ACADÉMIE
DES SCIENCES
INSTITUT DE FRANCE

Comptes Rendus
Mathématique

Giorgos Kapetanakis and Lucas Reis

Normal points on Artin–Schreier curves over finite fields

Volume 363 (2025), p. 541-554

Online since: 5 June 2025

https://doi.org/10.5802/crmath.740

The Comptes Rendus. Mathématique *are a member of the*
Mersenne Center for open scientific publishing
www.centre-mersenne.org — e-ISSN : 1778-3569

ACADÉMIE DES SCIENCES
INSTITUT DE FRANCE

Comptes Rendus. Mathématique
2025, Vol. 363, p. 541-554
https://doi.org/10.5802/crmath.740

Research article / *Article de recherche*
Algebra, Number theory / *Algèbre, Théorie des nombres*

Normal points on Artin–Schreier curves over finite fields

Points normaux sur les courbes d'Artin–Schreier sur des corps finis

Giorgos Kapetanakis [a] **and Lucas Reis** [b]

[a] Department of Mathematics, University of Thessaly, 3rd km Old National Road Lamia–Athens, 35100, Lamia, Greece

[b] Departamento de Matemática, Universidade Federal de Minas Gerais, UFMG, Belo Horizonte MG, Brazil

E-mails: kapetanakis@uth.gr, lucasreismat@mat.ufmg.br

Abstract. In 2022, S. D. Cohen and the two authors introduced and studied the concept of (r,n)-freeness on finite cyclic groups G for suitable integers r, n, which is an arithmetic way of capturing elements of special forms that lie in the subgroups of G. Combining this machinery with some character sum techniques, they explored the existence of points (x_0,y_0) on affine curves $y^n = f(x)$ defined over a finite field $\mathbb{F}$ whose coordinates are generators of the multiplicative cyclic group $\mathbb{F}^*$. In this paper we develop the natural additive counterpart of this work for finite fields. Namely, any finite extension $\mathbb{E}$ of a finite field $\mathbb{F}$ with Q elements is a cyclic $\mathbb{F}[x]$-module induced by the Frobenius automorphism $\alpha \mapsto \alpha^Q$, and any generator of this module is said to be a normal element over $\mathbb{F}$. We introduce and study the concept of (f,g)-freeness on this module structure for suitable polynomials $f,g \in \mathbb{F}[x]$. As a main application of the machinery developed in this paper, we study the existence of $\mathbb{F}_{p^n}$-rational points in the Artin–Schreier curve $\mathfrak{A}_f : y^p - y = f(x)$ whose coordinates are normal over the prime field $\mathbb{F}_p$ and establish concrete results.

Résumé. En 2022, S. D. Cohen et les deux auteurs ont introduit et étudié le concept de (r,n)-liberté dans les groupes cycliques finis G pour des entiers convenables r et n. Ce concept constitue une approche arithmétique permettant de capturer des éléments de formes spéciales qui appartiennent aux sous-groupes de G. En combinant cet outil avec certaines techniques de sommes de caractères, ils ont exploré l'existence de points (x_0,y_0) sur des courbes affines de la forme $y^p - y = f(x)$, définies sur un corps fini $\mathbb{F}$, dont les coordonnées sont des générateurs du groupe cyclique multiplicatif $\mathbb{F}^*$. Dans cet article, nous développons le pendant additif naturel de ce travail pour les corps finis. Plus précisément, toute extension finie $\mathbb{E}$ d'un corps fini $\mathbb{F}$ à Q éléments est un module cyclique sur $\mathbb{F}[x]$, induit par l'automorphisme de Frobenius $\alpha \mapsto \alpha^Q$, et tout générateur de ce module est appelé un élément normal sur $\mathbb{F}$. Nous introduisons et étudions le concept de (f,g)-liberté dans cette structure de module pour des polynômes convenables f et g dans $\mathbb{F}[x]$. Comme principale application de la théorie développée dans cet article, nous examinons l'existence de points rationnels sur $\mathbb{F}_{p^n}$ dans la courbe d'Artin–Schreier $\mathfrak{A}_f : y^p - y = f(x)$, dont les coordonnées sont normales sur le corps premier $\mathbb{F}_p$, et nous établissons des résultats concrets.

Keywords. Finite fields, character sums, normal elements, free elements, Artin–Schreier curves.

Mots-clés. Corps finis, sommes de caractères, éléments normaux, éléments libres, courbes d'Artin–Schreier.

2020 Mathematics Subject Classification. 11T30, 11T06, 11T23.

Funding. The second author was supported by FAPEMIG grant APQ-01712-23, CNPq grant 309844/2021-5 and CAPES – Brazil (Finance Code 001).

Manuscript received 10 December 2024, revised 7 March 2025, accepted 12 March 2025.

1. Introduction

Let q be a power of the prime p and, for each positive integer n, let $\mathbb{F}_{q^n}$ be the finite field with q^n elements. The field $\mathbb{F}_{q^n}$ has interesting structures related to the two basic field operations. Namely, the multiplicative group $\mathbb{F}_{q^n}^* = \mathbb{F}_{q^n} \setminus \{0\}$ is cyclic and any generator of such group is a *primitive element*. On the other hand, regarding the additive structure of $\mathbb{F}_{q^n}$, we can view $\mathbb{F}_{q^n}$ as an $\mathbb{F}_q[x]$-module induced by the Frobenius map $\alpha \mapsto \alpha^q$, namely

$$\sum_{i=0}^{m} a_i x^i \circ \alpha := \sum_{i=0}^{m} a_i \alpha^{q^i}.$$

It turns out that in this setting $\mathbb{F}_{q^n}$ is also cyclic and, regarding $\mathbb{F}_{q^n}$ as an $\mathbb{F}_q$-vector space, this means that there exists an $\mathbb{F}_q$-basis of the form $\{\beta, \beta^q, \dots, \beta^{q^{n-1}}\}$. In this case, any such $\beta \in \mathbb{F}_q$ is a *normal element* over $\mathbb{F}_q$. Both primitive and normal elements were extensively studied in the past decades, mainly motivated by theoretical problems, but also practical issues where such elements are employed. For instance, primitive elements are used in cryptographic applications such as the discrete logarithm problem (most notably, the Diffie–Hellman key exchange [6]). Moreover, normal elements can be useful in generic situations where finite field arithmetic is performed; see [7] for an overview on normal elements, and their theoretical and practical aspects.

In 1987, Lenstra and Schoof [10] proved that, for every prime power q and every positive integer $n \geq 2$, there exists an element $\alpha \in \mathbb{F}_{q^n}$ that is simultaneously primitive and normal over $\mathbb{F}_q$. This is widely known as the *Primitive Normal Basis Theorem* (PNBT). A crucial tool in the proof of the PNBT is to provide expressions for the characteristic functions of normal and primitive elements in finite fields by means of additive and multiplicative characters, respectively. The latter is obtained through the concept of *freeness*, which is a convenient way to capture elements that can be written in special forms when one considers the aforementioned cyclic group and $\mathbb{F}_q[x]$-module structure of finite fields. For more details, see [8, Definition 5.1]. In the original proof by Lenstra and Schoof [10], after some algebraic computations and estimates on certain character sums, the PNBT is proved up to a finite number of pairs (q, n). For these remaining pairs, the theorem is verified by direct computer search. A computer-free proof of the PNBT was later given by Cohen and Huczynska in 2003 in [4].

In the past decade, questions related to the PNBT have been proposed and many results have been established. In this context, a recurrent object of study is the existence of pairs of elements $\big(\alpha, f(\alpha)\big) \in \mathbb{F}_q \times \mathbb{F}_q$, $f \in \mathbb{F}_q(x)$ with special properties related to the multiplicative and additive structure of $\mathbb{F}_q$ (e.g., prescribed multiplicative order or k-normality[1]). Although the number of works in this line of research is extensive, we refer the interested reader, for example, to [3,9] and the references therein. Such pairs can be viewed as points (x_0, y_0) on affine curves $y = f(x)$ whose coordinates x_0, y_0 have the aforementioned properties. Motivated by the latter, in [5] the authors explore the existence of points $(x_0, y_0) \in \mathbb{F}_q \times \mathbb{F}_q$ on affine curves $y^n = f(x)$ such that x_0 and y_0 are both primitive elements of $\mathbb{F}_q$. In order to obtain existence results on the latter they generalized the concept of freeness for generic multiplicative finite cyclic groups, culminating in a character sum expression for the set of elements in $\mathbb{F}_{q^n}^*$ with prescribed multiplicative order.

In this paper we develop the natural additive counterpart of the concepts and results that are provided in [5]. Towards this end, we first present some background material in Section 2, then we introduce and study (f, g)-freeness for the additive structure of $\mathbb{F}_{q^n}$ in Sections 3 and 4. Finally, in Section 5 we confine ourselves to extensions over the prime field $\mathbb{F}_p$ and employ the developed theory, in order to study the existence of $\mathbb{F}_q$-rational points in the Artin–Schreier curve

[1] For the formal definition and basic properties of k-normal elements, see [8].

$\mathfrak{A}_f : y^p - y = f(x)$ with $\mathbb{F}_p$-normal coordinates. In particular, our main result is the following theorem.

Theorem 1. *Let $q = p^n$ be a prime power, where $n \geq 5$ and let $f \in \mathbb{F}_q[x]$ be a polynomial that is not of the form $ax^p + bx + c$ with $a, b, c \in \mathbb{F}_q$ satisfying $1 < \deg(f) \leq p+1$. Then there exists a point $(x_0, y_0) \in \mathbb{F}_q \times \mathbb{F}_q$ in the Artin–Schreier curve $\mathfrak{A}_f : y^p - y = f(x)$ such that both x_0, y_0 are normal over $\mathbb{F}_p$, provided that $(n,p) \neq (5,2), (5,5), (6,2), (6,3)$ or $(6,7)$.*

Remark 2. Theorem 1 entails that the pairs $(n,p) = (5,2), (5,5), (6,2), (6,3)$ and $(6,7)$ are *possible* exceptions, not necessarily genuine exceptions. However, a computer check reveals that the cases $(5,2)$ and $(6,2)$ are indeed genuine exceptions to Theorem 1: note that in this case we necessarily have $\deg(f) = 3$. For the pair $(5,2)$ we get exactly 4 exceptions while for the pair $(6,2)$ we get thousands of exceptions. For the remaining pairs, the number of possible f's is extremely large (about $p^{n(p+1)}$) and we were not able to check them fully, so we get no conclusion for them.

Remark 3. In this work, we employ the so-called *prime sieve*, see Theorem 24. In [2], an improvement of this technique, called the *modified prime sieve*, was introduced. However, the three *possible* exceptions, $(n,p) = (5,5), (6,3)$ and $(6,7)$, see Theorem 1 and Remark 2, fail to pass the resulting condition even if the modified prime sieve is employed.

2. Preparation

This section provides background material that will be used along the way. Throughout this paper, q is a prime power and $\mathbb{F}_q$ is the finite field with q elements, $\mathbb{F}_{q^n}$ is its extension of degree n and $\overline{\mathbb{F}}_q$ is its algebraic closure.

2.1. *Some arithmetic functions over $\mathbb{F}_q[x]$*

We present some arithmetic functions defined over polynomials that are further used.

Definition 4. *Let $f, g \in \mathbb{F}_q[x]$ be nonzero polynomials.*

(i) *We set $f_{(g)} = \frac{f}{\gcd(f,g)}$.*
(ii) *$\Phi_q(f)$ denotes the Euler totient function for polynomials, i.e., $\Phi_q(f) = \#\left(\frac{\mathbb{F}_q[x]}{f\cdot\mathbb{F}_q[x]}\right)^\times$ is the number of invertible cosets modulo $f(x)$.*
(iii) *$W(f)$ stands for the number of monic squarefree divisors of f in $\mathbb{F}_q[x]$.*
(iv) *$\mu_q(f)$ denotes the Möbius function for polynomials over $\mathbb{F}_q$. More precisely, $\mu_q(f) = 0$ if f is not squarefree and $\mu_q(f) = (-1)^r$ if f has $r \geq 0$ distinct irreducible monic divisors, defined over $\mathbb{F}_q$.*
(v) *$|f| = \#\left(\frac{\mathbb{F}_q[x]}{f\cdot\mathbb{F}_q[x]}\right) = q^{\deg f}$ is the number of cosets of $\mathbb{F}_q[x]$ modulo $f(x)$.*

It is well-known that if $\varphi = \Phi_q$, W or μ_q, then $\varphi(F\cdot G) = \varphi(F)\cdot\varphi(G)$ for all relatively prime polynomials $F, G \in \mathbb{F}_q[x]$, i.e., these functions are multiplicative. We will need the following result.

Lemma 5. *For nonzero polynomials $f, g \in \mathbb{F}_q[x]$, we have that*

$$T(f,g) := \sum_{t \mid f} \frac{\left|\mu_q(t_{(g)})\right|}{\Phi_q(t_{(g)})} \cdot \Phi_q(t) = \left|\gcd(f,g)\right| \cdot W\big(\gcd(f, f_{(g)})\big).$$

Proof. We observe that the functions $F_g(f) := \frac{|\mu_q(f_{(g)})|}{\Phi_q(f_{(g)})} \cdot \Phi_q(f)$ and $G_g(f) := \left|\gcd(f,g)\right| \cdot W\big(\gcd(f, f_{(g)})\big)$ are both multiplicative on f. In particular the multiplicativity of $F_g(f)$ implies the multiplicativity of $T(f,g)$ on f. Thus, it suffices to consider the case when f is a power of

an irreducible polynomial. So, we assume that $f = h^\kappa$, where $h \in \mathbb{F}_q[x]$ is irreducible and $\kappa \geq 0$. Further, write $g = h^\lambda r$, where $\lambda \geq 0$ and $\gcd(r,h) = 1$.

First, assume that $\kappa > \lambda$. Then

$$\begin{aligned} T(f,g) &= \sum_{t \mid f} \frac{\left|\mu_q(t_{(g)})\right|}{\Phi_q(t_{(g)})} \cdot \Phi_q(t) \\ &= \sum_{i=0}^{\lambda} \frac{\left|\mu_q(1)\right|}{\Phi_q(1)} \cdot \Phi_q(h^i) + \sum_{i=\lambda+1}^{\kappa} \frac{\left|\mu_q(h^{i-\lambda})\right|}{\Phi_q(h^{i-\lambda})} \cdot \Phi_q(h^i) \\ &= |h^\lambda| + \frac{\Phi_q(h^{\lambda+1})}{\Phi_q(h)} \\ &= 2 \cdot |h^\lambda|. \end{aligned}$$

Also, $\gcd(f,g) = h^\lambda$ and $\gcd(f, f_{(g)}) = h^{\kappa-\lambda}$, hence $G_g(f) = 2 \cdot |h^\lambda| = T(f,g)$.

Next, assume that $\kappa \leq \lambda$. In this case,

$$T(f,g) = \sum_{t \mid f} \frac{\left|\mu_q(t_{(g)})\right|}{\Phi_q(t_{(g)})} \cdot \Phi_q(t) = \sum_{i=0}^{\kappa} \frac{\left|\mu_q(1)\right|}{\Phi_q(1)} \cdot \Phi_q(h^i) = |h^\kappa|,$$

while $\gcd(f,g) = h^\kappa$ and $\gcd(f, f_{(g)}) = 1$, hence $G_g(f) = |h^\kappa| = T(f,g)$. The desired result follows. □

2.2. *The $\mathbb{F}_q$-order of an element in $\overline{\mathbb{F}}_q$*

We start with the following definition.

Definition 6. *For a polynomial $f \in \mathbb{F}_q[x]$ and $\alpha \in \overline{\mathbb{F}}_q$ with $f(x) = \sum_{i=0}^m a_i x^i$, we set $f \circ \alpha = \sum_{i=0}^m a_i \alpha^{q^i}$.*

The existence of normal elements is known for any extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$, see [11, Theorem 2.35]. The following well-known technical results are presented proofless. For more details, see [11, Section 3.4].

Lemma 7. *For any $f, g \in \mathbb{F}_q[x]$ and any $\alpha \in \overline{\mathbb{F}}_q$, we have that $(f+g) \circ \alpha = f \circ \alpha + g \circ \alpha$ and $(f \cdot g) \circ \alpha = f \circ (g \circ \alpha)$.*

Lemma 8. *Fix n a positive integer and $\beta \in \mathbb{F}_{q^n}$ a normal element. Then any $\alpha \in \mathbb{F}_{q^n}$ is written uniquely as $f \circ \beta$ for some $f \in \mathbb{F}_q[x]$ of degree at most $n-1$.*

If $\alpha \in \overline{\mathbb{F}}_q$, notice that $(x^n - 1) \circ \alpha = 0$ if and only if $\alpha^{q^n} - \alpha = 0$, i.e., $\alpha \in \mathbb{F}_{q^n}$. In particular, from Lemma 7, the set $\mathscr{I}_\alpha := \{h \in \mathbb{F}_q[x] \mid h \circ \alpha = 0\}$ is a nonzero ideal of $\mathbb{F}_q[x]$, hence is generated by a unique monic polynomial in $\mathbb{F}_q[x]$. This polynomial, denoted by $\mathrm{Ord}(\alpha)$, is called the *$\mathbb{F}_q$-order* of α.

The following lemma relates the $\mathbb{F}_q$-order of $\alpha = h \circ \beta$ with the $\mathbb{F}_q$-order of β in a natural way. For its proof, see [12, Lemma 2.6].

Lemma 9. *Let $\beta \in \overline{\mathbb{F}}_q$ and fix $g \in \mathbb{F}_q[x]$. If $\alpha = g \circ \beta$, then*

$$\mathrm{Ord}(\alpha) = \frac{\mathrm{Ord}(\beta)}{\gcd\big(\mathrm{Ord}(\beta), g(x)\big)} = \mathrm{Ord}(\beta)_{(g)}.$$

It follows by the definition of $\mathrm{Ord}(\alpha)$ that $\alpha \in \mathbb{F}_{q^n}$ if and only if $\mathrm{Ord}(\alpha) \mid x^n - 1$. From this observation and Lemmas 8 and 9, we readily obtain the following corollaries.

Corollary 10. *An element $\beta \in \mathbb{F}_{q^n}$ is normal over $\mathbb{F}_q$ if and only if* $\mathrm{Ord}(\beta) = x^n - 1$.

Corollary 11. *Let n be a positive integer and $\alpha, \beta \in \mathbb{F}_{q^n}$, where β is normal over $\mathbb{F}_q$. For a monic divisor $f \in \mathbb{F}_q[x]$ of x^n-1, we have that* $\operatorname{Ord}(\alpha) = f$ *if and only if $\alpha = h \circ \beta$, where $h = \frac{x^n-1}{f} \cdot g$ and $g \in \mathbb{F}_q[x]$ is of degree smaller than* $\deg(f)$ *and* $\gcd\big(g, f\big) = 1$. *In particular, for each monic divisor $f \in \mathbb{F}_q[x]$ of x^n-1, there exist $\Phi_q(f)$ elements in $\mathbb{F}_{q^n}$ with $\mathbb{F}_q$-order f.*

2.3. *Additive characters*

Write $q = p^k$. An additive character of $\mathbb{F}_{q^n}$ is a homomorphism ψ between the additive group $(\mathbb{F}_{q^n}, +)$ and the multiplicative group $\mathbb{C}^\times$ of invertible complex numbers. The *canonical* additive character of $\mathbb{F}_{q^n}$, denoted by ψ_1, is the map $\alpha \mapsto \exp\big(\frac{\operatorname{Tr}(\alpha)}{p}\big)$, where $\operatorname{Tr}(\alpha) = \sum_{i=0}^{kn} \alpha^{p^i} \in \mathbb{F}_p$ is the absolute field trace and $\exp(z) = e^{2\pi i z}$ denotes the complex exponential function. The set $\widehat{\mathbb{F}_{q^n}}$ of additive characters of $\mathbb{F}_{q^n}$ forms a multiplicative abelian group whose elements are the characters $\psi_a \colon \mathbb{F}_{q^n} \to \mathbb{C}^\times$, $a \in \mathbb{F}_{q^n}$ with $\psi_a(x) = \psi_1(ax)$; the character ψ_0 maps all the elements of $\mathbb{F}_{q^n}$ to $1 \in \mathbb{C}$ and is called *trivial*. Any other character in $\widehat{\mathbb{F}_{q^n}}$ is called *nontrivial*.

Similarly to the additive group $\mathbb{F}_{q^n}$, the set $\widehat{\mathbb{F}_{q^n}}$ has an $\mathbb{F}_q[x]$-module structure. For $f \in \mathbb{F}_q[x]$ and $\psi \in \widehat{\mathbb{F}_{q^n}}$, the map $x \mapsto \psi(f \circ x)$ defines another character of $\widehat{\mathbb{F}_{q^n}}$, which we denote by $f \circ \psi$. From the results of the previous subsection, we easily deduce that, for $\psi \in \widehat{\mathbb{F}_{q^n}}$, the set $\mathscr{I}_\psi \coloneqq \big\{h \in \mathbb{F}_q[x] \;\big|\; h \circ \psi = \psi_0\big\}$ is a nonzero ideal of $\mathbb{F}_q[x]$, hence it is generated by a unique monic polynomial in $\mathbb{F}_q[x]$. This polynomial is the $\mathbb{F}_q$-*order* of ψ and it is denoted by $\operatorname{Ord}(\psi)$.

It is clear that $\operatorname{Ord}(\psi)$ is a divisor of x^n-1. Conversely, for each monic divisor $f \in \mathbb{F}_q[x]$ of x^n-1, there exist $\Phi_q(f)$ additive characters of $\mathbb{F}_{q^n}$ with $\mathbb{F}_q$-order f.

Remark 12. It is clear that the trivial character is the only additive character of $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$-order 1.

We conclude this section with an important auxiliary result on additive character sums, see [11, Theorem 5.38].

Theorem 13. *Let $P \in \mathbb{F}_{q^n}[x]$ be a polynomial not of the form $r(x)^p - r(x) + \delta$ with $\delta \in \mathbb{F}_{q^n}$ and let ψ be a nontrivial additive character of $\mathbb{F}_{q^n}$. Then*

$$\left| \sum_{c \in \mathbb{F}_{q^n}} \psi\big(P(c)\big) \right| \leq \big(\deg(P) - 1\big) q^{n/2}.$$

The above implies that polynomials of the form $r(x)^p - r(x) + \delta$, with $\delta \in \mathbb{F}_{q^n}$, are special, so the following definition is essential.

Definition 14. *Let $P \in \mathbb{F}_{q^n}[x]$. If there exists some $r \in \mathbb{F}_{q^n}[x]$ and $\delta \in \mathbb{F}_{q^n}$, such that $P(x) = r(x)^p - r(x) + \delta$, then P is called* singular. *Otherwise, it is called* nonsingular.

3. Introducing (f, g)-freeness

In this section we introduce the (f, g)-free elements. We stress that these elements are in fact the additive analogues to (r, n)-free elements, as they were introduced in [5]. First, we recall the (additive) concept of freeness. For a positive integer n and a divisor $g \in \mathbb{F}_q[x]$ of x^n-1, an element $\alpha \in \mathbb{F}_{q^n}$ is g-*free* if the equality $\alpha = h \circ \beta$ with h a monic divisor of g and $\beta \in \mathbb{F}_{q^n}$ implies $h(x) = 1$ and $\alpha = \beta$.

Definition 15. *Let n be a positive integer and let $f, g \in \mathbb{F}_q[x]$ be such that $g(x)$ divides x^n-1 and $f(x)$ divides $\frac{x^n-1}{g(x)}$. An element $\alpha \in \mathbb{F}_{q^n}$ is* (f, g)-free *if the following hold:*

(i) $\operatorname{Ord}(\alpha)$ *divides* $\frac{x^n-1}{g(x)}$, *i.e.,* $\frac{x^n-1}{g(x)} \circ \alpha = 0$;

(ii) *α is f-free over the set of roots of the equation $\frac{x^n-1}{g(x)} \circ y = 0$, i.e., if $\alpha = f_0 \circ \beta$ with $f_0 \in \mathbb{F}_q[x]$ a monic divisor of f and $\frac{x^n-1}{g(x)} \circ \beta = 0$, then $f_0(x) = 1$ and $\alpha = \beta$.*

The following is straightforward.

Remark 16. Let n be a positive integer and let $f \in \mathbb{F}_q[x]$ be a divisor of $x^n - 1$:

(i) as $(x^n - 1) \circ \alpha = 0$ for every $\alpha \in \mathbb{F}_{q^n}$, the $(f, 1)$-free elements of $\mathbb{F}_{q^n}$ are just the usual f-free elements;

(ii) for $f \mid x^n - 1$, the $\left(\frac{x^n-1}{f}, f\right)$-free elements of $\mathbb{F}_{q^n}$ are exactly the elements α with $\mathrm{Ord}(\alpha) = \frac{x^n-1}{f(x)}$. In particular, an element $\alpha \in \mathbb{F}_{q^n}$ is normal over $\mathbb{F}_q$ if and only if it is $(x^n - 1, 1)$-free.

The following lemma characterizes the (f, g)-free elements based on their $\mathbb{F}_q$-orders.

Lemma 17. *Let $g \mid x^n - 1$ and $f \mid \frac{x^n-1}{g}$. Then some $\alpha \in \mathbb{F}_{q^n}$ is (f, g)-free if and only if $\alpha = g \circ \beta$ for some $\beta \in \mathbb{F}_{q^n}$ but α is not of the form $(gp) \circ \gamma$ with $\gamma \in \mathbb{F}_{q^n}$, for every irreducible factor $p \in \mathbb{F}_q[x]$ of f. In particular, $\alpha \in \mathbb{F}_{q^n}$ is (f, g)-free if and only if* $\gcd\left(fg, \frac{x^n-1}{\mathrm{Ord}(\alpha)}\right) = g$.

Proof. Clearly, the set $\{g \circ \beta \mid \beta \in \mathbb{F}_{q^n}\}$ describes the elements of $\mathbb{F}_{q^n}$ whose $\mathbb{F}_q$-order divides $\frac{x^n-1}{g}$, thus, the first statement follows directly by the definition of (f, g)-free elements.

For the second statement, from Lemma 8, $\alpha = h' \circ \delta'$, for some normal $\delta' \in \mathbb{F}_{q^n}$ and some $h' \in \mathbb{F}_q[x]$ of degree $\leq n-1$. Also, if we set $h = \gcd(h', x^n - 1)$, Lemma 9 entails that $\mathrm{Ord}(\alpha) = \frac{x^n-1}{h}$. Now, from the first part of the proof and the definition of (f, g)-freeness, it follows that α is (f, g)-free if and only if $\frac{x^n-1}{h}$ divides $\frac{x^n-1}{g}$ but does not divide $\frac{x^n-1}{gp}$ for any irreducible factor $p \in \mathbb{F}_q[x]$ of f. In other words, α is (f, g)-free if and only if $h = gs$ where $\gcd(s, f) = 1$. Since $\mathrm{Ord}(\alpha) = \frac{x^n-1}{h}$, we have that

$$\gcd\left(fg, \frac{x^n - 1}{\mathrm{Ord}(\alpha)}\right) = g \cdot \gcd(f, s),$$

from where the result follows. □

Remark 18. Observe that (f, g)-freeness is equivalent to (f', g)-freeness, where f' can be any polynomial in $\mathbb{F}_q[x]$ dividing $\frac{x^n-1}{g}$ that has exactly the same monic irreducible factors with f. In particular, we can replace f by its squarefree part. This will be done without further mention.

In the proceeding sections, we will need a convenient expression, using character sums, of the characteristic function of (f, g)-free elements of $\mathbb{F}_{q^n}$, i.e., of the function

$$\mathbb{I}_{f,g}(\alpha) := \begin{cases} 1, & \text{if } \alpha \text{ is } (f, g)\text{-free,} \\ 0, & \text{otherwise,} \end{cases}$$

where $\alpha \in \mathbb{F}_{q^n}$. Towards this end, we prove the following, which is the additive analogue to [5, Proposition 3.6] and, in fact, the arguments we use are merely an adaption of the ones found in the proof of [5, Proposition 3.6], adjusted accordingly to the present context.

Proposition 19. *Let $f, g \in \mathbb{F}_q[x]$ be such that $g \mid x^n - 1$ and $f \mid \frac{x^n-1}{g(x)}$. Then, for every $\alpha \in \mathbb{F}_{q^n}$, we have that*

$$\mathbb{I}_{f,g}(\alpha) = \frac{\Phi_q(f)}{|fg|} \sum_{t \mid fg} \frac{\mu_q(t_{(g)})}{\Phi_q(t_{(g)})} \sum_{\mathrm{Ord}(\psi) = t} \psi(\alpha),$$

where in the outer sum, the polynomial t is monic and polynomial division is over $\mathbb{F}_q$.

Proof. Take some $\alpha \in \mathbb{F}_{q^n}$. Let $p_1, \ldots, p_n$ be the distinct monic irreducible factors of f over $\mathbb{F}_q$. Lemma 17 implies that α is (f, g)-free if and only if α is of the form $g \circ \beta$ for some $\beta \in \mathbb{F}_{q^n}$, but not of the form $(gp_i) \circ \beta$ for any $1 \leq i \leq n$ and $\beta \in \mathbb{F}_{q^n}$. It follows that if I_h is the characteristic function for elements of the form $h \circ \beta$, where $h \in \mathbb{F}_q[x]$, such that $h \mid x^n - 1$, and $\beta \in \mathbb{F}_{q^n}$, then

$$\mathbb{I}_{f,g}(\alpha) = I_g(\alpha) \prod_{i=1}^{n} \left(1 - I_{gp_i}(\alpha)\right). \tag{1}$$

Clearly $I_g(\alpha)I_{gp_i}(\alpha) = I_{gp_i}(\alpha)$, for every $\alpha \in \mathbb{F}_{q^n}$ and $i = 1, \dots, n$, hence, eq. (1) yields

$$\mathbb{I}_{f,g}(\alpha) = \sum_{d \mid f} \mu_q(d) I_{gd}(\alpha), \tag{2}$$

where the sum is over the monic divisors of f, defined over $\mathbb{F}_q$. Regarding I_h, the orthogonality relations imply that, for every $h \in \mathbb{F}_q[x]$, such that $h \mid x^n - 1$,

$$I_h(\alpha) = \frac{1}{|h|} \sum_{\mathrm{Ord}(\psi) \mid h} \psi(\alpha) = \frac{1}{|h|} \sum_{d \mid h} \sum_{\mathrm{Ord}(\psi) = d} \psi(\alpha),$$

for every $\alpha \in \mathbb{F}_{q^n}$. Now, eq. (2) becomes

$$\begin{aligned}
\mathbb{I}_{f,g}(\alpha) &= \frac{1}{|g|} \sum_{d \mid f} \sum_{e \mid gd} \frac{\mu_q(d)}{|d|} \sum_{\mathrm{Ord}(\psi) = e} \psi(\alpha) \\
&= \frac{1}{|g|} \sum_{d \mid f} \sum_{e \mid gd} A(d) B_\alpha(e) \\
&= \frac{1}{|g|} \sum_{e \mid fg} \sum_{d \mid \frac{f}{e_{(g)}}} A(e_{(g)} d) B_\alpha(e) \\
&= \frac{1}{|g|} \sum_{e \mid fg} B_\alpha(e) \sum_{d \mid \frac{f}{e_{(g)}}} A(e_{(g)} d),
\end{aligned} \tag{3}$$

where, for each $h \in \mathbb{F}_q[X]$, we have that $A(h) \coloneqq \mu_q(h)/|h|$ and $B_\alpha(h) \coloneqq \sum_{\mathrm{Ord}(\psi) = h} \psi(\alpha)$. Regarding the inner sum in the last expression, we have that

$$\begin{aligned}
\sum_{d \mid \frac{f}{e_{(g)}}} A(e_{(g)} d) &= \sum_{d \mid \frac{f}{e_{(g)}}} \frac{\mu_q(e_{(g)} d)}{|e_{(g)} d|} \\
&= \frac{\mu_q(e_{(g)})}{|e_{(g)}|} \sum_{\substack{d \mid f \\ \gcd(d, e_{(g)}) = 1}} \frac{\mu_q(d)}{|d|} \\
&= \frac{\mu_q(e_{(g)})}{|e_{(g)}|} \cdot \frac{\Phi_q(f_{e,g})}{|f_{e,g}|} \\
&= \frac{\mu_q(e_{(g)})}{\Phi_q(e_{(g)})} \cdot \frac{\Phi_q(e_{(g)} f_{e,g})}{|e_{(g)} f_{e,g}|} \\
&= \frac{\mu_q(e_{(g)})}{\Phi_q(e_{(g)})} \cdot \frac{\Phi_q(f)}{|f|},
\end{aligned} \tag{4}$$

where $f_{e,g}$ is the highest-degree factor of f that is relatively prime to $e_{(g)}$. We plug the latter into eq. (3) and obtain

$$\mathbb{I}_{f,g}(\alpha) = \frac{\Phi_q(f)}{|fg|} \sum_{e \mid fg} \frac{\mu_q(e_{(g)})}{\Phi_q(e_{(g)})} B_\alpha(e).$$

The result follows upon replacing $B_\alpha(e)$ by $\sum_{\mathrm{Ord}(\psi) = e} \psi(\alpha)$. □

4. On (f, g)-freeness through polynomial values

For polynomials $h, H \in \mathbb{F}_{q^n}[x]$, we intend to study the number of pairs $\big(h(y), H(y)\big)$ with $y \in \mathbb{F}_{q^n}$ such that $h(y)$ is (f, g)-free and $H(y)$ is (F, G)-free. We aim to employ Theorem 13 but in order to effectively use this result, we must restrict ourselves to those pairs (h, H), such that for every $a, b \in \mathbb{F}_{q^n}$ with $(a, b) \neq (0, 0)$, the polynomial $ah(x) + bH(x)$ is nonsingular. For convenience, we

will call such pairs (h,H) *nonsingular*, while if there exist some $a,b\in\mathbb{F}_{q^n}$, with $(a,b)\neq(0,0)$, such that $ah(x)+bH(x)$ is singular, we will call the pair (h,H) *singular*.

We give a simple example, illustrating that the above can be necessary in order to have at least one pair $\big(h(y),H(y)\big)$ of polynomial values with prescribed freeness, thus it is natural to restrain ourselves to nonsingular pairs.

Example 20. Write $q=p^k$ and suppose that $H(x)=h(x)^q$. In particular, $H(x)-h(x)=h(x)^q-h(x)=r(x)^p-r(x)$ with $r(x)=\sum_{i=0}^{k-1}h(x)^{p^i}$, thus (h,H) is singular. For any $y\in\mathbb{F}_{q^n}$, we have that $H(y)=x\circ h(y)$. By Lemma 9, the $\mathbb{F}_q$-orders of $h(y)$, $H(y)$ coincide. From Remark 16, we can produce many examples in which no pair $\big(h(y),H(y)\big)$ with $y\in\mathbb{F}_{q^n}$ satisfies that $h(y)$ is (f,g)-free and $H(y)$ is (F,G)-free.

The next example provides a large family of nonsingular pairs.

Example 21. Observe that if $h,H\in\mathbb{F}_q[x]$ are nonzero polynomials of degree not divisible by p, then $ah(x)+bH(x)$ is nonsingular for $(a,b)\neq(0,0)$ unless $\deg(h)=\deg(H)=1$. In particular, if $\gcd\big(\deg(h)\cdot\deg(H),p\big)=1$ and $\deg(h)\cdot\deg(H)>1$, the pair (h,H) is nonsingular.

Regarding singularity, in the proceeding section, see Proposition 29, we highlight another case where singular pairs require special treatment. However, for now, we confine ourselves to nonsingular pairs and we obtain the following result.

Theorem 22. *Fix q a prime power and $n\geq 1$ a positive integer. Let $f,F\in\mathbb{F}_q[x]$ be divisors of x^n-1 and let $g,G\in\mathbb{F}_q[x]$ be such that g divides $\frac{x^n-1}{f(x)}$ and G divides $\frac{x^n-1}{F(x)}$. Let $h,H\in\mathbb{F}_{q^n}[x]$ be such that (h,H) is nonsingular. Set $D_1:=\deg(fFgG)$ and let D_2+1 be the maximum degree of the polynomials $ah(x)+bH(x)$ as a, b run over the elements of $\mathbb{F}_{q^n}$ with $(a,b)\neq(0,0)$. Then the number $N_{h,H}=N_{h,H}(f,g,F,G)$ of elements $y\in\mathbb{F}_{q^n}$ such that $h(y)$ is (f,g)-free and $H(y)$ is (F,G)-free satisfies*

$$\frac{N_{h,H}\cdot q^{D_1}}{\Phi_q(f)\Phi_q(F)}=q^n+\ell,$$

where $|\ell|\leq D_2W(f)W(F)q^{\deg(gG)+n/2}$.

Proof. It follows by the definition that

$$N_{h,H}=\sum_{w\in\mathbb{F}_{q^n}}\mathbb{I}_{f,g}\big(h(w)\big)\cdot\mathbb{I}_{F,G}\big(H(w)\big).$$

From Proposition 19, for $\delta=\frac{\Phi_q(f)\Phi_q(F)}{q^{D_1}}$, we have that

$$\frac{N_{h,H}}{\delta}=\sum_{t\,|\,fg,\ T\,|\,FG}\frac{\mu_q(t_{(g)})\cdot\mu_q(T_{(G)})}{\Phi_q(t_{(g)})\cdot\Phi_q(T_{(G)})}\sum_{\substack{\mathrm{Ord}(\psi)=t\\ \mathrm{Ord}(\psi')=T}}G_{h,H}(\psi,\psi'),$$

where $G_{h,H}(\psi,\psi')=\sum_{w\in\mathbb{F}_{q^n}}\psi\big(h(w)\big)\psi'\big(H(w)\big)$. Fix $t\,|\,fg$ and $T\,|\,FG$ and let ψ,ψ' be additive characters of $\mathbb{F}_{q^n}$ with $\mathbb{F}_q$-orders t and T, respectively. If $(t,T)\neq(1,1)$, we have that $(\psi,\psi')=(\psi_a,\psi_b)$ for some $a,b\in\mathbb{F}_{q^n}$ with $(a,b)\neq(0,0)$. In this case, $\psi\big(h(x)\big)\cdot\psi'\big(H(x)\big)=\psi_1\big(ah(x)+bH(x)\big)$ and $(a,b)\neq(0,0)$, where ψ_1 is the canonical additive character (hence nontrivial). Since (h,H) is nonsingular, $ah(x)+bH(x)$ is nonsingular and so Theorem 13 yields $\big|G_{h,H}(\psi,\psi')\big|\leq D_2q^{n/2}$. For $(t,T)=(1,1)$, $\psi=\psi'=\psi_0$ is the trivial additive character of $\mathbb{F}_{q^n}$ and so $\big|G_{h,H}(\psi_0,\psi_0)\big|=q^n$. Applying the above estimates we obtain

$$\left|\frac{N_{h,H}}{\delta}-q^n\right|\leq D_2q^{n/2}\cdot M,$$

where

$$M = \sum_{\substack{t \mid fg,\ T \mid FG \\ (t,T)\neq(1,1)}} \frac{\left|\mu_q(t_{(g)})\cdot\mu_q(T_{(G)})\right|}{\Phi_q(t_{(g)})\cdot\Phi_q(T_{(G)})} \sum_{\substack{\mathrm{Ord}(\psi)=t \\ \mathrm{Ord}(\psi')=T}} 1 = T(fg,g)\cdot T(FG,G) - 1,$$

and $T(f,g)$ is as in Lemma 5. Note that in the last equality we used the fact that for each monic divisor $R \in \mathbb{F}_q[x]$ of x^n-1 there exist $\Phi_q(R)$ characters of $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$-order R. Further, Lemma 5 implies $T(fg,g) = q^{\deg(g)}\cdot W(f)$ and $T(FG,G) = q^{\deg(G)}W(F)$, so

$$\begin{aligned}\left|\frac{N_{f,F}}{\delta} - q^n\right| &\le D_2 q^{n/2}\big(W(f)W(F)q^{\deg(gG)} - 1\big)\\ &\le D_2 W(f)W(F)q^{\deg(gG)+n/2}.\end{aligned}$$

□

The corollary below is an immediate consequence of Theorem 22 and it provides us with practical sufficient condition for the existence of elements $y \in \mathbb{F}_{q^n}$, such that $h(y)$ is (f,g)-free and $H(y)$ is (F,G)-free.

Corollary 23. *Assume the notation and the hypotheses of Theorem 22. We have that $N_{h,H} > 0$ if*

$$q^{n/2-\deg(gG)} > D_2 W(f)W(F).$$

Here, we point out that one of the main benefits of the introduction of (r,n)-freeness in [5] was its natural and seamless compatibility with the Cohen–Huczynska prime sieve [4]. As we will see in the following result, this benefit is carried over to the additive analogue that we study here and it enables us to further weaken the condition of Corollary 23. Also, since the two proofs are very similar, we leave the proof as an exercise to the interested reader and refer them to [5, Proposition 19 and Theorem 20] for the multiplicative analogue.

Theorem 24. *Fix q a prime power and $n \ge 1$ a positive integer. Let $f, F \in \mathbb{F}_q[x]$ be squarefree divisors of x^n-1 and let $g, G \in \mathbb{F}_q[x]$ be such that g divides $\frac{x^n-1}{f(x)}$ and G divides $\frac{x^n-1}{F(x)}$. Let $h, H \in \mathbb{F}_{q^n}[x]$ be such that (h,H) is nonsingular. Additionally, write $f = kp_1\cdots p_u$ and $F = KP_1\cdots P_v$, where $p_1,\dots,p_u,P_1,\dots,P_v$ are irreducible polynomials, such that*

$$\delta := 1 - \sum_{i=1}^{u} 1/|p_i| - \sum_{j=1}^{v} 1/|P_j| > 0.$$

Finally, set $D_1 := \deg(kKgG)$ and let D_2 be the maximum degree of the polynomials $ah(x)+bH(x)$ as a, b run over the elements of $\mathbb{F}_{q^n}$ with $(a,b)\neq(0,0)$. Then the number $N_{h,H} = N_{h,H}(f,g,F,G)$ of elements $y \in \mathbb{F}_{q^n}$ such that $h(y)$ is (f,g)-free and $H(y)$ is (F,G)-free satisfies

$$\frac{N_{h,H}\cdot q^{D_1}}{\delta\cdot\Phi_q(k)\Phi_q(K)} = q^n + \ell,$$

where $|\ell| \le D_2 W(k)W(K)\big(\frac{u+v}{\delta}+2\big)q^{\deg(gG)+n/2}$.

The following corollary translates the above theorem into a practical sufficient condition for the existence of elements with the desired properties, in a similar fashion as Corollary 23 did for Theorem 22.

Corollary 25. *Assume the notation and the assumptions of Theorem 24. Then $N_{h,H} > 0$, given that*

$$q^{n/2-\deg(gG)} > D_2 W(k)W(K)\left(\frac{u+v}{\delta}+2\right).$$

5. Normal points on Artin–Schreier curves

Throughout this section, we consider $\mathbb{F}_p$ as the base field, i.e., we write $q = p^n$ and so $\mathbb{F}_q = \mathbb{F}_{p^n}$ is viewed as the n-degree extension of $\mathbb{F}_p$. In particular, we adopt the concepts and results from Sections 2, 3 and 4 with $q = p$.

Recall that in [5], the authors explored the existence of points $(x_0, y_0) \in \mathbb{F}_q \times \mathbb{F}_q$ on curves $y^n = f(x)$ such that x_0 and y_0 are primitive elements of $\mathbb{F}_q$. As earlier mentioned this was done through a generalized concept of freeness over the cyclic group $\mathbb{F}_q^*$, which is just the multiplicative analogue of what we developed in Sections 2 and 3. Here we explore the natural additive counterpart of this problem. Namely, we study the existence of $\mathbb{F}_q$-affine points on Artin–Schreier curves whose coordinates are normal over $\mathbb{F}_p$. Recall that an *Artin–Schreier curve* is a plane curve defined over $\overline{\mathbb{F}}_q$ by an affine equation $y^p - y = f(x)$, where p is the characteristic of $\mathbb{F}_q$ and $f \in \mathbb{F}_q[x]$ is a polynomial not of the form $r(x)^p - r(x)$ for some $r \in \overline{\mathbb{F}}_q[x]$, or, equivalently, f is nonsingular over every extension of $\mathbb{F}_q$. In fact, the definition includes rational functions $f \in \mathbb{F}_q(x)$ but we are going to consider only polynomials. We introduce the following definition.

Definition 26. *Given an Artin–Schreier curve $\mathfrak{A}_f : y^p - y = f(x)$, an $\mathbb{F}_q$-rational point $(x_0, y_0) \in \mathbb{F}_q \times \mathbb{F}_q$ is an* $\mathbb{F}_q$-normal point *of $\mathfrak{A}_f$ if both x_0 and y_0 are normal over the prime field $\mathbb{F}_p$.*

The following lemma relates the existence of normal points on Artin–Schreier curves to the existence of special pairs of elements in $\mathbb{F}_q$ with prescribed freeness.

Lemma 27. *An Artin–Schreier curve $\mathfrak{A}_f : y^p - y = f(x)$ admits an $\mathbb{F}_q$-normal point if and only if there exists an element $z \in \mathbb{F}_q$ that is normal over $\mathbb{F}_p$ such that $f(z)$ has $\mathbb{F}_p$-order $\frac{x^n-1}{x-1}$. The latter is equivalent to the existence of an element $z \in \mathbb{F}_q$ such that z is $(x^n - 1, 1)$-free and $f(z)$ is $\left(\frac{x^n-1}{x-1}, x-1\right)$-free.*

Proof. The second statement follows directly by Remark 16. For the first statement, assume that $\mathfrak{A}_f$ admits an $\mathbb{F}_q$-normal point (x_0, y_0). Hence $z = x_0$ is normal over $\mathbb{F}_p$ and $f(z) = f(x_0) = y_0^p - y_0$. Since y_0 is also normal over $\mathbb{F}_p$, Corollary 11 implies that $f(z) = (x-1) \circ y_0$ has $\mathbb{F}_p$-order $\frac{x^n-1}{x-1}$. Conversely, suppose that there exists an element $z \in \mathbb{F}_q$ that is normal over $\mathbb{F}_p$ such that $f(z)$ has $\mathbb{F}_p$-order $\frac{x^n-1}{x-1}$. From Corollary 11, we have that $f(z) = (x-1) \circ ay_1$, where $a \in \mathbb{F}_p^*$ and y_1 is normal over $\mathbb{F}_p$. It is clear that ay_1 is also normal over $\mathbb{F}_p$. In particular, the point $(x_0, y_0) = (z, ay_1)$ has normal coordinates and belongs to the curve $\mathfrak{A}_f$, i.e., the curve $\mathfrak{A}_f$ admits an $\mathbb{F}_q$-normal point. □

We obtain the following result.

Corollary 28. *Assume the notation of Theorem 22. An Artin–Schreier curve $\mathfrak{A}_f : y^p - y = f(x)$ admits an $\mathbb{F}_q$-normal point whenever*

$$N_{x,f}\left(x^n - 1, 1, \frac{x^n-1}{x-1}, x-1\right) > 0.$$

In particular, the latter holds if the pair $\big(x, f(x)\big)$ is nonsingular and

$$p^{\frac{n}{2}-1} \geq (\deg f - 1)W(x^n - 1)W\left(\frac{x^n-1}{x-1}\right),$$

where for $g \in \mathbb{F}_p[x]$, $W(g)$ denotes the number of distinct monic squarefree divisors of g, defined over $\mathbb{F}_p$.

Proof. The first statement follows directly by Lemma 27. For the second statement, observe that our assumption on the pair $\big(x, f(x)\big)$ allows us to employ Theorem 22 and then the result follows from Corollary 23. □

In Example 21 we comment that, if $f(x)$ is linear, then the pair $\big(x, f(x)\big)$ is singular. In fact, for $f(x) = cx + d$ with $c \in \mathbb{F}_q^*$, we have that $ax + bf(x) = r(x)^p - r(x) - d$ for $(a,b) = (c,-1) \neq (0,0)$ and $r(x) = 0$. Motivated by Corollary 28, in the following proposition we show that we can actually obtain some existence results when $f(x)$ has degree one, without going through the character sum method.

Proposition 29. *Let $f(x) = ax + b \in \mathbb{F}_p[x]$, where $a \neq 0$ and $q = p^n$. If $b = 0$ or $n \equiv 0 \pmod p$, then the Artin–Schreier curve $\mathfrak{A}_f : y^p - y = f(x)$ does not admit an $\mathbb{F}_q$-normal point. On the other hand, if $n \not\equiv 0 \pmod p$, for every element $\alpha \in \mathbb{F}_q$ that is normal over $\mathbb{F}_p$, there exists a linear polynomial $F(x) = x + b \in \mathbb{F}_p[x]$ with $b \neq 0$ such that its associated Artin–Schreier curve $\mathfrak{A}_F : y^p - y = F(x)$ contains an $\mathbb{F}_q$-normal point of the form (α, y_0).*

Proof. Suppose by contradiction that there exists an $\mathbb{F}_q$-normal point (α, β) of $\mathfrak{A}_f$. In particular, for the trace polynomial $T_n(x) \coloneqq \sum_{i=0}^{n-1} x^{p^{i-1}}$, we have that

$$0 = \beta^q - \beta = T_n(\beta^p - \beta) = T_n\big(f(\alpha)\big) = T_n(a\alpha + b) = aT_n(\alpha) + nb = aT_n(\alpha),$$

where in the last equality we used the fact that $b = 0$ or $n \equiv 0 \pmod p$. Since $a \neq 0$, we obtain that $T_n(\alpha) = 0$. We observe that $T_n(\alpha) = \frac{x^n-1}{x-1} \circ \alpha$ and this is a contradiction with the assumption that α is normal over $\mathbb{F}_p$.

Now let $\alpha \in \mathbb{F}_q$ be normal over $\mathbb{F}_p$. In particular, $\delta \coloneqq T_n(\alpha) = \frac{x^n-1}{x-1} \circ \alpha \neq 0$. Since $n \not\equiv 0 \pmod p$, there exists $\Delta \in \mathbb{F}_p^*$ such that $n\Delta = 1 \in \mathbb{F}_p$. In this case, for $F(x) = x - \delta \cdot \Delta$, we have that

$$T_n\big(F(\alpha)\big) = T_n(\alpha - \delta \cdot \Delta) = T_n(\alpha) - \delta \cdot \Delta \cdot n = \delta - \delta = 0.$$

From [11, Theorem 3.78 and Corollary 3.79], there exists $\beta \in \mathbb{F}_q$ such that $F(\alpha) = \beta^p - \beta$. In particular, $(\alpha, \beta + t)$ is an $\mathbb{F}_q$-rational point of $\mathfrak{A}_F$ for arbitrary $t \in \mathbb{F}_p$. It remains to prove that there exists some $t_0 \in \mathbb{F}_p$ such that $\beta + t_0$ is normal over $\mathbb{F}_p$, hence producing the $\mathbb{F}_p$-normal point $(\alpha, \beta + t_0)$.

We first prove that $\operatorname{Ord}\big(F(\alpha)\big) = \frac{x^n-1}{x-1}$. As $\frac{x^n-1}{x-1} \circ \alpha = T_n\big(F(\alpha)\big) = 0$, it follows that $\operatorname{Ord}\big(F(\alpha)\big)$ divides $\frac{x^n-1}{x-1}$. On the other hand, since $\operatorname{Ord}\big(F(\alpha)\big) \circ F(\alpha) = 0$, we have that

$$\begin{aligned} 0 &= \big((x-1) \cdot \operatorname{Ord}\big(F(\alpha)\big)\big) \circ F(\alpha) \\ &= \operatorname{Ord}\big(F(\alpha)\big) \circ \big(F(\alpha)^p - F(\alpha)\big) \\ &= \operatorname{Ord}\big(F(\alpha)\big) \circ (\alpha^p - \alpha) \\ &= \big((x-1) \cdot \operatorname{Ord}\big(F(\alpha)\big)\big) \circ \alpha. \end{aligned}$$

Hence $\operatorname{Ord}(\alpha) = x^n - 1$ divides $(x-1)\operatorname{Ord}\big(F(\alpha)\big)$. Therefore, $\operatorname{Ord}\big(F(\alpha)\big)$ is divisible by $\frac{x^n-1}{x-1}$ and so $\operatorname{Ord}\big(F(\alpha)\big) = \frac{x^n-1}{x-1}$. Now, since $F(\alpha) = (x-1) \circ (\beta + t)$ for every $t \in \mathbb{F}_p$, it follows by Lemma 9 that $\operatorname{Ord}(\beta + t) = x^n - 1$ or $\frac{x^n-1}{x-1}$. In particular, $\operatorname{Ord}(\beta + t) = x^n - 1$ if and only if $T_n(\beta + t) = \frac{x^n-1}{x-1} \circ (\beta + t) \neq 0$. Since $n\Delta = 1 \in \mathbb{F}_p$, it follows that $T_n(\beta + t_0) = T_n(\beta) + nt_0 \neq 0$ for every $t_0 \in \mathbb{F}_p$ with $t_0 \neq -\Delta \cdot T_n(\beta)$. In particular, for any such t_0, we have $\operatorname{Ord}(\beta + t_0) = x^n - 1$ and so $\beta + t_0$ is normal over $\mathbb{F}_p$. □

5.1. *Proof of Theorem 1*

We observe that if $1 < \deg(f) \leq p + 1$, then the pair $\big(x, f(x)\big)$ is nonsingular whenever $f(x)$ is not of the form $ax^p + bx + c$ with $a, b, c \in \mathbb{F}_q$. Moreover, assuming the latter, from our previous discussion we conclude that the polynomial $y^p - y - f(x)$ gives rise to an Artin–Schreier curve. From Corollary 28 and the inequality $\deg(f) - 1 \leq p$, it suffices to verify the following inequality

$$p^{\frac{n}{2}-2} \geq W(x^n - 1)W\left(\frac{x^n - 1}{x - 1}\right). \tag{5}$$

We start with the following technical lemma: for its proof, see [1, Lemma 3.7].

Lemma 30. *Let p be a prime and let $n \geq 2$ be a positive integer. Then $W(x^n-1) \leq 2^{\frac{n+a}{b}}$, where $(a,b) = (14,5)$, $(20,4)$ and $(18,3)$ for $p = 2$, 3 and $p = 5$, respectively. Moreover, for $7 \leq p \leq 23$ and $p \geq 29$ we can take $(a,b) = (p-1,2)$ and $(a,b) = (0,1)$, respectively.*

Upon combining the previous lemma with the trivial bound

$$W\left(\frac{x^n-1}{x-1}\right) \leq \min\{W(x^n-1), 2^{n-1}\},$$

we obtain that ineq. (5) holds whether $n > 4$ and $p > 290000$, while for smaller values of p we also restrict, in Table 1, the possible pairs (n,p) where ineq. (5) might not hold.

Table 1. Pairs (n,p) that may not satisfy ineq. (5).

p	n
2	≤ 75
3	≤ 45
5	≤ 33
7	≤ 28
11, 13, 17, 19, 23	≤ 24
≤ 29	≤ 20
≤ 100	≤ 9
≤ 200	≤ 7
≤ 500	≤ 6
≤ 2100	≤ 5

Then, we consider the (finite) set of pairs (n,p) included in Table 1 and directly verify ineq. (5). In other words, we explicitly compute the value of $W(x^n-1)$ and $W\left(\frac{x^n-1}{x-1}\right)$. For $n = 5$, there are 5779 primes that fail to satisfy ineq. (5), while the explicit list of exceptional pairs (n,p), with $n \geq 6$, is presented in Table 2.

Finally, we turn our attention to the potential of ruling out most of the exceptional pairs using the sieve, as described in Theorem 24 and Corollary 25. More precisely, the aforementioned results imply that the condition of Corollary 28 may be improved as

$$p^{\frac{n}{2}-1} \geq (\deg f - 1) W(k_1) W(k_2) \left(\frac{2u}{\delta} + 2\right), \tag{6}$$

where (the squarefree part) of $(x^n-1)/(x-1)$ is $k_1 p_1 \cdots p_u$ and the (squarefree part) of x^n-1 is $k_2 r_1 \cdots r_v$ for some irreducible polynomials $p_1, \ldots, p_u, r_1, \ldots, r_v$, such that

$$\delta := 1 - \sum_{i=1}^{u} 1/|p_i| - \sum_{j=1}^{v} 1/|r_j|$$

is positive. In particular, in our test, for each pair (n,p), we choose the polynomials $p_1, \ldots, p_u, r_1, \ldots, r_v$ in such a way that u and v are maximum and δ remains positive and check whether ineq. (6) holds. A quick computer test reveals that among the aforementioned 6009 pairs (n,p) that did not satisfy ineq. (5), just 5 prove to be persistent enough to fail this test as well. These pairs (n,p) are $(5,2)$, $(5,5)$, $(6,2)$, $(6,3)$ and $(6,7)$. This concludes the proof of Theorem 1.

Acknowledgments

We are grateful to the anonymous reviewer for their efforts in reviewing our manuscript and their suggestions and improvements.

Table 2. Pairs (n, p) that do not satisfy ineq. (5), where $n \geq 6$.

n	p	#
6	2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 139, 151, 157, 163, 181, 193, 199, 211, 223, 229, 241, 271, 277, 283, 307, 313, 331, 337, 349, 367, 373, 379, 397, 409, 421, 433, 439, 457, 463, 487, 499, 523, 541, 547, 571, 577, 601, 607, 613, 619, 631, 643, 661, 673, 691, 709, 727, 733, 739, 751, 757, 769, 787, 811, 823, 829, 853, 859, 877, 883, 907, 919, 937, 967, 991, 997, 1009, 1021, 1033, 1039, 1051, 1063, 1069, 1087, 1093, 1117, 1123, 1129, 1153, 1171, 1201, 1213, 1231, 1237, 1249, 1279, 1291, 1297, 1303, 1321, 1327, 1381, 1399, 1423, 1429, 1447, 1453, 1459, 1471, 1483, 1489, 1531, 1543, 1549, 1567, 1579, 1597, 1609, 1621, 1627, 1657, 1663, 1669, 1693, 1699, 1723, 1741, 1747, 1753, 1759, 1777, 1783, 1789, 1801, 1831, 1861, 1867, 1873, 1879, 1933, 1951, 1987, 1993, 1999, 2011, 2017, 2029	168
7	2, 3, 13, 29, 43, 71, 113, 127, 197, 211, 239, 281, 337, 379	14
8	3, 5, 7, 11, 13, 17, 19, 29, 37, 41, 73, 89, 97, 113, 137	15
9	2, 7, 19, 37, 73	5
10	2, 3, 11, 31, 41, 61, 71	7
11	23	1
12	5, 7, 13, 19	4
13	3	1
14	2, 29	2
15	2	1
16	3, 5, 7, 17	4
18	19	1
20	3, 11	2
21	2	1
22	23	1
24	5, 7	2
26	3	1
	Total:	230

Declaration of interests

The authors do not work for, advise, own shares in, or receive funds from any organization that could benefit from this article, and have declared no affiliations other than their research organizations.

References

[1] J. J. R. Aguirre and V. G. Neumann, "Existence of primitive 2-normal elements in finite fields", *Finite Fields Appl.* **73** (2021), article no. 101864 (26 pages).

[2] G. Bailey, S. D. Cohen, N. Sutherland and T. Trudgian, "Existence results for primitive elements in cubic and quartic extensions of a finite field", *Math. Comput.* **88** (2019), no. 316, pp. 931–947.

[3] A. R. Booker, S. D. Cohen, N. Leong and T. Trudgian, "Primitive element pairs with a prescribed trace in the cubic extension of a finite field", *Bull. Aust. Math. Soc.* **106** (2022), no. 3, pp. 458–462.

[4] S. D. Cohen and S. Huczynska, "The primitive normal basis theorem—without a computer", *J. Lond. Math. Soc. (2)* **67** (2003), no. 1, pp. 41–56.

[5] S. D. Cohen, G. Kapetanakis and L. Reis, "The existence of $\mathbb{F}_q$-primitive points on curves using freeness", *C. R. Math.* **360** (2022), pp. 641–652.

[6] W. Diffie and M. E. Hellman, "New directions in cryptography", *IEEE Trans. Inf. Theory* **22** (1976), no. 6, pp. 644–654.
[7] S. Gao, *Normal basis over finite fields*, PhD thesis, University of Waterloo (Canada), 1993.
[8] S. Huczynska, G. L. Mullen, D. Panario and D. Thomson, "Existence and properties of k-normal elements over finite fields", *Finite Fields Appl.* **24** (2013), pp. 170–183.
[9] G. Kapetanakis and L. Reis, "Variations of the primitive normal basis theorem", *Des. Codes Cryptography* **87** (2019), no. 7, pp. 1459–1480.
[10] H. W. Lenstra Jr. and R. J. Schoof, "Primitive normal bases for finite fields", *Math. Comput.* **48** (1987), no. 177, pp. 217–231.
[11] R. Lidl and H. Niederreiter, *Finite fields*, Second edition, Encyclopedia of Mathematics and Its Applications, vol. 20, Cambridge University Press, 1997, pp. xiv+755.
[12] L. Reis, "Counting solutions of special linear equations over finite fields", *Finite Fields Appl.* **68** (2020), article no. 101759 (9 pages).