4, \varepsilon\}$.

COROLLARY 3.4. *Let $\mathcal{X}$ be a plane non-singular maximal curve over $\mathbb{F}_q$ of degree $d = \frac{1}{2}(\sqrt{q}+1)$. If $\sqrt{q} \geqslant 11$, then*

(1) *the Σ_2-orders are* $0, 1, 2, 3, 4, \sqrt{q}$;
(2) *the $\mathbb{F}_q$-Frobenius orders of Σ_2 are* $0, 1, 2, 3, \sqrt{q}$.

Proof. The curve $\mathcal{X}$ satisfies the hypotheses in Corollary 3.2. So, with the above notation, we have to show that $\varepsilon = v = \sqrt{q}$.

(a) First it is shown that $v = \varepsilon$.

We have already seen that $v \in \{4, \varepsilon\}$. From Section 2(5), (8) and the maximality of $\mathcal{X}$ we have that

$$\begin{aligned}\deg(S_2) &= (6+v)(2g-2) + (q+5)(\sqrt{q}+1) \\ &\geqslant 5\#\mathcal{X}(\mathbb{F}_q) \\ &= 5(\sqrt{q}+1)^2 + 5\sqrt{q}(2g-2),\end{aligned}$$

so that

$$(\sqrt{q}-5)(\sqrt{q}-6-v) \leqslant 0\,. \tag{3.1}$$

Then, if $v = 4$, we would have $\sqrt{q} \leqslant 10$, a contradiction.

(b) Now, p divides ε (see [G-Ho, Corollary 3]). From Section 2(6) and (a),

$$v = \varepsilon \leqslant j_5(P_0) - j_1(P_0) \leqslant \sqrt{q}\,.$$

Therefore, from (3.1), the fact that $\sqrt{q} > 5$, and (a),

$$\varepsilon \in \{\sqrt{q}-6, \sqrt{q}-5, \sqrt{q}-4, \sqrt{q}-3, \sqrt{q}-2, \sqrt{q}-1, \sqrt{q}\}\,.$$

Since $p > 2$ and p divides ε, the possibilities are reduced to the following:

$$\varepsilon \in \{\sqrt{q}-6, \sqrt{q}-5, \sqrt{q}-3, \sqrt{q}\}\,.$$

If $\varepsilon = \sqrt{q}-6$, then $p = 3$ and by the p-adic criterion [SV, Corollary 1.9] $\varepsilon = 6$ and so $\sqrt{q} = 12$, a contradiction.

If $\varepsilon = \sqrt{q}-5$, then $p = 5$. Since $\binom{\sqrt{q}-5}{5} \not\equiv 0 \pmod 5$, by the p-adic criterion we would have that 5 is also a Σ_2-order, a contradiction.

If $\varepsilon = \sqrt{q}-3$, then $p = 3$ and so $\sqrt{q} = 9$, which is eliminated by the hypothesis that $\sqrt{q} \geqslant 11$.

Hence $\varepsilon = \sqrt{q}$, which completes the proof.

Now the main result of this section can be stated. We recall that a maximal curve $\mathcal{X}$ over $\mathbb{F}_q$ is equipped with the $\mathbb{F}_q$-linear series $\mathcal{D}_{\mathcal{X}} := |(\sqrt{q}+1)P_0|$, $P_0 \in \mathcal{X}(\mathbb{F}_q)$, which is independent of P_0 and provides a lot of information about the curve (see [FGT, §1]).

THEOREM 3.5. *Let $\mathcal{X}$ be a plane maximal curve over $\mathbb{F}_q$ of degree $\frac{1}{2}(\sqrt{q}+1)$. Suppose that $\sqrt{q} \geqslant 11$. Then the linear series $\mathcal{D}_{\mathcal{X}}$ is the linear series Σ_2 cut out by conics.*

Proof. First it is shown that, for $P \in \mathcal{X}(\mathbb{F}_q)$, the intersection divisor of the osculating conic $\mathcal{C}_P^{(2)}$ and $\mathcal{X}$ satisfies

$$\mathcal{C}_P^{(2)}.\mathcal{X} = (\sqrt{q}+1)P. \tag{3.2}$$

To show this, let $P \in \mathcal{X}(\mathbb{F}_q)$; then, by Corollary 3.4(1) and Section 2(6), we have that $v = \sqrt{q} \leqslant j_5(P) - j_1(P) \leqslant \sqrt{q}$ (recall that $\deg(\Sigma_2) = \sqrt{q}+1$). Consequently $j_5^2(P) = \sqrt{q}+1$ and so (3.2) follows.

This implies that $\Sigma_2 \subseteq \mathcal{D}_{\mathcal{X}}$. Then to show the equality it is enough to show that $n+1 := \dim(\mathcal{D}_{\mathcal{X}}) \leqslant 5$. To see this we use Castelnuovo's genus bound for curves in projective spaces as given in [FGT, p. 34]: the genus g of $\mathcal{X}$ satisfies

$$2g \leqslant \begin{cases} (2\sqrt{q}-n)^2/(4n) & \text{if } n \text{ is even,} \\ ((2\sqrt{q}-n)^2-1)/(4n) & \text{if } n \text{ is odd.} \end{cases}$$

Suppose that $n+1 \geqslant 6$. Then, since $2g = (\sqrt{q}-1)(\sqrt{q}-3)/4$, we would have

$$(\sqrt{q}-1)(\sqrt{q}-3)/4 \leqslant ((2\sqrt{q}-5)^2-1)/20 = (\sqrt{q}-3)(\sqrt{q}-2)/5\,,$$

a contradiction. This finishes the proof.

Next we compute the (Σ_1, P)-orders for $P \in \mathcal{X}$.

LEMMA 3.6. *Let $\mathcal{X}$ be a plane maximal curve over $\mathbb{F}_q$ of degree $\frac{1}{2}(\sqrt{q}+1)$ and let $P \in \mathcal{X}$.*

(1) *Two types of $\mathbb{F}_q$-rational points of $\mathcal{X}$ are distinguished*:
   (a) *regular points, that is, points whose (Σ_1, P)-orders are $0, 1, 2$, so that $v_P(R_1) = 0$;*
   (b) *inflexion points, that is, points whose (Σ_1, P)-orders are $0, 1, \frac{1}{2}(\sqrt{q}+1)$, so that $v_P(R_1) = (\sqrt{q}-3)/2$.*

(2) *If $P \notin \mathcal{X}(\mathbb{F}_q)$, the (Σ_1, P)-orders are $0, 1, 2$, so that $v_P(R_1) = 0$.*

Proof. For each $P \in \mathcal{X}$ we have that $j_1^1(P) = 1$ because $\mathcal{X}$ is non-singular. So we just need to compute $j(P) := j_2^1(P)$.

We know that $\mathcal{D}_{\mathcal{X}} = \Sigma_2 = 2\Sigma_1$, $\dim(\Sigma_2) = 5$, and that $j_5^2(P) = \sqrt{q}+1$ provided that $P \in \mathcal{X}(\mathbb{F}_q)$ (see proof of Theorem 3.5). In addition, by [FGT, Thm. 1.4(ii)], $j_5^2(P) = \sqrt{q}$ for $P \notin \mathcal{X}(\mathbb{F}_q)$.

Suppose that $j(P) > 2$. Then from Remark 3.3 we must have $j_5^2(P) = 2j(P)$. Since $\sqrt{q}$ is odd, this is the case if and only if $2j(P) = \sqrt{q}+1$ and $P \in \mathcal{X}(\mathbb{F}_q)$, because of the above computations.

The computations for $v_P(R_1)$ follow from Section 2(3).

Let

$$M_q = M_q(\mathcal{X}) := \#\{P \in \mathcal{X}(\mathbb{F}_q) : j_2^1(P) = 2\},$$

and

$$M'_q = M'_q(\mathcal{X}) := \#\{P \in \mathcal{X}(\mathbb{F}_q) : j_2^1(P) = \tfrac{1}{2}(\sqrt{q}+1)\}.$$

THEOREM 3.7. *Let $\mathcal{X}$ be a plane maximal curve over $\mathbb{F}_q$ of degree $\frac{1}{2}(\sqrt{q}+1)$. Suppose that $\sqrt{q} \geqslant 11$. Then*

(1) $M_q = (\sqrt{q}+1)(q-\sqrt{q}-2)/4$;
(2) $M'_q = 3(\sqrt{q}+1)/2$.

https://doi.org/10.1023/A:1001826520682 Published online by Cambridge University Press

Proof. By Lemma 3.6,

$$M_q + M'_q = \#\mathcal{X}(\mathbb{F}_q). \tag{3.3}$$

From this result, Lemma 3.1 and §2(1),

$$\deg(R_1) = 3(2g-2) + \frac{3(\sqrt{q}+1)}{2} = \frac{\sqrt{q}-3}{2} M'_q. \tag{3.4}$$

The result now follows from (3.3) and (3.4), by taking into consideration the maximality of $\mathcal{X}$ and that $2g-2 = (\sqrt{q}-5)(\sqrt{q}+1)/4$.

4. The Example

In this section we study an example of a plane maximal curve of degree $\frac{1}{2}(\sqrt{q}+1)$. In the next section we will see that this example is, up to $\mathbb{F}_q$-isomorphism, the unique plane maximal curve of degree $\frac{1}{2}(\sqrt{q}+1)$.

Let q be a square power of a prime $p \geqslant 3$, and let $\mathcal{F}$ be the Fermat curve given by (1.3). Then $\mathcal{F}$ is non-singular and maximal. This is because $\mathcal{F}$ is covered by the Hermitian curve with equation $u^{\sqrt{q}+1} + v^{\sqrt{q}+1} + w^{\sqrt{q}+1} = 0$ via the morphism $(u, v, w) \mapsto (U, V, W) = (u^2, v^2, w^2)$ (La, Prop. 6).

Remark 4.1. (i) The inflexion points of $\mathcal{F}$ relative to Σ_1 are the ones over $U = \lambda$, over $V = \lambda$ and over $W = \lambda$ for λ a $(\sqrt{q}+1)/2$th root of -1. To see this we observe that the morphism $U : \mathcal{F} \to \mathbb{P}^1(\bar{\mathbb{F}}_q)$ has $(\sqrt{q}+1)/2$ points, say $Q_1, \ldots, Q_{(\sqrt{q}+1)/2}$ over $U = \infty$ and it has just one point, say P_i, over $U = \lambda_i$ with $\lambda_i^{(\sqrt{q}+1)/2} = -1$. Hence, for each $i = 1, \ldots, (\sqrt{q}+1)/2$, $\operatorname{div}(U - \alpha_i) = \frac{1}{2}(\sqrt{q}+1)P_i - \sum_j Q_j$. A similar result holds for $\operatorname{div}(V - \alpha_i)$ and $\operatorname{div}(W - \alpha_i)$.

(ii) The Weierstrass semigroup at any of the $3(\sqrt{q}+1)/2$ points above is $\langle 2(\sqrt{q}-1), 2(\sqrt{q}+1)\rangle$.

The fact that $(\sqrt{q}-1)/2$ is a non-gap at an inflexion point is explained as follows. In (i), the affine functions U, V, W are really the projective functions $U/W, V/W, W/U$. Hence $\operatorname{div}(1/(U/W) - \alpha_i) = \sum_j Q_j - \frac{1}{2}(\sqrt{q}+1)P_i$ and $\operatorname{div}(V/W) = \sum_j P_j - \sum_j Q_j$. Then by using the product of both functions we find that $(\sqrt{q}-1)/2$ is a Weierstrass non-gap at P_i.

Since this semigroup cannot be the Weierstrass semigroup at a point of the non-singular model $\mathcal{X}$ of $y^{\sqrt{q}} + y = x^{(\sqrt{q}+1)/4}$, $\sqrt{q} \equiv 3 \pmod 4$, [G-Vi], we conclude that $\mathcal{F}$ is not $\bar{\mathbb{F}}_q$-isomorphic to $\mathcal{X}$; hence these curves are not $\mathbb{F}_q$-isomorphic.

Let $\lambda_1, \ldots, \lambda_{(\sqrt{q}-1)/2}, \lambda := \lambda_{(\sqrt{q}+1)/2}$ be the roots of $T^{(\sqrt{q}+1)/2} = -1$, and so each λ_i is in $\mathbb{F}_q$. Let $\mathcal{Y}$ be the non-singular model of the affine curve with equation

$$X^{(\sqrt{q}+1)/2} = F(Y), \tag{4.1}$$

with $F(Y) \in \mathbb{F}_q[Y]$ satisfying the following properties:

(a) $\deg F = (\sqrt{q}-1)/2$;
(b) the roots of F are $c_j := (\lambda_j - \lambda)^{-1}$, $j = 1, \ldots, (\sqrt{q}-1)/2$;
(c) either $F(0)^{\sqrt{q}-1} = 1$ or $F(0)^{\sqrt{q}-1} = -1$.

PROPOSITION 4.2. *The curve $\mathcal{F}$ is $\mathbb{F}_q$-isomorphic to $\mathcal{Y}$.*

Proof. Write $f = U^{(\sqrt{q}+1)/2} = \sum_{j=0}^{(\sqrt{q}+1)/2} A_j(U-\lambda)^j$ with $A_j = (D_U^j f)(\lambda)$ and D_U^j the jth Hasse derivative. We have that $A_0 = -1$ and $A_{(\sqrt{q}+1)/2} = 1$, so that

$$\frac{U^{(\sqrt{q}+1)/2}+1}{(U-\lambda)^{(\sqrt{q}+1)/2}} = \sum_{j=1}^{(\sqrt{q}+1)/2} A_j \frac{1}{(U-\lambda)^{(\sqrt{q}+1)/2-j}}\,. \tag{4.2}$$

Also, Equation (1.3) with $W = 1$ is equivalent to

$$\left[\frac{V}{U-\lambda}\right]^{(\sqrt{q}+1)/2} = \sum_{j=1}^{(\sqrt{q}+1)/2} \frac{-A_j}{(U-\lambda)^{(\sqrt{q}+1)/2-j}}\,.$$

Consequently, for $X = V/(U-\lambda)$ and $Y = 1/(U-\lambda)$ we obtain an equation of type (4.1). From (4.2),

$$F(Y) = \sum_{j=1}^{(\sqrt{q}+1)/2} (-A_j) = -Y^{(\sqrt{q}+1)/2}\left[\left(\frac{1}{Y}+\lambda\right)^{(\sqrt{q}+1)/2} + 1\right]$$

belongs to $\mathbb{F}_q[Y]$, it has degree $(\sqrt{q}-1)/2$, its roots are $(\lambda_j-\lambda)^{-1}$ $(j = 1, \ldots, (\sqrt{q}-1)/2)$, and $F(0) = A_{(\sqrt{q}+1)/2} \in \mathbb{F}_{\sqrt{q}}$.

Conversely, let us start with (4.1). Writing $F(Y) = k\prod_{j=1}^{(\sqrt{q}-1)/2}(Y-c_j)$ with $k \in \mathbb{F}_q^*$, $c_j := \lambda_j - \lambda$, and setting $X = V/(U-\lambda)$ and $Y = 1/(U-\lambda)$, from (4.1) we find that

$$V^{(\sqrt{q}+1)/2} = k(-1)^{(\sqrt{q}-1)/2}\prod_j c_j(U^{(\sqrt{q}+1)/2}+1)\,.$$

Since $k(-1)^{(\sqrt{q}-1)/2}\prod_j c_j = F(0) =: c^{-1}$, we then have an equation of type

$$cV^{(\sqrt{q}+1)/2} = U^{(\sqrt{q}+1)/2} + 1 \text{ with } c^{2(\sqrt{q}-1)} = 1. \tag{4.3}$$

Let $\varepsilon \in \bar{\mathbb{F}}_p$ such that $c\varepsilon^{(\sqrt{q}+1)/2} = -1$. Then (4.3) implies that $\varepsilon \in \mathbb{F}_q^*$. Then setting $V = \varepsilon V'$ we obtain an equation of type (1.3) with $W = 1$.

5. Proof of the Main Result

Throughout the whole section we let $q \geqslant 121$ and fix the following notation:

(a) $\mathcal{X}$ is a non-singular plane maximal curve over $\mathbb{F}_q$ of degree $\frac{1}{2}(\sqrt{q}+1)$;
(b) $f = 0$ is a minimal equation of $\mathcal{X}$ with $f \in \mathbb{F}_q[X, Y]$.

https://doi.org/10.1023/A:1001826520682 Published online by Cambridge University Press

From Lemma 3.1 and Corollary 3.4, $\mathcal{X}$ has the following properties:

(i) $\mathcal{X}$ is classical for Σ_1;
(ii) $\mathcal{X}$ is non-classical for Σ_2;
(iii) $\mathcal{X}$ is Frobenius non-classical for Σ_2.

Plane curves satisfying (i), (ii), (iii) above have been characterized in terms of their equations [GV], [HK1].

LEMMA 5.1. *There exist* $h, s, z_0, \ldots, z_5 \in \mathbb{F}_q[X, Y]$ *such that*

$$hf = z_0^{\sqrt{q}} + z_1^{\sqrt{q}}X + z_2^{\sqrt{q}}Y + z_3^{\sqrt{q}}X^2 + z_4^{\sqrt{q}}XY + z_5^{\sqrt{q}}Y^2 \tag{5.1}$$

and

$$sf = z_0 + z_1X^{\sqrt{q}} + z_2Y^{\sqrt{q}} + z_3X^{2\sqrt{q}} + z_4(XY)^{\sqrt{q}} + z_5Y^{2\sqrt{q}}. \tag{5.2}$$

For a point $P = (a, b, 1) \in \mathcal{X}$ *such that* $z_i(a, b) \neq 0$ *for at least one index* i, $0 \leqslant i \leqslant 5$, *the conic with equation*

$$z_0(a, b) + z_1(a, b)X + z_2(a, b)Y + z_3(a, b)X^2 + z_4(a, b)XY + z_5(a, b)Y^2 = 0$$

is the osculating conic of $\mathcal{X}$ *at* P.

Note that Equation (5.2) is invariant under any change of projective coordinates. To see how the polynomials z_i change, we introduce the matrix

$$\Delta(z_0, \ldots, z_5) = \begin{pmatrix} 2z_0 & z_1 & z_2 \\ z_2 & 2z_3 & z_4 \\ z_3 & z_4 & 2z_5 \end{pmatrix}, \tag{5.3}$$

and use homogeneous coordinates $(X) = (X_0, X_1, X_2)$. Now, if the change from (X) to (X') is given by $(X) = A(X')$ where A is a non-singular matrix over $\bar{\mathbb{F}}_q$, then (5.2) becomes, again in non-homogeneous coordinates,

$$HF = Z_0^{\sqrt{q}} + Z_1^{\sqrt{q}}X' + Z_2^{\sqrt{q}}Y' + Z_3^{\sqrt{q}}X'^2 + Z_4^{\sqrt{q}}X'Y' + Z_5^{\sqrt{q}}Y'^2, \tag{5.4}$$

where $H, F, Z_0, \ldots, Z_5 \in \bar{\mathbb{F}}_q[X', Y']$ and $F = 0$ is the equation of $\mathcal{X}$ with respect to the new coordinate system. Also,

$$\Delta(Z_0, \ldots Z_5) = B^{tr}\Delta(z_0, \ldots, z_5)B, \tag{5.5}$$

where B is the matrix satisfying $B^{\sqrt{q}} = A$. If A is a matrix over $\mathbb{F}_q$, then $Z_0, \ldots, Z_5 \in \mathbb{F}_q[X', Y']$, and (5.1) becomes

$$SF = Z_0 + Z_1X'^{\sqrt{q}} + Z_2Y'^{\sqrt{q}} + Z_3X'^{2\sqrt{q}} + Z_4(X'Y')^{\sqrt{q}} + Z_5Y'^{2\sqrt{q}}. \tag{5.6}$$

For a rational function $u \in \bar{\mathbb{F}}_q(\mathcal{X})$, the symbol $v_P(u)$ denotes the order of u at $P \in \mathcal{X}$. Note that z_i, for $0 \leqslant i \leqslant 5$, can be viewed as a rational function of $\bar{\mathbb{F}}_q(\mathcal{X})$. We define $e_P := -\min_{0 \leqslant i \leqslant 5} v_P(z_i)$.

LEMMA 5.2. *For $P \in \mathcal{X}$, the order $v_P(\det(\Delta(z_0, \ldots, z_5)))$ is either $2 + e_P$ or e_P according as P is an inflexion point or not.*

Proof. Take P as the origin and the tangent to $\mathcal{X}$ at P as the X-axis. Since P is a non-singular point of $\mathcal{X}$, there exists a formal power series $y(x) \in \bar{\mathbb{F}}_q[[x]]$ of order $\geqslant 1$, such that $f(x, y(x)) = 0$. For $0 \leqslant i \leqslant 5$, put $m_i = z_i(x, y(x))x^{e_P}$, so that $v_P(m_i(x)) \geqslant 0$. From (5.1),

$$\begin{aligned} &m_0(x)^{\sqrt{q}} + m_1(x)^{\sqrt{q}}x + m_2(x)^{\sqrt{q}}y(x) + \\ &\quad + m_3(x)^{\sqrt{q}}x^2 + m_4(x)^{\sqrt{q}}xy(x) + m_5(x)^{\sqrt{q}}y(x)^2 = 0\,. \end{aligned}$$

Putting $y = c_s x^s + \ldots$, with $c_s \neq 0$ and $k_i = v_P(m_i(x))$, the left-hand side is the sum of six formal power series in the variable x whose orders are as follows:

$$k_0\sqrt{q},\ k_1\sqrt{q}+1,\ k_2\sqrt{q}+s,\ k_3\sqrt{q}+2,\ k_4\sqrt{q}+s+1,\ k_5\sqrt{q}+2s.$$

At least two of these orders are equal, and they are less than or equal to the remaining four. Because of Lemma 3.6 we have two possibilities:

(1) $s = \frac{1}{2}(\sqrt{q}+1)$, that is, P is an inflexion point, and $k_0 \geqslant 2$, $k_1 = 1$, $k_2 \geqslant 1$, $k_3 \geqslant 1$, $k_4 \geqslant 1$, $k_5 = 0$;
(2) $s = 2$, that is, P is a regular point, and $k_0 \geqslant 1$, $k_1 \geqslant 1$, $k_2 = k_3 = 0$, $k_4 \geqslant 0$, $k_5 \geqslant 0$.

In case (1), $\det(\Delta(z_0(x), \ldots, z_5(x))) = x^{e_P}[cx^2 + \ldots]$, where $c = -c_5c_1^2$ with $m_5(x) = c_5 + \ldots$ and $m_1(x) = c_1x + \ldots$. In case (2), $\det(\Delta(z_0(x), \ldots, z_5(x))) = x^{e_P}[c + \ldots]$, where $c = -c_3c_4$ with $m_3(x) = c_3 + \ldots$, and $m_4(x) = c_4 + \ldots$. This completes the proof of the lemma.

Following [SV, §1], let $\phi : \mathcal{X} \to \mathbb{P}^5(\bar{\mathbb{F}}_q)$ be the morphism where $\phi(Q) = (z_0, \ldots, z_5)$, for a point $Q \in \mathcal{X}$, and $z_i \in \bar{\mathbb{F}}_q(\mathcal{X})$. Since $P \in \mathcal{X}$ is a non-singular point of $\mathcal{X}$, there exists a formal power series $y(x) \in \bar{\mathbb{F}}_q[[x]]$ of order $\geqslant 1$ such that $f(x+a, y(x)+b) = 0$, where $P = (a, b, 1)$. Let

$$m_i(x) = z_i(x+a, y(x)+b)x^{e_P}\,,$$

with $i = 0, \ldots, 5$. Then we have

$$\phi(P) = (m_0(x), \ldots, m_5(x))\,,$$

which is a primitive branch representation of $\phi(P)$.

https://doi.org/10.1023/A:1001826520682 Published online by Cambridge University Press

LEMMA 5.3. *The degree of* $\phi(\mathcal{X})$ *is* $\sqrt{q}+1$.

Proof. Let Σ denote the cubic hypersurface in $\mathbb{P}^5(\bar{\mathbb{F}}_q)$ given by (5.3). By the previous lemma, the intersection multiplicity $I(\phi(\mathcal{X}), \Sigma; \phi(P))$ of $\phi(\mathcal{X})$ and Σ at $\phi(P)$ is either 2 or 0 according as P is an inflexion point or a regular point of $\mathcal{X}$. This shows that $\phi(\mathcal{X})$ is not contained in Σ. From Bézout's theorem and Theorem 3.7(2), we obtain $3\deg(\phi(\mathcal{X})) = 2.3(\sqrt{q}+1)/2$, whence $\deg(\phi(\mathcal{X})) = \sqrt{q}+1$.

LEMMA 5.4. *For a generic point* $P \in \mathcal{X}$, *there exists a hyperplane* H *such that*

(1) $I(\phi(\mathcal{X}), H; \phi(P)) \geqslant \sqrt{q}$;
(2) *the Frobenius image* $\Phi(\phi(P))$ *lies on* H.

Proof. Choose a point $P = (a, b, 1) \in \mathcal{X}$ such that $z_i(a, b) \neq 0$ for at least one index i, with $0 \leqslant i \leqslant 5$. Then

$$\phi(P) = (z_0(a, b), z_1(a, b), z_2(a, b), z_3(a, b), z_4(a, b), z_5(a, b)).$$

Note that all points of $\mathcal{X}$, apart from a finite number of them, are of this kind. Let $X_0 + \alpha X_1 + \beta X_2 + \alpha^2 X_3 + \alpha\beta X_4 + \beta^2 X_5 = 0$ be the equation of the hyperplane H, where $\alpha = a^{\sqrt{q}}$, $\beta = b^{\sqrt{q}}$. There exists a formal power series $y(x)$ of order $\geqslant 1$ such that $f(x+a, y(x)+b) = 0$. Putting $z_i(x) = z_i(x+a, y(x)+b)$, we have

$$\begin{aligned} &I(\phi(\mathcal{X}), \Sigma; \phi(P)) \\ &\quad = \operatorname{ord}\{z_0(x) + \alpha z_1(x) + \beta z_2(x) + \alpha^2 z_3(x) + \alpha\beta z_4(x) + \beta^2 z_5(x)\}. \end{aligned}$$

From (5.2) we have

$$\begin{aligned} &z_0(x) + z_1(x)(x+a)^{\sqrt{q}} + z_2(x)(y(x)+b)^{\sqrt{q}} + z_3(x)(x+a)^{2\sqrt{q}} + \\ &\quad + z_4(x)((x+a)(y(x)+b))^{\sqrt{q}} + z_5(x)(y(x)+b)^{2\sqrt{q}} = 0. \end{aligned}$$

Since $y(x)$ has order $\geqslant 1$, that is, $y(x) = cx + \ldots$, then

$$\begin{aligned} &z_0(x) + z_1(x)a^{\sqrt{q}} + z_2(x)b^{\sqrt{q}} + \\ &\quad + z_3(x)a^{2\sqrt{q}} + z_4(x)(ab)^{\sqrt{q}} + z_5(x)b^{2\sqrt{q}} + x^{\sqrt{q}}[\ldots] = 0, \end{aligned}$$

which proves (1).

To check (2), note that (5.1) yields

$$\begin{aligned} &z_0(a, b)^{\sqrt{q}} + z_1(a, b)^{\sqrt{q}}a + \\ &\quad + z_2(a, b)^{\sqrt{q}}b + z_3(a, b)^{\sqrt{q}}a^2 + z_4(a, b)^{\sqrt{q}}(ab) + z_5(a, b)^{\sqrt{q}}b^2 = 0\,. \end{aligned}$$

Thus

$$\begin{aligned} &z_0(a, b)^q + z_1(a, b)^q a^{\sqrt{q}} + z_2(a, b)^q b^{\sqrt{q}} + \\ &\quad + z_3(a, b)^q a^{2\sqrt{q}} + z_4(a, b)^q (ab)^{\sqrt{q}} + z_5(a, b)^q b^{2\sqrt{q}} = 0\,. \end{aligned}$$

Since

$$\Phi(\phi(P)) = (z_0(a,b)^q, z_1(a,b)^q, z_2(a,b)^q, z_3(a,b)^q, z_4(a,b)^q, z_5(a,b)^q),$$

and $\alpha = a^{\sqrt{q}}$, $\beta = b^{\sqrt{q}}$, so (2) follows.

Now, the linear series of hyperplanes sections of $\phi(\mathcal{X})$ is equivalent to the base-point-free linear series $\mathcal{D} - E$, where $\mathcal{D} \cong \mathbb{P}(\langle z_0, \ldots, z_5 \rangle)$ and $E := \sum_{P\in\mathcal{X}} e_P P$. By Lemma 5.3, this linear series is contained in $\mathcal{D}_{\mathcal{X}} = |(\sqrt{q}+1)P_0|$, $P_0 \in \mathcal{X}(\mathbb{F}_q)$, because $\mathcal{X}$ is maximal; hence $(\sqrt{q}+1)P_0 \sim \sqrt{q}P + \Phi_{\mathcal{X}}(P)$ ([FGT, Corollary 1.2]). Note that we do not assert that equality holds. In fact, this is the case if and only if $\phi(\mathcal{X})$ is not degenerate, that is, $z_0, \ldots, z_5$ are $\bar{\mathbb{F}}_q$-linearly independent. This gives the following result.

LEMMA 5.5. *The base-point-free linear series of $\mathcal{X}$ generated by the curves $z_0, \ldots, z_5$ is contained in $\mathcal{D}_{\mathcal{X}}$.*

The next step is to determine the degrees of the z_i.

LEMMA 5.6. *The degrees satisfy* $\max_{0\leqslant i\leqslant 5} \deg(z_i) = 2$.

Proof. As before, the base-point-free linear series $\sum_{i=0}^{5} c_i z_i - E$ on $\mathcal{X}$ is contained in $\mathcal{D}_{\mathcal{X}}$; hence it is contained in the linear series cut out by conics on $\mathcal{X}$, by Theorem 3.5. This implies the existence of constants $d_j^{(i)}$ such that $\operatorname{div}(z_i) - E = \operatorname{div}(d_i)$, $i = 0, \ldots, 5$, where

$$d_i = d_i(X, Y) = d_0{}^{(i)} + d_1{}^{(i)}X + d_2{}^{(i)}Y + d_3{}^{(i)}X^2 + d_4{}^{(i)}XY + d_5{}^{(i)}Y^2\,.$$

Choose an index k such that $z_k(X, Y) \not\equiv 0 \pmod{f(X, Y)}$. Then

$$\operatorname{div}(z_i/z_k) = \operatorname{div}(d_i/d_k).$$

Thus $z_i(X, Y)d_k(X, Y) \equiv z_k(X, Y)d_i(X, Y) \pmod{f(X, Y)}$. Now, re-write (5.1) in terms of $d_i(X, Y)$:

$$hfd_k = z_k{}^{\sqrt{q}}(d_0{}^{\sqrt{q}} + d_1^{\sqrt{q}}X + d_2^{\sqrt{q}}Y + d_3^{\sqrt{q}}X^2 + d_4^{\sqrt{q}}XY + d_5^{\sqrt{q}}Y^2)\,.$$

Since $z_k(X, Y) \not\equiv 0 \pmod{f(X, Y)}$, so $f(X, Y)$ must divide the other factor on the right-hand side, and hence there exists $g \in \bar{\mathbb{F}}_q[X, Y]$ such that

$$gf = d_0{}^{\sqrt{q}} + d_1^{\sqrt{q}}X + d_2^{\sqrt{q}}Y + d_3^{\sqrt{q}}X^2 + d_4^{\sqrt{q}}XY + d_5^{\sqrt{q}}Y^2\,,$$

with $\deg(d_i) \leqslant 2$, for $i = 0, \ldots 5$. Thus we may assume that $g = h$ and $d_i(X, Y) = z_i(X, Y)$ all i. It remains to show that at least one of the polynomials $z_i(X, Y)$ has degree 2. However, if $\deg(z_i(X, Y)) \leqslant 1$ for all i, then the linear series generated by $z_0, \ldots, z_5$ would be contained in the linear series cut out by lines. But this would imply that $\deg(\phi(\mathcal{X})) \leqslant (\sqrt{q}+1)/2$, contradicting Lemma 5.3.

LEMMA 5.7. *The polynomials h and s in Lemma 5.1 may be assumed to be equal.*

https://doi.org/10.1023/A:1001826520682 Published online by Cambridge University Press

Proof. Since $\deg(z_i) \leqslant 2$ for all i, we can re-write

$$z_0 + z_1 X^{\sqrt{q}} + z_2 Y^{\sqrt{q}} + z_3 X^{2\sqrt{q}} + z_4 (XY)^{\sqrt{q}} + z_5 Y^{2\sqrt{q}}$$

in the form

$$w_0^{\sqrt{q}} + w_1^{\sqrt{q}} X + w_2^{\sqrt{q}} Y + w_3^{\sqrt{q}} X^2 + w_4^{\sqrt{q}} XY + w_5^{\sqrt{q}} Y^2 ,$$

where $w_i \in \mathbb{F}_q[X, Y]$ and $\max_{0 \leqslant i \leqslant 5} \deg(w_i) = \max_{0 \leqslant i \leqslant 5} \deg(z_i)$. Comparing this with (5.1) we see that z_i and w_i only differ by a constant in $\mathbb{F}_q$ independent of i, $0 \leqslant i \leqslant 5$. Substituting cz_i for w_i then gives

$$\begin{aligned} &w_0^{\sqrt{q}} + w_1^{\sqrt{q}} X + w_2^{\sqrt{q}} Y + w_3^{\sqrt{q}} X^2 + w_4^{\sqrt{q}} XY + w_5^{\sqrt{q}} Y^2 \\ &\quad = c^{\sqrt{q}}(z_0{}^{\sqrt{q}} + z_1^{\sqrt{q}} X + z_2^{\sqrt{q}} Y + z_3^{\sqrt{q}} X^2 + z_4^{\sqrt{q}} XY + z_5^{\sqrt{q}} Y^2) \\ &\quad = c^{\sqrt{q}} hf . \end{aligned} \tag{5.7}$$

Now, by the previous lemma we can write z_i explicitly in the form

$$z_i = t_0^{(i)} + t_1^{(i)} X + t_2^{(i)} Y + t_3^{(i)} X^2 + t_4^{(i)} XY + t_5^{(i)} Y^2 , \tag{5.8}$$

for $i = 0, \dots 5$. Let $t := c^{\sqrt{q}} h$; then (5.7) yields that $(t_j^{(i)})^{\sqrt{q}} = ct_i{}^{(j)}$ for $0 \leqslant i, j \leqslant 5$. Putting $i = j$, this gives $c^{\sqrt{q}+1} = 1$. Choose an element k in $\bar{\mathbb{F}}_q$ such that $k^{\sqrt{q}-1} = c$, and put $d_i = k^{-1} z_i$, $0 \leqslant i \leqslant 5$. Then (5.1) and (5.2) become respectively

$$\begin{aligned} hk^{-\sqrt{q}} f &= d_0^{\sqrt{q}} + d_1^{\sqrt{q}} X + d_2^{\sqrt{q}} Y + d_3^{\sqrt{q}} X^2 + d_4^{\sqrt{q}} XY + d_5^{\sqrt{q}} Y^2, \\ tk^{-1} f &= k(d_0 + d_1 X^{\sqrt{q}} + d_2 Y^{\sqrt{q}} + d_3 X^{2\sqrt{q}} + d_4 (XY)^{\sqrt{q}} + d_5 Y^{2\sqrt{q}}. \end{aligned}$$

Put $h' = hk^{-\sqrt{q}}$ and $t' = tk^{-1}$. Then $h' = t'$, and this completes the proof.

Next we determine explicitly the coefficients $t_j^{(i)}$ given in (5.8) or, equivalently, the 6×6 matrix $T = (t_j^{(i)})$. From Lemma 5.7 we can assume that

$$(t_j^{(i)})^{\sqrt{q}} = t_i^{(j)} . \tag{5.9}$$

for $0 \leqslant i, j \leqslant 5$. In other words, we can assume that T is a Hermitian matrix over $\mathbb{F}_{\sqrt{q}}$.

To obtain further relations between elements of T, we go back to (5.3) and note that

$$(\det(\Delta(z_0, \dots, z_5)))^{\sqrt{q}} = 0$$

can actually be regarded as the equation of the Hessian curve $\mathcal{H}(Z)$ associated to the algebraic curve $\mathcal{Z}$ with equation

$$z_0^{\sqrt{q}} + z_1^{\sqrt{q}} X + z_2{}^{\sqrt{q}} Y + z_3{}^{\sqrt{q}} X^2 + z_4{}^{\sqrt{q}} XY + z_5{}^{\sqrt{q}} Y^2 = 0;$$

here $z_i = z_i(X, Y)$. Hence $\mathcal{H}(\mathcal{Z})$ is $\sqrt{q}$-fold covered by the curve $\mathcal{C}$ with equation $\det(\Delta(z_0, \dots, z_5)) = 0$, and Lemma 5.2 can be interpreted in terms of intersection multiplicities between $\mathcal{C}$ and $\mathcal{X}$; namely, $I(\mathcal{C}, \mathcal{X}; P)$ is either $2 + e_P$ or e_P according

https://doi.org/10.1023/A:1001826520682 Published online by Cambridge University Press

as $P \in \mathcal{X}$ is an inflexion point or not. Now, $I(\mathcal{H}(\mathcal{X}), \mathcal{X}; P) = s(P) - 2$, where $\mathcal{H}(\mathcal{X})$ is the Hessian of $\mathcal{X}$ and $s(P) := I(\mathcal{X}, l; P)$, with l the tangent to $\mathcal{X}$ at the point P; see, for example, (Wa, Ch.4, §6)) and, for a characteristic-free approach to Hessian curves, see (OO, Ch.17)). Comparing the intersection divisors $\mathcal{C}.\mathcal{X}$ and $\mathcal{H}(\mathcal{X}).\mathcal{X}$, we see that $(n-2)/2\, \mathcal{C}.\mathcal{X} \geqslant \mathcal{H}(\mathcal{X}).\mathcal{X}$ with $n = \frac{1}{2}(\sqrt{q}+1)$. Hence, by Noether's "$AF + BG$" Theorem, (Sei, p. 133), we obtain

$$(\det(\Delta(z_0, \dots, z_5)))^{(n-2)/2} = AF + BG\ ,$$

with F the projectivization of f and A, B, G homogeneous polynomials in $\bar{\mathbb{F}}_q[X_0, X_1, X_2]$, where $G = 0$ is the equation of $\mathcal{H}(\mathcal{X})$. As $\det(\Delta(z_0, \dots, z_5))$ is a polynomial of degree 6 (cf. Lemma 5.6), while $\deg(G) = 3(n-2)$, so B must be a constant. This yields that $e_P = 0$ for each $P \in \mathcal{X}$. For an inflexion point $P \in \mathcal{X}$, we can now infer from the proof of Lemma 5.2 that if $P = (0, 0, 1)$ and l is the X–axis, then $z_i(0, 0) = 0$, $i = 0, \dots 4$, and thus $\det(\Delta(z_0, \dots, z_5))$ has no terms of degree $\leqslant 2$. This shows that each inflexion point P of $\mathcal{X}$ is a singular point of $\mathcal{C}$.

By a standard argument depending on the upper bound for the number of singular points of an absolutely irreducible algebraic curve of degree m, namely $(m-1)(m-2)/2$, it can be shown that $\mathcal{C}$ is doubly covered by an absolutely irreducible cubic curve $\mathcal{U}$ of equation $u = 0$, with u homogeneous in $\bar{\mathbb{F}}_q[X_0, X_1, X_2]$. Hence,

$$\det(\Delta(z_0, \dots, z_5)) = u^2\,. \tag{5.10}$$

Consider now a minor Δ_{ij} of $\Delta(z_0, \dots, z_5)$, and suppose that Δ_{ij} is not the zero polynomial. Then $\Delta_{ij} = 0$ can be regarded as the equation of a quartic curve $\mathcal{V}_{ij}$. Since $\mathcal{V}_{ij}$ also passes through each inflexion point of $\mathcal{X}$, so $\mathcal{V}_{ij}$ and $\mathcal{U}$ have at least $3n$ common points. On the other hand, $\deg(\mathcal{V}_{ij})\deg(\mathcal{U}) = 12$, and because $3n > 12$, so $\mathcal{U}$ is a component of $\mathcal{V}_{ij}$. This shows the existence of linear homogeneous polynomials $l_0, \dots, l_5 \in \bar{\mathbb{F}}_q[X_0, X_1, X_2]$ such that

$$4z_3z_5 - z_4^2 = ul_0, \quad 2z_1z_5 - z_2z_4 = -ul_1, \quad z_1z_4 - 2z_2z_3 = ul_2, \tag{5.11}$$

$$4z_0z_5 - z_2^2 = ul_3, \quad 2z_0z_4 - z_1z_2 = -ul_4, \quad 4z_0z_3 - z_1^2 = ul_5. \tag{5.12}$$

Let L denote the matrix $\Delta(l_0, l_1, l_2, l_3, l_4, l_5)$. From elementary linear algebra, $\Delta^* = uL$ where Δ^* is the adjoint of $\Delta(z_0, \dots, z_5)$, and hence $(\det(\Delta(z_0, \dots, z_5)))^2 = u^3 \det(L)$. Comparison with (5.10) gives $u = \det(L)$. Thus $\Delta^* = \det(L)L$. Also, $\Delta(z_0, \dots, z_5) = \det(L)L^{-1}$; that is,

$$2z_0 = l_3l_5 - l_4^2, \quad z_1 = -(l_1l_5 - l_2l_4), \quad z_2 = l_1l_4 - l_2l_3, \tag{5.13}$$

$$2z_3 = l_0l_5 - l_2^2, \quad z_4 = -(l_0l_4 - l_1l_2), \quad 2z_5 = l_0l_3 - l_1^2. \tag{5.14}$$

Note that we have also seen that $\mathcal{U}$ has equation $\det(L) = 0$.

https://doi.org/10.1023/A:1001826520682 Published online by Cambridge University Press

Set

$$l_i = a_i X + b_i Y + c_i, \text{ for } i = 0, 2, 3, 5,$$
$$l_i = -a_i X - b_i Y - c_i, \text{ for } i = 1, 4.$$

Now we take an inflexion point P on $\mathcal{X}$ to be the origin and the tangent of $\mathcal{X}$ at P to be the X-axis. Also, $I(\mathcal{U}, \mathcal{X}; P) = 1$, so P is a non-singular point of $\mathcal{U}$, and the tangent to $\mathcal{U}$ at P is not the X-axis. We take this tangent to be the Y-axis. We are going to prove that the Y-axis is a component of $\mathcal{U}$. A direct computation shows that (5.11) yields

$$z_0(X, Y) = kY^2\,, \tag{5.15}$$
$$l_5 = a_5 X\,, \quad \text{with } a_5 \neq 0\,. \tag{5.16}$$

By (5.9) we also have

$$l_4 = -b_4 Y, \quad b_4 \neq 0\,. \tag{5.17}$$

The first relation in (5.11), again with $u = \det(L)$, together with (5.15) and (5.16) yields

$$l_3 = 0\,. \tag{5.18}$$

Then, with the unit point suitably chosen, we may also assume that

$$z_0(X, Y) = -\tfrac{1}{2}Y^2\,, \tag{5.19}$$

Again, a certain amount of computation shows that (5.9) yields

$$b_0 b_4 - 2b_1 b_2 = 0, \tag{5.20}$$
$$c_0 b_4 - 2c_1 b_2 = 0. \tag{5.21}$$

LEMMA 5.8. *If $P \in \mathcal{X}$ is an inflexion, then $\mathcal{U}$ has a linear component through P.*

Proof. We prove that the Y-axis is a linear component of $\mathcal{U}$. Equivalently, we can show that X is a factor of $\det(L)$. By (5.16) and (5.18), we must check that X divides $l_0 l_4 - 2l_1 l_2$. By (5.16) and $c_2 = 0$, this occurs if the polynomial $(b_0 b_4 - 2b_1 b_2)Y^2 + (c_0 b_4 - 2c_1 b_1)Y$ is identically zero. Hence the result is a consequence of (5.20) and (5.21).

It was shown in Theorem 3.7 that $\mathcal{X}$ has $3(\sqrt{q}+1)/2$ inflexion points altogether, and each one lies on a linear component of $\mathcal{U}$.

COROLLARY 5.9. *The cubic $\mathcal{U}$ splits into three distinct lines.*

Some more computations depending on (5.9) together with a suitable change of coordinates give the following result.

LEMMA 5.10. *There exist* $a_0, a_2, a_5 \in \mathbb{F}_{\sqrt{q}}$ *such that*

$$l_0 = a_0X, l_1 = 1, l_2 = -a_2X, l_3 = 0, l_4 = -Y, l_5 = a_5X, \tag{5.22}$$

$$z_0 = -\tfrac{1}{2}Y^2, z_1 = -a_5X + a_2XY, z_2 = -Y, \tag{5.23}$$

$$z_3 = \tfrac{1}{2}(a_0a_5 - a_2^2)X^2, z_4 = a_0XY - a_2X, z_5 = -1/2. \tag{5.24}$$

Now we want to show that, if $R = (0, \eta)$ is any further inflexion point of $\mathcal{X}$ lying on the Y-axis, then the tangent line r to $\mathcal{X}$ at R has equation $Y = \eta$. To do this it is sufficient to check that the curve $\mathcal{Z}$ with equation

$$z_0^{\sqrt{q}} + z_1^{\sqrt{q}}X + z_2^{\sqrt{q}}Y + z_3^{\sqrt{q}}X^2 + z_4^{\sqrt{q}}XY + z_5^{\sqrt{q}}Y^2 = 0$$

has a cusp at R, that is, a double point with only one tangent, such that the tangent is the horizontal line $Y = \eta$. Applying the translation $X' = X$, $Y' = Y - \eta$, the curve $\mathcal{Z}$ is transformed into the curve with equation

$$-\tfrac{1}{2}(\eta^{\sqrt{q}} + \eta)^2 + (\eta^{\sqrt{q}} + \eta)Y - \tfrac{1}{2}Y^2 + \alpha = 0\,,$$

where α represents terms of degree at least 3. Since this curve passes through the origin, we have $\eta^{\sqrt{q}} + \eta = 0$. Hence, the lowest degree term is $-\frac{1}{2}Y^2$ and so the origin is a cusp with tangent line $Y = 0$, as required. This gives the following situation.

THEOREM 5.11. *There exists a triangle such that the inflexion points of* $\mathcal{X}$ *lie* $\frac{1}{2}(\sqrt{q}+1)$ *on each side, none a vertex, and the inflexional tangents pass* $\frac{1}{2}(\sqrt{q}+1)$ *through each vertex, none being a side.*

We are now in a position to prove the main result, Theorem 1.1, stated in Section 1.

Let $n = (\sqrt{q}+1)/2$. We choose the triangle $\mathcal{T}$ of Theorem 5.11 as triangle of reference, and denote the inflexions on the X-axis by $(\xi_i, 0)$, $i = 1 \ldots n$, and those on the Y-axis by $(0, \eta_i)$, $i = 1 \ldots n$. Also, without loss of generality, we may assume that ${\xi_1}^n + 1 = 0$ and ${\eta_1}^n + 1 = 0$. Write $f(X, Y)$ in the form

$$f = a_0(X)Y^n + \ldots + a_j(X)Y^{n-j} + \ldots + a_n(X),$$

with $a_i(X)$ of degree i in $\mathbb{F}_q[X]$.

Since $(\xi_i, 0)$ lies on $\mathcal{X}$, so $a_n(\xi_i) = 0$. Since the line $x = \xi_i$ is the inflexional tangent at $(\xi_i, 0)$, so

$$a_0(\xi_i)Y^n + \ldots + a_{n-1}(\xi_i)Y = 0$$

has n repeated roots. So

$$a_1(\xi_i) = \ldots = a_{n-1}(\xi_i) = 0. \tag{5.25}$$

Since (5.25) is true for all ξ_i,

$$a_1(X) = \ldots = a_{n-1}(X) = 0.$$

Hence it follows that $f(X, Y) = a_0Y^n + a_n(X)$. A similar argument shows that $f(X, Y) = b_0X^n + b_n(Y)$. Thus $f(X, Y) = a_0X^n + b_0Y^n + c_0$, and it only remains

https://doi.org/10.1023/A:1001826520682 Published online by Cambridge University Press

to compute the coefficients. Since $f(\xi_1, 0) = 0$ and ${\xi_1}^n + 1 = 0$, we have $a_0 = c_0$. Similarly, from ${\eta_1}^n + 1 = 0$ we infer $b_0 = c_0$. This completes the proof.

Acknowledgements

The first and third authors were supported respectively by GNSAGA of the Italian CNR, the second by a NATO grant, and the fourth by Cnpq-Brazil. We are extremely grateful to the referee for the care with which the paper was read.

References

[AT] Abdon, M. and Torres, F.: On maximal curves in characteristic two, *Manuscripta Math.* **99**, (1998), 39–53.

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

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

[FT1] Fuhrmann, R. and Torres, F.: On Weierstrass points and optimal curves, *Rend. Circ. Mat. Palermo Suppl.* **51** (1998), 25–46.

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

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

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

[H] Hirschfeld, J. W. P.: *Projective Geometries Over Finite Fields*, 2nd edn, Oxford Univ. Press, Oxford, 1998.

[HK] Hirschfeld, J. W. P. and Korchmáros, G.: Embedding an arc into a conic in a finite plane, *Finite Fields Appl.* **2** (1996), 274–292.

[HK1] Hirschfeld, J. W. P. and Korchmáros, G.: On the number of points on an algebraic curve over a finite field, *Bull. Belg. Math. Soc. Simon Stevin* **5** (1998), 313–340.

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

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

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

[OO] Orzech, G. and Orzech, O.: *Plane Algebraic Curves*, M. Dekker, New York, 1981.

[Par] Pardini, R.: Some remarks on plane curves over fields of finite characteristic, *Compositio Math.* **60** (1986), 3–17.

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

[Sei] Seidenberg, A.: *Elements of the Theory of Algebraic Curves*, Addison-Wesley, Reading, Mass, 1969.

[Sti] Stichtenoth, H.: *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin, 1993.

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

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

[Wa] Walker, R. J.: *Algebraic Curves*, Princeton University Press, Princeton, 1950 (Dover, New York, 1962).

[We] Weil, A., *Courbes Algébriques et Variétés Abeliennes*, Hermann, Paris, 1948.