On the number of rational points on an algebraic curve over a finite field

J. W. P. Hirschfeld G. Korchmáros

Abstract

A new bound for the number of rational points on an algebraic curve over a finite field is obtained in Theorem 1.3. It is derived from previous work on the upper bounds for the size of a complete arc in a finite projective plane. In the terminology of plane curves, the main result is Theorem 1.4, and considers an absolutely irreducible, plane curve $\mathcal{C}$ of degree d defined over $\mathbf{F}_q$, $q = p^h$ with p prime and $p \geq 3$. An upper bound is obtained for the number of branches of $\mathcal{C}$ that are centred at $\mathbf{F}_q$-rational points. To do this, two types of branches are distinguished: (a) branches of order and class equal to r; (b) branches of order r and class different from r.

The main theorem counts twice the number of branches of type (a) plus the number of branches of type (b). As a corollary, this theorem gives an upper bound for the number of $\mathbf{F}_q$-rational points of $\mathcal{C}$, since simple non-inflexion points are branches of order 1 and class 1, while inflexions points are branches of order 1 and class greater than 1.

1 Introduction

For a projective, geometrically irreducible, non-singular, algebraic curve $\mathcal{C}$ defined over $\mathbf{F}_q$, the number N_1 of its rational points, that is, points with coordinates in $\mathbf{F}_q$, satisfies

$$|N_1 - (q+1)| \leq 2g\sqrt{q}. \tag{1.1}$$

Received by the editors October 1997.
Communicated by Aart Blokhuis.
1991 *Mathematics Subject Classification.* 11G20,51E21.
Key words and phrases. Algebraic curve, finite field, arc.

This is the Hasse-Weil theorem; a curve achieving the upper bound in (1.1) is called *maximal*. The bound was improved by Serre to the following:

$$|N_1 - (q+1)| \leq g\lfloor 2\sqrt{q} \rfloor. \tag{1.2}$$

If $\mathcal{C}$ is a non-singular plane curve of degree d, then (1.1) becomes

$$|N_1 - (q+1)| \leq (d-1)(d-2)\sqrt{q}. \tag{1.3}$$

These bounds are important for applications in Coding Theory (see [22]), Number Theory (see [18] for example on cyclotomy), and in Finite Geometry (see [11, Chapter 10]). However, in many applications what is actually required is to compute the number N of zeros of an absolutely irreducible polynomial $F(X,Y)$ with coefficients in $\mathbf{F}_q$. In geometrical terms, N means the total number of $\mathbf{F}_q$-rational points of the plane curve $\mathcal{C}$ with equation $F(X,Y) = 0$. Note that $\mathcal{C}$ may have singular points over $\mathbf{F}_q$ that do not correspond to points of a non-singular model of $\mathcal{C}$ over $\mathbf{F}_q$. Thus $N_1 \leq N$ but it is not necessarily true that $N_1 = N$. For example, a plane cubic curve with an isolated double point has $q+2$ rational points; the double point is not counted in the estimate (1.1).

If N_1 is replaced by N, equation (1.3) remains true for singular curves; see [17], [11, §2.8] for discussions of this. Also, as explained in [13], the main result [23, Theorem 2.13] of the Stöhr-Voloch theory still holds when N denotes the total number of $\mathbf{F}_q$-rational points of the model of the curve $\mathcal{X}$ associated to a base-point-free linear system defined on $\mathcal{X}$.

Our aim here is to find an upper bound for the number of $\mathbf{F}_q$-rational points of a plane curve $\mathcal{C}$ which only depends on the degree of $\mathcal{C}$ and the order of the field. Standard notation will be used; see [23, 4].

Let $\mathcal{X}$ be a projective, geometrically irreducible, non-singular, algebraic curve defined over $\mathbf{F}_q$, with $q = p^h$ and p an odd prime, and consider $\mathcal{X}$ over the algebraic closure $\overline{\mathbf{F}}_q$ equipped with the action of the Frobenius morphism relative to $\mathbf{F}_q$. Suppose that $\mathcal{X}$ admits two linear systems Σ_1 and Σ_2 such that

(A) Σ_1 cuts out on $\mathcal{X}$ a simple, not necessarily complete, base-point-free linear series g^2_d;

(B) $\Sigma_2 = 2\Sigma_1$, and Σ_2 cuts out on $\mathcal{X}$ a linear series g^5_{2d}.

Note that g^5_{2d} is also simple and base-point-free. For $i = 1, 2$, let π_i be the morphism associated to Σ_i. Then $\pi_1(\mathcal{X})$ is a plane curve of degree d defined over $\mathbf{F}_q$, and every absolutely irreducible plane curve can be obtained in this way.

The set of all $\mathbf{F}_q$-rational points on $\pi_1(\mathcal{X})$ is

$$\tilde{\mathcal{X}} = \tilde{\mathcal{X}}(\mathbf{F}_q) = \{P \in \mathcal{X} \mid \pi_1(P) \in \pi_1(\mathcal{X})(\mathbf{F}_q)\};$$

that is, $\tilde{\mathcal{X}}$ is the set of all points of $\mathcal{X}$ that correspond to branches of $\pi_1(\mathcal{X})$ centred at an $\mathbf{F}_q$-rational point. Since two types of points P in $\mathcal{X}$ are distinguished according as $\pi_1(P)$ is regular or an inflexion, so $\tilde{\mathcal{X}}(\mathbf{F}_q)$ splits into two sets:

$$\begin{array}{rcl} S_1 = \tilde{\mathcal{X}}_1(\mathbf{F}_q) & = & \{P \in \tilde{\mathcal{X}}(\mathbf{F}_q) \mid j^1_2(P) = 2j^1_1(P)\}, \\ S_2 = \tilde{\mathcal{X}}_2(\mathbf{F}_q) & = & \{P \in \tilde{\mathcal{X}}(\mathbf{F}_q) \mid j^1_2(P) > 2j^1_1(P)\}, \end{array} \tag{1.4}$$

where the symbol $j_r^1(P)$ stands for the r-th (Σ_1, P)-order of the ramification divisor R_1 associated with Σ_1. Now, put

$$M_q = \sum_{P \in S_1} j_1^1(P),$$
$$M_q' = \sum_{P \in S_2} j_1^1(P).$$

Then $M_q + M_q'$ is the total number of $\mathbf{F}_q$-rational points on $\pi_1(\mathcal{X})$; this may be greater than the number N_1 of $\mathbf{F}_q$-rational points on $\mathcal{X}$. Since M_q' only counts inflexion points, and so can be computed by standard techniques, the main problem consists in finding an upper bound for M_q. This explains why M_q and M_q' do not play a symmetrical role in our investigation. The following proposition shows that, if $2M_q + M_q'$ is large enough, then both the ramification divisor R_2 and the $\mathbf{F}_q$-Frobenius divisor S_2 associated to Σ_2 are non-classical; hence these divisors are of great importance in the study of curves with many rational points. This was first recognized in [23].

Proposition 1.1 *Let $\mathcal{X}$ be a curve over $\mathbf{F}_q$ satisfying* (A) *and* (B). *Also suppose that the following conditions hold*:
(H1) $2M_q + M_q' \geq d(q - \sqrt{q} + 1)$;
(H2)

$$3 \leq d \begin{cases} \leq \sqrt{q} & \text{when } q > 23^2, \\ & q \neq 3^6, 5^5, \\ \leq 22 & \text{when } q = 3^6, \\ \leq 48 & \text{when } q = 5^5, \\ < \min\{(q - 5\sqrt{q} + 45)/20, (q - 5\sqrt{q} + 57)/24\} & \text{when } q \leq 23^2; \end{cases}$$

(H3) $q \geq 16$;
(H4) $p \geq 3$, *and q is a square when $p = 3$.*
Then

(i) Σ_1 *is classical*;

(ii) q *is a square*;

(iii) *the Σ_2-orders are* $0, 1, 2, 3, 4, \sqrt{q}$;

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

(v) $d \geq \frac{1}{2}(\sqrt{q} + 1)$.

The proof of this proposition is given in Section 2 using an argument similar to that used by Voloch in [25].

The non-classicality of $\mathcal{X}$ with respect to Σ_2 allows us to introduce a further linear system on $\mathcal{X}$ and find an upper bound for its degree that depends on the degree of the plane curve $\pi_1(\mathcal{X})$. This upper bound together with some other results depending on the Σ_1-Weierstrass points of $\mathcal{X}$ gives the following result.

Proposition 1.2 *Let $\mathcal{X}$ be a curve over $\mathbf{F}_q$ satisfying* (A) *and* (B). *Suppose that the following conditions hold*:
(h1) $2M_q + M'_q \geq d(q - \sqrt{q} + 1)$;
(h2) $\lfloor 3 \leq d \leq \sqrt{q} - 3$;
(h3) *q is a square and $p \geq 3$*;
(h4) *Σ_1 is classical*;
(h5) *the Σ_2-orders are $0, 1, 2, 3, 4, \sqrt{q}$*;
(h6) *the $\mathbf{F}_q$-Frobenius orders for Σ_2 are $0, 1, 2, 3, \sqrt{q}$.*
Then

(i) $d = \frac{1}{2}(\sqrt{q} + 1)$;

(ii) $2M_q + M'_q = d(q - \sqrt{q} + 1)$.

The proof of Proposition 1.2 is the hard part of the work and is carried out in Sections 4 to 9. The conditions (h1) to (h6) are referred to throughout the rest of the paper.

Propositions 1.1 and 1.2 give the main result of the paper.

Theorem 1.3 *Let $\mathcal{X}$ be a curve over $\mathbf{F}_q$ satisfying conditions* (A) *and* (B). *Suppose also that $p \geq 3$, that q is a square if $p = 3$, and that*

$$3 \leq d \begin{cases} \leq \sqrt{q} - 3 & \text{if } q \neq 3^6, 5^5, \\ \leq 22 & \text{if } q = 3^6, \\ \leq 48 & \text{if } q = 5^5, \\ < \min\{(q - 5\sqrt{q} + 45)/20, (q - 5\sqrt{q} + 57)/24\} & \text{if } q \leq 23^2. \end{cases}$$

Then

(i) $2M_q + M'_q \leq d(q - \sqrt{q} + 1)$;

(ii) $2M_q + M'_q = d(q - \sqrt{q} + 1)$ *if and only* $d = \frac{1}{2}(\sqrt{q} + 1)$, *in which case the curve is maximal.*

Section 10 compares Theorem 1.3 with both the the Hasse-Weil theorem and the Stöhr-Voloch theorem. Finally, Section 11 applies Theorem 1.3 to arcs in $\mathrm{PG}(2, q)$, improving a result given in [13].

In terms of plane curves, Theorem 1.3 can be phrased in the following way, using the terminology of [21]. Let $\mathcal{C}$ be an absolutely irreducible, plane curve of degree d defined over $\mathbf{F}_q$. Two types of branch are distinguished, both centred at $\mathbf{F}_q$-rational points: (a) *the regular branches of order r*, that is, branches of order and class equal to r; (b) *the irregular branches of order r*, that is, branches of order r and class different from r. Then M_q and M'_q are the number of branches of type (a) and type (b) respectively, each counted r times.

Theorem 1.4 *Let $\mathcal{C}$ be an absolutely irreducible, plane curve of degree d defined over $\mathbf{F}_q$, with $q = p^h$ and $p \geq 3$ but q a square when $p = 3$. If the condition on d in Theorem 1.3 is satisfied, then the conclusions* (i) *and* (ii) *also hold.*

The result has some connection with recent investigations on maximal curves. The genus g of a maximal curve satisfies $g = \frac{1}{2}\sqrt{q}(\sqrt{q}-1)$ or $g \leq \frac{1}{4}(\sqrt{q}-1)^2$, a result conjectured in [27] and proved in [5]. It follows that, if a non-singular plane curve is maximal, then $d = \sqrt{q}+1$ or $d \leq \sqrt{(q/2)}$.

A final point is that, in Theorem 1.4, if as in (ii), the degree $d = \frac{1}{2}(\sqrt{q}+1)$, then it is shown in [2] that $\mathcal{C}$ is isomorphic to a Fermat curve with affine equation

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

2 The proof of Proposition 1.1

Let $\mathcal{X}$ be a projective, geometrically irreducible, non-singular algebraic curve defined over $\mathbf{F}_q$. Consider $\mathcal{X}$ over the algebraic closure $\overline{\mathbf{F}}_q$ equipped with the action of the Frobenius morphism relative to $\mathbf{F}_q$. To prove Proposition 1.1 the following results from [23, §§1–2] are needed. For a base-point-free linear series $\mathcal{D} = g^r_d$ on X defined over $\mathbf{F}_q$, let $R = R^{\mathcal{D}}$ be the ramification divisor and $S = S^{\mathcal{D},q}$ the $\mathbf{F}_q$-Frobenius divisor associated to $\mathcal{D}$. For $P \in \mathcal{X}$, let $j_i(P)$ be the i-th $(\mathcal{D}, P)$-order, let $\epsilon_i = \epsilon_i^{\mathcal{D}}$ be the i-th $\mathcal{D}$-order, and let $\nu_i = \nu_i^{(\mathcal{D},q)}$ be the i-th $\mathbf{F}_q$-Frobenius order. As in §1, for the system Σ_n the divisors R and S are denoted by R_n and S_n, $n = 1, 2$. For Σ_n, the parameters ϵ_i and ν_i are also denoted by ϵ_i^n and ν_i^n. Also, a divisor D is written $\sum v_P(D)\, P$. The following properties hold:

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

(b) $j_i(P) \geq \epsilon_i$;

(c) $v_P(R) \geq \sum_i (j_i(P) - \epsilon_i)$; equality holds if and only if $\det(\binom{j_i(P)}{\epsilon_j}) \not\equiv 0 \pmod{p}$;

(d) $\{\nu_i \mid i = 0, \ldots, r-1\}$ is a subsequence of the $\mathcal{D}$-orders;

(e) $\deg(S) = \sum_{i=0}^{r-1} \nu_i(2g-2) + (q+r)d$;

(f) $\nu_i \leq j_{i+1}(P) - j_1(P)$ for P in $\mathcal{X}(\mathbf{F}_q)$;

(g) $v_P(S) \geq \sum_{i=0}^{r-1}(j_{i+1}(P) - \nu_i)$ for P in $\mathcal{X}(\mathbf{F}_q)$; equality holds if and only if $\det(\binom{j_{i+1}(P)}{\nu_j}) \not\equiv 0 \pmod{p}$.

Note that properties (f) and (g) imply

(g′) $v_P(S) \geq r j_1(P)$ provided $P \in \mathcal{X}(\mathbf{F}_q)$.

Also note that (f), (g), (g′) are still valid for a point P in $\mathcal{X}$ such that $\pi(P) \in \pi(\mathcal{X})(\mathbf{F}_q)$, where π is the morphism over $\mathbf{F}_q$ associated to $\mathcal{D}$.

Let $N_1 = |\mathcal{X}(\mathbf{F}_q)|$. From (g′) and (e),

(h) (The Stöhr-Voloch theorem)

$$N_1 \leq r^{-1}\{\sum_{i=0}^{r-1} \nu_i(2g-2) + (q+r)d\}.$$

Assume now that (H1) and (H3) hold, and also that the following holds:

(H2a) $3 \le d \le \sqrt{q}$.

Lemma 2.1 *Σ_1 is classical.*

Proof. Suppose that $\epsilon = \epsilon_2^1 > 2$. Then, by the p-adic criterion of [23, Corollary 1.9], ϵ is a power of p (cf. [7, Proposition 2]) and so, reasoning as in proof of [13, Proposition 3.1], we have the following. For $P \in \mathcal{X}$ such that $\pi(P) \in \tilde{\mathcal{X}}(\mathbf{F}_q)$,

$$j_1^1(P)j_2^1(P)(j_2^1(P) - j_1^1(P)) \equiv 0 \pmod{p}. \tag{2.5}$$

Now consider two cases according as Σ_1 is $\mathbf{F}_q$-Frobenius classical or not.

Case 1: Σ_1 is $\mathbf{F}_q$-Frobenius classical.

Let $P \in \mathcal{X}$ such that $\pi(P) \in \tilde{\mathcal{X}}(\mathbf{F}_q)$. By (g),

$$v_P(S_1) \ge (j_2^1(P) - 1) + j_1^1(P).$$

Then $v_P(S_1) \ge 2j_1(P)$ for the case that $\pi(P) \in \tilde{\mathcal{X}}_2(\mathbf{F}_q)$. Also, (2.5) and (g) imply that $v_P(S_1) \ge 3j_1^1(P)$ for the case that $\pi(P) \in \tilde{\mathcal{X}}_1(\mathbf{F}_q)$. Consequently,

$$\deg(S_1) = (2g-2) + (q+2)d \ge 3M_q + 2M_q' \ge \tfrac{3}{2}(2M_q + M_q'). \tag{2.6}$$

Since $d(d-3) \ge 2g-2$, from (2.6) and (H1) we then have

$$(d-3) + (q+2) \ge 3(q - \sqrt{q} + 1)/2;$$

that is, $d \ge (q - 3\sqrt{q} + 5)/2$. Now (H2a) gives a contradiction for $q \ge 16$.

Case 2: Σ_1 is $\mathbf{F}_q$-Frobenius non-classical.

Here we are going to show that

$$d(2g-2) + 3d \ge \deg(R_1) = (1+\epsilon)(2g-2) + 3d \ge 2M_q + M_q'. \tag{2.7}$$

This gives a contradiction because $d(d-3) \ge 2g-2$ and (H1) imply that $d^2 - 3d + 3 \ge q - \sqrt{q} + 1$; that is, $(d - 3/2)^2 \ge (\sqrt{q} - 1)^2/2$ and so $d \ge \sqrt{q} + 1$.

To finish the proof of Lemma 2.1 we prove (2.7). The $\mathbf{F}_q$-Frobenius orders of Σ_1 are 0 and $\nu_1^1 = \epsilon$ (see (d)); then, $j_2^1(P) \ge \epsilon + j_1^1(P)$ for each $P \in \tilde{\mathcal{X}}(\mathbf{F}_q)$ (see (f)). Since $d \ge j_2^1(P)$ and $j_1^1(P) \ge 1$ we obtain $d \ge \epsilon + 1$ and hence the first inequality in (2.7). Also, by (c), $v_P(R_1) \ge (j_2^1(P) - \epsilon) + (j_1^1(P) - 1)$, whence $v_P(R_1) \ge 2j_1(P) - 1$. It turns out that (2.5) improves this bound to $v_P(R_1) \ge 2j_1^1(P)$ for each $P \in \tilde{\mathcal{X}}_1(\mathbf{F}_q)$ (see (c)). Finally $j_1^1(P) \ge 1$ implies $2j_1^1(P) - 1 \ge j_1^1(P)$. ∎

Corollary 2.2 *There exists $P \in \mathcal{X}$ with $\pi(P) \in \tilde{\mathcal{X}}(\mathbf{F}_q)$ and (Σ_1, P)-orders $0, 1, 2$.*

Proof. Suppose that $j_2^1(P) \ge 3$ for each $P \in \tilde{\mathcal{X}}(\mathbf{F}_q)$. Then, by Lemma 2.1 and (c), $v_P(R_1) \ge j_1^1(P)$; hence

$$\deg(R_1) = 3(2g-2) + 3d \ge M_q + M_q' \ge \tfrac{1}{2}(2M_q + M_q').$$

Again using $d(d-3) \ge 2g-2$ and (H1), this gives $d \ge (q - \sqrt{q} + 13)/6$, and again (H2a) gives a contradiction. ∎

From Corollary 2.2 and (f) the next result follows.

Corollary 2.3 Σ_1 *is* $\mathbf{F}_q$*-Frobenius classical.*

Remark 2.4 The condition $d \le \sqrt{q}$ is sharp. Indeed, consider the Hermitian curve $y^{\sqrt{q}} + y = x^{\sqrt{q}+1}$, with q a square. Then $\Sigma_1 = |(\sqrt{q}+1)P_0|$, where P_0 is an $\mathbf{F}_q$-rational point, and the Σ_1-orders are $0, 1, \sqrt{q}$. So $\tilde{\mathcal{X}}(\mathbf{F}_q) = \mathcal{X}(\mathbf{F}_q)$ and, for each $P \in \mathcal{X}(\mathbf{F}_q)$, the (Σ_1, P)-orders are $0, 1, \sqrt{q}+1$ (see [4]). In addition $2M_q + M'_q = M'_q = (\sqrt{q})^3 + 1 = (\sqrt{q}+1)(q - \sqrt{q} + 1)$. This example also shows that Corollary 2.2 is non-trivial.

Consider now the linear system Σ_2. Let $P_0 \in \mathcal{X}$ be a point satisfying Corollary 2.2. Then the (Σ_2, P_0)-orders are $0, 1, 2, 3, 4, j$, where $j = j_5^2(P_0)$ (Remark 2.4). Consequently, the Σ_2-orders are $0, 1, 2, 3, 4, \epsilon$, where $5 \le \epsilon = \epsilon_5^2 \le j$ (see (b)). Also, from (f) and (d), the $\mathbf{F}_q$-Frobenius orders of Σ_2 are $0, 1, 2, 3, \nu$, where $\nu = \nu_4^2 \in \{4, \epsilon\}$. From (e) and (g′) we have the following:

$$\deg(S_2) = (6+\nu)(2g-2) + (q+5)2d \ge 5(M_q + M'_q)\,. \tag{2.8}$$

Lemma 2.5 *Let* (H1), (H3), (H2b) *hold, where*

$$\text{(H2b)} \qquad 3 \le d \begin{cases} \le \sqrt{q} & \text{if } q > 23^2, \\ < (q - 5\sqrt{q} + 45)/20 & \text{if } q \le 23^2. \end{cases}$$

Then $\nu = \epsilon$.

Proof. Suppose that $\nu = 4$. Then $d(d-3) \ge 2g-2$, equation (2.8) and $5(M_q + M'_q) \ge \frac{5}{2}(2M_q + M'_q)$ imply that

$$10(d-3) + (q+5)2 \ge \tfrac{5}{2}(q - \sqrt{q} + 1);$$

that is, $d \ge (q - 5\sqrt{q} + 45)/20$, a contradiction. ∎

Lemma 2.6 *Assume that* (H1), (H3), (H2c) *hold, where*

$$\text{(H2c)} \qquad 3 \le d \begin{cases} \le \sqrt{q} & \text{if } q > 23^2, \\ < \min\{(q - 5\sqrt{q} + 45)/20, (q - 5\sqrt{q} + 57)/24\} & \text{if } q \le 23^2. \end{cases}$$

Then ϵ *is a power of* p.

Proof. By the previous lemma and [6, Corollary 3], p divides ϵ; so we may assume that $\epsilon > 5$. If ϵ were not a power of p, then by the p-adic criterion [23, Corollary 1.9] we would have $p \le 3$ and $\epsilon = 6$. Then, as in the proof of Lemma 2.5, we obtain

$$12(d-3) + (q+5)2 \ge \tfrac{5}{2}(q - \sqrt{q} + 1),$$

so that $d \ge (q - 5\sqrt{q} + 57)/24$ and hence $q > 23^2$ by (H2c).

From $(q - 5\sqrt{q} + 57)/24 \le d \le \sqrt{q}$, we find $q - 29\sqrt{q} + 57 \le 0$ and so $529 < q < 722$. This is a contradiction as no power of 2 or 3 lies in the interval $[529, 722]$. ∎

Lemma 2.7 *Assume that* (H1), (H2), (H3), (H4) *hold. Then* $\epsilon = \nu = \sqrt{q}$. *In particular, if* $p \geq 5$, *then* q *is a square.*

Proof. By Lemma 2.5 and (f), $\nu = \epsilon \leq j_5^2(P_0) - 1 \leq 2d - 1$; that is, $\nu \leq 2d - 1$.

Suppose that $\nu > \sqrt{q}$; that is, $\nu^2 = p^e q$ with $e \geq 1$. Now, $\nu \geq 2\sqrt{q}$; for, this is clear for $p \geq 5$ and, for $p = 3$, it follows from the hypothesis that q is a square. If it were false, then $\nu \leq 2d - 1$ would imply $d\sqrt{q}$, a contradiction.

Suppose now that $\nu < \sqrt{q}$; that is, $q = p^e \nu^2$, with $e \geq 1$. From $d(d-3) \geq 2g-2$, $\sqrt{q} \geq d$, (H1) and equation (2.8) we have

$$(6 + \nu)(\sqrt{q} - 3) + (q + 5)2 \geq (6 + \nu)(d - 3) + (q + 5)2 \geq \tfrac{5}{2}(q - \sqrt{q} + 1). \quad (2.9)$$

Hence $2\nu\sqrt{q} - 6\nu \geq q - 17\sqrt{q} + 21$; that is, $2\nu - 6/\sqrt{p^e} \geq \sqrt{q} - 17 + 21/\sqrt{q}$. So

$$17 - \frac{21}{\sqrt{q}} - \frac{6}{\sqrt{p^e}} \geq \nu(\sqrt{p^e} - 2)\,. \quad (2.10)$$

Since $\nu \geq 5$, we have $p^e < 36$. Since q is a square for $p = 3$ and $\nu \geq 5$ is a power of p we have the following possibilities:

$$(p^e, \nu, q) \in \{(9, 9, 729), (5, 5, 125), (5, 25, 3125), (7, 7, 343), (11, 11, 1331)\}.$$

From (2.10) we have respectively $d \geq 23, 6, 49, 13, 37$, and the proof follows from (H2). ∎

It remains to prove part (v) of Proposition 1.1. Take a point P on $\mathcal{X}$. By (iii), there is a divisor D in Σ_2 such that $v_P(D) = \sqrt{q}$. Hence $\deg D \geq \sqrt{q}$; on the other hand, $\deg D = 2d$ by condition (B). Thus $d \geq \frac{1}{2}\sqrt{q}$ and, as q is odd, so $d \geq \frac{1}{2}(\sqrt{q}+1)$. This completes the proof of Proposition 1.1.

3 On certain curves over finite fields

As always, $\mathcal{X}$ is a curve over $\mathbf{F}_q$ satisfying (A) and (B). Suppose that $\mathcal{X}$ satisfies (h4), (h5a), (h6a):

(h5a) the Σ_2-orders are $0, 1, 2, 3, 4, p^v$, with $p^v < q$;

(h6a) the $\mathbf{F}_q$-Frobenius orders for Σ_2 are $0, 1, 2, 3, p^v$.

Hypothesis (A) allows us to consider $\pi_1(\mathcal{X})$ in $\mathrm{PG}(2, q)$ as a parametrized plane curve $\mathcal{C}$. In this model, points of $\mathcal{C}$ are viewded as branches, and the linear series g_2^d is cut out by the linear system Σ_1 of all lines. By hypothesis (B), the linear series g_5^{2d} is cut out by the linear system Σ_2 of all conics. To prove Proposition 1.2, we will use this model and adopt standard terminology on plane curves; see [21].

The aim of this section is to determine, for a given branch γ of $\mathcal{C}$, the equation of a conic which meets γ with multiplicity at least p^v. The conic coincides, except for a finite number of branches of $\mathcal{C}$, with the osculating conic at γ. We will give a necessary and sufficient condition for $\mathcal{C}$ to be Frobenius non-classical for Σ_2.

By [7, Theorem 1] and [9, Satz 10], if $f(x, y) = 0$ is a minimal equation for $\mathcal{C}$, then there exist $h(x, y)$, $z_i = z_i(x, y)$ in $\overline{\mathbf{F}}_q[x, y]$, $i = 0, \ldots, 5$ such that

$$h(x, y)f(x, y) = z_0^{p^v} + z_1^{p^v} x + z_2^{p^v} y + z_3^{p^v} x^2 + z_4^{p^v} xy + z_5^{p^v} y^2. \quad (3.1)$$

It should be noted that the polynomials $h(x,y), z_0(x,y), \ldots, z_5(x,y)$ can be chosen in $\mathbf{F}_q[x,y]$. Further, $\mathcal{C}$ is not a component of the curve with equation $h(x,y)=0$; otherwise, $\mathcal{C}$ would not be classical for Σ_1, but would have order sequence $(0,1,p^v)$, which is not allowed by (h5a).

Conversely, given an absolutely irreducible curve classical for Σ_1, if $\mathcal{C}$ has a minimum equation $f(x,y)=0$ such that there exist $h, z_0, \ldots, z_5 \in \overline{\mathbf{F}}_q[x,y]$ satisfying (3.1), then $\mathcal{C}$ satisfies the conditions (h4), (h5).

Now, take a branch γ of $\mathcal{C}$ of order α and class β with the centre of γ at $P=(a,b)$, and fix a primitive representation $x=x(t), y=y(t)$, where $x(t), y(t) \in \mathbf{F}_q[[t]]$.

Denote $z_i(x(t),y(t))$ by $z_i(t)$, for $0 \le i \le 5$. Then, from (3.1),

$$z_0(t)^{p^v} + z_1(t)^{p^v}x(t) + z_2(t)^{p^v}y(t) + z_3(t)^{p^v}x(t)^2 + z_4(t)^{p^v}x(t)y(t) + z_5(t)^{p^v}y(t)^2 = 0.$$

Choose an index j with $0 \le j \le 5$ such that ord $z_j(t) \le$ ord $z_i(t)$ for $0 \le i \le 5$. Then $m_i(t) = z_i(t)/z_j(t)$ has non-negative order for $0 \le i \le 5$, and it follows that

$$\begin{aligned} m_0(t)^{p^v} + m_1(t)^{p^v}x(t) + m_2(t)^{p^v}y(t) + m_3(t)^{p^v}x(t)^2 + \\ m_4(t)^{p^v}x(t)y(t) + m_5(t)^{p^v}y(t)^2 = 0. \end{aligned} \tag{3.2}$$

with $m_j(t) = 1$.

The expansion of $m_i(t)$ can be written in the following form:

$$m_i(t) = \mu_i^{(0)} + \mu_i^{(1)}t + \ldots + \mu_i^{(k)}t^k + \ldots \tag{3.3}$$

for $0 \le i \le 5$. So

$$\begin{aligned} &[(\mu_0^{(0)})^{p^v} + (\mu_1^{(0)})^{p^v}x(t) + (\mu_2^{(0)})^{p^v}y(t) + (\mu_3^{(0)})^{p^v}x(t)^2 \\ &\quad +(\mu_4^{(0)})^{p^v}x(t)y(t) + (\mu_5^{(0)})^{p^v}y(t)^2] \\ &+ \quad t^{p^v}[(\mu_0^{(1)})^{p^v} + (\mu_1^{(1)})^{p^v}x(t) + (\mu_2^{(1)})^{p^v}y(t) + (\mu_3^{(1)})^{p^v}x(t)^2 \\ &\quad +(\mu_4^{(1)})^{p^v}x(t)y(t) + (\mu_5^{(1)})^{p^v}y(t)^2] \\ &+ \quad \ldots \\ &+ \quad t^{kp^v}[(\mu_0^{(k)})^{p^v} + (\mu_1^{(k)})^{p^v}x(t) + (\mu_2^{(k)})^{p^v}y(t) + (\mu_3^{(k)})^{p^v}x(t)^2 \\ &\quad +(\mu_4^{(k)})^{p^v}x(t)y(t) + (\mu_5^{(k)})^{p^v}y(t)^2] \\ &+ \quad \ldots = 0. \end{aligned}$$

For $k = 0, 1, \ldots$, put

$$s_k(x,y) = (\mu_0^{(k)})^{p^v} + (\mu_1^{(k)})^{p^v}x + (\mu_2^{(k)})^{p^v}y + (\mu_3^{(k)})^{p^v}x^2 + (\mu_4^{(k)})^{p^v}xy + (\mu_5^{(k)})^{p^v}y^2.$$

Then, with $s_k(t) = s_k(x(t),y(t))$, it follows that

$$s_0(t) + t^{p^v}s_1(t) + \ldots + t^{kp^v}s_k(t) + \ldots = 0. \tag{3.4}$$

As $s_0(x,y)$ contains a non-zero coefficient, $\mu_j^{(0)}$, we see that $s_0(x,y) = 0$ is the equation of a conic. For brevity, write $\mu_0^{(i)} = m_i(0) = m_i$; then the following result is obtained.

Proposition 3.1 (i) *The conic $\mathcal{C}_0^{(2)}$ with equation $s_0(x,y)=0$, where*

$$s_0(x,y) = m_0^{p^v} + m_1^{p^v}x + m_2^{p^v}y + m_3^{p^v}x^2 + m_4^{p^v}xy + m_5^{p^v}y^2,$$

meets γ with multiplicity at least p^v.
(ii) *This multiplicity is greater than p^v if and only if $s_1(a,b)=0$, where*

$$s_1(a,b)=(\mu_0^{(1)})^{p^v}+(\mu_1^{(1)})^{p^v}a+(\mu_2^{(1)})^{p^v}b+(\mu_3^{(1)})^{p^v}a^2+(\mu_4^{(1)})^{p^v}ab+(\mu_5^{(1)})^{p^v}b^2.$$

(iii) *If $P=(a,b)$ is not a common point of the six curves $z_i(x,y)=0$, for $0\le i\le 5$, then the equation of $\mathcal{C}_0^{(2)}$ is*

$$\begin{aligned}&z_0(a,b)^{p^v}+z_1(a,b)^{p^v}x+\\&\quad z_2(a,b)^{p^v}y+z_3(a,b)^{p^v}x^2+z_4(a,b)^{p^v}xy+z_5(a,b)^{p^v}y^2=0.\end{aligned}\tag{3.5}$$

In particular, if $P=(a,b)$ is a generic point of $\mathcal{C}$ then the osculating conic of $\mathcal{C}$ at $P(a,b)$ is $\mathcal{C}_0^{(2)}$ and has equation (3.5).

Remark 3.2 It may happen that a particular branch does not have $\mathcal{C}_0^{(2)}$ as osculating conic, as the following example shows. The Fermat curve $\mathcal{F}$ with equation

$$x^{p-1}+y^{p-1}+1=0,$$

satisfies (h4)and (h5) since $xy(x^{p-1}+y^{p-1}+1)=y^px+x^py+xy$. Now, take a point $P=(0,c)$ with $c^{p-1}=-1$ of $\mathcal{F}$ on the y-axis. Then P is an inflexion of $\mathcal{F}$; thus the osculating conic of $\mathcal{F}$ at P is degenerate and consists of the horizontal line $y=c$ through P counted twice. On the other hand, the conic $\mathcal{C}_0^{(2)}$ is also degenerate but consists of two distinct lines $x(y-c)=0$, namely the horizontal and vertical lines through P, since $c^px+xy=x(y-c)$.

Looking back through this section, or alternatively looking forward to §§4–8 we see that the conic $\mathcal{C}_0^{(2)}$ plays a central role in the study of non-classical curves with respect to Σ_2. When the symbol $\mathcal{C}_0^{(2)}$ is used it should be understood that $\mathcal{C}_0^{(2)}$ denotes the conic with equation

$$m_0^{p^v}+m_1^{p^v}x+m_2^{p^v}y+m_3^{p^v}x^2+m_4^{p^v}xy+m_5^{p^v}y^2=0.$$

Now, we consider the other relevant condition on $\mathcal{C}$, that $\mathcal{C}$ is Frobenius non-classical for Σ_2.

Proposition 3.3 *The curve $\mathcal{C}$ is Frobenius non-classical for Σ_2 if and only if there exists $s(x,y)$ in $\mathbf{F}_q[x,y]$ such that*

$$\begin{aligned}&s(x,y)f(x,y)=\\&\quad z_0(x,y)+z_1(x,y)x^{p^{h-v}}+z_2(x,y)y^{p^{h-v}}+\\&\quad z_3(x,y)x^{2p^{h-v}}+z_4(x,y)x^{p^{h-v}}y^{p^{h-v}}+z_5(x,y)y^{2p^{h-v}}.\end{aligned}\tag{3.6}$$

Proof. By the previous proposition, if $P=(a,b)$ is a generic point of $\mathcal{C}$, then the osculating conic of $\mathcal{C}$ at P has equation (3.5). Therefore, $\mathcal{C}$ is Frobenius non-classical if and only if

$$z_0(a,b)^{p^v}+z_1(a,b)^{p^v}a^q+z_2(a,b)^{p^v}b^q+z_3(a,b)^{p^v}a^{2q}+z_4(a,b)^{p^v}a^qb^q+z_5(a,b)^{p^v}b^{2q}=0,$$

for a generic point of $\mathcal{C}$. Since $\mathcal{C}$ is irreducible, the proposition follows. ∎

It should be noted that Proposition 3.3 will be crucial for embedding the curve $\mathcal{C}$ in $\mathrm{PG}(5,q)$.

4 Curves non-classical for conics

In this section we suppose (h2a), (h3a), (h4), (h5a), (h6a) hold:

(h2a) $d < p^v$;

(h3a) $p \geq 3$.

Now, we determine all possible triads $(0, r, s)$ that can be the order sequence of a branch γ of a curve $\mathcal{C}$ satisfying (h5a). Although there are, in general, many possibilities, the conditions (h2a) and (h3a) imply that there are only three types of branches. These will be studied in the subsequent sections.

Consider a branch γ of $\mathcal{C}$ of order r, class $\beta = s - r$ and centre $P = (a, b)$. We will say that γ is *regular* if it is a linear branch, that is of order $r = 1$ and class $\beta = 1$. In other words, γ is regular if the order sequence of γ with respect to Σ_1 is $(0, 1, 2)$.

Now, take a primitive representation of γ in the form

$$\begin{array}{rcccl} x & = & x(t) & = & a + m_{11}t^r + \ldots, \\ y & = & y(t) & = & b + m_{21}t^r + \ldots + b_s t^s + \ldots, \end{array} \tag{4.1}$$

where the tangent ℓ to γ has equation $m_{21}(x - a) - m_{11}(y - b) = 0$.

Introduce a new system of reference taking P to the origin and ℓ to the x-axis. This change of coordinates from (x, y) to (X, Y) is given by

$$\begin{array}{rcl} x & = & m_{11}X + m_{12}Y + a, \\ y & = & m_{21}X + m_{22}Y + b, \end{array} \tag{4.2}$$

with $a_r = m_{11}, b_r = m_{21}$. Equation (3.1) is invariant under this transformation. To see this, let us put, for $0 \leq i \leq 5$,

$$\begin{array}{l} z_i(x, y) = z_i(m_{11}X + m_{12}Y + a, m_{21}X + m_{22}Y + b) = \bar{z}_i(X, Y), \\ f(x, y) = f(m_{11}X + m_{12}Y + a,\ m_{21}X + m_{22}Y + b) = F(X, Y), \\ h(x, y) = h(m_{11}X + m_{12}Y + a,\ m_{21}X + m_{22}Y + b) = H(X, Y), \\ a = c^{p^v}, \quad b = d^{p^v}, \quad m_{ij} = {n_{ij}}^{p^v},\ i, j = 1, 2, \end{array}$$

and write $\bar{z}_i = \bar{z}_i(X, Y)$. Then, with

$$\begin{array}{l} Z_0(X, Y) = \bar{z}_0 + c\bar{z}_1 + d\bar{z}_2 + c^2\bar{z}_3 + cd\bar{z}_4 + d^2\bar{z}_5, \\ Z_1(X, Y) = n_{11}\bar{z}_1 + n_{21}\bar{z}_2 + 2cn_{11}\bar{z}_3 + (cn_{11} + dn_{21})\bar{z}_4 + 2dn_{21}\bar{z}_5, \\ Z_2(X, Y) = n_{12}\bar{z}_1 + n_{22}\bar{z}_2 + 2cn_{12}\bar{z}_3 + (cn_{22} + dn_{12})\bar{z}_4 + 2dn_{22}\bar{z}_5, \\ Z_3(X, Y) = {n_{11}}^2\bar{z}_3 + n_{11}n_{21}\bar{z}_4 + {n_{21}}^2\bar{z}_5, \\ Z_4(X, Y) = 2n_{11}n_{12}\bar{z}_3 + (n_{12}n_{21} + n_{11}n_{22})\bar{z}_4 + 2n_{21}n_{22}\bar{z}_5, \\ Z_5(X, Y) = {n_{12}}^2\bar{z}_3 + n_{12}n_{22}\bar{z}_4 + {n_{22}}^2\bar{z}_5, \end{array}$$

and with $Z_i = Z_i(X, Y),\ i = 0, \ldots, 5$, equation (3.1) becomes

$$H(X, Y)F(X, Y) = Z_0^{p^v} + Z_1^{p^v}X + Z_2^{p^v}Y + Z_3^{p^v}X^2 + Z_4^{p^v}XY + Z_5^{p^v}Y^2. \tag{4.3}$$

A primitive representation of γ in the new coordinate system is given by

$$\begin{array}{rcccl} X & = & X(t) & = & t^r + \ldots, \\ Y & = & Y(t) & = & ct^s + \ldots, \end{array} \tag{4.4}$$

where

$$\begin{aligned} x(t) &= m_{11}X(t) + m_{12}Y(t) + a, \\ y(t) &= m_{21}X(t) + m_{22}Y(t) + b. \end{aligned} \tag{4.5}$$

Put

$$\begin{aligned} z_i(t) &= z_i(x(t), y(t)) \\ &= z_i(m_{11}X(t) + m_{12}Y(t) + a,\ m_{21}X(t) + m_{22}Y(t) + b) \\ &= \bar{z}_i(X(t), Y(t)) \\ &= \bar{z}_i(t); \\ Z_i(t) &= Z_i(X(t), Y(t)), \end{aligned}$$

for $0 \le i \le 5$. Then, the relationship between the $Z_i(t)$ and the $\bar{z}_i(t)$ is exactly the same as between the $Z_i(X, Y)$ and the $\bar{z}_i(X, Y)$. Since this relationship is linear and invertible, it follows that

$$\min_{0\le i\le 5}\{\text{ord } z_i(t)\} = \min_{0\le i\le 5}\{\text{ord } Z_i(t)\}.$$

This shows that the index j introduced in §3 is invariant under a change of reference system in the sense that ord $Z_j(t) \le$ ord $Z_i(t)$ for $0 \le i \le 5$.

Put, as in §3, $M_i(t) = Z_i(t)/Z_j(t)$ and $M_i(0) = M_i$, for $0 \le i \le 5$. Then the conic $\mathcal{C}_0^{(2)}$ has equation

$$M_0^{p^v} + M_1^{p^v}X + M_2^{p^v}Y + M_3^{p^v}X^2 + M_4^{p^v}XY + M_5^{p^v}Y^2 = 0$$

with respect to the new reference system (X, Y). This proves that the conic $\mathcal{C}_0^{(2)}$ is a covariant of $\mathcal{C}$. From (4.3) we obtain

$$\begin{aligned} &M_0(t)^{p^v} + M_1(t)^{p^v}X + \\ &\quad M_2(t)^{p^v}Y + M_3(t)^{p^v}X^2 + M_4(t)^{p^v}XY + M_5(t)^{p^v}Y^2 = 0. \end{aligned} \tag{4.6}$$

The following proposition comes from [13, Proposition 3.4].

Proposition 4.1 *Let $\mathcal{C}$ be an irreducible algebraic curve of degree $d < p^v$ which satisfies* (h4), (h5). *If r is the order and $s - r$ is the class of a branch γ of $\mathcal{C}$, then one of the following holds*:

$$s = 2r, \text{ and } \mathcal{C}_0^{(2)} \text{ has equation } M_2Y + M_3X^2 + M_4XY + M_5Y^2 = 0 \tag{4.7}$$
$$\text{with } M_2M_3 \ne 0;$$
$$s = \tfrac{1}{2}(r + p^v), \text{ and } \mathcal{C}_0^{(2)} \text{ has equation } Y^2 = 0; \tag{4.8}$$
$$s = p^v - r, \text{ and } \mathcal{C}_0^{(2)} \text{ has equation } M_4XY + M_5Y^2 = 0 \text{ with } M_2 \ne 0. \tag{4.9}$$

In this proposition, the cases (4.7), (4.8), and (4.9) correspond to the conic $\mathcal{C}_0^{(2)}$ being non-degenerate, a repeated line, and a proper line-pair.

Finally, in this section, we prove a result that will be useful below. With

$$\Delta(w_0, w_1, w_2, w_3, w_4, w_5) = \begin{vmatrix} 2w_0 & w_1 & w_2 \\ w_1 & 2w_3 & w_4 \\ w_2 & w_4 & 2w_5 \end{vmatrix},$$

let us write

$$\begin{aligned} u_i(t) &= z_i(t)^{p^v}, \\ \|m(t)\| &= \Delta(m_0(t), m_1(t), m_2(t), m_3(t), m_4(t), m_5(t)), \\ a_2(t) &= u_2(t) + u_4(t)x(t) + 2u_5(t)y(t), \\ b_2(t) &= m_2(t)^{p^v} + m_4(t)^{p^v}x(t) + 2m_5(t)^{p^v}y(t). \end{aligned}$$

Analogously, we have $M(t),\ A_2(t),\ B_2(t)$.

Henceforth, let $m_{12} = 0$; in other words, the infinite point Y_∞ is the same for the two reference systems. Under this hypothesis, we prove the next result. Here, using (3.1) and (4.3),

$$\begin{aligned} z(t) &= h(x(t), y(t))\, f(x(t), y(t)), \\ Z(t) &= H(X(t), Y(t))\, F(X(t), Y(t)), \end{aligned}$$

and $\mathcal{G}$ is the curve given by $H(X, Y)F(X, Y) = 0$.

Proposition 4.2

$$\operatorname{ord} \|z(t)\| = \operatorname{ord} \|Z(t)\|; \tag{4.10}$$

$$\operatorname{ord} \|a_2(t)\| = \operatorname{ord} \|A_2(t)\|; \tag{4.11}$$

$$\operatorname{ord} \|m(t)\| = \operatorname{ord} \|M(t)\|; \tag{4.12}$$

$$\operatorname{ord} b_2(t) = \operatorname{ord} B_2(t). \tag{4.13}$$

Proof. For (4.10), both $\operatorname{ord} \|z(t)\|$ and $\operatorname{ord} \|Z(t)\|$ are equal to the intersection multiplicity of the branch γ with the Hessian of the curve $\mathcal{G}$. The first part of the proposition follows. The second part follows from the fact that the intersection multiplicity of γ with the polar curve of $\mathcal{G}$ with respect to the point Y_∞ is equal to both $\operatorname{ord} \|a_2(t)\|$ and $\operatorname{ord} \|A_2(t)\|$; by construction, the point Y_∞ is the point at infinity of both the y-axis and the Y-axis. Earlier in this section it was shown that $\min_{0 \le i \le 5}\{\operatorname{ord}\ z_i(t)\} = \min_{0 \le i \le 5}\{\operatorname{ord}\ Z_i(t)\}$. Now, the third and fourth parts follow similarly. ∎

5 Frobenius non-classical curves

Now, we examine more closely the effect of the condition (h6a) on $\mathcal{C}$; namely, that the $\mathbf{F}_q$-Frobenius orders for Σ_2 are $0, 1, 2, 3, p^v$.

(h6a) $\mathcal{C}$ is Frobenius non-classical with respect to Σ_2.

Some geometric properties of the branches of $\mathcal{C}$ will now be established, depending on the types of branches found in §4. These properties described in Propositions 5.2 − 5.5 are interesting in themselves, but will also allow the application of Plücker's formula and the Theorem of Stöhr and Voloch in §9 to non-classical curves with many rational points.

Some preliminary facts are required.

Proposition 5.1 *If $\mathcal{C}$ satisfies* (h6a), *then the conic $\mathcal{C}_0^{(2)}$ passes through the point $P' = (a^q, b^q)$.*

Proof. First,

$$\begin{aligned} \bar{x}(\tau) &= a^q + m_{11}^q \tau + \ldots, \\ \bar{y}(\tau) &= b^q + m_{21}^q \tau + \ldots \end{aligned}$$

is an irreducible representation of the branch $\bar{\gamma}$ of $\mathcal{C}$ which is the image of γ under the Frobenius collineation. We may argue as in the proof of Proposition 3.1. From (3.6) we obtain the following:

$$\begin{aligned} & [(\mu_0^{(0)})^{p^v} + (\mu_1^{(0)})^{p^v}\bar{x}(t^q) + (\mu_2^{(0)})^{p^v}\bar{y}(t^q) + (\mu_3^{(0)})^{p^v}\bar{x}(t^q)^2 \\ & \qquad +(\mu_4^{(0)})^{p^v}\bar{x}(t^q)\bar{y}(t^q) + (\mu_5^{(0)})^{p^v}\bar{y}(t^q)^2] \\ + \quad & t^{p^v}[(\mu_0^{(1)})^{p^v} + (\mu_1^{(1)})^{p^v}\bar{x}(t^q) + (\mu_2^{(1)})^{p^v}\bar{y}(t^q) + (\mu_3^{(1)})^{p^v}\bar{x}(t^q)^2 \\ & \qquad +(\mu_4^{(1)})^{p^v}\bar{x}(t^q)\bar{y}(t^q) + (\mu_5^{(1)})^{p^v}\bar{y}(t^q)^2] + \quad \ldots \\ + \quad & t^{kp^v}[(\mu_0^{(k)})^{p^v} + (\mu_1^{(k)})^{p^v}\bar{x}(t^q) + (\mu_2^{(k)})^{p^v}\bar{y}(t^q) + (\mu_3^{(k)})^{p^v}\bar{x}(t^q)^2 \\ & \qquad +(\mu_4^{(k)})^{p^v}\bar{x}(t^q)\bar{y}(t^q) + (\mu_5^{(k)})^{p^v}\bar{y}(t^q)^2] + \ldots = 0. \end{aligned}$$

For $k = 0, 1, \ldots$, put

$$s_k(\bar{x}, \bar{y}) = (\mu_0^{(k)})^{p^v} + (\mu_1^{(k)})^{p^v}\bar{x} + (\mu_2^{(k)})^{p^v}\bar{y} + (\mu_3^{(k)})^{p^v}\bar{x}^2 + (\mu_4^{(k)})^{p^v}\bar{x}\bar{y} + (\mu_5^{(k)})^{p^v}\bar{y}^2.$$

Then, with $\bar{s}_k(\tau) = s_k(\bar{x}(\tau), \bar{y}(\tau))$, it follows that

$$\bar{s}_0(t^q) + t^{p^v}\bar{s}_1(t^q) + \ldots + t^{kp^v}\bar{s}_k(t^q) + \ldots = 0. \tag{5.1}$$

So $\bar{s}_0(0) = 0$, whence $s_0(0) = 0$, since $\bar{s}_0(0) = s_0(0)$. This shows that $\mathcal{C}_0^{(2)}$ passes through $P' = (a^q, b^q)$. ∎

From (5.1) we can also infer that $\bar{s}_1(0) = 0$. However, $\bar{s}_1(0) = s_1(0)$ only holds in the case that γ is centred at an $\mathbf{F}_q$-rational point.

Proposition 3.1(ii) gives the next result.

Proposition 5.2 *If γ is a branch of $\mathcal{C}$ centred at an $\mathbf{F}_q$-rational point, then $\mathcal{C}_0^{(2)}$ meets γ with multiplicity greater than p^v.*

Now we are in a position to investigate each one the three possibilities of Proposition 4.1 under condition (h6a).

Proposition 5.3 *Let γ be a branch of $\mathcal{C}$ with centre $P = (a, b)$ not $\mathbf{F}_q$-rational such that (4.7) holds. If $\mathcal{C}$ satisfies* (h6a) *and $d < p^v$, then the point $P' = (a^q, b^q)$ does not lie on the tangent to γ; also, $(a - a^q)m_{21} - (b - b^q)m_{11} \neq 0$.*

Proof. By Proposition 5.1, the conic $\mathcal{C}_0^{(2)}$ passes through the point $P' = (a^q, b^q)$. On the other hand, from (4.7) we know that $\mathcal{C}_0^{(2)}$ is a non-degenerate conic whose tangent line at $P = (a, b)$ coincides with the tangent of γ. ∎

Proposition 5.4 *Let γ be a branch of $\mathcal{C}$ with centre $P = (a, b)$ not $\mathbf{F}_q$-rational such that (4.8) holds. If $\mathcal{C}$ satisfies* (h6a) *and $d < p^v$, then the point $P' = (a^q, b^q)$ lies on the tangent to γ; also, $(a - a^q)m_{21} - (b - b^q)m_{11} = 0$.*

Proof. By Proposition 4.1, $\mathcal{C}_0^{(2)}$ is a degenerate conic and consists of the tangent line of γ counted twice. Thus, our assertion is an immediate consequence of Proposition 5.1. ∎

Proposition 5.5 *Assume that $\mathcal{C}$ satisfies* (h6a) *and that $d < p^v$. If γ is a branch of $\mathcal{C}$ such that (4.9) holds, then the centre of γ is not $\mathbf{F}_q$-rational.*

Proof. In this case, $\mathcal{C}_0^{(2)}$ splits into two distinct lines, one of which coincides with the tangent of γ. This shows that $\mathcal{C}_0^{(2)}$ meets γ with multiplicity $s + r = p^v$. Hence, the result follows from Proposition 5.2. ∎

6 The ramification divisor cut out by lines

As in §2, denote by R_1 the linear series cut out on $\mathcal{C}$ by Σ_1. With $v_P(R_1)$ the weight of a point P, or more precisely of a branch, of $\mathcal{C}$, a count of the Weierstrass points, each with the proper weight, gives the Plücker equation as in property (a) of §2:

$$\sum_{P \in \mathcal{C}} v_P(R_1) \quad = \quad 3(2g - 2) + 3d. \tag{6.1}$$

It should be noticed that the classical Plücker formula

$$v_P(R_1) = r + s - 3$$

is not valid when one of $r, s, s - r$ is divisible by p. Instead, we can use the following formula (see [13, Proposition 4.1]).

Proposition 6.1 *If $\operatorname{ord} X(t)$ is not divisible by p^v,*

$$v_P(R_1) = p^v \operatorname{ord} \|Z(t)\| + 3[\operatorname{ord} X'(t) - \operatorname{ord} A_2(t)].$$

By Proposition 4.2, this proposition is valid for the original reference system, and we formulate this in the next result.

Proposition 6.2 *If $\operatorname{ord} x(t)$ is not divisible by p^v,*

$$v_P(R_1) = p^v \operatorname{ord} \|z(t)\| + 3[\operatorname{ord} x'(t) - \operatorname{ord} a_2(t)].$$

It will be convenient to have Propositions 6.1 and 6.2 in the same notation as that of §4. They become the following.

Proposition 6.3 *If $\operatorname{ord} x(t)$ is not divisible by p^v,*

$$v_P(R_1) = p^v \operatorname{ord} \|m(t)\| + 3[\operatorname{ord} x'(t) - \operatorname{ord} b_2(t)].$$

Proposition 6.4 *If $\operatorname{ord} X(t)$ is not divisible by p^v, then*

$$v_P(R_1) = p^v \operatorname{ord} \|M(t)\| + 3[\operatorname{ord} X'(t) - \operatorname{ord} B_2(t)].$$

7 The Frobenius divisor cut out by lines

The Frobenius divisor was originally used in [23, §2] to count, on a plane curve $\mathcal{C}$ that is $\mathbf{F}_q$-Frobenius classical, the points P such that the tangent at P passes through the image P' of P under the Frobenius collineation. For this case, (e) becomes the following:

$$\sum v_P(S_1) = (2g-2) + (q+2)d. \tag{7.1}$$

Now we state some useful formulas for the weight $v_P(S_1)$. Let γ be the branch of $\mathcal{C}$ with primitive representation (4.1). From [23, Proposition 2.3], $v_P(S_1)$ is given by

$$v_P(S_1) = \operatorname{ord}\{[x(t)-x(t)^q]y'(t) - [y(t)-y(t)^q]x'(t)\}.$$

Since $v_P(S_1)$ is not invariant under all affine transformations but only for those fixing the plane over $\mathbf{F}_q$, one needs to know how $v_P(S_1)$ changes under a linear transformation (4.2). With $x, x', y, y', X, X', Y, Y'$ all functions of t as in §4,

$$\begin{aligned}
&(x-x^q)y' - (y-y^q)x' \\
&= [a-a^q + m_{11}X + m_{12}Y - (m_{11}X+m_{12}Y)^q][m_{21}X' + m_{22}Y'] \\
&\quad -[b-b^q + m_{21}X + m_{22}Y - (m_{21}X+m_{22}Y)^q][m_{11}X' + m_{12}Y'] \\
&= [(a-a^q)m_{21} - (b-b^q)m_{11}]X' + [(a-a^q)m_{22} - (b-b^q)m_{12}]Y' \\
&\quad +(m_{11}m_{22} - m_{12}m_{21})(XY' - YX') - (m_{11}X+m_{12}Y)^q(m_{21}X' + m_{22}Y') \\
&\quad +(m_{21}X + m_{22}Y)^q(m_{11}X' + m_{12}Y').
\end{aligned}$$

Then, from [13, Section 4], we derive Propositions 7.1 to 7.4.

Proposition 7.1

$$\begin{aligned}
v_P(S_1) = \quad & \operatorname{ord} X' + \\
& \operatorname{ord}\{[(a-a^q)m_{21} - (b-b^q)m_{11}] \\
& \quad + [(a-a^q)m_{22} - (b-b^q)m_{12}]Y'/X' \\
& \quad + (m_{11}m_{22} - m_{12}m_{21})(XY'/X' - Y) \\
& \quad - (m_{11}X + m_{12}Y)^q(m_{21} + m_{22}Y'/X') \\
& \quad + (m_{21}X + m_{22}Y)^q(m_{11} + m_{12}Y'/X')\}.
\end{aligned}$$

A useful corollary to this result is the following.

Proposition 7.2 *Suppose that* $\operatorname{ord} X(t) = r$ *and* $\operatorname{ord} Y(t) = s$ *are both prime to* p. *Then one of the following three cases occurs*:

(i) *if* $a, b \in \mathbf{F}_q$, *then* $v_P(S_1) \geq r + s - 1$;

(ii) *if* $(a-a^q)m_{21} - (b-b^q)m_{11} = 0$, *but either* $a \notin \mathbf{F}_q$ *or* $b \notin \mathbf{F}_q$, *then* $v_P(S_1) = s-1$;

(iii) *if* $(a-a^q)m_{21} - (b-b^q)m_{11} \neq 0$, *then* $v_P(S_1) = r-1$.

Now, we show that this proposition allows us to establish a useful lower limit for $v_P(S_1)$ in the case that $d < p^v$.

Proposition 7.3 *If* $d < p^v$, *then*

$$\operatorname{ord}\{Y(t)/X(t)\} = \operatorname{ord}\{Y'(t)/X'(t)\}; \tag{7.2}$$

$$\operatorname{ord}\{X(t)Y'(t)/X'(t) - Y(t)\} \geq \operatorname{ord} Y(t). \tag{7.3}$$

Proof. See [13, Proposition 4.3]. ∎

Proposition 7.4 *Let $d < p^v$. Then one of the following holds*:

$$\begin{aligned} v_P(S_1) &\geq \operatorname{ord} X'(t) + \operatorname{ord} Y(t), \text{ if } a, b \in \mathbf{F}_q; && (7.4)\\ v_P(S_1) &= \operatorname{ord} X'(t) + \operatorname{ord} Y(t) - \operatorname{ord} X(t), && (7.5)\\ &\quad \text{if } (a-a^q)m_{21} - (b-b^q)m_{11} = 0 \text{ but } a \notin \mathbf{F}_q \text{ or } b \notin \mathbf{F}_q;\\ v_P(S_1) &= \operatorname{ord} X'(t) \text{ if } (a-a^q)m_{21} - (b-b^q)m_{11} \neq 0. && (7.6) \end{aligned}$$

Proof. See [13, Proposition 4.4]. ∎

8 The embedding in five dimensions

In the study of non-classical curves it is often convenient to consider a model embedded in a projective space of suitable dimension using the classical Veronese mapping. Here, we will use a different embedding connected to the Gauss map. This will allow us to find a bound for the degree of the embedded curve which depends on the number of its $\mathbf{F}_q$-rational points. In turn, this leads in (8.11) to a strong upper bound on the order of a branch γ of the curve $\mathcal{C}$.

We now consider the linear series Γ on $\mathcal{C}$ cut out by the linear system of all curves with equation $\lambda_0 z_0(x,y) + \lambda_1 z_1(x,y) + \ldots + \lambda_5 z_5(x,y) = 0$. We assume that Γ is base-point-free and that Γ is simple in the sense that those of its divisors which contain a generic point P of $\mathcal{C}$ cannot contain a further common point Q on $\mathcal{C}$. This follows from the hypothesis $d < p^v$ because the osculating conic of $\mathcal{C}$ at a point P cannot be the osculating conic at another point Q.

By the Veronese morphism Φ_2, the curve $\mathcal{C}$ is embedded in $\mathrm{PG}(5, \overline{\mathbf{F}}_q)$. Its dual curve $\mathcal{C}'$ is defined as the reduced closure of the set of osculating hyperplanes at generic points of the curve $\mathcal{C}$ in $\mathrm{PG}(5,q)$. By Proposition 3.1, the Gauss map $\sigma : \mathcal{C} \to \mathcal{C}'$ is the product of the morphism $\omega : \mathcal{C} \to \mathrm{PG}(5, \overline{\mathbf{F}}_q)$ given by

$$(1,x,y) \mapsto (z_0(x,y), z_1(x,y), z_2(x,y), z_3(x,y), z_4(x,y), z_5(x,y))$$

and the Frobenius collineation of $\mathrm{PG}(5,q)$ defined by

$$\varphi : (x_0, \ldots, x_5) \to (x_0^{p^v}, \ldots, x_5^{p^v}).$$

Let $\mathcal{Z}$ be the image curve of $\mathcal{C}$ under ω. Then $\mathcal{Z}$ is the *projective image of* $\mathcal{C}$ *with respect to* Γ, and $\deg \mathcal{Z} = \operatorname{ord} \Gamma$. In particular, $\mathcal{Z}$ and $\mathcal{C}$ are birationally isomorphic.

Now, a formula for $\deg \mathcal{Z}$ will be established. In §4, we the introduced the cubic hypersurface $\mathcal{S}^3$ with equation

$$\Delta(X_0, X_1, X_2, X_3, X_4, X_5) = 0.$$

Now, ord $\|m(t)\|$ is equal to the intersection multiplicity of $\mathcal{Z}$ with $\mathcal{S}^3$ at the point P; that is, it equals the weight of the branch γ in $\mathcal{Z} \cap \mathcal{S}^3$. By Bézout's theorem and (4.12),

$$\sum \operatorname{ord} \|M(t)\| = \operatorname{ord} \|m(t)\| = 3 \deg \mathcal{Z}, \tag{8.1}$$

where the summation is over all branches of $\mathcal{C}$. We are now ready to prove the next result.

Proposition 8.1 *If* $\operatorname{ord} x(t)$ *is not divisible by* p^v, *then*

$$p^v \deg \mathcal{Z} = m - d + \sum \operatorname{ord} B_2(t), \tag{8.2}$$

where m *is the class of* $\mathcal{C}$.

Proof. From property (a) in §2, equation (8.1), and Proposition 6.4,

$$3(2g-2) + 3d = \sum v_P(R_2) = 3p^v \deg \mathcal{Z} + 3\sum(\operatorname{ord} X'(t) - \operatorname{ord} B_2(t)).$$

Further, by Hurwitz's formula in the form of [13, Proposition 5.1],

$$\sum \operatorname{ord} X'(t) = 2g - 2 + 2d - m.$$

The result follows. ∎

The next step is to give an upper bound for $\sum \operatorname{ord} B_2(t)$ in order to obtain an upper bound for $\deg \mathcal{Z}$. We limit ourselves to the case $d < p^v$ and we also assume that (h6a) holds.

First, $\operatorname{ord} B_2(t)$ is calculated for each of the three cases of Proposition 4.1.

The Case $s = 2r$:

Here $\operatorname{ord} Z_2(t) = \operatorname{ord} Z_3(t)$ is strictly less than the orders of the four other $Z_i(t)$. Therefore,
$B_2(t) = 1 + [Z_4(t)/Z_2(t)]^{p^v} + [Z_5(t)/Z_2(t)]^{p^v} X(t)$. Hence, $\operatorname{ord} B_2(t) = 0$.

The Case $2s - r = p^v$:

This time, $\operatorname{ord} Z_5(t)$ is strictly less than the orders of the other $Z_i(t)$. Therefore, $B_2(t) = [Z_2(t)/Z_5(t)]^{p^v} + [Z_4(t)/Z_5(t)]^{p^v} X(t) + 2Y(t)$. Since $\operatorname{ord} Y(t) < p^v$, so $\operatorname{ord} B_2(t) = s$.

The Case $s + r = p^v$:

Now, $\operatorname{ord} Z_4(t)$ is strictly less than the orders of the other $Z_i(t)$. Therefore, $B_2(t) = [Z_2(t)/Z_4(t)]^{p^v} + X(t) + 2[Z_5(t)/Z_4(t)]^{p^v} Y(t)$. Since $\operatorname{ord} X(t) < p^v$, so $\operatorname{ord} B_2(t) = r$.

Proposition 8.2 *Let* $d < p^v$ *and suppose that* $\mathcal{C}$ *is Frobenius non-classical for* Σ_2.

(i) *If* $a, b \in \mathbf{F}_q$, *then*

$$\operatorname{ord} B_2(t) \le \begin{cases} v_P(S_1) - (3r-1) & \text{if (4.7) holds,} \\ v_P(S_1) - (r-1) & \text{if (4.8) holds.} \end{cases} \tag{8.3}$$

(ii) *If either* $a \notin \mathbf{F}_q$ *or* $b \notin \mathbf{F}_q$, *then*

$$\operatorname{ord} B_2(t) \le \begin{cases} v_P(S_1) - (r-1) & \text{if (4.7) holds,} \\ v_P(S_1) + 1 & \text{if (4.8) or (4.9) holds.} \end{cases} \tag{8.4}$$

Proof. Let $a, b \in \mathbf{F}_q$. From Proposition 7.4, $v_P(S_1) \ge s + r - 1$. By Proposition 5.5, either (4.7) or (4.8) holds. From above, in the former case, $\operatorname{ord} B_2(t) = 0$ and $s = 2r$; in the latter case, $\operatorname{ord} B_2(t) = s$ and $2s - r = p^v$. From this we obtain (i).

The argument is similar for (ii). Assume that either $a \notin \mathbf{F}_q$ or $b \notin \mathbf{F}_q$. If (4.7) holds, then Proposition 5.3 shows that we can apply (7.6) in Proposition 7.4; we obtain that $v_P(S_1) \ge r - 1$. If (4.8) holds, then (7.5) is applied following Proposition 5.4; here, we obtain $v_P(S_1) \ge s - 1$. Since $\operatorname{ord} B_2(t) = s$, we get the required result. Finally, if (4.9) holds, then $\operatorname{ord} B_2(t) = r$ and also $v_P(S_1) \ge r - 1$, using (7.5) and (7.6); hence $\operatorname{ord} B_2(t) \le v_P(S_1) + 1$. ∎

It may be observed that, from Proposition 5.5, in the same notation as (1.4),

$$\begin{aligned}\tilde{\mathcal{Z}}_1(\mathbf{F}_q) &= \{\text{branches centred at } \mathbf{F}_q\text{-points of type (4.7)}\}\,;\\ \tilde{\mathcal{Z}}_2(\mathbf{F}_q) &= \{\text{branches centred at } \mathbf{F}_q\text{-points of type (4.8)}\}\,.\end{aligned}$$

From (8.3) and (8.4) it follows immediately that

$$\sum \operatorname{ord} B_2(t) \le \sum v_P(S_1) - 2M_q - M_q' - \sum{}'(r-1) + N, \tag{8.5}$$

where M_q is the number of branches centred at an $\mathbf{F}_q$-rational point of $\mathcal{C}$ of type (4.7) and M_q' is the number of branches centred at an $\mathbf{F}_q$-rational point of type (4.8), each one counted with multiplicity $r \ge 1$, the summation $\sum'$ is over all branches of $\mathcal{C}$ of type (4.7), and N denotes the number of branches of type (4.8) and (4.9).

We observe that

$$N \le 6(2g-2+d)/(p^v-3). \tag{8.6}$$

In fact, from the inequality $v_P(R_1) \ge s+r-3$ ([23, Theorem 1.5]), it follows that

$$\sum(s+r-3) \le \sum v_P(R_1) = 3(2g-2)+3d.$$

On the other hand,

$$\sum(s+r-3) = N_0(p^v-3) + \sum{}''(p^v+3r-6)/2,$$

where N_0 is the number of branches of type (4.9) while the summation $\sum''$ is over the $N-N_0$ branches of type (4.8); therefore,

$$\sum(s+r-3) \ge N_0(p^v-3) + (N-N_0)(p^v-3)/2.$$

Hence, $\sum(s+r-3) \ge \frac{1}{2}N(p^v-3)$ and (8.6) follows. It should be noted that, since $2g-2 \le d(d-3)$ and $d \le p^v-1$, the expression on the right of (8.6) is at most $6d$. Hence (8.5) can be put in a more manageable but somewhat weaker form as follows:

$$\sum \operatorname{ord} B_2(t) \le \sum v_P(S_1) - 2M_q - M_q' + 6d. \tag{8.7}$$

Putting together (7.1), (8.2) and (8.7) gives the next result.

Proposition 8.3 *If $\mathcal{C}$ is Frobenius non-classical for Σ_2 of degree $d < p^v$, then*

$$p^v \deg \mathcal{Z} < m + (2g-2) + [(q+1)d - 2M_q - M_q'] + 6d, \tag{8.8}$$

where M_q and M_q' are the numbers of branches of $\mathcal{C}$ of type (4.7) and (4.8) centred at $\mathbf{F}_q$-rational points, each one counted with multiplicity equal to its order r.

To obtain a significant lower bound for the degree of $\mathcal{Z}$ depending only on d, only condition (h6a) is required. To this end, the criterion of Proposition 3.3 for $\mathcal{C}$ to be Frobenius non-classical will be useful.

The key idea for obtaining a lower bound for the degree of $\mathcal{Z}$ is to evaluate the intersection multiplicity of $\mathcal{Z}$ with a particular hyperplane at one of their common points. In fact, such an intersection multiplicity is always less than or equal to the degree of $\mathcal{Z}$. This motivates the following statement.

Proposition 8.4 *Suppose that $\mathcal{C}$ is Frobenius non-classical for Σ_2. If a branch γ of $\mathcal{C}$ has order r, then there is a hyperplane in $\mathrm{PG}(5,\overline{\mathbf{F}}_q)$ which meets the corresponding branch of $\mathcal{Z}$ with multiplicity at least rp^{h-v}.*

Proof. Let (4.1) be a primitive representation of γ. Then, with the notation introduced in the proof of Proposition 3.1, we have that

$$X_0(t) = m_0(t), \ldots, X_5(t) = m_5(t) \tag{8.9}$$

is a representation of the corresponding branch γ^* of $\mathcal{Z}$. Since $\mathcal{C}$ is a birational model of $\mathcal{Z}$, this is a primitive branch representation of γ^*. Let H be the hyperplane with equation

$$X_0 + \alpha X_1 + \beta X_2 + \alpha^2 X_3 + \alpha\beta X_4 + \beta^2 X_5 = 0,$$

where $\alpha = a^{p^{h-v}}$ and $\beta = b^{p^{h-v}}$. Then the intersection multiplicity of H and γ^* is given by

$$\begin{aligned} I(H,\gamma^*) &= \operatorname{ord}\{m_0(\tau) + \alpha m_1(\tau) + \beta m_2(\tau) + \alpha^2 m_3(\tau) + \alpha\beta m_4(\tau) + \beta^2 m_5(\tau)\} \\ &= \nu \operatorname{ord}\{m_0(t) + \alpha m_1(t) + \beta m_2(t) + \alpha^2 m_3(t) + \alpha\beta m_4(t) + \beta^2 m_5(t)\} \end{aligned} \tag{8.10}$$

where ν is taken as 1 when (8.9) is primitive.

Now, put $\alpha_r = a_r^{p^{h-v}}$, $\beta_r = b_r^{p^{h-v}}$ in (4.1) noting that $a_r = m_{11}, b_r = m_{21}$; from (3.6), we obtain

$$\begin{aligned} &[m_0(t) + \alpha m_1(t) + \beta m_2(t) + \alpha^2 m_3(t) + \alpha\beta m_4(t) + \beta^2 m_5(t)] + \\ &\quad t^{rp^{h-v}}[\alpha_r m_1(t) + \beta_r m_2(t) + 2\alpha\alpha_r m_3(t) + (\alpha\beta_r + \beta\alpha_r) m_4(t) + \\ &\qquad 2\beta\beta_r m_5(t) + \ldots] = 0, \end{aligned}$$

whence $I(H,\gamma^*) \geq rp^{h-v}$, which proves the result. ∎

Proposition 8.5 *Suppose that $\mathcal{C}$ is Frobenius non-classical for Σ_2. If $\mathcal{C}$ is singular, then $\deg \mathcal{Z} \geq 2p^{h-v}$.*

Proof. Let $P = (a,b)$ be a singular point of $\mathcal{C}$ and let H be the hyperplane defined in the proof of Proposition 8.4. If P is the centre of only one branch of $\mathcal{C}$, it must have order greater than 1, and Proposition 8.5 follows from Proposition 8.4. Let us suppose that there exist two branches γ_1 and γ_2 of $\mathcal{C}$ both centred at P. The corresponding branches γ_1^* and γ_2^* of $\mathcal{Z}$ are distinct, and so $I(\mathcal{Z},H) \geq I(\gamma_1^*,H) + I(\gamma_2^*,H)$. By Proposition 8.4, $I(\mathcal{Z},H) \geq 2p^v$. ∎

Propositions 8.3 and 8.4 also imply an interesting result on the order of the branches of $\mathcal{C}$.

Proposition 8.6 *If $d < p^v$ and $\mathcal{C}$ is Frobenius non-classical for Σ_2, the order r of a branch of $\mathcal{C}$ satisfies the following bound:*

$$r \leq \{m + (2g-2) + [(q+1)d - 2M_q - M_q'] + 6d\}/q. \tag{8.11}$$

9 The proof of Proposition 1.2

In this section, assume that all of (h1), (h2), (h3), (h4), (h5), (h6) hold. The results obtained in §8 can be applied effectively. It is now possible to show that the order of a branch is at most two. This implies among other things that branches of type (4.9) do not exist, and in particular that $\mathcal{C}_0^{(2)}$ coincides with the osculating conic at γ. Using formulas proved in §§6,7, it will finally be shown that a curve which is Frobenius non-classical for Σ_2 and which satisfies the hypotheses of Theorem 1.3 necessarily has degree $\frac{1}{2}(\sqrt{q}+1)$.

We start with a first application of (8.7). Since $m \le d(d-1)$ and $2g-2 \le d(d-3)$, from (8.8) and (8.11) the following result is obtained.

Proposition 9.1 *Let $\mathcal{C}$ be Frobenius non-classical for Σ_2 and of degree $d < p^v$. If*

$$2M_q + M_q' \ge d(q - \sqrt{q} + 1), \tag{9.1}$$

then

$$\begin{aligned} p^v \deg \mathcal{Z} &\le d(2d + \sqrt{q} + 2), & (9.2)\\ r &\le d(2d + \sqrt{q} + 2)/q. & (9.3) \end{aligned}$$

Now, we investigate more closely the case that q is a square and

$$p^v = \sqrt{q}. \tag{9.4}$$

Since $d \le \sqrt{q} - 1$, we have that $d(2d + \sqrt{q} + 2)/q \le 3 - 3/\sqrt{q} < 3$. From (9.3) we immediately deduce the following. It should be noted that the linearity of the branches of type (4.8) depends on the condition that $p > 2$.

Proposition 9.2 *Let $\mathcal{C}$ be Frobenius non-classical for Σ_2 and of degree $d < \sqrt{q}$ and suppose that (9.1) and (9.4) hold. Then*

(i) *the branches of $\mathcal{C}$ of type (4.8) are linear, while those of type (4.7) and (4.9) have order $r \le 2$;*

(ii) *if $\mathcal{C}$ has a branch γ of type (4.9), there are only two cases*: (a) *$d = \sqrt{q} - 2$ and the order of γ is* 2, (b) *$d = \sqrt{q} - 1$ and the order of γ is* 1.

A first consequence of this result is the following.

Proposition 9.3 *Let τ_1 and τ_2 be the respective numbers of branches of $\mathcal{C}$ of type (4.8) and (4.9). Then*

$$3 \deg \mathcal{Z} = 2\tau_1 + \tau_2. \tag{9.5}$$

If $d < \sqrt{q} - 2$, then $3 \deg \mathcal{Z} = 2\tau_1$.

Proof. Since the order of a branch γ of $\mathcal{C}$ is, by the previous proposition, less than the characteristic p of the ground field, the classical formulas $v_P(R_2) = s + r - 3$ and $\operatorname{ord} X'(t) = r - 1$ hold. From the results established in §8, we also know the exact value of $\operatorname{ord} B_2(t)$:

$$\operatorname{ord} B_2(t) = \begin{cases} 0 & \text{if } \gamma \text{ is of type (4.7)},\\ s & \text{if } \gamma \text{ is of type (4.8)},\\ r & \text{if } \gamma \text{ is of type (4.9)}. \end{cases}$$

From Proposition 6.4,

$$\operatorname{ord}\|m(t)\| = \begin{cases} 0 & \text{if } \gamma \text{ is of type (4.7)},\\ 2 & \text{if } \gamma \text{ is of type (4.8)},\\ 1 & \text{if } \gamma \text{ is of type (4.9)}. \end{cases}$$

Hence, from (8.1), equation (9.5) follows. The second assertion is a consequence of (9.5) and Proposition 9.2(ii). ∎

Proposition 9.4 *Let $\mathcal{C}$ be Frobenius non-classical for Σ_2 and of degree $d < \sqrt{q}-2$. If (9.1) and (9.4) hold, then*

$$\deg \mathcal{Z} \leq 2d; \tag{9.6}$$
$$\deg \mathcal{Z} < 2(\sqrt{q}-2). \tag{9.7}$$

Proof. Since $d < \sqrt{q}-2$ it follows from Proposition 9.2 that $\mathcal{C}$ has no branches of type (4.9). Hence,

$$3v_P(S_1) - v_P(R_2) = \begin{cases} 6r & \text{if } \gamma \text{ is of type (4.7) centred at an } \mathbf{F}_q\text{-rational point},\\ 0 & \text{if } \gamma \text{ is of type (4.7) centred at a point not } \mathbf{F}_q\text{-rational},\\ \sqrt{q}+3r & \text{if } \gamma \text{ is of type (4.8) centred at an } \mathbf{F}_q\text{-rational point},\\ \sqrt{q} & \text{if } \gamma \text{ is of type (4.8) centred at a point not } \mathbf{F}_q\text{-rational}. \end{cases}$$

Since

$$\sum 3v_P(S_1) - v_P(R_2) = 3(2g-2) + 3(q+2)d - 3(2g-2) - 3d = 3dq + 3d,$$

it follows that $3dq+3d = 6M_q+3M'_q+\tau_1\sqrt{q}$, whence $2(dq-2M_q-M'_q+d) = \sqrt{q}\deg\mathcal{Z}$, by Proposition 9.3. Now, taking (9.1) into account, (9.6) follows. Since $d < \sqrt{q}-2$, the inequality (9.7) follows. ∎

Proposition 9.5 *Let $\mathcal{C}$ be Frobenius non-classical for Σ_2 and of degree $d < \sqrt{q}-2$. If (9.1) and (9.4) hold, then $\mathcal{C}$ is non-singular.*

Proof. Suppose that $\mathcal{C}$ has a singular point. Then, from $p^{h-v} = \sqrt{q}$ and Proposition 8.5, it follows that $\deg\mathcal{Z} \geq 2\sqrt{q}$; this contradicts (9.7). ∎

Proposition 9.6 *Let $\mathcal{C}$ be Frobenius non-classical for Σ_2 and of degree $d < \sqrt{q}-2$. If (9.1) and (9.4) hold, then $d = \frac{1}{2}(\sqrt{q}+1)$.*

Proof. Since $\mathcal{C}$ is non-singular and since its inflexions are exactly the points of type (4.8), from the formula $\sum v_P(R_2) = 3d(d-2)$, we immediately deduce that $\tau_1 = 6d(d-2)/(\sqrt{q}-3)$; hence, by Proposition 9.3, $\deg\mathcal{Z} = 4d(d-2)/(\sqrt{q}-3)$. On the other hand, from (9.6) we have $\deg\mathcal{Z} \leq 2d$. Hence, $d \leq \frac{1}{2}(\sqrt{q}+1)$. Since $\mathcal{C}$ is non-classical for Σ_2, the intersection number of $\mathcal{C}$ and the osculating conic at a point P is $\sqrt{q}$, which is at most $2d$ by Bézout's theorem. Hence $d = \frac{1}{2}(\sqrt{q}+1)$. ∎

Proposition 9.7 *Let $\mathcal{C}$ be of degree $d = \frac{1}{2}(\sqrt{q}+1)$ and Frobenius non-classical for Σ_2, satisfying (9.1) and (9.4). Then equality holds in (9.1) and the number N_1 of $\mathbf{F}_q$-rational points of $\mathcal{C}$ satisfies*

$$N_1 = q + 1 + (d-1)(d-2)\sqrt{q};$$

that is, $\mathcal{C}$ is maximal.

Proof. We show that the points of inflexion of $\mathcal{C}$ are $\mathbf{F}_q$-rational. If this were not the case, $\mathcal{C}$ would have a point $P = (a, b)$ not $\mathbf{F}_q$-rational of type (4.8). By Proposition 5.4, the tangent ℓ to $\mathcal{C}$ at P would also pass through the point $P' = (a^q, b^q)$, and the the intersection ℓ with $\mathcal{C}$ would have cardinality at least $\frac{1}{2}(\sqrt{q}+1)+1$, which is impossible as $\mathcal{C}$ is an absolutely irreducible curve of degree $\frac{1}{2}(\sqrt{q}+1)$. Therefore, $\tau_1 = M'_q$. From §7 or [23, Proposition 2.4 (a)], it follows that

$$v_P(S_1) = \begin{cases} 0 & \text{if } P \text{ is a point which is not } \mathbf{F}_q\text{-rational,} \\ 2 & \text{if } P \text{ is a regular } \mathbf{F}_q\text{-rational point,} \\ \frac{1}{2}(\sqrt{q}+1) & \text{if } P \text{ is an } \mathbf{F}_q\text{-rational inflexion.} \end{cases}$$

From (7.1), it follows that $2M_q + \frac{1}{2}(\sqrt{q}+1)\tau_1 = d(d-3) + (q+2)d$. Since by (9.5), $\deg \mathcal{Z} = 2d$, we have $M'_q = 3d$. Hence, $M_q = \frac{1}{4}(\sqrt{q}+1)(q-\sqrt{q}-2)$; so there is equality in (9.1). The number N_1 of $\mathbf{F}_q$-rational points of $\mathcal{C}$ is given by $M_q + \frac{3}{2}(\sqrt{q}+1)$, which equals $q+1+\frac{1}{4}(\sqrt{q}-1)(\sqrt{q}-3)\sqrt{q}$, as required. ∎

Remark 9.8 For $d = \frac{1}{2}(\sqrt{q}+1)$, the Fermat curve $\mathcal{F}_d$ with equation $x^d + y^d + 1 = 0$ regarded as a curve over $\mathbf{F}_q$ with q an odd square has order sequence $(0, 1, 2, 3, 4, \sqrt{q})$ and is also Frobenius non-classical for Σ_2; see [8, p.354]. Both M_q and M'_q have the same value as in the final part of the previous proof. Hence $\mathcal{F}_d$ attains equality in (9.1).

The proof of Proposition 1.2 is now complete, and hence also the proofs of Theorems 1.3 and 1.4.

10 Comparison with previous results

The asymmetrical form of Theorem 1.4 does not allow a direct comparison with the Hasse-Weil and Stöhr-Voloch theorems. However, a comparison may be made in as follows.

I. *Let $\mathcal{C}$ be classical with respect to lines.*

Proposition 10.1 *For $\sqrt{q}-2 > d \geq \frac{1}{2}\sqrt{q}+6$, Theorem 1.4 is better than the bound (1.3).*

Proof. In this case, the number of inflexions is $M'_q \leq 3d(d-2)$. Hence, from Theorem 1.4, the number of rational points on $\mathcal{C}$ is

$$N_1 = M_q + M'_q \leq \tfrac{1}{2}d[(q - \sqrt{q} + 1) + 3(d-2)]. \tag{10.1}$$

The right-hand side of (10.1) is seen to be less than $q+1+(d-1)(d-2)\sqrt{q}$ for $d \geq \frac{1}{2}\sqrt{q}+6$, after some routine manipulations. ∎

Proposition 10.2 *For $M'_q \le d(d+\sqrt{q}-2)$, Theorem 1.4 is better than the Stöhr-Voloch bound.*

Proof. From Theorem 1.4,

$$2N_1 = 2(M_q + M'_q) \le M'_q + d(q - \sqrt{q} + 1). \tag{10.2}$$

The right-hand side of (10.2) less than or equal to $d(d-3) + (q+2)d$ under the given condition. ∎

Remark. If the number M'_q of inflexion points satisfies $M'_q \le 2d(d+1)$, then the proposition is applicable. So, roughly speaking, if the number of inflexions is of the order of $2d^2$ rather than the maximum of order $3d^2$, we have an improvement.

Comparing Theorem 1.4 with the Stöhr-Voloch theorem in the case that $n = 5$ gives a result similar to Proposition 10.1.

II. *$\mathcal{C}$ is non-classical and Frobenius classical for Σ_1.*

In this case, a generic point is an inflexion point. This means that the Hessian is indeterminate and it is no longer true that $M'_q \le 3d(d-2)$. To evaluate M'_q we can instead use Theorem 2.1 in the case that $n = 2$. It then makes no sense to compare Theorem 1.1 with the Stöhr-Voloch theorem. A comparison with the bound (1.3) is still worthwhile.

In a forthcoming paper [14], it is shown that, if $d < \sqrt{q}$, a non-classical curve is always Frobenius classical. Then result (h) in §2 gives

$$M'_q \le \tfrac{1}{2}[2g - 2 + (q+2)d] \le \tfrac{1}{2}d(q+d-1).$$

Hence,

$$2N_1 \le 2(M_q + M'_q) \le d(q - \sqrt{q} + 1) + \tfrac{1}{2}d(q+d-1),$$

whence

$$N_1 \le \tfrac{1}{2}d(\tfrac{3}{2}q - \sqrt{q} + \tfrac{1}{2}d - \tfrac{1}{2}).$$

Proposition 10.3 *If $\sqrt{q} \ge d \ge \frac{3}{4}\sqrt{q}+2$, then Theorem 1.1 is better than the bound (1.3).*

11 Some applications

Algebraic curves are important tools in finite geometry for solving problems on arcs and special point sets in general; these problems are often intractable by other means. It should be noted that the algebraic curves which appear in such contexts are not necessarily irreducible. So, it is of interest to extend Theorem 1.3 to reducible curves.

Let the curve $\mathcal{C}$ of degree d have absolutely irreducible components $\mathcal{D}_i$ of degree d_i, with numbers $M_q^{(i)}$, $M_q^{(i)'}$ of branches as in Theorem 1.3 and defined in §8. So, for $\mathcal{C}$ define

$$M_q = \sum_i M_q^{(i)}, \qquad M'_q = \sum_i M_q^{(i)'}.$$

Theorem 11.1 *Let $\mathcal{C}$ be a plane algebraic curve of degree d defined over $\mathbf{F}_q$, $q = p^h$. Suppose also that p, q, d satisfy the numerical conditions of Theorem 1.3. If $\mathcal{C}$ has neither a linear nor a quadratic component,*

$$2M_q + M_q' \leq d(q - \sqrt{q} + 1),$$

with equality if and only $d = \frac{1}{2}(\sqrt{q} + 1)$.

Proof. If $\mathcal{D}_i$ is not rational, then, arguing as in [11, Theorem 10.1.1], $\sum r^2 \leq d_i^2$ summed over the branches of $\mathcal{D}_i$ centred at an $\mathbf{F}_q$-rational point; hence

$$2M_q^{(i)} + M_q^{(i)\prime} \leq 2\sum r^2 \leq 2d_i^2 \leq 2d_i(\sqrt{q} - 2) < d_i(q - \sqrt{q} + 1).$$

For a rational component $\mathcal{D}_i$, Theorem 1.3 implies that

$$2M_q^{(i)} + M_q^{(i)\prime} \leq d_i(q - \sqrt{q} + 1).$$

Hence

$$\sum \left(2M_q^{(i)} + M_q^{(i)\prime}\right) \leq d(q - \sqrt{q} + 1),$$

which gives the result. ∎

We now discuss an application of Theorem 1.3. This will improve the previous best estimate in a long-standing question in finite geometry.

A *k-arc* $\mathcal{K}$ in $\mathrm{PG}(2, q)$, $q = p^r$ and p prime, is a set of k points no three of which are collinear. An arc is *complete* if it is maximal with respect to inclusion. A k-arc corresponds to a $[k, 3, k-2]$ *maximum distance separable* (MDS) code of length k, dimension 3 and minimum distance $k-2$; a complete arc corresponds to an MDS code that cannot be extended to another MDS code of greater length. The maximum size of an arc is denoted by $m(2, q)$ and the size of the second largest complete arc is denoted by $m'(2, q)$. Bose, in 1938, showed that $m(2, q) = q + 1$ when q is odd and $q + 2$ when q is even. In 1955 Segre [11, Theorem 8.14], showed that for q odd a $(q+1)$-arc is the set of rational points of an irreducible conic in $\mathrm{PG}(2, q)$. The problem of determining $m'(2, q)$ for q odd is still unsolved and seems to be difficult. Apart from small q, that is $q \leq 29$, the only case settled is for q an even square. Here the result is that $m'(2, q) = q - \sqrt{q} + 1$. It is conjectured that this result is also true for q an odd square. The connection with curves is via the following fundamental theorem of Segre connecting a k-arc $\mathcal{K}$ with an algebraic curve, [11, Theorems 10.1, 10.4].

Theorem 11.2 (i) *The $kt = k(q + 2 - k)$ tangents through the points of $\mathcal{K}$ lie on an algebraic envelope Γ' whose dual curve is of degree t or $2t$ according as q is even or odd.*
(ii) *The envelope Γ' contains no bisecant of $\mathcal{K}$ and so no pencil with vertex P in $\mathcal{K}$.*
(iii) *For q odd, the t tangents to $\mathcal{K}$ through a point P of $\mathcal{K}$ each count twice in the intersection of Γ' with the pencil $\mathcal{L}_P$ of lines through P.*
(iv) *For q odd, Γ' may contain components of multiplicity two, but does not consist entirely of double components.*
(v) *The arc $\mathcal{K}$ is incomplete if and only if Γ' has a rational linear component.*

For q a square, odd or even with $q > 4$, a complete $(q - \sqrt{q} + 1)$-arc was constructed as any orbit of the cyclic group $\langle T^{q+\sqrt{q}+1} \rangle$, where T is a projectivity acting on the points of $\mathrm{PG}(2, q)$ as a single cycle of length $q^2 + q + 1$. In this case, for q even, the curve Γ dual to Γ' has degree $\sqrt{q}+1$ and is Hermitian, [3, 15]. For q odd, the curve Γ has degree $2(\sqrt{q}+1)$ and it is shown in [1] that Γ has the following properties: (i) Γ is classical for Σ_1; (ii) Γ is non-classical for Σ_2; (iii) Γ is Frobenius non-classical; (iv) the genus of Γ is $\frac{1}{2}\sqrt{q}(\sqrt{q} - 1)$. By the theorem of [19], Γ is birationally isomorphic to a Hermitian curve.

The investigation of Γ in the more general case of an arbitrary k-arc led in [13] to the conclusion that, if $p \geq 5$, then $m'(2, q) \leq q - \frac{1}{2}\sqrt{q} + 5$. For q sufficiently large, our main theorem gives an improvement of this bound.

Theorem 11.3 *Let $q = p^h$ with $p \geq 3$, and let $q = 3^{2e}$ when $p = 3$. If $q \geq 23^2$ and $q \neq 3^6$ or 5^5, then*

$$m'(2, q) \leq q - \tfrac{1}{2}\sqrt{q} + \tfrac{5}{2}.$$

Also,

$$m'(2, q) \leq \begin{cases} q - 22 & \text{when } q = 5^5, \\ q - 9 & \text{when } q = 3^6, \\ q - 9 & \text{when } q = 23^2, \\ q - 5 & \text{when } q = 19^2. \end{cases}$$

Proof. An essential tool for the proof is Theorem 11.2. Let $\mathcal{K}$ be a complete k-arc in $\mathrm{PG}(2, q)$ and let $\mathcal{C}$ be the curve of degree $d = 2t$, with $t = q+2-k$, that corresponds to Γ' in the dual plane. By Segre's theorem, $\mathcal{C}$ does not have a linear component and if it has a component of degree two, then $\mathcal{K}$ is the set of rational points of a conic. So, assume that each component of $\mathcal{C}$ has degree at least three. Then from part (iii) of Segre's theorem the line ℓ corresponding to the point Q meets $\mathcal{C}$ in $\mathbf{F}_q$-rational points, in number t, and the intersection multiplicity $I_P(\ell, \mathcal{C})$ of ℓ and $\mathcal{C}$ at a common point P is still 2. If P is a simple point of $\mathcal{C}$, then P is a regular point of order 1. If P is a singular point of $\mathcal{C}$, then it is a double point; so P is the centre of either one branch of order 2 or of two branches of order 1. Thus P counts at least twice in $2M_q + M'_q$. Since $\mathcal{C}$ has kt such $\mathbf{F}_q$-rational points, we obtain $2M_q + M'_q \geq 2kt$.

Assume now that $\mathcal{K}$ is an arc with more than $q - \frac{1}{2}\sqrt{q} + 3$ points. Then $d = 2t = 2q - 2k + 4 \leq \sqrt{q} - 3$. Hence, by Theorem 11.1, $2M_q + M'_q \leq 2t(q - \sqrt{q} + 1)$ provided that the hypotheses are satisfied. This yields that $2kt \leq 2t(q - \sqrt{q} + 1)$ and hence $k \leq q - \sqrt{q} + 1$, contradicting that $k > q - \frac{1}{2}\sqrt{q} + 3$. Hence $k \leq q - \frac{1}{2}\sqrt{q} + 3$ and, since q is odd, in the relevant case in which q is a square, the 3 can be lowered to $\frac{5}{2}$.

A similar argument proves the second part of the theorem. ∎

Remark 11.4 The best result for the case $q = 3^{2e+1}$ is $m'(2, q) \leq q - \frac{\sqrt{3}}{4}\sqrt{q} + \frac{103}{16}$; see [25] and [11, Theorem 10.31].

Acknowledgements This research was carried out while the first author was visiting the Università della Basilicata with a grant from the Consiglio Nazionale delle Ricerche and while the second author was visiting the University of Sussex under the Royal Society-Accademia Nazionale dei Lincei exchange scheme.

The authors are also extremely grateful to the referee for an extremely thorough, lengthy and detailed report, which has led to considerable improvements in the paper.

References

[1] A. Cossidente and G. Korchmáros, The algebraic envelope associated to a complete arc, "Recenti Progressi in Geometria," *Rend. Circ. Mat. Palermo Suppl.* **51** (1998), 9–24.

[2] A. Cossidente, J.W.P. Hirschfeld, G. Korchmáros and F. Torres, On plane maximal curves, submitted.

[3] J. C. Fisher, J. W. P. Hirschfeld and J. A. Thas, Complete arcs in planes of square order, *Combinatorics '84*, Ann. Discrete Math. **30**, North Holland, 1986, pp. 243–250.

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

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

[6] A. Garcia and M. Homma, Frobenius order-sequences of curves, "Algebra and Number Theory" (Eds. G. Frey; J. Ritter), Walter de Gruyter Co., Berlin, 1994.

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

[8] A. Garcia and J. F. Voloch, Fermat curves over finite fields, *J. Number Theory* **30** (1988), 345–356.

[9] H. Hasse and F.K. Schmidt, Noch eine Begründung der Theorie der höheren Differentialquotienten in einem algebraischen Funktionenkörper einer Unbestimmten, *J. Reine Angew. Math.* **177** (1937), 215–237.

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

[11] J. W. P. Hirschfeld, "Projective Geometries Over Finite Fields," Second edition, Oxford University Press, Oxford, 1998.

[12] J. W. P. Hirschfeld, "Finite Projective Spaces Of Three Dimensions," Oxford University Press, Oxford, 1985.

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

[14] J. W. P. Hirschfeld and G. Korchmáros, Frobenius non-classical curves of low degree, in preparation.

[15] J. W. P. Hirschfeld, L. Storme, J. A. Thas, and J. F. Voloch, A characterization of Hermitian curves, *J. Geom.* **41** (1991), 72–78.

[16] J. W. P. Hirschfeld and J. A. Thas, "General Galois Geometries," Oxford University Press, Oxford, 1991.

[17] D. B. Leep and C. C. Yeomans, The number of points on a singular curve over a finite field, *Arch. Math.* **63** (1994), 420–426.

[18] R. Lidl and H. Niederreiter, "Finite Fields," Addison-Wesley, Reading, Mass., 1983 (Cambridge University Press, Cambridge, 1989).

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

[20] B. Segre, Introduction to Galois geometries, *Atti Accad. Naz. Lincei Mem.* **8**, 1967, 133–236.

[21] A. Seidenberg, "Elements of the Theory of Algebraic Curves," Addison Wesley, Reading, Mass., 1969.

[22] H. Stichtenoth, "Algebraic Function Fields and Codes," Springer-Verlag, Berlin, 1993.

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

[24] J. F. Voloch, Arcs in projective planes over prime fields. *J. Geom.* **38** (1990), 198–200.

[25] J. F. Voloch, Complete arcs in Galois planes of non-square order, *in* "Advances in Finite Geometries and Designs," J. W. P. Hirschfeld et al.(eds.), Isle of Thorns 1990, Oxford University Press, Oxford, 1991, pp. 401–405.

[26] R. J. Walker, "Algebraic Curves," Princeton University Press, Princeton, 1950 (Dover, New York, 1962).

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

J. W. P. Hirschfeld
School of Mathematical Sciences
University of Sussex
Brighton BN1 9QH
United Kingdom
jwph@sussex.ac.uk

G. Korchmáros
Dipartimento di Matematica
Università della Basilicata
85100 Potenza
Italy
korchmaros@unibas.it