Frobenius nonclassicality of Fermat curves with respect to cubics

Nazar Arakelian

IMECC, Universidade Estadual de Campinas, Campinas, Brazil

Herivelto Borges

ICMC, Universidade de São Paulo, São Carlos, Brazil

October 7, 2015

Abstract

For Fermat curves $\mathcal{F} : aX^n + bY^n = Z^n$ defined over $\mathbb{F}_q$, we establish necessary and sufficient conditions for $\mathcal{F}$ to be $\mathbb{F}_q$-Frobenius nonclassical with respect to the linear system of plane cubics. In the new $\mathbb{F}_q$-Frobenius nonclassical cases, we determine explicit formulas for the number $N_q(\mathcal{F})$ of $\mathbb{F}_q$-rational points on $\mathcal{F}$. For the remaining Fermat curves, nice upper bounds for $N_q(\mathcal{F})$ are immediately given by the Stöhr-Voloch Theory.

1 Introduction

Let $\mathbb{F}_q$ be the finite field with $q = p^h$ elements. For an irreducible Fermat curve

$$\mathcal{F} : aX^n + bY^n = Z^n \tag{1.1}$$

defined over $\mathbb{F}_q$, let $N_q(\mathcal{F})$ denote its number of $\mathbb{F}_q$-rational points. The celebrated Hasse-Weil Theorem gives

$$|N_q(\mathcal{F}) - (q+1)| \leq (n-1)(n-2)\sqrt{q}. \tag{1.2}$$

Estimating the number $N_q(\mathcal{F})$ is a classical problem of broad interest, with well-known applications in a range of different areas, such as coding theory, finite geometry, additive combinatorics, Waring's problem over finite fields and exponential sums, see e.g. [2], [3], [5], [9], [10], [13].

In 1986, Stöhr and Voloch introduced a new technique to bound the number of rational points on curves over finite fields [14] . Their method uses some data collected from embeddings of the curve in projective spaces, and in many circumstances it gives improvements upon the Hasse-Weil bound.

For example, let $\mathcal{F}$ be a Fermat curve as given in (1.1). For $s \in \{1, \ldots, n-1\}$, consider the linear system Σ_s of all curves in $\mathbb{P}^2(\overline{\mathbb{F}}_q)$ of degree s. Associated to Σ_s, there exists a sequence of $M = \binom{s+2}{2} - 1$ integers $0 = \nu_0 < \cdots < \nu_{M-1}$, depending on $\mathcal{F}$, q and s, called the $\mathbb{F}_q$-Frobenius order-sequence of $\mathcal{F}$

(see Section 2). If $\nu_i = i$ for all $i = 0, \ldots, M-1$, then the curve $\mathcal{F}$ is called $\mathbb{F}_q$-Frobenius classical with respect to Σ_s. Otherwise, $\mathcal{F}$ is called $\mathbb{F}_q$-Frobenius nonclassical. Together with [14, Proposition 2.4] and some remarks in Section 3 of [14], the Stöhr-Voloch Theorem [14, Theorem 2.13] applied to Σ_s gives

$$N_q(\mathcal{F}) \leq \frac{n(n-3)(\nu_1 + \cdots + \nu_{M-1}) + sn(q+M)}{M} - \sum_{P \in \mathcal{F}} \frac{A(P)}{M}, \tag{1.3}$$

where

$$A(P) = \begin{cases} \sum_{l=1}^{M} (j_l - \nu_{l-1}) - M, \text{ if } \quad P \text{ is an } \mathbb{F}_q\text{-rational point} \\ \sum_{l=1}^{M-1} (j_l - \nu_l), \text{ otherwise }, \end{cases}$$

and $0 = j_0 < j_1 < \cdots < j_M$ are the (Σ_s, P)-orders (see Section 2).

If $\mathcal{F}$ is $\mathbb{F}_q$-Frobenius classical with respect to Σ_s, then bound (1.3) reads (cf. [5, Theorem 1])

$$N_q(\mathcal{F}) \leq \frac{n(n-3)(M-1)}{2} + \frac{sn(q+M)}{M} - \frac{3nA + dB}{M}, \tag{1.4}$$

where $B = sn - M$,

$$A = \frac{1}{6}\left((n-s-1)s(s-1)(s+4) + \frac{s(s-1)(s-2)(s+5)}{4}\right),$$

and d is the number of $\mathbb{F}_q$-rational points $P = (u : v : w) \in \mathcal{F}$ for which $uvw = 0$. For instance, with the usual assumption that $n|q-1$, we have $N_q(\mathcal{F}) \equiv d \mod n^2$, and then for $n \geq 3$ bound (1.4) when $s = 1$ and $s = 2$ yields

$$N_q(\mathcal{F}) \leq \left\lfloor \frac{n+q-d-1}{2n} \right\rfloor n^2 + d \leq \left\lfloor \frac{1+t}{2} \right\rfloor n^2, \tag{1.5}$$

and

$$N_q(\mathcal{F}) \leq \left\lfloor \frac{2(2n+q-d-1)}{5n} \right\rfloor n^2 + d \leq \left\lfloor \frac{4+2t}{5} \right\rfloor n^2, \tag{1.6}$$

respectively, where $\lfloor e \rfloor$ denotes the integer part of e, and $t = (q-1)/n$.

The $\mathbb{F}_q$-Frobenius nonclassical Fermat curves with respect to Σ_s were completely characterized by Garcia and Voloch for the cases $s = 1$ and $s = 2$ (see Theorems 2.7 and 2.8). Later on, other authors obtained results that rely on these characterizations to some extent, see e.g. [2],[6] and [8]. It should be observed, for instance, that bound (1.6) was fundamental to prove the main result of [2, Section 2], which answers a question (raised by Voloch) regarding the arc property of certain curves. This latter subject, in turn, has a well-known close connection with 3-dimensional linear codes.

Th following is another important result obtained by Garcia and Voloch after a suitable choice of s for the bound (1.4), see [5, Section 3].

Lemma 1.1. *Let p be a prime and $a \in \mathbb{F}_p^*$. If $n \geq \sqrt[4]{p-1} + \frac{1}{2}$ is a proper divisor of $p-1$, then the number of solutions $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ of $x^n + y^n = a$ is at most $4t^{2/3}n^2$, where $t = (p-1)/n$.*

The above lemma, improved by Mattarei by bringing the constant 4 down to $3 \cdot 2^{-2/3}$ [10], has been used to refine results on some problems, such as Waring's problem over finite fields and Exponential sums, see e.g. [3], [13]. Naturally, any improvement/extension of Lemma 1.1 will be of interest. One way to achieve this is by explicitly characterizing the curves which are $\mathbb{F}_q$-Frobenius nonclassical w.r.t. curves of higher degree s. For instance, thanks to Theorem 2.8, we know exactly which Fermat curves are $\mathbb{F}_q$-Frobenius nonclassical when $s = 2$, and then bound (1.6) may be used for all remaining Fermat curves. It turns out that for such remaining curves, at least in a set of small values $t = \frac{p-1}{n}$, bound (1.6) may be better than that of Lemma 1.1, besides holding for nonprime fields as well. As a illustration, let N be the number of solutions $(x, y) \in \mathbb{F}_{71} \times \mathbb{F}_{71}$ of $x^7 + y^7 = 1$. From Theorem 2.8 , this curve is $\mathbb{F}_{71}$-Frobenius classical for $s = 2$, and then bound (1.6) (in the weaker version) yields $N \leq 196$, whereas Lemma 1.1 (Mattarei's version) gives $N \leq 429$.

In general, for large values of $\frac{q-1}{n}$, bound (1.6) will become stronger as s approaches, roughly, $(\frac{q-1}{n})^{1/3}$ (see e.g. proof of Lemma 1.1 in [5]). Note that the bound for the case $s = 3$, namely

$$N_q(\mathcal{F}) \leq \left\lfloor \frac{5n + q - d - 1}{3n} \right\rfloor n^2 + d \leq \left\lfloor \frac{5 + t}{3} \right\rfloor n^2, \tag{1.7}$$

is better than that of $s = 2$ when, roughly, $t = \frac{q-1}{n} > 13$. However, to make use of it, one must make sure that the target Fermat curve is $\mathbb{F}_q$-Frobenius classical w.r.t. Σ_3.

With regard to $N_q(\mathcal{F})$ when $\mathcal{F}$ is $\mathbb{F}_q$-Frobenius nonclassical, note that in (1.3) we will have

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

and then bound (1.4) may not hold. This suggests that such curves are likely to have many $\mathbb{F}_q$-rational points. For instance, the Hermitian curve

$$\mathcal{H} : x^{q+1} + y^{q+1} = z^{q+1},$$

which is the most famous $\mathbb{F}_{q^2}$-maximal curve, turns out to be $\mathbb{F}_{q^2}$-Frobenius nonclassical w.r.t. Σ_1. Note that since $N_{q^2}(\mathcal{H}) = 1 + q^3$, bound (1.5) fails for $\mathcal{H}$. This example should reminds us to consider Frobenius noncassical curves when searching for curves with many rational points.

The characterization of $\mathbb{F}_q$-Frobenius nonclassical curves may offer a two-fold benefit. If we can identify the $\mathbb{F}_q$-Frobenius nonclassical curves, then we are left with a class of curves for which a better upper bound (inequality (1.4)) for the number of $\mathbb{F}_q$-rational points holds. At the same time, the $\mathbb{F}_q$-Frobenius nonclassical curves provide a potential source of curves with many such points. In a nutshell, the characterization of $\mathbb{F}_q$-Frobenius nonclassical curves for larger values of $s \in \{1, 2, \cdots, n-1\}$ is highly

desirable.

In this manuscript, we establish the result for $s = 3$. That is, we characterize the $\mathbb{F}_q$-Frobenius nonclassical Fermat curves with respect to the linear systems of plane cubics. Our main result is the following:

Theorem 1.2. *Let $\mathcal{F} : aX^n + bY^n = Z^n$ be an irreducible Fermat curve defined over $\mathbb{F}_q$, where $q = p^h$, $p > 11$, and $n > 3$. Suppose that $\mathcal{F}$ is classical with respect to Σ_2. Then the curve $\mathcal{F}$ is $\mathbb{F}_q$-Frobenius nonclassical with respect to Σ_3 if and only if one of the following holds:*

(i) *$p|n-3$ and $n = \frac{3(p^h-1)}{p^r-1}$ for some $r < h$ such that $r|h$ and $a, b \in \mathbb{F}_{p^r}$.*

(ii) *$p|3n-1$ and $n = \frac{p^h-1}{3(p^r-1)}$ for some $r < h$ such that $r|h$ and $a^3, b^3 \in \mathbb{F}_{p^r}$.*

The exact number of $\mathbb{F}_q$-rational points on the curves given by the previous theorem will be presented later in section 5. Now, given Theorem 1.2, one can apply bound (1.7) for all remaining Fermat curves. For instance, for the curve

$$\mathcal{F} : X^8 + Y^8 + 1 = 0$$

over $\mathbb{F}_{13^2}$, bound (1.7) gives $N_{13^2}(\mathcal{F}) \leq 512$, and one can easily check that the bound is sharp for this particular case, i.e., 512 is the actual value of $N_{13^2}(\mathcal{F})$. Note that since the field is not prime, Lemma 1.1 cannot be applied to this case.

It is worth mentioning that some techniques applied here can be carried over to larger values of s, and thereby shed some light on the solution of this problem for the general linear system Σ_s (see Section 6).

The paper is organized as follows. Section 2 sets some notation and recalls results from the Stöhr-Voloch Theory. Section 3 provides necessary and sufficient conditions for the curve $\mathcal{F}$ to be nonclassical with respect to Σ_3. In particular, it answers a question raised by Garcia and Voloch in [5]. Section 4 presents a sequence of additional results culminating in the proof of Theorem 1.2. Section 5 determines the number of $\mathbb{F}_q$-rational points on curves given by Theorem 1.2 and provides some examples. Finally, Section 6 briefly discuss how the current approach can help investigating the problem for larger values of s. In the paper's appendix, we prove the irreducibility of some low-degree curves, and include a proof for a case of Frobenius nonclassicality with respect to Σ_2 which was apparently overlooked in [5]. An unpublished but very useful result, due to M. Homma and S. J. Kim, is also included in the appendix.

Notation

Hereafter, we use the following notation:

- $\mathbb{F}_q$ is the finite field with $q = p^h$ elements, with $h \geq 1$, for a prime integer p.
- $\overline{\mathbb{F}}_q$ is the algebraic closure of $\mathbb{F}_q$.

- Given an irreducible curve $\mathcal{C}$ over $\mathbb{F}_q$ and an algebraic extension $\mathbb{H}$ of $\mathbb{F}_q$, the function field of $\mathcal{C}$ over $\mathbb{H}$ is denoted by $\mathbb{H}(\mathcal{C})$.
- For a curve $\mathcal{C}$ and $r > 0$, the set of its $\mathbb{F}_{q^r}$-rational points is denoted by $\mathcal{C}(\mathbb{F}_{q^r})$.
- $N_{q^r}(\mathcal{C})$ is the number of $\mathbb{F}_{q^r}$-rational points of the curve $\mathcal{C}$.
- For a nonsingular point $P \in \mathcal{C}$, the discrete valuation at P is denoted by v_P.
- For two plane curves $\mathcal{C}_1$ and $\mathcal{C}_2$, the intersection multiplicity of $\mathcal{C}_1$ and $\mathcal{C}_2$ at the point P is denoted by $I(P, \mathcal{C}_1 \cap \mathcal{C}_2)$.
- Given $g \in \overline{\mathbb{F}}_q(\mathcal{C})$, t a separating variable of $\overline{\mathbb{F}}_q(\mathcal{C})$, and $r \geq 0$, the r-th Hasse derivative of g with respect to t is denoted by $D_t^{(r)}g$.

2 Preliminaries

Let us start by recalling the main results of [5] and [14]. For $n > 3$, consider an irreducible Fermat curve

$$\mathcal{F} : aX^n + bY^n = Z^n \tag{2.1}$$

defined over $\mathbb{F}_q$. For each $s \in \{1, \ldots, n-1\}$, denote by Σ_s the linear system of all projective plane curves of degree s. For any point $P \in \mathcal{F}$, an integer $j := j(P)$ is called a (Σ_s, P)-order if there exists a plane curve of degree s, say $\mathcal{C}_P$, such that $I(P, \mathcal{F} \cap \mathcal{C}_P) = j$. From the discussion in [14, Section 1], it follows that there exist exactly $M + 1$ (Σ_s, P)-orders

$$j_0(P) < j_1(P) < \cdots < j_M(P),$$

where $M = \binom{s+2}{2} - 1$. The sequence $(j_0(P), j_1(P), \ldots, j_M(P))$ is called (Σ_s, P)-order sequence. Note that $j_0(P) = 0$ and $j_1(P) = 1$ for all $P \in \mathcal{F}$. Moreover, there exists a unique curve $\mathcal{H}_P$ of degree s, called s-osculating curve of $\mathcal{F}$ at P, such that $I(P, \mathcal{F} \cap \mathcal{H}_P) = j_M(P)$ [14, Theorem 1.1]. All but finitely many points of $\mathcal{F}$ have the same order sequence, denoted by $(\varepsilon_0, \ldots, \varepsilon_M)$. This sequence is called order sequence of $\mathcal{F}$ w.r.t. Σ_s, and the integers ε_i are called Σ_s-orders.

Let $\overline{\mathbb{F}}_q(\mathcal{F}) = \overline{\mathbb{F}}_q(x, y)$ be the function field of $\mathcal{F}$, defined by $ax^n + by^n = 1$. To each linear series Σ_s, there corresponds a morphism

$$\phi_s = (\ldots : x^i y^j : \ldots) : \mathcal{F} \longrightarrow \mathbb{P}^M(\overline{\mathbb{F}}_q), \tag{2.2}$$

where $i + j \leq s$, called the s-Veronese morphism. Let t be a separating variable of $\overline{\mathbb{F}}_q(\mathcal{F})$ and $D_t^{(i)}$ denote the i-th Hasse derivative with respect to t. The Σ_s-orders of $\mathcal{F}$ can also be defined as the minimal

sequence with respect to the lexicographic order, for which the function

$$\det\left(D_t^{(\varepsilon_k)}(x^i y^j)\right)_{\substack{0\le k\le M,\\ 0\le i+j\le s}}$$

is nonvanishing. Moreover, this minimality implies that $\varepsilon_i \le j_i(P)$ for all $i \in \{0,\dots,M\}$ and $P \in \mathcal{F}$. The curve $\mathcal{F}$ is called classical w.r.t. Σ_s (or ϕ_s) if the sequence $(\varepsilon_0,\dots,\varepsilon_M)$ is $(0,\dots,M)$. Otherwise, it is called nonclassical.

The following result concerning Σ_s-orders is proved in [14, Corollary 1.9].

Theorem 2.1. *Let ε be a Σ_s-order. Then every integer μ such that*

$$\binom{\varepsilon}{\mu} \not\equiv 0 \mod p$$

is also a Σ_s-order. In particular, if $\varepsilon < p$, then $0,1,\dots,\varepsilon-1$ are Σ_s-orders.

The following is a significant criterion for determining whether $\mathcal{F}$ is classical (see [14, Proposition 1.7]).

Proposition 2.2. *Let $P \in \mathcal{F}$ be a point with order sequence $(j_0(P),\dots,j_M(P))$. If the integer*

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

is not divisible by p, then $\mathcal{F}$ is classical w.r.t. Σ_s.

The following result, concerning the elements of the order sequences, is given in [4, Proposition 2].

Proposition 2.3. *Let $\varepsilon_0 < \varepsilon_1 < \cdots < \varepsilon_M$ be the orders of $\mathcal{F}$ w.r.t. Σ_s. Suppose $p \ge M$ and $\varepsilon_i = i$ for $i = 0,1,\dots,M-1$. If $\varepsilon_M > M$, then ε_M is a power of p.*

From a Pardini's result [12], we know that the Fermat curve $\mathcal{F}$ is nonclassical w.r.t. Σ_1 if and only if p divides $n-1$, provided that $p > 2$. In [4, Theorem 3], Garcia and Voloch gave a similar complete characterization of the nonclassical Fermat curves w.r.t. conics:

Theorem 2.4. *Suppose $p > 5$. The Fermat curve $\mathcal{F}$ is nonclassical w.r.t. Σ_2 if and only if*

$$p \text{ divides } (n-2)(n-1)(n+1)(2n-1).$$

Let us recall that there exists a sequence of non-negative integers $(\nu_0,\dots,\nu_{M-1})$, chosen minimally

in the lexicographic order, such that

$$\begin{vmatrix} 1 & x^q & y^q & \dots & (x^iy^j)^q & \dots & (y^s)^q \\ D_t^{(\nu_0)}1 & D_t^{(\nu_0)}x & D_t^{(\nu_0)}y & \dots & D_t^{(\nu_0)}x^iy^j & \dots & D_t^{(\nu_0)}y^s \\ \vdots & \vdots & \vdots & \cdots & \vdots & \cdots & \vdots \\ D_t^{(\nu_{M-1})}1 & D_t^{(\nu_{M-1})}x & D_t^{(\nu_{M-1})}y & \cdots & D_t^{(\nu_{M-1})}x^iy^j & \dots & D_t^{(\nu_{M-1})}y^s \end{vmatrix} \neq 0, \tag{2.3}$$

where t is a separating variable of $\mathbb{F}_q(\mathcal{F})$ [14, Proposition 2.1]. This sequence is called the $\mathbb{F}_q$-Frobenius order sequence of $\mathcal{F}$ w.r.t. Σ_s. It turns out that $\{\nu_0, \dots, \nu_{M-1}\} = \{\varepsilon_0, \dots, \varepsilon_M\}\backslash\{\varepsilon_I\}$ for some $I \in \{1, \dots, M\}$ [14, Proposition 2.1]. If $(\nu_0, \dots, \nu_{M-1}) = (0, \dots, M-1)$, then the curve $\mathcal{F}$ is called $\mathbb{F}_q$-Frobenius classical w.r.t. Σ_s. Otherwise, it is called $\mathbb{F}_q$-Frobenius nonclassical.

The following result establishes a close relation between classicality and $\mathbb{F}_q$-Frobenius classicality, see [7, Remark 8.52].

Proposition 2.5. *Assume $p > M$. If $\mathcal{F}$ is $\mathbb{F}_q$-Frobenius nonclassical w.r.t. Σ_s, then $\mathcal{F}$ is nonclassical w.r.t. Σ_s.*

The $\mathbb{F}_q$-Frobenius map Φ_q is defined on $\mathcal{F}$ by

$$\begin{array}{rccc} \Phi_q : & \mathcal{F} & \longrightarrow & \mathcal{F} \\ & (a_0 : a_1 : a_2) & \longmapsto & (a_0^q : a_1^q : a_2^q). \end{array}$$

Note that by (2.3) and [14, Corollary 1.3], we have that $\mathcal{F}$ is $\mathbb{F}_q$-Frobenius nonclassical w.r.t. Σ_1 if and only if $\Phi_q(P)$ lies on the tangent line of $\mathcal{F}$ at P for all $P \in \mathcal{F}$. More generally, (2.3) and [14, Corollary 1.3] give the following:

Proposition 2.6. *Suppose the order sequence $(\varepsilon_0, \dots, \varepsilon_M)$ of $\mathcal{F}$ w.r.t. Σ_s is such that $\varepsilon_i = i$ for $i = 0, 1, \dots, M-1$. Let $\Phi_q : \mathcal{F} \to \mathcal{F}$ be the $\mathbb{F}_q$-Frobenius map, and for any point $P \in \mathcal{F}$, let $\mathcal{H}_P$ be the s-osculating curve to $\mathcal{F}$ at P. Then $\mathcal{F}$ is $\mathbb{F}_q$-Frobenius nonclassical w.r.t. Σ_s if and only if $\Phi_q(P) \in \mathcal{H}_P$ for infinitely many points $P \in \mathcal{F}$.*

With regard to the $\mathbb{F}_q$-Frobenius classicality of $\mathcal{F}$ in the cases $s = 1$ and $s = 2$, the following results were proved [5].

Theorem 2.7 (Garcia-Voloch)**.** *Suppose that $p > 2$ and let $q = p^h$. Then $\mathcal{F}$ is $\mathbb{F}_q$-Frobenius nonclassical w.r.t. Σ_1 if and only if $n = (q-1)/(p^r-1)$ for some integer $r < h$ with $r|h$ and $a, b \in \mathbb{F}_{p^r}$.*

Theorem 2.8 (Garcia-Voloch)**.** *Suppose that $p > 5$ and let $q = p^h$. Then $\mathcal{F}$ is $\mathbb{F}_q$-Frobenius nonclassical w.r.t. Σ_2 if and only if one of the following holds.*

(i) $p|(n-1)$.

(ii) $p|(n-2)$ *and* $n = \frac{2(q-1)}{p^r-1}$ *with $r < h$ such that $r|h$ and $a, b \in \mathbb{F}_{p^r}$.*

(iii) $p|(2n-1)$ *and* $n=\frac{q-1}{2(p^r-1)}$ *with* $r<h$ *such that* $r|h$ *and* $a^2,b^2\in\mathbb{F}_{p^r}$.

(iv) $q=n+1$ *and* $a+b=1$.

Remark 2.9. *Item (iv) of Theorem 2.8 is a minor case that was apparently overlooked in [5]. A proof of it is included in the appendix.*

The following result (see [9, Theorem 1.1] or [7, Remark 8.109]) will be used to compute the number of $\mathbb{F}_q$-rational points of certain Fermat curves in Section 5.

Theorem 2.10 (Korchmáros-Szönyi)**.** *Let* $\mathcal{F}: X^n+Y^n+Z^n=0$ *and* $q=p^r$. *Suppose that* n *divides* $\frac{q^m-1}{q-1}$, *where* $m>1$. *Let* t *be defined by* $q\equiv t \mod \frac{q^m-1}{n(q-1)}$ *and* $0<t<\frac{q^m-1}{n(q-1)}$. *If* $l=\gcd\left(\frac{q^m-1}{n(q-1)},t+1\right)$, *then*

$$N_{q^m}(\mathcal{F})=3n+n^2(q-2)+n^2(l-1)(l-2)$$

provided that

$$p>\left(\frac{2}{\sqrt[t+1]{\sin\left(\frac{n(q-1)\pi}{2(q^m-1)}\right)}}+1\right)^{(t-1)\left(\frac{q^m-1}{n(q-1)}-l\right)}.$$

3 Classicality of $\mathcal{F}$ with respect to cubics

Let us recall that $\mathcal{F}: aX^n+bY^n=Z^n$ is an irreducible curve defined over $\mathbb{F}_q$. Based on Proposition 2.5, the study of $\mathbb{F}_q$-Frobenius nonclassicality of $\mathcal{F}$ w.r.t. Σ_s, can benefit directly from the study of nonclassicality of $\mathcal{F}$. In this section, we establish necessary and sufficient conditions for $\mathcal{F}$ to be nonclassical w.r.t. Σ_3.

Remark 3.1. *As mentioned in Section 2, for any point* $P\in\mathcal{F}$, *the number of distinct* (Σ_s,P)*-orders is* $\binom{s+2}{2}$. *In particular, there exist* 10 *distinct* (Σ_3,P)*-orders.*

Note that if $p>3$ and the curve $\mathcal{F}$ is nonclassical w.r.t. lines, then it is also nonclassical and $\mathbb{F}_q$-Frobenius nonclassical w.r.t. conics. Indeed assume that the order sequence of $\mathcal{F}$ for Σ_1 is $(0,1,\varepsilon)$ with $\varepsilon>3$. Thus, considering the conics given by the union of two of these lines, we have that $0,1,2,\varepsilon,\varepsilon+1$, and 2ε comprise the 6 distinct Σ_2-orders (cf. Remark 3.1). Also, since

$$\{\nu_0,\nu_1,\nu_2,\nu_3,\nu_4\}\subseteq\{0,1,2,\varepsilon,\varepsilon+1,2\varepsilon\},$$

we have $\nu_3>3$, and then $\mathcal{F}$ is $\mathbb{F}_q$-Frobenius nonclassical. Similarly, one can see that if $p>3$ and $\mathcal{F}$ is nonclassical w.r.t. lines, then it is also nonclassical w.r.t. cubics.

Now assume that $p>7$ and that $\mathcal{F}$ is classical w.r.t. Σ_1 but nonclassical w.r.t. Σ_2. Then, by Proposition 2.3, the order sequence of $\mathcal{F}$ w.r.t. Σ_2 is $(0,1,2,3,4,p^r)$, for some integer $r>0$. Considering all possible unions of a conic and a line, we have that the order sequence of $\mathcal{F}$ w.r.t. Σ_3 is

$(0, 1, 2, 3, 4, 5, 6, p^r, p^r + 1, p^r + 2)$. Therefore, $\mathcal{F}$ is nonclassical w.r.t. Σ_3, and since $\nu_7 > 7$, $\mathcal{F}$ is also $\mathbb{F}_q$-Frobenius nonclassical w.r.t. Σ_3. The next lemma summarizes the above discussion.

Lemma 3.2. *Suppose $p > 7$. If $\mathcal{F}$ is nonclassical w.r.t. either Σ_1 or Σ_2, then $\mathcal{F}$ is nonclassical and $\mathbb{F}_q$-Frobenius nonclassical w.r.t. Σ_3.*

The following result, which will be a critical factor in our approach, extends [11, Lemma 1.3.8]. Its proof, which was provided by M. Homma and S. J. Kim in a private communication, can be found in the appendix.

Lemma 3.3 (Homma-Kim)**.** *Let S be a surface defined over an algebraically closed field K, and let $P \in S$ be a nonsingular point. If C, D_1 and D_2 are effective divisors, of which no two have a common component, and P is a nonsingular point of C, then*

$$I(D_1.D_2, P) \geq min\{I(C.D_1, P), I(C.D_2, P)\}.$$

The following sequence of preliminary results will lead us to the characterization of nonclassical Fermat curves w.r.t. Σ_3. For more generality, we refer to Section 6. Since a curve's classicality is a geometric property, for this section it is assumed that $a = b = 1$.

Lemma 3.4. *Assume $p > 7$. Let $\overline{\mathbb{F}}_q(x, y)$ be the function field of $\mathcal{F}$, and $P = (u : v : 1) \in \mathcal{F}$ be a generic point. Suppose that there exists a polynomial $G(X, Y) = \sum a_{ij}(x, y)^p X^i Y^j \in \overline{\mathbb{F}}_q[x, y][X, Y]$ of degree $d \geq 3$ such that $G(x, y) = 0$. For $G_P(X, Y) := \sum a_{ij}(u, v)^p X^i Y^j \in \overline{\mathbb{F}}_q[X, Y]$, the following holds:*

(a) *If $G_P(X, Y)$ is irreducible of degree $d = 3$, then $\mathcal{F}$ is nonclassical w.r.t. Σ_3 and the curve $\mathcal{G}_P : G_P(X, Y) = 0$ is the osculating cubic to $\mathcal{F}$ at P.*

(b) *If the curve $\mathcal{G}_P : G_P(X, Y) = 0$ is such that $I(P, \mathcal{G}_P \cap \mathcal{C}) < p$ for every cubic $\mathcal{C}$, then $\mathcal{F}$ is classical w.r.t. Σ_3.*

Proof. Let $\mathcal{G}_P$ be the curve defined by $G_P(X, Y) = 0$. Since

$$\begin{aligned} G_P(x, y) &= G_P(x, y) - G(x, y) \\ &= \sum (a_{ij}(u, v) - a_{ij}(x, y))^p x^i y^j, \end{aligned}$$

it follows that $v_P(G_P(x, y)) \geq p$, that is,

$$I(P, \mathcal{F} \cap \mathcal{G}_P) \geq p. \tag{3.1}$$

Let $\mathcal{H}_P$ be the osculating cubic to $\mathcal{F}$ at P. For assertion (a), note that $\deg(\mathcal{G}_P) = 3$ and inequality (3.1) imply $(P, \mathcal{F} \cap \mathcal{H}_P) \geq p$, and then Lemma 3.3 gives

$$I(P, \mathcal{H}_P \cap \mathcal{G}_P) \geq p > 9 = \deg(\mathcal{H}_P) \cdot \deg(\mathcal{G}_P).$$

Thus, by Bézout's theorem, $\mathcal{G}_P$ and $\mathcal{H}_P$ must be the same curve, and since P is generic the result follows. Assertion (b) follows directly from Lemma 3.3 and from the fact that the nonclassicality of $\mathcal{F}$ w.r.t. Σ_3 implies $I(P, \mathcal{F} \cap \mathcal{H}_P) \geq p$ (c.f. Theorem 2.1).

□

Remark 3.5. *Note that if $G_P(X,Y)$ is irreducible of degree $< p/3$, then, by Bézout's theorem, the conditions on Lemma 3.4(b) are fulfilled, i.e., $\mathcal{F}$ is classical w.r.t. Σ_3.*

Lemma 3.6. *If $p > 11$ divides $(n+2)(2n+1)(2n-3)(3n-2)$, then $\mathcal{F}$ is classical w.r.t. Σ_3.*

Proof. We first prove the result for $p > 17$.

Suppose $p|n+2$, and let $m, r > 0$ be integers such that $n = mp^r - 2$ and $p \nmid m$. It follows from $x^n + y^n = 1$ that $(x^n + y^n - 1)x^2y^2 = 0$, and then

$$(x^{mp^r})y^2 + (y^{mp^r})x^2 - x^2y^2 = 0.$$

Consider $P = (u : v : 1) \in \mathcal{F}$, with $uv \neq 0$, and set $\alpha = v^{mp^r}$ and $\beta = u^{mp^r}$. By Lemma A.1, the curve $\mathcal{G}_1 : \alpha X^2Z^2 + \beta Y^2Z^2 - X^2Y^2 = 0$ is irreducible. Therefore, Remark 3.5 implies that $\mathcal{F}$ is classical w.r.t. Σ_3. To address the cases $p|2n+1$ and $p|2n-3$, note that

$$\begin{aligned} x^n + y^n - 1 = 0 &\implies (x^n + y^n - 1)(x^n + y^n + 1)((x^n - y^n)^2 - 1) = 0 \\ &\implies x^{4n} - 2x^{2n}y^{2n} - 2x^{2n} + y^{4n} - 2y^{2n} + 1 = 0 \end{aligned}$$

yields

$$x^{2(2n+1)}y^2 - 2x^{2n+1}y^{2n+1}xy - 2x^{2n+1}xy^2 + y^{2(2n+1)}x^2 - 2y^{2n+1}x^2y + x^2y^2 = 0 \tag{3.2}$$

and

$$x^{2(2n-3)}x^6 - 2x^{2n-3}y^{2n-3}x^3y^3 - 2x^{2n-3}x^3 + y^{2(2n-3)}y^6 - 2y^{2n-3}y^3 + 1 = 0. \tag{3.3}$$

If $p|2n+1$, we consider integers $m, r > 0$ such that $2n+1 = mp^r$ and $p \nmid m$. Likewise, we write $2n-3 = mp^r$ for the case $p|2n-3$. Therefore (3.2) and (3.3) can be written as

$$(x^{2m})^{p^r}y^2 - 2(x^my^m)^{p^r}xy - 2(x^m)^{p^r}xy^2 + (y^{2m})^{p^r}x^2 - 2(y^m)^{p^r}x^2y + x^2y^2 = 0, \tag{3.4}$$

and

$$(x^{2m})^{p^r}x^6 + (y^{2m})^{p^r}y^6 - 2(x^m)^{p^r}x^3 - 2(y^m)^{p^r}y^3 - 2(x^my^m)^{p^r}x^3y^3 + 1 = 0, \tag{3.5}$$

respectively. In either case, we consider $P = (u : v : 1) \in \mathcal{F}$ such that $uv \neq 0$ and define $\alpha = u^{mp^r}$ and $\beta = v^{mp^r}$. The above equations give rise to the curves

$$\mathcal{G}_2 : \alpha^2Y^2Z^2 - 2\alpha\beta XYZ^2 - 2\alpha XY^2Z + \beta^2X^2Z^2 - 2\beta X^2YZ + X^2Y^2 = 0.$$

and

$$\mathcal{G}_3 : \alpha^2 X^6 + \beta^2 Y^6 + Z^6 - 2(\alpha X^3 Z^3 + \beta Y^3 Z^3 + \alpha\beta X^3 Y^3) = 0.$$

After scaling coordinates, it follows from Lemma A.1 that these curves are irreducible. Thus Remark 3.5 implies that $\mathcal{F}$ is classical w.r.t. Σ_3.

Finally, let us assume $p|3n-2$ and consider integers $m, r > 0$ such that $3n = mp^r + 2$ and $p \nmid m$. Thus

$$\begin{aligned} 1 = x^n + y^n &\implies 1 = (x^n + y^n)^3 \Longrightarrow 1 = x^{3n} + y^{3n} + 3x^n y^n \\ &\implies -27x^{3n}y^{3n} = (x^{3n} + y^{3n} - 1)^3 \\ &\implies -27(x^m y^m)^{p^r} x^2 y^2 = ((x^m)^{p^r} x^2 + (y^m)^{p^r} y^2 - 1)^3. \end{aligned}$$

Similarly to the previous cases, the latter equation gives rise to an irreducible curve (cf. Lemma A.1)

$$\mathcal{G}_4 : (\alpha X^2 + \beta Y^2 - Z^2)^3 + 27\alpha\beta X^2 Y^2 Z^2 = 0,$$

and then Remark 3.5 finishes the proof.

In all prior cases, since $p > 17$ and $\deg(\mathcal{G}_i) < p/3$ for each $i = 1, \ldots, 4$, Remark 3.5 is sufficient to prove the classicality $\mathcal{F}$ w.r.t. Σ_3. To address the cases $p \in \{13, 17\}$, the previous argument is slightly refined: note that using a suitable projective tranformation $(X : Y : Z) \mapsto (\lambda X : \lambda Y : Z)$, we can always choose a point $P_i = (u : u : 1) \in \mathcal{F}$ and a cubic $\mathcal{C}_i$ such that

$$I(P_i, \mathcal{G}_i \cap \mathcal{C}_i) = I(\tilde{P}_i, \tilde{\mathcal{G}}_i \cap \tilde{\mathcal{C}}_i) \in \{10, 12\},$$

where $\tilde{\mathcal{G}}_i, \tilde{\mathcal{C}}_i$ and $\tilde{P}_i$ are given by Lemma A.2. Since $\tilde{P}_i \in \tilde{\mathcal{G}}_i$ is a nonsingular point, then so is $P_i \in \mathcal{G}_i$. Now if there is another cubic $\mathcal{C}$ such that $I(P_i, \mathcal{G}_i \cap \mathcal{C}) \geq 10$, the by Lemma 3.3, $I(P_i, \mathcal{C}_i \cap \mathcal{C}) \geq 10$. This contradicts Bezout's Theorem as $\mathcal{C}_i \cong \tilde{C}_i$ is irreducible. Therefore,

$$I(P_i, \mathcal{G}_i \cap \mathcal{C}) \leq 12 < p$$

for all cubics $\mathcal{C}$, and then Lemma 3.4(b) gives the result.

□

Proposition 3.7. *If $p > 7$ divides $(n-3)(3n-1)$, then $\mathcal{F} : aX^n + bY^n = Z^n$ is nonclassical w.r.t. Σ_3. Moreover, for $P = (u : v : 1) \in \mathcal{F}$, $uv \neq 0$, the osculating cubic $\mathcal{H}_P$ to $\mathcal{F}$ at P is the irreducible curve $H_P(X, Y, Z) = 0$, where*

$$H_P(X,Y,Z) = \begin{cases} au^{n-3}X^3 + bv^{n-3}Y^3 - Z^3, & \text{if} \quad p \mid n-3 \\ (a^3u^{3n-1}X + b^3v^{3n-1}Y - Z)^3 + 27a^3b^3(uv)^{3n-1}XYZ, & \text{if} \quad p \mid 3n-1. \end{cases}$$

Proof. Suppose $p|n-3$, and let $m, r > 0$ be integers such that $n = mp^r + 3$ and $p \nmid m$. Note that for $G(X,Y) = ax^{mp^r}X^3 + by^{mp^r}Y^3 - 1$, we have $G(x,y) = 0$. Since $G_P(X,Y) := au^{mp^r}X^3 + bv^{mp^r}Y^3 - 1$ is irreducible of degree 3, Lemma 3.4(a) implies that $\mathcal{F}$ is nonclassical w.r.t. Σ_3 and $H_P(X,Y,Z) = 0$ is the osculating cubic to $\mathcal{F}$ at P.

For the case $p|3n-1$, note that $ax^n + by^n = 1$ implies

$$\begin{aligned} (ax^n + by^n)^3 &= 1 \Longrightarrow \\ a^3x^{3n} + b^3y^{3n} + 3abx^ny^n &= 1 \Longrightarrow \\ (a^3(x^m)^{p^r}x + b^3(y^m)^{p^r}y - 1)^3 &= -27a^3b^3(x^my^m)^{p^r}xy, \end{aligned} \tag{3.6}$$

where $m, r > 0$ are integers such that $3n = mp^r + 1$ and $p \nmid m$. That is, for $G(X,Y) := (a^3(x^m)^{p^r}X + b^3(y^m)^{p^r}Y - 1)^3 + 27a^3b^3(x^my^m)^{p^r}XY$, we have $G(x,y) = 0$. The irreducibility of $G_P(X,Y) := (a^3u^{3n-1}X + b^3v^{3n-1}Y - 1)^3 + 27a^3b^3(uv)^{3n-1}XY$ follows from that of $\tilde{\mathcal{G}}_4$ in Lemma A.1. Therefore, Lemma 3.4(a) gives the result.

□

Next we present the main result of this section.

Theorem 3.8. *If $p > 11$ then $\mathcal{F} : X^n + Y^n = Z^n$ is nonclassical w.r.t. Σ_3 if and only if*

$$p \text{ divides } (n-2)(n-1)(n+1)(2n-1)(n-3)(3n-1).$$

Proof. Suppose that $\mathcal{F}$ is nonclassical w.r.t. Σ_3. If $P = (u:0:1) \in \mathcal{F}(\overline{\mathbb{F}}_q)$, and ℓ_P is tangent line to $\mathcal{F}$ at P, then clearly $I(P, \mathcal{F} \cap \ell_P) = n$. Therefore, the (Σ_1, P)-order sequence is $(0,1,n)$, and then the (Σ_3, P)-order sequence is $(0,1,2,3,n,n+1,n+2,2n,2n+1,3n)$. Thus Proposition 2.2 implies that

$$p|(n-2)(n-1)(n+1)(2n-1)(3n-1)(n-3)(3n-2)(2n+1)(2n-3)(n+2).$$

From Lemma 3.6, we have that $p \nmid (3n-2)(2n+1)(2n-3)(n+2)$ and the result follows.

Conversely, suppose that $p|(n-2)(n-1)(n+1)(2n-1)(3n-1)(n-3)$. If $p|(n-2)(n-1)(n+1)(2n-1)$, then Theorem 2.4 implies that $\mathcal{F}$ is nonclassical w.r.t. Σ_2, and then $\mathcal{F}$ is nonclassical w.r.t. Σ_3 (cf. Lemma 3.2). The case $p|(3n-1)(n-3)$ follows from Lemma 3.7. □

Remark 3.9. *The restriction $p > 11$ in Theorem 3.8 cannot be dropped. To see this, consider the curve $\mathcal{F} : X^n + Y^n = Z^n$ over $\overline{\mathbb{F}}_{11}$ with $n \equiv -2 \mod 11$. For $P = (u:v:1) \in \mathcal{F}$ such that $uv \neq 0$, let $\mathcal{G}_1 : \alpha X^2Z^2 + \beta Y^2Z^2 - X^2Y^2 = 0$ be the irreducible curve as defined in the proof of Lemma 3.6. It can be checked that $\mathcal{G}_1$ is nonclassical w.r.t. Σ_3. That is, there exists a cubic $\mathcal{C}_P$ such that $I(P, \mathcal{G}_1 \cap \mathcal{C}_P) \geq 11$. Therefore, from Lemma 3.3, $I(P, \mathcal{F} \cap \mathcal{C}_P) \geq 11$. In other words, $11|n+2$, but the curve $\mathcal{F}$ is nonclassical w.r.t. Σ_3.*

Remark 3.10. *Assume $p > M$, and consider the Fermat curve $\mathcal{F} : x^n + y^n + 1 = 0$. Since the inflection points of $\mathcal{F}$ have (Σ_1, P)-order sequence $(0, 1, n)$, it follows from Proposition 2.2 that if $\mathcal{F}$ is nonclassical w.r.t. Σ_s, then p divides $\prod_{i=1}^{s}\prod_{t=-s}^{s-i}(in+t)$. In [4, Remark 5], Garcia and Voloch somewhat raised the question of whether or not the converse of this statement holds. Theorem 3.8 gives a negative answer: if $p|(3n-2)(2n+1)(2n-3)(n+2)$, then $\mathcal{F}$ is classical w.r.t. Σ_3.*

4 $\mathbb{F}_q$-Frobenius classicality of $\mathcal{F}$ with respect to cubics

In this section we provide the additional results that will lead us to the proof of Theorem 1.2. Henceforth, we consider the irreducible curve $\mathcal{F} : aX^n + bY^n = Z^n$, where $n > 3$ and $p > 7$.

Lemma 4.1. *If p divides $(n-3)(3n-1)$, then the following hold*

(a) *The order sequence of $\mathcal{F}$ w.r.t. Σ_3 is $(0, 1, 2, 3, 4, 5, 6, 7, 8, p^r)$, for some $r > 0$*

(b) *The curve $\mathcal{F}$ is $\mathbb{F}_q$-Frobenius nonclassical w.r.t. Σ_3 if and only if $\Phi_q(P) \in \mathcal{H}_P$ for infinitely many points $P \in \mathcal{F}$.*

Proof. Let $(\varepsilon_0, \ldots, \varepsilon_8, \varepsilon_9)$ be the order sequence of $\mathcal{F}$ w.r.t. Σ_3, and suppose that $\varepsilon_8 > 8$. Thus Theorem 2.1 implies $\varepsilon_8 \geq p$, and then $\varepsilon_9 > p$. Let $P \in \mathcal{F}$ be a Σ_3-ordinary point, that is, P is such that $j_i(P) = \varepsilon_i$ for all $i \in \{0, \ldots, 9\}$. Let $\mathcal{C}_P$ be a cubic for which $I(P, \mathcal{F} \cap \mathcal{C}_P) = \varepsilon_8 \geq p$ and let $\mathcal{H}_P$ be the osculating cubic to $\mathcal{F}$ at P. Note that $\mathcal{H}_P \neq \mathcal{C}_P$. Lemma 3.3 implies that

$$I(P, \mathcal{H}_P \cap \mathcal{C}_P) \geq p > 9 = \deg(\mathcal{H}_P) \cdot \deg(\mathcal{C}_P). \tag{4.1}$$

Thus by Bezout's Theorem the curves $\mathcal{H}_P$ and $\mathcal{C}_P$ have a common component. However, from Proposition 3.7, the osculating cubic $\mathcal{H}_P$ is irreducible. Therefore, $\mathcal{H}_P = \mathcal{C}_P$, a contradiction. Hence $\varepsilon_8 = 8$, and then $\varepsilon_i = i$ for all $i \leq 8$. Now it follows from Propositions 2.3 and 3.7 that $\varepsilon_9 = p^r$ for some $r > 0$. The second assertion follows directly from the first one together with Proposition 2.6.

□

The next result is straightforward.

Lemma 4.2. *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*

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

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

Proposition 4.3. *Suppose that p divides $n-3$. The curve $\mathcal{F}$ is $\mathbb{F}_q$-Frobenius nonclassical w.r.t. Σ_3 if and only if*

$$n = \frac{3(p^h - 1)}{p^r - 1}$$

for some $r < h$ such that $r|h$, and $a, b \in \mathbb{F}_{p^r}$.

Proof. By Lemma 4.1 $\mathcal{F}$ is $\mathbb{F}_q$-Frobenius nonclassical w.r.t. Σ_3 if and only if $\Phi(P) \in \mathcal{H}_P$ for infinitely many points $P \in \mathcal{F}$, where $\mathcal{H}_P$ denotes the osculating cubic to $\mathcal{F}$ at P. Thus Proposition 3.7 implies that this is equivalent to the function

$$ax^{n-3+3q} + by^{n-3+3q} - 1$$

being vanishing.

Therefore, seeing the functions as polynomials, $\mathcal{F}$ is $\mathbb{F}_q$-Frobenius nonclassical if and only if

$$y^n - \left(\frac{1}{b} - \frac{a}{b}x^n\right) \quad \text{divides} \quad y^{n+3(q-1)} - \left(\frac{1}{b} - \frac{a}{b}x^{n+3(q-1)}\right).$$

By Lemma 4.2, that means $n|n + 3(q-1)$ and

$$\left(\frac{1}{b} - \frac{a}{b}x^n\right)^{\frac{3(q-1)}{n}+1} = \frac{1}{b} - \frac{a}{b}x^{n+3(q-1)}. \tag{4.2}$$

Clearly equation (4.2) implies $\frac{3(q-1)}{n} + 1 = p^r$ for some $r > 0$, that is, $p^r - 1$ divides $3(p^h - 1)$. Since $n > 3$ and $p > 2$, it follows that $r < h$ and $r|h$. It is also clear that (4.2) gives $a, b \in \mathbb{F}_{p^r}$. Conversely, the latter conditions obviously imply equation (4.2), which completes the proof. □

Proposition 4.4. *Suppose that p divides $3n - 1$. The curve $\mathcal{F}$ is $\mathbb{F}_q$-Frobenius nonclassical w.r.t. Σ_3 if and only if*

$$n = \frac{p^h - 1}{3(p^r - 1)}$$

for some $r < h$ such that $r|h$, and $a^3, b^3 \in \mathbb{F}_{p^r}$.

Proof. As in the previous proof, by Lemma 4.1 and Proposition 3.7, the curve $\mathcal{F}$ is $\mathbb{F}_q$-Frobenius nonclassical w.r.t. Σ_3 if and only if the function

$$V := (a^3x^{3n-1+q} + b^3y^{3n-1+q} - 1)^3 + 27a^3b^3x^{3n-1+q}y^{3n-1+q} \tag{4.3}$$

is vanishing. Therefore, the condition $n = \frac{p^h-1}{3(p^r-1)}$, for some $r < h$ such that $r|h$, and $a^3, b^3 \in \mathbb{F}_{p^r}$ implies

$$V = \left((a^3x^{3n} + b^3y^{3n} - 1)^3 + (3abx^ny^n)^3\right)^{p^r}. \tag{4.4}$$

Using (4.4) to replace by^n by $1 - ax^n$ yields $V = 0$, which gives the result. Conversely, suppose $V = 0$. That is,

$$(a^3x^{3n+q-1} + b^3y^{3n+q-1} - 1)^3 + 27a^3b^3x^{3n+q-1}y^{3n+q-1} = (ax^n + by^n - 1)h(x, y) \tag{4.5}$$

for some $h(x,y) \in \mathbb{F}_q[x,y]\backslash\{0\}$. Evaluating both sides of (4.5) at $y=0$ yields

$$(a^3x^{3n+q-1}-1)^3 = (ax^n-1)h(x,0).$$

This implies that ax^n-1 divides $a^3x^{3n+q-1}-1$, and then $n \mid q-1$. Therefore, we may use (4.5) to replace y^n by $(1-ax^n)/b$, and then write

$$\Big(a^3x^{3n+q-1} + b^3(\frac{1-ax^n}{b})^{3+\frac{q-1}{n}} - 1\Big)^3 = -27a^3b^3x^{3n+q-1}(\frac{1-ax^n}{b})^{3+\frac{q-1}{n}}. \tag{4.6}$$

Since $(\frac{1-ax^n}{b})^{3+\frac{q-1}{n}}$ is a factor of both sides of (4.6), we conclude that $3n \mid q-1$.

Let r and t be integers such that $1+\frac{q-1}{3n} = p^rt$ and $p \nmid t$. From equation (4.6), we have

$$\Big(a^{\frac{3}{p^r}}x^{3nt} + b^{\frac{3}{p^r}}(\frac{1-ax^n}{b})^{3t} - 1\Big)^3 = -27(ab)^{\frac{3}{p^r}}x^{3nt}(\frac{1-ax^n}{b})^{3t}. \tag{4.7}$$

Now equation (4.7) implies that $(1-ax^n)^t$ is a factor of $a^{\frac{3}{p^r}}x^{3nt}-1$. Since the latter polynomial is separable, it follows that $t=1$. Hence $1+\frac{q-1}{3n} = p^r$, that is, $n = \frac{q-1}{3(p^r-1)}$. Moreover, using equation (4.7) to replace x^n by 0 and $1/a$, we obtain $b^3 \in \mathbb{F}_{p^r}$ and $a^3 \in \mathbb{F}_{p^r}$, respectively. This finishes the proof. □

Proof of Theorem 1.2: It follows directly from Theorems 2.4 and 3.8, and Propositions 4.3 and 4.4. □

5 The number of rational points

The possible values of $N_q(\mathcal{F})$ in the case of $\mathbb{F}_q$-Frobenius nonclassicality when $s=2$ are discussed in [5]. In this section, we determine $N_q(\mathcal{F})$ for the new curves in the case $s=3$, i.e., for those given by Theorem 1.2.

Theorem 5.1. *Suppose that* $n = \frac{3(p^h-1)}{p^r-1}$ *and* $a, b \in \mathbb{F}_{p^r}$.

(1) If $p^r \equiv 1 \mod 3$, *then*

$$N_q(\mathcal{F}) = \frac{n^2}{9}\Big(N_{p^r}(\mathcal{C}) - k\Big) + \frac{nk}{3},$$

where $\mathcal{C}$ *is the curve* $aX^3 + bY^3 = Z^3$ *defined over* $\mathbb{F}_{p^r}$, *and* $k := \#\{Q = (x_0 : x_1 : x_2) \in \mathcal{C}(\mathbb{F}_{p^r}) \mid x_0x_1x_2 = 0\}$.

(2) If $p^r \not\equiv 1 \mod 3$, *then* $N_q(\mathcal{F}) = \frac{n^2}{9}(p^r-2) + n$.

Proof. The map $\rho : \mathcal{F}(\mathbb{F}_q) \longrightarrow \mathcal{C}(\mathbb{F}_{p^r})$ given by $(x_0 : x_1 : x_2) \mapsto (x_0^{\frac{n}{3}} : x_1^{\frac{n}{3}} : x_2^{\frac{n}{3}})$ is clearly well defined. Since $x \mapsto x^{\frac{n}{3}}$ is the norm function of $\mathbb{F}_q$ onto $\mathbb{F}_{p^r}$, we have $\mathcal{F}(\mathbb{F}_q) = \bigcup_{Q\in\mathcal{C}(\mathbb{F}_{p^r})}\rho^{-1}(Q)$. Thus, setting $k := \#\{Q = (x_0 : x_1 : x_2) \in \mathcal{C}(\mathbb{F}_{p^r}) \mid x_0x_1x_2 = 0\}$, we arrive at

$$N_q(\mathcal{F}) = \Big(\frac{n}{3}\Big)^2\big(N_{p^r}(\mathcal{C}) - k\big) + \frac{n}{3}k,$$

which proves the first assertion.

Now note that in the case $p^r \not\equiv 1 \mod 3$, the map $\alpha \mapsto \alpha^3$ permutes $\mathbb{F}_{p^r}$, and then $k = 3$. Moreover, in this case, $N_{p^r}(\mathcal{C}) = p^r + 1$, which finishes the proof. □

Theorem 5.2. *If $n = \frac{p^h-1}{3(p^r-1)}$ and $a^3, b^3 \in \mathbb{F}_{p^r}$, then*

$$N_q(\mathcal{F}) = \begin{cases} 3n + n^2\big(p^r - 2\big), & \text{if} \quad p^r \equiv 1 \mod 3 \\ 3n + n^2 p^r, & \text{otherwise.} \end{cases}$$

Proof. Since $a^3, b^3 \in \mathbb{F}_{p^r}$, we may assume that $\mathcal{F}$ is defined by $X^n + Y^n + Z^n = 0$. Setting $m = h/r$, we obtain $\frac{(p^r)^m-1}{n(p^r-1)} = 3$. Thus the result follows from a direct application of Theorem 2.10, observing that:

- if $p^r \not\equiv 1 \mod 3$, then $t = 2$ and $l = 3$.
- if $p^r \equiv 1 \mod 3$, then $t = l = 1$.

□

Not surprisingly, using the two previous theorems, one can find examples of curves for which the upper bound (1.7) fails.

Example 5.3. *Consider the curve $\mathcal{F} : X^{294} + Y^{294} = Z^{294}$ over $\mathbb{F}_{97^2}$. Here $\mathcal{F}$ has degree $n = 3\frac{97^2-1}{97-1}$. The number of $\mathbb{F}_{97}$-rational points of the cubic $\mathcal{C} := X^3 + Y^3 = Z^3$ is $N_{97}(\mathcal{C}) = 117$. Thus Theorem 5.1 yields $N_{97^2}(\mathcal{F}) = 1038114$. Since, in this case, $d = 3n = 882$, it follows that $N_{97^2}(\mathcal{F})$ exceeds the upper bound in (1.7).*

Example 5.4. *Let $\mathcal{F}$ be the curve $X^8 + Y^8 + Z^8 = 0$ over $\mathbb{F}_{23^2}$. Since $\mathcal{F}$ has degree $n = \frac{23^2-1}{3(23-1)}$, it follows from Theorem 5.2 that $N_{23^2}(\mathcal{F}) = 1496$. One can check that $d = 24$, and then $N_{23^2}(\mathcal{F})$ exceeds the upper bound in (1.7).*

6 Remark on generalizations

In Section 3, we extensively used Lemma 3.4 to characterize the nonclassical Fermat curves $\mathcal{F} : aX^n + bY^n = Z^n$ w.r.t. Σ_3. To investigate the problem w.r.t. Σ_s for larger values of s, one may consider the following generalization of Lemma 3.4.

Lemma 6.1. *Assume $p > s^2$. Let $\overline{\mathbb{F}}_q(x, y)$ be the function field of $\mathcal{F}$, and $P = (u : v : 1) \in \mathcal{F}$ be a generic point. Suppose that there exists a polynomial $G(X, Y) = \sum a_{ij}(x, y)^p X^i Y^j \in \overline{\mathbb{F}}_q[x, y][X, Y]$ of degree $d \geq s$ such that $G(x, y) = 0$. For $G_P(X, Y) := \sum a_{ij}(u, v)^p X^i Y^j \in \overline{\mathbb{F}}_q[X, Y]$, the following holds:*

(a) *If $G_P(X, Y)$ is irreducible of degree $d = s$, then $\mathcal{F}$ is nonclassical w.r.t. Σ_s and $\mathcal{G}_P : G_P(X, Y) = 0$ is the s-osculating curve to $\mathcal{F}$ at P.*

(b) *If the curve $\mathcal{G}_P : G_P(X,Y) = 0$ is such that $I(P, \mathcal{G}_P \cap \mathcal{T}) < p$ for every curve $\mathcal{T}$ of degree s, then $\mathcal{F}$ is classical w.r.t. Σ_s.*

The proof this previous result is completely analogous the proof of Lemma 6.1. To illustrate its application in a general setting, in analogy to the case $p|n-3$, let us address the case $p|n-s$.

Proposition 6.2. *Let $s \in \{1, \ldots, n-1\}$. If $p > s^2$ divides $n-s$, then $\mathcal{F} : aX^n + bY^n = Z^n$ is nonclassical w.r.t. Σ_s. Moreover, for $P = (u : v : 1) \in \mathcal{F}$, $uv \neq 0$, the s-osculating curve $\mathcal{H}_P^s$ to $\mathcal{F}$ at P is the irreducible curve $H_P^s(X,Y,Z) = 0$, where $H_P^s(X,Y,Z) = au^{n-s}X^s + bv^{n-s}Y^s - Z^s$.*

Proof. Let m and r be positive integers such that $n = p^r m + s$, with $\gcd(m,p) = 1$. Then Lemma 6.1(a) applied to the polynomial $H(X,Y) = ax^{mp^r}X^s + by^{mp^r}Y^s - 1$ gives the result. □

Note that using Proposition 6.2 and arguing as in the proof of Lemma 4.1, we arrive at $(\varepsilon_1, \ldots, \varepsilon_{M-1}, \varepsilon_M) = (1, \ldots, M-1, p^r)$ for some $r > 0$ and $M = \binom{s+2}{2} - 1$. In fact, if $\varepsilon_{M-1} > M-1$, then Theorem 2.1 implies that $\varepsilon_{M-1} \geq p$. Thus, similarly to (4.1) in the proof of Lemma 4.1, we will reach a contradiction. Therefore, $\varepsilon_i = i$ for $i \leq M-1$, and then Propositions 2.3 and 6.2 will give $\varepsilon_M = p^r$. Now we can state the following:

Theorem 6.3. *Suppose that $p > s^2$ divides $n-s$. The curve $\mathcal{F}$ is $\mathbb{F}_q$-Frobenius nonclassical w.r.t. Σ_s if and only if*

$$n = \frac{s(p^h - 1)}{p^r - 1}$$

for some $r < h$ such that $r|h$, and $a, b \in \mathbb{F}_{p^r}$.

Proof. In view of the previous discussion and Propositions 2.6, 6.2, we have that $\mathcal{F}$ is $\mathbb{F}_q$-Frobenius nonclassical w.r.t. Σ_s if and only if the function $ax^{n-s+qs} + by^{n-s+qs} - 1$ is vanishing. Then, using Lemma 4.2 and arguing as in the proof of Proposition 4.3, we obtain the desired conclusion. □

Note that a complete investigation of the general problem requires looking at the remaining cases where $p|in+t$, with $1 \leq i \leq s$ and $-s \leq t \leq s-i$. In our case-by-case approach when $s = 3$, we often relied on the construction of some (preferably irreducible) auxiliary curve $\mathcal{G}$ of small degree, and then used Lemma 3.3 or Lemma 6.2. We point out that constructing such suitable curves $\mathcal{G}$ for each case $p|in+t$ is usually the tricky step to extend the characterization for larger values of s.

A Some irreducible curves

Lemma A.1. *If $p > 3$, then the following curves are irreducible over $\overline{\mathbb{F}}_q$:*

- $\tilde{\mathcal{G}}_1 : X^2Z^2 + Y^2Z^2 - X^2Y^2 = 0$
- $\tilde{\mathcal{G}}_2 : Y^2Z^2 + X^2Z^2 + X^2Y^2 - 2XYZ(X+Y+Z) = 0$
- $\tilde{\mathcal{G}}_3 : X^6 + Y^6 + Z^6 - 2(X^3Y^3 + X^3Z^3 + Y^3Z^3) = 0$

- $\tilde{\mathcal{G}}_4 : (X^2 + Y^2 - Z^2)^3 + 27X^2Y^2Z^2 = 0.$

Proof. The irreducibility of $\tilde{\mathcal{G}}_1$ and $\tilde{\mathcal{G}}_2$ follows from [1, Lemma A.1].

The proofs for the irreducibility of $\tilde{\mathcal{G}}_3$ and $\tilde{\mathcal{G}}_4$ are similar. Thus we will prove the latter case only.

For the curve $\tilde{\mathcal{G}}_4$, one can readily check that its set of singular points is given by $\mathscr{C} \cup \mathscr{N}$ where

$$\mathscr{C} = \{(0:1:1), (0:-1:1), (1:0:1), (-1:0:1), (i:1:0), (-i:1:0)\},$$

and

$$\mathscr{N} = \{(i:i:1), (i:-i:1), (-i:-i:1), (-i:i:1)\},$$

with $i^2 = -1$, are the sets of cusps and nodes of $\tilde{\mathcal{G}}_4$, respectively. We proceed to show that $\tilde{\mathcal{G}}_4$ has no component of degree ≤ 3. Note that the lines $x = 0, y = 0$ and $z = 0$ intersect $\tilde{\mathcal{G}}_4$ in pairs of cusps $\{P_1, P_2\}$, $\{Q_1, Q_2\}$ and $\{R_1, R_2\}$, whose union is $\mathscr{C}$. Therefore, any component of $\tilde{\mathcal{G}}_4$ must contain at least 3 points P_i, Q_j, R_k for some $(i, j, k) \in \{1, 2\}^3$. Since no choice of 3 such points will be collinear, the curve has no linear components.

Now assume $\tilde{\mathcal{G}}_4 = \mathcal{C} \cup \mathcal{Q}$, where $\mathcal{C}$ is a smooth conic and $\mathcal{Q}$ is an irreducible quartic. Since the quartic $\mathcal{Q}$ has at most 3 singularities, $\mathcal{C}$ and $\mathcal{Q}$ must intersect in at least 3 distinct cusps in $\mathscr{C}$. Thus, by Bézout's theorem, $\mathcal{C}$ and $\mathcal{Q}$ intersect in at most 5 distinct points, and then $\tilde{\mathcal{G}}_4$ has at most 8 singular points. This contradicts $\#(\mathscr{C} \cup \mathscr{N}) = 10$.

Suppose $\tilde{\mathcal{G}}_4$ is the union of 3 distinct smooth conics. By Bézout's theorem, the intersection of these conics yields 12 (counted with multiplicities) singular points of $\tilde{\mathcal{G}}_4$. Since all points of $\mathscr{C}$ are cusps, its 6 points must be counted at least twice. Thus all singular points of $\tilde{\mathcal{G}}_4$ lie in $\mathscr{C}$, a contradiction.

Finally, suppose that $\tilde{\mathcal{G}}_4$ is the union of 2 irreducible cubics. In the worst case scenario, each cubic has one cusp. Thus, similarly to the previous cases, the remaining 4 cusps will give rise to a counting contradiction. Therefore $\tilde{\mathcal{G}}_4$ is irreducible.

□

Lemma A.2. *Suppose $p \in \{13, 17\}$, and let $\tilde{\mathcal{G}}_i$ be the curves given by Lemma A.1. For each $i \in \{1, \ldots, 4\}$, there exist a nonsigular point $\tilde{P}_i = (s_i : s_i : 1) \in \tilde{\mathcal{G}}_i$ and a nonsingular cubic $\tilde{\mathcal{C}}_i$ such that*

$$I(\tilde{P}_i, \tilde{\mathcal{G}}_i \cap \tilde{\mathcal{C}}_i) \in \{10, 12\}$$

Proof. Due to its simple but computational nature, our proof will be limited to presenting each point $\tilde{P}_i = (s_i, s_i)$ and the corresponding cubic $\mathcal{C}_i$ in affine coordinates.

- $\tilde{P}_1 = (s, s)$ where $s^2 = 2$, and
  $\tilde{\mathcal{C}}_1 : x^3 + 1677x^2y - 1194sx^2 + 1677xy^2 - 1848sxy + 996x + y^3 - 1194sy^2 + 996y - 232s = 0.$

- $\tilde{P}_2 = (4,4)$, and
  $\tilde{\mathcal{C}}_2 : x^3 + 543x^2y - 672x^2 + 543xy^2 + 2112xy - 8448x + y^3 - 672y^2 - 8448y - 14336 = 0$

- $\tilde{P}_3 = (s,s)$ where $s^3 = 1/4$, and
  $\tilde{\mathcal{C}}_3 : 13x^3 + 27x^2y - 27sx^2 + 27xy^2 - 42sxy + 13y^3 - 27sy^2 + 4 = 0$

- $\tilde{P}_4 = (s,s)$ where $s^2 = 1/8$, and
  $\tilde{\mathcal{C}}_4 : 532x^3 + 804x^2y - 6216sx^2 + 804xy^2 - 9120sxy + 2841x + 532y^3 - 6216sy^2 + 2841y - 3322s = 0$

□

B Frobenius nonclassicality of $aX^{q-1} + (1-a)Y^{q-1} = Z^{q-1}$ with respect to conics

Theorem B.1. *Suppose $p > 5$ divides $n+1$. Then the Fermat curve $\mathcal{F} : aX^n + bY^n = Z^n$ is $\mathbb{F}_q$-Frobenius nonclassical w.r.t. Σ_2 if and only if $a + b = 1$ and $n = q - 1$.*

Proof. Set $x = X/Z$ and $y = Y/Z$, and let $\mathcal{F}(\overline{\mathbb{F}}_q) := \overline{\mathbb{F}}_q(x,y)$ be the function field of $\mathcal{F}$. If $\mathcal{F}$ is $\mathbb{F}_q$-Frobenius nonclassical, then it follows from the proof of ([5, Theorem 3]) that the function

$$G = x^q y^q - ax^{n+1}y^q - by^{n+1}x^q,$$

seen as a polynomial, must be identically zero. That is, $n + 1 = q$ and $a + b = 1$.

Conversely, suppose that $\mathcal{F}$ is given by $aX^{q-1} + (1-a)Y^{q-1} = Z^{q-1}$. Since $p \nmid n - 1$, it follows that $\mathcal{F}$ is classical w.r.t. Σ_1 [12, Corollary 2.2]. Thus the order sequence of $\mathcal{F}$ w.r.t. Σ_2 is $(0,1,2,3,4,\varepsilon)$ with $\varepsilon > 5$ ([4, Theorem 3]). Now, for $P = (u : v : 1) \in \mathcal{F}$, with $uv \neq 0$, we claim that the osculating conic to $\mathcal{F}$ at P has affine equation given by

$$\mathcal{C}_P : (au)^q Y + \big((1-a)v\big)^q X - XY = 0.$$

First note that $h(x,y) := (ax^{q-1} + (1-a)y^{q-1} - 1)xy = \big(ax\big)^q y + \big((1-a)y\big)^q x - xy = 0$. Setting

$$g(x,y) := (au)^q y + \big((1-a)v\big)^q x - xy,$$

it follows that

$$\begin{aligned} g(x,y) &= g(x,y) - h(x,y) \\ &= (au - ax)^q y + \big((1-a)v - (1-a)y\big)^q x, \end{aligned}$$

and then $v_P(g(x,y)) \geq q > 5$. That is, $(au)^q Y + \big((1-a)v\big)^q X - XY = 0$ is the osculating conic to $\mathcal{F}$ at $P = (u : v : 1)$.

Let $\Phi : \mathcal{F} \to \mathcal{F}$ be the $\mathbb{F}_q$-Frobenius map. Since $\mathcal{F}$ has order sequence $(0, 1, 2, 3, 4, \varepsilon)$, by Proposition 2.6 it is $\mathbb{F}_q$-Frobenius nonclassical w.r.t. Σ_2 if and only if the function

$$(ax)^q y^q + \big((1-a)y\big)^q x^q - x^q y^q$$

is vanishing. Thus the result follows. □

C Proof of Lemma 3.3

Proof. Let f, g, h be local equations of C, D_1, D_2 in $\mathcal{O}_{S,P}$, respectively. Then $I(D_1.D_2, P) = \dim_K \mathcal{O}_{S,P}/(g, h)$. Since $\mathcal{O}_{C,P} = \mathcal{O}_{S,P}/(f)$, the map $\mathcal{O}_{S,P}/(g, h) \to \mathcal{O}_{C,P}/(\overline{g}, \overline{h})$, where $\overline{g}$ and $\overline{h}$ are the images of f and g in $\mathcal{O}_{C,P}$, is surjective. Hence,

$$I(D_1.D_2, P) \geq \dim_K \mathcal{O}_{C,P}/(\overline{g}, \overline{h}). \tag{C.1}$$

On the other hand,

$$\begin{aligned} I(C.D_1, P) &= \dim_K \mathcal{O}_{S,P}/(f, g) \\ &= \dim_K \mathcal{O}_{C,P}/(\overline{g}) \\ &= v_P(\overline{g}) \end{aligned} \tag{C.2}$$

where v_P is the valuation of $\mathcal{O}_{C,P}$, and also

$$I(C.D_2, P) = v_P(\overline{h}). \tag{C.3}$$

Let $t \in \mathcal{O}_{C,P}$ be a local parameter. Then $\hat{\mathcal{O}}_{C,P} \cong K[[t]]$. Since $\dim_K K[[t]]/(\overline{g}) = v_P(\overline{g})$ and $\dim K[[t]]/(\overline{h}) = v_P(\overline{h})$, we have $\dim_K K[[t]]/(\overline{g}, \overline{h}) = min\{v_P(\overline{g}), v_P(\overline{h})\}$. Thus

$$\dim_K \mathcal{O}_{C,P}/(\overline{g}, \overline{h}) \geq min\{v_P(\overline{g}), v_P(\overline{h})\}, \tag{C.4}$$

because $\mathcal{O}_{C,P}/(\overline{g}, \overline{h}) \to K[[t]]/(\overline{g}, \overline{h})$ is surjective. Therefore, from C.1,C.2,C.3 and C.4, we have

$$I(D_1.D_2, P) \geq min\{I(C.D_1, P), I(C.D_2, P)\}.$$

□

Acknowledgments

The first author was supported by FAPESP-Brazil, grant 2013/00564-1. The second author is thankful for the great support received from the ICTP-Trieste, as a visitor, during the last two months of this

project.

References

[1] N. Arakelian, H. Borges, Frobenius nonclassicality with respect to linear systems of curves of arbitrary degree, Acta Arith, 167 (2015) 43–66.

[2] H. Borges, On complete (N,d)-arcs derived from plane curves, Finite Fields Appl. 15 (2009) 82–96.

[3] T. Cochrane, C. Pinner, Explicit bounds on monomial and binomial exponential sums, Quarterly J. of Math. 62(2011) no.2 323-349.

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

[5] A. Garcia, J.F. Voloch, Fermat Curves over finite fields, Journal of Number Theory 30(1988) 345-356.

[6] M. Giullietti, F Pambianco, F. Torres, E. Ughi, O complete arcs arising from plane curves, Des. Codes. Cryptogr. 25 (2002) 237-246.

[7] J.W.P. Hirschfeld, G. Korchmáros, F. Torres, Algebraic curves over a finite field, Princeton Series in Applied Mathematics, 2008.

[8] H.W. Lenstra Jr., On a Problem of Garcia, Stichtenoth and Thomas, Finite Fields and Their Applications, 8(2001) 1–5.

[9] G. Korchmáros, T. Szönyi, Fermat Curves over finite fields and cyclic subsets in high-dimensional projective spaces, Finite Fields and Their Applications, 5(1999) 206-217.

[10] S. Mattarei, On a bound of Garcia and Voloch for the number of points of a Fermat curve over a prime field, Finite Fields and Their Applications, 13(2007) 773-777.

[11] M. Namba, Geometry of projective algebraic curves, Pure and Applied Mathematics, Marcel Dekker Inc. (1984).

[12] R. Pardini, Some remarks on plane curves over fields of finite characteristic, Composito Math. 60(1986) 3-17.

[13] I.E. Shparlinski, Estimates of Gaussian Sums, Mat. Zametki, 50(1991) 122-130.

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