ACTA ARITHMETICA
167.1 (2015)

Frobenius nonclassicality with respect to linear systems of curves of arbitrary degree

by

NAZAR ARAKELIAN (Campinas) and HERIVELTO BORGES (São Carlos)

1. Introduction. Let p be a prime integer and $\mathbb{F}_q$ be a finite field with $q = p^h$ elements. The problem of estimating the number of rational points on curves over $\mathbb{F}_q$ has been extensively investigated in view of its broad relevance and applications, e.g., in finite geometry, number theory, coding theory, etc. (see [10], [8], [13, Chapter 6] and [16, Chapters 2 and 8]).

Let $\mathcal{X}$ be a projective, nonsingular, geometrically irreducible curve of genus g defined over $\mathbb{F}_q$, and let $N_q(\mathcal{X})$ be its number of $\mathbb{F}_q$-rational points. The most remarkable result regarding $N_q(\mathcal{X})$ is the Hasse–Weil bound, which states that

$$|N_q(\mathcal{X}) - (q+1)| \le 2g\sqrt{q}. \tag{1.1}$$

In 1986, Stöhr and Voloch [17] introduced a technique to estimate $N_q(\mathcal{X})$, which is dependent on the morphisms $\phi : \mathcal{X} \to \mathbb{P}^n$. In many instances, their results improve the Hasse–Weil bound ([17], [6]).

In this paper, we consider a family of curves $\mathcal{X}$ and focus on aspects relevant to the application of Stöhr–Voloch theory, addressing the Frobenius (non)classicality of $\mathcal{X}$ with respect to linear systems of curves of degree $s \ge 1$.

Let $F(x, y, z) \in \mathbb{F}_q[x, y, z]$ be a homogeneous polynomial such that

$$\mathcal{X} : F(x, y, z) = 0$$

is a nonsingular projective plane curve of degree d and genus g. Associated with the linear system of all plane curves of degree $s \in \{1, \dots, d-1\}$, the curve $\mathcal{X}$ has a linear series $\mathcal{D}_s$ of dimension $M = \binom{s+2}{2} - 1$ and degree sd [11, Section 7.7]. Applying Stöhr–Voloch's theorem [17, Theorem 2.13]

2010 *Mathematics Subject Classification*: Primary 11G20, 14H05; Secondary 14Hxx.
Key words and phrases: Stöhr–Voloch theory, Frobenius nonclassical curves, finite fields.

DOI: 10.4064/aa167-1-3

to $\mathcal{D}_s$ yields

$$N_q(\mathcal{X}) \leq \frac{d(d-3)(\nu_1 + \cdots + \nu_{M-1}) + sd(q+M)}{M}, \tag{1.2}$$

where $(\nu_0, \ldots, \nu_{M-1})$ is the $\mathbb{F}_q$-Frobenius order sequence of $\mathcal{X}$ with respect to $\mathcal{D}_s$. The curve $\mathcal{X}$ is called $\mathbb{F}_q$-*Frobenius classical* with respect to $\mathcal{D}_s$ if $\nu_i = i$ for all $i = 0, \ldots, M-1$. Note that for such a curve, the bound (1.2) reads

$$N_q(\mathcal{X}) \leq \frac{d(d-3)(M-1)}{2} + \frac{sd(q+M)}{M}. \tag{1.3}$$

The bound (1.3) improves the Hasse–Weil bound in several cases ([17, Section 3], [6]).

If $\nu_i \neq i$ for some i, then $\mathcal{X}$ is called $\mathbb{F}_q$-*Frobenius nonclassical* with respect to $\mathcal{D}_s$. Note that for this case, we have

$$\nu_1 + \cdots + \nu_{M-1} > M(M-1)/2.$$

Thus (1.2) indicates that Frobenius nonclassical curves are likely to have many rational points. Therefore, if we can identify the Frobenius nonclassical curves with respect to $\mathcal{D}_s$, we are left with the remaining curves for which a better upper bound, given by (1.3), holds. At the same time, the set of Frobenius nonclassical curves provides a potential source of curves with many points. Therefore, in light of (1.2), characterizing Frobenius nonclassical curves may offer a two-fold benefit.

In general, the effectiveness of (1.3) will vary according to the value of $s \in \{1, \ldots, d-1\}$. For instance, if $s = 1$ or $s = 2$, the bound (1.3) reads

$$N_q(\mathcal{X}) \leq \frac{d(d+q-1)}{2}, \tag{1.4}$$

$$N_q(\mathcal{X}) \leq \frac{2d(5d+q-10)}{5}, \tag{1.5}$$

respectively. Note that the bound (1.5) is better than (1.4) when, roughly, $d < q/15$. More generally, if $r \geq 1$, then (1.3) for $s = r+1$ is better than the corresponding bound for $s = r$ when, roughly,

$$d < \left(\frac{4}{(r+2)(r+3)(r+4)}\right) q. \tag{1.6}$$

These facts can be interpreted as follows. If we want to find plane curves of degree $d < q/15$ attaining the bound (1.4), we must look for plane curves that are $\mathbb{F}_q$-Frobenius nonclassical with respect to $\mathcal{D}_2$. Similarly, plane curves of degree $d < q/30$ attaining the bound (1.5) must be $\mathbb{F}_q$-Frobenius nonclassical with respect to $\mathcal{D}_3$, and so on. An explicit example of this phenomenon is given in Section 3. This also highlights the importance of Frobenius nonclassical curves for the construction of curves with many points.

Frobenius (non)classicality in the case $s = 1$ has been widely investigated with many examples cited in the literature ([2], [5], [6], [9]). Even for this case, however, a complete characterization of $\mathbb{F}_q$-Frobenius nonclassical curves is lacking. As observed by Hefez and Voloch [9], characterizing all such curves seems quite a complex problem.

In 1988, Garcia and Voloch [6] established necessary and sufficient conditions for a Fermat curve, i.e., a curve given by an equation of the type $ax^d + by^d = z^d$, $a, b \in \mathbb{F}_q$, $ab \neq 0$, to be $\mathbb{F}_q$-Frobenius nonclassical in the cases $s = 1$ and $s = 2$. It seems that, excluding the Fermat curves, not many $\mathbb{F}_q$-Frobenius nonclassical curves with respect to the linear system of conics are characterized.

In this paper, we study the $\mathbb{F}_q$-Frobenius (non)classicality of a generalization of the Fermat curve. More specifically, we study the smooth projective plane curves $\mathcal{X}$ of degree $d = sn$, defined over $\mathbb{F}_q$, and given by the equation $F(x, y, z) = 0$, where

$$F(x,y,z) = \sum_{i+j+t=s} c_{ij} x^{in} y^{jn} z^{tn}, \tag{1.7}$$

with $s \geq 1$ and $n \geq 2$.

The paper proceeds as follows. In Section 2, we set some notation and recall the main results of Stöhr–Voloch theory, which constitute the basis for this study. In Section 3, we provide criteria for the curves arising from (1.7) to be $\mathbb{F}_q$-Frobenius nonclassical with respect to the linear series $\mathcal{D}_s$. Then we take advantage of these criteria to construct new curves of degree $d < q/15$ attaining the Stöhr–Voloch bound (1.4). In Section 4, we fully characterize the $\mathbb{F}_q$-Frobenius nonclassical curves arising from (1.7) in the case $s = 2$. In Section 5, we determine the exact value of $N_q(\mathcal{X})$ when $\mathcal{X}$ is an $\mathbb{F}_q$-Frobenius nonclassical curve and, via Stöhr–Voloch theory, arrive at a nice upper bound for the number of $\mathbb{F}_q$-rational points on the remaining curves.

The paper's appendix provides facts about the irreducibility of some plane quartics. The results listed there are useful in certain proofs of Section 4.

Notation.

- $\mathbb{F}_q$ is the finite field with $q = p^h$ elements, with $h \geq 1$, for a prime integer p.
- $\mathbb{K}$ is the algebraic closure of $\mathbb{F}_q$.
- Given an irreducible curve $\mathcal{X}$ over $\mathbb{F}_q$ and an algebraic extension $\mathbb{H}$ of $\mathbb{F}_q$, the function field of $\mathcal{X}$ over $\mathbb{H}$ is denoted by $\mathbb{H}(\mathcal{X})$.
- For a curve $\mathcal{X}$ and $r > 0$, the set of its $\mathbb{F}_{q^r}$-rational points is denoted by $\mathcal{X}(\mathbb{F}_{q^r})$.

- $N_{q^r}(\mathcal{X})$ is the number of $\mathbb{F}_{q^r}$-rational points of the curve $\mathcal{X}$.
- For a nonsingular point $P \in \mathcal{X}$, the discrete valuation at P is denoted by v_P.
- For two plane curves $\mathcal{X}$ and $\mathcal{Y}$, the intersection multiplicity of $\mathcal{X}$ and $\mathcal{Y}$ at the point P is denoted by $I(P, \mathcal{X} \cap \mathcal{Y})$.
- Given $g \in \mathbb{K}(\mathcal{X})$, t a separating variable of $\mathbb{K}(\mathcal{X})$ and $r \geq 0$, the rth Hasse derivative of g with respect to t is denoted by $D_t^{(r)} g$.

2. Preliminaries. In this section, we recall results from [17]. Let $\mathcal{X}$ be a projective, irreducible, nonsingular curve of genus g defined over $\mathbb{F}_q$. Associated to a nondegenerated morphism $\phi = (f_0 : \ldots : f_n) : \mathcal{X} \to \mathbb{P}^n(\mathbb{K})$, there exists a base-point-free linear series given by

$$\mathcal{D}_\phi = \Big\{ \operatorname{div}\Big(\sum_{i=0}^{n} a_i f_i \Big) + E \;\Big|\; a_0, \ldots, a_n \in \mathbb{K} \Big\},$$

with $E := \sum_{P \in \mathcal{X}} e_P P$ and $e_P = -\min\{v_P(f_0), \ldots, v_P(f_n)\}$. Given a point $P \in \mathcal{X}$, there exists a sequence of nonnegative integers $(j_0(P), \ldots, j_n(P))$, such that $j_0(P) < \cdots < j_n(P)$, called the *order sequence* of P with respect to ϕ, which is defined by the numbers $j \geq 0$ such that $v_P(D) = j$ for some $D \in \mathcal{D}_\phi$. Except for a finite number of points of $\mathcal{X}$, the order sequence is the same, and is denoted by $(\epsilon_0, \ldots, \epsilon_n)$. This sequence can also be defined by the minimal sequence, with respect to the lexicographic order, for which

$$\det (D_t^{(\epsilon_i)} f_j)_{0 \leq i,j \leq n} \neq 0,$$

where t is a separating variable of $\mathbb{K}(\mathcal{X})$. Moreover, for each $P \in \mathcal{X}$,

$$\epsilon_i \leq j_i(P) \quad \text{for all } i \in \{0, \ldots, n\}. \tag{2.1}$$

The curve $\mathcal{X}$ is called *classical* with respect to ϕ (or $\mathcal{D}_\phi$) if the sequence $(\epsilon_0, \ldots, \epsilon_n)$ is $(0, \ldots, n)$. Otherwise, it is is called *nonclassical.*

Let $\mathbb{K}(\mathcal{X})$ be the function field of $\mathcal{X}$ and define the subfield

$$(\mathbb{K}(\mathcal{X}))_r = \{u^{p^r} \mid u \in \mathbb{K}(\mathcal{X})\}.$$

In [7, Theorem 1] the following criterion is proved, which is useful in determining whether $\mathcal{X}$ is classical with respect to the given morphism.

THEOREM 2.1. *Let $\phi = (f_0 : \ldots : f_n) : \mathcal{X} \to \mathbb{P}^n(\mathbb{K})$ be a morphism. Then $f_0, \ldots, f_n$ are linearly independent over $(\mathbb{K}(\mathcal{X}))_r$ if and only if there exist integers $\epsilon_0, \ldots, \epsilon_n$ with*

$$0 = \epsilon_0 < \cdots < \epsilon_n < p^r$$

such that $\det (D_t^{(\epsilon_i)} f_j)_{0 \leq i,j \leq n} \neq 0$.

Proposition 1.7 in [17] establishes the following.

PROPOSITION 2.2. *Let $P \in \mathcal{X}$ with order sequence $(j_0(P), \dots, j_n(P))$. If the integer*

$$\prod_{i>r} \frac{j_i(P) - j_r(P)}{i - r}$$

is not divisible by p, then $\mathcal{X}$ is classical with respect to $\mathcal{D}_\phi$.

Now suppose that ϕ is defined over $\mathbb{F}_q$. The sequence of nonnegative integers $(\nu_0, \dots, \nu_{n-1})$, chosen minimally in the lexicographic order, such that

$$\begin{vmatrix} f_0^q & \cdots & f_n^q \\ D_t^{(\nu_0)} f_0 & \cdots & D_t^{(\nu_0)} f_n \\ \vdots & \cdots & \vdots \\ D_t^{(\nu_{n-1})} f_0 & \cdots & D_t^{(\nu_{n-1})} f_n \end{vmatrix} \neq 0, \tag{2.2}$$

where t is a separating variable of $\mathbb{F}_q(\mathcal{X})$, is called the $\mathbb{F}_q$-*Frobenius sequence* of $\mathcal{X}$ with respect to ϕ. From [17, Proposition 2.1], we find that $\{\nu_0, \dots, \nu_{n-1}\} = \{\epsilon_0, \dots, \epsilon_n\} \backslash \{\epsilon_I\}$ for some $I \in \{1, \dots, n\}$. If $(\nu_0, \dots, \nu_{n-1}) = (0, \dots, n-1)$, then the curve $\mathcal{X}$ is called $\mathbb{F}_q$-*Frobenius classical* with respect to ϕ. Otherwise, it is called $\mathbb{F}_q$-*Frobenius nonclassical.*

The following result [11, Remark 8.52] shows the close relation between classicality and $\mathbb{F}_q$-Frobenius classicality.

PROPOSITION 2.3. *Let $\mathcal{D}$ be a linear series of the curve $\mathcal{X}$, defined over $\mathbb{F}_q$, such that $p > M := \dim \mathcal{D}$. If $\mathcal{X}$ is $\mathbb{F}_q$-Frobenius nonclassical with respect to $\mathcal{D}$, then $\mathcal{X}$ is nonclassical with respect to $\mathcal{D}$.*

If $\mathcal{X} \subseteq \mathbb{P}^n(\mathbb{K})$, the $\mathbb{F}_q$-*Frobenius map* Φ_q is defined on $\mathcal{X}$ by

$$\Phi_q : \mathcal{X} \to \mathcal{X}, \quad (a_0 : \dots : a_n) \mapsto (a_0^q : \dots : a_n^q).$$

Note that if $\mathcal{X}$ is a plane curve, then by (2.2) and [17, Corollary 1.3], $\mathcal{X}$ is $\mathbb{F}_q$-Frobenius nonclassical with respect to the linear system of lines if and only if $\Phi_q(P)$ lies on the tangent line of $\mathcal{X}$ at P for all $P \in \mathcal{X}$.

Now let $F(x, y, z) \in \mathbb{F}_q[x, y, z]$ be a homogeneous, irreducible polynomial of degree d such that

$$\mathcal{X} : F(x, y, z) = 0$$

is a nonsingular projective plane curve. The function field $\mathbb{K}(\mathcal{X})$ is given by $\mathbb{K}(x, y)$, where x and y satisfy $F(x, y, 1) = 0$. For each $s \in \{1, \dots, d-1\}$, consider the *Veronese morphism*

$$\phi_s = (1 : x : y : x^2 : \dots : x^i y^j : \dots : y^s) : \mathcal{X} \to \mathbb{P}^M(\mathbb{K}),$$

where $i + j \leq s$. It is well known that the linear series $\mathcal{D}_s$ associated with ϕ_s is base-point-free of degree sd and dimension $M = \binom{s+2}{2} - 1 = (s^2 + 3s)/2$.

The linear series $\mathcal{D}_s$ is also obtained by the cut out on $\mathcal{X}$ by the linear system of plane curves of degree s.

For any $P \in \mathcal{X}$, a $(\mathcal{D}_s, P)$-order $j := j(P)$ can be seen as the intersection multiplicity at P of $\mathcal{X}$ with some plane curve of degree s. That is, the integers $j_0(P) < \cdots < j_M(P)$ represent the possible intersection multiplicities of a plane curve of degree s with $\mathcal{X}$ at P. Moreover, by [17, Theorem 1.1], there is a unique curve $\mathcal{H}_P^s$ of degree s, called the *s-osculating curve* to $\mathcal{X}$ at P, such that

$$I(P, \mathcal{X} \cap \mathcal{H}_P^s) = j_M(P).$$

3. $\mathbb{F}_q$-Frobenius nonclassical curves. Let us recall that $\mathcal{X} : F(x, y, z) = 0$ is a smooth, projective plane curve of degree sn, defined over $\mathbb{F}_q$, where F is given by

$$F(x, y, z) = \sum_{i+j+t=s} c_{ij} x^{in} y^{jn} z^{tn}, \tag{3.1}$$

with $s \geq 1$ and $n \geq 2$. This section establishes sufficient conditions for $\mathcal{X}$ to be $\mathbb{F}_q$-Frobenius nonclassical with respect to $\mathcal{D}_s$. Note that the case $s = 1$ addresses the $\mathbb{F}_q$-Frobenius nonclassicality, with respect to lines, of Fermat curves

$$\mathcal{X} : ax^n + by^n + cz^n = 0. \tag{3.2}$$

However, for $p \neq 2$, it is a well-known result by Garcia and Voloch [6, Theorem 2] that the curve (3.2) is $\mathbb{F}_q$-Frobenius nonclassical, with respect to lines, if and only if $n = \frac{p^h-1}{p^v-1}$, and the curve is defined over $\mathbb{F}_{p^v}$, where $q = p^h$, $v > h$ and $v \mid h$. For an alternative proof including the case $p = 2$, see [1].

Henceforth, we consider a smooth curve $\mathcal{X}$ associated to (3.1) with the following assumptions:

(3.i) $s \geq 2$.
(3.ii) $p \mid n - 1$.
(3.iii) $p > 5$ for $s = 2$, and $p > s^2$ for $s \geq 3$ (in particular, $p > M := \dim \mathcal{D}_s$).

The following result will be a key ingredient in our approach. It is proved in [14, Lemma 1.3.8] and [12, Lemma A.2] for curves in characteristic $p = 0$ and $p \geq 0$, respectively.

LEMMA 3.1. *Let $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ be plane curves. If $\mathcal{F}$ is nonsingular, then*

$$I(P, \mathcal{H} \cap \mathcal{G}) \geq \min\{I(P, \mathcal{F} \cap \mathcal{G}), I(P, \mathcal{F} \cap \mathcal{H})\}$$

for all $P \in \mathcal{F}$.

LEMMA 3.2. *For all points $P = (a : b : c) \in \mathcal{X}$ such that $abc \neq 0$, the s-osculating curve $\mathcal{H}_P^s$ to $\mathcal{X}$ at P is an irreducible curve given by the equation $H_P(x, y, z) = 0$, where*

$$H_P(x,y,z) = \sum_{i+j+t=s} c_{ij}(a^{im}b^{jm}c^{tm})^{p^v} x^i y^j z^t, \tag{3.3}$$

$n = mp^v + 1$ and $\gcd(p, m) = 1$. Furthermore, $\mathcal{X}$ is nonclassical with respect to $\mathcal{D}_s$ but classical with respect to $\mathcal{D}_i$, $1 \leq i \leq s-1$.

Proof. Set $f(x, y) := F(x, y, 1)$, and note that $f(x, y) = 0$ can be written as

$$\sum_{0 \leq i+j \leq s} c_{ij}(x^{im}y^{jm})^{p^v} x^i y^j = 0 \in \mathbb{K}(\mathcal{X}). \tag{3.4}$$

Therefore, if $(\epsilon_0, \ldots, \epsilon_M)$ is the $\mathcal{D}_s$-order sequence of $\mathcal{X}$, then Theorem 2.1 implies that $\epsilon_M \geq p^v > M$. Thus $\mathcal{X}$ is nonclassical with respect to $\mathcal{D}_s$. Let $P = (a : b : c)$ be a point of $\mathcal{X}$, with $abc \neq 0$, and consider the curve

$$\mathcal{C} : H_P(x, y, z) = 0$$

of degree s (cf. (3.3)). We claim that $\mathcal{C}$ is irreducible. To see this, consider the polynomial $G(x, y, z) := \sum_{i+j+t=s} c_{ij} x^i y^j z^t$, and note that

$$G(a^{mp^v}x, b^{mp^v}y, c^{mp^v}z) = H_P(x, y, z).$$

Therefore, we need only prove that $G(x, y, z)$ is irreducible. But this follows immediately from the fact that $\mathcal{X}$ is irreducible and $F(x, y, z) = G(x^n, y^n, z^n)$. We may assume $P = (a : b : 1)$, and then for $h(x, y) := H_P(x, y, 1)$, we see that $h(x, y) = h(x, y) - f(x, y) \in \mathbb{K}(\mathcal{X})$ can be written as

$$h(x,y) = \sum_{0 \leq i+j \leq s} c_{ij}(a^{im}b^{jm} - x^{im}y^{jm})^{p^v} x^i y^j. \tag{3.5}$$

Therefore, $v_P(h(x, y)) \geq p^v$, and then $I(P, \mathcal{X} \cap \mathcal{C}) \geq p^v$. Let $\mathcal{H}_P^s$ be the s-osculating curve to $\mathcal{X}$ at P. Since $\epsilon_M \geq p^v$, it follows from (2.1) that

$$I(P, \mathcal{X} \cap \mathcal{H}_P^s) = j_M(P) \geq p^v.$$

Thus from Lemma 3.1, we have $I(P, \mathcal{C} \cap \mathcal{H}_P^s) \geq p^v$. As we are assuming that $p > s^2$, we have

$$I(P, \mathcal{C} \cap \mathcal{H}_P^s) > s^2 = \deg(\mathcal{C}) \cdot \deg(\mathcal{H}_P^s).$$

Therefore by Bézout's Theorem, the curves $\mathcal{C}$ and $\mathcal{H}_P^s$ have a common component. However, since $\mathcal{C}$ is irreducible and $\deg(\mathcal{C}) = \deg(\mathcal{H}_P^s)$, it follows that $\mathcal{C} = \mathcal{H}_P^s$. In particular, the s-osculating curve $\mathcal{H}_P^s$ is irreducible.

For the lemma's last statement, since $p > s^2$, it suffices to prove classicality with respect to $\mathcal{D}_{s-1}$. Suppose that $\mathcal{X}$ is nonclassical with respect to $\mathcal{D}_{s-1}$. Then by [17, Corollary 1.9], the intersection multiplicity of $\mathcal{X}$ with the

$(s-1)$-osculating curve $\mathcal{H}_P^{s-1}$ to $\mathcal{X}$ at any point $P \in \mathcal{X}$ is $I(P, \mathcal{X} \cap \mathcal{H}_P^{s-1}) \geq p$. By Lemma 3.1,

$$I(P, \mathcal{H}_P^{s-1} \cap \mathcal{H}_P^s) \geq p > s^2 > s(s-1) = \deg(\mathcal{H}_P^s) \cdot \deg(\mathcal{H}_P^{s-1}),$$

and thus Bézout's Theorem implies that $\mathcal{H}_P^s$ and $\mathcal{H}_P^{s-1}$ have a common component. Since this contradicts the irreducibility of $\mathcal{H}_P^s$, the result follows. ∎

Next we give the main result of the section.

THEOREM 3.3. *Let $\mathcal{H}_P^s$ be the s-osculating curve to $\mathcal{X}$ at P. Then $\Phi_q(P)$ is in $\mathcal{H}_P^s$ for infinitely many points $P \in \mathcal{X}$ if and only if $n = (p^h-1)/(p^v-1)$, and $\mathcal{X}$ is defined over $\mathbb{F}_{p^v}$, where $q = p^h$, $h > v$ and $v \mid h$.*

Proof. Since $p \mid n-1$, we see that $n = mp^v + 1$ for some positive integers v, m, where $\gcd(p, m) = 1$. Suppose that $\Phi_q(P) \in \mathcal{H}_P^s$ for infinitely many points $P \in \mathcal{X}$. By Lemma 3.2, this means that the function

$$g(x,y) := \sum_{0 \leq i+j \leq s} c_{ij} (x^{im} y^{jm})^{p^v} x^{iq} y^{jq} \in \mathbb{K}(\mathcal{X}) \tag{3.6}$$

is zero, that is, the polynomial $f(x,y) := F(x,y,1)$ divides $g(x,y)$. Since $mp^v + q = n + q - 1$, the polynomial $g(x,y)$ can be written as

$$g(x,y) = \sum_{0 \leq i+j \leq s} c_{ij} x^{i(n+q-1)} y^{j(n+q-1)}. \tag{3.7}$$

Note that $g(x,y)$ is a nonzero polynomial of degree $s(n+q-1)$. Also, it is easy to see that $p^v < q = p^h$, i.e., $v < h$. Indeed, if $p^v \geq q$, then (3.6) gives $g(x,y) = l(x,y)^q$, where $l(x,y)$ is a polynomial of degree $s(n+q-1)/q$. This implies that $f(x,y)$ divides $l(x,y)$, and then

$$sn = \deg f(x,y) \leq \deg l(x,y) = s(n+q-1)/q,$$

which is impossible for $n > 1$.

Therefore, $n+q-1$ is divisible by p^v, and so (3.7) gives $g(x,y) = r(x,y)^{p^v}$, where

$$r(x,y) = \sum_{0 \leq i+j \leq s} c_{ij}^{1/p^v} x^{i(m+p^{h-v})} y^{j(m+p^{h-v})}.$$

Furthermore, $f(x,y) \mid r(x,y)$. Now we claim that $r(x,y)$ is irreducible. To see this, let $\mathcal{R}$ be the projective closure of the curve $r(x,y) = 0$. One can easily check that if $P = (a : b : c) \in \mathcal{R}$ is a singular point, and $\alpha, \beta, \gamma \in \mathbb{K}$ are roots of $x^n = a^{(m+p^{h-v})p^v}$, $x^n = b^{(m+p^{h-v})p^v}$ and $x^n = c^{(m+p^{h-v})p^v}$, respectively, then $(\alpha : \beta : \gamma)$ is a singular point of $\mathcal{X}$. However, since $\mathcal{X}$ is smooth, the curve $\mathcal{R}$ must be smooth, and so $r(x,y)$ is irreducible. This implies $f(x,y) = \alpha r(x,y)$ for some $\alpha \in \mathbb{K}^*$. Now $\deg f(x,y) = \deg r(x,y)$ gives $n(p^v - 1) = p^h - 1$, as desired. In addition, $c_{ij} = \alpha {c_{ij}}^{1/p^v}$ for all i, j implies that $c_{ij}/c_{kl} \in \mathbb{F}_{p^v}$ whenever $c_{kl} \neq 0$. That is, the curve $\mathcal{X}$ is defined over $\mathbb{F}_{p^v}$.

Conversely, suppose that $n = (p^h - 1)/(p^v - 1)$ with $h > v$ and $v \mid h$, and that $\mathcal{X}$ is defined over $\mathbb{F}_{p^v}$. We may assume that all coefficients c_{ij} lie in $\mathbb{F}_{p^v}$. From Lemma 3.2, it suffices to prove that $f(x,y) \mid g(x,y)$, where $g(x,y)$ is given by (3.6). Note that $n + q - 1 = np^v$, and then (3.7) implies $g(x,y) = f(x,y)^{p^v}$, which completes the proof. ∎

Corollary 3.4. *Suppose that $n = (p^h-1)/(p^v-1)$ and that $\mathcal{X}$ is defined over $\mathbb{F}_{p^v}$, where $h > v$ and $v \mid h$. Then $\mathcal{X}$ is $\mathbb{F}_q$-Frobenius nonclassical with respect to $\mathcal{D}_s$.*

Proof. By Theorem 3.3, $\Phi_q(P) \in \mathcal{H}_P^s$ for infinitely many points $P \in \mathcal{X}$. Hence, if τ is a separating variable of $\mathbb{F}_q(\mathcal{X})$, by [17, Corollary 1.3],

$$\begin{vmatrix} 1 & f_1^q & \cdots & f_M^q \\ 1 & f_1 & \cdots & f_M \\ 0 & D_\tau^{(\epsilon_1)}(f_1) & \cdots & D_\tau^{(\epsilon_1)}(f_M) \\ \vdots & \vdots & \cdots & \vdots \\ 0 & D_\tau^{(\epsilon_{M-1})}(f_1) & \cdots & D_\tau^{(\epsilon_{M-1})}(f_M) \end{vmatrix} = 0,$$

where $1, f_1, \ldots, f_M$ are the coordinate functions of the Veronese morphism ϕ_s. Thus $\nu_i > \epsilon_i$ for some $i = 1, \ldots, M-1$, and therefore $\mathcal{X}$ is $\mathbb{F}_q$-Frobenius nonclassical. ∎

As mentioned in the introduction, the construction of plane curves of degree $d < q/15$ attaining the bound (1.4) requires constructing $\mathbb{F}_q$-Frobenius nonclassical curves with respect to $\mathcal{D}_2$. Next, we take advantage of our previous characterization to find explicit examples illustrating this phenomenon.

Suppose that, in addition to our standard hypotheses, the curve $\mathcal{X} : F(x,y,z) = 0$ satisfies the assumptions of Corollary 3.4. In particular, $\mathcal{X}$ is $\mathbb{F}_q$-Frobenius nonclassical with respect to $\mathcal{D}_s$. Let $\mathcal{C} : G(x,y,z) = 0$ be the curve of degree s, defined over $\mathbb{F}_{p^v}$, where

$$G(x,y,z) = \sum_{i+j+t=s} c_{ij} x^i y^j z^t. \tag{3.8}$$

Note that $F(x,y,z) = G(x^n, y^n, z^n)$ and that the smoothness of $\mathcal{X}$ implies that $\mathcal{C}$ is smooth as well.

Theorem 3.5. *If $N_{p^v}(\mathcal{C}) = s(s + p^v - 1)/2$, and there is no $\mathbb{F}_{p^v}$-rational point $P = (a : b : c) \in \mathcal{C}$ with $abc = 0$, then*

$$N_q(\mathcal{X}) = d(d + q - 1)/2$$

with $q = p^h$ and $d = sn$. In particular, if $s = 2$ and $p^v > 31$, then $\mathcal{X}$ is a curve of degree $d < q/15$ attaining the bound (1.4).

Proof. Note that since $\mathcal{X}$ is Frobenius nonclassical with respect to $\mathcal{D}_s$ and $s \geq 2$, Lemma 3.2 implies that $\mathcal{X}$ is classical with respect to $\mathcal{D}_1$. Therefore, since $p > M = \dim(\mathcal{D}_s)$, Proposition 2.3 implies that $\mathcal{X}$ is $\mathbb{F}_q$-Frobenius classical with respect to $\mathcal{D}_1$. Hence (1.4) gives $N_q(\mathcal{X}) \le d(d+q-1)/2$.

Recall that $\mathcal{X} : F(x,y,z) = 0$ and $\mathcal{C} : G(x,y,z) = 0$ are such that $F(x,y,z) = G(x^n, y^n, z^n)$ and $n = \frac{q-1}{p^v-1}$. Therefore, the map $\pi : \mathcal{X}(\mathbb{F}_q) \to \mathcal{C}(\mathbb{F}_{p^v})$ given by $\pi(\alpha : \beta : \gamma) \mapsto (\alpha^n : \beta^n : \gamma^n)$ is well defined. Since the norm function $x \mapsto x^{(q-1)/(p^v-1)}$ maps $\mathbb{F}_q$ onto $\mathbb{F}_{p^v}$, we have

$$\mathcal{X}(\mathbb{F}_q) = \bigcup_{Q \in \mathcal{C}(\mathbb{F}_{q^v})} \pi^{-1}(Q). \tag{3.9}$$

For $Q = (a : b : c) \in \mathcal{C}$ with $abc \neq 0$, we have $\#\pi^{-1}(Q) = n^2$, and so $N_q(\mathcal{X}) = n^2 N_{p^v}(\mathcal{C})$. Therefore,

$$N_q(\mathcal{X}) = \frac{n^2 s(s+p^v-1)}{2} = \frac{s}{2} \cdot \left(\frac{(q-1)^2}{(p^v-1)^2} s + \frac{(q-1)^2}{p^v-1} \right) = \frac{sn(sn+q-1)}{2},$$

and the result follows. Note that in the case $s = 2$ and $p^v > 31$, the curve $\mathcal{X}$ has degree $d = 2n = \frac{2(q-1)}{p^v-1} < \frac{q-1}{15} < \frac{q}{15}$, as claimed. ∎

Constructing curves illustrating the case $s = 2$ in Theorem 3.5 is straightforward. One need only select one of the many irreducible conics $\mathcal{C}$, defined over $\mathbb{F}_{p^v}$, with no $\mathbb{F}_{p^v}$-rational points $P := (a : b : c)$ with $abc = 0$. Since $N_{p^v}(\mathcal{C}) = p^v + 1$, the curve $\mathcal{C}$ attains the bound (1.4), and the result follows.

4. The case $s = 2$. As mentioned in Section 3, if $s = 1$, then

$$\mathcal{X} : \sum_{i+j+t=s} c_{ij} x^{in} y^{jn} z^{tn} = 0$$

is a Fermat curve $ax^n + by^n = z^n$, and its classicality and $\mathbb{F}_q$-Frobenius classicality with respect to $\mathcal{D}_1$ and $\mathcal{D}_2$ were studied in [7] and [6], respectively. In this section, we exploit the case $s = 2$. More precisely, we consider the curve $\mathcal{X} : F(x,y,z) = 0$, where

$$F(x,y,z) = a_1 x^{2n} + a_2 x^n y^n + a_3 y^{2n} + a_4 x^n z^n + a_5 y^n z^n + a_6 z^{2n} \tag{4.1}$$

with $a_i \in \mathbb{F}_q$, $i \in \{1,2,3,4,5,6\}$, and assume the following:

(4.i) $p > 2$.
(4.ii) $\mathcal{X}$ is nonsingular (in particular, $a_1 a_3 a_6 \neq 0$).
(4.iii) At least one of the coefficients a_2, a_4 or a_5 is nonzero. In other words, equation (4.1) is not of Fermat type.

With these assumptions, we prove that $\mathcal{X}$ is $\mathbb{F}_q$-Frobenius classical with respect to $\mathcal{D}_1$, and establish necessary and sufficient conditions for the curve $\mathcal{X}$ to be $\mathbb{F}_q$-Frobenius nonclassical with respect to $\mathcal{D}_2$.

REMARK 4.1. Since $\mathcal{X}$ is irreducible, the conic given by the equation $a_1x^2 + a_2xy + a_3y^2 + a_4xz + a_5yz + a_6z^2 = 0$ is irreducible, i.e.,

$$\begin{vmatrix} a_1 & a_2/2 & a_4/2 \\ a_2/2 & a_3 & a_5/2 \\ a_4/2 & a_5/2 & a_6 \end{vmatrix} \neq 0. \tag{4.2}$$

Throughout this section, $F(x, y, 1)$ will be denoted by $f(x, y)$.

PROPOSITION 4.2. *There exists a point $P \in \mathcal{X}$ whose $(\mathcal{D}_1, P)$-order sequence is $(0, 1, n)$. In particular, if $\mathcal{X}$ is nonclassical with respect to $\mathcal{D}_1$, then $p \mid n(n-1)$.*

Proof. Using assumption (4.iii), without loss of generality, we assume $a_2 \neq 0$. If $P = (u : 0 : 1) \in \mathcal{X}$, then $f(u, 0) = a_1u^{2n} + a_4u^n + a_6 = 0$ (in particular, $u \neq 0$) and the tangent line to $\mathcal{X}$ at P is given by $\ell_P : x - uz = 0$. Thus

$$f(u, y) = y^n g(y), \tag{4.3}$$

where $g(y) = a_2u^n + a_5 + a_3y^n \neq 0$. Then $I(P, \ell_P \cap \mathcal{X}) = n$ if and only if $a_2u^n + a_5 \neq 0$. Our remaining problem reduces to finding a point $P = (u : 0 : 1) \in \mathcal{X}$ for which $a_2u^n + a_5 \neq 0$.

Suppose there is no such point, that is, all the roots of $a_1x^{2n} + a_4x^n + a_6 = 0$ are roots of $a_2x^n + a_5 = 0$. This implies that $a_1x^2 + a_4x + a_6 = 0$ has a double root $\alpha = -a_5/a_2$, which yields

$$a_4^2 - 4a_1a_6 = 0 \quad \text{and} \quad a_1a_5^2 - a_2a_4a_5 + a_2^2a_6 = 0. \tag{4.4}$$

One can easily check that (4.4) gives

$$\begin{vmatrix} a_1 & a_2/2 & a_4/2 \\ a_2/2 & a_3 & a_5/2 \\ a_4/2 & a_5/2 & a_6 \end{vmatrix} = 0,$$

which contradicts (4.2).

The last statement of the proposition follows directly from Proposition 2.2. ∎

PROPOSITION 4.3. *The curve $\mathcal{X}$ is classical with respect to $\mathcal{D}_1$. Consequently, $\mathcal{X}$ is $\mathbb{F}_q$-Frobenius classical with respect to $\mathcal{D}_1$.*

Proof. Suppose that $\mathcal{X}$ is nonclassical with respect to $\mathcal{D}_1$. Since $\mathcal{X}$ is nonsingular and $p > 2$, by [15, Corollary 2.2], $p \mid 2n - 1$. On the other hand, by Proposition 4.2, we have $p \mid n(n-1)$. However, $\gcd(2n-1, n^2-n) = 1$, and then $\mathcal{X}$ must be classical with respect to $\mathcal{D}_1$. Thus by Proposition 2.3, the curve $\mathcal{X}$ is $\mathbb{F}_q$-Frobenius classical with respect to $\mathcal{D}_1$. ∎

Remark 4.4. It follows from Proposition 4.3 that the bound (1.4) can always be applied to the curve $\mathcal{X}$. In other words, $N_q(\mathcal{X}) \leq d(d+q-1)/2$.

We now study the (non)classicality and $\mathbb{F}_q$-Frobenius (non)classicality of $\mathcal{X}$ with respect to the linear series $\mathcal{D}_2$, making the following assumptions:

(4.iv) $p > 7$.
(4.v) $n > 2$.

The following theorems will be proved after a sequence of partial results.

Theorem 4.5. *The curve $\mathcal{X}$ is nonclassical with respect to $\mathcal{D}_2$ if and only if one of the following holds:*

(1) $p \mid n-1$.
(2) $p \mid 2n-1$ *and all but one of the coefficients* a_2, a_4 *and* a_5 *are zero.*

Theorem 4.6. *The curve $\mathcal{X}$ is $\mathbb{F}_q$-Frobenius nonclassical with respect to $\mathcal{D}_2$ if and only if one of the following holds:*

(1) $p \mid n-1$ *and* $n = \frac{p^h-1}{p^v-1}$ *for some integer* $v < h$ *with* $v \mid h$, *and* $\mathcal{X}$ *is defined over* $\mathbb{F}_{p^v}$.
(2) $p \mid 2n-1$, *all but one of the coefficients* a_2, a_4 *and* a_5 *are zero,* $n = \frac{p^h-1}{2(p^v-1)}$ *for some integer* $v < h$ *with* $v \mid h$ *and, up to an* $\mathbb{F}_q$*-scaling of the coordinates, the curve* $\mathcal{X}$ *is defined over* $\mathbb{F}_{p^v}$.

The next three lemmas will provide the key ingredients for the proof of Theorem 4.5.

Lemma 4.7. *If* $p \mid (n+1)(n-2)$, *then $\mathcal{X}$ is classical with respect to* $\mathcal{D}_2$.

Proof. Since $\mathcal{X}$ is classical with respect to $\mathcal{D}_1$, the $\mathcal{D}_2$-order sequence of $\mathcal{X}$ is given by $(0,1,2,3,4,\epsilon)$, where $\epsilon \geq 5$. Suppose that $\epsilon > 5$, i.e., $\mathcal{X}$ is nonclassical for $\mathcal{D}_2$. Then by [7, Proposition 2], $\epsilon = p^s$ for some $s > 0$.

First, assume $p \mid n-2$. Hence $n = mp^v + 2$ for some $m, v > 0$ with $\gcd(m,p) = 1$, and then $f(x,y) = 0$ can be written as

$$a_1(x^{2m})^{p^v}x^4 + a_2(x^m y^m)^{p^v}x^2y^2 + a_3(y^{2m})^{p^v}y^4 + a_4(x^m)^{p^v}x^2 + a_5(y^m)^{p^v}y^2 + a_6 = 0.$$

Let $P = (u : w : 1) \in \mathcal{X}$ with $uw \neq 0$ and consider the projective closure $\mathcal{Q}_P \subset \mathbb{P}^2(\mathbb{K})$ of the curve given by

$$\begin{aligned} r(x,y) = a_1(u^{2m})^{p^\nu}x^4 + a_2(u^m w^m)^{p^\nu}x^2y^2 + a_3(w^{2m})^{p^\nu}y^4 \\ + a_4(u^m)^{p^\nu}x^2 + a_5(w^m)^{p^\nu}y^2 + a_6 = 0. \end{aligned}$$

Note that $\mathcal{Q}_P$ is an irreducible quartic. In fact, $\mathcal{Q}_P$ is projectively equivalent to the curve $\mathcal{C}$ given by

$$a_1x^4 + a_2x^2y^2 + a_3y^4 + a_4x^2z^2 + a_5y^2z^2 + a_6z^4 = 0.$$

The curve $\mathcal{C}$, on the other hand, is nonsingular. Indeed, if $(a : b : c)$ is a singular point of $\mathcal{C}$, then $(\alpha : \beta : \gamma)$ is a singular point of $\mathcal{X}$, where $\alpha, \beta, \gamma \in \mathbb{K}$ are roots of $x^n = a^2$, $x^n = b^2$, and $x^n = c^2$ respectively. This contradicts the smoothness of $\mathcal{X}$.

Now for all $P = (u : w : 1) \in \mathcal{X}$ with $uw \neq 0$,

$$\begin{aligned} r(x,y) &= r(x,y) - f(x,y) \\ &= a_1(u^{2m} - x^{2m})^{p^v} x^4 + a_2(u^m w^m - x^m y^m)^{p^v} x^2 y^2 \\ &\quad + a_3(w^{2m} - y^{2m})^{p^v} y^4 + a_4(u^m - x^m)^{p^v} x^2 + a_5(w^m - y^m)^{p^v} y^2. \end{aligned}$$

Then $I(P, \mathcal{Q}_P \cap \mathcal{X}) \geq p^v$. Let $\mathcal{H}_P^2$ be the osculating conic to $\mathcal{X}$ at P. Since $\epsilon = p^s$, we have $I(P, \mathcal{H}_P^2 \cap \mathcal{X}) \geq p^s$. However, Lemma 3.1 with our assumption that $p > 7$ gives

$$I(P, \mathcal{H}_P^2 \cap \mathcal{Q}_P) \geq p \geq 11 > 8 = \deg(\mathcal{H}_P^2) \cdot \deg(\mathcal{Q}_P),$$

which implies, by Bézout's Theorem, that $\mathcal{H}_P^2$ is a component of $\mathcal{Q}_P$. This contradicts the irreducibility of $\mathcal{Q}_P$. Therefore, $\mathcal{X}$ is classical.

Suppose $p \mid n+1$, and let $m, v > 0$ be such that $n = mp^v - 1$ and $\gcd(m,p) = 1$. From $f(x,y) = 0$ we obtain

$$0 = f(x,y)x^2y^2$$

and so

$$\begin{aligned} 0 = a_1(x^{2m})^{p^v} y^2 + a_2(x^m y^m)^{p^v} xy + a_3(y^{2m})^{p^v} x^2 \\ + a_4(x^m)^{p^v} xy^2 + a_5(y^m)^{p^v} x^2 y + a_6 x^2 y^2. \end{aligned}$$

Consider a point $P = (u : w : 1) \in \mathcal{X}$ with $uw \neq 0$ and the projective closure $\mathcal{Q}'_P \subset \mathbb{P}^2(\mathbb{K})$ of the curve given by $l(x,y) = 0$, where

$$\begin{aligned} l(x,y) &= a_6 x^2 y^2 + a_5(w^m)^{p^v} x^2 y + a_4(u^m)^{p^v} xy^2 \\ &\quad + a_3(w^{2m})^{p^v} x^2 + a_2(u^m w^m)^{p^v} xy + a_1(u^{2m})^{p^v} y^2. \end{aligned}$$

Since $a_6 \neq 0$, $\mathcal{Q}'_P$ is a quartic. Let $\alpha = u^{mp^v}$ and $\beta = w^{mp^v}$. Multiplying $l(x,y)$ by $1/(\alpha^2\beta^2)$, we see that $\mathcal{Q}'_P$ is the projective closure of the curve given by the equation

$$a_6 \frac{x^2y^2}{\alpha^2\beta^2} + a_5 \frac{x^2y}{\alpha^2\beta} + a_4 \frac{xy^2}{\alpha\beta^2} + a_3 \frac{x^2}{\alpha^2} + a_2 \frac{xy}{\alpha\beta} + a_1 \frac{y^2}{\beta^2} = 0.$$

Hence $\mathcal{Q}'_P$ is projectively equivalent to the curve $\mathcal{Y}$ given by

$$H(x,y,z) = a_6 x^2 y^2 + a_5 x^2 yz + a_4 xy^2 z + a_3 x^2 z^2 + a_2 xyz^2 + a_1 y^2 z^2 = 0.$$

Then Lemma A.1 and Remark 4.1 imply that $\mathcal{Q}'_P$ is irreducible.

Moreover,

$$l(x,y) = l(x,y) - f(x,y)x^2y^2.$$

Therefore, $I(P, \mathcal{Q}'_P \cap \mathcal{X}) \geq p^v \geq 11$. If $\mathcal{H}_P^2$ is the osculating conic to $\mathcal{X}$ at P, we have $I(P, \mathcal{H}_P^2 \cap \mathcal{X}) \geq p^s \geq 11$. By Lemma 3.1 and Bézout's Theorem, $\mathcal{H}_P^2$ is a component of $\mathcal{Q}'_P$. This is a contradiction, and thus the curve $\mathcal{X}$ is classical. ∎

LEMMA 4.8. *If $\mathcal{X}$ is nonclassical with respect to $\mathcal{D}_2$, then $p \mid (n–1)(2n–1)$.*

Proof. By Proposition 4.2, there exists a point $P \in \mathcal{X}$ with order sequence $(0, 1, n)$ with respect to $\mathcal{D}_1$, i.e., 0, 1 and n are the possible intersection multiplicities of $\mathcal{X}$ with a line at P. Hence there are degenerated conics in $\mathbb{P}^2(\mathbb{K})$ whose intersection multiplicities with $\mathcal{X}$ at P are $0, 1, 2, n, n+1$ and $2n$. Since $\mathcal{D}_2$ has projective dimension 5, these are the possible intersection multiplicities of $\mathcal{X}$ with a conic at P. In other words, the order sequence of P with respect to $\mathcal{D}_2$ is $(0, 1, 2, n, n+1, 2n)$. Thus by Proposition 2.2, p divides $n(n-1)(2n-1)(n+1)(n-2)$. Since the irreducibility of $\mathcal{X}$ together with Lemma 4.7 gives $p \nmid n(n+1)(n-2)$, the result follows. ∎

The next two lemmas will address the converse of Lemma 4.8.

LEMMA 4.9. *If $p \mid n-1$, then $\mathcal{X}$ is nonclassical with respect to $\mathcal{D}_2$.*

Proof. This follows immediately from Lemma 3.2 applied to $s = 2$. ∎

LEMMA 4.10. *Assume that $p \mid 2n-1$. The curve $\mathcal{X}$ is nonclassical with respect to $\mathcal{D}_2$ if and only if all but one of the coefficients a_2, a_4 and a_5 are zero.*

Proof. Let m, v be such that $2n = mp^v + 1$ and $\gcd(m, p) = 1$. Assume that all but one of the coefficients a_2, a_4 and a_5 are zero. We may suppose that $F(x, y, z) = a_1x^{2n} + a_2x^ny^n + a_3y^{2n} + a_6z^{2n}$ with $a_2 \neq 0$ (the other two cases are analogous). We have

$$0 = a_1x^{2n} + a_2x^ny^n + a_3y^{2n} + a_6,$$

hence

$$-a_2x^ny^n = a_1(x^m)^{p^v}x + a_3(y^m)^{p^v}y + a_6,$$

and consequently

$$(a_2^{2/p^v}x^my^m)^{p^v}xy = \big((a_1^{1/p^v}x^m)^{p^v}x + (a_3^{1/p^v}y^m)^{p^v}y + (a_6^{1/p^v})^{p^v}\big)^2. \tag{4.5}$$

Since $\mathcal{X}$ is classical with respect to $\mathcal{D}_1$, the $\mathcal{D}_2$-order sequence of $\mathcal{X}$ is $(0, 1, 2, 3, 4, \epsilon)$ for some $\epsilon \geq 5$. In view of (3.4), Theorem 2.1 implies that $\epsilon \geq p^v > 5$. Hence $\mathcal{X}$ is nonclassical for $\mathcal{D}_2$.

Now assume $\mathcal{X}$ is nonclassical, and suppose that at least two of the constants a_2, a_4 and a_5 are nonzero. Recall that the smoothness of $\mathcal{X}$ implies $a_1a_3a_6 \neq 0$, and then after scaling we may set $a_1 = a_3 = a_6 = 1$. Thus since $f(x, y) = x^{2n} + a_2x^ny^n + y^{2n} + a_4x^n + a_5y^n + 1 = 0 \in \mathbb{K}(\mathcal{X})$, we have

$$(x^{2n}+a_2x^ny^n+y^{2n}+a_4x^n+a_5y^n+1)(x^{2n}-a_2x^ny^n+y^{2n}-a_4x^n+a_5y^n+1)=0,$$

and then

$$\begin{aligned}(4.6)\qquad x^{4n}+(2-a_2^2)x^{2n}y^{2n}+(2-a_4^2)x^{2n}+y^{4n}+(a_5^2+2)y^{2n}+1\\ =2y^n\big((a_2a_4-a_5)x^{2n}-a_5y^{2n}-a_5\big).\end{aligned}$$

Squaring both sides of (4.6) yields

$$\begin{aligned}(4.7)\qquad \big((x^{2m})^{p^v}x^2+(2-a_2^2)(x^my^m)^{p^v}xy+(2-a_4^2)(x^m)^{p^v}x\\ +(y^{2m})^{p^v}y^2+(a_5^2+2)(y^m)^{p^v}y+1\big)^2\\ =4(y^m)^{p^v}y\big((a_2a_4-a_5)(x^m)^{p^v}x-a_5(y^m)^{p^v}y-a_5\big)^2.\end{aligned}$$

Let $P=(u:w:1)\in\mathcal{X}$ with $uw\neq 0$, and $\mathcal{Q}_P$ be the projective closure of the quartic given by $r(x,y)=0$, where

$$\begin{aligned}(4.8)\qquad r(x,y)=\big((u^{2m})^{p^v}x^2+(2-a_2^2)(u^mw^m)^{p^v}xy+(2-a_4^2)(u^m)^{p^v}x\\ +(w^{2m})^{p^v}y^2+(a_5^2+2)(w^m)^{p^v}y+1\big)^2\\ -4(w^m)^{p^v}y\big((a_2a_4-a_5)(u^m)^{p^v}x-a_5(w^m)^{p^v}y-a_5\big)^2.\end{aligned}$$

We claim that $\mathcal{Q}_P$ is irreducible. In fact, via $(x:y:z)\mapsto(u^{mp^v}x:w^{mp^v}y:z)$, the quartic $\mathcal{Q}_p$ is projectively equivalent to

$$\big((x+y+z)^2-a_2^2xy-a_4^2xz+a_5^2yz\big)^2-4\big((a_2a_4-a_5)x-a_5y-a_5z\big)^2yz=0.$$

Thus if $\mathcal{Q}_P$ is reducible, then Theorem A.3 implies $a_2^2+a_4^2+a_5^2-a_2a_4a_5=4$ (since we are assuming that at least two of the constants a_2,a_4 and a_5 are nonzero). But then

$$\begin{vmatrix}1 & a_2/2 & a_4/2\\ a_2/2 & 1 & a_5/2\\ a_4/2 & a_5/2 & 1\end{vmatrix}=\frac{a_2a_4a_5-(a_2^2+a_4^2+a_5^2)}{4}+1=0,$$

which contradicts (4.2).

Hence using the same arguments as in the proof of Lemma 4.7, we get $I(P,\mathcal{Q}_P\cap\mathcal{X})\geq p$. Since $\mathcal{X}$ is classical with respect to $\mathcal{D}_1$ and nonclassical with respect to $\mathcal{D}_2$, by [7, Proposition 2] the order sequence of $\mathcal{X}$ with respect to $\mathcal{D}_2$ is $(0,1,2,3,4,p^s)$ for some $s>0$. Therefore, if $\mathcal{H}_P^2$ is the osculating conic to $\mathcal{X}$ at P, we have $I(P,\mathcal{H}_P^2\cap\mathcal{X})\geq p^s$. Using Lemma 3.1, as in the previous cases, we obtain a contradiction by Bézout's Theorem since we are assuming that $p>7$. ■

Proof of Theorem 4.5. This follows directly from Lemmas 4.8–4.10. ■

We use the following lemmas to build our proof of Theorem 4.6.

Lemma 4.11. *Assume that $p \mid n-1$. Then $\mathcal{X}$ is $\mathbb{F}_q$-Frobenius nonclassical with respect to $\mathcal{D}_2$ if and only if $n = \frac{p^h-1}{p^v-1}$ with $h > v$, $v \mid h$ and $\mathcal{X}$ is defined over $\mathbb{F}_{p^v}$.*

Proof. If $n = \frac{p^h-1}{p^v-1}$ with $h > v$, $v \mid h$ and $\mathcal{X}$ is defined over $\mathbb{F}_{p^v}$, by Corollary 3.4 applied in the case $s = 2$, $\mathcal{X}$ is $\mathbb{F}_q$-Frobenius nonclassical with respect to $\mathcal{D}_2$. For the converse, note that by Proposition 2.3, $\mathcal{X}$ must be nonclassical with respect to $\mathcal{D}_2$. Since $\mathcal{X}$ is classical with respect to $\mathcal{D}_1$ (Proposition 4.3), its $\mathcal{D}_2$-order sequence is $(0, 1, 2, 3, 4, \epsilon)$, where $\epsilon > 5$. The $\mathbb{F}_q$-Frobenius nonclassicality of $\mathcal{X}$ with respect to $\mathcal{D}_2$ is equivalent to

$$\begin{vmatrix} 1 & x^q & y^q & x^{2q} & x^q y^q & y^{2q} \\ 1 & x & y & x^2 & xy & y^2 \\ 0 & D_\tau^{(1)}(x) & D_\tau^{(1)}(y) & D_\tau^{(1)}(x^2) & D_\tau^{(1)}(xy) & D_\tau^{(1)}(y^2) \\ 0 & D_\tau^{(2)}(x) & D_\tau^{(2)}(y) & D_\tau^{(2)}(x^2) & D_\tau^{(2)}(xy) & D_\tau^{(2)}(y^2) \\ 0 & D_\tau^{(3)}(x) & D_\tau^{(3)}(y) & D_\tau^{(3)}(x^2) & D_\tau^{(3)}(xy) & D_\tau^{(3)}(y^2) \\ 0 & D_\tau^{(4)}(x) & D_\tau^{(4)}(y) & D_\tau^{(4)}(x^2) & D_\tau^{(4)}(xy) & D_\tau^{(4)}(y^2) \end{vmatrix} = 0,$$

where τ is a separating variable of $\mathbb{F}_q(\mathcal{X})$. Then by [17, Corollary 1.3], $\Phi_q(P) \in \mathcal{H}_P^2$ for infinitely many points of $\mathcal{X}$. Hence the result follows from Theorem 3.3. ∎

The next lemma is a consequence of [3, Theorem 3.2].

Lemma 4.12. *Let K be an arbitrary field. Consider nonconstant polynomials $b_1(x), b_2(x) \in K[x]$, and let l and m be positive integers. Then*

$$y^l - b_1(x) \quad \textit{divides } y^m - b_2(x)$$

if and only if $l \mid m$ and $b_2(x) = b_1(x)^{m/l}$.

Lemma 4.13. *Assume that $p \mid 2n-1$. The curve $\mathcal{X}$ is $\mathbb{F}_q$-Frobenius nonclassical with respect to $\mathcal{D}_2$ if and only if all but one of the coefficients a_2, a_4 and a_5 are zero, $n = \frac{q-1}{2(p^v-1)}$ for some integer $v < h$ with $v \mid h$, and up to an $\mathbb{F}_q$-scaling of the coordinates, the curve $\mathcal{X}$ is defined over $\mathbb{F}_{p^v}$.*

Proof. Suppose that $\mathcal{X}$ is $\mathbb{F}_q$-Frobenius nonclassical. By Proposition 2.3, the curve $\mathcal{X}$ is nonclassical and therefore, by Lemma 4.10, all but one of a_2, a_4, and a_5 are zero. We can assume that $a_4 \neq 0$. Dehomogenizing $F(x, y, z)$ with respect to z and setting $a := -a_1/a_3$, $b := -a_4/a_3$, and $c := -a_6/a_3$, we find that $\mathcal{X}$ is given by the affine equation

$$y^{2n} = ax^{2n} + bx^n + c. \tag{4.9}$$

Since $p \nmid 2n$, we see that x is a separating variable of $\mathbb{F}_q(\mathcal{X})$. The assumption that $\mathcal{X}$ is $\mathbb{F}_q$-Frobenius nonclassical is equivalent to $W = 0 \in \mathbb{F}_q(\mathcal{X})$, where

$$W := \begin{vmatrix} x - x^q & x^2 - x^{2q} & y - y^q & xy - x^q y^q & y^2 - y^{2q} \\ 1 & 2x & D_x^{(1)}(y) & D_x^{(1)}(xy) & D_x^{(1)}(y^2) \\ 0 & 1 & D_x^{(2)}(y) & D_x^{(2)}(xy) & D_x^{(2)}(y^2) \\ 0 & 0 & D_x^{(3)}(y) & D_x^{(3)}(xy) & D_x^{(3)}(y^2) \\ 0 & 0 & D_x^{(4)}(y) & D_x^{(4)}(xy) & D_x^{(4)}(y^2) \end{vmatrix}. \tag{4.10}$$

Using the formula $D_x^{(i)}(fg) = \sum_{j=0}^{i} D_x^{(j)}(f) D_x^{(i-j)}(g)$ (see e.g. [11, Lemma 5.72]) and elementary properties of determinants, we obtain

$$W = \begin{vmatrix} x - x^q & x^2 - x^{2q} & y - y^q & 0 & -(y^q - y)^2 \\ 1 & 2x & D_x^{(1)}(y) & y - y^q & 0 \\ 0 & 1 & D_x^{(2)}(y) & D_x^{(1)}(y) & (D_x^{(1)}(y))^2 \\ 0 & 0 & D_x^{(3)}(y) & D_x^{(2)}(y) & 2D_x^{(1)}(y)D_x^{(2)}(y) \\ 0 & 0 & D_x^{(4)}(y) & D_x^{(3)}(y) & 2D_x^{(1)}(y)D_x^{(3)}(y) + (D_x^{(2)}(y))^2 \end{vmatrix}.$$

Equation (4.9) with the hypothesis $p \mid 2n-1$ gives us

$$D_x^{(1)}(y) = \frac{2ax^{2n-1} + bx^{n-1}}{2y^{2n-1}} \quad \text{and} \quad D_x^{(i)}(y) = \frac{(n-1)\dots(n-i+1)bx^{n-i}}{2i!y^{2n-1}}$$

for $i > 1$. Through standard computations and bearing in mind $p \mid 2n-1$, we obtain

$$\begin{aligned} W = \frac{b^2x^{2n-6}}{1024y^{8n-4}} \big(&-2bx^n y^{2n} - 2y^{4n+q-1} - 2abx^{3n+q-1} + 2abx^{3n} + y^{4n} \\ &+ 2bx^n y^{2n+q-1} + y^{4n+2q-2} + a^2x^{4n} + b^2x^{2n} \\ &+ a^2x^{4n+2q-2} - b^2x^{2n+q-1} - 2a^2x^{4n+q-1} - 2ax^{2n}y^{2n} \\ &+ 2ax^{2n}y^{2n+q-1} + 2ax^{2n+q-1}y^{2n} - 2ax^{2n+q-1}y^{2n+q-1}\big). \end{aligned}$$

Therefore, $W = \frac{b^2x^{2n-6}}{1024y^{8n-4}} W_1 W_2$, where

$$\begin{aligned} W_1 &:= ax^{2n+q-1} - y^{2n+q-1} + bx^{\frac{2n+q-1}{2}} + y^{2n} - ax^{2n} - bx^n, \\ W_2 &:= ax^{2n+q-1} - y^{2n+q-1} - bx^{\frac{2n+q-1}{2}} + y^{2n} - ax^{2n} - bx^n. \end{aligned}$$

From (4.9), we can write

$$W_1 = y^{2n+q-1} - ax^{2n+q-1} - bx^{\frac{2n+q-1}{2}} - c, \tag{4.11}$$

$$W_2 = y^{2n+q-1} - ax^{2n+q-1} + bx^{\frac{2n+q-1}{2}} - c. \tag{4.12}$$

Now consider W_1 and W_2 as polynomials. Since $W = 0 \in \mathbb{F}_q(\mathcal{X})$, there are two possibilities:

(i) $(y^{2n}-ax^{2n}-bx^n-c)\mid W_1$. In this case, by Lemma 4.12, $2n\mid 2n+q-1$ and
$$ax^{2n+q-1}+bx^{\frac{2n+q-1}{2}}+c=(ax^{2n}+bx^n+c)^{\frac{2n+q-1}{2n}}.$$
It can be checked that the equality above implies $\frac{2n+q-1}{2n}=p^v$ for some $v>0$, i.e., $n=\frac{q-1}{2(p^v-1)}$, and hence v is a proper divisor of h. Furthermore, $a^{p^v}=a$, $b^{p^v}=b$ and $c^{p^v}=c$, which means that $a,b,c\in\mathbb{F}_{p^v}$.

(ii) $(y^{2n}-ax^{2n}-bx^n-c)\mid W_2$. By Lemma 4.12, $n=\frac{q-1}{2(p^v-1)}$, where v is a proper divisor of h. Moreover, $a^{p^v}=a$, $b^{p^v}=-b$ and $c^{p^v}=c$. Hence $a,c\in\mathbb{F}_{p^v}$ and $b\in\mathbb{F}_q$ is such that $b^{p^v-1}=-1$. Since $b^2\in\mathbb{F}_{p^v}$, there exists $\alpha\in\mathbb{F}_q$ such that $\alpha^{2n}=b^2$, using the surjectivity of the norm map $N:\mathbb{F}_q\to\mathbb{F}_{p^v}$. Thus, up to the $\mathbb{F}_q$-scaling $(x,y)\mapsto(\alpha x,y)$, the curve $\mathcal{X}$ is defined over $\mathbb{F}_{p^v}$.

Conversely, assume that all but one of the coefficients a_2, a_4 and a_5 are zero, $n=\frac{q-1}{2(p^v-1)}$ for some integer $v<h$ with $v\mid h$ and that, up to $\mathbb{F}_q$-scaling, the curve $\mathcal{X}$ is defined over $\mathbb{F}_{p^v}$. We can suppose that $a_4\neq 0$ and $a_1,a_3,a_4,a_6\in\mathbb{F}_{p^v}$. Then $\mathcal{X}$ is determined by the affine equation (4.9) with $a,b,c\in\mathbb{F}_{p^v}$. Hence
$$W=\frac{b^2x^{2n-6}}{1024y^{8n-4}}\cdot W_1\cdot W_2$$
with W, W_1 and W_2 as in (4.10), (4.11), and (4.12), respectively. Since $n=\frac{q-1}{2(p^v-1)}$, we have
$$2n+q-1=2np^v.$$
Therefore,
$$\begin{aligned}W_1&=y^{2n+q-1}-ax^{2n+q-1}-bx^{\frac{2n+q-1}{2}}-c\\&=(y^{2n}-ax^{2n}-bx^n-c)^{p^v}=0.\end{aligned}$$
Thus $W=0$, i.e., $\mathcal{X}$ is $\mathbb{F}_q$-Frobenius nonclassical with respect to $\mathcal{D}_2$. ■

Proof of Theorem 4.6. This follows directly from Lemmas 4.8, 4.11 and 4.13. ■

5. The number of rational points. In this section, we use the preceding results to discuss the possible values of $N_q(\mathcal{X})$ in the case $s=2$. Since the necessary and sufficient conditions for the $\mathbb{F}_q$-Frobenius nonclassicality of $\mathcal{X}$ have been established, we will be able to provide the exact number of $\mathbb{F}_q$-rational points for these curves. In the remaining cases, i.e., for the $\mathbb{F}_q$-Frobenius classical curves $\mathcal{X}$, the Stöhr–Voloch bound (1.3) gives

$$N_q(\mathcal{X})\le\frac{2d(5d+q-10)}{5},\tag{5.1}$$

where $d = \deg \mathcal{X}$. The next result gives the number of $\mathbb{F}_q$-rational points on the $\mathbb{F}_q$-Frobenius nonclassical curves $\mathcal{X}$ satisfying condition (1) of Theorem 4.6.

THEOREM 5.1. *If $n = \frac{q-1}{p^v-1}$ with $v < h$ such that $v \mid h$, and $a_1, \dots, a_6$ in $\mathbb{F}_{p^v}$ are such that the curve $\mathcal{X} : a_1x^{2n} + a_2x^ny^n + a_3y^{2n} + a_4x^nz^n + a_5y^nz^n + a_6z^{2n} = 0$ is smooth, then*

$$N_q(\mathcal{X}) = n(n(p^v + 1) - \delta(n - 1)), \tag{5.2}$$

where δ is the number of $\mathbb{F}_{p^v}$-rational points $P = (a : b : c)$ on the conic $\mathcal{C} : a_1x^2 + a_2xy + a_3y^2 + a_4xz + a_5yz + a_6z^2 = 0$ satisfying $abc = 0$.

Proof. As in the proof of Theorem 3.5, consider the map $\pi : \mathcal{X}(\mathbb{F}_q) \to \mathcal{C}(\mathbb{F}_{p^v})$ given by $\pi(\alpha : \beta : \gamma) = (\alpha^n : \beta^n : \gamma^n)$. Since $\mathcal{X}$ is nonsingular, $(1 : 0 : 0), (0 : 1 : 0), (0 : 0 : 1) \notin \mathcal{X}$. Hence $\#\pi^{-1}(Q) = n$ for all $Q = (a : b : c) \in \mathcal{C}(\mathbb{F}_{p^v})$ such that $abc = 0$. Additionally, $\#\pi^{-1}(Q) = n^2$ for all $Q = (a : b : c) \in \mathcal{C}(\mathbb{F}_{p^v})$ such that $abc \neq 0$. Since $N_{p^v}(\mathcal{C}) = p^v + 1$, equation (3.9) gives the result. ∎

EXAMPLE 5.2. Consider the curve $\mathcal{X} : x^{88} + 3x^{44}y^{44} + y^{88} + 3x^{44}z^{44} + 3y^{44}z^{44} + z^{88} = 0$ over $\mathbb{F}_{43^2}$. We see that $\mathcal{X}$ has degree $d = 2n$, where $n = \frac{43^2-1}{43-1}$. It can be checked that the conic $\mathcal{C} : x^2 + 3xy + y^2 + 3xz + 3yz + z^2 = 0$ has no $\mathbb{F}_{43}$-rational points $P = (a : b : c)$ with $abc = 0$. Hence (5.2) gives $N_q(\mathcal{X}) = 85184$.

For the curves corresponding to case (2) of Theorem 4.6, we have the following.

THEOREM 5.3. *If $n = \frac{q-1}{2(p^v-1)}$ with $v < h$ such that $v \mid h$, and $a, b, c \in \mathbb{F}_{p^v}^*$ are such that the curve $\mathcal{X} : ax^{2n} + bx^ny^n + cy^{2n} + z^{2n} = 0$ is smooth, then*

$$N_q(\mathcal{X}) = n(q + 3 - (2n - 1)\eta), \tag{5.3}$$

where η is the number of distinct $\mathbb{F}_{p^v}$-roots of $ax^2 + bx + c = 0$.

Proof. Considering the irreducible conic $\mathcal{C} : ax^2 + bxy + cy^2 + z^2 = 0$ shows that the map $\varphi : \mathcal{X} \to \mathcal{C}$ given by $(x : y : z) \mapsto (x^n : y^n : z^n)$ is well defined. Thus since $n = \frac{q-1}{2(p^v-1)}$, a point $P \in \mathcal{X}$ is $\mathbb{F}_q$-rational if and only if the nonzero coordinates of $Q = \varphi(P)$ satisfy the equation $t^{2(p^v-1)} = 1$. That is, the point Q is defined over either $\mathbb{F}_{p^v}$ or $\lambda \cdot \mathbb{F}_{p^v}$, where λ is such that $\lambda^{p^v-1} = -1$. Note that the fiber of each point $Q = (x : y : z) \in \mathcal{C}$ has either n^2 or n points, with the latter case corresponding to the points for which $xyz = 0$. Therefore, counting the $\mathbb{F}_q$-rational points on $\mathcal{X}$ reduces to counting the points $Q = (x : y : z) \in \mathcal{C}$ defined over the set $S := \lambda \cdot \mathbb{F}_{p^v} \cup \mathbb{F}_{p^v}$, where $\lambda^{p^v-1} = -1$.

The computation will be based on two types of points $(x : y : z) \in \mathcal{C}$.

(i) *Case* $xyz \neq 0$. For $f(x,y) := ax^2 + bxy + cy^2 + 1 = 0$, let x_0, y_0 in $S \setminus \{0\}$ be such that $f(x_0, y_0) = 0$. Since $a, b, c \in \mathbb{F}_{p^v}$, either $x_0, y_0 \in \mathbb{F}_{p^v}$ or $x_0, y_0 \in \lambda \cdot \mathbb{F}_{p^v}$. Hence the number sought is given by the number of points $(x_0, y_0) \in \mathbb{F}_{p^v}^* \times \mathbb{F}_{p^v}^*$ on the union of the two distinct and irreducible conics

$$\mathcal{C}_1 : ax^2 + bxy + cy^2 + 1 = 0 \quad \text{and} \quad \mathcal{C}_2 : ax^2 + bxy + cy^2 + 1/\lambda^2 = 0.$$

Clearly this number is $2(p^v + 1) - (\#\mathcal{Z}_1 + \#\mathcal{Z}_2)$, where $\mathcal{Z}_i$ is the set of points $Q = (x : y : z)$ with $xyz = 0$ on the projective closure of $\mathcal{C}_i$, $i = 1, 2$. Let $\mathcal{Z}_i \cap \{z = 0\} \subseteq \mathcal{Z}_i$ be the set of points on the line $z = 0$. Note that $\mathcal{Z}_1 \cap \{z = 0\} = \mathcal{Z}_2 \cap \{z = 0\} = \mathcal{Z}_1 \cap \mathcal{Z}_2$, and then

$$\eta := \#(\mathcal{Z}_1 \cap \mathcal{Z}_2)$$

is the number of distinct $\mathbb{F}_{p^v}$-roots of $ax^2 + bx + c = 0$. Since $1/\lambda^2 \in \mathbb{F}_{p^v}$ is not a square, we can see that

$$\#((\mathcal{Z}_1 \cup \mathcal{Z}_2) \cap \{xy = 0\}) = 4,$$

and so $\#\mathcal{Z}_1 + \#\mathcal{Z}_2 = 4 + 2\eta$. Therefore, the number of $\mathbb{F}_q$-rational points on $\mathcal{X}$ with nonzero coordinates is given by

$$n^2(2(p^v + 1) - (4 + 2\eta)). \tag{5.4}$$

(ii) *Case* $xyz = 0$. We use the notation from the previous case. Clearly the set of points on $\mathcal{C}$ with coordinates defined over S and satisfying $xyz = 0$ is $\mathcal{Z}_1 \cup \mathcal{Z}_2$. Based on our previous discussion, we deduce that $\#(\mathcal{Z}_1 \cup \mathcal{Z}_2) = 4 + \eta$. Hence there will be $n(4 + \eta)$ $\mathbb{F}_q$-rational points on $\mathcal{X} \cap \{xyz = 0\}$.

Finally, adding $n(4 + \eta)$ to the number given in (5.4) yields (5.3). ∎

Example 5.4. Consider the curve

$$\mathcal{X} : x^{20} + 2x^{10}y^{10} - y^{20} + z^{20} = 0$$

over $\mathbb{F}_{19^2}$. Note that $\mathcal{X}$ has degree $d = 2n$, where $n = \frac{19^2-1}{2(19-1)}$. Since the equation $x^2 + 2x - 1 = 0$ has no $\mathbb{F}_{19}$-rational roots, Theorem 5.3 gives $N_q(\mathcal{X}) = 3640$.

Remark 5.5. Note that, in contrast to the $\mathbb{F}_q$-Frobenius classical case, the number $N_q(\mathcal{X})$ in examples 5.2 and 5.4 exceed the upper bound in (5.1).

Appendix. A special family of plane quartics. In what follows, we note some simple facts regarding the irreducibility of certain plane quartics that are used in some of the proofs of this paper. Despite the simplicity, their detailed proofs can be quite lengthy. Thus for the sake of brevity, in some cases we omit the details and just indicate the main steps.

Hereafter, we assume K is an algebraically closed field with $\mathrm{char}(K) \neq 2$.

Lemma A.1. *Let $a, b, c, d, e, f \in K$ be such that $\mathcal{Q} : a(xy)^2 + b(xz)^2 + c(yz)^2 + xyz(dx + ey + fz) = 0$ is a projective plane quartic. Then $\mathcal{Q}$ is* *irreducible if and only if*

$$abc \cdot \begin{vmatrix} a & d/2 & e/2 \\ d/2 & b & f/2 \\ e/2 & f/2 & c \end{vmatrix} \neq 0. \tag{A.1}$$

Proof. Consider the conic $\mathcal{C} : ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0$ and assume condition (A.1). Then $\mathcal{C}$ is irreducible and does not pass through any of the points $(1 : 0 : 0)$, $(0 : 1 : 0)$, and $(0 : 0 : 1)$. Therefore, the quartic $\mathcal{Q}$ is the image of $\mathcal{C}$ by the standard Cremona transformation $(x : y : z) \mapsto (xy : xz : zy)$. Hence $\mathcal{Q}$ is irreducible. The converse is trivial. ■

For $b, d, e \in K$, not all being zero, consider the plane projective quartic $\mathcal{Q} : F(x, y, z) = 0$, where

$$\begin{aligned} &F(x,y,z) \\ &:= \big((x+y+z)^2 - b^2xy - d^2xz + e^2yz\big)^2 - 4\big((bd-e)x - ey - ez\big)^2 yz. \end{aligned} \tag{A.2}$$

The idea is to find conditions on a, b and c for which the quartic $\mathcal{Q}$ is irreducible. We begin with the following result, which states some basic facts about $\mathcal{Q}$. The proof is trivial and will be omitted.

Lemma A.2.

(i) *The polynomial F defining the quartic $\mathcal{Q}$ satisfies*

$$\begin{aligned} &F(x,y,z) \\ &= \big((x+y+z)^2 - e^2yz - d^2xz + b^2xy\big)^2 - 4\big((ed-b)z - by - bx\big)^2 xy. \end{aligned}$$

(ii) *The points $P_1 = (e^2 : d^2 : bde - d^2 - e^2)$, $P_2 = (e^2 : bde - b^2 - e^2 : b^2)$ and $P_3 = (bde - d^2 - b^2 : d^2 : b^2)$ lie on $\mathcal{Q}$. Moreover, P_1, P_2, and P_3 are collinear if and only if*

$$bde(b^2 + d^2 + e^2 - bde) = 0.$$

Theorem A.3. *The quartic $\mathcal{Q}$ is reducible if and only if at least two of the elements $b, d, e \in K$ are zero or $b^2 + d^2 + e^2 - bde = 4$.*

Proof. If two of the elements $b, d, e \in K$ are zero, then the reducibility of $\mathcal{Q}$ follows directly from (A.2) and Lemma A.2. If $b^2 + d^2 + e^2 - bde = 4$, then let $u, v \in K$ be such that $b = u + 1/u$ and $e = v + 1/v$. In this case, note that $d = t + 1/t$ where either $t = uv$ or $t = u/v$. From this, it can be checked that the factorization of $F(x, y, z)$ is given by

$$F(x,y,z) = H(x, u^2y, t^2z) \cdot H(x, (1/u^2)y, (1/t^2)z),$$

where $H(x, y, z) = x^2 + z^2 + y^2 - 2(xy + xz + yz)$. To prove the converse, we consider the following three cases:

(1) $b^2+d^2+e^2=bde$. In this case, $P_1=P_2=P_3=(e^2:d^2:b^2)$, and without loss of generality, we assume $b\neq 0$. Dehomogenizing $F(x,y,z)$ with respect to the variable z and considering the change of variables

$$f(x,y):=F(x-y+e^2/b^2,y+d^2/b^2,1),$$

we focus on the affine curve $\mathcal{F}: f(x,y)=0$. Given the condition $b^2+d^2+e^2=bde$, it turns out that $f(x,y)=f_4(x,y)+f_3(x,y)$, where

$$\begin{aligned}f_4(x,y)&=b^2x^4-2b^4x^3y+(b^6+2b^4)x^2y^2-2b^6xy^3+b^6y^4,\\ f_3(x,y)&=4(bde-b^2d^2)x^3+4(2b^3de-b^4-2b^2e^2)x^2y\\ &\quad+4(b^4-2b^3de+b^2d^2+b^2e^2)xy^2.\end{aligned}$$

One can check that $\mathrm{resultant}(f_4(x,1),f_3(x,1))=b^{30}\neq 0$. Thus $\gcd(f_4,f_3)=1$, which implies that $\mathcal{F}$ is an irreducible curve (see e.g. [4, Problem 2.34]).

(2) $b^2+d^2+e^2-bde\neq 0,4$ *and only one of the constants* b,d,e *is zero.* Without loss of generality, we may assume that $e=0$, and therefore $bd(b^2+d^2)\neq 0$. Setting $u:=(b^2+d^2)/b^2$ and

$$M:=\begin{pmatrix}-u & 0 & 0\\ u-1 & -1 & -u\\ 1 & 1 & 0\end{pmatrix},$$

we have $\det M=-u^2\neq 0$. Let T be the projective transformation associated to the matrix M and define $G(x,y,z):=F(T(x,y,z))$. Dehomogenizing $G(x,y,z)$ with respect to the variable z, we find that the curve may be given by $f(x,y)=0$, where

$$f(x,y)=\left(y^2+2y+\frac{b^2(b^2+d^2)+4d^2}{b^2(b^2+d^2)}\right)x^2-\frac{2}{b^2}\left(\frac{b^2-d^2}{b^2+d^2}y+1\right)x+\frac{1}{b^4}.$$

Note that f is a quadratic polynomial in $K(y)[x]$, which is reducible if and only if its discriminant

$$\Delta_f:=-\frac{16d^2}{b^2(b^2+d^2)^2}\left(y^2+\frac{b^2+d^2}{b^2}y+\frac{b^2+d^2}{b^4}\right)$$

is a square in $K(y)$. This condition is equivalent to the discriminant of $g(y)=y^2+(\frac{b^2+d^2}{b^2})y+\frac{b^2+d^2}{b^4}$, namely $\Delta_g:=(d^2+b^2)(d^2+b^2-4)/b^4$, being zero. Hence the result follows.

(3) $b^2+d^2+e^2-bde\neq 0,4$ *and* $bde\neq 0$. By Lemma A.2, the points $P_1=(e^2:d^2:bde-d^2-e^2)$, $P_2=(e^2:bde-b^2-e^2:b^2)$, and $P_3=(bde-d^2-b^2:d^2:b^2)$ lie on $\mathcal{Q}$ and are not collinear. Consider the projective change of coordinates mapping P_1, P_2, and P_3 to $(1:0:0),(0:1:0)$ and $(0:0:1)$, respectively. Based on this map, it can be checked that $\mathcal{Q}$ is

projectively equivalent to the quartic defined by

$$D(e^4x^2y^2 + d^4x^2z^2 + b^4y^2z^2) + 2xyz(Ax + By + Cz) = 0,$$

where $A = e^2d^2(bde + b^2 - d^2 - e^2)$, $B = e^2b^2(bde - b^2 + d^2 - e^2)$, $C = d^2b^2(bde - b^2 - d^2 + e^2)$ and $D := b^2 + d^2 + e^2 - bde$. Since

$$\begin{vmatrix} De^4 & A & B \\ A & Dd^4 & C \\ B & C & Db^4 \end{vmatrix} = (bde)^6(b^2 + d^2 + e^2 - bde - 4) \neq 0,$$

Lemma A.1 implies that $\mathcal{Q}$ is irreducible. ∎

Acknowledgements. The authors were partly supported by FAPESP-Brazil, grants 2013/00564-1 (N.A.) and 2011/19446-3 (H.B.).

References

[1] H. Borges, *Frobenius nonclassical components of curves with separated variables*, arXiv:1311.4438 (2013).
[2] H. Borges, *On multi-Frobenius non-classical plane curves*, Arch. Math. (Basel) 93 (2009), 541–553.
[3] M. D. Fried and R. E. MacRae, *On curves with separated variables*, Math. Ann. 180 (1969), 220–226.
[4] W. Fulton, *Algebraic Curves*, Benjamin, New York, 1969.
[5] A. Garcia, *The curves $y^n = f(x)$ over finite fields*, Arch. Math. (Basel) 54 (1990), 36–44.
[6] A. Garcia and J. F. Voloch, *Fermat curves over finite fields*, J. Number Theory 30 (1988), 345–356.
[7] A. Garcia and J. F. Voloch, *Wronskians and linear independence in fields of prime characteristic*, Manuscripta Math. 59 (1987), 457–469.
[8] M. Giulietti, *On the number of chords of an affinely regular polygon passing through a given point*, Acta Sci. Math. (Szeged) 74 (2008), 901–913.
[9] A. Hefez and J. F. Voloch, *Frobenius non-classical curves*, Arch. Math. (Basel) 54 (1990), 263–273.
[10] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, 2nd ed., Oxford Univ. Press, 1998.
[11] J. W. P. Hirschfeld, G. Korchmáros and F. Torres, *Algebraic Curves over a Finite Field*, Princeton Ser. Appl. Math., Princeton Univ. Press, 2008.
[12] M. Homma, *Funny plane curves in characteristic $p > 0$*, Comm. Algebra 15 (1987), 1469–1501.
[13] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge Univ. Press, 1984.
[14] M. Namba, *Geometry of Projective Algebraic Curves*, Monogr. Textbooks Pure Appl. Math. 88, Dekker, 1984.
[15] R. Pardini, *Some remarks on plane curves over fields of positive characteristic*, Compos. Math. 60 (1986), 3–17.
[16] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, Berlin, 1993.
[17] K.-O. Stöhr and J. F. Voloch, *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. 52 (1986), 1–19.

Nazar Arakelian
Instituto de Matemática, Estatística
e Computação Científica
Universidade Estadual de Campinas
Rua Sérgio Buarque de Holanda, 651
CEP 13083-859, Campinas SP, Brazil
E-mail: nazar@ime.unicamp.br

Herivelto Borges
Instituto de Ciências Matemáticas
e de Computação
Universidade de São Paulo
Avenida Trabalhador São-carlense, 400
CEP 13566-590, São Carlos SP, Brazil
E-mail: hborges@icmc.usp.br

Received on 16.8.2014 (7757)