EQUIDISTRIBUTION OF POLYNOMIAL SEQUENCES IN FUNCTION FIELDS, WITH APPLICATIONS

THÁI HOÀNG LÊ, YU-RU LIU, AND TREVOR D. WOOLEY

Abstract. We prove a function field analog of Weyl's classical theorem on equidistribution of polynomial sequences. Our result covers the case in which the degree of the polynomial is greater than or equal to the characteristic of the field, which is a natural barrier when applying the Weyl differencing process to function fields. We also discuss applications to van der Corput, intersective and Glasner sets in function fields.

1. Introduction

Equidistribution theory started with Weyl's seminal paper [35]. We recall that a sequence $(a_n)_{n=1}^{\infty}$ of real numbers is said to be *equidistributed* (mod 1) if for any interval $[\alpha, \beta] \subset [0, 1)$, we have

$$\lim_{N\to\infty} N^{-1}\mathrm{card}\big\{n \in [1, N] \cap \mathbb{Z}^+ \colon \{a_n\} \in [\alpha, \beta]\big\} = \beta - \alpha.$$

Here, we write $\mathbb{Z}^+$ for the set of positive integers and $\{a\}$ for the fractional part of a real number a, which is to say $a - \lfloor a \rfloor$, where $\lfloor a \rfloor$ denotes the largest integer not exceeding a. Write $e(x) = e^{2\pi ix}$. Then *Weyl's criterion* asserts that the sequence $(a_n)_{n=1}^{\infty}$ is equidistributed (mod 1) if and only if for any integer $m \neq 0$, we have

$$\lim_{N\to\infty} \frac{1}{N}\Big|\sum_{n=1}^{N} e(ma_n)\Big| = 0.$$

Let $f(u) = \sum_{r=0}^{k} \alpha_r u^r$ be a polynomial with real coefficients having degree k. Weyl made the important observation that by squaring the sum $\big|\sum_{n=1}^{N} e(f(n))\big|$, one can estimate it in terms of other exponential sums involving the shift $f(u + h) - f(u)$, which is, for each $h \in \mathbb{Z}^+$, a polynomial of degree $k - 1$. This process is called *Weyl differencing*. If one continues the differencing process, then the polynomial in question becomes linear after $k - 1$ steps. Using this observation, Weyl [35] proved that the sequence $(f(n))_{n=1}^{\infty}$ is equidistributed (mod 1) if and only if at least one of the coefficients $\alpha_1, \dots, \alpha_k$ of f is irrational. The proof of this result was later simplified with the help of *van der Corput's difference theorem* [33], which shows that, if for any $h \in \mathbb{Z}^+$ the sequence $(a_{n+h} - a_n)_{n=1}^{\infty}$

2010 *Mathematics Subject Classification.* 11J71, 11T55.

Key words and phrases. Equidistribution, function fields, intersective sets, van der Corput sets, Glasner sets.

The first author is supported by NSF grant DMS-2246921 and a travel award from the Simons Foundation. The second author is supported by an NSERC discovery grant. The third author is supported by NSF grants DMS-1854398 and DMS-2001549.

is equidistributed (mod 1), then the sequence $(a_n)_{n=1}^{\infty}$ is also equidistributed (mod 1). Using van der Corput's difference theorem, Weyl's equidistribution theorem for polynomials follows easily by induction on the degree of the polynomial. This remains to date the standard proof of Weyl's result.

Denote by $\mathbb{F}_q$ the finite field of q elements whose characteristic is p and let $\mathbb{F}_q[t]$ be the polynomial ring over $\mathbb{F}_q$. Since $\mathbb{Z}$ and $\mathbb{F}_q[t]$ share many similarities from analytic and number-theoretic points of view, it is natural to study equidistribution in the latter setting. Let $\mathbb{K} = \mathbb{F}_q(t)$ be the field of fractions of $\mathbb{F}_q[t]$. When $f/g \in \mathbb{K}$, with $f, g \in \mathbb{F}_q[t]$ and $g \neq 0$, we define a norm $|f/g| = q^{\deg f - \deg g}$ (with the convention that $\deg 0 = -\infty$). The completion of $\mathbb{K}$ with respect to this norm is $\mathbb{K}_\infty = \mathbb{F}_q((1/t))$, the field of formal Laurent series in $1/t$. In other words, every element $\alpha \in \mathbb{K}_\infty$ can be written in the form $\alpha = \sum_{i=-\infty}^{n} a_i t^i$ for some $n \in \mathbb{Z}$ and $a_i \in \mathbb{F}_q$ $(i \leq n)$. Therefore, one sees that $\mathbb{F}_q[t]$, $\mathbb{K}$, $\mathbb{K}_\infty$ play the roles of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, respectively. Let

$$\mathbb{T} = \left\{ \sum_{i \leq -1} a_i t^i \colon a_i \in \mathbb{F}_q \ (i \leq -1) \right\}.$$

This compact group is the analog of $\mathbb{R}/\mathbb{Z}$, namely the unit interval $[0, 1)$ with addition modulo 1. Let λ be a normalized Haar measure on $\mathbb{T}$ such that $\lambda(\mathbb{T}) = 1$. For $M \in \mathbb{Z}^+$, let $I = (c_1, \dots, c_M)$ be a finite sequence of elements of $\mathbb{F}_q$. A set of the form

$$\mathcal{C}_I = \left\{ \sum_{i \leq -1} a_i t^i \in \mathbb{T} \colon a_i = c_{-i} \ (-M \leq i \leq -1) \right\}$$

satisfies $\lambda(\mathcal{C}_I) = q^{-M}$. Thus, we refer to the set $\mathcal{C}_I$ as a *cylinder set of radius* q^{-M}. The topology on $\mathbb{T}$ induced by the norm $|\cdot|$ is generated by cylinder sets. Therefore, cylinder sets play the role of intervals.

For $\alpha = \sum_{i=-\infty}^{n} a_i t^i \in \mathbb{K}_\infty$ with $a_n \neq 0$, we define $\operatorname{ord} \alpha = n$. Therefore, one has $|\alpha| = q^{\operatorname{ord} \alpha}$. We say α is *rational* if $\alpha \in \mathbb{K}$ and *irrational* if $\alpha \notin \mathbb{K}$. We define $\{\alpha\} = \sum_{i \leq -1} a_i t^i \in \mathbb{T}$ to be the *fractional part* of α, and we refer to a_{-1} as the *residue* of α, denoted by $\operatorname{res} \alpha$. Next we define the exponential function on $\mathbb{K}_\infty$. Let $\operatorname{tr} \colon \mathbb{F}_q \to \mathbb{F}_p$ denote the familiar trace map given by

$$\operatorname{tr}(a) = a + a^p + a^{p^2} + \ldots + a^{p^{m-1}},$$

in which we suppose that $q = p^m$. There is a non-trivial additive character $e_q \colon \mathbb{F}_q \to \mathbb{C}^\times$ defined for each $a \in \mathbb{F}_q$ by taking $e_q(a) = e(\operatorname{tr}(a)/p)$. This character induces a map, which we also denote by $e(\cdot)$, from $\mathbb{K}_\infty$ to $\mathbb{C}^\times$ by defining, for each element $\alpha \in \mathbb{K}_\infty$, the value of $e(\alpha)$ to be $e_q(\operatorname{res} \alpha)$. For $N \in \mathbb{Z}^+$, we write $\mathbb{G}_N$ for the set of all polynomials in $\mathbb{F}_q[t]$ having degree smaller than N. The following notion of equidistribution was first introduced by Carlitz in [8] (see also [19, Chapter 5, Section 3]).

Definition 1.1. Let $(a_x)_{x \in \mathbb{F}_q[t]}$ be a sequence indexed by $\mathbb{F}_q[t]$ and taking values in $\mathbb{K}_\infty$. We say that $(a_x)_{x \in \mathbb{F}_q[t]}$ is *equidistributed* in $\mathbb{T}$ if for any cylinder set $\mathcal{C} \subset \mathbb{T}$, we have

$$\lim_{N \to \infty} q^{-N} \operatorname{card} \{x \in \mathbb{G}_N \colon \{a_x\} \in \mathcal{C}\} = \lambda(\mathcal{C}).$$

Since one can prove analogs of Weyl's criterion and van der Corput's difference theorem in function fields, one expects to establish an $\mathbb{F}_q[t]$-analog of Weyl's equidistribution theorem for polynomial sequences. Let $f(u) = \sum_{r=0}^{k} \alpha_r u^r$ be a polynomial with coefficients in $\mathbb{K}_\infty$ having degree k. All earlier works on equidistribution in $\mathbb{T}$ have been restricted to the case in which $k < p$. Under this condition, Carlitz [8] proved an analog of Weyl's equidistribution theorem for the sequence $(f(x))_{x\in\mathbb{F}_q[t]}$. Dijksma [10] also established the same result for another stronger notion of equidistribution, subject to the same constraint $k < p$. In the work of both Carlitz and Dijksma, the use of Weyl differencing produces a factor of $k!$. When $k \geq p$, the latter factor is 0, and hence this differencing method becomes ineffective in producing the desired equidistribution result. Actually, the following example, already known to Carlitz [8, equation (6.8)], shows that a direct $\mathbb{F}_q[t]$-analog of Weyl's equidistribution theorem is not always true when $k \geq p$.

Example 1.2. For $\alpha = \sum_{i=-\infty}^{n} a_i t^i \in \mathbb{K}_\infty$, define

$$T(\alpha) = a_{-1}t^{-1} + a_{-p-1}t^{-2} + a_{-2p-1}t^{-3} + \cdots . \tag{1.1}$$

Then T is a linear map from $\mathbb{K}_\infty$ to $\mathbb{T}$ (this map will also be used in Section 5). By setting $a_{-1} = a_{-p-1} = \ldots = 0$, a countability argument shows that we can find an irrational element $\alpha \in \mathbb{K}_\infty$ with $T(\alpha) = 0$. Given such an irrational element α, it follows that for any element $x = \sum_{i=0}^{m} x_i t^i$ of $\mathbb{F}_q[t]$, the coefficient of t^{-1} in αx^p is equal to

$$a_{-1}x_0^p + a_{-p-1}x_1^p + a_{-2p-1}x_2^p + \cdots = 0,$$

and thus the sequence $(\alpha x^p)_{x\in\mathbb{F}_q[t]}$ is not equidistributed in $\mathbb{T}$.

It is desirable to give a complete description of all polynomials $f(u) \in \mathbb{K}_\infty[u]$ for which the sequence $(f(x))_{x\in\mathbb{F}_q[t]}$ is equidistributed in $\mathbb{T}$. However, in view of Example 1.2, such a description may be complicated and not easy to state in such arithmetic terms as irrationality. In particular, equidistribution could fail if the degree of $f(u)$ is divisible by p. Furthermore, for a polynomial such as $\alpha x^p + \beta x$, it is not possible to determine whether or not one has equidistribution if one is equipped with information concerning α or β alone, since the terms x^p and x "interfere" with one another, as the map $x \mapsto x^p$ is linear (see also [8, equation (6.9)]). However, one may suspect that the only pathologies that prevent equidistribution are the ones described above (namely, exponents divisible by p and interfering exponents). Thus one can make the following conjecture, which is the best possible insofar as irrationality hypotheses are imposed on a single coefficient.

Conjecture 1.3. *Let $\mathcal{K}$ be a finite set of positive integers, suppose that $\alpha_r \in \mathbb{K}_\infty$ for $r \in \mathcal{K} \cup \{0\}$, and define*

$$f(u) = \sum_{r\in\mathcal{K}\cup\{0\}} \alpha_r u^r.$$

Suppose that α_k is irrational for some $k \in \mathcal{K}$ satisfying $p \nmid k$ and furthermore $p^v k \notin \mathcal{K}$ for any $v \in \mathbb{Z}^+$. Then the sequence $(f(x))_{x\in\mathbb{F}_q[t]}$ is equidistributed in $\mathbb{T}$.

In this paper, we make some progress towards this conjecture. Given a set of positive integers $\mathcal{K}$, we define the *shadow* of $\mathcal{K}$ to be the set

$$\mathcal{S}(\mathcal{K}) = \left\{ j \in \mathbb{Z}^+ : p \nmid \binom{r}{j} \text{ for some } r \in \mathcal{K} \right\}.$$

Here, as usual, we adopt the convention that $\binom{r}{j} = 0$ when $j > r$. Note in particular that whenever $\mathcal{K}$ is a set of positive integers, then $\mathcal{K} \subseteq \mathcal{S}(\mathcal{K})$. We provide a convenient interpretation of the shadow of $\mathcal{K}$ in the preamble to Lemma 2.1 that makes for easy computation in terms of the base p digital expansions of the elements of $\mathcal{K}$. We may now announce our main equidistribution result, which has no restriction on the degree of the polynomial $f(u)$ in question.

Theorem 1.4. *Let $\mathcal{K}$ be a finite set of positive integers, suppose that $\alpha_r \in \mathbb{K}_\infty$ for $r \in \mathcal{K} \cup \{0\}$, and define*

$$f(u) = \sum_{r \in \mathcal{K} \cup \{0\}} \alpha_r u^r.$$

Suppose that α_k is irrational for some $k \in \mathcal{K}$ satisfying $p \nmid k$ and furthermore $p^v k \notin \mathcal{S}(\mathcal{K})$ for any $v \in \mathbb{Z}^+$. Then the sequence $(f(x))_{x \in \mathbb{F}_q[t]}$ is equidistributed in $\mathbb{T}$.

Example 1.5. If k is the largest element of a finite set of positive integers $\mathcal{K}$, and furthermore $p \nmid k$ and α_k is irrational, then Theorem 1.4 shows that the sequence $(f(x))_{x \in \mathbb{F}_q[t]}$ is equidistributed in $\mathbb{T}$. More generally, let $f(u) = \sum_{r=0}^{k} \alpha_r u^r \in \mathbb{K}_\infty[u]$, and suppose that α_r is irrational for some integer r with $k/p < r \le k$ and $p \nmid r$. Then, as a direct consequence of Theorem 1.4, the sequence $(f(x))_{x \in \mathbb{F}_q[t]}$ is equidistributed in $\mathbb{T}$.

Example 1.6. Consider the situation in which $q = 3$ and $\mathcal{K} = \{7, 11, 45\}$. A modest computation confirms that $\mathcal{S}(\mathcal{K}) = \{1, 2, 3, 4, 6, 7, 9, 10, 11, 18, 27, 36, 45\}$. By applying Theorem 1.4, we see that the sequence $(\alpha x^{45} + \beta x^{11} + \gamma x^7)_{x \in \mathbb{F}_q[t]}$ is equidistributed in $\mathbb{T}$ if either β or γ is irrational. This fact does not follow from Example 1.5 because $11 < 45/3$.

Example 1.7. Suppose that $p > 3$ and $\alpha, \beta, \gamma \in \mathbb{K}_\infty$ with β irrational. We consider the situation with $\mathcal{K} = \{1, 3, 3p + 1\}$. Since $3p \in \mathcal{S}(\mathcal{K})$, we find that Theorem 1.4 does not imply directly the equidistribution of the sequence $(\alpha x + \beta x^3 + \gamma x^{3p+1})_{x \in \mathbb{F}_q[t]}$. However, we will prove a more general form of Theorem 1.4 (see Proposition 5.2 below), and from this one can conclude that the above sequence is equidistributed in $\mathbb{T}$. In contrast, we are not able to confirm that the sequence $(\beta x^3 + \gamma x^{4p})_{x \in \mathbb{F}_q[t]}$ is equidistributed in $\mathbb{T}$, although Conjecture 1.3 suggests that such should be the case.

Remark 1.8. A result similar to that in Example 1.5 was proved independently by Bergelson and Leibman [3, Corollary 0.5] using a different method. See the discussion concluding this section for a comparison of the latter results with those contained in this paper.

As experts will anticipate, our proof of Theorem 1.4 is based on an estimate for the sum $|\sum_{x \in \mathbb{G}_N} e(f(x))|$ of minor arc type. By combining the large sieve inequality with a generalization of Vinogradov's mean value theorem to the setting of $\mathbb{F}_q[t]$, we obtain a Weyl-type estimate which avoids the problematic use of Weyl differencing. The reader will find a detailed explanation of this procedure in Section 3. This approach allows us to surmount the barriers that previously obstructed viable conclusions when the degree of $f(u)$ exceeds or is equal to p. The assumption $p^v k \notin \mathcal{S}(\mathcal{K})$ in Theorem 1.4 comes from the use of the Weyl shift in our minor arc estimate. The latter produces terms whose degrees may lie throughout the set $\mathcal{S}(\mathcal{K})$, instead of being restricted to the potentially smaller set $\mathcal{K}$ (see equation (3.1)). Therefore, we need to consider a mean value estimate whose associated indices are elements of $\mathcal{S}(\mathcal{K})$. Such an "extension of indices" is a common theme

in the study of Diophantine problems. It occurs, for example, in Vinogradov's approach to the asymptotic formula in Waring's problem, where one relates an equation involving k-th powers to Vinogradov's system of equations having degrees ranging from 1 to k (see [34, Section 5.3] for more details). In the situation of Theorem 1.4, it requires the stronger assumption $p^v k \notin \mathcal{S}(\mathcal{K})$, instead of $p^v k \notin \mathcal{K}$. Although, for this reason, we are unable to prove Conjecture 1.3 in general, we can confirm it in the special case when $q = p$ (see Corollary 5.4). This follows from a more general form of Theorem 1.4 which we present in Proposition 5.2 and Corollary 5.3.

Our equidistribution result is applicable in virtually any situation involving some notion of equidistribution for polynomials in $\mathbb{T}$. In particular, in Sections 6 and 7, we investigate some special sets in $\mathbb{F}_q[t]$ closely related to equidistribution and presently less well understood than their integer counterparts. These are van der Corput, intersective and Glasner sets. An accessible consequence of this work is the following result, which is a consequence of our Theorem 6.3, established in Section 6.

Theorem 1.9. *Let $\mathcal{K}$ be a finite set of positive integers, suppose that $a_r \in \mathbb{F}_q[t]$ for $r \in \mathcal{K} \cup \{0\}$, and define*

$$\Phi(u) = \sum_{r \in \mathcal{K} \cup \{0\}} a_r u^r.$$

Suppose that $\Phi(u)$ has a root modulo g for any $g \in \mathbb{F}_q[t] \setminus \{0\}$. Suppose further that $a_k \neq 0$ for some $k \in \mathcal{K}$ satisfying $p \nmid k$ and $p^v k \notin \mathcal{S}(\mathcal{K})$ for any $v \in \mathbb{Z}^+$. Then for any subset $\mathcal{A}$ of positive upper density in $\mathbb{F}_q[t]$, there exist distinct elements a and a' of $\mathcal{A}$, and some $x \in \mathbb{F}_q[t]$, for which $a - a' = \Phi(x)$.

As is well-known, the condition that $\Phi(u)$ have a root modulo g, for any $g \in \mathbb{F}_q[t] \setminus \{0\}$, is required in order to handle scenarios in which the elements of $\mathcal{A}$ all lie in a common congruence class modulo h, for some $h \in \mathbb{F}_q[t] \setminus \{0\}$. Polynomials Φ having a root modulo g for any $g \in \mathbb{F}_q[t] \setminus \{0\}$ are called *intersective*. The above theorem is an $\mathbb{F}_q[t]$-analog of a result of Sárközy [30]. Previously, such a result with no restriction on the degree of Φ was not available, except in cases where $\Phi(0) = 0$ [4] (see also [14]). We refer the reader to Section 6 for an introduction to intersective and van der Corput sets and for the statement of our results.

Remark 1.10. A result similar to Theorem 1.9 was proved independently by Bergelson and Leibman [3, Theorem 9.5] using different methods. Bergelson and Leibman also addressed a notion of intersective polynomials, although their notion differs from ours. It is a non-trivial problem to determine if these two notions are one and the same. We refer the reader to Question 1 in Section 6 and the associated discussion for an account of similarities and differences between our Theorem 1.9 and [3, Theorem 9.5].

Our next application concerns Glasner sets in $\mathbb{F}_q[t]$. Generalizing a result of Glasner, it was shown by Alon and Peres [2] that given a non-constant polynomial $\Phi(u) \in \mathbb{Z}[u]$, for any infinite subset Y of $\mathbb{R}/\mathbb{Z}$ and any $\epsilon > 0$, there exists $n \in \mathbb{Z}$ such that the set $\Phi(n)Y = \{\Phi(n)y \colon y \in Y\}$ intersects any interval of length ϵ in $\mathbb{R}/\mathbb{Z}$. In view of Example 1.2 and the discussion preceding Conjecture 1.3, it is not surprising that an exact analog of the result of Alon and Peres over $\mathbb{F}_q[t]$ is *not* true in general. We establish the following $\mathbb{F}_q[t]$-analog of the latter result.

Theorem 1.11. *Let $\mathcal{K}$ be a finite set of positive integers, suppose that $a_r \in \mathbb{F}_q[t]$ for $r \in \mathcal{K} \cup \{0\}$, and define*

$$\Phi(u) = \sum_{r \in \mathcal{K} \cup \{0\}} a_r u^r.$$

Suppose that $a_k \neq 0$ for some $k \in \mathcal{K}$ satisfying $k \geq 1$ with $p \nmid k$, and furthermore $p^v k \notin \mathcal{S}(\mathcal{K})$ for any $v \in \mathbb{Z}^+$. Then for any infinite subset $Y \subset \mathbb{T}$ and any $M \in \mathbb{Z}^+$, there exists $x \in \mathbb{F}_q[t]$ having the property that the set $\Phi(x)Y$ intersects any cylinder set of radius q^{-M} in $\mathbb{T}$.

This theorem is a restatement in different language of Theorem 7.3, which is itself an immediate consequence of Theorem 7.4. We refer the reader to Section 7 for an introduction to Glasner sets and for the statement and proof of our results.

We conclude this section with a brief comparison between the results of Bergelson and Leibman and the results of this paper. As mentioned earlier in Remarks 1.8 and 1.10, some results in this paper were obtained independently by Bergelson and Leibman [3], at about the same time as an earlier version of this memoir[1], using rather different methods. The approach of Bergelson and Leibman is qualitative and very general. Their main result, [3, Theorem 0.3], concerns multi-dimensional tori $\mathbb{T}^c$. It asserts that any (multi-variate) polynomial sequence in $\mathbb{T}^c$ is equidistributed in a finite union of cosets of a subgroup of $\mathbb{T}^c$. It also gives a condition for when a polynomial sequence is equidistributed in the full torus. However, this condition is not easy to check in practice for a given polynomial and we do not know if [3, Theorem 0.3] implies our Theorem 1.4. There are two important features of our own work. First, our method (which relies on the large sieve inequality and Vinogradov's Mean Value Theorem) offers scope for *quantitative* applications. For example, it was used by Yamagishi in work on Diophantine approximation [38] and Waring's problem over $\mathbb{F}_q[t]$ [37]. Second, the flexibility of our approach makes it applicable to variants of Weyl sums in which summands are restricted in various ways. Indeed, in recent work with Zhenchao Ge [12], the first and second authors extend the methods of the current paper to study Weyl sums over the set $\mathbb{I}_q$ of monic irreducible elements in $\mathbb{F}_q[t]$, thereby obtaining equidistribution results for the sequence $(f(x))_{x \in \mathbb{I}_q}$ with concomitant conclusions for allied Diophantine and combinatorial problems.

This paper is organized as follows. In Section 2 we introduce the preliminary infrastructure needed to prove our results. We prove an estimate of minor arc type in Section 3 and derive an extension of this conclusion suitable for our subsequent applications in Section 4. Then, in Section 5, we apply these estimates to prove Theorem 1.4. Finally, in Sections 6 and 7, we discuss applications of our equidistribution results to van der Corput, intersective and Glasner sets over $\mathbb{F}_q[t]$.

Acknowledgements: We are grateful to Vitaly Bergelson for explaining aspects of the paper [3], and to Bhawesh Mishra for interesting conversations related to the topic of our paper and directing us to [1]. We are also grateful to the referee for their useful comments.

[1]The first version of our paper was posted on arxiv (https://arxiv.org/abs/1311.0892) in November 2013.

2. Preliminaries

We begin this section by reviewing an orthogonality relation for the function $e(\cdot)$ defined in Section 1. As is explained in [18, Lemma 7], for example, when $\alpha \in \mathbb{K}_\infty$, we have

$$\sum_{x \in \mathbb{G}_N} e(x\alpha) = \begin{cases} q^N, & \text{when } \operatorname{ord}\{\alpha\} < -N, \\ 0, & \text{when } \operatorname{ord}\{\alpha\} \geq -N. \end{cases} \tag{2.1}$$

Therefore, for any polynomials $a, g \in \mathbb{F}_q[t]$ with $g \neq 0$, we have

$$\sum_{\operatorname{ord} x < \operatorname{ord} g} e\left(\frac{xa}{g}\right) = \begin{cases} |g|, & \text{when } a \equiv 0 \pmod{g}, \\ 0, & \text{otherwise.} \end{cases} \tag{2.2}$$

As promised in the preamble to the statement of Theorem 1.4, we now interpret the shadow $\mathcal{S}(\mathcal{K})$ of a set of indices $\mathcal{K}$ in a manner that eases explicit computations. First, given $j, r \in \mathbb{Z}^+$, we write $j \preceq_p r$ when $p \nmid \binom{r}{j}$. By Lucas' theorem, the latter holds precisely when all of the digits of j in base p are less than or equal to the corresponding digits of r. From this characterization, it is easy to see that the relation $\preceq_p$ defines a partial order on $\mathbb{Z}^+$. Note in particular that if $j \preceq_p r$, then we necessarily have $j \leq r$. Equipped with this notation, we see that

$$\mathcal{S}(\mathcal{K}) = \left\{ j \in \mathbb{Z}^+ \colon j \preceq_p r \text{ for some } r \in \mathcal{K} \right\}. \tag{2.3}$$

This interpretation makes clear the origin of the elements of $\mathcal{S}(\mathcal{K})$ occurring in Example 1.6. Thus, in transparent notation, the base 10 number 7 has base 3 expansion $(21)_3$, and thus $\mathcal{S}(\mathcal{K})$ must contain the numbers $7 = (21)_3$, $6 = (20)_3$, $4 = (11)_3$, $3 = (10)_3$ and $1 = (1)_3$. Likewise, the base 10 number 11 has base 3 expansion $(102)_3$, and hence $\mathcal{S}(\mathcal{K})$ must contain the numbers $11 = (102)_3$, $10 = (101)_3$, $9 = (100)_3$, $2 = (2)_3$ and $1 = (1)_3$. Finally, the base 10 number 45 has base 3 expansion $(1200)_3$, and hence $\mathcal{S}(\mathcal{K})$ contains the numbers $45 = (1200)_3$, $36 = (1100)_3$, $27 = (1000)_3$, $18 = (200)_3$ and $9 = (100)_3$.

Our conclusions concerning estimates of Weyl-type and associated equidistribution results extend beyond those announced in Theorem 1.4. For ease of reference, we take the opportunity here to collect together the definitions of certain subsets of the set of indices $\mathcal{K}$ making an appearance later in this paper. First, define

$$\mathcal{K}^* = \left\{ k \in \mathcal{K} \colon p \nmid k \text{ and } p^v k \notin \mathcal{S}(\mathcal{K}) \text{ for any } v \in \mathbb{Z}^+ \right\}. \tag{2.4}$$

The set $\mathcal{K}^*$ is therefore the subset of $\mathcal{K}$ that is compatible with an application of Theorem 1.4, namely the subset of $\mathcal{K}$ consisting of indices, no non-trivial p-power multiple of which lies in the shadow of $\mathcal{K}$. The set $\mathcal{K} \setminus \mathcal{K}^*$ consists of indices not immediately accessible to Theorem 1.4. However, if we throw out the accessible exponents $\mathcal{K}^*$ and treat the remaining set $\mathcal{K} \setminus \mathcal{K}^*$ in isolation, it may well be that a new set $(\mathcal{K} \setminus \mathcal{K}^*)^*$ can be identified itself accessible to Theorem 1.4, and this process can be iterated. We are therefore led to define the set $\widetilde{\mathcal{K}}$ as follows. We put $\mathcal{K}_0 = \mathcal{K}$, and inductively define for each $n \geq 1$ the set

$$\mathcal{K}_n = \mathcal{K}_{n-1} \setminus \mathcal{K}_{n-1}^*.$$

We then define the set of indices

$$\widetilde{\mathcal{K}} = \bigcup_{n=0}^{\infty} \mathcal{K}_n^*. \tag{2.5}$$

We show in Proposition 5.2 that the conclusion of Theorem 1.4 may be extended so that indices k remain accessible throughout the set $\widetilde{\mathcal{K}}$, instead of being constrained to lie in $\mathcal{K}^*$.

Next, consider a set $\mathcal{K} \subset \mathbb{Z}^+$. We say that an element $k \in \mathcal{K}$ is *maximal* if it is maximal with respect to the partial ordering $\preceq_p$. Thus, for any $r \in \mathcal{K}$, one has either $r \preceq_p k$ or else r and k are not comparable. We record for future reference the following observations concerning the partial ordering $\preceq_p$.

Lemma 2.1. *Suppose that $\mathcal{K} \subset \mathbb{Z}^+$. Then the following hold.*

(a) The index k is maximal in $\mathcal{S}(\mathcal{K})$ whenever k is maximal in $\mathcal{K}$;

(b) One has $\mathcal{K}^* \subset \mathcal{S}(\mathcal{K})^*$;

(c) If $k \in \mathcal{K}^*$, and $j \in \mathcal{K}$ satisfies $k \preceq_p j$, then $j \in \mathcal{K}^*$.

Proof. The maximality property (a) is immediate from the definition of $\mathcal{S}(\mathcal{K})$. Property (b), meanwhile, follows from the definition (2.4) of $\mathcal{K}^*$ on observing that $\mathcal{S}(\mathcal{S}(\mathcal{K})) = \mathcal{S}(\mathcal{K})$. Finally, under the hypotheses of part (c), we have $p \nmid k$ and $p \nmid \binom{j}{k}$. By Lucas' theorem, it follows that $p \nmid j$. A second application of Lucas' theorem reveals that for any $v \in \mathbb{Z}^+$, we have $p^v k \preceq_p p^v j$. If we were to have $p^v j \in \mathcal{S}(\mathcal{K})$ for some $v \in \mathbb{Z}^+$, then for some $r \in \mathcal{K}$ we would have $p^v k \preceq_p p^v j \preceq_p r$, whence $k \notin \mathcal{K}^*$, yielding a contradiction. So $p^v j \notin \mathcal{S}(\mathcal{K})$ for any $v \in \mathbb{Z}^+$, and we conclude that $j \in \mathcal{K}^*$. □

In order to state the version of the large sieve inequality that we employ to derive a minor arc estimate, we must introduce some notation. Suppose that $\Gamma \subset \mathbb{K}_\infty$. We say that the elements of Γ are *q^δ-spaced in* $\mathbb{T}$ if, for any distinct elements $\gamma_1, \gamma_2 \in \Gamma$, we have $\operatorname{ord}\{\gamma_1 - \gamma_2\} \geq \delta$.

Theorem 2.2. *Let K and N be positive integers. Suppose that $\Gamma \subset \mathbb{K}_\infty$ is a q^{-K}-spaced set in $\mathbb{T}$. Consider a sequence $(b_x)_{x \in \mathbb{F}_q[t]}$ of complex numbers, and when $\beta \in \mathbb{K}_\infty$ define*

$$\mathcal{S}(\beta) = \sum_{x \in \mathbb{G}_N} b_x\, e(x\beta).$$

Then

$$\sum_{\gamma \in \Gamma} |\mathcal{S}(\gamma)|^2 \leq \max\{q^N, q^{K-1}\} \sum_{x \in \mathbb{G}_N} |b_x|^2.$$

Proof. This is Hsu [15, Theorem 2.4]. □

In order to apply Theorem 2.2, we employ a construction from [28]. It is convenient in this setting to introduce some further notation.

Definition 2.3. Suppose that $k \in \mathbb{Z}^+$ and $g \in \mathbb{F}_q[t] \setminus \{0\}$. We say that a set of monic polynomials $\mathcal{L} \subset \mathbb{F}_q[t]$ is a *(k, g)-set* if, for any $\ell_1, \ell_2 \in \mathcal{L}$, one has $\ell_1^k \equiv \ell_2^k \pmod g$ if and only if $\ell_1 \equiv \ell_2 \pmod g$.

The next lemma allows us to partition a given finite subset of $\mathbb{F}_q[t]$ into a small number of (k,g)-sets.

Lemma 2.4. *Let k be a positive integer satisfying $p \nmid k$. Also, let $g \in \mathbb{F}_q[t]$, and suppose that A is a subset of $\mathbb{F}_q[t]$, all of whose elements are coprime to g. Then for each $\epsilon > 0$, the set A can be partitioned into $O_{k,q,\epsilon}(|g|^\epsilon)$ subsets, each of which is a (k,g)-set.*

Proof. This is essentially [28, equation (12.4)], though for completeness we include a proof. We begin with an estimate for the number of solutions of a certain polynomial congruence. Working under the hypotheses of the statement of the lemma, when $a \in \mathbb{F}_q[t]$, denote by $J(g,a)$ the number of solutions of the congruence $x^k \equiv a \pmod g$ with $\deg(x) < \deg(g)$ and $(x,g) = 1$. Thus, necessarily, one has $(a,g) = 1$. Then we claim that $J(g,a) \le k^{\omega(g)}$, where $\omega(g)$ denotes the number of distinct monic irreducible factors of g. For each $a \in \mathbb{F}_q[t]$, we write $\{x_1(a), \dots, x_J(a)\}$ for the set of solutions of the above congruence, where $J = J(g,a)$ and the elements $x_i(a)$ are distinct for $1 \le i \le J$. Then A can be partitioned into the sets

$$A_i = \{x \in A\colon \text{there exists } a \in \mathbb{F}_q[t] \text{ such that } J(g,a) \ge i \text{ and } x \equiv x_i(a) \pmod g\},$$

for $1 \le i \le k^{\omega(g)}$, each of which is a (k,g)-set. The conclusion of the lemma follows by means of the familiar estimate

$$\omega(g) \le \log_2 d(g) \ll_q \frac{\deg g}{\log \deg g},$$

where $d(g)$ denotes the number of divisors of g (see for example [23, Lemma 5]).

We now set about confirming the above claim. For each irreducible polynomial ℓ with $\ell \mid g$, the congruence $x^k \equiv a \pmod \ell$ has at most k solutions. Thus, since $p \nmid k$, it follows from Hensel's lemma that for any $r \ge 2$, each solution of $x^k \equiv a \pmod \ell$ lifts uniquely to a corresponding solution modulo ℓ^r. Factoring g as a product of powers of irreducible polynomials in the form $\prod \ell_j^{r_j}$, and counting solutions modulo $\ell_j^{r_j}$ for each j, we deduce via the Chinese Remainder Theorem that there are at most $k^{\omega(g)}$ solutions modulo g. This completes the proof of the lemma. □

We next state a mean value theorem for a system of equations having indices defined by the elements of the set $\mathcal{S}(\mathcal{K})$ defined in (2.3). For $N \in \mathbb{Z}^+$, denote by $J_s(\mathcal{S}(\mathcal{K}); N)$ the number of solutions of the system

$$u_1^j + \cdots + u_s^j = v_1^j + \cdots + v_s^j \quad (j \in \mathcal{S}(\mathcal{K})),$$

with $u_r, v_r \in \mathbb{G}_N$ $(1 \le r \le s)$. Since $(u_1 + \cdots + u_s)^p = u_1^p + \cdots + u_s^p$, these equations are not always independent. To obtain independence, we consider the set

$$\mathcal{S}(\mathcal{K})' = \left\{i \in \mathbb{Z}^+\colon p \nmid i \text{ and } p^v i \in \mathcal{S}(\mathcal{K}) \text{ for some } v \in \mathbb{Z}^+ \cup \{0\}\right\}. \tag{2.6}$$

We note that when $j = p^v i$ with $p \nmid i$, we have $u_1^j + \cdots + u_s^j = (u_1^i + \cdots + u_s^i)^{p^v}$. It therefore follows that $J_s(\mathcal{S}(\mathcal{K}); N)$ also counts the number of solutions of the system

$$u_1^i + \cdots + u_s^i = v_1^i + \cdots + v_s^i \quad (i \in \mathcal{S}(\mathcal{K})'),$$

with $u_r, v_r \in \mathbb{G}_N$ $(1 \le r \le s)$. We shall find it useful to define three quantities associated with this system of equations, namely

$$\psi(\mathcal{K}) = \operatorname{card} \mathcal{S}(\mathcal{K})', \quad \phi(\mathcal{K}) = \max_{i \in \mathcal{S}(\mathcal{K})'} i \quad \text{and} \quad \kappa(\mathcal{K}) = \sum_{i \in \mathcal{S}(\mathcal{K})'} i. \tag{2.7}$$

Where the intended meaning is unambiguous, we drop mention of $\mathcal{K}$ from this notation without comment. The following result gives an upper bound on $J_s(\mathcal{S}(\mathcal{K}); N)$.

Theorem 2.5. *Suppose that $s \ge \psi(\phi + 1)$. Then for any $\epsilon > 0$, there exists a constant $C_1 = C_1(s; \mathcal{K}; \epsilon; q) > 0$ such that*

$$J_s(\mathcal{S}(\mathcal{K}); N) \le C_1 (q^N)^{2s - \kappa + \epsilon}.$$

Proof. Observe that whenever $j \in \mathcal{S}(\mathcal{K})$, and $i \in \mathbb{Z}^+$ satisfies $i \preceq_p j$, one has $i \in \mathcal{S}(\mathcal{K})$. Therefore, the set $\mathcal{S}(\mathcal{K})$ satisfies the inclusion relation defined in Condition$\star$ of [20, Section 1]. The desired conclusion therefore follows as a special case of [20, Theorem 1.1]. □

We remark that a multidimensional generalization of Theorem 2.5 can be found in [20]. Meanwhile, the condition $s \ge \psi(\phi + 1)$ of this theorem can be refined, as is shown in [29].

We now recall some facts about continued fractions in $\mathbb{K}_\infty$ needed in our proof of Theorem 1.4. For any irrational element α lying in $\mathbb{K}_\infty$, we can write α as an infinite continued fraction in the form

$$\alpha = b_0 + \cfrac{1}{b_1 + \frac{1}{b_2 + \cdots}} = [b_0; b_1, b_2, \ldots],$$

with $b_i \in \mathbb{F}_q[t]$ and $\operatorname{ord} b_i > 0$ $(i \ge 1)$. When α is a rational element of $\mathbb{K}_\infty$, meanwhile, one may write α as a finite continued fraction of the form

$$\alpha = b_0 + \cfrac{1}{b_1 + \frac{1}{b_2 + \frac{1}{\cdots + \frac{1}{b_n}}}} = [b_0; b_1, b_2, \ldots, b_n],$$

with $b_i \in \mathbb{F}_q[t]$ and $\operatorname{ord} b_i > 0$ $(1 \le i \le n)$. We note that continued fraction expansions in $\mathbb{K}_\infty$ are uniquely defined. We define two sequences $(a_n)_{n \ge -2}$ and $(g_n)_{n \ge -2}$ in $\mathbb{F}_q[t]$ recursively by putting

$$a_{-2} = 0, \quad g_{-2} = 1, \quad a_{-1} = 1, \quad g_{-1} = 0,$$

and for all $n \ge 0$,

$$a_n = b_n a_{n-1} + a_{n-2} \quad \text{and} \quad g_n = b_n g_{n-1} + g_{n-2}.$$

Then for all $n \ge 0$, we have

$$g_n a_{n-1} - a_n g_{n-1} = (-1)^n \qquad \text{and} \qquad [b_0; b_1, \ldots, b_n] = a_n / g_n.$$

The fractions a_n/g_n $(n \ge 0)$ are called the *convergents* of α. An inductive argument shows that the sequence $(\operatorname{ord} g_n)_{n \ge 0}$ is strictly increasing.

Proposition 2.6. *Suppose that $\alpha \in \mathbb{K}_\infty$. Then the convergents a_n/g_n $(n \ge 0)$ of α satisfy the following properties.*

(a) One has $\operatorname{ord}(g_n \alpha - a_n) = -\operatorname{ord} g_{n+1}$ $(n \ge 0)$.

(b) If $a, g \in \mathbb{F}_q[t]$ satisfy $\operatorname{ord}(g\alpha - a) < -\operatorname{ord} g$, then a/g is a convergent of α.

Proof. See [32, Section 1]. □

The conclusion (b) of Proposition 2.6 is sometimes referred to as Legendre's theorem. The following lemma concerns elements of $\mathbb{K}_\infty$ well-approximated by rationals.

Lemma 2.7. *Let $\alpha \in \mathbb{K}_\infty$. Suppose that there exists a constant $\kappa > 1$ such that, for all sufficiently large N, there exist $a \in \mathbb{F}_q[t]$ and $g \in \mathbb{F}_q[t] \setminus \{0\}$ with $\operatorname{ord}(g\alpha - a) \le -\kappa N$ and $\operatorname{ord} g < N$. Then α is rational.*

Proof. Suppose that α is irrational and a_n/g_n $(n \ge 0)$ are the convergents of α. Since α is irrational, we have $\lim_{n\to\infty} \operatorname{ord} g_n = \infty$. We take n sufficiently large and put $N = \operatorname{ord} g_n$. By hypothesis, there exist $a \in \mathbb{F}_q[t]$ and $g \in \mathbb{F}_q[t] \setminus \{0\}$ such that $\operatorname{ord} g < N$ and

$$\operatorname{ord}(g\alpha - a) \le -\kappa N < -\operatorname{ord} g_n = -N < -\operatorname{ord} g. \tag{2.8}$$

It therefore follows from Proposition 2.6(b) that a/g is a convergent of α. But $\operatorname{ord} g < N = \operatorname{ord} g_n$ and the sequence $(\operatorname{ord} g_n)_{n\ge 0}$ is strictly increasing, so there exists $m \in \mathbb{Z}^+ \cup \{0\}$ with $m < n$ such that $a = a_m$ and $g = g_m$. However, we find from Proposition 2.6(a) that

$$\operatorname{ord}(g\alpha - a) = \operatorname{ord}(g_m\alpha - a_m) = -\operatorname{ord}(g_{m+1}) \ge -\operatorname{ord} g_n,$$

and this contradicts (2.8). We thus conclude that α is rational. □

We end this section by recalling Weyl's criterion for equidistribution in $\mathbb{F}_q[t]$.

Theorem 2.8. *The sequence $(a_x)_{x\in\mathbb{F}_q[t]} \subset \mathbb{K}_\infty$ is equidistributed in $\mathbb{T}$ if and only if for any $m \in \mathbb{F}_q[t] \setminus \{0\}$, we have*

$$\lim_{N\to\infty} \frac{1}{q^N} \left| \sum_{x\in\mathbb{G}_N} e(ma_x) \right| = 0.$$

Proof. This is Carlitz [8, Theorem 4]. □

3. A Weyl-type estimate

Our goal in this section is the proof of an estimate of minor arc type for a certain exponential sum. In advance of the statement of this estimate, we recall the definition (2.4) of the set $\mathcal{K}^*$.

Theorem 3.1. *Fix q and a finite set $\mathcal{K} \subset \mathbb{Z}^+$. There exist positive constants c and C, depending only on $\mathcal{K}$ and q, such that the following holds. Let $\epsilon > 0$ and let N be sufficiently large in terms of $\mathcal{K}$, ϵ and q. Suppose that $f(u) = \sum_{r\in\mathcal{K}\cup\{0\}} \alpha_r u^r$ is a polynomial with coefficients in $\mathbb{K}_\infty$ satisfying the bound*

$$\left| \sum_{x\in\mathbb{G}_N} e(f(x)) \right| \ge q^{N-\eta},$$

for some positive number η with $\eta \le cN$. Then, for each maximal $k \in \mathcal{K}^*$, there exist $a \in \mathbb{F}_q[t]$ and monic $g \in \mathbb{F}_q[t]$ having the property that

$$\operatorname{ord}(g\alpha_k - a) < -kN + \epsilon N + C\eta \quad \text{and} \quad \operatorname{ord} g \le \epsilon N + C\eta.$$

We remark that an ϵ-free version of this conclusion could be derived by making use of major arc approximations to the exponential sum under consideration. We direct the interested reader to [36, Lemma 2.1] for a model of the kind of argument that would be required to achieve such a conclusion. Observe also that in Theorem 3.1, the coefficient α_k plays the role of the leading coefficient of the polynomial, and might be regarded as the "true" $\mathbb{F}_q[t]$-analog of the leading coefficient. Furthermore, clearly, if k is the greatest element in $\mathcal{K}$, then k is maximal in $\mathcal{K}$. However, a set may have more than one maximal element. For example, if $p = 2$ and $\mathcal{K} = \{1, 3, 5, 9\}$ then 9, 5, and 3 are all maximal elements of $\mathcal{K}$ and they all satisfy the hypothesis of Theorem 3.1.

We require two auxiliary lemmas in our proof of Theorem 3.1. First, we recall a familiar lemma employing Weyl shifts of a form suitable for our subsequent deliberations.

Lemma 3.2. *Let $\mathcal{A}$ be a multiset of elements from $\mathbb{G}_N$, and write $|\mathcal{A}|$ for card$(\mathcal{A})$. Then we have*

$$\sum_{x\in\mathbb{G}_N} e(f(x)) = |\mathcal{A}|^{-1} \sum_{x\in\mathbb{G}_N} \sum_{y\in\mathcal{A}} e(f(y-x)).$$

Proof. For $y \in \mathbb{G}_N$, it follows via a change of variable that

$$\sum_{x\in\mathbb{G}_N} e(f(x)) = \sum_{x\in\mathbb{G}_N} e(f(y-x)).$$

Thus, it follows that

$$|\mathcal{A}| \sum_{x\in\mathbb{G}_N} e(f(x)) = \sum_{y\in\mathcal{A}} \sum_{x\in\mathbb{G}_N} e(f(y-x)) = \sum_{x\in\mathbb{G}_N} \sum_{y\in\mathcal{A}} e(f(y-x)),$$

and the desired conclusion is immediate. □

Consider a finite subset $\mathcal{K}$ of $\mathbb{Z}^+$ and its shadow $\mathcal{S}(\mathcal{K})$. Let $f(u) = \sum_{r\in\mathcal{K}\cup\{0\}} \alpha_r u^r$ be a polynomial with coefficients in $\mathbb{K}_\infty$, and write $\boldsymbol{\alpha}$ for $\{\alpha_r\}_{r\in\mathcal{K}}$. For any $r \in \mathcal{K}$, we have

$$(y-x)^r = \sum_{j\preceq_p r} \binom{r}{j} y^j (-x)^{r-j} + (-x)^r.$$

Therefore, if k is maximal in $\mathcal{K}$, then for a fixed $x \in \mathbb{G}_N$ there exist

$$\gamma_0 = \gamma_0(\alpha_0, \boldsymbol{\alpha}; x) \in \mathbb{K}_\infty \qquad \text{and} \qquad \gamma_j = \gamma_j(\boldsymbol{\alpha}; x) \in \mathbb{K}_\infty \quad (j \in \mathcal{S}(\mathcal{K}) \setminus \{k\})$$

such that

$$f(y-x) = \alpha_k(y-x)^k + \sum_{r\in\mathcal{K}\setminus\{k\}} \alpha_r(y-x)^r + \alpha_0 = \alpha_k y^k + \sum_{j\in\mathcal{S}(\mathcal{K})\setminus\{k\}} \gamma_j y^j + \gamma_0. \tag{3.1}$$

The next lemma provides a conclusion occurring within the argument of the proof of [28, Lemma 12.1].

Lemma 3.3. *Let $M \in \mathbb{Z}^+$ with $M \le N$, and let $k \in \mathbb{Z}^+$ with $p \nmid k$ and $\alpha_k \in \mathbb{K}_\infty$. Suppose that $a, g \in \mathbb{F}_q[t]$ with $(a, g) = 1$ and $\operatorname{ord}(g\alpha_k - a) < -kM$, and suppose further that either $\operatorname{ord}(g\alpha_k - a) \ge M - kN$ or $\operatorname{ord} g > M$. Finally, let $\mathcal{L}_0$ be a (k, g)-subset of monic polynomials of degree M. Then the points $\{\alpha_k l^k : l \in \mathcal{L}_0\}$ are spaced at least $\min\{|g|^{-1}, q^{k(M-N)}\}$ apart in $\mathbb{T}$.*

Proof. Suppose that $l_1, l_2 \in \mathcal{L}_0$ with $l_1 \not\equiv l_2 \pmod{g}$. Then, since $\mathcal{L}_0$ is a (k,g)-subset, we have $l_1^k \not\equiv l_2^k \pmod{g}$. Write $\alpha_k = a/g + \beta$. Then

$$\operatorname{ord}\{\alpha_k(l_1^k - l_2^k)\} = \operatorname{ord}\{a(l_1^k - l_2^k)/g + \beta(l_1^k - l_2^k)\}.$$

Since $\operatorname{ord}(g\beta) < -kM$ and $\operatorname{ord} l_1 = \operatorname{ord} l_2 = M$, we have

$$\operatorname{ord}\{\beta(l_1^k - l_2^k)\} < -kM - \operatorname{ord} g + kM = -\operatorname{ord} g.$$

Also, since $l_1^k \not\equiv l_2^k \pmod{g}$ and $(a,g) = 1$, we have

$$\operatorname{ord}\{a(l_1^k - l_2^k)/g\} \geq -\operatorname{ord} g.$$

We therefore deduce that

$$\operatorname{ord}\{\alpha_k(l_1^k - l_2^k)\} = \operatorname{ord}\{a(l_1^k - l_2^k)/g\} \geq -\operatorname{ord} g. \tag{3.2}$$

We now divide into cases, according to the size of $\operatorname{ord} g$.

Case 1. Suppose first that $\operatorname{ord} g > M$. In this case, the elements of $\mathcal{L}_0$ are distinct $\pmod{g}$. Consequently, by (3.2), the points $\alpha_k l^k$ are spaced at least $|g|^{-1}$ apart in $\mathbb{T}$.

Case 2. If instead $\operatorname{ord} g \leq M$, then the hypotheses of the lemma ensure that one has $\operatorname{ord}(g\alpha_k - a) \geq M - kN$. When $l_1, l_2 \in \mathcal{L}_0$ satisfy the condition $l_1 \not\equiv l_2 \pmod{g}$, then it follows from (3.2) that αl_1^k and αl_2^k are spaced at least $|g|^{-1}$ apart in $\mathbb{T}$. Otherwise, when $l_1 \equiv l_2 \pmod{g}$, the bounds $\operatorname{ord}(g\alpha_k - a) < -kM$ and $\operatorname{ord}(g\alpha_k - a) \geq M - kN$ lead to the relation

$$\begin{aligned}\operatorname{ord}\{\alpha_k(l_1^k - l_2^k)\} &= \operatorname{ord}\{(\alpha_k - a/g)(l_1^k - l_2^k)\} \\ &= \operatorname{ord}\big((\alpha_k - a/g)(l_1^k - l_2^k)\big) \\ &\geq M - kN - \operatorname{ord} g + \operatorname{ord}(l_1^k - l_2^k). \end{aligned} \tag{3.3}$$

We note that

$$\operatorname{ord}(l_1^k - l_2^k) = \operatorname{ord}(l_1 - l_2) + \operatorname{ord}(l_1^{k-1} + l_1^{k-2}l_2 + \cdots + l_2^{k-1}).$$

If $l_1 \neq l_2$ and $l_1 \equiv l_2 \pmod{g}$, we have $\operatorname{ord}(l_1 - l_2) \geq \operatorname{ord} g$. Furthermore, since the elements of $\mathcal{L}_0$ are monic and of degree M, the term $l_1^{k-1} + l_1^{k-2}l_2 + \cdots + l_2^{k-2}$ is of degree $(k-1)M$ with leading coefficient k. Since $p \nmid k$, we have

$$\operatorname{ord}(l_1^{k-1} + l_1^{k-2}l_2 + \cdots + l_2^{k-1}) = (k-1)M.$$

On combining the above two estimates, we obtain the lower bound

$$\operatorname{ord}(l_1^k - l_2^k) \geq \operatorname{ord} g + (k-1)M,$$

and hence we infer from (3.3) that

$$\operatorname{ord}\{\alpha_k(l_1^k - l_2^k)\} \geq k(M - N).$$

In this case, therefore, we find that αl_1^k and αl_2^k are spaced at least $q^{k(M-N)}$ apart in $\mathbb{T}$.

Combining the bounds obtained in the two respective cases, we conclude that for any distinct elements $l_1, l_2 \in \mathcal{L}_0$, the points $\alpha_k l_1^k$ and $\alpha_k l_2^k$ are spaced at least $\min\{|g|^{-1}, q^{k(M-N)}\}$ apart in $\mathbb{T}$. This completes the proof of the lemma. □

We are now ready to prove Theorem 3.1.

Proof of Theorem 3.1. We first note that should Theorem 3.1 hold for the polynomial $f(u) - \alpha_0 = \sum_{r\in\mathcal{K}} \alpha_r u^r$, then it holds also for $f(u)$. There is consequently no loss of generality in assuming that $\alpha_0 = 0$. Next, let k be a maximal element of $\mathcal{K}$ satisfying $p \nmid k$ and $p^v k \notin \mathcal{S}(\mathcal{K})$ for any $v \in \mathbb{Z}^+$. Let $\alpha_k \in \mathbb{K}_\infty$ and consider $M \in \mathbb{Z}^+$ with $2M \le N$. By Dirichlet's approximation theorem in $\mathbb{F}_q[t]$ (see [18, Lemma 3]), there exist $a \in \mathbb{F}_q[t]$ and monic $g \in \mathbb{F}_q[t]$ with

$$(a, g) = 1, \quad \operatorname{ord}(g\alpha_k - a) < -kM \quad \text{and} \quad \operatorname{ord} g \le kM.$$

Suppose that either

$$\operatorname{ord}(g\alpha_k - a) \ge M - kN \quad \text{or} \quad \operatorname{ord} g > M. \tag{3.4}$$

We will show that, for M suitably chosen, such an assumption leads to an upper bound for $\big|\sum_{x\in\mathbb{G}_N} e(f(x))\big|$, which contradicts the lower bound asserted in the statement of the theorem.

Let $\mathcal{L}$ be the set of monic irreducible polynomials l satisfying $\operatorname{ord} l = M$ and $(l, g) = 1$. Since $\operatorname{ord} g \le kM$, the polynomial g has at most k irreducible factors of degree M. It therefore follows from the prime number theorem in $\mathbb{F}_q[t]$ that when M is sufficiently large in terms of k (and thus also $\mathcal{K}$) and q, we have

$$q^M/(2M) \le \operatorname{card}(\mathcal{L}) \le q^M/M.$$

Let $\mathcal{A}$ be the multiset

$$\mathcal{A} = \big\{y \in \mathbb{G}_N : y = lw \text{ with } l \in \mathcal{L} \text{ and } w \in \mathbb{G}_{N-M}\big\}, \tag{3.5}$$

where the multiplicity of each element y of $\mathcal{A}$ is equal to the number of its representations $y = lw$. Then

$$|\mathcal{A}| = \operatorname{card}(\mathcal{A}) \ge q^{N-M} \cdot q^M/(2M) = q^N/(2M).$$

By Lemma 3.2 and (3.1), we therefore find that

$$\begin{aligned}\Big|\sum_{x\in\mathbb{G}_N} e(f(x))\Big| &\le 2Mq^{-N}\Big|\sum_{x\in\mathbb{G}_N}\sum_{y\in\mathcal{A}} e\Big(\alpha_k y^k + \sum_{j\in\mathcal{S}(\mathcal{K})\setminus\{k\}} \gamma_j(\boldsymbol{\alpha}; x)y^j\Big)\Big| \\ &\le 2M \max_{x\in\mathbb{G}_N}\Big|\sum_{y\in\mathcal{A}} e\Big(\alpha_k y^k + \sum_{j\in\mathcal{S}(\mathcal{K})\setminus\{k\}} \gamma_j(\boldsymbol{\alpha}; x)y^j\Big)\Big|.\end{aligned}$$

For $j \in \mathcal{S}(\mathcal{K}) \setminus \{k\}$, fix $\gamma_j = \gamma_j(\boldsymbol{\alpha}; x)$ to be the element of $\mathbb{K}_\infty$ corresponding to the choice of x which maximizes the expression on the right hand side here.

Recall the definitions (2.7) of ψ and ϕ, and let s be a positive integer with $s \ge \psi\phi + \psi$. Then in view of (3.5), an application of Hölder's inequality delivers the bound

$$\Big|\sum_{x\in\mathbb{G}_N} e(f(x))\Big|^{2s} \le (2M)^{2s}(q^M/M)^{2s-1}\sum_{l\in\mathcal{L}}\Big|\sum_{w\in\mathbb{G}_{N-M}} e\Big(\alpha_k(lw)^k + \sum_{j\in\mathcal{S}(\mathcal{K})\setminus\{k\}} \gamma_j(lw)^j\Big)\Big|^{2s}.$$

Let $\epsilon > 0$ be arbitrary. By Lemma 2.4, there exists a constant $C_1 = C_1(k, q, \epsilon) > 0$ such that the set $\mathcal{L}$ can be divided into $L \le C_1|g|^\epsilon$ subsets $\mathcal{L}_1, \dots, \mathcal{L}_L$, having the property that

$\mathcal{L}_i$ is a (k,g)-set for $1 \le i \le L$. Then there exists $r \in \mathbb{Z}^+$ with $r \le L$ for which

$$\Big|\sum_{x\in\mathbb{G}_N} e(f(x))\Big|^{2s} \le 2^{2s}M(q^M)^{2s-1}C_1|g|^{\epsilon}\Psi, \tag{3.6}$$

where

$$\Psi = \sum_{l\in\mathcal{L}_r}\Big|\sum_{w\in\mathbb{G}_{N-M}} e\Big(\alpha_k(lw)^k + \sum_{j\in\mathcal{S}(\mathcal{K})\setminus\{k\}}\gamma_j(lw)^j\Big)\Big|^{2s}. \tag{3.7}$$

Let $\mathcal{S}(\mathcal{K})'$ be the relation of the shadow set defined in (2.6). For $\mathbf{h} = (h_i)_{i\in\mathcal{S}(\mathcal{K})'}$ with $h_i \in \mathbb{F}_q[t]$, let $b(\mathbf{h})$ denote the number of solutions of the system

$$w_1^i + \cdots + w_s^i = h_i \quad (i \in \mathcal{S}(\mathcal{K})'),$$

with $w_r \in \mathbb{G}_{N-M}$ $(1 \le r \le s)$. For $i \in \mathcal{S}(\mathcal{K})'$, we have $h_i \in \mathbb{G}_{i(N-M)}$. Furthermore, for $j = p^v i \in \mathcal{S}(\mathcal{K})$, with $i \in \mathcal{S}(\mathcal{K})'$ and $v \in \mathbb{Z}^+$, we have $w_1^j + \cdots + w_s^j = h_i^{p^v}$. Therefore, by defining $h_j = h_i^{p^v}$, we see that $b(\mathbf{h})$ also counts the number of solutions of the system

$$w_1^j + \cdots + w_s^j = h_j \quad (j \in \mathcal{S}(\mathcal{K})), \tag{3.8}$$

with $w_r \in \mathbb{G}_{N-M}$ $(1 \le r \le s)$. We remark here that since $p \nmid k$, we have $k \in \mathcal{S}(\mathcal{K})'$. Moreover, since $p^v k \notin \mathcal{S}(\mathcal{K})$ for any $v \in \mathbb{Z}^+$, the equation of degree k in (3.8) is independent of the remaining equations of degree $j \in \mathcal{S}(\mathcal{K}) \setminus \{k\}$. Therefore, we deduce from (3.7) that

$$\Psi = \sum_{l\in\mathcal{L}_r}\Big|\sum_{\substack{h_i\in\mathbb{G}_{i(N-M)}\\ i\in\mathcal{S}(\mathcal{K})'}} b(\mathbf{h})e\Big(\alpha_k h_k l^k + \sum_{j\in\mathcal{S}(\mathcal{K})\setminus\{k\}}\gamma_j h_j l^j\Big)\Big|^2.$$

On recalling the definition (2.7) of $\kappa(\mathcal{K})$, we have

$$\sum_{i\in\mathcal{S}(\mathcal{K})'\setminus\{k\}} i = \kappa(\mathcal{K}) - k.$$

Thus, we may conclude via Cauchy's inequality that

$$\Psi \le (q^{N-M})^{\kappa(\mathcal{K})-k}\sum_{\substack{h_i\in\mathbb{G}_{i(N-M)}\\ i\in\mathcal{S}(\mathcal{K})'\setminus\{k\}}}\sum_{l\in\mathcal{L}_r}\Big|\sum_{h_k\in\mathbb{G}_{k(N-M)}} b(\mathbf{h})e(\alpha_k h_k l^k)\Big|^2. \tag{3.9}$$

Since $p \nmid k$, it follows from Theorem 2.2 and Lemma 3.3 that

$$\sum_{l\in\mathcal{L}_r}\Big|\sum_{h_k\in\mathbb{G}_{k(N-M)}} b(\mathbf{h})e(\alpha_k h_k l^k)\Big|^2 \le \big(|g| + q^{k(N-M)}\big)\sum_{h_k\in\mathbb{G}_{k(N-M)}}|b(\mathbf{h})|^2.$$

Furthermore, by considering the underlying equations and recalling our assumption that $s \ge \psi\phi+\psi$, it follows from Theorem 2.5 that there exists a constant $C_2 = C_2(s;\mathcal{K};\epsilon;q) > 0$ having the property that

$$\sum_{\substack{h_i\in\mathbb{G}_{i(N-M)}\\ i\in\mathcal{S}(\mathcal{K})'\setminus\{k\}}}\sum_{h_k\in\mathbb{G}_{k(N-M)}}|b(\mathbf{h})|^2 \le J_s(\mathcal{S}(\mathcal{K});N-M) \le C_2(q^{N-M})^{2s-\kappa(\mathcal{K})+\epsilon}.$$

Since $\operatorname{ord} g \le kM$ and $2M \le N$, we may combine these estimates within (3.9) to obtain the bound

$$\begin{aligned}\Psi &\le C_2(q^{N-M})^{2s-k+\epsilon}\big(|g| + q^{k(N-M)}\big)\\ &\le 2C_2(q^{N-M})^{2s+\epsilon}.\end{aligned}$$

We substitute this bound into (3.6), again noting that $\operatorname{ord} g \le kM$, to obtain the estimate

$$\Big|\sum_{x\in\mathbb{G}_N} e(f(x))\Big| \le 2q^N\big(2C_1C_2M(q^M)^{-1}(q^{kM})^{\epsilon}\big(q^{N-M})^{\epsilon}\big)^{1/(2s)}.$$

Therefore, there exists a constant $C_3 = C_3(s;\mathcal{K};\epsilon;q) > 0$ such that for values of M sufficiently large in terms of $\mathcal{K}$, ϵ and q, one has

$$\Big|\sum_{x\in\mathbb{G}_N} e(f(x))\Big| \le q^N\big(C_3(q^M)^{-1}(q^N)^{k\epsilon}\big)^{1/(2s)}.$$

We now make the specific choice

$$M = \lfloor \log_q C_3 + kN\epsilon + 2s\eta + 1\rfloor. \tag{3.10}$$

Then it follows that

$$\Big|\sum_{x\in\mathbb{G}_N} e(f(x))\Big| < q^{N-\eta},$$

which contradicts the lower bound assumed in the statement of Theorem 3.1. In view of the assumed bounds (3.4), this contradiction forces us to conclude that there exist $a \in \mathbb{F}_q[t]$ and monic $g \in \mathbb{F}_q[t]$ such that

$$\operatorname{ord}(g\alpha_k - a) < -kN + M \quad \text{and} \quad \operatorname{ord} g \le M.$$

Take $s = \psi\phi + \psi$, and then put $c = 1/(8s)$ and $C = 2s$. By assuming that $\epsilon < 1/(4(k+1))$, we see that the requirement $2M \le N$ is satisfied when $0 < \eta \le cN$, provided that N is sufficiently large in terms of $\mathcal{K}$, ϵ and q. We note that c and C are then constants depending only on $\mathcal{K}$ and q. Moreover, when N is sufficiently large, it follows from (3.10) that

$$M \le N(k+1)\epsilon + 2s\eta \le N(k+1)\epsilon + C\eta.$$

Since $\epsilon > 0$ is arbitrary, the conclusion of Theorem 3.1 follows. □

4. Extending the Weyl-type estimate to other coefficients

In this section, we extend Theorem 3.1 to indices which are not maximal. In preparation for the statement of this conclusion, we recall the definition (2.4) of $\mathcal{K}^*$.

Theorem 4.1. *Fix q and a finite set $\mathcal{K} \subset \mathbb{Z}^+$, and consider an integer $k \in \mathcal{K}^*$. There exist positive constants c_k and C_k, depending only on k, $\mathcal{K}$ and q, such that the following holds. Let $\epsilon > 0$ and let N be sufficiently large in terms of $\mathcal{K}$, ϵ and q. Suppose that $f(u) = \sum_{r\in\mathcal{K}\cup\{0\}} \alpha_r u^r$ is a polynomial with coefficients in $\mathbb{K}_\infty$ satisfying the bound*

$$\Big|\sum_{x\in\mathbb{G}_N} e(f(x))\Big| \ge q^{N-\eta},$$

for some positive number η with $\eta \le c_k N$. Then, there exist $a_k \in \mathbb{F}_q[t]$ and monic $g_k \in \mathbb{F}_q[t]$ such that

$$\operatorname{ord}(g_k\alpha_k - a_k) < -kN + \epsilon N + C_k\eta \quad \textit{and} \quad \operatorname{ord} g_k \le \epsilon N + C_k\eta.$$

Proof. Without loss of generality, we can assume that $\alpha_0 = 0$. We prove this theorem by downward induction on $k \in \mathcal{K}^*$ with respect to the partial order $\preceq_p$. If k is maximal in $\mathcal{K}$, then the conclusion is immediate from Theorem 3.1. Suppose that the conclusion of the theorem has been established for any $h \in \mathcal{K}^*$ with $k \preceq_p h$ and $h \ne k$. Define

$$\mathcal{H}_0 = \{h \in \mathcal{K}\colon k \preceq_p h \text{ and } h \ne k\} \quad \text{and} \quad \mathcal{H}_1 = \mathcal{K} \setminus \mathcal{H}_0. \tag{4.1}$$

Then it follows from Lemma 2.1(c) that $\mathcal{H}_0 \subset \mathcal{K}^*$. For $h \in \mathcal{H}_0$, let c_h and C_h be the positive constants whose existence is assured by the inductive hypothesis, as a consequence of the conclusion of Theorem 4.1. Let

$$c = \min\{c_h\colon h \in \mathcal{H}_0\} \quad \text{and} \qquad C = \sum_{h\in\mathcal{H}_0} C_h.$$

Suppose that for some positive number η with $\eta \le cN$, one has

$$\Big|\sum_{x\in\mathbb{G}_N} e(f(x))\Big| \ge q^{N-\eta}. \tag{4.2}$$

Let $\epsilon > 0$ be arbitrary, and let N be sufficiently large in terms of $\mathcal{K}$, ϵ and q. Then, by the inductive hypothesis, for any $h \in \mathcal{H}_0$ there exist $a_h \in \mathbb{F}_q[t]$ and monic $g_h \in \mathbb{F}_q[t]$ such that

$$\operatorname{ord}(g_h\alpha_h - a_h) < -hN + |\mathcal{H}_0|^{-1}\epsilon N + C_h\eta \quad \text{and} \quad \operatorname{ord} g_h \le |\mathcal{H}_0|^{-1}\epsilon N + C_h\eta.$$

Define

$$g = \prod_{h\in\mathcal{H}_0} g_h \quad \text{and} \quad b_h = a_h \prod_{j\in\mathcal{H}_0\setminus\{h\}} g_j.$$

Then g is monic and we have

$$\operatorname{ord}(g\alpha_h - b_h) < -hN + \epsilon N + C\eta \quad \text{and} \quad \operatorname{ord} g \le \epsilon N + C\eta. \tag{4.3}$$

Consider a positive integer M with $M < N - \operatorname{ord} g$. We rewrite the set $\mathbb{G}_N$ first as a union of arithmetic progressions modulo g, and then subdivide these arithmetic progressions into subprogressions of appropriately small length. Thus we obtain

$$\begin{aligned}\mathbb{G}_N &= \{gv + w\colon v \in \mathbb{G}_{N-\operatorname{ord} g} \text{ and } w \in \mathbb{G}_{\operatorname{ord} g}\}\\ &= \{g(t^M z + y) + w\colon z \in \mathbb{G}_{N-M-\operatorname{ord} g},\ y \in \mathbb{G}_M \text{ and } w \in \mathbb{G}_{\operatorname{ord} g}\}.\end{aligned}$$

For each $z \in \mathbb{G}_{N-M-\operatorname{ord} g}$ and $w \in \mathbb{G}_{\operatorname{ord} g}$, write $s = gt^M z + w$. Then $\operatorname{ord} s < N$ and we see that the set $\mathbb{G}_N$ can be partitioned into q^{N-M} blocks of the form

$$\mathcal{B}_s = \{gy + s\colon y \in \mathbb{G}_M\}.$$

Then it follows from the lower bound (4.2) that there exists a block $\mathcal{B}_s$ such that

$$\Big|\sum_{x\in\mathcal{B}_s} e(f(x))\Big| = \Big|\sum_{y\in\mathbb{G}_M} e(f(gy+s))\Big| \ge q^{N-\eta}\big(q^{N-M}\big)^{-1} = q^{M-\eta}. \tag{4.4}$$

By reference to (4.1), we see that

$$\Big|\sum_{y\in\mathbb{G}_M} e(f(gy+s))\Big| = \Big|\sum_{y\in\mathbb{G}_M} e\Big(\sum_{h\in\mathcal{H}_0}\alpha_h(gy+s)^h + \sum_{h\in\mathcal{H}_1}\alpha_h(gy+s)^h\Big)\Big|.$$

Write $\beta_h = \alpha_h - b_h/g$ $(h\in\mathcal{H}_0)$. Also, note that

$$e\Big(\sum_{h\in\mathcal{H}_0}\alpha_h s^h\Big)$$

is a constant independent of y, and

$$e\Big(\sum_{h\in\mathcal{H}_0}\frac{b_h}{g}\Big((gy+s)^h - s^h\Big)\Big) = 1.$$

Then we see that

$$\Big|\sum_{y\in\mathbb{G}_M} e(f(gy+s))\Big| = \Big|\sum_{y\in\mathbb{G}_M} e\Big(\sum_{h\in\mathcal{H}_0}\beta_h\big((gy+s)^h - s^h\big) + \sum_{h\in\mathcal{H}_1}\alpha_h(gy+s)^h\Big)\Big|. \tag{4.5}$$

For any $y\in\mathbb{G}_M$ and $h\in\mathcal{H}_0$, we have

$$\begin{aligned}\operatorname{ord}\big((gy+s)^h - s^h\big) &\le \operatorname{ord}(gy) + (h-1)\cdot\max\big\{\operatorname{ord}(gy),\operatorname{ord}s\big\}\\ &< \operatorname{ord}g + M + (h-1)N.\end{aligned}$$

It therefore follows from (4.3) that

$$\begin{aligned}\operatorname{ord}\big(\beta_h\big((gy+s)^h - s^h\big)\big) &< (-hN + \epsilon N + C\eta - \operatorname{ord}g) + (\operatorname{ord}g + M + (h-1)N)\\ &= \epsilon N + C\eta + M - N.\end{aligned}$$

We now make the specific choice

$$M = \lfloor (1-\epsilon)N - C\eta - 1\rfloor.$$

Then it follows that

$$\epsilon N + C\eta + M - N \le -1,$$

and hence

$$\operatorname{ord}\big(\beta_h\big((gy+s)^h - s^h\big)\big) < -1.$$

Therefore, we have

$$e\Big(\sum_{h\in\mathcal{H}_0}\beta_h\big((gy+s)^h - s^h\big) + \sum_{h\in\mathcal{H}_1}\alpha_h(gy+s)^h\Big) = e\Big(\sum_{h\in\mathcal{H}_1}\alpha_h(gy+s)^h\Big). \tag{4.6}$$

Combining (4.4), (4.5) and (4.6), we obtain the lower bound

$$\Big|\sum_{y\in\mathbb{G}_M} e\Big(\sum_{h\in\mathcal{H}_1}\alpha_h(gy+s)^h\Big)\Big| \ge q^{M-\eta}. \tag{4.7}$$

We note here that from (4.3) we have $\operatorname{ord}g \le \epsilon N + C\eta$, and thus for N sufficiently large, the above choice of M satisfies $0 < M < N - \operatorname{ord}g$.

In view of the definition (2.3), we have

$$\sum_{h\in\mathcal{H}_1}\alpha_h(gy+s)^h = \sum_{j\in\mathcal{S}(\mathcal{H}_1)\cup\{0\}}\gamma_j y^j, \tag{4.8}$$

for suitable coefficients $\gamma_j = \gamma_j(\boldsymbol{\alpha}, g, s) \in \mathbb{K}_\infty$. Since $k \in \mathcal{K}^*$ is maximal in $\mathcal{H}_1$, it follows from Lemma 2.1 that k is maximal in $\mathcal{S}(\mathcal{H}_1)$ and $k \in \mathcal{S}(\mathcal{H}_1)^*$. Furthermore, the coefficient of y^k in the polynomial on the left hand side of (4.8) is $\alpha_k g^k$. Note also that we may suppose the parameter M to be sufficiently large in terms of $\mathcal{K}$, ϵ and q. Thus, by Theorem 3.1, there exist positive constants d_k and D_k having the property that whenever the lower bound (4.7) holds for some positive number η with $\eta \le d_k M$, then there exist $\widetilde{a}_k \in \mathbb{F}_q[t]$ and monic $\widetilde{g}_k \in \mathbb{F}_q[t]$ such that

$$\operatorname{ord}(\widetilde{g}_k \alpha_k g^k - \widetilde{a}_k) < -kM + \epsilon M + D_k \eta \quad \text{and} \quad \operatorname{ord} \widetilde{g}_k \le \epsilon M + D_k \eta.$$

Let $g_k = \widetilde{g}_k g^k$ and $a_k = \widetilde{a}_k$. Since $(1-\epsilon)N - C\eta - 2 < M \le N$, for N sufficiently large, we have

$$\begin{aligned} \operatorname{ord}(g_k \alpha_k - a_k) &< -k\big((1-\epsilon)N - C\eta - 2\big) + \epsilon N + D_k \eta \\ &< -kN + \epsilon(k+2)N + (kC + D_k)\,\eta \end{aligned}$$

and, on recalling (4.3),

$$\operatorname{ord} g_k \le (\epsilon M + D_k \eta) + k(\epsilon N + C\eta) \le \epsilon(k+1)N + (kC + D_k)\eta.$$

Since $\epsilon > 0$ is arbitrary, the conclusion of Theorem 4.1 follows for k by taking $c_k = \min\{c, d_k\}$ and $C_k = kC + D_k$. This confirms the inductive step, and thus the proof of the theorem is complete. □

One can extend Theorem 4.1 to indices that are not in $\mathcal{K}^*$. Recall the definition (2.5) of $\widetilde{\mathcal{K}}$. Then by induction on n, one can apply the method of the proof of Theorem 4.1 to obtain the following conclusion.

Proposition 4.2. *Fix q and a finite set $\mathcal{K} \subset \mathbb{Z}^+$. There exist positive constants c and C, depending only on $\mathcal{K}$ and q, such that the following holds. Let $\epsilon > 0$ and let N be sufficiently large in terms of $\mathcal{K}$, ϵ and q. Suppose that $f(u) = \sum_{r \in \mathcal{K} \cup \{0\}} \alpha_r u^r$ is a polynomial with coefficients in $\mathbb{K}_\infty$ satisfying the bound*

$$\Big| \sum_{x \in \mathbb{G}_N} e(f(x)) \Big| \ge q^{N-\eta},$$

for some positive number η with $\eta \le cN$. Then, for any $k \in \widetilde{\mathcal{K}}$, there exist $a_k \in \mathbb{F}_q[t]$ and monic $g_k \in \mathbb{F}_q[t]$ such that

$$\operatorname{ord}(g_k \alpha_k - a_k) < -kN + \epsilon N + C\eta \quad \textit{and} \quad \operatorname{ord} g_k \le \epsilon N + C\eta.$$

It seems that there is no simple description of the set $\widetilde{\mathcal{K}}$. In many cases, it is apparent that $\widetilde{\mathcal{K}}$ is larger than $\mathcal{K}^*$. For example, if $p > 3$ and $\mathcal{K} = \{1, 3, 3p+1\}$ (as in the first case of Example 1.7), then

$$\mathcal{S}(\mathcal{K}) = \{1, 2, 3, p, p+1, 2p, 2p+1, 3p, 3p+1\},$$

and so $\mathcal{K}^* = \{3p+1\}$. Meanwhile, since $\mathcal{K}_1 = \{1, 3\}$, one finds that $\mathcal{K}_1^* = \{1, 3\}$, and since $\mathcal{S}(\mathcal{K}_1) = \{1, 2, 3\}$, it follows from (2.5) that $\widetilde{\mathcal{K}} = \mathcal{K}$. More generally, if $(k, p) = 1$ for any $k \in \mathcal{K}$, then it can be proved by induction that $\widetilde{\mathcal{K}} = \mathcal{K}$. On the other hand, if $p > 3$ and $\mathcal{K} = \{3, 4p\}$ (as in the second case of Example 1.7), then

$$\mathcal{S}(\mathcal{K}) = \{1, 2, 3, p, 2p, 3p, 4p\},$$

and hence $\mathcal{K}^* = \emptyset$. Thus we find that in this case, one has $\widetilde{\mathcal{K}} = \emptyset$. Therefore, we cannot go as far as proving Conjecture 1.3 by using this method.

5. Equidistribution of polynomial sequences

In this section, we first prove the equidistribution result recorded in Theorem 1.4, and then discuss a variant of this theorem. The following lemma is essential for our proof of Theorem 1.4. We again recall the set of exponents $\mathcal{K}^*$ defined in (2.4).

Lemma 5.1. *Fix q and a finite set $\mathcal{K} \subset \mathbb{Z}^+$. Let $f(u) = \sum_{r \in \mathcal{K} \cup \{0\}} \alpha_r u^r$ be a polynomial with coefficients in $\mathbb{K}_\infty$. For $k \in \mathcal{K}^*$, suppose that k is maximal in $\mathcal{K}$ and α_k is irrational. Then, for any fixed $\eta > 0$, there exists $N_0 \in \mathbb{Z}^+$ such that, for any $s \in \mathbb{F}_q[t]$, we have*

$$\left| \sum_{y \in \mathbb{G}_{N_0}} e(f(y+s)) \right| < q^{N_0 - \eta}.$$

Proof. By way of deriving a contradiction, suppose that $\eta > 0$, and that for any $N \in \mathbb{Z}^+$, there exists $s_N \in \mathbb{F}_q[t]$ such that

$$\left| \sum_{y \in \mathbb{G}_N} e(f(y+s_N)) \right| \geq q^{N-\eta}. \tag{5.1}$$

We note that for each $s \in \mathbb{F}_q[t]$, the only monomials y^r having non-zero coefficient in the expansion of $f(y+s)$ are those with $r \in \mathcal{S}(\mathcal{K})$. Since $k \in \mathcal{K}^*$ is maximal in $\mathcal{K}$, it follows from Lemma 2.1 that k is maximal in $\mathcal{S}(\mathcal{K})$ and further that $k \in \mathcal{S}(\mathcal{K})^*$. Moreover, the coefficient of y^k in $f(y+s)$ is α_k. Applying Theorem 3.1 with $\epsilon = 1/3$, we find that there exists a constant $C > 0$ such that, for N sufficiently large in terms of $\mathcal{K}$ and q, there exist $a \in \mathbb{F}_q[t]$ and monic $g \in \mathbb{F}_q[t]$ having the property that

$$\operatorname{ord}(g\alpha_k - a) \leq -kN + N/3 + C\eta \quad \text{and} \quad \operatorname{ord} g < N/3 + C\eta.$$

For each sufficiently large $M \in \mathbb{Z}^+$, we apply these inequalities with $N = \lfloor 3(M - C\eta) \rfloor$. Thus, we have

$$\operatorname{ord}(g\alpha_k - a) \leq -(3k-1)M + (3kC\eta + k - 1/3) \leq -3M/2 \quad \text{and} \quad \operatorname{ord} g < M.$$

Since these inequalities hold for all sufficiently large $M \in \mathbb{Z}^+$, we deduce from Lemma 2.7 that α_k is rational, contradicting the hypothesis that α_k is irrational. Consequently, the assumed lower bound (5.1) is untenable, and the conclusion of the lemma follows. □

We are now equipped for the proof of Theorem 1.4.

Proof of Theorem 1.4. It is apparent that there is no loss of generality in assuming that $\alpha_0 = 0$. Let $k \in \mathcal{K}^*$ and suppose that α_k is irrational. We prove Theorem 1.4 by downward induction on k with respect to the partial order $\preceq_p$. Suppose first that k is maximal in $\mathcal{K}$ and $\eta > 0$. Let N_0 be the natural number provided in the conclusion of Lemma 5.1. For any $N \geq N_0$, we can partition the set $\mathbb{G}_N$ into q^{N-N_0} blocks of the form

$$\mathcal{B}_s = \{y + s : y \in \mathbb{G}_{N_0}\},$$

where $s = t^{N_0}z$ for some $z \in \mathbb{G}_{N-N_0}$. Therefore, it follows from Lemma 5.1 that

$$\Big|\sum_{x\in\mathbb{G}_N} e(f(x))\Big| \le q^{N-N_0} \sup_{s\in\mathbb{F}_q[t]}\Big|\sum_{y\in\mathbb{G}_{N_0}} e(f(y+s))\Big| < q^{N-N_0}q^{N_0-\eta} = q^{N-\eta}.$$

Since $\eta > 0$ is arbitrary, it follows that

$$\lim_{N\to\infty} \frac{1}{q^N}\Big|\sum_{x\in\mathbb{G}_N} e(f(x))\Big| = 0.$$

We note that for any $m \in \mathbb{F}_q[t] \setminus \{0\}$, this relation holds with f replaced by mf, where mf is the polynomial

$$mf(u) = \sum_{r\in\mathcal{K}\cup\{0\}} m\alpha_r u^r.$$

By reference to Theorem 2.8, we therefore conclude that Theorem 1.4 holds in the special case in which k is maximal in $\mathcal{K}$.

Suppose next that the theorem is established for any $h \in \mathcal{K}^*$ with $k \preceq_p h$ and $h \ne k$. We define $\mathcal{H}_0$ and $\mathcal{H}_1$ as in (4.1). Note that, should there exist $h \in \mathcal{H}_0$ for which α_h is irrational, then Theorem 1.4 follows from the inductive hypothesis. Therefore, it suffices to consider the situation in which all of the coefficients α_h ($h \in \mathcal{H}_0$) are rational. Let g be the common denominator of the coefficients α_h for $h \in \mathcal{K}_0$. Then for any $s \in \mathbb{F}_q[t]$ and $M \in \mathbb{Z}^+$, we have

$$\begin{aligned}\Big|\sum_{y\in\mathbb{G}_M} e(f(gy+s))\Big| &= \Big|\sum_{y\in\mathbb{G}_M} e\Big(\sum_{h\in\mathcal{K}} \alpha_h(gy+s)^h\Big)\Big| \\ &= \Big|\sum_{y\in\mathbb{G}_M} e\Big(\sum_{h\in\mathcal{H}_0} \alpha_h\Big((gy+s)^h - s^h\Big) + \sum_{h\in\mathcal{H}_1} \alpha_h(gy+s)^h\Big)\Big|.\end{aligned}$$

Here, we have made use of the observation that

$$e\Big(\sum_{h\in\mathcal{H}_0} \alpha_h(-s^h)\Big)$$

is a unimodular constant independent of y. Since the definition of g implies that $g\alpha_h \in \mathbb{F}_q[t]$ for each $h \in \mathcal{H}_0$, we have

$$e\Big(\sum_{h\in\mathcal{H}_0} \alpha_h\Big((gy+s)^h - s^h\Big)\Big) = 1.$$

It follows that

$$\Big|\sum_{y\in\mathbb{G}_M} e(f(gy+s))\Big| = \Big|\sum_{y\in\mathbb{G}_M} e\Big(\sum_{h\in\mathcal{H}_1} \alpha_h(gy+s)^h\Big)\Big|. \tag{5.2}$$

Given $N \in \mathbb{Z}^+$ with $N > \operatorname{ord} g$, we define the integer $M \in \mathbb{Z}^+$ by putting $M = N - \operatorname{ord} g$. Then we can partition the set $\mathbb{G}_N$ into q^{N-M} blocks of the form

$$\mathcal{B}_s = \{gy + s \colon y \in \mathbb{G}_M\},$$

where $s \in \mathbb{G}_{\operatorname{ord} g}$. We now deduce from (5.2) that

$$\begin{aligned}\Big|\sum_{x\in\mathbb{G}_N} e(f(x))\Big| &\le q^{N-M} \max_{s\in\mathbb{G}_{\operatorname{ord} g}} \Big|\sum_{y\in\mathbb{G}_M} e(f(gy+s))\Big| \\ &= q^{N-M} \max_{s\in\mathbb{G}_{\operatorname{ord} g}} \Big|\sum_{y\in\mathbb{G}_M} e\Big(\sum_{h\in\mathcal{H}_1} \alpha_h(gy+s)^h\Big)\Big|. \end{aligned} \tag{5.3}$$

We observe that for each $s \in \mathbb{F}_q[t]$, the only monomials y^r having non-zero coefficient in the expansion of

$$\sum_{h\in\mathcal{H}_1} \alpha_h(gy+s)^h \tag{5.4}$$

are those with $r \in \mathcal{S}(\mathcal{H}_1)$. Since $k \in \mathcal{K}^*$ is maximal in $\mathcal{H}_1$, we discern from Lemma 2.1 that k is maximal in $\mathcal{S}(\mathcal{H}_1)$ and $k \in \mathcal{S}(\mathcal{H}_1)^*$. Furthermore, the coefficient of y^k in the polynomial (5.4) is $\alpha_k g^k$, which is irrational since α_k is irrational. We are now in the situation already handled in the first part of the proof, and thus, we have

$$\lim_{M\to\infty} \frac{1}{q^M}\Big|\sum_{y\in\mathbb{G}_M} e\Big(\sum_{h\in\mathcal{H}_1} \alpha_h(gy+s)^h\Big)\Big| = 0.$$

Then it follows from (5.3) that

$$\lim_{N\to\infty} \frac{1}{q^N}\Big|\sum_{x\in\mathbb{G}_N} e(f(x))\Big| = 0.$$

We again note that for any $m \in \mathbb{F}_q[t] \setminus \{0\}$, this relation remains valid with f replaced by mf, and thus Theorem 2.8 shows the sequence $(f(x))_{x\in\mathbb{F}_q[t]}$ to be equidistributed in $\mathbb{T}$. This confirms the inductive step, and thus the proof of the theorem is complete. □

By an observation similar to the one made following the proof of Theorem 4.1, one can apply the method of the proof of Theorem 1.4 to obtain the following result. Here, once again, we recall the definition (2.5) of the set of exponents $\widetilde{\mathcal{K}}$.

Proposition 5.2. *Fix q and a finite set $\mathcal{K} \subset \mathbb{Z}^+$. Let $f(u) = \sum_{r\in\mathcal{K}\cup\{0\}} \alpha_r u^r$ be a polynomial with coefficients in $\mathbb{K}_\infty$. Suppose that α_k is irrational for some $k \in \widetilde{\mathcal{K}}$. Then the sequence $(f(x))_{x\in\mathbb{F}_q[t]}$ is equidistributed in $\mathbb{T}$.*

Of notable significance in this conclusion is the situation in which $(k, p) = 1$ for all $k \in \mathcal{K}$, for then we have $\widetilde{\mathcal{K}} = \mathcal{K}$. Using the latter observation, we now show that the above proposition implies Conjecture 1.3 in the special case $q = p$. For the rest of this section, we assume that $q = p$.

Let $T\colon \mathbb{K}_\infty \to \mathbb{T}$ be the map defined in (1.1). Using the fact that $a^p = a$ for any $a \in \mathbb{F}_p$, one can show that for any $x \in \mathbb{F}_p[t]$, one has

$$e\left(\alpha x^p\right) = e\left(T(\alpha)x\right).$$

Therefore, for any $x \in \mathbb{F}_p[t]$ and $v \in \mathbb{Z}^+ \cup \{0\}$, we have

$$e\left(\alpha x^{p^v}\right) = e\left(T^v(\alpha)x\right), \tag{5.5}$$

where T^v is the v-fold composition of T. Let

$$f(u) = \sum_{r \in \mathcal{K} \cup \{0\}} \alpha_r u^r \in \mathbb{K}_\infty[u],$$

and let

$$\mathcal{I} = \{k \in \mathbb{Z}^+ \colon (k,p) = 1 \text{ and } p^v k \in \mathcal{K} \text{ for some } v \in \mathbb{Z}^+ \cup \{0\}\}. \tag{5.6}$$

For each $k \in \mathcal{I}$, define

$$S_k(f) = \sum_{\substack{v \geq 0 \\ p^v k \in \mathcal{K}}} T^v(\alpha_{p^v k}). \tag{5.7}$$

Then it follows from (5.5) that for any $x \in \mathbb{F}_p[t]$, one has

$$e\left(f(x)\right) = e\bigg(\sum_{k \in \mathcal{I}} S_k(f) x^k + \alpha_0\bigg). \tag{5.8}$$

Since $(k,p) = 1$ for any $k \in \mathcal{I}$, we have $\widetilde{\mathcal{I}} = \mathcal{I}$. Let $m \in \mathbb{F}_p[t] \setminus \{0\}$. Then Proposition 5.2 shows that whenever there exists $k \in \mathcal{I}$ such that $S_k(mf)$ is irrational, one has

$$\lim_{N \to \infty} \frac{1}{q^N} \bigg| \sum_{x \in \mathbb{G}_N} e(mf(x)) \bigg| = \lim_{N \to \infty} \frac{1}{q^N} \bigg| \sum_{x \in \mathbb{G}_N} e\bigg(\sum_{k \in \mathcal{I}} S_k(mf) x^k + m\alpha_0 \bigg) \bigg| = 0. \tag{5.9}$$

Therefore, on making use of Theorem 2.8, we may conclude as follows.

Corollary 5.3. *Fix $q = p$ and a finite set $\mathcal{K} \subset \mathbb{Z}^+$. Let $f(u) = \sum_{r \in \mathcal{K} \cup \{0\}} \alpha_r u^r$ be a polynomial with coefficients in $\mathbb{K}_\infty$. Suppose that the polynomial f satisfies the property that for some $k \in \mathcal{I}$, we have*

$$S_k(mf) \text{ is irrational for any } m \in \mathbb{F}_p[t] \setminus \{0\}. \tag{5.10}$$

Then the sequence $(f(x))_{x \in \mathbb{F}_p[t]}$ is equidistributed in $\mathbb{T}$.

We remark that since the map T does not commute with multiplication by m, the condition (5.10) may not be described in simpler terms. This condition might also be unnecessary for the equidistribution of $(f(x))_{x \in \mathbb{F}_p[t]}$. Regardless of these observations, suppose that $k \in \mathcal{K}$ and $p^v k \notin \mathcal{K}$ for any $v \in \mathbb{Z}^+$. Then $S_k(f) = \alpha_k$ and $S_k(mf) = m\alpha_k$ for any $m \in \mathbb{F}_p[t] \setminus \{0\}$. Therefore, should α_k be irrational, then the condition (5.10) is satisfied. This simple observation establishes Conjecture 1.3 in the special case $q = p$. We can formulate this conclusion more precisely in the following corollary.

Corollary 5.4. *Fix $q = p$ and a finite set $\mathcal{K} \subset \mathbb{Z}^+$. Let $f(u) = \sum_{r \in \mathcal{K} \cup \{0\}} \alpha_r u^r$ be a polynomial with coefficients in $\mathbb{K}_\infty$. Suppose that α_k is irrational for some $k \in \mathcal{K}$ satisfying $p \nmid k$ and furthermore $p^v k \notin \mathcal{K}$ for any $v \in \mathbb{Z}^+$. Then the sequence $(f(x))_{x \in \mathbb{F}_p[t]}$ is equidistributed in $\mathbb{T}$.*

6. Van der Corput and intersective sets in $\mathbb{F}_q[t]$

6.1. **Background and statement of results.** We define the *upper density* $\overline{d}(\mathcal{A})$ of a set $\mathcal{A} \subset \mathbb{Z}^+$ by means of the relation

$$\overline{d}(\mathcal{A}) = \limsup_{N\to\infty} \frac{\operatorname{card}(\mathcal{A} \cap \{1, \dots, N\})}{N}.$$

We say that $\mathcal{A}$ is *dense* if $\overline{d}(\mathcal{A}) > 0$. A set $\mathcal{H} \subset \mathbb{Z}^+$ is called *intersective* if, for any dense subset $\mathcal{A} \subset \mathbb{Z}^+$, there exist $a, a' \in \mathcal{A}$ such that $a - a' \in \mathcal{H}$. Thus, the set $\mathcal{H}$ is intersective if for any dense subset $\mathcal{A}$ of positive integers, one has $\mathcal{H} \cap (\mathcal{A} - \mathcal{A}) \neq \emptyset$. In the late 1970s, Sárközy [30] and Furstenberg [11] proved independently that the set $\{n^2 \colon n \in \mathbb{Z}^+\}$ is intersective. Their proofs make use of the circle method and ergodic theory, respectively. Sárközy went on to prove that the sets $\{n^2 - 1 \colon n \in \mathbb{Z}^+ \setminus \{1\}\}$ and $\{p - 1 \colon p \in \mathbb{Z} \text{ is prime}\}$ are also intersective (see [31]). We refer the reader to a survey paper of the first author [21] for results and open problems regarding intersective sets.

In a seemingly unrelated context, motivated by van der Corput's difference theorem, Kamae and Mendès France [16] made the following definition. A set $\mathcal{H} \subset \mathbb{Z}^+$ is said to be *van der Corput* if the sequence $(a_n)_{n=1}^{\infty}$ is equidistributed $(\mathrm{mod}\, 1)$ whenever the sequence $(a_{n+h} - a_n)_{n=1}^{\infty}$ is equidistributed $(\mathrm{mod}\, 1)$ for each $h \in \mathcal{H}$. Therefore, it follows from van der Corput's difference theorem that $\mathbb{Z}^+$ is van der Corput. However, there are sparser sets which are van der Corput. In [16], Kamae and Mendès France proved that any van der Corput set is intersective. Their result gives another approach to intersective sets. The converse of their theorem is not true. In [6], Bourgain constructed a set that is intersective but not van der Corput.

Let $\Phi(u) \in \mathbb{Z}[u]$ and consider the set $\{\Phi(n) \colon n \in \mathbb{Z}\} \cap \mathbb{Z}^+$. We note that for any $g \in \mathbb{Z}^+$, the set of all multiples of g is dense. Therefore, if the set $\{\Phi(n) \colon n \in \mathbb{Z}\} \cap \mathbb{Z}^+$ is van der Corput (and hence intersective), then g divides $\Phi(n)$ for some $n \in \mathbb{Z}$. The following result of Kamae and Mendès France [16] shows that the divisibility condition is not only necessary, but also sufficient.

Proposition 6.1. *Let $\Phi(u) \in \mathbb{Z}[u] \setminus \{0\}$, and suppose that Φ has a root $(\mathrm{mod}\ g)$ for any $g \in \mathbb{Z}^+$. Then the set $\{\Phi(n) \colon n \in \mathbb{Z}\} \cap \mathbb{Z}^+$ is van der Corput (and hence intersective) whenever it is infinite.*

Notice that these notions of intersective and van der Corput sets, and the concommitant conclusions, extend readily to the situation that $\mathcal{A} \subset \mathbb{Z}$ and $\mathcal{H} \subset \mathbb{Z} \setminus \{0\}$. Given the similarity of $\mathbb{Z}$ and $\mathbb{F}_q[t]$, it is natural to study analogous notions in $\mathbb{F}_q[t]$. We define the *upper density* $\overline{d}(\mathcal{A})$ of a set $\mathcal{A} \subset \mathbb{F}_q[t]$ by means of the relation

$$\overline{d}(\mathcal{A}) = \limsup_{N\to\infty} \frac{\operatorname{card}(\mathcal{A} \cap \mathbb{G}_N)}{q^N}.$$

We say a set $\mathcal{A}$ is *dense* if $\overline{d}(\mathcal{A}) > 0$. A set $\mathcal{H} \subset \mathbb{F}_q[t] \setminus \{0\}$ is called *intersective* if, for any dense subset $\mathcal{A} \subset \mathbb{F}_q[t]$, we have $\mathcal{H} \cap (\mathcal{A} - \mathcal{A}) \neq \emptyset$. A set $\mathcal{H} \subset \mathbb{F}_q[t] \setminus \{0\}$ is said to be *van der Corput* if the sequence $(a_x)_{x\in\mathbb{F}_q[t]}$ is equidistributed in $\mathbb{T}$ whenever the sequence $(a_{x+h} - a_x)_{x\in\mathbb{F}_q[t]}$ is equidistributed in $\mathbb{T}$ for each $h \in \mathcal{H}$. Many characterizations

of intersective and van der Corput sets carry over from $\mathbb{Z}$ to $\mathbb{F}_q[t]$, and we refer the reader to the Ph.D. thesis of the first author [22, Chapter 2] for an exposition. In particular, in [22, Theorem 2.3.5], it was proved that any van der Corput set in $\mathbb{F}_q[t]$ is intersective. It is an interesting problem to construct a set in $\mathbb{F}_q[t]$ that is intersective but not van der Corput (Bourgain's construction in $\mathbb{Z}$ is very specific to the real numbers).

We now consider explicit examples of intersective and van der Corput sets in $\mathbb{F}_q[t]$ that are of arithmetic interest, similar to the results of Sárközy and Furstenberg. In the work of the first two authors [24], intersectivity is obtained, in a quantitative sense, for the set $\{x^2 \colon x \in \mathbb{F}_q[t]\} \setminus \{0\}$. Furthermore, in joint work of the first author with Spencer [25], intersectivity, in a quantitative sense, is also established for the set

$$\{l + r \colon l \in \mathbb{F}_q[t], \text{ with } l \text{ monic and irreducible}\},$$

for any fixed $r \in \mathbb{F}_q \setminus \{0\}$. Motivated by Proposition 6.1, we formulate the following conjecture.

Conjecture 6.2. *For $\Phi(u) \in \mathbb{F}_q[t, u] \setminus \{0\}$, suppose that*

$$\text{for all } g \in \mathbb{F}_q[t], \text{ there exists } x \in \mathbb{F}_q[t] \text{ such that } \Phi(x) \equiv 0 \pmod{g}. \tag{6.1}$$

Then the set $\{\Phi(x) \colon x \in \mathbb{F}_q[t]\} \setminus \{0\}$ is van der Corput (and hence intersective).

Again, the divisibility condition is easily seen to be necessary. Quite surprisingly, this conjecture remains an open problem when the degree of Φ is greater than or equal to p. When $\Phi(0) = 0$, it follows from the polynomial Szemerédi theorem for modules over countable integral domains, proved by Bergelson, Leibman and McCutcheon [4], that the set $\{\Phi(x) \colon x \in \mathbb{F}_q[t]\} \setminus \{0\}$ is intersective. Recently, using the polynomial method of Croot, Lev and Pach [9], it was shown by Green [14] that this conjecture holds in a strong quantitative sense, under the condition that $\Phi(u) \in \mathbb{F}_q[u]$ and the number of roots of $\Phi(u)$ in $\mathbb{F}_q$ is coprime to q. The latter constraint was recently removed by Li and Sauermann [26] (see also [5] for a simpler argument). We note that the condition (6.1) is weaker than demanding that $\Phi(u)$ has a root in $\mathbb{F}_q[t]$. Indeed, by analogy with well-known examples over the rational integers, we observe that when $p > 2$ and a and b are distinct irreducible polynomials of even degree in $\mathbb{F}_p[t]$ with b a quadratic residue modulo a (and hence also a a quadratic residue modulo b), the polynomial $\Phi(u) = (u^2 - a)(u^2 - b)(u^2 - ab)$ fails to have roots in $\mathbb{F}_p[t]$, yet nonetheless possesses solutions modulo g, for all $g \in \mathbb{F}_p[t]$. We direct the reader to Li [27, Example 1] and Yamagishi [38, Appendix A] for examples of polynomials Φ satisfying (6.1) but not having roots in $\mathbb{F}_q[t]$.

Equipped now with our equidistribution theorem, we make some progress in this section towards Conjecture 6.2. In Section 6.3 we prove the following conclusion, which is slightly stronger than Theorem 1.9. Here, we recall the definition (2.4) of the set of exponents $\mathcal{K}^*$.

Theorem 6.3. *Let $\mathcal{K}$ be a finite set of positive integers, suppose that $a_r \in \mathbb{F}_q[t]$ for $r \in \mathcal{K} \cup \{0\}$, and define*

$$\Phi(u) = \sum_{r \in \mathcal{K} \cup \{0\}} a_r u^r.$$

Suppose that Φ satisfies the condition (6.1)*. Suppose further that $a_k \neq 0$ for some $k \in \mathcal{K}^*$. Then the set $\{\Phi(x) \colon x \in \mathbb{F}_q[t]\} \setminus \{0\}$ is van der Corput (and hence intersective).*

We remark that, as a direct consequence of Theorem 6.3, one finds that Conjecture 6.2 holds whenever the degree of Φ is coprime to p. Moreover, in view of Proposition 5.2, the condition in the theorem requiring $a_k \neq 0$ for some $k \in \mathcal{K}^*$ can be relaxed to one requiring only that $a_k \neq 0$ for some $k \in \widetilde{\mathcal{K}}$, where $\widetilde{\mathcal{K}}$ is defined as in (2.5).

By assuming the stronger conditions $q = p$ and $\Phi(0) = 0$, we obtain the following result in Section 6.3.

Theorem 6.4. *Let $\Phi(u) \in \mathbb{F}_p[t,u] \setminus \{0\}$, and suppose that $\Phi(0) = 0$. Then the set $\{\Phi(x) \colon x \in \mathbb{F}_p[t]\} \setminus \{0\}$ is van der Corput (and hence intersective).*

We remark here that the conclusion of Theorem 4.1 can be applied to prove intersectivity of the set $\{\Phi(x) \colon x \in \mathbb{F}_q[t]\} \setminus \{0\}$ in Theorem 6.3 in a quantitative sense, in a manner similar to that employed in the proof of [24, Theorem 3]. However, we opt to make use of Theorem 1.4 since the deduction is quicker, and the van der Corput property is a stronger notion than intersectivity.

6.2. **Comparison with Bergelson-Leibman's result.** Bergelson and Leibman [3] also applied their equidistribution result to study intersective sets in $\mathbb{F}_q[t]$. As such, our results in this section overlap with the conclusion of their Theorem 9.5, though they are not identical. Before proceeding with the proofs of Theorems 6.3 and 6.4, we make a comparison between these theorems and [3, Theorem 9.5], which we rephrase below.

Theorem (Bergelson-Leibman)**.** *Let $\Phi(u) \in \mathbb{F}_q[t,u] \setminus \{0\}$, and suppose that $\Phi(0) = 0$. Then the set $\{\Phi(x) \colon x \in \mathbb{F}_q[t]\} \setminus \{0\}$ is intersective. Furthermore, the same conclusion holds provided that Φ satisfies the condition*[2,3] *that*

$$\text{for all subgroups } \Lambda \text{ of finite index in } (\mathbb{F}_q[t],+), \text{ there exists } x \in \mathbb{F}_q[t] \text{ such that } \Phi(x) \in \Lambda. \tag{6.2}$$

Bergelson and Leibman proved this theorem following the proof by Furstenberg [11] of Sárközy's theorem in $\mathbb{Z}$ (and in fact they proved a Khintchine-type theorem for single recurrence). On the other hand, our proofs of Theorems 6.3 and 6.4 follow the treatment of Kamae and Mendès France of van der Corput sets in $\mathbb{Z}$. Since in $\mathbb{F}_q[t]$, van der Corput sets and intersective sets are (conjecturally) two distinct notions, our own results and those of Bergelson and Leibman [3, Theorem 9.5] do not imply each other.

The condition (6.2) is clearly necessary in order that the set $\{\Phi(x) \colon x \in \mathbb{F}_q[t]\} \setminus \{0\}$ be intersective. It is also easy to see that the condition (6.2) (an algebraic condition) implies (6.1) (an arithmetic condition). We note, however, that there are plenty of subgroups of finite index in the additive group $\mathbb{F}_q[t]$ which are not of the shape $g\mathbb{F}_q[t]$ for any $g \in \mathbb{F}_q[t]$. For each irrational $\alpha \in \mathbb{K}_\infty$, an example of such a subgroup is the Bohr set consisting

[2]See the remark in [3, p. 949], though there is a misprint in the definition of intersectivity therein.

[3]Just prior to the submission of this paper, Ackelsberg and Bergelson uploaded a paper [1] to the arXiv in which some correction and clarification concerning their notion of intersectivity over $\mathbb{F}_q[t]$ is made (see the first footnote on page 2 of [1] and the accompanying discussion). Nonetheless, at this time we remain unable to identify a source in the literature for a proof of Conjecture 6.2, and it seems fair to describe the current status of the notion of intersectivity associated with this perspective as being in a state of flux.

of all poynomials $x \in \mathbb{F}_q[t]$ satisfying the condition $\operatorname{ord}\{\alpha x\} < -1$. We cannot help but wonder if the conditions (6.2) and (6.1) are in fact the same condition. (This issue does not arise in $\mathbb{Z}$, since all subgroups of finite index of $\mathbb{Z}$ are of the form $a\mathbb{Z}$ for some $a \neq 0$.)

Question 1. *Does the condition* (6.1) *imply* (6.2)*? In other words, as far as polynomials in* $\mathbb{F}_q[t]$ *are concerned, does "meeting all subgroups of arithmetic nature" imply "meeting all subgroups of finite index"?*

6.3. **The proofs of Theorems 6.3 and 6.4.** Among the many characterizations of van der Corput sets in $\mathbb{F}_q[t]$, we will apply the following one found in [22, Theorem 2.4.5 (2)]. Let μ be a finite non-negative measure on $\mathbb{T}$. We say that μ is *continuous* at 0 if $\mu(\{0\}) = 0$. For any $h \in \mathbb{F}_q[t]$, the *Fourier transform* of μ is denoted by $\widehat{\mu}$ and defined by

$$\widehat{\mu}(h) = \int_{\mathbb{T}} e(-\alpha h)\, \mathrm{d}\mu(\alpha).$$

We say that $\widehat{\mu}$ *vanishes* on a set $\mathcal{H} \subset \mathbb{F}_q[t]$ if $\widehat{\mu}(h) = 0$ for all $h \in \mathcal{H}$.

Theorem 6.5 (Kamae & Mendès France, Ruzsa)**.** *A set* $\mathcal{H} \subset \mathbb{F}_q[t] \setminus \{0\}$ *is van der Corput if and only if any finite measure* μ *on* $\mathbb{T}$*, with* $\widehat{\mu}$ *vanishing on* $\mathcal{H}$*, is continuous at* 0*.*

We are now equipped to prove Theorems 6.3 and 6.4.

Proof of Theorem 6.3. Suppose that $\Phi(u) = \sum_{k \in \mathcal{K} \cup \{0\}} a_r u^r \in \mathbb{F}_q[t, u]$ has a root $(\bmod g)$ for any $g \in \mathbb{F}_q[t] \setminus \{0\}$. Suppose further that $a_k \neq 0$ for some $k \in \mathcal{K}^*$. Let

$$\mathcal{H} = \{\Phi(x) \colon x \in \mathbb{F}_q[t]\} \setminus \{0\}. \tag{6.3}$$

Also, let $\alpha \in \mathbb{T}$ be irrational, and consider $s \in \mathbb{F}_q[t]$ and monic $g \in \mathbb{F}_q[t]$. By the orthogonality relation (2.2), we have

$$\begin{aligned}\frac{1}{q^N} \sum_{\substack{x \in \mathbb{G}_N \\ x \equiv s \,(\bmod g)}} e\left(\alpha \Phi(x)\right) &= \frac{1}{q^N} \sum_{x \in \mathbb{G}_N} e\left(\alpha \Phi(x)\right) \frac{1}{|g|} \sum_{y \in \mathbb{G}_{\operatorname{ord} g}} e\left(\frac{y(x-s)}{g}\right) \\ &= \frac{1}{|g|} \sum_{y \in \mathbb{G}_{\operatorname{ord} g}} \frac{1}{q^N} \sum_{x \in \mathbb{G}_N} e\left(\alpha \Phi(x) + \frac{y(x-s)}{g}\right).\end{aligned}$$

We observe that the coefficient of x^k in the polynomial $\alpha\Phi(x) + y(x-s)/g$ is either αa_k or $\alpha a_k + y/g$, according to whether $k \neq 1$ or $k = 1$, and in either case this coefficient is irrational. Therefore, it follows from Theorem 1.4 that for any $y \in \mathbb{G}_{\operatorname{ord} g}$, we have

$$\lim_{N \to \infty} \frac{1}{q^N} \left| \sum_{x \in \mathbb{G}_N} e\left(\alpha \Phi(x) + \frac{y(x-s)}{g}\right) \right| = 0,$$

whence

$$\lim_{N \to \infty} \frac{1}{|g|} \sum_{y \in \mathbb{G}_{\operatorname{ord} g}} \frac{1}{q^N} \left| \sum_{x \in \mathbb{G}_N} e\left(\alpha \Phi(x) + \frac{y(x-s)}{g}\right) \right| = 0.$$

Combining these relations, we infer that for any irrational $\alpha \in \mathbb{T}$, and for all $s \in \mathbb{F}_q[t]$ and monic $g \in \mathbb{F}_q[t]$, one has

$$\lim_{N\to\infty} \frac{1}{q^N} \Big| \sum_{x\in\mathbb{G}_N} e\left(\alpha\Phi(gx+s)\right)\Big| = |g| \lim_{N\to\infty} \frac{1}{q^N} \Big| \sum_{\substack{x\in\mathbb{G}_N \\ x\equiv s \pmod g}} e\left(\alpha\Phi(x)\right)\Big| = 0. \tag{6.4}$$

For any $M \in \mathbb{Z}^+$, let g_M be the product of all of the monic polynomials in $\mathbb{G}_M$. We consider a root $s_M \in \mathbb{F}_q[t]$ of $\Phi \pmod{g_M}$, the existence of which is guaranteed by our hypotheses concerning Φ. For $\alpha \in \mathbb{T}$, let

$$T_{M,N}(\alpha) = \frac{1}{q^N} \sum_{x\in\mathbb{G}_N} e(\alpha\Phi(g_M x + s_M)). \tag{6.5}$$

It is useful also to define the associated Fourier coefficients

$$\widehat{T_{M,N}}(h) = \int_{\mathbb{T}} T_{M,N}(\alpha) e(-\alpha h)\, \mathrm{d}\alpha.$$

Then

$$T_{M,N}(\alpha) = \sum_{h\in\mathbb{F}_q[t]} \widehat{T_{M,N}}(h) e(\alpha h).$$

We now analyze the quantity $T_{M,N}(\alpha)$, dividing our discussion into cases according to whether α is rational or irrational.

Case 1. Suppose that $\alpha \in \mathbb{T}$ is irrational. In this case, we find from (6.4) that for any $M \in \mathbb{Z}^+$ and any irrational $\alpha \in \mathbb{T}$, we have

$$\lim_{N\to\infty} T_{M,N}(\alpha) = 0.$$

Case 2. Suppose that $\alpha \in \mathbb{T}$ is rational. In this case, we observe that a trivial estimate supplies the bound $|T_{M,N}(\alpha)| \le 1$, so that the sequence $(T_{M,N}(\alpha))_{N\in\mathbb{Z}^+}$ is bounded uniformly in M and α. Thus, since the set

$$\{(\alpha, M)\colon \alpha \in \mathbb{T} \text{ is rational and } M \in \mathbb{Z}^+\}$$

is countable, it follows from a diagonalization process that we can extract a subsequence $(N_i)_{i=1}^{\infty}$ of the natural numbers having the property that, for any $M \in \mathbb{Z}^+$ and any rational $\alpha \in \mathbb{T}$, the limit

$$\lim_{i\to\infty} T_{M,N_i}(\alpha)$$

exists. We observe next that s_M is a root of $\Phi \pmod{g_M}$, and hence $\Phi(g_M x + s_M)$ is divisible by g_M. Consequently, whenever M is large enough that $g_M\alpha \in \mathbb{F}_q[t]$, we have $T_{M,N}(\alpha) = 1$.

Combining the analyses of the above two cases, we discern that

$$\lim_{M\to\infty} \lim_{i\to\infty} T_{M,N_i}(\alpha) = \begin{cases} 0, & \text{when } \alpha \text{ is irrational,} \\ 1, & \text{when } \alpha \text{ is rational.} \end{cases}$$

Now let μ be a finite non-negative measure on $\mathbb{T}$. By applying the dominated convergence theorem twice, we see that

$$\lim_{M\to\infty}\lim_{i\to\infty}\int_{\mathbb{T}} T_{M,N_i}(\alpha)\,\mathrm{d}\mu(\alpha) = \int_{\mathbb{T}} \lim_{M\to\infty}\lim_{i\to\infty} T_{M,N_i}(\alpha)\,\mathrm{d}\mu(\alpha) = \sum_{\substack{\alpha\in\mathbb{T}\\ \alpha \text{ rational}}} \mu(\{\alpha\}),$$

whence

$$\lim_{M\to\infty}\lim_{i\to\infty}\int_{\mathbb{T}} T_{M,N_i}(\alpha)\,\mathrm{d}\mu(\alpha) \geq \mu(\{0\}). \tag{6.6}$$

Suppose next that $\widehat{\mu}$ vanishes on $\mathcal{H}$. We note that, on recalling the definition (6.3) of $\mathcal{H}$, the definition of $T_{M,N}$ implies that we have $\widehat{T_{M,N}}(h) \neq 0$ only if $h \in \mathcal{H}\cup\{0\}$. Therefore, we have

$$\left|\int_{\mathbb{T}} T_{M,N}(\alpha)\,\mathrm{d}\mu(\alpha)\right| = \left|\sum_{x\in\mathbb{F}_q[t]} \widehat{T_{M,N}}(x)\overline{\widehat{\mu}(x)}\right| = |\widehat{T_{M,N}}(0)\widehat{\mu}(0)| = |\widehat{T_{M,N}}(0)|\mu(\mathbb{T}).$$

On recalling (6.5), we find that

$$|\widehat{T_{M,N}}(0)| = \frac{1}{q^N}\mathrm{card}\{x\in\mathbb{G}_N\colon \Phi(g_M x + s_M) = 0\} \leq \frac{\deg(\Phi)}{q^N}.$$

By working harder, one can confirm that this upper bound $\deg(\Phi)/q^N$ may be replaced by $1/q^M$ whenever M is large enough in terms of the coefficients of $\Phi(u)$. Hence, we deduce that

$$\left|\int_{\mathbb{T}} T_{M,N}(\alpha)\,\mathrm{d}\mu(\alpha)\right| \leq \frac{\deg(\Phi)}{q^N}\mu(\mathbb{T}). \tag{6.7}$$

Combining the two inequalities (6.6) and (6.7), we find that $\mu(\{0\}) = 0$ for any finite non-negative measure μ on $\mathbb{T}$ with $\widehat{\mu}$ vanishing on $\mathcal{H}$. Therefore, we deduce from Theorem 6.5 that $\mathcal{H}$ is van der Corput. □

Proof of Theorem 6.4. Suppose that $q = p$ and $\Phi(u) = \sum_{r\in\mathcal{K}} a_r u^r \in \mathbb{F}_p[t,u]$. Let

$$\mathcal{H} = \{\Phi(x)\colon x\in\mathbb{F}_p[t]\}\setminus\{0\}.$$

Also, let $\mathcal{I}$ and $S_k(\Phi)$ ($k\in\mathcal{I}$) be defined as in (5.6) and (5.7), respectively. We have seen in (5.8) that

$$e(\alpha\Phi(x)) = e\biggl(\sum_{k\in\mathcal{I}} S_k(\alpha\Phi)x^k\biggr).$$

For any $M\in\mathbb{Z}^+$, let g_M be the product of all of the monic polynomials in $\mathbb{G}_M$. Then, when $\alpha\in\mathbb{T}$, we put

$$T_{M,N}(\alpha) = \frac{1}{p^N}\sum_{x\in\mathbb{G}_N} e(\alpha\Phi(g_M x)) = \frac{1}{p^N}\sum_{x\in\mathbb{G}_N} e\biggl(\sum_{k\in\mathcal{I}} S_k(\alpha\Phi)(g_M x)^k\biggr).$$

If we now define

$$\mathcal{Q} = \{\alpha\in\mathbb{T}\colon S_k(\alpha\Phi) \text{ is irrational for some } k\in\mathcal{I}\},$$

then we see from (5.9) that for any $\alpha\in\mathcal{Q}$, we have

$$\lim_{N\to\infty} T_{M,N}(\alpha) = 0.$$

On the other hand, when $\alpha \notin \mathcal{Q}$, then $S_k(\alpha\Phi)$ is rational for all $k \in \mathcal{I}$. Since the rational elements $\alpha \in \mathbb{T}$ are countable, the set of all polynomials of the form

$$\sum_{k\in\mathcal{I}} S_k(\alpha\Phi)y^k \quad (\alpha \notin \mathcal{Q})$$

is countable. It is worth noting at this point that the set $\mathbb{T} \setminus \mathcal{Q}$ itself need not be countable. Since $|T_{M,N}(\alpha)| \leq 1$, it follows via a diagonalization process that we can extract a subsequence $(N_i)_{i=1}^{\infty}$ of natural numbers having the property that, for any $M \in \mathbb{Z}^+$ and any $\alpha \notin \mathcal{Q}$, the limit

$$\lim_{i\to\infty} T_{M,N_i}(\alpha)$$

exists. Also, by following an argument similar to that applied in Case 2 of the proof of Theorem 6.3, we find that for M sufficiently large, one has $T_{M,N}(\alpha) = 1$ for any $\alpha \notin \mathcal{Q}$. It follows that

$$\lim_{M\to\infty}\lim_{i\to\infty} T_{M,N_i}(\alpha) = \begin{cases} 0, & \text{when } \alpha \in \mathcal{Q}, \\ 1, & \text{when } \alpha \notin \mathcal{Q}. \end{cases}$$

We may now argue as in the proof of Theorem 6.3, mutatis mutandis, to confirm that $\mu(\{0\}) = 0$ for any finite non-negative measure μ on $\mathbb{T}$ satisfying the property that $\widehat{\mu}$ vanishes on $\mathcal{H}$. Therefore, we deduce from Theorem 6.5 that $\mathcal{H}$ is van der Corput. □

7. Glasner sets in $\mathbb{F}_q[t]$

7.1. **Background and statement of results.** We first introduce some notation and nomenclature relevant for the discussion of Glasner sets in $\mathbb{F}_q[t]$. A subset $Y \subset \mathbb{R}/\mathbb{Z}$ is called ϵ-*dense* in $\mathbb{R}/\mathbb{Z}$ if it intersects every interval of length 2ϵ in $\mathbb{R}/\mathbb{Z}$. A *dilation* of Y is a set of the form $nY = \{ny\colon y \in Y\} \subset \mathbb{R}/\mathbb{Z}$ for some $n \in \mathbb{Z}$. In 1979, Glasner [13] proved that for any infinite subset Y of $\mathbb{R}/\mathbb{Z}$ and any $\epsilon > 0$, there exists $n \in \mathbb{Z}$ having the property that the dilation nY is ϵ-dense in $\mathbb{R}/\mathbb{Z}$. It transpires that the same conclusion can be obtained when one restricts n to be an element of a relatively sparse subset of the integers. Motivated by Glasner's theorem, we say that a set $\mathcal{H} \subset \mathbb{Z}$ is *Glasner* if for any infinite subset Y of $\mathbb{R}/\mathbb{Z}$ and any $\epsilon > 0$, there exists $n \in \mathcal{H}$ having the property that nY is ϵ-dense in $\mathbb{R}/\mathbb{Z}$. In their paper [2], Alon and Peres showed that the set of primes is Glasner. They also proved that if $\Phi(u) \in \mathbb{Z}[u]$ is a non-constant polynomial, then the set $\{\Phi(n)\colon n \in \mathbb{Z}\}$ is Glasner. By using harmonic analysis, Alon and Peres obtained quantitative versions of their results. Thus, for each of the above two Glasner sets $\mathcal{H}$ and any $\epsilon > 0$, there exists an ϵ-dense dilation nY of Y with $n \in \mathcal{H}$, provided that the cardinality $|Y|$ of Y is sufficiently large in terms of ϵ and $\mathcal{H}$. The method and results of Alon and Peres were generalized to multi-dimensional tori in [17] and [7].

One can define an analog of the notion of a Glasner set in $\mathbb{F}_q[t]$. For $M \in \mathbb{Z}^+$, a subset $Y \subset \mathbb{T}$ is called q^{-M}-*dense* in $\mathbb{T}$ if it intersects every cylinder set $\mathcal{C}$ of radius q^{-M} in $\mathbb{T}$. We call a set $\mathcal{H} \subset \mathbb{F}_q[t]$ *Glasner* if for any infinite subset $Y \subset \mathbb{T}$ and any $M \in \mathbb{Z}^+$, there exists $x \in \mathcal{H}$ having the property that the dilation xY is q^{-M}-dense in $\mathbb{T}$. In view of the result of Alon and Peres, one may ask if the set of values of a polynomial with coefficients in $\mathbb{F}_q[t]$ is Glasner. However, the following examples show that an exact analog of the result of Alon and Peres is *not* true in general.

Example 7.1. Let Y be the set of all $\alpha \in \mathbb{T}$ with $T(\alpha) = 0$, where T is the map defined in (1.1). Then Y is infinite (and indeed uncountable). We have seen in Example 1.2 that for any $x \in \mathbb{F}_q[t]$ and $\alpha \in Y$, we have $\mathrm{res}(x^p\alpha) = 0$. This shows that the set $\{x^p \colon x \in \mathbb{F}_q[t]\}$ is not Glasner, since for any $x \in \mathbb{F}_q[t]$, the set x^pY fails to be q^{-1}-dense.

Example 7.2. Let us assume that $q = p$. Let Y be the set of all $\alpha \in \mathbb{T}$ with $T(\alpha)+\alpha = 0$. One sees again that Y is infinite (and indeed uncountable). Then for any $x \in \mathbb{F}_q[t]$, we have $\mathrm{res}((x^p + x)\alpha) = \mathrm{res}((T(\alpha) + \alpha)x) = 0$. This shows that the set $\{x^p + x \colon x \in \mathbb{F}_q[t]\}$ is not Glasner, since for any $x \in \mathbb{F}_q[t]$, the set $(x^p + x)Y$ fails to be q^{-1}-dense.

One could formulate a conjecture similar to Conjecture 1.3 asserting that Examples 7.1 and 7.2 encapsulate all the obstructions preventing a polynomial sequence in $\mathbb{F}_q[t]$ from being Glasner. We have some preliminary ideas that might establish such a conjecture, and this is a subject to which we intend to return on a future occasion. For now we note that such a conjecture would follow from Conjecture 1.3. Moreover, partial progress is made possible by making use of Theorem 1.4. Here, once again, we recall the definition (2.4) of the set of exponents $\mathcal{K}^*$.

Theorem 7.3. *Let $\mathcal{K}$ be a finite set of positive integers, suppose that $a_r \in \mathbb{F}_q[t]$ for $r \in \mathcal{K} \cup \{0\}$, and define*

$$\Phi(u) = \sum_{r \in \mathcal{K} \cup \{0\}} a_r u^r.$$

Suppose further that $a_k \neq 0$ for some $k \in \mathcal{K}^*$ with $k \geq 1$. Then the set $\{\Phi(x) \colon x \in \mathbb{F}_q[t]\}$ is Glasner.

By adapting the harmonic-analytic approach of Alon and Peres described in [2], we prove the following quantitative version of Theorem 1.11 analogous to the bound of Alon and Peres obtained in [2, Theorem 6.3].

Theorem 7.4. *Let $\mathcal{K}$ be a finite set of positive integers, suppose that $a_r \in \mathbb{F}_q[t]$ for $r \in \mathcal{K} \cup \{0\}$, and define*

$$\Phi(u) = \sum_{r \in \mathcal{K} \cup \{0\}} a_r u^r.$$

Suppose further that $a_k \neq 0$ for some $k \in \mathcal{K}^*$ with $k \geq 1$. Then there exists a positive constant C, depending on Φ, such that whenever $M > 0$ and $|Y| \geq q^{CM}$, there is a dilation of the form $\Phi(x)Y$ of Y that is q^{-M}-dense.

We remark that, as a direct consequence of Theorem 1.11, the set of values of Φ is Glasner whenever $\deg \Phi \geq 1$ and $(\deg \Phi, p) = 1$. Also, in view of Proposition 5.2, the condition $a_k \neq 0$ for some $k \in \mathcal{K}^*$ can be relaxed to the constraint that $a_k \neq 0$ for some $k \in \widetilde{\mathcal{K}}$, where $\widetilde{\mathcal{K}}$ is defined as in (2.5).

7.2. **Proof of Theorem 7.4.** We first derive the following cheap consequence of Theorem 4.1. It is analogous to Hua's classical bound on complete exponential sums with polynomial argument over the integers, a version of which could certainly be derived in the setting of $\mathbb{F}_q[t]$. Whilst the latter would deliver stronger conclusions than those we obtain below, the extra effort involved has no impact on the application that we have in mind.

Lemma 7.5. *Let $\mathcal{K}$ be a finite set of positive integers, suppose that $a_r \in \mathbb{F}_q[t]$ for $r \in \mathcal{K} \cup \{0\}$, and define*

$$\Phi(u) = \sum_{r \in \mathcal{K} \cup \{0\}} a_r u^r.$$

Suppose further that $a_k \neq 0$ for some $k \in \mathcal{K}^*$ with $k \geq 1$. Then there exists a constant $C_k > 1$, depending only on k, $\mathcal{K}$ and q, such that for any monic $g \in \mathbb{F}_q[t]$ and any $\epsilon > 0$, we have

$$\Big| \sum_{x \in \mathbb{G}_{\operatorname{ord} g}} e\Big(\frac{\Phi(x)}{g}\Big) \Big| \ll_{\mathcal{K},\epsilon,q} |(g, a_k)|^{1/C_k} |g|^{1-1/C_k+\epsilon}. \tag{7.1}$$

Proof. There is no loss of generality in supposing that $a_r \neq 0$ for all $r \in \mathcal{K}$. Suppose first that $a_k \neq 0$ for no $k \in \mathcal{K}^*$ with $k > 1$, and yet $1 \in \mathcal{K}^*$ and $a_1 \neq 0$. Then whenever $k \in \mathcal{K}$ and $p \nmid k$, we must have $k = 1$. If $lp^v \in \mathcal{K}$ for some $v \geq 1$ and $l \in \mathbb{Z}^+$ with $(l, p) = 1$, meanwhile, then $p^v \in \mathcal{S}(\mathcal{K})$, and hence $1 \notin \mathcal{K}^*$. We are therefore forced to conclude in this scenario that $\mathcal{K} = \{1\}$ and hence $\Phi(u) = a_1 u$ with $a_1 \neq 0$. The desired conclusion (7.1) follows by orthogonality in this trivial situation.

We may assume henceforth that $a_k \neq 0$ for some $k \in \mathcal{K}^*$ with $k > 1$. We fix the positive constants c_k and C_k, depending at most on k, $\mathcal{K}$ and q, in accordance with the conclusion of Theorem 4.1. Write $N = \operatorname{ord} g$ and $M = \operatorname{ord}(g, a_k)$, and put

$$\eta = \min\{c_k N, (1/C_k - \epsilon)N - M/C_k\}. \tag{7.2}$$

On observing that the bound (7.1) is trivial when $\eta \leq 0$, we see that there is no loss of generality in assuming henceforth that $\eta > 0$. We may also suppose that N is sufficiently large in terms of $\mathcal{K}$, ϵ and q. Suppose, by way of deriving a contradiction, that

$$\Big| \sum_{x \in \mathbb{G}_N} e\Big(\frac{\Phi(x)}{g}\Big) \Big| \geq q^{N-\eta}.$$

Then we infer from Theorem 4.1 that there exist $b \in \mathbb{F}_q[t]$ and monic $h \in \mathbb{F}_q[t]$ such that

$$\operatorname{ord}\left(h\frac{a_k}{g} - b\right) < -kN + \epsilon N + C_k\eta \quad \text{and} \quad \operatorname{ord} h \leq \epsilon N + C_k\eta. \tag{7.3}$$

We see from (7.2) that $M + C_k\eta \leq (1 - C_k\epsilon)N$. It therefore follows from (7.3) that

$$\operatorname{ord}(g, a_k h) \leq M + \operatorname{ord} h \leq M + \epsilon N + C_k\eta \leq (1 + \epsilon - C_k\epsilon)N < N.$$

Since $\operatorname{ord} g = N$, we deduce that g does not divide $(g, a_k h)$. Consequently, the fraction ha_k/g has a reduced form with denominator $g/(g, a_k h)$ having order at least 1. Thus, we have

$$\operatorname{ord}\left(h\frac{a_k}{g} - b\right) \geq \operatorname{ord}\left(\frac{1}{g/(g, a_k h)}\right) = \operatorname{ord}(g, a_k h) - \operatorname{ord} g \geq M - N. \tag{7.4}$$

Combining (7.3) and (7.4), we obtain the bound

$$M - N \leq -kN + \epsilon N + C_k\eta \leq -kN + \epsilon N + (1 - C_k\epsilon)N - M.$$

Since $k > 1$, we arrive at a contradiction. We are therefore forced to conclude that $\eta \leq 0$, a scenario in which the conclusion of the lemma follows, as we have already observed. □

As we have already noted, one may prove the bound (7.1) by more classical methods. Thus, with additional effort it would be possible to establish a version of Lemma 7.5 with $C_k = \deg(\Phi)$. We also need an analog of [2, Proposition 1.3], the statement of which requires that we introduce some additional notation. Consider a set $Y = \{y_1, \dots, y_\kappa\} \subset \mathbb{T}$. For each $g \in \mathbb{F}_q[t]\backslash\{0\}$, we denote by $h_g = h_g(Y)$ the number of pairs (i, j) with $1 \le i, j \le \kappa$ and $i \ne j$ satisfying $g(y_i - y_j) \in \mathbb{F}_q[t]$. Finally, we define $H_L = H_L(Y)$ by putting

$$H_L(Y) = \sum_{g \in \mathbb{G}_L \setminus \{0\}} h_g(Y).$$

Lemma 7.6. *Let $Y = \{y_1, \dots, y_\kappa\}$ be a set of κ distinct elements in $\mathbb{T}$. Then for each non-negative integer L, one has $H_L(Y) \le \kappa q^{2L}$.*

Proof. For each index i with $1 \le i \le \kappa$ and $g \in \mathbb{G}_L \setminus \{0\}$, the number of indices j for which $g(y_i - y_j) \in \mathbb{F}_q[t]$ is at most $|g| \le q^L$. Thus, we deduce that

$$H_L(Y) \le \sum_{1 \le i \le \kappa} \sum_{g \in \mathbb{G}_L \setminus \{0\}} q^L \le \kappa q^{2L},$$

and the proof of the lemma is complete. □

Proof of Theorem 7.4. We prove Theorem 7.4 by establishing the contrapositive. Suppose then that a set of κ distinct elements $Y = \{y_1, \dots, y_\kappa\} \subset \mathbb{T}$ has the property that $\Phi(x)Y$ is not q^{-M}-dense for any $x \in \mathbb{F}_q[t]$. We seek to derive an upper bound for κ of the shape $\kappa < q^{CM}$, with C a suitable positive constant depending on Φ.

Consider any element $x \in \mathbb{F}_q[t]$. We may suppose that $\Phi(x)Y$ is not q^{-M}-dense in $\mathbb{T}$, and hence there exists $\xi_x \in \mathbb{T}$ having the property that all elements of $\Phi(x)Y$ lie outside of the cylinder set $\{\xi \in \mathbb{T} \colon |\xi - \xi_x| < q^{-M}\}$. Thus, for all $1 \le i \le \kappa$, we have

$$\operatorname{ord}\{\Phi(x)y_i - \xi_x\} \ge -M.$$

In view of (2.1), we see that for each $x \in \mathbb{F}_q[t]$ and index i, one has

$$\sum_{z \in \mathbb{G}_M} e\left(z\left(\Phi(x)y_i - \xi_x\right)\right) = 0.$$

Consequently, isolating the term $z = 0$ in each sum, we deduce that for each positive integer N one has the relation

$$\sum_{x \in \mathbb{G}_N} \sum_{i=1}^{\kappa} \sum_{z \in \mathbb{G}_M \setminus \{0\}} e\left(z\left(\Phi(x)y_i - \xi_x\right)\right) = -\kappa q^N.$$

Interchanging the innermost summations and applying Cauchy's inequality, we therefore obtain the relation

$$\begin{aligned}\kappa^2 q^{2N} &\le q^{N+M} \sum_{x \in \mathbb{G}_N} \sum_{z \in \mathbb{G}_M \setminus \{0\}} \left| \sum_{i=1}^{\kappa} e\left(z\left(\Phi(x)y_i - \xi_x\right)\right)\right|^2 \\ &= q^{N+M} \sum_{x \in \mathbb{G}_N} \sum_{z \in \mathbb{G}_M \setminus \{0\}} \sum_{i=1}^{\kappa} \sum_{j=1}^{\kappa} e\left(z\Phi(x)(y_i - y_j)\right).\end{aligned}$$

Therefore, again interchanging orders of summation, we find that

$$\begin{aligned}\kappa^2 &\le q^M \sum_{z\in\mathbb{G}_M\setminus\{0\}} \sum_{i=1}^{\kappa}\sum_{j=1}^{\kappa} \frac{1}{q^N} \sum_{x\in\mathbb{G}_N} e\left(z\Phi(x)(y_i-y_j)\right)\\ &\le q^{2M} \max_{z\in\mathbb{G}_M\setminus\{0\}} \sum_{i=1}^{\kappa}\sum_{j=1}^{\kappa} \Theta(z;y_i-y_j), \end{aligned} \tag{7.5}$$

where

$$\Theta(z;u) = \limsup_{N\to\infty}\left|\frac{1}{q^N}\sum_{x\in\mathbb{G}_N} e\left(z\Phi(x)u\right)\right|. \tag{7.6}$$

We now analyse the limit $\Theta(z;y_i-y_j)$ when $z\in\mathbb{G}_M\setminus\{0\}$, with the result depending on whether or not y_i-y_j is rational.

Case 1. Suppose that $i=j$. Then we find from (7.6) that $\Theta(z;y_i-y_j)=\Theta(z;0)=1$.

Case 2. Suppose that y_i-y_j is irrational. In this scenario, when $z\in\mathbb{G}_M\setminus\{0\}$, we find that $z(y_i-y_j)$ is also irrational, and hence it follows from Theorem 1.4 that $\Theta(z;y_i-y_j)=0$.

Case 3. Suppose that y_i-y_j is a non-zero rational. In these circumstances, we write $y_i-y_j=a/g$ as a reduced fraction with $a\in\mathbb{F}_q[t]$ and monic $g\in\mathbb{F}_q[t]$. Given $z\in\mathbb{G}_M\setminus\{0\}$, we may in turn write $z(y_i-y_j)=a'/g'$ as a reduced fraction with $g'=g/(z,g)$ and $a'=az/(z,g)$. In particular, therefore, we have $|g'|\ge|g|/q^M$. We now recall (7.6) and appeal to Lemma 7.5. Thus, there exists a constant $C_k>1$, depending only on k, $\mathcal{K}$ and q, such that

$$\Theta(z;y_i-y_j)=\frac{1}{|g'|}\left|\sum_{x\in\mathbb{G}_{\operatorname{ord} g'}} e\left(\frac{a'\Phi(x)}{g'}\right)\right| \ll_{\mathcal{K}} |g'|^{-1/(2C_k)}|(g',a'a_k)|^{1/C_k}.$$

On noting that $(g',a')=1$, we deduce that

$$\Theta(z;y_i-y_j)\ll_{\mathcal{K}} |g'|^{-1/(2C_k)}|a_k|^{1/C_k}\ll_{\Phi}|g|^{-1/(2C_k)}q^M. \tag{7.7}$$

For each monic $g\in\mathbb{F}_q[t]\setminus\{0\}$, denote by $\widetilde{h}_g$ the number of pairs (i,j) with $1\le i,j\le\kappa$ and $i\ne j$ satisfying the condition that y_i-y_j may be written as a reduced fraction with denominator g. Then it follows from (7.5) via (7.7) and the above analysis dividing into three cases that we have the estimate

$$\kappa^2\ll_{\Phi}\kappa q^{2M}+q^{3M}\sum_{\substack{g\in\mathbb{F}_q[t]\\ g\text{ monic}}}|g|^{-1/(2C_k)}\widetilde{h}_g. \tag{7.8}$$

Next we estimate the right hand side of (7.8) using Lemma 7.6. For any $L\in\mathbb{Z}^+$, let

$$\widetilde{H}_L=\sum_{\substack{g\in\mathbb{G}_L\\ g\text{ monic}}}\widetilde{h}_g.$$

On noting that $\widetilde{H}_1 = 0$, we find by partial summation that

$$\sum_{\substack{g\in\mathbb{F}_q[t]\\ g \text{ monic}}} |g|^{-1/(2C_k)}\widetilde{h}_g = \sum_{L=1}^{\infty} q^{-L/(2C_k)}\big(\widetilde{H}_{L+1} - \widetilde{H}_L\big)$$

$$= \sum_{L=2}^{\infty} \widetilde{H}_L\big(q^{-(L-1)/(2C_k)} - q^{-L/(2C_k)}\big). \tag{7.9}$$

For any non-negative integer L, we have the trivial estimate $\widetilde{H}_L \le \kappa^2$. Meanwhile, as a consequence of Lemma 7.6, we have $\widetilde{H}_L \le H_L \le \kappa q^{2L}$. Write $L_0 = \big\lfloor (\log_q \kappa)/2 \big\rfloor$. Then

$$\sum_{L=2}^{L_0} \widetilde{H}_L\big(q^{-(L-1)/(2C_k)} - q^{-L/(2C_k)}\big) \le \kappa \sum_{L=2}^{L_0} q^{2L}\big(q^{-(L-1)/(2C_k)} - q^{-L/(2C_k)}\big)$$

$$\le 2\kappa q^{1+L_0(2-1/(2C_k))}$$

and

$$\sum_{L=L_0+1}^{\infty} \widetilde{H}_L\big(q^{-(L-1)/(2C_k)} - q^{-L/(2C_k)}\big) \le \kappa^2 \sum_{L=L_0+1}^{\infty} \big(q^{-(L-1)/(2C_k)} - q^{-L/(2C_k)}\big)$$

$$\le \kappa^2 q^{-L_0/(2C_k)}.$$

On recalling that $L_0 = \big\lfloor (\log_q \kappa)/2 \big\rfloor$ and substituting these bounds into (7.9), we see that

$$\sum_{\substack{g\in\mathbb{F}_q[t]\\ g \text{ monic}}} |g|^{-1/(2C_k)}\widetilde{h}_g \le 3q\kappa^{2-1/(4C_k)}.$$

Equipped with this estimate, the relation (7.8) now yields the bound

$$\kappa^2 \ll_\Phi \kappa q^{2M} + q^{3M+1}\kappa^{2-1/(4C_k)},$$

and thus $|Y| = \kappa \ll_\Phi q^{4C_k(3M+1)}$. In view of our opening discussion, this completes the proof of Theorem 7.4. □

References

[1] E. Ackelsberg and V. Bergelson, *Asymptotic total ergodicity for actions of $\mathbb{F}[t]$ and Furstenberg-Sárközy-type theorems over finite fields and rings*, arXiv:2303.00100.

[2] N. Alon and Y. Peres, *Uniform dilations*, Geom. Funct. Anal. 2 (1992), no. 1, 1–28.

[3] V. Bergelson and A. Leibman, *A Weyl-type equidistribution theorem in finite characteristic*, Adv. Math. 289 (2016), 928–950.

[4] V. Bergelson, A. Leibman and R. McCutcheon, *Polynomial Szemerédi theorem for countable modules over integral domains and finite fields*, J. Anal. Math. 95 (2005), 243–296.

[5] P.-Y. Bienvenu, T. H. Lê and G. Wathodkar, *A generalization of Sárközy's theorem in function fields*, preprint.

[6] J. Bourgain, *Ruzsa's problem on sets of recurrence*, Israel J. Math. 59 (1987), no. 2, 150–166.

[7] K. Bulinski and A. Fish, *Glasner property for unipotently generated group actions on tori*, Israel J. Math. (2022), in press.

[8] L. Carlitz, *Diophantine approximation in fields of characteristic p*, Trans. Amer. Math. Soc. 72 (1952), 187–208.

[9] E. Croot, V. F. Lev and P. P. Pach, *Progression-free sets in $\mathbb{Z}_4^n$ are exponentially small*, Ann. of Math. (2) 185 (2017), no. 1, 331–337.
[10] A. Dijksma, *Uniform distribution of polynomials over $GF\{q, x\}$ in $GF[q, x]$. II*, Indag. Math. 32 (1970), 187–195.
[11] H. Furstenberg, *Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions*, J. Anal. Math. 31 (1977), 204–256.
[12] Z. Ge, T. H. Lê and Y.-R. Liu, *A Weyl-type inequality for irreducible elements in function fields*, preprint.
[13] S. Glasner, *Almost periodic sets and measures on the torus*, Israel J. Math. 32 (1979), no. 2-3, 161–172.
[14] B. Green, *Sárközy's theorem in function fields*, Q. J. Math. 68 (2017), no. 1, 237–242.
[15] C.-N. Hsu, *A large sieve inequality for rational function fields*, J. Number Theory 58 (1996), no. 2, 267–287.
[16] T. Kamae and M. Mendès France, *van der Corput's difference theorem*, Israel J. Math. 31 (1978), no. 3-4, 335–342.
[17] M. Kelly and T. H. Lê, *Uniform dilations in higher dimensions*, J. Lond. Math. Soc. (2) 88 (2013), no. 3, 925–940.
[18] R. M. Kubota, *Waring's problem for $\mathbb{F}_q[x]$*, Dissertationes Math. (Rozprawy Mat.) 117 (1974), 60pp.
[19] L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, John Wiley & Sons Inc. (1974), reprinted by Dover Publishing, 2006.
[20] W. Kuo, Y.-R. Liu and X. Zhao, *Multidimensional Vinogradov-type estimates in function fields*, Canad. J. Math. 66 (2014), no. 4, 844–873.
[21] T. H. Lê, *Problems and results on intersective sets*, Combinatorial and additive number theory-CANT 2011 and 2012, 115–128, Springer Proc. Math. Stat., 101, Springer, New York, 2014.
[22] T. H. Lê, *Topics in arithmetic combinatorics in function fields*, PhD Thesis, UCLA, 2010.
[23] T. H. Lê, *Green-Tao theorem in function fields*, Acta Arith. **147** (2011), no. 2, 129–152.
[24] T. H. Lê and Y.-R Liu, *On sets of polynomials whose difference set contains no squares*, Acta Arith. 161 (2013), no. 2, 127–143.
[25] T. H Lê and C. V. Spencer, *Difference sets and the irreducibles in function fields*, Bull. Lond. Math. Soc. 43 (2011), no. 2, 347–358.
[26] A. Li and L. Sauermann, *Sárközy's theorem in various finite field settings*, SIAM J. Discrete Math. **38** (2024), no. 2, 1409–1416.
[27] G. Li, *The Furstenberg-Sárközy theorem for intersective polynomials in function fields*, Finite Fields Appl. 58 (2019), 1–31.
[28] Y.-R. Liu and T. D. Wooley, *Waring's problem in function fields*, J. Reine Angew. Math. 638 (2010), 1–67.
[29] Y.-R. Liu and T. D. Wooley, *Vinogradov's mean value theorem in function fields*, in preparation.
[30] A. Sárközy, *On difference sets of sequences of integers, I*, Acta Math. Acad. Sci. Hungar. 31 (1978), no. 1-2, 125–149.
[31] A. Sárközy, *On difference sets of sequences of integers, III*, Acta Math. Acad. Sci. Hungar. 31 (1978), no. 3-4, 355–386.
[32] W. M. Schmidt, *On continued fractions and Diophantine approximation in power series fields*, Acta Arith. 95 (2000), no. 2, 139–166.
[33] J. G. van der Corput, *Diophantische Ungleichungen. I. Zur Gleichverteilung Modulo Eins*, Acta Math. 56 (1931), 373–456.
[34] R. C. Vaughan, *The Hardy-Littlewood method*, 2nd edition, Cambridge University Press, Cambridge, 1997.
[35] H. Weyl, *Über die Gleichverteilung von Zahlen mod. Eins*, Math. Ann. 77 (1916), 313–352.
[36] T. D. Wooley, *On Diophantine inequalities: Freeman's asymptotic formulae*, Proceedings of the session in analytic number theory and Diophantine equations (Bonn, January – June, 2002), Bonn 2003, Edited by D. R. Heath-Brown and B. Z. Moroz, Bonner Mathematische Schriften, Nr. 360, Article 30, 32pp.
[37] S. Yamagishi, *The asymptotic formula for Waring's problem in function fields*, Int. Math. Res. Not. IMRN 2016 (2016), no. 23, 7137–7178.

[38] S. Yamagishi, *Diophantine approximation of polynomials over $\mathbb{F}_q[t]$ satisfying a divisibility condition*, Int. J. Number Theory 12 (2016), no. 5, 1371–1390.

T. H. Lê, Department of Mathematics, University of Mississippi, 305 Hume Hall, University, MS 38677, USA

Email address: leth@olemiss.edu

Y.-R. Liu, Department of Pure Mathematics, University of Waterloo, 200 University Avenue West, Waterloo, ON, N2L 3G1, Canada

Email address: yrliu@uwaterloo.ca

T. D. Wooley, Department of Mathematics, Purdue University, 150 N. University Street, West Lafayette, IN 47907, USA

Email address: twooley@purdue.edu