EQUIDISTRIBUTION OF POLYNOMIAL SEQUENCES IN FUNCTION FIELDS, WITH APPLICATIONS

THÁI HOÀNG LÊ AND YU-RU LIU

Abstract. We prove a function field analog of Weyl's classical theorem on equidistribution of polynomial sequences. Our result covers the case when 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 [27]. We recall that a sequence $(a_n)_{n=1}^{\infty}$ of real numbers is said to be *equidistributed* $(\mathrm{mod}\, 1)$ if for any interval $[\alpha, \beta] \subset [0,1)$, we have

$$\lim_{N\to\infty} \frac{\#\{a_n : 1 \le n \le N \text{ and } \{a_n\} \in [\alpha,\beta]\}}{N} = \beta - \alpha,$$

where $\{a\}$ is the fractional part of a real number a. *Weyl's criterion* says that the sequence $(a_n)_{n=1}^{\infty}$ is equidistributed $(\mathrm{mod}\, 1)$ if and only if for any integer $m \neq 0$, we have

$$\lim_{N\to\infty} \frac{1}{N} \left| \sum_{n=1}^{N} e(m a_n) \right| = 0,$$

where $e(x) = e^{2\pi i x}$.

Let $f(u) = \sum_{r=0}^{k} \alpha_r u^r$ be a polynomial with coefficients in $\mathbb{R}$ and degree k. Weyl made the important observation that by squaring the sum $\left|\sum_{n=1}^{N} e(f(n))\right|$, 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's differencing*. If one continues the differencing process, then the polynomial in question becomes linear after $(k-1)$ steps. Using this observation, Weyl [27] proved that the sequence $(f(n))_{n=1}^{\infty}$ is equidistributed $(\mathrm{mod}\, 1)$ if and only if at least one of the coefficients $\alpha_1, \ldots, \alpha_k$ of f is irrational. The proof of this result was later simplified with the help of *van der Corput's*

Date: March 24, 2014.

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

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

Work on this project began when the first author was visiting the University of Waterloo in June 2013. He would like to thank the Pure Mathematics department for its hospitality. The research of the second author is supported in part by an NSERC discovery grant.

difference theorem [23], which says that if for any $h \in \mathbb{Z}^+$, the sequence $(a_{n+h} - a_n)_{n=1}^{\infty}$ is equidistributed $(\bmod 1)$, then the sequence $(a_n)_{n=1}^{\infty}$ is also equidistributed $(\bmod 1)$. 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.

Let $\mathbb{F}_q$ be the finite field of q elements whose characteristic is p. 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 $\mathbb{F}_q[t]$. For $f/g \in \mathbb{K}$, 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 as $\alpha = \sum_{i=-\infty}^{n} a_i t^i$ for some $n \in \mathbb{Z}$ and $a_i \in \mathbb{F}_q$ $(i \leq n)$. Therefore, $\mathbb{F}_q[t], \mathbb{K}, \mathbb{K}_\infty$ play the roles of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ respectively. Let

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

This is the analog of the unit interval $[0, 1)$ and is a compact group. 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

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

satisfies $\lambda(\mathcal{C}_I) = q^{-M}$. Thus we refer the set 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 plays the role of intervals.

For $\alpha = \sum_{i=-\infty}^{n} a_i t^i \in \mathbb{K}_\infty$, if $a_n \neq 0$, we define $\operatorname{ord} \alpha = n$. Therefore, $|\alpha| = q^{\operatorname{ord} \alpha}$. We say α is *rational* if $\alpha \in \mathbb{K}$ and *irrational* if $\alpha \notin \mathbb{K}$. We define $\{\alpha\} = \sum_{i=-\infty}^{-1} a_i t^i \in \mathbb{T}$ to be the *fractional part* of α, and we refer to a_{-1} as the *residue* of α, denoted by $\operatorname{res} \alpha$. We now define the exponential function on $\mathbb{K}_\infty$. Let $\operatorname{tr} : \mathbb{F}_q \to \mathbb{F}_p$ denote the familiar trace map. There is a non-trivial additive character $e_q : \mathbb{F}_q \to \mathbb{C}^\times$ defined for each $a \in \mathbb{F}_q$ by taking $e_q(a) = e(\operatorname{tr}(a)/p)$. This character induces a map $e : \mathbb{K}_\infty \to \mathbb{C}^\times$ 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 $\mathbb{F}_q[t]$ whose degree are less than N. The following notion of equidistribution was first introduced by Carlitz in [4] (see also [12, 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 the sequence $(a_x)_{x \in \mathbb{F}_q[t]}$ is *equidistributed* in $\mathbb{T}$ if for any cylinder set $\mathcal{C} \subset \mathbb{T}$, we have

$$\lim_{N \to \infty} \frac{\# \{a_x : x \in \mathbb{G}_N \text{ and } \{a_x\} \in \mathcal{C}\}}{q^N} = \lambda(\mathcal{C}).$$

Since one can prove the exact analogs of Weyl's criterion and van der Corput's difference theorem in function fields, one expects to establish a $\mathbb{F}_q[t]$ 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 $\mathbb{K}_\infty$ and degree k. All earlier works on equidistribution in $\mathbb{T}$ have been restricted to the case when $k < p$. Under this condition, Carlitz [4] proved an exact analog of Weyl's equidistribution theorem for the sequence $(f(x))_{x\in\mathbb{F}_q[t]}$. Dijksma [5] also established the same result for another stronger notion of equidistribution, subject to the same constraint $k < p$. In Carlitz's and Dijksma's work, the use of Weyl's differencing produces a factor of $k!$. When $k \geq p$, the factor is 0, and hence the differencing method becomes ineffective in producing a desirable result. Actually, the following example, already known to Carlitz [4, (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 1.1. For $\alpha = \sum_{i=-\infty}^{n} a_i t^i \in \mathbb{K}_\infty$, we define

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

Then T is a linear map from $\mathbb{K}_\infty$ to $\mathbb{T}$ (this map will be used in Section 5). For any $x = \sum_{i=0}^{m} x_i t^i \in \mathbb{F}_q[t]$, the coefficient of t^{-1} in αx^p is

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

which is 0 if $T(\alpha) = 0$. Therefore, the sequence $(\alpha x^p)_{x\in\mathbb{F}_q[t]}$ is not equidistributed in $\mathbb{T}$ if $T(\alpha) = 0$. By a countability argument, we can find an irrational element $\alpha \in \mathbb{K}_\infty$ with $T(\alpha) = 0$.

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 1.1, such a description may be complicated and not easy to state in arithmetic terms such as irrationality. In particular, equidistribution could fail if the degree of $f(u)$ is divisible by p. Furthermore, for a polynomial like $(\alpha x^p + \beta x)$, it is impossible to say about equidistribution if one has information on α or β alone, since the terms x^p and x "interfere" with each other, as the map $x \mapsto x^p$ is linear (see also [4, (6.9)]). However, one may suspect that the only pathologies that prevent equidistribution are the ones described above (i.e., exponents divisible by p and intefering exponents). Thus one can make the following conjecture, which is the best possible as far as a single coefficient is concerned.

Conjecture 1. *Let $f(u) = \sum_{r\in\mathcal{K}\cup\{0\}} \alpha_r u^r$ be a polynomial supported on a set $\mathcal{K} \subset \mathbb{Z}^+$ with coefficients in $\mathbb{K}_\infty$. Suppose that α_k is irrational for some $k \in \mathcal{K}$ satisfying $p \nmid k$ and $p^v k \notin \mathcal{K}$ 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 $\mathcal{K}$, we define the *shadow* of $\mathcal{K}$, $\mathcal{S}(\mathcal{K})$, to be

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

Below is our equidistribution result, which has no restriction on the degree of $f(u)$.

Theorem 2. *Let $f(u) = \sum_{r\in\mathcal{K}\cup\{0\}} \alpha_r u^r$ be a polynomial supported on a set $\mathcal{K} \subset \mathbb{Z}^+$ with coefficients in $\mathbb{K}_\infty$. Suppose that α_k is irrational 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 the sequence $(f(x))_{x\in\mathbb{F}_q[t]}$ is equidistributed in $\mathbb{T}$.*

Example 1.2. If $p \nmid k$ and α is irrational, then Theorem 2 implies that the sequence $(\alpha x^k)_{x\in\mathbb{F}_q[t]}$ 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 r with $p \nmid r$ and $r > k/p$. As a direct consequence of Theorem 2, the sequence $(f(x))_{x\in\mathbb{F}_q[t]}$ is equidistributed in $\mathbb{T}$.

Example 1.3. Let $p > 3$ and $\alpha, \beta, \gamma \in \mathbb{K}_\infty$ with β irrational. Theorem 2 does not imply directly the equidistribution of the sequence $(\alpha x + \beta x^3 + \gamma x^{3p+1})_{x\in\mathbb{F}_q[t]}$ as $3p \in \mathcal{S}(\mathcal{K})$. However, we will prove a more general form of Theorem 2 (Proposition 18), from which we can conclude that the above sequence is equidistributed in $\mathbb{T}$. In contrast, we are not able to confirm if the sequence $(\beta x^3 + \gamma x^{4p})_{x\in\mathbb{F}_q[t]}$ is equidistributed in $\mathbb{T}$, though Conjecture 1 suggests that it is the case.

Our proof of Theorem 2 is based on a "minor arc estimate" of the sum $|\sum_{x\in\mathbb{G}_N} e(f(x))|$. By combining the large sieve inequality with a generalized Vinogradov's mean value theorem in $\mathbb{F}_q[t]$, we obtain a Weyl-type estimate, which avoids the problematic use of Weyl's differencing. This approach allows us to surmount the barriers that previously obstructed viable conclusions when the degree of $f(u)$ exceeds or equals to p. The idea of using minor arc estimates to prove equidistribution was already known to Vinogradov, when he established the equidistribution of the sequence $(p\alpha)_{p \text{ prime}}$ for any irrational number $\alpha \in \mathbb{R}$ (see [26, Chapter XI] or [6, Chapter 9]). In his proof, information on the major arcs is also required. In contrast, by relying on properties of continued fractions, we obtain our result exclusively from a minor arc estimate.

The assumption $p^v k \notin \mathcal{S}(\mathcal{K})$ in Theorems 2 comes from the use of Weyl's shift in our minor arc estimate. Such a "shift" produces terms whose degrees are elements not only in $\mathcal{K}$, but also in $\mathcal{S}(\mathcal{K})$ (see (6) in Section 3). Therefore, we need to consider a mean value estimate whose indices are elements of $\mathcal{S}(\mathcal{K})$. Such an "extension of indices" is a common theme in the study of Diophantine problems. For example, to establish an asymptotic formula of Waring's problem, one relates an equation of kth powers to Vinogradov's system of equations whose degrees range from 1 to k (see [24, Section 5.3] for more details). The extension process produces an extra k factor in the bound $\widetilde{G}(k)$ (for definition, see [25, Section 10]) of Waring's problem, and in our case, it requires the stronger assumption $p^v k \notin \mathcal{S}(\mathcal{K})$, instead of $p^v k \notin \mathcal{K}$. Although we are unable to prove Conjecture 1, we can confirm it in the special case when $q = p$, which follows from a more general form of Theorem 2. We defer to Section 5 for the precise statements of the results (Proposition 18 and Corollary 19).

Our equidistribution result is virtually applicable in any situation that involves equidistribution and polynomials in $\mathbb{T}$. In particular, we will study some special sets in $\mathbb{F}_q[t]$ which are closely related to equidistribution and at present less well understood than their integer counterparts. These are van der Corput, intersective and Glasner sets. In particular, we will prove the following result.

Theorem 3. *Let $\Phi(u) = \sum_{r\in\mathcal{K}\cup\{0\}} a_r u^r$ be a polynomial supported on a set $\mathcal{K} \subset \mathbb{Z}^+$ with coefficients in $\mathbb{F}_q[t]$. Suppose that $\Phi(u)$ has a root (mod 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 of $\mathbb{F}_q[t]$, there exist distinct elements a, a' of $\mathcal{A}$ such that $a - a' = \Phi(x)$ for some $x \in \mathbb{F}_q[t]$.*

The above theorem is an $\mathbb{F}_q[t]$ analog of a result of Sárközy [20]. Previously, such a result with no restriction on the degree of Φ was not available, except in the case $\Phi(0) = 0$ [2]. We defer to Section 6 for an introduction to intersective and van der Corput sets and the statement of our results.

Our next application is about Glasner sets in $\mathbb{F}_q[t]$. Generalizing a result of Glasner, Alon and Peres proved 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 $\Phi(n)Y = \{\Phi(n)y : y \in Y\}$ intersects any interval of length ϵ in $\mathbb{R}/\mathbb{Z}$. In view of Example 1.1 and the discussion preceding Conjecture 1, it is not surprising that an exact analog of Alon and Peres' result in $\mathbb{F}_q[t]$ is *not* true in general. We will prove the following $\mathbb{F}_q[t]$ analog of Alon and Peres' result.

Theorem 4. *Let $\Phi(u) = \sum_{r\in\mathcal{K}\cup\{0\}} a_r u^r$ be a polynomial supported on a set $\mathcal{K} \subset \mathbb{Z}^+$ with coefficients in $\mathbb{F}_q[t]$. Suppose that $a_k \neq 0$ for some $k \in \mathcal{K}$ satisfying $k > 1, p \nmid k$ and $p^v k \notin \mathcal{S}(\mathcal{K})$ for any $v \in \mathbb{Z}^+$. Then for any infinite subset $Y \subset \mathbb{T}$ and any $M \in \mathbb{Z}^+$, there exists $x \in \mathbb{F}_q[t]$ such that the set*

$$\Phi(x)Y = \{\Phi(x)y : y \in Y\} \subset \mathbb{T}$$

intersects any cylinder set of radius q^{-M} in $\mathbb{T}$.

We defer to Section 7 for an introduction to Glasner sets and the statement of our results.

The paper is organized as follows. In Section 2, we introduce some preliminaries that are needed to prove our results. We prove a minor arc estimate in Section 3 and we derive its generalization in Section 4. Then we use these results to prove Theorem 2 in Section 5. Finally, in Sections 6 and 7, we discuss applications of our equidistribution result to van der Corput, intersective and Glasner sets in $\mathbb{F}_q[t]$.

2. Preliminaries

We begin this section by reviewing an orthogonal relation of the exponential function $e(\cdot)$ that is defined in Section 1. For $\alpha \in \mathbb{K}_\infty$, we have [11, Lemma 7]:

$$\sum_{x\in\mathbb{G}_N} e(x\alpha) = \begin{cases} q^N, & \text{if } \operatorname{ord}\{\alpha\} < -N, \\ 0, & \text{if } \operatorname{ord}\{\alpha\} \geq -N. \end{cases} \tag{2}$$

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

$$\sum_{x\in\mathbb{G}_{\operatorname{ord} g}} e\left(\frac{xa}{g}\right) = \begin{cases} |g|, & \text{if } a \equiv 0 \pmod{g}, \\ 0, & \text{otherwise.} \end{cases} \tag{3}$$

To simplify notation in the proofs of the paper, we need to introduce additional definitions. Given $j, r \in \mathbb{Z}^+$, we write $j \preceq_p r$ if $p \nmid \binom{r}{j}$. By Lucas' theorem, this happens precisely when all 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 $\mathbb{Z}^+$. If $j \preceq_p r$, then we necessarily have $j \leq r$. Let $\mathcal{K} \subset \mathbb{Z}^+$. We say an element

$k \in \mathcal{K}$ is *maximal* if it is maximal with respect to $\preceq_p$, that is, for any $r \in \mathcal{K}$, either $r \preceq_p k$ or r and k are not comparable. We recall that

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

Define

$$\mathcal{K}^* = \left\{ k \in \mathcal{K} : p \nmid k \text{ and } p^v k \notin \mathcal{S}(\mathcal{K}) \text{ for any } v \in \mathbb{Z}^+ \right\}. \tag{4}$$

We have the following facts about the partial ordering $\preceq_p$.

Lemma 5. *For $\mathcal{K} \subset \mathbb{Z}^+$, we have*
(1) *if k is maximal in $\mathcal{K}$, then k is maximal in $\mathcal{S}(\mathcal{K})$.*
(2) *$\mathcal{K}^* \subset \mathcal{S}(\mathcal{K})^*$.*

Proof. The first part of the lemma is immediate from the definition of $\mathcal{S}(\mathcal{K})$. The second part follows from the observation that $\mathcal{S}(\mathcal{S}(\mathcal{K})) = \mathcal{S}(\mathcal{K})$. □

Lemma 6. *Let $\mathcal{K} \subset \mathbb{Z}^+$ and $k \in \mathcal{K}^*$. If $j \in \mathcal{K}$ satisfies $k \preceq_p j$, then $j \in \mathcal{K}^*$.*

Proof. We have $p \nmid k$ and $p \nmid \binom{j}{k}$. By Lucas' theorem, it follows that $p \nmid j$. Again, by Lucas' theorem, for any $v \in \mathbb{Z}^+$, we have $p^v k \preceq_p p^v j$. It follows that $p^v j \notin \mathcal{S}(\mathcal{K})$, and hence $j \in \mathcal{K}^*$. □

We will apply the following large sieve inequality to get a minor arc estimate. Given a set $\Gamma \subset \mathbb{K}_\infty$, if for any distinct elements $\gamma_1, \gamma_2 \in \Gamma$, we have $\operatorname{ord}\{(\gamma_1 - \gamma_2)\} \geq \delta$, then we say that the points $\{\gamma : \gamma \in \Gamma\}$ are *spaced at least q^δ apart in $\mathbb{T}$.*

Theorem 7. (Hsu [9, Theorem 2.4]) *Given $K \in \mathbb{Z}^+$, let $\Gamma \subset \mathbb{K}_\infty$ be a set whose elements are spaced at least q^{-K} apart in $\mathbb{T}$. Let $(b_x)_{x \in \mathbb{F}_q[t]}$ be a sequence of complex numbers. For $\beta \in \mathbb{K}_\infty$, define*

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

Then we have

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

In the following, we state a mean value theorem whose indices are elements of $\mathcal{S}(\mathcal{K})$. For $j \in \mathcal{S}(\mathcal{K})$, by the definition of $\mathcal{S}(\mathcal{K})$, if $i \in \mathbb{Z}^+$ satisfies $i \preceq_p j$, then $i \in \mathcal{S}(\mathcal{K})$. Therefore, the set $\mathcal{S}(\mathcal{K})$ satisfies Condition* which is defined in [13, Section 1]. For $N \in \mathbb{Z}^+$, let $J_s(\mathcal{S}(\mathcal{K}); N)$ denote 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 $u_r, v_r \in \mathbb{G}_N$ $(1 \leq r \leq s)$. Since $(u_1 + \cdots + u_s)^p = u_1^p + \cdots + u_s^p$, the above equations are not always independent. To obtain independence, we consider the set

$$\mathcal{S}(\mathcal{K})' = \left\{ i \in \mathbb{Z}^+ : p \nmid i \text{ and } p^v i \in \mathcal{S}(\mathcal{K}) \text{ for some } v \in \mathbb{Z}^+ \right\}. \tag{5}$$

We note that for $j = p^v i$ with $p \nmid i$, we have $u_1^j + \cdots + u_s^j = (u_1^i + \cdots + u_s^i)^{p^v}$. Therefore, $J_s(\mathcal{S}(\mathcal{K}); N)$ 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 $u_r, v_r \in \mathbb{G}_N$ $(1 \leq r \leq s)$. The following result gives an upper bound of $J_s(\mathcal{S}(\mathcal{K}); N)$.

Theorem 8. (Liu & Wooley [19]; see also [13, Theorem 1.1]) *Let* $\psi = \#\mathcal{S}(\mathcal{K})'$, $\phi = \max_{i \in \mathcal{S}(\mathcal{K})'} i$ *and* $\kappa = \sum_{i \in \mathcal{S}(\mathcal{K})'} i$. *Suppose that* $\phi \geq 2$ *and* $s \geq (\psi\phi + \psi)$. *Then for any* $\epsilon > 0$, *there exists a constant* $C_1 = C_1(s; \mathcal{K}; \epsilon; q) > 0$ *such that*

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

We now recall some facts about continued fractions in $\mathbb{K}_\infty$ which are needed in the proof of Theorem 2. For any $\alpha \in \mathbb{K}_\infty$, we can write

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

where $b_i \in \mathbb{F}_q[t]$ and $\operatorname{ord} b_i > 0$ $(i \geq 1)$. We note that α is irrational if and only if its continued fraction expansion is infinite. In contrast with the real case where rational numbers have two continued fraction expansions (e.g, $1/3 = [0, 3, 0] = [0, 2, 1]$), continued fraction expansions in $\mathbb{K}_\infty$ are unique. We define two sequences $(a_n)_{n \geq -2}$ and $(g_n)_{n \geq -2}$ in $\mathbb{F}_q[t]$ recursively by putting $a_{-2} = 0, g_{-2} = 1, a_{-1} = 1, g_{-1} = 0$, and for all $n \geq 0$,

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

Then for all $n \geq 0$, 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 $(n \geq 0)$ are called the *convergents* of α. One can also show by induction that the sequence $(\operatorname{ord} g_n)_{n \geq 0}$ is strictly increasing.

Proposition 9. ([22, Section 1]) *Let* a_n/g_n $(n \geq 0)$ *be convergents of* α. *We have*

1. $\operatorname{ord}(g_n \alpha - a_n) = -\operatorname{ord} g_{n+1}$ $(n \geq 0)$.
2. (Legendre's theorem) *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.

The following lemma is about elements in $\mathbb{K}_\infty$ that are well approximated by rationals.

Lemma 10. *Suppose that* $\alpha \in \mathbb{K}_\infty$ *satisfies the following condition: there exists a constant* $\kappa > 1$, *such that, for all* N *sufficiently large, there exist* $a, g \in \mathbb{F}_q[t]$ *with* $\operatorname{ord}(g\alpha - a) \leq -\kappa N$ *and* $\operatorname{ord} g < N$. *Then* α *is rational.*

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

$$\operatorname{ord}(g\alpha - a) \leq -\kappa N < -\operatorname{ord} g_n.$$

By Proposition 9(2), a/g is a convergent of α. Since $\operatorname{ord} g < N = \operatorname{ord} g_n$ and the sequence $(\operatorname{ord} g_n)_{n \geq 0}$ is strictly increasing, there exists $m \in \mathbb{Z}^+ \cup \{0\}$ with $m < n$ such that $a = a_m$ and $g = g_m$. By Proposition 9(1),

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

which contradicts the previous inequality. Therefore, α is rational. □

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

Theorem 11. (Carlitz [4, Theorem 4]) *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*

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

3. A Weyl-type estimate

In this section, we will establish the following minor arc estimate.

Theorem 12. *Let* $f(u) = \sum_{r\in\mathcal{K}\cup\{0\}} \alpha_r u^r$ *be a polynomial supported on a set* $\mathcal{K} \subset \mathbb{Z}^+$ *with coefficients in* $\mathbb{K}_\infty$*. Suppose that* $k \in \mathcal{K}^*$ *(defined as in (4)) is maximal in* $\mathcal{K}$*. Then there exist constants* $c, C > 0$*, depending only on* $\mathcal{K}$ *and* q*, such that the following holds: suppose that for some* $0 < \eta \le cN$*, we have*

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

Then for any $\epsilon > 0$ *and* N *sufficiently large in terms of* $\mathcal{K}$*,* ϵ *and* q*, there exist* $a, g \in \mathbb{F}_q[t]$ *such that*

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

Remark.

- In Theorem 12, the coefficient α_k plays the role of the leading coefficient of the polynomial. This is, in a sense, the "true" $\mathbb{F}_q[t]$ analog of the leading coefficient.
- 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 $\mathcal{K} = \{9, 5, 3, 1\}$ then $9, 5, 3$ are maximal elements of $\mathcal{K}$ and they all satisfy the hypothesis of Theorem 12.

The following two lemmas are needed in our proof of Theorem 12.

Lemma 13. (Weyl's shift) *Let* $\mathcal{A}$ *be a subset of* $\mathbb{G}_N$*. 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 $y \in \mathcal{A} \subset \mathbb{G}_N$, we have

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

It follows that

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

$\square$

For $\mathcal{K} \subset \mathbb{Z}^+$, let $\mathcal{S}(\mathcal{K})$ be its shadow. Let $f(u) = \sum_{r\in\mathcal{K}\cup\{0\}} \alpha_r u^r$ be a polynomial supported on $\mathcal{K}$ with coefficients in $\mathbb{K}_\infty$. 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, for a fixed $x \in \mathbb{G}_N$, if k is maximal in $\mathcal{K}$, then there exist $\gamma_j = \gamma_j(\{\alpha_r\}_{r\in\mathcal{K}}; x) \in \mathbb{K}_\infty$ $(j \in \mathcal{S}(\mathcal{K}) \setminus \{k\})$ and $\gamma = \gamma(\{\alpha_r\}_{r\in\mathcal{K}\cup\{0\}}; x) \in \mathbb{K}_\infty$ such that

$$f(y-x) = \alpha_k(y-x)^k + \sum_{r\in\mathcal{K}\setminus\{k\}} \alpha_r(y-x)^r + \alpha_0 = \alpha_k y^k + \sum_{j\in\mathcal{S}(\mathcal{K})\setminus\{k\}} \gamma_j y^j + \gamma. \tag{6}$$

Lemma 14. *Let $M \in \mathbb{Z}^+$ with $M \le N$. 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 $(a, g) = 1$, $\operatorname{ord}(g\alpha_k - a) < -kM$ and either $\operatorname{ord}(g\alpha_k - a) \ge (M - kN)$ or $\operatorname{ord} g > M$. Let $\mathcal{L}_0$ be a subset of monic irreducible polynomials of degree M, such that, for any distinct elements $l_1, l_2 \in \mathcal{L}_0$, we have $l_1^k \equiv l_2^k \pmod{g}$ if and only if $l_1 \equiv l_2 \pmod{g}$. 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. Let $l_1, l_2 \in \mathcal{L}_0$ with $l_1 \not\equiv l_2 \pmod{g}$. Then by the property of $\mathcal{L}_0$, 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

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

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

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

Therefore, it follows that

$$\operatorname{ord}\{\alpha_k(l_1^k - l_2^k)\} = \operatorname{ord}\{a(l_1^k - l_2^k)/g\} \ge -\operatorname{ord} g. \tag{7}$$

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

Case 1. Suppose that $\operatorname{ord} g > M$. In this case, the elements of $\mathcal{L}_0$ are distinct (mod g). By (7), the points $\alpha_k l^k$ are spaced at least $|g|^{-1}$ apart in $\mathbb{T}$.

Case 2. Suppose that $\operatorname{ord} g \le M$. Then by the assumption, we have $\operatorname{ord}(g\alpha_k - a) \ge (M - kN)$. If $l_1, l_2 \in \mathcal{L}_0$ satisfy $l_1 \not\equiv l_2 \pmod{g}$, then it follows from (7) that αl_1^k and αl_2^k are spaced at least $|g|^{-1}$ apart in $\mathbb{T}$. If $l_1 \equiv l_2 \pmod{g}$, since $\operatorname{ord}(g\alpha_k - a) < -kM$ and $\operatorname{ord}(g\alpha_k - a) \ge (M - kN)$, we have

$$\begin{aligned}\operatorname{ord}\{\alpha_k(l_1^k - l_2^k)\} &= \operatorname{ord}\{(\alpha_k - a/g)(l_1^k - l_2^k)\}\\ &= \operatorname{ord}\big((\alpha_k - a/g)(l_1^k - l_2^k)\big)\\ &\ge M - kN - \operatorname{ord} g + \operatorname{ord}(l_1^k - l_2^k).\end{aligned} \tag{8}$$

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 have

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

and hence by (8) we have

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

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

Combining the above two cases, we see that for any distinct elements $l_1, l_2 \in \mathcal{L}$, they are spaced at least $\min\{|g|^{-1}, q^{k(M-N)}\}$ apart in $\mathbb{T}$. $\square$

We are now ready to prove Theorem 12.

Proof of Theorem 12. We first note that if Theorem 12 holds for $f(u) - \alpha_0 = \sum_{r \in \mathcal{K}} \alpha_r u^r$, then it holds for $f(u)$. Therefore, without loss of generality, we can assume $\alpha_0 = 0$. Let k be a maximal element of $\mathcal{K}$ which satisfies $p \nmid k$ and $p^v k \notin \mathcal{S}(\mathcal{K})$ for any $v \in \mathbb{Z}^+$. Let $\alpha_k \in \mathbb{K}_\infty$ and $M \in \mathbb{Z}^+$ with $2M \leq N$. By Dirichlet's theorem in $\mathbb{F}_q[t]$ [11, Lemma 3], there exist $a, g \in \mathbb{F}_q[t]$ with $(a, g) = 1$, $\operatorname{ord}(g\alpha_k - a) < -kM$ and $\operatorname{ord} g \leq kM$. Suppose that either $\operatorname{ord}(g\alpha_k - a) \geq (M - kN)$ or $\operatorname{ord} g > M$. We will show that, for M suitably chosen, such an assumption leads to an upper bound for $\left|\sum_{x \in \mathbb{G}_N} e(f(x))\right|$, which contradicts the lower bound stated in the theorem.

Let $\mathcal{L}$ be the set of monic irreducible polynomials l satisfying $\operatorname{ord} l = M$ and $(l, g) = 1$. Since $\operatorname{ord} g \leq kM$, g has at most k irreducible factors of degree M. Therefore, by the prime number theorem in $\mathbb{F}_q[t]$, for M sufficiently large, in terms of k (thus $\mathcal{K}$) and q, we have $\#\mathcal{L} \geq q^M/(2M)$. Let $\mathcal{A}$ be the multiset

$$\mathcal{A} = \{y = lw : l \in \mathcal{L} \text{ and } w \in \mathbb{F}_q[t] \text{ with } w \in \mathbb{G}_{(N-M)}\},$$

where the multiplicity of each y is the number of its representations $y = lw$. Then $\mathcal{A} \subseteq \mathbb{G}_N$ and

$$\#\mathcal{A} \geq q^M/(2M) \cdot q^{(N-M)} = q^N/(2M).$$

By Lemma 13 and (6), we have

$$\begin{aligned}\sum_{x \in \mathbb{G}_N} e(f(x)) &= 2q^{-N} M \sum_{x \in \mathbb{G}_N} \sum_{y \in \mathcal{A}} e\Big(\alpha_k y^k + \sum_{j \in \mathcal{S}(\mathcal{K}) \setminus \{k\}} \gamma_j(\{\alpha_r\}_{r \in \mathcal{K}}; x) y^j + \gamma(\{\alpha_r\}_{r \in \mathcal{K}}; x)\Big) \\ &\leq 2M \max_{x \in \mathbb{G}_N} \left| \sum_{y \in \mathcal{A}} e\Big(\alpha_k y^k + \sum_{j \in \mathcal{S}(\mathcal{K}) \setminus \{k\}} \gamma_j(\{\alpha_r\}_{r \in \mathcal{K}}; x) y^j\Big) \right|.\end{aligned}$$

Let $\gamma_j = \gamma_j(\{\alpha_r\}_{r \in \mathcal{K}}; x) \in \mathbb{K}_\infty$ $(j \in \mathcal{S}(\mathcal{K}) \setminus \{k\})$ correspond to the choice of x which maximizes the above expression, and we fix them from now on.

Let $s \in \mathbb{Z}^+$ with $s \geq (\psi\phi + \psi)$, where ψ and ϕ are defined as in Theorem 8. By Hölder's inequality,

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

Let $\epsilon > 0$ be arbitrary. For $h, g \in \mathbb{F}_q[t]$ with $(h, g) = 1$, by Hensel's lemma, there exists $C_2 = C_2(\epsilon; q) > 0$ such that (see [18, Corollary 7.2 and (12.4)] for more details)

$$\#\big\{z \in \mathbb{F}_q[t] : z^k \equiv h \pmod{g} \text{ and } \operatorname{ord} z < \operatorname{ord} g\big\} \leq C_2 |g|^{\epsilon}.$$

Therefore, there exists $L \in \mathbb{Z}^+$ satisfying $L \leq C_2|g|^{\epsilon}$ with the following property: the set $\mathcal{L}$ can be divided into L classes, $\mathcal{L}_1, \ldots, \mathcal{L}_L$, such that, for any distinct elements $l_1, l_2 \in \mathcal{L}_r$ $(1 \leq r \leq L)$, we have $l_1^k \equiv l_2^k \pmod{g}$ if and only if $l_1 \equiv l_2 \pmod{g}$. Then there exists $r \in \mathbb{Z}^+$ with $r \leq L$ for which

$$\left|\sum_{x \in \mathbb{G}_N} e(f(x))\right|^{2s} \leq (2M)^{2s}(q^M)^{2s-1} C_2 |g|^{\epsilon} \sum_{l \in \mathcal{L}_r} \left|\sum_{w \in \mathbb{G}_{(N-M)}} e\Big(\alpha_k (lw)^k + \sum_{j \in \mathcal{S}(\mathcal{K}) \setminus \{k\}} \gamma_j (lw)^j\Big)\right|^{2s}.$$

Let $\mathcal{S}(\mathcal{K})'$ be defined as in (5). 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 $w_r \in \mathbb{G}_{(N-M)}$ $(1 \leq r \leq s)$. 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

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

with $w_r \in \mathbb{G}_{(N-M)}$ $(1 \leq r \leq s)$. 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 $v \in \mathbb{Z}^+$, a sum over h_k is independent of another h_j $(j \in \mathcal{S}(\mathcal{K}) \setminus \{k\})$. Therefore, we have

$$\begin{aligned}
&\left|\sum_{x \in \mathbb{G}_N} e(f(x))\right|^{2s} \\
&\leq (2M)^{2s}(q^M)^{2s-1} C_2 |g|^{\epsilon} \sum_{l \in \mathcal{L}_r} \left|\sum_{\substack{h_i \in \mathbb{G}_{i(N-M)} \\ i \in \mathcal{S}(\mathcal{K})'}} b(\mathbf{h}) e\Big(\alpha_k h_k l^k + \sum_{j \in \mathcal{S}(\mathcal{K}) \setminus \{k\}} \gamma_j h_j l^j\Big)\right|^2 \\
&\leq (2M)^{2s}(q^M)^{2s-1} C_2 |g|^{\epsilon} (q^{(N-M)})^{\sum_{i \in \mathcal{S}(\mathcal{K})' \setminus \{k\}} i} \sum_{\substack{h_i \in \mathbb{G}_{i(N-M)} \\ i \in \mathcal{S}(\mathcal{K})' \setminus \{k\}}} \sum_{l \in \mathcal{L}_r} \left|\sum_{h_k \in \mathbb{G}_{k(N-M)}} b(\mathbf{h}) e(\alpha_k h_k l^k)\right|^2.
\end{aligned}$$

Since $p \nmid k$, by Theorem 7 and Lemma 14, we have

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

Furthermore, by considering the underlying equations, by Theorem 8, there exists a constant $C_1 = C_1(s; \mathcal{K}; \epsilon; q) > 0$ such that

$$\sum_{\substack{h_i \in \mathbb{G}_{i(N-M)} \\ i \in \mathcal{S}(\mathcal{K})' \setminus \{k\}}} \sum_{h_k \in \mathbb{G}_{k(N-M)}} |b(\mathbf{h})|^2 \leq J_s(\mathcal{S}(\mathcal{K}); (N-M)) \leq C_1 (q^{N-M})^{2s - \sum_{i \in \mathcal{S}(\mathcal{K})'} i + (k+1)\epsilon}.$$

Combining the above three estimates, it follows that

$$\left| \sum_{x \in \mathbb{G}_N} e(f(x)) \right|^{2s} \leq (2M)^{2s} C_1 (q^N)^{2s} (q^M)^{-1} C_2 |g|^{\epsilon} \left(|g| q^{k(M-N)} + 1\right) \left(q^{(N-M)}\right)^{(k+1)\epsilon}.$$

Since $\operatorname{ord} g \leq kM$ and $2M \leq N$, we have

$$\left| \sum_{x \in \mathbb{G}_N} e(f(x)) \right| \leq 2M q^N \left(2 C_1 C_2 (q^M)^{-1} (q^{kM})^{\epsilon} \left(q^{(N-M)}\right)^{(k+1)\epsilon}\right)^{1/2s}.$$

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

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

We now make the specific choice

$$M = [\log_q C_3 + N(k+1)\epsilon + 2s\eta + 1].$$

Then it follows that

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

which contradicts the assumption of Theorem 12. This implies that there exist $a, g \in \mathbb{F}_q[t]$ such that

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

By assuming $\epsilon < 1/(4(k+1))$, we see that the requirement $2M \leq N$ is satisfied when $0 < \eta \leq N/(8s)$ and N is sufficiently large, in terms of $\mathcal{K}$, ϵ and q. In addition, for N sufficiently large, we have

$$M \leq N(k+2)\epsilon + 2s\eta.$$

Take $s = (\psi\phi + \psi)$. Since $\epsilon > 0$ is arbitrary, by taking $c = 1/(8s)$ and $C = 2s$, which are constants depending only on $\mathcal{K}$ and q, Theorem 12 follows. □

4. Extending the Weyl-type estimate to other coefficients

In this section, we will extend Theorem 12 to indices which are not maximal.

Theorem 15. *Let $f(u) = \sum_{r\in\mathcal{K}\cup\{0\}} \alpha_r u^r$ be a polynomial supported on a set $\mathcal{K} \subset \mathbb{Z}^+$ with coefficients in $\mathbb{K}_\infty$. Then for any $k \in \mathcal{K}^*$ (defined as in (4)), there exist constants $c_k, C_k > 0$, depending only on $\mathcal{K}$ and q, such that the following holds: suppose that for some $0 < \eta \le c_k N$, we have*

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

Then for any $\epsilon > 0$ and N sufficiently large in terms of $\mathcal{K}$, ϵ and q, there exist $a_k, g_k \in \mathbb{F}_q[t]$ such that

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

Proof. Without loss of generality, we can assume $\alpha_0 = 0$. 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 statement follows from Theorem 12. Suppose that the theorem is established for any $h \in \mathcal{K}^*$ with $k \preceq_p h$ and $h \ne k$. Define

$$\mathcal{K}_0 = \{h \in \mathcal{K} : k \preceq_p h \text{ and } h \ne k\} \qquad \text{and} \qquad \mathcal{K}_1 = \mathcal{K}\setminus\mathcal{K}_0. \tag{9}$$

By Lemma 6, $\mathcal{K}_0 \subset \mathcal{K}^*$. For $h \in \mathcal{K}_0$, let c_h, C_h be defined as in Theorem 15. Let

$$c = \min\left\{c_h : h \in \mathcal{K}_0\right\} \qquad \text{and} \qquad C = \sum_{h\in\mathcal{K}_0} C_h.$$

Suppose that for some $0 \le \eta \le cN$.

$$\left|\sum_{x\in\mathbb{G}_N} e(f(x))\right| \ge q^{N-\eta}. \tag{10}$$

Let $\epsilon > 0$ be arbitrary. By induction hypothesis, for any $h \in \mathcal{K}_0$ and N sufficiently large, in terms of $\mathcal{K}, \epsilon$ and q, there exist $a_h, g_h \in \mathbb{F}_q[t]$ $(h \in \mathcal{K}_0)$ such that

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

Define

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

Then we have

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

Let $M \in \mathbb{Z}^+$ with $M < (N - \operatorname{ord} g)$. We can rewrite the set $\mathbb{G}_N$ as follows:

$$\begin{aligned}\mathbb{G}_N &= \left\{gv + w : \operatorname{ord} v < (N - \operatorname{ord} g) \text{ and } \operatorname{ord} w < \operatorname{ord} g\right\}\\ &= \left\{g(t^M z + y) + w : \operatorname{ord} z < (N - \operatorname{ord} g - M),\ \operatorname{ord} y < M \text{ and } \operatorname{ord} w < \operatorname{ord} g\right\}\\ &= \left\{gy + (gt^M z + w) : \operatorname{ord} z < (N - \operatorname{ord} g - M),\ \operatorname{ord} y < M \text{ and } \operatorname{ord} w < \operatorname{ord} g\right\}.\end{aligned}$$

Let $s = (gt^M z + w)$ with $z \in \mathbb{G}_{N-\operatorname{ord} g - M}$ and $\operatorname{ord} w \in \mathbb{G}_{\operatorname{ord} g}$. Then $\operatorname{ord} s < N$ and the set $\mathbb{G}_N$ can be partitioned into q^{N-M} blocks of the form

$$\mathcal{B}_s = \{gy + s : \operatorname{ord} y < M\}.$$

Then (10) implies that there exists a block $\mathcal{B}_s$ such that

$$\left|\sum_{x\in\mathcal{B}_s} e(f(x))\right| = \left|\sum_{y\in\mathbb{G}_M} e(f(gy+s))\right| \geq q^{N-\eta}\left(q^{N-M}\right)^{-1} = q^{M-\eta}. \tag{11}$$

We have

$$\begin{aligned}
&\left|\sum_{y\in\mathbb{G}_M} e(f(gy+s))\right| \\
&= \left|\sum_{y\in\mathbb{G}_M} e\left(\sum_{h\in\mathcal{K}} \alpha_h (gy+s)^h\right)\right| \\
&= \left|\sum_{y\in\mathbb{G}_M} e\left(\sum_{h\in\mathcal{K}_0} \alpha_h (gy+s)^h + \sum_{h\in\mathcal{K}_1} \alpha_h (gy+s)^h\right)\right| \\
&= \left|\sum_{y\in\mathbb{G}_M} e\left(\sum_{h\in\mathcal{K}_0} (\alpha_h - b_h/g)\left((gy+s)^h - s^h\right) + \sum_{h\in\mathcal{K}_1} \alpha_h (gy+s)^h\right)\right|,
\end{aligned} \tag{12}$$

where the last equation holds since $e\left(\sum_{h\in\mathcal{K}_0} \alpha_h(-s^h)\right)$ is a constant independent of y and $e\left(\sum_{h\in\mathcal{K}_0} -b_h/g\left((gy+s)^h - s^h\right)\right) = 1$. For any $y \in \mathbb{G}_M$ and $h \in \mathcal{K}_0$, we have

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

It follows that

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

We now make the specific choice

$$M = [(1-\epsilon)N - C\eta - 1].$$

Then it follows that

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

and hence

$$\operatorname{ord}\ (\alpha_h - b_h/g)\left((gy+s)^h - s^h\right) < -1.$$

Therefore, we have

$$e\left(\sum_{h\in\mathcal{K}_0}(\alpha_h - a_h/g)\Big((gy+s)^h - s^h\Big) + \sum_{h\in\mathcal{K}_1}\alpha_h(gy+s)^h\right) = e\left(\sum_{h\in\mathcal{K}_1}\alpha_h(gy+s)^h\right). \tag{13}$$

Combining (11), (12) and (13), we have

$$\left|\sum_{y\in\mathbb{G}_M} e\left(\sum_{h\in\mathcal{K}_1}\alpha_h(gy+s)^h\right)\right| \geq q^{M-\eta}.$$

We note here that since $\operatorname{ord} g \leq (\epsilon N + C\eta)$, for N sufficiently large, the above choice of M satisfies $0 < M < (N - \operatorname{ord} g)$.

The polynomial $\sum_{h\in\mathcal{K}_1}\alpha_h(gy+s)^h$ is supported on $\mathcal{S}(\mathcal{K}_1)$. Since $k\in\mathcal{K}^*$ is maximal in $\mathcal{K}_1$, by Lemma 5, k is maximal in $\mathcal{S}(\mathcal{K}_1)$ and $k\in\mathcal{S}(\mathcal{K}_1)^*$. Furthermore, the coefficient of y^k in $\sum_{h\in\mathcal{K}_1}\alpha_h(gy+s)^h$ is $\alpha_k g^k$. By Theorem 12, there exist constants $d_k, D_k > 0$ and $\widetilde{a}_k, \widetilde{g}_k \in \mathbb{F}_q[t]$, such that, for $0 < \eta \leq d_k N$ and N sufficiently large,

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

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

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

and

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

Since $\epsilon > 0$ is arbitrary, by taking $c_k = \min\{c, d_k\}$ and $C_k = (kC + D_k)$, Theorem 15 follows. $\square$

One can extend Theorem 15 to indices that are not in $\mathcal{K}^*$. Let $\mathcal{K}_0 = \mathcal{K}$, and for any $n \geq 1$, let

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

Define

$$\widetilde{\mathcal{K}} = \bigcup_{n=0}^{\infty} K^*_n. \tag{14}$$

Then by induction on n, one can apply the method of the proof of Theorem 15 to obtain the following result.

Proposition 16. *Let $f(u) = \sum_{r\in\mathcal{K}\cup\{0\}}\alpha_r u^r$ be a polynomial supported on a set $\mathcal{K}\subset\mathbb{Z}^+$ with coefficients in $\mathbb{K}_\infty$. Then for any $k\in\widetilde{\mathcal{K}}$, there exist constants $c_k, C_k > 0$, depending only on $\mathcal{K}$ and q, such that the following holds: suppose that for some $0 < \eta \leq c_k N$, we have*

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

Then for any $\epsilon > 0$ and N sufficiently large, in terms of $\mathcal{K}$, ϵ and q, there exist $a_k, g_k \in \mathbb{F}_q[t]$ such that

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

It seems that there is no simple description of $\widetilde{\mathcal{K}}$. In many cases, $\widetilde{\mathcal{K}}$ is larger than $\mathcal{K}^*$. For example, if $p > 3$ and $\mathcal{K} = \{1, 3, 3p+1\}$ (as in the first case of Example 1.3), then $\mathcal{K}^* = \{3p+1\}$, but $\widetilde{\mathcal{K}} = \mathcal{K}$. 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 1.3), then $\mathcal{K}^* = \emptyset$, and hence $\widetilde{\mathcal{K}} = \emptyset$. Therefore, we cannot go as far as proving Conjecture 1 by using this method.

5. Equidistribution of polynomial sequences

In this section, we prove Theorem 2. Then we discuss a variant of the theorem. The following lemma is essential for our proof of Theorem 2.

Lemma 17. *Let $f(u) = \sum_{r\in\mathcal{K}\cup\{0\}} \alpha_r u^r$ be a polynomial supported on a set $\mathcal{K} \subset \mathbb{Z}^+$ with coefficients in $\mathbb{K}_\infty$. For $k \in \mathcal{K}^*$ (defined as in (4), 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. To prove the lemma, we suppose the contrary. Then for any $N \in \mathbb{Z}^+$, there exists $s_N \in \mathbb{F}_q[t]$ such that

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

We note that for each $s \in \mathbb{F}_q[t]$, the polynomial $f(y+s)$ is supported on $\mathcal{S}(\mathcal{K})$. Since $k \in \mathcal{K}^*$ is maximal in $\mathcal{K}$, by Lemma 5, k is maximal in $\mathcal{S}(\mathcal{K})$ and $k \in \mathcal{S}(\mathcal{K})^*$. Furthermore, the coefficient of y^k in $f(y+s)$ is α_k. Applying Theorem 12 with $\epsilon = 1/3$, there exists a constant $C > 0$, such that, for any N sufficiently large, in terms of $\mathcal{K}$ and q, there exist $a, g \in \mathbb{F}_q[t]$ such that

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

For $M \in \mathbb{Z}^+$, we apply the above inequalities with $N = [3(M - C\eta)]$. Then for M sufficiently large, we have

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

By Lemma 10, the above inequalities implies that α_k is rational, which leads to a contradiction. This completes the proof of the lemma. $\square$

We are now ready to prove Theorem 2.

Proof of Theorem 2. Without loss of generality, we can assume $\alpha_0 = 0$. Let $k \in \mathcal{K}^*$ and suppose that α_k is irrational. We prove Theorem 2 by downward induction on k with respect to the partial order $\preceq_p$. Suppose that k is maximal in $\mathcal{K}$. Let η and N_0 be defined as in Lemma 17. For any $N \geq N_0$, we can partition the set $\mathbb{G}_N$ as q^{N-N_0} blocks of the form

$$\mathcal{B}_s = \{y + s : \operatorname{ord} y < N_0\},$$

where $s = t^{N_0} z$ for some $z \in \mathbb{G}_{N-N_0}$. Therefore, it follows from Lemma 17 that

$$\left| \sum_{x \in \mathbb{G}_N} e(f(x)) \right| < q^{N-N_0} q^{N_0 - \eta} = q^{N-\eta}.$$

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

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

which establishes Theorem 2 in the special case when k is maximal in $\mathcal{K}$.

Suppose that the theorem is established for any $h \in \mathcal{K}^*$ with $k \preceq_p h$ and $h \neq k$. Let $\mathcal{K}_0$ and $\mathcal{K}_1$ be defined as in (9). We note that if there exists $h \in \mathcal{K}_0$ such that α_h is irrational, then Theorem 2 follows from induction hypothesis. Therefore, it suffices to consider the case that all the α_h ($h \in \mathcal{K}_0$) are rational. Let g be the common denominator of α_h ($h \in \mathcal{K}_0$) and $s \in \mathbb{F}_q[t]$ be arbitrary. For any $M \in \mathbb{Z}^+$, we have

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

where the last equality follows since $e\big(\sum_{h \in \mathcal{K}_0} \alpha_h(-s^h)\big)$ is a constant independent of y. By the definition of g, we have

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

It follows that

$$\left| \sum_{y \in \mathbb{G}_M} e(f(gy + s)) \right| = \left| \sum_{y \in \mathbb{G}_M} e\left(\sum_{h \in \mathcal{K}_1} \alpha_h (gy + s)^h \right) \right|. \tag{15}$$

For $N \in \mathbb{Z}^+$ with $N > \operatorname{ord} g$, we write $N = M + \operatorname{ord} g$ for some $M \in \mathbb{Z}^+$. Then we can partition the set $\mathbb{G}_N$ as q^{N-M} blocks of the form

$$\mathcal{B}_s = \{gy + s : \operatorname{ord} y < M\},$$

where $s \in \mathbb{G}_{\operatorname{ord} g}$. It follows from (15) that

$$\begin{aligned} \left| \sum_{x \in \mathbb{G}_N} e(f(x)) \right| &\leq q^{N-M} \max_{s \in \mathbb{G}_{\operatorname{ord} g}} \left| \sum_{y \in \mathbb{G}_M} e(f(gy+s)) \right| \\ &= q^{N-M} \max_{s \in \mathbb{G}_{\operatorname{ord} g}} \left| \sum_{y \in \mathbb{G}_M} e\left(\sum_{h \in \mathcal{K}_1} \alpha_h (gy+s)^h \right) \right|. \end{aligned} \tag{16}$$

The polynomial $\sum_{h \in \mathcal{K}_1} \alpha_h (gy+s)^h$ is supported on $\mathcal{S}(\mathcal{K}_1)$. Since $k \in \mathcal{K}^*$ is maximal in $\mathcal{K}_1$, by Lemma 5, k is maximal in $\mathcal{S}(\mathcal{K}_1)$ and $k \in \mathcal{S}(\mathcal{K}_1)^*$. Furthermore, the coefficient of y^k in $\sum_{h \in \mathcal{K}_1} \alpha_h (gy+s)^h$ is $\alpha_k g^k$, which is irrational since α_k is irrational. By the first part of the proof, we have

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

Then it follows from (16) that

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

By Theorem 11, it follows that the sequence $(f(x))_{x \in \mathbb{F}_p[t]}$ is equidistributed in $\mathbb{T}$. $\square$

By an observation similar to the one following the proof of Theorem 15, one can apply the method of the proof of Theorem 2 to obtain the following result.

Proposition 18. *Let $f(u) = \sum_{r \in \mathcal{K} \cup \{0\}} \alpha_r u^r$ be a polynomial supported on a set $\mathcal{K} \subset \mathbb{Z}^+$ with coefficients in $\mathbb{K}_\infty$. Suppose that α_k is irrational for some $k \in \widetilde{\mathcal{K}}$ (defined as in (14)). Then the sequence $(f(x))_{x \in \mathbb{F}_q[t]}$ is equidistributed in $\mathbb{T}$.*

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

Let $T : \mathbb{K}_\infty \to \mathbb{T}$ be defined as in (1). Using the fact that $a^p = a$ for any $a \in \mathbb{F}_p$, one can show that for any $x \in \mathbb{F}_p[t]$,

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

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

$$e\left(\alpha x^{p^v}\right) = e(T^v(\alpha) x), \tag{17}$$

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

$$\mathcal{I}=\{k\in\mathbb{Z}^+:(k,p)=1 \text{ and } p^v k\in\mathcal{K} \text{ for some } v\in\mathbb{Z}^+\cup\{0\}\}. \tag{18}$$

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

$$S_k(f)=\sum_{\substack{v\geq 0\\ p^v k\in\mathcal{K}}} T^v(\alpha_{p^v k}). \tag{19}$$

Then it follows from (17) that for any $x\in\mathbb{F}_p[t]$,

$$e\left(f(x)\right)=e\left(\sum_{k\in\mathcal{I}}S_k(f)x^k+\alpha_0\right). \tag{20}$$

Since $(k,p)=1$ for any $k\in\mathcal{I}$, we have $\widetilde{\mathcal{I}}=\mathcal{I}$. By Proposition 18, if there exists $k\in\mathcal{I}$ such that $S_k(f)$ is irrational, then

$$\lim_{N\to\infty}\frac{1}{q^N}\left|\sum_{x\in\mathbb{G}_N}e(f(x))\right|=\lim_{N\to\infty}\frac{1}{q^N}\left|\sum_{x\in\mathbb{G}_N}e\left(\sum_{k\in\mathcal{I}}S_k(f)x^k+\alpha_0\right)\right|=0. \tag{21}$$

We note that for any $m\in\mathbb{F}_p[t]\setminus\{0\}$, the above equalities holds with f replaced by mf, where mf is the polynomial $mf(u)=\sum_{r\in\mathcal{K}\cup\{0\}}m\alpha_r u^r$. Therefore, by Theorem 11, we have

Corollary 19. *Let $f(u)=\sum_{r\in\mathcal{K}\cup\{0\}}\alpha_r u^r$ be a polynomial supported on a set $\mathcal{K}\subset\mathbb{Z}^+$ with coefficients in $\mathbb{K}_\infty$. Suppose that for some $k\in\mathcal{I}$, we have*

$$S_k(mf) \text{ is irrational for any } m\in\mathbb{F}_p[t]\setminus\{0\}. \tag{22}$$

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 (22) may not be described in simpler terms. It may also not be necessary for the equidistribution of $(f(x))_{x\in\mathbb{F}_p[t]}$. Regardless, 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, if α_k is irrational, then the condition (22) is satisfied. This simple observation establishes Conjecture 1 in the special case $q=p$. More precisely, we have

Corollary 20. *Let $f(u)=\sum_{r\in\mathcal{K}\cup\{0\}}\alpha_r u^r$ be a polynomial supported on a set $\mathcal{K}\subset\mathbb{Z}^+$ with coefficients in $\mathbb{K}_\infty$. Suppose that α_k is irrational for some $k\in\mathcal{K}^*$ (defined as in (4). 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.** For a set $\mathcal{A}\subset\mathbb{Z}^+$, we define its *upper density*

$$\overline{d}(\mathcal{A})=\lim_{N\to\infty}\frac{\#\mathcal{A}\cap\{1,\ldots,N\}}{N}.$$

We say $\mathcal{A}$ 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 $a-a'\in\mathcal{H}$. In other words, we have

$\mathcal{H}\cap(\mathcal{A}-\mathcal{A})\neq\emptyset$. In the late 1970s, Sárközy [20] and Furstenberg [7] proved independently that the set $\{n^2 : n\in\mathbb{Z}^+\}$ is intersective. Their proofs use the circle method and ergodic theory, respectively. Sárközy went on and proved that the sets $\{n^2-1 : n\in\mathbb{Z}^+\setminus\{1\}\}$ and $\{p-1 : p\in\mathbb{Z}$ is prime$\}$ are also intersective [21]. We refer the reader to a survey paper of the first author [14] 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 [10] 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 $(\bmod 1)$ whenever the sequence $(a_{n+h}-a_n)_{n=1}^{\infty}$ is equidistributed $(\bmod 1)$ for each $h\in\mathcal{H}$. Therefore, van der Corput's difference theorem says that $\mathbb{Z}^+$ is van der Corput, but there are sparser sets which are van der Corput. In [10], 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 [3], Bourgain constructed a set that is intersective but not van der Corput.

Let $\Phi(u)\in\mathbb{Z}[u]$ and consider the set $\{\Phi(n) : n\in\mathbb{Z}\}\cap\mathbb{Z}^+$. We note that for any $g\in\mathbb{Z}^+$, the set of all multiples of g is dense. Therefore, if the set $\{\Phi(n) : n\in\mathbb{Z}\}\cap\mathbb{Z}^+$ is van der Corput (hence intersective), then g divides $\Phi(n)$ for some $n\in\mathbb{Z}$. The following result of Kamae and Mendès France [10] shows that the divisibility condition is not only necessary, but also sufficient.

Proposition 21. *For $\Phi(u)\in\mathbb{Z}[u]\setminus\{0\}$, suppose that Φ has a root $(\bmod g)$ for any $g\in\mathbb{Z}^+$. Then the set $\{\Phi(n) : n\in\mathbb{Z}\}\cap\mathbb{Z}^+$ is van der Corput (hence intersective).*

Given the similarity of $\mathbb{Z}$ and $\mathbb{F}_q[t]$, it is natural to study analogous notions in $\mathbb{F}_q[t]$. For a set $\mathcal{A}\subset\mathbb{F}_q[t]$, we define its *upper density*

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

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 $\mathbb{Z}$ carry over to $\mathbb{F}_q[t]$, and we refer the reader to the Ph.D. thesis of the first author [15, Chapter 2] for an exposition. In particular, in [15, Theorem 2.3.5], it was proved that any van der Corput set in $\mathbb{F}_q[t]$ is intersective. It remains an open 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 our work [16], we obtained intersectivity, in a quantitative sense, for the set $\left\{x^2 : x\in\mathbb{F}_q[t]\right\}\setminus\{0\}$. In a joint work of the first author with Spencer [17], the intersectivity, in a quantitative sense, is also established for the set $\{l+r : l\in\mathbb{F}_q[t]$ is monic and irreducible$\}$ for any fixed $r\in\mathbb{F}_q\setminus\{0\}$. Motivated by Proposition 21, one comes to the following conjecture.

Conjecture 22. *For $\Phi(u)\in\mathbb{F}_q[t][u]\setminus\{0\}$, suppose that Φ has a root $(\bmod g)$ for any $g\in\mathbb{F}_q[t]\setminus\{0\}$. Then the set $\{\Phi(x) : x\in\mathbb{F}_q[t]\}\setminus\{0\}$ is van der Corput (hence intersective).*

Again, the divisibility condition is easily seen to be necessary. Quite surprisingly, the conjecture remains an open problem when the degree of Φ is bigger 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, Leiman and McCutcheon [2], that the set $\{\Phi(x) : x \in \mathbb{F}_q[t]\} \setminus \{0\}$ is intersective. Given our equidistribution theorem, in this section, we make some progress towards Conjecture 22. We will prove the following theorem which is slightly stronger than Theorem 3.

Theorem 23. *Let $\Phi(u) = \sum_{r\in\mathcal{K}\cup\{0\}} a_r u^r$ be a polynomial supported on a set $\mathcal{K} \subset \mathbb{Z}^+$ with coefficients in $\mathbb{F}_q[t]$. Suppose that Φ has a root $\pmod g$ for any $g \in \mathbb{F}_q[t] \setminus \{0\}$. Suppose further that $a_k \neq 0$ for some $k \in \mathcal{K}^*$ (defined as in (4)). Then the set $\{\Phi(x) : x \in \mathbb{F}_q[t]\} \setminus \{0\}$ is van der Corput (hence intersective).*

Remark.

- As a direct consequence of Theorem 23, we see that Conjecture 22 is true whenever the degree of Φ is coprime to p.
- In view of Proposition 18, the condition $a_k \neq 0$ for some $k \in \mathcal{K}^*$ can be relaxed to $a_k \neq 0$ for some $k \in \widetilde{\mathcal{K}}$, where $\widetilde{\mathcal{K}}$ is defined as in (14).

By assuming the stronger conditions that $q = p$ and $\Phi(0) = 0$, we will prove the following result.

Theorem 24. *Let $\Phi(u) \in \mathbb{F}_p[t][u]\setminus\{0\}$ with $\Phi(0) = 0$. Then the set $\{\Phi(x) : x \in \mathbb{F}_p[t]\}\setminus\{0\}$ is van der Corput (hence intersective).*

We remark here that the minor arc estimate in Theorem 15 can be used to prove intersectivity of the set $\{\Phi(x) : x \in \mathbb{F}_q[t]\} \setminus \{0\}$ in Theorem 23 in a quantitative sense, similar to [16, Theorem 3]. However, we opt to use Theorem 2 since the deduction is quicker, and the van der Corput property is a stronger notion than intersectivity.

6.2. **Proofs of Theorem 23 and Theorem 24.** Among the many characterizations of van der Corput sets in $\mathbb{F}_q[t]$, we will be using the following [15, Theorem 2.4.5 (2)]. Let μ be a finite measure on $\mathbb{T}$. We say μ is *continuous* at 0 if $\mu(\{0\}) = 0$. For any $h \in \mathbb{F}_q[t]$, the *Fourier transform*, $\widehat{\mu}$, of μ is defined by

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

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

Theorem 25. (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.*

Proof of Theorem 23. Suppose that $\Phi(u) = \sum_{k\in\mathcal{K}\cup\{0\}} a_r u^r \in \mathbb{F}_q[t][u]$ has a root $\pmod g$ for any $g \in \mathbb{F}_q[t] \setminus \{0\}$. Suppose further that $a_k \neq 0$ for some $k \in \mathcal{K}^*$. Let

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

Let $\alpha \in \mathbb{T}$ be irrational and $g, s \in \mathbb{F}_q[t]$ with $g \neq 0$. By (3), we have

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

We observe that the coefficient of x^k in $(\alpha\Phi(x) + y(x-s)/g)$ is αa_k or $(\alpha a_k + y/g)$, depending on whether $k \neq 1$ or $k = 1$, which in any case is irrational. Therefore, by Theorem 2, for any $y \in \mathbb{G}_{\mathrm{ord}\, g}$, we have

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

Combining the above two equations, it follows that for any irrational $\alpha \in \mathbb{T}$ and $g, s \in \mathbb{F}_q[t]$ with $g \neq 0$,

$$\lim_{N \to \infty} \frac{1}{q^N} \left| \sum_{x \in \mathbb{G}_N} e\left(\alpha \Phi(gx+s)\right) \right| = \lim_{N \to \infty} \frac{1}{q^N} \left| \sum_{\substack{x \in \mathbb{G}_N \\ x \equiv s \pmod{g}}} e\left(\alpha \Phi(x)\right) \right| = 0. \tag{23}$$

For any $M \in \mathbb{Z}^+$, let g_M be the product of all monic polynomials in $\mathbb{G}_M$. Let $s_M \in \mathbb{F}_q[t]$ be a root of $\Phi \pmod{g_M}$. For $\alpha \in \mathbb{T}$, let

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

We now analyze $T_{M,N}(\alpha)$, depending on the rationality of α.
Case 1. Suppose that $\alpha \in \mathbb{T}$ is irrational. By (23), 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. Since $|T_{M,N}(\alpha)| \leq 1$ and the set $\{(\alpha, M) : \alpha \in \mathbb{T} \text{ is rational and } M \in \mathbb{Z}^+\}$ is countable, by a diagonalization process, we can extract a subsequence $N_i \subset \mathbb{Z}^+$ such that the limit $\lim_{i \to \infty} T_{M,N_i}(\alpha)$ exists, for any $M \in \mathbb{Z}^+$ and any rational $\alpha \in \mathbb{T}$. Since s_M is a root of $\Phi \pmod{g_M}$, $\Phi(g_M x + s_M)$ is divisible by g_M. Therefore, for M sufficiently large such that g_M absorbs the denominator of α, we have $T_{M,N}(\alpha) = 1$.
Combining the above two cases, it follows that

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

Let μ be a finite measure on $\mathbb{T}$. By applying the dominated convergence theorem twice, we have

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

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

$$\left|\int_{\mathbb{T}} T_{M,N}(\alpha)d\mu(\alpha)\right| = \left|\sum_{x\in\mathbb{G}_N}\widehat{T_{M,N}}(x)\widehat{\mu}(x)\right| = \left|\widehat{T_{M,N}}(0)\widehat{\mu}(0)\right| = \left|\widehat{T_{M,N}}(0)\right|\mu(\mathbb{T}) \leq \frac{\mu(\mathbb{T})}{q^N}.$$

Combining the above two inequalities, it follows that $\mu(\{0\})=0$ for any finite measure μ on $\mathbb{T}$ with $\widehat{\mu}$ vanishing on $\mathcal{H}$. Therefore, $\mathcal{H}$ is van der Corput. $\square$

Proof of Theorem 24. Suppose that $q=p$ and $\Phi(u)=\sum_{r\in\mathcal{K}} a_r u^r\in\mathbb{F}_p[t][u]$. Let

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

Let $\mathcal{I}$ and $S_k(\Phi)$ $(k\in\mathcal{I})$ be defined as in (18) and (19), respectively. We have seen in (20) that

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

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

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

Let

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

From (21), for any $\alpha\in\mathcal{Q}$, we have

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

On the other hand, if $\alpha\notin\mathcal{Q}$, then $S_k(\alpha\Phi)$ is rational for any $k\in\mathcal{I}$. Since the rationals are countable, the set of all polynomials of the form $\sum_{k\in\mathcal{I}} S_k(\alpha\Phi)y^k$ $(\alpha\notin\mathcal{Q})$ is countable ($\mathbb{T}\setminus\mathcal{Q}$ need not be countable). Since $|T_{M,N}(\alpha)|\leq 1$, by a diagonalization process, we can extract a subsequence $N_i\subset\mathbb{Z}^+$ such that the limit $\lim_{i\to\infty} T_{M,N_i}(\alpha)$ exists for any $M\in\mathbb{Z}^+$ and any $\alpha\notin\mathcal{Q}$. Then similarly to Case 2 of the proof of Theorem 23, for M sufficiently large, we have $T_{M,N}(\alpha)=1$ for any $\alpha\notin\mathcal{Q}$. It follows that

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

By arguing as in the proof of Theorem 23, we see that $\mu(\{0\})=0$ for any finite measure μ on $\mathbb{T}$ with $\widehat{\mu}$ vanishing on $\mathcal{H}$. Therefore, $\mathcal{H}$ is van der Corput. $\square$

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

7.1. **Background and statement of results.** 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 $nY = \{ny : y \in Y\} \subset \mathbb{R}/\mathbb{Z}$ for some $n \in \mathbb{Z}$. In 1979, Glasner [8] proved that for any infinite subset Y of $\mathbb{R}/\mathbb{Z}$ and any $\epsilon > 0$, there exists $n \in \mathbb{Z}$ such that the dilation nY is ϵ-dense in $\mathbb{R}/\mathbb{Z}$. It turns out that one can even restrict n to be an element of relatively sparse subsets 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 $n \in \mathcal{H}$ such that nY is ϵ-dense in $\mathbb{R}/\mathbb{Z}$. In their paper [1], 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 $\{\Phi(n) : n \in \mathbb{Z}\}$ is Glasner. By using harmonic analysis, Alon and Peres obtained their results quantitatively, namely that 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 $|Y|$ is sufficiently large depending on ϵ and $\mathcal{H}$.

One can define the analogous notion of Glasner sets 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 $x \in \mathcal{H}$ such that the dilation xY is q^{-M}-dense in $\mathbb{T}$. In view of of Alon and Peres' result, 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 Alon and Peres' result 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). Then Y is infinite (indeed uncountable). We have seen in Example 1.1 that for any $x \in \mathbb{F}_q[t]$, we have $\operatorname{res}(x^p\alpha) = 0$. This shows that the set $\{x^p : x \in \mathbb{F}_q[t]\}$ 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 $T(\alpha) + \alpha = 0$. Again, it can be seen that Y is infinite (indeed uncountable). Then for any $x \in \mathbb{F}_q[t]$, we have $\operatorname{res}((x^p + x)\alpha) = \operatorname{res}((T(\alpha) + \alpha)x) = 0$. This shows that the set $\{x^p + x : x \in \mathbb{F}_q[t]\}$ 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 make a conjecture similar to Conjecture 1 which says that Examples 7.1 and 7.2 encapsulates all the obstructions that prevent a polynomial sequence in $\mathbb{F}_q[t]$ from being Glasner. Such a conjecture would follow from Conjecture 1, and we don't expect to prove the former before establishing the latter. However, given Theorem 2, we can prove the following.

Theorem 4. *Let $\Phi(u) = \sum_{r \in \mathcal{K}\cup\{0\}} a_r u^r$ be a polynomial supported on a set $\mathcal{K} \subset \mathbb{Z}^+$ with coefficients in $\mathbb{F}_q[t]$. Suppose that $a_k \neq 0$ for some $k \in \mathcal{K}^*$ (defined as in (4)) and $k > 1$. Then the set $\{\Phi(x) : x \in \mathbb{F}_q[t]\}$ is Glasner.*

Notice the extra requirement $k > 1$ in Theorem 4, in contrast with Theorem 3. By adapting the harmonic-analytic approach of Alon and Peres in [1], we will prove the following quantitative version of Theorem 4 which is analogous to Alon-Peres' bound [1, Theorem 6.3].

Theorem 26. *Let $\Phi(u) = \sum_{r\in\mathcal{K}\cup\{0\}} a_r u^r$ be a polynomial supported on a set $\mathcal{K} \subset \mathbb{Z}^+$ with coefficients in $\mathbb{F}_q[t]$. Suppose that $a_k \neq 0$ for some $k \in \mathcal{K}^*$ (defined as in (4)) and $k > 1$. Then there exists a constant C depending on Φ such that, for any $M > 0$, there is a dilation of the form $\Phi(x)Y$ of Y that is q^{-M}-dense, whenever*

$$|Y| \gg_\Phi q^{CM}.$$

Remark.

- As a direct consequence of Theorem 4, we see that the set of values of Φ is Glasner whenever $\deg\Phi > 1$ and $(\deg\Phi, p) = 1$.
- In view of Proposition 18, the condition $a_k \neq 0$ for some $k \in \mathcal{K}^*$ can be relaxed to $a_k \neq 0$ for some $k \in \widetilde{\mathcal{K}}$, where $\widetilde{\mathcal{K}}$ is defined as in (14).

7.2. **Proof of Theorem 26.** We first derive the following lemma from Theorem 15. It is analogous to Hua's classical bound on exponential sums over polynomials in the integers.

Lemma 27. *Let $\Phi(u) = \sum_{r\in\mathcal{K}\cup\{0\}} a_r u^r$ be a polynomial supported on a set $\mathcal{K} \subset \mathbb{Z}^+$ with coefficients in $\mathbb{F}_q[t]$. Suppose that $a_k \neq 0$ for some $k \in \mathcal{K}^*$ (defined as in (4)) and $k > 1$. Let C_k, c_k be constants given by Theorem 15. Then for any $g \in \mathbb{F}_q[t] \setminus \{0\}$ and any $\epsilon > 0$ we have*

$$\left|\sum_{x\in\mathbb{G}_{\mathrm{ord}\, g}} e\left(\frac{\Phi(x)}{g}\right)\right| \ll_{\mathcal{K},\epsilon,q} |(g,a_k)|^{1/C_k} |g|^{1-1/C_k+\epsilon}. \tag{24}$$

Proof. Put $N = \operatorname{ord} g$ and $M = \operatorname{ord}(g, a_k)$. Note that (24) is trivial if $(1/C_k - \epsilon)N \leq M/C_k$. Thus we can assume that $(1/C_k - \epsilon)N > M/C_k$. Let $\eta = (1/C_k - \epsilon)N - M/C_k > 0$. Suppose for a contradiction that

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

By Theorem 15, for N sufficiently large, there exist $b, h \in \mathbb{F}_q[t]$ such that

$$\operatorname{ord}\left(h\frac{a_k}{g} - b\right) < -kN + \epsilon N + C_k\eta \qquad \text{and} \qquad \operatorname{ord} h < \epsilon N + C_k\eta. \tag{25}$$

Note that

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

Therefore, g does not divide $(g, a_k h)$ and $h\frac{a_k}{g}$ in its reduced form is a fraction with denominator $\frac{g}{(g,a_k h)}$, whose order is ≥ 1. We make the trivial observation that for any $x, y, z \in \mathbb{F}_q[t]$ with $(x, y) = 1$ and $\operatorname{ord} y \geq 1$, then

$$\operatorname{ord}\left(\frac{x}{y} - z\right) \geq -\operatorname{ord} y.$$

Therefore,

$$\operatorname{ord}\left(h\frac{a_k}{g} - b\right) \geq \operatorname{ord}(g, a_k h) - \operatorname{ord} g \geq M - N. \tag{26}$$

Combining (26) and (25), we have

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

which is a contradiction since $k>1$. □

We also need the following analog of [1, Proposition 1.3].

Lemma 28. *Let $Y=\{y_1,\dots,y_k\}$ be a set of k distinct elements in $\mathbb{T}$. For each $g\in\mathbb{F}_q[t]\backslash\{0\}$, let h_g be the number of pairs (i,j) with $1\leq i,j\leq k, i\neq j$ with $g(y_i-y_j)\in\mathbb{F}_q[t]$. Let $H_L=\sum_{g\in\mathbb{G}_L\backslash\{0\}}h_g$. Then we have the bound*

$$H_L\leq kq^{2L}.$$

Proof. For each $1\leq i\leq k$ and $g\in\mathbb{G}_L\backslash\{0\}$, the number of j such that $g(y_i-y_j)\in\mathbb{F}_q[t]$ is at most $|g|\leq q^L$. Summing up this inequality over all i and g gives the desired estimate. □

Proof of Theorem 26. We will prove Theorem 26 by contraposition. Suppose that a set $Y=\{y_1,\dots,y_k\}\subset\mathbb{T}$ has the property that $\Phi(x)Y$ is not q^{-M}-dense for any $x\in\mathbb{F}_q[t]$, we will derive an upper bound for k.

For each $x\in\mathbb{F}_q[t]$, since $\Phi(x)Y$ is not q^{-M}-dense in $\mathbb{T}$, there is $\xi_x\in\mathbb{T}$ such that all elements of $\Phi(x)Y$ lie outside of the cylinder set $\{\xi\in\mathbb{T}:|\xi-\xi_x|<q^{-M}\}$. In other words, for all $1\leq i\leq k$, we have

$$\mathrm{ord}\ \{\Phi(x)y_i-\xi_x\}\geq -M.$$

By (2), we have

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

Since the above equality holds for any x and i, we have, for any $N>0$

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

Therefore, by removing the term $z=0$, we get

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

By the Cauchy-Schwarz inequality, we have

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

Therefore,

$$k^2 \le \sum_{z \in \mathbb{G}_M \setminus \{0\}} \sum_{i,j=1}^{k} q^{M-N} \sum_{x \in \mathbb{G}_N} e\left(z\Phi(x)(y_i - y_j)\right).$$

Since this is true for any N, we have

$$k^2 \le \sum_{z \in \mathbb{G}_M \setminus \{0\}} \sum_{i,j=1}^{k} \lim_{N \to \infty} \left| q^{M-N} \sum_{x \in \mathbb{G}_N} e\left(z\Phi(x)(y_i - y_j)\right) \right|. \tag{27}$$

Let $z \in \mathbb{G}_M \setminus \{0\}$ maximize the expression inside the first sum, and we fix z from now on. Then we have

$$k^2 \le q^{2M} \sum_{i,j=1}^{k} \lim_{N \to \infty} \left| \frac{1}{q^N} \sum_{x \in \mathbb{G}_N} e\left(z\Phi(x)(y_i - y_j)\right) \right|. \tag{28}$$

Let us now analize the limit $\lim_{N\to\infty} \left| \frac{1}{q^N} \sum_{x \in \mathbb{G}_N} e\left(z\Phi(x)(y_i - y_j)\right) \right|$, depending on the rationality of $(y_i - y_j)$.

Case 1. If $i = j$, then this is 1.

Case 2. If $(y_i - y_j)$ is irrational, then this is 0 by Theorem 2.

Case 3. If $(y_i - y_j)$ is a non-zero rational, we write $(y_i - y_j) = \frac{a}{g}$ as a reduced fraction. Then as a reduced fraction, $z(y_i - y_j) = \frac{a'}{g'}$ where $g' = \frac{g}{\gcd(z,g)}$. In particular, we have $|g'| \ge |g|/q^M$. By Lemma 27, we have

$$\begin{aligned}
\lim_{N \to \infty} \left| \frac{1}{q^N} \sum_{x \in \mathbb{G}_N} e\left(z\Phi(x)(y_i - y_j)\right) \right| &= \left| \frac{1}{|g'|} \sum_{x \in \mathbb{G}_{\operatorname{ord} g'}} e\left(\frac{a'\Phi(x)}{g'} \right) \right| \\
&\ll_{\mathcal{K}} |g'|^{-1/(2C_k)} |\gcd(g', a'a_k)|^{1/C_k} \\
&= |g'|^{-1/(2C_k)} |\gcd(g', a_k)|^{1/C_k} \\
&\le |g'|^{-1/(2C_k)} |a_k|^{1/C_k} \\
&\ll_{\Phi} |g|^{-1/(2C_k)} q^M.
\end{aligned} \tag{29}$$

For each $g \in \mathbb{F}_q[t] \setminus \{0\}$, let $\widetilde{h}_g$ be the number of pairs (i,j) such that $1 \le i,j \le k$, $i \ne j$ and $(y_i - y_j)$ is a reduced fraction with denominator g. From the above analysis and (28) we have the estimate

$$k^2 \ll_{\Phi} kq^{2M} + q^{2M} \sum_{g \in \mathbb{F}_q[t] \setminus \{0\}} |g|^{-\frac{1}{2C_k}} \widetilde{h}_g. \tag{30}$$

Next we estimate the right hand side of (30) using Lemma 28. For any $L \in \mathbb{Z}^+$, let

$$\widetilde{H}_L = \sum_{g \in \mathbb{G}_L \setminus \{0\}} \widetilde{h}_g.$$

Note that $\widetilde{H}_L \le H_L \le kq^{2L}$, where H_L is the quantity defined in Lemma 28. We also have the trivial bound $\widetilde{H}_L \le k^2$ for any L. Let $L_0 = \left[\frac{\log_q k}{2}\right]$. By partial summation, we have

$$\begin{aligned}
&\sum_{g\in\mathbb{F}_q[t]\setminus\{0\}} |g|^{-1/(2C_k)}\widetilde{h}_g \\
&= \sum_{L=1}^{\infty} q^{-L/(2C_k)}\left(H_{L+1} - H_L\right) \\
&= \sum_{L=2}^{\infty} H_L\left(q^{-(L-1)/(2C_k)} - q^{-L/(2C_k)}\right) \qquad \text{(since } H_1 = 0) \\
&\le k^2 \sum_{L=L_0+1}^{\infty}\left(q^{-(L-1)/(2C_k)} - q^{-L/(2C_k)}\right) + \sum_{L=2}^{L_0} kq^{2L}\left(q^{-(L-1)/(2C_k)} - q^{-L/(2C_k)}\right) \\
&\ll_q k^2 q^{-L_0/(2C_k)} + kq^{L_0(2-1/(2C_k))} \\
&\ll_q k^{2(1-1/(4C_k))}
\end{aligned}$$

Combining (30) with the above inequality, we obtain that

$$k^2 \ll_\Phi kq^{2M} + q^{2M}k^{2(1-1/4C_k)}$$

which implies that $k \ll_\Phi q^{4C_kM}$. This completes the proof of Theorem 26. □

References

[1] N. Alon, Y. Peres, *Uniform dilations*, Geometric & Functional Analysis 2 (1992), 1–28.
[2] V. Bergelson, A. Leibman, R. McCutcheon, *Polynomial Szemerédi theorem for countable modules over integral domains and finite fields*, Journal d′ Analyse Mathématique 95 (2005), 243–296.
[3] J. Bourgain, *Ruzsa's problem on sets of recurrence*, Israel J. Math. 59 (1987), 150–166.
[4] L. Carlitz, *Diophantine approximation in fields of characteristic* p, Trans. Amer. Math. Soc. 72 (1952), 187–208.
[5] A. Dijksma, *Uniform distribution of polynomials over* $GF\{q,x\}$ *in* $GF[q,x]$*. II.*, Indag. Math. 32 (1970), 187–195.
[6] W. J. Ellison, *Les nombres premiers*, Hermann, Paris (1975).
[7] H. Furstenberg, *Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions*, J. Analyse Math. 31 (1977), 204–256.
[8] S. Glasner, *Almost periodic sets and measures on the torus*, Israel J. Math. 32 (1979), 161–172.
[9] C.-N. Hsu, *A large sieve inequality for rational function fields*, J. Number Theory 58 (1996), 267–287.
[10] T. Kamae & M. Mendès France, *Van der Corput's difference theorem*, Israel J. Math. 31 (1978), 335–342.
[11] R. M. Kubota, *Waring's problem for* $\mathbb{F}_q[x]$, Dissertationes Math. (Rozprawy Mat.) 117 (1974), 60pp.
[12] L. Kuipers, H. Niederreiter, *Uniform distribution of sequences*, John Wiley & Sons Inc. (1974), reprinted by Dover Publishing (2006).
[13] W. Kuo, Y.-R. Liu, X. Zhao, *Multidimensional Vinogradov-type estimates in function fields*, to appear in Canadian Journal of Mathematics.
[14] T. H. Lê, *Problems and results on intersective sets*, to appear in Proceedings of Combinatorial and Additive Number Theory 2011.
[15] T. H. Lê, *Topics in arithmetic combinatorics in function fields*, PhD Thesis, UCLA (2010).
[16] T. H. Lê, Y.-R Liu, *On sets of polynomials whose difference set contains no squares*, to appear in Acta Arithmetica.

[17] T. H Lê & C. V. Spencer, *Difference sets and the irreducibles in function fields*, B. Lond. Math. Soc. 43 (2011), 347–358.
[18] Y.-R. Liu, T. Wooley, *Waring's problem in function fields*, J. Reine Angew. Math. 638 (2010), 1–67.
[19] Y.-R. Liu, T. Wooley, *Vinogradov's mean value theorem in function fields*, in preparation.
[20] A. Sárközy, *On difference sets of sequences of integers, I.*, Acta Math. Acad. Sci. Hungar. 31 (1978), 125–149.
[21] A. Sárközy, *On difference sets of sequences of integers, III.*, Acta Math. Acad. Sci. Hungar. 31 (1978), 355–386.
[22] W. M. Schmidt, *On continued fractions and Diophantine approximation in power series fields*, Acta Arith. 95 (2000), 139–165.
[23] J. van der Corput, *Diophantische Ungleichungen. I. Zur Gleichverteilung Modulo Eins*, Acta Mathematica (Springer Netherlands) 56 (1931), 373–456.
[24] R. C. Vaughan, *The Hardy-Littlewood method*, Cambridge University Press, 2nd edition (1997).
[25] R. C. Vaughan & T. D. Wooley, *Waring's problem: a survey*, Number Theory for the Millenium, Vol. III , A. K. Peters (2002), 301–340.
[26] I. M. Vinogradov, *Method of trigonometrical sums in the theory of numbers*, Interscience Publishers (1954), reprinted by Dover Publications (2004).
[27] H. Weyl, *Über die Gleichverteilung von Zahlen mod. Eins*, Math. Ann. 77 (1916), 313–352.

T. H. Lê, Department of Mathematics, The University of Texas at Austin, 1 University Station, C1200 Austin, Texas 78712

E-mail address: `leth@math.utexas.edu`

Y.-R. Liu, Department of Pure Mathematics, Faculty of Mathematics, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1

E-mail address: `yrliu@math.uwaterloo.ca`