Frobenius nonclassical components of curves with separated variables

Herivelto Borges

Universidade de São Paulo, Inst. de Ciências Matemáticas e de Computação, São Carlos, SP 13560-970, Brazil.

Abstract

We establish a relation between minimal value set polynomials defined over \( F_q \) and certain \( q \)-Frobenius nonclassical curves. The connection leads to a characterization of the curves of type \( g(y) = f(x) \), whose irreducible components are \( q \)-Frobenius nonclassical. An immediate consequence will be the realization of rich sources of new \( q \)-Frobenius nonclassical curves.

Keywords: Frobenius nonclassical curve, Finite Field, minimal value set polynomial.

2010 Mathematics Subject Classification: Primary 14H45, 11C08; Secondary 14Hxx.

1. Introduction

Let \( p \) be a prime number, and \( F_q \) be the field with \( q = p^s \) elements. An irreducible plane curve \( F : F(x, y) = 0 \) defined over \( F_q \) is called \( q \)-Frobenius nonclassical if

\[
F(x, y) \text{ divides } (x^q - x) \frac{\partial F}{\partial x} + (y^q - y) \frac{\partial F}{\partial y}. \tag{1}
\]

Otherwise, \( F \) is called \( q \)-Frobenius classical. Note that the previous condition above has a geometric meaning: the \( F_q \)-Frobenius map takes any simple point \( P \) of \( F \) to the tangent line of \( F \) at \( P \).

Frobenius nonclassical curves were first introduced in the work of Stöhr and Voloch [23]. It is well known that such curves potentially have many rational points and interesting arithmetic and geometric properties ([12],[23]). This fact, along with other related results ([2],[8], [10],[11]), makes the characterization of these curves highly desirable. This common sense is reaffirmed by the following quotation from the recent book by Hirschfeld, Korchmáros...
and Torres [13, p. 407]: “it is hard to find Frobenius nonclassical curves. What emerges is that they are rare but important curves”.

With regard to the number of rational points, one important result is the following (cf. [23, Theorem 2.3]).

**Theorem 1.1** (Stöhr-Voloch). Let $\mathcal{X}$ be an irreducible plane curve of degree $d$ and genus $g$ defined over $\mathbb{F}_q$. If $N := \#\mathcal{X}(\mathbb{F}_q)$ is the number of $\mathbb{F}_q$-rational points on $\mathcal{X}$, then

$$N \leq \frac{\nu(2g - 2) + (q + 2)d}{2},$$

where

$$\nu = \begin{cases} p^h, & \text{for some } h \geq 1, \text{ if } \mathcal{X} \text{ is } q\text{-Frobenius nonclassical} \\ 1, & \text{otherwise.} \end{cases}$$

Thus if we are able to identify the $q$-Frobenius nonclassical curves, we will be left with the remaining curves for which a better upper bound holds (inequality (2) with $\nu = 1$). At the same time, the set of $q$-Frobenius nonclassical curves provides a potential source of curves with many points. Therefore, in light of Theorem 1.1, characterizing $q$-Frobenius nonclassical curves may offer a two-fold benefit.

Examples of $q$-Frobenius nonclassical curves are the Fermat curves

$$x^{\frac{q-1}{q'-1}} + y^{\frac{q-1}{q'-1}} + 1 = 0,$$

where $\mathbb{F}_{q'} \subseteq \mathbb{F}_q$ (see [7, Theorem 2]) Note that, in particular, the Hermitian curve (case $q' = \sqrt{q}$) is $q$-Frobenius nonclassical. Additional examples can be found in the literature ([2],[8],[12]).

The purpose of this paper is to present a new connection between certain $q$-Frobenius nonclassical curves and minimal value set polynomials, i.e., polynomials $f(x) \in \mathbb{F}_q[x]$ for which $V_f = \{f(\alpha) : \alpha \in \mathbb{F}_q\}$ has size $[q/\deg f]$. This relation leads us to a characterization of the curves $f(x) = g(y)$ for which all irreducible components are $q$-Frobenius nonclassical. For a prototype of this connection, note that

$$f(x) = x^{\frac{q-1}{q'-1}} \text{ and } g(y) = -(y^{\frac{q-1}{q'-1}} + 1)$$

are minimal value set polynomials over $\mathbb{F}_q$, with $V_f = V_g = \mathbb{F}_{q'}$, and that $f(x) = g(y)$ is the $q$-Frobenius nonclassical curve given in (4).

A consequence of this correspondence will be the realization of new sources of Frobenius nonclassical curves. It is worth noting that, as one would expect, some curves in this new family will have many rational points. For instance,
we will see that the so-called generalized Hermitian curve, the curve over \( \mathbb{F}_{q^k} \) \((k \geq 2)\) given by

\[
\mathcal{GS} : y^{q^{k-1}} + \cdots + y^q + y = x^{q^k+1} + x^{1+q^2} + \cdots + x^{q^{k-1}+q^{k-2}},
\]

is Frobenius nonclassical. The curve (5), introduced by Garcia and Stichtenoth in [9], has genus \( g = (q^{k-1} - 1)q^{k-1}/2 \), and \( N = q^{2k-1} + 1 \) \( \mathbb{F}_{q^k} \)-rational points.

Additional arithmetic properties of the curve \( \mathcal{GS} \) ([4],[20], [21]) make it suitable for construction of algebraic geometric codes with good parameters.

It should be mentioned that, using the characterization established in this paper, an alternative generalization of the Hermitian curve (with an even better ratio \( N/g \)) can be constructed. This will be the content of a subsequent paper.

The present paper is organized as follows. In Section 2, we recall the main facts and results related to minimal value set polynomials. In Section 3, we establish a connection between Frobenius nonclassical curves and minimal value set polynomials, and prove Theorem 3.4 and Corollary 3.5, the main results of this paper. In Section 4, we consider the minimal value set polynomials \( F \in \mathbb{F}_q[x] \) for which \( |V_F| \leq 2 \). As observed by Carlitz et al. [5], these polynomials do not follow the general pattern. Nonetheless, we will be able to characterize the ones that do give rise to Frobenius nonclassical curves. In Section 5, we make use of the preceding results to characterize Frobenius nonclassical curves of type \( y^n = f(x) \). This will incorporate Garcia’s results in [8]. In Section 6, we provide additional examples and briefly discuss some problems related to Frobenius classicality. In particular, we answer a question raised by Giulietti et al. [10] regarding the arc property of Frobenius nonclassical curves.

**Notation**

- \( q \) denotes a power of a prime \( p \).
- \( \overline{\mathbb{F}_q} \) denotes the algebraic closure of \( \mathbb{F}_q \).
- If \( f(x, y) \in \mathbb{F}_q[x, y] \), and the affine curve \( \mathcal{F} : f(x, y) = 0 \) is irreducible, we denote by \( \mathcal{F}(\overline{\mathbb{F}_q}) \) the set of \( \mathbb{F}_q \)-rational points on the projective closure of \( \mathcal{F} \).
- We will omit the \( q \)-part in the name \( q \)-Frobenius (non)classical, when the finite field \( \mathbb{F}_q \) is clear or irrelevant in the context.
- For any polynomial \( f \in \mathbb{F}_q[x] \), the symbol \( f' \) will denote the formal derivative of \( f \).
2. Minimal value set polynomials

For any nonconstant polynomial $F \in \mathbb{F}_q[x]$, let $V_F = \{F(\alpha) : \alpha \in \mathbb{F}_q\}$ be its value set. One can easily verify that $V_F$ satisfies

$$\left\lfloor \frac{q - 1}{\deg F} \right\rfloor + 1 \leq |V_F| \leq q. \quad (6)$$

**Definition 1.** A polynomial $F \in \mathbb{F}_q[x]$ is called minimal value set polynomial (shortened to MVSP) if $|V_F|$ attains the lower bound in (6).

Despite significant past results in [5] and [17], and recent progress presented in [3], the complete characterization of MVSPs is still an open problem.

A fundamental result concerning these polynomials is the following (cf. [17, Theorem 1]).

**Theorem 2.1** (Mills). Let $F \in \mathbb{F}_q[x]$ be nonconstant polynomial, and consider the following.

(i) Let $V_F = \{\gamma_0, \gamma_1, \ldots, \gamma_r\} \subseteq \mathbb{F}_q$ be the value set of $F$.

(ii) For each $i \in \{0, \ldots, r\}$, set $L_i := \gcd(F - \gamma_i, x^q - x)$.

(iii) Suppose $\gamma_i$ are arranged in such a way that $\deg L_0 \leq \deg L_i$, $1 \leq i \leq r$.

If $F$ is an MVSP and $r > 1$, then there exist positive integers $v, m, k$; a polynomial $N \in \mathbb{F}_q[x]$, and $\omega_0, \omega_1, \ldots, \omega_m \in \mathbb{F}_q$, with $0 \neq \omega_0$ and $\omega_m = 1$, such that

(a) $v | (p^k - 1)$, $1 + vr = p^{mk}$, $L_0 \nmid N$, and $L_0'$ is a $p^{mk}$-th power.

(b) $F = L_0^v N^{p^{mk}} + \gamma_0$.

(c) $\prod_{i=1}^r (x - \gamma_i + \gamma_0) = \sum_{i=0}^m \omega_i x^{(p^{ki} - 1)/v}$.

(d) $\sum_{i=0}^m \omega_i L_0^{p^{ki}} N^{p^{mk}(p^{ki} - 1)/v} = -\omega_0(x^q - x)L_0'$.

In the remainder of this section, we provide additional results on MVSPs that bear upon the sections that follow. The next theorem will be a key ingredient. It is a slightly extended version of [3, Theorem 3.1], which in turn is partially derived from results in [17].
Remark 2.1. Note that if $a, b \in \mathbb{F}_q$ are distinct, and

$$S_{\{a,b\}} = \left\{ F \in \mathbb{F}_q[x] : V_F = \{a, b\} \right\},$$

then a map $S_{\{a,b\}} \to S_{\{0,1\}}$ given by $F \mapsto \frac{1}{a-b}(F-b)$ is a bijection. We use this fact in some of our later proofs.

**Theorem 2.2.** Let $F \in \mathbb{F}_q[x]$ be a polynomial of degree $d \geq 1$. If there exists $\theta \in \mathbb{F}_q^*$, and a monic polynomial $T \in \mathbb{F}_q[x]$ such that

$$T(F) = \theta(x^q - x)F',$$  \hspace{1cm} (7)

then $T = \prod_{\gamma_i \in V_F} (x - \gamma_i)$ and $F$ is an MVSP. Conversely, suppose that $F$ is an MVSP and $T = \prod_{\gamma_i \in V_F} (x - \gamma_i)$. If either $|V_F| > 2$ or $|V_F| = 2 = p$, then there exists $\theta \in \mathbb{F}_q^*$ such that (7) holds.

**Proof.** Set $t := \deg T$, and let $S \subseteq \mathbb{F}_q$ be the set of distinct roots of $T$. Note that $V_F \subseteq S$, and so $|V_F| \leq |S| \leq t$. On the other hand, equating degrees in (7), gives

$$t \cdot d = q + \deg F' \leq q - 1 + d.$$  

Thus $(t - 1)d \leq q - 1$, which gives $t \leq \frac{q-1}{d} + 1$, and then

$$|V_F| \leq |S| \leq t \leq \left\lfloor \frac{q-1}{d} \right\rfloor + 1 \leq |V_F|.$$  

Therefore, $|V_F| = |S| = t = \left\lfloor \frac{q-1}{d} \right\rfloor + 1$. That is, $F$ is an MVSP and $T = \prod_{\gamma_i \in V_F} (x - \gamma_i)$. For the converse, if $|V_F| > 2$, one can readily check that the result follows from [17, equation (4)] and [17, Lemma 1]. For the case $|V_F| = 2 = p$, we show that the result follows from [3, Lemma 4.1]. In fact, from Remark 2.1, we may assume $V_F = \{0, 1\}$, and then [3, Lemma 4.1] implies that $F^2 - F = (x^q - x)F'$, which completes the proof. \hfill $\square$

**Lemma 2.3.** Let $F \in \mathbb{F}_q[x]$ be a nonconstant polynomial, and let

$$V_F = \{\gamma_0, \gamma_1, \ldots, \gamma_r\}$$

be its value set. For each $\gamma_i \in V_F$, define $F_i := F - \gamma_i$. If $F$ satisfies equation (7) in Theorem 2.2, then the following hold.

(i) If $\alpha \in \mathbb{F}_q \backslash \mathbb{F}_q$ is a root of $F_i$ of multiplicity $k \geq 1$, then $p \mid k$.  


(ii) If \( k \geq 1 \) is the multiplicity of an \( \mathbb{F}_q \)-root of any \( F_i \), then \( T'(\gamma_i) = -\theta k \).
In particular, \( p \nmid k \).

(iii) \( F' \neq 0 \), and if \( r > 0 \), then there exists \( \gamma_i \in V_F \) such that \( T'(\gamma_i) = -\theta \).

(iv) If \( r > 0 \), then \( F'' = 0 \) if and only if \( T' \) is constant.

Proof. Without loss of generality, we prove assertions (i) and (ii) for \( F_0 = F - \gamma_0 \). Suppose \( F_0 = \prod (x - a_j)^{k_j} \), where \( a_j \in \mathbb{F}_q \) are distinct, and \( k_j \geq 1 \) are integers. To prove (i), we may assume that \( a_i \notin \mathbb{F}_q \), and then from

\[
T(F) = F_0 F_1 \cdots F_r = \theta(x^q - x)F'(x)
\tag{8}
\]

we have that \((x - a_1)^{k_1} \) divides \( F'(x) = F'_0(x) \). But since \( k_1 \) is the multiplicity of \( a_1 \), we have that \( p \nmid k_1 \). To prove (ii), first note that (8) implies that

\[
\frac{T(F)}{F_0} = \theta(x^q - x)\frac{F'_0(x)}{F_0(x)} = \theta(x^q - x) \sum_{j=1}^{d} \frac{k_j}{x - a_j}.
\tag{9}
\]

Now if \( a_\alpha \in \mathbb{F}_q \) is any root of \( F_0 \), then evaluating the left and right sides of (9) at \( x = a_\alpha \) we get \( T'(\gamma_0) = -\theta k_\lambda \), which provides the result. Also observe that since \( T(\gamma_0) = 0 \) and \( T \) is separable, we have \( 0 \neq T'(\gamma_i) = -\theta k \) and so \( p \nmid k \).

For the third assertion, first note that \( F' \neq 0 \) is clearly given by equation (8). For the following statement, just differentiate both sides of equation (7) in Theorem 2.2, and then evaluate at any \( x = \alpha \in \mathbb{F}_q \) for which \( F'(\alpha) \neq 0 \). The existence of such \( \alpha \) comes from the fact that \( F' \neq 0 \) and \( \deg F' < q \).

To prove the lemma’s last claim, observe that if \( T' = \theta \) is constant then (iii) gives \( T' = -\theta \). Thus (iv) will follow immediately after we differentiate both sides of (7) in Theorem 2.2. This finishes the proof.

\[\square\]

Lemma 2.4. Notation and hypotheses as in Lemma 2.3. Assume \( r > 1 \) and let \( l_i \) be the degree of \( L_i := \gcd(F_i, x^q - x) \). If \( \gamma_i \in V_F \) are labelled in such a way that \( l_0 \leq l_i \) for \( i = 1, \ldots, r \), then

(i) The multiplicities of all \( \mathbb{F}_q \)-roots of \( F_1, \ldots, F_r \) reduce to 1 mod \( p \).

(ii) \( \theta = -T(\gamma_i) \) for all \( \gamma_i \in V_F \setminus \{\gamma_0\} \).

Proof. From Theorem 2.2, we have that \( F \) is an MVSP. Clearly \( F_i = L_i U_i \), for some polynomial \( U_i \), \( i = 0, \ldots, r \). Now the first assertion is given directly by [17, Lemma 2] (see also notation between (2) an (3) therein), followed by [17, condition (11)] and [17, Lemma 3]. Item (ii) is given directly from assertions (ii) and (i) of our Lemmas 2.3 and 2.4, respectively. This gives the result.

\[\square\]
2.1. Minimal value sets polynomials $F \in \mathbb{F}_{q^k}[x]$ with $V_F = \mathbb{F}_q$

The Theorem 4.7 in [3] gives a complete characterization of MVSPs $F \in \mathbb{F}_{q^k}[x]$ for which $V_F = \mathbb{F}_q$. To enhance clarity, we state this result in a slightly different way and provide its proof adjusted accordingly.

**Theorem 2.5.** Let $F \in \mathbb{F}_{q^k}[x]$ be a nonconstant polynomial. Then $F$ is an MVSP with $V_F = \mathbb{F}_q$ if and only if there exists a nonconstant $H \in \mathbb{F}_{q^k}[x]$ such that

(i) the monomials of $H$ are of the form $cx^{\alpha_0 + \alpha_1 q^2 + \cdots + \alpha_{k-1} q^{k-1}} \in \mathbb{F}_{q^k}[x]$, where each $\alpha_i$ is either 0 or 1.

(ii)

$$F = T_k(H) \mod (x^{q^k} - x),$$

where $T_k(x) := \sum_{i=0}^{k-1} x^i$ is the trace polynomial.

**Proof.** Assuming (i) and (ii), we clearly have $V_F \subseteq \mathbb{F}_q$ and

$$\deg F \leq q^{k-1} + \cdots + q + 1 = \frac{q^k - 1}{q-1}. \quad (11)$$

Thus [3, Lemma 4.1] implies that $F \in \mathbb{F}_{q^k}[x]$ is an MVSP with $V_F = \mathbb{F}_q$. Conversely, if $F$ is an MVSP with $V_F = \mathbb{F}_q$, then [3, Theorem 4.7] asserts that $F$ is a sum of polynomials of the form

$$\mathfrak{F} := \sum_{i=0}^{t-1} \left( m(x)^{\eta^i} \mod (x^{q^n} - x) \right), \quad (12)$$

where $m(x) \in \mathbb{F}_{q^t}[x]$ is a monomial of degree $\alpha_{n-1} q^{n-1} + \cdots + \alpha_1 q + \alpha_0$, $\alpha_i \in \{0, 1\}$, and $t$ is the size of the orbit of $m(x)$ under the action of $G := \text{Gal}(\mathbb{F}_{q^t}/\mathbb{F}_q)$ on the set of monomials of $F$ (cf. [3, Proposition 4.2]). Therefore, it suffices to prove (i) and (ii) for the polynomial $\mathfrak{F}$ in (12). Note that $\mathfrak{F}$ is $G$-invariant, that is, $\mathfrak{F}^{\eta^i} \mod (x^{q^n} - x) = \mathfrak{F}$ for any integer $i \geq 0$. Now if we take $\lambda \in \mathbb{F}_{q^k}$ such that $T_k(\lambda) = 1$, and define $H := \lambda \mathfrak{F}$, we obtain

$$T_k(H) \mod (x^{q^k} - x) = T_k(\lambda \mathfrak{F}) \mod (x^{q^k} - x) = T_k(\lambda) \cdot \mathfrak{F} = \mathfrak{F},$$

and the result follows. \qed
Remark 2.2. Note that from Theorem 2.5 the set
\[ W := \{ \text{MVSPs } F \in \mathbb{F}_{q^k}[x] : V_F = \mathbb{F}_q \} \] (13)
can be explicitly constructed. As a matter of fact, it follows from [3, Theorem 4.8] that the set \( W \cup \mathbb{F}_q \) is an \( \mathbb{F}_q \)-vector space of dimension \( 2^k \) (in particular, \( \#W = q^{2^k} - q \)). For example, if \( k = 2 \), one can easily check that this \( \mathbb{F}_q \)-vector space is given by
\[ W \cup \mathbb{F}_q = \langle 1, x^{q+1}, x + x^q, \lambda x + (\lambda x)^q \rangle \] (14)
for any fixed \( \lambda \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q \). We will address the set \( W \) again in Section 4.

We finish this section with a slight extension of [3, Proposition 2.5].

Lemma 2.6. Let \( F \in \mathbb{F}_q[x] \) be an MVSP such that \( \deg F \leq \sqrt{q} \). If \( G \in \mathbb{F}_q[x] \) is an MVSP with \( \deg G \leq \sqrt{q} \) and \( V_F = V_G \), then \( G = F(ax + b) \) for some \( a, b \in \mathbb{F}_q \).

Proof. Note that when \( |V_F| > 2 \) the result is given by [3, Proposition 2.5]. Since \( q > 4 \) implies
\[ |V_F| = 1 + \left\lfloor \frac{q - 1}{\deg F} \right\rfloor = \left\lceil \frac{q}{\deg F} \right\rceil \geq \lceil \sqrt{q} \rceil > 2, \]
we may assume \( q \leq 4 \) and \( |V_F| \leq 2 \). If \( q < 4 \), then the condition \( \deg G, \deg F \leq \sqrt{q} \) implies that \( F \) and \( G \) are linear, and the result follows trivially. Therefore, the only case we are left with is
\[ q = 4 \text{ and } \deg G = \deg F = |V_F| = |V_G| = 2. \]
By Remark 2.1, we may assume \( V_F = V_G = \mathbb{F}_2 \). Thus (14) implies that \( F(x) = (\lambda x)^2 + \lambda x + \alpha \) and \( G(x) = (\gamma x)^2 + \gamma x + \beta \), for some \( \lambda, \gamma \in \mathbb{F}_4^* \) and \( \alpha, \beta \in \mathbb{F}_2 \). Now taking \( b \in \mathbb{F}_4 \) such that \( F(b) = \beta \), and \( a = \gamma/\lambda \), we have \( G = F(ax + b) \), as claimed. \( \square \)

3. The main results

The primary goal of this section is to prove Theorem 3.4 and Corollary 3.5, which establish a relation between certain Frobenius nonclassical curves and MVSPs. To this end, we start by presenting some preliminary results.

The following result corresponds to [6, Theorem 3.2].
Lemma 3.1 (Fried-MacRae). Let $K$ be an arbitrary field. Let $f(x), g(x), a(x)$ and $b(x)$ be nonconstant polynomials in $K[x]$. The polynomial $f(x) - g(y)$ is a factor of $a(x) - b(y)$ if and only there exists a polynomial $T \in K[x]$ such that

$$T(f(x)) = a(x) 	ext{ and } T(g(y)) = b(y).$$

Lemma 3.2. Let $f(x)$ and $g(y)$ be nonconstant polynomials defined over $\overline{F}_q$ such that $F(x, y) = f(x) - g(y) \notin \overline{F}_q[x^p, y^p]$. If $F = \prod_{i=1}^{r} F_i$ is the factorization of $F$ into irreducible factors, then the $F_i$ are pairwise coprime.

Proof. Write $F(x, y) = f(x) - g(y) = \prod_{i=1}^{r} F_i^{m_i}$, where $(F_i, F_j) = 1$ for $i \neq j$, and $m_i \geq 1$ are integers. Without loss of generality, suppose that $m_1 > 1$, $f'(x) \neq 0$, and then write

$$f(x) - g(y) = F_1^{m_1}G$$

for some $G \in \overline{F}_q[x, y]$. Differentiating both sides of (15) with respect to $x$ gives $f'(x) = F_1^{m_1-1} \left( m_1 \frac{\partial F}{\partial x} G + F_1 \frac{\partial G}{\partial x} \right)$. Therefore, $F_1$ divides $f'(x) \neq 0$, that is, $F_1$ is a nonconstant polynomial in $x$ only. Thus, since $F_1$ divides $f(x) - g(y)$, it follows that $g(y)$ is constant, a contradiction. This completes the proof. \( \square \)

Lemma 3.3. Let $F(x, y) \in \overline{F}_q[x, y]$ be a nonconstant polynomial, and write $F = \prod_{i=1}^{r} F_i$ where each $F_i$ is irreducible. If the $F_i$ are pairwise coprime, then the following are equivalent.

(i) $F$ divides $(x^q - x) \frac{\partial F}{\partial x} + (y^q - y) \frac{\partial F}{\partial y}$.

(ii) $F_i$ divides $(x^q - x) \frac{\partial F_i}{\partial x} + (y^q - y) \frac{\partial F_i}{\partial y}$ for all $i = 1, \ldots, r$.

Proof. For each $i \in \{1, \ldots, r\}$, define $H_i := \prod_{j \neq i} F_j$ and write $F = F_iH_i$.

Computing $\frac{\partial (F_iH_i)}{\partial x}$ and $\frac{\partial (F_iH_i)}{\partial y}$ and multiplying the results by $x^q - x$ and $y^q - y$, respectively, yields the identity

$$(x^q - x) \frac{\partial F}{\partial x} + (y^q - y) \frac{\partial F}{\partial y} = \left( (x^q - x) \frac{\partial F_i}{\partial x} + (y^q - y) \frac{\partial F_i}{\partial y} \right) H_i + \left( (x^q - x) \frac{\partial H_i}{\partial x} + (y^q - y) \frac{\partial H_i}{\partial y} \right) F_i.$$  (16)

The equality (16) clearly gives that (ii) implies (i). The converse also follows from (16), when we use the fact that $(F_i, F_j) = 1$, for $i \neq j$, implies $(F_i, H_i) = 1$. \( \square \)
3.4. Let \( f(x), g(x) \in \mathbb{F}_q[x] \) be nonconstant polynomials such that \( f(x) - g(y) \notin \mathbb{F}_q[x^p, y^p] \). Suppose that the irreducible components of \( F : f(x) = g(y) \) are defined over \( \mathbb{F}_q \). The irreducible components of \( F \) are \( q \)-Frobenius nonclassical if and only if there exist a monic polynomial \( T \in \mathbb{F}_q[x] \) and a constant \( \theta \in \mathbb{F}_q^* \) such that
\[
T(f(x)) = \theta(x^q - x)f'(x) \quad \text{and} \quad T(g(y)) = \theta(y^q - y)g'(y). \tag{17}
\]

Proof. We begin by proving (17). Set \( f(x) - g(y) = \prod_{i=1}^r F_i \), where \( F_i \in \mathbb{F}_q[x, y] \) are absolutely irreducible, and let us assume that each curve \( F_i = 0 \) is \( q \)-Frobenius nonclassical. That is,
\[
F_i \text{ divides } (x^q - x)\frac{\partial F_i}{\partial x} + (y^q - y)\frac{\partial F_i}{\partial y} \quad \text{for all } i = 1, \ldots, r.
\]

From Lemma 3.2 the \( F_i \) are pairwise coprime, and so Lemma 3.3 implies that
\[
f(x) - g(y) \text{ divides } (x^q - x)f'(x) - (y^q - y)g'(y). \tag{18}
\]

Now with the conditions \( f(x) - g(y) \notin \mathbb{F}_q[x^p, y^p] \) and (18), the statement (17) follows directly from Lemma 3.1. The converse follows easily from the fact that \( f(x) - g(y)\big|T(f(x)) - T(g(y)) \) together with Lemmas 3.2 and 3.3.

\[
\square
\]

3.5. Let \( f(x), g(x) \in \mathbb{F}_q[x] \) be nonconstant polynomials such that \( f(x) - g(y) \notin \mathbb{F}_q[x^p, y^p] \). Suppose that the irreducible components of \( F : f(x) = g(y) \) are defined over \( \mathbb{F}_q \). If the irreducible component of \( F \) are \( q \)-Frobenius nonclassical, then \( f(y) \) and \( g(x) \) are MVSPs with \( V_f = V_g \). Conversely, suppose that \( f(x) \) and \( g(y) \) are are MVSPs with \( V_f = V_g \). If \( |V_f| > 2 \) or \( |V_f| = 2 = p \), then the irreducible components of \( F \) are \( q \)-Frobenius nonclassical.

Proof. This is an immediate consequence of Theorems 2.2 and 3.4.

\[
\square
\]

3.1. Some Consequences

Next, we point out some facts that follow immediately from Corollary 3.5.

3.6. If \( H = \{a_i x - b_i | i = 1, \ldots, n \} \) is a subgroup of \( \text{Aut}(\mathbb{F}_q(x)) \) and \( f(x) = \prod_{i=1}^n (a_i x - b_i) \), then \( f(x) \) is an MVSP.
Proof. Since \((H, \circ)\) is a group, the polynomial of degree \(n\)
\[
F(x, y) = f(x) - f(y) = \prod_{i=1}^{n} (a_i x - b_i) - \prod_{i=1}^{n} (a_i y - b_i)
\]
is such that \(F(x, a_i x + b_i) = 0\) for all \(i = 1, \ldots, n\). Therefore, the plane curve \(F(x, y) = 0\) is the union of \(n\) distinct lines \(y = a_i x + b_i\). In particular, \(f'(x) \neq 0\) and the \(n\) irreducible components of \(F(x, y) = 0\) are Frobenius nonclassical curves. Therefore Corollary 3.5 gives the result.

Hefez and Voloch [12, Proposition 6] have proved that if a \(q\)-Frobenius nonclassical curve of degree \(d > 1\) is nonsingular, then \(d \geq \sqrt{q} + 1\). Next, we show that the nonsingularity condition can be dropped for the curves considered here.

**Corollary 3.7.** Any nonlinear \(q\)-Frobenius nonclassical curve \(F : f(y) = g(x)\) has degree \(d \geq \sqrt{q} + 1\).

Proof. From Corollary 3.5, \(f\) and \(g\) are MVSPs with \(V_f = V_g\). Now suppose \(\deg F \leq \sqrt{q}\), i.e., \(\deg f, \deg g \leq \sqrt{q}\). Thus Lemma 2.6 implies \(g(x) = f(ax + b)\) for some \(a, b \in \mathbb{F}_q\). Hence the line \(y = ax + b\) is a component of the curve \(F\), which contradicts its irreducibility. This finishes the proof.

Recall from Remark 2.2 that \(\mathcal{W}\) denotes the set of MVSPs in \(\mathbb{F}_{q^k}[x]\), whose value set is \(\mathbb{F}_q\). From the characterization given by Corollary 3.5, the set \(\mathcal{W}\) turns into a productive source of new Frobenius nonclassical curves. In other words, we have the following.

**Corollary 3.8.** Let \(f, g\) be polynomials in \(\mathcal{W}\). If the irreducible components of \(F : f(y) = g(x)\) are defined over \(\mathbb{F}_{q^k}\), then all such components are \(q^k\)-Frobenius nonclassical curves.

Taking into account Corollary 3.8, it follows that all irreducible curves of type \(y^{q^k-1} = f(x)\), where \(f(x) \in \mathcal{W}\), are \(q^k\)-Frobenius nonclassical. In particular, the so-called Norm-Trace curve
\[
y^{q^k-1} + \cdots + y + x = x^{q^k-1} + \cdots + x^q + x
\]
is \(q^k\)-Frobenius nonclassical. The Frobenius nonclassicality of cyclic coverings of \(\mathbb{P}^1\) (e.g. curve (19)) will be the focus of Section 5.
4. Frobenius nonclassicality in the cases $|V_f| \leq 2$

Recall from Theorem 2.2 that all nonconstant polynomials $f \in \mathbb{F}_q[x]$ satisfying equation (7) are MVSPs. The converse also holds for MVSPs for which either $|V_f| > 2$ or $|V_f| = 2 = p$. However, if $|V_f| = 1$ or $|V_f| = 2 < p$, one can easily find examples for which equation (7) fails, i.e.,

$$T(f) = (x^q - x)h(x), \text{ but } h(x) \neq \theta \cdot f'(x) \text{ for all } \theta \in \mathbb{F}_q^*.$$  \hfill (20)

It is easy to check that the polynomials $f(x) = (x^q - x)x$ and $g(x) = \frac{x^q - x}{x^{p-2}} + x^{q-1} - 1$ (for $p > 2$) are examples of such a failure. As remarked by Carlitz et al. [5], the MVSPs $f$ with $|V_f| \leq 2$ do not fit the general pattern. That is the reason why they were left out in Theorems 2.2.

The objective of this section is to characterize the MVSPs $f \in \mathbb{F}_q[x]$, where $|V_f| \leq 2$, for which the polynomial $h(x)$ in (20) is indeed $\theta \cdot f'(x)$ for some $\theta \in \mathbb{F}_q^*$. The results here will complement the converse of Corollary 3.5. That is, we will complete the characterization of our Frobenius nonclassical curves in terms of MVSPs.

4.1. Case $|V_f| = 1$

It is straightforward to see that a nonconstant polynomial $f \in \mathbb{F}_q[x]$ satisfies $|V_f| = 1$ if and only if

$$f = (x^q - x)r(x) + \alpha,$$  \hfill (21)

where $r \in \mathbb{F}_q[x] \setminus \{0\}$ and $\alpha \in \mathbb{F}_q$. Out of these MVSPs, the ones that give rise to Frobenius nonclassical curves will be characterized in the next theorem. Note that from (21), to study the curves $f(x) = g(y)$ where $V_f = V_g$, we may assume $\alpha = 0$.

**Theorem 4.1.** Let $f(x)$ and $g(y)$ be nonconstant polynomials defined over $\mathbb{F}_q$ such that $f(x) - g(y) \notin \mathbb{F}_q[x^p, y^p]$. Suppose that the irreducible components of the curve $F : f(x) = g(y)$ are defined over $\mathbb{F}_q$ and that $f(x)$ and $g(y)$ are MVSPs with $V_f = V_g = \{0\}$. Then the irreducible components of $F$ are $q$-Frobenius nonclassical if and only if there exist positive integers $n, m$, where $n \equiv m \mod p$, and polynomials $a(t), b(t) \in \mathbb{F}_q[t]$, not divisible by $t^q - t$, such that

$$f(x) = (x^q - x)^n a(x)^p \text{ and } g(y) = (y^q - y)^m b(y)^p.$$  \hfill (22)

**Proof.** It is clear that any nonconstant polynomial $h \in \mathbb{F}_q[t]$ for which $V_h = \{0\}$ can be written as $h(t) = (t^q - t)^n u(t)$, where $n$ is a positive integer, and $u \in \mathbb{F}_q[t]$ is such that $(t^q - t) \nmid u(t)$. Thus writing $f$ and $g$ in this way, we have

$$f(x) = (x^q - x)^n u(x) \text{ and } g(y) = (y^q - y)^m v(y).$$

12
Now if the irreducible components of \( \mathcal{F} \) are \( q \)-Frobenius nonclassical, then Theorem 3.4 implies

\[
(x^q - x)^n u(x) = \theta(x^q - x)^n(-nu(x) + (x^q - x)u'(x)) \tag{23}
\]

and

\[
(y^q - y)^m v(y) = \theta(y^q - y)^m(-mv(y) + (y^q - y)v'(y)) \tag{24}
\]

for some \( \theta \in \mathbb{F}_q^* \). Since (23) is equivalent to \((1 + \theta n)u(x) = \theta(x^q - x)u'(x)\) and furthermore \((x^q - x) \not| u(x)\), we have \(u'(x) = 0\) and \(1 + \theta n = 0\). That is, \(u(x) = a(x)^p\) for some \(a(x) \in \mathbb{F}_q[x]\) and \(\theta = -1/n\). Similarly, (24) yields \(v(y) = b(y)p\) for some \(b(y) \in \mathbb{F}_q[y]\) and \(\theta = -1/m\), and then (22) follows. Conversely, note that (22) implies that \(f\) and \(g\) satisfy equation \(T(h(x)) = \theta(x^q - x)h'(x)\) for \(T(x) = x\) and \(\theta = -1/m = -1/n\). Thus Theorem 3.4 gives the result.

4.2. Case \(|V_f| = 2 < p\)

Note that MVSPs \(f \in \mathbb{F}_q[x]\) with \(|V_f| = 2\) correspond to polynomials of degree \(\leq q - 1\) with value set of size two. Using Lagrange interpolation, it follows that the polynomials \(f \in \mathbb{F}_q[x]\), for which \(V_f = \{\alpha, \beta\}\), are given by

\[
f(x) = \alpha \sum_{a \in S} \left(1 - (x - a)^{q-1}\right) + \beta \sum_{b \in \mathbb{F}_q \setminus S} \left(1 - (x - b)^{q-1}\right),
\]

where \(S \subset \mathbb{F}_q\) is an arbitrary nonempty set (see e.g. [16, p. 348]). Note if \(S \subset \mathbb{F}_q\) is fixed, then by Remark 2.1 we may assume \(V_f = \{0, 1\}\), and then write

\[
f(x) = \sum_{a \in S} \left(1 - (x - a)^{q-1}\right). \tag{25}
\]

We begin by providing an alternative description for the polynomials (25).

**Lemma 4.2.** Let \(S \subset \mathbb{F}_q\) be a nonempty set. If \(g(x) = \prod_{a \in S} (x - a)\) and \(h(x) = \prod_{b \in \mathbb{F}_q \setminus S} (x - b)\), then \(f = -gh\) is an MVSP with \(V_f = \{0, 1\}\). Moreover, all MVSPs \(f \in \mathbb{F}_q[x]\), with \(V_f = \{0, 1\}\), arise in this way.

**Proof.** Clearly \(g(x)h(x) = x^q - x\), and then \(g'h + gh' = -1\). The last equality implies that \(f := -g'h\) is such that \(V_f = \{0, 1\}\) and \(\deg f \leq q - 1\). In particular, \(f\) is an MVSP. It is easy to check that different subsets \(S_1\) and \(S_2\) of \(\mathbb{F}_q\) will give rise to different polynomials \(f_1\) and \(f_2\). That is, the number
of polynomials arising in this way corresponds to the number of nonempty subsets $S \subseteq \mathbb{F}_q$, which is $2^q - 2$. Obviously, the number of polynomials given by (25) is the same. This completes the proof.

We now seek an additional condition on the polynomial $g$ (in Lemma 4.2) so that the corresponding $f \in \mathbb{F}_q[x]$ satisfies equation (7). As we will soon see, it turns out that such a condition is precisely $g'' = 0$. That is, $g$ is of the form $x \cdot a(x)^p + b(x)^p \in \mathbb{F}_q[x]$. In particular, linear polynomials and arbitrary polynomials in characteristic two will always be suitable choices for $g$.

Definition 2. Consider the following sets of polynomials in $\mathbb{F}_q[t]$.

- $A = \{ g'g(t^q-t) : g$ is a monic proper divisor of $t^q-t$ and $g'' = 0 \}$.
- $B = \{ 1-f : f \in A \}$.

We say that $f(x) \in \mathbb{F}_q[x]$ is a polynomial of type $A$ or $B$ if $f(t) \in A$ or $f(t) \in B$, respectively. Note that since $q$ is odd we have $A \cap B = \emptyset$.

Remark 4.1. It is easy to construct polynomials of type $A$, and then of type $B$. One source of such polynomials is the set $W$ in (13), as follows from Lemma 2.3 (iv). So as long as $g \in W$ is separable, its roots will lie in $\mathbb{F}_{q^k}$ (Lemma 2.3 (i)), and then, assuming $g$ monic, we have that $\frac{g'}{g}(t-t^{q^k})$ is of type $A$. The polynomials $g = t^{q^k-1} + \cdots + t^q + t$ and $g = t^{q^k-1} - 1$ are some examples.

Alternatively, one can follow a more general procedure: Choose coprime polynomials $a(t), b(t) \in \mathbb{F}_q[t]$ such that $g := ta^p + b^p$ is monic. Thus $g$ is separable, and for any extension $\mathbb{F}_{q^s}$ containing the splitting field of $g$, the polynomial $\frac{g'}{g}(t-t^{q^s})$ will be of type $A$.

Lemma 4.3. Let $f \in \mathbb{F}_q$ be an MVSP, where $V_f = \{0, 1\}$ and $q$ is odd. Then

$$f(f-1) = \theta(x^q-x)f', \text{ for some } \theta \in \mathbb{F}_q^*, \text{ if and only if } f \in A \cup B.$$  

Furthermore, $\theta = 1$ if $f \in A$, and $\theta = -1$ if $f \in B$.

Proof. Suppose $f(f-1) = \theta(x^q-x)f'$ for some $\theta \in \mathbb{F}_q^*$. Since $T'(x) = 2x-1$ and $V_f = \{0, 1\}$, it follows from Lemma 2.3 (iii) that $\theta = \pm 1$. 

14
(i) Case \( \theta = 1 \). Suppose
\[
f(f - 1) = (x^q - x)f'.
\]
We shall prove that \( f \in A \). In fact, from Lemma 4.2, \( f = (x - x^q)\frac{g'}{g} \)
for some monic divisor \( g \) of \( x - x^q \). Thus \( f' = \frac{(x-x^q)(g''g - g^2) + g'g}{g^2} \), and
(26) implies
\[
(x - x^q)\frac{g'}{g}((x - x^q)\frac{g'}{g} - 1) = (x^q - x)\frac{(x - x^q)(g''g - g^2) + g'g}{g^2}.
\]
A straightforward simplification leads to \( (x - x^q)g''g = 0 \), and then \( g'' = 0 \). Therefore, \( f \in A \).

(ii) Case \( \theta = -1 \). Note that if \( f(f - 1) = -(x^q - x)f' \), then \( 1 - f \) satisfies
\[
(1 - f)(1 - f') = (x^q - x)(1 - f'),
\]
Thus the case \( \theta = 1 \) implies \( 1 - f \in A \), and then \( f \in B \).

Now we prove the converse. Suppose \( f \in A \), i.e.,
\[
f = (x - x^q)\frac{g'}{g}, \text{ where } g \text{ is a monic proper divisor of } x - x^q \text{ and } g'' = 0.
\]

Therefore, using the fact that \( f(f - 1) = (x^q - x)G(x) \), for some \( G(x) \in \mathbb{F}_q[x] \),
we obtain
\[
G(x) = \frac{1}{(x^q - x)}f(f - 1) = \frac{-h'}{h'}\left((x - x^q)\frac{h'}{h} - 1\right) = \frac{h' - (x^q - x)h'2}{h} = f'.
\]
A similar computation for \( f \in B \) implies \( G(x) = -f' \).

The following result will complement Corollary 3.5 for the case \( |V_f| = 2 < p \).

**Theorem 4.4.** Let \( f(x) \) and \( g(y) \) be nonconstant polynomials defined over \( \mathbb{F}_q \) such that \( f(x) - g(y) \notin \mathbb{F}_q[x^p, y^p] \). Suppose that the irreducible components of the curve \( \mathcal{F} : f(x) = g(y) \) are defined over \( \mathbb{F}_q \), and that \( f(x) \) and \( g(y) \) are MVSPs with \( V_f = V_g = \{0, 1\} \). Then the irreducible components of \( \mathcal{F} \) are \( q \)-Frobenius nonclassical if and only if \( f \) and \( g \) are both of type A or of type B.
Proof. If the irreducible components of $\mathcal{F}$ are $q$-Frobenius nonclassical, then by Theorem 3.4, there exists a monic $T \in \mathbb{F}_q[x]$ and $\theta \in \mathbb{F}_q^*$ such that

$$T(f) = \theta(x^q - x)f'(x) \quad \text{and} \quad T(g) = \theta(y^q - y)g'(y). \quad (27)$$

From Theorem 2.2, $T(x) = x(x-1)$, and then Lemma 2.3 (iii) gives $\theta = \pm 1$. Therefore, Lemma 4.3 implies that $f$ and $g$ are of the same type. Conversely, if $f$ and $g$ are of the same type, then Lemma 4.3 implies that (27) holds for $T(x) = x(x-1)$ and some $\theta \in \{-1, 1\}$. Therefore $F = f - g$ divides

$$(x^q - x)f'(x) - (x^q - x)g'(y) = (x^q - x)\frac{\partial F}{\partial x} + (x^q - x)\frac{\partial F}{\partial y},$$

and the result follows from Lemmas 3.2 and 3.3.

5. The curves $y^n = f(x)$

The objective of this section is to apply the previous results to the curves $y^n = f(x)$. The work presented here will subsume the related results of Garcia’s investigation of the Frobenius nonclassicality of a class of curves of type $y^n = f(x)$ [8]. The case $\text{char}(\mathbb{F}_q) = 2$ (not covered in [8]) will also be included. We begin with some preliminary facts.

Remark 5.1. Hereafter, we say that $x_0 \in \mathbb{F}_q$ is a root of $f(x)$ of multiplicity $k = 0$, if $f(x_0) \neq 0$. Note that if $\deg f < q$, then there always exists such $x_0 \in \mathbb{F}_q$.

Lemma 5.1. Consider the curve $\mathcal{F} : y^n = f(x)$, where $f(x) \in \mathbb{F}_q[x]$ is a polynomial of positive degree $d \leq n$ and has an root $x_0 \in \mathbb{F}_q$ of multiplicity $k \geq 0$. Then there exists a polynomial $g(x) \in \mathbb{F}_q[x]$, of degree $n - k$ such that the projective completions of $\mathcal{G} : y^n = g(x)$ and $\mathcal{F}$ are $\mathbb{F}_q$-projectively equivalent. In particular, if the components of $\mathcal{F}$ are $q$-Frobenius nonclassical, then so are the components of $\mathcal{G}$.

Proof. Without loss of generality, we can assume $x_0 = 0$ and write $f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_k x^k$, where $k \geq 0$ and $a_k \neq 0$. Homogenizing $y^n - f(x)$ w.r.t. the variable $z$ yields

$$y^n - (a_d x^d z^{n-d} + a_{d-1} x^{d-1} z^{n-d+1} + \cdots + a_k x^k z^{n-k}).$$

Interchanging $x$ and $z$, and dehomogenizing w.r.t. the variable $z$ leads to a curve $\mathcal{G} : y^n = g(x)$, where $\deg g = n - k$, as desired. Note that preceding operations correspond to an $\mathbb{F}_q$-projective change of coordinates. And so the $q$-Frobenius nonclassicality of the components is preserved.

\[\square\]
Lemma 5.2. Let $n$ be a divisor of $q - 1$ and $f(x) \in \mathbb{F}_q[x]$ be a nonconstant polynomial. If $y^n = f(x)$ has a solution $(x_0, y_0) \in \mathbb{F}_q \times \mathbb{F}_q^*$, then the $\mathbb{F}_q$-irreducible factors of $y^n - f(x)$ are absolutely irreducible.

Proof. Let us write $y^n - f(x) = \prod_{i=1}^r F_i(x, y)$, where $F_i(x, y) \in \mathbb{F}_q[x, y]$ are irreducible. Considered as polynomials in the variable $y$, we clearly have that

$$\deg_y F_i \geq 1 \quad \text{and} \quad \sum_{i=1}^r \deg_y F_i = n. \quad (28)$$

Since $n|(q - 1)$ and $(x_0, y_0) \in \mathbb{F}_q \times \mathbb{F}_q^*$ is such that $y_0^n = f(x_0)$, the equation $y^n = f(x)$ has $n$ distinct roots in $\mathbb{F}_q$. Thus (28) implies that each $F_i(x_0, y)$ is a nonconstant separable polynomial whose roots lie in $\mathbb{F}_q$. Suppose one of the factors of $y^n - f(x)$, say $F_1(x, y)$, is not absolutely irreducible. Without loss of generality, we may also assume $F_1(P) = 0$ for $P = (x_0, y_0)$. Let $G_1 = \sum \alpha_{i,j} x^i y^j \in \mathbb{F}_q[x, y]/\mathbb{F}_q[x, y]$ be a factor of $F_1$ such that $G_1(P) = 0$. Clearly, $G_2 := \sum \alpha_{i,j} x^i y^j$ is another Galois conjugate dividing $F_1$, and the fact that $P$ is an $\mathbb{F}_q$-point of $G_1 = 0$ implies $G_2(P) = 0 = G_1(P)$. Therefore, $P = (x_0, y_0)$, where $y_0 \neq 0$, is a singular point of $y^n - f(x) = 0$, which is a contradiction to $\frac{\partial(y^n - f(x))}{\partial y}(P) \neq 0$.

\[\square\]

Theorem 5.3. Let $f(x) \in \mathbb{F}_q[x]$ be a nonconstant polynomial and $n \geq 1$ be an integer such that $y^n - f(x) \notin \mathbb{F}_q[x^p, y^p]$. Then the irreducible components of $\mathcal{F} : y^n = f(x)$ are $q$-Frobenius nonclassical if and only if $n \mid (q - 1)$ and

$$n \cdot f(x)(f(x)^{\frac{n-1}{n}} - 1) = (x^q - x)f'(x). \quad (29)$$

Proof. Note that if the irreducible components of $\mathcal{F}$ are $q$-Frobenius nonclassical, then (17) in Theorem 3.4 implies

$$T(y^n) = n\theta(y^{q-1+n} - y^n),$$

for some monic polynomial $T \in \mathbb{F}_q[x]$, and $\theta \in \mathbb{F}_q^*$. Therefore,

$$n|(q - 1), T(x) = x(x^{\frac{n-1}{n}} - 1) \quad \text{and} \quad \theta = 1/n,$$

and then (29) follows when (17) is applied to $f(x)$. Conversely, if $n|(q - 1)$ and (29) holds, then one can readily verify that $y^n = f(x)$ has a solution in $\mathbb{F}_q \times \mathbb{F}_q^*$. Thus from Lemma 5.2, the irreducible components of $\mathcal{F}$ are defined over $\mathbb{F}_q$. Now, since (29) implies (17) for $T(x) = x(x^{\frac{n-1}{n}} - 1)$ and $\theta = 1/n$, the result follows from Theorem 3.4.

\[\square\]
Corollary 5.4. Notation and hypotheses as in Theorem 5.3. If the components of $F : y^n = f(x)$ are $q$-Frobenius nonclassical, then

(i) $p \nmid n$ and $f' \neq 0$.

(ii) $\frac{nq}{n + q - 1} \leq \deg f \leq n$, and the upper bound (resp. lower bound) for $\deg f$ is attained if and only if $p \nmid \deg f$ (resp. $f'$ is constant).

(iii) if $f = c \prod_{i=1}^{s} (x - a_i)^{k_i} \in \mathbb{F}_q[x]$, then $a_i \in \mathbb{F}_q$ if and only if $p \nmid k_i$. In particular, all simple roots of $f$ lie in $\mathbb{F}_q$.

(iv) $f$ has an $\mathbb{F}_q$-root, and if $f$ has a simple root, then $n \equiv 1 \mod p$.

(v) $n \equiv 1 \mod p$ if and only if $f'' = 0$.

(vi) if an $\mathbb{F}_q$-root of $f$ has multiplicity $k$, where $0 < k < \deg f$, then $k \leq \frac{n-1}{|V_f|}$ and $k \equiv n \mod p$.

Proof. (i) From equation (29), $p \nmid n$ if and only if $f' \neq 0$. Since $n|(q - 1)$ the result follows.

(ii) Equating degrees on both side of (29) yields

$$\left(\frac{q-1}{n} + 1\right) \deg f = \deg f' + q.$$  

Using both inequalities of $0 \leq \deg f' \leq \deg f - 1$ gives the result.

(iii) Since $f \in \mathbb{F}_q[x]$ satisfies equation (7) in Theorem 2.2, this follows directly from Lemma 2.3 (i), (ii).

(iv) Since $0 \in V_{y^n} = V_f$, it is obvious that $f$ has an $\mathbb{F}_q$-root. Differentiating both sides of (29) gives

$$(n-1)f'(x)(f(x)^{\frac{n-1}{n}} - 1) = (x^q - x)f''(x). \quad (30)$$

If $x_0 \in \mathbb{F}_q$ is a simple root of $f$, then Lemma 2.3 implies $x_0 \in \mathbb{F}_q$. Thus evaluating both sides of (30) at a simple root of $f$, we arrive at $n \equiv 1 \mod p$.

(v) Using that $f' \neq 0$, the claim follows directly from equation (30).
(vi) From Lemma 5.1, we may assume that \( \deg f = n - k \). Now item (ii) above implies \( n - k \geq \frac{nq}{n + q - 1} \), and then \( k \leq \frac{n - 1}{1 + \frac{q - 1}{n}} = \frac{n - 1}{\sqrt{q}} \), which proves the first assertion. Also, since \( \deg f = n - k < n \), again from item (ii), we have \( p | (n - k) \), which finishes the proof.

The following result retrieves [7, Theorem 2] and the “Remark” in [8, p. 38]. We will see that the hypotheses \( p \neq 2 \) and \( p \nmid nd \), included therein, are not necessary.

**Corollary 5.5.** Let \( a, b \in \mathbb{F}_q^* \), and let \( n \) and \( d \) be positive integers. If

\[
F : y^n = ax^d + b
\]

is \( q \)-Frobenius nonclassical curve, then \( F \) is a Fermat curve of degree \( n = d = \frac{q - 1}{q' - 1} \), and \( a, b \in \mathbb{F}_q^* \).

**Proof.** The curves \( y^n = ax^d + b \) and \( x^d = y^n/a - b/a \) are clearly the same. Thus Corollary 5.4 (ii) gives \( n = d \). Since \( p \nmid d \), the polynomial \( f(x) = ax^d + b \) has no repeated roots, and from Corollary 5.4 (v), we have \( n \equiv 1 \mod p \). Now equation (29) yields

\[
(ax^d + b)(ax^d + b)^{q - 1} - 1 = (x^q - 1)ax^d,
\]

and then

\[
(ax^d + b)^{q - 1} = ax^{d+q-1} + b.
\]

However, such a polynomial identity holds if and only if \( \frac{2q - 1}{d} + 1 = q' \), that is, \( d = \frac{q - 1}{q' - 1} \). Clearly this also implies \( b^d = b \) and \( a^d = a \), as claimed.

**Remark 5.2.** Note that any irreducible curve \( F : y^n = f(x) \), defined over \( \mathbb{F}_q \) and not meeting the conditions/results established in this section, must satisfy the Stöhr-Voloch bound for \( \nu = 1 \) (cf. (2) in Section 1):

\[
\# F(\mathbb{F}_q) \leq g - 1 + d(q + 2)/2.
\]

As mentioned previously, the characterization of Frobenius nonclassical curves is motivated in part by the need to identify the curves for which (31)
may not hold. This gives a rather nice bound applicable for the remaining curves. For a simple illustration, consider the following curve over $\mathbb{F}_5^3$:

$$\mathcal{F} : y^{62} = x^{62} + (x + 1)^{62} + 1.$$  

It is easy to see that $f(x) = x^{62} + (x + 1)^{62} + 1$ has no repeated roots. Therefore, since $62 \not\equiv 1 \mod 5$, Corollary 5.4 (iv) fails, and so bound (31) holds. That is,

$$\#\mathcal{F}(\mathbb{F}_{125}) \leq (62 - 1)(62 - 2)/2 - 1 + 62(5^3 + 2)/2 = 5766.$$  

Interestingly, it turns out that 5766 is the actual value of $\#\mathcal{F}(\mathbb{F}_{125})$.

### 5.1. Additional Remarks

In what follows, we provide some additional facts related to Frobenius nonclassical curves of type $y^n = f(x)$. Some well-known examples of this type of Frobenius nonclassical curve are

- $y^{q+1} = x^q + x$ (the Hermitian curve over $\mathbb{F}_{q^2}$).
- $x^{\frac{q^k - 1}{q - 1}} + y^{\frac{q^k - 1}{q - 1}} = 1$ (the Fermat curves over $\mathbb{F}_{q^k}$).
- $y^{\frac{q^k - 1}{q - 1}} = x^{\frac{q^k - 1}{q - 1}} + (x^{q^k - 1} + \cdots + x^q + x)$, over $\mathbb{F}_{q^k}$ (see [10, Remark 2.9]).

Note that in the preceding cases, we have $n = \frac{q^k - 1}{q - 1}$. The next result generalizes these examples.

**Theorem 5.6.** Let $f(x) \in \mathbb{F}_{q^k}[x]$ be a nonconstant polynomial, and let $\mathcal{W}$ be the set of MVSPs defined in (13). The components of the curve $y^{\frac{q^k - 1}{q - 1}} = f(x)$ are $q$-Frobenius nonclassical if and only if $f(x) \in \mathcal{W}$. Moreover, a curve $y^{\frac{q^k - 1}{q - 1}} = f(x)$, with $f(x) \in \mathcal{W}$, is irreducible with probability at least $1 - 1/q$.

**Proof.** The first statement follows immediately from Corollary 3.5, since $g(y) = y^{\frac{q^k - 1}{q - 1}} \in \mathcal{W}$. For the second, let $f(x) \in \mathcal{W}$ be a fixed MVSP, and consider the $q$ polynomials $f_i := f(x) + \alpha_i \in \mathcal{W}$, where $\alpha_i \in \mathbb{F}_q$. It follows from [3, Lemma 2.4 (ii)] that at most one such $f_i$ has no simple root. So out of the $\#\mathcal{W} = q^{2k} - q$ (cf. Remark 2.2) curves $y^{\frac{q^k - 1}{q - 1}} = f(x)$, with $f(x) \in \mathcal{W}$, at most $(q^{2k} - q)/q$ curves will be reducible. That is, the probability of being reducible is no greater than $\frac{(q^{2k} - q)/q}{q^{2k} - q} = 1/q$, which gives the result. 

\[\square\]
Remark 5.3. Recall that a detailed description of $W$ in the case $k = 2$ is given in (14). From that, it can be verified that all irreducible curves $y^{q+1} = f(x)$ arising from Theorem 5.6 are $\mathbb{F}_q$-isomorphic to the Hermitian curve.

Hefez and Voloch [12, Theorem 1] have proved that if $F$ a plane smooth $q$-Frobenius nonclassical curve of degree $n$, then

$$\# F(\mathbb{F}_q) = n(q - n + 2).$$

(32)

Next we show that for $q$-Frobenius nonclassical curves of type $y^n = f(x)$, the number given in (32) is, in fact, a lower bound for $\# F(\mathbb{F}_q)$. So as far as the number of rational points is concerned, the singular curves $y^n = f(x)$ may be of considerable interest.

Theorem 5.7. Let $f(x) \in \mathbb{F}_q[x]$ be a nonconstant polynomial and $F : y^n = f(x)$ be a $q$-Frobenius nonclassical curve. Then

$$\# F(\mathbb{F}_q) \geq n(q - n + 2),$$

and equality holds if and only if $F$ is smooth.

Proof. In view of (32), we only need to prove that if $F$ is singular, then $\# F(\mathbb{F}_q) > n(q - n + 2)$. Let $r$ be the number of distinct $\mathbb{F}_q$-roots of $f(x)$, so by Corollary 5.4 we have

$$1 \leq r \leq \deg f \leq n.$$

From Corollary 3.5, $f(x)$ and $g(y) = y^n$ are MVSPs with $V_f = V_g$. In particular, $n|(q - 1)$. Thus the $q - r$ nonroots of $f(x)$ in $\mathbb{F}_q$ will give rise to $n(q - r)$ affine $\mathbb{F}_q$-points of $F$. Now assume that $F$ is singular and $\# F(\mathbb{F}_q) \leq n(q - n + 2)$.

First, let us consider the case $r \in \{n - 1, n\}$. If $f(x)$ is separable, then $\# F(\mathbb{F}_q) > n(q - n + 2)$. Let $r$ be the number of distinct $\mathbb{F}_q$-roots of $f(x)$, so by Corollary 5.4 we have

$$1 \leq r \leq \deg f \leq n.$$

From Corollary 3.5, $f(x)$ and $g(y) = y^n$ are MVSPs with $V_f = V_g$. In particular, $n|(q - 1)$. Thus the $q - r$ nonroots of $f(x)$ in $\mathbb{F}_q$ will give rise to $n(q - r)$ affine $\mathbb{F}_q$-points of $F$. Now assume that $F$ is singular and $\# F(\mathbb{F}_q) \leq n(q - n + 2)$. In particular, $n(q - r) \leq n(q - n + 2)$ i.e. $r \geq n - 2$.

First, let us consider the case $r \in \{n - 1, n\}$. If $f(x)$ is separable, then $\# F(\mathbb{F}_q) > n(q - n + 2)$. Let $r$ be the number of distinct $\mathbb{F}_q$-roots of $f(x)$, so by Corollary 5.4 we have

$$1 \leq r \leq \deg f \leq n.$$

From Corollary 3.5, $f(x)$ and $g(y) = y^n$ are MVSPs with $V_f = V_g$. In particular, $n|(q - 1)$. Thus the $q - r$ nonroots of $f(x)$ in $\mathbb{F}_q$ will give rise to $n(q - r)$ affine $\mathbb{F}_q$-points of $F$. Now assume that $F$ is singular and $\# F(\mathbb{F}_q) \leq n(q - n + 2)$ i.e. $r \geq n - 2$.

First, let us consider the case $r \in \{n - 1, n\}$. If $f(x)$ is separable, then $\# F(\mathbb{F}_q) > n(q - n + 2)$. Let $r$ be the number of distinct $\mathbb{F}_q$-roots of $f(x)$, so by Corollary 5.4 we have

$$1 \leq r \leq \deg f \leq n.$$

From Corollary 3.5, $f(x)$ and $g(y) = y^n$ are MVSPs with $V_f = V_g$. In particular, $n|(q - 1)$. Thus the $q - r$ nonroots of $f(x)$ in $\mathbb{F}_q$ will give rise to $n(q - r)$ affine $\mathbb{F}_q$-points of $F$. Now assume that $F$ is singular and $\# F(\mathbb{F}_q) \leq n(q - n + 2)$ i.e. $r \geq n - 2$.

First, let us consider the case $r \in \{n - 1, n\}$. If $f(x)$ is separable, then $\# F(\mathbb{F}_q) > n(q - n + 2)$. Let $r$ be the number of distinct $\mathbb{F}_q$-roots of $f(x)$, so by Corollary 5.4 we have

$$1 \leq r \leq \deg f \leq n.$$

From Corollary 3.5, $f(x)$ and $g(y) = y^n$ are MVSPs with $V_f = V_g$. In particular, $n|(q - 1)$. Thus the $q - r$ nonroots of $f(x)$ in $\mathbb{F}_q$ will give rise to $n(q - r)$ affine $\mathbb{F}_q$-points of $F$. Now assume that $F$ is singular and $\# F(\mathbb{F}_q) \leq n(q - n + 2)$ i.e. $r \geq n - 2$.

First, let us consider the case $r \in \{n - 1, n\}$. If $f(x)$ is separable, then $\# F(\mathbb{F}_q) > n(q - n + 2)$. Let $r$ be the number of distinct $\mathbb{F}_q$-roots of $f(x)$, so by Corollary 5.4 we have

$$1 \leq r \leq \deg f \leq n.$$
6. Final Remarks

In this section, we provide some additional examples, and briefly discuss some problems related to Frobenius nonclassical curves.

In Sections 3 and 4, we offered some examples of \( q^k \)-Frobenius nonclassical curves \( f(x) = g(y) \), where \( f \) and \( g \) are polynomials given by the set \( W \) in (13). Given the potentially relevant properties of the curves arising in this way, it could be beneficial to characterize them further. One nice example is the so-called generalized Hermitian curve

\[
\mathcal{GS} : y^{q^k-1} + \cdots + y^q + y = x^{q^k+1} + x^{q^k+q^2} + \cdots + x^{q^k+q^k-2} \tag{33}
\]

over \( \mathbb{F}_{q^k} \) \((k \geq 2)\), which was introduced by Garcia and Stichtenoth [9]. They proved that \( \mathcal{GS} \) has genus \( g = q^{n-1}(q^{n-1} - 1)/2 \) and \( N = q^{2k-1} + 1 \) \( \mathbb{F}_{q^k} \)-rational points. Some authors have used additional arithmetic properties of this curve to construct algebraic geometric codes with good parameters (see [4], [20], [21]).

To see that \( \mathcal{GS} \) is indeed \( q^k \)-Frobenius nonclassical, note that the polynomial \( f(x) \) on the right side of (33) is defined as \( f(x) = s_2(x, x^q, \ldots, x^{q^{k-1}}) \), where

\[
s_2(x_1, x_2, \ldots, x_n) = \sum_{i<j} x_i x_j
\]

is the second elementary symmetric polynomial. Therefore \( f \in \mathbb{F}_{q^k}[x] \) is a polynomial of degree \( q^{k-2} + q^{k-1} \leq q^{k-1} \) such that \( V_f \subseteq \mathbb{F}_q \). Thus from [3, Lemma 4.1], \( f \in \mathbb{F}_{q^k}[x] \) is an MVSP with \( V_f = \mathbb{F}_q \). Clearly, \( g(y) = y^{q^k-1} + \cdots + y^q + y \in \mathbb{F}_{q^k}[x] \) is an MVSP with \( V_g = \mathbb{F}_q \) as well. Hence the \( q^k \)-Frobenius nonclassicality of \( \mathcal{GS} \) follows from Corollary 3.5.

A natural question is whether the curve \( \mathcal{GS} \) can be further generalized. For instance, one way of doing that is to identify a family of polynomials \( \{ f_i(x) \} \subseteq W \) for which some of the curves

\[
y^{q^{k-1}} + \cdots + y^q + y = f_i(x) \tag{34}
\]

have a good ratio \( N/g \). That is to say at least as good as the corresponding ratio for the curve \( \mathcal{GS} \). Regarding this particular class of curves, we have made some progress which we hope to report in the near future. However, there is certainly room for additional research, some of which can be quite challenging. For instance, consider the irreducible curves over \( \mathbb{F}_{q^k} \)

\[
F_{a,b} : y^{q^k-1} = \frac{x^{q^k-1}}{q^k-1} + a(x^{q^k-1} + \cdots + x^q + x) + b,
\]
where \( a, b \in \mathbb{F}_q \). It is not hard to see that computing the genus and the number of \( \mathbb{F}_{q^k} \)-rational points of \( \mathcal{F}_{a,b} \) boils down to determining the cardinality \( N_{k-1}(u,v) \) of
\[
\{ \alpha \in \mathbb{F}_{q^k-1} \mid T(\alpha) = u \text{ and } N(\alpha) = v \},
\]
(35)
where \( u, v \in \mathbb{F}_q \), and \( T, N : \mathbb{F}_{q^k-1} \to \mathbb{F}_q \) are the trace and norm functions, respectively. Apart from a few particular cases, determining \( N_{k-1}(u,v) \) is still an open problem. Nicolas Katz [15] used deep results from algebraic geometry to set bounds for the number \( N_{k-1}(u,v) \). More recently, Moisio and Wan [19] used results on the zeta function of certain toric Calabi-Yau hypersurfaces to improve Katz’s bound. Part of the motivation to determine \( N_{k-1}(u,v) \) is given by its known connections with many other problems (e.g. [14],[18],[24]). Accordingly, this new relation with certain Frobenius nonclassical curves establishes an additional motivation.

6.1. Some curves \( y^{q^k-1} = f(x) \)

Recall from Theorem 5.3 that the \( \mathbb{F}_{q^k} \)-Frobenius nonclassical curves of type \( y^{q^k-1} = f(x) \) are irreducible ones for which \( f(x) \) satisfies
\[
f(x)(f(x) - 1) = (x - x^{q^k})f'(x).
\]
We know (see proof of Theorem 5.3) that the polynomial \( f(x) \) must be of type \( B \), i.e., \( f = 1 - \frac{g'}{g}(x - x^{q^k}) \) where
\[
g \text{ is a monic divisor of } x^{q^k} - x \text{ such that } g'' = 0.
\]
As was noted previously, such polynomials \( f \in \mathbb{F}_{q^k}[x] \) can be easily constructed. The following result is an explicit example arising from this construction.

**Theorem 6.1.** If \( k \geq 3 \), then the curve
\[
\mathcal{F} : y^{q^k-1} = 1 - \frac{x^{q^k} - x}{x^q - x}
\]
is \( \mathbb{F}_{q^k} \)-Frobenius nonclassical of genus
\[
g(\mathcal{F}) = \frac{(q^k - 2)(q^{k-1} - 1) - (q + 1)(q - 2)}{2},
\]
and has at least \((q^k - 1)(q^{k-1} - q)\) \( \mathbb{F}_{q^k} \)-rational points. Moreover, if \( q = 2 \) then its number of rational points is \((2^k - 1)(2^k - 2) + 3\).
Proof. Note that $f(x) = 1 - x^{q^k - 1}$ is the polynomial of degree $\deg f = q^k - q$ given by
\[
f(x) = (x^q - x)^{q-1} \prod_{\alpha \in \mathbb{F}_{q^k - 1}\setminus \mathbb{F}_q} (x - \alpha)^q.
\]
Since $k \geq 3$, there exist two roots of $f(x)$ whose multiplicities are coprime. Therefore, the curve $\mathcal{F}$ is irreducible. The genus follows directly from the Hurwitz-Zeuthen formula (see e.g. [22]).

Note that for $g(x) = x^q - x \in \mathbb{F}_{q^k}[x]$, we have $\frac{g'}{g}(x^q - x) = \frac{x^{q^k - 1} - x}{x^q - x} \in \mathcal{A}$, and then $f := 1 - \frac{x^{q^k - 1} - x}{x^q - x} \in \mathcal{B}$. Therefore, $\mathcal{F}$ is $\mathbb{F}_{q^k}$-Frobenius nonclassical. The first assertion about the number of $\mathbb{F}_{q^k}$-rational points, follows (similarly to the proof of Theorem 5.7) directly from the fact that $f(x)$ has exactly $q$ $\mathbb{F}_{q^k}$-roots. If $q = 2$, the three additional points come from ramification points over the places $P_x, P_{x-1}$ and $P_{\infty}$. This finishes the proof.

Remark 6.1. It can be checked that some of the current records of curves with many points, listed at http://www.manypoints.org, are held by Frobenius nonclassical curves. For an example, note that for the case $q = 2$ in Theorem 6.1, the values $k = 3$ and $k = 4$ yield $(g(\mathcal{F}), \#\mathcal{F}(\mathbb{F}_8)) = (9, 45)$ and $(g(\mathcal{F}), \#\mathcal{F}(\mathbb{F}_{16})) = (49, 213)$, respectively. Both cases are current records listed at http://www.manypoints.org.

We turn our attention to an object in Finite Geometry that was investigated in connection with Frobenius nonclassical curves in [10].

An $(N, d)$-arc is a subset of $N$ points in $PG(2, q)$ with at most $d$ points on any line and $d$ on some line. The $(N, d)$-arc is called complete if it is not contained in an $(N + 1, d)$-arc. When $\mathcal{F}$ is a projective plane curve of degree $d$, defined over $\mathbb{F}_q$, that intersects at least one line in $d$ distinct $\mathbb{F}_q$-points then $\mathcal{F}(\mathbb{F}_q)$, the set of $\mathbb{F}_q$-points of $\mathcal{F}$, is an example of $(N, d)$-arc. If such $(N, d)$-arc is complete, we say that $\mathcal{F}$ has the arc property.

In [10], the authors proved the arc property for several $q$-Frobenius nonclassical curves and raised the question of whether or not all $q$-Frobenius nonclassical curves have the arc property. In [1], we gave a negative answer to this question using a particular singular curve. The next theorem will provide additional counter-examples, but now arising from nonsingular curves.

**Theorem 6.2.** If $q$ is a power of 2 and $k \geq 3$ is an integer, then the curve
\[
\mathcal{F} : y^{q^k - 1} = \frac{x^{q^k} - x}{x^q - x}
\]
is \(q^k\)-Frobenius nonclassical. Moreover, if \(q = 2\) then \(\mathcal{F}\) is smooth and does not have the arc property.

**Proof.** Note that \(f(x) = \frac{x^{q^n} - x}{x^q - x}\) has no repeated roots, and so the curve \(\mathcal{F}\) is irreducible. Its \(q^k\)-Frobenius nonclassicality follows directly from (29) in Theorem 5.3. It is clear that for \(q = 2\), \(\mathcal{F}\) is a smooth curve of degree \(d = q^k - 1\). In this case, the Hefez-Voloch formula in (32) gives

\[
\#\mathcal{F}(\mathbb{F}_{q^k}) = d(q^k - d + 2) = 3d.
\]

Now one can easily check that these 3\(d\) rational points of \(\mathcal{F}\) lie on the union of lines given by \(xy(x - z) = 0\), with \(d = q^k - 1\) point on each line. Let \(P \in PG(2,q^k)\) be a point on the complement of the union of these three lines. Clearly, any line incident to \(P\) will intersect this set of \(3d\) points in at most 3 points. Since \(k > 2\), we have \(d = 2^k - 1 > 3\), and so the arc is not complete.

\(\square\)

7. Acknowledgments

I thank Felipe Voloch for so many insightful discussions and comments during the course of this project. I would like to thank Michael Zieve for pointing out that a result proved in a previous version of this paper, namely Lemma 3.1, was known and due to Michael D. Fried and R. E. MacRae. I also thank James Hirschfeld for giving several suggestions to improve the presentation of this manuscript.

The author was partially supported by FAPESP-Brazil grant 2011/19446-3.

References

[1] Herivelto Borges. On complete \((N,d)\)-arcs derived from plane curves. *Finite Fields Appl.*, 15(1):82–96, 2009.

[2] Herivelto Borges. On multi-Frobenius non-classical plane curves. *Arch. Math. (Basel)*, 93(6):541–553, 2009.

[3] Herivelto Borges and Ricardo Conceição. On the characterization of minimal value set polynomials. *J. Number Theory*, 133(6):2021–2035, 2013.

[4] S. V. Bulygin. Generalized Hermitian codes over GF(\(2^r\)). *IEEE Trans. Inform. Theory*, 52(10):4664–4669, 2006.
[5] L. Carlitz, D. J. Lewis, W. H. Mills, and E. G. Straus. Polynomials over finite fields with minimal value sets. *Mathematika*, 8:121–130, 1961.

[6] Michael D. Fried and R. E. MacRae. On curves with separated variables. *Math. Ann.*, 180:220–226, 1969.

[7] A. García and J. F. Voloch. Fermat curves over finite fields. *J. Number Theory*, 30(3):345–356, 1988.

[8] Arnaldo García. The curves $y^n = f(x)$ over finite fields. *Arch. Math. (Basel)*, 54(1):36–44, 1990.

[9] Arnaldo Garcia and Henning Stichtenoth. A class of polynomials over finite fields. *Finite Fields Appl.*, 5(4):424–435, 1999.

[10] Massimo Giulietti, Fernanda Pambianco, Fernando Torres, and Emanuela Ughi. On complete arcs arising from plane curves. *Des. Codes Cryptogr.*, 25(3):237–246, 2002.

[11] Abramo Hefez. On the value sets of special polynomials over finite fields. *Finite Fields Appl.*, 2(4):337–347, 1996.

[12] Abramo Hefez and José Felipe Voloch. Frobenius nonclassical curves. *Arch. Math. (Basel)*, 54(3):263–273, 1990.

[13] J. W. P. Hirschfeld, G. Korchmáros, and F. Torres. *Algebraic curves over a finite field*. Princeton Series in Applied Mathematics. Princeton University Press, Princeton, NJ, 2008.

[14] Sophie Huczynska and Stephen D. Cohen. Primitive free cubics with specified norm and trace. *Trans. Amer. Math. Soc.*, 355(8):3099–3116 (electronic), 2003.

[15] Nicholas M. Katz. Estimates for Soto-Andrade sums. *J. Reine Angew. Math.*, 438:143–161, 1993.

[16] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn.

[17] W. H. Mills. Polynomials with minimal value sets. *Pacific J. Math.*, 14:225–241, 1964.

[18] Marko Moisio. Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm. *Acta Arith.*, 132(4):329–350, 2008.
[19] Marko Moisio and Daqing Wan. On Katz’s bound for the number of elements with given trace and norm. *J. Reine Angew. Math.*, 638:69–74, 2010.

[20] C. Munuera, A. Sepúlveda, and F. Torres. Generalized Hermitian codes. *Des. Codes Cryptogr.*, 69(1):123–130, 2013.

[21] Carlos Munuera, Alonso Sepúlveda, and Fernando Torres. Castle curves and codes. *Adv. Math. Commun.*, 3(4):399–408, 2009.

[22] Henning Stichtenoth. *Algebraic function fields and codes*. Universitext. Springer-Verlag, Berlin, 1993.

[23] Karl-Otto Stöhr and José Felipe Voloch. Weierstrass points and curves over finite fields. *Proc. London Math. Soc. (3)*, 52(1):1–19, 1986.

[24] Daqing Wan. Generators and irreducible polynomials over finite fields. *Math. Comp.*, 66(219):1195–1212, 1997.