Asymptotic Estimates for Rational Spaces on Hypersurfaces in Function Fields

by

Xiaomei Zhao

A thesis

presented to the University of Waterloo

in fulfilment of the

thesis requirement for the degree of

Doctor of Philosophy

in

Pure Mathematics

Waterloo, Ontario, Canada, 2010

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

The ring of polynomials over a finite field has many arithmetic properties similar to those of the ring of rational integers. In this thesis, we apply the Hardy-Littlewood circle method to investigate the density of rational points on certain algebraic varieties in function fields. The aim is to establish asymptotic relations that are relatively robust to changes in the characteristic of the base finite field. More notably, in the case when the characteristic is "small", the results are sharper than their integer analogues.

Acknowledgments

First of all, I would like to thank my supervisor, Yu-Ru Liu. This work would not have been possible without her guidance, advice, and encouragement. I also appreciate her generous financial support for me to attend conferences.

I am grateful to Cameron Stewart, David McKinnon, Kumar Murty, and Alfred Menezes for serving on my committee. I thank Shonn Martin for her help and advice on the thesis submission. I also wish to thank Kathryn Hare and Che Tat Ng for their kind support.

I also want to acknowledge the important roles of Cameron Stewart and Michael Rubinstein in my number theory education at Waterloo. I have benefited from several advanced courses taught by them. In particular, Cameron's lectures on p-adic analysis play a significant role in my thesis.

I am thankful to Craig Spencer and Dilian Yang for sharing with me their research experience.

Finally, I heartily thank my parents for having never lost faith in me.

Contents

Chapter 1

Introduction

1.1 Motivation

The problem concerning integral points lying on the hypersurface defined by an additive equation has occupied a prominent position in number theory over the past century. Let $\mathbb{Z}$ be the ring of integers and let $\mathbb{N} = \{0, 1, 2, \ldots\}$. For nonzero $k \in \mathbb{N}$ and nonzero $a_1, \ldots, a_s \in \mathbb{Z}$, one wishes to establish an asymptotic estimate for the density of integral points lying on the hypersurface

$$a_1 w_1^k + \cdots + a_s w_s^k = 0. \tag{1.1}$$

For positive $P \in \mathbb{R}$, the set of real numbers, let $M_{s,k}(P)$ denote the number of integral solutions of (1.1) in the box $[-P, P]^s$. When k is sufficiently large, subject to a local solubility hypothesis, the work of Wooley [21] on Waring's problem can be used to show that $M_{s,k}(P) \gg P^{s-k}$ whenever $s \geq k \log k + O(k \log \log k)$. Moreover, by the work of Ford in [6], we may prove that there are two positive constants $D_1 = D_1(s, k; a_1, \ldots, a_s)$ and $\mu_1 = \mu_1(k)$ such that

$$M_{s,k}(P) = D_1 P^{s-k} + O(P^{s-k-\mu_1}),$$

whenever $s \geq k^2 \log k + O(k^2 \log \log k)$.

Because of the homogeneity of (1.1), if a nonzero integral point $\mathbf{w} = (w_1, \ldots, w_s)$ lies on (1.1), then the rational line determined by this point $\{b\mathbf{w} \,|\, b \in \mathbb{Q}\}$ is also contained in

(1.1). Thus the above question is about the density of linear spaces of dimension 1. It is therefore natural to ask about linear spaces of higher dimension. Asymptotic estimates for the number of such spaces up to a given height have been considered in recent work of Parsell (see [13], [14], [15], and [16]). Let V be a rational linear space of dimension d when $d \in \mathbb{N}$ and $d \geq 2$. Suppose that $\mathbf{u}_1, \dots, \mathbf{u}_d \in \mathbb{Z}^s$ form a basis of V. Then

$$V = \mathrm{Span}\{\mathbf{u}_1, \dots, \mathbf{u}_d\} = \big\{ b_1\mathbf{u}_1 + \cdots + b_d\mathbf{u}_d \,\big|\, b_1, \dots, b_d \in \mathbb{Q} \big\}.$$

V is contained in the hypersurface defined by (1.1) if and only if every vector $\mathbf{v} = (v_1, \dots, v_s) \in V$ is a solution of (1.1). Write $\mathbf{v} = b_1\mathbf{u}_1 + \cdots + b_d\mathbf{u}_d$. Thus,

$$v_j = b_1u_{1,j} + \cdots + b_du_{d,j} \ (1 \leq j \leq s).$$

Note that $\mathbf{v} = (v_1, \dots, v_s)$ is a solution of (1.1) if and only if

$$a_1v_1^k + \cdots + a_sv_s^k = 0,$$

i.e.,

$$a_1(b_1u_{1,1} + \cdots + b_du_{d,1})^k + \cdots + a_s(b_1u_{1,s} + \cdots + b_du_{d,s})^k = 0.$$

Using the multinomial theorem, for each j with $1 \leq j \leq s$, we have

$$(b_1u_{1,j} + \cdots + b_du_{d,j})^k = \sum_{i_1+\cdots+i_d=k} \frac{k!}{i_1! \cdots i_d!} b_1^{i_1} \cdots b_d^{i_d} u_{1,j}^{i_1} \cdots u_{d,j}^{i_d}.$$

On collecting the coefficients of $b_1^{i_1} \cdots b_d^{i_d}$ for each d-tuple $(i_1, \dots, i_d)$ with $i_1 + \cdots + i_d = k$, we have

$$\sum_{i_1+\cdots+i_d=k} \frac{k!}{i_1! \cdots i_d!} \big(a_1u_{11}^{i_1} \cdots u_{d1}^{i_d} + \cdots + a_su_{1s}^{i_1} \cdots u_{ds}^{i_d}\big) b_1^{i_1} \cdots b_d^{i_d} = 0.$$

Certainly, the above equation is true for every d-tuple $(b_1, \dots, b_d) \in \mathbb{Q}^d$ if and only if $\mathbf{u}_1, \dots, \mathbf{u}_d$ satisfy the following system

$$a_1u_{11}^{i_1} \cdots u_{d1}^{i_d} + \cdots + a_su_{1s}^{i_1} \cdots u_{ds}^{i_d} = 0 \quad (i_1 + \cdots + i_d = k). \tag{1.2}$$

The number of equations of the system (1.2) is given by

$$n_1 = \begin{pmatrix} k+d-1 \\ k \end{pmatrix}.$$

Let $M_{s,k,d}(P)$ denote the number of solutions of the system (1.2) with $u_{i,j} \in [-P, P] \cap \mathbb{Z}$ $(1 \le i \le d,\ 1 \le j \le s)$. In [15], Parsell applied the Hardy-Littlewood circle method to estimate $M_{s,k,d}(P)$. In particular, he proved a generalization of Vinogradov's mean value theorem, which concerns the number of solutions of an auxiliary symmetric system

$$u_{11}^{i_1} \cdots u_{d1}^{i_d} + \cdots + u_{1s}^{i_1} \cdots u_{ds}^{i_d} = v_{11}^{i_1} \cdots v_{d1}^{i_d} + \cdots + v_{1s}^{i_1} \cdots v_{ds}^{i_d} \quad (1 \le |\mathbf{i}| \le k), \tag{1.3}$$

where $|\mathbf{i}| = i_1 + \cdots + i_d$. The number of equations of the above system is

$$n_2 = \left(\begin{array}{c} k+d \\ k \end{array} \right) - 1.$$

The result in [15, Theorem 1.4] states that when k is sufficiently large in terms of d, subject to a local solubility hypothesis, there are two positive constants $D_2 = D_2(s, k, d; a_1, \ldots, a_s)$ and $\mu_2 = \mu_2(k, d)$ such that

$$M_{s,k,d}(P) = D_2 P^{sd - n_1 k} + O\big(P^{sd - n_1 k - \mu_2}\big),$$

whenever

$$s \ge 2n_2 k\big((2/3)\log n_2 + (1/2)\log k\big) + O\big(n_2 k \log\log k\big). \tag{1.4}$$

Let $\mathbb{F}_q[t]$ be the ring of polynomials over the finite field $\mathbb{F}_q$ of q elements whose characteristic is p. Because of the remarkable analogy between $\mathbb{Z}$ and $\mathbb{F}_q[t]$, we can consider a polynomial analogue of the above question. Let $k \in \mathbb{N}$ with $p \nmid k$. For fixed coefficients $c_1, \ldots, c_s \in \mathbb{F}_q[t] \setminus \{0\}$, we consider the hypersurface defined by

$$c_1 z_1^k + \cdots + c_s z_s^k = 0. \tag{1.5}$$

For $P \in \mathbb{R}$ with $P > 0$, let $N_{s,k}(P)$ denote the number of solutions of (1.5) in $\mathbb{F}_q[t]^s$ with $\deg z_j < P$ $(1 \le j \le s)$. When k is sufficiently large, subject to a local solubility assumption, Liu and Wooley [11] proved that $N_{s,k}(P) \gg \big(q^P\big)^{s-k}$ whenever $s \ge k \log k + O(k \log\log k)$. They [12] also proved that there are two positive constants $D_3 = D_3(s, k; q; c_1, \ldots, c_s)$ and $\mu_3 = \mu_3(k, q)$ such that

$$N_{s,k}(P) = D_3\big(q^P\big)^{s-k} + O\big(\big(q^P\big)^{s-k-\mu_3}\big)$$

whenever $s \ge 2n_3 k \log(n_3 k) + O\big(n_3 k \log(n_3 k)\big)$, where $1 \le n_3 = n_3(k) \le k$.

In this thesis, we extend the result in [12] to higher dimensions. For $d \in \mathbb{N}$ with $d \geq 2$, let $\mathbf{x}_1, \ldots, \mathbf{x}_d \in \mathbb{F}_q[t]^s$ be linearly independent vectors and define

$$\mathrm{Span}\{\mathbf{x}_1, \ldots, \mathbf{x}_d\} = \big\{ \mathfrak{f}_1\mathbf{x}_1 + \cdots + \mathfrak{f}_d\mathbf{x}_d \,\big|\, \mathfrak{f}_1, \ldots, \mathfrak{f}_d \in \mathbb{F}_q(t) \big\}.$$

The hypersurface (1.5) contains this space if and only if

$$c_1(\mathfrak{f}_1 x_{1,1} + \cdots + \mathfrak{f}_d x_{d,1})^k + \cdots + c_s(\mathfrak{f}_1 x_{1,s} + \cdots + \mathfrak{f}_d x_{d,s})^k = 0.$$

Using the multinomial theorem, for each j, we have

$$(\mathfrak{f}_1 x_{1,j} + \cdots + \mathfrak{f}_d x_{d,j})^k = \sum_{i_1+\cdots+i_d=k} \frac{k!}{i_1! \cdots i_d!} (\mathfrak{f}_1)^{i_1} \cdots (\mathfrak{f}_d)^{i_d} x_{1,j}^{i_1} \cdots x_{d,j}^{i_d}.$$

This equation is true for every d-tuple $(\mathfrak{f}_1, \ldots, \mathfrak{f}_d) \in \mathbb{F}_q(t)$ if and only if $\mathbf{x}_1, \ldots, \mathbf{x}_d$ satisfy simultaneously the following equations

$$\frac{k!}{i_1! \cdots i_d!} \Big(c_1 x_{11}^{i_1} \cdots x_{d1}^{i_d} + \cdots + c_s x_{1s}^{i_1} \cdots x_{ds}^{i_d} \Big) = 0 \;\; (i_1 + \cdots + i_d = k).$$

Since $\mathrm{char}\, \mathbb{F}_q = p$, the above system is equivalent to the following system

$$c_1 x_{11}^{i_1} \cdots x_{d1}^{i_d} + \cdots + c_s x_{1s}^{i_1} \cdots x_{ds}^{i_d} = 0 \;\; \Big((i_1, \ldots, i_d) \in \mathcal{L} \Big). \tag{1.6}$$

where the set $\mathcal{L}$ is defined by

$$\mathcal{L} = \left\{ (i_1, \ldots, i_d) \in \mathbb{N}^d \,\middle|\, i_1 + \cdots + i_d = k \;\text{ and } p \nmid \frac{k!}{i_1! \cdots i_d!} \right\}.$$

The cardinality of the set $\mathcal{L}$ can be calculated explicitly as follows. For every $i \in \mathbb{N}$, it can be represented uniquely as

$$i = \sum_{h=0}^{\infty} a_h(i) p^h$$

where $a_h(i) \in [0, p-1] \cap \mathbb{Z}$ $(h \in \mathbb{N})$. Write

$$k = a_0(k) + a_1(k)p + \cdots + a_D(k)p^D.$$

From Lemma 61, we have

$$\mathrm{card}\, \mathcal{L} = \prod_{h=0}^{D} \begin{pmatrix} a_h(k) + d - 1 \\ a_h(k) \end{pmatrix}.$$

For a positive number P, let $N_{s,k,d,\mathbf{c}}(P) = N_{s,k,d}(P)$ denote the number of the solutions of the system (1.6) with $x_{ij} \in \mathbb{F}_q[t]$ and $\deg x_{ij} < P$ $(1 \le i \le d,\ 1 \le j \le s)$. We shall frequently abbreviate a monomial of the shape $x_1^{i_1} \cdots x_d^{i_d}$ by $\mathbf{x}^{\mathbf{i}}$. Also, for $\mathbf{i} = (i_1, \dots, i_d) \in \mathbb{N}^d$, we write $p \nmid \mathbf{i}$ if $p \nmid i_l$ for some l with $1 \le l \le d$. Motivated by Parsell's work in [15], to estimate $N_{s,k,d}(P)$, we consider a generalization of Vinogradov-type mean value theorem. More precisely, we need to investigate the number of solutions of the system

$$\mathbf{x}_1^{\mathbf{i}} + \cdots + \mathbf{x}_s^{\mathbf{i}} = \mathbf{y}_1^{\mathbf{i}} + \cdots + \mathbf{y}_s^{\mathbf{i}} \quad (\mathbf{i} \in \mathcal{R}_0') \tag{1.7}$$

where $\mathcal{R}_0'$ is a set of certain d-tuples satisfying

$$\mathcal{L} \subseteq \mathcal{R}_0' \subseteq \{\mathbf{i} \in \mathbb{N}^d \,|\, 1 \le |\mathbf{i}| \le k,\ p \nmid \mathbf{i}\}. \tag{1.8}$$

When $k < p$, let $\mathcal{R}_0' = \{\mathbf{i} \in \mathbb{N}^d \,|\, 1 \le |\mathbf{i}| \le k\}$. Thus the system (1.7) has the same shape as the system (1.3). By applying the Linnik-Karatsuba method and the repeated efficient differencing process, we may obtain results that are of the same strength as the integer analogue considered in [15]. The case when $k > p$ is much more complicated. Since

$$x_{11}^p \cdots x_{d1}^p + \cdots + x_{1s}^p \cdots x_{ds}^p = \big(x_{11} \cdots x_{d1} + \cdots + x_{1s} \cdots x_{ds}\big)^p,$$

the second containment in (1.8) is necessary in order to guarantee that the equations of the system (1.7) are independent. However, one difficulty occurs as the Linnik-Karatsuba method used in the integer case is ineffective for the system (1.7). To surmount this barrier, we choose

$$\mathcal{R}_0' = \{\mathbf{i} \in \mathcal{R}_0 \,|\, p \nmid \mathbf{i}\},$$

where

$$\mathcal{R}_0 = \big\{\mathbf{i} \in \mathbb{N}^d \,|\, \exists l \in \mathbb{N} \text{ s.t. } a_l(k) \ge 1 \text{ and } |a_h(\mathbf{i})| \le a_{h+l}(k)\ (h \in \mathbb{N})\big\}.$$

It transpires that the system (1.7) is equivalent to the following augmented system

$$\mathbf{x}_1^{\mathbf{i}} + \cdots + \mathbf{x}_s^{\mathbf{i}} = \mathbf{y}_1^{\mathbf{i}} + \cdots + \mathbf{y}_s^{\mathbf{i}} \quad (\mathbf{i} \in \mathcal{R}_0). \tag{1.9}$$

Furthermore, the Linnik-Karatsuba method is applicable to the system (1.9). Indeed, the conclusion on the system (1.9) mirrors an expected Vinogradov-type result for the system (1.7). From Lemma 69, we have

$$\nu \le \operatorname{card} \mathcal{R}_0' < \nu\Big(1 + \frac{1+d}{d^2}\Big),$$

where

$$\nu = \left(\begin{pmatrix} a_0(k)+d \\ d \end{pmatrix} - 1 \right) \prod_{h=1}^{D} \begin{pmatrix} a_h(k)+d \\ d \end{pmatrix}.$$

Under a similar solubility condition as in [15], we employ a variant of the Hardy-Littlewood circle method to prove the following theorem.

Theorem 1. *Let p be the characteristic of $\mathbb{F}_q$. Suppose that $p \nmid k$ and $k \geq d+2$. Further suppose that the system* (1.6) *has a non-singular solution in the completion of $\mathbb{F}_q(t)$ at ∞ and a non-singular solution in the completion $\mathbb{F}_q(t)_w$ of $\mathbb{F}_q(t)$ at every irreducible element w in $\mathbb{F}_q[t]$. Let $\iota = \operatorname{card} \mathcal{L}$ and $r = \operatorname{card} \mathcal{R}_0'$. Whenever*

$$s \geq 2rk\Big(\log(\iota rk) + \log\big(\log\big((2\iota-1)rk\log k\big) + 2k^{-1}\big) + 3 + \log 4 - \log\big(1-(\log k)^{-1}\big)\Big),$$

there is a positive constant $C = C(s,k,d;q;c_1,\dots,c_s)$ such that

$$N_{s,k,d,\mathbf{c}}(P) = C\big(q^P\big)^{sd-\iota k} + O\Big(\big(q^P\big)^{sd-\iota k-\delta}\Big),$$

where

$$\delta = \min\left\{ \frac{1}{18k\iota}, \frac{1-(\log k)^{-1}}{4\iota rk(\log((2\iota-1)rk\log k) + 2k^{-1})} \right\},$$

and the implicit constant depends on s,k,d,q and $c_1,\dots,c_s$.

Let $v_{q,d}(k)$ denote the least positive integer s for which the above asymptotic formula holds. It is remarkable that when k satisfies certain properties, both ι and r only depend on d. For example, when $k = 1+p^D$ ($D \in \mathbb{N}\setminus\{0\}$), we may find that $\iota = d^2$ and $r = d(d+1)$. Thus $v_{q,d}(k) = O_{q,d}(k\log k)$, which is sharper than its integer analogue expressed in (1.4).

Furthermore, Theorem 1 establishes the existence of many rational linear spaces of dimension d on the hypersurface (1.1), provided that the conditions in Theorem 1 are satisfied. We define the height of a vector $\mathbf{x} = (x_1,\dots,x_n) \in \mathbb{F}_q[t]^n$ to be

$$H(\mathbf{x}) = \frac{\max_{1\leq i\leq n}\langle x_i\rangle}{\langle \gcd(x_1,\dots,x_n)\rangle},$$

where for $x \in \mathbb{F}_q[t]$, $\langle x\rangle = q^{\deg x}$. Now for a subspace $V \subseteq \mathbb{F}_q(t)^s$ with basis vectors $\mathbf{x}_1,\dots,\mathbf{x}_d \in \mathbb{F}_q[t]^s$, we write

$$H(V) = H(\mathbf{x}_1 \wedge \cdots \wedge \mathbf{x}_d).$$

If $\mathbf{y}_1, \dots, \mathbf{y}_d \in \mathbb{F}_q[t]^s$ is another basis for V, then we have $Y = XB$, where X and Y denote the $s \times d$ matrices corresponding to each basis and where B is an invertible $d \times d$ change-of-basis matrix. Since

$$\mathbf{y}_1 \wedge \cdots \wedge \mathbf{y}_d = (\det B)\mathbf{x}_1 \wedge \cdots \wedge \mathbf{x}_d,$$

we see that the definition of $H(V)$ does not depend on the basis. Let $\mathcal{N}_{s,k,d}(P)$ denote the number of distinct linear spaces V of dimension d and height at most q^P, lying on the hypersurface (1.5). We may deduce from Theorem 1 that

Theorem 2. *Under the same conditions as the ones in Theorem 1, there are two positive constants $C_1 = C_1(s, k, d; q; c_1, \dots, c_s) > 0$ and $C_2 = C_2(s, k, d; q; c_1, \dots, c_s) > 0$ such that*

$$\mathcal{N}_{s,k,d}(P) \geq C_1\big(q^P\big)^{s-\frac{k\iota}{d}-d} - C_2\big(q^P\big)^{s-\frac{k\iota}{d}-d-\frac{\delta}{d}},$$

where δ is defined as in Theorem 1.

1.2 The circle method for polynomial rings

Let $\mathbb{A} = \mathbb{F}_q[t]$ be the ring of polynomials over the finite field $\mathbb{F}_q$. Let p be the characteristic of $\mathbb{F}_q$. In what follows, write $\mathbb{K}_\infty = \mathbb{F}_q((1/t))$ for the completion of $\mathbb{F}_q(t)$ at ∞. We may write each element $\alpha \in \mathbb{K}_\infty$ in the shape $\alpha = \sum_{i \leq n} a_i t^i$ for some $n \in \mathbb{Z}$ and coefficients $a_i = a_i(\alpha) \in \mathbb{F}_q$ $(i \leq n)$. We define $\operatorname{ord}\alpha$ to be the largest integer i for which $a_i(\alpha) \neq 0$ and write $\langle\alpha\rangle = q^{\operatorname{ord}\alpha}$. In this context, we adopt the convention that $\operatorname{ord} 0 = -\infty$ and $\langle 0\rangle = 0$. Let $\mathbb{T} = \{\alpha \in \mathbb{K}_\infty | \langle\alpha\rangle < 1\}$. We may normalize any Haar measure $d\alpha$ on $\mathbb{K}_\infty$ in such a manner that $\int_{\mathbb{T}} 1 d\alpha = 1$.

Let $\operatorname{tr} : \mathbb{F}_q \to \mathbb{F}_p$ denote the familiar trace map. Also let $e_q : \mathbb{F}_q \to \mathbb{C}^\times$ be a non-trivial additive character defined for each $a \in \mathbb{F}_q$ by taking $e_q(a) = e\big(\operatorname{tr}(a)/p\big)$, where we write $e(z)$ for $e^{2\pi i z}$.

We are now in a position to define an analogue of the exponential function. For $\alpha = \sum_{i \leq n} a_i t^i \in \mathbb{K}_\infty$, define $\operatorname{res}\alpha = a_{-1}$. The exponential function $e : \mathbb{K}_\infty \to \mathbb{C}^\times$ is induced by defining, for each element $\alpha \in \mathbb{K}_\infty$, the value of $e(\alpha)$ to be $e_q\big(\operatorname{res}\alpha\big)$. Then we

have the following orthogonality relation [10, Lemma 1],

$$\int_{\mathbb{T}} e(x\alpha)\, d\alpha = \begin{cases} 1, & \text{when } x = 0, \\ 0, & \text{when } x \in \mathbb{F}_q[t] \setminus \{0\}. \end{cases}$$

Therefore, for $n \in \mathbb{N} \setminus \{0\}$, $(x_1, \cdots, x_n) \in \mathbb{F}_q[t]^n$, and $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_n) \in \mathbb{K}_\infty^n$, we have

$$\begin{aligned} \int_{\mathbb{T}^n} e(x_1\alpha_1 + \cdots + x_n\alpha_n)\, d\boldsymbol{\alpha} &= \prod_{i=1}^{n} \int_{\mathbb{T}} e(x_i\alpha_i)\, d\alpha_i \\ &= \begin{cases} 1, & \text{when } x_i = 0\,(1 \le i \le n), \\ 0, & \text{otherwise.} \end{cases} \end{aligned} \tag{1.10}$$

For $P \in \mathbb{R}$, let $\hat{P} = q^P$ and $I_P = \{x \in \mathbb{A} \,|\, \langle x \rangle < \hat{P}\}$. For $\boldsymbol{\alpha} = (\alpha_{\mathbf{i}})_{\mathbf{i} \in \mathcal{L}} \in \mathbb{K}_\infty^\iota$ and $P \in \mathbb{R}$ with $P > 0$, define

$$f_j(\boldsymbol{\alpha}) = f_j(\boldsymbol{\alpha}; P) = \sum_{\mathbf{x} \in I_P^d} e\Big(\sum_{\mathbf{i} \in \mathcal{L}} c_j \alpha_{\mathbf{i}} \mathbf{x}^{\mathbf{i}} \Big) \quad (1 \le j \le s).$$

By (1.10), we see that

$$N_{s,k,d}(P) = \int_{\mathbb{T}^\iota} \prod_{j=1}^{s} f_j(\boldsymbol{\alpha}) d\boldsymbol{\alpha}.$$

We analyze the above integral via the Hardy-Littlewood circle method. To this end, we divide $\mathbb{T}^\iota$ into the Farey arcs defined as follows: given $\mathbf{a} = (a_{\mathbf{i}})_{\mathbf{i} \in \mathcal{L}} \in \mathbb{A}^\iota$, $g \in \mathbb{A}$ with $\gcd(\mathbf{a}, g) = 1$, we define the *Farey arc* $\mathfrak{M}(g, \mathbf{a})$ about $\mathbf{a}/g$ by

$$\mathfrak{M}(g, \mathbf{a}) = \Big\{ \boldsymbol{\alpha} \in \mathbb{T}^\iota \;\Big|\; \langle g\alpha_{\mathbf{i}} - a_{\mathbf{i}} \rangle < \hat{P}^{\frac{1}{2}-k} \ (\mathbf{i} \in \mathcal{L}) \Big\}. \tag{1.11}$$

Write $\langle c \rangle = \max_{1 \le j \le s} \langle c_j \rangle$. The set of *major arcs* $\mathfrak{M}$ is defined to be the union of all $\mathfrak{M}(g, \mathbf{a})$ with

$$\mathbf{a} \in \mathbb{A}^\iota,\ g \in \mathbb{A},\ g \,\text{monic},\ \gcd(\mathbf{a}, g) = 1,\ \text{and } 0 \le \langle a_{\mathbf{i}} \rangle < \langle g \rangle \le \langle c \rangle \hat{P}^{\frac{1}{2}}\ (\mathbf{i} \in \mathcal{L}). \tag{1.12}$$

The conditions (1.11) and (1.12) ensure that the arcs $\mathfrak{M}(g, \mathbf{a})$ comprising $\mathfrak{M}$ are disjoint. Furthermore, we write $\mathfrak{m} = \mathbb{T}^\iota \setminus \mathfrak{M}$ for the complementary set of *minor arcs*. In Chapter 2, we estimate the major arc contribution and obtain

$$\int_{\mathfrak{M}} \prod_{j=1}^{s} f_j(\boldsymbol{\alpha}) d\boldsymbol{\alpha} = C\hat{P}^{sd-\iota k} + O(\hat{P}^{sd-\iota k-\delta}), \tag{1.13}$$

for some $\delta > 0$ whenever

$$s \geq 2k(\iota + 1) + 1,$$

where the constant C depends on s, k, d, q and $c_1, \dots, c_s$ and $C > 0$ if the system (1.6) satisfies the solubility hypothesis as in Theorem 1. In Chapter 3, we show that the contribution over minor arcs is of the form

$$\int_{\mathfrak{m}} \prod_{j=1}^{s} f_j(\boldsymbol{\alpha}) d\boldsymbol{\alpha} = O(\hat{P}^{sd-\iota k-\delta}),$$

for some $\delta > 0$ whenever

$$s \geq 2rk\Big(\log(\iota rk) + \log\big(\log\big((2\iota - 1)rk \log k\big) + 2k^{-1}\big) + 3 + \log 4 - \log\big(1 - (\log k)^{-1}\big)\Big).$$

Then in Chapter 4, we combine the above estimates to prove Theorem 1.

Notation Generally, the variable ϵ denotes a small positive number whose value may change from statement to statement. The implicit constants in our analysis may depend at most on ϵ, s, k, d, q and $c_1, \dots, c_s$. Since our methods involve only a finite number of steps, all implicit constants that arise remain under control.

Chapter 2

The major arc contribution

2.1 The generating functions

We recall that for $P \in \mathbb{R}$ with $P > 0$ and $\boldsymbol{\alpha} = (\alpha_{\mathbf{i}})_{\mathbf{i}\in\mathcal{L}} \in \mathbb{T}^{\iota}$,

$$f_j(\boldsymbol{\alpha}) = \sum_{\mathbf{x}\in I_P^d} e\Big(\sum_{\mathbf{i}\in\mathcal{L}} c_j \alpha_{\mathbf{i}} \mathbf{x}^{\mathbf{i}}\Big) \quad (1 \le j \le s),$$

and for $g \in \mathbb{A}$ and $\mathbf{a} = (a_{\mathbf{i}})_{\mathbf{i}\in\mathcal{L}} \in \mathbb{A}^{\iota}$,

$$\mathfrak{M}(g, \mathbf{a}) = \big\{\mathbf{a} \in \mathbb{T}^{\iota} \,\big|\, \langle g\alpha_{\mathbf{i}} - a_{\mathbf{i}}\rangle < \hat{P}^{\frac{1}{2}-k} \quad (\mathbf{i} \in \mathcal{L})\big\}.$$

The first step is to establish control of the generating functions $f_j(\boldsymbol{\alpha})$ for $\boldsymbol{\alpha} \in \mathfrak{M}(g, \mathbf{a}) \subseteq \mathfrak{M}$ by the auxiliary functions

$$S(g, \mathbf{a}) = \sum_{\mathbf{x}\in I_{\mathrm{ord}\, g}^d} e\Big(\sum_{\mathbf{i}\in\mathcal{L}} \frac{a_{\mathbf{i}}}{g} \mathbf{x}^{\mathbf{i}}\Big),$$

and

$$S_j(g, \mathbf{a}) = S(g, c_j\mathbf{a}) \quad (1 \le j \le s).$$

For this purpose, we introduce two useful lemmas.

Lemma 3. *The exponential function $e : \mathbb{K}_\infty \to \mathbb{C}^\times$ has the following properties.*
(1) e is a continuous function.
(2) $e(\alpha + \beta) = e(\alpha)e(\beta)$.

(3) $e(x) = 1$, *if* $x \in \mathbb{A}$.

(4) If $m \in \mathbb{N}$ *and* $x \in \mathbb{A}$, *then*

$$\int_{\operatorname{ord}\alpha<-m} e(x\alpha)d\alpha = \begin{cases} q^{-m}, & \text{if } \operatorname{ord} x < m, \\ 0, & \textit{otherwise.} \end{cases}$$

(5) If $a, g \in \mathbb{A}$, *then*

$$\frac{1}{\langle g\rangle}\sum_{x\in I_{\operatorname{ord} g}} e\Big(\frac{ax}{g}\Big) = \begin{cases} 1, & \text{if } g \mid a, \\ 0, & \text{if } g \nmid a. \end{cases}$$

(6) For $\alpha, \beta \in \mathbb{K}_\infty$, *if* $\langle \alpha - \beta\rangle < q^{-1}$, *then* $e(\alpha) = e(\beta)$.

Proof. This is [10, Lemma 1]. □

For $\mathbf{i} = (i_1, \dots, i_d), \mathbf{j} = (j_1, \dots, j_d) \in \mathbb{N}^d$, write

$$\left(\begin{array}{c} \mathbf{i} \\ \mathbf{j} \end{array}\right) = \left(\begin{array}{c} i_1 \\ j_1 \end{array}\right) \cdots \left(\begin{array}{c} i_d \\ j_d \end{array}\right).$$

Lemma 4. *For* $\mathbf{i} \in \mathbb{N}^d$, *define*

$$\mathcal{R}_{\mathbf{i}} = \left\{ \mathbf{j} \in \mathbb{N}^d \,\Big|\, p \nmid \left(\begin{array}{c} \mathbf{i} \\ \mathbf{j} \end{array}\right) \right\}.$$

For $\mathbf{x}, \mathbf{y} \in \mathbb{K}_\infty$, *we have*

$$(\mathbf{x} + \mathbf{y})^{\mathbf{i}} = \sum_{\mathbf{j}\in\mathcal{R}_{\mathbf{i}}} \left(\begin{array}{c} \mathbf{i} \\ \mathbf{j} \end{array}\right) \mathbf{x}^{\mathbf{j}}\mathbf{y}^{\mathbf{i}-\mathbf{j}}.$$

Proof. Let $\mathbf{i} = (i_1, \dots, i_d)$, $\mathbf{x} = (x_1, \dots, x_d)$ and $\mathbf{y} = (y_1, \dots, y_d)$. Recall that $(\mathbf{x} + \mathbf{y})^{\mathbf{i}} = (x_1 + y_1)^{i_1} \cdots (x_d + y_d)^{i_d}$. By the binomial theorem, we have

$$(x_l + y_l)^{i_l} = \sum_{j_l=0}^{i_l} \left(\begin{array}{c} i_l \\ j_l \end{array}\right) x_l^{j_l} y_l^{i_l - j_l} \quad (1 \le l \le d).$$

Thus,

$$\begin{aligned}(\mathbf{x}+\mathbf{y})^{\mathbf{i}} &= \prod_{l=1}^{d}\sum_{j_l=0}^{i_l}\binom{i_l}{j_l}x_l^{j_l}y_l^{i_l-j_l}\\ &= \sum_{j_1=0}^{i_1}\cdots\sum_{j_d=0}^{i_d}\binom{i_1}{j_1}\cdots\binom{i_d}{j_d}(x_1^{j_1}y_1^{i_1-j_1})\cdots(x_d^{j_d}y_d^{i_d-j_d})\\ &= \sum_{\mathbf{j}\in\mathcal{R}_{\mathbf{i}}}\binom{\mathbf{i}}{\mathbf{j}}\mathbf{x}^{\mathbf{j}}\mathbf{y}^{\mathbf{i}-\mathbf{j}}.\end{aligned}$$

This completes the proof of the lemma. □

Lemma 5. *Suppose that* $\boldsymbol{\alpha}=(\alpha_{\mathbf{i}})_{\mathbf{i}\in\mathcal{L}}\in\mathbb{T}^{\iota}$ *and that* $\boldsymbol{\alpha}=\mathbf{a}/g+\boldsymbol{\beta}$ *with* $g\in\mathbb{A}$, $\mathbf{a}=(a_{\mathbf{i}})_{\mathbf{i}\in\mathcal{L}}\in\mathbb{A}^{\iota}$, $\langle a_{\mathbf{i}}\rangle<\langle g\rangle\le\langle c\rangle\hat{P}^{\frac{1}{2}}$ *and* $\langle\beta_{\mathbf{i}}\rangle<\langle g\rangle^{-1}\hat{P}^{\frac{1}{2}-k}$ $\big(\mathbf{i}\in\mathcal{L}\big)$. *If* $\langle c\rangle\le\hat{P}^{\frac{1}{2}}$ *, then*

$$f_j(\boldsymbol{\alpha})=\langle g\rangle^{-d}S_j(g,\mathbf{a})f_j(\boldsymbol{\beta})\quad(1\le j\le s).$$

Proof. Fix $\mathbf{x}\in I_P^d$. We can write $\mathbf{x}$ uniquely as $\mathbf{x}=g\mathbf{y}+\mathbf{z}$ with $\mathbf{z}\in I^d_{\operatorname{ord} g}$ and $\mathbf{y}\in I_Q^d$, where $Q=P-\operatorname{ord} g$. Since $(g\mathbf{y}+\mathbf{z})^{\mathbf{i}}\equiv\mathbf{z}^{\mathbf{i}}\,(\operatorname{mod} g)$, by Lemmas 3 and 4, we have

$$e\Big(\sum_{\mathbf{i}\in\mathcal{L}}\frac{c_ja_{\mathbf{i}}}{g}(g\mathbf{y}+\mathbf{z})^{\mathbf{i}}\Big)=e\Big(\sum_{\mathbf{i}\in\mathcal{L}}\frac{c_ja_{\mathbf{i}}}{g}\mathbf{z}^{\mathbf{i}}\Big).$$

It follows that

$$\begin{aligned}f_j(\boldsymbol{\alpha}) &= \sum_{\mathbf{y}\in I_Q^d}\sum_{\mathbf{z}\in I^d_{\operatorname{ord} g}}e\Big(\sum_{\mathbf{i}\in\mathcal{L}}c_j\alpha_{\mathbf{i}}(g\mathbf{y}+\mathbf{z})^{\mathbf{i}}\Big)\\ &= \sum_{\mathbf{y}\in I_Q^d}\sum_{\mathbf{z}\in I^d_{\operatorname{ord} g}}e\Big(\sum_{\mathbf{i}\in\mathcal{L}}\frac{c_ja_{\mathbf{i}}}{g}(g\mathbf{y}+\mathbf{z})^{\mathbf{i}}\Big)e\Big(\sum_{\mathbf{i}\in\mathcal{L}}c_j\beta_{\mathbf{i}}(g\mathbf{y}+\mathbf{z})^{\mathbf{i}}\Big)\\ &= \sum_{\mathbf{z}\in I^d_{\operatorname{ord} g}}e\Big(\sum_{\mathbf{i}\in\mathcal{L}}\frac{c_ja_{\mathbf{i}}}{g}\mathbf{z}^{\mathbf{i}}\Big)\sum_{\mathbf{y}\in I_Q^d}e\Big(\sum_{\mathbf{i}\in\mathcal{L}}c_j\beta_{\mathbf{i}}(g\mathbf{y}+\mathbf{z})^{\mathbf{i}}\Big)\\ &= S_j(g,\mathbf{a})\sum_{\mathbf{y}\in I_Q^d}e\Big(\sum_{\mathbf{i}\in\mathcal{L}}c_j\beta_{\mathbf{i}}(g\mathbf{y}+\mathbf{z})^{\mathbf{i}}\Big).\end{aligned}\tag{2.1}$$

To treat the above sum, note that for each $\mathbf{i}\in\mathcal{L}$,

$$\operatorname{ord}\beta_{\mathbf{i}}<-\operatorname{ord} g+(1/2-k)P\quad\text{ and }\quad|\mathbf{i}|=k.$$

Moreover, since $g\mathbf{y} \in I_P^d$ and $\mathbf{z} \in I_{\operatorname{ord} g}^d$, we deduce from Lemma 4 that

$$\begin{aligned}
&\operatorname{ord}\left(c_j\beta_{\mathbf{i}}(g\mathbf{y}+\mathbf{z})^{\mathbf{i}} - c_j\beta_{\mathbf{i}}(g\mathbf{y})^{\mathbf{i}}\right)\\
=&\operatorname{ord} c_j + \operatorname{ord}\beta_{\mathbf{i}} + \operatorname{ord}\left((g\mathbf{y}+\mathbf{z})^{\mathbf{i}} - (g\mathbf{y})^{\mathbf{i}}\right)\\
<&\operatorname{ord} c - \operatorname{ord} g + (1/2-k)P + \max\left\{\operatorname{ord}\left((g\mathbf{y})^{\mathbf{i}-\mathbf{l}}\mathbf{z}^{\mathbf{l}}\right) \;\middle|\; \mathbf{l}\in\mathcal{R}_{\mathbf{i}}, \mathbf{l}\neq\mathbf{0}\right\}\\
\leq&\operatorname{ord} c - \operatorname{ord} g + (1/2-k)P + \max\left\{(k-|\mathbf{l}|)(P-1) + |\mathbf{l}|(\operatorname{ord} g - 1) \;\middle|\; \mathbf{l}\in\mathcal{R}_{\mathbf{i}}, \mathbf{l}\neq\mathbf{0}\right\}\\
=&\max\left\{\operatorname{ord} c + (1/2-|\mathbf{l}|)P + (|\mathbf{l}|-1)\operatorname{ord} g - k \;\middle|\; \mathbf{l}\in\mathcal{R}_{\mathbf{i}}, \mathbf{l}\neq\mathbf{0}\right\}.
\end{aligned}$$

Since $\operatorname{ord} g \leq \operatorname{ord} c + \frac{1}{2}P$ and $\operatorname{ord} c \leq \frac{1}{2}P$, we have

$$\operatorname{ord}\left(c_j\beta_{\mathbf{i}}(g\mathbf{y}+\mathbf{z})^{\mathbf{i}} - c_j\beta_{\mathbf{i}}(g\mathbf{y})^{\mathbf{i}}\right) < -k \leq -1.$$

Thus, by Lemma 3 , we obtain

$$e\Big(c_j\beta_{\mathbf{i}}(g\mathbf{y}+\mathbf{z})^{\mathbf{i}} - c_j\beta_{\mathbf{i}}(g\mathbf{y})^{\mathbf{i}}\Big) = 1,$$

i.e.,

$$e\Big(c_j\beta_{\mathbf{i}}(g\mathbf{y}+\mathbf{z})^{\mathbf{i}}\Big) = e\Big(c_j\beta_{\mathbf{i}}(g\mathbf{y})^{\mathbf{i}}\Big).$$

Therefore,

$$\begin{aligned}
f_j(\boldsymbol{\beta}) &= \sum_{\mathbf{z}\in I_{\operatorname{ord} g}^d}\sum_{\mathbf{y}\in I_Q^d} e\Big(\sum_{\mathbf{i}\in\mathcal{L}} c_j\beta_{\mathbf{i}}(g\mathbf{y}+\mathbf{z})^{\mathbf{i}}\Big)\\
&= \langle g\rangle^d \sum_{\mathbf{y}\in I_Q^d} e\Big(\sum_{\mathbf{i}\in\mathcal{L}} c_j\beta_{\mathbf{i}}(g\mathbf{y})^{\mathbf{i}}\Big).
\end{aligned} \tag{2.2}$$

By (2.1) and (2.2), we conclude that

$$f_j(\boldsymbol{\alpha}) = \langle g\rangle^{-d} S_j(g,\mathbf{a}) f_j(\boldsymbol{\beta}).$$

This completes the proof of the lemma. □

For every $g \in \mathbb{A}$, write

$$\mathcal{A}_g = \left\{\mathbf{a} = (a_{\mathbf{i}})_{\mathbf{i}\in\mathcal{L}} \in I_{\operatorname{ord} g}^{\iota} \;\middle|\; \gcd(\mathbf{a}, g) = 1\right\},$$

and

$$\mathcal{B}_g = \left\{\boldsymbol{\beta} = (\beta_{\mathbf{i}})_{\mathbf{i}\in\mathcal{L}} \in \mathbb{T}^{\iota} \;\middle|\; \langle\beta_{\mathbf{i}}\rangle < \langle g\rangle^{-1}\hat{P}^{\frac{1}{2}-k}\ \big(\mathbf{i}\in\mathcal{L}\big)\right\}.$$

In view of the definition of the major arcs, we have

$$\mathfrak{M} = \bigcup_{\substack{\langle g\rangle \le \langle c\rangle \hat{P}^{\frac{1}{2}} \\ g \text{ monic}}} \bigcup_{\mathbf{a}\in\mathcal{A}_g} \mathfrak{M}(g,\mathbf{a}).$$

Lemma 6.

$$\int_{\mathfrak{M}} \prod_{j=1}^{s} f_j(\boldsymbol{\alpha}) d\boldsymbol{\alpha} = \sum_{\substack{\langle g\rangle \le \langle c\rangle \hat{P}^{\frac{1}{2}} \\ g \text{ monic}}} \sum_{\mathbf{a}\in\mathcal{A}_g} \Big(\prod_{j=1}^{s} \langle g\rangle^{-d} S_j(g,\mathbf{a}) \Big) \int_{\mathcal{B}_g} \prod_{j=1}^{s} f_j(\boldsymbol{\beta}) d\boldsymbol{\beta}.$$

Proof. For $\mathfrak{M}(g,\mathbf{a}) \subseteq \mathfrak{M}$, it follows from Lemma 5 that

$$\int_{\mathfrak{M}(g,\mathbf{a})} \prod_{j=1}^{s} f_j(\boldsymbol{\alpha}) d\boldsymbol{\alpha} = \Big(\prod_{j=1}^{s} \langle g\rangle^{-d} S_j(g,\mathbf{a}) \Big) \int_{\mathcal{B}_g} \prod_{j=1}^{s} f_j(\boldsymbol{\beta}) d\boldsymbol{\beta}.$$

Since all $\mathfrak{M}(g,\mathbf{a}) \subseteq \mathfrak{M}$ are pairwise disjoint, the result follows. □

2.2 Preliminary observations in p-adic analysis

To obtain the asymptotic formula given by (1.13), we need to establish some results in p-adic analysis. Let K be a complete field with respect to a discrete non-archimedean valuation $|\cdot|$. Let $R = \{x \in K \mid |x| \le 1\}$, π a primitive element, and $F = R/(\pi)$. We also suppose that F is a finite extension over $\mathbb{F}_p$.

Definition 7. *Let $a \in K \setminus \{0\}$. Define*

$$\tau(a) = \log|a| / \log|\pi| \quad \textit{and} \quad \tau(0) = \infty.$$

Let $\varphi(x) = a_n x^n + \cdots + a_1 x + a_0 \in K[x]$. Define

$$\tau(\varphi) = \min_{0\le i\le n} \tau(a_i), \tag{2.3}$$

and

$$\operatorname{ind}\varphi = \max\big\{ j \;\big|\; 0 \le j \le n,\ \tau(a_j) = \tau(\varphi) \big\}.$$

Lemma 8. *Let $\varphi(x) \in K[x] \setminus \{0\}$. Let $\psi(x) = \varphi(\pi x)$ and $\phi(x) = \pi^u \varphi(x)$ where $u \in \mathbb{N}$. Then*

$$\operatorname{ind} \phi = \operatorname{ind} \varphi \quad \textit{and} \quad \operatorname{ind} \psi \leq \operatorname{ind} \varphi.$$

Let φ' and ψ' be the derivatives of φ and ψ with respect to x respectively. Suppose that $\varphi' \neq 0$. Then

$$\operatorname{ind} \psi' \leq \operatorname{ind} \varphi'.$$

Proof. Suppose that $\varphi(x) = a_n x^n + \cdots + a_1 x + a_0$. For convenience, write $j = \operatorname{ind} \varphi$ and $\tau_i = \tau(a_i)\,(0 \leq i \leq n)$. Thus, we have $\tau_j = \tau(\varphi)$ and

$$\tau_i > \tau_j, \text{ if } \ i > j; \ \ \tau_i \geq \tau_j, \text{ if } i < j. \tag{2.4}$$

For any $u \in \mathbb{N}$, $\tau(\pi^u a_i) = u + \tau_i\ (0 \leq i \leq n)$. Thus,

$$\tau(\pi^u a_i) = \begin{cases} \tau_i + u > \tau_j + u, & \text{if } \ i > j, \\ \tau_i + u \geq \tau_j + u, & \text{if } i < j. \end{cases}$$

Hence

$$\operatorname{ind} \phi = j = \operatorname{ind} \varphi.$$

Since

$$\psi(x) = \varphi(\pi x) = (a_n \pi^n) x^n + \cdots + (a_1 \pi) x + a_0,$$

it follows from (2.4) that for $i > j$,

$$\tau(a_i \pi^i) = \tau_i + i > \tau_j + j = \tau(a_j \pi^j). \tag{2.5}$$

Thus

$$\operatorname{ind} \psi \leq j = \operatorname{ind} \varphi.$$

Since $\psi'(x) = \pi \varphi'(\pi x)$, we have

$$\operatorname{ind} \psi'(x) = \operatorname{ind} \varphi'(\pi x) \leq \operatorname{ind} \varphi'(x).$$

This completes the proof of the lemma. □

Lemma 9. *Let $\varphi(x)$ and $\psi(x)$ be defined as in Lemma 8. Let $\lambda \in R$. The following hold.*
(1) If $\operatorname{ind} \psi = \operatorname{ind} \varphi$ and $\tau(\varphi(\lambda)) \geq \tau(\varphi) + 1$, then $\tau(\lambda) \geq 1$.
(2) If $\varphi' \neq 0$, $\operatorname{ind} \psi' = \operatorname{ind} \varphi'$, and $\tau(\varphi'(\lambda)) \geq \tau(\varphi') + 1$, then $\tau(\lambda) \geq 1$.

Proof. (1) Let $\varphi(x) = a_n x^n + \cdots + a_1 x + a_0$ and $j = \operatorname{ind}\varphi$. Write $\tau_i = \tau(a_i)$ $(0 \le i \le n)$. By Lemma 8, we have $\operatorname{ind}\psi = \operatorname{ind}\varphi = j$. Since $\tau(a_i\pi^i) = \tau_i + i\,(0 \le i \le n)$, we see that for $i < j$, $\tau_i + i \ge \tau_j + j$ and hence $\tau_i > \tau_j$. In combination with (2.4), it follows that

$$\tau_i > \tau_j \quad (i \ne j). \tag{2.6}$$

Since $\lambda \in R$, we have $|\lambda| \le 1$, i.e., $\tau(\lambda) \ge 0$. Suppose that $\tau(\lambda) = 0$. From (2.6), we deduce that $\tau(\varphi(\lambda)) = \tau_j = \tau(\varphi)$, which contradicts the condition that $\tau(\varphi(\lambda)) \ge \tau(\varphi)+1$. Thus $\tau(\lambda) \ge 1$.

(2) Since $\psi'(x) = \pi\varphi'(\pi x)$, we obtain that $\operatorname{ind}\psi'(x) = \operatorname{ind}\varphi'(\pi x)$. If $\operatorname{ind}\psi' = \operatorname{ind}\varphi'$, we have $\operatorname{ind}\varphi'(\pi x) = \operatorname{ind}\varphi'(x)$. Hence the result follows from *(1)*. □

Lemma 10. *Let $\varphi(x) \in K[x] \setminus \{0\}$ and $\lambda, \lambda_1, \lambda_2 \in R$. Define $\phi(x) = \varphi(x + \lambda)$ and $\varphi_\lambda(x) = \varphi(\pi x + \lambda)$. The following hold.*
(1) $\operatorname{ind}\phi = \operatorname{ind}\varphi$ *and* $\tau(\phi) = \tau(\varphi)$.
(2) If $\operatorname{ind}\varphi_\lambda = \operatorname{ind}\varphi$ *and* $\tau(\varphi(\lambda_1)) \ge \tau(\varphi) + 1$, *then* $\tau(\lambda_1 - \lambda) \ge 1$.
(3) Suppose that $\varphi' \ne 0$. *Then* $\operatorname{ind}\phi' = \operatorname{ind}\varphi'$ *and* $\tau(\phi') = \tau(\varphi')$.
(4) Suppose that $\varphi' \ne 0$. *If* $\operatorname{ind}\varphi'_\lambda = \operatorname{ind}\varphi'$ *and* $\tau(\varphi'(\lambda_2)) \ge \tau(\varphi') + 1$, *then* $\tau(\lambda_2 - \lambda) \ge 1$.

Proof. (1) Write $\varphi(x) = a_n x^n + \cdots + a_1 x + a_0$ and $\phi(x) = b_n x^n + \cdots + b_1 x + b_0$. Then

$$b_i = \sum_{h=i}^{n} \binom{h}{i} a_h \lambda^{h-i} = a_i + \sum_{h=i+1}^{n} \binom{h}{i} a_h \lambda^{h-i} \quad (0 \le i \le n). \tag{2.7}$$

Write $j = \operatorname{ind}\varphi$. Since $\tau(\lambda) \ge 0$, by (2.4) and (2.7), we deduce that

$$\tau(b_i) > \tau(a_j), \text{ if } i > j; \quad \tau(b_j) = \tau(a_j), \text{ if } i = j; \quad \tau(b_i) \ge \tau(a_j), \text{ if } i < j.$$

Thus

$$j = \operatorname{ind}\phi \quad \text{and} \quad \tau(\phi) = \tau(a_j) = \tau(\varphi).$$

(2) Since $\tau(\phi) = \tau(\varphi)$ and $\phi(\lambda_1 - \lambda) = \varphi(\lambda_1)$, we find that

$$\tau\big(\phi(\lambda_1 - \lambda)\big) = \tau\big(\varphi(\lambda_1)\big) \ge \tau(\varphi) + 1 = \tau(\phi) + 1.$$

If $\operatorname{ind}\varphi_\lambda = \operatorname{ind}\varphi$, we have from *(1)* that $\operatorname{ind}\varphi_\lambda = \operatorname{ind}\phi$. Since $\varphi_\lambda(x) = \phi(\pi x)$, it follows from Lemma 9 that $\tau(\lambda_1 - \lambda) \ge 1$.

(3) Since $\phi'(x) = \varphi'(x+\lambda)$, we can deduce *(3)* from *(1)* .

(4) Note that $\varphi'_\lambda(x) = \pi\varphi'(\pi x+\lambda)$. It follows from Lemma 8 that

$$\operatorname{ind}\varphi'(\pi x+\lambda) = \operatorname{ind}\varphi'_\lambda(x) = \operatorname{ind}\varphi'(x).$$

By *(2)*, we have $\tau(\lambda_2-\lambda)\geq 1$. □

Lemma 11. *Let* $\varphi(x) = a_n x^n + \cdots + a_1 x + a_0 \in K[x]\setminus\{0\}$. *For* $\lambda \in R$, *let*

$$\varphi_\lambda(x) = \varphi(\pi x+\lambda) \text{ and } \psi_\lambda(x) = \varphi(\pi x+\lambda) - \varphi(\lambda).$$

The following hold.
(1) $\tau(\varphi) + \operatorname{ind}\varphi_\lambda \leq \tau(\varphi_\lambda) \leq \tau(\varphi) + \operatorname{ind}\varphi$. *Furthermore, if* $\tau(\varphi(\lambda)) \geq \tau(\varphi)+1$, *then* $\tau(\varphi_\lambda)\geq\tau(\varphi)+1$.
(2) If $\operatorname{ind}\varphi > 0$, *then* $\tau(\varphi)+1 \leq \tau(\psi_\lambda) \leq \tau(\varphi)+n$.
(3) Suppose that $\varphi' \neq 0$. *Then* $1+\tau(\varphi') \leq \tau(\psi'_\lambda) = \tau(\varphi'_\lambda) \leq n+\tau(\varphi')$.
(4) $\operatorname{ind}\varphi_\lambda \leq \varphi$ *and* $\operatorname{ind}\varphi'_\lambda \leq \operatorname{ind}\varphi'$.

Proof. (1) Suppose that $\varphi_\lambda(x) = b_n x^n + \cdots + b_1 x + b_0$. Then

$$b_i = \sum_{h=i}^{n} \binom{h}{i} a_h \lambda^{h-i}\pi^i = a_i\pi^i + \sum_{h=i+1}^{n} \binom{h}{i} a_h\lambda^{h-i}\pi^i. \tag{2.8}$$

Let $j = \operatorname{ind}\varphi$. Then for each i with $0\leq i\leq n$, we have $|a_j|\geq|a_i|$ and hence $|b_i|\leq|a_j||\pi^i|$. Let $l = \operatorname{ind}\varphi_\lambda$. Then

$$\tau(\varphi)+l = \tau(a_j)+l \leq \tau(b_l) = \tau(\varphi_\lambda).$$

Since $|a_j| > |a_i|$ when $i>j$, we have $|b_j| = |a_j||\pi^j|$. Thus, by (2.3), we find that

$$\tau(\varphi_\lambda) \leq \tau(b_j) = \tau(a_j)+j = \tau(\varphi)+j. \tag{2.9}$$

It follows that

$$\tau(\varphi)+\operatorname{ind}\varphi_\lambda \leq \tau(\varphi_\lambda) \leq \tau(\varphi)+\operatorname{ind}\varphi. \tag{2.10}$$

Now suppose that $\tau(\varphi(\lambda))\geq\tau(\varphi)+1$. If $\operatorname{ind}\varphi_\lambda > 0$, by (2.10), we get $\tau(\varphi_\lambda)\geq\tau(\varphi)+1$. If $\operatorname{ind}\varphi_\lambda = 0$, then

$$\tau(\varphi_\lambda) = \tau(b_0) = \tau(\varphi(\lambda)) \geq \tau(\varphi)+1.$$

(2) Note that $\psi_\lambda(x) = \varphi_\lambda(x) - \varphi_\lambda(0) = b_n x^n + \cdots + b_1 x$, where the b_i's $(1 \le i \le n)$ are defined as in (2.8). Let $m = \operatorname{ind} \psi_\lambda$. Then $|b_m| \le |a_j||\pi^m|$. Since $j = \operatorname{ind} \varphi > 0$, we have $m \ge 1$ and hence

$$\tau(\psi_\lambda) = \tau(b_m) \ge \tau(\varphi) + m \ge \tau(\varphi) + 1.$$

Moreover, we deduce from (2.3) and (2.9) that

$$\tau(\psi_\lambda) \le \tau(b_j) = \tau(a_j) + j \le \tau(\varphi) + n.$$

(3) Since $\varphi'_\lambda(x) = \psi'_\lambda(x) = \pi\varphi'(\pi x + \lambda)$, we can see from *(1)* that

$$\tau(\varphi') + 1 \le \tau(\varphi'_\lambda) = \tau(\psi'_\lambda) \le \tau(\varphi') + (n-1) + 1 = \tau(\varphi') + n.$$

(4) It follows from *(1)* that

$$\tau(\varphi) + \operatorname{ind} \varphi_\lambda \le \tau(\varphi) + \operatorname{ind} \varphi.$$

Hence $\operatorname{ind} \varphi_\lambda \le \operatorname{ind} \varphi$. Note that $\varphi'_\lambda = \pi\varphi'(\pi x + \lambda)$. By Lemma 8, we have

$$\operatorname{ind} \varphi'_\lambda(x) = \operatorname{ind} \varphi'(\pi x + \lambda) \le \operatorname{ind} \varphi'(x).$$

□

Lemma 12. *Let $\varphi(x) \in K[x] \setminus \{0\}$ be of degree n. For $u, v \in \mathbb{N}$ with $u \ge v > n$, define*

$$N_{u,v}(\varphi) = \big\{\alpha (\operatorname{mod} \pi^u) \;\big|\; \alpha \in R,\, \tau(\varphi(\alpha)) \ge v + \tau(\varphi)\big\}.$$

Then

$$\operatorname{card} N_{u,v}(\varphi) \le (\operatorname{card} F)^{n+1+u-\frac{v}{n}}.$$

Proof. Suppose that $x_1, x_2 \in R$, $|x_1 - x_2| \le |\pi|^v$, and $|\varphi(x_2)| \le |\pi|^{\tau(\varphi)+v}$. We have

$$|\varphi(x_1) - \varphi(x_2)| \le |\pi|^{\tau(\varphi)} |x_1 - x_2| \le |\pi|^{\tau(\varphi)+v}.$$

Hence, the set $N_{u,v}(\varphi)$ is well-defined and

$$\operatorname{card} N_{u,v}(\varphi) = (\operatorname{card} F)^{u-v} \cdot \operatorname{card} N_{v,v}(\varphi). \tag{2.11}$$

For $\lambda \in R$, define

$$\varphi_\lambda(x) = \varphi(\pi x + \lambda).$$

Write $\Lambda = \{\lambda \in R \,|\, \tau(\varphi(\lambda)) \geq \tau(\varphi) + 1\}$. If $\Lambda = \emptyset$, then $N_{u,v}(\varphi) = \emptyset$ and hence the result holds immediately. We now suppose that $\Lambda \neq \emptyset$ and consider two cases.

Case 1: Suppose that there exists some $\lambda \in \Lambda$ such that $\operatorname{ind}\varphi_\lambda = \operatorname{ind}\varphi$. Then for any $\xi \in \Lambda$, by Lemma 10(2), we have $\tau(\xi - \lambda) \geq 1$. Hence $\xi = \lambda + \pi y$ for some $y \in R$. Thus,

$$\begin{aligned}\operatorname{card} N_{v,v}(\varphi) &= \operatorname{card}\Big\{\alpha \pmod{\pi^v} \;\Big|\; \tau\big(\varphi(\alpha)\big) \geq v + \tau(\varphi) \text{ and } \alpha \equiv \lambda \pmod{\pi}\Big\} \\ &= \operatorname{card}\Big\{y \pmod{\pi^{v-1}} \;\Big|\; \tau\big(\varphi(\pi y + \lambda)\big) \geq v + \tau(\varphi)\Big\} \\ &= \operatorname{card}\Big\{y \pmod{\pi^{v-1}} \;\Big|\; \tau\big(\varphi_\lambda(y)\big) \geq v + \tau(\varphi)\Big\}.\end{aligned} \tag{2.12}$$

Let $\sigma = \tau(\varphi_\lambda) - \tau(\varphi)$. Then by Lemma 11(1), we have

$$1 \leq \sigma \leq n.$$

On recalling (2.12), we see that

$$\begin{aligned}\operatorname{card} N_{v,v}(\varphi) &= \operatorname{card}\Big\{y \pmod{\pi^{v-1}} \;\Big|\; \tau\big(\varphi_\lambda(y)\big) \geq v - \sigma + \tau(\varphi_\lambda)\Big\} \\ &= (\operatorname{card} F)^{\sigma-1}\operatorname{card}\Big\{y \pmod{\pi^{v-\sigma}} \;\Big|\; \tau\big(\varphi_\lambda(y)\big) \geq v - \sigma + \tau(\varphi_\lambda)\Big\} \\ &= (\operatorname{card} F)^{\sigma-1}\operatorname{card} N_{v-\sigma,v-\sigma}(\varphi_\lambda).\end{aligned} \tag{2.13}$$

Case 2: Suppose that for any $\lambda \in \Lambda$, $\operatorname{ind}\varphi_\lambda \neq \operatorname{ind}\varphi$. Then from Lemma 11(4), we have

$$\operatorname{ind}\varphi_\lambda < \operatorname{ind}\varphi. \tag{2.14}$$

Let $\{\lambda_1, \ldots, \lambda_l\}$ be a complete set of representatives of $\big\{\lambda \pmod{\pi} \;\big|\; \lambda \pmod{\pi^v} \in N_{v,v}\big\}$. Also, let $\sigma_i = \tau(\varphi_{\lambda_i}) - \tau(\varphi)\,(1 \leq i \leq l)$. By a similar argument as in Case 1, for each $\lambda_i \in \Lambda$, we see that

$$1 \leq \sigma_i \leq n,$$

and that

$$\begin{aligned}&\operatorname{card}\Big\{x \pmod{\pi^v} \;\Big|\; \tau\big(\varphi(x)\big) \geq v + \tau(\varphi) \text{ and } x \equiv \lambda_i \pmod{\pi}\Big\} \\ =&(\operatorname{card} F)^{\sigma_i-1}\operatorname{card} N_{v-\sigma_i,v-\sigma_i}(\varphi_\lambda).\end{aligned}$$

Thus

$$\begin{aligned}\operatorname{card} N_{v,v}(\varphi) &= \sum_{i=1}^{l} \operatorname{card}\Big\{x \pmod{\pi^v} \;\Big|\; \tau\big(\varphi(x)\big) \geq v + \tau(\varphi) \text{ and } x \equiv \lambda_i \pmod{\pi}\Big\} \\ &\leq \operatorname{card} F \cdot \max_{1\leq i\leq l}(\operatorname{card} F)^{\sigma_i-1} \cdot \operatorname{card} N_{v-\sigma_i,v-\sigma_i}(\varphi_{\lambda_i}).\end{aligned} \tag{2.15}$$

Suppose that this procedure is repeated m times and we obtain that $N_{v_j,v_j}(\varphi_j)$ $(1 \le j \le m)$, which satisfy that

$$\deg \varphi_j = n, \quad 1 \le v_j - v_{j-1} \le n, \quad \text{and} \quad v_m \le n, \tag{2.16}$$

where $\varphi_0 = \varphi$ and $v_0 = v$. We note here that Case 2 occurs not exceeding n times because of the inequality (2.14). Therefore, by estimating $\operatorname{card} N_{v_m,v_m}$ trivially and combining (2.13) with (2.15), we find that

$$\begin{aligned} \operatorname{card} N_{v,v} &\le (\operatorname{card} F)^n \cdot (\operatorname{card} F)^{v-v_m-m} \cdot \operatorname{card} N_{v_m,v_m} \\ &\le (\operatorname{card} F)^n \cdot (\operatorname{card} F)^{v-v_m-m} \cdot (\operatorname{card} F)^{v_m} \\ &\le (\operatorname{card} F)^{n+v-m}. \end{aligned} \tag{2.17}$$

It follows from (2.16) that

$$mn \ge v - v_m \ge v - n,$$

which yields that $m \ge \frac{v}{n} - 1$. On recalling (2.11) and (2.17), we can deduce that

$$\operatorname{card} N_{u,v} \le (\operatorname{card} F)^{n+u-m} \le (\operatorname{card} F)^{n+1+u-\frac{v}{n}}.$$

This completes the proof of the lemma. □

Lemma 13. *Let $\psi_1, \dots, \psi_n$ be polynomials in $R[x_1, \dots, x_n]$ with Jacobian $\Delta(\boldsymbol{\psi}; \mathbf{x})$, and suppose that $\mathbf{a} = (a_1, \dots, a_n) \in R^n$ satisfies*

$$\big|\psi_j(\mathbf{a})\big| < \big|\Delta(\boldsymbol{\psi}; \mathbf{a})\big|^2 \quad (1 \le j \le n).$$

Then there exists a unique $\mathbf{b} = (b_1, \dots, b_n) \in R^n$ such that

$$\psi_j(\mathbf{b}) = 0 \quad (1 \le j \le n) \quad \text{and} \quad \big|b_i - a_i\big| < \big|\Delta(\boldsymbol{\psi}; \mathbf{a})\big| \quad (1 \le i \le n).$$

Proof. This is [7, Proposition 5.20]. □

Lemma 14. *For $h \in \mathbb{N} \setminus \{0\}$ and $\gamma_1, \dots, \gamma_s \in R \setminus \{0\}$, define*

$$M(\pi^h; \boldsymbol{\gamma}) = \operatorname{card}\big\{\mathbf{x} \ (\operatorname{mod} \pi^h) \ \big| \ \gamma_1 \mathbf{x}_1^{\mathbf{i}} + \cdots + \gamma_s \mathbf{x}_s^{\mathbf{i}} \equiv 0 \ (\operatorname{mod} \pi^h) \ \ (\mathbf{i} \in \mathcal{L})\big\}.$$

Suppose that the system $\gamma_1 \mathbf{x}_1^{\mathbf{i}} + \cdots + \gamma_s \mathbf{x}_s^{\mathbf{i}} = 0$ $(\mathbf{i} \in \mathcal{L})$ has a non-singular solution $\mathbf{a} \in R^{ds}$. Then there exists an integer $u = u(\boldsymbol{\gamma}; \mathbf{a})$ such that whenever $h \ge u$, we have

$$M(\pi^h; \boldsymbol{\gamma}) \ge (\operatorname{card} F)^{(h-u)(ds-\iota)}.$$

Proof. We relabel the variables by writing

$$(z_1, \dots, z_{ds}) = (x_{11}, \dots, x_{d1}, \dots, x_{1s}, \dots, x_{ds}). \tag{2.18}$$

For every $\mathbf{i} \in \mathcal{L}$, we let $\psi_{\mathbf{i}}(\mathbf{z})$ denote the polynomial $\gamma_1 \mathbf{x}_1^{\mathbf{i}} + \cdots + \gamma_s \mathbf{x}_s^{\mathbf{i}}$ with $\mathbf{x}$ replaced by $\mathbf{z}$ as in (2.18). Write $\boldsymbol{\psi} = \big(\psi_{\mathbf{i}}\big)_{\mathbf{i} \in \mathcal{L}}$. Let $\mathbf{a} = (a_1, \dots, a_{ds}) \in R^{ds}$ be a non-singular solution of the system $\psi_{\mathbf{i}}(\mathbf{z}) = 0$ $\big(\mathbf{i} \in \mathcal{L}\big)$. Then there exist $i_1, \dots, i_\iota$ such that

$$\Delta(\boldsymbol{\psi}; a_{i_1}, \dots, a_{i_\iota}) \neq 0.$$

Thus we can find an integer u satisfying

$$\big|\Delta(\boldsymbol{\psi}; a_{i_1}, \dots, a_{i_\iota})\big|^2 = |\pi|^{u-1}.$$

For $i \notin \{i_1, \dots, i_\iota\}$, choose $b_i \in R$ with $b_i \equiv a_i \,(\mathrm{mod}\, \pi^u)$. Write $v_i = a_i$ for $i \in \{i_1, \dots, i_\iota\}$ and $v_i = b_i$ otherwise. Then we see that for every $\mathbf{i} \in \mathcal{L}$,

$$\psi_{\mathbf{i}}(\mathbf{v}) \equiv \psi_{\mathbf{i}}(\mathbf{a}) \equiv 0 \ (\mathrm{mod}\, \pi^u),$$

and hence

$$\big|\psi_{\mathbf{i}}(\mathbf{v})\big| \leq |\pi|^u < \big|\Delta(\boldsymbol{\psi}; a_{i_1}, \dots, a_{i_\iota})\big|^2.$$

Fix such a choice for $\mathbf{b}$. We may regard $\psi_{\mathbf{i}}(\mathbf{z})$ as a polynomial in ι variables $z_{i_1}, \dots, z_{i_\iota}$ after substituting $z_i = b_i$ for $i \notin \{i_1, \dots, i_\iota\}$. By applying Lemma 13, we obtain $u_{i_1}, \dots, u_{i_\iota} \in R$ such that

$$\psi_{\mathbf{i}}(\mathbf{u}, \mathbf{b}) = 0 \ (\mathbf{i} \in \mathcal{L}).$$

Thus for every $h \in \mathbb{N}$ with $h \geq u$, we have

$$\psi_{\mathbf{i}}(\mathbf{u}, \mathbf{b}) \equiv 0 \ (\mathrm{mod}\, \pi^h) \ (\mathbf{i} \in \mathcal{L}).$$

Furthermore, since there are $(\mathrm{card}\, F)^{(h-u)(ds-\iota)}$ possible choices for the $b_{\mathbf{i}} \,(\mathrm{mod}\, \pi^h)$, we see that

$$M(\pi^h; \boldsymbol{\gamma}) \geq (\mathrm{card}\, F)^{(h-u)(ds-\iota)}.$$

□

2.3 Estimates for exponential sums I

In this section, we aim to estimate the auxiliary functions

$$S(g, \mathbf{a}) = \sum_{\mathbf{x} \in I^d_{\operatorname{ord} g}} e\Big(\sum_{\mathbf{i} \in \mathcal{L}} \frac{a_{\mathbf{i}}}{g} \mathbf{x}^{\mathbf{i}} \Big),$$

and

$$S_j(g, \mathbf{a}) = S(g, c_j \mathbf{a}) \quad (1 \le j \le s).$$

Let $w \in \mathbb{A}$ be an irreducible element. Write $|\cdot|_w$ for the usual w-adic valuation normalized, i.e., $|w|_w = \langle w \rangle^{-1}$. Then $R = \mathbb{A}_w$, $\pi = w$ and $F = \mathbb{A}_w/(w)$. Thus, $\operatorname{card} F = \langle w \rangle$. For future reference, we now illustrate the definition of τ in this situation. For $a \in \mathbb{A} \setminus \{0\}$, since

$$\tau(a) = \log |a|_w / \log |w|_w,$$

$\tau(a)$ is the greatest integer τ for which w^τ divides a. For $\varphi(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{A}[x]$,

$$\tau(\varphi) = \min_{0 \le i \le n} \tau(a_i),$$

and

$$\operatorname{ind} \varphi = \max \big\{ j \;\big|\; 0 \le j \le n,\ \tau(a_j) = \tau(\varphi) \big\}.$$

On applying Lemmas 10, 11, and 12 to $R = \mathbb{A}_w$ and $|\cdot| = |\cdot|_w$, we obtain the following Lemmas 15 and 16.

Lemma 15. *Let $\varphi(x) \in \mathbb{A}[x] \setminus \{0\}$ be of degree n with $\tau(\varphi) = 0$ and $\varphi(0) = 0$. For $\lambda \in \mathbb{A}$, let*

$$\psi_\lambda(x) = \varphi(wx + \lambda) - \varphi(\lambda).$$

Suppose that $\varphi' \neq 0$. The following hold.
(1) $1 \le \tau(\psi_\lambda) \le n$ and $\tau(\psi'_\lambda) \le n + \tau(\varphi')$.
(2) $\operatorname{ind} \psi'_\lambda \le \operatorname{ind} \varphi'$. If $\operatorname{ind} \psi'_\lambda = \operatorname{ind} \varphi'$ and $\varphi'(\lambda_1) \equiv 0 \pmod{w^{\tau(\varphi')+1}}$, then $\lambda \equiv \lambda_1 \pmod{w}$.

Proof. (1) Since $\tau(\varphi) = 0$ and $\varphi(0) = 0$, we have $\operatorname{ind} \varphi > 0$ and it follows from Lemma 11(2) that $1 \le \tau(\psi_\lambda) \le n$. In view of Lemma 11(3), we see that $\tau(\psi'_\lambda) \le n + \tau(\varphi')$.

(2) The result follows from Lemmas 10(4) and 11(4) immediately. □

Lemma 16. *Let $\varphi(x) \in \mathbb{A}[x] \setminus \{0\}$ be of degree n. For $u, v \in \mathbb{N}$ with $u \geq v > n$, let*

$$N_{u,v}(\varphi) = \left\{ a \pmod{w^u} \,\middle|\, a \in \mathbb{A},\ \tau(\varphi(x)) \geq v + \tau(\varphi) \right\}.$$

Then

$$\operatorname{card} N_{u,v}(\varphi) \leq \langle w \rangle^{n+1+u-\frac{v}{n}}.$$

Proposition 17. *Let $\varphi(x) \in \mathbb{A}[x]$ be of degree n with $\tau(\varphi) = 0$ and $\varphi(0) = 0$. For $l \in \mathbb{N}$, define*

$$S\left(\frac{\varphi(x)}{w^l}\right) = \sum_{x \in I_{\operatorname{ord} w^l}} e\left(\frac{\varphi(x)}{w^l}\right).$$

Suppose that $\varphi' \neq 0$. Then for all $l \in \mathbb{N}$ with $l > 2\tau(\varphi') + 1$, we have

$$\left| S\left(\frac{\varphi(x)}{w^l}\right) \right| < n^n \langle w \rangle^{l(1-\frac{1}{2n})+\frac{\tau(\varphi')}{n}}. \tag{2.19}$$

Proof. For $\lambda \in \mathbb{A}$, define

$$\psi_\lambda(x) = \varphi(wx + \lambda) - \varphi(\lambda)$$

and define $g_\lambda(x) \in \mathbb{A}[x]$ by

$$\psi_\lambda(x) = w^{\tau_\lambda} g_\lambda(x)$$

where $\tau_\lambda = \tau(\psi_\lambda)$. We have

$$\deg g_\lambda = n, \quad g_\lambda(0) = 0, \quad \tau(g_\lambda) = 0, \quad g'_\lambda \neq 0.$$

By Lemma 15, we obtain

$$1 \leq \tau_\lambda \leq n, \quad \tau_\lambda + \tau(g'_\lambda) = \tau(\psi'_\lambda) \leq n + \tau(\varphi'). \tag{2.20}$$

Fix $l \in \mathbb{N}$ with $l > 2\tau(\varphi') + 1$. For $\lambda \in \mathbb{A}$, define

$$S_\lambda = \sum_{\substack{x \in I_{\operatorname{ord} w^l} \\ x \equiv \lambda \pmod{w}}} e\left(\frac{\varphi(x)}{w^l}\right).$$

Note that

$$\begin{aligned}|S_\lambda| &= \left| \sum_{\substack{x \in I_{\operatorname{ord} w^l} \\ x \equiv \lambda \,(\operatorname{mod} w)}} e\left(\frac{\varphi(x)}{w^l}\right) \right| \\ &= \left| \sum_{y \in I_{\operatorname{ord} w^{l-1}}} e\left(\frac{\varphi(wy+\lambda) - \varphi(\lambda)}{w^l}\right) \right| \\ &= \left| \sum_{y \in I_{\operatorname{ord} w^{l-1}}} e\left(\frac{w^{\tau_\lambda} g_\lambda(y)}{w^l}\right) \right|.\end{aligned}$$

If $l > n$, by (2.20), we have $l > \tau_\lambda$ and hence

$$|S_\lambda| = \langle w \rangle^{\tau_\lambda - 1} \left| \sum_{y \in I_{\operatorname{ord} w^{l-\tau_\lambda}}} e\left(\frac{g_\lambda(y)}{w^{l-\tau_\lambda}}\right) \right|. \tag{2.21}$$

If $l \leq n$, we have

$$|S_\lambda| \leq \langle w \rangle^{l-1}. \tag{2.22}$$

Next, we shall relate $S\left(\frac{\varphi(x)}{w^l}\right)$ to S_λ. For convenience, write $\sigma = \tau(\varphi')$. Since $l > 2\sigma + 1$, we have

$$\begin{aligned}S_\lambda &= \sum_{\substack{y \in I_{\operatorname{ord} w^{l-\sigma-1}} \\ y \equiv \lambda \,(\operatorname{mod} w)}} \sum_{z \in I_{\operatorname{ord} w^{\sigma+1}}} e\left(\frac{\varphi(y + w^{l-\sigma-1} z)}{w^l}\right) \\ &= \sum_{\substack{y \in I_{\operatorname{ord} w^{l-\sigma-1}} \\ y \equiv \lambda \,(\operatorname{mod} w)}} \sum_{z \in I_{\operatorname{ord} w^{\sigma+1}}} e\left(\frac{\varphi(y) + \varphi'(y) w^{l-\sigma-1} z}{w^l}\right) \\ &= \sum_{\substack{y \in I_{\operatorname{ord} w^{l-\sigma-1}} \\ y \equiv \lambda \,(\operatorname{mod} w)}} e\left(\frac{\varphi(y)}{w^l}\right) \sum_{z \in I_{\operatorname{ord} w^{\sigma+1}}} e\left(\frac{\varphi'(y) z}{w^{\sigma+1}}\right).\end{aligned}$$

If $\varphi'(\lambda) \not\equiv 0 \,(\operatorname{mod} w^{\sigma+1})$, for each $y \equiv \lambda \,(\operatorname{mod} w)$, we have

$$\varphi'(y) \equiv \varphi'(\lambda) \not\equiv 0 \,(\operatorname{mod} w^{\sigma+1}),$$

which gives that $S_\lambda = 0$ by Lemma 3. Let $\{\lambda_1, \ldots, \lambda_h\} \subseteq I_{\operatorname{ord} w}$ be a complete set of representatives of

$$\left\{ \lambda \,(\operatorname{mod} w) \,\middle|\, \varphi'(\lambda) \equiv 0 \,(\operatorname{mod} w^{\sigma+1}) \right\}.$$

Thus,

$$S\left(\frac{\varphi(x)}{w^l}\right) = \sum_{i=1}^{h} S_{\lambda_i}. \tag{2.23}$$

We consider two cases.

Case 1: Suppose that there exists some λ_i such that $\operatorname{ind}\psi'_{\lambda_i} = \operatorname{ind}\varphi'$. By Lemma 15, we have $\lambda_j \equiv \lambda_i \pmod{w}$ $(1 \le j \le h)$. Thus, $h = 1$ and (2.23) can be reduced to

$$S\left(\frac{\varphi(x)}{w^l}\right) = S_{\lambda_i}. \tag{2.24}$$

Case 2: Suppose that $\operatorname{ind}\psi'_{\lambda_i} < \operatorname{ind}\varphi'$ $(1 \le i \le h)$. Then

$$\operatorname{ind} g'_{\lambda_i} = \operatorname{ind}\psi'_{\lambda_i} < \operatorname{ind}\varphi' \ (1 \le i \le h). \tag{2.25}$$

Since there are at most $(n-1)$ different $\lambda \pmod{w}$ with $\varphi'(\lambda) \equiv 0 \pmod{w^{\sigma+1}}$, it follows from (2.23) that

$$\left|S\left(\frac{\varphi(x)}{w^l}\right)\right| \le n \max_{1\le i\le h} \left|S_{\lambda_i}\right|. \tag{2.26}$$

If $l \le n$, from (2.22), (2.24) and (2.26), it follows that

$$\left|S\left(\frac{\varphi(x)}{w^l}\right)\right| \le n\langle w\rangle^{l-1} \le n\langle w\rangle^{l(1-\frac{1}{n})}. \tag{2.27}$$

If $l > n$, on applying (2.21), (2.24) and (2.26), we can reduce $S\left(\frac{\varphi(x)}{w^l}\right)$ to a similar sum where the exponent of w is less than l. More precisely, suppose that this procedure is repeated m times and we obtain $S\left(\frac{g_i(x)}{w^{l_i}}\right)$ and τ_i $(1 \le i \le m)$ which satisfy the following properties as in (2.20):

$$\begin{aligned}
&\deg g_i = n,\ g_i(0) = 0,\ \tau(g_i) = 0,\ g'_i \ne 0,\\
&1 \le \tau_i \le n,\ \tau_i + \tau(g'_i) \le n + \tau(g'_{i-1}),\ l_i = l_{i-1} - \tau_i,\\
&l_j > \max\{2\tau(g'_j) + 1,\ n\}\ (0 \le j < m),\ l_m \le \max\{2\tau(g'_m) + 1,\ n\},
\end{aligned} \tag{2.28}$$

where $g_0 = \varphi$ and $l_0 = l$. Note that Case 2 occurs less than n times because of the inequality (2.25). Therefore, from (2.21), (2.24) and (2.26), we have

$$\left|S\left(\frac{\varphi(x)}{w^l}\right)\right| \le n^{n-1}\langle w\rangle^{\tau_1+\cdots+\tau_m-m}\left|S\left(\frac{g_m(x)}{w^{l_m}}\right)\right|. \tag{2.29}$$

We now consider the situation when $l_m \leq 2\tau(g'_m) + 1$. By (2.28), we have

$$l - \tau_1 - \cdots - \tau_m = l_m \leq 2\tau(g'_m) + 1,$$

i.e.,

$$\tau_1 + \cdots + \tau_m + 2\tau(g'_m) \geq l - 1. \tag{2.30}$$

Furthermore, since $\tau_i + \tau(g'_i) \leq n + \tau(g'_{i-1})$, we deduce that

$$\tau_1 + \cdots + \tau_m + \tau(g'_m) \leq mn + \tau(\varphi'). \tag{2.31}$$

On combining (2.28), (2.30) with (2.31), we find that

$$2mn + 2\tau(\varphi') \geq 2(\tau_1 + \cdots + \tau_m) + 2\tau(g'_m) \geq 1 + l - 1 = l.$$

Thus,

$$m \geq \frac{l}{2n} - \frac{\tau(\varphi')}{n}.$$

Then by estimating $S\Big(\frac{g_m(x)}{w^{l_m}}\Big)$ trivially, from (2.29) and the above inequality, we see that

$$\begin{aligned} \left|S\left(\frac{\varphi(x)}{w^l}\right)\right| &\leq n^{n-1}\langle w\rangle^{\tau_1+\cdots+\tau_m-m+l_m} = n^{n-1}\langle w\rangle^{l-m} \\ &< n^n\langle w\rangle^{l(1-\frac{1}{2n})+\frac{\tau(\varphi')}{n}}. \end{aligned} \tag{2.32}$$

It remains to treat the case when $2\tau(g'_m) + 1 < l_m \leq n$. On applying (2.27) to $S\Big(\frac{g_m(x)}{w^{l_m}}\Big)$, we have

$$\left|S\left(\frac{g_m(x)}{w^{l_m}}\right)\right| \leq n\langle w\rangle^{l_m-1}. \tag{2.33}$$

Since $1 \leq \tau_i \leq n$, we have $l - l_m = \tau_1 + \cdots + \tau_m \leq mn$. Thus,

$$\frac{l-n}{n} \leq \frac{l-l_m}{n} \leq m, \quad \text{i.e.,} \quad \frac{l}{n} \leq m + 1.$$

From (2.29), (2.33) and the above inequality, it follows that

$$\left|S\left(\frac{\varphi(x)}{w^l}\right)\right| \leq n^n\langle w\rangle^{\tau_1+\cdots+\tau_m-m+l_m-1} = n^n\langle w\rangle^{l-m-1} \leq n^n\langle w\rangle^{l(1-\frac{1}{n})}. \tag{2.34}$$

By combining (2.27) with (2.32) and (2.34), the proposition follows. □

We are now ready to estimate the exponential sums when $\langle w\rangle$ is small.

Corollary 18. *Under the conditions of the above lemma, if $\langle w\rangle \leq n$, then for $l \in \mathbb{N}\setminus\{0\}$, we have*

$$\left|S\left(\frac{\varphi(x)}{w^l}\right)\right| < n^n \langle w\rangle^{l(1-\frac{1}{2n})+\frac{\tau(\varphi')}{n}}.$$

Proof. From Proposition 17, it follows that the result is true for all $l > 2\tau(\varphi')+1$. When $1 \leq l \leq 2\tau(\varphi')+1$, we have

$$\left|S\left(\frac{\varphi(x)}{w^l}\right)\right| \leq \langle w\rangle^l = \langle w\rangle^{l(1-\frac{1}{2n})+\frac{l}{2n}} < n^n \langle w\rangle^{l(1-\frac{1}{2n})+\frac{\tau(\varphi')}{n}}.$$

This completes the proof of the corollary. □

Lemma 19. *Let $n \in \mathbb{N}\setminus\{0\}$. For each d-tuple $(i_1,\ldots,i_d)$ with $0 \leq i_1,\ldots,i_d \leq n$, let $a_{i_1,\ldots,i_d} \in \mathbb{A}$. Define*

$$F(\mathbf{x}) = \sum_{0\leq i_1,\ldots,i_d\leq n} a_{i_1,\ldots,i_d} x_1^{i_1}\cdots x_d^{i_d},$$
$$\tau(F) = \min\{\tau(a_{i_1,\ldots,i_d}) \,|\, 0 \leq i_1,\ldots,i_d \leq n\},$$

and

$$S\left(\frac{F(\mathbf{x})}{w^l}\right) = \sum_{\mathbf{x}\in I^d_{\mathrm{ord}\, w^l}} e\left(\frac{F(\mathbf{x})}{w^l}\right).$$

Suppose that $\tau(F) = 0$ and that there exists some nonzero $a_{\mathbf{j}}$ with $p \nmid \mathbf{j}$. Let $\tau_{\mathbf{j}} = \tau(a_{\mathbf{j}})$. If $\langle w\rangle \leq n$, then for all $l \geq 1$, we have

$$\left|S\left(\frac{F(\mathbf{x})}{w^l}\right)\right| < l^{d-1} n^{(n+1)d} \langle w\rangle^{l(d-\frac{1}{2n})+\frac{\tau_{\mathbf{j}}}{n}}. \tag{2.35}$$

Proof. We will prove this lemma by induction on d. For $d = 1$, if there exists a nonzero a_j with $p \nmid j$, then $F'(x) \neq 0$ and $\tau(F') \leq \tau_j$. By Corollary 18, we have for all $l \geq 1$,

$$\left|S\left(\frac{F(x)}{w^l}\right)\right| = \left|S\left(\frac{F(x)-F(0)}{w^l}\right)\right| < n^n \langle w\rangle^{l(1-\frac{1}{2n})+\frac{\tau(F')}{n}} \leq n^n \langle w\rangle^{l(1-\frac{1}{2n})+\frac{\tau_j}{n}}.$$

Suppose that the lemma holds for $d-1$ variables and for any $l \geq 1$. Consider the case of d variables. If $l \leq \tau_{\mathbf{j}} + n + 1$, since $\langle w \rangle \leq n$, we have

$$\begin{aligned} \left| S\Big(\frac{F(\mathbf{x})}{w^l} \Big) \right| &\leq \langle w \rangle^{ld} = \langle w \rangle^{l(d-\frac{1}{2n})+\frac{l}{2n}} \\ &\leq n \langle w \rangle^{l(d-\frac{1}{2n})+\frac{\tau_{\mathbf{j}}}{2n}} \\ &< l^{d-1} \cdot n^{(n+1)d} \cdot \langle w \rangle^{l(d-\frac{1}{2n})+\frac{\tau_{\mathbf{j}}}{n}}. \end{aligned} \tag{2.36}$$

It remains to consider the case when $l > \tau_{\mathbf{j}} + n + 1$. Write $\mathbf{j} = (j_1, \dots, j_d)$. Without loss of generality, assume that $w \nmid a_{\mathbf{j}}$ and $p \nmid j_1$. Define

$$\varphi_{i_1,\dots,i_{d-1}}(x_d) = \sum_{i_d=0}^{n} a_{i_1,\dots,i_d} x_d^{i_d} \quad (0 \leq i_1, \dots, i_{d-1} \leq n),$$

and

$$S(x_d) = \left| \sum_{x_1,\dots,x_{d-1} \in I_{\operatorname{ord} w^l}} e\Big(\frac{F(x_1, \dots, x_{d-1}, x_d)}{w^l} \Big) \right|.$$

For each $u \in \mathbb{N}$, write

$$N_u = \big\{ x_d \in I_{\operatorname{ord} w^l} \;\big|\; \tau\big(\varphi_{j_1,\dots,j_{d-1}}(x_d)\big) = u \big\},$$

and

$$S_u = \sum_{x_d \in N_u} S(x_d). \tag{2.37}$$

Let

$$\Gamma_1 = \sum_{u \leq \tau_{\mathbf{j}} + n} S_u, \quad \Gamma_2 = \sum_{\tau_{\mathbf{j}} + n < u < l} S_u, \quad \text{and} \quad \Gamma_3 = \sum_{u \geq l} S_u.$$

Then

$$\left| S\Big(\frac{F(\mathbf{x})}{w^l} \Big) \right| \leq \Gamma_1 + \Gamma_2 + \Gamma_3. \tag{2.38}$$

For $x_d \in I_{\operatorname{ord} w^l}$, let

$$\mu(x_d) = \min \big\{ \tau\big(\varphi_{i_1,\dots,i_{d-1}}(x_d)\big) \;\big|\; 0 \leq i_1, \dots, i_{d-1} \leq n \big\}.$$

Thus,

$$\begin{aligned} S(x_d) &= \left| \sum_{x_1,\dots,x_{d-1} \in I_{\operatorname{ord} w^l}} e\Big(\frac{w^{-\mu(x_d)} F(x_1, \dots, x_{d-1}, x_d)}{w^{l-\mu(x_d)}} \Big) \right| \\ &= \left| \sum_{x_1,\dots,x_{d-1} \in I_{\operatorname{ord} w^l}} e\left(\frac{\sum_{0 \leq i_1,\dots,i_{d-1} \leq n} x_1^{i_1} \cdots x_{d-1}^{i_{d-1}} \big(w^{-\mu(x_d)} \varphi_{i_1,\dots,i_{d-1}}(x_d) \big)}{w^{l-\mu(x_d)}} \right) \right|. \end{aligned}$$

If $x_d \in N_u$ with $0 \le u \le l-1$, then $0 \le \mu(x_d) \le u$ and

$$\tau\Big(w^{-\mu(x_d)}\varphi_{j_1,\dots,j_{d-1}}(x_d)\Big) = u - \mu(x_d).$$

By the induction hypothesis, we have

$$\begin{aligned} S(x_d) &\le (l-\mu(x_d))^{d-2} \cdot n^{(d-1)(n+1)} \cdot \langle w\rangle^{(l-\mu(x_d))(d-1-\frac{1}{2n})+\frac{u-\mu(x_d)}{n}} \\ &\le l^{d-2} \cdot n^{(d-1)(n+1)} \cdot \langle w\rangle^{l(d-1-\frac{1}{2n})+\frac{u}{n}}. \end{aligned} \tag{2.39}$$

For each u with $0 \le u \le \tau_{\mathbf{j}} + n$, since $\operatorname{card} N_u \le \langle w\rangle^l$ and $\langle w\rangle \le n$, by (2.39) we have

$$\begin{aligned} \Gamma_1 = \sum_{u=0}^{\tau_{\mathbf{j}}+n} S_u &\le \sum_{u=0}^{\tau_{\mathbf{j}}+n} l^{d-2} \cdot n^{(d-1)(n+1)} \cdot \langle w\rangle^{l(d-1-\frac{1}{2n})+\frac{u}{n}} \cdot \langle w\rangle^l \\ &\le (\tau_{\mathbf{j}} + n + 1) \cdot l^{d-2} \cdot n^{d(n+1)} \cdot \langle w\rangle^{l(d-\frac{1}{2n})+\frac{\tau_{\mathbf{j}}}{n}}. \end{aligned} \tag{2.40}$$

For each u with $\tau_{\mathbf{j}} + n < u \le l-1$, since $\tau(\varphi_{j_1,\dots,j_{d-1}}) \le \tau(a_{\mathbf{i}}) = \tau_{\mathbf{j}}$, we have

$$u - \tau(\varphi_{j_1,\dots,j_{d-1}}) \ge u - \tau_{\mathbf{j}} > n. \tag{2.41}$$

Noticing that

$$N_u \subseteq \big\{x_d \in I_{\operatorname{ord} w^l} \big| \, \tau\big(\varphi_{j_1,\dots,j_{d-1}}(x_d)\big) \ge u\big\},$$

we deduce from Lemma 16 and (2.41) that

$$\operatorname{card} N_u \le \langle w\rangle^{n+1+l-\frac{u-\tau_{\mathbf{j}}}{n}} \le n^{n+1} \cdot \langle w\rangle^{l-\frac{u}{n}+\frac{\tau_{\mathbf{j}}}{n}}. \tag{2.42}$$

It follows from (2.37),(2.39), and (2.42) that

$$\begin{aligned} \Gamma_2 = \sum_{u=\tau_{\mathbf{j}}+n+1}^{l-1} S_u &\le \sum_{u=\tau_{\mathbf{j}}+n+1}^{l-1} l^{d-2} \cdot n^{(d-1)(n+1)} \cdot \langle w\rangle^{l(d-1-\frac{1}{2n})+\frac{u}{n}} \cdot n^{n+1} \cdot \langle w\rangle^{l-\frac{u}{n}+\frac{\tau_{\mathbf{j}}}{n}} \\ &\le (l-2-\tau_{\mathbf{j}}-n) \cdot l^{d-2} \cdot n^{d(n+1)} \cdot \langle w\rangle^{l(d-\frac{1}{2n})+\frac{\tau_{\mathbf{j}}}{n}}. \end{aligned} \tag{2.43}$$

Recalling that $\tau(\varphi_{j_1,\dots,j_{d-1}}) \le \tau_{\mathbf{j}}$, we find that

$$\bigcup_{u\ge l} N_u \subseteq \big\{x_d \in I_{\operatorname{ord} w^l} \big| \, \tau(\varphi_{j_1,\dots,j_{d-1}}) \ge (l-\tau_{\mathbf{i}}) + \tau(\varphi_{j_1,\dots,j_{d-1}})\big\}.$$

Since $l - \tau_{\mathbf{j}} > n+1$, it follows from Lemma 16 that

$$\operatorname{card} \bigcup_{u\ge l} N_u \le n^{n+1}\langle w\rangle^{l-\frac{l}{n}+\frac{\tau_{\mathbf{j}}}{n}}.$$

Observing that $S(x_d) \le \langle w\rangle^{l(d-1)}$, we have

$$\Gamma_3 \le \langle w\rangle^{l(d-1)} \cdot n^{n+1}\langle w\rangle^{l-\frac{l}{n}+\frac{\tau_{\mathbf{j}}}{n}} < l^{d-2}n^{d(n+1)}\langle w\rangle^{l(d-\frac{1}{2n})+\frac{\tau_{\mathbf{j}}}{n}}. \tag{2.44}$$

Therefore, by (2.38), (2.40), (2.43) and (2.44), we have

$$\left|S\left(\frac{F(\mathbf{x})}{w^l}\right)\right| \le \Gamma_1+\Gamma_2+\Gamma_3 \le l^{d-1}n^{d(n+1)}\langle w\rangle^{l(d-\frac{1}{2n})+\frac{\tau_{\mathbf{j}}}{n}}.$$

Thus, the lemma holds by induction. □

To estimate the exponential sums where $\langle w\rangle$ is large, we need to establish some technical lemmas.

Lemma 20. *Let $\varphi(x) = a_nx^n+\cdots+a_1x+a_0 \in \mathbb{A}[x]$ with $w \nmid a_n$ and $p \nmid n$. Let $S\left(\frac{\varphi(x)}{w^l}\right)$ be defined as in Proposition 17. Then for all $l \ge 1$, we have*

$$\left|S\left(\frac{\varphi(\mathbf{x})}{w^l}\right)\right| < n^n\langle w\rangle^{l(1-\frac{1}{2n})}. \tag{2.45}$$

Proof. Since $w \nmid a_n$ and $p \nmid n$, we have $\varphi' \neq 0$ and $\tau(\varphi) = \tau(\varphi') = 0$. It follows from Proposition 17 that for all $l \ge 2$,

$$\left|S\left(\frac{\varphi(\mathbf{x})}{w^l}\right)\right| = \left|S\left(\frac{\varphi(x)-\varphi(0)}{w^l}\right)\right| < n^n\langle w\rangle^{l(1-\frac{1}{2n})}. \tag{2.46}$$

It remains to show that the lemma holds for $l = 1$. Let $\mathbf{x} = (x_1,\dots,x_n)$ and $\mathbf{y} = (y_1,\dots,y_n)$. For each $1 \le j \le n$, write

$$X_j = x_1^j+\cdots+x_n^j \quad \text{and} \quad Y_j = y_1^j+\cdots+y_n^j.$$

We have

$$\begin{aligned}
&\sum_{b_1,\dots,b_n \,(\mathrm{mod}\, w)}\left|\sum_{x\,(\mathrm{mod}\,w)} e\left(\frac{b_nx^n+\cdots+b_1x}{w}\right)\right|^{2n}\\
=&\sum_{\mathbf{b},\mathbf{x},\mathbf{y}\,(\mathrm{mod}\,w)} e\left(\frac{b_n(X_n-Y_n)+\cdots+b_1(X_1-Y_1)}{w}\right)\\
=&\sum_{\mathbf{x},\mathbf{y}\,(\mathrm{mod}\,w)}\prod_{j=1}^{n}\left(\sum_{b_j\,(\mathrm{mod}\,w)} e\left(\frac{b_j(X_j-Y_j)}{w}\right)\right)\\
=&\langle w\rangle^n N,
\end{aligned} \tag{2.47}$$

where $N = \operatorname{card}\big\{(\mathbf{x},\mathbf{y}) \,(\mathrm{mod}\, w)\big|\, X_j \equiv Y_j \,(\mathrm{mod}\, w)\,(1 \le j \le n)\big\}$. By Newton's formula, every $(\mathbf{x},\mathbf{y})\,(\mathrm{mod}\, w)$ counted by N must satisfy

$$(x - x_1)\cdots(x - x_n) \equiv (x - y_1)\cdots(x - y_n) \,(\mathrm{mod}\, w).$$

Thus,

$$N \le n!\langle w\rangle^n. \tag{2.48}$$

Fix $\bar{b} \in \mathbb{A}$. For any $b \in \mathbb{A}$, $\varphi(bx) \equiv \varphi(\bar{b}x)\,(\mathrm{mod}\, w)$ must imply that $b^n a_n \equiv \bar{b}^n a_n \,(\mathrm{mod}\, w)$. Since $w \nmid a_n, w$, there are at most n choices for $b(\mathrm{mod}\, w)$ such that $\varphi(bx) \equiv \varphi(\bar{b}x)\,(\mathrm{mod}\, w)$. Thus, for $b_1, \ldots, b_n \in \mathbb{A}$,

$$\operatorname{card}\big\{b(\mathrm{mod}\, w) \,\big|\, \varphi(bx) \equiv b_n x^n + \cdots + b_1 x_1 \,(\mathrm{mod}\, w)\big\} \le n.$$

Hence,

$$\frac{1}{n} \sum_{\substack{b \in I_{\mathrm{ord}\, w} \\ b \not\equiv 0 \,(\mathrm{mod}\, w)}} \left| S\Big(\frac{\varphi(bx)}{w}\Big)\right|^{2n} \le \sum_{b_1,\ldots,b_n \,(\mathrm{mod}\, w)} \left| \sum_{x \,(\mathrm{mod}\, w)} e\Big(\frac{b_n x^n + \cdots + b_1 x}{w}\Big)\right|^{2n}. \tag{2.49}$$

Note that if $\gcd(b, w) = 1$, then

$$S\Big(\frac{\varphi(bx)}{w}\Big) = S\Big(\frac{\varphi(x)}{w}\Big).$$

We deduce from (2.47), (2.48), and (2.49) that

$$\frac{\langle w\rangle - 1}{n}\left| S\Big(\frac{\varphi(x)}{w}\Big)\right|^{2n} \le n!\langle w\rangle^{2n}.$$

Therefore,

$$\left| S\Big(\frac{\varphi(x)}{w}\Big)\right| \le n\langle w\rangle^{1-\frac{1}{2n}}.$$

This completes the proof of the lemma. □

Lemma 21. *Let $n \in \mathbb{N}$ with $p \nmid n$. For each $\mathbf{i} \in \mathbb{N}^d$ with $|\mathbf{i}| \le n$, let $a_{\mathbf{i}} \in \mathbb{A}$ with $\gcd(a_{(n,0,\ldots,0)}, w) = 1$. Define*

$$F(\mathbf{x}) = \sum_{\mathbf{i}\in\mathbb{N}^d,\, |\mathbf{i}|\le n} a_{\mathbf{i}}\mathbf{x}^{\mathbf{i}} \quad \text{and} \quad S\Big(\frac{F(\mathbf{x})}{w^l}\Big) = \sum_{\mathbf{x}\in I^d_{\mathrm{ord}\, w^l}} e\Big(\frac{F(\mathbf{x})}{w^l}\Big).$$

Then for all $l \ge 1$, we have

$$\left| S\Big(\frac{F(\mathbf{x})}{w^l}\Big)\right| < n^n\langle w\rangle^{l(d-\frac{1}{2n})}.$$

Proof. Fix any choice of $(x_2, \ldots, x_d)$. Then

$$\sum_{\mathbf{i}\in\mathbb{N}^d,\, |\mathbf{i}|\le n} a_{\mathbf{i}}\mathbf{x}^{\mathbf{i}} = a_{(n,0,\ldots,0)}x_1^n + \sum_{|\mathbf{i}|\le n,\, i_1<n} a_{\mathbf{i}}\mathbf{x}^{\mathbf{i}}$$

is a polynomial in terms of x_1. By Lemma 20, we can obtain that for all $l \ge 1$

$$\left| S\left(\frac{a_{(n,0,\ldots,0)}x_1^n + \sum_{|\mathbf{i}|\le n,\, i_1<n} a_{\mathbf{i}}\mathbf{x}^{\mathbf{i}}}{w^l} \right) \right| < n^n \langle w \rangle^{l(1-\frac{1}{2n})}.$$

Thus,

$$\begin{aligned} \left| S\left(\frac{F(\mathbf{x})}{w^l}\right) \right| &\le \sum_{x_2,\ldots,x_d \in I_{\mathrm{ord}\, w^l}} \left| \sum_{x_1 \in I_{\mathrm{ord}\, w^l}} e\left(\frac{F(\mathbf{x})}{w^l}\right) \right| \\ &\le \langle w \rangle^{l(d-1)} \cdot n^n \cdot \langle w \rangle^{l(1-\frac{1}{2n})} \\ &= n^n \langle w \rangle^{l(d-\frac{1}{2n})}. \end{aligned}$$

This completes the proof of the lemma. □

Lemma 22. *For each* $\mathbf{i} \in \mathbb{N}^d$ *with* $|\mathbf{i}| \le n$, *let* $a_{\mathbf{i}} \in \mathbb{A}$. *Define*

$$G(\mathbf{x}) = \sum_{\mathbf{i}\in\mathbb{N}^d,\, |\mathbf{i}|\le n} a_{\mathbf{i}}\mathbf{x}^{\mathbf{i}} \quad \text{and} \quad S\left(\frac{G(\mathbf{x})}{w^l}\right) = \sum_{\mathbf{x}\in I^d_{\mathrm{ord}\, w^l}} e\left(\frac{G(\mathbf{x})}{w^l}\right).$$

Suppose that $\gcd(\mathbf{a}, w) = 1$ *and* $\langle w \rangle > n$. *Then there exists* $(f_1, \ldots, f_d) \in \mathbb{A}^d$ *such that*

$$w \nmid G(f_1, \ldots, f_d).$$

Proof. We will prove this lemma by induction on d. When $d = 1$, since $\gcd(\mathbf{a}, w) = 1$, we may consider $G(x)$ as a nonzero polynomial in $\mathbb{A}/(w)[x]$. Suppose that for each $f \in \mathbb{A}/(w)$, $G(f) = 0$. Then $x^{\langle w \rangle} - x \mid G(x)$ in $\mathbb{A}/(w)[x]$. Thus $n \ge \deg G(x) \ge \langle w \rangle$, contradicting $\langle w \rangle > n$. Therefore, there must exist some $f \in \mathbb{A}$ satisfying $w \nmid G(f)$.
Assume that the lemma is true for $d - 1$. Now we prove that the statement holds for d. Since $\gcd(\mathbf{a}, w) = 1$, there exists some $\mathbf{j}$ such that $\gcd(a_{\mathbf{j}}, w) = 1$. Let

$$\mathcal{I} = \left\{ \mathbf{i} \in \mathbb{N}^d \,\middle|\, |\mathbf{i}| \le n, (i_2, \ldots, i_d) \ne (j_2, \ldots, j_d) \right\}.$$

Hence

$$G(\mathbf{x}) = g(x_1)x_2^{j_2} \cdots x_d^{j_d} + \sum_{\mathbf{i}\in\mathcal{I}} a_{\mathbf{i}}\mathbf{x}^{\mathbf{i}},$$

where

$$g(x_1) = \sum_{i_1=0}^{n-j_2-\cdots-j_d} a_{i_1,j_2,\ldots,j_d} x_1^{i_1}.$$

Since $\gcd(a_{\mathbf{j}}, w) = 1$ and $\langle w \rangle > n \geq n - j_2 - \cdots - j_d$, by applying the result in the case when $d = 1$ to $g(x_1)$, we have that $w \nmid g(f_1)$ for some $f_1 \in \mathbb{A}$. Then

$$G(f_1, x_2, \ldots, x_d) = g(f_1) x_2^{j_2} \cdots x_d^{j_d} + \sum_{\mathbf{i} \in \mathcal{I}} (a_{\mathbf{i}} f_1^{i_1}) x_2^{i_2} \cdots x_d^{i_d}.$$

By the induction hypothesis, there exists $(f_2, \ldots, f_d) \in \mathbb{A}^{d-1}$ such that

$$w \nmid G(f_1, f_2, \ldots, f_d).$$

By induction, the lemma follows. □

Lemma 23. *For each* $\mathbf{i} \in \mathbb{N}^d$ *with* $|\mathbf{i}| = n$, *let* $a_{\mathbf{i}} \in \mathbb{A}$. *Define*

$$G(\mathbf{x}) = \sum_{\mathbf{i} \in \mathbb{N}^d,\, |\mathbf{i}| = n} a_{\mathbf{i}} \mathbf{x}^{\mathbf{i}} \quad \text{and} \quad S\left(\frac{G(\mathbf{x})}{w^l}\right) = \sum_{\mathbf{x} \in I^d_{\operatorname{ord} w^l}} e\left(\frac{G(\mathbf{x})}{w^l}\right).$$

Suppose that $\gcd(\mathbf{a}, w) = 1$ *and* $\langle w \rangle > n$. *Then there exists*

$$F(\mathbf{x}) = \sum_{\mathbf{i} \in \mathbb{N}^d,\, |\mathbf{i}| \leq n} b_{\mathbf{i}} \mathbf{x}^{\mathbf{i}}$$

with $b_{\mathbf{i}} \in \mathbb{A}$ *and* $\gcd(b_{(n,0,\ldots,0)}, w) = 1$ *such that for all* $l \geq 1$,

$$S\left(\frac{G(\mathbf{x})}{w^l}\right) = S\left(\frac{F(\mathbf{x})}{w^l}\right),$$

where $S\left(\frac{F(\mathbf{x})}{w^l}\right)$ *is defined as in Lemma 21.*

Proof. From Lemma 22, it follows that there exists $(f_1, \ldots, f_d) \in \mathbb{A}^d$ such that

$$w \nmid G(f_1, \ldots, f_d).$$

Suppose that $w \mid f_i$ for each $1 \leq i \leq d$. Since every monomial in $G(\mathbf{x})$ has total degree n, $w \mid G(f_1, \ldots, f_d)$. This is a contradiction. Thus, without loss of generality, we assume that $w \nmid f_1$. For each $1 \leq i, j \leq d$, define $f_{i,j}$ by the following rule:

$$f_{i,j} = \begin{cases} f_i, & \text{if } j = 1, \\ 1, & \text{if } i = j \geq 2, \\ 0, & \text{if } i \neq j \text{ and } j \geq 2. \end{cases}$$

Hence the matrix $\big(f_{i,j}\big) = \big(f_{i,j}\big)_{1\le i,j\le d}$ has determinant f_1, which is a unit in $\mathbb{A}/(w^l)$ because $w \nmid f_1$. Thus, the matrix $\big(f_{i,j}\big)$ is invertible over $\mathbb{A}/(w^l)$. Therefore, we have a bijection from $\big(\mathbb{A}/(w^l)\big)^d$ to $\big(\mathbb{A}/(w^l)\big)^d$, defined by

$$\mathbf{x} \mapsto (f_1x_1, f_2x_1 + x_2, \dots, f_dx_1 + x_d) = \big(f_{i,j}\big)\mathbf{x}.$$

Hence

$$S\bigg(\frac{G(\mathbf{x})}{w^l}\bigg) = S\bigg(\frac{G\big(\big(f_{i,j}\big)\mathbf{x}\big)}{w^l}\bigg).$$

Let

$$F(\mathbf{x}) = G\big(\big(f_{i,j}\big)\mathbf{x}\big) = \sum_{\mathbf{i}\in\mathbb{N}^d,\,|\mathbf{i}|\le n} b_{\mathbf{i}}\mathbf{x}^{\mathbf{i}}.$$

It remains to show that $w \nmid b_{(n,0,\dots,0)}$. Since

$$\begin{aligned} F(x_1, x_2, \dots, x_d) &= G(f_1x_1, f_2x_1 + x_2, \dots, f_dx_1 + x_d) \\ &= \sum_{\mathbf{i}\in\mathbb{N}^d,\,|\mathbf{i}|=n} a_{\mathbf{i}}(f_1x_1)^{i_1}(f_2x_1 + x_2)^{i_2}\cdots(f_dx_1 + x_d)^{i_d}, \end{aligned}$$

we have

$$\begin{aligned} F(x_1, 0, \dots, 0) &= G(f_1x_1, f_2x_1, \dots, f_dx_1) \\ &= \sum_{\mathbf{i}\in\mathbb{N}^d,\,|\mathbf{i}|=n} a_{\mathbf{i}}(f_1x_1)^{i_1}(f_2x_1)^{i_2}\cdots(f_dx_1)^{i_d} \\ &= \bigg(\sum_{\mathbf{i}\in\mathbb{N}^d,\,|\mathbf{i}|=n} a_{\mathbf{i}}f_1^{i_1}f_2^{i_2}\cdots f_d^{i_d}\bigg)x_1^n \\ &= G(f_1, f_2, \dots, f_d)x_1^n. \end{aligned}$$

Thus, $w \nmid G(f_1, \dots, f_d) = b_{(n,0,\dots,0)}$. This completes the proof of the lemma. □

Lemma 24. *For each* $\mathbf{i} \in \mathbb{N}^d$, $|\mathbf{i}| = k$, *let* $a_{\mathbf{i}} \in \mathbb{A}$. *Define*

$$G(\mathbf{x}) = \sum_{\mathbf{i}\in\mathbb{N}^d,\,|\mathbf{i}|=k} a_{\mathbf{i}}\mathbf{x}^{\mathbf{i}} \quad\text{and}\quad S\bigg(\frac{G(\mathbf{x})}{w^l}\bigg) = \sum_{\mathbf{x}\in I^d_{\operatorname{ord} w^l}} e\bigg(\frac{G(\mathbf{x})}{w^l}\bigg).$$

Suppose that $\gcd(\mathbf{a}, w) = 1$. *Then for all* $l \ge 1$,

$$\bigg|S\bigg(\frac{G(\mathbf{x})}{w^l}\bigg)\bigg| \le k^{(k+1)d}l^{d-1}\langle w\rangle^{l(d-\frac{1}{2k})}.$$

Proof. Since $\gcd(\mathbf{a}, w) = 1$, there exists $a_{\mathbf{j}}$ such that $(a_{\mathbf{j}}, w) = 1$ and then $\tau(a_{\mathbf{j}}) = 0$. Since $|\mathbf{j}| = k$ and $p \nmid k$, we have $p \nmid \mathbf{j}$. When $\langle w \rangle \leq k$, from Lemma 19, it follows that for all $l \geq 1$,

$$\left| S\left(\frac{G(\mathbf{x})}{w^l} \right) \right| < k^{(k+1)d} l^{d-1} \langle w \rangle^{l(d-\frac{1}{2k})}.$$

On the other hand, when $\langle w \rangle > k$, by Lemmas 21, 22, and 23, we have that for all $l \geq 1$,

$$\left| S\left(\frac{G(\mathbf{x})}{w^l} \right) \right| < k^{(k+1)d} l^{d-1} \langle w \rangle^{l(d-\frac{1}{2k})}.$$

This completes the proof of the lemma. □

Lemma 25. *For each $\mathbf{i} \in \mathbb{N}^d$, $|\mathbf{i}| = k$, let $a_{\mathbf{i}} \in \mathbb{A}$. Suppose that $g \in \mathbb{A}$ is monic and that* $\gcd(\mathbf{a}, g) = 1$. *Define*

$$G(\mathbf{x}) = \sum_{\mathbf{i} \in \mathbb{N}^d,\, |\mathbf{i}| = k} a_{\mathbf{i}} \mathbf{x}^{\mathbf{i}} \quad \text{and} \quad S\left(\frac{G(\mathbf{x})}{g} \right) = \sum_{\mathbf{x} \in I^d_{\operatorname{ord} g}} e\left(\frac{G(\mathbf{x})}{g} \right).$$

Then

$$\left| S\left(\frac{G(\mathbf{x})}{g} \right) \right| \leq k^{(k+1)d\nu(g)} \Omega(g)^{d-1} \langle g \rangle^{d-\frac{1}{2k}},$$

where $\nu(g)$ is the number of distinct monic irreducible divisors of g and $\Omega(g)$ is the number of distinct monic divisors of g.

Proof. Let $g = w_1^{l_1} \cdots w_m^{l_m}$ be the canonical factorization of g into monic irreducible powers. Then $m = \nu(g)$ and $(1 + l_1) \cdots (1 + l_m) = \Omega(g)$. For each j with $1 \leq j \leq m$, let

$$g_j = g w_j^{-l_j}$$

and

$$G_j(\mathbf{x}) = g_j^{k-1} G(\mathbf{x}).$$

Since $\gcd(g_j^{k-1}\mathbf{a}, w_j) = 1$, it follows from Lemma 24 that

$$\left| S\left(\frac{G_j(\mathbf{x})}{w_j^{l_j}} \right) \right| < k^{(k+1)d} l_j^{d-1} \langle w_j \rangle^{l_j(d-\frac{1}{2k})}. \tag{2.50}$$

For each integer pair (i,j) with $1 \le i \le d$ and $1 \le j \le m$, if $y_{i,j}$ runs through a complete set of residues $\bmod w_j^{l_j}$, then $x_i = g_1 y_{i,1} + \cdots + g_m y_{i,m}$ runs through a complete set of residues $\bmod g$. Moreover, we have

$$\begin{aligned} & G(g_1\mathbf{y}_1 + \cdots + g_m\mathbf{y}_m) \\ =& \sum_{|\mathbf{i}|=k} a_{\mathbf{i}}(g_1 y_{1,1} + \cdots + g_m y_{1,m})^{i_1} \cdots (g_1 y_{d,1} + \cdots + g_m y_{d,m})^{i_d} \\ \equiv& \sum_{j=1}^{m} \sum_{|\mathbf{i}|=k} a_{\mathbf{i}} g_j^k y_{1,j}^{i_1} \cdots y_{d,j}^{i_d} \pmod g \\ \equiv& \sum_{j=1}^{m} g_j G_j(\mathbf{y}_j) \pmod g. \end{aligned} \tag{2.51}$$

From (2.51), we see that

$$\begin{aligned} S\Big(\frac{G(\mathbf{x})}{g}\Big) &= \sum_{\mathbf{x} \,(\mathrm{mod}\, g)} e\Big(\frac{G(\mathbf{x})}{g}\Big) \\ &= \sum_{\mathbf{y}_1 \,(\mathrm{mod}\, w_1^{l_1})} \cdots \sum_{\mathbf{y}_m \,(\mathrm{mod}\, w_m^{l_m})} e\Big(\frac{G(g_1\mathbf{y}_1 + \cdots + g_m\mathbf{y}_m)}{g}\Big) \\ &= \sum_{\mathbf{y}_1 \,(\mathrm{mod}\, w_1^{l_1})} \cdots \sum_{\mathbf{y}_m \,(\mathrm{mod}\, w_m^{l_m})} e\Big(\frac{g_1 G_1(\mathbf{y}_1) + \cdots + g_m G_m(\mathbf{y}_m)}{g}\Big) \\ &= \prod_{j=1}^{m} \Bigg(\sum_{\mathbf{y}_j \,(\mathrm{mod}\, w_j^{l_j})} e\Big(\frac{g_j G_j(\mathbf{y}_j)}{g}\Big) \Bigg) \\ &= \prod_{j=1}^{m} S\Big(\frac{G_j(\mathbf{x})}{w_j^{l_j}}\Big). \end{aligned}$$

Therefore, by (2.50), we have

$$\begin{aligned} \Big|S\Big(\frac{G(\mathbf{x})}{g}\Big)\Big| &= \prod_{j=1}^{m} \Big|S\Big(\frac{G_j(\mathbf{x})}{w_j^{l_j}}\Big)\Big| \\ &\le \prod_{j=1}^{m} \Big(k^{(k+1)d} l_j^{d-1} \langle w_j\rangle^{l_j(d-\frac{1}{2k})}\Big) \\ &\le k^{(k+1)d\nu(g)} \Omega(g)^{d-1} \langle g\rangle^{d-\frac{1}{2k}}. \end{aligned}$$

This completes the proof of the lemma. □

Recall that

$$S(g,\mathbf{a}) = \sum_{\mathbf{x}\in I^d_{\mathrm{ord}\, g}} e\Big(\sum_{\mathbf{i}\in\mathcal{L}} \frac{a_{\mathbf{i}}\mathbf{x}^{\mathbf{i}}}{g}\Big).$$

We now are ready to estimate $S_j(g,\mathbf{a}) = S(g, c_j\mathbf{a})$ $(1 \le j \le s)$.

Lemma 26. *Let $g \in \mathbb{A}$ and $\mathbf{a} = (a_{\mathbf{i}})_{\mathbf{i}\in\mathcal{L}}$ with $\gcd(\mathbf{a},\, g) = 1$. Then for each j with $1 \le j \le s$,*

$$\big|S_j(g,\mathbf{a})\big| = \big|S(g, c_j\mathbf{a})\big| \le \langle c_j\rangle^d k^{(k+1)d\nu(g)}\Omega(g)^{d-1}\langle g\rangle^{d-\frac{1}{2k}}.$$

Proof. Let $g_1 = g/\gcd(g, c_j)$ and $\mathbf{b} = c_j\mathbf{a}/\gcd(g, c_j)$. Then $\gcd(g_1, \mathbf{b}) = 1$ and

$$\begin{aligned} S_j(g,\mathbf{a}) &= \sum_{\mathbf{x}\,(\mathrm{mod}\, g)} e\Big(\frac{c_j}{g}\sum_{\mathbf{i}\in\mathcal{L}} a_{\mathbf{i}}\mathbf{x}^{\mathbf{i}}\Big) \\ &= \sum_{\mathbf{x}\,(\mathrm{mod}\, g)} e\Big(\frac{1}{g_1}\sum_{\mathbf{i}\in\mathcal{L}} b_{\mathbf{i}}\mathbf{x}^{\mathbf{i}}\Big) \\ &= \langle\gcd(g,\, c_j)\rangle^d \sum_{\mathbf{x}\,(\mathrm{mod}\, g_1)} e\Big(\frac{1}{g_1}\sum_{\mathbf{i}\in\mathcal{L}} b_{\mathbf{i}}\mathbf{x}^{\mathbf{i}}\Big) \\ &= \langle\gcd(g,\, c_j)\rangle^d S(g_1,\mathbf{b}). \end{aligned}$$

Applying Lemma 25 to $S(g_1,\mathbf{b})$, we obtain

$$\begin{aligned} \big|S_j(g,\mathbf{a})\big| &\le \langle c_j\rangle^d \big|S(g_1,\mathbf{b})\big| \\ &\le \langle c_j\rangle^d k^{(k+1)d\nu(h)}\Omega(g_1)^{d-1}\langle h\rangle^{d-\frac{1}{2k}} \\ &\le \langle c_j\rangle^d k^{(k+1)d\nu(g)}\Omega(g)^{d-1}\langle g\rangle^{d-\frac{1}{2k}}. \end{aligned}$$

This completes the proof of the lemma. □

2.4 Singular series

We now introduce the *singular series*

$$\mathfrak{S}_{k,d,s} = \sum_{g\,\mathrm{monic}} S(g), \tag{2.52}$$

where

$$S(g) = \langle g\rangle^{-ds} \sum_{\substack{\gcd(\mathbf{a},g)=1\\ \mathbf{a}\in I^s_{\mathrm{ord}\, g}}} \prod_{j=1}^{s} S_j(g,\mathbf{a}). \tag{2.53}$$

Also for $Q \in \mathbb{R}$ with $Q > 0$, we define

$$\mathfrak{S}_{k,d,s}(Q) = \sum_{\substack{\langle g \rangle \leq \hat{Q} \\ g \text{ monic}}} S(g). \tag{2.54}$$

In this section, we aim to show that whenever s is sufficiently large, $1 \ll \mathfrak{S}_{k,d,s} \ll 1$ and $\mathfrak{S}_{k,d,s} - \mathfrak{S}_{k,d,s}(Q) \ll \hat{Q}^{-\delta}$ for some $\delta > 0$.

Lemma 27. *When $s > 2k(\iota + 1)$, the following hold.*
(1) $\mathfrak{S}_{k,d,s}$ absolutely converges.
(2) $\left|\mathfrak{S}_{k,d,s} - \mathfrak{S}_{k,d,s}(Q)\right| \ll \hat{Q}^{1+\iota-\frac{s}{2k}+\epsilon}$.

Proof. For each $g \in \mathbb{A} \setminus \{0\}$, since $2^{\nu(g)} \leq \Omega(g)$, we have

$$k^{(k+1)d\nu(g)} \leq \Omega(g)^{2(\log k)(k+1)d},$$

and it follows from [10, Lemma 8] that

$$\langle c_j \rangle^d k^{(k+1)d\nu(g)} \Omega(g)^{d-1} \ll \langle g \rangle^{\epsilon}.$$

By Lemma 26, we see that

$$\langle g \rangle^{-ds} \prod_{j=1}^{s} S_j(g, \mathbf{a}) \ll \langle g \rangle^{-\frac{s}{2k}+\epsilon}.$$

Thus,

$$S(g) \ll \langle g \rangle^{\iota-\frac{s}{2k}+\epsilon},$$

which implies that

$$\left|\mathfrak{S}_{k,d,s}(Q)\right| \leq \sum_{m=0}^{Q} \sum_{\substack{\text{ord } g = m \\ g \text{ monic}}} \left|S(g)\right| \ll \sum_{m=0}^{Q} q^{m+m(\iota-\frac{s}{2k}+\epsilon)}.$$

Note that if $s > 2k(\iota + 1)$, we obtain $1 + \iota - \frac{s}{2k} + \epsilon < 0$. It follows that

$$\left|\mathfrak{S}_{k,d,s}\right| \ll \sum_{m=0}^{\infty} q^{m(1+\iota-\frac{s}{2k}+\epsilon)} \ll 1,$$

and

$$\left|\mathfrak{S}_{k,d,s} - \mathfrak{S}_{k,d,s}(Q)\right| \ll_{k,d,s,\epsilon} \hat{Q}^{1+\iota-\frac{s}{k}+\epsilon}.$$

Thus the lemma follows. □

Note that

$$S(g) = \langle g \rangle^{-ds} \sum_{\substack{\mathbf{a} \,(\mathrm{mod}\, g) \\ \gcd(\mathbf{a},g)=1}} \prod_{j=1}^{s} S_j(g, \mathbf{a}).$$

Lemma 28. *The function $S(g)$ is multiplicative.*

Proof. Suppose that g_1 and g_2 are monic polynomials in $\mathbb{A}$ with $(g_1,\, g_2) = 1$. Thus,

$$S(g_1g_2) = \langle g_1g_2 \rangle^{-ds} \sum_{\substack{\mathbf{a} \,(\mathrm{mod}\, g_1g_2) \\ (\mathbf{a},g_1g_2)=1}} \prod_{j=1}^{s} S_j(g_1g_2, \mathbf{a}).$$

As $\mathbf{b}_i$ runs over $\big\{\mathbf{x} \,(\mathrm{mod}\, g_i) \big| \, (\mathbf{x}, g_1) = 1\big\}$ $(i = 1, 2)$, by the Chinese Remainder Theorem, $\big(g_2\mathbf{b}_1 + g_1\mathbf{b}_2\big)$ runs over

$$\big\{\mathbf{x} \,(\mathrm{mod}\, g_1g_2) \big| \, (\mathbf{x}, g_1g_2) = 1\big\}.$$

Therefore,

$$\begin{aligned}
S(g_1g_2) &= \langle g_1g_2 \rangle^{-ds} \sum_{\substack{\mathbf{b}_1 \,(\mathrm{mod}\, g_1) \\ (\mathbf{b}_1,g_1)=1}} \sum_{\substack{\mathbf{b}_2 \,(\mathrm{mod}\, g_2) \\ (\mathbf{b}_2,g_2)=1}} \prod_{j=1}^{s} S_j(g_1g_2, g_2\mathbf{b}_1 + g_1\mathbf{b}_2) \\
&= \langle g_1g_2 \rangle^{-ds} \sum_{\substack{\mathbf{b}_1 \,(\mathrm{mod}\, g_1) \\ (\mathbf{b}_1,g_1)=1}} \sum_{\substack{\mathbf{b}_2 \,(\mathrm{mod}\, g_2) \\ (\mathbf{b}_2,g_2)=1}} \prod_{j=1}^{s} \sum_{\mathbf{x} \,(\mathrm{mod}\, g_1)} \sum_{\mathbf{y} \,(\mathrm{mod}\, g_1)} e\bigg(\frac{c_j}{g_1g_2} \sum_{\mathbf{i} \in \mathcal{L}} \big(g_2 b_{\mathbf{i},1}\mathbf{x}^{\mathbf{i}} + g_1 b_{\mathbf{i},2}\mathbf{y}^{\mathbf{i}}\big)\bigg) \\
&= \langle g_1g_2 \rangle^{-ds} \sum_{\substack{\mathbf{b}_1 \,(\mathrm{mod}\, g_1) \\ (\mathbf{b}_1,g_1)=1}} \sum_{\substack{\mathbf{b}_2 \,(\mathrm{mod}\, g_2) \\ (\mathbf{b}_2,g_2)=1}} \prod_{j=1}^{s} \sum_{\mathbf{x} \,(\mathrm{mod}\, g_1)} \sum_{\mathbf{y} \,(\mathrm{mod}\, g_2)} e\bigg(\frac{c_j}{g_1} \sum_{\mathbf{i} \in \mathcal{L}} b_{\mathbf{i},1}\mathbf{x}^{\mathbf{i}}\bigg) e\bigg(\frac{c_j}{g_2} \sum_{\mathbf{i} \in \mathcal{L}} b_{\mathbf{i},2}\mathbf{y}^{\mathbf{i}}\bigg) \\
&= \langle g_1g_2 \rangle^{-ds} \sum_{\substack{\mathbf{b}_1 \,(\mathrm{mod}\, g_1) \\ (\mathbf{b}_1,g_1)=1}} \sum_{\substack{\mathbf{b}_2 \,(\mathrm{mod}\, g_2) \\ (\mathbf{b}_2,g_2)=1}} \prod_{j=1}^{s} S_j(g_1, \mathbf{b}_1) S_j(g_2, \mathbf{b}_2) \\
&= S(g_1)S(g_2).
\end{aligned}$$

This completes the proof of the lemma. □

Since

$$\mathfrak{S}_{k,d,s} = \sum_{g \,\mathrm{monic}} S(g),$$

converges absolutely when $s > 2k(\iota + 1)$ and $S(g)$ is multiplicative, we have

$$\mathfrak{S}_{k,d,s} = \prod_{\substack{w \,\mathrm{monic} \\ \mathrm{irreducible}}} \sigma(w),$$

where

$$\sigma(w) = \sum_{h=0}^{\infty} S(w^h).$$

Moreover, there exists a constant $C = C(k, d, s)$ such that

$$\frac{1}{2} < \left| \prod_{\substack{w \text{ monic} \\ \text{irreducible} \\ \text{ord } w > C}} \sigma(w) \right| < \frac{3}{2}. \tag{2.55}$$

For $g \in \mathbb{A}$, let

$$M(g) = \operatorname{card}\big\{\mathbf{x} \,(\mathrm{mod}\, g) \big| \, c_1\mathbf{x}_1^{\mathbf{i}} + \cdots + c_s\mathbf{x}_s^{\mathbf{i}} \equiv 0 \,(\mathrm{mod}\, g) \ (\mathbf{i} \in \mathcal{L})\big\}.$$

Proposition 29. *We have*

$$\sum_{\substack{g_1 | g \\ g_1 \text{monic}}} S(g_1) = \langle g \rangle^{\iota - ds} M(g),$$

where $\iota = \operatorname{card} \mathcal{L}$.

Proof. By Lemma 3(5), we have

$$\begin{aligned} M(g) &= \sum_{\mathbf{x} \,(\mathrm{mod}\, g)} \prod_{\mathbf{i} \in \mathcal{L}} \langle g \rangle^{-1} \sum_{a_{\mathbf{i}} \,(\mathrm{mod}\, g)} e\bigg(\frac{a_{\mathbf{i}}}{g}\big(c_1\mathbf{x}_1^{\mathbf{i}} + \cdots + c_s\mathbf{x}_s^{\mathbf{i}}\big)\bigg) \\ &= \langle g \rangle^{-\iota} \sum_{\mathbf{x},\, \mathbf{a} \,(\mathrm{mod}\, g)} e\bigg(\frac{1}{g}\sum_{\mathbf{i} \in \mathcal{L}} a_{\mathbf{i}}\big(c_1\mathbf{x}_1^{\mathbf{i}} + \cdots + c_s\mathbf{x}_s^{\mathbf{i}}\big)\bigg) \\ &= \langle g \rangle^{-\iota} \sum_{\mathbf{a} \,(\mathrm{mod}\, g)} \prod_{j=1}^{s} \bigg(\sum_{\mathbf{x}_j \,(\mathrm{mod}\, g)} e\bigg(\frac{c_j}{g}\sum_{\mathbf{i} \in \mathcal{L}} a_{\mathbf{i}}\mathbf{x}_j^{\mathbf{i}}\bigg)\bigg). \end{aligned} \tag{2.56}$$

Write $g_1 = \gcd(\mathbf{a}, g)$. Let $g_2 = g/g_1$ and $\mathbf{b} = \mathbf{a}/g_1$. Then

$$\begin{aligned} \prod_{j=1}^{s} \bigg(\sum_{\mathbf{x}_j \,(\mathrm{mod}\, g)} e\bigg(\frac{c_j}{g}\sum_{\mathbf{i} \in \mathcal{L}} a_{\mathbf{i}}\mathbf{x}_j^{\mathbf{i}}\bigg)\bigg) &= \prod_{j=1}^{s} \bigg(\sum_{\mathbf{x}_j \,(\mathrm{mod}\, g)} e\bigg(\frac{c_j}{g_2}\sum_{\mathbf{i} \in \mathcal{L}} b_{\mathbf{i}}\mathbf{x}_j^{\mathbf{i}}\bigg)\bigg) \\ &= \langle g_1 \rangle^{ds} \prod_{j=1}^{s} \bigg(\sum_{\mathbf{x}_j \,(\mathrm{mod}\, g_2)} e\bigg(\frac{c_j}{g_2}\sum_{\mathbf{i} \in \mathcal{L}} b_{\mathbf{i}}\mathbf{x}_j^{\mathbf{i}}\bigg)\bigg) \\ &= \langle g_1 \rangle^{ds} \prod_{j=1}^{s} S_j(g_2, \mathbf{b}). \end{aligned}$$

On recalling (2.56), we see that

$$\begin{aligned} M(g) &= \langle g\rangle^{-\iota} \sum_{\substack{g_1|g\\ g_1 \text{ monic}}} \sum_{\substack{\mathbf{a} \,(\mathrm{mod}\, g)\\ (\mathbf{a},g)=g_1}} \langle g_1\rangle^{ds} \prod_{j=1}^{s} S_j(g/g_1, \mathbf{a}/g_1) \\ &= \langle g\rangle^{-\iota} \sum_{\substack{g_1|g\\ g_1 \text{ monic}}} \langle g_1\rangle^{ds} \langle g/g_1\rangle^{ds} S(g/g_1) \\ &= \langle g\rangle^{-\iota+ds} \sum_{\substack{g_1|g\\ g_1 \text{ monic}}} S(g/g_1). \end{aligned}$$

Thus the proposition follows. □

Corollary 30. *Suppose that w is a monic irreducible polynomial in $\mathbb{A}$. Then we have*

$$\sigma(w) = \lim_{h\to\infty} \langle w\rangle^{h(\iota-ds)} M(w^h).$$

Proof. Applying Proposition 29 to $M(w^h)$, we obtain that

$$\sigma(w) = \sum_{h=0}^{\infty} S(w^h) = \lim_{h\to\infty} \sum_{l=0}^{h} S(w^l) = \lim_{h\to\infty} \langle w^h\rangle^{\iota-ds} M(w^h).$$

□

Recall that w is an irreducible element in $\mathbb{A}$. On applying Lemma 14 to $R = \mathbb{A}_w$ and $\pi = w$, we have the following result.

Lemma 31. *Suppose that $c_1\mathbf{x}_1^{\mathbf{i}} + \cdots + c_s\mathbf{x}_s^{\mathbf{i}} = 0$ $(\mathbf{i} \in \mathcal{L})$ has a non-singular w-adic solution. Then there exists an integer $n = n(w)$ such that whenever $h \geq n$, we have*

$$M(w^h) \geq \langle w\rangle^{(h-n)(ds-\iota)}.$$

Theorem 32. *Suppose that for every irreducible element $w \in \mathbb{A}$, the system*

$$c_1\mathbf{x}_1^{\mathbf{i}} + \cdots + c_s\mathbf{x}_s^{\mathbf{i}} = 0 \ (\mathbf{i} \in \mathcal{L})$$

has a non-singular w-adic solution. When $s > 2k(\iota+1)$, we have

$$\mathfrak{S}_{k,d,s} > 0.$$

Proof. By (2.55) and Corollary 30, there exists a constant $C = C(k, d, s)$ such that

$$\frac{1}{2} < \prod_{\substack{w \text{ monic} \\ \text{irreducible} \\ \text{ord } w > C}} \sigma(w) < \frac{3}{2}.$$

It suffices to deal with the monic irreducible elements w with $\operatorname{ord} w \le C$. On combining Corollary 30 with Lemma 31, for all w with $\operatorname{ord} w \le C$ we have

$$\sigma(w) = \lim_{h\to\infty} \langle w\rangle^{h(\iota - ds)} M(w^h) \ge \langle w\rangle^{-n(ds-\iota)}.$$

Thus,

$$\mathfrak{S}_{k,d,s} = \prod_{\substack{w \text{ monic} \\ \text{irreducible}}} \sigma(w) > 0.$$

This completes the proof of the theorem. □

2.5 Estimates for exponential sums II

In preparation for the next section, the goal of this section is to analyze the exponential sums of the form

$$T_P(F) = \sum_{\mathbf{x}\in I_{-P}^d} e\Big(\sum_{i_1=0}^{n} \cdots \sum_{i_d=0}^{n} \alpha_{i_1,\dots,i_d} x_1^{i_1} \cdots x_d^{i_d}\Big),$$

where $\alpha_{i_1,\dots,i_d} \in \mathbb{K}_\infty$, $P \in \mathbb{R}$ with $P > 0$, and

$$I_{-P} = \big\{\beta \in \mathbb{K}_\infty \big| \beta = b_{-P+1}t^{-P+1} + \cdots + b_{-1}t^{-1} + b_0 \ (b_i \in \mathbb{F}_q)\big\}.$$

Consider $(K, |\cdot|) = (\mathbb{K}_\infty, \langle\cdot\rangle)$, $R = \{x \in \mathbb{K}_\infty \mid \langle x\rangle \le 1\}$ and $\pi = t^{-1}$. Thus for $\alpha \in \mathbb{K}_\infty$, we have

$$\tau(\alpha) = \log\langle\alpha\rangle / \log\langle t^{-1}\rangle = -\operatorname{ord}\alpha.$$

Then whenever $\tau(\alpha) \ge 2$, $e(\alpha) = 1$. On applying Lemmas 10, 11 and 12, we obtain the following Lemmas.

Lemma 33. *Let $f(x) \in \mathbb{K}_\infty[x]$ with $f' \ne 0$ and $\deg f \le n$. For $a \in \mathbb{F}_q$, let $g_a(x) = f(t^{-1}x + a) - f(a)$. The following hold.*
(1) If $f(0) = 0$, then $1 + \tau(f) \le \tau(g_a) \le n + \tau(f)$.
(2) $1 + \tau(f') \le \tau(g_a') \le n + \tau(f')$.
(3) $\operatorname{ind} g_a' \le \operatorname{ind} f'$. If $\operatorname{ind} g_a' = \operatorname{ind} f'$ and $\tau(f'(b)) \ge \tau(f') + 1$ for some $b \in \mathbb{F}_q$, then $a = b$.

Proof. (1) Since $f \neq 0$ and $f(0) = 0$, we have $\operatorname{ind} f > 0$. It follows from Lemma 11(2) that $1 + \tau(f) \leq \tau(g_a) \leq n + \tau(f)$.

(2) It follows from Lemma 11(2) directly.

(3) By Lemma 11(4), we have

$$\operatorname{ind} g_a' \leq \operatorname{ind} f'.$$

If $\operatorname{ind} g_a' = \operatorname{ind} f'$ and $\tau(f'(b)) \geq \tau(f') + 1$, we deduce from Lemma 10(4) that $\tau(a-b) \geq 1$. Since $a, b \in \mathbb{F}_q$, we have $a = b$. □

Lemma 34. *Let $f(x) \in \mathbb{K}_\infty[x] \setminus \{0\}$ with $\deg f \leq n$. For $u, v \in \mathbb{N}$ with $u \geq v > n$, let*

$$N_{u,v}(f) = \big\{\beta \in \mathbb{K}_\infty \big| \beta = b_{-u+1}t^{-u+1} + \cdots + b_{-1}t^{-1} + b_0 \,(b_i \in \mathbb{F}_q),\ \tau(f(\beta)) \geq v + \tau(f)\big\}.$$

Then

$$\operatorname{card} N_{u,v}(f) \leq q^{n+1+u-\frac{v}{n}}.$$

Proof. Note that $\big\{\beta \in \mathbb{K}_\infty \big| \beta = b_{-u+1}t^{-u+1} + \cdots + b_{-1}t^{-1} + b_0 \,(b_i \in \mathbb{F}_q)\big\}$ is a complete set of coset representatives of (π^u) in R. Since $R/(\pi) = \mathbb{F}_q$, we see from Lemma 12 that $\operatorname{card} N_{u,v}(f) \leq q^{n+1+u-\frac{v}{n}}$. □

Before proceeding to the next lemma, it is necessary to introduce some new notations. For $P \in \mathbb{N} \setminus \{0\}$ and $a \in \mathbb{F}_q$, let

$$I_{-P} = \big\{\beta \in \mathbb{K}_\infty \big| \beta = b_{-P+1}t^{-P+1} + \cdots + b_{-1}t^{-1} + b_0 \ (b_i \in \mathbb{F}_q)\big\},$$

and

$$I_{a,-P} = \big\{\beta \in \mathbb{K}_\infty \big| \beta = b_{-P+1}t^{-P+1} + \cdots + b_{-1}t^{-1} + a \ (b_i \in \mathbb{F}_q)\big\}.$$

Let $f(x) \in \mathbb{K}_\infty[x]$. Define

$$T_P(f) = \sum_{\beta \in I_{-P}} e\big(f(\beta)\big),$$

and

$$T_{a,P}(f) = \sum_{\beta \in I_{a,-P}} e\big(f(\beta)\big).$$

Moreover, for $\alpha \in \mathbb{K}_\infty$ and S_1, $S_2 \subseteq \mathbb{K}_\infty$, define

$$\alpha S_1 = \big\{\alpha\beta \,\big|\, \beta \in S_1\big\} \quad \text{and} \quad S_1 + S_2 = \big\{\beta_1 + \beta_2 \,\big|\, \beta_i \in S_i \,(i = 1, 2)\big\}.$$

Lemma 35. *Let $f(x) \in \mathbb{K}_\infty[x]$ with $2\tau(f') \le \tau(f) \le 0$. Let $P \in \mathbb{N}$ satisfy $P + \tau(f) \ge 2$. If $\tau\big(f'(a)\big) = \tau(f')$ for some $a \in \mathbb{F}_q$, then $T_{a,P}(f) = 0$.*

Proof. Let $u = -\tau(f') + 1$. On combining $\tau(f) \le \tau(f') \le 0$ with $P + \tau(f) \ge 2$, we obtain

$$1 \le u \le -\tau(f) + 1 \le P - 1.$$

Thus $I_{a,-P} = I_{a,-u} + t^{-u} I_{-P+u}$ and

$$T_{a,P}(f) = \sum_{\beta_1 \in I_{a,-u}} \sum_{\beta_2 \in I_{-P+u}} e\big(f(\beta_1 + t^{-u}\beta_2)\big). \tag{2.57}$$

Fix $\beta_1 \in I_{a,-u}$ and $\beta_2 \in I_{a,-P+u}$. On letting $f(x) = \alpha_n x^n + \cdots + \alpha_1 x + \alpha_0$, we find that

$$f(\beta_1 + t^{-u}\beta_2) = \sum_{h=0}^{n} \alpha_h \sum_{i=0}^{h} \left(\begin{array}{c} h \\ i \end{array} \right) \beta_1^{h-i} \beta_2^i t^{-ui} = \sum_{i=0}^{n} \sum_{h=i}^{n} \left(\begin{array}{c} h \\ i \end{array} \right) \alpha_h \beta_1^{h-i} \beta_2^i t^{-ui}.$$

For $h \ge i \ge 2$, since

$$2\tau(f') \le \tau(f) \le \tau(\alpha_n), \quad \tau(\beta_1) \ge 0, \quad \text{and} \quad \tau(\beta_2) \ge 0,$$

we see that

$$\tau\big(\alpha_h \beta_1^{h-i} \beta_2^i t^{-ui}\big) \ge \tau(f) + 2u = \tau(f) + 2(-\tau(f') + 1) \ge 2.$$

Thus

$$e\Big(f(\beta_1 + t^{-u}\beta_2) - f(\beta_1) - f'(\beta_1) t^{-u} \beta_2\Big) = e\left(\sum_{i=2}^{n} \sum_{h=i}^{n} \left(\begin{array}{c} h \\ i \end{array} \right) \alpha_h \beta_1^{h-i} \beta_2^i t^{-ui} \right) = 1.$$

Hence

$$e\big(f(\beta_1 + t^{-u}\beta_2)\big) = e\big(f(\beta_1) + f'(\beta_1) t^{-u} \beta_2\big).$$

Let $\gamma = \beta_1 - a$. Since $\beta_1 \in I_{a,-u}$, we have $\gamma \in \mathbb{T}$, i.e., $\tau(\gamma) \ge 1$. Since

$$f'(x) = n\alpha_n x^{n-1} + \cdots + 2\alpha_2 x + \alpha_1,$$

we have

$$f'(\beta_1) = f'(a + \gamma) = \sum_{i=0}^{n-1} \sum_{v=i}^{n-1} \left(\begin{array}{c} v \\ i \end{array} \right) (v+1) \alpha_{v+1} a^{v-i} \gamma^i.$$

Note that if $i \geq 1$, then

$$\tau\Big(\sum_{v=i}^{n-1}\binom{v}{i}(v+1)\alpha_{v+1}a^{v-i}\gamma^i\Big) \geq \tau(f') + \tau(\gamma) \geq \tau(f') + 1.$$

Otherwise, if $i = 0$, then

$$\tau\Big(\sum_{v=i}^{n-1}\binom{v}{i}(v+1)\alpha_{v+1}a^{v-i}\gamma^i\Big) = \tau(f'(a)) = \tau(f').$$

Hence $\tau\big(f'(\beta_1)\big) = \tau(f'(a)) = \tau(f') = 1-u$. Write $f'(\beta_1) = \sum_{j\leq u-1} b_j t^j$ where $b_j \in \mathbb{F}_q$ $(j \leq u-1)$ and $b_{u-1} \neq 0$. Therefore

$$\begin{aligned}\sum_{\beta_2\in I_{-P+u}} e\big(f'(\beta_1)t^{-u}\beta_2\big) &= \sum_{\substack{a_i\in\mathbb{F}_q\\ -P+u<i\leq 0}} e\Big(f'(\beta_1)t^{-u}\sum_{-P+u<i\leq 0} a_i t^i\Big)\\ &= \prod_{-P+u<i\leq 0}\sum_{a_i\in\mathbb{F}_q} e\big(f'(\beta_1)t^{-u}a_i t^i\big)\\ &= \prod_{-P+u<i\leq 0}\sum_{a_i\in\mathbb{F}_q} e\Big(\sum_{j\leq u-1} b_j a_i t^{i+j-u}\Big).\end{aligned}$$

For $i = 0$ and $j \leq u-2$, we have $i+j-u \leq u-2-u = -2$. Hence

$$e\Big(\sum_{j\leq u-2} b_j a_0 t^{0+j-u}\Big) = 1.$$

We have

$$\sum_{a_0\in\mathbb{F}_q} e\Big(\sum_{j\leq u-1} b_j a_0 t^{0+j-u}\Big) = \sum_{a_0\in\mathbb{F}_q} e(b_{u-1}a_0 t^{-1}) = \sum_{a_0\in\mathbb{F}_q} e_q(b_{u-1}a_0).$$

On noting that

$$\sum_{a_0\in\mathbb{F}_q} e_q(a_0) = \sum_{j=0}^{p-1} e^{2\pi ij/p}\cdot \operatorname{card}\big(\ker(\mathrm{tr})\big) = 0,$$

since $b_{u-1} \neq 0$, we see that

$$\sum_{a_0\in\mathbb{F}_q} e_q(b_{u-1}a_0) = 0.$$

Hence

$$\sum_{\beta_2\in I_{-P+u}} e\big(f'(\beta_1)t^{-u}\beta_2\big) = 0.$$

From (2.57) and the above equality, it follows that

$$\begin{aligned} T_{a,P}(f) &= \sum_{\beta_1 \in I_{a,-u}} \sum_{\beta_2 \in I_{-P+u}} e\big(f(\beta_1) + f'(\beta_1)t^{-u}\beta_2\big) \\ &= \sum_{\beta_1 \in I_{a,-u}} e\big(f(\beta_1)\big) \sum_{\beta_2 \in I_{-P+u}} e\big(f'(\beta_1)t^{-u}\beta_2\big) \\ &= 0. \end{aligned}$$

This completes the proof of the lemma. □

Lemma 36. *Let $f(x) \in \mathbb{K}_\infty[x]$ with $2\tau(f') \le \tau(f) \le 0$. For every $a \in \mathbb{F}_q$, let*

$$g_a(x) = f(t^{-1}x + a) - f(a) \quad \text{and} \quad \delta_a = \begin{cases} 1, & \text{if} \quad \operatorname{ind} g_a' < \operatorname{ind} f', \\ 0, & \text{if} \quad \operatorname{ind} g_a' = \operatorname{ind} f'. \end{cases}$$

Suppose that $P \in \mathbb{N}$ satisfies $P + \tau(f) \ge 2$. Then there exists $b \in \mathbb{F}_q$ such that

$$|T_P(f)| \le q^{\delta_b} \big|T_{b,P}(f)\big|.$$

Proof. For every $a \in \mathbb{F}_q$, since $\tau(f'(a)) \ge \tau(f')$, from Lemma 35, we find that

$$T_P(f) = \sum_{a \in \mathbb{F}_q} T_{a,P}(f) = \sum_{\tau(f'(a)) > \tau(f')} T_{a,P}(f). \tag{2.58}$$

Suppose that every $a \in \mathbb{F}_q$ satisfies $\operatorname{ind} g_a' < \operatorname{ind} f$. We have

$$|T_P(f)| \le q \max_{a \in \mathbb{F}_q} |T_{a,P}(f)| = q^{\delta_b} |T_{b,P}(f)|$$

for some $b \in \mathbb{F}_q$. Otherwise, suppose that there exists $b \in \mathbb{F}_q$ such that $\operatorname{ind} g_b' = \operatorname{ind} f'$. By Lemma 33(3), for every $a \in \mathbb{F}_q$ with $\tau\big(f'(a)\big) > \tau(f')$, we have $a = b$. By (2.58), we see that $|T_P(f)| \le |T_{b,P}(f)| = q^{\delta_b}|T_{b,P}(f)|$. □

Proposition 37. *Let $f(x) \in \mathbb{K}_\infty[x]$ with $\deg f = n$ and $2\tau(f') \le \tau(f) \le 0$. Let $P \in \mathbb{N}$ satisfy $P + \tau(f) \ge 2$. Then*

$$|T_P(f)| \le q^{n+P-\frac{1+\tau(f)-2\tau(f')}{2n}}.$$

Proof. Since

$$T_P(f) = \sum_{\beta \in I_{-P}} e\big(f(\beta)\big),$$

we have $|T_P(f)| = \big|T_P\big(f - f(0)\big)\big|$. Without loss of generality, we assume that $f(0) = 0$. For $a \in \mathbb{F}_q$, let $g_a(x) = f(t^{-1}x + a) - f(a)$. Then

$$|T_{a,P}| = \Big| \sum_{\beta \in I_{a,-P}} e\big(f(\beta)\big) \Big| = \Big| \sum_{\gamma \in I_{-P+1}} e\big(f(a + t^{-1}\gamma) - f(a)\big) \Big| = \big|T_{P-1}(g_a)\big|.$$

It follows from Lemma 33 that for every $a \in \mathbb{F}_q$,

$$1 \le \tau(g_a') - \tau(f') \le n \quad \text{and} \quad 1 \le \tau(g_a) - \tau(f) \le n.$$

Thus

$$P - 1 + \tau(g_a) \ge P - 1 + \tau(f) + 1 \ge 2.$$

Let b and δ_b be defined as in Lemma 36. We have

$$|T_P(f)| \le q^{\delta_b} |T_{P-1}(g_b)| \quad \text{and} \quad P - 1 + \tau(g_b) \ge 2.$$

If $2\tau(g_b') \le \tau(g_b) \le 0$, we apply Lemmas 35 and 36 to $T_{P-1}(g_b)$ and repeat this procedure until we obtain $T_Q(g)$ such that $\tau(g) \le 2\tau(g') - 1$ or $\tau(g) > 0$. More concretely, suppose that we stop after getting $T_P(g_0) = T_P(f)$, $T_{P-1}(g_1), \ldots, T_{P-m}(g_m)$, which satisfy

$$\begin{aligned}
&\deg g_i = n, \quad g_i' \ne 0, \quad \tau(g_i') - \tau(g_{i-1}') \le n, \quad 1 \le \tau(g_i) - \tau(g_{i-1}) \ (1 \le i \le m); \\
&2\tau(g_i') \le \tau(g_i) \le 0 \ (1 \le i \le m-1); \quad \tau(g_m) \le 2\tau(g_m') - 1 \quad \text{or} \quad \tau(g_m) > 0; \\
&|T_{P-i+1}(g_{i-1})| \le q^{\delta_i} |T_{P-i}(g_i)| \ (\delta_i = \delta_{b_i}, \ 1 \le i \le m).
\end{aligned} \tag{2.59}$$

By Lemma 36, in (2.59), $\delta_i = 1$ if and only if $\operatorname{ind} g_i < \operatorname{ind} g_{i-1}$. Thus, this case occurs less than n times. Therefore,

$$|T_P(f)| \le q^n |T_{P-m}(g_m)| \le q^{n+P-m}. \tag{2.60}$$

By (2.59), we have

$$\tau(g_m') - \tau(f') \le mn \quad \text{and} \quad \tau(g_m) - \tau(f) \ge m. \tag{2.61}$$

If $\tau(g_m) \le 2\tau(g_m') - 1$, by (2.61), we have

$$2mn \ge 2\tau(g_m') - 2\tau(f') \ge \tau(g_m) + 1 - 2\tau(f') > \tau(f) + 1 - 2\tau(f'),$$

and hence

$$m \ge \frac{1 + \tau(f) - 2\tau(f')}{2n}.$$

On recalling (2.60), we have

$$|T_P(f)| < q^{n+P-\frac{1+\tau(f)-2\tau(f')}{2n}}.$$

It remains to consider the case when $\tau(g_m) > 0$. Since $\tau(f) \leq \tau(f')$, we have

$$mn \geq \tau(g_m) - \tau(f) \geq 1 - \tau(f) \geq 1 + \tau(f) - 2\tau(f').$$

Thus

$$|T_P(f)| < q^{n+P-\frac{1+\tau(f)-2\tau(f')}{2n}}.$$

This completes the proof of the proposition. □

Corollary 38. *Let $f(x) \in \mathbb{K}_\infty[x]$ with $\deg f \leq n$ and $\tau(f) \leq 0$. Let $P \in \mathbb{N}$ satisfy $P + \tau(f) \geq 2$. Then*

$$|T_P(f)| \leq q^{n+P-\frac{1+\tau(f)-2\tau(f')}{2n}}.$$

Proof. If $2\tau(f') \leq \tau(f) \leq 0$, then the result is true by Proposition 37. If $2\tau(f') > \tau(f)$, then

$$|T_P(f)| \leq q^P \leq q^{n+P-\frac{1+\tau(f)-2\tau(f')}{2n}}.$$

□

Lemma 39. *For $n \in \mathbb{N} \setminus \{0\}$, let*

$$F(\mathbf{x}) = \sum_{i_1=0}^{n} \cdots \sum_{i_d=0}^{n} \alpha_{i_1,\ldots,i_d} x_1^{i_1} \cdots x_d^{i_d} \ \in \mathbb{K}_\infty[\mathbf{x}],$$

and for $P \in \mathbb{N} \setminus \{0\}$, let

$$T_P(F) = \sum_{\mathbf{x} \in I_{-P}^d} e\big(F(\mathbf{x})\big).$$

Let $\tau(F) = \min\{\tau\big(\alpha_{i_1,\ldots,i_d}\big) \big| 0 \leq i_1, \ldots, i_d \leq n\}$. If there exists $\mathbf{j}$ such that $p \nmid \mathbf{j}$ and $\tau(\alpha_{\mathbf{j}}) \leq 0$, then whenever $P + \tau(F) \geq 2$ we have

$$|T_P(F)| \leq (-\tau(F) + 2)^{d-1} q^{(n+1)d+Pd-\frac{1+\tau(F)-2\tau(\alpha_{\mathbf{j}})}{2n}}.$$

Proof. We will prove the lemma by induction on d. When $d = 1$, since there exists j with $p \nmid j$ such that $\tau(\alpha_j) \leq 0$, we have

$$\tau(F) \leq \tau(F') \leq \tau(\alpha_j) \leq 0.$$

By Corollary 38, we see that

$$|T_P(F)| \le q^{n+P-\frac{1+\tau(F)-2\tau(F')}{2n}} \le q^{n+P-\frac{1+\tau(F)-2\tau(\alpha_j)}{2n}}.$$

Assume that the lemma is true for $d-1$. We first deal with the case when $-\tau(\alpha_{\mathbf{j}}) \le 2n$. Since

$$(n+1)d - \frac{1+\tau(F)-2\tau(\alpha_{\mathbf{j}})}{2n} \ge \frac{\tau(\alpha_{\mathbf{j}})-\tau(F)}{2n} \ge 0,$$

we find that

$$|T_P(F)| \le q^{Pd} \le q^{(n+1)d+Pd-\frac{1+\tau(F)-2\tau(\alpha_{\mathbf{j}})}{2n}}.$$

We now consider the case when $-\tau(\alpha_{\mathbf{j}}) \ge 2n+1$. Without loss of generality, suppose that $\mathbf{j} = (j_1, \dots, j_d)$ satisfies $p \nmid j_1$ and define

$$\varphi(y) = \sum_{i=0}^{n} \alpha_{j_1,\dots,j_{d-1},i} y^i, \quad F_y(\mathbf{x}) = F(x_1, \dots, x_{d-1}, y),$$
$$T_P(F_y) = \sum_{\mathbf{x} \in I_{-P}^{d-1}} e\big(F_y(\mathbf{x})\big), \quad \text{and} \quad T(y) = \big|T_P(F_y)\big|.$$

Since

$$\tau(\varphi) = \min\big\{\tau(\alpha_{j_1,\dots,j_{d-1},i}) \big| 0 \le i \le d\big\} \le \tau(\alpha_{\mathbf{j}}),$$

we have

$$-\tau(\varphi) \ge -\tau(\alpha_{\mathbf{j}}) \ge 2n+1.$$

For each $u \in \mathbb{N}$, define

$$N_u = \big\{y \in I_{-P} \,\big|\, \tau\big(\varphi(y)\big) = u + \tau(\varphi)\big\} \quad \text{and} \quad T_u = \sum_{y \in N_u} T(y).$$

Note that for each $y \in I_{-P}$, $\tau\big(\varphi(y)\big) \ge \tau(\varphi)$. Then $I_{-P} = \sqcup_{u \in \mathbb{N}} N_u$. Let

$$S_1 = \sum_{u=0}^{n} T_u, \quad S_2 = \sum_{u=n+1}^{-\tau(\varphi)} T_u \quad \text{and} \quad S_3 = \sum_{u > -\tau(\varphi)} T_u.$$

Thus

$$|T_P(F)| \le \sum_{y \in I_{-P}} T(y) = \sum_{u \in \mathbb{N}} T_u = S_1 + S_2 + S_3. \tag{2.62}$$

Claim 1. For $y \in N_u$ with $0 \le u \le -\tau(\varphi)$, we have

$$T(y) \le (-\tau(F)+2)^{d-2} \cdot q^{(n+1)(d-1)+P(d-1)-\frac{1+\tau(F)-2(u+\tau(\varphi))}{2n}}.$$

Proof. Let $\varphi_{i_1,\dots,i_{d-1}}(y)$ be the coefficient of $x_1^{i_1}\cdots x_{d-1}^{i_{d-1}}$ in the expansion of F_y, i.e.,

$$\varphi_{i_1,\dots,i_{d-1}}(y)=\sum_{i_d=0}^{n}\alpha_{i_1,\dots,i_d}y^{i_d}.$$

For each $y\in I_{-P}$, we see that

$$\langle\varphi_{i_1,\dots,i_{d-1}}(y)\rangle\le\max\{\langle\alpha_{i_1,\dots,i_d}\rangle\,|\,0\le i_d\le n\}.$$

Thus

$$\tau\big(\varphi_{i_1,\dots,i_{d-1}}(y)\big)\ge\min\big\{\tau(\alpha_{i_1,\dots,i_{d-1},i_d})\,|\,0\le i_d\le n\big\}\ge\tau(F). \tag{2.63}$$

Furthermore,

$$\tau(F_y)=\min\big\{\tau\big(\varphi_{i_1,\dots,i_{d-1}}(y)\big)|0\le i_1,\dots,i_{d-1}\le n\big\}\ge\tau(F).$$

Since $P+\tau(F)\ge 2$, we have $P+\tau(F_y)\ge 2$. Note that $p\nmid(j_1,\dots,j_{d-1})$ and $\varphi_{j_1,\dots,j_{d-1}}=\varphi$. Hence for $y\in N_u$ with $0\le u\le-\tau(\varphi)$, we have

$$\tau\big(\varphi_{j_1,\dots,j_{d-1}}(y)\big)=\tau\big(\varphi(y)\big)=u+\tau(\varphi)\le 0.$$

Now we are ready to apply the induction hypothesis to $T_P(F_y)$ with $y\in\bigcup_{u=0}^{-\tau(\varphi)}N_u$. We obtain that

$$\begin{aligned}T(y)=\big|T_P(F_y)\big|&\le(-\tau(F_y)+2)^{d-2}\cdot q^{(n+1)(d-1)+P(d-1)-\frac{1+\tau(F_y)-2\tau(\varphi(y))}{2n}}\\&\le(-\tau(F)+2)^{d-2}\cdot q^{(n+1)(d-1)+P(d-1)-\frac{1+\tau(F)-2(u+\tau(\varphi))}{2n}}.\end{aligned}$$

This completes the proof of Claim 1.

Claim 2. $\big|T_P(F)\big|\le(-\tau(F)+2)^{d-1}q^{(n+1)d+Pd-\frac{1+\tau(F)-2\tau(\varphi)}{2n}}$.

Proof. Since $\operatorname{card}N_u\le\operatorname{card}I_{-P}=q^P$, by Claim 1, we can see that

$$\begin{aligned}S_1=\sum_{0\le u\le n}T_u&=\sum_{0\le u\le n}\sum_{y\in N_u}T(y)\\&\le(n+1)\cdot(-\tau(F)+2)^{d-2}\cdot q^P\cdot q^{(n+1)(d-1)+P(d-1)-\frac{1+\tau(F)-2(n+\tau(\varphi))}{2n}}\\&\le(n+1)\cdot(-\tau(F)+2)^{d-2}\cdot q^{(n+1)d+Pd-\frac{1+\tau(F)-2\tau(\varphi)}{2n}}.\end{aligned} \tag{2.64}$$

For $v\in\mathbb{N}$ with $v\ge n+1$, let

$$M_v=\big\{y\in I_{-P}\big|\,\tau(\varphi(y))\ge v+\tau(\varphi)\big\}.$$

Since $\tau(F) \leq \tau(\varphi_{j_1,\dots,j_{d-1}}) = \tau(\varphi)$, we have $P \geq -\tau(F)+2 \geq -\tau(\varphi)+2$. It follows from Lemma 34 that for $v \in \mathbb{N}$ with $n+1 \leq v \leq -\tau(\varphi)+1$,

$$\operatorname{card} N_v \leq \operatorname{card} M_v \leq q^{n+1+P-\frac{v}{n}}. \tag{2.65}$$

From Claim 1 and (2.65), we have

$$\begin{aligned} S_2 &\leq \sum_{n<u\leq -\tau(\varphi)} \operatorname{card} N_u \cdot (-\tau(F)+2)^{d-2} \cdot q^{(n+1)(d-1)+P(d-1)-\frac{1+\tau(F)-2(u+\tau(\varphi))}{2n}} \\ &\leq \sum_{n<u\leq -\tau(\varphi)} (-\tau(F)+2)^{d-2} \cdot q^{n+1+P-\frac{u}{n}} \cdot q^{(n+1)(d-1)+P(d-1)-\frac{1+\tau(F)-2(u+\tau(\varphi))}{2n}} \\ &\leq (-\tau(\varphi)-n) \cdot (-\tau(F)+2)^{d-2} \cdot q^{(n+1)d+Pd-\frac{1+\tau(F)-2\tau(\varphi)}{2n}}. \end{aligned} \tag{2.66}$$

On noting that $T(y) \leq q^{P(d-1)}$ and $\tau(F) \leq 0$, we see from (2.65) that

$$\begin{aligned} S_3 = \sum_{u>-\tau(\varphi)} \sum_{y\in N_u} T(y) &\leq \Big(\operatorname{card} M_{-\tau(\varphi)+1}\Big) \cdot q^{P(d-1)} \\ &\leq q^{n+1+P-\frac{-\tau(\varphi)+1}{n}} \cdot q^{P(d-1)} \\ &\leq q^{(n+1)d+Pd-\frac{1+\tau(F)-2\tau(\varphi)}{2n}}. \end{aligned} \tag{2.67}$$

Therefore, by combining (2.62), (2.64), (2.66) and (2.67), we have

$$\begin{aligned} |T_P(F)| &\leq S_1 + S_2 + S_3 \\ &\leq (-\tau(\varphi)+2) \cdot (-\tau(F)+2)^{d-2} \cdot q^{(n+1)d+Pd-\frac{1+\tau(F)-2\tau(\varphi)}{2n}} \\ &\leq (-\tau(F)+2)^{d-1} \cdot q^{(n+1)d+Pd-\frac{1+\tau(F)-2\tau(\varphi)}{2n}}. \end{aligned}$$

This completes the proof of Claim 2.

By combining Claims 1 and 2, since

$$\tau(\varphi) = \min\left\{\tau(\alpha_{j_1,\dots,j_{d-1},i}) \middle| 0 \leq i \leq d\right\} \leq \tau(\alpha_{\mathbf{j}}),$$

we see that

$$|T_P(F)| \leq (-\tau(F)+2)^{d-1} \cdot q^{(n+1)d+Pd-\frac{1+\tau(F)-2\tau(\alpha_{\mathbf{j}})}{2n}}.$$

The lemma follows by induction. □

2.6 Singular integral

In Lemma 6, we establish the following relation for the major arc contribution.

$$\int_{\mathfrak{M}} \prod_{j=1}^{s} f_j(\boldsymbol{\alpha}; P) d\boldsymbol{\alpha} = \sum_{\substack{\langle g \rangle \leq \langle c \rangle \hat{P}^{\frac{1}{2}} \\ g \text{ monic}}} \sum_{\mathbf{a} \in \mathcal{A}_g} \Big(\prod_{j=1}^{s} \langle g \rangle^{-d} S_j(g, \mathbf{a}) \Big) \int_{\mathcal{B}_g} \prod_{j=1}^{s} f_j(\boldsymbol{\beta}) d\boldsymbol{\beta},$$

where

$$\mathcal{A}_g = \big\{ \mathbf{a} = (a_{\mathbf{i}})_{\mathbf{i} \in \mathcal{L}} \in I^{\iota}_{\operatorname{ord} g} \;\big|\; \gcd(\mathbf{a}, g) = 1 \big\},$$

and

$$\mathcal{B}_g = \big\{ \boldsymbol{\beta} = (\beta_{\mathbf{i}})_{\mathbf{i} \in \mathcal{L}} \in \mathbb{T}^{\iota} \;\big|\; \langle \beta_{\mathbf{i}} \rangle < \langle g \rangle^{-1} \hat{P}^{\frac{1}{2}-k} \ \big(\mathbf{i} \in \mathcal{L}\big) \big\}.$$

We have treated the above sum by estimating the singular series. In this section, we plan to analyze the the integrals of the shape

$$\int_{\mathcal{B}_g} \prod_{j=1}^{s} f_j(\boldsymbol{\beta}; P) d\boldsymbol{\beta}. \tag{2.68}$$

Some preparation is required before we can introduce our strategy. For $\boldsymbol{\alpha} = (\alpha_{\mathbf{i}})_{\mathbf{i} \in \mathcal{L}}$ and $\mathbf{x} = (\mathbf{x}_1, \dots, \mathbf{x}_s)$ where $\mathbf{x}_j = (x_{1j}, \dots, x_{dj})$, write

$$G(\boldsymbol{\alpha}; \mathbf{x}) = G(\boldsymbol{\alpha}; \mathbf{x}_1, \dots, \mathbf{x}_s; \mathbf{c}) = \sum_{\mathbf{i} \in \mathcal{L}} \boldsymbol{\alpha}_{\mathbf{i}} \big(c_1 \mathbf{x}_1^{\mathbf{i}} + \cdots + c_s \mathbf{x}_s^{\mathbf{i}} \big),$$

and define the *singular integral* to be

$$\mathfrak{J} = \mathfrak{J}_{s,d,k} = \int_{\mathbb{K}^{\iota}_{\infty}} \Big(\int_{\mathbb{T}^{ds}} G(\boldsymbol{\alpha}, \mathbf{x}) d\mathbf{x} \Big) d\boldsymbol{\alpha}.$$

We will first relate the integrals as in (2.68) to $\mathfrak{J} \hat{P}^{sd-\iota k}$ and then show that $1 \ll \mathfrak{J} \ll 1$.

2.6.1 Preliminaries

Let G be a locally compact group and $\mathcal{B}(G)$ be the class of Borel sets, i.e., the smallest σ-algebra containing the closed sets.

Definition 40. *A function $\mu : \mathcal{B}(G) \longrightarrow \mathbb{R}$ is said to be an* inner regular left invariant measure *if the following conditions hold.*

(1) For any $E \in \mathcal{B}(G)$, $\mu(E) \geq 0$.
(2) $\mu(\emptyset) = 0$.
(3) For any sequence E_i of disjoint Borel sets, $\mu\Big(\bigsqcup_{i\geq 1} E_i\Big) = \sum_{i\geq 1} \mu(E_i)$.
(4) For any $g \in G$ and $E \in \mathcal{B}(G)$, $\mu(gE) = \mu(E)$.
(5) For any $E \in \mathcal{B}(G)$, $\mu(E) = \sup\big\{\mu K : K \subseteq E,\ K \text{ compact},\ K \in \mathcal{B}(G)\big\}$.

Definition 41. *A* left Haar measure on a locally compact group G *is the completion of an inner regular left invariant Borel measure.*

Theorem 42. *Let G be a locally compact group. Then there is a left Haar measure μ on G.*

Proof. This is [18, Theorem 14.14]. □

Theorem 43. *Any two left Haar measures on a locally compact group G are the same, apart from a multiplicative constant.*

Proof. This is [18, Corollary 14.22]. □

Let $G = (\mathbb{K}_\infty, +, \langle\cdot\rangle)$. Then G is a locally compact group. Let μ be the Haar measure on G normalized by $\mu(\mathbb{T}) = 1$.

Lemma 44. *For $Q \in \mathbb{Z}$, let $\mathcal{B}_Q = \big\{t^Q E \big| E \in \mathcal{B}(G)\big\}$. Then $\mathcal{B}_Q = \mathcal{B}(G)$.*

Proof. Let $f_Q : \mathbb{K}_\infty \longrightarrow \mathbb{K}_\infty$ defined by $f_Q(\alpha) = t^Q\alpha$. Then f_Q is a homeomorphism. Since $\mathcal{B}(G)$ is a σ-algebra containing all the closed sets, $\mathcal{B}_Q = f_Q\big(\mathcal{B}(G)\big)$ is also a σ-algebra containing all the closed sets. Therefore, $\mathcal{B}_Q \supseteq \mathcal{B}(G)$. Since Q can be chosen from $\mathbb{Z}$ arbitrarily, we have $\mathcal{B}_{-Q} \supseteq \mathcal{B}(G)$. Note that $\mathcal{B}(G) = \big\{t^Q E \big| E \in \mathcal{B}_{-Q}\big\}$. We obtain $\mathcal{B}(G) \supseteq \big\{t^Q E \big| E \in \mathcal{B}(G)\big\} = \mathcal{B}_Q$. Thus $\mathcal{B}_Q = \mathcal{B}(G)$. □

Lemma 45. *For $Q \in \mathbb{Z}$, define $\mu_Q : \mathcal{B}(G) \longrightarrow \mathbb{R}$ by $\mu_Q(E) = \mu(t^Q E)$. Then μ_Q is a Haar measure on G and $\mu_Q = \hat{Q}\mu$.*

Proof. Note that μ_Q satisfies Conditions (1), (2) and (3) of Definition 40 immediately. Let f_Q be defined as in the proof of Lemma 44. Since f_Q is a homeomorphism, μ_Q satisfies Condition (5). For any $\alpha \in \mathbb{K}_\infty$ and $E \in \mathcal{B}(G)$,

$$\mu_Q(\alpha + E) = \mu(t^Q\alpha + t^Q E) = \mu(t^Q E) = \mu_Q(E).$$

Therefore, μ_Q satisfies Condition (4). Thus μ_Q is a Haar measure on G. Since $\mu_Q(\mathbb{T}) = \mu(t^Q\mathbb{T}) = \hat{Q}$, from Theorem 43 we have $\mu_Q = \hat{Q}\mu$. □

Lemma 46. *Let $\varphi = \sum_{i=1}^{n} r_i\chi_{E_i}$ be a non-negative simple function and X a measurable subset of G. Then*

$$\hat{Q}\int_{t^{-Q}X}\varphi(t^Q\alpha)d\alpha = \int_X \varphi(\alpha)d\alpha.$$

Proof. Note that

$$\varphi(t^Q\alpha) = \sum_{i=1}^{n} r_i\chi_{E_i}(t^Q\alpha) = \sum_{i=1}^{n} r_i\chi_{t^{-Q}E_i}(\alpha).$$

Thus

$$\int_{t^{-Q}X}\varphi(t^Q\alpha)d\alpha = \sum_{i=1}^{n} r_i\mu\big(t^{-Q}E_i \cap t^{-Q}X\big).$$

Therefore

$$\begin{aligned}\int_X \varphi(\alpha)d\alpha &= \sum_{i=1}^{n} r_i\mu(E_i\cap X) = \sum_{i=1}^{n} r_i\mu_Q\big(t^{-Q}(E_i\cap X)\big)\\ &= \hat{Q}\sum_{i=1}^{n} r_i\mu\big(t^{-Q}E_i\cap t^{-Q}X\big)\\ &= \hat{Q}\int_{t^{-Q}X}\varphi(t^Q\alpha)d\alpha.\end{aligned}$$

This completes the proof of the lemma. □

Lemma 47. *Let $Q \in \mathbb{Z}$ and $X \subseteq \mathbb{K}_\infty$ be measurable. If $f : \mathbb{K}_\infty \longrightarrow \mathbb{C}$ is integrable, then*

$$\hat{Q}\int_{t^{-Q}X} f(t^Q\alpha)d\alpha = \int_X f(\alpha)d\alpha.$$

Proof. Write $f = f_1 + if_2$ with $f_i : \mathbb{K}_\infty \longrightarrow \mathbb{R}$ $(i = 1, 2)$. Let $\{\varphi_{j,n}\}_{n\in\mathbb{N}}$ $(j = 1, 2)$ be two monotonic increasing sequences of non-negative simple functions such that $\lim_{n\to\infty}(\varphi_{1,n} -$

$\varphi_{2,n}) = f_1$. By Lemma 46, we have

$$\begin{aligned}\int_X f_1(\alpha)d\alpha &= \int_X \lim_{n\to\infty} \big(\varphi_{1,n}(\alpha) - \varphi_{2,n}(\alpha)\big)d\alpha \\ &= \lim_{n\to\infty} \left(\int_X \varphi_{1,n} d\alpha - \int_X \varphi_{2,n} d\alpha \right) \\ &= \hat{Q} \lim_{n\to\infty} \left(\int_{t^{-Q}X} \varphi_{1,n}(t^Q\alpha)d\alpha - \int_{t^{-Q}X} \varphi_{2,n}(t^Q\alpha)d\alpha \right) \\ &= \hat{Q} \int_{t^{-Q}X} \lim_{n\to\infty} \big(\varphi_{1,n}(t^Q\alpha) - \varphi_{2,n}(t^Q\alpha)\big)d\alpha \\ &= \hat{Q} \int_{t^{-Q}X} f_1(t^Q\alpha)d\alpha.\end{aligned}$$

Similarly, we have

$$\int_X f_2(\alpha)d\alpha = \hat{Q} \int_{t^{-Q}X} f_2(t^Q\alpha)d\alpha.$$

Thus

$$\int_X f(\alpha)d\alpha = \hat{Q} \int_{t^{-Q}X} f(t^Q\alpha)d\alpha.$$

This completes the proof of the lemma. □

Let $\tau : \mathbb{K}_\infty \to \mathbb{Z}$ be defined as in Section 2.5. In what follows, write

$$\tau(\mathbf{c}) = \min_{1\le j\le s} \tau(c_j).$$

For $\boldsymbol{\alpha} = (\alpha_{\mathbf{i}})_{\mathbf{i}\in\mathcal{L}}$, write

$$\tau(\boldsymbol{\alpha}) = \min_{\mathbf{i}\in\mathcal{L}} \tau(\alpha_{\mathbf{i}}) \quad \text{and} \quad F(\boldsymbol{\alpha};\mathbf{x}) = \sum_{\mathbf{i}\in\mathcal{L}} \alpha_{\mathbf{i}}\mathbf{x}^{\mathbf{i}}.$$

For $m \in \mathbb{Z}$, define

$$J_m = \{\alpha \in \mathbb{K}_\infty \,|\, \operatorname{ord}\alpha \le m\}.$$

Moreover, recall that for $\alpha \in \mathbb{K}_\infty$ and $S_1, S_2 \subseteq \mathbb{K}_\infty$,

$$\alpha S_1 = \big\{\alpha\beta \,\big|\, \beta \in S_1\big\} \quad \text{and} \quad S_1 + S_2 = \big\{\beta_1 + \beta_2 \,\big|\, \beta_i \in S_i\,(i = 1, 2)\big\}.$$

Lemma 48. *Let $m, Q \in \mathbb{Z}$. Then*

$$\int_{J_m^\iota} e\big(G(\boldsymbol{\alpha};\mathbf{x})\big)d\boldsymbol{\alpha} = \hat{Q}^{-\iota} \int_{J_{m+Q}^\iota} e\big(G(t^{-Q}\boldsymbol{\alpha};\mathbf{x})\big)d\boldsymbol{\alpha}.$$

Proof. On recalling that $G(\boldsymbol{\alpha};\mathbf{x}) = \sum_{\mathbf{i}\in\mathcal{L}} \alpha_{\mathbf{i}}\big(c_1\mathbf{x}_1^{\mathbf{i}} + \cdots + c_s\mathbf{x}_s^{\mathbf{i}}\big)$, we find from Lemma 47 that

$$\begin{aligned}\int_{J_m^\iota} e\big(G(\boldsymbol{\alpha};\mathbf{x})\big)d\boldsymbol{\alpha} &= \int_{J_m^\iota} \prod_{\mathbf{i}\in\mathcal{L}} e\Big(\alpha_{\mathbf{i}}\big(c_1\mathbf{x}_1^{\mathbf{i}} + \cdots + c_s\mathbf{x}_s^{\mathbf{i}}\big)\Big)d\boldsymbol{\alpha}\\ &= \prod_{\mathbf{i}\in\mathcal{L}} \int_{J_m} e\Big(\alpha_{\mathbf{i}}\big(c_1\mathbf{x}_1^{\mathbf{i}} + \cdots + c_s\mathbf{x}_s^{\mathbf{i}}\big)\Big)d\alpha_{\mathbf{i}}\\ &= \prod_{\mathbf{i}\in\mathcal{L}} \hat{Q}^{-1} \int_{J_{m+Q}} e\Big(t^{-Q}\alpha_{\mathbf{i}}\big(c_1\mathbf{x}_1^{\mathbf{i}} + \cdots + c_s\mathbf{x}_s^{\mathbf{i}}\big)\Big)d\alpha_{\mathbf{i}}\\ &= \hat{Q}^{-\iota} \int_{J_{m+Q}^\iota} e\Big(G(t^{-Q}\boldsymbol{\alpha},\mathbf{x})\Big)d\boldsymbol{\alpha}.\end{aligned}$$

This completes the proof of the lemma. □

Lemma 49. *Suppose that $P\in\mathbb{N}$ and $\boldsymbol{\alpha} = (\alpha_{\mathbf{i}})_{\mathbf{i}\in\mathcal{L}} \in \mathbb{K}_\infty^\iota$ such that $P + \tau(\boldsymbol{\alpha}) + \tau(\mathbf{c}) \geq 1$. Then we have*

$$\hat{P}^{-ds} \sum_{\mathbf{x}\in(t^{-P}I_P)^{ds}} e\big(G(\boldsymbol{\alpha};\mathbf{x})\big) = \int_{\mathbb{T}^{ds}} e\big(G(\boldsymbol{\alpha};\mathbf{x})\big)d\mathbf{x}.$$

Proof. Fix $\mathbf{x}\in(t^{-P}I_P)^d$ and $\mathbf{z}\in(t^{-P}\mathbb{T})^d$. Let $\mathbf{y} = \mathbf{x}+\mathbf{z}$. For every $\mathbf{i}\in\mathcal{L}$,

$$\mathbf{y}^{\mathbf{i}} - \mathbf{x}^{\mathbf{i}} = (\mathbf{x}+\mathbf{z})^{\mathbf{i}} - \mathbf{x}^{\mathbf{i}} = \sum_{\mathbf{j}\in\mathcal{R}_{\mathbf{i}}\setminus\{\mathbf{0}\}} \begin{pmatrix}\mathbf{i}\\ \mathbf{j}\end{pmatrix} \mathbf{z}^{\mathbf{j}}\mathbf{x}^{\mathbf{i}-\mathbf{j}}.$$

Since $\mathbf{x} = (x_1,\ldots,x_d)\in(t^{-P}I_P)^d$ and $\mathbf{z} = (z_1,\ldots,z_d)\in(t^{-P}\mathbb{T})^d$, for $\mathbf{i} = (i_1,\ldots,i_d)\in\mathcal{L}$ and $(j_1,\ldots,j_d)\in\mathcal{R}_{\mathbf{i}}\setminus\{\mathbf{0}\}$, we have

$$\operatorname{ord}\mathbf{x}^{\mathbf{i}-\mathbf{j}} = \operatorname{ord} x_1^{i_1-j_1}\cdots x_d^{i_d-j_d} \leq 0,$$

and

$$\operatorname{ord}\mathbf{z}^{\mathbf{j}} = \operatorname{ord} z_1^{j_1}\cdots z_d^{j_d} \leq -P-1.$$

Thus,

$$\operatorname{ord}\big(\mathbf{y}^{\mathbf{i}} - \mathbf{x}^{\mathbf{i}}\big) \leq \max_{\mathbf{j}\in\mathcal{R}_{\mathbf{i}}\setminus\{0\}} \operatorname{ord}\big(\mathbf{z}^{\mathbf{j}}\mathbf{x}^{\mathbf{i}-\mathbf{j}}\big) \leq \max_{\mathbf{j}\in\mathcal{R}_{\mathbf{i}}\setminus\{0\}} \operatorname{ord}\mathbf{z}^{\mathbf{j}} \leq -P-1.$$

On recalling $F(\boldsymbol{\alpha};\mathbf{x}) = \sum_{\mathbf{i}\in\mathcal{L}} \alpha_{\mathbf{i}}\mathbf{x}^{\mathbf{i}}$, we find that

$$\operatorname{ord}\big(F(\boldsymbol{\alpha};\mathbf{y}) - F(\boldsymbol{\alpha};\mathbf{x})\big) \leq \max_{\mathbf{i}\in\mathcal{L}} \operatorname{ord}\boldsymbol{\alpha}_{\mathbf{i}} - P - 1 = -\tau(\boldsymbol{\alpha}) - P - 1.$$

Thus for each $\mathbf{x}_j \in (t^{-P}I_P)^d$ and $\mathbf{y}_j \in \mathbf{x}_j + (t^{-P}\mathbb{T})^d$ $(1 \le j \le s)$, we have

$$\begin{aligned}\operatorname{ord}\big(G(\boldsymbol{\alpha};\mathbf{y}) - G(\boldsymbol{\alpha};\mathbf{x})\big) &= \operatorname{ord}\sum_{j=1}^{s} c_j\big(F(\boldsymbol{\alpha};\mathbf{y}_j) - F(\boldsymbol{\alpha};\mathbf{x}_j)\big)\\ &\le \max_{1\le j\le s} \operatorname{ord} c_j\big(F(\boldsymbol{\alpha};\mathbf{y}_j) - F(\boldsymbol{\alpha};\mathbf{x}_j)\big)\\ &\le -\tau(\mathbf{c}) - \tau(\boldsymbol{\alpha}) - P - 1.\end{aligned}$$

Since $P+\tau(\boldsymbol{\alpha})+\tau(\mathbf{c}) \ge 1$, it follows that $\operatorname{ord}\big(G(\boldsymbol{\alpha};\mathbf{y})-G(\boldsymbol{\alpha};\mathbf{x})\big) \le -2$. Hence $e\big(G(\boldsymbol{\alpha};\mathbf{y})-G(\boldsymbol{\alpha};\mathbf{x})\big) = 1$, i.e., $e\big(G(\boldsymbol{\alpha};\mathbf{y})\big) = e\big(G(\boldsymbol{\alpha};\mathbf{x})\big)$. Therefore, for each $\mathbf{x} = (\mathbf{x}_1,\dots,\mathbf{x}_s) \in (t^{-P}I_P)^{ds}$, we have

$$\begin{aligned}\hat{P}^{-ds} e\big(G(\boldsymbol{\alpha};\mathbf{x})\big) &= e\big(G(\boldsymbol{\alpha};\mathbf{x})\big)\int_{\mathbf{x}+(t^{-P}\mathbb{T})^{ds}} 1 d\mathbf{y}\\ &= \int_{\mathbf{x}+(t^{-P}\mathbb{T})^{ds}} e\big(G(\boldsymbol{\alpha};\mathbf{x})\big) d\mathbf{y}\\ &= \int_{\mathbf{x}+(t^{-P}\mathbb{T})^{ds}} e\big(G(\boldsymbol{\alpha};\mathbf{y})\big) d\mathbf{y}.\end{aligned} \tag{2.69}$$

On noting that $\bigsqcup_{\mathbf{x}\in(t^{-P}I_P)^{ds}} \Big(\mathbf{x} + (t^{-P}\mathbb{T})^{ds}\Big) = \mathbb{T}^{ds}$, by (2.69), we have

$$\hat{P}^{-ds} \sum_{\mathbf{x}\in(t^{-P}I_P)^{ds}} e\big(G(\boldsymbol{\alpha};\mathbf{x})\big) = \int_{\mathbb{T}^{ds}} e\big(G(\boldsymbol{\alpha};\mathbf{y})\big) d\mathbf{y}.$$

This completes the proof of the lemma. □

Lemma 50. *Let $m \in \mathbb{Z}$ and $P \in \mathbb{N}$ with $m \le (1-k)P + \tau(\mathbf{c}) - 1$. Then*

$$\int_{J_m^\iota} \prod_{j=1}^{s} f_j(\boldsymbol{\alpha};P) d\boldsymbol{\alpha} = \hat{P}^{sd-\iota k} \int_{J_{m+kP}^\iota} \bigg(\int_{\mathbb{T}^{ds}} e\big(G(\boldsymbol{\alpha};\mathbf{x})\big) d\mathbf{x} \bigg) d\boldsymbol{\alpha}.$$

Proof. On recalling $\displaystyle\prod_{j=1}^{s} f_j(\boldsymbol{\alpha};P) = \sum_{\mathbf{x}\in I_P^{ds}} e\big(G(\boldsymbol{\alpha};\mathbf{x})\big)$, we deduce from Lemma 48 that

$$\begin{aligned}\int_{J_m^\iota} \prod_{j=1}^{s} f_j(\boldsymbol{\alpha};P) d\boldsymbol{\alpha} &= \sum_{\mathbf{x}\in I_P^{ds}} \int_{J_m^\iota} e\big(G(\boldsymbol{\alpha};\mathbf{x})\big) d\boldsymbol{\alpha}\\ &= \hat{P}^{-k\iota} \sum_{\mathbf{x}\in I_P^{ds}} \int_{J_{m+kP}^\iota} e\big(G(t^{-kP}\boldsymbol{\alpha};\mathbf{x})\big) d\boldsymbol{\alpha}\\ &= \hat{P}^{-k\iota} \int_{J_{m+kP}^\iota} \sum_{\mathbf{x}\in I_P^{ds}} e\big(G(t^{-kP}\boldsymbol{\alpha};\mathbf{x})\big) d\boldsymbol{\alpha}.\end{aligned} \tag{2.70}$$

On letting $\mathbf{y} = t^{-P}\mathbf{x}$, we see that

$$\begin{aligned}\sum_{\mathbf{x}\in I_P^{ds}} e\big(G(t^{-kP}\boldsymbol{\alpha};\mathbf{x})\big) &= \sum_{\mathbf{x}\in I_P^{ds}} e\bigg(\sum_{\mathbf{i}\in\mathcal{L}} t^{-kP}\alpha_{\mathbf{i}}\big(c_1\mathbf{x}_1^{\mathbf{i}} + \cdots + c_s\mathbf{x}_s^{\mathbf{i}}\big)\bigg)\\ &= \sum_{\mathbf{y}\in(t^{-P}I_P)^{ds}} e\big(G(\boldsymbol{\alpha};\mathbf{y})\big).\end{aligned}$$

For $\boldsymbol{\alpha} \in J^{\iota}_{m+kP}$, we have

$$P + \tau(\boldsymbol{\alpha}) + \tau(\mathbf{c}) \geq P - (m+kP) + \tau(\mathbf{c}) = (1-k)P - m + \tau(\mathbf{c}) \geq 1.$$

It follows from (2.70) and Lemma 49 that

$$\begin{aligned}\int_{J^{\iota}_m} \prod_{j=1}^{s} f_j(\boldsymbol{\alpha};P)d\boldsymbol{\alpha} &= \hat{P}^{-k\iota}\int_{J^{\iota}_{m+kP}} \sum_{\mathbf{y}\in(t^{-P}I_P)^{ds}} e\big(G(\boldsymbol{\alpha};\mathbf{y})\big)d\boldsymbol{\alpha}\\ &= \hat{P}^{ds-k\iota}\int_{J^{\iota}_{m+kP}} \bigg(\int_{\mathbb{T}^{ds}} e\big(G(\boldsymbol{\alpha};\mathbf{y})\big)d\mathbf{y}\bigg)d\boldsymbol{\alpha}.\end{aligned}$$

This completes the proof of the lemma. □

Remark 1 Throughout, for $m, Q \in \mathbb{Z}$, define

$$\mathfrak{J}(m,Q) = \int_{J^{\iota}_{m+kQ}} \bigg(\int_{\mathbb{T}^{ds}} e\big(G(\boldsymbol{\alpha};\mathbf{y})\big)d\mathbf{y}\bigg)d\boldsymbol{\alpha}.$$

Let $P \geq 2(1-\tau(\mathbf{c}))$. For $g \in \mathbb{A}$, let

$$m_g = \begin{cases} -\operatorname{ord} g + [(\frac{1}{2}-k)P], & \text{if } \ \frac{1}{2}P \notin \mathbb{N};\\ -\operatorname{ord} g + (\frac{1}{2}-k)P - 1, & \text{otherwise.}\end{cases}$$

By recalling

$$\mathcal{B}_g = \big\{\boldsymbol{\beta} \in \mathbb{K}^{\iota}_{\infty} \,|\operatorname{ord}\beta_{\mathbf{i}} < -\operatorname{ord} g + (1/2-k)P \ (\mathbf{i}\in\mathcal{L})\big\},$$

we have $\mathcal{B}_g = J^{\iota}_{m_g}$. Since $P \geq 2(1-\tau(\mathbf{c}))$, it follows that

$$m_g \leq (1/2-k)P \leq (1-k)P + \tau(\mathbf{c}) - 1.$$

By Lemma 50, we have

$$\int_{\mathcal{B}_g} \prod_{j=1}^{s} f_j(\boldsymbol{\beta};P)d\boldsymbol{\beta} = \hat{P}^{sd-\iota k}\mathfrak{J}(m_g,P). \tag{2.71}$$

Next, we will treat $\mathfrak{J}_{s,d,k}$ and $\mathfrak{J}_{s,d,k} - \mathfrak{J}(m_g,P)$.

2.6.2 Estimates for $\mathfrak{J}_{s,d,k}$

We first show that $\mathfrak{J}_{s,d,k}$ is bounded by a constant depending on s, d, k, and q. Recall that

$$F(\boldsymbol{\alpha}; \mathbf{x}) = \sum_{\mathbf{i} \in \mathcal{L}} \alpha_{\mathbf{i}} \mathbf{x}^{\mathbf{i}},$$

and

$$f_j(\boldsymbol{\alpha}; P) = \sum_{\mathbf{x} \in I_P^d} e\big(c_j F(\boldsymbol{\alpha}; \mathbf{x})\big) \ (1 \le j \le s).$$

For $\boldsymbol{\alpha} = (\alpha_{\mathbf{i}})_{\mathbf{i} \in \mathcal{L}}$ and $P \in \mathbb{N}$, define

$$T_P(F; \boldsymbol{\alpha}) = \sum_{\mathbf{x} \in I_{-P}^d} e\big(F(\boldsymbol{\alpha}; \mathbf{x})\big).$$

Lemma 51. *Suppose that $P \in \mathbb{N}$ and $\boldsymbol{\alpha} = (\alpha_{\mathbf{i}})_{\mathbf{i} \in \mathcal{L}}$ such that $P + \tau(\boldsymbol{\alpha}) + \tau(\mathbf{c}) \ge 1$. Then we have*

$$\hat{P}^{-ds} \prod_{j=1}^{s} T_P\big(F; c_j t^{-k} \boldsymbol{\alpha}\big) = \int_{\mathbb{T}^{ds}} e\big(G(\boldsymbol{\alpha}; \mathbf{x})\big) d\mathbf{x}.$$

Proof. By Lemma 49, we have

$$\hat{P}^{-ds} \sum_{\mathbf{x} \in (t^{-P} I_P)^{ds}} e\big(G(\boldsymbol{\alpha}; \mathbf{x})\big) = \int_{\mathbb{T}^{ds}} e\big(G(\boldsymbol{\alpha}; \mathbf{x})\big) d\mathbf{x}.$$

It remains to show that

$$\sum_{\mathbf{x} \in (t^{-P} I_P)^{ds}} e\big(G(\boldsymbol{\alpha}; \mathbf{x})\big) = \prod_{j=1}^{s} T_P\big(F; c_j t^{-k} \boldsymbol{\alpha}\big).$$

Since $G(\boldsymbol{\alpha}; \mathbf{x}) = \sum_{j=1}^{s} c_j F(\boldsymbol{\alpha}; \mathbf{x}_j)$, it follows that

$$\sum_{\mathbf{x} \in (t^{-P} I_P)^{ds}} e\big(G(\boldsymbol{\alpha}; \mathbf{x})\big) = \prod_{j=1}^{s} \sum_{\mathbf{x}_j \in (t^{-P} I_P)^d} e\big(c_j F(\boldsymbol{\alpha}; \mathbf{x}_j)\big). \tag{2.72}$$

On letting $\mathbf{x}_j = t^{-1} \mathbf{y}_j \, (1 \le j \le s)$, we see that $\mathbf{x}_j \in (t^{-P} I_P)^d$ if and only if $\mathbf{y}_j \in I_{-P}^d$. Thus,

$$\sum_{\mathbf{x}_j \in (t^{-P} I_P)^d} e\big(c_j F(\boldsymbol{\alpha}; \mathbf{x}_j)\big) = \sum_{\mathbf{y}_j \in I_{-P}^d} e\big(c_j F(\boldsymbol{\alpha}; t^{-1} \mathbf{y}_j)\big) \ (1 \le j \le s).$$

Note that for each j with $1 \le j \le s$,

$$c_j F(\boldsymbol{\alpha}; t^{-1}\mathbf{y}_j) = c_j \sum_{\mathbf{i}\in\mathcal{L}} \alpha_{\mathbf{i}} (t^{-1}\mathbf{y}_j)^{\mathbf{i}} = c_j t^{-k} \sum_{\mathbf{i}\in\mathcal{L}} \alpha_{\mathbf{i}} \mathbf{y}_j^{\mathbf{i}} = F(c_j t^{-k}\boldsymbol{\alpha}; \mathbf{y}). \tag{2.73}$$

We deduce from (2.72) and (2.73) that

$$\sum_{\mathbf{x}\in(t^{-P}I_P)^{ds}} e\big(G(\boldsymbol{\alpha};\mathbf{x})\big) = \prod_{j=1}^{s} \sum_{\mathbf{y}_j\in I_{-P}^d} e\big(F(c_j t^{-k}\boldsymbol{\alpha};\mathbf{y})\big) = \prod_{j=1}^{s} T_P\big(F; c_j t^{-k}\boldsymbol{\alpha}\big).$$

This completes the proof of the lemma. □

Lemma 52. *Let* $E = \frac{s}{\iota}\big(\frac{1}{2k} - \epsilon(d-1)\big) \in \mathbb{R}$ *with* $\epsilon(d-1) \in (0, \frac{1}{2k})$. *Then there exists a constant* $C = C(s,k,d;q;\mathbf{c};\epsilon) > 0$ *such that*

$$\left| \int_{\mathbb{T}^{ds}} e\big(G(\boldsymbol{\alpha};\mathbf{x})\big) d\mathbf{x} \right| \le C \prod_{\mathbf{i}\in\mathcal{L}} \big(1 + \langle \alpha_{\mathbf{i}} \rangle\big)^{-E}.$$

Proof. Recall that $\tau(\boldsymbol{\alpha}) = \min_{\mathbf{i}\in\mathcal{L}} \tau(\boldsymbol{\alpha}_{\mathbf{i}})$. We now consider two cases.

Case 1: $\tau(\boldsymbol{\alpha}) > -k$, i.e., $\tau(\alpha_{\mathbf{i}}) > -k$ ($\mathbf{i} \in \mathcal{L}$). Hence

$$\langle \alpha_{\mathbf{i}} \rangle = q^{-\tau(\alpha_{\mathbf{i}})} < q^k \ (\mathbf{i} \in \mathcal{L}).$$

Thus

$$\left| \int_{\mathbb{T}^{ds}} e\big(G(\boldsymbol{\alpha};\mathbf{x})\big) d\mathbf{x} \right| \le 1 < (1+q^k)^{\iota E} \prod_{\mathbf{i}\in\mathcal{L}} \big(1 + \langle \alpha_{\mathbf{i}} \rangle\big)^{-E}. \tag{2.74}$$

Case 2: $\tau(\boldsymbol{\alpha}) \le -k$. Take $P \in \mathbb{N}$ with $P + \tau(\boldsymbol{\alpha}) + \tau(\mathbf{c}) \ge 1$. Fix $j \in \mathbb{N}$ with $1 \le j \le s$. Since $\tau(\mathbf{c}) \le \tau(c_j) \le 0$, we have

$$\tau(\mathbf{c}) + k + \tau(\boldsymbol{\alpha}) \le \tau(c_j t^{-k}\boldsymbol{\alpha}) = \tau(c_j) + k + \tau(\boldsymbol{\alpha}) \le 0$$

and

$$P + \tau(c_j t^{-k}\boldsymbol{\alpha}) \ge P + \tau(\boldsymbol{\alpha}) + \tau(\mathbf{c}) + k \ge 1 + k \ge 2.$$

Thus we deduce from Lemma 39 that

$$\begin{aligned} \big|T_P(F; c_j t^{-k}\boldsymbol{\alpha})\big| &\le (-\tau(c_j t^{-k}\boldsymbol{\alpha}) + 2)^{d-1} \cdot q^{(k+1)d + Pd - \frac{1-\tau(c_j t^{-k}\boldsymbol{\alpha})}{2k}} \\ &\le (-\tau(\mathbf{c}) - k - \tau(\boldsymbol{\alpha}) + 2)^{d-1} \cdot q^{(k+1)d + Pd - \frac{1-k-\tau(\boldsymbol{\alpha})}{2k}} \\ &< (-\tau(\mathbf{c}) - k - \tau(\boldsymbol{\alpha}) + 2)^{d-1} \cdot q^{(k+1)d + \frac{\tau(\boldsymbol{\alpha})+k}{2k}} \hat{P}^d. \end{aligned}$$

For any $\epsilon > 0$, since $\lim_{x\to\infty} \frac{-\tau(\mathbf{c})+\log_q x+2}{x^\epsilon} = 0$, there exits $C_1 = C_1(q;\mathbf{c};\epsilon) > 0$ such that

$$(-\tau(\mathbf{c}) + \log_q x + 2)^{d-1} \le C_1^{d-1} x^{\epsilon(d-1)}$$

for $x \ge 1$. Since $q^{-\tau(\boldsymbol{\alpha})-k} \ge 1$, on letting $C_2 = C_1^{d-1} q^{(k+1)d}$, we have

$$\begin{aligned}(-\tau(\mathbf{c}) - k - \tau(\boldsymbol{\alpha}) + 2)^{d-1} q^{(k+1)d+\frac{\tau(\boldsymbol{\alpha})+k}{2k}} &\le C_2\big(q^{-\tau(\boldsymbol{\alpha})-k}\big)^{\epsilon(d-1)} q^{\frac{\tau(\boldsymbol{\alpha})+k}{2k}} \\ &= C_2 q^{(\tau(\boldsymbol{\alpha})+k)(\frac{1}{2k}-\epsilon(d-1))}.\end{aligned}$$

Thus

$$|T_P(F; c_j t^{-k}\boldsymbol{\alpha})| \le C_2 q^{(\tau(\boldsymbol{\alpha})+k)(\frac{1}{2k}-\epsilon(d-1))} \hat{P}^d. \tag{2.75}$$

Since $\tau(\boldsymbol{\alpha}) \le 0$, we have $q^{\tau(\boldsymbol{\alpha})}\big(1 + q^{-\tau(\boldsymbol{\alpha})}\big) \le 2$. Since $\frac{1}{2k} - \epsilon(d-1) > 0$, we see that

$$q^{\tau(\boldsymbol{\alpha})(\frac{1}{2k}-\epsilon(d-1))} \le 2^{\frac{1}{2k}-\epsilon(d-1)}\big(1 + q^{-\tau(\boldsymbol{\alpha})}\big)^{-(\frac{1}{2k}-\epsilon(d-1))}.$$

On letting $C_3 = C_2(2q^k)^{\frac{1}{2k}-\epsilon(d-1)}$, we deduce from (2.75) that

$$|T_P(F; c_j t^{-k}\boldsymbol{\alpha})| \le C_3\big(1 + q^{-\tau(\boldsymbol{\alpha})}\big)^{-(\frac{1}{2k}-\epsilon(d-1))} \hat{P}^d. \tag{2.76}$$

On noting that $-\tau(\boldsymbol{\alpha}) \ge -\tau(\alpha_{\mathbf{i}})$ $(\mathbf{i} \in \mathcal{L})$, we find that

$$1 + q^{-\tau(\boldsymbol{\alpha})} \ge \prod_{\mathbf{i}\in\mathcal{L}} \Big(1 + q^{-\tau(\alpha_{\mathbf{i}})}\Big)^{\frac{1}{\iota}} = \prod_{\mathbf{i}\in\mathcal{L}} \big(1 + \langle\alpha_{\mathbf{i}}\rangle\big)^{\frac{1}{\iota}}.$$

It follows from (2.76) that

$$|T_P(F; c_j t^{-k}\boldsymbol{\alpha})| \le \hat{P}^d C_3 \prod_{\mathbf{i}\in\mathcal{L}} \big(1 + \langle\alpha_{\mathbf{i}}\rangle\big)^{-\frac{1}{\iota}(\frac{1}{2k}-\epsilon(d-1))}.$$

Since $E = \frac{s}{\iota}(\frac{1}{2k} - \epsilon(d-1))$, by Lemma 51, we have

$$\left|\int_{\mathbb{T}^{ds}} e\big(G(\boldsymbol{\alpha};\mathbf{x})\big)d\mathbf{x}\right| = \hat{P}^{-ds}\left|\prod_{j=1}^{s} T_P(F; c_j t^{-k}\boldsymbol{\alpha})\right| \le C_3^s \prod_{\mathbf{i}\in\mathcal{L}} \big(1 + \langle\alpha_{\mathbf{i}}\rangle\big)^{-E}. \tag{2.77}$$

On letting $C = \max(C_3^s,\ (1+q^k)^{\iota E})$ and combining Case 1 with Case 2, we have

$$\left|\int_{\mathbb{T}^{ds}} e\big(G(\boldsymbol{\alpha};\mathbf{x})\big)d\mathbf{x}\right| \le C \prod_{\mathbf{i}\in\mathcal{L}} \big(1 + \langle\alpha_{\mathbf{i}}\rangle\big)^{-E}.$$

This completes the proof of the lemma. □

Lemma 53. *For $m \in \mathbb{Z}$, let $J_m = \{\alpha \in \mathbb{K}_\infty \,|\, \operatorname{ord}\alpha \le m\}$. If $m \in \mathbb{N}$, then*

$$\int_{J_m} \big(1+\langle\alpha\rangle\big)^{-E} d\alpha = \int_{\mathbb{T}} \big(1+\langle\alpha\rangle\big)^{-E} d\alpha + (q-1)\sum_{v=0}^{m} q^v (1+q^v)^{-E}.$$

Proof. For each $m \in \mathbb{N}$, we have

$$J_m = \big\{\alpha \in \mathbb{K}_\infty \,\big|\, \operatorname{ord}\alpha \le m\big\} = \mathbb{T} \bigsqcup \bigg(\bigsqcup_{v=0}^{m} \bigsqcup_{\substack{x\in\mathbb{A}\\ \operatorname{ord} x = v}} \big(x+\mathbb{T}\big)\bigg).$$

Note that for each $x \in \mathbb{A}$ with $\operatorname{ord} x = v$,

$$\int_{x+\mathbb{T}} \big(1+\langle\alpha\rangle\big)^{-E} d\alpha = (1+q^v)^{-E} \int_{x+\mathbb{T}} 1 d\alpha = (1+q^v)^{-E}.$$

Since $\operatorname{card}\{x \in \mathbb{A} \,|\, \operatorname{ord} x = v\} = (q-1)q^v$, we obtain that

$$\begin{aligned}\int_{J_m} \big(1+\langle\alpha\rangle\big)^{-E} d\alpha &= \int_{\mathbb{T}} \big(1+\langle\alpha\rangle\big)^{-E} d\alpha + \sum_{v=0}^{m} \sum_{\substack{x\in\mathbb{A}\\ \operatorname{ord} x = v}} \int_{x+\mathbb{T}} \big(1+\langle\alpha\rangle\big)^{-E} d\alpha \\ &= \int_{\mathbb{T}} \big(1+\langle\alpha\rangle\big)^{-E} d\alpha + (q-1)\sum_{v=0}^{m} q^v (1+q^v)^{-E}.\end{aligned}$$

This completes the proof of the lemma. □

Lemma 54. *For $m \in \mathbb{Z}$, let $J_m = \{\alpha \in \mathbb{K}_\infty \,|\, \operatorname{ord}\alpha \le m\}$. Whenever $s > 2k\iota$, there exist two constants $C = C(s,k,d;q;\mathbf{c}) > 0$ and $\tilde{C} = \tilde{C}(s,k,d;q;\mathbf{c}) > 0$ such that the following inequalities hold.*

(1) $\big|\mathfrak{J}\big| \le \displaystyle\int_{\mathbb{K}_\infty^\iota} \bigg| \int_{\mathbb{T}^{ds}} e\big(G(\boldsymbol{\alpha};\mathbf{x})\big) d\mathbf{x} \bigg| d\boldsymbol{\alpha} \le C.$

(2) $\displaystyle\int_{\mathbb{K}_\infty^\iota \setminus J_m^\iota} \bigg| \int_{\mathbb{T}^{ds}} e\big(G(\boldsymbol{\alpha};\mathbf{x})\big) d\mathbf{x} \bigg| d\boldsymbol{\alpha} \le \tilde{C} q^{-(m+1)/(3k\iota)} \quad (m \in \mathbb{N}).$

Proof. (1) Recall that

$$\mathfrak{J} = \int_{\mathbb{K}_\infty^\iota} \int_{\mathbb{T}^{ds}} e\big(G(\boldsymbol{\alpha};\mathbf{x})\big) d\mathbf{x} d\boldsymbol{\alpha}.$$

Then

$$\big|\mathfrak{J}\big| \le \int_{\mathbb{K}_\infty^\iota} \bigg| \int_{\mathbb{T}^{ds}} e\big(G(\boldsymbol{\alpha};\mathbf{x})\big) d\mathbf{x} \bigg| d\boldsymbol{\alpha}.$$

Take $\epsilon = \big(6kd(2k\iota+1)\big)^{-1}$ and let $E = \frac{s}{\iota}\big(\frac{1}{2k} - \epsilon(d-1)\big)$. By Lemma 52, there exists $C_1 > 0$ such that

$$\bigg| \int_{\mathbb{T}^{ds}} e\big(G(\boldsymbol{\alpha};\mathbf{x})\big) d\mathbf{x} \bigg| \le C_1 \prod_{\mathbf{i}\in\mathcal{L}} \big(1+\langle\alpha_{\mathbf{i}}\rangle\big)^{-E}. \tag{2.78}$$

Thus

$$\begin{aligned}\int_{\mathbb{K}_\infty^\iota}\bigg|\int_{\mathbb{T}^{ds}} e\big(G(\boldsymbol{\alpha};\mathbf{x})\big)d\mathbf{x}\bigg|d\boldsymbol{\alpha} &\le C_1\int_{\mathbb{K}_\infty^\iota}\prod_{\mathbf{i}\in\mathcal{L}}\big(1+\langle\alpha_{\mathbf{i}}\rangle\big)^{-E}d\boldsymbol{\alpha}\\ &= C_1\prod_{\mathbf{i}\in\mathcal{L}}\int_{\mathbb{K}_\infty}\big(1+\langle\alpha_{\mathbf{i}}\rangle\big)^{-E}d\alpha_{\mathbf{i}}\\ &= C_1\bigg(\int_{\mathbb{K}_\infty}\big(1+\langle\alpha\rangle\big)^{-E}d\alpha\bigg)^{\iota}.\end{aligned}\tag{2.79}$$

Since $\mathbb{K}_\infty=\cup_{m\ge0}J_m$ and $J_m\subset J_{m+1}$, we deduce from Lemma 53 that

$$\begin{aligned}\int_{\mathbb{K}_\infty}\big(1+\langle\alpha\rangle\big)^{-E}d\alpha &= \lim_{m\to\infty}\int_{J_m}\big(1+\langle\alpha\rangle\big)^{-E}d\alpha\\ &= \int_{\mathbb{T}}\big(1+\langle\alpha\rangle\big)^{-E}d\alpha+(q-1)\sum_{v=0}^{\infty}q^v(1+q^v)^{-E}.\end{aligned}\tag{2.80}$$

Since $E>0$ and $1+\langle\alpha\rangle>1$, we see that $\int_{\mathbb{T}}\big(1+\langle\alpha\rangle\big)^{-E}d\alpha<1$. Moreover, whenever $s\ge2k\iota+1$, we have

$$E=\frac{s}{\iota}\Big(\frac{1}{2k}-\frac{d-1}{6dk(2k\iota+1)}\Big)>\frac{2k\iota+1}{\iota}\Big(\frac{1}{2k}-\frac{1}{6k(2k\iota+1)}\Big)=1+\frac{1}{3k\iota}.$$

Hence

$$(q-1)\sum_{v=0}^{\infty}q^v(1+q^v)^{-E}<(q-1)\sum_{v=0}^{\infty}q^{v(1-E)}<\infty.$$

It follows from (2.80) that

$$\int_{\mathbb{K}_\infty}\big(1+\langle\alpha\rangle\big)^{-E}d\alpha<1+(q-1)\sum_{v=0}^{\infty}q^{v(1-E)}<\infty.$$

On letting $C=C_1\Big(\int_{\mathbb{K}_\infty}\big(1+\langle\alpha\rangle\big)^{-E}d\alpha\Big)^{\iota}$, we can deduce from (2.79) that

$$\int_{\mathbb{K}_\infty^\iota}\bigg|\int_{\mathbb{T}^{ds}} e\big(G(\boldsymbol{\alpha};\mathbf{x})\big)d\mathbf{x}\bigg|d\boldsymbol{\alpha}\le C.$$

(2) Fix $m\in\mathbb{N}$. Since $\mathbb{K}_\infty^\iota\setminus J_m^\iota=\bigcup_{\mathbf{i}\in\mathcal{L}}\big\{\boldsymbol{\alpha}\in\mathbb{K}_\infty^\iota\,\big|\,\operatorname{ord}\alpha_{\mathbf{i}}>m\big\}$, from (2.78), we have

that

$$\begin{aligned}
&\int_{\mathbb{K}_\infty^\iota \setminus J_m^\iota} \Big| \int_{\mathbb{T}^{ds}} e\big(G(\boldsymbol{\alpha};\mathbf{x})\big) d\mathbf{x} \Big| d\boldsymbol{\alpha} \\
\le &\int_{\mathbb{K}_\infty^\iota \setminus J_m^\iota} C_1 \prod_{\mathbf{i}\in\mathcal{L}} \big(1+\langle \alpha_{\mathbf{i}}\rangle\big)^{-E} d\boldsymbol{\alpha} \\
\le &C_1 \sum_{\mathbf{i}\in\mathcal{L}} \bigg(\int_{\mathbb{K}_\infty} \big(1+\langle\alpha\rangle\big)^{-E} d\alpha \bigg)^{\iota-1} \int_{\operatorname{ord}\alpha_{\mathbf{i}}>m} \big(1+\langle\alpha_{\mathbf{i}}\rangle\big)^{-E} d\alpha_{\mathbf{i}} \\
\le &\iota C_1 \bigg(\int_{\mathbb{K}_\infty} \big(1+\langle\alpha\rangle\big)^{-E} d\alpha \bigg)^{\iota-1} \int_{\operatorname{ord}\alpha>m} \big(1+\langle\alpha\rangle\big)^{-E} d\alpha.
\end{aligned}$$

On combining Lemma 53 with (2.80) and recalling $E \ge 1+(3k\iota)^{-1}$, we find that

$$\begin{aligned}
\int_{\operatorname{ord}\alpha>m} \big(1+\langle\alpha\rangle\big)^{-E} d\alpha &= (q-1) \sum_{u=m+1}^{\infty} q^u (1+q^u)^{-E} \\
&< (q-1) \sum_{u=m+1}^{\infty} q^{(1-E)u} \\
&= q^{(1-E)(m+1)} (q-1) \sum_{u=0}^{\infty} q^{(1-E)u} \\
&\le q^{-(m+1)/(3k\iota)} (q-1) \sum_{u=0}^{\infty} q^{-u/(3k\iota)}.
\end{aligned}$$

On letting $\tilde{C} = \iota C_1 \Big(\int_{\mathbb{K}_\infty} \big(1+\langle\alpha\rangle\big)^{-E} d\alpha \Big)^{\iota-1} (q-1) \sum_{u=0}^{\infty} q^{-u/(3k\iota)}$, we have

$$\int_{\mathbb{K}_\infty^\iota \setminus J_m^\iota} \Big| \int_{\mathbb{T}^{ds}} e\big(G(\boldsymbol{\alpha};\mathbf{x})\big) d\mathbf{x} \Big| d\boldsymbol{\alpha} \le \tilde{C} q^{-(m+1)/(3k\iota)}.$$

This completes the proof of the lemma. □

Next, we aim to show that $\mathfrak{J}_{s,k,d} > 0$.

Lemma 55. *For $P, m \in \mathbb{N}$, define*

$$V_s(P;m) = \operatorname{card}\big\{ \mathbf{x} \in I_P^{ds} \;\big|\; \operatorname{ord}\left(c_1 \mathbf{x}_1^{\mathbf{i}} + \cdots + c_s \mathbf{x}_s^{\mathbf{i}}\right) < m \ (\mathbf{i} \in \mathcal{L}) \big\}.$$

Suppose that the system $c_1 \mathbf{x}_1^{\mathbf{i}} + \cdots + c_s \mathbf{x}_s^{\mathbf{i}} = 0$ $(\mathbf{i} \in \mathcal{L})$ has a non-singular solution $\boldsymbol{\eta} \in \mathbb{K}_\infty^{ds}$. Let $m' = -m + k(P-1) - \tau(\mathbf{c}) + 1$. Then there exists an integer $u = u(\mathbf{c}, \boldsymbol{\eta})$ such that whenever $u \le m' \le P$, we have

$$V_s(P;m) \ge q^{(P-u)ds - (m'-u)\iota}.$$

Proof. For each j with $1 \le j \le s$, let

$$\tilde{c}_j = t^{\tau(\mathbf{c})} c_j \quad \text{and} \quad \mathbf{y}_j = t^{-P+1}\mathbf{x}_j.$$

Then for every $\mathbf{i} \in \mathcal{L}$, we have

$$\begin{aligned} c_1\mathbf{x}_1^{\mathbf{i}} + \cdots + c_s\mathbf{x}_s^{\mathbf{i}} &= t^{-\tau(\mathbf{c})}\tilde{c}_1(t^{P-1}\mathbf{y}_1)^{\mathbf{i}} + \cdots + \tilde{c}_s(t^{P-1}\mathbf{y}_s)^{\mathbf{i}} \\ &= t^{-\tau(\mathbf{c})+k(P-1)}(\tilde{c}_1\mathbf{y}_1^{\mathbf{i}} + \cdots + \tilde{c}_s\mathbf{y}_s^{\mathbf{i}}). \end{aligned}$$

Since $I_{-P} = t^{-P+1}I_P$, on noting that $-m' = m + \tau(\mathbf{c}) - k(P-1) - 1$, we have

$$\begin{aligned} V_s(P;m) &= \operatorname{card}\big\{\mathbf{y} \in I_{-P}^{ds} \;\big|\; \operatorname{ord}(\tilde{c}_1\mathbf{y}_1^{\mathbf{i}} + \cdots + \tilde{c}_s\mathbf{y}_s^{\mathbf{i}}) \le -m' \ (\mathbf{i} \in \mathcal{L})\big\} \\ &= \operatorname{card}\big\{\mathbf{y} \ (\mathrm{mod}\, t^{-P}) \;\big|\; \operatorname{ord}(\tilde{c}_1\mathbf{y}_1^{\mathbf{i}} + \cdots + \tilde{c}_s\mathbf{y}_s^{\mathbf{i}}) \equiv 0 \ (\mathrm{mod}\, t^{-m'}) \ (\mathbf{i} \in \mathcal{L})\big\}. \end{aligned}$$

Write

$$U(m') = \operatorname{card}\big\{\mathbf{y} \ (\mathrm{mod}\, t^{-m'}) \;\big|\; \operatorname{ord}(\tilde{c}_1\mathbf{y}_1^{\mathbf{i}} + \cdots + \tilde{c}_s\mathbf{y}_s^{\mathbf{i}}) \equiv 0 \ (\mathrm{mod}\, t^{-m'}) \ (\mathbf{i} \in \mathcal{L})\big\}.$$

When $m' \le P$, we find that

$$V_s(P;m) = q^{(P-m')ds}U(m'). \tag{2.81}$$

By homogeneity, we can re-scale to ensure that $\boldsymbol{\eta} \in R^{ds}$. Thus the system $\tilde{c}_1\mathbf{y}_1^{\mathbf{i}} + \cdots + \tilde{c}_s\mathbf{y}_s^{\mathbf{i}} = 0 \, (\mathbf{i} \in \mathcal{L})$ has a non-singular solution in R^{ds}. It follows from Lemma 14 that there exists an integer $u = u(\mathbf{c}, \boldsymbol{\eta})$ such that whenever $m' \ge u$, we have

$$U(m') \ge q^{(m'-u)(ds-\iota)}.$$

On recalling (2.81), we see that

$$V_s(P;m) \ge q^{(P-m')ds}q^{(m'-u)(ds-\iota)} = q^{(P-u)ds-(m'-u)\iota}.$$

This completes the proof of the lemma. □

Lemma 56. *For $P, m \in \mathbb{N}$, let $V_s(P;m)$ be defined as in Lemma 55. Then*

$$\int_{J_{-m-1}^{\iota}} \prod_{j=1}^{s} f_j(\boldsymbol{\beta}; P)d\boldsymbol{\beta} = q^{-\iota m}V_s(P;m).$$

Proof. Since

$$\prod_{j=1}^{s} f_j(\boldsymbol{\beta}; P) = \sum_{\mathbf{x}\in I_P^{ds}} e\Big(\sum_{\mathbf{i}\in\mathcal{L}} \beta_{\mathbf{i}}(c_1\mathbf{x}_1^{\mathbf{i}} + \cdots + c_s\mathbf{x}_s^{\mathbf{i}})\Big),$$

we have

$$\int_{J^{\iota}_{-m-1}} \prod_{j=1}^{s} f_j(\boldsymbol{\beta}; P)d\boldsymbol{\beta} = \sum_{\mathbf{x}\in I_P^{ds}} \prod_{\mathbf{i}\in\mathcal{L}} \int_{\mathrm{ord}\,\beta_{\mathbf{i}}<-m} e\big(\beta_{\mathbf{i}}(c_1\mathbf{x}_1^{\mathbf{i}} + \cdots + c_s\mathbf{x}_s^{\mathbf{i}})\big)d\beta_{\mathbf{i}}.$$

By Lemma 3(4), for every $\mathbf{i} \in \mathcal{L}$ and $\mathbf{x} \in I_P^{ds}$, we have

$$\int_{\mathrm{ord}\,\beta_{\mathbf{i}}<-m} e\big(\beta_{\mathbf{i}}(c_1\mathbf{x}_1^{\mathbf{i}} + \cdots + c_s\mathbf{x}_s^{\mathbf{i}})\big)d\beta_{\mathbf{i}} = \begin{cases} q^{-m}, & \text{if ord}\,(c_1\mathbf{x}_1^{\mathbf{i}} + \cdots + c_s\mathbf{x}_s^{\mathbf{i}}) < m\ , \\ 0, & \text{otherwise.} \end{cases}$$

Thus

$$\int_{J^{\iota}_{-m-1}} \prod_{j=1}^{s} f_j(\boldsymbol{\beta}; P)d\boldsymbol{\beta} = q^{-\iota m}V_s(P; m).$$

□

Lemma 57. *Suppose that the system $c_1\mathbf{x}_1^{\mathbf{i}} + \cdots + c_s\mathbf{x}_s^{\mathbf{i}} = 0$ $(\mathbf{i} \in \mathcal{L})$ has a non-singular solution $\boldsymbol{\eta} \in \mathbb{K}_\infty^{ds}$. Then there exists an integer $u = u(\mathbf{c}, \boldsymbol{\eta})$ such that whenever $P \geq \max\{2(1-\tau(\mathbf{c})), 2(u+\tau(\mathbf{c})+k-1)\}$, we have*

$$\int_{J^{\iota}_{[\frac{1}{2}P]-1}} \Big(\int_{\mathbb{T}^{ds}} e\Big(G(\boldsymbol{\alpha}; \mathbf{x})\Big)d\mathbf{x}\Big)d\boldsymbol{\alpha} \geq q^{-sdu-(1-\tau(\mathbf{c})-k-u)\iota}.$$

Proof. Let $m = kP - [\frac{1}{2}P]$ and let $m' = -m + k(P-1) + 1 - \tau(\mathbf{c})$. When $P \geq 2(1-\tau(\mathbf{c}))$, we see that

$$m' = [(1/2)P] - k - \tau(\mathbf{c}) + 1 < P.$$

By Lemma 55, there exists an integer $u = u(\mathbf{c}, \boldsymbol{\eta})$ such that whenever $m' \geq u$, we have

$$V_s(P; m) \geq q^{(P-u)ds-(m'-u)\iota}.$$

When $P \geq 2(u + k + \tau(\mathbf{c}) - 1)$, we have

$$m' = [(1/2)P] - k - \tau(\mathbf{c}) + 1 \geq u.$$

Thus whenever $P \geq \max\{2(1-\tau(\mathbf{c})), 2(u+\tau(\mathbf{c})+k-1)\}$, it follows from Lemma 56 that

$$\begin{aligned}\int_{J^\iota_{-m-1}} \prod_{j=1}^{s} f_j(\boldsymbol{\beta}; P) d\boldsymbol{\beta} &= q^{-\iota m} V_s(P; m) \\ &\geq q^{(P-u)ds-(m'-u)\iota-\iota m} \\ &= q^{(P-u)ds-(kP+1-\tau(\mathbf{c})-k-u)\iota} \\ &= q^{-sdu-(1-\tau(\mathbf{c})-k-u)\iota} \hat{P}^{sd-k\iota}.\end{aligned}$$

Since

$$-m-1 = -kP + [(1/2)P] - 1 \leq (1-k)P + \tau(\mathbf{c}) - 1,$$

we obtain from Lemma 50 that

$$\int_{J^\iota_{-m-1}} \prod_{j=1}^{s} f_j(\boldsymbol{\beta}; P) d\boldsymbol{\beta} = \hat{P}^{sd-\iota k} \int_{J^\iota_{-m-1+kP}} \bigg(\int_{\mathbb{T}^{ds}} e\Big(G(\boldsymbol{\alpha}; \mathbf{x})\Big) d\mathbf{x} \bigg) d\boldsymbol{\alpha}.$$

On noting that $-m-1+kP = [\frac{1}{2}P] - 1$, we see that

$$\int_{J^\iota_{[\frac{1}{2}P]-1}} \bigg(\int_{\mathbb{T}^{ds}} e\Big(G(\boldsymbol{\alpha}; \mathbf{x})\Big) d\mathbf{x} \bigg) d\boldsymbol{\alpha} \geq q^{-sdu-(1-\tau(\mathbf{c})-k-u)\iota}.$$

□

Theorem 58. *Suppose that the system $c_1\mathbf{x}_1^{\mathbf{i}} + \cdots + c_s\mathbf{x}_s^{\mathbf{i}} = 0$ $(\mathbf{i} \in \mathcal{L})$ has a non-singular solution in $\mathbb{K}_\infty$. Then*

$$\mathfrak{J} = \int_{\mathbb{K}^\iota_\infty} \bigg(\int_{\mathbb{T}^{ds}} e\Big(G(\boldsymbol{\alpha}; \mathbf{x})\Big) d\mathbf{x} \bigg) d\boldsymbol{\alpha} > 0.$$

Proof. Let $m = kP - [\frac{1}{2}P]$. Then $-m-1+kP = [\frac{1}{2}P] - 1$. Recall that for $n, Q \in \mathbb{Z}$,

$$\mathfrak{J}(n, Q) = \int_{J^\iota_{n+kQ}} \bigg(\int_{\mathbb{T}^{ds}} e\big(G(\boldsymbol{\alpha}; \mathbf{y})\big) d\mathbf{y} \bigg) d\boldsymbol{\alpha}.$$

By Lemma 54(2), we deduce that

$$\big|\mathfrak{J} - \mathfrak{J}(-m-1, P)\big| \ll q^{-([\frac{1}{2}P])/(3k\iota)} < q\hat{P}^{-1/(6k\iota)}.$$

From Lemma 57, there exists an integer u such that

$$\mathfrak{J} = \lim_{P\to\infty} \mathfrak{J}(-m-1, P) \geq q^{-sdu-(1-\tau(\mathbf{c})-k-u)\iota} > 0.$$

This completes the proof of the theorem. □

2.7 The major arc contribution

We are now in a position to obtain asymptotic estimates for the contribution of the major arcs.

Theorem 59. *Suppose that for every irreducible element $w \in \mathbb{A}$, the system*

$$c_1\mathbf{x}_1^{\mathbf{i}} + \cdots + c_s\mathbf{x}_s^{\mathbf{i}} = 0 \ (\mathbf{i} \in \mathcal{L})$$

has a non-singular w-adic solution. Further suppose that this system has a non-singular solution in $\mathbb{K}_\infty$. When $s > 2k(\iota+1)$, we have

$$\int_{\mathfrak{M}} \prod_{j=1}^{s} f_j(\boldsymbol{\alpha}; P)d\boldsymbol{\alpha} = \mathfrak{J}\mathfrak{S}\hat{P}^{sd-\iota k} + O\big(\hat{P}^{sd-\iota k-\delta}\big)$$

where $0 < \mathfrak{J}\mathfrak{S} \ll 1$ and $\delta = \frac{1}{18k\iota}$.

Proof. By Lemma 6, we have

$$\int_{\mathfrak{M}} \prod_{j=1}^{s} f_j(\boldsymbol{\alpha})d\boldsymbol{\alpha} = \sum_{\substack{\langle g\rangle \le \langle c\rangle \hat{P}^{\frac{1}{2}} \\ g \text{ monic}}} \sum_{\mathbf{a}\in\mathcal{A}_g} \Big(\prod_{j=1}^{s} \langle g\rangle^{-d} S_j(g, \mathbf{a}) \Big) \int_{\mathcal{B}_g} \prod_{j=1}^{s} f_j(\boldsymbol{\beta})d\boldsymbol{\beta}.$$

Let $P \ge 2(1-\tau(\mathbf{c}))$. For $g \in \mathbb{A}$, let

$$m_g = \begin{cases} -\operatorname{ord} g + [(\frac{1}{2} - k)P], & \text{if } \ \frac{1}{2}P \notin \mathbb{N}, \\ -\operatorname{ord} g + (\frac{1}{2} - k)P - 1, & \text{otherwise.} \end{cases} \tag{2.82}$$

On recalling (2.71), we obtain

$$\int_{\mathcal{B}_g} \prod_{j=1}^{s} f_j(\boldsymbol{\beta}; P)d\boldsymbol{\beta} = \hat{P}^{sd-\iota k}\mathfrak{J}(m_g, P).$$

On letting $Q = -\tau(\mathbf{c}) + \frac{1}{2}P$, we deduce that

$$\begin{aligned} \int_{\mathfrak{M}} \prod_{j=1}^{s} f_j(\boldsymbol{\alpha}; P)d\boldsymbol{\alpha} &= \hat{P}^{sd-\iota k} \sum_{\substack{\langle g\rangle \le \hat{Q} \\ g \text{ monic}}} S(g)\mathfrak{J}(m_g, P) \\ &= \hat{P}^{sd-\iota k}\Big(\mathfrak{J}\mathfrak{S}(Q) + \sum_{\substack{\langle g\rangle \le \hat{Q} \\ g \text{ monic}}} S(g)\big(-\mathfrak{J} + \mathfrak{J}(m_g, P)\big) \Big) \\ &= \hat{P}^{sd-\iota k}\Big(\mathfrak{J}\mathfrak{S} + \mathfrak{J}\big(\mathfrak{S}(Q) - \mathfrak{S}\big) + \sum_{\substack{\langle g\rangle \le \hat{Q} \\ g \text{ monic}}} S(g)\big(-\mathfrak{J} + \mathfrak{J}(m_g, P)\big) \Big). \end{aligned}$$

By Lemma 54, for $s \geq 2\iota k+1$ and $g \in \mathbb{A}$ with $\langle g\rangle \leq \hat{P}^{\frac{1}{3}}$, we see that

$$-\mathfrak{J}+\mathfrak{J}(m_g,P) \ll q^{-(m_g+kP+1)/(3k\iota)} \leq q^{-(\frac{1}{2}P-\operatorname{ord} g)/(3k\iota)} \leq \hat{P}^{-\frac{1}{18k\iota}}.$$

Hence by Lemma 27 for $s \geq 2k(\iota+1)+1$, we find that

$$\sum_{\substack{\langle g\rangle \leq \hat{P}^{\frac{1}{3}} \\ g \text{ monic}}} S(g)\big(-\mathfrak{J}+\mathfrak{J}(m_g,P) = O(\hat{P}^{-\frac{1}{18k\iota}}).$$

By combining Lemma 54 with Lemma 27, for $s \geq 2k(\iota+1)+1$, there exist $\delta_1 = \frac{1}{6k}-\epsilon > 0$ and $\delta_2 = \frac{1}{4k}-\epsilon > 0$ such that

$$\sum_{\substack{\hat{P}^{\frac{1}{3}} < \langle g\rangle \leq \langle c\rangle \hat{P}^{\frac{1}{2}} \\ g \text{ monic}}} S(g)\big(-\mathfrak{J}+\mathfrak{J}(m_g,P)\big) = O(\hat{P}^{-\delta_1}),$$

and

$$\mathfrak{J}\big(\mathfrak{S}(Q)-\mathfrak{S}\big) = O(\hat{P}^{-\delta_2}).$$

On letting $\delta = \frac{1}{18k\iota}$, we obtain

$$\int_{\mathfrak{M}} \prod_{j=1}^{s} f_j(\boldsymbol{\alpha};P)d\boldsymbol{\alpha} = \mathfrak{J}\mathfrak{S}\hat{P}^{sd-\iota k} + O\big(\hat{P}^{sd-\iota k-\delta}\big).$$

By Theorems 32 and 58, $0 < \mathfrak{J}\mathfrak{S} \ll 1$. This completes the proof of the theorem. □

Chapter 3

The minor arc contribution

In this chapter, we will focus on the contribution of the minor arcs. More precisely, we want to find a condition on s such that

$$\int_{\mathfrak{m}} \prod_{j=1}^{s} f_j(\boldsymbol{\alpha}; P) d\boldsymbol{\alpha} \ll \hat{P}^{sd-\iota k-\delta}$$

for some $\delta > 0$. To this end, we need to establish a generalization of Vinogradov's mean value theorem in $\mathbb{F}_q[t]$ and Weyl-type estimates for $f_j(\boldsymbol{\alpha}; P)$ over the minor arcs.

3.1 Preliminaries

We first introduce some new notations. Fix $k, d \in \mathbb{N}$ and $\theta \in \mathbb{R}$ with $0 < \theta \leq 1/k$. For every $i \in \mathbb{N}$, it can be represented uniquely as

$$i = \sum_{h=0}^{\infty} a_h(i) p^h$$

where $a_h(i) \in [0, p-1] \cap \mathbb{Z}$ $(h \in \mathbb{N})$. Throughout, write $D = D(k) = \max\{h \in \mathbb{N} \,|\, a_h(k) > 0\}$. It is useful to define the function $\gamma_q : \mathbb{N} \to \mathbb{N}$ by

$$\gamma_q(i) = \sum_{h=0}^{\infty} a_h(i).$$

Also, for each $\mathbf{i} = (i_1, \ldots, i_d) \in \mathbb{N}^d$, write

$$a_h(\mathbf{i}) = \big(a_h(i_1), \ldots, a_h(i_d)\big) \quad \text{and} \quad \gamma_q(\mathbf{i}) = \big(\gamma_q(i_1), \ldots, \gamma_q(i_d)\big).$$

Recall that for $\mathbf{j} = (j_1, \ldots, j_d) \in \mathbb{N}^d$, $|\mathbf{j}| = j_1 + \cdots + j_d$. For $0 \le j < \gamma_q(k)$, we define

$$\begin{aligned}\mathcal{R}_j = &\big\{\mathbf{i} \in \mathbb{N}^d \,\big|\, |\gamma_q(\mathbf{i})| \le \gamma_q(k) - j\big\} \cap \\ &\big\{\mathbf{i} \in \mathbb{N}^d \,\big|\, \exists l \in \mathbb{N} \text{ s.t. } a_l(k) \ge 1 \text{ and } |a_h(\mathbf{i})| \le a_{h+l}(k)\ (h \in \mathbb{N})\big\},\end{aligned}$$

and define

$$\mathcal{R}'_j = \{\mathbf{n} \in \mathcal{R}_j |\ p \nmid \mathbf{n}\} \quad \text{and} \quad \mathcal{R}''_j = \{\mathbf{m} \in \mathcal{R}_j |\ p \mid \mathbf{m}\}.$$

For convenience, let $r_0 = \operatorname{card} \mathcal{R}_0$ and $r = \operatorname{card} \mathcal{R}'_0$. Moreover, recall that for each $\mathbf{i} \in \mathbb{N}^d$,

$$\mathcal{R}_{\mathbf{i}} = \left\{ \mathbf{j} \in \mathbb{N}^d \,\middle|\, 0 \le j_l \le i_l\,(1 \le l \le d),\ p \nmid \binom{i_1}{j_1} \cdots \binom{i_d}{j_d} \right\}.$$

Lemma 60. *For $\mathbf{i} \in \mathbb{N}^d$ with $|\mathbf{i}| \le k$, the following are equivalent.*
(1) $p \nmid \frac{k!}{i_1! \cdots i_d! (k - |\mathbf{i}|)!}$.
(2) For every $h \in \mathbb{N}$, $a_h(k) = a_h(i_1) + \cdots + a_h(i_d) + a_h(k - |\mathbf{i}|)$.
(3) For every $h \in \mathbb{N}$, $a_h(k) \ge a_h(i_1) + \cdots + a_h(i_d)$.

Proof. We first show that *(1)* $\Leftrightarrow$ *(2)*. Let $\sigma : \mathbb{N} \to \mathbb{N}$ be the function defined by

$$\sigma(z) = \sum_{h=0}^{\infty} \left[\frac{z}{p^h} \right].$$

Thus, we have $p^{\sigma(z)} \parallel z!$. Therefore $p \nmid \frac{k!}{i_1! \cdots i_d! (k - |\mathbf{i}|)!}$ if and only if

$$\sigma(k) = \sigma(i_1) + \cdots + \sigma(i_d) + \sigma(k - |\mathbf{i}|),$$

i.e.,

$$\sum_{h=0}^{\infty} \left[\frac{k}{p^h} \right] = \sum_{h=0}^{\infty} \left(\left[\frac{i_1}{p^h} \right] + \cdots + \left[\frac{i_d}{p^h} \right] + \left[\frac{k - |\mathbf{i}|}{p^h} \right] \right).$$

Since $i_1 + \cdots + i_d + (k - |\mathbf{i}|) = k$, the above identity is also equivalent to

$$\sum_{h=0}^{\infty} \left\{ \frac{k}{p^h} \right\} = \sum_{h=0}^{\infty} \left(\left\{ \frac{i_1}{p^h} \right\} + \cdots + \left\{ \frac{i_d}{p^h} \right\} + \left\{ \frac{k - |\mathbf{i}|}{p^h} \right\} \right). \tag{3.1}$$

Furthermore, from the equation $i_1 + \cdots + i_d + (k - |\mathbf{i}|) = k$ we deduce that for every $h \in \mathbb{N}$,

$$\left\{ \frac{k}{p^h} \right\} \le \left\{ \frac{i_1}{p^h} \right\} + \cdots + \left\{ \frac{i_d}{p^h} \right\} + \left\{ \frac{k - |\mathbf{i}|}{p^h} \right\}.$$

Thus (3.1) is equivalent to

$$\left\{\frac{k}{p^h}\right\} = \left\{\frac{i_1}{p^h}\right\} + \cdots + \left\{\frac{i_d}{p^h}\right\} + \left\{\frac{k-|\mathbf{i}|}{p^h}\right\} \quad (h \in \mathbb{N}). \tag{3.2}$$

For any $z \in \mathbb{N} \setminus \{0\}$, since $z = \sum_{h=0}^{\infty} a_h(z)p^h$, it follows that

$$\left\{\frac{z}{p^n}\right\} = \frac{1}{p^n}\sum_{l=0}^{n-1} a_l(z)p^l \quad (n \in \mathbb{N} \setminus \{0\}).$$

Thus (3.2) is equivalent to

$$a_h(k) = a_h(i_1) + \cdots + a_h(i_d) + a_h(k-|\mathbf{i}|) \quad (h \in \mathbb{N}). \tag{3.3}$$

Hence we have *(1)* $\Leftrightarrow$ *(2)*. To show *(2)* $\Leftrightarrow$ *(3)*, we observe that *(2)* implies

$$a_h(k) \geq a_h(i_1) + \cdots + a_h(i_d) \quad (h \in \mathbb{N}). \tag{3.4}$$

It remains to show that (3.4) implies (3.3). Since $|\mathbf{i}| = \sum_{h=0}^{\infty} |a_h(\mathbf{i})|p^h$, we have

$$k - |\mathbf{i}| = \sum_{h=0}^{\infty} \big(a_h(k) - |a_h(\mathbf{i})|\big)p^h.$$

It follows from (3.4) that $a_h(k-|\mathbf{i}|) = a_h(k) - |a_h(\mathbf{i})|$ $(h \in \mathbb{N})$. Therefore, *(3)* $\Rightarrow$ *(2)*. This completes the proof of the lemma. □

Recall that

$$\mathcal{L} = \left\{ \mathbf{i} \in \mathbb{N}^d \,\middle|\, |\mathbf{i}| = k, p \nmid \frac{k!}{i_1! \cdots i_d!(k-|\mathbf{i}|)!} \right\}.$$

As an application of the above lemma, we may represent $\iota = \operatorname{card} \mathcal{L}$ in terms of k, d.

Lemma 61. *Let*

$$\mathcal{L}_1 = \big\{ \mathbf{i} \in \mathbb{N}^d \,\big|\, |a_h(\mathbf{i})| = a_h(k) \ (h \in \mathbb{N}) \big\},$$

and

$$\mathcal{L}_2 = \big\{ \mathbf{i} \in \mathcal{R}_0' \,\big|\, |\gamma_q(\mathbf{i})| = \gamma_q(k) \big\}.$$

Then we have $\mathcal{L} = \mathcal{L}_1 = \mathcal{L}_2$. *Furthermore,*

$$\iota = \operatorname{card} \mathcal{L} = \prod_{h=0}^{D} \begin{pmatrix} a_h(k) + d - 1 \\ a_h(k) \end{pmatrix}.$$

Proof. Since $p \nmid k$, we have $a_0(k) > 0$. Thus $p \nmid \mathbf{i}$ for every $\mathbf{i} \in \mathcal{L}_1$ and hence $\mathcal{L}_1 \subseteq \mathcal{R}_0'$. Since $|\gamma_q(\mathbf{i})| = \sum_{h=0}^{\infty} |a_h(\mathbf{i})|$, we have $\mathcal{L}_1 \subseteq \mathcal{L}_2$. From Lemma 60(2), we have

$$\mathcal{L} = \left\{ \mathbf{i} \in \mathbb{N}^d \middle| \, |\mathbf{i}| = k,\, a_h(k) = |a_h(\mathbf{i})| + a_h(k - |\mathbf{i}|) \ (h \in \mathbb{N}) \right\} \subseteq \mathcal{L}_1. \tag{3.5}$$

We therefore have $\mathcal{L} \subseteq \mathcal{L}_1 \subseteq \mathcal{L}_2$. It remains to show that $\mathcal{L}_2 \subseteq \mathcal{L}$. Let $\mathbf{i} \in \mathcal{L}_2$. Then $|\gamma_q(\mathbf{i})| = \gamma_q(k)$ and $\mathbf{i} \in \mathcal{R}_0'$. In view of the definition of $\mathcal{R}_0'$, there exists some $l \in \mathbb{N}$ such that

$$|a_h(\mathbf{i})| \le a_{h+l}(k) \ (h \in \mathbb{N}). \tag{3.6}$$

Thus

$$\gamma_q(k) = |\gamma_q(\mathbf{i})| = \sum_{h=0}^{\infty} |a_h(\mathbf{i})| \le \sum_{h=0}^{\infty} a_{h+l}(k) \le \gamma_q(k).$$

It follows that

$$\sum_{h=0}^{\infty} |a_h(\mathbf{i})| = \sum_{h=0}^{\infty} a_{h+l}(k) = \gamma_q(k) = \sum_{h=0}^{\infty} a_h(k). \tag{3.7}$$

Since $a_0(k) > 0$, by (3.7), $l = 0$. Then by (3.6), $|a_h(\mathbf{i})| \le a_h(k)$ $(h \in \mathbb{N})$. From the first equality in (3.7) we see that

$$|a_h(\mathbf{i})| = a_h(k) \ (h \in \mathbb{N}), \tag{3.8}$$

and hence

$$|\mathbf{i}| = \sum_{h=0}^{\infty} |a_h(\mathbf{i})| p^h = \sum_{h=0}^{\infty} a_h(k) p^h = k.$$

On recalling (3.5), we have $\mathbf{i} \in \mathcal{L}$ and it follows that $\mathcal{L}_2 \subseteq \mathcal{L}$. Since

$$\mathcal{L} \subseteq \mathcal{L}_1 \subset \mathcal{L}_2 \subseteq \mathcal{L},$$

we have $\mathcal{L} = \mathcal{L}_1 = \mathcal{L}_2$. Since $|a_h(\mathbf{i})| = a_h(i_1) + \cdots + a_h(i_d)$ $(h \in \mathbb{N})$, it follows from (3.8) that

$$\iota = \operatorname{card} \mathcal{L} = \operatorname{card} \mathcal{L}_2 = \prod_{h=0}^{D} \begin{pmatrix} a_h(k) + d - 1 \\ a_h(k) \end{pmatrix}.$$

□

Lemma 62. *(1) For $\mathbf{i} \in \mathbb{N}^d$, if $\mathbf{j} \in \mathcal{R}_\mathbf{i}$, then $\mathcal{R}_\mathbf{j} \subseteq \mathcal{R}_\mathbf{i}$ and $|a_h(\mathbf{j})| \le |a_h(\mathbf{i})|$ $(h \in \mathbb{N})$.*
(2) For $j \in \mathbb{N}$ with $0 \le j \le \gamma_q(k)$, if $\mathbf{i} \in \mathcal{R}_j''$, then $\mathcal{R}_\mathbf{i} \subseteq \mathcal{R}_j''$.
(3) $\mathcal{R}_0 = \cup_{\mathbf{i} \in \mathcal{R}_0'} \mathcal{R}_\mathbf{i} = \cup_{\mathbf{i} \in \mathcal{R}_0} \mathcal{R}_\mathbf{i}$.

Proof. (1) From Lemma 60 we deduce that

$$p \nmid \begin{pmatrix} i_1 \\ j_1 \end{pmatrix} \cdots \begin{pmatrix} i_d \\ j_d \end{pmatrix}$$

if and only if for all $1 \leq l \leq d$ and $h \geq 0$,

$$a_h(j_l) \leq a_h(i_l).$$

Thus, in view of the definition of $\mathcal{R}_{\mathbf{i}}$, if $\mathbf{j} \in \mathcal{R}_{\mathbf{i}}$, then $|a_h(\mathbf{j})| \leq |a_h(\mathbf{i})|$ ($h \in \mathbb{N}$). Furthermore, for $\mathbf{n} \in \mathcal{R}_{\mathbf{j}}$ and $\mathbf{j} \in \mathcal{R}_{\mathbf{i}}$, we have

$$a_h(n_l) \leq a_h(j_l) \leq a_h(i_l),$$

and hence $\mathbf{n} \in \mathcal{R}_{\mathbf{i}}$. In particular, $\mathbf{i} = \mathbf{j}$ if and only if $|\gamma_q(\mathbf{i})| = |\gamma_q(\mathbf{j})|$.

(2) Note that $\mathbf{i} \in \mathcal{R}''_j$ implies that $p \mid \mathbf{i}$. Thus we have $|a_0(\mathbf{i})| = 0$. Take $\mathbf{j} \in \mathcal{R}_{\mathbf{i}}$. Using a similar argument as in the previous part, we have that for all $1 \leq l \leq d$ and $h \geq 0$,

$$a_h(j_l) \leq a_h(i_l).$$

Thus $|a_0(\mathbf{j})| = 0$ and $|\gamma_q(\mathbf{j})| = |\gamma_q(\mathbf{i})| \leq \gamma_q(k) - j$, which implies that $\mathbf{j} \in \mathcal{R}''_j$.

(3) Clearly, $\cup_{\mathbf{i} \in \mathcal{R}'_0} \mathcal{R}_{\mathbf{i}} \subseteq \cup_{\mathbf{i} \in \mathcal{R}_0} \mathcal{R}_{\mathbf{i}}$. Let $\mathbf{i} \in \mathcal{R}_0$. For each $\mathbf{l} \in \mathcal{R}_{\mathbf{i}}$ and $h \in \mathbb{N}$, we have

$$|a_h(\mathbf{l})| \leq |a_h(\mathbf{i})| \leq a_{h+l}(k). \tag{3.9}$$

Hence $\mathcal{R}_{\mathbf{i}} \subseteq \mathcal{R}_0$. Thus $\cup_{\mathbf{i} \in \mathcal{R}_0} \mathcal{R}_{\mathbf{i}} \subseteq \mathcal{R}_0$. It now suffices to show that $\mathcal{R}_0 \subseteq \cup_{\mathbf{i} \in \mathcal{R}'_0} \mathcal{R}_{\mathbf{i}}$. Suppose that $\mathbf{j} \in \mathcal{R}_0$. There are two cases: $p \nmid \mathbf{j}$ and $p \mid \mathbf{j}$. In the first case, $\mathbf{j} \in \mathcal{R}'_0 \subseteq \cup_{\mathbf{i} \in \mathcal{R}'_0} \mathcal{R}_{\mathbf{i}}$. In the second case, $|a_0(\mathbf{j})| = 0$. Let $\mathbf{i} = (j_1 + 1, j_2, \ldots, j_d)$. Since there exists $l \in \mathbb{N}$ such that $a_l(k) \geq 1$ and $|a_h(\mathbf{j})| \leq a_{h+l}(k)$ for all $h \in \mathbb{N} \setminus \{0\}$, we have

$$|a_0(\mathbf{i})| = 1 \leq a_l(k) \quad \text{and} \quad |a_h(\mathbf{i})| = |a_h(\mathbf{j})| \leq a_{h+l}(k).$$

It follows that $\mathbf{j} \in \mathcal{R}_{\mathbf{i}}$ and $\mathbf{i} \in \mathcal{R}'_0$. Hence $\mathbf{j} \in \cup_{\mathbf{i} \in \mathcal{R}'_0} \mathcal{R}_{\mathbf{i}}$. We therefore conclude that $\mathcal{R}_0 \subseteq \cup_{\mathbf{i} \in \mathcal{R}'_0} \mathcal{R}_{\mathbf{i}}$. □

Suppose that $(\mathbf{f})$ is a system of polynomials in $\mathbb{A}[x_1, .., x_v]$ and w is an irreducible element in $\mathbb{A}$. For every v-tuple $\mathbf{z} \in \mathbb{A}^v$, we write $\operatorname{rk} \operatorname{Jac}(\mathbf{f}; \mathbf{z}; w)$ for the rank of the Jacobian matrix $\operatorname{Jac}(\mathbf{f}; \mathbf{z})$ over $\mathbb{A}/(w)$.

Lemma 63. *For $v \in \mathbb{N} \setminus \{0\}$, let $\mathcal{R}$ be a subset of $\{\mathbf{i} \in \mathbb{N}^d | 1 \le |\mathbf{i}| \le k\}$ of cardinality less than v. For each $\mathbf{i} \in \mathcal{R}$, let $f_{\mathbf{i}}$ be a polynomial over $\mathbb{A}$ in v variables of total degree not exceeding k. For every irreducible $w \in \mathbb{A}$, let $\mathcal{C}_{w,\mathcal{R}}(\mathbf{f}; \mathbf{a})$ denote the set of solutions $\mathbf{x} \in \big(\mathbb{A}/(w)\big)^v$ of the system*

$$f_{\mathbf{i}}(\mathbf{x}) \equiv a_{\mathbf{i}} \pmod{w} \quad (\mathbf{i} \in \mathcal{R})$$

for which $\operatorname{rk} \operatorname{Jac}(\mathbf{f}; \mathbf{x}; w) = \operatorname{card} \mathcal{R}$. *Also, let $\mathcal{B}_{w,\mathcal{R}}(\mathbf{f}; \mathbf{u})$ denote the set of solutions $\mathbf{x} \in \big(\mathbb{A}/(w^k)\big)^v$ of the system*

$$f_{\mathbf{i}}(\mathbf{x}) \equiv u_{\mathbf{i}} \pmod{w^{|\mathbf{i}|}} \quad (\mathbf{i} \in \mathcal{R})$$

for which $\operatorname{rk} \operatorname{Jac}(\mathbf{f}; \mathbf{x}; w) = \operatorname{card} \mathcal{R}$. *Then we have*

$$\operatorname{card} \mathcal{C}_{w,\mathcal{R}}(\mathbf{f}; \mathbf{a}) \ll_{v,k,d} \langle w \rangle^{v - \operatorname{card} \mathcal{R}} \quad \text{and} \quad \operatorname{card} \mathcal{B}_{w,\mathcal{R}}(\mathbf{f}; \mathbf{u}) \ll_{v,k,d} \langle w \rangle^{kv - K_{\mathcal{R}}}, \tag{3.10}$$

where $K_{\mathcal{R}} = \sum_{\mathbf{i} \in \mathcal{R}} |\mathbf{i}|$.

Proof. (1) for each $L \subseteq \{1, 2, \dots, v\}$ with $\operatorname{card} L = \operatorname{card} \mathcal{R}$, write $\mathcal{C}_{w,\mathcal{R},L}(\mathbf{f}; \mathbf{a})$ for the set of solutions counted by $\mathcal{C}_{w,\mathcal{R}}(\mathbf{f}; \mathbf{a})$ and with $\det(\partial f_{\mathbf{i}} / \partial x_l)_{\mathbf{i} \in \mathcal{R}, l \in L} \neq 0$. From [12, Lemma 4], it follows that

$$\operatorname{card} \mathcal{C}_{w,\mathcal{R},L}(\mathbf{f}; \mathbf{a}) \ll_{k,d} \langle w \rangle^{v - \operatorname{card} \mathcal{R}}.$$

Thus,

$$\operatorname{card} \mathcal{C}_{w,\mathcal{R}}(\mathbf{f}; \mathbf{a}) \le \sum_{\substack{L \subseteq \{1,2,\dots,v\} \\ \operatorname{card} L = \operatorname{card} \mathcal{R}}} \operatorname{card} \mathcal{C}_{w,\mathcal{R},L} \ll_{v,k,d} \langle w \rangle^{v - \operatorname{card} \mathcal{R}}.$$

(2) To show the second inequality in (3.10), we note that the number of choices for $\mathbf{a} \in (\mathbb{A}/(w^k))^{\operatorname{card} \mathcal{R}}$ which satisfy

$$a_{\mathbf{i}} \equiv u_{\mathbf{i}} \pmod{w^{|\mathbf{i}|}} \quad (\mathbf{i} \in \mathcal{R})$$

is $\langle w \rangle^{\sum_{\mathbf{i} \in \mathcal{R}} (k - |\mathbf{i}|)}$. Fix any choice for $\mathbf{a}$. By [12, Lemma 4], the number of solutions $\mathbf{x}$ modulo w^k of the system

$$f_{\mathbf{i}}(\mathbf{x}) \equiv a_{\mathbf{i}} \pmod{w^k} \quad (\mathbf{i} \in \mathcal{R})$$

is bounded by $O_{v,k,d}(\langle w^k \rangle^{v - \operatorname{card} \mathcal{R}})$. Thus,

$$\operatorname{card} \mathcal{B}_{w,\mathcal{R}}(\mathbf{f}; \mathbf{u}) \ll_{v,k,d} \langle w \rangle^{\sum_{\mathbf{i} \in \mathcal{R}} (k - |\mathbf{i}|)} \langle w^k \rangle^{v - \operatorname{card} \mathcal{R}} \ll_{v,k,d} \langle w \rangle^{kv - K_{\mathcal{R}}},$$

where $K_{\mathcal{R}} = \sum_{\mathbf{i} \in \mathcal{R}} |\mathbf{i}|$. This completes the proof of this lemma. □

Lemma 64. *Let $w \in \mathbb{A}$ be irreducible and $v \in \mathbb{N}$ with $v \geq r$. We denote by S_w the set of $\mathbf{z} = (\mathbf{z}_1, \dots, \mathbf{z}_v)$, for which $\mathbf{z}_n \in (\mathbb{A}/(w))^d \, (1 \leq n \leq v)$ and $\operatorname{rk} \operatorname{Jac}((\mathbf{x}^{\mathbf{n}})_{\mathbf{n} \in \mathcal{R}_0'}; \mathbf{z}; w) < r$. Then we have*

$$\operatorname{card} S_w \ll_{v,k,d} \langle w \rangle^{v(d-1)+r-1}.$$

Proof. For each $\mathbf{z} = (\mathbf{z}_1, \dots, \mathbf{z}_v)$ with each $\mathbf{z}_n \in (\mathbb{A}/(w))^d$, if

$$\operatorname{rk} \operatorname{Jac}((\mathbf{x}^{\mathbf{n}})_{\mathbf{n} \in \mathcal{R}_0'}; \mathbf{z}; w) < r,$$

then there exist $c_{\mathbf{i}} \in \mathbb{A}/(w) \, (\mathbf{i} \in \mathcal{R}_0')$, not all zero, such that for all $1 \leq l \leq d$ and $1 \leq n \leq v$,

$$\sum_{\mathbf{i} \in \mathcal{R}_0'} c_{\mathbf{i}} \partial \mathbf{x}^{\mathbf{i}} / \partial x_l(\mathbf{z}_n) \equiv 0 \pmod{w}.$$

Define

$$R_1 = \left\{ \mathbf{i} \in \mathcal{R}_0' \,\middle|\, p \nmid i_1 \right\} \quad \text{and} \quad R_l = \left\{ \mathbf{i} \in \mathcal{R}_0' \,\middle|\, p | i_1, \dots, p | i_{l-1}, p \nmid i_l \right\} (2 \leq l \leq d).$$

Then $\mathcal{R}_0'$ is a disjoint union of $R_1, \dots, R_d$. Also, define $R_l' = \{\mathbf{i} \in R_l \mid c_{\mathbf{i}} \neq 0\} \, (1 \leq l \leq d)$. Since the $c_{\mathbf{i}}$ are not all zero, there must exist some l such that R_l' is nonempty. Let $m = \min\{l \mid R_l' \neq \emptyset\}$. For each $\mathbf{i} \in R_m$, since $p \nmid i_m$ and $\partial \mathbf{x}^{\mathbf{i}} / \partial x_m = i_m \mathbf{x}^{\mathbf{i}} x_m^{-1}$, we have

$$\sum_{\mathbf{i} \in R_m} c_{\mathbf{i}} \partial \mathbf{x}^{\mathbf{i}} / \partial x_m = \sum_{\mathbf{i} \in R_m} c_{\mathbf{i}} i_m \mathbf{x}^{\mathbf{i}} x_m^{-1} \neq 0$$

in $\mathbb{A}/(w)[\mathbf{x}]$. By the minimality of m, for any $\mathbf{i} \in R_l$ with $l < m$, $c_{\mathbf{i}} = 0$ and so

$$\sum_{\substack{\mathbf{i} \in R_l \\ l < m}} c_{\mathbf{i}} \partial \mathbf{x}^{\mathbf{i}} / \partial x_m = 0$$

in $\mathbb{A}/(w)[\mathbf{x}]$. For $l > m$, $\mathbf{i} \in R_l$ implies that $p | i_m$ and hence $\partial \mathbf{x}^{\mathbf{i}} / \partial x_m = 0$. Thus

$$\sum_{\mathbf{i} \in \mathcal{R}_0'} c_{\mathbf{i}} \partial \mathbf{x}^{\mathbf{i}} / \partial x_m = \sum_{\mathbf{i} \in R_m} c_{\mathbf{i}} \partial \mathbf{x}^{\mathbf{i}} / \partial x_m \neq 0,$$

which yields that the $\mathbf{z}_n$ are the roots of a nontrivial polynomial in $\mathbb{A}/(w)[\mathbf{x}]$. Thus, for a fixed choice of the $c_{\mathbf{i}}$, the number of choices for $(\mathbf{z}_1, \dots, \mathbf{z}_v)$ modulo w is $O_{v,k,d}\big(\langle w \rangle^{v(d-1)}\big)$. Also, the number of the choices for the $c_{\mathbf{i}}$ is $O_{k,d}\big(\langle w \rangle^{r-1}\big)$ because one of them can be normalized to 1. Hence the total number of possibilities for the $\mathbf{z}_n$ is $O_{v,k,d}\big(\langle w \rangle^{v(d-1)+r-1}\big)$. □

Definition 65. *We say that the system of polynomials* $(\mathbf{\Psi})$ *is of* type (j, P) *if it satisfies the following three conditions.*
(1) $(\mathbf{\Psi})$ *consists of polynomials* $\Psi_{\mathbf{i}} \in \mathbb{A}[x_1, \ldots, x_d]$ $(\mathbf{i} \in \mathcal{R}_0)$.
(2) For all $\mathbf{i} \in \mathcal{R}_0$, $\mathbf{n} \in \mathcal{R}'_j$ *and* $\mathbf{m} \in \mathcal{R}''_j$, *there exist* $T_{\mathbf{i},\mathbf{n}}$ *and* $T_{\mathbf{i},\mathbf{m}} \in \mathbb{A}$ *such that*

$$\Psi_{\mathbf{i}}(\mathbf{x}) = \sum_{\mathbf{n}\in\mathcal{R}'_j} T_{\mathbf{i},\mathbf{n}}\mathbf{x}^{\mathbf{n}} + \sum_{\mathbf{m}\in\mathcal{R}''_j} T_{\mathbf{i},\mathbf{m}}\mathbf{x}^{\mathbf{m}}.$$

Furthermore, for each $\mathbf{n} \in \mathcal{R}'_j$, $T_{\mathbf{i},\mathbf{n}} = 0$ *either if* $\mathbf{i} \in \mathcal{R}'_0$ *with* $|\gamma_q(\mathbf{i})| - |\gamma_q(\mathbf{n})| < j$ *or if* $\mathbf{i} \in \mathcal{R}''_0$. *In addition, there exist* $\mathbf{i} \in \mathcal{R}'_0$ *and* $\mathbf{n} \in \mathcal{R}'_j$ *with* $|\gamma_q(\mathbf{i})| - |\gamma_q(\mathbf{n})| = j$ *such that* $T_{\mathbf{i},\mathbf{n}}$ *is nonzero.*
(3) For every $\mathbf{i} \in \mathcal{R}_0$ *and* $\mathbf{l} \in \mathcal{R}_j = \mathcal{R}'_j \cup \mathcal{R}''_j$, $\langle T_{\mathbf{i},\mathbf{l}} \rangle \leq \hat{P}^{kj}$.

For simplicity, throughout this chapter, we write k' for $\gamma_q(k)$.

Remark 2 (1) Let $(\mathbf{\Psi})$ be of type (j, P). Then we have the coefficient matrix $T = \begin{pmatrix} T_1 & T_2 \\ 0 & T_3 \end{pmatrix}$ such that

$$\begin{pmatrix} (\Psi_{\mathbf{i}})_{\mathbf{i}\in\mathcal{R}'_0} \\ (\Psi_{\mathbf{j}})_{\mathbf{j}\in\mathcal{R}''_0} \end{pmatrix} = \begin{pmatrix} T_1 & T_2 \\ 0 & T_3 \end{pmatrix} \begin{pmatrix} (\mathbf{x}^{\mathbf{n}})_{\mathbf{n}\in\mathcal{R}'_j} \\ (\mathbf{x}^{\mathbf{m}})_{\mathbf{m}\in\mathcal{R}''_j} \end{pmatrix}.$$

Furthermore, by setting $\mathcal{R}'_{j,u} = \left\{\mathbf{i} \in \mathcal{R}'_j \,\middle|\, |\gamma_q(\mathbf{i})| = u\right\}$ and $T_{u,v} = (T_{\mathbf{i},\mathbf{n}})_{\mathbf{i}\in\mathcal{R}'_{0,u},\mathbf{n}\in\mathcal{R}'_{j,v}}$, we have

$$T_1 = \begin{pmatrix} (T_{u,v})_{u\geq j+1,\, v\in\{k'-j,\ldots,1\}} \\ (T_{u,v})_{u\leq j,\, v\in\{k'-j,\ldots,1\}} \end{pmatrix}.$$

From Condition (2) in Definition 65, we deduce that $T_{u,v} = 0$ whenever $u - v < j$. Note that in T_1 we have $v \geq 1$ and so $(T_{u,v})_{u\leq j} = 0$. Therefore, T_1 is in the following row-echelon form

$$T_1 = \begin{pmatrix} T_{k',k'-j} & * & \cdots & * \\ 0 & T_{k'-1,k'-1-j} & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & T_{j+1,1} \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Again, by Condition (2) in Definition 65, we find that the $T_{u,u-j}$ are not all zero.

(2) Clearly $T_1 \neq 0$. Let $r' = \operatorname{rk} T_1$. Then $0 < r' \leq r$. In view of Condition (3) in Definition 65, the determinant of every $r' \times r'$ sub-matrix of T_1 can be bounded by $\hat{P}^{rk^2}$. Furthermore, for each of these nonzero determinants, the number of its irreducible divisors w of degree $[\theta P]+1$ is bounded in terms of k,d and θ. Furthermore, the total number of irreducible divisors of all the nonzero determinants under consideration is bounded by a constant $c = c(k, d, \theta)$.

(3) Whenever P is sufficiently large and ϵ is small enough, there exists a set consisting of $[1/\theta - \epsilon]$ irreducible polynomials of degree $[\theta P]+1$, none of which divides any nonzero determinant as in the above remark. Throughout, let $\mathcal{P}(\theta, \epsilon)$ denote this set.

(4) For $\mathcal{R} \subseteq \mathcal{R}'_0$, define

$$T_{u,v,\mathcal{R}} = (T_{\mathbf{i},\mathbf{n}})_{\mathbf{i}\in\mathcal{R}\cap\mathcal{R}'_{0,u},\mathbf{n}\in\mathcal{R}'_{j,v}} \tag{3.11}$$

and

$$T_{\mathcal{R}} = \begin{pmatrix} T_{k',k'-j,\mathcal{R}} & 0 & \cdots & 0 \\ 0 & T_{k'-1,k'-1-j,\mathcal{R}} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & T_{j+1,1,\mathcal{R}} \end{pmatrix}. \tag{3.12}$$

Since the $T_{u,u-j}$ are not all zero, there exists a subset $\mathcal{R}$ of $\left\{\mathbf{i} \in \mathcal{R}'_0 \,\middle|\, |\gamma_q(\mathbf{i})| \geq j+1\right\}$ such that the matrix $T_{\mathcal{R}}$ has rank $\operatorname{card}\mathcal{R}$. The construction of $\mathcal{P}(\theta, \epsilon)$ yields that $T_{\mathcal{R}} (\operatorname{mod} w)$ has rank $\operatorname{card}\mathcal{R}$ whenever $w \in \mathcal{P}(\theta, \epsilon)$. In what follows, it is convenient to write $K(\mathbf{\Psi})$ for $\max\limits_{\mathcal{R}} \sum\limits_{\mathbf{i}\in\mathcal{R}} |\mathbf{i}|$ where $\mathcal{R}$ runs over all the subsets as above.

Lemma 66. *Let $\mathbf{a} \in \mathbb{A}^d$. Define $A = (a_{\mathbf{i},\mathbf{j}})_{\mathbf{i},\mathbf{j}\in\mathcal{R}_0}$ with*

$$a_{\mathbf{i},\mathbf{j}} = \begin{cases} \begin{pmatrix} i_1 \\ j_1 \end{pmatrix} \cdots \begin{pmatrix} i_d \\ j_d \end{pmatrix} (-\mathbf{a})^{\mathbf{i}-\mathbf{j}}, & \text{if} \quad \mathbf{j} \in \mathcal{R}_{\mathbf{i}}, \\ 0, & \text{otherwise.} \end{cases}$$

Let $A_{u,v} = (a_{\mathbf{i},\mathbf{j}})_{\mathbf{i}\in\mathcal{R}'_{0,u},\mathbf{j}\in\mathcal{R}'_{0,v}}$. Then for every $u \in \{k', \ldots, 1\}$, $A_{u,u}$ is the identity matrix, denoted by I_u, and $A_{u,v} = 0$ whenever $u < v$. That is, the sub-matrix $A_1 = \left(A_{u,v}\right)_{u,v\in\{k',\ldots,1\}}$

is of the following form

$$\begin{pmatrix} I_{k'} & * & \cdots & * \\ 0 & I_{k'-1} & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & I_1 \end{pmatrix}.$$

Proof. Suppose that $\mathbf{i} \in \mathcal{R}'_0$ and $\mathbf{j} \in \mathcal{R}_{\mathbf{i}}$. By the proof of Lemma 62(1), we deduce that $|\gamma_q(\mathbf{i})| \geq |\gamma_q(\mathbf{j})|$ as well as $|\gamma_q(\mathbf{i})| = |\gamma_q(\mathbf{j})|$ if and only if $\mathbf{i} = \mathbf{j}$. Moreover, since $a_{\mathbf{i},\mathbf{i}} = 1$, we have $A_{u,u} = I_u$ and $A_{u,v} = 0$ when $u < v$. □

Remark 3 Let A be defined as in Lemma 66. For $\mathbf{j} \in \mathcal{R}''_0$ and $\mathbf{l} \in \mathcal{R}_{\mathbf{j}}$, it follows from Lemma 62(2) that $\mathbf{l} \in \mathcal{R}''_0$. Thus, $a_{\mathbf{j},\mathbf{i}} = 0$ whenever $\mathbf{j} \in \mathcal{R}''_0$ and $\mathbf{i} \in \mathcal{R}'_0$. Suppose that $(\mathbf{\Psi})$ is of type (j, P) and $(\mathbf{\Phi}) = A(\mathbf{\Psi})$. More precisely, we have

$$\begin{pmatrix} (\Phi_{\mathbf{i}})_{\mathbf{i}\in\mathcal{R}'_0} \\ (\Phi_{\mathbf{j}})_{\mathbf{j}\in\mathcal{R}''_0} \end{pmatrix} = \begin{pmatrix} A_1 & A_2 \\ 0 & A_3 \end{pmatrix} \begin{pmatrix} (\Psi_{\mathbf{i}})_{\mathbf{i}\in\mathcal{R}'_0} \\ (\Psi_{\mathbf{j}})_{\mathbf{j}\in\mathcal{R}''_0} \end{pmatrix}.$$

As in Remark 2, we have

$$\begin{pmatrix} (\Psi_{\mathbf{i}})_{\mathbf{i}\in\mathcal{R}'_0} \\ (\Psi_{\mathbf{j}})_{\mathbf{j}\in\mathcal{R}''_0} \end{pmatrix} = \begin{pmatrix} T_1 & T_2 \\ 0 & T_3 \end{pmatrix} \begin{pmatrix} (\mathbf{x}^{\mathbf{n}})_{\mathbf{n}\in\mathcal{R}'_j} \\ (\mathbf{x}^{\mathbf{m}})_{\mathbf{m}\in\mathcal{R}''_j} \end{pmatrix},$$

and hence,

$$\begin{pmatrix} (\Phi_{\mathbf{i}})_{\mathbf{i}\in\mathcal{R}'_0} \\ (\Phi_{\mathbf{j}})_{\mathbf{j}\in\mathcal{R}''_0} \end{pmatrix} = \begin{pmatrix} A_1T_1 & * \\ 0 & A_3T_3 \end{pmatrix} \begin{pmatrix} (\mathbf{x}^{\mathbf{n}})_{\mathbf{n}\in\mathcal{R}'_j} \\ (\mathbf{x}^{\mathbf{m}})_{\mathbf{m}\in\mathcal{R}''_j} \end{pmatrix}.$$

Thus,

$$\mathrm{Jac}\begin{pmatrix} (\Phi_{\mathbf{i}})_{\mathbf{i}\in\mathcal{R}'_0} \\ (\Phi_{\mathbf{j}})_{\mathbf{j}\in\mathcal{R}''_0} \end{pmatrix} = \begin{pmatrix} A_1T_1 & * \\ 0 & A_3T_3 \end{pmatrix} \begin{pmatrix} \mathrm{Jac}(\mathbf{x}^{\mathbf{n}})_{\mathbf{n}\in\mathcal{R}'_j} \\ \mathrm{Jac}(\mathbf{x}^{\mathbf{m}})_{\mathbf{m}\in\mathcal{R}''_j} \end{pmatrix}.$$

Since $p|\mathbf{m}$ whenever $\mathbf{m} \in \mathcal{R}''_j$, we see that

$$\mathrm{Jac}\begin{pmatrix} (\Phi_{\mathbf{i}})_{\mathbf{i}\in\mathcal{R}'_0} \\ (\Phi_{\mathbf{j}})_{\mathbf{j}\in\mathcal{R}''_0} \end{pmatrix} = \begin{pmatrix} A_1T_1\mathrm{Jac}(\mathbf{x}^{\mathbf{n}})_{\mathbf{n}\in\mathcal{R}'_j} \\ 0 \end{pmatrix}.$$

From Remark 2(1) and Lemma 66, it follows that

$$A_1T_1 = \begin{pmatrix} I_{k'} & * & \cdots & * & * & \cdots & * \\ 0 & I_{k'-1} & \cdots & * & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & I_{j+1} & * & & * \\ 0 & 0 & \cdots & 0 & I_j & \cdots & * \\ \vdots & \vdots & & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & I_1 \end{pmatrix} \begin{pmatrix} T_{k',k'-j} & * & \cdots & * \\ 0 & T_{k'-1,k'-1-j} & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & T_{j+1,1} \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Thus A_1T_1 is of the form

$$\begin{pmatrix} T_{k',k'-j} & * & \cdots & * \\ 0 & T_{k'-1,k'-1-j} & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & T_{j+1,1} \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}.$$

For every $w \in \mathcal{P}(\theta, \epsilon)$, whenever $\mathbf{z}$ satisfies that $\operatorname{rk} \operatorname{Jac}((\mathbf{x}^{\mathbf{n}})_{\mathbf{n}\in\mathcal{R}'_j}; \mathbf{z}; w) = \operatorname{card} \mathcal{R}'_j$, on taking $\mathcal{R}$ as in Remark 2(4), we may observe that the rows of A_1T_1 indexed by $\mathbf{i} \in \mathcal{R}$ form a sub-matrix $M_{\mathcal{R}}(\operatorname{mod} w)$ of rank $\operatorname{card} \mathcal{R}$ and hence

$$\operatorname{Jac}((\Phi_{\mathbf{i}})_{\mathbf{i}\in\mathcal{R}}; \mathbf{z}; w) = M_{\mathcal{R}} \operatorname{Jac}((\mathbf{x}^{\mathbf{n}})_{\mathbf{n}\in\mathcal{R}'_j}; \mathbf{z}; w) = \operatorname{card} \mathcal{R}.$$

3.2 The fundamental lemma

Let $J_{s,k,d}(P)$ denote the number of solutions of the system

$$\mathbf{x}_1^{\mathbf{i}} + \cdots + \mathbf{x}_s^{\mathbf{i}} = \mathbf{y}_1^{\mathbf{i}} + \cdots + \mathbf{y}_s^{\mathbf{i}} \quad (\mathbf{i} \in \mathcal{R}'_0), \tag{3.13}$$

with $\mathbf{x}_n, \mathbf{y}_n \in I_P^d$. In this section, we aim to establish a fundamental lemma for building up Vinogradov-type estimates for $J_{s,k,d}(P)$. It is convenient to have available a lemma that provides the basis of our strategy in our subsequent deliberations.

Lemma 67. *For every nonzero* $\mathbf{j} \in \mathcal{R}_0$*, there exist* $\mathbf{n} \in \mathcal{R}_0'$ *and* $v \in \mathbb{N}$ *such that* $\mathbf{j} = p^v\mathbf{n}$.

Proof. Suppose that $\mathbf{j} \in \mathcal{R}_0 \setminus \{\mathbf{0}\}$. Then there exists $(\mathbf{n}, v) \in \mathbb{N}^d \times \mathbb{N}$ such that

$$\mathbf{j} = p^v\mathbf{n} = p^v \sum_{h\geq 0} a_h(\mathbf{n})p^h = \sum_{h\geq 0} a_h(\mathbf{n})p^{h+v}.$$

Hence there exists $l \in \mathbb{N}$ such that $a_l(k) > 0$ and

$$|a_h(\mathbf{n})| = |a_{h+v}(\mathbf{j})| \leq a_{h+v+l}(k) \ (h \in \mathbb{N}).$$

Thus $\mathbf{n} \in \mathcal{R}_0'$. This completes the proof of the lemma. □

In order to estimate $J_{s,k,d}(P)$ via the Linnik-Karatsuba method, we shall analyze an alternative system of equations. For any nonzero $\mathbf{j} \in \mathcal{R}_0$, Lemma 67 implies that $\mathbf{j} = p^v\mathbf{n}$ for some $\mathbf{n} \in \mathcal{R}_0'$ and $v \in \mathbb{N}$, and so

$$\sum_{m=1}^{s}(\mathbf{x}_m^{\mathbf{j}} - \mathbf{y}_m^{\mathbf{j}}) = \bigg(\sum_{m=1}^{s}(\mathbf{x}_m^{\mathbf{n}} - \mathbf{y}_m^{\mathbf{n}})\bigg)^{p^v} = 0,$$

whenever $(\mathbf{x}, \mathbf{y})$ is a solution of the system (3.13). Moreover, since $\mathcal{R}_0' \subseteq \mathcal{R}_0$, the system (3.13) is equivalent to the following system

$$\mathbf{x}_1^{\mathbf{i}} + \cdots + \mathbf{x}_s^{\mathbf{i}} = \mathbf{y}_1^{\mathbf{i}} + \cdots + \mathbf{y}_s^{\mathbf{i}} \ \ (\mathbf{i} \in \mathcal{R}_0). \tag{3.14}$$

Therefore, $J_{s,k,d}(P)$ is also the number of solutions of (3.14) with $\mathbf{x}_n, \mathbf{y}_n \in I_P^d$.

We are in a position to establish the fundamental lemma by analyzing the system (3.14). For $\boldsymbol{\alpha} \in \mathbb{T}^{r_0}$ and $P \in \mathbb{R}$ with $P > 0$, define

$$f(\boldsymbol{\alpha}; P) = \sum_{\mathbf{i}\in I_P^d} e\bigg(\sum_{\mathbf{i}\in\mathcal{R}_0} \alpha_{\mathbf{i}}\mathbf{x}^{\mathbf{i}}\bigg).$$

Let $K_s(P, Q; \boldsymbol{\Psi})$ denote the number of solutions of the system

$$\sum_{n=1}^{r}\Big(\Psi_{\mathbf{i}}(\mathbf{z}_n) - \Psi_{\mathbf{i}}(\mathbf{z}_n')\Big) = \sum_{m=1}^{s}(\mathbf{x}_m^{\mathbf{i}} - \mathbf{y}_m^{\mathbf{i}}) \ \ (\mathbf{i} \in \mathcal{R}_0)$$

with $\mathbf{z}_n, \mathbf{z}_n' \in I_P^d$ and $\mathbf{x}_m, \mathbf{y}_m \in I_Q^d$. Furthermore, let $L_s(P, Q, \theta, w; \boldsymbol{\Psi})$ denote the number of solutions of the system

$$\sum_{n=1}^{r}\Big(\Psi_{\mathbf{i}}(\mathbf{z}_n) - \Psi_{\mathbf{i}}(\mathbf{z}_n')\Big) = w^{|\mathbf{i}|}\sum_{m=1}^{s}(\mathbf{u}_m^{\mathbf{i}} - \mathbf{v}_m^{\mathbf{i}}) \ \ (\mathbf{i} \in \mathcal{R}_0)$$

with $\mathbf{z}$ and $\mathbf{z}'$ as above, $\mathbf{u}_m, \mathbf{v}_m \in I^d_{Q-\theta P}$, and $z_{nl} \equiv z'_{nl} \pmod{w^k}\,(1 \le l \le d)$. Finally, we write

$$L_s(P, Q, \theta; \mathbf{\Psi}) = \max_{w \in \mathcal{P}(\theta,\epsilon)} L_s(P, Q, \theta, w; \mathbf{\Psi}).$$

Lemma 68. *Suppose that $\theta P \le Q \le P$ and that $(\mathbf{\Psi})$ is a system of type (j, P). Then for $s \ge 2\mu - 1$, there is a system $(\mathbf{\Phi})$ as in Remark 3, such that*

$$K_s(P, Q; \mathbf{\Psi}) \ll \hat{P}^{2rd-(r+1)(1-\theta)+\epsilon} J_s(Q) + \hat{P}^{\theta(2sd+krd-\mu-K)} L_s(P, Q, \theta; \mathbf{\Phi}),$$

where $\mu = \operatorname{card}\{\mathbf{i} \in \mathcal{R}'_0 | \Psi_{\mathbf{i}} \text{ is a constant in } \mathbb{A}\}$ and $K = K(\mathbf{\Psi})$ defined as in Remark 2(4).

Proof. Let S_1 denote the number of solutions counted by $K_s(P, Q; \mathbf{\Psi})$ such that for all $w \in \mathcal{P}(\theta, \epsilon)$,

$$\operatorname{rk} \operatorname{Jac}\big((\mathbf{x}^{\mathbf{n}})_{\mathbf{n} \in \mathcal{R}'_0}; \mathbf{z}, \mathbf{z}'; w\big) < r.$$

Let S_2 denote the number of remaining solutions, i.e., the solutions for which

$$\operatorname{rk} \operatorname{Jac}\big((\mathbf{x}^{\mathbf{n}})_{\mathbf{n} \in \mathcal{R}'_0}; \mathbf{z}, \mathbf{z}'; w\big) = r$$

for some $w \in \mathcal{P}(\theta, \epsilon)$. Hence, $K_s(P, Q; \mathbf{\Psi}) = S_1 + S_2$. There are two cases.

Case 1: Suppose that $S_2 \le S_1$. For every $w \in \mathcal{P}(\theta, \epsilon)$, on taking $v = 2r$, it follows from Lemma 64 that the number of possibilities for $(\mathbf{z}, \mathbf{z}') \in \big(\mathbb{A}/(w)\big)^{2rd}$ with

$$\operatorname{rk} \operatorname{Jac}\big((\mathbf{x}^{\mathbf{n}})_{\mathbf{n} \in \mathcal{R}'_0}; \mathbf{z}, \mathbf{z}'; w\big) < r$$

is $O\big(\langle w \rangle^{2rd-r-1}\big)$. Let $u = \prod_{w \in \mathcal{P}(\theta,\epsilon)} w$. By the Chinese Remainder Theorem, the total number of choices for $(\mathbf{z}, \mathbf{z}') \in \big(\mathbb{A}/(u)\big)^{2rd}$ is $O\big(\langle u \rangle^{2rd-r-1)}\big)$. For each fixed choice $(\mathbf{z}_0, \mathbf{z}'_0) (\operatorname{mod} u)$, there are at most $(\hat{P}/\langle u \rangle)^{2rd}$ choices for the $(\mathbf{z}, \mathbf{z}') \in I_P^{2rd}$ with $(\mathbf{z}, \mathbf{z}') \equiv (\mathbf{z}_0, \mathbf{z}'_0) (\operatorname{mod} u)$, and hence the number of $(\mathbf{z}, \mathbf{z}') \in I_P^{2rd}$ under consideration can be estimated by $O\big(\hat{P}^{2rd} \langle u \rangle^{-r-1}\big)$. Since $\langle u \rangle > \big(\hat{P}^{\theta}\big)^{[1/\theta-\epsilon]} > \hat{P}^{1-\theta-\epsilon}$, we have

$$\hat{P}^{2rd} \langle u \rangle^{-r-1} < \hat{P}^{2rd-(r+1)(1-\theta-\epsilon)}.$$

Thus,

$$K_s(P, Q; \mathbf{\Psi}) \le 2S_1 \ll \hat{P}^{2rd-(r+1)(1-\theta)+\epsilon} J_s(Q).$$

Case 2: Suppose that $S_1 \le S_2$. It follows that

$$S_2 \le \sum_{w \in \mathcal{P}(\theta,\epsilon)} S_3(w)$$

where $S_3(w)$ denote the number of solutions with

$$\operatorname{rk}\operatorname{Jac}\big((\mathbf{x}^{\mathbf{n}})_{\mathbf{n}\in\mathcal{R}_0'};\mathbf{z},\mathbf{z}';w\big)=r.$$

For each $\boldsymbol{\eta}\in\{\pm1\}^r$, write

$$\mathcal{G}(\boldsymbol{\alpha};\boldsymbol{\eta})=\sum_{\substack{\mathbf{z}=(\mathbf{z}_1,\dots,\mathbf{z}_r)\\ \mathbf{z}_m\in I_P^d}} e\Big(\sum_{\mathbf{i}\in\mathcal{R}_0}\alpha_{\mathbf{i}}s_{\mathbf{i}}(\mathbf{z},\boldsymbol{\eta})\Big), \tag{3.15}$$

where

$$s_{\mathbf{i}}(\mathbf{z},\boldsymbol{\eta})=\eta_1\Psi_{\mathbf{i}}(\mathbf{z}_1)+\cdots+\eta_r\Psi_{\mathbf{i}}(\mathbf{z}_r).$$

Let $\mathcal{G}_w(\boldsymbol{\alpha};\boldsymbol{\eta})$ denote the same sum in (3.15), but restricted to those $\mathbf{z}$ for which $\operatorname{rk}\operatorname{Jac}\big((\mathbf{x}^{\mathbf{n}})_{\mathbf{n}\in\mathcal{R}_0'};\mathbf{z};w\big)=r$. After rearranging variables, we deduce that

$$S_3(w)\le\sum_{\boldsymbol{\eta}\in\{\pm1\}^r}\int_{\mathbb{T}^{r_0}}\mathcal{G}(\boldsymbol{\alpha};\boldsymbol{\eta})\mathcal{G}_w(-\boldsymbol{\alpha};\boldsymbol{\eta})\big|f(\boldsymbol{\alpha};Q)\big|^{2s}d\boldsymbol{\alpha}.$$

Thus by the Cauchy-Schwarz inequality, we have

$$S_3(w)\ll\bigg(\int_{\mathbb{T}^{r_0}}\big|\mathcal{G}(\boldsymbol{\alpha};\boldsymbol{\eta})\big|^2\big|f(\boldsymbol{\alpha};Q)\big|^{2s}d\boldsymbol{\alpha}\bigg)^{\frac12}\bigg(\int_{\mathbb{T}^{r_0}}\big|\mathcal{G}_w(\boldsymbol{\alpha};\boldsymbol{\eta})\big|^2\big|f(\boldsymbol{\alpha};Q)\big|^{2s}d\boldsymbol{\alpha}\bigg)^{\frac12},$$

for some $\boldsymbol{\eta}\in\{\pm1\}^r$. It follows by taking complex conjugates that $\big|\mathcal{G}(\boldsymbol{\alpha};\boldsymbol{\eta})\big|=\big|\mathcal{G}(\boldsymbol{\alpha};\mathbf{1})\big|$ and hence that the integral in the first factor above is equal to $K_s(P,Q;\boldsymbol{\Psi})$. Let $S_4(w;\boldsymbol{\eta})$ denote the number of solutions of the system

$$\sum_{n=1}^{r}\eta_n\Big(\Psi_{\mathbf{i}}(\mathbf{z}_n)-\Psi_{\mathbf{i}}(\mathbf{z}_n')\Big)=\sum_{m=1}^{s}(\mathbf{x}_m^{\mathbf{i}}-\mathbf{y}_m^{\mathbf{i}})\quad(\mathbf{i}\in\mathcal{R}_0)$$

with $\operatorname{rk}\operatorname{Jac}\big((\mathbf{x}^{\mathbf{n}})_{\mathbf{n}\in\mathcal{R}_0'};\mathbf{z};w\big)=r=\operatorname{rk}\operatorname{Jac}\big((\mathbf{x}^{\mathbf{n}})_{\mathbf{n}\in\mathcal{R}_0'};\mathbf{z}';w\big)$. On noting that $\mathcal{P}(\theta,\epsilon)\ll1$, we find that

$$K_s(P,Q;\boldsymbol{\Psi})\le2S_2\ll\max_{\substack{w\in\mathcal{P}(\theta,\epsilon)\\ \boldsymbol{\eta}\in\{\pm1\}^r}}S_4(w;\boldsymbol{\eta}). \tag{3.16}$$

For convenience, we write $S_4(w)$ for the maximum in (3.16). Now consider the system

$$\sum_{m=1}^{s}(\mathbf{x}_m^{\mathbf{i}}-\mathbf{y}_m^{\mathbf{i}})=0$$

for all $\mathbf{i} \in \mathcal{R}_0'$ with with $\Psi_{\mathbf{i}}$ a constant in $\mathbb{A}$. So we can classify the solutions counted by $S_4(w)$ according to the common residue classes of $\mathbf{x}_1^{\mathbf{i}} + \cdots + \mathbf{x}_s^{\mathbf{i}}$ and $\mathbf{y}_1^{\mathbf{i}} + \cdots + \mathbf{y}_s^{\mathbf{i}}$ modulo w. Then, we write $\mathcal{C}_w(\mathbf{a})$ for the set of solutions modulo w of the system of congruences

$$\sum_{m=1}^{s} \mathbf{x}_m^{\mathbf{i}} \equiv a_{\mathbf{i}} \pmod{w}$$

for all $\mathbf{i} \in \mathcal{R}_0'$ with $\Psi_{\mathbf{i}}$ a constant in $\mathbb{A}$. From Lemma 63 , it follows that the number of non-singular solutions counted by $\mathcal{C}_w(\mathbf{a})$ is $O(\langle w \rangle^{sd-\mu})$. Moreover, since $w \in \mathcal{P}(\theta, \epsilon)$, Lemma 64 yields that the number of singular solutions is $O\big(\langle w \rangle^{s(d-1)+\mu-1}\big)$. Therefore, we deduce that

$$\operatorname{card} \mathcal{C}_w(\mathbf{a}) \ll \langle w \rangle^{sd-\mu},$$

provided that $s \geq 2\mu - 1$.

Next, we introduce the exponential sum

$$f_w(\boldsymbol{\alpha}; \mathbf{y}) = \sum_{\substack{\mathbf{x} \in I_Q^d \\ \mathbf{x} \equiv \mathbf{y} (\operatorname{mod} w)}} e\Big(\sum_{\mathbf{i} \in \mathcal{R}_0} \alpha_{\mathbf{i}} \mathbf{x}^{\mathbf{i}} \Big).$$

Note that

$$S_4(w; \boldsymbol{\eta}) = \int_{\mathbb{T}^{r_0}} \big| \mathcal{G}_w(\boldsymbol{\alpha}; \boldsymbol{\eta}) \big|^2 \sum_{\mathbf{a} \in (\mathbb{A}/(w))^{\mu}} \big| U_w(\boldsymbol{\alpha}; \mathbf{a}) \big|^2 d\boldsymbol{\alpha},$$

where

$$U_w(\boldsymbol{\alpha}; \mathbf{a}) = \sum_{(\mathbf{u}_1, \ldots, \mathbf{u}_s) \in \mathcal{C}_w(\mathbf{a})} f_w(\boldsymbol{\alpha}; \mathbf{u}_1) \cdots f_w(\boldsymbol{\alpha}; \mathbf{u}_s).$$

Then it follows from Cauchy's inequality that

$$\begin{aligned} \big| U_w(\boldsymbol{\alpha}; \mathbf{a}) \big|^2 &\ll \operatorname{card} \mathcal{C}_w(\mathbf{a}) \sum_{\mathbf{u} \in \mathcal{C}_w(\mathbf{a})} \big| f_w(\boldsymbol{\alpha}; \mathbf{u}_1) \cdots f_w(\boldsymbol{\alpha}; \mathbf{u}_s) \big|^2 \\ &\ll \langle w \rangle^{sd-\mu} \sum_{\mathbf{u} \in \mathcal{C}_w(\mathbf{a})} \sum_{i=1}^{s} \big| f_w(\boldsymbol{\alpha}; \mathbf{u}_i) \big|^{2s}, \end{aligned}$$

which yields that

$$S_4(w; \boldsymbol{\eta}) \ll \langle w \rangle^{2sd-\mu} \max_{\mathbf{a} \in (\mathbb{A}/(w))^d} S_5(\mathbf{a}, w; \boldsymbol{\eta}),$$

where

$$S_5(\mathbf{a}, w; \boldsymbol{\eta}) = \int_{\mathbb{T}^{r_0}} \big| \mathcal{G}_w(\boldsymbol{\alpha}; \boldsymbol{\eta}) \big|^2 \big| f_w(\boldsymbol{\alpha}; \mathbf{a}) \big|^{2s} d\boldsymbol{\alpha}.$$

We may observe that $S_5(\mathbf{a}, w; \boldsymbol{\eta})$ is the number of solutions of the system

$$\sum_{n=1}^{r} \eta_n \Big(\Psi_{\mathbf{i}}(\mathbf{z}_n) - \Psi_{\mathbf{i}}(\mathbf{z}'_n) \Big) = \sum_{m=1}^{s} \Big((w\mathbf{x}_m + \mathbf{a})^{\mathbf{i}} - (w\mathbf{y}_m + \mathbf{a})^{\mathbf{i}} \Big) \ (\mathbf{i} \in \mathcal{R}_0)$$

with $\mathbf{z}_n, \mathbf{z}'_n \in I_P^d$, $\mathbf{x}_m, \mathbf{y}_m \in \mathbb{A}^d$, $\langle x_{ml} \rangle, \langle y_{ml} \rangle \le \hat{Q}/\langle w \rangle$, and

$$\operatorname{rk} \operatorname{Jac}((\mathbf{x}^{\mathbf{n}})_{\mathbf{n} \in \mathcal{R}'_0}; \mathbf{z}; w) = r = \operatorname{rk} \operatorname{Jac}((\mathbf{x}^{\mathbf{n}})_{\mathbf{n} \in \mathcal{R}'_0}; \mathbf{z}'; w).$$

By [15, Lemma 2.3], we see that $S_5(\mathbf{a}, w; \boldsymbol{\eta})$ is also equal to the number of solutions of the system

$$\sum_{n=1}^{r} \eta_n \Big(\Phi_{\mathbf{i}}(\mathbf{z}_n) - \Phi_{\mathbf{i}}(\mathbf{z}'_n) \Big) = w^{|\mathbf{i}|} \sum_{m=1}^{s} (\mathbf{x}_m^{\mathbf{i}} - \mathbf{y}_m^{\mathbf{i}}) \ \ (\mathbf{i} \in \mathcal{R}_0)$$

with $\mathbf{z}, \mathbf{z}', \mathbf{x}, \mathbf{y}$ as above and $(\boldsymbol{\Phi})$ as in Lemma 64. Now let $\mathcal{R}$ be chosen as in Remark 2(4) such that $\sum_{\mathbf{i} \in \mathcal{R}} |\mathbf{i}| = K(\boldsymbol{\Psi})$. Since

$$\operatorname{rk} \operatorname{Jac}\big((\mathbf{x}^{\mathbf{n}})_{\mathbf{n} \in \mathcal{R}'_0}; \mathbf{z}; w\big) = \operatorname{card} \mathcal{R}'_0 = r,$$

we have $\operatorname{rk} \operatorname{Jac}\big((\mathbf{x}^{\mathbf{n}})_{\mathbf{n} \in \mathcal{R}'_j}; \mathbf{z}; w\big) = \operatorname{card} \mathcal{R}'_j$. Hence by Remark 3, we have $\operatorname{rk} \operatorname{Jac}\big((\boldsymbol{\Phi}_{\mathbf{i}})_{\mathbf{i} \in \mathcal{R}}; \mathbf{z}; w\big) = \operatorname{card} \mathcal{R}$. Thus $S_5(\mathbf{a}, w; \boldsymbol{\eta}) \ll S_6(\mathbf{a}, w; \boldsymbol{\eta}; \mathcal{R})$, where $S_6(\mathbf{a}, w; \boldsymbol{\eta}; \mathcal{R})$ counts the number of solutions of the system

$$\sum_{n=1}^{r} \eta_n \Big(\Phi_{\mathbf{i}}(\mathbf{z}_n) - \Phi_{\mathbf{i}}(\mathbf{z}'_n) \Big) = w^{|\mathbf{i}|} \sum_{m=1}^{s} (\mathbf{x}_m^{\mathbf{i}} - \mathbf{y}_m^{\mathbf{i}}) \ \ (\mathbf{i} \in \mathcal{R}_0),$$

with $\mathbf{x}_m, \mathbf{y}_m \in I_{Q-\theta P}^d$, $\mathbf{z}_n, \mathbf{z}'_n \in I_P^d$, and

$$\operatorname{rk} \operatorname{Jac}\big((\boldsymbol{\Phi}_{\mathbf{i}})_{\mathbf{i} \in \mathcal{R}}; \mathbf{z}; w\big) = \operatorname{rk} \operatorname{Jac}\big((\boldsymbol{\Phi}_{\mathbf{i}})_{\mathbf{i} \in \mathcal{R}}; \mathbf{z}'; w\big) = \operatorname{card} \mathcal{R}.$$

Write $\boldsymbol{\alpha}\boldsymbol{w}$ for the r_0-dimensional vector whose component indexed by $\mathbf{i}$ is $\alpha_{\mathbf{i}} w^{|\mathbf{i}|}$ and put

$$t_{\mathbf{i}}(\mathbf{z}, \boldsymbol{\eta}) = \eta_1 \Phi_{\mathbf{i}}(\mathbf{z}_1) + \cdots + \eta_r \Phi_{\mathbf{i}}(\mathbf{z}_r).$$

Now let $\mathcal{B}_w(\mathbf{u}; \boldsymbol{\Phi}, \mathcal{R}; \boldsymbol{\eta})$ denote the set of solutions $\mathbf{z}$ modulo w^k to the system of congruences

$$t_{\mathbf{i}}(\mathbf{z}, \boldsymbol{\eta}) \equiv u_{\mathbf{i}} \pmod{w^{|\mathbf{i}|}} \ \ (\mathbf{i} \in \mathcal{R})$$

with $\operatorname{rk} \operatorname{Jac}((\boldsymbol{\Phi}_{\mathbf{i}})_{\mathbf{i} \in \mathcal{R}}; \mathbf{z}; w) = \operatorname{card} \mathcal{R}$. For simplicity, in the following, we write $\mathcal{B}$ for $\mathcal{B}_w(\mathbf{u}; \boldsymbol{\Phi}, \mathcal{R}; \boldsymbol{\eta})$. Let

$$\widetilde{\mathcal{G}}_w(\boldsymbol{\alpha}; \mathbf{z}; \boldsymbol{\eta}) = \sum_{\substack{\mathbf{x} \in I_P^{dr} \\ \mathbf{x} \equiv \mathbf{z} \, (\mathrm{mod}\ w^k)}} e\Big(\sum_{\mathbf{i} \in \mathcal{R}_0} \alpha_{\mathbf{i}} t_{\mathbf{i}}(\mathbf{x}, \boldsymbol{\eta}) \Big).$$

Let

$$I_w(\boldsymbol{\alpha};\boldsymbol{\eta};\mathcal{R}) = \sum_{\mathbf{u}} \Big| \sum_{\mathbf{z}\in\mathcal{B}} \widetilde{\mathcal{G}}_w(\boldsymbol{\alpha};\mathbf{z};\boldsymbol{\eta})\Big|^2,$$

where the first summation is over $\mathbf{u}$ with $u_{\mathbf{i}} \in \mathbb{A}/(w^{|\mathbf{i}|})$ ($\mathbf{i} \in \mathcal{R}$). Thus

$$S_6(\mathbf{a}, w;\boldsymbol{\eta};\mathcal{R}) \le \int_{\mathbb{T}^{r_0}} I_w(\boldsymbol{\alpha};\boldsymbol{\eta};\mathcal{R})\big|f(\boldsymbol{\alpha}\boldsymbol{w}; Q-\theta P)^{2s}\big|d\boldsymbol{\alpha}.$$

By Cauchy's inequality and Lemma 63, we deduce that

$$I_w(\boldsymbol{\alpha};\boldsymbol{\eta};\mathcal{R}) \le \sum_{\mathbf{u}} \operatorname{card}\mathcal{B} \sum_{\mathbf{z}\in\mathcal{B}} \big|\widetilde{\mathcal{G}}_w(\boldsymbol{\alpha};\mathbf{z};\boldsymbol{\eta})\big|^2 \ll \langle w\rangle^{krd-K} \sum_{\mathbf{u}} \sum_{\mathbf{z}\in\mathcal{B}} \big|\widetilde{\mathcal{G}}_w(\boldsymbol{\alpha};\mathbf{z};\boldsymbol{\eta})\big|^2.$$

Thus,

$$\begin{aligned} S_4(w;\boldsymbol{\eta}) &\ll \langle w\rangle^{2sd-\mu} \max_{\mathbf{a}\in(\mathbb{A}/(w))^{dr}} S_6(\mathbf{a}, w;\boldsymbol{\eta};\mathcal{R}) \\ &\ll \langle w\rangle^{2sd+krd-\mu-K} \sum_{\mathbf{z}\in(\mathbb{A}/(w^k))^d} \int_{\mathbb{T}^{r_0}} \big|\widetilde{\mathcal{G}}_w(\boldsymbol{\alpha};\mathbf{z};\boldsymbol{\eta})^2 f(\boldsymbol{\alpha}\boldsymbol{w}; Q-\theta P)^{2s}\big|d\boldsymbol{\alpha}. \end{aligned}$$

On noting that $\big|\widetilde{\mathcal{G}}_w(\boldsymbol{\alpha};\mathbf{z};\boldsymbol{\eta})\big| = \big|\widetilde{\mathcal{G}}_w(\boldsymbol{\alpha};\mathbf{z};\mathbf{1})\big|$ and considering the underlying equations, the lemma now follows. □

3.3 Vinogradov-type mean value estimates

In this section, the purpose is to establish an estimate of the shape

$$J_{s,k,d}(P) \ll \hat{P}^{2sd-K_0+\Delta_s},$$

where

$$K_0 = \sum_{\mathbf{i}\in\mathcal{R}_0'} |\mathbf{i}|.$$

Lemma 69. *Define*

$$\mathcal{V} = \big\{\mathbf{i}\in\mathbb{N}^d \,\big|\, |a_0(\mathbf{i})| \ge 1 \text{ and } |a_h(\mathbf{i})| \le a_h(k)\ (h\in\mathbb{N})\big\}$$

and $\nu = \operatorname{card}\mathcal{V}$. *The following hold.*

(1) $\nu = \left(\begin{pmatrix} a_0(k)+d \\ d \end{pmatrix} - 1 \right) \prod_{h=1}^{D} \begin{pmatrix} a_h(k)+d \\ d \end{pmatrix}$.

(2) If $D = 0$, *then* $r = \nu$. *If* $D > 0$, *then*

$$\nu \le r < \nu(1 + \frac{1+d}{d^2}).$$

(3) Let $K_{\mathcal{V}} = \sum_{\mathbf{i} \in \mathcal{V}} |\mathbf{i}|$. *Then*

$$K_{\mathcal{V}} \le \frac{\nu(dk+1)}{d+1}.$$

(4) If $k \ge d+2$, *then*

$$K_0 < (k-1)(r+1).$$

Proof. (1) The result follows from the fact that $\mathbf{i} \in \mathcal{V}$ if and only if

$$1 \le |a_0(\mathbf{i})| \le a_0(k) \quad \text{and} \quad 0 \le |a_h(\mathbf{i})| \le a_h(k) \quad \big(h \in \mathbb{N} \setminus \{0\}\big).$$

(2) If $D = 0$, in view of the definition of $\mathcal{R}_0'$, we have

$$\mathcal{R}_0' = \big\{ \mathbf{i} \in \mathbb{N}^d \;\big|\; |a_0(\mathbf{i})| \ge 1 \text{ and } |a_h(\mathbf{i})| \le a_h(k) \ (h \in \mathbb{N}) \big\} = \mathcal{V}.$$

Thus $r = \nu$. We now consider the case when $D > 0$. Since $\mathcal{V} \subseteq \mathcal{R}_0'$, we have $\nu \le r$. Suppose that $\{l \in \mathbb{N} \mid a_l(k) \ge 1\} = \{l_0, \dots, l_m\}$ where $0 = l_0 < l_1 < \cdots < l_m = D$. For every i with $1 \le i \le m$, define

$$\begin{cases} \mathcal{V}_i = \big\{ \mathbf{i} \in \mathbb{N}^d \;\big|\; |a_0(\mathbf{i})| \ge 1 \text{ and } |a_h(\mathbf{i})| \le a_{h+l_i}(k) \ (h \in \mathbb{N}) \big\}, \\ \nu_i = \operatorname{card} \mathcal{V}_i, \\ k_i = p^{-l_i}\big(a_{l_i}(k)p^{l_i} + \cdots + a_D(k)p^D\big). \end{cases}$$

Then $\mathcal{R}_0' = \mathcal{V} \cup \big(\cup_{i=1}^m \mathcal{V}_i \big)$. Fix i with $1 \le i \le m$. Since $a_h(k_i) = a_{h+l_i}(k)$ $(h \in \mathbb{N})$, we have

$$\mathcal{V}_i = \big\{ \mathbf{i} \in \mathbb{N}^d \;\big|\; |a_0(\mathbf{i})| \ge 1 \text{ and } |a_h(\mathbf{i})| \le a_h(k_i) \ (h \in \mathbb{N}) \big\}.$$

By Lemma 69(1), we see that

$$\begin{aligned} \nu_i &= \left(\begin{pmatrix} a_0(k_i)+d \\ d \end{pmatrix} - 1 \right) \prod_{h=1}^{D-l_i} \begin{pmatrix} a_h(k_i)+d \\ d \end{pmatrix} \\ &= \left(\begin{pmatrix} a_{l_i}(k)+d \\ d \end{pmatrix} - 1 \right) \prod_{h=1+l_i}^{D} \begin{pmatrix} a_h(k)+d \\ d \end{pmatrix}. \end{aligned}$$

Note that

$$\begin{pmatrix} n+d \\ d \end{pmatrix} \geq nd+1 \quad (n \in \mathbb{N}).$$

Thus

$$\begin{aligned}
\frac{\nu_i}{\nu} &= \left(\begin{pmatrix} a_{l_i}(k)+d \\ d \end{pmatrix} - 1 \right) \left(\begin{pmatrix} a_0(k)+d \\ d \end{pmatrix} - 1 \right)^{-1} \prod_{h=1}^{l_i} \begin{pmatrix} a_h(k)+d \\ d \end{pmatrix}^{-1} \\
&< \left(\begin{pmatrix} a_0(k)+d \\ d \end{pmatrix} - 1 \right)^{-1} \prod_{h=1}^{l_{i-1}} \begin{pmatrix} a_{h+l_i}(k)+d \\ d \end{pmatrix}^{-1} \\
&\leq \big(a_0(k)d\big)^{-1} \prod_{h=1}^{l_{i-1}} \big(1+a_h(k)d\big)^{-1} \\
&\leq d^{-1}(1+d)^{-i+1}.
\end{aligned}$$

Therefore,

$$\begin{aligned}
r &\leq \nu + \nu_1 + \cdots + \nu_m < \nu + \nu d^{-1} \sum_{i=1}^{m} (1+d)^{-i+1} \\
&< \nu + \nu \cdot \frac{1+d}{d^2} = \nu\Big(1 + \frac{1+d}{d^2}\Big).
\end{aligned}$$

(3) We consider two cases.

Case 1: Let $h \in \mathbb{N} \setminus \{0\}$. Since for $u \in \mathbb{N}$ with $1 \leq u \leq a_h(k)$,

$$\operatorname{card}\big\{\mathbf{i} \in \mathcal{V} \,\big|\, |a_h(\mathbf{i})| = u\big\} = \nu \cdot \begin{pmatrix} a_h(k)+d \\ d \end{pmatrix}^{-1} \cdot \begin{pmatrix} u+d-1 \\ d-1 \end{pmatrix}.$$

By [15, Lemma 2.1], we have

$$\begin{aligned}
\sum_{\mathbf{i} \in \mathcal{V}} |a_h(\mathbf{i})| &= \sum_{u=1}^{a_h(k)} u \cdot \operatorname{card}\big\{\mathbf{i} \in \mathcal{V} \,\big|\, |a_h(\mathbf{i})| = u\big\} \\
&= \nu \cdot \begin{pmatrix} a_h(k)+d \\ d \end{pmatrix}^{-1} \cdot \sum_{u=1}^{a_h(k)} u \begin{pmatrix} u+d-1 \\ d-1 \end{pmatrix} \\
&= \nu \cdot \begin{pmatrix} a_h(k)+d \\ d \end{pmatrix}^{-1} \cdot \frac{da_h(k)}{d+1} \begin{pmatrix} a_h(k)+d \\ d \end{pmatrix} \\
&= \frac{\nu d a_h(k)}{d+1}.
\end{aligned}$$

Case 2: Let $h = 0$. Since for $u \in \mathbb{N}$ with $1 \le u \le a_0(k)$,

$$\operatorname{card}\left\{\mathbf{i} \in \mathcal{V} \,\middle|\, |a_0(\mathbf{i})| = u\right\} = \nu \cdot \left(\begin{pmatrix} a_0(k)+d \\ d \end{pmatrix} - 1 \right)^{-1} \cdot \begin{pmatrix} u+d-1 \\ d-1 \end{pmatrix}.$$

We have

$$\begin{aligned}
\sum_{\mathbf{i}\in\mathcal{V}} |a_0(\mathbf{i})| &= \sum_{u=1}^{a_0(k)} u \cdot \operatorname{card}\left\{\mathbf{i} \in \mathcal{V} \,\middle|\, |a_0(\mathbf{i})| = u\right\} \\
&= \nu \cdot \left(\begin{pmatrix} a_0(k)+d \\ d \end{pmatrix} - 1 \right)^{-1} \cdot \sum_{u=1}^{a_0(k)} u \begin{pmatrix} u+d-1 \\ d-1 \end{pmatrix} \\
&= \nu \cdot \left(\begin{pmatrix} a_0(k)+d \\ d \end{pmatrix} - 1 \right)^{-1} \cdot \frac{da_0(k)}{d+1} \begin{pmatrix} a_h(k)+d \\ d \end{pmatrix} \\
&= \frac{\nu d a_0(k)}{d+1} \left(1 + \left(\begin{pmatrix} a_0(k)+d \\ d \end{pmatrix} - 1 \right)^{-1} \right).
\end{aligned}$$

Since $\begin{pmatrix} a_0(k)+d \\ d \end{pmatrix} - 1 \ge a_0(k)d$, it follows that

$$\begin{aligned}
K_{\mathcal{V}} = \sum_{\mathbf{i}\in\mathcal{V}} |\mathbf{i}| &= \sum_{\mathbf{i}\in\mathcal{V}} \sum_{h=0}^{D} |a_h(\mathbf{i})| p^h = \sum_{h=0}^{D} p^h \sum_{\mathbf{i}\in\mathcal{V}} |a_h(\mathbf{i})| \\
&= \frac{\nu d k}{d+1} + \frac{\nu d a_0(k)}{d+1} \left(\begin{pmatrix} a_0(k)+d \\ d \end{pmatrix} - 1 \right)^{-1} \\
&\le \frac{\nu(dk+1)}{d+1}.
\end{aligned}$$

(4) Suppose that $k \ge d+2$. Since

$$(\nu+1)(k-1) - \frac{\nu(dk+1)}{d+1} = k\big(\nu(d+1)^{-1}+1\big) - \nu(d+2)(d+1)^{-1} - 1 > 0,$$

we have

$$K_{\mathcal{V}} < (k-1)(\nu+1).$$

Take $\mathbf{i} \in \mathcal{R}_0' - \mathcal{V}$ arbitrarily. Then there exists some $l \in \mathbb{N} \setminus \{0\}$ such that

$$|a_h(\mathbf{i})| \le a_{h+l}(k) \quad (h \in \mathbb{N}).$$

Hence

$$p^l|\mathbf{i}| = \sum_{h\geq 0} |a_h(\mathbf{i})|p^{h+l} \leq \sum_{h\geq 0} a_{h+l}(k)p^{h+l} = \sum_{h\geq l} a_h(k)p^h \leq k-1,$$

where the last inequality holds because $l > 0$. Thus,

$$K_0 - K_{\mathcal{V}} \leq p^{-l}(r-\nu)(k-1) < (r-\nu)(k-1).$$

Therefore, whenever $k \geq d+2$,

$$K_0 = (K_0 - K_{\mathcal{V}}) + K_{\mathcal{V}} < (r-\nu)(k-1) + (k-1)(\nu+1) = (k-1)(r+1).$$

This completes the proof of the lemma. □

We now define

$$(\mathbf{\Psi}_0) = \big\{ \Psi_{\mathbf{i},0} \in \mathbb{A}[\mathbf{x}] \;\big|\; \Psi_{\mathbf{i},0} = \mathbf{x}^{\mathbf{i}} \ (\mathbf{i} \in \mathcal{R}_0) \big\}.$$

Also, we define

$$(\mathbf{\Phi}_0) = A(\mathbf{\Psi}_0),$$

where A is an $r_0 \times r_0$ invertible matrix over $\mathbb{A}$ defined as in Lemma 66. On recalling Remark 2(4), we see that

$$K(\mathbf{\Psi}_0) = \sum_{\mathbf{i}\in\mathcal{R}_0'} |\mathbf{i}| = K_0.$$

Write $\lambda_s = 2sd - K_0 + \Delta_s$. We say that λ_s and Δ_s are *admissible* if $J_{s,k,d}(P) \ll \hat{P}^{\lambda_s}$.

Lemma 70. *If Δ_s is an admissible exponent satisfying $\Delta_s < (k-1)(r+1)$, then the exponent $\Delta_{s+r} = \Delta_s(1-\frac{1}{k})$ is also admissible.*

Proof. Let $\theta = \frac{1}{k}$. Since

$$\mu = \operatorname{card}\{\mathbf{i} \in \mathcal{R}_0' | \Psi_{\mathbf{i},0} \in (\mathbf{\Psi}_0) \text{ and } \Psi_{\mathbf{i},0} = 0\} = 0,$$

it follows from Lemma 68 that

$$K_s(P,P;\mathbf{\Psi}_0) \ll \hat{P}^{2rd-(r+1)(1-\theta)+\epsilon} J_s(P) + \hat{P}^{\theta(2sd+krd-K_0)} L_s(P,P,\theta;\mathbf{\Phi}_0). \tag{3.17}$$

For every $w \in \mathcal{P}(\theta,\epsilon)$, we have $\langle w\rangle > q^{\theta P}$ and hence $\langle w^k\rangle > q^{k\theta P} = \hat{P}$. Since $\mathbf{z} \equiv \mathbf{z}' \pmod{w^k}$ and $\mathbf{z}, \mathbf{z}' \in I_P^{rd}$, we have $\mathbf{z} = \mathbf{z}'$. Then by the definitions of $L_s(P,Q,\theta,w;\mathbf{\Phi}_0)$ and $J_s(Q)$, we have

$$L_s(P,P,\theta,w;\mathbf{\Phi}_0) = \hat{P}^{rd} J_s((1-\theta)P).$$

Thus

$$L_s(P,P,\theta;\mathbf{\Phi}_0)=\max_{w\in\mathcal{P}(\theta,\epsilon)}L_s(P,P,\theta,w;\mathbf{\Phi}_0)=\hat{P}^{rd}J_s((1-\theta)P).$$

We deduce from (3.17) that

$$K_s(P,P;\mathbf{\Psi}_0)\ll\hat{P}^{2rd-(r+1)(1-\theta)+\epsilon}J_s(P)+\hat{P}^{\theta(2sd+krd-K_0)+rd}J_s((1-\theta)P). \tag{3.18}$$

Suppose that $\lambda_s=2sd-K_0+\Delta_s$ is admissible, where $\Delta_s<(k-1)(r+1)$. Then $J_s(P)\ll\hat{P}^{\lambda_s}$ and $J_s((1-\theta)P)\ll\hat{P}^{(1-\theta)\lambda_s}$. On recalling $\theta=\frac{1}{k}$, from (3.18) we have

$$J_{s+r}(P)=K_s(P,P;\mathbf{\Psi}_0)\ll\hat{P}^{\Lambda_1}+\hat{P}^{\Lambda_2},$$

where

$$\Lambda_1=2(s+r)d-K_0+\Delta_s-(r+1)(1-\theta)+\epsilon$$

and

$$\Lambda_2=2(s+r)d-K_0+\Delta_s(1-\theta).$$

Since $\Delta_s<(k-1)(r+1)$, it follows that $\Lambda_1\leq\Lambda_2$. Thus $J_{s+r}(P)\ll\hat{P}^{\Lambda_2}$, i.e., $\Delta_{s+r}=\Delta_s(1-\frac{1}{k})$ is admissible. □

Theorem 71. *For $k\geq d+2$ and $s\in\mathbb{N}$ with $s\geq r$, we have*

$$J_{s,k,d}(P)\ll\hat{P}^{2sd-K_0+\Delta_s},$$

where $\Delta_s=rke^{-\frac{s-r}{rk}}$.

Proof. By Lemmas 69 and 70 , $\Delta_s^*=K_0(1-\frac{1}{k})^{\frac{s-r}{r}}$ is admissible. Since $K_0<rk$, $\Delta_s=rke^{-\frac{s-r}{rk}}$ is also admissible . □

3.4 Weyl-type estimates

For $\boldsymbol{\alpha}\in\mathbb{T}^r$ and $P\in\mathbb{R}$ with $P>0$, define

$$\tilde{f}(\boldsymbol{\alpha})=\tilde{f}(\boldsymbol{\alpha};P)=\sum_{\mathbf{x}\in I_P^d}e\Big(\sum_{\mathbf{i}\in\mathcal{R}_0'}\alpha_{\mathbf{i}}\mathbf{x}^{\mathbf{i}}\Big).$$

Theorem 72. *Fix $\mathbf{j} \in \mathcal{L}$. Let $M, P \in \mathbb{R}$ with $1 \le M \le P$. Let a and $g \in \mathbb{A}$ with $\gcd(a,g) = 1$ and $\operatorname{ord} g \ll_k M$. For $\boldsymbol{\alpha} \in \mathbb{T}^r$, suppose that $\langle g\alpha_{\mathbf{j}} - a\rangle < \hat{M}^{-k}$ and that either $\langle g\alpha_{\mathbf{j}} - a\rangle \ge \hat{M}\hat{P}^{-k}$ or $\langle g\rangle > \hat{M}$. Then there exists a constant $C(q,k,\epsilon) > 0$ such that for every $s \in \mathbb{N}$ with $s \ge r$, we have*

$$\big|\tilde{f}(\boldsymbol{\alpha})\big| \le C(q,k,\epsilon)\langle g\rangle^{\epsilon}\hat{P}^{d+\epsilon}\Big(\hat{M}^{-1}(\hat{P}/\hat{M})^{\Delta_s}\big(1 + \langle g\rangle(\hat{P}/\hat{M})^{-k}\big)\Big)^{1/2s}.$$

Proof. Let

$$\mathcal{U} = \big\{u \in \mathbb{A} \;\big|\; \gcd(u,g) = 1,\ u \text{ is monic and irreducible with } \operatorname{ord} u = [M]\big\}.$$

Since $\operatorname{ord} g \ll_k M$, there exists $C_1(k,\epsilon) > 0$ such that when M is sufficiently large,

$$\operatorname{card}\mathcal{U} \ge 2C_1\big(\hat{M}^{1-\epsilon} - \langle g\rangle^{\epsilon}\big) \ge C_1\hat{M}^{1-\epsilon}. \tag{3.19}$$

Note that for each $\mathbf{y} \in I_P^d$, we have

$$\tilde{f}(\boldsymbol{\alpha}) = \sum_{\mathbf{x}\in I_P^d} e\Big(\sum_{\mathbf{i}\in\mathcal{R}_0'} \alpha_{\mathbf{i}}(\mathbf{x}+\mathbf{y})^{\mathbf{i}}\Big).$$

For $\mathbf{u} = (u_1,\dots,u_d)$ and $\mathbf{v} = (v_1,\dots,v_d)$, write $\mathbf{uv} = (u_1v_1,\dots,u_dv_d)$. Thus

$$\begin{aligned}\Big|\operatorname{card}\mathcal{U}^d \cdot \big(\hat{P}^d/\hat{M}^d\big)\cdot\tilde{f}(\boldsymbol{\alpha})\Big| &= \Big|\sum_{\mathbf{u}\in\mathcal{U}^d}\sum_{\mathbf{v}\in I_{P-M}^d}\sum_{\mathbf{x}\in I_P^d} e\Big(\sum_{\mathbf{i}\in\mathcal{R}_0'}\alpha_{\mathbf{i}}(\mathbf{x}+\mathbf{uv})^{\mathbf{i}}\Big)\Big| \\ &\le \hat{P}^d \max_{\mathbf{x}\in I_P^d}\big|\mathcal{H}(\boldsymbol{\alpha},\mathbf{x})\big|,\end{aligned}$$

where

$$\mathcal{H}(\boldsymbol{\alpha},\mathbf{x}) = \sum_{\mathbf{u}\in\mathcal{U}^d}\sum_{\mathbf{v}\in I_{P-M}^d} e\Big(\sum_{\mathbf{i}\in\mathcal{R}_0'}\alpha_{\mathbf{i}}(\mathbf{x}+\mathbf{uv})^{\mathbf{i}}\Big).$$

We have

$$\big|\mathcal{H}(\boldsymbol{\alpha},\mathbf{x})\big|^{2s} = \Big|\sum_{\mathbf{u}\in\mathcal{U}^d}\sum_{\mathbf{v}\in I_{P-M}^d} e\Big(\sum_{\mathbf{i}\in\mathcal{R}_0'}\alpha_{\mathbf{i}}(\mathbf{x}+\mathbf{uv})^{\mathbf{i}}\Big)\Big|^{2s}.$$

Let $\mathbf{j} = (j_1,\dots,j_d)$. Without loss of generality, assume that $p \nmid j_1$. By Hölder's inequality, we obtain

$$\begin{aligned}\big|\mathcal{H}(\boldsymbol{\alpha},\mathbf{x})\big|^{2s} &\le (\operatorname{card}\mathcal{U}^d)^{2s-1}\sum_{\mathbf{u}\in\mathcal{U}^d}\Big|\sum_{\mathbf{v}\in I_{P-M}^d} e\Big(\sum_{\mathbf{i}\in\mathcal{R}_0'}\alpha_{\mathbf{i}}\sum_{\mathbf{l}\in\mathcal{R}_{\mathbf{i}}\setminus\{\mathbf{0}\}}\binom{\mathbf{i}}{\mathbf{l}}\mathbf{x}^{\mathbf{i}-\mathbf{l}}\mathbf{u}^{\mathbf{l}}\mathbf{v}^{\mathbf{l}}\Big)\Big|^{2s} \\ &\le (\operatorname{card}\mathcal{U})^{2sd-1}\max_{u_2,\dots,u_d\in\mathcal{U}}\sum_{u_1\in\mathcal{U}}\Big|\sum_{\mathbf{v}\in I_{P-M}^d} e\Big(\sum_{\mathbf{i}\in\mathcal{R}_0'}\alpha_{\mathbf{i}}\sum_{\mathbf{l}\in\mathcal{R}_{\mathbf{i}}\setminus\{\mathbf{0}\}}\binom{\mathbf{i}}{\mathbf{l}}\mathbf{x}^{\mathbf{i}-\mathbf{l}}\mathbf{u}^{\mathbf{l}}\mathbf{v}^{\mathbf{l}}\Big)\Big|^{2s}.\end{aligned}$$

Define

$$\widetilde{\mathcal{H}}(\boldsymbol{\alpha})=\widetilde{\mathcal{H}}(\boldsymbol{\alpha};u_2,..,u_d;\mathbf{x})=\sum_{u_1\in\mathcal{U}}\bigg|\sum_{\mathbf{v}\in I_{P-M}^d}e\Big(\sum_{\mathbf{i}\in\mathcal{R}_0'}\alpha_{\mathbf{i}}\sum_{\mathbf{l}\in\mathcal{R}_{\mathbf{i}}\setminus\{\mathbf{0}\}}\begin{pmatrix}\mathbf{i}\\ \mathbf{l}\end{pmatrix}\mathbf{x}^{\mathbf{i}-\mathbf{l}}\mathbf{u}^{\mathbf{l}}\mathbf{v}^{\mathbf{l}}\Big)\bigg|^{2s}.$$

Thus we have

$$\big|\tilde{f}(\boldsymbol{\alpha})\big|^{2s}\le\big(\mathrm{card}\mathcal{U}\big)^{-1}\big(\hat{P}/\hat{M}\big)^{-2sd}\cdot\hat{P}^{2sd}\cdot\widetilde{\mathcal{H}}(\boldsymbol{\alpha}).\tag{3.20}$$

Note that

$$\widetilde{\mathcal{H}}(\boldsymbol{\alpha})=\sum_{u_1\in\mathcal{U}}\bigg|\sum_{\mathbf{v}_1,\dots,\mathbf{v}_s\in I_{P-M}^d}e\Big(\sum_{\mathbf{i}\in\mathcal{R}_0'}\alpha_{\mathbf{i}}\sum_{\mathbf{l}\in\mathcal{R}_{\mathbf{i}}\setminus\{\mathbf{0}\}}\begin{pmatrix}\mathbf{i}\\ \mathbf{l}\end{pmatrix}\mathbf{x}^{\mathbf{i}-\mathbf{l}}\mathbf{u}^{\mathbf{l}}(\mathbf{v}_1^{\mathbf{l}}+\cdots+\mathbf{v}_s^{\mathbf{l}})\Big)\bigg|^{2}.$$

For $\mathbf{y}=\big\{y_{\mathbf{h}}\in I_{|\mathbf{h}|(P-M)}\ \big|\ \mathbf{h}\in\mathcal{R}_0'\big\}$, define

$$a(\mathbf{y})=\mathrm{card}\big\{(\mathbf{v}_1,\dots,\mathbf{v}_s)\in\big(I_{P-M}^d\big)^s\ \big|\ \mathbf{v}_1^{\mathbf{h}}+\cdots+\mathbf{v}_s^{\mathbf{h}}=y_{\mathbf{h}}\ \big(\mathbf{h}\in\mathcal{R}_0'\big)\big\}.$$

For each $\mathbf{l}\in\mathcal{R}_0\setminus\{\mathbf{0}\}$, by Lemma 67, there exists a unique pair $(\mathbf{h}_{\mathbf{l}},n_{\mathbf{l}})\in\mathcal{R}_0'\times\mathbb{N}$ with $\mathbf{l}=p^{n_{\mathbf{l}}}\mathbf{h}_{\mathbf{l}}$. Then we have

$$\mathbf{v}_1^{\mathbf{l}}+\cdots+\mathbf{v}_s^{\mathbf{l}}=(\mathbf{v}_1^{\mathbf{h}_{\mathbf{l}}}+\cdots+\mathbf{v}_s^{\mathbf{h}_{\mathbf{l}}})^{p^{n_{\mathbf{l}}}}.$$

Thus for every $\mathbf{y}\in\big\{y_{\mathbf{h}}\in I_{|\mathbf{h}|(P-M)}\ \big|\ \mathbf{h}\in\mathcal{R}_0'\big\}=\prod_{\mathbf{h}\in\mathcal{R}_0'}I_{|\mathbf{h}|(P-M)}$, we have

$$a(\mathbf{y})=\mathrm{card}\big\{(\mathbf{v}_1,\dots,\mathbf{v}_s)\in\big(I_{P-M}^d\big)^s\ \big|\ \mathbf{v}_1^{\mathbf{l}}+\cdots+\mathbf{v}_s^{\mathbf{l}}=(y_{\mathbf{h}_{\mathbf{l}}})^{p^{n_{\mathbf{l}}}}\ \big(\mathbf{l}\in\mathcal{R}_0\setminus\{\mathbf{0}\}\big)\big\}.$$

Therefore

$$\widetilde{\mathcal{H}}(\boldsymbol{\alpha})=\sum_{u_1\in\mathcal{U}}\bigg|\sum_{\mathbf{y}}a(\mathbf{y})e\Big(\sum_{\mathbf{l}\in\mathcal{R}_0\setminus\{\mathbf{0}\}}\sigma_{\mathbf{l}}(u_1)(y_{\mathbf{h}_{\mathbf{l}}})^{p^{n_{\mathbf{l}}}}\Big)\bigg|^2,$$

where $\mathbf{y}$ runs over $\prod_{\mathbf{h}\in\mathcal{R}_0'}I_{|\mathbf{h}|(P-M)}$ and

$$\sigma_{\mathbf{l}}(u_1)=\sum_{\mathbf{i}\in\mathcal{R}_0',\,\mathbf{l}\in\mathcal{R}_{\mathbf{i}}}\alpha_{\mathbf{i}}\begin{pmatrix}\mathbf{i}\\ \mathbf{l}\end{pmatrix}\mathbf{x}^{\mathbf{i}-\mathbf{l}}\mathbf{u}^{\mathbf{l}}\quad\big(\mathbf{l}\in\mathcal{R}_0\setminus\{\mathbf{0}\}\big).$$

By the argument of [12, Lemma 20], there exists a subset $\mathcal{W}$ of $\mathcal{U}$ satisfying that for any two distinct elements u,w in $\mathcal{W}$, we have $u^{j_1}\equiv w^{j_1}\pmod g$ if and only if $u\equiv w\pmod g$ and satisfying that

$$\widetilde{\mathcal{H}}(\boldsymbol{\alpha})\le C_2\langle g\rangle^{\epsilon}\sum_{u\in\mathcal{W}}\bigg|\sum_{\mathbf{y}}a(\mathbf{y})e\Big(\sum_{\mathbf{l}\in\mathcal{R}_0\setminus\{\mathbf{0}\}}\sigma_{\mathbf{l}}(u)(y_{\mathbf{h}_{\mathbf{l}}})^{p^{n_{\mathbf{l}}}}\Big)\bigg|^2,\tag{3.21}$$

where $C_2 = C_2(q,k,\epsilon) > 0$. Note that for each $\mathbf{y} \in \prod_{\mathbf{h}\in\mathcal{R}_0'} I_{|\mathbf{h}|(P-M)}$, we may write $\mathbf{y} = (\mathbf{z}, y_{\mathbf{j}})$ with $\mathbf{z} \in \prod_{\mathbf{h}\in\mathcal{R}_0'\setminus\{\mathbf{j}\}} I_{|\mathbf{h}|(P-M)}$. Rewrite $a(\mathbf{y})$ with $a(\mathbf{z}, y_{\mathbf{j}})$. It follows from Cauchy's inequality that

$$\Big|\sum_{\mathbf{y}} a(\mathbf{y}) e\Big(\sum_{\mathbf{l}\in\mathcal{R}_0\setminus\{\mathbf{0}\}} \sigma_{\mathbf{l}}(u)(y_{\mathbf{h_l}})^{p^{n_{\mathbf{l}}}}\Big)\Big|^2 \le (\hat{P}/\hat{M})^{K'} \sum_{\mathbf{z}} \Big|\sum_{y_{\mathbf{j}}} a(\mathbf{z}, y_{\mathbf{j}}) e\big(\sigma_{\mathbf{j}}(u) y_{\mathbf{j}}\big)\Big|^2,$$

where $K' = \sum_{\mathbf{h}\in\mathcal{R}_0'\setminus\{\mathbf{j}\}} |\mathbf{h}|$. Since $|\mathbf{j}| = k$, $\mathbf{i} \in \mathcal{R}_0$ and $p \nmid \binom{\mathbf{i}}{\mathbf{j}}$, we have $\mathbf{i} = \mathbf{j}$ so that $\sigma_{\mathbf{j}}(u) = \alpha_{\mathbf{j}} u^{j_1} u_2^{j_2} \cdots u_d^{j_d}$. Now suppose that for any two distinct elements u, w in $\mathcal{W}$, we have

$$\langle \| \sigma_{\mathbf{j}}(u) - \sigma_{\mathbf{j}}(w) \| \rangle \ge q^{-k+1} \cdot \min\{\langle g\rangle^{-1}, (\hat{P}/\hat{M})^{-k}\}.$$

On applying the large sieve inequality for function field as given by [9, Theorem 2.4], we deduce that

$$\sum_{u\in\mathcal{W}} \Big|\sum_{y_{\mathbf{j}}} a(\mathbf{z}, y_{\mathbf{j}}) e\big(\sigma_{\mathbf{j}}(u) y_{\mathbf{j}}\big)\Big|^2 \le C_3\big(\langle g\rangle + (\hat{P}/\hat{M})^k\big) \sum_{y_{\mathbf{j}}} \big|a(\mathbf{z}, y_{\mathbf{j}})\big|^2,$$

where $C_3 = C_3(q,k) > 0$. Recalling (3.19), (3.20), and (3.21), we find that

$$\begin{aligned}\big|\tilde{f}(\boldsymbol{\alpha})\big|^{2s} &\le (\mathrm{card}\mathcal{U})^{-1}\big(\hat{P}/\hat{M}\big)^{-2sd} \cdot \hat{P}^{2sd} \cdot \widetilde{\mathcal{H}}(\boldsymbol{\alpha}) \\ &\le C\hat{M}^{-1+\epsilon}(\hat{P}/\hat{M})^{-2sd} \cdot \hat{P}^{2sd} \cdot \langle g\rangle^{\epsilon}(\hat{P}/\hat{M})^{K'}\big(\langle g\rangle + (\hat{P}/\hat{M})^k\big) \sum_{\mathbf{z}, y_{\mathbf{j}}} \big|a(\mathbf{z}, y_{\mathbf{j}})\big|^2,\end{aligned}$$

where $C = C_1^{-1}C_2C_3 + 1$. Note that $\sum_{\mathbf{z}, y_{\mathbf{j}}} \big|a(\mathbf{z}, y_{\mathbf{j}})\big|^2 = \sum_{\mathbf{y}} \big|a(\mathbf{y})\big|^2 = J_s(P-M)$, and that $K' = K_0 - |\mathbf{j}| = K_0 - k$. We obtain

$$\begin{aligned}\big|\tilde{f}(\boldsymbol{\alpha})\big|^{2s} &\le C\langle g\rangle^{\epsilon}\hat{P}^{2sd}\hat{M}^{-1+\epsilon}\big(\langle g\rangle + (\hat{P}/\hat{M})^k\big)(\hat{P}/\hat{M})^{-2sd+K'} J_s(P-M) \\ &\le C\langle g\rangle^{\epsilon}\hat{P}^{2sd}\hat{M}^{-1+\epsilon}\big(\langle g\rangle + (\hat{P}/\hat{M})^k\big)(\hat{P}/\hat{M})^{-k+\Delta_s} \\ &\le C\langle g\rangle^{\epsilon}\hat{P}^{2sd}\hat{M}^{-1+\epsilon}\big(\langle g\rangle(\hat{P}/\hat{M})^{-k} + 1\big)(\hat{P}/\hat{M})^{\Delta_s}.\end{aligned}$$

Thus

$$\big|\tilde{f}(\boldsymbol{\alpha})\big| \le C\langle g\rangle^{\epsilon}\hat{P}^{d+\epsilon}\Big(\hat{M}^{-1}\big(\langle g\rangle(\hat{P}/\hat{M})^{-k} + 1\big)(\hat{P}/\hat{M})^{\Delta_s}\Big)^{1/2s}.$$

It therefore remains to show that for distinct u, $w \in \mathcal{W}$, we have

$$\langle \| \sigma_{\mathbf{j}}(u) - \sigma_{\mathbf{j}}(w) \| \rangle \ge q^{-k+1} \cdot \min\{\langle g\rangle^{-1}, (\hat{P}/\hat{M})^{-k}\}.$$

Now write $\beta = \alpha_{\mathbf{j}} - a/g$. For $u, w \in \mathcal{W}$ with $u \not\equiv w (\mathrm{mod}\, g)$, we have $u^{j_1} \not\equiv w^{j_1} (\mathrm{mod}\, g)$. Since $\langle g\beta \rangle < \hat{M}^{-k}$ and $\mathrm{ord}\, u = [M]$, it follows that $\mathrm{ord}\, \beta < -kM - \mathrm{ord}\, g$ and hence

$$\mathrm{ord}\left(\beta(u^{j_1} - w^{j_1})u_2^{j_2} \cdots u_d^{j_d}\right) < -kM - \mathrm{ord}\, g + kM = -\mathrm{ord}\, g.$$

Also, since $\gcd(au_2^{j_2} \cdots u_d^{j_d}, g) = 1$ and $u^{j_1} - w^{j_1} \not\equiv 0 (\mathrm{mod}\, g)$, we have

$$\mathrm{ord}\ \| a(u^{j_1} - w^{j_1})u_2^{j_2} \cdots u_d^{j_d}/g \| \geq -\mathrm{ord}\, g.$$

Therefore

$$\mathrm{ord}\ \| \sigma_{\mathbf{j}}(u) - \sigma_{\mathbf{j}}(w) \| \geq -\mathrm{ord}\, g.$$

We now divide into two cases.
(i) Suppose that $\langle g \rangle > \hat{M}$. Since every element in $\mathcal{W}$ has order less than M, one can easily see that the elements in $\mathcal{W}$ are distinct modulo g and so are spaced at least $\langle g \rangle^{-1}$ apart.
(ii) Suppose that $\langle g \rangle \leq \hat{M}$. For two distinct elements $u, w \in \mathcal{W}$, if $u \not\equiv w (\mathrm{mod}\, g)$, then they are at least $\langle g \rangle^{-1}$ apart. Instead, if $u \equiv w (\mathrm{mod}\, g)$, then we have

$$\mathrm{ord}\ \| \alpha_{\mathbf{j}}(u^{j_1} - w^{j_1})u_2^{j_2} \cdots u_d^{j_d} \| = \mathrm{ord}\ \| \beta(u^{j_1} - w^{j_1})u_2^{j_2} \cdots u_d^{j_d} \| .$$

Since $\langle g\alpha_{\mathbf{j}} - a \rangle \geq \hat{M}\hat{P}^{-k}$, we get $\langle g\beta \rangle \geq \hat{M}\hat{P}^{-k}$, i.e., $\langle \beta \rangle \geq \hat{M}\hat{P}^{-k}\langle g \rangle^{-1}$. Thus,

$$\mathrm{ord}\left(\beta(u^{j_1} - w^{j_1})u_2^{j_2} \cdots u_d^{j_d}\right) \geq M - kP - \mathrm{ord}\, g + \mathrm{ord}\,(u^{j_1} - w^{j_1}) + (|\mathbf{j}| - j_1)(M-1).$$

Note that since $p \nmid j_1$, the argument of [12, Lemma 20] yields

$$\mathrm{ord}\,(u^{j_1} - w^{j_1}) \geq \mathrm{ord}\, g + (j_1 - 1)(M-1).$$

Therefore

$$\mathrm{ord}\ \| \sigma_{\mathbf{j}}(u) - \sigma_{\mathbf{j}}(w) \| = \mathrm{ord}\ \| \alpha_{\mathbf{j}}(u^{j_1} - w^{j_1})u_2^{j_2} \cdots u_d^{j_d} \| \geq -kP + kM - (k-1).$$

This completes the proof of the theorem.

3.5 The minor arc contribution

Recall that for each j with $1 \leq j \leq s$,

$$f_j(\boldsymbol{\alpha}) = f_j(\boldsymbol{\alpha}; P) = \sum_{\mathbf{x} \in I_P^d} e\Big(\sum_{\mathbf{i} \in \mathcal{L}} \alpha_{\mathbf{i}} \mathbf{x}^{\mathbf{i}}\Big).$$

Consider $s = l + 2m$ with $l, m \in \mathbb{N}$ and $m \geq r$.

Lemma 73. *For each j with $1 \le j \le l$, we have*

$$\sup_{\boldsymbol{\alpha}\in\mathfrak{m}} |f_j(\boldsymbol{\alpha})| \ll \hat{P}^{d-\sigma+\epsilon}$$

where $\sigma = \max_{n\in\mathbb{N}} \dfrac{1-(2\iota-1)\Delta_{nr}}{4nr\iota}$.

Proof. Take $\boldsymbol{\alpha} \in \mathfrak{m}$ and $M = \frac{1}{2\iota}P$. By [10, Lemma 3], for each $\mathbf{i} \in \mathcal{L}$, there exist $a_{\mathbf{i}} \in \mathbb{A}$ and monic $g_{\mathbf{i}} \in \mathbb{A}$ satisfying

$$0 \le \langle a_{\mathbf{i}}\rangle < \langle g_{\mathbf{i}}\rangle \le \hat{M}^k, \ \gcd(a_{\mathbf{i}}, g_{\mathbf{i}}) = 1, \text{ and } \ \langle g_{\mathbf{i}}c_j\alpha_{\mathbf{i}} - a_{\mathbf{i}}\rangle < \hat{M}^{-k}.$$

Assume that for every $\mathbf{i} \in \mathcal{L}$,

$$\langle g_{\mathbf{i}}\rangle \le \hat{M} \text{ and } \ \langle g_{\mathbf{i}}c_j\alpha_{\mathbf{i}} - a_{\mathbf{i}}\rangle < \hat{M}\hat{P}^{-k}.$$

Let $g = c_j \mathrm{lcm}\{g_{\mathbf{i}} | \mathbf{i} \in \mathcal{L}\}$ and $b_{\mathbf{i}} = ga_{\mathbf{i}}/c_j g_{\mathbf{i}}$. Then $\gcd(g, \mathbf{b}) = 1$. Moreover, for every $\mathbf{i} \in \mathcal{L}$,

$$\langle g\rangle \le \langle c_j\rangle \prod_{\mathbf{j}\in\mathcal{L}} \langle g_{\mathbf{j}}\rangle \le \langle c\rangle\langle g_{\mathbf{i}}\rangle \hat{M}^{\iota-1} \le \langle c\rangle \hat{P}^{1/2},$$

and

$$\langle g\alpha_{\mathbf{i}} - b_{\mathbf{i}}\rangle = \langle g\alpha_{\mathbf{i}} - \frac{a_{\mathbf{i}}g}{c_j g_{\mathbf{i}}}\rangle = \frac{\langle g\rangle}{\langle c_j g_{\mathbf{i}}\rangle}\langle c_j g_{\mathbf{i}}\alpha_{\mathbf{i}} - a_{\mathbf{i}}\rangle \le \hat{M}^{\iota-1}\hat{M}\hat{P}^{-k} = \hat{P}^{\frac{1}{2}-k}.$$

Thus $\alpha \in \mathfrak{M}$, contradicting the condition that $\alpha \in \mathfrak{m}$. Hence for some $\mathbf{i} \in \mathcal{L}$, $\langle g_{\mathbf{i}}\rangle > \hat{M}$ or $\langle g_{\mathbf{i}}c_j\alpha_{\mathbf{i}} - a_{\mathbf{i}}\rangle \ge \hat{M}\hat{P}^{-k}$. Then by Theorem 72, we have

$$|f_j(\boldsymbol{\alpha})| \ll \hat{P}^{d+\epsilon-\frac{1-(2\iota-1)\Delta_{nr}}{4nr\iota}}$$

for every $n \in \mathbb{N}$ with $n \ge 1$. □

Let $I_{m,k,d}(P)$ denotes the number of solutions of the system

$$\mathbf{x}_1^{\mathbf{i}} + \cdots + \mathbf{x}_m^{\mathbf{i}} = \mathbf{y}_1^{\mathbf{i}} + \cdots + \mathbf{y}_m^{\mathbf{i}} \ \ (\mathbf{i} \in \mathcal{L}) \tag{3.22}$$

with $\mathbf{x}_n, \mathbf{y}_n \in I_P^d$. For $\mathbf{h} \in \mathbb{A}^r$, write $J_{m,k,d}(P, \mathbf{h})$ for the number of solutions of the system

$$\left(\mathbf{x}_1^{\mathbf{i}} + \cdots + \mathbf{x}_m^{\mathbf{i}}\right) - \left(\mathbf{y}_1^{\mathbf{i}} + \cdots + \mathbf{y}_m^{\mathbf{i}}\right) = h_{\mathbf{i}} \ \ (\mathbf{i} \in \mathcal{R}_0')$$

with $\mathbf{x}_n, \mathbf{y}_n \in I_P^d$. By Lemma 61, $\mathcal{L} \subseteq \mathcal{R}_0'$. Hence we see that

$$I_{m,k,d}(P) = \sum_{\mathbf{h}} J_{m,k,d}(P, \mathbf{h})$$

where the summation is over all the vectors $\mathbf{h} \in \prod_{\mathbf{i} \in \mathcal{R}_0'} I_{|\mathbf{i}|P}$ with $h_{\mathbf{i}} = 0$ when $\mathbf{i} \in \mathcal{L}$. Thus,

$$I_{m,k,d}(P) \le \hat{P}^{K_0 - \iota k} J_{m,k,d}(P) \ll_{m,k,d} \hat{P}^{2md - \iota k + \Delta_m}.$$

Lemma 74. *Whenever* $s > \min\{l + 2m \,|\, l\sigma > \Delta_m, m \ge r, l, m \in \mathbb{N}\}$, *we have*

$$\int_{\mathfrak{m}} \prod_{j=1}^{s} f_j(\boldsymbol{\alpha}) d\boldsymbol{\alpha} \ll \hat{P}^{sd - \iota k - \delta}$$

for some $\delta > 0$.

Proof. It suffices to show that the result holds when

$$s = l + 2m = \min\{l + 2m \,|\, l\sigma > \Delta_m, m \ge r, l, m \in \mathbb{N}\}.$$

Note that

$$\int_{\mathfrak{m}} \prod_{j=1}^{s} f_j(\boldsymbol{\alpha}) d\boldsymbol{\alpha} \le \prod_{j=1}^{l} \sup_{\boldsymbol{\alpha} \in \mathfrak{m}} \big|f_j(\boldsymbol{\alpha})\big| \int_{\mathbb{T}^\iota} \prod_{j=l+1}^{l+2m} \big|f_j(\boldsymbol{\alpha})\big| d\boldsymbol{\alpha}.$$

By Hölder's inequality, we have

$$\int_{\mathbb{T}^\iota} \prod_{j=l+1}^{l+2m} \big|f_j(\boldsymbol{\alpha})\big| d\boldsymbol{\alpha} \le \prod_{j=l+1}^{l+2m} \bigg(\int_{\mathbb{T}^\iota} \big|f_j(\boldsymbol{\alpha})\big|^{2m} d\boldsymbol{\alpha} \bigg)^{1/2m}.$$

On considering the underlying diophantine equations, for each j with $l + 1 \le j \le l + 2m$, we have

$$\int_{\mathbb{T}^\iota} \big|f_j(\boldsymbol{\alpha})\big|^{2m} d\boldsymbol{\alpha} = I_{m,k,d}(P) \ll \hat{P}^{2md - \iota k + \Delta_m}.$$

Hence, it follows from Lemma 73 that

$$\int_{\mathfrak{m}} \prod_{j=1}^{s} f_j(\boldsymbol{\alpha}) d\boldsymbol{\alpha} \ll \Big(\hat{P}^{d - \sigma + \epsilon}\Big)^l \cdot \hat{P}^{2md - \iota k + \Delta_m} = \hat{P}^{sd - \iota k - (l\sigma - \Delta_m) + l\epsilon}$$

which can be bounded above by $\hat{P}^{sd - \iota k - \delta}$ for some $\delta > 0$ provided that $l\sigma > \Delta_m$. □

Lemma 75. *Let* $f(x) = Ce^{-Ex} + 2x$ *with* $C, E > 0$. *Then* $f(x)$ *obtains its minimum at* $x_0 = E^{-1} \log(CE/2)$ *and* $f(x_0) = 2E^{-1}\big(1 + \log(CE/2)\big)$.

Proof. Since $f'(x) = -CEe^{-Ex} + 2$ is an increasing function and $f'(x_0) = 0$, $f(x_0) = \min f(x)$. On noting that

$$f(x_0) = Ce^{-\log(CE/2)} + 2E^{-1}\log(CE/2) = 2E^{-1}\big(1 + \log(CE/2)\big),$$

the lemma follows. □

Theorem 76. *Suppose that $k \ge d + 2$. Whenever*

$$s \ge 2rk\Big(\log(\iota rk) + \log\big(\log\big((2\iota - 1)rk\log k\big) + 2k^{-1}\big) + 3 + \log 4 - \log\big(1 - (\log k)^{-1}\big)\Big),$$

we have

$$\int_{\mathfrak{m}} \prod_{j=1}^{s} f_j(\boldsymbol{\alpha}) d\boldsymbol{\alpha} \ll \hat{P}^{sd-\iota k-\delta},$$

where

$$\delta = \frac{1 - (\log k)^{-1}}{4\iota rk(\log((2\iota - 1)rk\log k) + 2k^{-1}\big)}.$$

Proof. By Theorem 71, $\Delta_s = rke^{-\frac{s-r}{rk}}$ is admissible. Let $f_0(x) = C_0e^{-E_0(x-r)} + 2x$ with $C_0 = \sigma^{-1}rk$ and $E_0 = \frac{1}{rk}$, where σ is defined as in Lemma 73. By Lemma 75, $\min f_0(x) = f(x_0)$ where $x_0 = r + E_0^{-1}\log(C_0E_0/2)$. Write $f_1(x) = rke^{-\frac{x-r}{rk}}$. Let

$$l_0 = [\sigma^{-1}f_1(x_0)] + 2 \quad \text{and} \quad m_0 = [x_0] + 1.$$

Then

$$l_0 > \sigma^{-1}f_1(x_0) + 1 > \sigma^{-1}f_1(m_0) + 1 = \sigma^{-1}\Delta_{m_0} + 1.$$

By Lemma 74, whenever $s \ge l_0 + 2m_0$, we have

$$\int_{\mathfrak{m}} \prod_{j=1}^{s} f_j(\boldsymbol{\alpha}) d\boldsymbol{\alpha} \ll \hat{P}^{sd-\iota k-\delta_0} \tag{3.23}$$

where $\delta_0 = l_0\sigma - \Delta_{m_0} - l_0\epsilon > \sigma$ if we choose ϵ small enough. Note that

$$\begin{aligned} l_0 + 2m_0 &\le \sigma^{-1}f_1(x_0) + 2x_0 + 4 = f_0(x_0) + 4 \\ &= 2E_0^{-1}\big(1 + \log(C_0E_0/2)\big) + 2r + 4 \\ &< 2rk\big(\log\sigma^{-1} + 3\big). \end{aligned} \tag{3.24}$$

On taking

$$n = [k\big(\log((2\iota-)rk\log k)\big)] + 2,$$

we deduce that

$$\sigma = \max_{n\in\mathbb{N}} \frac{1-(2\iota-1)\Delta_{nr}}{4nr\iota} > \frac{1-(\log k)^{-1}}{4\iota rk(\log((2\iota-1)rk\log k)+2k^{-1})},$$

i.e.,

$$\log\sigma^{-1} < \log(\iota rk) + \log\big(\log\big((2\iota-1)rk\log k\big)+2k^{-1}\big) + \log 4 - \log\big(1-(\log k)^{-1}\big).$$

On recalling (3.23) and (3.24), whenever

$$s \geq 2rk\Big(\log(\iota rk) + \log\big(\log\big((2\iota-1)rk\log k\big)+2k^{-1}\big) + 3 + \log 4 - \log\big(1-(\log k)^{-1}\big)\Big),$$

we have

$$\int_{\mathfrak{m}} \prod_{j=1}^{s} f_j(\boldsymbol{\alpha}) d\boldsymbol{\alpha} \ll \hat{P}^{sd-\iota k-\delta},$$

where

$$\delta = \frac{1-(\log k)^{-1}}{4\iota rk(\log((2\iota-1)rk\log k)+2k^{-1})}.$$

□

3.6 Refinements via repeated differencing process

In order to apply the repeat differencing process, we first describe the systems $\boldsymbol{\Psi}$ of type (j,P). To this end, we then need to define the difference operators. Suppose that $f(\mathbf{x})$ is a function from $\mathbb{A}^d$ to $\mathbb{A}$. For $\mathbf{h}=(\mathbf{h}_1,\dots,\mathbf{h}_j)\in(\mathbb{A}^j)^d$, define $\Delta_j(f(\mathbf{x});\mathbf{h})$ recursively by

$$\Delta_0(f(\mathbf{x})) = f(\mathbf{x}),$$

$$\Delta_1(f(\mathbf{x});\mathbf{h}_1) = f(\mathbf{x}+\mathbf{h}_1) - f(\mathbf{x}),$$

and

$$\Delta_j(f(\mathbf{x});\mathbf{h}_1,\dots,\mathbf{h}_j) = \Delta_1\big(\Delta_{j-1}(f(\mathbf{x});\mathbf{h}_1,\dots,\mathbf{h}_{j-1});\mathbf{h}_j\big).$$

Next for $w_1,\dots,w_j\in\mathbb{A}$, we define $\Psi_{\mathbf{i},j}$ ($\mathbf{i}\in\mathcal{R}_0$) recursively by taking $\Psi_{\mathbf{i},0}(\mathbf{x})=\mathbf{x}^{\mathbf{i}}$, defining

$$\Phi_{\mathbf{i},j-1}\big(\mathbf{x};\Psi_{\mathbf{i},j-1}(\mathbf{x};\mathbf{h}_1,\dots,\mathbf{h}_{j-1};w_1,\dots,w_{j-1})\big) \tag{3.25}$$

as in Remark 3, and setting

$$\Psi_{\mathbf{i},j}(\mathbf{x};\mathbf{h};\mathbf{w}) = w_j^{-|\mathbf{i}|}\Delta_1\big(\Phi_{\mathbf{i},j-1}(\mathbf{x});\mathbf{h}_j w_j^k\big). \tag{3.26}$$

We now remark that each $\Phi_{\mathbf{i},j-1}$ is a linear combination of $(\mathbf{\Psi}_{j-1})$. More precisely, there exists a d-tuple $\mathbf{a} \in \mathbb{A}^d$ with $\langle a_l \rangle \le \langle w_j \rangle^k$ $(1 \le l \le d)$ for which we may define a matrix C_j over $\mathbb{A}$ as in Lemma 64 such that

$$(\mathbf{\Phi}_{j-1}) = C_j\big(\Psi_{\mathbf{i},j-1}(\mathbf{x};\mathbf{h}_1,\dots,\mathbf{h}_{j-1};w_1,\dots,w_{j-1})\big)_{\mathbf{i}\in\mathcal{R}_0} = C_j(\mathbf{\Psi}_{j-1}).$$

On writing W_j for the diagonal matrix $(w_{\mathbf{i},\mathbf{j}})_{\mathbf{i},\mathbf{j}\in\mathcal{R}_0}$ with $w_{\mathbf{i},\mathbf{i}} = w_j^{-|\mathbf{i}|}$ $(\mathbf{i} \in \mathcal{R}_0)$, we have

$$(\mathbf{\Psi}_j) = \big(\Psi_{\mathbf{i},j}(\mathbf{x};\mathbf{h};\mathbf{w})\big)_{\mathbf{i}\in\mathcal{R}_0} = W_j C_j \Delta_1\big(\mathbf{\Psi}_{j-1}(\mathbf{x});\mathbf{h}_j w_j^k\big).$$

Thus,

$$\begin{aligned}(\mathbf{\Psi}_j) &= W_j C_j \cdots W_1 C_1 \Delta_j\big(\mathbf{\Psi}_0(\mathbf{x});\mathbf{h}_1 w_1^k,\dots,\mathbf{h}_j w_j^k\big)\\ &= W_j C_j \cdots W_1 C_1 \Delta_j\big((\mathbf{x}^{\mathbf{i}})_{\mathbf{i}\in\mathcal{R}_0};\mathbf{h}_1 w_1^k,\dots,\mathbf{h}_j w_j^k\big).\end{aligned} \tag{3.27}$$

For each $j \in \mathbb{N}$ with $1 \le j \le \gamma_q(k)$, we aim to show that $(\mathbf{\Psi}_j)$ is of type (j,P) when we take $w_1,\dots,w_j$ as in the proof of the fundamental lemma. It suffices to show the following:
(i) There is a block matrix

$$T = \begin{pmatrix} T_1 & T_2 \\ 0 & T_3 \end{pmatrix}$$

over $\mathbb{A}$ with each entry bounded by $\hat{P}^{kj}$ such that

$$\begin{pmatrix} (\Psi_{\mathbf{i},j})_{\mathbf{i}\in\mathcal{R}_0'} \\ (\Psi_{\mathbf{j},j})_{\mathbf{j}\in\mathcal{R}_0''} \end{pmatrix} = \begin{pmatrix} T_1 & T_2 \\ 0 & T_3 \end{pmatrix} \begin{pmatrix} (\mathbf{x}^{\mathbf{n}})_{\mathbf{n}\in\mathcal{R}_j'} \\ (\mathbf{x}^{\mathbf{m}})_{\mathbf{m}\in\mathcal{R}_j''} \end{pmatrix}. \tag{3.28}$$

(ii) We define in Remark 2(1) that

$$\mathcal{R}_{j,u}' = \big\{\mathbf{i} \in \mathcal{R}_j' \,|\, |\gamma_q(\mathbf{i})| = u\big\} \quad \text{and} \quad T_{u,v} = \big(T_{\mathbf{i},\mathbf{n}}\big)_{\mathbf{i}\in\mathcal{R}_{0,u}',\mathbf{n}\in\mathcal{R}_{j,v}'}.$$

For $u \in \{1,\dots,\gamma_q(k)\}$ and $v \in \{1,\dots,\gamma_q(k)-j\}$, we have that

$$T_{u,v} = 0 \quad \text{whenever} \quad u - v < j, \tag{3.29}$$

and

$$T_{u,u-j} \ne 0 \quad \text{for some} \quad u \ge j. \tag{3.30}$$

By (3.27), we start with analyzing $\Delta_j(\mathbf{x}^{\mathbf{i}}; \mathbf{h}_1, \dots, \mathbf{h}_j)$. Let $\mathcal{A}$ and $\mathcal{B}$ be two disjoint subsets of $\{1, 2, \dots, n\}$. Write $\mathcal{B} = \{j_1, \dots, j_m\}$. For $h_1, \dots, h_n \in \mathbb{A}$, define

$$D_m\big(f(z); \mathbf{h}; \mathcal{A}; \mathcal{B}\big) = \Delta_m\bigg(f\bigg(z + \sum_{i \in \mathcal{A}} h_i\bigg); h_{j_1}, \dots, h_{j_m}\bigg), \tag{3.31}$$

where Δ_m is the one-dimensional version of the difference operator defined above.

Lemma 77. *Let $j \in \mathbb{N} \setminus \{0\}$ and let $\mathbf{h}_l = (h_{l1}, \dots, h_{ld})$ $(1 \le l \le j)$. We have*

$$\Delta_j(\mathbf{x}^{\mathbf{i}}; \mathbf{h}_1, \dots, \mathbf{h}_j) = \sum_{\substack{\mathcal{A}_1 \sqcup \cdots \sqcup \mathcal{A}_d \\ = \{1, \dots, j\}}} \prod_{n=1}^{d} D_{|\mathcal{A}_n|}\big(x_n^{i_n}; \mathbf{h}_n^*; \mathcal{A}_1 \sqcup \cdots \sqcup \mathcal{A}_{n-1}; \mathcal{A}_n\big),$$

where $\mathbf{h}_n^* = (h_{1n}, \dots, h_{jn})$.

Proof. The proof is identical to the one of [15, Lemma 3.3]. □

For a positive integer i, we denote the set

$$\tilde{i} = \bigg\{ l \in \mathbb{Z} \,\Big|\, 0 \le l < i,\ p \nmid \binom{i}{l} \bigg\}.$$

By Lemma 60, $l \in \tilde{i}$ if and only if

$$l \ne i \quad \text{and} \quad 0 \le a_n(l) \le a_n(i)\ (n \in \mathbb{N}). \tag{3.32}$$

Furthermore, if $l \in \tilde{i}$, then

$$\gamma_q(i - l) = \sum_{n \ge 0} \big(a_n(i) - a_n(l)\big) = \gamma_q(i) - \gamma_q(l). \tag{3.33}$$

Proposition 78. *Let $j \in \mathbb{N} \setminus \{0\}$ and $h_1, w_1, \dots, h_j, w_j \in \mathbb{A}$. Then the following hold.*
(1) If $1 \le j \le \gamma_q(i)$, then

$$\Delta_j(x^i; h_1, \dots, h_j) = \sum_{\substack{\gamma_q(i - l_j) \ge j \\ l_j \in \tilde{i}}} f_{l_j}(h_1, \dots, h_j) x^{l_j},$$

where

$$f_{l_j}(h_1, \dots, h_j) = \sum_{l_1 \in \tilde{i}, l_2 \in \widetilde{l_1}, \dots, l_j \in \widetilde{l_{j-1}}} \binom{i}{l_1} \cdots \binom{l_{j-1}}{l_j} h_1^{i - l_1} \cdots h_j^{l_{j-1} - l_j}$$

is a nonzero polynomial in $\mathbb{F}_q[h_1,\dots,h_j]$ *and is divisible by* $h_1\cdots h_j$.
(2) If $j>\gamma_q(i)$, *then* $\Delta_j(x^i;h_1,\dots,h_j)$ *is identically zero in* $\mathbb{A}[x]$.
(3) Let $\mathcal{A}$ *and* $\mathcal{B}$ *be two disjoint subsets of* $\{1,\dots,j\}$ *and let* $\mathcal{B}=\{j_1,\dots,j_m\}$. *Then*

$$D_m\big(x^i;h_1w_1^k,\dots,h_jw_j^k;\mathcal{A};\mathcal{B}\big)=\sum_{\substack{\gamma_q(v)\geq m\\ v\in\tilde{i}\cup\{i\}}}\sum_{\substack{\gamma_q(v-l)\geq m\\ l\in\tilde{v}}}g_{v,l}(\mathbf{h},\mathbf{w})x^l,$$

where

$$g_{v,l}(\mathbf{h},\mathbf{w})=\binom{i}{v}\Big(\sum_{u\in\mathcal{A}}h_uw_u^k\Big)^{i-v}f_l\big(h_{j_1}w_{j_1}^k,\dots,h_{j_m}w_{j_m}^k\big),$$

and $g_{v,l}(\mathbf{h},\mathbf{w})$ *is divisible by* $h_{j_1}w_{j_1}^k\cdots h_{j_m}w_{j_m}^k$.

Proof. (1) We prove it by induction on j. When $j=1$, we see that

$$\Delta_1(x^i;h_1)=(x+h_1)^i-x^i=\sum_{0\leq l_1<i}\binom{i}{l_1}x^l=\sum_{\substack{\gamma_q(i-l_1)\geq 1\\ l_1\in\tilde{i}}}f_{l_1}(h_1)x^{l_1},$$

where $f_{l_1}(h_1)=\binom{i}{l_1}h_1^{i-l_1}$ is nonzero since $p\nmid\binom{i}{l_1}$. Suppose that the result is true for j. By the induction hypothesis, we have

$$\begin{aligned}\Delta_{j+1}(x^i;h_1,\dots,h_{j+1})&=\Delta_1(\Delta_j(x^i;h_1,\dots,h_j);h_{j+1})\\&=\Delta_1\bigg(\sum_{\substack{\gamma_q(i-l_j)\geq j\\ l_j\in\tilde{i}}}f_{l_j}(h_1,\dots,h_j)x^{l_j};h_{j+1}\bigg).\end{aligned}$$

On applying the result in the case when $j=1$, we see that

$$\begin{aligned}\Delta_{j+1}(x^i;h_1,\dots,h_{j+1})&=\sum_{\substack{\gamma_q(i-l_j)\geq j\\ l_j\in\tilde{i}}}f_{l_j}(h_1,\dots,h_j)\Delta_1(x^{l_j};h_{j+1})\\&=\sum_{\substack{\gamma_q(i-l_j)\geq j\\ l_j\in\tilde{i}}}f_{l_j}(h_1,\dots,h_j)\sum_{\substack{l_{j+1}\in\tilde{l_j}\\ \gamma_q(l_j-l_{j+1})\geq 1}}\binom{l_j}{l_{j+1}}h_{j+1}^{(l_j-l_{j+1})}x^{l_{j+1}}\\&=\sum_{\substack{\gamma_q(i-l_j)\geq j\\ \gamma_q(l_j-l_{j+1})\geq 1\\ l_j\in\tilde{i},l_{j+1}\in\tilde{l_j}}}\binom{l_j}{l_{j+1}}f_{l_j}(h_1,\dots,h_j)h_{j+1}^{(l_j-l_{j+1})}x^{l_{j+1}}.\end{aligned}$$

It follows from (3.32) and (3.33) that

$$\Delta_{j+1}(x^i; h_1, \ldots, h_{j+1}) = \sum_{\substack{\gamma_q(i-l_{j+1}) \geq j+1 \\ l_{j+1} \in \tilde{i}}} f_{l_{j+1}}(h_1, \ldots, h_{j+1}) x^{l_{j+1}}.$$

Note that if $l_1 \in \tilde{i}, l_2 \in \widetilde{l_1}, \ldots, l_j \in \widetilde{l_{j-1}}$, then

$$i - l_1, l_1 - l_2, \ldots, l_{j-1} - l_j > 0.$$

In view of the definition of the function $f_{l_j}(h_1, \ldots, h_j)$, we see that $h_1 \cdots h_j$ divides $f_{l_j}(h_1, \ldots, h_j)$.

(2) Note that $\gamma_q(i-l) \geq \gamma_q(i)$ with $l \in \tilde{i}$ if and only if $l = 0$. Thus, when $j = \gamma_q(i)$,

$$\Delta_j(x^i; h_1, \ldots, h_j) = f_0(h_1, \ldots, h_j).$$

Hence, when $j > \gamma_q(i)$, $\Delta_j(x^i; h_1, \ldots, h_j) = 0$.

(3) By (3.31) and the linearity of the difference operator Δ, we have

$$\begin{aligned} D_m(x^i; h_1 w_1^k, \ldots, h_j w_j^k; \mathcal{A}; \mathcal{B}) &= \Delta_m \left(\left(x + \sum_{u \in \mathcal{A}} h_u w_u^k \right)^i ; h_{j_1} w_{j_1}^k, \ldots, h_{j_m} w_{j_m}^k \right) \\ &= \sum_{\substack{\gamma_q(v) \geq m \\ v \in \tilde{i} \cup \{i\}}} \binom{i}{v} \left(\sum_{u \in \mathcal{A}} h_u w_u^k \right)^{i-v} \Delta_m\big(x^v; h_{j_1} w_{j_1}^k, \ldots, h_{j_m} w_{j_m}^k\big). \end{aligned}$$

From Proposition 78(1), we find that

$$\Delta_m(x^v; h_{j_1} w_{j_1}^k, \ldots, h_{j_m} w_{j_m}^k) = \sum_{\substack{\gamma_q(v-l) \geq m \\ l \in \tilde{v}}} f_l\big(h_{j_1} w_{j_1}^k, \ldots, h_{j_m} w_{j_m}^k\big) x^l.$$

Thus

$$D_m(x^i; h_1 w_1^k, \ldots, h_j w_j^k; \mathcal{A}; \mathcal{B}) = \sum_{\substack{\gamma_q(v) \geq m \\ v \in \tilde{i} \cup \{i\}}} \sum_{\substack{\gamma_q(v-l) \geq m \\ l \in \tilde{v}}} g_{v,l}(\mathbf{h}, \mathbf{w}) x^l,$$

where

$$g_{v,l}(\mathbf{h}, \mathbf{w}) = \binom{i}{v} \left(\sum_{u \in \mathcal{A}} h_u w_u^k \right)^{i-v} f_l\big(h_{j_1} w_{j_1}^k, \ldots, h_{j_m} w_{j_m}^k\big).$$

Again by Proposition 78(1), $g_{v,l}(\mathbf{h}, \mathbf{w})$ is divisible by $h_{j_1} w_{j_1}^k \cdots h_{j_m} w_{j_m}^k$. This completes the proof of the proposition. □

Corollary 79. *Let $j \in \mathbb{Z}$ with $1 \le j \le k'$, $\mathbf{h}_l = (h_{l1}, \dots, h_{ld}) \in \mathbb{A}^d$ and $w_l \in \mathbb{A}$ $(1 \le l \le j)$. Then the following hold.*
(1) For every $\mathbf{i} \in \mathcal{R}_0$, we have

$$\Delta_j(\mathbf{x}^{\mathbf{i}}; \mathbf{h}_1 w_1^k, \dots, \mathbf{h}_j w_j^k) = \sum_{\mathbf{l} \in \mathcal{R}_j} b_{\mathbf{i},\mathbf{l}} \mathbf{x}^{\mathbf{l}}, \tag{3.34}$$

where each $b_{\mathbf{i},\mathbf{l}}$ is a polynomial in $(\mathbf{h}_1, \dots, \mathbf{h}_j; w_1, \dots, w_j)$ and is divided by $w_1^k \cdots w_j^k$.
(2) For $\mathbf{i} \in \mathcal{R}_0$ and $\mathbf{l} \in \mathcal{R}_j$ with $|\gamma_q(\mathbf{i})| - |\gamma_q(\mathbf{l})| < j$, we have $b_{\mathbf{i},\mathbf{l}} = 0$.
(3) For $\mathbf{j} \in \mathcal{R}_0''$ and $\mathbf{n} \in \mathcal{R}_j'$, we have $b_{\mathbf{j},\mathbf{n}} = 0$.
(4) For every $u \in \mathbb{N}$ with $j+1 \le u \le k'$, there exist $\mathbf{i} \in \mathcal{R}_0'$ with $|\gamma_q(\mathbf{i})| = u$ and $\mathbf{n} \in \mathcal{R}_j' \cap \mathcal{R}_{\mathbf{i}}$ with $|\gamma_q(\mathbf{n})| = u - j$ such that $b_{\mathbf{i},\mathbf{n}}$ is a nonzero polynomial in $(\mathbf{h}_1, \dots, \mathbf{h}_j; w_1, \dots, w_j)$.

Proof. (1) In view of Lemma 77, if $\Delta_j\big(\mathbf{x}^{\mathbf{i}}; \mathbf{h}_1 w_1^k, \dots, \mathbf{h}_j w_j^k\big)$ contains $\mathbf{x}^{\mathbf{l}} = x_1^{l_1} \cdots x_d^{l_d}$ explicitly, then there exists a disjoint union $\mathcal{A}_1 \sqcup \cdots \sqcup \mathcal{A}_d = \{1, \dots, j\}$ such that each $x_n^{l_n}$ $(1 \le n \le d)$ appears in

$$D_{|\mathcal{A}_n|}\big(x_n^{i_n}; \mathbf{h}_n^*; \mathcal{A}_1 \sqcup \cdots \sqcup \mathcal{A}_{n-1}; \mathcal{A}_n\big).$$

From Proposition 78(3) we deduce that for each $n \in \mathbb{N}$ with $1 \le n \le d$, there exists $v_n \in \widetilde{i_n} \cup \{i_n\}$ such that

$$l_n \in \widetilde{v_n} \quad \text{and} \quad |\gamma_q(v_n)| - |\gamma_q(l_n)| \ge |\mathcal{A}_n|.$$

On writing $\mathbf{v} = (v_1, \dots, v_d)$, we have

$$\mathbf{l} \in \mathcal{R}_{\mathbf{v}} \quad \text{and} \quad |\gamma_q(\mathbf{v})| - |\gamma_q(\mathbf{l})| \ge \sum_{n=1}^{d} |\mathcal{A}_n| = j.$$

Since $v_n \in \widetilde{i_n} \cup \{i_n\}$ $(1 \le n \le d)$, we have $\mathbf{v} \in \mathcal{R}_{\mathbf{i}}$. It follows from Lemma 62(2) that

$$\mathbf{l} \in \mathcal{R}_{\mathbf{v}} \subseteq \mathcal{R}_{\mathbf{i}} \quad \text{and} \quad |\gamma_q(\mathbf{i})| - |\gamma_q(\mathbf{l})| \ge |\gamma_q(\mathbf{v})| - |\gamma_q(\mathbf{l})| \ge j. \tag{3.35}$$

Since $|\gamma_q(\mathbf{i})| \le \gamma_q(k) = k'$ and

$$\mathcal{R}_j = \big\{\mathbf{i} \in \mathcal{R}_0 \,\big|\, |0 \le |\gamma_q(\mathbf{i})| \le k' - j\big\},$$

by Lemma 62(4), we have $\mathbf{l} \in \mathcal{R}_j$. Thus

$$\Delta_j\big(\mathbf{x}^{\mathbf{i}}; \mathbf{h}_1 w_1^k, \dots, \mathbf{h}_j w_j^k\big) = \sum_{\mathbf{l} \in \mathcal{R}_{\mathbf{i}} \cap \mathcal{R}_j} b_{\mathbf{i},\mathbf{l}} \mathbf{x}^{\mathbf{l}}, \tag{3.36}$$

where $b_{\mathbf{i},\mathbf{l}} = b_{\mathbf{i},\mathbf{l}}(\mathbf{h},\mathbf{w}) \in \mathbb{A}$. Next we will prove each $b_{\mathbf{i},\mathbf{l}}$ is divisible by $w_1^k \cdots w_j^k$. Fix a disjoint union $\mathcal{A}_1 \sqcup \cdots \sqcup \mathcal{A}_d = \{1,\ldots,j\}$. For $n \in \mathbb{N}$ with $1 \le n \le d$, by Proposition 78(3), whenever $\mathcal{A}_n \neq \emptyset$, we see that $\prod_{u\in\mathcal{A}_n} w_u^k$ divides the coefficients of the polynomial

$$D_{|\mathcal{A}_n|}\big(x_n^{i_n}; (\mathbf{hw})_n^*; \mathcal{A}_1 \sqcup \cdots \sqcup \mathcal{A}_{n-1}; \mathcal{A}_n\big),$$

where $(\mathbf{hw})_n^* = \big(h_{1n}w_1^k, \cdots, h_{jn}w_j^k\big)$. It follows from Lemma 77 and Proposition 78 that $w_1^k \cdots w_j^k$ divides the coefficients of $\Delta_j\big(\mathbf{x}^{\mathbf{i}}; \mathbf{h}_1 w_1^k, \ldots, \mathbf{h}_j w_j^k\big)$.

(2) By (3.35), every nonzero $b_{\mathbf{i},\mathbf{l}}$ in (3.34) satisfies $|\gamma_q(\mathbf{i})| - |\gamma_q(\mathbf{l})| \ge j$.

(3) Suppose that $\mathbf{j} \in \mathcal{R}_0''$. It follows from Lemma 62(3) that if $\mathbf{l} \in \mathcal{R}_{\mathbf{j}}$ then $\mathbf{l} \in \mathcal{R}_0''$. Thus $\mathcal{R}_{\mathbf{j}} \cap \mathcal{R}_j \subseteq \mathcal{R}_j''$. By (3.36), we obtain $b_{\mathbf{j},\mathbf{n}} = 0$ whenever $\mathbf{n} \in \mathcal{R}_j'$.

(4) Fix $u \in \mathbb{N}$ with $j+1 \le u \le k'$. Then there exists $\mathbf{i} = (i_1,\ldots,i_d) \in \mathcal{R}_0'$ such that

$$|\gamma_q(\mathbf{i})| = u, \quad \gamma_q(i_1) \ge j+1 \quad \text{and} \quad a_0(i_1) \ge 1.$$

Therefore, there exists $n_1 \in \widetilde{i_1}$ with $p \nmid n_1$ and $\gamma_q(n_1) = \gamma_q(i_1) - j$. Write $\mathbf{n} = (n_1, i_2, \ldots, i_d)$. Hence $|\gamma_q(\mathbf{n})| = u - j$ and $\mathbf{n} \in \mathcal{R}_{\mathbf{i}} \cap \mathcal{R}_j'$. By Proposition 78(1), $\Delta_j(x^{i_1}; h_1, \ldots, h_j)$ contains $f(h_1,\ldots,h_j)x^{n_1}$, where

$$f(h_1,\ldots,h_j) = \sum_{\substack{l_1 \in \widetilde{l_0}, l_2 \in \widetilde{l_1}, \ldots, l_j \in \widetilde{l_{j-1}} \\ l_0 = i_1, l_j = n_1}} \binom{l_0}{l_1} \cdots \binom{l_{j-1}}{l_j} h_1^{l_0 - l_1} \cdots h_j^{l_{j-1} - l_j}$$

is a nonzero polynomial in $\mathbb{F}_q[h_1,\ldots,h_j]$. On taking

$$\mathcal{A}_1 = \{1,\ldots,j\},\ \mathcal{A}_2 = \cdots = \mathcal{A}_d = \emptyset,$$

we have

$$\begin{aligned} &\Delta_j(x^{i_1}; h_{1n}w_1^k, \ldots, h_{jn}w_j^k) x_2^{i_2} \cdots x_d^{i_d} \\ &= \prod_{n=1}^{j} D_{|\mathcal{A}_n|}\big(x_n^{i_n}; (\mathbf{hw})_n^*; \mathcal{A}_1 \sqcup \cdots \sqcup \mathcal{A}_{n-1}; \mathcal{A}_n\big). \end{aligned} \tag{3.37}$$

Thus the coefficient of $x_1^{n_1} x_2^{i_2} \cdots x_d^{i_d}$ appearing in (3.37) is $f(h_{11}w_1^k, \ldots, h_{j1}w_j^k)$. For a disjoint union $\mathcal{A}_1 \sqcup \cdots \sqcup \mathcal{A}_d = \{1,\ldots,j\}$ with $\mathcal{A}_n \neq \emptyset$ for some $2 \le n \le d$, by Proposition 78(2), $D_{|\mathcal{A}_n|}\big(x_n^{i_n}; (\mathbf{hw})_l^*; \mathcal{A}_1 \sqcup \cdots \sqcup \mathcal{A}_{n-1}; \mathcal{A}_n\big)$ does not contain $x_n^{i_n}$ explicitly. Therefore, $x_1^{n_1} x_2^{i_2} \cdots x_d^{i_d}$ only appears in (3.37) explicitly. Thus in (3.34) $b_{\mathbf{i},\mathbf{n}} = f(h_{11}w_1^k, \ldots, h_{j1}w_j^k)$ is a nonzero polynomial in $(\mathbf{h},\mathbf{w})$. □

Remark 4 (1) For every $1 \leq j \leq k'$, by Corollary 79(1) and 79(3), we have

$$\Delta_j\left(\begin{pmatrix} (\mathbf{x}^{\mathbf{i}})_{\mathbf{i}\in\mathcal{R}'_0} \\ (\mathbf{x}^{\mathbf{j}})_{\mathbf{j}\in\mathcal{R}''_0} \end{pmatrix}; \mathbf{h}_1 w_1^k, \ldots, \mathbf{h}_j w_j^k\right) = \begin{pmatrix} B_1 & B_2 \\ 0 & B_3 \end{pmatrix} \begin{pmatrix} (\mathbf{x}^{\mathbf{n}})_{\mathbf{n}\in\mathcal{R}'_j} \\ (\mathbf{x}^{\mathbf{m}})_{\mathbf{m}\in\mathcal{R}''_j} \end{pmatrix}, \tag{3.38}$$

where $B_1 = \left(b_{\mathbf{i},\mathbf{n}}\right)_{\mathbf{i}\in\mathcal{R}'_0,\mathbf{n}\in\mathcal{R}'_j}$, $B_2 = \left(b_{\mathbf{i},\mathbf{m}}\right)_{\mathbf{i}\in\mathcal{R}'_0,\mathbf{m}\in\mathcal{R}''_j}$, and $B_3 = \left(b_{\mathbf{j},\mathbf{m}}\right)_{\mathbf{j}\in\mathcal{R}''_0,\mathbf{m}\in\mathcal{R}''_j}$ with all entries defined as (3.34). By (3.27) and (3.38), we have

$$\left(\mathbf{\Psi}_j\right) = \begin{pmatrix} (\Psi_{\mathbf{i},j})_{\mathbf{i}\in\mathcal{R}'_0} \\ (\Psi_{\mathbf{j},j})_{\mathbf{j}\in\mathcal{R}''_0} \end{pmatrix} = W_j C_j \cdots W_1 C_1 \begin{pmatrix} B_1 & B_2 \\ 0 & B_3 \end{pmatrix} \begin{pmatrix} (\mathbf{x}^{\mathbf{n}})_{\mathbf{n}\in\mathcal{R}'_j} \\ (\mathbf{x}^{\mathbf{m}})_{\mathbf{m}\in\mathcal{R}''_j} \end{pmatrix}. \tag{3.39}$$

(2) Let

$$T = W_j C_j \cdots W_1 C_1 \begin{pmatrix} B_1 & B_2 \\ 0 & B_3 \end{pmatrix}.$$

To prove that $(\mathbf{\Psi}_j)$ is of type (j, P), we shall show that T satisfies (3.28), (3.29) and (3.30). By Remark 3 and Lemma 66, for every $l \in \mathbb{N}$ with $1 \leq l \leq j$, we may write

$$C_l = \begin{pmatrix} C_{l1} & C_{l2} \\ 0 & C_{l3} \end{pmatrix}, \tag{3.40}$$

where

$$C_{l1} = \begin{pmatrix} I_{k'} & * & \cdots & * \\ 0 & I_{k'-1} & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & I_1 \end{pmatrix}. \tag{3.41}$$

Recall that for each l with $1 \leq l \leq j$,

$$W_l = \left(w_{\mathbf{i},\mathbf{j}}^{(l)}\right)_{\mathbf{i},\mathbf{j}\in\mathcal{R}_0}$$

is the diagonal matrix with $w_{\mathbf{i},\mathbf{i}}^{(l)} = w_l^{-|\mathbf{i}|}$. For $u \in \mathbb{N}$ with $1 \leq u \leq k'$, write

$$W_{l,1,u} = \left(w_{\mathbf{i},\mathbf{j}}^{(l)}\right)_{\mathbf{i},\mathbf{j}\in\mathcal{R}'_{0,u}}.$$

Then we can represent W_l by

$$W_l = \begin{pmatrix} W_{l1} & 0 \\ 0 & W_{l3} \end{pmatrix}, \tag{3.42}$$

where

$$W_{l1} = \begin{pmatrix} W_{l,1,k'} & 0 & \cdots & 0 \\ 0 & W_{l,1,k'-1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & W_{l,1,1} \end{pmatrix}. \tag{3.43}$$

By (3.40) and (3.42), we find that

$$\begin{aligned} T &= W_j C_j \cdots W_1 C_1 \begin{pmatrix} B_1 & B_2 \\ 0 & B_3 \end{pmatrix} \\ &= \begin{pmatrix} W_{j1}C_{j1}\cdots W_{11}C_{11}B_1 & * \\ 0 & W_{j3}C_{j3}\cdots W_{13}C_{13}B_3 \end{pmatrix}. \end{aligned}$$

For $i \in \{1, 3\}$, write

$$T_i = W_{j1}C_{ji}\cdots W_{1i}C_{1i}B_i. \tag{3.44}$$

From (3.39) and Corollary 79(1), we see that

$$T = \begin{pmatrix} T_1 & T_2 \\ 0 & T_3 \end{pmatrix}$$

having entries over $\mathbb{A}$ and satisfies (3.28).

(3) To show that T also satisfies (3.29) and (3.30), we start by considering B_1 in (3.38). Recall that $\mathcal{R}'_{j,v} = \{\mathbf{n} \in \mathcal{R}'_j \mid |\gamma_q(\mathbf{n})| = v\}$ $(0 \le j \le k')$. Then by setting

$$B_{u,v} = (b_{\mathbf{i},\mathbf{n}})_{\mathbf{i}\in\mathcal{R}'_{0,u},\mathbf{n}\in\mathcal{R}'_{j,v}},$$

we have

$$B_1 = \begin{pmatrix} (B_{u,v})_{u\ge j+1} \\ (B_{u,v})_{u\le j} \end{pmatrix}.$$

By Corollary 79(2), we have $B_{u,v} = 0$ whenever $u - v < j$. Thus

$$B_1 = \begin{pmatrix} B_{k',k'-j} & * & \cdots & * \\ 0 & B_{k'-1,k'-1-j} & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & B_{j+1,1} \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}.$$

By (3.41), (3.43) and (3.44), we have

$$T_1 = \begin{pmatrix} T_{k',k'-j} & * & \cdots & * \\ 0 & T_{k'-1,k'-1-j} & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & T_{j+1,1} \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix},$$

where

$$T_{u,u-j} = \prod_{l=1}^{j} W_{l,1,u} B_{u,u-j} \quad \big(u \in \{k', \ldots, j+1\}\big).$$

Moreover, the zero blocks imply that $T_{u,v} = 0$ whenever $u - v < j$. This means that T satisfies (3.29).

(4) For every $j+1 \leq u \leq k'$, write

$$T_{u,u-j} = (T_{\mathbf{i},\mathbf{n}})_{\mathbf{i} \in \mathcal{R}'_{0,u}, \mathbf{n} \in \mathcal{R}'_{j,u-j}}.$$

By Remark 4(2), we have

$$T_{\mathbf{i},\mathbf{n}} = (w_j \cdots w_1)^{-|\mathbf{i}|} b_{\mathbf{i},\mathbf{n}}.$$

By Corollary 79(4), $B_{u,u-j} \neq 0$. Thus, $T_{u,u-j} \neq 0$ for every $u \in \mathbb{N}$ with $j+1 \leq u \leq k'$. Thus T satisfies (3.30).

(5) It is worth a reminder that to prove that $(\mathbf{\Psi}_j)$ is of type (j, P), since T has satisfied (3.28), (3.29) and (3.30), it remains to show that every entry of T can be bounded by $\hat{P}^{kj}$.

Corollary 80. *Let $\mathbf{h} \in I_P^d$. Then the coefficients of $\Delta_1(\mathbf{x}^{\mathbf{i}}; \mathbf{h})$ can be bounded above by $\hat{P}^{|\mathbf{i}|}$.*

Proof. By Lemma 77, we have

$$\Delta_1(\mathbf{x}^{\mathbf{i}}; \mathbf{h}) = \sum_{\substack{\mathbf{j} \in \mathbb{N}^d \\ |\mathbf{j}|=1}} \prod_{l=1}^{d} \Delta_{j_l}(x^{i_l}; h_l).$$

Every $\mathbf{j} \in \mathbb{N}^d$ with $|\mathbf{j}| = 1$ only has one $j_l = 1$ and has the other coordinates equal to 0. It follows from Proposition 78(1) that

$$\Delta_1(x^{i_l}; h_l) = \sum_{n \in \tilde{i}_l} \begin{pmatrix} i_l \\ n \end{pmatrix} h_l^{(i_l - n)} x^n.$$

Thus every nonzero coefficient of $\Delta_1(\mathbf{x}^{\mathbf{i}}; \mathbf{h})$ must be of form $\begin{pmatrix} i_l \\ n \end{pmatrix} h_l^{i_l - n}$, which is bounded above by $\hat{P}^{|\mathbf{i}|}$. □

Lemma 81. *Let $j \in \mathbb{N}$ with $0 \le j \le k'$. The following hold.*
(1) The polynomials $\Psi_{\mathbf{i},j}(\mathbf{i} \in \mathcal{R}_0)$ form a system of type (j, P).
(2) Suppose that $j > 0$. For $\mathbf{h}_l = (h_{l1}, \ldots, h_{ld}) \in \mathbb{A}^d$ and $w_l \in \mathbb{A}$ $(1 \le l \le j)$, suppose that $\mathbf{h}_l w_l^k \in I_P^d$. Then for $j \in \mathbb{N}$ with $1 \le j < a_D(k)$, we have $K(\mathbf{\Psi}_j) \ge K_{\mathcal{R}}$ where $K_{\mathcal{R}} = \sum_{\mathbf{i} \in \mathcal{R}} |\mathbf{i}|$ and

$$\mathcal{R} = \begin{cases} \{\mathbf{i} \in \mathcal{R}_0' \,|\, a_D(i_1) \ge j,\ |a_0(i_1)| \ge 1\}, & \text{if } D > 0, \\ \{\mathbf{i} \in \mathcal{R}_0' \,|\, |\mathbf{i}| \ge j+1, i_1 \ge j\}, & \text{if } D = 0. \end{cases}$$

Proof. (1) When $j = 0$, $\Psi_{\mathbf{i},0}(\mathbf{x}) = \mathbf{x}^{\mathbf{i}}$, which is of type $(0, P)$. For $j > 0$, as we mention in Remark 4(5), it suffices to show that each entry of

$$T = W_j C_j \cdots W_1 C_1 \begin{pmatrix} B_1 & B_2 \\ 0 & B_3 \end{pmatrix}$$

can be bounded above by $\hat{P}^{kj}$. We prove it by induction on j. Assume that the result is true for $j \ge 0$, i.e.,

$$\Psi_{\mathbf{i},j}(\mathbf{x}) = \sum_{\mathbf{l} \in \mathcal{R}_j} T_{\mathbf{i},\mathbf{l}} \mathbf{x}^{\mathbf{l}}$$

with $T_{\mathbf{i},\mathbf{l}} \le \hat{P}^{kj}$ $\big(\mathbf{i} \in \mathcal{R}_0, \mathbf{l} \in \mathcal{R}_j\big)$. Moreover, $(\mathbf{\Phi})_j = C_{j+1}(\mathbf{\Psi})_j$ where $C_{j+1} = (a_{\mathbf{i},\mathbf{j}})_{\mathbf{i},\mathbf{j} \in \mathcal{R}_0}$ is defined as in Lemma 66 by

$$a_{\mathbf{i},\mathbf{j}} = \begin{cases} \begin{pmatrix} i_1 \\ j_1 \end{pmatrix} \cdots \begin{pmatrix} i_d \\ j_d \end{pmatrix} (-\mathbf{a})^{\mathbf{i}-\mathbf{j}}, & \text{if } \ \mathbf{j} \in \mathcal{R}_{\mathbf{i}}, \\ 0, & \text{otherwise.} \end{cases}$$

Hence

$$\Phi_{\mathbf{i},j}(\mathbf{x}) = \sum_{\mathbf{j}\in\mathcal{R}_\mathbf{i}} a_{\mathbf{i},\mathbf{j}}\Psi_{\mathbf{j},j}(\mathbf{x}) \quad (\mathbf{i}\in\mathcal{R}_0).$$

By (3.26) and the linearity of Δ_1, we have

$$\begin{aligned}\Psi_{\mathbf{i},j+1}(\mathbf{x};\mathbf{h};\mathbf{w}) &= w_{j+1}^{-|\mathbf{i}|}\Delta_1(\Phi_{\mathbf{i},j}(\mathbf{x});\mathbf{h}_{j+1}w_{j+1}^k)\\ &= w_{j+1}^{-|\mathbf{i}|}\sum_{\mathbf{j}\in\mathcal{R}_\mathbf{i}} a_{\mathbf{i},\mathbf{j}}\sum_{\mathbf{l}\in\mathcal{R}_j} T_{\mathbf{i},\mathbf{l}}\Delta_1(\mathbf{x}^\mathbf{n};\mathbf{h}_{j+1}w_{j+1}^k).\end{aligned}$$

Note that we can pick $\mathbf{a} = (a_1,\ldots,a_d)\in\mathbb{A}^d$ with $\langle a_l\rangle < \langle w_{j+1}\rangle$ $(1\le l\le d)$. Thus $\langle a_{\mathbf{i},\mathbf{j}}\rangle < \langle w_{j+1}\rangle^{|\mathbf{i}|}$. Also, since $\langle T_{\mathbf{i},\mathbf{l}}\rangle \le \hat{P}^{kj}$, it follows from Corollary 80 that the coefficients of $\Psi_{\mathbf{i},j+1}$ can be bounded by $\hat{P}^{k(j+1)}$. Thus, by induction, the system $\mathbf{\Psi}_j$ is of type (j,P).

(2) Suppose $0\le j < a_D(k)$. It suffices to show that the matrix $T_\mathcal{R}$ defined by (3.12) has rank $\operatorname{card}\mathcal{R}$. Write $B_1 = \left(b_{\mathbf{i},\mathbf{n}}\right)_{\mathbf{i}\in\mathcal{R}'_0,\mathbf{n}\in\mathcal{R}'_j}$. On recalling Remark 2(4) and 4(4), we have

$$T_\mathcal{R} = \begin{pmatrix} T_{k',k'-j,\mathcal{R}} & 0 & \cdots & 0\\ 0 & T_{k'-1,k'-1-j,\mathcal{R}} & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & T_{j+1,1,\mathcal{R}}\end{pmatrix}, \tag{3.45}$$

where for $u\in\mathbb{N}$ with $j+1\le u\le k'$,

$$T_{u,u-j,\mathcal{R}} = \left((w_j\cdots w_1)^{-|\mathbf{i}|}b_{\mathbf{i},\mathbf{n}}\right)_{\mathbf{i}\in\mathcal{R}\cap\mathcal{R}'_{0,u},\mathbf{n}\in\mathcal{R}'_{j,u-j}}.$$

Define

$$\mathcal{C}_u = \left\{\left(i_1 - jp^D, i_2,\ldots,i_d\right) \mid (i_1,i_2,\ldots,i_d)\in\mathcal{R}\cap\mathcal{R}'_{0,u}\right\}.$$

By the definition of $\mathcal{R}$, we have $\mathcal{R}\subseteq\mathcal{R}'_j$. Also, let M_u denote the sub-matrix of $T_{u,u-j,\mathcal{R}}$ consisting of the entries $(w_j\cdots w_1)^{-|\mathbf{i}|}b_{\mathbf{i},\mathbf{n}}$ indexed by $\mathbf{i}\in\mathcal{R}\cap\mathcal{R}'_{0,u}$ and $\mathbf{n}\in\mathcal{C}_u$. Assume that every M_u has rank $\operatorname{card}(\mathcal{R}\cap\mathcal{R}'_{0,u})$. Thus, $T_{u,u-j,\mathcal{R}}$ has rank $\operatorname{card}(\mathcal{R}\cap\mathcal{R}'_{0,u})$. Since $\mathcal{R}\subseteq\cup_{u=j+1}^{k'}\mathcal{R}'_{0,u}$, we obtain

$$\sum_{u=j+1}^{k'}\operatorname{card}(\mathcal{R}\cap\mathcal{R}'_{0,u}) = \operatorname{card}\mathcal{R}.$$

Hence $T_\mathcal{R}$ has rank $\operatorname{card}\mathcal{R}$ and $K(\mathbf{\Psi}_j)\ge K_\mathcal{R}$.

It remains to show that every M_u has rank $\mathrm{card}\,(\mathcal{R}\cap\mathcal{R}'_{0,u})$. Now we write $\mathbf{i}\succ\mathbf{j}$ if and only if there exists $l\in\mathbb{N}$ with $1\le l<d$ such that $i_1=j_1,\dots,i_l=j_l$ and $i_{l+1}>j_{l+1}$. For every $u\in\mathbb{N}$ with $j+1\le u\le k'$, we can place the entries of M_u in lexicographic order "$\succ$". More precisely, $b_{\mathbf{i}',\mathbf{n}}$ is above $b_{\mathbf{i},\mathbf{n}}$ if $\mathbf{i}'\succ\mathbf{i}$. Similarly, $b_{\mathbf{i},\mathbf{n}'}$ is at the left of $b_{\mathbf{i},\mathbf{n}}$ if $\mathbf{n}'\succ\mathbf{n}$. We will show that M_u is a lower triangular matrix with nonzero diagonal entries. For $\mathbf{i}\in\mathcal{R}\cap\mathcal{R}'_{0,u}$, let $\mathbf{i}_j=(i_1-jp^D,i_2,\dots,i_d)\in\mathcal{C}_u$. Thus the $b_{\mathbf{i},\mathbf{i}_j}$ are the diagonal entries, which are not zero by the argument of Corollary 79(4) with $n_1=i_1-jp^D$. Take $\mathbf{i}',\mathbf{i}\in\mathcal{R}\cap\mathcal{R}'_{0,u}$ with $\mathbf{i}'\succ\mathbf{i}$. Then $\mathbf{i}'_j\succ\mathbf{i}_j$ and we have the following array of entries of M_u

$$\begin{array}{ccc}(\mathbf{i}',\mathbf{i}'_j) & \cdots & (\mathbf{i}',\mathbf{i}_j)\\ \vdots & \ddots & \vdots\\ (\mathbf{i},\mathbf{i}'_j) & \cdots & (\mathbf{i},\mathbf{i}_j).\end{array}$$

Assume that the $(\mathbf{i}',\mathbf{i}_j)$-th entry is nonzero, i.e., $(w_j\cdots w_1)^{-|\mathbf{i}|}b_{\mathbf{i}',\mathbf{i}_j}\neq 0$. Then $\mathbf{i}_j\in\mathcal{R}_{\mathbf{i}'}$ and for all $2\le l\le d$, $h\ge 0$ and $0\le n<D$, we have

$$a_h(i_l)\le a_h(i'_l),\quad a_n(i_1)\le a_n(i'_1),\quad\text{and}\quad a_D(i_1)-j\le a_D(i'_1).\tag{3.46}$$

Since $|\gamma_q(\mathbf{i}_j)|=|\gamma_q(\mathbf{i})|-j=u-j$, we have

$$j=|\gamma_q(\mathbf{i}')|-|\gamma_q(\mathbf{i}_j)|=\sum_{l=2}^{d}\Big(\gamma_q(i'_l)-\gamma_q(i_l)\Big)+\sum_{h=0}^{D}\Big(a_h(i'_1)-a_h(i_1)\Big)+j.\tag{3.47}$$

Thus

$$\sum_{l=2}^{d}\Big(\gamma_q(i'_l)-\gamma_q(i_l)\Big)+\sum_{h=0}^{D}\Big(a_h(i'_1)-a_h(i_1)\Big)=0.$$

Since $i'_1\ge i_1$, we have $a_D(i'_1)\ge a_D(i_1)$. On recalling (3.46), we conclude that for all $1\le l\le d$ and $h\ge 0$,

$$a_h(i_l)=a_h(i'_l).$$

Thus, $\mathbf{i}'=\mathbf{i}$, which contradicts $\mathbf{i}'\succ\mathbf{i}$. Therefore, $b_{\mathbf{i}',\mathbf{i}_j}$ must be zero. This completes the proof of the lemma. □

Recall that

$$f(\boldsymbol{\alpha};P)=\sum_{\mathbf{i}\in I_P^d}e\Big(\sum_{\mathbf{i}\in\mathcal{R}_0}\alpha_{\mathbf{i}}\mathbf{x}^{\mathbf{i}}\Big),$$

and hat $J_s(P) = J_{s,k,d}(P)$ is defined to be the number of solutions of the system

$$\mathbf{x}_1^{\mathbf{i}} + \cdots + \mathbf{x}_s^{\mathbf{i}} = \mathbf{y}_1^{\mathbf{i}} + \cdots + \mathbf{y}_s^{\mathbf{i}} \quad (\mathbf{i} \in \mathcal{R}_0)$$

with $\mathbf{x}_m$, $\mathbf{y}_m \in I_P^d$. Also, recall that we denote by $K_s(P, Q; \mathbf{\Psi})$ the number of solutions of the system

$$\sum_{n=1}^{r} \Big(\Psi_{\mathbf{i}}(\mathbf{z}_n) - \Psi_{\mathbf{i}}(\mathbf{z}'_n) \Big) = \sum_{m=1}^{s} (\mathbf{x}_m^{\mathbf{i}} - \mathbf{y}_m^{\mathbf{i}}) \quad (\mathbf{i} \in \mathcal{R}_0)$$

with $\mathbf{z}_n, \mathbf{z}'_n \in I_P^d$ and $\mathbf{x}_m, \mathbf{y}_m \in I_Q^d$. Furthermore, we denote by $L_s(P, Q, \theta, w; \mathbf{\Psi})$ the number of solutions of the system

$$\sum_{n=1}^{r} \Big(\Psi_{\mathbf{i}}(\mathbf{z}_n) - \Psi_{\mathbf{i}}(\mathbf{z}'_n) \Big) = w^{|\mathbf{i}|} \sum_{m=1}^{s} (\mathbf{u}_m^{\mathbf{i}} - \mathbf{v}_m^{\mathbf{i}}) \quad (\mathbf{i} \in \mathcal{R}_0)$$

with $\mathbf{z}$ and $\mathbf{z}'$ as above, $\mathbf{u}_m, \mathbf{v}_m \in I_{Q-\theta P}^d$, and $z_{nl} \equiv z'_{nl} \pmod{w^k}$ $(1 \le l \le d)$. We now set up the apparatus necessary to achieve the efficient differencing process.

Lemma 82. *Let $(\mathbf{\Phi}_j)$ be the system defined as in (3.25). Suppose that $\theta P \le Q \le P$. Write $H = (1 - k\theta)P$. Then there exist $\mathbf{h} \in \mathbb{A}^d$ with $1 \le \langle h_l \rangle \le \hat{H}$ and $w \in \mathcal{P}(\theta, \epsilon)$ such that*

$$L_s(P, Q, \theta; \mathbf{\Phi}_j) \ll \hat{P}^{(2d-1-(d-1)k\theta)r} J_s(Q - \theta P) + \hat{H}^{dr} \Big(K_s(P, Q - \theta P; \mathbf{\Psi}_{j+1}) J_s(Q - \theta P) \Big)^{1/2},$$

where $(\mathbf{\Psi}_{j+1})$ is given by (3.26), i.e.,

$$\Psi_{\mathbf{i},j+1}(\mathbf{z}) = w^{-|\mathbf{i}|} \Big(\Phi_{\mathbf{i},j}(\mathbf{z} + \mathbf{h}w^k) - \Phi_{\mathbf{i},j}(\mathbf{z}) \Big) \quad (\mathbf{i} \in \mathcal{R}_0).$$

Proof. Fix $w \in \mathcal{P}(\theta, \epsilon)$. For each $\mathbf{i} \in \mathcal{R}_0$, the coefficients of $\Psi_{\mathbf{i},j+1}(\mathbf{z})$ lie in $\mathbb{A}[\mathbf{h}]$. Consider the roots $\mathbf{h}$ of the nonzero coefficients for all $\Psi_{\mathbf{i},j+1}(\mathbf{z})$, and let $\mathcal{T}$ denote the set of roots which also lie in

$$\big\{ \mathbf{h} \in \mathbb{A}^d \,\big|\, \langle h_l \rangle \le \hat{H} \ (1 \le l \le d) \big\}.$$

Then we have $L_s(P, Q, \theta, w; \mathbf{\Phi}_j) = U_0 + U_1$, where U_0 denotes the number of solutions for which $\mathbf{z}_n = \mathbf{z}'_n + \mathbf{h}w^k$ for some $n \in \mathbb{N}$ with $1 \le n \le r$ and $\mathbf{h} \in \mathcal{T}$, and where U_1 is the number of solutions with $\mathbf{z}_n \ne \mathbf{z}'_n + \mathbf{h}w^k$ for all n $(1 \le n \le r)$ and $\mathbf{h} \in \mathcal{T}$.

First, suppose that $U_0 \ge U_1$. Since the number of nonzero coefficients can be bounded by a constant in terms of k and d, we have

$$\operatorname{card} \mathcal{T} = O\big(\hat{H}^{d-1}\big) = O\big(\hat{P}^{(1-k\theta)(d-1)}\big).$$

It follows that the number of pairs $(\mathbf{z}_n, \mathbf{z}'_n)$ with $\mathbf{z}_n = \mathbf{z}'_n + \mathbf{h}w^k$ for some $\mathbf{h} \in \mathcal{T}$ is $O\big(\hat{P}^d \hat{P}^{(1-k\theta)(d-1)}\big)$. Write $\boldsymbol{\alpha w} = (\alpha_{\mathbf{i}} w^{|\mathbf{i}|})_{\mathbf{i}\in\mathcal{R}_0}$. In view of the congruence conditions on $\mathbf{z}$ and $\mathbf{z}'$, we have

$$U_0 \ll \hat{P}^d \hat{P}^{(1-k\theta)(d-1)} \int_{\mathbb{T}^{r_0}} V_w(\boldsymbol{\alpha})^{r-1} \Big| f(\boldsymbol{\alpha w}; Q-\theta P)^{2s} \Big| d\boldsymbol{\alpha},$$

where

$$V_w(\boldsymbol{\alpha}) = \sum_{\mathbf{z}\in(\mathbb{A}/(w^k))^d} \Bigg| \sum_{\substack{\mathbf{x}\in I_P^d \\ \mathbf{x}\equiv\mathbf{z}(\mathrm{mod}\, w^k)}} e\Big(\sum_{\mathbf{i}\in\mathcal{R}_0} \alpha_{\mathbf{i}} \Phi_{\mathbf{i}}(\mathbf{x}, \boldsymbol{\eta}) \Big) \Bigg|^2.$$

It now follows from Hölder's inequality that U_0 is bounded above by

$$\hat{P}^d \hat{P}^{(1-k\theta)(d-1)} \Big(\int_{\mathbb{T}^{r_0}} g_w(\boldsymbol{\alpha})^r \Big| f(\boldsymbol{\alpha w}; Q-\theta P)^{2s} \Big| d\boldsymbol{\alpha} \Big)^{1-1/r} \Big(\int_{\mathbb{T}^{r_0}} \Big| f(\boldsymbol{\alpha w}; Q-\theta P)^{2s} \Big| d\boldsymbol{\alpha} \Big)^{1/r}.$$

On considering the underlying equations, we see that

$$L_s(P, Q, \theta, w; \boldsymbol{\Phi}_j) \ll \hat{P}^{(2d-1-(d-1)k\theta)r} J_s(Q-\theta P). \tag{3.48}$$

Next suppose that $U_1 \geq U_0$ instead. Write

$$z'_{nl} = z_{nl} + h_{nl} w^k \quad (1 \leq n \leq r,\ 1 \leq l \leq d),$$

where h_{nl} satisfy $1 \leq \langle h_{nl} \rangle \leq \hat{H}$ and $\mathbf{h} \notin \mathcal{T}$. Therefore, U_1 can be bounded above by the number of solutions of the system

$$\sum_{n=1}^{r} \Psi_{\mathbf{i},j+1}(\mathbf{z}_n; \mathbf{h}_n; w) = \sum_{m=1}^{s} (\mathbf{u}_m^{\mathbf{i}} - \mathbf{v}_m^{\mathbf{i}}) \quad (\mathbf{i} \in \mathcal{R}_0),$$

where $\mathbf{z}_n \in I_P^d$, $\mathbf{h}_n \in I_H^d$, and $\mathbf{u}_m, \mathbf{v}_m \in I_{Q-\theta P}^d$. Now write

$$W_w(\boldsymbol{\alpha}; \mathbf{h}) = \sum_{\mathbf{z}\in I_P^d} e\Big(\sum_{\mathbf{i}\in\mathcal{R}_0} \alpha_{\mathbf{i}} \Psi_{\mathbf{i},j+1}(\mathbf{z}; \mathbf{h}; w) \Big).$$

Then we have

$$U_1 \ll \int_{\mathbb{T}^{r_0}} \Bigg(\sum_{\mathbf{h}\in I_H^d} W_w(\boldsymbol{\alpha}; \mathbf{h}) \Bigg)^r \Big| f(\boldsymbol{\alpha w}; Q-\theta P)^{2s} \Big| d\boldsymbol{\alpha}.$$

Furthermore, by Hölder's inequality, we deduce that

$$\Bigg(\sum_{\mathbf{h}\in I_H^d} W_w(\boldsymbol{\alpha}; \mathbf{h}) \Bigg)^r \ll \hat{H}^{d(r-1)} \sum_{\mathbf{h}\in I_H^d} \Big| W_w(\boldsymbol{\alpha}; \mathbf{h}) \Big|^r.$$

Thus,

$$U_1 \ll \hat{H}^{d(r-1)+d} \max_{\mathbf{h}} \int_{\mathbb{T}^{r_0}} \Big| W_w(\boldsymbol{\alpha}; \mathbf{h})^r f(\boldsymbol{\alpha}\boldsymbol{w}; Q-\theta P)^{2s} \Big| d\boldsymbol{\alpha}$$
$$\leq \hat{H}^{dr} \max_{\mathbf{h}} \left(\int_{\mathbb{T}^{r_0}} \Big| W_w(\boldsymbol{\alpha}; \mathbf{h})^{2r} f(\boldsymbol{\alpha}\boldsymbol{w}; Q-\theta P)^{2s} \Big| d\boldsymbol{\alpha} \right)^{1/2} \left(\int_{\mathbb{T}^{r_0}} \Big| f(\boldsymbol{\alpha}\boldsymbol{w}; Q-\theta P)^{2s} \Big| d\boldsymbol{\alpha} \right)^{1/2}.$$

Since the first integral above is bounded by $K_s(P, Q-\theta P; \boldsymbol{\Psi}_{j+1})$ where $\Psi_{\mathbf{i},j+1} = \Psi_{\mathbf{i},j+1}(\mathbf{z}; \mathbf{h}; w)$ for some $\mathbf{h} \in \mathbb{A}^d$ with $1 \leq \langle h_l \rangle \leq \hat{H}$. On recalling (3.48) and taking the maximum over $w \in \mathcal{P}(\theta, \epsilon)$, the lemma follows. □

In what follows, write $K_j = K(\boldsymbol{\Psi}_j)$, $\mu_j = \operatorname{card}\big\{\mathbf{i} \in \mathcal{R}_0' \,\big|\, |\gamma_q(\mathbf{i}) \leq j\big\}$, and $\Omega_j = K_0 - K_j - \mu_j$.

Theorem 83. *Let $u \in \mathbb{N}$ with $u \geq r$. Suppose that $\Delta_u < (k-1)(r+1)$ is an admissible exponent, and let $j \in \mathbb{N}$ with $1 \leq j \leq \gamma_q(k)$. For each $l \in \mathbb{N} \setminus \{0\}$, we write $s = u + lr$ and define the numbers $\phi(j, s, J)$, θ_s, and Δ_s recursively as follows. Given a value of Δ_{s-r}, we set $\phi(j, s, j) = 1/k$ and evaluate $\phi(j, s, J-1)$ successively for $J = j, \dots, 2$ by setting*

$$\phi^*(j, s, J-1) = \frac{1}{2k} + \left(\frac{1}{2} + \frac{\Omega_{J-1} - \Delta_{s-r}}{2kr} \right) \phi(j, s, J),$$

and

$$\phi(j, s, J-1) = \min\big\{1/k, \phi^*(j, s, J-1)\big\}.$$

Finally, we set

$$\theta_s = \min_{1 \leq j \leq \gamma_q(k)} \phi(j, s, 1)$$

and

$$\Delta_s = \Delta_{s-r}(1-\theta_s) + r(k\theta_s - 1).$$

Then Δ_s is an admissible exponent for $s = u + lr$ for all $l \in \mathbb{N} \setminus \{0\}$.

Proof. Fix $s \geq u$ and suppose that δ_s is an admissible exponent. According to the hypothesis of Δ_u, we have

$$\Delta_s \leq \Delta_u < (k-1)(r+1). \tag{3.49}$$

Take j to be the least integer for which $\phi(j, s+r, 1) = \theta_{s+r}$, and write $\phi_J = \phi(j, s+r, J)$ for $J = j, \dots, 1$. The minimality of j ensures that $\phi_J < 1/k$ whenever $J < j$. We adopt the notation

$$M_i = \phi_i P, \quad H_i = (1 - k\phi_i)P, \quad Q_i = (1 - \phi_1 - \cdots - \phi_i)P \quad (1 \leq i \leq j),$$

with the convention that $Q_0 = P$. We now show inductively that for each $J = j-1, \dots, 0$,

$$L_s(P, Q_J, \phi_{J+1}; \mathbf{\Phi}_J) \ll \hat{P}^{(2d-1-(d-1)k\phi_{J+1})r} \widehat{Q_{J+1}}^{\lambda_s}. \tag{3.50}$$

When $J = j-1$, it follows from Lemma 82 that

$$L_s(P, Q_{j-1}, \phi_j; \mathbf{\Phi}_{j-1}) \ll \hat{P}^{(2d-1-(d-1)k\phi_j)r} J_s(Q_j) + \widehat{H_j}^{dr} \big(K_s(P, Q_j; \mathbf{\Psi}_j) J_s(Q_j)\big)^{1/2}.$$

Since $\phi_j = 1/k$, we have $\widehat{H_j} = 1$. By estimating $K_s(P, Q_j; \mathbf{\Psi}_j) \ll \hat{P}^{2rd} \widehat{Q_j}^{\lambda_s}$, we obtain

$$L_s(P, Q_{j-1}, \phi_j; \mathbf{\Phi}_{j-1}) \ll \hat{P}^{dr} J_s(Q_j) \ll \hat{P}^{dr} \widehat{Q_j}^{\lambda_s}.$$

Now suppose that the result holds for $J \in \{j-1, \dots, 1\}$. Then by Lemmas 68 and 82, we see that

$$L_s(P, Q_{J-1}, \phi_J; \mathbf{\Phi}_{J-1}) \ll \hat{P}^{(2d-1-(d-1)k\phi_J)r} J_s(Q_J) + \widehat{H_J}^{dr} \big(K_s(P, Q_J; \mathbf{\Psi}_J) J_s(Q_J)\big)^{1/2},$$

and

$$K_s(P, Q_J; \mathbf{\Psi}_J) \ll \hat{P}^{\Gamma_1} J_s(Q_J) + \hat{P}^{\Gamma_2} L_s(P, Q_J, \phi_{J+1}; \mathbf{\Phi}_J),$$

where $\Gamma_1 = 2rd - (r+1)(1-\phi_{J+1}) + \epsilon$ and $\Gamma_2 = \phi_{J+1}(2sd + krd - \mu_J - K_J)$. By the induction hypothesis, we have

$$L_s(P, Q_{J-1}, \phi_J; \mathbf{\Phi}_{J-1}) \ll \hat{P}^{(2d-1-(d-1)k\phi_J)r} J_s(Q_J) + \widehat{H_J}^{dr} \widehat{Q_J}^{\lambda_s} (E_1 + E_2)^{1/2},$$

where

$$E_1 = \hat{P}^{2rd-r-1+\epsilon} \widehat{M_{J+1}}^{r+1} \quad \text{and} \quad E_2 = \hat{P}^{2rd-r} \widehat{M_{J+1}}^{2sd+kr-\mu_J-K_J-\lambda_s}.$$

On combining (3.49) with $\lambda_s = 2sd - K_0 + \Delta_s$ and $\mu_J + K_J \le K_0$, we have

$$\begin{aligned} E_1/E_2 &= \hat{P}^{\epsilon-1+\phi_{J+1}(r+1)-\phi_{J+1}(kr-\mu_J-K_J+K_0-\Delta_s)} \\ &\le \hat{P}^{\epsilon-1+\phi_{J+1}(r+1-kr+\Delta_s)} < 1, \end{aligned}$$

i.e., $E_1 < E_2$. Thus

$$L_s(P, Q_{J-1}, \phi_J; \mathbf{\Phi}_{J-1}) \ll \widehat{Q_J}^{\lambda_s} (\hat{P}^{\Lambda_1} + \hat{P}^{\Lambda_2}),$$

where

$$\Lambda_1 = (2d - 1 - (d-1)k\phi_J)r,$$

and

$$\Lambda_2 = dr(1-k\phi_J) + \frac{1}{2}(2rd-r) + \frac{1}{2}(2sd+kr-\mu_J-K_J-\lambda_s)\phi_{J+1}.$$

Then by the definition of ϕ_J, we have $\Lambda_1 = \Lambda_2$. By induction, (3.50) follows. On applying (3.50) with $J=0$, we conclude that

$$L_s(P,P,\phi_1;\mathbf{\Phi}_0) \ll \hat{P}^{(2d-1-(d-1)k\phi_1)r+(1-\phi_1)\lambda_s}.$$

Thus we obtain from Lemma 68 that

$$J_{s+r}(P) = K_s(P,P,\mathbf{\Psi}_0) \ll \hat{P}^{\Lambda_3} + \hat{P}^{\Lambda_4},$$

where

$$\Lambda_3 = 2rd - (1-\phi_1)(r+1) + \lambda_s + \epsilon,$$

and

$$\Lambda_4 = (1-\phi_1)\lambda_s + \big(2d-1-(d-1)k\phi_1\big)r + \phi_1(2sd+krd-K_0).$$

By (3.49) and $\lambda_s = 2sd - K_0 + \Delta_s$, we see that

$$\begin{aligned}\Lambda_3 - \Lambda_4 &= \epsilon - 1 + \phi_1(r+1) + \phi_1 kr(d-1) - \phi_1(krd-\Delta_s)\\ &= \epsilon - 1 + \phi_1(r+1+\Delta_s - kr)\\ &\le 0,\end{aligned}$$

i.e., $\Lambda_3 \le \Lambda_4$. Hence the exponent

$$\lambda_{s+r} = \Lambda_4 = 2(s+r)d - K_0 + \Delta_s(1-\phi_1) + r(k\phi_1 - 1)$$

is admissible. On recalling that $\phi_1 = \theta_{s+r}$, the theorem follows by induction. □

Lemma 84. *Let $j \ge 2$. Suppose that $\Delta_{s-r} < (k-1)(r+1)$ is an admissible exponent. Furthermore, suppose that $\Omega_1, \dots, \Omega_{j-1} \le f < g \le \Delta_{s-r}$. Set*

$$\omega = \begin{cases} 2f/g, & \text{if } j > 1 + \log_2(g/f);\\ 2^{1-j} + f/g, & \text{if } j \le 1 + \log_2(g/f).\end{cases}$$

Also suppose that $\phi(j,s,1)$ and Δ_s are defined as in Theorem 83. Let $\delta = \Delta_{s-r}/rk$ and $\delta_s = \Delta_s/rk$. Then

$$\phi(j,s,1) \le \frac{1+\omega\delta}{k(1+\delta)},$$

and

$$\delta_s < \delta\Big(1 - \frac{2-\omega}{k(1+\delta)}\Big).$$

Furthermore,

$$\delta_s + \log\delta_s < \delta + \log\delta - \frac{2-\omega}{k}.$$

Proof. On writing $\phi_J = \phi(j,s,I)$ $(1 \le J \le j)$ and $\delta' = (\Delta_{s-r} - f)/rk$, from Theorem 83 we have

$$\phi_{J-1} \le \frac{1}{2k} + \frac{1}{2}(1-\delta')\phi_J \qquad (2 \le J \le j).$$

Using a downward induction, we can find that

$$\phi_J \le \frac{1}{k(1+\delta')}\left(1 + \delta'\Big(\frac{1-\delta'}{2}\Big)^{j-J}\right) \qquad (1 \le J \le j).$$

In particular, we see that

$$\phi_1 \le \frac{1 + \delta' 2^{1-j}}{k(1+\delta')}. \tag{3.51}$$

Note that $\frac{1+\alpha x}{1+x}$ is a decreasing function of x whenever $\alpha < 1$. Since $\delta' > \delta(1 - f/g)$, it follows from (3.51) that

$$\phi_1 \le \frac{1 + \delta(1-f/g)2^{1-j}}{k\big(1+\delta(1-f/g)\big)} \le \frac{1 + \delta(2^{1-j} + f/g)}{k(1+\delta)}.$$

For $j > 1 + \log_2(g/f)$, we have $2^{1-j} + f/g < 2f/g$. Thus $\omega \ge 2^{1-j} + f/g$. Therefore

$$\phi(j,s,1) \le \frac{1+\omega\delta}{k(1+\delta)}.$$

Since

$$\delta_s = \delta(1-\theta_s) + (\theta_s - 1/k) \le (1-\delta)\phi_1 + \delta - 1/k,$$

we have

$$\begin{aligned}\delta_s &\le (1-\delta)\frac{1+\omega\delta}{k(1+\delta)} + \delta - \frac{1}{k} = \frac{(\omega-2)\delta - \omega\delta^2}{k(1+\delta)} + \delta \\ &< \frac{(\omega-2)\delta}{k(1+\delta)} + \delta = \delta\Big(1 - \frac{2-\omega}{k(1+\delta)}\Big).\end{aligned}$$

Thus

$$\begin{aligned}\delta_s + \log\delta_s &< \delta + \log\delta - \frac{(2-\omega)\delta}{k(1+\delta)} + \log\left(1 - \frac{2-\omega}{k(1+\delta)}\right) \\ &< \delta + \log\delta - \frac{(2-\omega)\delta}{k(1+\delta)} - \frac{2-\omega}{k(1+\delta)} \\ &= \delta + \log\delta - \frac{2-\omega}{k}.\end{aligned}$$

This completes the proof of the lemma. □

Proposition 85. *Let $j \geq 2$. Suppose that $\Omega_1, \ldots, \Omega_{j-1} \leq f < g \leq (k-1)(r+1)$. Let ω be defined as in Lemma 84 and let*

$$s_g = 3r + rk(2-\omega)^{-1}(1 - g/rk - \log(g/rk)).$$

If γ_s is the unique positive solution of the equation

$$\gamma_s + \log \gamma_s = 1 - \frac{(s-2r)(2-\omega)}{rk},$$

then $\Delta_s = rk\gamma_s$ is admissible whenever $2r < s \leq s_g$.

Proof. For $s \in \mathbb{N}$ with $2r < s \leq 3r$, $rk(1-1/k)$ is admissible because $\Delta_{2r} = rk(1-1/k)$ is admissible. Since $0 < s - 2r \leq r$, we have

$$\gamma_s + \log \gamma_s \geq 1 - r(2-\omega)/(rk) > 1 - 2/k > 1 - 1/k + \log(1-1/k),$$

Thus $\Delta_s = rk\gamma_s > rk(1-\frac{1}{k})$ and $\Delta_s = rk\gamma_s$ is admissible. When $3r < s \leq s_g$, assume that $\Delta_{s-r} = rk\gamma_{s-r}$ is admissible. Let $\delta = \min\{\gamma_{s-r}, (k-1)(r+1)/(rk)\}$. Then $\Delta^*_{s-r} = rk\delta$ is admissible. Since $s \leq s_g$ implies that

$$\gamma_{s-r} + \log \gamma_{s-r} = 1 - (s-3r)(2-\omega)/(rk) \geq g/(rk) + \log\big(g/(rk)\big),$$

we get $\Delta^*_{s-r} = rk\delta \geq g$. Let δ_s be defined as in Lemma 84. Since $\Delta^*_{s-r} = rk\delta \leq (k-1)(r+1)$ is admissible, by Theorem 83, $\Delta^*_s = rk\delta_s$ is admissible. By Lemma 84, we have

$$\delta + \log \delta - (2-\omega)/k > \delta_s + \log \delta_s. \tag{3.52}$$

Since

$$\gamma_s + \log \gamma_s = \gamma_{s-r} + \log \gamma_{s-r} - (2-\omega)/k \geq \delta + \log \delta - (2-\omega)/k,$$

it follows from (3.52) that

$$\gamma_s + \log \gamma_s \geq \delta_s + \log \delta_s,$$

and hence $\gamma_s \geq \delta_s$. Thus $\Delta_s = rk\gamma_s$ is admissible since $\Delta^*_s = rk\delta_s$ is admissible. □

Corollary 86. *Suppose that k is sufficiently large in terms of d. When $1 \leq s \leq s_g$,*

$$\Delta_s = rke^2 e^{-\frac{s(2-\omega)}{rk}}$$

is admissible.

Proof. Let γ_s be defined as in Proposition 85. For $2r < s \le s_g$, on noting that

$$\log \gamma_s < 1 + 2r(2-\omega)/(rk) - s(2-\omega)/(rk),$$

we have $\gamma_s < e^{2-s(2-\omega)/(rk)}$. Thus $\Delta_s = rke^2e^{-\frac{s(2-\omega)}{rk}}$ is admissible. For $0 < s \le 2r$, since

$$\Delta_s = rke^2e^{-\frac{s(2-\omega)}{rk}} > rke^{2-4/k} \ge rk,$$

it is admissible. This completes the proof of the corollary. □

Lemma 87. *Let $k < p$ and $s_0 = \frac{1}{2}rk(\log k - 2\log\log k)$. Suppose that k is sufficiently large. Then the exponents*

$$\Delta_s = \begin{cases} rke^3e^{-\frac{2s}{rk}} & 1 \le s \le s_0, \\ r(\log k)^2e^3e^{-\frac{s-s_0}{rk}} & s \ge s_0, \end{cases}$$

are admissible.

Proof. For a fixed j with $2 \le j \le k$, in order to bound $\Omega_J (1 \le J \le j-1)$ we need to choose some subsets of $\mathcal{R}_0'$ appropriately to approximate $K(\mathbf{\Psi}_J)$. Take $\tilde{\mathcal{R}}_J$ as in Lemma 81(2) and let $r_J = \operatorname{card}\tilde{\mathcal{R}}_J$ and $\tilde{K}_J = \sum_{\mathbf{i}\in\tilde{\mathcal{R}}_J} |\mathbf{i}|$. It follows from Lemma 81(2) that $K(\mathbf{\Psi}_J) \ge \tilde{K}_J$. By [15, Lemma 2.1], we have

$$\tilde{K}_J = \frac{dk+J}{d+1}\begin{pmatrix} k-J+d \\ d \end{pmatrix} - J.$$

On picking $j = [(\log k)^{1/3}]$, whenever $0 \le J < j$ for k sufficiently large, since $\mu_J \ge J$, we obtain

$$\Omega_J = K_0 - \tilde{K}_J - \mu_J \le \frac{dk}{d+1}\left(\begin{pmatrix} k+d \\ d \end{pmatrix} - \begin{pmatrix} k-j+d \\ d \end{pmatrix}\right) \le r(\log k)^{1/2}.$$

Let $f = r(\log k)^{1/2}$, $g = r(\log k)^2$, $\omega = 2f/g$ and $s_g = 3r + rk(2-\omega)^{-1}(1 - g/rk - \log(g/rk))$. For sufficiently large k, we have

$$1 + \log_2(g/f) = 1 + \log_2\big(\log k\big)^{\frac{3}{2}} < [(\log k)^{\frac{1}{3}}] = j.$$

By applying Lemma 85 and Corollary 86, the exponents

$$\Delta_s = rke^2e^{-\frac{s(2-\omega)}{rk}} \ (1 \le s \le s_g)$$

are admissible. Note that

$$\begin{aligned}
s_g &= 3r + rk(2-\omega)^{-1}(1 - g/rk - \log(g/rk)) \\
&= 3r + rk\Big(2 - 2(\log k)^{-\frac{3}{2}}\Big)^{-1}\Big(1 - (\log k)^2/k - \log\big((\log k)^2/k\big)\Big) \\
&> 3r + 2^{-1}rk\Big(1 + (\log k)^{-\frac{3}{2}}\Big)\Big(1 - (\log k)^2/k - 2\log\log k + \log k\Big) \\
&> 2^{-1}rk(\log k - 2\log\log k).
\end{aligned}$$

On letting $s_0 = 2^{-1}rk(\log k - 2\log\log k)$, we have $s_0 < s_g$ and

$$\frac{s_0\omega}{rk} = \big(\log k - 2\log\log k\big)(\log k)^{-\frac{3}{2}} < 1.$$

Thus the exponents

$$\Delta_s = rke^3e^{-\frac{2s}{rk}}\ (1 \le s \le s_0)$$

are admissible. Since $\Delta_{s_0} = rke^3e^{-\frac{2s_0}{rk}} = r(\log k)^2e^3$, it follows from Theorem 70 that

$$\Delta_s = \begin{cases} rke^3e^{-\frac{2s}{rk}} & 1 \le s \le s_0, \\ r(\log k)^2e^3e^{-\frac{s-s_0}{rk}} & s \ge s_0, \end{cases}$$

are admissible. The lemma follows. □

Theorem 88. *Let $k < p$. Whenever*

$$s > 2rk\Big(2^{-1}\log k + \log(r\iota) + \log\log k + \log\big(\log\big((2\iota-1)rk\log k\big) + 2k^{-1}\big) + 6 - \log\big(1-(\log k)^{-1}\big)\Big),$$

we have

$$\int_{\mathfrak{m}}\prod_{j=1}^{s} f_j(\boldsymbol{\alpha})d\boldsymbol{\alpha} \ll \hat{P}^{sd-\iota k-\delta}$$

for some $\delta > 0$.

Proof. By Theorem 87, on letting $s_0 = \frac{1}{2}rk(\log k - 2\log\log k)$, we have that

$$\Delta_s = \begin{cases} rke^3e^{-\frac{2s}{3rk}} & 1 \le s \le s_0, \\ r(\log k)^2e^3e^{-\frac{s-s_0}{rk}} & s \ge s_0, \end{cases}$$

are admissible. Now let $f(x) = Ce^{-E(x-s_0)} + 2x + 1$ with $C = \sigma^{-1}r(\log k)^2e^3$ and $E = \frac{1}{rk}$. By Lemma 74, whenever $s > \min\{f(x) \,|\, x \ge s_0\}$, we have

$$\int_{\mathfrak{m}}\prod_{j=1}^{s} f_j(\boldsymbol{\alpha})d\boldsymbol{\alpha} \ll \hat{P}^{sd-\iota k-\delta}$$

for some $\delta > 0$. By Lemma 75, $\min\{f(x) \,|\, x \geq s_0\} = 2E^{-1}\big(1 + \log(CE/2)\big) + 2s_0 + 1$. Note that

$$\log(CE/2) = \log \sigma^{-1} + 2 \log\log k - \log k + 3 - \log 2$$

and

$$\log \sigma^{-1} < \log(\iota rk) + \log\Big(\log\big((2\iota - 1)rk \log k\big) + 2k^{-1}\Big) + \log 4 - \log\big(1 - (\log k)^{-1}\big).$$

We have

$$\begin{aligned}
\min_{x \geq s_0} f(x) &= 2E^{-1}\big(1 + \log(CE/2)\big) + 1 + 2s_0 \\
&< 2rk\big(\log \sigma^{-1} + 2 \log\log k - \log k + 2^{-1} \log k - \log\log k + 4\big) \\
&< 2rk\Big(2^{-1} \log k + \log(r\iota) + \log\log k + \log\Big(\log\big((2\iota - 1)rk \log k\big) + 2k^{-1}\Big) \\
&\quad + 6 - \log\big(1 - (\log k)^{-1}\big)\Big).
\end{aligned}$$

This completes the proof of the lemma. □

Roughly speaking, comparing the lower bounds for s in Theorem 76 and Theorem 88, we achieve savings of the order of magnitude $rk \log k$ in the case when $k < p$ via repeated differencing process. Consider the case when $k > p$. On rewriting k as $a_0(k) + a_1(k)p + \cdots + a_D(k)p^D$, we have $D > 0$. It transpires that when $a_D(k)$ is sufficiently large, we may obtain savings of the order of magnitude $rk \log a_D(k)$ by following similar arguments to Theorem 88.

Chapter 4

The proofs of Theorems 1 and 2

4.1 The proof of Theorem 1

Theorem 1. *Let p be the characteristic of $\mathbb{F}_q$. Suppose that $p \nmid k$ and $k \geq d+2$. Further suppose that the system (1.6) has a non-singular solution in the completion of $\mathbb{F}_q(t)$ at ∞ and a non-singular solution in the completion $\mathbb{F}_q(t)_w$ of $\mathbb{F}_q(t)$ at every irreducible element w in $\mathbb{F}_q[t]$. Let $\iota = \operatorname{card}\mathcal{L}$ and $r = \operatorname{card}\mathcal{R}_0'$. Whenever*

$$s \geq 2rk\Big(\log(\iota rk) + \log\big(\log\big((2\iota-1)rk\log k\big) + 2k^{-1}\big) + 3 + \log 4 - \log\big(1-(\log k)^{-1}\big)\Big),$$

there is a positive constant $C = C(s,k,d;q;c_1,\dots,c_s)$ such that

$$N_{s,k,d}(P) = C\big(q^P\big)^{sd-\iota k} + O\Big(\big(q^P\big)^{sd-\iota k-\delta}\Big),$$

where

$$\delta = \min\left\{\frac{1}{18k\iota}, \frac{1-(\log k)^{-1}}{4\iota rk(\log((2\iota-1)rk\log k) + 2k^{-1})}\right\}.$$

Proof. It follows from Theorem 76 that

$$\int_{\mathfrak{m}} \prod_{j=1}^{s} f_j(\boldsymbol{\alpha}) d\boldsymbol{\alpha} = O\big(\hat{P}^{sd-\iota k-\delta}\big).$$

Moreover, by applying Theorem 59, we have

$$\int_{\mathfrak{M}} \prod_{j=1}^{s} f_j(\boldsymbol{\alpha}) d\boldsymbol{\alpha} = C\hat{P}^{sd-\iota k} + O\big(\hat{P}^{sd-\iota k-\delta}\big),$$

where $C = C(q,k,d,s) > 0$. Since

$$N_{s,k,d}(P) = \int_{\mathbb{T}^\iota} \prod_{j=1}^{s} f_j(\boldsymbol{\alpha}) d\boldsymbol{\alpha} = \int_{\mathfrak{M}} \prod_{j=1}^{s} f_j(\boldsymbol{\alpha}) d\boldsymbol{\alpha} + \int_{\mathfrak{m}} \prod_{j=1}^{s} f_j(\boldsymbol{\alpha}) d\boldsymbol{\alpha},$$

the result follows. □

It is worth a remark that when $k < p$, by applying Theorem 88, Theorem 1 holds whenever

$$s \geq \big(1 + o(1)\big) rk\big(\log k + 2\log(r\iota)\big),$$

as $k \to \infty$.

4.2 The proof of Theorem 2

Recall that the height of a vector $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{A}^n$ is defined to be

$$H(\mathbf{x}) = \frac{\max_{1 \leq i \leq n} \langle x_i \rangle}{\langle \gcd(x_1, \ldots, x_n) \rangle}.$$

For a subspace $V \subseteq \mathbb{F}_q(t)^s$ with basis vectors $\mathbf{x}_1, \ldots, \mathbf{x}_d \in \mathbb{A}^s$, define

$$H(V) = H(\mathbf{x}_1 \wedge \cdots \wedge \mathbf{x}_d).$$

Let $N^*_{s,k,d}(P)$ denote the number of solutions of (1.6) for which the vectors $\mathbf{x}_1, \ldots, \mathbf{x}_d$ are linearly independent and counted by $N_{s,k,d}(P)$. Let $\mathcal{N}_{s,k,d}(P)$ denote the number of distinct linear spaces V of dimension d and height at most $\hat{P}$, lying on the hypersurface (1.5).

Lemma 89. *Let $Q \in \mathbb{R}$ with $Q > 0$. For a subspace $V \subseteq \mathbb{F}_q(t)^s$ of dimension d, define $\beta_Q(V)$ to be the number of bases for V with all basis vectors lying in I^s_Q. Then*

$$\beta_Q(V) < \hat{Q}^{d^2}.$$

Proof. Fix a polynomial basis $\mathbf{x}_1, \ldots, \mathbf{x}_d$ for V. Without loss of generality, assume that the matrix $\big(x_{i,j}\big) = \big(x_{i,j}\big)_{1 \leq i,j \leq d}$ consisting of the first d rows of the matrix $X = (\mathbf{x}_1, \ldots, \mathbf{x}_d)$ is non-singular. For another polynomial basis $\mathbf{y}_1, \ldots, \mathbf{y}_d$, there exists a $d \times d$ matrix B such that $Y = (\mathbf{y}_1, \ldots, \mathbf{y}_d) = XB$. Thus B is uniquely determined by $\big(y_{i,j}\big)_{1 \leq i,j \leq d}$. Hence the number of choices for B is less than $\hat{Q}^{d^2}$. □

Lemma 90. *Let $\beta_Q(V)$ be defined as in Lemma 89. If $\hat{Q} = (\hat{P})^{1/d}$, then we have*

$$N^*_{s,k,d}(Q) \le \sum_{H(V)\le \hat{P}} \beta_Q(V) \le \Big(\max_V \beta_Q(V)\Big)\mathcal{N}_{s,k,d}(P).$$

Proof. Suppose that $\mathbf{x}_1, \dots, \mathbf{x}_d \in I_Q^s$ are linearly independent. Let $V = \mathrm{Span}\{\mathbf{x}_1, \dots, \mathbf{x}_d\}$. Since

$$H(V) = H(\mathbf{x}_1 \wedge \cdots \wedge \mathbf{x}_d) \le \hat{Q}^d = \hat{P},$$

the results follows immediately. □

We are now in a position to prove Theorem 2.

Theorem 2. *Under the same conditions as the ones in Theorem 1, there are two positive constants $C_1 = C_1(s,k,d;q;c_1,\dots,c_s) > 0$ and $C_2 = C_2(s,k,d;q;c_1,\dots,c_s) > 0$ such that*

$$\mathcal{N}_{s,k,d}(P) \ge C_1\big(q^P\big)^{s-\frac{k\iota}{d}-d} - C_2\big(q^P\big)^{s-\frac{k\iota}{d}-d-\frac{\delta}{d}},$$

where δ is defined as in Theorem 1.

Proof. Let $\hat{Q} = (\hat{P})^{1/d}$. By combining Lemma 89 with Lemma 90, we have

$$\mathcal{N}_{s,k,d}(P) \ge N^*_{s,k,d}(Q)\hat{Q}^{-d^2}.$$

Let w be an irreducible polynomial in $\mathbb{A}$ with $\deg w = [Q]+1$. If $\mathbf{x}_1, \dots, \mathbf{x}_d \in I_Q^s$ are linearly dependent over $\mathbb{F}_q(t)$, then they must be linearly dependent modulo w. Thus, there exist $a_1, \dots, a_d \pmod w$, not all zero, such that $a_1\mathbf{x}_1 + \cdots + a_d\mathbf{x}_d \equiv \mathbf{0} \pmod w$. The number of choices for the coefficients $a_1, \dots, a_d$ is $O\big(\langle w\rangle^{d-1}\big)$, since one of them may be normalized to be 1. For each fixed choice of $a_1, \dots, a_d$, the number of vectors $\mathbf{x}_1, \dots, \mathbf{x}_d \pmod w$ such that $a_1\mathbf{x}_1 + \cdots + a_d\mathbf{x}_d \equiv \mathbf{0} \pmod w$ is $O\big(\langle w\rangle^{s(d-1)}\big)$. Thus the number of linearly dependent vectors $\mathbf{x}_1, \dots, \mathbf{x}_d \pmod w$ is $O\big(\langle w\rangle^{sd-s+d-1}\big)$. Hence the number of dependent vectors $\mathbf{x}_1, \dots, \mathbf{x}_d \in I_Q^s$ is

$$O\big(\langle w\rangle^{sd-s+d-1}\big) = O\big(\hat{Q}^{sd-s+d-1}\big) = O(\hat{Q}^{sd-\iota k-2}).$$

By Theorem 1, there exist $C_1 = C_1(s,k,d,q) > 0$ and $C_2 = C_2(s,k,d,q) > 0$ such that

$$N^*_{s,k,d}(Q) \ge C_1\hat{Q}^{sd-\iota k} - C_2\big(\hat{Q}^{sd-\iota k-\delta}\big).$$

Therefore,

$$\begin{aligned}\mathcal{N}_{s,k,d}(P) &\geq N^*_{s,k,d}(Q)\hat{Q}^{-d^2} \\ &\geq C_1\hat{Q}^{sd-\iota k-d^2} - C_2\hat{Q}^{sd-\iota k-d^2-\delta} \\ &= C_1\hat{P}^{s-\frac{\iota k}{d}-d} - C_2\hat{P}^{s-\frac{\iota k}{d}-d-\frac{\delta}{d}}.\end{aligned}$$

This completes the proof of the theorem. □

4.3 Future work about the circle method in $\mathbb{F}_q[t]$

In Theorem 1, we obtain a lower bound for s such that $N_{s,k,d}(P)$ is of magnitude $\hat{P}^{sd-\iota k}$. A future research project is to largely reduce the lower bound for s by applying another variant of the circle method. Recently, Parsell [16] studied an integer analogue of this question and achieved impressive results. Motivated by his work, we may investigate mean values of exponential sums over the polynomials having only small degree irreducible divisors, called smooth polynomials. Such estimates are essential to the savings on s. Furthermore, we may generalize our results to general function fields. In particular, we could study Waring's Problem and Vinogradov's mean value theorem for finite extensions of $\mathbb{F}_q(t)$.

Another direction that we may pursue is to consider the polynomial analogues of Roth's theorem on progressions. For $N \in \mathbb{N} \setminus \{0\}$, let $D_3([1,N])$ denote the maximal cardinality of an integer set $A \subseteq [1,N]$ containing no 3-term arithmetic progression. In [17], Roth established a variant of the circle method and showed that $D_3([1,N]) \ll N/\log\log N$. Since his fundamental work, further refinements have been achieved by Heath-Brown [8], Szemerédi [19], and Bourgain [3]. Therefore, it is interesting to find new variants of the circle method to analyze the similar questions in function fields.

Bibliography

[1] G. I. Arkhipov, A. A. Karatsuba, and V. N. Chubarikov, *Multiple trigonometric sums*, Trudy Mat. Inst. Steklov 151 (1980) 1-126.

[2] B. J. Birch, *Homogeneous forms of odd degree in a large number of invaribles*, Mathematika 4 (1957) 102-105.

[3] J. Bourgain, *Roth's theorem on progressions revisited*, J. Anal. Math. 104 (2008) 155-192.

[4] R. Brauer, *A note on systems of homogeneous algebraic equations*, Bull. Amer. Math. Soc. 51 (1945) 749-755.

[5] H. Davenport and D.J. Lewis, *Homogeneous additive equations*, Proc. Roy. Soc. Ser. A 274 (1963) 443-460.

[6] K. B. Ford, *New estimates for mean values of Weyl sums*, Internat. Math. Res. Notices. (1995) 155-171.

[7] M. J. Greenberg, *Lectures on forms in many variables*, New York-Amsterdam 1969.

[8] D. R. Heath-Brown, *Integer sets containing no arithmetic progressions*, J. London Math. Soc. 35 (1987) 385-394.

[9] C.-N. Hsu, *A large sieve inequality for rational function fields*, J. Number Theory 58 (1996) 267-287.

[10] R. M. Kubota, Waring's problem for $\mathbb{F}_q[x]$, Ph. D. Thesis, University of Michigan, Ann Arbor, 1971.

[11] Y.-R. Liu and T. D. Wooley, *Waring's problem in function fields*, to appear in J. Reine Angew. Math.

[12] Y.-R. Liu and T. D. Wooley, *Vinagradov's mean value theorem in function fields*, preprint.

[13] S. T. Parsell, *The density of rational lines on cubic hypersurfaces*, Trans. Amer. Math. Soc. 352 (2000) 5045-5062.

[14] S. T. Parsell, *Mutiple exponential sums over smooth numbers*, J. Reine Angew. Math. 532 (2001) 47-104.

[15] S. T. Parsell, *A generalization of Vinogradov's mean value theorem*, Proc. London Math. Soc. (3) 91 (2005) 1-32.

[16] S. T. Parsell, *Asymptotic estimates for rational linear spaces on hypersurfaces*, Trans. Amer. Math. Soc. 361 (2009) 2929-2957.

[17] K. F. Roth, *On certain sets of integers*, J. London Math. Soc. 28 (1953) 104-109.

[18] H. L. Royden, *Real analysis (Third Edition)*, New York : Macmillan 1998.

[19] E. Szemerédi, *Integer sets containing no arithmetic progressions*, Acta Math. Hungar. 56 (1990) 155-158.

[20] I. M. Vinogradov, *Trigonometrical sums in number theory*, rev. ed., "Nauka", Moscow, 1971; English transl., Statist. Publ. Soc., Calcutta 1975.

[21] T. D. Wooley, *Large improvements in Waring's problem*, Ann. of Math. (2) 135 (1992) 131-164.

[22] T. D. Wooley, *On Vinogradov's mean value theorem*, Mathematika 39 (1992) 379-399.

Index

$\mathbb{N}$	the set of nonnegative integers $0, 1, 2, \ldots$
$\mathbb{Z}$	the set of integers $0, \pm 1, \pm 2, \ldots$
$\mathbb{Q}$	the set of rational numbers
$\mathbb{R}$	the set of real numbers
$\mathbb{C}$	the set of complex numbers
$\mathbb{F}_q$	the finite field of q elements
p	the characteristic of $\mathbb{F}_q$
$\mathbb{A} = \mathbb{F}_q[t]$	the ring of polynomials over $\mathbb{F}_q$
$\mathbf{c}$	$c_1, \ldots, c_s \in \mathbb{F}_q[t] \setminus \{0\}$
$\mathbb{F}_q(t)$	the fraction field of $\mathbb{F}_q[t]$
$\mathbb{K}_\infty = \mathbb{F}_q((1/t))$	the field of formal power series in terms of $1/t$ over $\mathbb{F}_q$
$\alpha \in \mathbb{K}_\infty$	$\alpha = \sum_{i \le n} a_i t^i$ with $a_i \in \mathbb{F}_q$ and $n \in \mathbb{Z}$
$\|\alpha\|$	$\|\alpha\| = \sum_{i<0} a_i t^i$ if $\alpha = \sum_{i \le n} a_i t^i$
$\operatorname{ord} \alpha$	the integer n if $\alpha = \sum_{i \le n} a_i t^i$ and $a_n \neq 0$
$\langle \alpha \rangle$	$q^{\operatorname{ord} \alpha}$
$\hat{P}$	q^P
$\mathbb{T}$	the set of elements $\alpha \in \mathbb{K}_\infty$ with $\operatorname{ord} \alpha < 0$
$e_q : \mathbb{F}_q \to \mathbb{C}$	a character of $\mathbb{F}_q$ (page 7)
$e : \mathbb{K}_\infty \to \mathbb{C}$	an exponential function (pages 7, 10)

$\mathfrak{M}$	the major arc (page 8)
$\mathfrak{m}$	the minor arc (page 8)
$\mathfrak{S}_{s,d,k}$	singular series (page 37)
$\mathfrak{J}_{s,d,k}$	singular integral (page 52)
J_m	the set of elements $\alpha \in \mathbb{K}_\infty$ with $\operatorname{ord}\alpha \le m$
I_P	the set of polynomials in $\mathbb{F}_q[t]$ of degree $< P$
$N_{s,k,d}(P)$	the number of solutions of the system (1.6) in I_P^{sd}
$J_{s,k,d}(P)$	the number of solutions of the system (3.13) in I_P^{sd}
$I_{m,k,d}(P)$	the number of solutions of the system (3.22) in I_P^{md}
$\mathbf{i}$	$(i_1, \dots, i_d)$
$\lvert\mathbf{i}\rvert$	$i_1 + \cdots + i_d$
$\mathbf{x}^{\mathbf{i}}$	$x_1^{i_1} \cdots x_d^{i_d}$
$\mathcal{R}_{\mathbf{i}}, \mathcal{R}_j, \mathcal{R}'_j, \mathcal{R}''_j$	certain sets of d-tuples (pages 11, 71)
$\mathcal{L}$	a set of d-tuples (pages 4, 72)
ι	the cardinality of the set $\mathcal{L}$ (pages 4, 72)
r	the cardinality of the set $\mathcal{R}'_0$ (pages 5, 71, 87)
r_0	the cardinality of the set $\mathcal{R}_0$
K_0	$\sum_{\mathbf{i}\in\mathcal{R}'_0} \lvert\mathbf{i}\rvert$
$F(\boldsymbol{\alpha}, \mathbf{x})$	$\sum_{\mathbf{i}\in\mathcal{L}} \alpha_{\mathbf{i}}\mathbf{x}^{\mathbf{i}}$
$G(\boldsymbol{\alpha}, \mathbf{x})$	$c_1F(\boldsymbol{\alpha}, \mathbf{x}_1) + \cdots + c_sF(\boldsymbol{\alpha}, \mathbf{x}_s)$
$f_j(\boldsymbol{\alpha}) = f_j(\boldsymbol{\alpha}; P)$	$\sum_{\mathbf{x}\in I_P^d} e\big(c_jF(\boldsymbol{\alpha}, \mathbf{x})\big)$
$f(\boldsymbol{\alpha}; P)$	$\sum_{\mathbf{x}\in I_P^d} e\Big(\sum_{\mathbf{i}\in\mathcal{R}_0} \alpha_{\mathbf{i}}\mathbf{x}^{\mathbf{i}}\Big)$
$\tilde{f}(\boldsymbol{\alpha}; P)$	$\sum_{\mathbf{x}\in I_P^d} e\Big(\sum_{\mathbf{i}\in\mathcal{R}'_0} \alpha_{\mathbf{i}}\mathbf{x}^{\mathbf{i}}\Big)$
I_{-P}	the set of elements in $\mathbb{K}_\infty$ of the shape $\sum_{-P<i\le 0} a_it^i$
$T_P(F; \boldsymbol{\alpha})$	$\sum_{\mathbf{x}\in I_{-P}^d} e\big(F(\boldsymbol{\alpha}; \mathbf{x})\big)$

$S(g, \mathbf{a})$	$\sum_{\mathbf{x} \in I^d_{\operatorname{ord} g}} e\big(F(\mathbf{a}/g; \mathbf{x})\big)$ where $g \in \mathbb{A} \setminus \{0\}$ and $\mathbf{a} = (a_{\mathbf{i}})_{\mathbf{i} \in \mathcal{L}} \in \mathbb{A}^{\iota}$
$S_j(g, \mathbf{a})$	$S(g, c_j \mathbf{a})$
w	an irreducible polynomial in $\mathbb{F}_q[t]$
$\operatorname{rk} \operatorname{Jac}(\mathbf{f}; \mathbf{z}; w)$	the rank of the Jacobian matrix $\operatorname{Jac}(\mathbf{f}; \mathbf{z})$ over $\mathbb{A}/(w)$
$a_h(i)$	$i = \sum_{h \geq 0} a_h(i) p^h$ where $a_h(i) \in [0, p-1] \cap \mathbb{Z}$
$\gamma_q(i)$	$a_0(i) + a_1(i) + a_2(i) + \cdots$
$\operatorname{ind}(\cdot)$	see page 14
$\tau(\cdot)$	see pages 14, 22, 42, 55