Some additive results in $\mathbb{F}_q[t]$

by

Shuntaro Yamagishi

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Pure Mathematics

Waterloo, Ontario, Canada, 2015

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

We collected several results in $\mathbb{Z}$ of additive number theory and translated to results in $\mathbb{F}_q[t]$. The results we collected are related to slim exceptional sets and the asymptotic formula in Waring's problem, a diophantine approximation of polynomials over $\mathbb{Z}$ satisfying divisibility conditions, and the problem of Sidon regarding the existence of certain thin sequences.

Acknowledgements

First of all, I would like to thank my supervisor Yu-Ru Liu for all of her help, guidance, and patience throughout for this would not have been possible otherwise. I would also like to thank Michael O. Rubinstein for his guidance during my Master's and at the beginning of my PhD. I am grateful for the opportunities I had to work on interesting projects with Kathryn E. Hare and Wentang Kuo. I am also thankful for Chantal David, Kevin Hare, David McKinnon, and David Jao for being on the examining committee of my thesis.

There are so many amazing people I met while I was in Waterloo that I would like to thank, but this space is too small to list them all... First of all, I want to thank my office mate Michael Hartz and my roommate Matthew Beckett for all of their support. I want to thank Stanley Yao Xiao for being such a good fellow grad student in number theory. I also want to thank Jena Durastanti, Bart Fu, and Neeraj Thomas for lots of fun memories at Waterloo. Alejandra Vicente-Colmenares and Omar Leon Sanchez had been really great to me as well. I also want to thank the Cuban Salsa club, the Mambo Club, and the Muay Thai club at University of Waterloo, and everyone from these clubs for making my experience in Waterloo so enjoyable. There are so many other people I want to thank, Lis D'Alessio, Nancy Maloney, Pavlina Penk, Shonn Martin, and Racehl Hull for all of their help, Andrew Poon, Daniel Ivan, Mohammed Hamdy, Suazzane Findleton, Phil Lamoureux, Ryan (93) Hutchins, Ben Smith, Suzie, Rishikesh, Duc Khiem Huynh, Andy Yang, Melissa Tardibuono, Rog and Pam, Cassie, Marie-Sarah, Wu, Gary, Michael Coons, ... the list just keeps going, so I am going to stop around here.

Dedication

I would like to dedicate this thesis to my family, Sumiko, Toshiyuki and Ginjiro Yamagishi, my uncle Takayuki (Byron) Yamagishi, and my grand parents Taka and Sadao Kojima, and Hiroko and Teiji Yamagishi.

Table of Contents

1 Introduction **1**

2 Waring's problem in function fields **3**

2.1 Introduction 3

2.2 Preliminary 8

2.3 Technical Lemmas 14

2.3.1 Case $p \nmid (k-1)$ 16

2.3.2 Case $k = mp^b + 1$ with $m > 1$ 17

2.4 A bound on the minor arcs 22

2.4.1 Cases $p \nmid (k-1)$ and $p = mk^b + 1$, $m > 1$ 22

2.4.2 Case $k = p^b + 1$ 29

2.5 Weyl Differencing 33

2.6 Asymptotic Formula and $\tilde{G}_q(k)$ 35

2.7 Slim Exceptional Sets 41

3 Diophantine approximation of polynomials over $\mathbb{F}_q[t]$ satisfying a divisibility condition **50**

3.1 Introduction 50

3.2 Preliminaries 54

3.3 Basic Linear Algebra 59

3.4 Proof of the Main Results 65

4 On a problem of Sidon for polynomials over finite fields 72

4.1 Introduction 72

4.2 Preliminaries 74

4.3 Probability Space $(\Omega, \mathcal{M}, P)$ 76

4.4 Technical Lemmas 78

4.5 Proof of Theorem 4.8 87

4.6 Proof of Theorem 4.9 89

4.7 Proof of Theorem 4.10 91

References 92

Chapter 1

Introduction

An important topic in number theory is the study of the similarity between the ring of rational integers $\mathbb{Z}$, and the polynomial rings in a single variable $\mathbb{F}_q[t]$, defined over $\mathbb{F}_q$, the finite field of q elements. The analogy between $\mathbb{Z}$ and $\mathbb{F}_q[t]$ is an instance of a more general analogy that relates number fields to function fields. In some cases, a proof over function fields can inspire ideas to solve analogous problems over number fields, or results in functions fields can be applied to answer questions in $\mathbb{Z}$. Even though the characteristic of $\mathbb{Z}$ is zero, and that of $\mathbb{F}_q[t]$ is equal to the characteristic of $\mathbb{F}_q$, a positive prime number that we denote by p, the two rings resemble one another in many ways. We are interested in translating conclusions from $\mathbb{Z}$ to $\mathbb{F}_q[t]$ and obtain results that are uniform in characteristic.

In this thesis, we collect several results in $\mathbb{Z}$ of additive number theory and translate them into results in $\mathbb{F}_q[t]$. The results we collected are related to slim exceptional sets and the asymptotic formula in Waring's problem, a diophantine approximation of polynomials over $\mathbb{Z}$ satisfying divisibility conditions, and the problem of Sidon regarding the existence of certain thin sequences, treated in Chapters 2, 3, and 4, respectively. As these three topics are fairly distinct, we only give a brief introduction of them here and postpone the detailed introduction to the corresponding chapters. We also made these three chapters self contained, in a sense that they are separate from each other. In other words, a reader can only read the chapters of interest instead of having to have to go through the entire thesis. Thus we emphasize here that notation in one chapter does not necessarily carry over to another chapter.

In Chapter 2, we consider Waring's problem in $\mathbb{F}_q[t]$. Let $\widetilde{G}_q(k)$ be the least integer t_0 with the property that for all $s \geq t_0$, the expected asymptotic formula in Waring's problem for $\mathbb{F}_q[t]$ is true for sums of s k-th powers of polynomials in $\mathbb{F}_q[t]$. We derive a minor arc bound from Vinogradov-type estimates and obtain bounds on $\widetilde{G}_q(k)$ that are quadratic in k, in fact linear in k in some special cases, when $p \nmid k$, in contrast to the bounds that are exponential in k available when $k < p$. We also obtain estimates related to slim exceptional sets associated to the asymptotic formula.

Polynomials over $\mathbb{Z}$ which have a root modulo n for every $n \in \mathbb{N}$ are known as intersective polynomials [13]. In Chapter 3, we prove an estimate for fractional parts of polynomials over $\mathbb{F}_q[t]$ satisfying a certain divisibility condition analogous to that of intersective polynomials in the case of integers. We then extend our result to consider linear combinations of such polynomials as well.

We use probabilistic methods in Chapter 4. Let ω be a sequence of positive integers. Given a positive integer n, we define

$$r_n(\omega) = |\{(a,b) \in \mathbb{N} \times \mathbb{N} \colon a, b \in \omega, a+b=n, 0<a<b\}|.$$

S. Sidon conjectured that there exists a sequence ω such that $r_n(\omega) > 0$ for all n sufficiently large and, for all $\epsilon > 0$,

$$\lim_{n\to\infty} \frac{r_n(\omega)}{n^\epsilon} = 0.$$

P. Erdős proved this conjecture by showing the existence of a sequence ω of positive integers such that

$$\log n \ll r_n(\omega) \ll \log n.$$

In Chapter 4, we prove an analogue of this conjecture in $\mathbb{F}_q[t]$. More precisely, let ω be a sequence in $\mathbb{F}_q[t]$. Given a polynomial $h \in \mathbb{F}_q[t]$, we define

$$r_h(\omega) = |\{(f,g) \in \mathbb{F}_q[t] \times \mathbb{F}_q[t] : f, g \in \omega, f+g=h, \deg f, \deg g \leq \deg h, f \neq g\}|.$$

We show that there exists a sequence ω of polynomials in $\mathbb{F}_q[t]$ such that

$$\deg h \ll r_h(\omega) \ll \deg h$$

for $\deg h$ sufficiently large.

Chapter 2

Waring's problem in function fields

2.1 Introduction

Waring's problem is regarding the representation of a natural number as a sum of integer powers. More precisely, given $n, s, k \in \mathbb{N}$, $k \geq 2$, we let

$$R_{s,k}(n) = \#\{(x_1, ..., x_s) \in \mathbb{N}^s : x_1^k + ... + x_s^k = n,\ x_i \leq n^{1/k}\ (1 \leq i \leq s)\},$$

and we consider the smallest number s such that $R_{s,k}(n) > 0$. Let $G(k)$ be the smallest integer s such that every *sufficiently large* natural number n satisfies $R_{s,k}(n) > 0$. Using the methods of smooth numbers and efficient differencing, Wooley [22, 23] proved that for k sufficiently large,

$$G(k) \leq k(\log k + \log\log k + O(1)).$$

One can also ask a more 'refined' question by considering the asymptotic formula of $R_{s,k}(n)$. As stated in [25], by a heuristic application of the Hardy-Littlewood circle method, one expects that when $k \geq 3$ and $s \geq k+1$,

$$R_{s,k}(n) = \frac{\Gamma(1+1/k)^s}{\Gamma(s/k)} \mathfrak{S}_{s,k}(n) n^{\frac{s}{k}-1} + o(n^{\frac{s}{k}-1}), \tag{2.1}$$

where

$$\mathfrak{S}_{s,k}(n) = \sum_{a=1}^{\infty} \sum_{\substack{a=1 \\ (a,q)=1}}^{\infty} \left(\frac{1}{q} \sum_{r=1}^{q} e^{2\pi i (ar^k/q)} \right)^s e^{-2\pi i (na/q)}.$$

We note that subject to modest congruence conditions on n, one has $1 \ll \mathfrak{S}_{s,k}(n) \ll n^{\varepsilon}$ [21, Chapter 4]. Let $\widetilde{G}(k)$ be the least integer t_0 with the property that, for all $s \geq t_0$, and all sufficiently large natural numbers n, one has the asymptotic formula (2.1). As a consequence of his recent work concerning Vinogradov's mean value theorem, Wooley has significantly improved estimates on $\widetilde{G}(k)$ [24, 25, 26]. In particular, it was proved in [26] that $\widetilde{G}(k) \leq 2k^2 - 2k - 8$ $(k \geq 6)$.

In this chapter, we consider the asymptotic Waring's problem over $\mathbb{F}_q[t]$, where $\mathbb{F}_q$ is a finite field of q elements. We later define $\widetilde{G}_q(k)$, an analgoue of $\widetilde{G}(k)$ over $\mathbb{F}_q[t]$, and establish bounds on it. As the function field analogue of Wooley's work on Vinogradov's mean value theorem [24] has been established in [16] and its multidimensional version in [10], it is natural to consider its consequences in improving the number of variables required to establish the asymptotic formula in Waring's problem over $\mathbb{F}_q[t]$. Here we accomplish this task by taking the approach of [25].

Before we can state our main results, we need to introduce notation, some of which we paraphrase from the material in introduction of [15]. We denote the characteristic of $\mathbb{F}_q$, a positive prime number, by $\text{ch}(\mathbb{F}_q) = p$. Unless we specify otherwise, we always assume p to be the characteristic of $\mathbb{F}_q$ even if it is not explicitly stated so. Let k be an integer with $k \geq 2$, let $s \in \mathbb{N}$, and consider a polynomial $n \in \mathbb{F}_q[t]$. We are interested in the representation of n of the form

$$n = x_1^k + x_2^k + \dots + x_s^k, \tag{2.2}$$

where $x_i \in \mathbb{F}_q[t]$ $(1 \leq i \leq s)$. It is possible that a representation of the shape (2.2) is obstructed for every natural number s. For example, if the characteristic p of $\mathbb{F}_q$ divides k, then $x_1^k + x_2^k + \dots + x_s^k = \left(x_1^{k/p} + x_2^{k/p} + \dots + x_s^{k/p}\right)^p$, and thus n necessarily fails to admit a representation of the shape (2.2) whenever $n \notin \mathbb{F}_q[t^p]$, no matter how large s may be. In order to accommodate this and other intrinsic obstructions, we define $\mathbb{J}_q^k[t]$ to be the additive closure of the set of k-th powers of polynomials in $\mathbb{F}_q[t]$, and we restrict attention to those n lying in the subring $\mathbb{J}_q^k[t]$ of $\mathbb{F}_q[t]$. It is also convenient to define $\mathbb{J}_q^k$ to be the additive closure of the set of k-th powers of elements of $\mathbb{F}_q$.

Given $n \in \mathbb{J}_q^k[t]$, we say that n is an *exceptional element* of $\mathbb{J}_q^k[t]$ when its leading coefficient lies in $\mathbb{F}_q \backslash \mathbb{J}_q^k$, and in addition k divides $\deg n$. As explained in [15], the strongest constraint on the degrees of the variables that might still permit the existence of a representation of the shape (2.2) is plainly $\deg x_i \leq \lceil (\deg n)/k \rceil$ $(1 \leq i \leq s)$. When $p < k$, however, it is possible that $\mathbb{J}_q^k$ is not equal to $\mathbb{F}_q$, and then the leading coefficient of n need not be an element of $\mathbb{J}_q^k$. If k divides $\deg n$, so that n is an exceptional polynomial, such circumstances obstruct the existence of a representation (2.2) of n with variables x_i satisfying the above constraint on their degrees. For these reasons, following [15], we define $P = P_k(n)$ by setting

$$P = \begin{cases} \left\lceil \frac{\deg n}{k} \right\rceil, & \text{if } n \text{ is not exceptional,} \\ \frac{\deg n}{k} + 1, & \text{if } n \text{ is exceptional.} \end{cases}$$

In particular, when n is not exceptional, then P is the unique integer satisfying $k(P-1) < \deg n \leq kP$. We say that n admits a *strict representation* as a sum of s k-th powers when for some $x_i \in \mathbb{F}_q[t]$ with $\deg x_i \leq P_k(n)$ $(1 \leq i \leq s)$, the equation (2.2) is satisfied.

For notational convenience, let $X = X_k(n) := P_k(n) + 1$, and we define $I_X := \{x \in \mathbb{F}_q[t] : \deg x < X\}$. For n a polynomial in $\mathbb{F}_q[t]$, we denote $R_{s,k}(n)$ to be the number of strict representations of n, in other words

$$R_{s,k}(n) = \#\{(x_1, ..., x_s) \in (I_X)^s : x_1^k + ... + x_s^k = n\}.$$

Though it is not explicit in the notation, $R_{s,k}(n)$ does depend on q. Suppose the leading coefficient of the polynomial n is $c(n)$. We define $b = b(n)$ to be $c(n)$ when k divides $\deg n$ and n is not exceptional, and otherwise we set $b(n)$ to be 0. In addition, we write $J_\infty(n) = J_\infty(n; q)$ for the number of solutions of the equation $y_1^k + ... + y_s^k = b$ with $(y_1, ..., y_s) \in \mathbb{F}_q^s \backslash \{\mathbf{0}\}$. Analogously to the case of integers, one expects the following asymptotic formula

$$R_{s,k}(n) = \mathfrak{S}_{s,k}(n) J_\infty(n) q^{(s-k)P} + o\left(q^{(s-k)P}\right), \tag{2.3}$$

where

$$\mathfrak{S}_{s,k}(n) = \sum_{\substack{g \in \mathbb{F}_q[t] \\ g \text{ is monic}}} \frac{1}{q^{s(\deg g)}} \sum_{\substack{\deg a < \deg g \\ (a,g)=1}} \left(\sum_{\deg r < \deg g} e(ar^k/g) \right)^s e(-na/g),$$

to hold whenever s is sufficiently large with respect to k. We postpone the definition of the exponential function $e(\cdot)$ to Section 2.2. By making the circle method applicable over $\mathbb{F}_q[t]$, the following theorem was proved in [19, Theorem 30]. We note that the theorem stated below is slightly different from the statement of [19, Theorem 30]. The reason for this difference is explained in the paragraph before Theorem 2.9 on page 10.

Theorem 2.1 (Theorem 30, [19]). *Suppose $3 \leq k < p$ and $s \geq 2^k + 1$. Let $n \in \mathbb{F}_q[t]$. Then there exists $\epsilon > 0$ such that the following asymptotic formula holds,*

$$R_{s,k}(n) = \mathfrak{S}_{s,k}(n) J_\infty(n) q^{(s-k)P} + O\left(q^{(s-k-\epsilon)P}\right), \tag{2.4}$$

where

$$1 \ll \mathfrak{S}_{s,k}(n) J_\infty(n) \ll 1. \tag{2.5}$$

Note that the implicit constants in the theorem may depend on k, s, and q, where the constant in (2.4) may also depend on ϵ, but they are independent of n and P.

We denote $\widetilde{G}_q(k)$ to be the least integer t_0 with the property that, for all $s \geq t_0$, and all $n \in \mathbb{J}_q^k[t]$ with $\deg n$ sufficiently large, one has the above asymptotic formula (2.3). Thus, in this language we have the following corollary as an immediate consequence of Theorem 2.1, except for the case $k = 2$. (The estimate on $\widetilde{G}_q(2)$ is treated in the paragraph after the proof of Theorem 2.9 on page 11.)

Corollary 2.2. *Suppose $2 \leq k < p$. Then we have*

$$\widetilde{G}_q(k) \leq \begin{cases} 2^k + 1, & \text{if } k \geq 3, \\ 5, & \text{if } k = 2. \end{cases}$$

It is worth mentioning that one of the main advantages of using Vinogradov-type estimates established in [10] or [16] is that we can avoid the use of Weyl differencing as the primary tool during the computation of minor arc bounds, which is the source of the restriction $k < p$ in Theorem 2.1 and Corollary 2.2. Thus, via Vinogradov-type estimates we can obtain an estimate for $\widetilde{G}_q(k)$ for a larger range of k, which is for all k not divisible by p.

We are now ready to state our main results. To avoid clutter in the exposition, we present the cases $k > p$ and $k < p$ separately. When $k > p$, as a result of our approach we further consider three cases, $p \nmid (k-1)$, $k = p^b + 1$, and $k = mp^b + 1$, where $b, m \in \mathbb{N}$ and $p \nmid m$. Throughout the chapter, whenever we write $k = mp^b + 1$ we are assuming $b, m \in \mathbb{N}$ and $p \nmid m$, even when these conditions are not explicitly stated.

Theorem 2.3. *Let $k \geq 3$ be an integer, where $p \nmid k$. Suppose $k > p$, then we have*

$$\widetilde{G}_q(k) \leq \begin{cases} 2k\left(k - \left\lfloor \frac{k}{p} \right\rfloor\right) - 5 + \left\lfloor \frac{6\lfloor k/p \rfloor - 4}{k-2} \right\rfloor, & \text{if } p \nmid (k-1), \\ 4k + 5, & \text{if } k = p^b + 1, \\ \left(2 - \frac{2}{p}\right) k^2 - 2(p^b - p^{b-1} - 2)k - c_k, & \text{if } k = mp^b + 1 \text{ and } m > 1, \end{cases} \tag{2.6}$$

where $c_k = 2\left(p^b - p^{b-1} - 1 - \frac{1}{p}\right) + \left\lfloor \frac{(m-1)(1-1/p)}{2} \right\rfloor$.

We note that when $p \nmid (k-1)$ the above theorem is proved using Lemma 2.15 in Section 2.3, which involves an application of the pigeon hole principle. However, when $k = mp^b + 1$ this approach is no longer effective. As a result, we have to use analogous results which rely on the large sieve inequality instead when $m > 1$, and another separate approach when $m = 1$. This explains why we consider the three cases separately.

We also remark that when $k > p$ our estimates for $\widetilde{G}_q(k)$ given above are sharper than the current available bound of $\widetilde{G}(k) \leq 2k^2 - 2k - 8$ $(k \geq 6)$ for the integer case [26]. In particular, note that in the special case when $k = p^b + 1$ and $k > 3$, we obtain a sharp linear bound of $\widetilde{G}_q(k) \leq 4k + 5$ in contrast to the quadratic bound for $\widetilde{G}(k)$.

We now state the result for the case $3 \leq k < p$.

Theorem 2.4. *Suppose $3 \leq k < p$. Then we have $\widetilde{G}_q(k) \leq 2k^2 - 2\lfloor(\log k)/(\log 2)\rfloor$. Furthermore, $\widetilde{G}_q(7) \leq 86$ and $\widetilde{G}_q(k) \leq 2k^2 - 11$ when $k \geq 8$.*

We also study the slim exceptional sets associated to the asymptotic formula (2.3). These sets measure the frequency with which the expected formula (2.3) does not hold. In other words, we estimate the number of polynomials that in a certain sense do not satisfy the asymptotic formula. For $\psi(z)$ a function of positive variable z, we denote by $\widetilde{E}_{s,k}(N, \psi)$ the set of $n \in I_N \cap \mathbb{J}_q^k[t]$ for which

$$\left| R_{s,k}(n) - \mathfrak{S}_{s,k}(n) J_\infty(n) q^{(s-k)P} \right| > q^{(s-k)P} \psi(q^P)^{-1}. \tag{2.7}$$

Note that $\widetilde{E}_{s,k}(N, \psi)$ is dependent on q. We define $\widetilde{G}_q^+(k)$ to be the least positive integer s for which $|\widetilde{E}_{s,k}(N, \psi)| = o(q^N)$ for some function $\psi(z)$ increasing to infinity with z. We obtain the following estimates on $\widetilde{G}_q^+(k)$. We first present the case $k > p$.

Theorem 2.5. *Let $k \geq 3$ be an integer, where $p \nmid k$. Suppose $k > p$, then we have*

$$\widetilde{G}_q^+(k) \leq \begin{cases} k\left(k - \left\lfloor \frac{k}{p} \right\rfloor\right) - 2 + \left\lfloor \frac{3\lfloor k/p \rfloor - 2}{k-2} \right\rfloor, & \text{if } p \nmid (k-1), \\ 2k + 3, & \text{if } k = p^b + 1, \\ \left(1 - \frac{1}{p}\right) k^2 - (p^b - p^{b-1} - 2)k - c'_k, & \text{if } k = mp^b + 1 \text{ and } m > 1, \end{cases} \tag{2.8}$$

where $c'_k = \left(p^b - p^{b-1} - 1 - \frac{1}{p}\right) + \left\lfloor \frac{(m-1)(1-1/p)}{4} \right\rfloor$.

We now state the result for the case $3 \le k < p$.

Theorem 2.6. *Suppose $3 \le k < p$. Then we have $\widetilde{G}_q^+(k) \le k^2 - \lfloor (\log k)/(\log 2) \rfloor$. Furthermore, we have $\widetilde{G}_q^+(7) \le 43$, and $\widetilde{G}_q^+(k) \le k^2 - 5$ when $k \ge 8$.*

The organization of the rest of the chapter is as follows. In Section 2.2, we introduce some notation and basic notions required to carry out our discussion in the setting over $\mathbb{F}_q[t]$. In Section 2.3, we go through technical details to prove an upper bound for $\psi(\alpha, \theta)$, which is defined in (2.30). This estimate is one of the main ingredients to obtain our minor arc estimates, for the cases $p \nmid (k-1)$ and $k = mp^b + 1$ with $m > 1$, in Section 2.4. We also obtain minor arc estimates for the case $k = p^b + 1$ in Section 2.4. We then prove a useful result related to Weyl differencing in Section 2.5. The content of Sections 2.6 and 2.7 are similar; we combine the material from previous sections to obtain a variant of minor arc estimates achieved in Section 2.4, from which our results follow.

We denote $\mathbf{x} = (x_1, ..., x_{2s})$, where $x_i \in \mathbb{F}_q[t]$ $(1 \le i \le 2s)$. We write $N_1 \le \operatorname{ord} \mathbf{x} \le N_2$ to denote that $N_1 \le \operatorname{ord} x_i \le N_2$ for $1 \le i \le 2s$, and given $n_0 \in \mathbb{F}_q[t]$, we write $(\mathbf{x} - n_0)$ to denote the $2s$-tuple $(x_1 - n_0, ..., x_{2s} - n_0)$. Confusion should not arise if the reader interprets analogous statements in a similar manner.

2.2 Preliminary

While the Hardy-Littlewood circle method for $\mathbb{F}_q[t]$ mirrors the classical version familiar from applications over $\mathbb{Z}$, the substantial differences in detail between these rings demand explanation. Our goal in the present section is to introduce notation and basic notions that are subsequently needed to initiate discussion of key components of this version of the circle method. The material here is taken from various sources including [10], [14], [12], [15], and [19]. Associated with the polynomial ring $\mathbb{F}_q[t]$ defined over the field $\mathbb{F}_q$ is its field of fractions $\mathbb{K} = \mathbb{F}_q(t)$. For $f/g \in \mathbb{K}$, we define an absolute value $\langle \cdot \rangle : \mathbb{K} \to \mathbb{R}$ by $\langle f/g \rangle = q^{\deg f - \deg g}$ (with the convention that $\deg 0 = -\infty$ and $\langle 0 \rangle = 0$). The completion of $\mathbb{K}$ with respect to this absolute value 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 $n \in \mathbb{Z}$, coefficients $a_i = a_i(\alpha)$ in $\mathbb{F}_q$ $(i \le n)$ and $a_n \ne 0$. For each such $\alpha \in \mathbb{K}_\infty$, we refer to $a_{-1}(\alpha)$ as the *residue* of α, an element of $\mathbb{F}_q$ that we abbreviate to $\operatorname{res} \alpha$. If $n < -1$, then we let $\operatorname{res} \alpha = 0$. We also define the order of α to be $\operatorname{ord} \alpha = n$. Thus if f is a polynomial in $\mathbb{F}_q[t]$, then $\operatorname{ord} f = \deg f$. Note that the order on $\mathbb{K}_\infty$ satisfies the following property: if

$\alpha, \beta \in \mathbb{K}_\infty$ satisfies $\operatorname{ord}\alpha > \operatorname{ord}\beta$, then

$$\operatorname{ord}(\alpha+\beta) = \operatorname{ord}\alpha. \tag{2.9}$$

The field $\mathbb{K}_\infty$ is a locally compact field under the topology induced by the absolute value $\langle\cdot\rangle$. Let $\mathbb{T} = \{\alpha \in \mathbb{K}_\infty : \operatorname{ord}\alpha < 0\}$. Every element $\alpha \in \mathbb{K}_\infty$ can be written uniquely in the shape $\alpha = [\alpha] + \|\alpha\|$, where the *integral part* of α is $[\alpha] \in \mathbb{F}_q[t]$ and the *fractional part* of α is $\|\alpha\| \in \mathbb{T}$. Note that $[\cdot]$ and $\|\cdot\|$ are $\mathbb{F}_q$-linear functions on $\mathbb{K}_\infty$ [19, pp.12]. Since $\mathbb{T}$ is a compact additive subgroup of $\mathbb{K}_\infty$, it possesses a unique Haar measure $d\alpha$. We normalise it, so that $\int_{\mathbb{T}} 1 \, d\alpha = 1$. The Haar measure on $\mathbb{T}$ extends easily to a product measure on the D-fold Cartesian product $\mathbb{T}^D$, for any positive integer D. For convenience, we will use the notation

$$\oint d\boldsymbol{\alpha} := \int_{\mathbb{T}} ... \int_{\mathbb{T}} d\alpha_1 ... \, d\alpha_D,$$

where the positive integer D should be clear from the context.

We are now equipped to define an analogue of the exponential function. Recall $\operatorname{ch}(\mathbb{F}_q) = p$. 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 $e_q(a) = \exp(2\pi i \ \operatorname{tr}(a)/p)$, where $\operatorname{tr} : \mathbb{F}_q \to \mathbb{F}_p$ denotes the familiar trace map. 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 $e_q(a_{-1}(\alpha))$. The orthogonality relation underlying the Fourier analysis of $\mathbb{F}_q[t]$ takes the following shape.

Lemma 2.7. *Let h be a polynomial in $\mathbb{F}_q[t]$. Then we have*

$$\int_{\mathbb{T}} e(h\alpha) \, d\alpha = \begin{cases} 0, & \textit{if } h \in \mathbb{F}_q[t]\backslash\{0\}, \\ 1, & \textit{if } h = 0. \end{cases} \tag{2.10}$$

Proof. This is [19, Lemma 1 (f)]. □

The following estimate on exponential sums will be useful during the analysis in subsequent sections.

Lemma 2.8. *Let $Y \in \mathbb{N}$. Then we have*

$$\sum_{\operatorname{ord} x \le Y} e(\beta x) = \begin{cases} q^{Y+1}, & \textit{if } \operatorname{ord} ||\beta|| < -Y-1, \\ 0, & \textit{if } \operatorname{ord} ||\beta|| \ge -Y-1. \end{cases} \tag{2.11}$$

Proof. This is [19, Lemma 7]. □

For each $k \geq 2$, we define the following exponential sum

$$g(\alpha) = \sum_{x \in I_X} e(\alpha x^k). \tag{2.12}$$

Then, it is a consequence of the orthogonality relation (2.10) that

$$R_{s,k}(n) = \int_{\mathbb{T}} g(\alpha)^s e(-n\alpha)\ d\alpha. \tag{2.13}$$

We analyse the integral (2.13) via the Hardy-Littlewood circle method, and to this end we define sets of *major* and *minor arcs* corresponding to well and poorly approximable elements of $\mathbb{T}$. Let $R_k = (k-1)X$. Given polynomials a and g with $(a, g) = 1$ and g monic, we define the *Farey arcs* $\mathfrak{M}_k(g, a)$ about a/g (associated to k) by

$$\mathfrak{M}_k(g, a) = \{\alpha \in \mathbb{T} : \operatorname{ord}(\alpha - a/g) < -R_k - \operatorname{ord} g\}. \tag{2.14}$$

The set of major arcs $\mathfrak{M}_k$ is defined to be the union of the sets $\mathfrak{M}_k(g, a)$ with

$$a, g \in \mathbb{F}_q[t], \quad g \text{ monic}, \quad 0 \leq \operatorname{ord} a < \operatorname{ord} g \leq X, \quad \text{and} \quad (a, g) = 1. \tag{2.15}$$

The set of minor arcs is defined to be $\mathfrak{m}_k = \mathbb{T} \backslash \mathfrak{M}_k$. It follows from [19, Lemma 3] that $\mathfrak{m}_k$ is the union of the sets $\mathfrak{M}_k(g, a)$ with

$$a, g \in \mathbb{F}_q[t], \quad g \text{ monic}, \quad 0 \leq \operatorname{ord} a < \operatorname{ord} g, \quad X < \operatorname{ord} g \leq R_k, \quad \text{and} \quad (a, g) = 1. \tag{2.16}$$

Notice $\mathfrak{m}_2 = \varnothing$ and for this reason, we assume $k \geq 3$ for results involving minor arcs. We will suppress the subscript k whenever there is no ambiguity with the choice of k being used. We can then rewrite (2.13) as

$$R_{s,k}(n) = \int_{\mathfrak{M}} g(\alpha)^s e(-n\alpha)\ d\alpha + \int_{\mathfrak{m}} g(\alpha)^s e(-n\alpha)\ d\alpha, \tag{2.17}$$

and study the contribution from the major arcs and the minor arcs separately.

We have the following estimate on the major arcs, which is slightly different from what is established in [19]. The difference comes from our choice of $P(n)$ following [15], instead of the approach taken in [19], and this choice allows us to have a cleaner statement of the result. Applying Theorem 2.9 below for the estimate of the major arcs results in the statement of Theorem 2.1 in contrast to that of [19, Theorem 30].

Theorem 2.9. *Suppose $p \nmid k$ and $s \geq 2k+1$. Then there exists $\epsilon > 0$ such that given any $n \in \mathbb{J}_q^k[t]$, the following asymptotic formula holds*

$$\int_{\mathfrak{M}} g(\alpha)^s \, d\alpha = \mathfrak{S}_{s,k}(n) J_\infty(n) q^{(s-k)P} + O\left(q^{(s-k-\epsilon)P}\right), \tag{2.18}$$

where

$$1 \ll \mathfrak{S}_{s,k}(n) J_\infty(n) \ll 1.$$

Note that the implicit constants in the theorem may depend on s, q, and k, where the constant in (2.18) may also depend on ϵ, but they are independent of n and P.

Proof. Let $0 < \varepsilon < 1$. Similarly as explained in the proof of [15, Lemma 5.3], by applying Lemma 17 of [19] with $m = X$ and $m' = R_k + \operatorname{ord} g$, where $\operatorname{ord} g \leq \varepsilon X$, we obtain

$$\int_{\operatorname{ord}\beta < -R_k - \operatorname{ord} g} g(\beta)^s e(-n\beta) \, d\beta = J_\infty(n) q^{(s-k)P} + O(1), \tag{2.19}$$

where the implicit constant may depend on s, k, q, and ε. We note that when P is sufficiently large in terms of k and ε, it is only the cases (a) and (b) of [19, Lemma 17] that are relevant, and in fact we obtain (2.19) without the $O(1)$ term. The $O(1)$ term in (2.19) comes from the small values of P where this does not apply. It is also explained in the proof of [15, Lemma 5.3] that for $s \geq k+1$, we have $1 \leq J_\infty(n) \ll 1$. By [15, Lemma 5.2], we know that if $n \in \mathbb{J}_q^k[t]$ and $s \geq 2k+1$, then $1 \ll \mathfrak{S}_{s,k}(n) \ll 1$.

The equation (2.18) is a consequence of (2.19) and [15, Lemma 5.2], and it is essentially contained in the proof of [19, Theorem 30], where we replace the use of [19, Theorem 18] with (2.19). We remark that the condition $s \geq 3k+1$ is imposed in [19, Lemma 23], which is also used in the proof of [19, Theorem 30]. However, as stated in [15, pp.19] this is a result of an oversight and in fact we can relax the condition to $s \geq 2k+1$ in [19, Lemma 23]. It can easily be verified that the arguments to prove (2.18) within [19, Theorem 30] also remains valid when $s \geq 2k+1$. □

When $k = 2$, we know that $\mathfrak{m}_2 = \varnothing$. Hence, it follows that

$$R_{s,k}(n) = \int_{\mathfrak{M}} g(\alpha)^s \, d\alpha. \tag{2.20}$$

Therefore, as an immediate consequence of Theorem 2.9 we obtain $\widetilde{G}_q(2) \leq 5$.

It was proved in [19, Lemma 28] that $\mathbb{F}_q[t] = \mathbb{J}_q^k[t]$ when $k < p$, which explains the use of $\mathbb{F}_q[t]$ in the statement of Theorem 2.1 instead of $\mathbb{J}_q^k[t]$ as above in Theorem 2.9.

Let $\mathcal{R}$ be a finite subset of $\mathbb{N}$ satisfying the following condition in [10, pp.846] with $d = 1$:

$$\text{Condition*: Given } l \in \mathbb{N}, \text{ if there exists } j \in \mathcal{R} \text{ such that } p \nmid \binom{j}{l}, \text{ then } l \in \mathcal{R}. \tag{2.21}$$

Let $J_s(\mathcal{R}; X)$ denote the number of solutions of the system

$$u_1^j + \ldots + u_s^j = v_1^j + \ldots + v_s^j \ (j \in \mathcal{R}), \tag{2.22}$$

with $u_i, v_i \in I_X$ $(1 \leq i \leq s)$. Since p is the characteristic of $\mathbb{F}_q$, if there exists $j, j' \in \mathcal{R}$ with $j' = p^v j$ for some $v \in \mathbb{N}$, then we have

$$\sum_{i=1}^{s} (u_i^{j'} - v_i^{j'}) = \left(\sum_{i=1}^{s} (u_i^j - v_i^j) \right)^{p^v}.$$

Thus, the equations in (2.22) are not always independent. The absence of independence suggests that Vinogradov-type estimates for integers cannot be adapted directly into a function field setting. To regain independence, we instead consider

$$\mathcal{R}' = \{ j \in \mathbb{N} : p \nmid j \text{ and } p^v j \in \mathcal{R} \text{ for some } v \in \mathbb{N} \cup \{0\} \}. \tag{2.23}$$

Then we see that $J_s(\mathcal{R}; X)$ also counts the number of solutions of the system

$$u_1^j + \ldots + u_s^j = v_1^j + \ldots + v_s^j \ (j \in \mathcal{R}'), \tag{2.24}$$

with $u_i, v_i \in I_X$ $(1 \leq i \leq s)$, or in other words $J_s(\mathcal{R}; X) = J_s(\mathcal{R}'; X)$. We note here that although the equations in (2.24) are independent, the set $\mathcal{R}'$ is not necessarily contained in $\mathcal{R}$. The following theorem was proved in [16] and in [10, Theorem 1.1] with $d = 1$.

Theorem 2.10 (Theorem 1.1, [10]). *Suppose $\mathcal{R}$ satisfies Condition* given in (2.21). Let $r = \operatorname{card} \mathcal{R}'$, $\phi = \max_{j \in \mathcal{R}'} j$, and $\kappa = \sum_{j \in \mathcal{R}'} j$. Suppose $\phi \geq 2$ and $s \geq r\phi + r$. Then for each $\epsilon > 0$, there exists a positive constant $C = C(s; r, \phi, \kappa; q; \epsilon)$ such that*

$$J_s(\mathcal{R}; X) \leq C \left(q^X \right)^{2s - \kappa + \epsilon}.$$

The following is a useful criterion, which we utilize.

Lemma 2.11. *Let p be any prime and $k = a_h p^h + ... + a_1 p + a_0$ with $0 \leq a_i < p$ $(0 \leq i \leq h)$ and $a_h \neq 0$. The binomial coefficient $\binom{k}{n}$ is coprime to p if and only if $n = b_h p^h + ... + b_1 p + b_0$, where $0 \leq b_i \leq a_i$ $(0 \leq i \leq h)$.*

Proof. It follows by Lucas' Criterion [15, pp.33] or apply [28, Lemma A.1] with $d = 1$. □

As a consequence of Lemma 2.11, we have the following lemma.

Lemma 2.12. *Let p be any prime. Suppose $k = mp^b + 1$ with $m, b \in \mathbb{N}$ and $p \nmid m$. Then, $(k - p^b)$ is the largest number less than $(k - 1)$ such that $\binom{k}{k-p^b} \not\equiv 0$ (mod p).*

Proof. Let $m = c_a p^a + c_{a-1} p^{a-1} + ... + c_1 p + c_0$ with $0 \leq c_i < p$ and $0 < c_0$. Thus, we have $k = c_a p^{a+b} + c_{a-1} p^{a-1+b} + ... + c_1 p^{b+1} + c_0 p^b + 1$. For $1 \leq j \leq p^b$, write $k - j = c_a p^{a+b} + c_{a-1} p^{a-1+b} + ... + c_1 p^{b+1} + d_b p^b + d_{b-1} p^{b-1} + ... + d_1 p + d_0$ with $0 \leq d_i < p$. Then, by Lemma 2.11, $\binom{k}{k-j} \not\equiv 0 \pmod{p}$ if and only if $d_b \leq c_0$, $d_i = 0$ $(1 \leq i < b)$ and $d_0 \leq 1$. Therefore, it is not too difficult to verify that $\binom{k}{k-j} \not\equiv 0 \pmod{p}$ only when $j = 1$ and p^b in the range $1 \leq j \leq p^b$. □

For a prime $p = \mathrm{ch}(\mathbb{F}_q)$ and $k \in \mathbb{N}$ with $p \nmid k$, we define $j_0(k, q) = j_0$ to be

$$j_0 := \max_{0<j<k} \left\{ j : p \nmid j \text{ and } \binom{k}{j} \not\equiv 0 \pmod{p} \right\}. \tag{2.25}$$

If $p \nmid (k-1)$, then $j_0 = k - 1$. On the other hand, if $k = mp^b + 1$ for some $m, b \in \mathbb{N}$ and $p \nmid m$, then $j_0 = k - p^b$ by Lemma 2.12. We record the values of j_0 here for reference,

$$j_0 = \begin{cases} k - 1, & \text{if } p \nmid (k-1), \\ (m-1)p^b + 1, & \text{if } k = mp^b + 1. \end{cases} \tag{2.26}$$

With application of Theorem 2.10 in mind, we define the following two sets

$$\mathcal{R} = \{1, 2, ..., j_0, k\} \cup \{k - 1\} \tag{2.27}$$

and

$$\begin{aligned} \mathcal{R}' &= \{j \in \mathbb{N} : p \nmid j \text{ and } p^v j \in \mathcal{R} \text{ for some } v \in \mathbb{N} \cup \{0\}\} \qquad (2.28) \\ &= \{j : j \in \mathcal{R} \text{ and } p \nmid j\}. \end{aligned}$$

The first equality is the definition of $\mathcal{R}'$, which comes from (2.23), but the second equality requires a slight justification. If $p \nmid (k-1)$, then $\mathcal{R} = \{1, 2, ..., k\}$ and the second equality of (2.28) is immediate. If $k = mp^b + 1$, then $k \in \mathcal{R}'$. We also have $k - 1 = mp^b \notin \mathcal{R}'$ and $m \in \mathcal{R}'$. However, since $j_0 = (m-1)p^b + 1 > m$ and $p \nmid m$, it follows that $\mathcal{R}' = \{j : 1 \leq j \leq j_0 \text{ and } p \nmid j\} \cup \{k\}$ from which we obtain the second equality of (2.28).

We let $\operatorname{card} \mathcal{R}' = r$ and let $\mathcal{R}' = \{t_1, ..., t_r\}$, where $t_1 < ... < t_r$. Clearly, we have $t_r = k$ and it follows by our definition of j_0 and $\mathcal{R}$ that $t_{r-1} = j_0$. We can verify by simple calculation that

$$r = \begin{cases} k - \lfloor k/p \rfloor, & \text{if } p \nmid (k-1), \\ (1 - 1/p)(k - p^b) + (1 + 1/p), & \text{if } k = mp^b + 1. \end{cases} \tag{2.29}$$

In particular, if $k = p^b + 1$, then $r = 2$. For the remainder of the chapter, whenever we refer to $\mathcal{R}$, $\mathcal{R}'$ and r, we mean (2.27), (2.28), and (2.29), respectively.

Lemma 2.13. *$\mathcal{R}$ satisfies Condition* given in (2.21).*

Proof. If $p \nmid (k-1)$, then $\mathcal{R} = \{1, 2, ..., k\}$ and it satisfies Condition*. This is easy to see, because suppose for some $l \in \mathbb{N}$, there exists $j \in \mathcal{R}$ such that $p \nmid \binom{j}{l}$. Then we have $1 \leq l \leq j \leq k$, and hence $l \in \mathcal{R}$. On the other hand, if $k = mp^b + 1$, then we have $\mathcal{R} = \{1, 2, ..., j_0, k-1, k\}$. Suppose we are given some $l \in \mathbb{N}$. It is clear that if $l > k$, then there does not exist $j \in \mathcal{R}$ such that $p \nmid \binom{j}{l}$, because $\binom{j}{l} = 0$. Thus, it suffices to show that for $j_0 < l < (k-1)$, $\binom{j}{l} \equiv 0 \pmod{p}$ for all $j \in \mathcal{R}$. Clearly, $\binom{j}{l} \equiv 0 \pmod{p}$ for $j \leq j_0$. Lemma 2.12 gives us that $\binom{k}{l} \equiv 0 \pmod{p}$ for $j_0 < l < (k-1)$. Therefore, we only need to verify $\binom{k-1}{l} \equiv 0 \pmod{p}$ for $j_0 = (k - p^b) < l < (k-1)$. Every l in this range can be written as $l = (m-1)p^b + c_{b-1}p^{b-1} + ... + c_1 p + c_0$, where $0 \leq c_i < p$. Since $(k-1) = mp^b$, by Lemma 2.11 we have $\binom{k-1}{l} \not\equiv 0 \pmod{p}$ if and only if $c_i = 0$ for $0 \leq i < b$, or in other words $l = (m-1)p^b = k - p^b - 1$. Because $l = k - p^b - 1$ is not in the range of l we are considering, it follows that $\mathcal{R}$ satisfies Condition*. □

2.3 Technical Lemmas

We will be applying the following large sieve inequality in this section. Given a set $\Gamma \subseteq \mathbb{K}_\infty$, if for any distinct elements $\gamma_1, \gamma_2 \in \Gamma$ we have $\operatorname{ord}(\gamma_1 - \gamma_2) > \delta$, then we say the points $\{\gamma : \gamma \in \Gamma\}$ are *spaced at least q^δ apart in* $\mathbb{T}$.

Theorem 2.14 (Theorem 2.4, [9]). *Given $A, Z \in \mathbb{Z}^+$, let $\Gamma \subseteq \mathbb{K}_\infty$ be a set whose elements are spaced at least q^{-A} apart in $\mathbb{T}$. Let $(c_x)_{x\in\mathbb{F}_q[t]}$ be a sequence of complex numbers. For $\alpha \in \mathbb{K}_\infty$, define*

$$\mathcal{S}(\alpha) = \sum_{\operatorname{ord} x \leq Z} c_x e(x\alpha).$$

Then we have

$$\sum_{\gamma\in\Gamma} |\mathcal{S}(\gamma)|^2 < \max\{q^{Z+1}, q^{A-1}\} \sum_{\operatorname{ord} x\leq Z} |c_x|^2.$$

Recall $I_X := \{x \in \mathbb{F}_q[t] : \operatorname{ord} x < X\}$. Let $k \geq 3$, $\theta \in \mathfrak{m}_k$, $0 \neq c \in \mathbb{F}_q$, $\alpha \in \mathbb{T}$, and j_0 be as defined in Section 2.2. In this section, we find an upper bound for the following exponential sum,

$$\psi(\theta, \alpha) = q^{-X} \sum_{y\in I_X} \sum_{\operatorname{ord} h\leq j_0(X-1)} e(-chy^{k-j_0}\theta - \alpha h). \tag{2.30}$$

The estimates obtained for $\psi(\theta, \alpha)$ is one of our main ingredients for computing the minor arc estimates in Section 2.4. To achieve this goal, the precise value of j_0 with respect to k plays an important role. Hence, we consider the following two cases separately: $p \nmid (k-1)$ and $k = mp^b + 1$ with $m, b \in \mathbb{N}$, $m > 1$, and $p \nmid m$. We do not consider the case $k = p^b + 1$ here, because we apply a different method to bound the minor arcs in this case.

First, we make several observations, which we use throughout this section. Let $\theta = a/g + \beta$, where $(a, g) = 1$. Let x, $y \in I_X$ and $x \neq y$. Then, since $\|\cdot\|$ is $\mathbb{F}_q$-linear, we have

$$\begin{aligned} \operatorname{ord}(\|cx^{k-j_0}\theta + \alpha\| - \|cy^{k-j_0}\theta + \alpha\|) &= \operatorname{ord}\|(x^{k-j_0} - y^{k-j_0})\theta\| \qquad (2.31)\\ &= \operatorname{ord}(\|(x^{k-j_0} - y^{k-j_0})a/g\| + \|(x^{k-j_0} - y^{k-j_0})\beta\|). \end{aligned}$$

Since $\mathbb{F}_q[t]$ is a unique factorization domain, we have $(x^{k-j_0} - y^{k-j_0})a \neq 0$ as long as $a \neq 0$. Note that it is possible to get $a = 0$, when $\operatorname{ord} g = 0$.

Suppose $(x^{k-j_0} - y^{k-j_0})a/g \in \mathbb{F}_q[t]$. Then, we have $\|(x^{k-j_0} - y^{k-j_0})a/g\| = 0$ and

$$\operatorname{ord}(\|cx^{k-j_0}\theta + \alpha\| - \|cy^{k-j_0}\theta + \alpha\|) = \operatorname{ord}\|(x^{k-j_0} - y^{k-j_0})\beta\|. \tag{2.32}$$

On the other hand, if $(x^{k-j_0} - y^{k-j_0})a/g \notin \mathbb{F}_q[t]$, write

$$\frac{a}{g}(x^{k-j_0} - y^{k-j_0}) = s_0 + a_{-j}t^{-j} + a_{-j-1}t^{-j-1} + \ldots$$

with $s_0 \in \mathbb{F}_q[t]$, $a_i \in \mathbb{F}_q$ for $i \le -j \le -1$ and $a_{-j} \neq 0$. Here we know such $a_{-j} \neq 0$ exists, because $(x^{k-j_0} - y^{k-j_0})a/g \notin \mathbb{F}_q[t]$. Then it follows that

$$a(x^{k-j_0} - y^{k-j_0}) - gs_0 = g(a_{-j}t^{-j} + a_{-j-1}t^{-j-1} + \dots).$$

Since the left hand side is a polynomial, we have $-j + \operatorname{ord} g \ge 0$. Consequently, we obtain

$$\operatorname{ord} \|(x^{k-j_0} - y^{k-j_0})a/g\| \ge -\operatorname{ord} g. \tag{2.33}$$

2.3.1 Case $p \nmid (k-1)$

Here we have $j_0 = k-1$, or equivalently $k - j_0 = 1$. In this situation, we obtain an upper bound for $\psi(\theta, \alpha)$ in a way analogous to the case for integers in [25]. We have the following lemma.

Lemma 2.15. *Suppose $k \ge 3$, $p \nmid k$, and $p \nmid (k-1)$. Let $\theta \in \mathfrak{m}_k$ and $\alpha \in \mathbb{T}$. Then we have*

$$\psi(\theta, \alpha) \le q^{(j_0-1)X}.$$

Proof. Let $\theta = a/g + \beta \in \mathfrak{M}_k(g,a) \subseteq \mathfrak{m}_k$. Let $x,\ y \in I_X$ and $x \neq y$. Then, we know $(x^{k-j_0} - y^{k-j_0})a/g \notin \mathbb{F}_q[t]$, because $k - j_0 = 1$ and $\operatorname{ord} g > X$. Consequently, we have (2.33). Recall $R_k = (k-1)X$. For simplicity we let $R = R_k$. Since $R > (k-j_0)(X-1)$ and $\operatorname{ord}\beta < (-R - \operatorname{ord} g)$, we have

$$\operatorname{ord}\,(x^{k-j_0} - y^{k-j_0})\beta < (k-j_0)(X-1) - R - \operatorname{ord} g < -\operatorname{ord} g \le 0.$$

Thus, we obtain from (2.9) and (2.31)

$$\operatorname{ord}\,\big(\|cx^{k-j_0}\theta + \alpha\| - \|cy^{k-j_0}\theta + \alpha\|\big) = \operatorname{ord}\|(x^{k-j_0} - y^{k-j_0})a/g\| \ge -\operatorname{ord} g \ge -R. \tag{2.34}$$

Suppose there exists $y \in I_X$ such that $\operatorname{ord}\|cy^{k-j_0}\theta + \alpha\| < (-j_0(X-1) - 1)$, or equivalently,

$$\operatorname{ord}\|cy\theta + \alpha\| < -(k-1)(X-1) - 1. \tag{2.35}$$

This means the first $((k-1)(X-1)+1)$ coefficients of $\|cy\theta + \alpha\|$ are 0. Hence, it takes the form

$$\|cy\theta+\alpha\| = 0\,t^{-1} + 0\,t^{-2} + \dots + 0\,t^{-(k-1)(X-1)-1} + a_{-(k-1)(X-1)-2}t^{-(k-1)(X-1)-2} + \dots + a_{-R}t^{-R} + \dots .$$

Note that there are only q^{k-2} possibilities for the $(k-2)$-tuple $(a_{-(k-1)(X-1)-2}, \cdots, a_{-R})$. Thus, if there are more than q^{k-2} such polynomials $y \in I_X$ satisfying (2.35), then by the pigeon hole principle there exists a pair x and y in I_X for which the first R coefficients of $\|cx\theta + \alpha\|$ and $\|cy\theta + \alpha\|$ agree. However, this contradicts (2.34). Therefore, it follows by (2.30) and Lemma 2.8 that

$$\psi(\theta, \alpha) \leq q^{-X+k-2+(k-1)(X-1)+1} = q^{(k-2)X}.$$

□

2.3.2 Case $k = mp^b + 1$ with $m > 1$

Here we have $j_0 = k - p^b > p^b = k - j_0$. When $p \nmid (k-1)$, we had that the difference between $j_0(X-1)+1$ and $R_k = (k-1)X$ was small enough compared to X - in fact it was constant with respect to X - which was the reason our application of the pigeon hole principle was effective in Lemma 2.15. However, when $k = mp^b + 1$ this is no longer the case as $R_k - j_0(X-1) - 1 = (p^b - 1)X + (k - p^b - 1)$.

It follows from the definition of the major arcs that $\mathfrak{M}_k \subseteq \mathfrak{M}_{k-j_0+1}$, hence $\mathfrak{m}_{k-j_0+1} \subseteq \mathfrak{m}_k$. Therefore, given $\theta \in \mathfrak{m}_k$, we have either $\theta \in \mathfrak{m}_{k-j_0+1}$ or $\theta \in \mathfrak{M}_{k-j_0+1}$. We consider these two cases separately in Lemmas 2.16 and 2.17. The argument in Lemma 2.16 is similar to that of Lemma 2.15. However, in Lemma 2.17 we use a different approach, which relies on the large sieve inequality given in Theorem 2.14 instead.

Lemma 2.16. *Let $k = mp^b + 1$ with $m > 1$ and $\theta \in \mathfrak{m}_k$. Suppose $\theta \in \mathfrak{m}_{k-j_0+1}$. Then we have*

$$\psi(\theta, \alpha) \ll q^{(j_0 - 1/p^b)X},$$

where the implicit constant depends only on q and k.

Proof. Let $\theta = a/g + \beta \in \mathfrak{M}_{k-j_0+1}(g, a) \subseteq \mathfrak{m}_{k-j_0+1}$, and we know $R' \geq \operatorname{ord} g > X$, where $R' = R_{k-j_0+1} = (k - j_0)X$. Given $y \in I_X$, it takes the form

$$y = c_{X-1}t^{X-1} + ... + c_{\lfloor X/p^b \rfloor} t^{\lfloor X/p^b \rfloor} + ... + c_0. \tag{2.36}$$

Let $L = (X - \lfloor X/p^b \rfloor)$. Order the L-tuples of elements of $\mathbb{F}_q$ in any way, for example, we may take one bijection between $\mathbb{F}_q$ and $\{1, ..., q\}$, and use the lexicographic ordering on

$(\mathbb{F}_q)^L$. We can then split I_X into q^L subsets $T_1, T_2, ..., T_{q^L}$, where

$$T_l = \{y \in I_X : \text{ given } y \text{ in the form (2.36), the coefficients } \left(c_{X-1}, ..., c_{\lfloor X/p^b \rfloor}\right) \text{ is exactly the } l\text{-th } L\text{-tuple}\}.$$

Then, we have for some $T' = T_l$

$$\psi(\theta, \alpha) \ll q^{-X+X-X/p^b} \Big| \sum_{y \in T'} \sum_{\text{ord } h \leq j_0(X-1)} e(-chy^{k-j_0}\theta - \alpha h) \Big|. \tag{2.37}$$

Given any distinct $x, y \in T'$, we have

$$\text{ord}\,(x^{k-j_0} - y^{k-j_0}) = \text{ord}\,(x-y)^{p^b} \leq X,$$

and hence, $(x^{k-j_0} - y^{k-j_0})a/g \notin \mathbb{F}_q[t]$. Thus, by (2.33) we have $\text{ord}\,\|(x^{k-j_0} - y^{k-j_0})a/g\| \geq -\text{ord}\,g$. Since $\text{ord}\,\beta < -R' - \text{ord}\,g$ and $R' = (k-j_0)X > X$, we have $\text{ord}\,(x^{k-j_0} - y^{k-j_0})\beta < X - R' - \text{ord}\,g < -\text{ord}\,g \leq 0$. Therefore, by (2.9) and (2.31), we obtain

$$\text{ord}\,\left(\|cx^{k-j_0}\theta + \alpha\| - \|cy^{k-j_0}\theta + \alpha\|\right) \geq -\text{ord}\;g \geq -R'. \tag{2.38}$$

Suppose there exists $y \in T'$ such that $\text{ord}\,\|cy^{k-j_0}\theta + \alpha\| < -j_0(X-1) - 1$. This means the first $j_0(X-1)+1$ coefficients of $\|cy^{k-j_0}\theta + \alpha\|$ must be 0, or in other words it takes the form

$$\|cy^{k-j_0}\theta + \alpha\| = 0\;t^{-1} + 0\;t^{-2} + ... \;+ 0\;t^{-j_0(X-1)-1} + a_{-j_0(X-1)-2}t^{-j_0(X-1)-2} + ...$$

If there is another distinct $x \in T'$, which satisfies the same condition, then the first $j_0(X-1)+1$ coefficients of $\|cx^{k-j_0}\theta + \alpha\|$ agree with that of $\|cy^{k-j_0}\theta + \alpha\|$. However, this contradicts (2.38) as $R' = (k-j_0)X < j_0(X-1)+1$ for X sufficiently large. Hence, there is at most one such y. Therefore, it follows by (2.37) and Lemma 2.8 that

$$\psi(\theta, \alpha) \ll q^{-X+X-X/p^b + j_0(X-1)+1} \ll q^{(j_0 - 1/p^b)X}.$$

□

Lemma 2.17. *Let $k = mp^b + 1$ with $m > 1$ and $\theta \in \mathfrak{m}_k$. Suppose $\theta \in \mathfrak{M}_{k-j_0+1}$. Then we have*

$$\psi(\theta, \alpha) \ll q^{(j_0 - 1/(4p^b))X},$$

where the implicit constant depends only on q.

Proof. Let $\theta = a/g + \beta \in \mathfrak{M}_{k-j_0+1}(g, a) \subseteq \mathfrak{M}_{k-j_0+1}$. Then, we have $\operatorname{ord} g \leq X$ and

$$-R_k - \operatorname{ord} g \leq \operatorname{ord} \beta < -R_{k-j_0+1} - \operatorname{ord} g, \tag{2.39}$$

where $R_k = (k-1)X$ and $R_{k-j_0+1} = (k-j_0)X$. For simplicity, we denote $R = R_k$ and $R' = R_{k-j_0+1}$. We have the above lower bound, for otherwise it would mean $\theta \in \mathfrak{M}_k$.

By the Cauchy-Schwartz inequality, we obtain

$$\psi(\theta, \alpha) \ll q^{-X} q^{X/2} S^{1/2}, \tag{2.40}$$

where

$$S = \sum_{y \in I_X} \Big| \sum_{\operatorname{ord} h \leq j_0(X-1)} e(-chy^{k-j_0}\theta - \alpha h) \Big|^2.$$

Let $\delta' > 0$ be sufficiently small, and in particular we make sure $\delta' \leq 1$. We consider two cases: $\operatorname{ord} g > \delta' X$ and $\operatorname{ord} g \leq \delta' X$.

Case 1: Suppose $\operatorname{ord} g > \delta' X$. Given $y \in I_X$, it takes the form

$$y = c_{X-1}t^{X-1} + ... + c_{\lfloor \delta' X/p^b \rfloor} t^{\lfloor \delta' X/p^b \rfloor} + ... + c_0. \tag{2.41}$$

Let $L = X - \lfloor \delta' X/p^b \rfloor$. Order the L-tuples of elements of $\mathbb{F}_q$ in any way. We can then split I_X into q^L subsets, $T_1, T_2, ..., T_{q^L}$, where

$T_l = \{y \in I_X :$ given y in the form (2.41), the coefficients $\big(c_{X-1}, ..., c_{\lfloor \delta' X/p^b \rfloor}\big)$
is exactly the l-th L-tuple$\}$.

Then we have for some $T' = T_l$

$$S \ll q^{X - \delta' X/p^b} \sum_{y \in T'} \Big| \sum_{\operatorname{ord} h \leq j_0(X-1)} e(-chy^{k-j_0}\theta - \alpha h) \Big|^2. \tag{2.42}$$

Recall $k - j_0 = p^b$. Given any $x, y \in T'$, we have

$$\operatorname{ord} \big(x^{k-j_0} - y^{k-j_0}\big) = \operatorname{ord} (x-y)^{p^b} \leq \delta' X,$$

and hence, $(x^{k-j_0} - y^{k-j_0})a/g \notin \mathbb{F}_q[t]$. Thus, we have $\operatorname{ord} \|(x^{k-j_0} - y^{k-j_0})a/g\| \geq -\operatorname{ord} g$ by

(2.33). Since $\operatorname{ord}\beta < (-R' - \operatorname{ord} g)$ and $R' = X > \delta' X$, we have

$$\operatorname{ord}(x^{k-j_0} - y^{k-j_0})\beta < \delta' X - R' - \operatorname{ord} g < -\operatorname{ord} g \leq 0.$$

Therefore, by (2.9) and (2.31), we obtain

$$\operatorname{ord}\left(\|(cx^{k-j_0}\theta + \alpha)\| - \|(cy^{k-j_0}\theta + \alpha)\|\right) \geq -\operatorname{ord} g \geq -X. \tag{2.43}$$

Since $\max\{X, j_0(X-1)+1\} \leq j_0 X$, we have by Theorem 2.14

$$S \ll q^{X - \delta' X/p^b} \sum_{y \in T'} \Bigg| \sum_{\operatorname{ord} h \leq j_0(X-1)} e(-chy^{k-j_0}\theta - \alpha h)\Bigg|^2 \ll q^{X - \delta' X/p^b} q^{2j_0 X}. \tag{2.44}$$

Case 2: Suppose $\operatorname{ord} g \leq \delta' X$. Let $\epsilon > 0$ be sufficiently small. We order the polynomials of degree less than $L' = \lceil (1-\epsilon)X \rceil$ in any way, and call them $p_1, p_2, ..., p_{q^{L'}}$. We then split I_X into $q^{L'}$ subsets, $T_1, T_2, ..., T_{q^{L'}}$, where given any $x \in T_l$, $1 \leq l \leq q^{L'}$, the coefficients of x for powers less than L' agree with that of p_l. Thus, we have for some $T' = T_l$

$$S \ll q^{(1-\epsilon)X} \sum_{y \in T'} \Bigg| \sum_{\operatorname{ord} h \leq j_0(X-1)} e(-chy^{k-j_0}\theta - \alpha h)\Bigg|^2. \tag{2.45}$$

Given any x, $y \in T'$ with $x^{k-j_0} \not\equiv y^{k-j_0} (\operatorname{mod}\, g)$, we have $(x^{k-j_0} - y^{k-j_0})a/g \notin \mathbb{F}_q[t]$. Thus, by (2.33) we have $\operatorname{ord}\|(x^{k-j_0} - y^{k-j_0})a/g\| \geq -\operatorname{ord} g$. Since $\operatorname{ord}\beta < -R' - \operatorname{ord} g$ and $R' = (k-j_0)X > (k-j_0)(X-1)$, we have

$$\operatorname{ord}(x^{k-j_0} - y^{k-j_0})\beta < (k-j_0)(X-1) - R' - \operatorname{ord} g < -\operatorname{ord} g \leq 0. \tag{2.46}$$

Therefore, by (2.9) and (2.31), we obtain

$$\operatorname{ord}\left(\|(cx^{k-j_0}\theta + \alpha)\| - \|(cy^{k-j_0}\theta + \alpha)\|\right) \geq -\operatorname{ord} g \geq -\delta' X. \tag{2.47}$$

On the other hand, suppose we have distinct $x, y \in T'$, where $x^{k-j_0} \equiv y^{k-j_0} (\operatorname{mod}\, g)$. Then we have $(x^{k-j_0} - y^{k-j_0})a/g \in \mathbb{F}_q[t]$ from which (2.32) follows. Also, because $x, y \in T'$ and $k - j_0 = p^b$, we obtain

$$\operatorname{ord}(x^{k-j_0} - y^{k-j_0}) = \operatorname{ord}(x-y)^{p^b} \geq p^b L'.$$

Therefore, it follows by (2.32), (2.39) and (2.46),

$$\begin{aligned} \text{ord}\,\big(\|(cx^{k-j_0}\theta+\alpha)\| - \|(cy^{k-j_0}\theta+\alpha)\|\big) &= \text{ord}\,(x^{k-j_0}-y^{k-j_0})\beta \\ &\geq p^b L' - R - \text{ord}\,g \\ &\geq (k-j_0)(1-\epsilon)X - (k-1)X - \delta' X \\ &= -j_0X + (1-(k-j_0)\epsilon - \delta')X \\ &\geq -j_0X. \end{aligned} \tag{2.48}$$

Since $\max\{\delta' X, j_0X, j_0(X-1)+1\} \leq j_0X$, we have by Theorem 2.14

$$S \ll q^{(1-\epsilon)X} \sum_{y\in T'} \Big| \sum_{\text{ord}\,h \leq j_0(X-1)} e(-chy^{k-j_0}\theta - \alpha h)\Big|^2 \ll q^{(1-\epsilon)X} q^{2j_0X}. \tag{2.49}$$

Note that the only restrictions we had so far for δ' and ϵ were: $0 < \delta' \leq 1$, $0 < \epsilon$, and

$$0 \leq 1 - (k-j_0)\epsilon - \delta'. \tag{2.50}$$

We have by (2.44) and (2.49)

$$S \ll q^{X-\delta' X/p^b} q^{2j_0X} + q^{(1-\epsilon)X} q^{2j_0X}.$$

In order to minimize the right hand side of the above inequality, we set $\epsilon = \delta'/p^b$. Then, since $k - j_0 = p^b$, (2.50) can be simplified to

$$2\delta' \leq 1.$$

By letting $\delta' = 1/2$, we obtain by (2.40)

$$\psi(\theta,\alpha) \ll q^{-X/2} S^{1/2} \ll q^{(j_0-\delta)X},$$

where $\delta = 1/(4p^b)$.

□

2.4 A bound on the minor arcs

We obtain estimates on the minor arcs in this section. In Section 2.4.1, we give bounds on the minor arcs when $p \nmid (k-1)$ and $p = mk^b + 1$, $m > 1$. The remaining case when $k = p^b + 1$ requires a different approach, and it is treated separately in Section 2.4.2. The reason we require a different approach is that when $k = p^b + 1$, the method in Section 2.4.1 results in an exponential sum that is more complicated to estimate than $\psi(\alpha, \theta)$. Thus we take a more basic approach in this case.

2.4.1 Cases $p \nmid (k-1)$ and $p = mk^b + 1$, $m > 1$

Let $\mathcal{R}'$ be as defined in (2.28). Recall from the paragraph after Lemma 2.13 that $\operatorname{card} \mathcal{R}' = r$, and $t_1, ..., t_r$ are the elements of $\mathcal{R}'$ in increasing order. The main results of this section are the following estimates on the minor arcs.

Theorem 2.18. *Suppose $k \geq 3$ and $p \nmid k$. Suppose further that either $p \nmid (k-1)$ or $p = mk^b + 1$, $m > 1$. Let $\kappa = \sum_{j=1}^{r} t_j$, where $\mathcal{R}' = \{t_1, ..., t_r\}$ and $t_j \leq t_{j+1}$. Let*

$$\delta_0 = \begin{cases} 1, & \text{if } p \nmid (k-1), \\ \frac{1}{4p^b}, & \text{if } k = mp^b + 1, m > 1. \end{cases}$$

Then we have

$$\int_{\mathfrak{m}} |g(\alpha)|^{2s} \, d\alpha \ll q^{(\kappa - k - \delta_0)X} J_s(\mathcal{R}', X),$$

where the implicit constant depends only on q and k.

Recall from above that if $p \nmid (k-1)$, then $r = k - \lfloor k/p \rfloor$. On the other hand, if $k = mp^b + 1$, then $r = (1 - 1/p)(k - p^b) + (1 + 1/p)$.

Corollary 2.19. *Suppose $k \geq 3$, $p \nmid k$ and $s \geq (rk + r)$. Suppose further that either $p \nmid (k-1)$ or $p = mk^b + 1$, $m > 1$. Let δ_0 be as in the statement of Theorem 2.18. Then for each $\epsilon > 0$, we have*

$$\int_{\mathfrak{m}} |g(\alpha)|^{2s} \, d\alpha \ll q^{(2s - k - \delta_0 + \epsilon)X},$$

where the implicit constant depends only on $s, q, k, \mathcal{R}'$, and ϵ.

Proof. This is an immediate consequence of applying Theorem 2.10 to Theorem 2.18. □

Before we begin with our proof of Theorem 2.18, we set some notation. First we define the following exponential sums:

$$f(\boldsymbol{\alpha}) = \sum_{x\in I_X} e\left(\sum_{j=1}^{r-1} \alpha_{t_j} x^{t_j} + \alpha_k x^k\right), \tag{2.51}$$

and

$$F(\boldsymbol{\beta},\theta) = \sum_{x\in I_X} e\left(\sum_{j=1}^{r-2} \beta_{t_j} x^{t_j} + \theta x^k\right). \tag{2.52}$$

We will also use the notation $f(\boldsymbol{\alpha},\theta)$ to mean

$$f(\boldsymbol{\alpha},\theta) = f(\alpha_{t_1}, \alpha_{t_2}, ..., \ \alpha_{t_{r-1}}, \theta).$$

We also define for $1 \le j \le k$,

$$\sigma_{s,j}(\mathbf{x}) = \sum_{i=1}^{s} (x_i^j - x_{s+i}^j). \tag{2.53}$$

Recall $J_s(\mathcal{R}', X)$ is the number of solutions of the system

$$u_1^j + ... + u_s^j = v_1^j + ... + v_s^j \quad (j \in \mathcal{R}')$$

with $u_j, v_j \in I_X$ $(1 \le j \le s)$. By the orthogonality relation (2.10), it follows that

$$J_s(\mathcal{R}', X) = \oint |f(\boldsymbol{\alpha})|^{2s} \, d\boldsymbol{\alpha}. \tag{2.54}$$

Proof of Theorem 2.18. We begin by expressing the mean value of $g(\alpha)$ in terms of mean value of $F(\boldsymbol{\beta},\theta)$. Since $\overline{F(\boldsymbol{\beta},\theta)} = F(-\boldsymbol{\beta},-\theta)$, we see that

$$\begin{aligned} |F(\boldsymbol{\beta},\theta)|^{2s} &= \prod_{i=1}^{s}\left(\sum_{x_i, x_{s+i}\in I_X} e\left(\sum_{j=1}^{r-2} \beta_{t_j}(x_i^{t_j} - x_{s+i}^{t_j}) + \theta(x_i^k - x_{s+i}^k)\right)\right) \\ &= \sum_{\operatorname{ord}\mathbf{x}<X} e\left(\sum_{j=1}^{r-2} \beta_{t_j}\sigma_{s,t_j}(\mathbf{x}) + \theta\sigma_{s,k}(\mathbf{x})\right). \end{aligned}$$

Then for $\mathbf{h} = (h_{t_1}, ..., h_{t_{r-2}}) \in \mathbb{F}_q[t]^{r-2}$, we have

$$\int_{\mathfrak{m}} \oint |F(\boldsymbol{\beta}, \theta)|^{2s} e\left(\sum_{j=1}^{r-2} -\beta_{t_j} h_{t_j}\right) \, d\boldsymbol{\beta} \, d\theta = \sum_{\operatorname{ord} \mathbf{x} < X} \delta(\mathbf{x}, \mathbf{h}) \int_{\mathfrak{m}} e(\theta \sigma_{s,k}(\mathbf{x})) \, d\theta, \tag{2.55}$$

where

$$\delta(\mathbf{x}, \mathbf{h}) = \prod_{j=1}^{r-2} \left(\oint e(\beta_{t_j}(\sigma_{s,t_j}(\mathbf{x}) - h_{t_j})) \, d\beta_{t_j} \right). \tag{2.56}$$

Thus, the orthogonality relation (2.10) gives us

$$\oint e(\beta_{t_j}(\sigma_{s,t_j}(\mathbf{x}) - h_{t_j})) \, d\beta_{t_j} = \begin{cases} 1, & \text{when } \sigma_{s,t_j}(\mathbf{x}) = h_{t_j}, \\ 0, & \text{when } \sigma_{s,t_j}(\mathbf{x}) \neq h_{t_j}. \end{cases} \tag{2.57}$$

When $\operatorname{ord} \mathbf{x} < X$, we have $\operatorname{ord} \sigma_{s,t_j}(\mathbf{x}) \leq t_j(X-1)$ for $1 \leq j \leq r-2$, and so it follows from (2.56) and (2.57) that

$$\sum_{\operatorname{ord} h_{t_1} \leq t_1(X-1)} \cdots \sum_{\operatorname{ord} h_{t_{r-2}} \leq t_{r-2}(X-1)} \delta(\mathbf{x}, \mathbf{h}) = 1. \tag{2.58}$$

Since

$$|g(\theta)|^{2s} = \sum_{\operatorname{ord} \mathbf{x} < X} e(\theta \sigma_{s,k}(\mathbf{x})),$$

we obtain by (2.55) and (2.58),

$$\begin{aligned} &\sum_{\operatorname{ord} h_{t_1} \leq t_1(X-1)} \cdots \sum_{\operatorname{ord} h_{t_{r-2}} \leq t_{r-2}(X-1)} \int_{\mathfrak{m}} \oint |F(\boldsymbol{\beta}, \theta)|^{2s} e\left(\sum_{j=1}^{r-2} -\beta_{t_j} h_{t_j}\right) \, d\boldsymbol{\beta} \, d\theta \\ = \ &\int_{\mathfrak{m}} \sum_{\operatorname{ord} \mathbf{x} < X} \left(\sum_{\mathbf{h}} \delta(\mathbf{x}, \mathbf{h}) \right) e(\theta \sigma_{s,k}(\mathbf{x})) \, d\theta \\ = \ &\int_{\mathfrak{m}} |g(\theta)|^{2s} \, d\theta. \end{aligned}$$

It therefore follows by the triangle inequality,

$$\begin{aligned}\int_{\mathfrak{m}} |g(\alpha)|^{2s}\, d\alpha &\leq \sum_{\operatorname{ord} h_{t_1} \leq t_1(X-1)} \cdots \sum_{\operatorname{ord} h_{t_{r-2}} \leq t_{r-2}(X-1)} \int_{\mathfrak{m}} \oint |F(\boldsymbol{\beta}, \theta)|^{2s}\, d\boldsymbol{\beta}\, d\theta \quad (2.59)\\ &\leq q^{(\kappa - k - t_{r-1})X} \int_{\mathfrak{m}} \oint |F(\boldsymbol{\beta}, \theta)|^{2s}\, d\boldsymbol{\beta}\, d\theta.\end{aligned}$$

An argument similar to that employed in the last paragraph permits us to relate the mean value of $F(\boldsymbol{\beta}, \theta)$ to a sum of integrals involving $f(\boldsymbol{\alpha}, \theta)$ as follows

$$\int_{\mathfrak{m}} \oint |F(\boldsymbol{\beta}, \theta)|^{2s}\, d\boldsymbol{\beta}\, d\theta = \sum_{\operatorname{ord} h \leq t_{r-1}(X-1)} \int_{\mathfrak{m}} \oint |f(\boldsymbol{\alpha}, \theta)|^{2s} e(-\alpha_{t_{r-1}} h)\, d\boldsymbol{\alpha}\, d\theta. \qquad (2.60)$$

The advantage of this maneuver is that we can rewrite the integral in the summand with similar expression involving an extra new variable $y \in I_X$. We then take the average of these integrals over $y \in I_X$ to get a sharper upper bound for the left hand side of (2.60), which ultimately gives us the desired result. This task will be achieved during the course of the rest of the proof, but first we prove (2.60). For $h \in \mathbb{F}_q[t]$, let

$$\widetilde{\delta}(\mathbf{x}, h) = \oint e(\alpha_{t_{r-1}}(\sigma_{s,t_{r-1}}(\mathbf{x}) - h))\, d\alpha_{t_{r-1}}. \qquad (2.61)$$

We have by the orthogonality relation (2.10),

$$\widetilde{\delta}(\mathbf{x}, h) = \begin{cases} 1, & \text{when } \sigma_{s,t_{r-1}}(\mathbf{x}) = h, \\ 0, & \text{when } \sigma_{s,t_{r-1}}(\mathbf{x}) \neq h. \end{cases}$$

Clearly, $\operatorname{ord} \mathbf{x} < X$ implies $\operatorname{ord} \sigma_{s,t_{r-1}}(\mathbf{x}) \leq t_{r-1}(X-1)$. Hence we have

$$\sum_{\operatorname{ord} h \leq t_{r-1}(X-1)} \widetilde{\delta}(\mathbf{x}, h) = 1. \qquad (2.62)$$

Since $\overline{f(\boldsymbol{\alpha},\theta)} = f(-\boldsymbol{\alpha},-\theta)$, we get

$$\begin{aligned}|f(\boldsymbol{\alpha},\theta)|^{2s} &= \prod_{i=1}^{s}\left(\sum_{x_i,x_{s+i}\in I_X} e\left(\sum_{j=1}^{r-1}\alpha_{t_j}(x_i^{t_j}-x_{s+i}^{t_j})+\theta(x_i^k-x_{s+i}^k)\right)\right)\\ &= \sum_{\operatorname{ord}\mathbf{x}<X} e\left(\sum_{j=1}^{r-1}\alpha_{t_j}\sigma_{s,t_j}(\mathbf{x})+\theta\sigma_{s,k}(\mathbf{x})\right).\end{aligned}$$

Thus, it follows by (2.61) that

$$\int_{\mathfrak{m}}\oint |f(\boldsymbol{\alpha},\theta)|^{2s} e\left(-\alpha_{t_{r-1}}h\right)\, d\boldsymbol{\alpha}\, d\theta = \sum_{\operatorname{ord}\mathbf{x}<X}\widetilde{\delta}(\mathbf{x},h)\int_{\mathfrak{m}}\oint e\left(\sum_{j=1}^{r-2}\beta_{t_j}\sigma_{s,t_j}(\mathbf{x})+\theta\sigma_{s,k}(\mathbf{x})\right)\, d\boldsymbol{\beta}\, d\theta. \tag{2.63}$$

Therefore, we obtain by (2.62) and (2.63),

$$\begin{aligned}&\sum_{\operatorname{ord} h\le t_{r-1}(X-1)}\int_{\mathfrak{m}}\oint |f(\boldsymbol{\alpha},\theta)|^{2s} e\left(-\alpha_{t_{r-1}}h\right)\, d\boldsymbol{\alpha}\, d\theta \qquad (2.64)\\ &= \sum_{\operatorname{ord}\mathbf{x}<X}\ \sum_{\operatorname{ord} h\le t_{r-1}(X-1)}\widetilde{\delta}(\mathbf{x},h)\int_{\mathfrak{m}}\oint e\left(\sum_{j=1}^{r-2}\beta_{t_j}\sigma_{s,t_j}(\mathbf{x})+\theta\sigma_{s,k}(\mathbf{x})\right)\, d\boldsymbol{\beta}\, d\theta\\ &= \int_{\mathfrak{m}}\oint \sum_{\operatorname{ord}\mathbf{x}<X} e\left(\sum_{j=1}^{r-2}\beta_{t_j}\sigma_{s,t_j}(\mathbf{x})+\theta\sigma_{s,k}(\mathbf{x})\right)\, d\boldsymbol{\beta}\, d\theta\\ &= \int_{\mathfrak{m}}\oint |F(\boldsymbol{\beta},\theta)|^{2s}\, d\boldsymbol{\beta}\, d\theta,\end{aligned}$$

which is exactly the equation (2.60) we aimed to prove.

Given $y\in I_X$, observe that I_X is invariant under translation by y, or in other words

$$I_X = \{x : x\in\mathbb{F}_q[t], \operatorname{ord} x < X\} = \{x+y : x\in\mathbb{F}_q[t], \operatorname{ord} x < X\}.$$

Let

$$\lambda(z;\boldsymbol{\alpha}) = \sum_{j=1}^{r-1}\alpha_{t_j}z^{t_j}+\alpha_k z^k.$$

By the above observation, shifting the variable of summation in $f(\boldsymbol{\alpha})$ by y gives us

$$f(\boldsymbol{\alpha}) = \sum_{x \in I_X} e\left(\lambda(x; \boldsymbol{\alpha})\right) = \sum_{x \in I_X} e\left(\lambda(x - y; \boldsymbol{\alpha})\right). \tag{2.65}$$

Define $\Delta(\theta, h, y)$ as follows:

$$\Delta(\theta, h, y) = e(\theta \sigma_{s,k}(\mathbf{x} - y)),$$

when the $2s$-tuple $\mathbf{x}$ satisfies

$$\sum_{i=1}^{s} ((x_i - y)^{t_j} - (x_{s+i} - y)^{t_j}) = 0 \quad (1 \le j \le r - 2) \tag{2.66}$$

and

$$\sum_{i=1}^{s} ((x_i - y)^{t_{r-1}} - (x_{s+i} - y)^{t_{r-1}}) = h. \tag{2.67}$$

Otherwise, we let $\Delta(\theta, h, y) = 0$. Substituting the expression (2.65) for $f(\boldsymbol{\alpha}, \theta)$, we find by the orthogonality relation (2.10),

$$\oint |f(\boldsymbol{\alpha}, \theta)|^{2s} e(-\alpha_{t_{r-1}} h)\, d\boldsymbol{\alpha} = \sum_{\operatorname{ord} \mathbf{x} < X} \Delta(\theta, h, y). \tag{2.68}$$

We now simplify the function $\Delta(\theta, h, y)$ and obtain another expression for the left hand side of (2.68). First, we prove that the $2s$-tuple $\mathbf{x}$ satisfies (2.66) and (2.67) if and only if $\mathbf{x}$ satisfies

$$\sum_{i=1}^{s} (x_i^{t_j} - x_{s+i}^{t_j}) = 0 \quad (1 \le j \le r - 2) \tag{2.69}$$

and

$$\sum_{i=1}^{s} (x_i^{t_{r-1}} - x_{s+i}^{t_{r-1}}) = h. \tag{2.70}$$

Suppose $\mathbf{x}$ satisfies (2.66) and (2.67). Since $\mathbb{F}_q$ has characteristic p, we have $(x-y)^p = x^p - y^p$. Recall $t_{r-1} = j_0$. Thus, we can prove by induction and the definition of $\mathcal{R}'$ that (2.66) implies

$$\sum_{i=1}^{s} ((x_i - y)^j - (x_{s+i} - y)^j) = 0 \quad (1 \le j < t_{r-1}). \tag{2.71}$$

Note we can verify that $t_{r-1} > 1$ for the cases we consider here. By applying the binomial theorem, we obtain that whenever a $2s$-tuple $\mathbf{x}$ satisfies (2.67) and the system (2.71), then $\mathbf{x}$ satisfies

$$\sum_{i=1}^{s}(x_i^j - x_{s+i}^j) = 0 \quad (1 \le j < t_{r-1}) \tag{2.72}$$

and (2.70). Clearly the system (2.72) implies (2.69). For the converse direction, since (2.69) implies (2.72), we can obtain the desired result in a similar manner as in the forward direction.

Suppose $\mathbf{x}$ satisfies (2.69) and (2.70), and consequently (2.72). If $p \nmid (k-1)$, then $t_{r-1} = j_0 = k-1$ and we have

$$\sigma_{s,k}(\mathbf{x} - y) = \sum_{i=1}^{s}((x_i - y)^k - (x_{s+i} - y)^k) = \sigma_{s,k}(\mathbf{x}) - chy^{k-t_{r-1}}, \tag{2.73}$$

where $c = \binom{k}{t_{r-1}} \not\equiv 0 \pmod{p}$. If $k = mp^b + 1$, then we can deduce from $t_{r-1} = j_0 = (m-1)p^b + 1 > m$, which we note does not hold if $m = 1$, and (2.72) that

$$\sum_{i=1}^{s} x_i^{k-1} - x_{s+i}^{k-1} = \left(\sum_{i=1}^{s} x_i^m - x_{s+i}^m\right)^{p^b} = 0.$$

Therefore, by the binomial theorem, the above equation, and the definition of j_0 given in (2.25), we also obtain (2.73) when k is of the form $k = mp^b + 1$, $m > 1$. Thus, we can rewrite the definition of $\Delta(\theta, h, y)$ as

$$\Delta(\theta, h, y) = e(\theta\sigma_{s,k}(\mathbf{x}) - chy^{k-t_{r-1}}\theta),$$

whenever $\mathbf{x}$ satisfies (2.69) and (2.70); otherwise, $\Delta(\theta, h, y)$ is equal to 0. Thus, we have

$$\oint |f(\boldsymbol{\alpha}, \theta)|^{2s} e(-chy^{k-t_{r-1}}\theta - \alpha_{t_{r-1}}h)\, d\boldsymbol{\alpha} = \sum_{\operatorname{ord}\mathbf{x} < X} \Delta(\theta, h, y),$$

and consequently, it follows from (2.68) that

$$\oint |f(\boldsymbol{\alpha}, \theta)|^{2s} e(-\alpha_{t_{r-1}}h)\, d\boldsymbol{\alpha} = \oint |f(\boldsymbol{\alpha}, \theta)|^{2s} e(-chy^{k-t_{r-1}}\theta - \alpha_{t_{r-1}}h)\, d\boldsymbol{\alpha}.$$

From here, we have by (2.60),

$$\begin{aligned} &\int_{\mathfrak{m}} \oint |F(\boldsymbol{\beta},\theta)|^{2s}\ d\boldsymbol{\beta}\ d\theta \\ = &\int_{\mathfrak{m}} \oint |f(\boldsymbol{\alpha},\theta)|^{2s} \sum_{\operatorname{ord} h \le t_{r-1}(X-1)} e(-chy^{k-t_{r-1}}\theta - \alpha_{t_{r-1}}h)\ d\boldsymbol{\alpha}\ d\theta. \end{aligned} \tag{2.74}$$

Since the left hand side of (2.74) is independent of y, we can average the right hand side over $y \in I_X$ to obtain

$$\begin{aligned} &\int_{\mathfrak{m}} \oint |F(\boldsymbol{\beta},\theta)|^{2s}\ d\boldsymbol{\beta}\ d\theta \\ = \ & q^{-X} \sum_{y \in I_X} \int_{\mathfrak{m}} \oint |f(\boldsymbol{\alpha},\theta)|^{2s} \sum_{\operatorname{ord} h \le t_{r-1}(X-1)} e(-chy^{k-t_{r-1}}\theta - \alpha_{t_{r-1}}h)\ d\boldsymbol{\alpha}\ d\theta \\ = \ & \int_{\mathfrak{m}} \oint |f(\boldsymbol{\alpha},\theta)|^{2s} \psi(\theta, \alpha_{t_{r-1}})\ d\boldsymbol{\alpha}\ d\theta. \end{aligned} \tag{2.75}$$

In the last equality displayed above, we invoked (2.30), the definition of $\psi(\theta,\alpha)$. We apply the appropriate lemma depending on k from Section 2.3, namely Lemmas 2.15, 2.16 and 2.17, to $\psi(\theta,\alpha)$ and obtain an upper bound for the right hand side of (2.75). We then use the resulting estimate and (2.54) to bound (2.59), from which we obtain

$$\int_{\mathfrak{m}} |g(\alpha)|^{2s}\ d\alpha \ll q^{(\kappa-k-t_{r-1})X} q^{(j_0-\delta)X} J_s(\mathcal{R}', X) = q^{(\kappa-k-\delta)X} J_s(\mathcal{R}', X), \tag{2.76}$$

for suitable $\delta > 0$. □

2.4.2 Case $k = p^b + 1$

Recall from above that if $k = p^b + 1$, then $r = (1-1/p)(k-p^b) + (1+1/p) = 2$. We obtain the following minor arc bound when $k = p^b + 1$.

Theorem 2.20. *Suppose $k \geq 3$ and $k = p^b + 1$. Let $\kappa = 1 + k$, $\mathcal{R}' = \{1, k\}$, and*

$$\delta_0 = \frac{1}{16(p^b+2)}.$$

Then we have

$$\int_{\mathfrak{m}} |g(\alpha)|^{2s+1} \, d\alpha \ll q^{(1+\kappa-k-\delta_0)X} J_s(\mathcal{R}', X),$$

where the implicit constant depends only on q and k.

By applying Theorem 2.10 to Theorem 2.20, we also obtain the following corollary.

Corollary 2.21. *Suppose $k \geq 3$, $k = p^b + 1$, and $s \geq (2k+2)$. Let*

$$\delta_0 = \frac{1}{16(p^b+2)}.$$

Then for each $\epsilon > 0$, we have

$$\int_{\mathfrak{m}} |g(\alpha)|^{2s+1} \, d\alpha \ll q^{(2s+1-k-\delta_0+\epsilon)X},$$

where the implicit constant depends only on s, q, k, and ϵ.

We introduce some notation before we get into the proof of Theorem 2.20. Given $j, j' \in \mathbb{Z}^+$, we write $j \preceq_p j'$ if $p \nmid \binom{j'}{j}$. 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 $j \preceq_p j'$, then we necessarily have $j \leq j'$. Let $\mathcal{K} \subseteq \mathbb{Z}^+$. We say an element $k \in \mathcal{K}$ is *maximal* if it is maximal with respect to $\preceq_p$, that is, for any $j \in \mathcal{K}$, either $j \preceq_p k$ or j and k are not comparable. Following the notation of [12], we define the *shadow* of $\mathcal{K}$, $\mathcal{S}(\mathcal{K})$, to be

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

We also define

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

We invoke the following result from [12]. The theorem allows us to estimate certain coefficients of a polynomial $h(u)$ by an element in $\mathbb{K}$ when the exponential sum of $h(u)$ is sufficiently large. We use the result to bound exponential sums over the minor arcs.

Theorem 2.22 (Theorem 12, [12])**.** *Let $\mathcal{K} \subseteq \mathbb{Z}^+$ and $h(u) = \sum_{j \in \mathcal{K} \cup \{0\}} \alpha_j u^j \in \mathbb{K}_\infty[u]$, where $\alpha_j \neq 0$ $(j \in \mathcal{K})$. Suppose that $k \in \mathcal{K}^*$ 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 $0 < \eta \leq cX$, we have

$$\Big| \sum_{x \in I_X} e(h(x)) \Big| \geq q^{X-\eta}.$$

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

$$\operatorname{ord}(g\alpha_k - a) < -kX + \epsilon X + C\eta \quad \textit{and} \quad \operatorname{ord} g \leq \epsilon X + C\eta.$$

Proof of Theorem 2.20. We bound $\sup_{\theta \in \mathfrak{m}} |g(\theta)|$ using Theorem 2.22. For $g(\theta)$ with $k = p^b + 1$, we have $\mathcal{K} = \{k\}$, and thus

$$\mathcal{S}(\mathcal{K}) = \{k, p^b, 1\},$$

and

$$\mathcal{K}^* = \{k\}.$$

Clearly, k is maximal in $\mathcal{K}$. We also have

$$\begin{aligned} \mathcal{S}(\mathcal{K})' &:= \{i \in \mathbb{N} : p \nmid i \text{ and } p^v i \in \mathcal{S}(\mathcal{K}) \text{ for some } v \in \mathbb{N} \cup \{0\}\} \\ &= \{k, 1\}. \end{aligned}$$

It is given at the end of the proof of [12, Theorem 12] that we may take $c = 1/(8(r_0\phi + r_0))$ and $C = 2(r_0\phi + r_0)$, where $r_0 = \#\ \mathcal{S}(\mathcal{K})'$ and $\phi = \max_{i \in \mathcal{S}(\mathcal{K})'} i$. Therefore, we can apply Theorem 2.22 with

$$c = \frac{1}{8(2k+2)} = \frac{1}{16(p^b+2)} \quad \text{and} \quad C = 2(2k+2).$$

Take any $\theta \in \mathfrak{m}$. We set $\epsilon = 1/2$. Suppose for some X sufficiently large, with respect to $\mathcal{K}$ and q, we have

$$|g(\theta)| \geq q^{X - cX}.$$

Then, by Theorem 2.22, there exist $\tilde{g}, \tilde{a} \in \mathbb{F}_q[t]$ such that

$$\operatorname{ord}(\tilde{g}\theta - \tilde{a}) < -kX + \epsilon X + \frac{1}{4}X \quad \text{and} \quad \operatorname{ord} \tilde{g} \leq \epsilon X + \frac{1}{4}X.$$

Let $(\tilde{g}, \tilde{a}) = \ell$, and denote $\tilde{g} = \ell g_0$ and $\tilde{a} = \ell a_0$. We obtain from above inequalities,

$$\operatorname{ord}(\theta - a_0/g_0) = \operatorname{ord}(\theta - \tilde{a}/\tilde{g}) < -kX + \epsilon X + \frac{1}{4}X - \operatorname{ord}\tilde{g} \leq -(k-1)X - \operatorname{ord} g_0$$

and

$$\operatorname{ord} g_0 \leq \operatorname{ord}\tilde{g} \leq \epsilon X + \frac{1}{4}X < X.$$

By the definition of major arcs (2.14), this implies that $\theta \in \mathfrak{M}_k$, which is a contradiction. Therefore, we must have

$$|g(\theta)| < q^{X - cX}$$

for all X sufficiently large with respect to $\mathcal{K}$ and q. Since the result is independent of the choice of $\theta \in \mathfrak{m}$, it follows that

$$\sup_{\theta \in \mathfrak{m}_k} |g(\theta)| < q^{X - \frac{1}{16(p^b+2)}X}. \tag{2.77}$$

When $k = p^b + 1$, we have $r = 2$; therefore, we have $F(\boldsymbol{\beta}, \theta) = g(\theta)$. Thus, we obtain by (2.60) and the triangle inequality that

$$\begin{aligned} & \int_{\mathfrak{m}} |g(\theta)|^{2s+1} \, d\theta \\ \leq\ & \sup_{\theta \in \mathfrak{m}} |g(\theta)| \cdot \int_{\mathfrak{m}} |g(\theta)|^{2s} \, d\theta \\ =\ & \sup_{\theta \in \mathfrak{m}} |g(\theta)| \cdot \sum_{h \in I_X} \int_{\mathfrak{m}} \oint |f(\alpha, \theta)|^{2s} e(-\alpha h) \, d\alpha \, d\theta \\ \leq\ & \sup_{\theta \in \mathfrak{m}} |g(\theta)| \cdot q^X \cdot \oint \oint |f(\alpha, \theta)|^{2s} \, d\alpha \, d\theta \\ =\ & \sup_{\theta \in \mathfrak{m}} |g(\theta)| \cdot q^X \cdot J_s(\mathcal{R}', X). \end{aligned} \tag{2.78}$$

Consequently, substituting (2.77) into the above inequality (2.78) gives us

$$\int_{\mathfrak{m}} |g(\theta)|^{2s+1} \, d\theta \ll q^{2X - \frac{1}{16(p^b+2)}X} J_s(\mathcal{R}', X).$$

□

2.5 Weyl Differencing

Let $w_0(u)$ be a polynomial in $\mathbb{F}_q[t][u]$. Let $z_1, ..., z_h$ be indeterminates. We define the differencing operator Δ_{z_1} by

$$\Delta_{z_1}(w_0)(u) = w_0(u+z) - w_0(u) \in \mathbb{F}_q[t][u, z_1],$$

where we denote $\Delta_{z_1}(w_0) = \Delta_{z_1}(w_0)(u)$. We also define recursively

$$\Delta_{z_h}...\Delta_{z_1}(w_0)(u) = \Delta_{z_{h-1}}...\Delta_{z_1}(w_0)(u+z_h) - \Delta_{z_{h-1}}...\Delta_{z_1}(w_0)(u) \in \mathbb{F}_q[t][u, z_1, ..., z_h],$$

and we denote $\Delta_{z_h}...\Delta_{z_1}(w_0) = \Delta_{z_h}...\Delta_{z_1}(w_0)(u)$.

While in characteristic zero the above differencing process, known as Weyl differencing, decreases the degree (in u) of the polynomial by one, the situation in positive characteristic is more subtle. With application of Hua's lemma (Proposition 2.24) in mind, it will be useful to know how many times one can apply Weyl differencing to u^k in $\mathbb{F}_q[t][u]$ before it becomes identically zero. Note that given an indeterminate z and a monomial u^ℓ, we have $\Delta_z(u^\ell) = 0$ if and only if $\ell = 0$. To see this, suppose we have $\ell \geq 1$ and

$$0 = \Delta_z(u^\ell) = (u+z)^\ell - u^\ell = \sum_{j=0}^{\ell-1} \binom{\ell}{j} u^j z^{\ell-j}.$$

Then, in particular it must be that $\binom{\ell}{0} = 1 \equiv 0 \pmod{p}$, which is a contradiction. Therefore, we have $\ell = 0$. The converse direction is trivial. The following lemma can be obtained by a slight modification of [15, Lemma 8.1], but for the sake of completeness we present the proof below.

Lemma 2.23. *Let $k = c_v p^v + ... + c_0$ with $0 \leq c_i < p$ $(0 \leq i \leq v)$, and let $h_0 = h_0(k) = c_v + ... + c_0$. Let $z_1, ..., z_{h_0+1}$ be indeterminates. Then, we have*

$$0 \neq \Delta_{z_{h_0}}...\Delta_{z_1} u^k \in \mathbb{F}_q[t][u, z_1, ..., z_{h_0}]$$

and

$$0 = \Delta_{z_{h_0+1}}...\Delta_{z_1} u^k \in \mathbb{F}_q[t][u, z_1, ..., z_{h_0+1}].$$

Proof. For conveneince we use z_0 in place of u here. It is clear that $\Delta_{z_h}...\Delta_{z_1}{z_0}^k$ is a homogeneous polynomial of degree k in $z_0, z_1, ..., z_h$. Let S_h be the collection of $(h+1)$-tuples $\mathbf{i} = (i_0, ..., i_h)$ such that the coefficient of $\mathbf{z}^\mathbf{i} = z_0^{i_0}...z_h^{i_h}$ in $\Delta_{z_h}...\Delta_{z_1}{z_0}^k$ is not zero. Let $\Delta_{z_h}...\Delta_{z_1}{z_0}^k = \sum_{\mathbf{i}\in S_h} c_\mathbf{i}\mathbf{z}^\mathbf{i}$.

Suppose $\mathbf{i} = (i_0, ..., i_h), \mathbf{i}' = (i'_0, ..., i'_h) \in S_h$ and $\mathbf{i} \neq \mathbf{i}'$. Let

$$\Delta_{z_{h+1}} c_{\mathbf{i}} \mathbf{z}^{\mathbf{i}} = c_{\mathbf{i}} z_1^{i_1} ... z_h^{i_h} \Delta_{z_{h+1}} z_0^{i_0} = c_{\mathbf{i}} z_1^{i_1} ... z_h^{i_h} \sum_{a=0}^{i_0 - 1} \binom{i_0}{a} z_0^a z_{h+1}^{i_0 - a} = \sum_{a=0}^{i_0 - 1} c_{\mathbf{i}} \binom{i_0}{a} z_0^a z_1^{i_1} ... z_h^{i_h} z_{h+1}^{i_0 - a},$$

and similarly,

$$\Delta_{z_{h+1}} c_{\mathbf{i}'} \mathbf{z}^{\mathbf{i}'} = \sum_{a'=0}^{i'_0 - 1} c_{\mathbf{i}'} \binom{i'_0}{a'} z_0^{a'} z_1^{i'_1} ... z_h^{i'_h} z_{h+1}^{i'_0 - a'}.$$

We claim that $\Delta_{z_{h+1}} c_{\mathbf{i}} \mathbf{z}^{\mathbf{i}}$ and $\Delta_{z_{h+1}} c_{\mathbf{i}'} \mathbf{z}^{\mathbf{i}'}$ have no monomials in common. This is clear if there exists some $0 < w \leq h$ for which $i_w \neq i'_w$. On the other hand, if $i_w = i'_w$ $(0 < w \leq h)$, then we must have $i_0 \neq i'_0$. In this case, since there do not exist $0 \leq a < i_0$ and $0 \leq a' < i'_0$ which satisfy $(a, i_0 - a) = (a', i'_0 - a')$, the claim follows. Thus, no cancellation can occur amongst the monomials of $\Delta_{z_{h+1}} c_{\mathbf{i}} \mathbf{z}^{\mathbf{i}}$ and $\Delta_{z_{h+1}} c_{\mathbf{i}'} \mathbf{z}^{\mathbf{i}'}$ for any distinct $\mathbf{i}$ and $\mathbf{i}' \in S_h$. Therefore, it follows that if we can find a monomial $\mathbf{z}^{\mathbf{i}}$ with $\mathbf{i} \in S_h$ such that $\Delta_{z_{h+1}} \mathbf{z}^{\mathbf{i}}$ has at least one monomial divisible by z_0, then $\Delta_{z_{h+1}} ... \Delta_{z_1} {z_0}^k \notin \mathbb{F}_q[t][z_1, ..., z_{h+1}]$. In other words, $\Delta_{z_{h+1}} ... \Delta_{z_1} {z_0}^k$ has a monomial with a factor of z_0 and $\Delta_{z_{h+2}} ... \Delta_{z_1} {z_0}^k \neq 0$ in $\mathbb{F}_q[t][z_0, z_1, ..., z_{h+2}]$.

Suppose we have $\ell = a_v p^v + ... + a_0$ with $0 \leq a_i < p$ $(0 \leq i \leq v)$. By Lemma 2.11, we have that

$$\binom{\ell}{n} \not\equiv 0 \ (\mathrm{mod}\ p) \tag{2.79}$$

if and only if $n \in \{\ell\} \cup A_\ell$, where

$$A_\ell := \{n \in \mathbb{N} \cup \{0\} : n = d_v p^v + ... + d_1 p + d_0 \text{ with } 0 \leq d_i \leq a_i \ (0 \leq i \leq v) \text{ and } n < \ell\}.$$

Therefore, it follows that if $\mathbf{i} \in S_h$, then

$$\Delta_{z_{h+1}} c_{\mathbf{i}} \mathbf{z}^{\mathbf{i}} = \sum_{n \in A_{i_0}} c_{\mathbf{i}} \binom{i_0}{n} z_0^n z_1^{i_1} ... z_h^{i_h} z_{h+1}^{i_0 - n}. \tag{2.80}$$

In particular, every coefficient in (2.80) is non-zero.

Consider a finite sequence of natural numbers $\{s_j\}$ constructed in the following way. Let $s_0 = k$. Pick any monomial $z_0^a z_1^{k-a}$ of $\Delta_{z_1} {z_0}^k$ with non-zero coefficient and let $s_1 = a$. Then pick any monomial of $\Delta_{z_2} z_0^a z_1^{k-a}$ with non-zero coefficient and let s_2 be its exponent of z_0. We define s_j recursively until $s_T = 0$ for some T, where we terminate the procedure.

Define $h_0 := h_0(k)$ to be the number such that

$$\Delta_{z_{h_0}} ... \Delta_{z_1} {z_0}^k \neq 0,$$

but

$$\Delta_{z_{h_0+1}} ... \Delta_{z_1} {z_0}^k = 0.$$

It is easy to see that h_0 is exactly the maximum value of T we can obtain from the sequence $\{s_j\}$.

It follows from (2.80) that if $s_j = \ell$, then

$$s_{j+1} \in A_\ell.$$

Therefore, in order to construct the sequence $\{s_j\}$ with maximum value of T, at each step we do the following. Suppose $s_j = a_v p^v + ... + a_0$ with $0 \leq a_i < p$ $(0 \leq i \leq v)$. We pick any w such that $a_w \neq 0$. Note that we can always find such w as long as $s_j \neq 0$. We let $s_{j+1} = s_j - p^w$. It is then immediate that the maximum value of T we can achieve is $(c_v + ... + c_0)$. □

Combining Lemma 2.23 and [19, Proposition 13], we have the following version of Hua's lemma.

Proposition 2.24. *Let $w_0(u)$ be a polynomial in $\mathbb{F}_q[t][u]$ of degree k in u, and let $w(\alpha) = \sum_{x \in I_X} e(w_0(x)\alpha)$. Let $h_0(k)$ be as defined in the statement of Lemma 2.23. Suppose $j \leq h_0(k)$. Then for every $\epsilon > 0$, we have*

$$\oint |w(\alpha)|^{2^j} \, d\alpha \ll q^{(2^j - j + \epsilon)X},$$

where the implicit constant depends only on k, q, and ϵ.

We apply Proposition 2.24 in Sections 2.6 and 2.7 with $w_0(u) = u^k$.

2.6 Asymptotic Formula and $\tilde{G}_q(k)$

We now lower the bound on s in Corollary 2.19 via combination of Proposition 2.24 and Hölder's inequality, and obtain Theorems 2.3 and 2.4. First, we consider the case when $p \nmid (k-1)$ in Proposition 2.25. We then take care of the case $k = mp^b + 1$ in Proposition 2.26.

Let

$$s_0'(j) = 2k^2 + 1 - \left\lceil \frac{2kj - 2^j}{k+1-j} \right\rceil.$$

If $k < p$, we set

$$s_1(k) = \min_{\substack{1 \le j < k \\ 2^j \le k(2k+1)}} s_0'(j). \tag{2.81}$$

On the other hand, if $k > p$ and $p \nmid (k-1)$, we set

$$s_1(k) = 2rk + 1 - \left\lceil \frac{6r-8}{k-2} \right\rceil. \tag{2.82}$$

Proposition 2.25. *Suppose $k \ge 3$, $p \nmid k$, and $p \nmid (k-1)$. Let $s_1(k)$ be as given in (2.81) when $k < p$ and in (2.82) when $k > p$. If $s \ge s_1(k)$, then there exists $\delta_1 > 0$ such that*

$$\int_{\mathfrak{m}} |g(\alpha)|^s \, d\alpha \ll q^{(s-k-\delta_1)X},$$

where the implicit constant depends only on $s, q, k, \mathcal{R}'$, and δ_1.

Proof. Let $h_0(k)$ be as in the statement of Lemma 2.23. We have by Proposition 2.24, if $j \le h_0(k)$, then for any $\epsilon > 0$,

$$\oint |g(\alpha)|^j \, d\alpha \ll q^{(2^j - j + \epsilon)X}. \tag{2.83}$$

We let $s_0(j) = 2r(k+1)a' + 2^j b'$, where $a' + b' = 1$. Then Hölder's inequality gives us

$$\int_{\mathfrak{m}} |g(\alpha)|^{s_0(j)} \, d\alpha \le \left(\int_{\mathfrak{m}} |g(\alpha)|^{2r(k+1)} \, d\alpha \right)^{a'} \left(\oint |g(\alpha)|^{2^j} \, d\alpha \right)^{b'}. \tag{2.84}$$

Recall for the range of k we are considering, we can take $\delta_0 = 1$ in Corollary 2.19. We consider j in the following range: $1 \le j < k$, $2^j \le (2r-1)(k+1)+1$ and $j \le h_0(k)$. Define

$$\eta(j) = \frac{2rj}{k-j+1} - \frac{2^j}{k-j+1}$$

and let

$$\gamma(j) = 1 + \eta(j) - \lceil \eta(j) \rceil.$$

We choose

$$a' = \frac{k-j}{k-j+1} + \frac{\gamma(j)}{2r(k+1)-2^j}$$

and

$$b' = \frac{1}{k-j+1} - \frac{\gamma(j)}{2r(k+1)-2^j}.$$

Note that our restriction on j ensures $b' > 0$. Also, this choice of a' and b' ensures $a' - (k-j)b' > 0$. Then, by Corollary 2.19 and (2.83), we have the following bound for (2.84):

$$\int_{\mathfrak{m}} |g(\alpha)|^{s_0(j)}\, d\alpha \ll q^{\epsilon X} q^{a'(2r(k+1)-k-1)X} q^{b'(2^j-j)X} \ll q^{(s_0(j)-k-(a'-(k-j)b')+\epsilon)X}.$$

By the trivial bound $|g(\alpha)| \leq q^X$, it follows that for any $s \geq s_0(j)$ we have

$$\int_{\mathfrak{m}} |g(\alpha)|^{s}\, d\alpha \ll q^{(s-s_0(j))X} \int_{\mathfrak{m}} |g(\alpha)|^{s_0(j)}\, d\alpha \ll q^{(s-k-(a'-(k-j)b')+\epsilon)X}.$$

We can simplify $s_0(j)$ as

$$\begin{aligned} s_0(j) &= 2r(k+1)\left(\frac{k-j}{k-j+1} + \frac{\gamma(j)}{2r(k+1)-2^j}\right) + 2^j\left(\frac{1}{k-j+1} - \frac{\gamma(j)}{2r(k+1)-2^j}\right) \\ &= 2rk - \eta(j) + \gamma(j) \\ &= 2rk + 1 - \lceil \eta(j) \rceil. \end{aligned}$$

To establish our result, all we have left is to choose j within the appropriate range given above such that $s_0(j)$ is as small as possible. This value of $s_0(j)$ will be our $s_1(k)$. We consider the two cases separately.

Case 1: $k > p$. From $p \nmid k$, $p \nmid (k-1)$, and $k > p$, we can verify that $3 \leq h_0(k)$. Thus we know we can apply Weyl differencing at least three times. Therefore, we set $s_1(k) = s_0(3)$. Since

$$0 < \eta(3) = \frac{6r-8}{k-2}, \tag{2.85}$$

we obtain

$$s_1(k) = 2rk + 1 - \left\lceil \frac{6r-8}{k-2} \right\rceil.$$

Case 2: $k < p$. In this case, we have $h_0(k) = k$. We set

$$s_1(k) = \min_{\substack{1 \le j < k \\ 2^j \le (2r-1)(k+1)+1}} s_0(j). \tag{2.86}$$

Since $r = k - \lfloor k/p \rfloor = k$, we have $s_0(j) = s_0'(j)$ and $(2r-1)(k+1)+1 = k(2k+1)$. Therefore, we see that $s_1(k)$ given above in (2.86) coincides with (2.81).

□

Now we consider the case $k = mp^b + 1$. If $m = 1$, we set $s_1(k) = 4k+5$. If $m > 1$, then we set

$$s_1(k) = 2rk + 2r - \left\lfloor \frac{(m-1)(1-1/p)}{2} \right\rfloor. \tag{2.87}$$

Proposition 2.26. *Suppose $k = mp^b + 1$ with $p \nmid m$. Let $s_1(k)$ be $4k+5$ when $m = 1$ and as in (2.87) when $m > 1$. If $s \ge s_1(k)$, then there exists $\delta_1 > 0$ such that*

$$\int_{\mathfrak{m}} |g(\alpha)|^s \, d\alpha \ll q^{(s-k-\delta_1)X},$$

where the implicit constant depends only on $s, q, k, \mathcal{R}'$, and δ_1.

Proof. We first deal with the case $m > 1$. Let $h_0(k)$ be as in the statement of Lemma 2.23. If $j \le h_0(k)$, then for any $\epsilon > 0$ we have (2.83). We let $s_0(j) = 2r(k+1)a' + 2^j b'$, where $a' + b' = 1$, as before in Proposition 2.25. Then by Hölder's inequality, we have (2.84). We consider j in the following range: $1 \le j < k$, $2^j \le (2r-1)(k+1)+1$ and $j \le h_0(k)$. Let $\epsilon(j)$ be a small positive number. We choose

$$a' = \frac{k-j}{k-j+\delta} + \frac{\epsilon(j)}{2r(k+1) - 2^j}$$

and

$$b' = \frac{\delta}{k-j+\delta} - \frac{\epsilon(j)}{2r(k+1) - 2^j},$$

where we let $\delta = \delta_0 = 1/(4p^b)$ from Corollary 2.19.

Note that we pick $\epsilon(j)$ sufficiently small to make sure $b' > 0$. Also, the range of j we are considering and this choice of a' and b' ensure

$$\delta a' - (k-j)b' = \frac{(\delta + k - j)\epsilon(j)}{2r(k+1) - 2^j} > 0.$$

By Corollary 2.19 and (2.83), we have the following bound for (2.84):

$$\int_{\mathfrak{m}} |g(\alpha)|^{s_0(j)}\ d\alpha \ll q^{\epsilon X} q^{a'(2r(k+1)-k-\delta)X} q^{b'(2^j-j)X} \ll q^{(s_0(j)-k-(\delta a'-(k-j)b')+\epsilon)X}.$$

By the trivial bound $|g(\alpha)| \leq q^X$, it follows that for any $s \geq s_0(j)$ we have

$$\int_{\mathfrak{m}} |g(\alpha)|^{s}\ d\alpha \ll q^{(s-s_0(j))X} \int_{\mathfrak{m}} |g(\alpha)|^{s_0(j)}\ d\alpha \ll q^{(s-k-(\delta a'-(k-j)b')+\epsilon)X}.$$

We can simplify $s_0(j)$ as

$$\begin{aligned} s_0(j) &= 2r(k+1)\left(\frac{k-j}{k-j+\delta} + \frac{\epsilon(j)}{2r(k+1)-2^j}\right) + 2^j\left(\frac{\delta}{k-j+\delta} - \frac{\epsilon(j)}{2r(k+1)-2^j}\right) \\ &= 2rk + 2(1-\delta)k - \frac{2r(j+(1-\delta)(\delta-j))}{k-j+\delta} + \frac{2^j\delta}{k-j+\delta} + \epsilon(j) \\ &= 2rk + 2(1-\delta)r - \delta\frac{2r(1+j-\delta)-2^j}{k-j+\delta} + \epsilon(j) \\ &= 2rk + 2r - \delta\frac{2r(k+1)-2^j}{k-j+\delta} + \epsilon(j). \end{aligned}$$

To establish our result, all we have left is to choose j within the appropriate range given above such that $s_0(j)$ is as small as possible. We would like to maximize the value

$$\delta\frac{2r(k+1)-2^j}{k-j+\delta}$$

in order to minimize $s_0(j)$. We then let the smallest integer greater than the $s_0(j)$ found to be our $s_1(k)$.

Since $m > 1$, we can verify that $h_0(k) \geq 3$. Thus we know we can apply Weyl differencing at least three times. We have

$$r = (1-1/p)(k-p^b) + (1+1/p) = (m-1)(p^b - p^{b-1}) + 2.$$

Also, recall from above we have set $\delta = \delta_0 = 1/(4p^b)$. Let $j = 3$ and we obtain

$$\begin{aligned}
s_0(3) &= 2rk + 2r - \frac{2r(k+1) - 2^3}{4p^b(k-3+\delta)} + \epsilon(3) \\
&= 2rk + 2r - \frac{2(m-1)(p^b - p^{b-1})(k+1)}{4p^b(k-3+\delta)} - \frac{4(k+1)}{4p^b(k-3+\delta)} + \frac{8}{4p^b(k-3+\delta)} + \epsilon(3) \\
&= 2rk + 2r - \frac{(m-1)(1-1/p)(k+1)}{2(k-3+\delta)} - \frac{k-1}{p^b(k-3+\delta)} + \epsilon(3) \\
&\leq 2rk + 2r - \frac{(m-1)(1-1/p)(k+1)}{2(k-3+\delta)} \\
&\leq 2rk + 2r - \frac{(m-1)(1-1/p)}{2}.
\end{aligned}$$

Therefore, we let $s_1(k) = \left\lceil 2rk + 2r - \frac{(m-1)(1-1/p)}{2} \right\rceil = 2rk + 2r - \left\lfloor \frac{(m-1)(1-1/p)}{2} \right\rfloor \geq s_0(3)$.

The case $m = 1$ is an immediate consequence of Corollary 2.21. When $m = 1$, we have $r = 2$ and the saving in the exponent of $\delta_0 = \frac{1}{16(p^b+2)}$ from Corollary 2.21, however, with these values our approach above is not effective as in the case $m > 1$. Therefore, we let $s_1(k) = 4k + 5$ in this case. □

We are now in position to prove Theorems 2.3 and 2.4. By using the bounds on minor arcs from this section, we obtain an estimate for $\widetilde{G}_q(k)$.

Proof of Theorems 2.3 and 2.4. Let $n \in \mathbb{J}_q^k[t]$. By applying Theorem 2.9 and Propositions 2.25 and 2.26 to (2.17), we obtain that there exists $\epsilon > 0$ such that for $s \geq \max\{s_1(k), 2k+1\}$,

$$\begin{aligned}
R_{s,k}(n) &= \int_{\mathfrak{M}} g(\alpha)^s e(-n\alpha)\, d\alpha + \int_{\mathfrak{m}} g(\alpha)^s e(-n\alpha)\, d\alpha \\
&= \mathfrak{S}_{s,k}(n) J_\infty(n) q^{(s-k)P} + O(q^{(s-k-\epsilon)P}) \\
&= \mathfrak{S}_{s,k}(n) J_\infty(n) q^{(s-k)P} + o\left(q^{(s-k)P}\right),
\end{aligned}$$

which is the asymptotic formula (2.3). We then simplify $s_1(k)$ from Propositions 2.25 and 2.26 via (2.29) to obtain the estimates given in the statement of Theorem 2.3. When $k < p$, we see that $s_1(k)$ given in (2.81) is identical to that defined for the integer case in [25]. Consequently, our estimates for $\widetilde{G}_q(k)$ when $k < p$ are identical to the estimates of $\widetilde{G}(k)$ obtained in [25]. □

2.7 Slim Exceptional Sets

We carry out a similar calculation here as in Section 2.6 and obtain Theorems 2.5 and 2.6. Recall from Section 2.1 that $\widetilde{E}_{s,k}(N,\psi)$ is defined to be the set of $n \in I_N \cap \mathbb{J}_q^k[t]$ which satisfies (2.7). As in [25], we refer to a function $\psi(z)$ as being *sedately increasing* when $\psi(z)$ is a function of positive variable z increasing monotonically to infinity, and satisfying the condition that when z is large, one has $\psi(z) = O(z^\epsilon)$ for a positive number ϵ sufficiently small in the ambient context. We also prove the following theorem on the estimate of $|\widetilde{E}_{s,k}(N,\psi)|$ when ψ is a sedately increasing function. In order to avoid clutter in the exposition, we present the case $k = p^b + 1$ separately from the rest of the cases.

Theorem 2.27. *Suppose $k \geq 3$ and $p \nmid k$. Suppose further that either $p \nmid (k-1)$ or $k = mp^b + 1$, $m > 1$. Let δ_0 be as in the statement of Theorem 2.18. If $\psi(z)$ is a sedately increasing function, then for $s \geq rk + r$ we have*

$$|\widetilde{E}_{s,k}(N,\psi)| \ll q^{(k-\delta_0+\epsilon)P}\psi(q^P)^2,$$

where the implicit constant depends on $s, q, k, \epsilon, \mathcal{R}'$, and ψ.

Theorem 2.28. *Suppose $k \geq 3$ and $p \nmid k$. Suppose further that $k = p^b + 1$. Let*

$$\delta_0 = \frac{1}{16(p^b+2)}.$$

If $\psi(z)$ is a sedately increasing function, then for $s \geq 2k + 3$ we have

$$|\widetilde{E}_{s,k}(N,\psi)| \ll q^{(k-\delta_0+\epsilon)P}\psi(q^P)^2,$$

where the implicit constant depends on $s, q, k, \epsilon, \mathcal{R}'$, and ψ.

First, we consider the case when $p \nmid (k-1)$ in Proposition 2.29. We then take care of the case $k = mp^b + 1$ in Proposition 2.30.

Let

$$u_0'(j) = k^2 + 1 - \left\lceil \frac{kj - 2^{j-1}}{k+1-j} \right\rceil.$$

If $k < p$, we set

$$u_2(k) = \min_{\substack{1 \leq j < k \\ 2^j \leq k(2k+1)}} u_0'(j). \tag{2.88}$$

On the other hand, if $k > p$ and $p \nmid (k-1)$, we set

$$u_2(k) = rk + 1 - \left\lceil \frac{3r-4}{k-2} \right\rceil. \tag{2.89}$$

Proposition 2.29. *Suppose $k \geq 3$, $p \nmid k$, and $p \nmid (k-1)$. Let $u_2(k)$ be as given in (2.88) when $k < p$ and in (2.89) when $k > p$. If $s \geq u_2(k)$, then there exists $\delta_2 > 0$ such that*

$$\int_{\mathfrak{m}} |g(\alpha)|^{2s} \, d\alpha \ll q^{(2s-k-\delta_2)X},$$

where the implicit constant depends only on $s, q, k, \mathcal{R}'$, and δ_2.

Proof. Let $h_0(k)$ be as in the statement of Lemma 2.23. We let $2u_0(j) = 2r(k+1)a' + 2^j b'$, where $a' + b' = 1$. By Hölder's inequality, we have

$$\int_{\mathfrak{m}} |g(\alpha)|^{2u_0(j)} \, d\alpha \leq \left(\int_{\mathfrak{m}} |g(\alpha)|^{2r(k+1)} \, d\alpha \right)^{a'} \left(\oint |g(\alpha)|^{2^j} \, d\alpha \right)^{b'}. \tag{2.90}$$

Recall that for the range of k we are considering, we can take $\delta_0 = 1$ in Corollary 2.19. We consider j in the following range: $1 \leq j < k$, $2^j \leq (2r-1)(k+1)+1$ and $j \leq h_0(k)$. Define

$$\eta(j) = \frac{rj}{k-j+1} - \frac{2^{j-1}}{k-j+1}$$

and let

$$\gamma(j) = 1 + \eta(j) - \lceil \eta(j) \rceil.$$

We choose

$$a' = \frac{k-j}{k-j+1} + \frac{\gamma(j)}{r(k+1) - 2^{j-1}}$$

and

$$b' = \frac{1}{k-j+1} - \frac{\gamma(j)}{r(k+1) - 2^{j-1}}.$$

Note that our restriction on j ensures $b' > 0$. Also, this choice of a' and b' ensures $a' - (k-j)b' > 0$. Then, by Corollary 2.19 and (2.83), we have the following bound for

(2.90):

$$\int_{\mathfrak{m}} |g(\alpha)|^{2u_0(j)}\, d\alpha \ll q^{\epsilon X} q^{a'(2r(k+1)-k-1)X} q^{b'(2^j-j)X} \ll q^{(2u_0(j)-k-(a'-(k-j)b')+\epsilon)X}.$$

By the trivial bound $|g(\alpha)| \leq q^X$, it follows that for any $s \geq u_0(j)$ we have

$$\int_{\mathfrak{m}} |g(\alpha)|^{2s}\, d\alpha \ll q^{(2s-2u_0(j))X} \int_{\mathfrak{m}} |g(\alpha)|^{2u_0(j)}\, d\alpha \ll q^{(2s-k-(a'-(k-j)b')+\epsilon)X}.$$

We can simplify $2u_0(j)$ as

$$\begin{aligned} 2u_0(j) &= 2r(k+1)\left(\frac{k-j}{k-j+1} + \frac{\gamma(j)}{r(k+1)-2^{j-1}}\right) + 2^j\left(\frac{1}{k-j+1} - \frac{\gamma(j)}{r(k+1)-2^{j-1}}\right) \\ &= 2rk - \frac{2rj}{k-j+1} + \frac{2^j}{k-j+1} + 2\gamma(j) \\ &= 2rk - 2\eta(j) + 2\gamma(j), \end{aligned} \tag{2.91}$$

or equivalently,

$$u_0(j) = rk - \eta(j) + \gamma(j) = rk + 1 - \lceil \eta(j) \rceil.$$

To establish our result, all we have left is to choose j within the appropriate range given above such that $u_0(j)$ is as small as possible. This value of $u_0(j)$ will be our $u_2(k)$. We consider the two cases separately.

Case 1: $k > p$. From $p \nmid k$, $p \nmid (k-1)$, and $k > p$, we can verify that $3 \leq h_0(k)$. Thus we know we can apply Weyl differencing at least three times. Therefore, we set $u_2(k) = u_0(3)$. Since

$$0 < \eta(3) = \frac{3r-4}{k-2}, \tag{2.92}$$

we obtain

$$u_2(k) = rk + 1 - \left\lceil \frac{3r-4}{k-2} \right\rceil.$$

Case 2: Suppose $k < p$. In this case, we set

$$u_2(k) = \min_{\substack{1 \leq j < k \\ 2^j \leq (2r-1)(k+1)+1}} u_0(j). \tag{2.93}$$

Since $r = k - \lfloor k/p \rfloor = k$, we have $u_0(j) = u_0'(j)$ and $(2r-1)(k+1)+1 = k(2k+1)$.

Therefore, we see that $u_2(k)$ given above in (2.93) coincides with (2.88). □

Now we consider the case $k = mp^b + 1$. If $m = 1$, we set $u_2(k) = 2k + 3$. If $m > 1$, then we set

$$u_2(k) = rk + r - \left\lfloor \frac{(m-1)(1-1/p)}{4} \right\rfloor. \tag{2.94}$$

Proposition 2.30. *Suppose $k = mp^b + 1$ with $p \nmid m$. Let $u_2(k)$ be $2k + 3$ when $m = 1$ and as in (2.94) when $m > 1$. If $s \geq u_2(k)$, then there exists $\delta_2 > 0$ such that*

$$\int_{\mathfrak{m}} |g(\alpha)|^{2s} \, d\alpha \ll q^{(2s-k-\delta_2)X},$$

where the implicit constant depends only on $s, q, k, \mathcal{R}'$, and δ_2.

Proof. For the case $m = 1$, by a similar reasoning as in Proposition 2.26, we let $u_2(k) = 2k + 3$, and the result is an immediate consequence of Corollary 2.21. We now deal with the case $m > 1$. Let $h_0(k)$ be as in the statement of Lemma 2.23. If $j \leq h_0(k)$, then for any $\epsilon > 0$ we have (2.83). We let $2u_0(j) = 2r(k+1)a' + 2^j b'$, where $a' + b' = 1$, as before in Proposition 2.29. Then by Hölder's inequality, we have (2.90). We consider j in the following range: $1 \leq j < k$, $2^j \leq (2r-1)(k+1) + 1$ and $j \leq h_0(k)$.

Let $\epsilon(j)$ be a small positive number. We choose

$$a' = \frac{k-j}{k-j+\delta} + \frac{\epsilon(j)}{r(k+1) - 2^{j-1}}$$

and

$$b' = \frac{\delta}{k-j+\delta} - \frac{\epsilon(j)}{r(k+1) - 2^{j-1}},$$

where we let $\delta = \delta_0 = 1/(4p^b)$ from Corollary 2.19.

Note that we pick $\epsilon(j)$ sufficiently small such that $b' > 0$. Also, the range of j we are considering and this choice of a' and b' ensure

$$\delta a' - (k-j)b' = \frac{(\delta + k - j)\epsilon(j)}{r(k+1) - 2^{j-1}} > 0.$$

By Corollary 2.19 and (2.83), we have the following bound for (2.90):

$$\int_{\mathfrak{m}} |g(\alpha)|^{2u_0(j)} \, d\alpha \ll q^{\epsilon X} q^{a'(2r(k+1)-k-\delta)X} q^{b'(2^j - j)X} \ll q^{(2u_0(j)-k-(\delta a' - (k-j)b') + \epsilon)X}.$$

By the trivial bound $|g(\alpha)| \leq q^X$, it follows that for any $s \geq u_0(j)$ we have

$$\int_{\mathfrak{m}} |g(\alpha)|^{2s} \, d\alpha \ll q^{2(s-u_0(j))X} \int_{\mathfrak{m}} |g(\alpha)|^{2u_0(j)} \, d\alpha \ll q^{(2s-k-(\delta a'-(k-j)b')+\epsilon)X}.$$

We can simplify $2u_0(j)$ as

$$\begin{aligned} 2u_0(j) &= 2r(k+1)\left(\frac{k-j}{k-j+\delta} + \frac{\epsilon(j)}{r(k+1)-2^{j-1}}\right) + 2^j\left(\frac{\delta}{k-j+\delta} - \frac{\epsilon(j)}{r(k+1)-2^{j-1}}\right) \\ &= 2rk + 2(1-\delta)r - \frac{2r(j+(1-\delta)(\delta-j))}{k-j+\delta} + \frac{2^j\delta}{k-j+\delta} + 2\epsilon(j) \\ &= 2rk + 2(1-\delta)r - \delta\frac{2r(1+j-\delta)-2^j}{k-j+\delta} + 2\epsilon(j) \\ &= 2rk + 2r - \delta\frac{2r(k+1)-2^j}{k-j+\delta} + 2\epsilon(j), \end{aligned}$$

or equivalently,

$$u_0(j) = rk + r - \delta\frac{r(k+1)-2^{j-1}}{k-j+\delta} + \epsilon(j).$$

To establish our result, all we have left is to choose j within the appropriate range given above such that $u_0(j)$ is as small as possible. We would like to maximize the value

$$\delta\frac{r(k+1)-2^{j-1}}{k-j+\delta}$$

in order to minimize $u_0(j)$. We then let the smallest integer greater than the $u_0(j)$ found to be our $u_2(k)$.

Since $m > 1$, we can verify that $h_0(k) \geq 3$. Thus we know we can apply Weyl differencing at least three times. We have

$$r = (1-1/p)(k-p^b) + (1+1/p) = (m-1)(p^b - p^{b-1}) + 2.$$

Also, recall from above we have set $\delta = \delta_0 = 1/(4p^b)$. Let $j = 3$ and we obtain

$$\begin{aligned}
u_0(3) &= rk + r - \frac{r(k+1) - 2^{3-1}}{4p^b(k-3+\delta)} + \epsilon(3) \\
&= rk + r - \frac{r(k+1)}{4p^b(k-3+\delta)} + \frac{4}{4p^b(k-3+\delta)} + \epsilon(3) \\
&= rk + r - \frac{(m-1)(p^b - p^{b-1})(k+1)}{4p^b(k-3+\delta)} - \frac{2(k+1)}{4p^b(k-3+\delta)} + \frac{4}{4p^b(k-3+\delta)} + \epsilon(3) \\
&\leq rk + r - \frac{(m-1)(p^b - p^{b-1})(k+1)}{4p^b(k-3+\delta)} - \frac{k-1}{2p^b(k-3+\delta)} + \epsilon(3) \\
&\leq rk + r - \frac{(m-1)(1-1/p)(k+1)}{4(k-3+\delta)} \\
&\leq rk + r - \frac{(m-1)(1-1/p)}{4}.
\end{aligned}$$

Therefore, we set

$$\begin{aligned}
u_2(k) &= \left\lceil rk + r - \frac{(m-1)(1-1/p)}{4} \right\rceil \\
&= rk + r - \left\lfloor \frac{(m-1)(1-1/p)}{4} \right\rfloor \\
&\geq u_0(3).
\end{aligned}$$

□

For $\psi(z)$ a function of positive variable z, recall we denote $\widetilde{E}_{s,k}(N,\psi)$ to be the set of $n \in I_N \cap \mathbb{J}_q^k[t]$ for which

$$\left| R_{s,k}(n) - \mathfrak{S}_{s,k}(n) J_\infty(n) q^{(s-k)P} \right| > q^{(s-k)P} \psi(q^P)^{-1}. \tag{2.95}$$

By Theorem 2.9, for $s \geq 2k+1$ and any polynomial $n \in \widetilde{E}_{s,k}(N,\psi)$ we have

$$\int_{\mathfrak{M}} g(\alpha)^s e(-n\alpha)\, d\alpha = \mathfrak{S}_{s,k}(n) J_\infty(n) q^{(s-k)P} + O\left(q^{(s-k-2\epsilon)P}\right), \tag{2.96}$$

for sufficiently small $\epsilon > 0$. Hence, it follows by (2.17) that

$$\begin{aligned} R_{s,k}(n) &= \mathfrak{S}_{s,k}(n)J_\infty(n)q^{(s-k)P} + \int_{\mathfrak{m}} g(\alpha)^s e(-n\alpha)\ d\alpha \\ &\qquad\qquad\qquad\qquad + O\left(q^{(s-k-2\epsilon)P}\right). \end{aligned} \tag{2.97}$$

By (2.95), (2.97) and the triangle inequality, we see that there exists a constant $C_1 > 0$ such that given any $n \in \widetilde{E}_{s,k}(N,\psi)$,

$$\left|\int_{\mathfrak{m}} g(\alpha)^s e(-n\alpha)\ d\alpha\right| + C_1 q^{(s-k-2\epsilon)P} > q^{(s-k)P}\psi(q^P)^{-1}. \tag{2.98}$$

Suppose $\psi(z) < C_2 z^\epsilon$ for some constant $C_2 > 0$. Then it follows that $C_1 q^{(s-k-2\epsilon)P} < C_3 q^{(s-k-\epsilon)P}\psi(q^P)^{-1}$ for some constant $C_3 > 0$. Now there exists $M_0 > 0$ such that $C_3 q^{-\epsilon P} < 1/2$ for all $P \geq M_0$. Therefore, for P sufficiently large we have that given any $n \in \widetilde{E}_{s,k}(N,\psi)$,

$$\left|\int_{\mathfrak{m}} g(\alpha)^s e(-n\alpha)\ d\alpha\right| > \frac{1}{2} q^{(s-k)P}\psi(q^P)^{-1}. \tag{2.99}$$

Let $E = |\widetilde{E}_{s,k}(N,\psi)|$. Define the complex numbers $\eta(n)$, depending on s and k, for $n \in \widetilde{E}_{s,k}(N,\psi)$ by means of the equation

$$\left|\int_{\mathfrak{m}} g(\alpha)^s e(-n\alpha)\ d\alpha\right| = \eta(n)\int_{\mathfrak{m}} g(\alpha)^s e(-n\alpha)\ d\alpha.$$

Clearly, $|\eta(n)| = 1$ for all $n \in \widetilde{E}_{s,k}(N,\psi)$. Define the exponential sum $K(\alpha)$ by

$$K(\alpha) = \sum_{n\in\widetilde{E}_{s,k}(N,\psi)} \eta(n)e(n\alpha). \tag{2.100}$$

Then, it follows from (2.99) that for P sufficiently large

$$\begin{aligned} \frac{1}{2} q^{(s-k)P}\psi(q^P)^{-1}E &< \sum_{n\in\widetilde{E}_{s,k}(N,\psi)} \eta(n)\int_{\mathfrak{m}} g(\alpha)^s e(-n\alpha)\ d\alpha \\ &= \int_{\mathfrak{m}} g(\alpha)^s K(-\alpha)\ d\alpha. \end{aligned} \tag{2.101}$$

We apply Cauchy-Schwartz inequality to the right hand side of (2.101) to obtain

$$\frac{1}{2}q^{(s-k)P}\psi(q^P)^{-1}E < \left(\int_{\mathfrak{m}} |g(\alpha)|^{2s}\, d\alpha\right)^{1/2} \left(\int_{\mathfrak{m}} |K(-\alpha)|^{2}\, d\alpha\right)^{1/2}. \tag{2.102}$$

We note that we have established the above inequality (2.102) assuming $s \geq 2k+1$ here. The orthogonality relation (2.10) gives us

$$\oint |K(\alpha)|^2\, d\alpha = \sum_{n \in \widetilde{E}_{s,k}(N,\psi)} 1 = E. \tag{2.103}$$

With this set up, we are ready to prove Theorems 2.5, 2.6, 2.27, and 2.28.

Proof of Theorems 2.5, 2.6, 2.27, and 2.28. Recall we defined $X = P+1$. By Propositions 2.29 and 2.30, for $s \geq u_2(k)$ we know there exists $\delta_2 > 0$ such that

$$\left(\int_{\mathfrak{m}} |g(\alpha)|^{2s}\, d\alpha\right)^{1/2} \ll q^{(s-k/2-\delta_2/2)P}.$$

Therefore, we can further bound the right hand side of (2.102) by the above inequality and (2.103), and obtain for $s \geq \max\{u_2(k), 2k+1\}$,

$$\frac{1}{2}q^{(s-k)P}\psi(q^P)^{-1}E^{1/2} < \left(\int_{\mathfrak{m}} |g(\alpha)|^{2s}\, d\alpha\right)^{1/2} \ll q^{(s-k/2-\delta_2/2)P},$$

which simplifies to

$$E \ll q^{(k-\delta_2)P}\psi(q^P)^2. \tag{2.104}$$

Fix $\epsilon > 0$ sufficiently small and let $\psi(z)$ be such that $\psi(q^P) \ll q^{\epsilon P/2}$. Then we have by (2.104) that

$$E \ll q^{(k-\delta_2+\epsilon)P} < q^{\operatorname{ord} n-(\delta_2-\epsilon)P} \ll q^{N-(\delta_2-\epsilon)\frac{N}{k}} = o(q^N).$$

Therefore, we obtain $\widetilde{G}_q^+(k) \leq \max\{u_2(k), 2k+1\}$. We then simplify $u_2(k)$ via (2.29) to obtain the estimates given in the statement of Theorem 2.5. When $k < p$, we see that $u_2(k)$ given in (2.88) is identical to $u_1(k)$ defined in [25]. Consequently, our estimates for $\widetilde{G}_q^+(k)$ when $k < p$ are identical to the estimates of $\widetilde{G}^+(k)$ obtained in [25]. We have now completed the proof of Theorems 2.5 and 2.6.

Finally, to prove Theorems 2.27 and 2.28, we substitute (2.103) into (2.102), apply

Corollary 2.19 or Corollary 2.21 (depending on k and p), and obtain for P sufficiently large

$$\frac{1}{2}q^{(s-k)P}\psi(q^P)^{-1}E^{1/2} < \left(\int_{\mathfrak{m}} |g(\alpha)|^{2s} \, d\alpha\right)^{1/2} \ll q^{(s-k/2-\delta_0/2+\epsilon/2)P}.$$

Rearranging the above inequality yields

$$E \ll q^{(k-\delta_0+\epsilon)P}\psi(q^P)^2,$$

as desired. □

Chapter 3

Diophantine approximation of polynomials over $\mathbb{F}_q[t]$ satisfying a divisibility condition

3.1 Introduction

In 1927, Vinogradov [20] proved the following result, confirming a conjecture of Hardy and Littlewood [6]. Let $\| \cdot \|$ denote the distance to the nearest integer.

Theorem 3.1. *For every positive integer k, there exists an exponent $\theta_k > 0$ such that*

$$\min_{1 \leq n \leq N} \|\alpha n^k\| \ll_k N^{-\theta_k}$$

for any positive integer N and real number α.

A brief history and introduction to the topic is given in [13, Section 1], which we paraphrase here. Vinogradov showed that one could take $\theta_k = \frac{k}{k2^{k-1}+1} - \epsilon$ for any $\epsilon > 0$. In particular, one can take $\theta_2 = 2/5 - \epsilon$. Heilbronn [8] improved this to $\theta_2 = 1/2 - \epsilon$. The best result to date is due to Zaharescu [28], who showed we can take $\theta_2 = 4/7 - \epsilon$, though his method is not applicable to higher powers. It is an open conjecture that we can choose θ_2 (and more generally θ_k) to be $1 - \epsilon$.

Natural generalizations of Vinogradov's result have been made. Davenport [2] obtained an analogue of Theorem 3.1 when n^k is replaced by a polynomial $f(n)$ of degree k without a constant term (the corresponding bound being uniform in the coefficients of f and depending only on k). Notably, the best bound is due to Wooley, who showed that we can choose $\theta_k = \frac{1}{4k(k-2)} - \epsilon$ for $k \geq 4$, as a consequence of his recent breakthrough [24] on Vinogradov's mean value theorem. We note that Vinogradov's result has also been generalized to simultaneous approximation, where we consider multiple polynomials at once. However, we focus on the single polynomial case in this chapter and we refer the reader to [13, Section 1] for more information on simultaneous approximation.

In contrast, Lê and Spencer put more emphasis on the qualitative side of these problems in [13]. They were interested in generalizing Theorem 3.1 in the following manner. For instance, is it possible to replace n^k in Theorem 3.1 with a polynomial $h \in \mathbb{Z}[x]$? That is, for which polynomials $h \in \mathbb{Z}[x]$ do we have

$$\min_{1 \leq n \leq N} \|\alpha h(n)\| \ll_h N^{-\theta} \tag{3.1}$$

for some $\theta = \theta(h)$, uniformly in α and N? By the result of Davenport [2] mentioned in the previous paragraph, this is the case if h is without a constant term, but apparently these are not all the polynomials satisfying this property. By considering $\alpha = 1/q$, we see that in order for such a bound to exist, h must have a root modulo q for every $q \in \mathbb{Z}^+$. (If h does not have a root modulo q, then $\|h(n)/q\| \geq 1/q$ for all $n \in \mathbb{N}$, and consequently, (3.1) can not be satisfied uniformly in α and N.) Clearly, this condition is satisfied by polynomials without constant terms. Lê and Spencer proved that this condition is also sufficient.

Theorem 3.2. *[13, Theorem 3] Let h be a polynomial in $\mathbb{Z}[x]$ with the property that for every $q \neq 0$, there exists $n_q \in \mathbb{Z}$, $0 \leq n_q < q$, such that $h(n_q) \equiv 0 \pmod{q}$. Then there is an exponent $\theta > 0$ depending only on the degree of h such that*

$$\min_{1 \leq n \leq N} \|\alpha h(n)\| \ll_h N^{-\theta}$$

for any positive integer N and real number α.

Our goal in this chapter is to consider analogous problems of qualitative nature over $\mathbb{F}_q[t]$, where $\mathbb{F}_q$ is a finite field of q elements, taking the approach of Lê and Spencer in [13]. However, before we can state our results we need to introduce notation, some of which we take from the material in [12, Section 1]. We denote the characteristic of $\mathbb{F}_q$, a positive prime number, by $\mathrm{ch}(\mathbb{F}_q) = p$. Let $\mathbb{K} = \mathbb{F}_q(t)$ be the field of fractions of the polynomial ring $\mathbb{F}_q[t]$. For $f/g \in \mathbb{K}$, we define the 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, $\mathbb{F}_q[t], \mathbb{K}$, and $\mathbb{K}_\infty$ play the roles of $\mathbb{Z}, \mathbb{Q}$, and $\mathbb{R}$, respectively. Let

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

which is the analogue of the unit interval $[0, 1)$.

For $\alpha = \sum_{i=-\infty}^{n} a_i t^i \in \mathbb{K}_\infty$, if $a_n \neq 0$, we define $\operatorname{ord} \alpha = n$. 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. 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 $e_q(a) = e^{2\pi i(\operatorname{tr}(a)/p)}$. 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.

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 $\mathcal{K} \subseteq \mathbb{Z}^+$. 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. Following the notation of [12], we define the *shadow* of $\mathcal{K}$, $\mathcal{S}(\mathcal{K})$, to be

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

We also define

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

Given $f(u) \in \mathbb{K}_\infty[u]$, we mean by $f(u)$ is *supported on a set* $\mathcal{K} \subseteq \mathbb{Z}^+$ that $f(u) = \sum_{r \in \mathcal{K} \cup \{0\}} \alpha_r u^r$, where $0 \neq \alpha_r \in \mathbb{K}_\infty$ $(r \in \mathcal{K})$. As explained in the remark of [12, Theorem 12], the non-zero coefficient α_k, for $k \in \mathcal{K}^*$ which is maximal in $\mathcal{K}$, plays the role of the leading coefficient of the polynomial. This is, in a sense, the "true" $\mathbb{F}_q[t]$ analogue of the leading coefficient.

We are now in position to state one of our main results. The following theorem is an analogue of Theorem 3.2.

Theorem 3.3. *Let* $h(u) = \sum_{r \in \mathcal{K} \cup \{0\}} c_r u^r$ *be a polynomial supported on a set* $\mathcal{K} \subseteq \mathbb{Z}^+$ *with coefficients in* $\mathbb{F}_q[t]$. *Suppose* $c_k \neq 0$ *for some* $k \in \mathcal{K}^*$. *Suppose further that for every* g

in $\mathbb{F}_q[t]\backslash\{0\}$, there exists an $m_g \in \mathbb{G}_{\deg g}$ such that $h(m_g) \equiv 0 \pmod g$. Then there exist $\theta = \theta(\mathcal{K}, q, \deg h) > 0$ and $N_0 = N_0(\mathcal{K}, q, h, \theta) \in \mathbb{Z}^+$ such that for any $N > N_0$, we have

$$\min_{x\in\mathbb{G}_N} \operatorname{ord}\{\beta h(x)\} \leq -\theta N$$

uniformly in $\beta \in \mathbb{K}_\infty$.

Lê and Spencer also proved the following theorem in [13].

Theorem 3.4. *[13, Theorem 6] Suppose the polynomials $h_1, ..., h_L$ of distinct degrees are such that any linear combination of them with integer coefficients has a root modulo q for any $q \in \mathbb{N}$. Let $\alpha_1, ..., \alpha_L \in \mathbb{R}$. Then there is an exponent $\theta > 0$ (depending at most on $h_1, ..., h_L$) such that*

$$\min_{1\leq n\leq N} \|\alpha_1 h_1(n) + ... + \alpha_L h_L(n)\| \ll N^{-\theta}$$

uniformly in $\alpha_1, ..., \alpha_L, N$.

Suppose we have polynomials $h_1, ..., h_L \in \mathbb{F}_q[t][u]$, where $h_j(u) = \sum_{r\in\mathcal{K}_j\cup\{0\}} c_{j,r}u^r$, and $\mathcal{K}_j \subseteq \mathbb{Z}^+$ $(1 \leq j \leq L)$. Let $\mathcal{K} = \mathcal{K}_1 \cup ... \cup \mathcal{K}_L$. We define the *$\mathcal{K}^*$-portion* of h_j as

$$h_j^*(u) := \sum_{r\in\mathcal{K}_j\cap\mathcal{K}^*} c_{j,r}u^r.$$

We say the *$\mathcal{K}^*$-portion of $(h_j)_{j=1}^L$ is linearly independent* if $h_1^*, ..., h_L^*$ are linearly independent over $\mathbb{K}$. We also define a slightly stronger notion, the *maximal $\mathcal{K}^*$-portion* of h_j as

$$h_j^{\max}(u) := \sum_{\substack{r\in\mathcal{K}_j\cap\mathcal{K}^* \\ r \text{ is maximal in } \mathcal{K}}} c_{j,r}u^r.$$

We say the *maximal $\mathcal{K}^*$-portion of $(h_j)_{j=1}^L$ is linearly independent* if $h_1^{\max}, ..., h_L^{\max}$ are linearly independent over $\mathbb{K}$.

The following theorem is an analogue of Theorem 3.4.

Theorem 3.5. *Let $h_j \in \mathbb{F}_q[t][u]$ be supported on a set $\mathcal{K}_j \subseteq \mathbb{Z}^+$ $(1 \leq j \leq L)$, and let $\mathcal{K} = \mathcal{K}_1 \cup ... \cup \mathcal{K}_L$. Suppose any linear combination of them with $\mathbb{F}_q[t]$ coefficients has a root modulo g for any $g \in \mathbb{F}_q[t]\backslash\{0\}$. Suppose further that the $\mathcal{K}^*$-portion of $(h_j)_{j=1}^L$ is linearly independent. Then there exist $\theta = \theta\left(\mathcal{K}, q, \max_{1\leq j\leq L} \deg h_j\right) > 0$ and $N_0 = N_0(\mathcal{K}, q, \theta, h_1, ..., h_L) \in \mathbb{Z}^+$ such that for any $N > N_0$, we have*

$$\min_{x\in\mathbb{G}_N} \operatorname{ord}\{\beta_1 h_1(x) + ... + \beta_L h_L(x)\} \leq -\theta N$$

uniformly in $\beta_1, ..., \beta_L \in \mathbb{K}_\infty$.

We also prove an analogue of [13, Theorem 7] in Theorem 3.15, which is a (partial) generalization of Theorem 3.5. However, we defer stating the result to Section 3.4 in order to avoid introducing further notation here.

The organization of the rest of the chapter is as follows. In Section 3.2, we introduce some notation and notions required to carry out our discussions in the setting over $\mathbb{F}_q[t]$. In Section 3.3, we prove lemmas involving basic linear algebra utilized in the proof of our main results given in Section 3.4. Finally, we note that Lê and Spencer generalized [13, Theorem 7], which Theorem 3.15 is an analogue of, and obtained results on simultaneous approximation [13, Theorems 4 and 8]. However, due to complications that arose during our attempt from certain arguments in linear algebra and geometry of numbers in the setting over $\mathbb{F}_q[t]$, at present time we decided to leave generalizing Theorem 3.15 in a similar manner as a possible future work.

3.2 Preliminaries

Suppose a system of polynomials $(h_1, ..., h_L)$ satisfies the following,

Condition $(\star)$: For every $g \in \mathbb{F}_q[t]\backslash\{0\}$, there exists $m_g \in \mathbb{F}_q[t]$ such that $h_i(m_g) \equiv 0 \pmod{g}$ for $i = 1, ..., L$.

In the case of $\mathbb{Z}$ (in place of $\mathbb{F}_q[t]$), such a system of polynomials satisfying the analogous condition is called *jointly interesective polynomials.*

We have the following analogue of [1, Proposition 6.1].

Lemma 3.6. *A system of polynomials $(h_1, ..., h_L)$ in $\mathbb{F}_q[t][u]$ satisfies Condition $(\star)$ if and only if there exists a polynomial $d \in \mathbb{F}_q[t][u]$, which has a root modulo g for every $g \in \mathbb{F}_q[t]\backslash\{0\}$, and $d|h_i$ $(1 \leq i \leq L)$ over $\mathbb{F}_q[t]$.*

Proof. Suppose a system of polynomials $(h_1, ..., h_L)$ in $\mathbb{F}_q[t][u]$ satisfies Condition $(\star)$. Let $\widetilde{d}$, a monic polynomial in $\mathbb{K}[u]$, be the greatest common divisor of $h_1, ..., h_L$. Then we know there exist $a_1, ..., a_L \in \mathbb{K}[u]$ such that

$$a_1(u)h_1(u) + ... + a_L(u)h_L(u) = \widetilde{d}(u). \tag{3.2}$$

Let $c \in \mathbb{F}_q[t]$ be such that $c\widetilde{d}(u) \in \mathbb{F}_q[t][u]$ and has content 1. Since $\widetilde{d}|h_i$ over $\mathbb{K}$, we have $c\widetilde{d}|h_i$ over $\mathbb{F}_q[t]$ by Gauss' Lemma. Let $d(u) = c\widetilde{d}(u)$. By multiplying both sides of the equation (3.2) by c, without loss of generality we may replace $\widetilde{d}(u)$ by $d(u)$ in the equation. Let $c' \in \mathbb{F}_q[t]$ be the common denominator of $a_1, ..., a_L$. Again by multiplying both sides of the equation by c', we have $c'a_1(u)h_1(u) + ... + c'a_L(u)h_L(u) = c'd(u)$, where $c'a_i(u) \in \mathbb{F}_q[t][u]$. Then it is clear that $c'd(u)$ has a root modulo g for every $g \in \mathbb{F}_q[t] \backslash \{0\}$.

Suppose we are given $g = a\prod_{j=1}^{L'} w_j^{S_j}$, where each w_j's are distinct monic irreducibles in $\mathbb{F}_q[t]$ and $a \in \mathbb{F}_q$. For $w, g \in \mathbb{F}_q[t]$, where w is irreducible, and $T \in \mathbb{N}$, we write $w^T||g$ to mean $w^T|g$, but $w^{T+1} \nmid g$. For each j, let $w_j^{T_j}||c'$ and $y_j \in \mathbb{F}_q[t]$ be such that

$$c'd(y_j) \equiv 0 \pmod{w_j^{T_j+S_j}},$$

which we know exists. Consequently, we have

$$d(y_j) \equiv 0 \pmod{w_j^{S_j}}$$

for each j. By the Chinese Remainder Theorem, we can find y such that $y \equiv y_j \pmod{w_j^{S_j}}$ for $1 \leq j \leq L'$. Since $d(y) \equiv 0 \pmod{w_j^{S_j}}$ for $1 \leq j \leq L'$, again by the Chinese Remainder Theorem we have $d(y) \equiv 0 \pmod{g}$. The converse direction is immediate. □

Let w be a monic irreducible polynomial in $\mathbb{F}_q[t]$. Let λ_N be the canonical projection from $\mathbb{F}_q[t]/w^{N+1}\mathbb{F}_q[t]$ to $\mathbb{F}_q[t]/w^N\mathbb{F}_q[t]$. For each w, we define the projective limit

$$\lim_{\substack{\leftarrow \\ N}} \mathbb{F}_q[t]/w^N\mathbb{F}_q[t] = \left\{(x_i)_{i\in\mathbb{N}} \in \prod_{i=1}^{\infty} \mathbb{F}_q[t]/w^i\mathbb{F}_q[t] : \lambda_i(x_{i+1}) = x_i, i = 1, 2, ...\right\}.$$

Take $\bar{x} = (x_i)_{i\in\mathbb{N}} \in \lim\limits_{\substack{\leftarrow \\ N}} \mathbb{F}_q[t]/w^N\mathbb{F}_q[t]$. We say that $\bar{x}$ is a solution to the equation $f(u) = 0$, if $\bar{x}$ satisfies

$$f(x_i) \equiv 0 \ (mod\ w^i)$$

for all $i \in \mathbb{N}$.

We have the following lemma, which its proof follows closely that of the p-adic integers, for example see [18, Chapter II, Proposition 1.4].

Lemma 3.7. *Let f be a polynomial in $\mathbb{F}_q[t][u]$ and w a monic irreducible in $\mathbb{F}_q[t]$. Then f has a root modulo w^N for every $N \in \mathbb{N}$ if and only if the equation $f(u) = 0$ has a solution in $\lim\limits_{\substack{\leftarrow \\ N}} \mathbb{F}_q[t]/w^N\mathbb{F}_q[t]$.*

Proof. Suppose we have $(x_i)_{i\in\mathbb{N}} \in \prod_{i=1}^{\infty} \mathbb{F}_q[t]/w^i\mathbb{F}_q[t]$ and that x_i is a solution of

$$f(x_i) \equiv 0 \pmod{w^i}$$

for every $i \in \mathbb{N}$. If $(x_i)_{i\in\mathbb{N}}$ is already in $\varprojlim_N \mathbb{F}_q[t]/w^N\mathbb{F}_q[t]$, then we are done. However, this is not automatically the case. We will therefore extract a sequence from $(x_i)_{i\in\mathbb{N}}$ which fits our needs. In what follows, we view $(x_i)_{i\in\mathbb{N}}$ as a sequence in $\mathbb{F}_q[t]$. Since $\mathbb{F}_q[t]/w\mathbb{F}_q[t]$ is finite, there are infinitely many terms x_i, which modulo w are congruent to the same element $y_1 \in \mathbb{F}_q[t]/w\mathbb{F}_q[t]$. Hence we may choose a subsequence $\{x_i^{(1)}\}$ of $\{x_i\}$ such that

$$x_i^{(1)} \equiv y_1 \pmod{w} \quad \text{and} \quad f(x_i^{(1)}) \equiv 0 \pmod{w}.$$

Likewise, we may extract from $\{x_i^{(1)}\}$ a subsequence $\{x_i^{(2)}\}$ such that

$$x_i^{(2)} \equiv y_2 \pmod{w^2} \quad \text{and} \quad f(x_i^{(2)}) \equiv 0 \pmod{w^2},$$

where $y_2 \in \mathbb{F}_q[t]/w^2\mathbb{F}_q[t]$ evidently satisfies $y_2 \equiv y_1 \pmod{w}$. Continuing this way, we obtain for each $k \geq 2$ a subsequence $\{x_i^{(k)}\}$ from $\{x_i^{(k-1)}\}$ the terms of which satisfy the congruences

$$x_i^{(k)} \equiv y_k \pmod{w^k} \quad \text{and} \quad f(x_i^{(k)}) \equiv 0 \pmod{w^k},$$

for some $y_k \in \mathbb{F}_q[t]/w^k\mathbb{F}_q[t]$ such that

$$y_k \equiv y_{k-1} \pmod{w^{k-1}}.$$

The y_k's define an element in the projective limit, $(y_k)_{k\in\mathbb{N}} \in \varprojlim_N \mathbb{F}_q[t]/w^N\mathbb{F}_q[t]$, satisfying

$$f(y_k) \equiv 0 \pmod{w^k}$$

for all $k \geq 1$. The converse direction is immediate. □

Lemma 3.8. *Let f be a polynomial in $\mathbb{F}_q[t][u]$. Then f has a root modulo g for every $g \in \mathbb{F}_q[t]\backslash\{0\}$ if and only if for every monic irreducible w, the equation $f(u) = 0$ has a solution in $\varprojlim_N \mathbb{F}_q[t]/w^N\mathbb{F}_q[t]$.*

Proof. If f has a root modulo g for every $g \in \mathbb{F}_q[t]\backslash\{0\}$, then in particular it has a root modulo w^N for every $N \in \mathbb{N}$. Thus the result follows from Lemma 3.7. For the converse direction, suppose we are given $g = a\prod_{i=1}^{T} w_i^{S_i}$, where the w_i's are distinct monic irreducibles in $\mathbb{F}_q[t]$ and $a \in \mathbb{F}_q$. By the hypothesis and Lemma 3.7, there exists $x_i \in \mathbb{F}_q[t]/w_i^{S_i}\mathbb{F}_q[t]$ such that $f(x_i) \equiv 0 \pmod{w_i^{S_i}}$ for each i. Then by the Chinese Remainder Theorem, we can find $x \in \mathbb{F}_q[t]$ such that $x \equiv x_i \pmod{w_i^{S_i}}$ for $1 \leq i \leq T$. Since $f(x) \equiv 0 \pmod{w_i^{S_i}}$ for $1 \leq i \leq T$, again by the Chinese Remainder Theorem we have $f(x) \equiv 0 \pmod{\prod_{i=1}^{T} w_i^{S_i}}$. Then it is immediate that $f(x) \equiv 0 \pmod{g}$. □

Corresponding to any system of polynomials $(h_1, ..., h_L)$ satisfying Condition $(\star)$, there exists $d \in \mathbb{F}_q[t][u]$ satisfying the conditions of Lemma 3.6. Given a monic irreducible w, by Lemma 3.8, we know there exists $(r_{w^j}) \in \lim\limits_{\overleftarrow{N}} \mathbb{F}_q[t]/w^N\mathbb{F}_q[t]$ which is a solution to $d(u) = 0$, in other words $d(r_{w^j}) \equiv 0 \ (mod\ w^j)$ and $r_{w^j} \equiv r_{w^{j+1}} \ (mod\ w^j)$ for all $j \in \mathbb{N}$. We fix such a solution for each w. Suppose we are given $g = a\prod_{i=1}^{T} w_i^{S_i} = ag_1$, where the w_i's are distinct monic irreducibles in $\mathbb{F}_q[t]$ and $a \in \mathbb{F}_q$. By the Chinese Remainder Theorem, we define r_g to be the unique element in $\mathbb{F}_q[t]/(g_1)$ such that $r_g \equiv r_{w_i^{S_i}} \ (mod\ w_i^{S_i})$ for $1 \leq i \leq T$. Since $d(r_g) \equiv 0 \ (mod\ w_i^{S_i})$ for $1 \leq i \leq T$, it follows that $d(r_g) \equiv 0 \ (mod\ g)$. Suppose we have $y = b\prod_{i=1}^{T} w_i^{S_i'}$, where $S_i' \leq S_i$ and $b \in \mathbb{F}_q$, so that $y|g$. Then since $r_g \equiv r_{w_i^{S_i}} \equiv r_{w_i^{S_i'}} \ (mod\ w_i^{S_i'})$ for $1 \leq i \leq T$, we obtain $r_g \equiv r_y (mod\ y)$. Finally, for $a \in \mathbb{F}_q$ we let $r_a = 0$.

Therefore, corresponding to any system of polynomials $(h_1, ..., h_L)$ satisfying Condition $(\star)$, we can associate a sequence $(r_x)_{x \in \mathbb{F}_q[t]\setminus\{0\}} \subseteq \mathbb{F}_q[t]$ such that for any $m, y \in \mathbb{F}_q[t]\setminus\{0\}$, $r_y \in \mathbb{G}_{\mathrm{ord}\, y}$, $r_{my} \equiv r_y \ (mod\ y)$, and

$$h_j(r_y) \equiv 0 \ (mod\ y) \quad (1 \leq j \leq L). \tag{3.3}$$

We note that the approach to define the sequence $(r_x)_{x \in \mathbb{F}_q[t]\setminus\{0\}}$ here was taken from [17], which deals with the case of $\mathbb{Z}$.

For any element $\alpha \in \mathbb{K}_\infty$, it is easy to see that

$$\mathrm{ord}\,\{\alpha\} = \min_{z \in \mathbb{F}_q[t]} \mathrm{ord}\,(\alpha - z),$$

where the minimum is achieved when $z = \alpha - \{\alpha\}$, the integral part of α. Also for $\alpha_1, ..., \alpha_L \in \mathbb{K}_\infty$, we have

$$\mathrm{ord}\left\{\sum_{j=1}^{L} \alpha_j\right\} \leq \mathrm{ord}\left(\sum_{j=1}^{L} \alpha_j - \sum_{j=1}^{L}(\alpha_j - \{\alpha_j\})\right) = \mathrm{ord}\left(\sum_{j=1}^{L}\{\alpha_j\}\right) \leq \max_{1 \leq j \leq L} \mathrm{ord}\,\{\alpha_j\}. \tag{3.4}$$

Lemma 3.9. *Let* $\beta_1, \beta_2, ..., \beta_R \in \mathbb{K}_\infty$ *and suppose* $\operatorname{ord}\{\beta_j\} \geq -M$ $(1 \leq j \leq R)$. *Then there exists* $x \in \mathbb{G}_M \backslash \{0\}$ *such that*

$$\Big|\sum_{j=1}^{R} e(x\beta_j)\Big| \geq \frac{R}{q^M - 1}.$$

Proof. For $\alpha \in \mathbb{K}_\infty$, we have by [19, Lemma 7]

$$\sum_{x \in \mathbb{G}_M} e(x\alpha) = \begin{cases} q^M, & \text{if } \operatorname{ord}\{\alpha\} < -M, \\ 0, & \text{if } \operatorname{ord}\{\alpha\} \geq -M. \end{cases} \tag{3.5}$$

Since $\operatorname{ord}\{\beta_j\} \geq -M$ $(1 \leq j \leq R)$, we have

$$\sum_{j=1}^{R} \sum_{x \in \mathbb{G}_M} e(x\beta_j) = 0.$$

Therefore, it follows that

$$\sum_{x \in \mathbb{G}_M \backslash \{0\}} \Big|\sum_{j=1}^{R} e(x\beta_j)\Big| \geq R,$$

from which we obtain our result. □

We invoke the following result from [12]. The theorem allows us to estimate certain coefficients of a polynomial $f(u)$ *by an element in* $\mathbb{K}$ *when the exponential sum of* $f(u)$ *is sufficiently large.*

Theorem 3.10. *[12, Theorem 15] Let* $f(u) = \sum_{r \in \mathcal{K} \cup \{0\}} \alpha_r u^r$ *be a polynomial supported on a set* $\mathcal{K} \subseteq \mathbb{Z}^+$ *with coefficients in* $\mathbb{K}_\infty$. *Then for any* $k \in \mathcal{K}^*$, *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*

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

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*

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

We have the following corollary where we replace the polynomial $g_k \in \mathbb{F}_q[t]$ and constants $c_k, C_k > 0$ in the statement of Theorem 3.10 with $g \in \mathbb{F}_q[t]$ and $c, C > 0$, which are independent of the choice of $k \in \mathcal{K}^*$, respectively.

Corollary 3.11. *Let $f(u) = \sum_{r \in \mathcal{K} \cup \{0\}} \alpha_r u^r$ be a polynomial supported on a set $\mathcal{K} \subseteq \mathbb{Z}^+$ with coefficients in $\mathbb{K}_\infty$. There exist constants $c, C > 0$, depending only on $\mathcal{K}$ and q, such that the following holds: suppose that for some $0 < \eta \leq cN$, we have*

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

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

$$\operatorname{ord}\{g\alpha_k\} < -kN + \epsilon N + C\eta \quad (k \in \mathcal{K}^*) \textit{ and } \quad \operatorname{ord} g \leq \epsilon N + C\eta.$$

Proof. For each $k \in \mathcal{K}^*$, let c_k, C_k be the constants, depending only on $\mathcal{K}$ and q, and a_k, g_k be the polynomials from the statement of Theorem 3.10. Let $c = \min_{k \in \mathcal{K}^*} c_k$ and $C = \max_{k \in \mathcal{K}^*} C_k$. We let $g = \prod_{k \in \mathcal{K}^*} g_k$ and $C' = |\mathcal{K}^*|C$. Since $\operatorname{ord} g_k \leq \epsilon N + C_k\eta$ $(k \in \mathcal{K}^*)$, it follows that

$$\operatorname{ord} g \leq |\mathcal{K}^*|\epsilon N + C'\eta.$$

We also obtain

$$\operatorname{ord}\{g\alpha_k\} \leq \operatorname{ord}\left(g\alpha_k - a_k \prod_{j \in \mathcal{K}^* \setminus \{k\}} g_j \right) \leq -kN + |\mathcal{K}^*|\epsilon N + C'\eta.$$

□

We note that all of our main results, Theorems 3.3, 3.5 and 3.15, rely on Corollary 3.11, which explains the reason for our assumptions on the coefficients of the polynomials in these theorems.

3.3 Basic Linear Algebra

In this section, we prove lemmas involving basic linear algebra which are utilized in the proofs of our main results. Given a polynomial $f(u) \in \mathbb{K}_\infty[u]$, we use the notation $[f]_i$ to *mean the u^i coefficient of f. We have the following lemma, which is an analogue of [13, Lemma 1].*

Lemma 3.12. *Suppose $d, s \in \mathbb{F}_q[t]$, $d \neq 0$, and $f_1, ..., f_L \in \mathbb{F}_q[t][u]$ with $\deg f_1 < ... < \deg f_L$. There exist polynomials $g_1, ..., g_L \in \mathbb{F}_q[t][u]$, depending on d and s, and an $L \times L$ matrix $\mathcal{A}$ with entries in $\mathbb{F}_q[t]$ satisfying the following properties:*

(1) $\mathcal{A} \begin{pmatrix} f_1(du+s) \\ \vdots \\ f_L(du+s) \end{pmatrix} = \begin{pmatrix} g_1(u) \\ \vdots \\ g_L(u) \end{pmatrix}$

(2) $\mathcal{A}$ is lower triangular with entries in $\mathbb{F}_q[t]$. All its diagonal entries are equal to a constant $c \in \mathbb{F}_q[t]$ depending only on $f_1, .., f_L$. In fact, every entry of $\mathcal{A}$ is dependent at most on s and $f_1, .., f_L$.

(3) We have $[g_i]_{\deg g_j} = 0$ if $i \neq j$. Also, $\deg g_j = \deg f_j$ and $[g_j]_{\deg g_j} = cd^{\deg f_j}[f_j]_{\deg f_j}$ for all $1 \leq j \leq L$.

Proof. Let $\mathcal{A}' = (a_{i,j})$ be a lower triangular matrix with all entries on the main diagonal equal to 1. For each $1 \leq i \leq L$, one can successively select elements in $\mathbb{K}$, $a_{i,i-1}, ..., a_{i,1}$ so that in the polynomial

$$h_i(u) = a_{i,1}f_1(du+s) + a_{i,2}f_2(du+s) + ... + a_{i,i-1}f_{i-1}(du+s) + f_i(du+s),$$

the coefficient of $u^{\deg f_j}$ is 0 for every $j < i$. We prove by induction that $a_{i,j}$ $(j < i)$ depend only on s and $f_1, ..., f_L$, and that their denominators depend only on $f_1, ..., f_L$. Fix $1 \leq i \leq L$. For the base case $j = i-1$, we have

$$\begin{aligned} 0 &= [h_i]_{\deg f_{i-1}} \\ &= [a_{i,i-1}f_{i-1}(du+s) + f_i(du+s)]_{\deg f_{i-1}} \\ &= a_{i,i-1}[f_{i-1}]_{\deg f_{i-1}} d^{\deg f_{i-1}} + \sum_{l=\deg f_{i-1}}^{\deg f_i} [f_i]_l \binom{l}{\deg f_{i-1}} d^{\deg f_{i-1}} s^{l-\deg f_{i-1}}. \end{aligned}$$

By rearraging the last equality above, we obtain the following equaiton

$$a_{i,i-1} = \frac{-1}{[f_{i-1}]_{\deg f_{i-1}}} \sum_{l=\deg f_{i-1}}^{\deg f_i} [f_i]_l \binom{l}{\deg f_{i-1}} s^{l-\deg f_{i-1}},$$

from which we deduce our base case. Suppose the statement holds for $j_0 < j < i$. Then we have by similar calculations as above and the induction hypothesis that

$$\begin{aligned} 0 &= [h_i]_{\deg f_{j_0}} \\ &= [a_{i,j_0} f_{j_0}(du+s) + \ldots + a_{i,i-1} f_{i-1}(du+s) + f_i(du+s)]_{\deg f_{j_0}} \\ &= a_{i,j_0} d^{\deg f_{j_0}} [f_{j_0}]_{\deg f_{j_0}} + d^{\deg f_{j_0}} \ \widetilde{a}, \end{aligned}$$

where $\widetilde{a} \in \mathbb{K}$ depends only on s and $f_1, \ldots, f_L$, and its denominator depends only on $f_1, \ldots, f_L$. We then obtain our claim for $j = j_0$ by rearranging the last equation displayed above. Let $c \in \mathbb{F}_q[t]$ be the common denominator of the non-zero entries in $\mathcal{A}'$; the matrix $\mathcal{A} = c\mathcal{A}'$ and the polynomials $g_j(u) = ch_j(u)$ $(1 \le j \le L)$ satisfy the desired properties. □

By Lemma 3.12, we obtain Lemmas 3.13 and 3.14 which involve polynomials with $\mathcal{K}^*$-portion and maximal $\mathcal{K}^*$-portion, respectively, that are linearly independent.

Lemma 3.13. *Let $h_j \in \mathbb{F}_q[t][u]$ be supported on a set $\mathcal{K}_j \subseteq \mathbb{Z}^+$ $(1 \le j \le L)$, and let $\mathcal{K} = \mathcal{K}_1 \cup \ldots \cup \mathcal{K}_L$. Suppose the $\mathcal{K}^*$-portion of $(h_j)_{j=1}^L$ is linearly independent. Let $\beta_1, \ldots, \beta_L \in \mathbb{K}_\infty$. Then we can find an $L \times L$ matrix $\mathcal{T}$ with entries in $\mathbb{F}_q[t]$ and $g_j \in \mathbb{F}_q[t][u]$ $(1 \le j \le L)$ with the following properties:*

(1) g_j is a polynomial supported on a subset of $\mathcal{K}$.

(2) $\mathcal{T} \begin{pmatrix} h_1(u) \\ \vdots \\ h_L(u) \end{pmatrix} = \begin{pmatrix} g_1(u) \\ \vdots \\ g_L(u) \end{pmatrix}.$

(3) There exist $T_j \in \mathcal{K}^*$ $(1 \le j \le L)$ such that $[g_i]_{T_j} = 0$ if $i \neq j$.

(4) There exist $\gamma_j \in \mathbb{K}_\infty$ $(1 \le j \le L)$ such that

$$\beta_1 h_1(u) + \ldots + \beta_L h_L(u) = \gamma_1 g_1(u) + \ldots + \gamma_L g_L(u).$$

Proof. By the hypothesis, the polynomials $\{h_j^*\}_{j=1}^L$ are linearly independent over $\mathbb{K}$. Therefore, we can find an $L \times L$ invertible matrix $\mathcal{B}$ with entries in $\mathbb{K}$ such that

$$\mathcal{B} \ (h_1^*, \ldots, h_L^*)^T = (b_1, \ldots, b_L)^T,$$

where $b_j \in \mathbb{F}_q[t][u]$ with coefficients supported on a subset of $\mathcal{K}^*$ and $\deg b_1 < \ldots < \deg b_L$. Let $\mathcal{A}$ and $g_1', \ldots, g_L'$ be the matrix and polynomials, respectively, obtained by applying

Lemma 3.12 to the polynomials $b_1, ..., b_L$ with $d = 1$ and $s = 0$. It follows that the polynomials g'_j have coefficients supported on a subset of $\mathcal{K}^*$. Let $T_j = \deg g'_j = \deg b_j \in \mathcal{K}^* (1 \leq j \leq L)$. Also let

$$(g''_1, ..., g''_L)^T = \mathcal{AB}\ (h_1 - h^*_1, ..., h_L - h^*_L)^T$$

and

$$g_j := g'_j + g''_j\ (1 \leq j \leq L).$$

Let c_j be the common denominator of the coefficients of $g_j \in \mathbb{K}[u]$ $(1 \leq j \leq L)$, c' be the common denominator of the matrix $\mathcal{AB}$, and $c = c' \prod_{j=1}^{L} c_j$. By construction, we see that cg_j is a polynomial in $\mathbb{F}_q[t][u]$ with coefficients supported on a subset of $\mathcal{K}$,

$$(cg_j)^* = c(g^*_j) = cg'_j,$$

and

$$(cg_1(u), ..., cg_L(u))^T = c\mathcal{AB}\ (h_1(u), ..., h_L(u))^T.$$

Since $[g'_i]_{T_j} = 0$ if $i \neq j$, it follows that $[cg_i]_{T_j} = 0$ if $i \neq j$. Let

$$(\gamma_1, ..., \gamma_L) = (\beta_1, ..., \beta_L)\ (c\mathcal{AB})^{-1}.$$

Then we have

$$\gamma_1 cg_1(u) + ... + \gamma_L cg_L(u) = \beta_1 h_1(u) + ... + \beta_L h_L(u).$$

Therefore, we see that the matrix $c\mathcal{AB}$ and the polynomials cg_j $(1 \leq j \leq L)$ satisfy the desired properties. □

Let $f(u) = \sum_{r \in \mathcal{K} \cup \{0\}} \alpha_r u^r$ be a polynomial supported on a set $\mathcal{K} \subseteq \mathbb{Z}^+$ with coefficients in $\mathbb{K}_\infty$. For any $r \in \mathcal{K}$ and $y, s \in \mathbb{F}_q[t]$, we have

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

Therefore, for a fixed s, if k is maximal in $\mathcal{K}$, then there exist $\alpha'_j = \alpha'_j(\{\alpha_r\}_{r \in \mathcal{K}}; s) \in \mathbb{K}_\infty$ $(j \in \mathcal{S}(\mathcal{K}) \backslash \{k\})$ and $\alpha'_0 = \alpha'_0(\{\alpha_r\}_{r \in \mathcal{K} \cup \{0\}}; s) \in \mathbb{K}_\infty$ such that

$$f(y + s) = \alpha_k (y + s)^k + \sum_{r \in \mathcal{K} \backslash \{k\}} \alpha_r (y + s)^r + \alpha_0 = \alpha_k y^k + \sum_{j \in \mathcal{S}(\mathcal{K}) \backslash \{k\}} \alpha'_j y^j + \alpha'_0.$$

In other words, the y^k coefficient of $f(y)$ and $f(y+s)$ are the same. Therefore, it follows that if $k_1, ..., k_M$ are maximal in $\mathcal{K}$, then

$$f(y+s) = \sum_{i=1}^{M} \alpha_{k_i} y^{k_i} + \sum_{j \in \mathcal{S}(\mathcal{K}) \setminus \{k_1, ..., k_M\}} \alpha'_j y^j + \alpha'_0. \tag{3.6}$$

Lemma 3.14. *Let $h_j \in \mathbb{F}_q[t][u]$ be supported on a set $\mathcal{K}_j \subseteq \mathbb{Z}^+$ $(1 \leq j \leq L)$, and let $\mathcal{K} = \mathcal{K}_1 \cup ... \cup \mathcal{K}_L$. Suppose the maximal $\mathcal{K}^*$-portion of $(h_j)_{j=1}^L$ is linearly independent. Let $\beta_1, ..., \beta_L \in \mathbb{K}_\infty$ and $s, d \in \mathbb{F}_q[t]$ with $d \neq 0$. Then we can find $g_j \in \mathbb{F}_q[t][u]$ $(1 \leq j \leq L)$, depending on d and s, and an $L \times L$ matrix $\mathcal{T}$ with entries in $\mathbb{F}_q[t]$ with the following properties:*

(1) g_j is a polynomial supported on a subset of $\mathcal{S}(\mathcal{K})$ and every entry of $\mathcal{T}$ depends only on $h_1, ..., h_L$.

(2) $\mathcal{T} \begin{pmatrix} h_1(du+s) \\ \vdots \\ h_L(du+s) \end{pmatrix} = \begin{pmatrix} g_1(u) \\ \vdots \\ g_L(u) \end{pmatrix}.$

(3) For $x \in \mathbb{F}_q[t]$, we have

$$\operatorname{ord} g_j(x) \leq \left(\max_{1 \leq j \leq L} \deg h_j \right) \operatorname{ord}(dx+s) + D,$$

where D is some constant dependent only on $h_1, ..., h_L$.

(4) There exist $T_j \in \mathcal{K}^*$ $(1 \leq j \leq L)$ such that T_j is maximal in $\mathcal{K}$ and $[g_i]_{T_j} = 0$ if $i \neq j$. Moreover, we have $[g_j]_{T_j} = \tilde{c}_j d^{T_j}$ for some $\tilde{c}_j \in \mathbb{F}_q[t]$ dependent only on $h_1, ..., h_L$.

(5) There exist $\gamma_j \in \mathbb{K}_\infty$ $(1 \leq j \leq L)$ such that

$$\beta_1 h_1(du+s) + ... + \beta_L h_L(du+s) = \gamma_1 g_1(u) + ... + \gamma_L g_L(u).$$

Proof. Let $h_j(u) = \sum_{r \in \mathcal{K}_j \cup \{0\}} c_{j,r} u^r$ for $1 \leq j \leq L$. We also let $\mathcal{H}_j = \{r \in \mathcal{K}_j \cap \mathcal{K}^* :$ r is maximal in $\mathcal{K}\}$ so that $h_j^{\max}(u) = \sum_{r \in \mathcal{H}_j} c_{j,r} u^r$. Let $\mathcal{H} = \mathcal{H}_1 \cup ... \cup \mathcal{H}_L$. We have by

(3.6), the maximality condition of $r \in \mathcal{H}_j$, that

$$h_j(du+\widetilde{s}) = \sum_{r\in\mathcal{H}_j} c_{j,r}(du)^r + \sum_{v\in\mathcal{S}(\mathcal{K}_j)\backslash\mathcal{H}_j} c'_{j,v}u^v + c'_{j,0}$$

for some $c'_{j,0}, c'_{j,v} \in \mathbb{F}_q[t]$ $(1 \leq j \leq L, v \in \mathcal{S}(\mathcal{K}_j)\backslash\mathcal{H}_j)$. For any $l \neq j$, we have $(\mathcal{S}(\mathcal{K}_j)\backslash\mathcal{H}_j) \cap \mathcal{H}_l = \varnothing$. Suppose $v \in (\mathcal{S}(\mathcal{K}_j)\backslash\mathcal{H}_j) \cap \mathcal{H}_l$. Since v is maximal in $\mathcal{K}$, the only way v can be an element of $\mathcal{S}(\mathcal{K}_j)$ is if $v \in \mathcal{K}_j$. However, this forces $v \in \mathcal{H}_j$ which is a contradiction. Therefore, we can in fact write $h_j(du+\widetilde{s})$ as

$$h_j(du+\widetilde{s}) = h_j^{\max}(du) + \sum_{v\in\mathcal{S}(\mathcal{K})\backslash\mathcal{H}} c'_{j,v}u^v + c'_{j,0}. \tag{3.7}$$

By the hypothesis, the polynomials $\{h_j^{\max}\}_{j=1}^{L}$ are linearly independent over $\mathbb{K}$. Therefore, we can find an $L \times L$ invertible matrix $\mathcal{B}$ with entries in $\mathbb{F}_q[t]$ such that

$$\mathcal{B}\ (h_1^{\max}, ..., h_L^{\max})^T = (b_1, ..., b_L)^T,$$

where $b_j \in \mathbb{F}_q[t][u]$ $(1 \leq j \leq L)$ with coefficients supported on a subset of $\mathcal{H}$ and $\deg b_1 < ... < \deg b_L$. The entries of the matrix $\mathcal{B}$ and the polynomials $b_1, ..., b_L$ are dependent only on $h_1^{\max}, ..., h_L^{\max}$. Clearly we have

$$\mathcal{B}\ (h_1^{\max}(du), ..., h_L^{\max}(du))^T = (b_1(du), ..., b_L(du))^T.$$

Let $\mathcal{A}$ and $g'_1, ..., g'_L$ be the matrix and polynomials, respectively, obtained by applying Lemma 3.12 to the polynomials $b_1, ..., b_L$ with $s = 0$ and d. It follows that the coefficients of g'_j $(1 \leq j \leq L)$ are supported on a subset of $\mathcal{H}$. Note by (2) of Lemma 3.12, the entries of $\mathcal{A}$ depend only on $h_1, ..., h_L$. Let $T_j = \deg g'_j = \deg b_j \in \mathcal{H}$ $(1 \leq j \leq L)$. We have by (3) of Lemma 3.12 that $[g'_j]_{T_j} = cd^{T_j}[b_j]_{T_j}$ for some $c \in \mathbb{F}_q[t]$ dependent only on $b_1, ..., b_L$, and $[g'_i]_{T_j} = 0$ if $i \neq j$. Let

$$(g''_1, ..., g''_L)^T = \mathcal{A}\mathcal{B}\ (h_1(du+\widetilde{s}) - h_1^{\max}(du), ..., h_L(du+\widetilde{s}) - h_L^{\max}(du))^T.$$

We define polynomials g_j by

$$g_j := g'_j + g''_j\ (1 \leq j \leq L),$$

then we have

$$(g_1(u), ..., g_L(u))^T = \mathcal{A}\mathcal{B}\ (h_1(du+\widetilde{s}), ..., h_L(du+\widetilde{s}))^T. \tag{3.8}$$

By construction, we see that g_j and g_j'' are polynomials in $\mathbb{F}_q[t][u]$ with coefficients supported on a subset of $\mathcal{S}(\mathcal{K})$ and a subset of $\mathcal{S}(\mathcal{K})\backslash\mathcal{H}$, respectively. Then (4) of this lemma follows by the fact that $[g_i]_{T_j} = [g_i']_{T_j}$ $(1 \leq i, j \leq L)$.

Let

$$(\gamma_1, ..., \gamma_L) = (\beta_1, ..., \beta_L)\ (\mathcal{A}\mathcal{B})^{-1}.$$

Then we have

$$\gamma_1 g_1(u) + ... + \gamma_L g_L(u) = \beta_1 h_1(du + \widetilde{s}) + ... + \beta_L h_L(du + \widetilde{s}).$$

Finally, recall from above that the entries of matrices $\mathcal{A}$ and $\mathcal{B}$ are dependent only on $h_1, ..., h_L$. Then (3) of this lemma follows easily from (3.8). □

3.4 Proof of the Main Results

We have collected enough material in the previous sections to prove our main results of the chapter. We begin this section by proving Theorems 3.3 and 3.5.

Proof of Theorem 3.3. Let β be an arbitrary element in $\mathbb{K}_\infty$. Let $M = \lfloor \theta N \rfloor + 1$, where θ is a sufficiently small positive number to be chosen later. We prove by contradiction that for any N sufficiently large,

$$\min_{x \in \mathbb{G}_N} \operatorname{ord} \{\beta h(x)\} \leq -M \leq -\theta N.$$

Suppose for some N sufficiently large in terms of $\mathcal{K}$, q, θ, and $\operatorname{ord} c_k$, we have $\operatorname{ord}\{\beta h(x)\} > -M$ for all $x \in \mathbb{G}_N$. Then by Lemma 3.9, there exists $y \in \mathbb{G}_M\backslash\{0\}$ such that

$$\Big| \sum_{x \in \mathbb{G}_N} e(y\beta h(x)) \Big| \geq \frac{q^N}{q^M - 1} > q^{N-M}.$$

It follows by Corollary 3.11 that for $\theta < c$ there exists $g \in \mathbb{F}_q[t]$ such that $\operatorname{ord} g < CM$ and $\operatorname{ord}\{gy\beta c_k\} \leq -kN + CM$ for some constants $c, C > 0$, depending only on $\mathcal{K}$ and q.

By the hypothesis, we know there exists $x \in \mathbb{G}_{\operatorname{ord}(gyc_k)}$ such that $h(x) \equiv 0 \pmod{gyc_k}$. Since N is sufficiently large, by taking $\theta < 1/(C+1)$ we have

$$\operatorname{ord} x < \operatorname{ord}(gyc_k) < CM + M + \operatorname{ord} c_k \leq N.$$

We denote by D some constant dependent only on h. We have

$$\begin{aligned}
\operatorname{ord}\{\beta h(x)\} &\leq \min_{z\in\mathbb{F}_q[t]} \operatorname{ord}\left(\beta h(x) - \frac{h(x)}{gyc_k}z\right) \\
&= \operatorname{ord}\left(\frac{h(x)}{gyc_k}\right) + \operatorname{ord}\{gy\beta c_k\} \\
&\leq D + (\operatorname{ord} g + \operatorname{ord} y)(\deg h - 1) + \operatorname{ord}\{gy\beta c_k\} \\
&\leq D + (CM + M)(\deg h - 1) + CM - kN \\
&= D + ((C+1)(\deg h - 1) + C)M - kN.
\end{aligned}$$

Suppose

$$\theta < \min\left\{\frac{1}{(C+1)(\deg h - 1) + C + 1}, \frac{1}{C+1}\right\}.$$

Then for N sufficiently large in terms of D, we obtain from above that $\operatorname{ord}\{\beta h(x)\} \leq -M$, which is a contradiction. □

Proof of Theorem 3.5. Let $\beta_1, ..., \beta_L$ be arbitrary elements in $\mathbb{K}_\infty$. Let $M = \lfloor \theta N \rfloor + 1$ and θ be a sufficiently small positive number to be chosen later. To obtain contradiction, suppose for some N sufficiently large in terms of $\mathcal{K}$, q and θ, we have

$$\operatorname{ord}\{\beta_1 h_1(x) + ... + \beta_L h_L(x)\} > -M$$

for all $x \in \mathbb{G}_N$.

Let $\mathcal{T}$ and $g_1, ..., g_L$ be the matrix and polynomials, respectively, obtained by applying Lemma 3.13 to the polynomials $h_1, ..., h_L$. We also have by (3) and (4) of Lemma 3.13 that there exist $T_j \in \mathcal{K}^*$ $(1 \leq j \leq L)$ such that $[g_i]_{T_j} = 0$ if $i \neq j$, and $\gamma_j \in \mathbb{K}_\infty$ $(1 \leq j \leq L)$ such that

$$\beta_1 h_1(u) + ... + \beta_L h_L(u) = \gamma_1 g_1(u) + ... + \gamma_L g_L(u).$$

Hence for all $x \in \mathbb{G}_N$, we have

$$\operatorname{ord}\{\gamma_1 g_1(x) + ... + \gamma_L g_L(x)\} > -M. \tag{3.9}$$

Then, by Lemma 3.9, there exists $y \in \mathbb{G}_M \backslash \{0\}$ with

$$\Big|\sum_{x\in\mathbb{G}_N} e(y\gamma_1 g_1(x) + ... + y\gamma_L g_L(x))\Big| \geq \frac{q^N}{q^M - 1} > q^{N-M}.$$

Let $f(u) = y\gamma_1 g_1(u) + ... + y\gamma_L g_L(u)$, and suppose it is supported on $\widehat{\mathcal{K}} \subseteq \mathbb{Z}^+$. We can verify that each $T_j \in (\widehat{\mathcal{K}})^*$. Applying Corollary 3.11 with $f(u)$, we obtain that for $\theta < c$ there exists $g \in \mathbb{F}_q[t]$ such that $\operatorname{ord} g < CM$ and

$$\operatorname{ord}\{g[f]_{T_j}\} = \operatorname{ord}\{gy\gamma_j[g_j]_{T_j}\} \leq CM - T_jN \ (1 \leq j \leq L), \tag{3.10}$$

for some constants $c, C > 0$ depending only on $\mathcal{K}$ and q.

Let $v = gy\prod_{j=1}^{L}[g_j]_{T_j}$ and let D be some constant dependent only on $g_1, ..., g_L$. Consequently, D is dependent only on $h_1, ..., h_L$. Note the actual value of D may vary from line to line during calculations. Then

$$\operatorname{ord} v \leq D + \operatorname{ord} gy \leq D + CM + M$$

and we make sure $\operatorname{ord} v < N$ by taking N sufficiently large with respect to D. Thus for all $1 \leq j \leq L$, we have

$$\begin{aligned} \operatorname{ord}\{v\gamma_j\} &= \min_{z\in\mathbb{F}_q[t]} \operatorname{ord}(v\gamma_j - z) \qquad (3.11) \\ &\leq \min_{z\in\mathbb{F}_q[t]} \operatorname{ord}\left(v\gamma_j - z\prod_{i\neq j}[g_i]_{T_i}\right) \\ &= \min_{z\in\mathbb{F}_q[t]} \operatorname{ord}\left(\prod_{i\neq j}[g_i]_{T_i}\right) + \operatorname{ord}\left(gy\gamma_j[g_j]_{T_j} - z\right) \\ &= \operatorname{ord}\left(\prod_{i\neq j}[g_i]_{T_i}\right) + \min_{z\in\mathbb{F}_q[t]} \operatorname{ord}\left(gy\gamma_j[g_j]_{T_j} - z\right) \\ &= \sum_{i\neq j} \operatorname{ord}\left([g_i]_{T_i}\right) + \operatorname{ord}\{gy\gamma_j[g_j]_{T_j}\} \\ &\leq D + CM - T_jN, \end{aligned}$$

where we used (3.10) to obtain the last inequality. It follows that if we let $a_j = (v\gamma_j - \{v\gamma_j\}) \in \mathbb{F}_q[t]$, then we have

$$\operatorname{ord}\left(\gamma_j - \frac{a_j}{v}\right) \leq D + CM - T_jN - \operatorname{ord} v \quad (1 \leq j \leq L).$$

Recall each g_j is a linear combination over $\mathbb{F}_q[t]$ of $h_1, ..., h_L$. Thus by the hypothesis, we know there exists $n \in \mathbb{G}_{\text{ord}\, v}$ such that

$$a_1 g_1(n) + ... + a_L g_L(n) \equiv 0 \text{ (mod } v).$$

Clearly, we have $\max_{1\le j\le L} \deg g_j \le \max_{1\le j\le L} \deg h_j$. Thus we obtain

$$\begin{aligned}
\text{ord}\left\{\sum_{j=1}^{L} \gamma_j g_j(n)\right\} &\le \text{ord}\left(\sum_{j=1}^{L} \gamma_j g_j(n) - \frac{1}{v}\sum_{j=1}^{L} a_j g_j(n)\right) \\
&= \text{ord}\left(\sum_{j=1}^{L} \left(\gamma_j - \frac{a_j}{v}\right) g_j(n)\right) \\
&\le \max_{1\le j\le L} \text{ord}\left(\left(\gamma_j - \frac{a_j}{v}\right) g_j(n)\right) \\
&\le \max_{1\le j\le L} CM - T_j N + (\text{ord}\, v)(\deg g_j - 1) + D \\
&\le \max_{1\le j\le L} CM - T_j N + (CM + M)(\deg g_j - 1) + D \\
&\le -N + CM + (C+1)\left(\max_{1\le j\le L} \deg h_j - 1\right) M + D.
\end{aligned}$$

Suppose θ is sufficiently small in terms of C and $\max_{1\le j\le L} \deg h_j$. Then it is not too difficult to see that the final quantity obtained above is less than or equal to $-M$ for N sufficiently large, which contradicts (3.9). Therefore, there exists some $m \in \mathbb{G}_N$ such that

$$\text{ord}\,\{\beta_1 h_1(m) + ... + \beta_L h_L(m)\} \le -M \le -\theta N.$$

□

Recall from Section 3.2 that corresponding to any system of polynomials $(h_1, ..., h_L)$ *satisfying Condition* $(\star)$, *we can associate a sequence* $(r_x)_{x\in\mathbb{F}_q[t]\setminus\{0\}}$ *such that (3.3) is satisfied. We prove the following theorem.*

Theorem 3.15. *Let* $h_j \in \mathbb{F}_q[t][u]$ *be supported on a set* $\mathcal{K}_j \subseteq \mathbb{Z}^+$ $(1 \le j \le L)$, *and let* $\mathcal{K} = \mathcal{K}_1 \cup ... \cup \mathcal{K}_L$. *Suppose the system* $(h_j)_{j=1}^L$ *satisfies Condition* $(\star)$ *and that the maximal* $\mathcal{K}^*$-*portion of* $(h_j)_{j=1}^L$ *is linearly independent. Then there exist* $\theta = \theta(\mathcal{K}, q, \max_{1\le j\le L} \deg h_j), \sigma = \sigma(h_1, ..., h_L) > 0$ *and* $N_0 = N_0(\mathcal{K}, q, \theta, \sigma, h_1, ..., h_L) \in \mathbb{Z}^+$ *such that the following holds when* $N > N_0$. *Given any* $d \in \mathbb{F}_q[t]$ *with* $\text{ord}\, d < \lfloor \sigma N \rfloor$, *and* $\beta_1, ..., \beta_L$ *in* $\mathbb{K}_\infty$, *there exists* $n \in \mathbb{G}_N$ *such that* $n \equiv r_d$ *(mod* d*) and*

$$\text{ord}\,\{\beta_1 h_1(n) + ... + \beta_L h_L(n)\} \le -\theta N.$$

Proof. Let $\beta_1, ..., \beta_L$ be arbitrary elements in $\mathbb{K}_\infty$ and d be an arbitrary element in $\mathbb{G}_{\lfloor \sigma N \rfloor}$. Let θ and σ be positive real numbers sufficiently small to be chosen later, and let $M = \lfloor \theta N \rfloor + 1$. Suppose for some N sufficiently large in terms of $\mathcal{K}$, q, σ, and θ, we have

$$\operatorname{ord}\{\beta_1 h_1(dx + r_d) + ... + \beta_L h_L(dx + r_d)\} > -M$$

for all $x \in \mathbb{G}_{\lfloor (1-\sigma)N \rfloor}$. Let $\mathcal{T}$ and $g_1, ..., g_L$ be the matrix and polynomials, respectively, obtained by applying Lemma 3.14 to the polynomials $h_1, ..., h_L$ with $s = r_d$ and d. By (4) of Lemma 3.14, we know there exist $T_j \in \mathcal{K}^*$ $(1 \le j \le L)$ such that T_j is maximal in $\mathcal{K}$, $[g_i]_{T_j} = 0$ if $i \neq j$, and $[g_j]_{T_j} = \tilde{c}_j d^{T_j}$ for some $\tilde{c}_j \in \mathbb{F}_q[t]$ dependent only on $h_1, ..., h_L$. We also know there exist $\gamma_j \in \mathbb{K}_\infty$ $(1 \le j \le L)$ such that

$$\beta_1 h_1(du + r_d) + ... + \beta_L h_L(du + r_d) = \gamma_1 g_1(u) + ... + \gamma_L g_L(u).$$

Thus we have

$$\operatorname{ord}\{\gamma_1 g_1(x) + ... + \gamma_L g_L(x)\} > -M \tag{3.12}$$

for all $x \in \mathbb{G}_{\lfloor (1-\sigma)N \rfloor}$. By Lemma 3.9, there exists $y \in \mathbb{G}_M \backslash \{0\}$ such that

$$\Big| \sum_{x \in \mathbb{G}_{\lfloor (1-\sigma)N \rfloor}} e(y\gamma_1 g_1(x) + ... + y\gamma_L g_L(x)) \Big| \ge \frac{q^{\lfloor (1-\sigma)N \rfloor}}{q^M - 1} > q^{N - (\sigma+\theta)N}.$$

Let $f(u) = y\gamma_1 g_1(u) + ... + y\gamma_L g_L(u)$, and suppose it is supported on $\widehat{\mathcal{K}} \subseteq \mathbb{Z}^+$. We can verify that each $T_j \in (\widehat{\mathcal{K}})^*$. Applying Corollary 3.11 with $f(u)$, we obtain that for $(\sigma + \theta) < c$ there exists $g \in \mathbb{F}_q[t]$ such that $\operatorname{ord} g < C(\sigma + \theta)N$ and

$$\operatorname{ord}\{g[f]_{T_j}\} = \operatorname{ord}\{gy\gamma_j[g_j]_{T_j}\} \le C(\sigma + \theta)N - T_j\lfloor (1-\sigma)N \rfloor \quad (1 \le j \le L), \tag{3.13}$$

for some constants $c, C > 0$ depending only on $\mathcal{K}$ and q. Let $v = gy\prod_{j=1}^{L}[g_j]_{T_j}$ and let D be some constant dependent only on $h_1, ..., h_L$ (note the actual value of D may vary from line to line during calculations). We define $T' = \sum_{1 \le j \le L} T_j$. Then

$$\operatorname{ord} v \le \operatorname{ord} gy + T' \operatorname{ord} d + D \le C(\sigma + \theta)N + M + T'\lfloor \sigma N \rfloor + D.$$

In particular, we have $\operatorname{ord} v < \lfloor (1-\sigma)N \rfloor$ for N sufficiently large with respect to D and θ, σ sufficiently small.

For simplicity denote $n = r_v \in \mathbb{G}_{\operatorname{ord} v}$, then $h_j(n)$ is divisible by v for any $1 \le j \le L$. We also have $n \equiv r_d \pmod{d}$, because $d|v$. Each $g_j(u)$ can be written as an $\mathbb{F}_q[t]$-linear combination of the polynomials $h_1(du+r_d), ..., h_L(du+r_d)$. Thus if we write $n = dw + r_d$ for some $w \in \mathbb{G}_{\operatorname{ord} v}$, then $g_j(w)$ is divisible by v for any $1 \leq j \leq L$. Let $H = \max_{1 \leq j \leq L} \deg h_j$. Then it follows that

$$\begin{aligned}
\operatorname{ord}\{\gamma_j g_j(w)\} &\leq \min_{z \in \mathbb{F}_q[t]} \operatorname{ord}\left(\gamma_j g_j(w) - z\frac{g_j(w)}{v}\right) \\
&= \operatorname{ord}\left(\frac{g_j(w)}{v}\right) + \min_{z \in \mathbb{F}_q[t]} \operatorname{ord}\left(v\gamma_j - z\right) \\
&= \operatorname{ord}\left(\frac{g_j(w)}{v}\right) + \operatorname{ord}\{v\gamma_j\} \\
&\leq D + H(\operatorname{ord} d + \operatorname{ord} w) - \operatorname{ord} v + \operatorname{ord}\{v\gamma_j\},
\end{aligned} \tag{3.14}$$

where the last inequality is obtained via (3) of Lemma 3.14. We also have by similar calculations as in (3.11) that for $1 \leq j \leq L$,

$$\begin{aligned}
\operatorname{ord}\{v\gamma_j\} &= \min_{z \in \mathbb{F}_q[t]} \operatorname{ord}\left(v\gamma_j - z\right) \\
&\leq \min_{z \in \mathbb{F}_q[t]} \operatorname{ord}\left(v\gamma_j - z\prod_{i \neq j}[g_i]_{T_i}\right) \\
&= \operatorname{ord}\left(\prod_{i \neq j}[g_i]_{T_i}\right) + \min_{z \in \mathbb{F}_q[t]} \operatorname{ord}\left(gy\gamma_j[g_j]_{T_j} - z\right) \\
&= \sum_{i \neq j} \operatorname{ord}\left([g_i]_{T_i}\right) + \operatorname{ord}\{gy\gamma_j[g_j]_{T_j}\} \\
&= \left(\sum_{i \neq j} \operatorname{ord} \tilde{c}_i + T_i \operatorname{ord} d\right) + \operatorname{ord}\{gy\gamma_j[g_j]_{T_j}\} \\
&\leq T' \operatorname{ord} d + D + C(\sigma + \theta)N - T_j\lfloor(1-\sigma)N\rfloor,
\end{aligned} \tag{3.15}$$

where we used (3.13) to obtain the last inequality. Therefore, we have by (3.4), (3.14), and (3.15) that

$$\begin{aligned}
&\operatorname{ord}\Big\{\sum_{j=1}^{L}\gamma_j g_j(w)\Big\}\\
\leq\;& \max_{1\leq j\leq L}\operatorname{ord}\{\gamma_j g_j(w)\}\\
\leq\;& T'\operatorname{ord} d + D + C(\sigma+\theta)N - \lfloor(1-\sigma)N\rfloor \min_{1\leq j\leq L} T_j + H(\operatorname{ord} d + \operatorname{ord} w) - \operatorname{ord} v\\
\leq\;& \sigma T'N + D + C(\sigma+\theta)N - \lfloor(1-\sigma)N\rfloor \min_{1\leq j\leq L} T_j + H(\sigma N + \operatorname{ord} v) - \operatorname{ord} v\\
\leq\;& \sigma T'N + D + C(\sigma+\theta)N - \lfloor(1-\sigma)N\rfloor + \sigma HN + H(C(\sigma+\theta)N + M + \sigma T'N).
\end{aligned}$$

Suppose θ is sufficiently small in terms of C and H, and also that σ is sufficiently small in terms of C, T' and H. Then for N sufficiently large, the final quantity obtained above is less than or equal to $-M$, which contradicts (3.12). Therefore, there exists $x \in \mathbb{G}_{\lfloor(1-\sigma)N\rfloor}$ such that $m = dx + r_d \in \mathbb{G}_N$ and

$$\operatorname{ord}\{\beta_1 h_1(m) + ... + \beta_L h_L(m)\} \leq -M \leq -\theta N.$$

□

Chapter 4

On a problem of Sidon for polynomials over finite fields

4.1 Introduction

In the course of investigations on Fourier series by S. Sidon, several questions arose concerning the existence and nature of certain positive integer sequences ω for which $r_n(\omega) = |\{(a, b) \in \omega \times \omega \colon a + b = n, 0 < a < b\}|$ is bounded or, in some sense, exceptionally small, where $|S|$ denotes the cardinality of the set S. In particular, he asked the following question in 1932, known as the Sidon Problem [3]:

> *Does there exist a sequence ω such that $r_n(\omega) > 0$ for all n sufficiently large and, for all $\epsilon > 0$,*
> $$\lim_{n\to\infty} \frac{r_n(\omega)}{n^\epsilon} = 0 \ ?$$

In 1954, P. Erdős answered positively to the question by proving the following [3]:

Theorem 4.1 (Erdős)**.** *There exists a sequence ω such that*

$$\log n \ll r_n(\omega) \ll \log n$$

for all n sufficiently large.

In other words, there exists a "thin" set ω such that every positive integer sufficiently large can be represented as a sum of two elements in ω. On the other direction, Erdős and Rényi proved in [4] that there exists a "thick" set ω such that $r_n(\omega)$ is bounded for all n.

Theorem 4.2 (Erdős-Rényi)**.** *For any $\varepsilon > 0$, there exists a positive number $G = G(\varepsilon)$ and a sequence ω, such that $r_n(\omega) < G$ for all n and*

$$|\{m \in \omega : m \leq n\}| > n^{\frac{1}{2}-\varepsilon}$$

for sufficiently large n.

We note that the result is best possible up to the ε term. One way to see this fact is by the pigeon hole principle. Suppose we have $\omega_0 \subseteq \mathbb{N}$, where $r_n(\omega_0) < G$ for all $n \in \mathbb{N}$. Given any $m_1, m_2 \in \{m \in \omega_0 : m \leq n\}$, we have $1 < m_1 + m_2 \leq 2n$. Therefore, by the pigeon hold principle, it follows that

$$G > \max_{1<m\leq 2n} r_m(\omega_0) \geq \frac{|\{m \in \omega_0 : m \leq n\}|^2 - |\{m \in \omega_0 : m \leq n\}|}{2(2n-1)}.$$

Consequently, we obtain

$$|\{m \in \omega_0 : m \leq n\}| \ll n^{1/2}.$$

In this chapter, we prove an analogue of these results in the setting of $\mathbb{F}_q[t]$.

Let ω be a sequence of polynomials in $\mathbb{F}_q[t]$. For each $h \in \mathbb{F}_q[t]$, we define

$$r_h(\omega) = |\{(f,g) \in \mathbb{F}_q[t] \times \mathbb{F}_q[t] : f, g \in \omega, h = f+g, \deg f, \deg g \leq \deg h, f \neq g\}|.$$

Note $\deg f$ is the degree of $f \in \mathbb{F}_q[t]$ with the convention that $\deg 0 = -\infty$. We prove the following results which are joint work with Wentang Kuo.

Theorem 4.3 (Kuo & Yamagishi)**.** *There exists a sequence ω of polynomials in $\mathbb{F}_q[t]$ such that*

$$\deg h \ll r_h(\omega) \ll \deg h$$

for $\deg h$ sufficiently large.

On the other direction, we prove that there exists a "thick" set with bounded value $r_h(\omega)$. We denote the elements of ω by $\omega = \{f_i\}_{i \in \mathbb{N}}$, where $\deg f_i \leq \deg f_j$ $(i < j)$.

Theorem 4.4 (Kuo & Yamagishi)**.** *For each $\epsilon > 0$, there exists a sequence $\omega = \{f_i\}$ of polynomials in $\mathbb{F}_q[t]$ and a positive integer K such that $r_h(\omega) < K$ for all $h \in \mathbb{F}_q[t]$ and $q^{\deg f_i} \ll i^{2+\epsilon}$.*

For each $h \in \mathbb{F}_q[t]$, we define

$$\widetilde{t}_h(\omega) = |\{(f,g) \in \mathbb{F}_q[t] \times \mathbb{F}_q[t] : f, g \in \omega, h = f - g, \deg f, \deg g \leq \deg h\}|.$$

We also prove the following variation of the existence of thick sets.

Theorem 4.5 (Kuo & Yamagishi)**.** *For each $\epsilon > 0$, there exists a sequence $\omega = \{f_i\}$ of polynomials in $\mathbb{F}_q[t]$ and a positive integer K' such that $\widetilde{t}_h(\omega) < K'$ for all $h \in \mathbb{F}_q[t]$ and $q^{\deg f_i} \ll i^{2+\epsilon}$.*

We prove our theorems following the methods of Chapter III of [5], which utilizes the language of probability. Roughly speaking, we set up a probability space to study the probability of the events $\{\omega | r_h(\omega) = d\}$ for all non-negative integer d. Using the Borel-Cantelli lemma, we show that the sequences satisfy the desired properties with probability 1. We also remark that Theorems 4.4 and 4.5 have been generalized to m-fold sums and differences by K. E. Hare and Yamagishi in [7].

The organization of this chapter is as follows. In Section 4.2, we first review the basic probability theory and state the Borel-Cantelli lemma. Next, in Section 4.3, we state the equivalent statements of our theorems and set up the probability space used in our proof. In Section 4.4, we establish several technical lemmas. Finally, the remaining sections are devoted to the proof of our main results.

4.2 Preliminaries

We start with probability theory. Let $\{X_j\}$ be a sequence of spaces and write

$$X = \prod_{j=0}^{\infty} X_j.$$

Let $\mathcal{M}_j$ be a σ-algebra of subsets of X_j. A measurable rectangle with respect to the sequence $\{\mathcal{M}_j\}$ is defined to be a subset W of X which is representable in the form

$$W = \prod_{j=0}^{\infty} W_j,$$

where $W_j \in \mathcal{M}_j$ and $W_j = X_j$ except for finitely many j. The following two theorems are standard results in probability theory, see for example [5, p. 123, Thm. 5] and [5, p. 135] for reference.

Theorem 4.6. *Let $\{(X_j, \mathcal{M}_j, P_j)\}_{j \geq 0}$ be a sequence of probability spaces, and write*

$$X = \prod_{j=0}^{\infty} X_j.$$

Let $\mathcal{M}$ be the minimal σ-algebra of subsets of X containing every measurable rectangle with respect to the sequence $\{\mathcal{M}_j\}$. Then there exists a unique measure P on $\mathcal{M}$ with the property that for every non-empty measurable rectangle W,

$$P(W) = \prod_{j=0}^{\infty} P_j(W_j), \tag{4.1}$$

where the W_j are defined by $W = \prod_{j=0}^{\infty} W_j$, $W_j \in \mathcal{M}_j$ $(j \geq 0)$.

We remark that the product in (4.1) is, in essence, a finite product by the definition of measurable rectangles with respect to the sequence $\{\mathcal{M}_j\}$. Furthermore, since

$$P(X) = \prod_{j=0}^{\infty} P_j(X_j) = 1,$$

the σ-algebra $\mathcal{M}$ in conjunction with the measure P constitutes a probability space $(X, \mathcal{M}, P)$. We note that Theorem 4.6 requires axiom of choice.

Theorem 4.7 (The Borel-Cantelli Lemma)**.** *Let $(X', \mathcal{M}', P')$ be a probability space. Let $\{W_\ell\}$ be a sequence of measurable events. If*

$$\sum_{\ell=1}^{\infty} P'(W_\ell) < \infty,$$

then, with probability 1, at most finite number of the events W_ℓ can occur; or, equivalently,

$$P'\left(\bigcap_{i=1}^{\infty} \bigcup_{\ell=i}^{\infty} W_\ell\right) = 0.$$

4.3 Probability Space $(\Omega, \mathcal{M}, P)$

We let $q = p^s$ for a prime p, and denote $\mathbb{F}_q$ to be the finite field of q elements. Let $\mathbb{F}_q[t]$ be the polynomial ring over $\mathbb{F}_q$. Let ι be any bijective map from $\mathbb{Z} \cap [0, q-1]$ to $\mathbb{F}_q$. We label each of the polynomials in $\mathbb{F}_q[t]$ as follows. Let $\mathbb{Z}_{\geq 0}$ be the set of all non-negative integers. For every $N \in \mathbb{Z}_{\geq 0}$, we define

$$p_N := \iota(c_0) + \iota(c_1)t + \ldots\ + \iota(c_n)t^n,$$

where $N = c_0 + c_1 q + \ldots\ + c_n q^n$ and $0 \leq c_i < q$ $(1 \leq i \leq n)$. It is clear that this identification gives a one-to-one correspondence of sets between $\mathbb{Z}_{\geq 0}$ and $\mathbb{F}_q[t]$.

We use ω to denote a subsequence of the sequence of all polynomials in $\mathbb{F}_q[t]$, i.e. $p_0, p_1, p_2, p_3, \ldots$ and Ω to denote the space of all such sequences ω. By $f \in \omega$, we mean $f \in \mathbb{F}_q[t]$ appears in the sequence ω. Given $N \in \mathbb{Z}_{\geq 0}$ and $\omega \in \Omega$, we define

$$r_N(\omega) = |\{(a,b) \in \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0} \colon p_a, p_b \in \omega,\ p_N = p_a + p_b,\ \deg p_a, \deg p_b \leq \deg p_N,\ a < b\}|,$$

and

$$\widetilde{t}_N(\omega) = |\{(a,b) \in \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0} \colon p_a, p_b \in \omega,\ p_N = p_a - p_b,\ \deg p_a, \deg p_b \leq \deg p_N\}|.$$

We prove the following results which our main theorems, namely Theorems 4.3, 4.4 and 4.5, are consequences of.

Theorem 4.8. *There exists a sequence ω of polynomials in $\mathbb{F}_q[t]$ such that*

$$\log N \ll r_N(\omega) \ll \log N$$

for N sufficiently large.

Theorem 4.9. *For each $\epsilon > 0$, there exists a sequence $\omega = \{p_{b_j}\}$ of polynomials in $\mathbb{F}_q[t]$ and a positive integer K_0 such that $r_N(\omega) < K_0$ for all $N \in \mathbb{Z}_{\geq 0}$ and $b_j \ll j^{2+\epsilon}$.*

Theorem 4.10. *For each $\epsilon > 0$, there exists a sequence $\omega = \{p_{b_j}\}$ of polynomials in $\mathbb{F}_q[t]$ and a positive integer K_0' such that $\widetilde{t}_N(\omega) < K_0'$ for all $N \in \mathbb{Z}_{\geq 0}$ and $b_j \ll j^{2+\epsilon}$.*

Since $\deg p_N \leq \log_q N < \deg p_N + 1$, we can easily derive Theorems 4.3, 4.4, and 4.5, from Theorems 4.8, 4.9, and 4.10, respectively.

We now prove the existence of the following probability space. The content of this theorem is essentially [5, p. 141, Thm. 13].

Theorem 4.11. *Let*

$$\alpha_0, \alpha_1, \alpha_2, \alpha_3, ..,$$

be real numbers satisfying $0 \leq \alpha_i \leq 1$ $(i \geq 0)$*. Then there exists a probability space* $(\Omega, \mathcal{M}, P)$ *with the following two properties:*

(i) For every non-negative integer m*, the event* $\mathfrak{B}_m = \{\omega \in \Omega \colon p_m \in \omega\}$ *is measurable and* $P(\mathfrak{B}_m) = \alpha_m$*.*

(ii) The events $\mathfrak{B}_0, \mathfrak{B}_1, \mathfrak{B}_2, ...$ *are independent.*

Proof. Let Y be the space of two elements, y_0 and y_1 say. For each sequence ω we associate the sequence $\{x_j\}$ of elements of Y, defined by

$$x_j = \begin{cases} y_0, & \text{if } p_j \notin \omega, \\ y_1, & \text{if } p_j \in \omega, \end{cases}$$

for $j \geq 0$. The space X consisting of all the sequences $x = \{x_j\}$ is given by

$$X = \prod_{j=0}^{\infty} X_j,$$

where $X_j = Y$ for $j \geq 0$. Let $\mathcal{M}_j = \{\phi, \{y_0\}, \{y_1\}, X_j\}$, the non-trivial σ-algebra of X_j, and let P_j be the probability measure on $\mathcal{M}_j$ such that $P_j(\{y_1\}) = \alpha_j$.

We apply Theorem 4.6 to the sequence $\{X_j, \mathcal{M}_j, P_j\}$ of probability spaces. In view of the one-to-one correspondence between the elements of X and Ω, we may denote the resulting probability space as $(\Omega, \mathcal{M}, P)$.

Now, we prove $(\Omega, \mathcal{M}, P)$ satisfies the two properties (i) and (ii). Clearly, we have

$$\mathfrak{B}_m = \{\omega \in \Omega \colon p_m \in \omega\} = \prod_{j=0}^{\infty} W_j,$$

where $W_j = X_j$ for all j except $j = m$ and $W_m = \{y_1\}$. Then, (i) follows, because $\mathfrak{B}_m \in \mathcal{M}$ by the definition of $\mathcal{M}$, and by (4.1) we have

$$P(\mathfrak{B}_m) = \prod_{j=0}^{\infty} P_j(W_j) = P_m(\{y_1\}) = \alpha_m.$$

For (ii), we consider any finite subset of $\{\mathfrak{B}_j\}$, say $\mathfrak{B}_{j_1}, \mathfrak{B}_{j_2}, \dots , \mathfrak{B}_{j_\ell}$. Then, clearly we have

$$\bigcap_{i=1}^{\ell} \mathfrak{B}_{j_i} = \big\{\omega \in \Omega \colon p_{j_i} \in \omega \ (1 \le i \le \ell)\big\} = \prod_{j=0}^{\infty} W_j,$$

where $W_j = X_j$ for all j except $j = j_1, \dots , j_\ell$ and $W_{j_i} = \{y_1\}$ for $1 \le i \le \ell$. Thus, by (4.1) and (i) we obtain

$$P\left(\bigcap_{i=1}^{\ell} \mathfrak{B}_{j_i}\right) = \prod_{j=0}^{\infty} P_j(W_j) = \prod_{i=1}^{\ell} P_{j_i}(\{y_1\}) = \prod_{i=1}^{\ell} \alpha_{j_i} = \prod_{i=1}^{\ell} P(\mathfrak{B}_{j_i}),$$

from which (ii) follows. □

4.4 Technical Lemmas

In this section, we prove several technical lemmas used in our proofs. For each $N \in \mathbb{Z}_{\ge 0}$, let $p_N \in \mathbb{F}_q[t]$ be as prescribed in the previous section. Define

$$n := n(N) = \deg p_N = \lfloor \log_q N \rfloor.$$

Suppose $p \ne 2$. Since $\mathbb{F}_q = 2\mathbb{F}_q$, we know there exists p_{N_0} such that $p_N = p_{N_0} + p_{N_0}$. It is clear that $\deg p_{N_0} = n$; therefore, $q^n \le N_0 < q^{n+1}$. Since $\mathbb{F}_q[t]$ is closed under addition, we can uniquely pair up the rest of polynomials of degree less than or equal to n by

$$p_N = p_a + p_{\widetilde{a}},$$

where $a, \widetilde{a} \in \mathbb{Z}_{\ge 0}$, $a < \widetilde{a}$. We collect all such pairs $(a, \widetilde{a})$ and form

$$A_N = \{a \in \mathbb{Z}_{\ge 0} \colon p_N = p_a + p_{\widetilde{a}}, a < \widetilde{a}, \ \textit{and} \ \deg p_a, \deg p_{\widetilde{a}} \le n\},$$

and

$$\widetilde{A}_N = \{\widetilde{a} \in \mathbb{Z}_{\geq 0} \colon p_N = p_a + p_{\widetilde{a}}, a < \widetilde{a}, \text{ and } \deg p_a, \deg p_{\widetilde{a}} \leq n\}.$$

We have $|A_N| = |\widetilde{A}_N| = (q^{n+1} - 1)/2$*, and*

$$\{0, \dots, q^{n+1} - 1\} = A_N \bigcup \widetilde{A}_N \bigcup \{N_0\},$$

where all the unions are disjoint. Further, it is easy to see that $\{0, 1, \dots, q^n - 1\} \subseteq A_N$*, because if* $0 \leq a < q^n$*, then* p_a *has degree at most* $n - 1$*. Thus, the corresponding* $p_{\widetilde{a}}$ *must have degree* n*; therefore,* $q^n \leq \widetilde{a} < q^{n+1}$*. Hence, it follows that*

$$\widetilde{A}_N \subseteq \{q^n, q^n + 1, \dots, q^{n+1} - 1\}. \tag{4.2}$$

Let $M := M(N) = (q^{n+1} - 1)/2$*. For convenience we label the* M *elements of* A_N *by* a_i*, where* $1 \leq i \leq M$*, and the corresponding elements of* $\widetilde{A}_N$ *by* $\widetilde{a}_i$*.*

We also define λ_N *and* λ'_N *to be*

$$\lambda_N = \sum_{1 \leq i \leq M} \alpha_{a_i} \alpha_{\widetilde{a}_i},$$

and

$$\lambda'_N = \sum_{1 \leq i \leq M} \frac{\alpha_{a_i} \alpha_{\widetilde{a}_i}}{1 - \alpha_{a_i} \alpha_{\widetilde{a}_i}}.$$

Note when $p = 2$*, for* $N > 0$*, we do not have to consider the polynomial* p_{N_0} *as above. Thus we let* $M := M(N) = q^{n+1}/2$ *and we can argue in a similar manner.*

Define

$$s^*_N(\omega) = \sum_{m=0}^{N} \mathbf{1}_{\mathfrak{B}_m}(\omega),$$

where $\mathbf{1}_{\mathfrak{B}_m}$ *is the characteristic function on the set* $\mathfrak{B}_m$*. Let* $E(f)$ *denote the expectation of a random variable* f*, defined by* $E(f) = \int_X f \, dP$*. We define*

$$m^*_N = E(s^*_N) = \sum_{m=0}^{N} \alpha_m.$$

We need our sequence $\{\alpha_j\}$ to satisfy the following condition.

Hypothesis A. *The sequence $\{\alpha_j\}$ of probabilities (introduced in Theorem 4.11) satisfies the conditions: $0 < \alpha_j < 1$ $(j \geq 0)$, $\{\alpha_j\}$ is monotonic and decreasing from some point onward (i.e. for $j \geq j_1$), and $\alpha_j \to 0$ as $j \to \infty$.*

Given two sequences of real numbers π_N, π'_N $(N \geq 0)$, we denote $\pi_N \sim \pi'_N$ to mean $\frac{\pi_N}{\pi'_N} \to 1$ as $N \to \infty$. We have the following result for $s^*_N(\omega)$ and its expected value m^*_N.

Lemma 4.12. *If, in addition to Hypothesis A,*

$$m^*_N \to \infty \tag{4.3}$$

as $N \to \infty$, and

$$\sum_{N=0}^{\infty} \frac{\alpha_N}{(m^*_N)^2} < \infty, \tag{4.4}$$

then with probability 1, we have $s^*_N(\omega) \sim m^*_N$ as $N \to \infty$.

Proof. We denote $D^2(f)$ to be the variance of a random variable f, defined by

$$D^2(f) = E\big((f - E(f))^2\big).$$

The proof is basically an application of a variant of the strong law of large numbers [5, p. 140, Thm. 11], which is as follows. Let $\{f_j\}$ be a sequence of independent random variables, and let

$$s_i(\omega) = \sum_{j=0}^{i} f_j(\omega) \quad (i \geq 0).$$

Suppose we have

$$E(f_j) > 0 \quad (j \geq 0),$$
$$\lim_{i\to\infty} E(s_i) = \infty,$$

and

$$\sum_{i=0}^{\infty} \frac{D^2(f_i)}{(E(s_i))^2} < \infty.$$

Then, with probability 1, we have

$$s_i(\omega) = \big(1 + \mathbf{o}(1)\big)E(s_i)$$

as $i \to \infty$. We know that the sets $\mathfrak{B}_j$ are independent, which is equivalent to $\mathbf{1}_{\mathfrak{B}_j}(\omega)$ being independent. Thus we apply this theorem with $f_j(\omega) = \mathbf{1}_{\mathfrak{B}_j}(\omega)$, and obtain our result. □

For every $N, d \in \mathbb{Z}_{\geq 0}$, we define the event $\mathfrak{e}(N, d)$ as

$$\mathfrak{e}(N, d) = \{\omega \in \Omega : r_N(\omega) = d\}.$$

As mentioned in Section 4.1, we need to study the probability of the event $\mathfrak{e}(N, d)$. We start with the following lemma.

Lemma 4.13. *For all non-negative integers N and d, we have*

$$P\big(\mathfrak{e}(N, d)\big) = \left(\prod_{1 \leq k \leq M} (1 - \alpha_{a_k} \alpha_{\widetilde{a}_k})\right) \widetilde{\sigma}_d(N), \tag{4.5}$$

where $\widetilde{\sigma}_0(N) = 1$ and, if $d \geq 1$,

$$\widetilde{\sigma}_d(N) = \sum_{1 \leq k_1 < \ldots < k_d \leq M} \prod_{1 \leq i \leq d} \frac{\alpha_{a_{k_i}} \alpha_{\widetilde{a}_{k_i}}}{1 - \alpha_{a_{k_i}} \alpha_{\widetilde{a}_{k_i}}}. \tag{4.6}$$

Proof. We begin with the case $d = 0$. It is easy to see that

$$\mathfrak{e}(N, 0) = \bigcap_{1 \leq k \leq M} \left(\mathfrak{B}_{a_k} \cap \mathfrak{B}_{\widetilde{a}_k}\right)^{\mathbf{c}},$$

where $\mathbf{c}$ denotes taking the complement of the set. Since the sets $\mathfrak{B}_j$ ($j \geq 0$) are independent, we know that $\mathfrak{B}_{a_k} \cap \mathfrak{B}_{\widetilde{a}_k}$ ($1 \leq k \leq M$) are independent as $\{a_k : 1 \leq k \leq M\} \bigcap \{\widetilde{a}_k : 1 \leq k \leq M\} = \varnothing$. Thus, it follows that $(\mathfrak{B}_{a_k} \cap \mathfrak{B}_{\widetilde{a}_k})^{\mathbf{c}}$ ($1 \leq k \leq M$) are also independent. Hence, we have

$$P(\mathfrak{e}(N, 0)) = \prod_{1 \leq k \leq M} P\left((\mathfrak{B}_{a_k} \cap \mathfrak{B}_{\widetilde{a}_k})^{\mathbf{c}}\right) = \prod_{1 \leq k \leq M} (1 - \alpha_{a_k} \alpha_{\widetilde{a}_k}).$$

Suppose $1 \leq d \leq M$ and $\omega' \in \mathfrak{e}(N, d)$. Then there exist $k_1, k_2, \ldots, k_d$ such that $1 \leq k_i \leq M$, $a_{k_i}, \widetilde{a}_{k_i} \in \omega'$ ($1 \leq i \leq d$), and further, if $k \neq k_i$ and $1 \leq k \leq M$, then we have either $a_k \notin \omega'$ or $\widetilde{a}_k \notin \omega'$. From this observation, we can deduce that

$$P\big(\mathfrak{e}(N, d)\big) = \sum_{1 \leq k_1 < \ldots < k_d \leq M} P\big(\mathfrak{E}(k_1, \ldots, k_d)\big),$$

where $\mathfrak{E}(k_1, \dots, k_d)$ is the event

$$\bigcap_{1\le i\le d}\left(\mathfrak{B}_{a_{k_i}} \cap \mathfrak{B}_{\widetilde{a}_{k_i}}\right) \bigcap \bigcap_{\substack{1\le k\le M\\ k\ne k_i (1\le i\le d)}} \left(\mathfrak{B}_{a_k} \cap \mathfrak{B}_{\widetilde{a}_k}\right)^{\mathbf{c}}.$$

Again, by independence, we have

$$\begin{aligned} P\big(\mathfrak{E}(k_1, \dots, k_d)\big) &= \prod_{1\le i\le d} P\left(\mathfrak{B}_{a_{k_i}} \cap \mathfrak{B}_{\widetilde{a}_{k_i}}\right) \cdot \prod_{\substack{1\le k\le M\\ k\ne k_i(1\le i\le d)}} P\left(\left(\mathfrak{B}_{a_k} \cap \mathfrak{B}_{\widetilde{a}_k}\right)^{\mathbf{c}}\right) \\ &= \prod_{1\le i\le d} \alpha_{a_{k_i}}\alpha_{\widetilde{a}_{k_i}} \cdot \prod_{\substack{1\le k\le M\\ k\ne k_i(1\le i\le d)}} \left(1-\alpha_{a_k}\alpha_{\widetilde{a}_k}\right) \\ &= \prod_{1\le k\le M} \left(1-\alpha_{a_k}\alpha_{\widetilde{a}_k}\right) \cdot \prod_{1\le i\le d} \frac{\alpha_{a_{k_i}}\alpha_{\widetilde{a}_{k_i}}}{1-\alpha_{a_{k_i}}\alpha_{\widetilde{a}_{k_i}}}, \end{aligned}$$

from which the desired result follows.

Finally, if $d > M$, then the sum $\widetilde{\sigma}_d(N)$ is empty, and both sides of (4.5) are 0. □

To estimate $\widetilde{\sigma}_d(N)$, we use the following result for elementary symmetric functions.

Lemma 4.14 ([5], p. 147, Lem. 13)**.** *Let $y_1, y_2, \dots y_{M'}$ be M' non-negative real numbers. For each positive integer d, not exceeding M', let*

$$\sigma_d = \sum_{1\le k_1<\dots<k_d\le M'} y_{k_1}y_{k_2}\dots y_{k_d},$$

so that σ_d is the d-th elementary symmetric function of the y_k's. Then, for each d, we have

$$\frac{1}{d!}\sigma_1^d\left(1-\binom{d}{2}\frac{1}{\sigma_1^2}\sum_{k=1}^{M'} y_k^2\right) \le \sigma_d \le \frac{1}{d!}\sigma_1^d, \tag{4.7}$$

where we interpret $\binom{d}{2}$ to be 0 when $d = 1$.

The next lemma gives us bounds on the probability of the event $\mathfrak{e}(N, d)$ in terms of λ_N and λ'_N.

Lemma 4.15. *Let N and d be non-negative integers. Then we have*

$$P\big(\mathfrak{e}(N,d)\big) \leq \frac{(\lambda'_N)^d}{d!} e^{-\lambda_N}. \tag{4.8}$$

Furthermore, if $d \leq M$, we have

$$P\big(\mathfrak{e}(N,d)\big) \geq \frac{(\lambda'_N)^d}{d!} e^{-\lambda'_N} \left(1 - \binom{d}{2} (\lambda'_N)^{-2} Q^*\right), \tag{4.9}$$

where

$$Q^* = \sum_{1 \leq k \leq M} \left(\frac{\alpha_{a_k}\alpha_{\widetilde{a}_k}}{1 - \alpha_{a_k}\alpha_{\widetilde{a}_k}}\right)^2,$$

and $\binom{d}{2}$ is interpreted to be 0 if $d < 2$.

Proof. We note that if $d > M$, then the event $\mathfrak{e}(N,d)$ is empty and (4.8) is trivial. Suppose $1 \leq d \leq M$. We apply (4.7) with $M' = M$ and $y_k = \alpha_{a_k}\alpha_{\widetilde{a}_k}/(1 - \alpha_{a_k}\alpha_{\widetilde{a}_k})$ to estimate $\widetilde{\sigma}_d(N)$ in (4.5); thus noting that $\widetilde{\sigma}_1(N) = \lambda'_N$, we obtain

$$P\big(\mathfrak{e}(N,d)\big) \leq \left(\prod_{1 \leq k \leq M} (1 - \alpha_{a_k}\alpha_{\widetilde{a}_k})\right) \frac{(\lambda'_N)^d}{d!},$$

and

$$P\big(\mathfrak{e}(N,d)\big) \geq \left(\prod_{1 \leq k \leq M} (1 - \alpha_{a_k}\alpha_{\widetilde{a}_k})\right) \frac{(\lambda'_N)^d}{d!} \left(1 - \binom{d}{2} (\lambda'_N)^{-2} Q^*\right).$$

Applying the inequality $e^{-t/(1-t)} < 1 - t < e^{-t}$, which holds for $0 < t < 1$, with $t = \alpha_{a_k}\alpha_{\widetilde{a}_k}$ $(1 \leq k \leq M)$, we obtain

$$e^{-\lambda'_N} < \left(\prod_{1 \leq k \leq M} (1 - \alpha_{a_k}\alpha_{\widetilde{a}_k})\right) < e^{-\lambda_N}, \tag{4.10}$$

and our result follows. When $d = 0$, we have

$$P\big(\mathfrak{e}(N,d)\big) = \prod_{1 \leq k \leq M} (1 - \alpha_{a_k}\alpha_{\widetilde{a}_k}),$$

and the result is immediate from (4.10) in this case. □

To estimate λ_N and λ'_N, we first prove the following lemma.

Lemma 4.16. *If Hypothesis A is satisfied, then*

$$\lambda'_N \sim \lambda_N \tag{4.11}$$

as $N \to \infty$.

Proof. Recall from (4.2) that if $1 \leq k \leq M$, then $q^n \leq \widetilde{a}_k < q^{n+1}$. Consequently, we have

$$\alpha_{a_k}\alpha_{\widetilde{a}_k} < \alpha_{\widetilde{a}_k} \leq \alpha_{q^n} = \mathbf{o}(1)$$

as $N \to \infty$. Therefore, we obtain

$$\begin{aligned}\lambda'_N - \lambda_N &= \sum_{1\leq k\leq M} \alpha_{a_k}\alpha_{\widetilde{a}_k}\left(\frac{1}{1-\alpha_{a_k}\alpha_{\widetilde{a}_k}} - 1\right) \\ &= \sum_{1\leq k\leq M} \alpha_{a_k}\alpha_{\widetilde{a}_k}\left(\frac{\alpha_{a_k}\alpha_{\widetilde{a}_k}}{1-\alpha_{a_k}\alpha_{\widetilde{a}_k}}\right) \\ &\leq \alpha_{q^n}\lambda'_N,\end{aligned}$$

from which the result follows. □

Therefore, it is enough to estimate λ_N. The following lemma gives us an estimate for λ_N sufficient for our purpose.

Lemma 4.17. *Suppose that the sequence $\{\alpha_j\}$, introduced in Theorem 4.11, is such that*

$$\alpha_j = \alpha\frac{(\log j)^{c'}}{j^c}$$

for $j \geq j_0$; where j_0, α, c, c' are constants such that $\alpha > 0$, $0 < \alpha_j < 1$ $(j \geq 0)$, $0 < c < 1$, and $c' \geq 0$. Then, for sufficiently large H, there exist positive constants D_1 and D_2, which depend at most on c, c', and q, such that

$$\alpha^2 D_1(\log N)^{2c'}q^{n(1-2c)} < \lambda_N < \alpha^2 D_2(\log N)^{2c'}q^{n(1-2c)} \tag{4.12}$$

for all $N > H$.

Furthermore, we have

$$m^*_N \sim \frac{\alpha}{1-c}(\log N)^{c'}N^{(1-c)}. \tag{4.13}$$

Finally, if $c' = 0$, then with probability 1, the numbers b_j of the sequence $\omega = \{p_{b_j}\}$ satisfy

$$b_j \sim \left(\frac{1-c}{\alpha} j\right)^{1/(1-c)} \tag{4.14}$$

as $j \to \infty$.

Proof. We begin by finding a lower bound for λ_N. We assume $p \neq 2$. The case $p = 2$ can be treated in a similar manner. Suppose $N > q \cdot (j_0 + 1)$ from which it follows that $q^n > j_0$. Let C_0 and C_0' be the positive constants defined by

$$C_0 = \sum_{1 \leq j < j_0} \alpha_j,$$

and

$$C_0' = \sum_{1 \leq j < j_0} \frac{(\log j)^{c'}}{j^c}.$$

Since $q^n \leq \widetilde{a}_i < q^{n+1}$, $0 \leq a_i < q^{n+1}$, and $(\log x)^{c'}/x^c$ is a decreasing function, we obtain

$$\begin{aligned}
\lambda_N = \sum_{1 \leq i \leq M} \alpha_{a_i} \alpha_{\widetilde{a}_i} &> \frac{\alpha (\log q^{n+1})^{c'}}{q^{(n+1)c}} \sum_{1 \leq i \leq M} \alpha_{a_i} \\
&> \frac{\alpha^2 (\log q^{n+1})^{c'}}{q^{(n+1)c}} \left(\sum_{j=(q^{n+1}-1)/2}^{q^{n+1}-1} \frac{(\log j)^{c'}}{j^c} - C_0' \right) \\
&> \frac{\alpha^2 (\log q^{n})^{2c'}}{q^{(n+1)c}} \left(\sum_{j=(q^{n+1}-1)/2}^{q^{n+1}-1} \frac{1}{j^c} - C_0' \right).
\end{aligned}$$

We know that for all $s, s' \in \mathbb{N}$, $0 < s < s'$,

$$\frac{1}{1-c}(s'+1)^{1-c} - \frac{1}{1-c} s^{1-c} \leq \sum_{s \leq j \leq s'} \frac{1}{j^c} \leq \frac{1}{1-c}(s')^{1-c} - \frac{1}{1-c}(s-1)^{1-c}. \tag{4.15}$$

Thus, by (4.15) we can give the following lower bound for λ_N,

$$\begin{aligned} \lambda_N &> \frac{\alpha^2(\log q^n)^{2c'}}{q^{(n+1)c}} \left(\frac{1}{1-c}(q^{n+1})^{1-c} - \frac{1}{1-c}\left(\frac{q^{n+1}-1}{2}\right)^{1-c} - C_0' \right) \qquad (4.16) \\ &= \frac{\alpha^2(\log q^n)^{2c'}}{(1-c)q^c} q^{n(1-2c)} \left(q^{1-c} - \left(\frac{q}{2} - \frac{1}{2q^n}\right)^{1-c} - \frac{1-c}{q^{n(1-c)}} \cdot C_0' \right). \end{aligned}$$

Since $q^n \le N < q^{n+1}$, we have $\log N(1 - \log q/\log N) < \log q^n$. It follows from (4.16) that by taking H sufficiently large, we obtain

$$\lambda_N > \alpha^2 \frac{q^{1-2c}}{2(1-c)} \left(1 - \frac{1}{2^{1-c}}\right) (\log N)^{2c'} q^{n(1-2c)} \qquad (4.17)$$

for all $N > H$.

Now, we find an upper bound for λ_N. Again, since $q^n \le \widetilde{a}_i < q^{n+1}$ and $0 \le a_i < q^{n+1}$, by similar calculations as before we have

$$\lambda_N < \frac{\alpha(\log q^{n+1})^{c'}}{q^{nc}} \sum_{1 \le i \le M} \alpha_{a_i} < \frac{\alpha(\log q^{n+1})^{c'}}{q^{nc}} \left(C_0 + \alpha \sum_{j=1}^{M} \frac{(\log q^{n+1})^{c'}}{j^c} \right).$$

Thus, by applying (4.15), we obtain

$$\begin{aligned} \lambda_N &< \frac{\alpha^2(\log q^{n+1})^{2c'}}{q^{nc}} \left(\frac{C_0}{\alpha(\log q^{n+1})^{c'}} + \frac{1}{1-c}\left(\frac{q^{n+1}-1}{2}\right)^{1-c} \right) \\ &= \frac{\alpha^2(\log q^{n+1})^{2c'}}{(1-c)} q^{n(1-2c)} \left(\frac{C_0(1-c)}{\alpha(\log q^{n+1})^{c'} q^{n(1-c)}} + \left(\frac{q}{2} - \frac{1}{2q^n}\right)^{1-c} \right). \end{aligned}$$

Therefore, by taking H sufficiently large, we obtain that

$$\lambda_N < \alpha^2 \frac{2^{2c'+1}}{(1-c)} \left(\frac{q}{2}\right)^{1-c} (\log q^n)^{2c'} q^{n(1-2c)}$$

for all $N > H$. Then, since $q^n \le N < q^{n+1}$, we are done with the first part of the lemma.

Clearly, we have

$$m_N^* = \sum_{j=1}^{N} \alpha \frac{(\log j)^{c'}}{j^c} + \mathbf{O}(1) = \big(1 + \mathbf{o}(1)\big) \frac{\alpha}{1-c} (\log N)^{c'} N^{(1-c)},$$

and this proves (4.13). We note (4.13) shows that (4.3) and (4.4) are satisfied.

The final assertion of the lemma follows from (4.13), in view of Lemma 4.12, and the fact that $s_{b_j}^*(\omega) = j$ for $\omega = \{p_{b_j}\}_{j\in\mathbb{N}}$; for in this way it follows that, if $c' = 0$, we have with probability 1,

$$j = s_{b_j}^*(\omega) \sim m_{b_j}^* \sim \frac{\alpha}{1-c} b_j^{1-c},$$

or equivalently, $b_j \sim \big(\frac{1-c}{\alpha} j\big)^{1/(1-c)}$. □

We also make use of the following lemma.

Lemma 4.18 ([5], p. 149, Lem. 17)**.** *If* $0 < \xi \le U$, *then*

$$\sum_{d \ge U} \frac{\xi^d}{d!} \le \left(\frac{e\xi}{U}\right)^U,$$

and if $0 < V \le \xi$, *then*

$$\sum_{0 \le d \le V} \frac{\xi^d}{d!} \le \left(\frac{e\xi}{V}\right)^V.$$

4.5 Proof of Theorem 4.8

Let $c = c' = 1/2$. *We choose a number* $\alpha > 0$ *to satisfy*

$$\alpha^2 \frac{q^{1-2c}}{2(1-c)} \left(1 - \frac{1}{2^{1-c}}\right) > 1.$$

We then define a sequence $\{\alpha_j\}$ *by*

$$\alpha_j = \alpha \left(\frac{\log j}{j}\right)^{1/2} \tag{4.18}$$

for all $j \geq j_0$, where j_0 is a positive integer sufficient large such that the expression in (4.18) is less than $1/2$ for all $j \geq j_0$. For $1 \leq j < j_0$, we let $\alpha_j = 1/2$. The precise value of α_j for small j is unimportant, but the above choices ensure $0 < \alpha_j < 1$, so that Hypothesis A is satisfied. By (4.17) in the proof of Lemma 4.17, we have for all N sufficiently large that

$$\lambda_N \geq \alpha^2 D_1 \log N > \log N. \tag{4.19}$$

Hence, we know there exists $\delta > 0$ such that

$$e^{-\lambda_N} \ll N^{-1-\delta}. \tag{4.20}$$

We establish the theorem by showing that, with probability 1, $\log N \ll r_N(\omega) \ll \log N$ for large N, or equivalently (in view of Lemmas 4.16 and 4.17)

$$\lambda_N' \ll r_N(\omega) \ll \lambda_N' \tag{4.21}$$

for $N > N_0(\omega)$. We apply the Borel-Cantelli lemma twice to prove that each of the two assertions of (4.21) holds with probability 1. For this purpose, we must show that if C_1, C_2 are suitably chosen positive constants, then we have

$$\sum_{N=0}^{\infty} P(\{\omega \in \Omega \colon r_N(\omega) > C_1 \lambda_N'\}) < \infty \tag{4.22}$$

and

$$\sum_{N=0}^{\infty} P(\{\omega \in \Omega \colon r_N(\omega) < C_2 \lambda_N'\}) < \infty. \tag{4.23}$$

By Lemmas 4.15 and 4.18, we have

$$\begin{aligned} P(\{\omega \in \Omega \colon r_N(\omega) > C_1 \lambda_N'\}) &\leq e^{-\lambda_N} \sum_{d \geq C_1 \lambda_N'} \frac{(\lambda_N')^d}{d!} \\ &\leq e^{-\lambda_N} \left(\frac{e}{C_1}\right)^{C_1 \lambda_N'}, \end{aligned}$$

provided $C_1 \geq 1$. Thus, by choosing $C_1 = e$, we obtain a bound $e^{-\lambda_N}$ for the summand of (4.22), and the inequality (4.22) follows from (4.20).

On the other hand, again by Lemmas 4.15 and 4.18, we obtain the following estimate *for the summand of (4.23),*

$$P(\{\omega \in \Omega \colon r_N(\omega) < C_2\lambda'_N\}) \leq e^{-\lambda_N} \sum_{0 \leq d \leq C_2\lambda'_N} \frac{(\lambda'_N)^d}{d!}$$
$$\leq e^{-\lambda_N} \left(\frac{e}{C_2}\right)^{C_2\lambda'_N},$$

provided $C_2 \leq 1$. Thus, it suffices to show that C_2 can be chosen to satisfy, in addition to $0 < C_2 \leq 1$,

$$\left(\frac{e}{C_2}\right)^{C_2\lambda'_N} \ll N^{\delta/2};$$

for (4.23) will then follow from (4.20). By Lemmas 4.16 and 4.17, we know there exists $D > 0$ such that $\lambda'_N \leq D \log N$ for N sufficiently large. Therefore, we only need to choose a small positive constant C_2 satisfying

$$\left(\frac{e}{C_2}\right)^{C_2} \leq e^{\delta/(2D)},$$

which is certainly possible since $(\mathrm{e}/\mathrm{t})^t \to 1$ as $t \to 0$ from the positive side.

We have now shown that ω has each of the desired properties with probability 1, and this proves the theorem.

□

4.6 Proof of Theorem 4.9

Let $\epsilon > 0$ be given. We define a sequence $\{\alpha_j\}$ by $\alpha_0 = 1/2$ and

$$\alpha_j = \frac{1}{2\ j^{1-1/(2+\epsilon)}}$$

for $j \geq 1$. It then follows by Lemma 4.17 (with $\alpha = 1/2$, $c = 1 - 1/(2+\epsilon)$, and $c' = 0$) that, with probability 1, $\omega = \{p_{b_j}\}$ satisfies $b_j \sim c^* j^{2+\epsilon}$, where c^* is some positive constant.

Since the sequence $\{\alpha_j\}$ satisfies Hypothesis A, we have $\lambda'_N \sim \lambda_N$ by Lemma 4.16.

Thus, by Lemma 4.17 we know that there exist positive constants D_1 and D_2 such that

$$D_1 q^{-\epsilon n/(2+\epsilon)} < \lambda_N, \lambda'_N < D_2 q^{-\epsilon n/(2+\epsilon)} \tag{4.24}$$

for N sufficiently large.

We again appeal to the Borel-Cantelli Lemma. It follows from this lemma that if a positive number K satisfies the property

$$\sum_{N=0}^{\infty} P(\{\omega \in \Omega\colon r_N(\omega) \geq K\}) < \infty, \tag{4.25}$$

then, with probability 1, we have

$$r_N(\omega) < K$$

for $N > N_0(\omega)$.

We note that, by (4.24), $\lambda_N \to 0$ and $\lambda'_N \to 0$ as $N \to \infty$. Thus, by Lemmas 4.15 and 4.18, we obtain the following estimate for the summand of (4.25),

$$P(\{\omega \in \Omega\colon r_N(\omega) \geq K\}) \leq e^{-\lambda_N} \sum_{d \geq K} \frac{(\lambda'_N)^d}{d!} \leq e^{-\lambda_N} \left(\frac{e\lambda'_N}{K}\right)^K \ll (\lambda'_N)^K$$

for N sufficiently large. Since $q^n \leq N < q^{n+1}$, we have

$$(\lambda'_N)^K \leq D_2^K q^{-\epsilon n K/(2+\epsilon)} \ll N^{-\epsilon K/(2+\epsilon)}.$$

Therefore, provided $\epsilon K/(2+\epsilon) > 1$, or equivalently,

$$K > 1 + 2\epsilon^{-1},$$

it is clear that (4.25) is achieved. Accordingly we have, with probability 1,

$$r_N(\omega) < 2(1 + \epsilon^{-1})$$

for $N > N_1(\epsilon, \omega)$. This completes the proof of the theorem.

□

4.7 Proof of Theorem 4.10

Recall we defined $\widetilde{t}_N(\omega)$ *to be*

$$\widetilde{t}_N(\omega) = |\{(a,b) \in \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0} \colon p_a, p_b \in \omega,\ p_N = p_a - p_b,\ \deg p_a, \deg p_b \leq \deg p_N\}|.$$

As before given $p_N \in \mathbb{F}_q[t]$*, we let* $n := n(N) = \deg p_N = \lfloor \log_q N \rfloor$*. It is clear that for* $p_N \neq 0$*, there exist* q^{n+1} *pairs of polynomials* (p_a, p_b) *such that* $p_N = p_a - p_b$ *and* $\deg p_a$, $\deg p_b \leq n$*. Also, every polynomial of degree less than or equal to* n *will appear as* p_a *and* p_b *exactly once. Let* $S_{\widehat{u},n}$ *denote the set of all polynomials in* $\mathbb{F}_q[t]$ *whose degree are less than or equal to* n*, and the coefficient of* t^n *is* $\widehat{u} \in \mathbb{F}_q$*. Clearly, we have* $|S_{\widehat{u},n}| = q^n$*. If we consider each polynomial in* $S_{\widehat{u},n}$ *as* p_b*, then the corresponding set of* p_a*'s is* $S_{u,n}$ *for some* $u \neq \widehat{u}$ *as* $\deg p_N = n$*.*

For each $u \in \mathbb{F}_q$*, we consider*

$$\widetilde{t}_{N,u}(\omega) = |\{(a,b) \in \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0} \colon p_N = p_a - p_b,\ \textit{where } p_a, p_b \in \omega \textit{ and } p_a \in S_{u,n}\}|.$$

If $p_N = p_a - p_b$*, we relabel* p_b *as* $p_{\widehat{a}}$ *to make its correspondence with* p_a *more explicit. We form the following two disjoint sets*

$$\mathcal{A}_N = \{a \in \mathbb{Z}_{\geq 0} \colon p_a \in S_{u,n}\} = \{\iota^{-1}(u)q^n, ..., (\iota^{-1}(u)+1)q^n - 1\}$$

and

$$\widehat{\mathcal{A}}_N = \{\widehat{a} \in \mathbb{Z}_{\geq 0} \colon p_{\widehat{a}} \in S_{\widehat{u},n}\} = \{\iota^{-1}(\widehat{u})q^n, ..., (\iota^{-1}(\widehat{u})+1)q^n - 1\}.$$

Let $M_0 := M_0(N) = |\mathcal{A}_N| = |\widehat{\mathcal{A}}_N| = q^n$*. For convenience, we label the* M_0 *elements of* $\mathcal{A}_N$ *by* a_i $(1 \leq i \leq M_0)$*, and the corresponding elements of* $\widehat{\mathcal{A}}_N$ *by* $\widehat{a}_i$*, in other words we have* $p_N = p_{a_i} - p_{\widehat{a}_i}$ $(1 \leq i \leq M_0)$*.*

We also define $\lambda_{N,u}$ *and* $\lambda'_{N,u}$ *to be*

$$\lambda_{N,u} = \sum_{1 \leq i \leq M_0} \alpha_{a_i}\alpha_{\widehat{a}_i},$$

and

$$\lambda'_{N,u} = \sum_{1 \leq i \leq M_0} \frac{\alpha_{a_i}\alpha_{\widehat{a}_i}}{1 - \alpha_{a_i}\alpha_{\widehat{a}_i}}.$$

With this set up we can recover analogues of all the previous lemmas in terms of M_0*,* $\lambda_{N,u}$*,* $\lambda'_{N,u}$*, and* $\widetilde{t}_{N,u}(\omega)$*, in place of* M*,* λ_N*,* λ'_N*, and* $r_N(\omega)$*, respectively. Therefore, by a similar* *argument we obtain Theorem 4.9 with* $\widetilde{t}_{N,u}(\omega)$ *in place of* $r_N(\omega)$*. Since this result holds with probability* 1*, and*

$$\widetilde{t}_N(\omega) = \sum_{u \in \mathbb{F}_q} \widetilde{t}_{N,u}(\omega),$$

we have our result.

□

References

[1] *V. Bergelson, A. Leibman, and E. Lesigne, Interesective polynomials and the polynomial Szemerédi theorem, Adv. Math. 219 (2008), no. 1, 369-388.*

[2] *H. Davenport, On a theorem of Heilbronn, Quart. J. Math. Oxford Ser. (2)* ***18*** *(1967), 399 - 344.*

[3] *P. Erdős, On a problem of Sidon in additive number thoery, Acta Sci. Math. Szeged 15 (1954), pp255–259.*

[4] *P. Erdős and A. Rényi, Additive properties of random sequences of positive integers, Acta Arith. 6 (1960), 83–110.*

[5] *H. Halberstam and K.F. Roth, Sequences, Springer-Verlag, New York, 1983.*

[6] *G. H. Hardy and J. E. Littlwood, Some problems of diophantine approximation Part I. The frational part of $n^k\theta$, Acta Math. 37 (1914), no. 1, 155-191.*

[7] *K. E. Hare and S. Yamagishi, A generalization of a theorem of Erdős-Rényi to m-fold sums and differences, to appear in Acta Arithmetica.*

[8] *H. Heilbronn, On the distribution of the sequence $n^2\theta$ (mod 1), Quart. J. Math. Oxford Ser.* ***19*** *(1948), 249 - 256.*

[9] *C.-N. Hsu, A large sieve inequality for rational function fields, J. Number Th.* ***58****(1996), 267-287.*

[10] *W. Kuo, Y.-R. Liu and X. Zhao, Multidimensional Vinogrado-type estimates in function fields, Canad. J. Math. Vol.****66****(4), 2014, 844-873.*

[11] *T.H. Lê, Problems and results on intersective sets, to appear in Proceedings of Combinatorial and Additive Number Theory 2011.*

[12] T.H. Lê and Y.-R. Liu, Equidistribution of polynomial sequences in function fields, with applications, arXiv:1311.0892.

[13] T.H. Lê and C. V. Spencer, Intersective polynomials and diophantine approximation, Internat. Math. Res. Notices (2014), no.5, 1153-1173.

[14] S.-L. A. Lee, Birch's theorem in function fields, arXiv:1109.4953.

[15] Y.-R. Liu and T. D. Wooley, Waring's problem in function fields, J. Reine Angew. Math. ***638*** *(2010), 1 - 67.*

[16] Y.-R. Liu and T. D. Wooley, Efficient congruencing in function fields, in preparation.

[17] J.Lucier, Interesective sets given by a polynomial, Acta Arith. 123 (2006), 57-95.

[18] J. Neukirch, Algebraic number theory. Translated from the 1992 German original and with a note by Norbert Schappacher. With a foreword by G. Harder, Grundlehren der Mathematischen Wissenschaften (Fundamental Principles of Mathematical Sciences), 322. Springer-Verlag, Berlin, 1999. xviii+571 pp.

[19] R. M. Kubota, Waring's problem for $\mathbb{F}_q[x]$*, Dissert. Math. (Rozprawy Mat.)* ***117****(1974), 60pp.*

[20] I. M. Vinogradov, Analytischer Beweis des Satzes über die Verteilung der Bruchteile eines ganzen Polynoms, Bull. Acad. Sci. USSR (6) 21 (1927), 567-578.

[21] R. C. Vaughan, The Hardy-Littlewood Method, 2nd ed. Cambridge: Cambridge University Press, 1997.

[22] T. D. Wooley, Large improvements in Waring's problm, Ann. of Math. ***135****(1992), 131 - 164.*

*[23] T. D. Wooley, New estimates for smooth Weyl sums, J. London Math. Soc. (2)****51****(1995), 1 - 13.*

[24] T. D. Wooley, Vinogradov's mean value theorem via efficient congruencing, Ann. of Math. ***175****(2012), no. 3, 1575 - 1627.*

[25] T. D. Wooley, The asymptotic formula in Waring's Problem, Internat. Math. Res. Notices (2012), no.7, 1485-1504.

[26] T. D. Wooley, Vinogradov's mean value theorem via efficient congruencing, II, Duke Math. J. ***162****(2013), no. 4, 673 - 730.*

[27] *A. Zaharescu, Small values of* $n^2\alpha$ *(mod* 1*), Invent. Math.* ***121*** *(1995), no. 2, 379 - 388.*

[28] *X. Zhao, Asymptotic estimates for rational spaces on hypersurface in function fields, Proc. London Math. Soc.(3)* ***104*** *(2012), 287-322.*