ANALYTIC METHODS FOR DIOPHANTINE PROBLEMS

by

Craig Valere Spencer

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Mathematics)
in The University of Michigan
2008

Doctoral Committee:

Professor Trevor D. Wooley, University of Bristol, Co-Chair
Emeritus Professor Donald J. Lewis, Co-Chair
Professor Jeffrey C. Lagarias
Assistant Professor Vilma M. Mesa
Assistant Professor Djordje Milicevic

© Craig Valere Spencer 2008
All Rights Reserved

dedicated to Verna Kisling, Marie Spencer, and the memory of Lyle Kisling and Eldon Spencer

ACKNOWLEDGEMENTS

I would like to thank Trevor Wooley for his advice, help, funding, and patience. Without his guidance, this thesis would not have been possible, and I would have probably left Michigan after my second year. I consider myself very fortunate to have been able to learn how to use the circle method and pursue math research from Professor Wooley.

I would also like to thank Donald Lewis for stepping in during my last year of graduate school as my advisor. He provided me we wonderful guidance and support as I wrote this thesis and applied for jobs.

The material in Chapters III and IV of this thesis were written with Yu-Ru Liu. I would like to thank Professor Liu for working with me, giving me advice about research and jobs, and financing a visit to the University of Waterloo.

I would also like to thank all of my math instructors from the University of Wisconsin-Stout, the USA/Canada Mathcamp, Carleton College, and the University of Michigan. In particular, I have benefited greatly by studying under Jinho Baik, Brian Conrad, Stephen DeBacker, Tina Garrett, Jerome William Hoffman, Mark Krusemeyer, Jeffrey Lagarias, Djordje Milicevic, Hugh Montgomery, David Romano, and Kannan Soundararajan. In addition, discussions at conferences with Andrew Granville, Roger Heath-Brown, Henryk Iwaniec, Scott Parsell, Emmanuel Peyre, and Lynne Walling have helped me select directions for my research. I am also very grateful to Jeffrey Lagarias, Donald Lewis, Vilma Mesa, Djordje Milicevic, and

Trevor Wooley for serving on my committee. I would like to thank James Hirschfeld for providing a reference to [19] and Michael Lipnowski for finding an error in the original proof of Theorem 4.1.

I have been fortunate to have the encouragement of very understanding friends and family members. Dave Allen, Dave Anderson, Matt Bush, Suzy Dixon, Hualong Feng, Jasun Gong, Wendy Grus, Mark Iwen, Kelly Kinser, Ryan Kinser, Joel Lepak, Mike Lieberman, John Mackay, Jared Maruskin, Yogesh More, Kamilah Neighbors, Andrew Ostergaard, Feng Rong, Sourya Shrestha, Charlotte Spencer, James Spencer, Ryan Spencer, Suzanne Spencer, Ahmed Teleb, and Diane Vavrichek have put up with my complaining and helped cheer me up when I have been stuck on problems. I would also like to thank Jonathan Bober, Peng Gao, Leo Goldmakher, Hester Graves, Rizwan Khan, Greg McNulty, Matthew Smith, and Ben Weiss for creating an active learning environment at the University of Michigan for analytic number theory.

Lastly, I would like to thank my best friend, Stacey Doan. She has always been there for me, and I cannot imagine my life without her.

TABLE OF CONTENTS

CHAPTER I

Introduction

1.1 Background

A main theme in mathematics is the study of integer solutions to equations and inequalities. These questions are called Diophantine problems in honor of Diophantus of Alexandria's contributions to the subject in the third century. The study of such topics as the Fermat equation $x^n + y^n = z^n$ have spanned centuries, beginning with the study of Pythagorean triples and concluding with the recent work of Taylor and Wiles (see [41] and [46]). Once thought of as strictly an area of pure mathematics, Diophantine problems currently lie at the very center of applied fields such as cryptography and coding theory.

One of the main tools for counting integer solutions to equations and inequalities is the circle method. Stemming from work of Hardy and Littlewood in the 1920's (see [16]), the circle method serves as an interface between Diophantine problems and harmonic analysis. Namely, detector functions from Fourier analysis can be used to count integer solutions to Diophantine equations and inequalities. This thesis explores various themes in number theory through the use of the circle method.

It should be noted that Chapters III and IV cover work completed with Yu-Ru Liu. Furthermore, the material in Chapters II, III, IV, and V include work from [37],

[26], [25], and [36], respectively.

1.2 Notation

Although some notation changes from chapter to chapter, we now fix certain notation which is used throughout the whole thesis. Let $f(x)$ and $g(x)$ be real-valued functions of x, and suppose that $g(x)$ only takes on positive values. If there exists a constant $c > 0$ such that $|f(x)| \leq cg(x)$ for all x, we write $f(x) \ll g(x)$ or $f(x) = O(g(x))$. If $\lim_{x\to\infty} f(x)/g(x) = 0$, we say that $f(x) = o\big(g(x)\big)$. If $\lim_{x\to\infty} f(x)/g(x)$ approaches a positive constant, then $f(x) \sim g(x)$. If $f(x)$ is a positive-valued function and $f(x) \ll g(x)$, we may also write $g(x) \gg f(x)$. Lastly, whenever ϵ appears in a statement, we are asserting that the statement holds for any $\epsilon > 0$.

1.3 Diophantine Inequalities

In 1929, Oppenheim (see [31]) stated a weaker version of the following conjecture, which became known as the Oppenheim conjecture.

Conjecture 1.1. *Let $Q(x_1, \ldots, x_n)$ be a nondegenerate quadratic form. Suppose that $n \geq 3$, that $Q(\mathbf{x})$ takes on both positive and negative values, and that there does not exist a non-zero real number γ such that $\gamma Q(\mathbf{x})$ has only integral coefficients. Then, for any $\delta > 0$, there exists a non-trivial integral solution to the inequality $|Q(x_1, \ldots x_n)| < \delta$.*

This conjecture, which was eventually proved by Margulis in [29] via algebraic group theory and ergodic theory, motivated many number theorists to study Diophantine inequalities. In Chapters II, we study the solvability of diagonal Diophantine inequalities in function fields via the Davenport-Heilbronn method.

1.3.1 Diagonal Diophantine Inequalities in Function Fields

Over 60 years ago, the Davenport-Heilbronn method (see [8]) was introduced to study non-trivial integral solutions of diagonal quadratic inequalities. Let k and s be positive integers with $k > 1$, and let δ be some fixed positive real number. Suppose that $\lambda_1, \dots, \lambda_s$ are non-zero real numbers, not all in rational ratio. Let $N_0(P, \boldsymbol{\lambda})$ denote the number of solutions $\mathbf{x} \in [-P, P]^s \cap \mathbb{Z}^s$ that satisfy

$$|\lambda_1 x_1^k + \cdots + \lambda_s x_s^k| < \delta.$$

Plainly, in the case that k is an even number, we must impose the restriction that the numbers λ_i do not all share the same sign in order to guarantee the existence of a non-trivial solution of $\lambda_1 z_1^k + \cdots + \lambda_s z_s^k = 0$ in $\mathbb{R}^s$. Davenport and Heilbronn proved in [8] that if $s > 2^k$, then $N_0(P_n, \boldsymbol{\lambda}) \gg P_n^{s-k}$ for a sequence $(P_n)_{n=1}^{\infty}$ which increases to infinity. This sequence is determined from the convergents of the continued fraction expansion for an irrational number of the form λ_i/λ_j, and as a result, the sequence $(P_n)_{n=1}^{\infty}$ may be arbitrarily sparse. In the last decade, the Bentkus-Götze-Freeman version of the Davenport-Heilbronn method (see [3], [10], [11], and [47]) has been used to establish an asymptotic formula for $N_0(P, \boldsymbol{\lambda})$, valid for all large enough values of P, provided that

$$s \geq k^2(\log k + \log\log k + O(1)),$$

and an asymptotic lower bound for $N_0(P, \boldsymbol{\lambda})$, valid for all large enough values of P, provided that

$$s \geq k(\log k + \log\log k + 2 + o(1)).$$

In Chapter II, we use the Bentkus-Götze-Freeman version of the Davenport-Heilbronn method to study the analogous problem in function fields.

In order to state our main result, it is first necessary to record some notation. Let $\mathbb{A} = \mathbb{F}_q[t]$ denote the ring of polynomials over $\mathbb{F}_q$, the finite field of q elements. Let $\mathbb{K}_\infty = \mathbb{F}_q((1/t))$ be the completion of $\mathbb{K} = \mathbb{F}_q(t)$ at the infinite place. In Chapter II, we wish to exploit the basic observation that $\mathbb{A}$ behaves like $\mathbb{Z}$, that $\mathbb{K}$ behaves like $\mathbb{Q}$, and that $\mathbb{K}_\infty$ behaves like $\mathbb{R}$.

Let k and s be positive integers with $k > 1$. Let p denote the characteristic of $\mathbb{F}_q$. Each non-zero element α in $\mathbb{K}_\infty$ can be written as $\alpha = \sum_{i \le n} a_i t^i$, where each a_i is an element in $\mathbb{F}_q$ and $a_n \neq 0$. We define $\operatorname{ord} \alpha$ to be n and $\operatorname{lead}(\alpha)$ to be a_n in this situation. Furthermore, we define $\operatorname{res} \alpha$ to be the coefficient of t^{-1} in such an expansion, and we adopt the conventions that $\operatorname{ord} 0 = -\infty$ and $\operatorname{lead}(0) = 0$. There exists a natural non-Archimedean valuation $\langle x \rangle = q^{\operatorname{ord} x}$ on $\mathbb{K}_\infty$. For any real number u, we let $\widehat{u}$ denote q^u. For a positive number x, we let $\operatorname{Log} x = \max(1, \log x)$. When k has a base-p expansion $k = a_0 + a_1 p + \cdots + a_n p^n$ with $0 \le a_i \le p-1$ $(0 \le i \le n)$, we define $\gamma(k) = \gamma_q(k)$ by

$$\gamma(k) = a_0 + a_1 + \cdots + a_n.$$

Define the constant $B = B_q(k)$ by

$$B_q(k) = \begin{cases} 1, & \text{when } k \le 2^{\gamma-2}, \\ (1 - 2^{-\gamma(k)})^{-1}, & \text{when } k > 2^{\gamma-2}. \end{cases}$$

Let

$$s_{q,k} = Bk(\operatorname{Log} k + \operatorname{Log}\operatorname{Log} k + 2 + B \operatorname{Log}\operatorname{Log} k / \operatorname{Log} k).$$

We are now in a position to state the main result from Chapter II.

Theorem 1.2. *There exists a positive absolute constant C with the following property. Suppose that k and s are natural numbers with*

$$s \ge s_{q,k} + Ck\sqrt{\operatorname{Log}\operatorname{Log} k}/\operatorname{Log} k$$

and $\mathrm{char}(\mathbb{F}_q) \nmid k$. *For* $z \in \mathbb{F}_q((1/t))$ *and* $u \in \mathbb{R}$, *let* $\langle z \rangle = q^{\mathrm{ord}\, z}$ *and* $\widehat{u} = q^u$. *Let* τ *be some fixed integer, and let* $\lambda_1, \dots, \lambda_s$ *be fixed non-zero elements of* $\mathbb{K}_\infty$, *not all in* $\mathbb{F}_q(t)$*-rational ratio. Suppose also that the equation*

$$\lambda_1 z_1^k + \cdots + \lambda_s z_s^k = 0$$

has a non-trivial solution $\mathbf{z}$ *in* $\mathbb{K}_\infty^s$. *Then, for all sufficiently large positive real numbers* P, *the number of* $\mathbb{F}_q[t]$*-solutions* $N(P; \boldsymbol{\lambda})$ *of*

$$\langle \lambda_1 x_1^k + \cdots + \lambda_s x_s^k \rangle < \widehat{\tau}, \tag{1.1}$$

with $\langle x_i \rangle \le \widehat{P}$ $(1 \le i \le s)$, *satisfies*

$$N(P, \boldsymbol{\lambda}) \gg \widehat{P}^{s-k}.$$

Here, the implicit constant depends on $\boldsymbol{\lambda}, \tau, k, s,$ *and* q.

A few comments about the above theorem are in order. If $p \nmid k$, then $\gamma_q(k) \ge 2$, and it follows that $B_q(k)$ satisfies $1 \le B_q(k) \le 4/3$. Also, one should note that our function $s_{q,k}$ corresponds to the quantity $\widehat{G}_q(k)$ defined in [28] in the context of Waring's problem in function fields, and our work depends on mean value estimates arising from the use of efficient differencing technology for the latter problem. By incorporating any improvements to this machinery into the arguments of Chapter II, one would be able to get comparable improvements in Theorem 1.2. In the case that $k < \mathrm{char}(\mathbb{F}_q)$, a combination of Proposition 13 of [23], the amplification method discussed in Section 1 of [47], and the ideas in Chapter II would give a result similar to Theorem 1.2 with $s \ge 2^k + 1$. This bound would be stronger than that of Theorem 1.2 for small values of k. Also, by Lemma 2.12, the equation $\lambda_1 z_1^k + \cdots + \lambda_s z_s^k = 0$ has a non-trivial solution $\mathbf{z} \in \mathbb{K}_\infty^s$ whenever $s \ge k^2 + 1$, whenever $q > k^4$ and $s \ge 2k + 1$, or whenever $(k, q-1) = 1$ and $s \ge k + 1$. Lastly, it's worth noting that the question

of finding solutions to (1.1), where each x_i is a monic, irreducible polynomial in $\mathbb{F}_q[t]$, has already been studied by Hsu in [20] through the use of the Davenport-Heilbronn method. Hsu's paper was restricted to the case that $k < p$ and

$$s \geq \begin{cases} 2^k + 1, & \text{when } 2 \leq k < 11, \\ 2[2k^2 \log k + k^2 \log\log k + 2k^2 - 2k] + 1, & \text{when } k \geq 11. \end{cases}$$

1.3.2 Diophantine Inequalities and Quasi-Algebraically Closed Fields

The theory of quasi-algebraically closed fields originated with work of Tsen (see [43]) in 1933 and Lang (see [24]) in 1952, and historically, this theory has primarily been used to study questions concerning the solvability of Diophantine equations and of systems of Diophantine equations. It should be noted that the theory of quasi-algebraically closed fields also provides information about Diophantine inequalities in function fields.

For example, suppose that

$$G_1(\mathbf{x}), \ldots, G_h(\mathbf{x}) \in \Big(\mathbb{F}_q((1/t))\Big)[x_1, \ldots, x_s]$$

are forms of degree k in $s > hk^2$ variables, and let $M = \max_\lambda \operatorname{ord} \lambda$, where λ ranges over all of the coefficients of the h forms. Let

$$x_i = \sum_{j=0}^{R} a_{ij} t^j \qquad (1 \leq i \leq s).$$

For $l \in \{1, \ldots, h\}$, the coefficients of $t, t^2, \ldots, t^{kR+M}$ in $G_l(x_1, \ldots, x_s)$ that are not identically zero can be written as forms of degree k over $\mathbb{F}_q$ in variables (a_{ij}).

Thus, to find a non-trivial common solution to the system of inequalities

$$\operatorname{ord} G_l(x_1, \ldots, x_s) < 1 \qquad (1 \leq l \leq h), \tag{1.2}$$

it is enough to find a non-trivial solution (a_{ij}) to our system of at most $h(kR+M)$ forms over $\mathbb{F}_q$ of degree k in $s(R+1)$ variables. The theory of quasi-algebraically closed fields guarantees (see [24, Theorem 3]) the existence of such a solution whenever

$$s(R+1) > hk(kR+M). \tag{1.3}$$

Since $s > hk^2$, this inequality will be satisfied for large enough values of R, and hence, there exists a non-trivial solution $(x_1, \dots, x_s) \in \mathbb{F}_q[t]$ to our system of inequalities (1.2). In the case of a single quadratic form, this implies that only 5 variables are needed to guarantee a non-trivial solution. Furthermore, when $M > k$, our inequality (1.3) can be used to show that there exists a non-trivial solution $(x_1, \dots, x_s) \in \mathbb{F}_q[t]$ to our system of inequalities (1.2) with

$$\max_{1 \le i \le s} \operatorname{ord} x_i \le \frac{hk(M-k)}{s - hk^2}.$$

Generalizations and applications of this theme can be found in the author and Trevor Wooley's manuscript [38].

1.4 Additive Combinatorics

For $k \in \mathbb{N} = \{1, 2, \dots\}$, let $D_3([1,k])$ denote the maximal cardinality of an integer set $A \subseteq \{1, \dots, k\}$ containing no non-trivial 3-term arithmetic progression. In a fundamental paper [35], Roth proved that $D_3([1,k]) \ll k/\log\log k$ via an application of the circle method. His result was later improved by Heath-Brown (see [18]) and Szemerédi (see [40]) to $D_3([1,k]) \ll k/(\log k)^\alpha$ for some small positive constant $\alpha > 0$. Recently, Bourgain (see [4]) proved that $D_3([1,k]) \ll k(\log\log k)^{1/2}/(\log k)^{1/2}$, which provides the best bound currently known. During the last few years, Gowers has proved quantitative bounds for the more general question with n-term arithmetic

progressions (see [12] and [13]), and Green and Tao have also shown that there are arbitrarily long arithmetic progressions of prime numbers (see [14] and [15]).

A main theme in additive combinatorics is that sets are either *random* or *structured*. Suppose that $A \subseteq \{0, \dots, k\}$ has no non-trivial 3-term arithmetic progression. When using the circle method, the set A is random if it is well-distributed throughout residue classes for all small q, and A is structured if it is biased toward a particular residue class modulo a small number q. Note that (x_1, x_2, x_3) is a 3-term arithmetic progression if and only if $x_1 - 2x_2 + x_3 = 0$. The set A has $|A|$ trivial solutions to this equation of the form (a, a, a) and no non-trivial solutions.

When the set A is random, the circle method can be used to show that

$$\frac{|A|^3}{4k} \approx \#\{(x_1, x_2, x_3) \in A^3 \,:\, x_1 - 2x_2 + x_3 = 0\} = |A|.$$

If the set A is structured, then it is biased toward an arithmetic progression $\mathcal{P} = \{x \in \mathbb{Z} \,:\, x \equiv a \,(\mathrm{mod}\, q)\}$, where q is relatively small and $0 \leq a < q$. Suppose that $|\mathcal{P} \cap A| = (1+\delta)|A|/q$. Since

$$(qx_1 + a) - 2(qx_2 + a) + (qx_3 + a) = 0 \quad \Leftrightarrow \quad x_1 - 2x_2 + x_3 = 0,$$

we have a set $\{(x-a)/q \,:\, x \in \mathcal{P} \cap A\} \subseteq \{0, \dots, \lfloor k/q \rfloor\}$, which has no non-trivial 3-term arithmetic progressions and is denser in $\{0, \dots, \lfloor k/q \rfloor\}$ than A is in $\{0, \dots, k\}$ by roughly a factor of $(1+\delta)$.

In this thesis, we prove generalizations of Roth's theorem in both function fields and finite Abelian groups through the use of the circle method.

1.4.1 A Generalization of Roth's Theorem in Function Fields

Let $\mathbb{F}_q[t]$ denote the ring of polynomials over the finite field $\mathbb{F}_q$. For $N \in \mathbb{N}$, let $\mathcal{S}_N$ denote the subset of $\mathbb{F}_q[t]$ containing all polynomials of degree strictly less than

N. For an integer $s \geq 3$, let $\mathbf{r} = (r_1, \ldots, r_s)$ be a vector of non-zero elements of $\mathbb{F}_q$ satisfying $r_1 + \cdots + r_s = 0$. A solution $\mathbf{x} = (x_1, \ldots, x_s) \in \mathcal{S}_N^s$ of $r_1x_1 + \cdots + r_sx_s = 0$ is said to be *trivial* if $x_{j_1} = \cdots = x_{j_l}$ for some subset $\{j_1, \ldots, j_l\} \subseteq \{1, \ldots, s\}$ with $r_{j_1} + \cdots + r_{j_l} = 0$. Otherwise, we say a solution $\mathbf{x}$ is *non-trivial*. Let $D_{\mathbf{r}}(\mathcal{S}_N)$ denote the maximal cardinality of a set $A \subseteq \mathcal{S}_N$ which contains no non-trivial solution of $r_1x_1 + \cdots + r_sx_s = 0$ with $x_i \in A$ $(1 \leq i \leq s)$. In Chapter III, we prove the following theorem.

Theorem 1.3. *For $N \in \mathbb{N}$,*

$$D_{\mathbf{r}}(\mathcal{S}_N) \ll \frac{|\mathcal{S}_N|}{(\log_q |\mathcal{S}_N|)^{s-2}} = \frac{q^N}{N^{s-2}}.$$

Here, the implicit constant depends only on $\mathbf{r}$.

In the special case that $\mathbf{r}' = (1, -2, 1)$ and $\gcd(2, q) = 1$, the number $D_{\mathbf{r}'}(\mathcal{S}_N)$ denotes the maximal cardinality of a set $A \subseteq \mathcal{S}_N$ which contains no non-trivial 3-term arithmetic progression. As a direct consequence of Theorem 1.3, we have $D_{\mathbf{r}'}(\mathcal{S}_N) \ll |\mathcal{S}_N|/\log_q |\mathcal{S}_N|$. We note that this result is sharper than its integer analogue proved by Bourgain. Our improvement comes from being able to provide a better estimate for an exponential sum in $\mathbb{F}_q[t]$ than for the analogous exponential sum in $\mathbb{Z}$ (see Lemma 3.2). In addition, when $\mathbf{r}' = (1, -2, 1)$ and $\gcd(2, q) = 1$, by viewing $\mathcal{S}_N$ as a vector space over $\mathbb{F}_p$ of dimension MN, where $q = p^M$, one can also derive the above bound for $D_{\mathbf{r}'}(\mathcal{S}_N)$ from the result of Meshulam on finite Abelian groups in [30, Theorem 1.2]. However, for a general $\mathbf{r} = (r_1, \ldots, r_s)$, if $r_i \in \mathbb{F}_q \setminus \mathbb{F}_p$ for some $1 \leq i \leq s$, then Meshulam's method can not be extended to bound $D_{\mathbf{r}}(\mathcal{S}_N)$. In order to prove Theorem 1.3, we employ a variant of the Hardy-Littlewood circle method for $\mathbb{F}_q[t]$.

One can also obtain some information about irreducible polynomials from The-

orem 1.3. Let $\mathcal{P}_N$ denote the set of all monic irreducible polynomials in $\mathbb{F}_q[t]$ of degree strictly less than N, and let A_N denote a subset of $\mathcal{P}_N$. By the prime number theorem for $\mathbb{F}_q[t]$ (see [5, Theorem 2.2]), we have $|\mathcal{P}_N| \gg |\mathcal{S}_N|/\log_q |\mathcal{S}_N|$. For $s \geq 4$, Theorem 1.3 implies that for each $\mathbf{r}$, there exists a positive constant $c(\mathbf{r})$ such that whenever $|A_N| \geq c(\mathbf{r})|\mathcal{P}_N|/(\log_q |\mathcal{S}_N|)^{s-3}$, it follows that A_N contains a non-trivial solution of $r_1x_1 + \cdots + r_sx_s = 0$ with $x_i \in A_N$ $(1 \leq i \leq s)$.

1.4.2 A Generalization of Roth's Theorem in Finite Abelian Groups

For a natural number $s \geq 3$, let $\mathbf{r} = (r_1, \ldots, r_s)$ be a vector of non-zero integers satisfying $r_1 + \cdots + r_s = 0$. Given a finite Abelian group M, we can write

$$M \simeq \mathbb{Z}/k_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/k_n\mathbb{Z},$$

where $\mathbb{Z}/k_i\mathbb{Z}$ is a cyclic group $(1 \leq i \leq n)$ and $k_i | k_{i-1}$ $(2 \leq i \leq n)$. We denote by $c(M) = n$ the number of constituents $\mathbb{Z}/k_i\mathbb{Z}$ of M. Moreover, we say that M is *coprime to* $\mathbf{r}$ provided that $(r_i, k_1) = 1$ for all $1 \leq i \leq s$.

A solution $\mathbf{x} = (x_1, \ldots, x_s) \in M^s$ of $r_1x_1 + \cdots + r_sx_s = 0$ is said to be *trivial* if $x_{j_1} = \cdots = x_{j_l}$ for some subset $\{j_1, \ldots, j_l\} \subseteq \{1, \ldots, s\}$ with $r_{j_1} + \cdots + r_{j_l} = 0$. Otherwise, we say that a solution $\mathbf{x}$ is *non-trivial*. For a finite Abelian group M coprime to $\mathbf{r}$, let $D_{\mathbf{r}}(M)$ denote the maximal cardinality of a set $A \subseteq M$ which contains no non-trivial solution of $r_1x_1 + \cdots + r_sx_s = 0$ with $x_i \in A$ $(1 \leq i \leq s)$. Also, for $n \in \mathbb{N}$, we denote by $d_{\mathbf{r}}(n)$ the supremum of $D_{\mathbf{r}}(M)/|M|$ as M ranges over all finite Abelian groups M with $c(M) \geq n$ and M coprime to $\mathbf{r}$. In Chapter III, we prove the following theorem.

Theorem 1.4. *Let $\mathbf{r} = (r_1, \ldots, r_s)$ be a vector of non-zero integers satisfying $r_1 + \cdots + r_s = 0$. There exists an effectively computable constant $C(\mathbf{r}) > 0$ such that for*

$n \in \mathbb{N}$,

$$d_{\mathbf{r}}(n) \leq \frac{C(\mathbf{r})^{s-2}}{n^{s-2}}.$$

We note that in the special case that $\mathbf{r}' = (1, -2, 1)$ and G is a finite Abelian group of odd order, the number $D_{\mathbf{r}'}(G)$ denotes the maximal cardinality of a set $A \subseteq G$ which contains no non-trivial 3-term arithmetic progression. Moreover, the constant $C(\mathbf{r}')$ can be taken to be 2 in this case (see Remark 4.6). Hence, we can deduce the result of Meshulam in [30, Theorem 1.2] which states that if G is a finite Abelian group of odd order, then $D_{\mathbf{r}'}(G) \leq 2|G|/c(G)$.

In the following corollary, we provide an application of Theorem 1.4.

Corollary 1.5. *Let p be an odd prime and $q = p^h$ for some $h \in \mathbb{N}$. For $n \in \mathbb{N}$, let $PG(n, q)$ denote the projective space of dimension n over the finite field $\mathbb{F}_q$ of q elements. For $v \in \mathbb{N}$ with $v > 1$, let $\mathcal{M}_v(n, q)$ denote the maximum cardinality of a set $A \subseteq PG(n, q)$ for which no $(v + 1)$ points in A are linearly dependent over $\mathbb{F}_q$. Then, there exists an effectively computable constant $\tilde{C}(p, v) > 0$ such that*

$$\mathcal{M}_v(n, q) \leq \frac{\tilde{C}(p, v)}{h^{v-1}} \cdot \sum_{j=1}^{n} \frac{q^j}{j^{v-1}} + 1.$$

An m-cap is a set of m points of $PG(n, q)$ for which no three points are collinear. In the special case that $v = 2$, the quantity $\mathcal{M}_2(n, q)$ denotes the maximal value of m for which there exists an m-cap in $PG(n, q)$. For an odd prime p, we can take $\tilde{C}(p, 2) = 2$ (see Remark 4.6). Hence, Corollary 1.5 implies the result of Storme, Thas, and Vereecke in [39, Theorem 1.2] about the sizes of caps in finite projective spaces.

For $v \in \mathbb{N}$ with $v > 1$, let $\mathbf{M}_v(n, q)$ denote the maximum cardinality of a set $A \subseteq PG(n, q)$ for which no $(v + 1)$ points in A are linearly dependent over $\mathbb{F}_q$, and some $(v+2)$ points in A are linearly dependent over $\mathbb{F}_q$. In [19], Hirschfeld and Storme

provide a general discussion on $\mathbf{M}_v(n,q)$. We note that $\mathbf{M}_v(n,q) \leq \mathcal{M}_v(n,q)$. Hence, Corollary 1.5 gives a bound for $\mathbf{M}_v(n,q)$ which is useful when n is sufficiently large.

1.5 The Manin Conjecture

For a number field k, a fundamental problem in arithmetic geometry is to describe the set of k-rational points on a projective variety $X(k)$ in terms of its geometric invariants. Let $X(k)$ denote a Fano variety with anticanonical height function $H : X(k) \to \mathbb{R}$. For a suitably nice open subset $U \subseteq X$, the Manin conjecture states that

$$\#\{x \in U(k) \,:\, H(x) \leq B\} \sim aB(\log B)^{b-1},$$

where $a = a(X(k))$ is a constant and $b = b(X(k))$ is the rank of the Picard group of $X(k)$. Furthermore, Peyre provides an interpretation for the constant $a(X(k))$ in [32].

Although Batyrev and Tschinkel have found a counterexample (see [2]) to Manin's conjecture, many cases of the conjecture have been demonstrated through a variety of techniques. For example, Franke, Manin, and Tschinkel originally proved this conjecture for flag varieties (see [9]). In [1], Batyrev and Tschinkel verified that the Manin conjecture holds for toric varieties. De la Bretèche and Browning have also shown that the asymptotic holds for many cases of del Pezzo surfaces (see, for instance, [5] and [6]).

We consider the variety defined by $x_0y_0 + \cdots + x_sy_s = 0$ in $\mathbb{P}^s(\mathbb{Q}) \times \mathbb{P}^s(\mathbb{Q})$. This is a flag variety with anticanonical height function

$$H(\mathbf{x},\mathbf{y}) = \max_{0\leq i,j\leq s} |x_iy_j|^s,$$

where we choose representatives $\mathbf{x} = (x_0,\ldots,x_s) \in \mathbb{Z}^{s+1}$ and $\mathbf{y} = (y_0,\ldots,y_s) \in \mathbb{Z}^{s+1}$

with $\gcd(x_0, \dots, x_s) = \gcd(y_0, \dots, y_s) = 1$. Let

$$N(B) = \#\{(\mathbf{x}, \mathbf{y}) \in \mathbb{P}^s(\mathbb{Q}) \times \mathbb{P}^s(\mathbb{Q}) \, : \mathbf{x} \cdot \mathbf{y} = 0, \, x_0 \cdots x_s y_0 \cdots y_s \neq 0, \text{ and } H(\mathbf{x}, \mathbf{y}) < B\}.$$

For the variety $x_0 y_0 + \cdots + x_s y_s = 0$, the Manin conjecture predicts that $N(B) \sim \kappa B \log B$, where κ is a constant.

The general case of the Manin conjecture for flag varieties was first proved in [9] by Franke, Manin, and Tschinkel via deep results concerning the meromorphic continuation of Eisenstein series. The result has also been studied by Thunder, Peyre, and Robbiani in [42], [32], and [33], respectively. Thunder's approach employs the geometry of numbers and estimates for the number of lattice points in bounded domains. Robbiani uses a complicated variant of a new form of the circle method due to Heath-Brown (see [17]), and such an approach cannot be used for forms of degree greater than three due to limitations of the underlying method. Furthermore, Robbiani's proof requires that $s \geq 3$.

The purpose of Chapter V is to demonstrate that $N(B) \sim \kappa B \log B$ via a classical form of the circle method. The motivation for this new proof is to provide a method which has the potential of working in a more general setting. In Chapter V, we prove the following theorem.

Theorem 1.6. *For $s \geq 2$ and $B \geq 2$, we have*

$$N(B) = \left(\frac{s+1}{2s}\right) \zeta(s)^{-2} \left(\sum_{q=1}^{\infty} \frac{\phi(q)}{q^{s+1}}\right) \left(\int_{\mathcal{X}} d\mathbf{x} d\mathbf{y}\right) B \log B + O(B),$$

where

$$\mathcal{X} = \{(\mathbf{x}, \mathbf{y}) \in [-1, 1]^{2s} \, : \, |\mathbf{x} \cdot \mathbf{y}| \leq 1\}.$$

CHAPTER II

Diophantine Inequalities in Function Fields

2.1 Overview

In order to state our main result of this chapter, it is first necessary to record some notation. Let $\mathbb{A} = \mathbb{F}_q[t]$ denote the ring of polynomials over $\mathbb{F}_q$, the finite field of q elements. Let $\mathbb{K}_\infty = \mathbb{F}_q((1/t))$ be the completion of $\mathbb{K} = \mathbb{F}_q(t)$ at the infinite place.

Let k and s be positive integers with $k > 1$. Let p denote the characteristic of $\mathbb{F}_q$. Each non-zero element α in $\mathbb{K}_\infty$ can be written as $\alpha = \sum_{i \le n} a_i t^i$, where each a_i is an element in $\mathbb{F}_q$ and $a_n \neq 0$. We define $\operatorname{ord} \alpha$ to be n and $\operatorname{lead}(\alpha)$ to be a_n in this situation. Furthermore, we define $\operatorname{res} \alpha$ to be the coefficient of t^{-1} in such an expansion, and we adopt the convention that $\operatorname{ord} 0 = -\infty$. There exists a natural non-Archimedean valuation $\langle x \rangle = q^{\operatorname{ord} x}$ on $\mathbb{K}_\infty$. For any real number u, we let $\widehat{u}$ denote q^u. For a positive number x, we let $\operatorname{Log} x = \max(1, \log x)$. When k has a base-p expansion $k = a_0 + a_1 p + \cdots + a_n p^n$ with $0 \le a_i \le p - 1$ $(0 \le i \le n)$, we define $\gamma(k) = \gamma_q(k)$ by

$$\gamma(k) = a_0 + a_1 + \cdots + a_n.$$

Define the constant $B = B_q(k)$ by

$$B_q(k) = \begin{cases} 1, & \text{when } k \le 2^{\gamma-2}, \\ (1 - 2^{-\gamma(k)})^{-1}, & \text{when } k > 2^{\gamma-2}. \end{cases} \tag{2.1}$$

Let

$$s_{q,k} = Bk(\operatorname{Log} k + \operatorname{Log}\operatorname{Log} k + 2 + B \operatorname{Log}\operatorname{Log} k/ \operatorname{Log} k). \tag{2.2}$$

We are now in a position to state the main result of this chapter.

Theorem 2.1. *There exists a positive absolute constant C with the following property. Suppose that k and s are natural numbers with*

$$s \ge s_{q,k} + Ck\sqrt{\operatorname{Log}\operatorname{Log} k}/ \operatorname{Log} k$$

and $\operatorname{char}(\mathbb{F}_q) \nmid k$. *For $z \in \mathbb{F}_q((1/t))$ and $u \in \mathbb{R}$, let $\langle z \rangle = q^{\operatorname{ord} z}$ and $\widehat{u} = q^u$. Let τ be some fixed integer, and let $\lambda_1, \dots, \lambda_s$ be fixed non-zero elements of $\mathbb{K}_\infty$, not all in $\mathbb{F}_q(t)$-rational ratio. Suppose also that the equation*

$$\lambda_1 z_1^k + \cdots + \lambda_s z_s^k = 0 \tag{2.3}$$

has a non-trivial solution $\mathbf{z}$ in $\mathbb{K}_\infty^s$. Then, for all sufficiently large positive real numbers P, the number of $\mathbb{F}_q[t]$-solutions $N(P; \boldsymbol{\lambda})$ of

$$\langle \lambda_1 x_1^k + \cdots + \lambda_s x_s^k \rangle < \widehat{\tau}, \tag{2.4}$$

with $\langle x_i \rangle \le \widehat{P}$ $(1 \le i \le s)$, satisfies

$$N(P, \boldsymbol{\lambda}) \gg \widehat{P}^{s-k}.$$

Here, the implicit constant depends on $\boldsymbol{\lambda}, \tau, k, s$, and q.

This chapter is based on the author's submitted manuscript [37].

2.2 The Davenport-Heilbronn Method for Function Fields

In this section, we set up the Davenport-Heilbronn Method for function fields. We combine Hsu's version of the Davenport-Heilbronn method (see [20]) with the ideas of Bentkus and Götze (see [3]) and those of Freeman (see [10] and [11]) in order to prove Theorem 2.1.

Define a non-trivial additive character $e_q : \mathbb{F}_q \to \mathbb{C}^\times$ by $e_q(a) = e^{2\pi i \operatorname{tr}(a)/p}$, where $\operatorname{tr} : \mathbb{F}_q \to \mathbb{F}_p$ denotes the trace map. This character induces a map $e : \mathbb{K}_\infty \to \mathbb{C}^\times$ defined by $e(\alpha) = e_q(\operatorname{res}\alpha)$. Let $\mathbb{T}$ be the compact additive subgroup of $\mathbb{K}_\infty$ given by $\mathbb{T} = \{\alpha \in \mathbb{K}_\infty : \langle\alpha\rangle < 1\}$, and note that we may normalize a Haar measure $d\alpha$ on $\mathbb{K}_\infty$ so that $\int_{\mathbb{T}} d\alpha = 1$. By Lemma 2.2 of [20], for $\tau \in \mathbb{Z}$, if we define a function $\chi_\tau : \mathbb{K}_\infty \to \mathbb{R}$ by

$$\chi_\tau(\alpha) = \begin{cases} \widehat{\tau}, & \text{when } \langle\alpha\rangle < \widehat{\tau}^{-1}, \\ 0, & \text{when } \langle\alpha\rangle \geq \widehat{\tau}^{-1}, \end{cases} \tag{2.5}$$

we obtain a method of detecting when $\langle\beta\rangle < \widehat{\tau}$ for an element $\beta \in \mathbb{K}_\infty$ by noting that

$$\int_{\mathbb{K}_\infty} e(\alpha\beta)\chi_\tau(\alpha)\, d\alpha = \begin{cases} 1, & \text{when } \langle\beta\rangle < \widehat{\tau}, \\ 0, & \text{when } \langle\beta\rangle \geq \widehat{\tau}. \end{cases} \tag{2.6}$$

When R and P are positive numbers with $R \leq P$, we define the set of *R-smooth polynomials* $\mathcal{A}(P, R)$ to be the set of all $x \in \mathbb{A}$ satisfying both $\langle x\rangle \leq \widehat{P}$ and the property that whenever $\varpi | x$ for an irreducible polynomial ϖ, then $\langle\varpi\rangle < \widehat{R}$. We now can define our classical Weyl sum

$$F(\alpha) = F(\alpha; P) = \sum_{\langle x\rangle \leq \widehat{P}} e(\alpha x^k)$$

and our smooth Weyl sum

$$f(\alpha) = f(\alpha; P, R) = \sum_{x \in \mathcal{A}(P,R)} e(\alpha x^k).$$

Let $F_i(\alpha) = F(\lambda_i \alpha)$ for $1 \le i \le s$, and let $f_j(\alpha) = f(\lambda_j \alpha)$ for $3 \le j \le s$. It now follows from (2.6) that the integral

$$\int_{\mathbb{K}_\infty} F_1(\alpha) F_2(\alpha) f_3(\alpha) \cdots f_s(\alpha) \chi_\tau(\alpha)\, d\alpha \tag{2.7}$$

counts the number of solutions $\mathbf{x} \in \mathbb{A}^s$ of

$$\langle \lambda_1 x_1^k + \cdots + \lambda_s x_s^k \rangle < \widehat{\tau}$$

with $\langle x_i \rangle \le \widehat{P}$ $(i = 1, 2)$ and $x_j \in \mathcal{A}(P, R)$ $(3 \le j \le s)$. Thus, the integral in (2.7) serves as a lower bound for $N(P, \boldsymbol{\lambda})$. For the remainder of this chapter, whenever R appears in a statement, implicitly or explicitly, we are asserting that there exists a positive number $\eta_0 = \eta_0(s, u, v, q, k; \boldsymbol{\lambda})$ such that the statement holds whenever $R = \eta P$, where $0 < \eta \le \eta_0$.

Let $\mathfrak{n}$ denote the set of elements α of $\mathbb{T}$ satisfying the property that whenever a and g are elements of $\mathbb{A}$ such that $\langle g\alpha - a \rangle < \widehat{P}^{1-k}$ and $g \ne 0$, then $\langle g \rangle > \widehat{P}$. We say that a positive number $u > 2k - 2$ is *accessible to the exponent* k when there exists a positive number δ for which

$$\int_{\mathfrak{n}} |F(\alpha, P)^2 f(\alpha, P, R)^u|\, d\alpha \ll \widehat{P}^{u+2-k-\delta}.$$

By Lemma A.4, there exists a positive absolute constant C such that if

$$u + 5 \ge s_{q,k} + Ck\sqrt{\operatorname{Log}\operatorname{Log} k}/\operatorname{Log} k,$$

then u is accessible to the exponent k. Hence, Theorem 2.1 is a consequence of the following result.

Theorem 2.2. *Suppose that k and s are natural numbers with* $\mathrm{char}(\mathbb{F}_q) \nmid k$. *Furthermore, assume that $u > 2k-2$ is accessible to the exponent k and that $s \geq u+5$. For $z \in \mathbb{F}_q((1/t))$ and $u \in \mathbb{R}$, let $\langle z \rangle = q^{\mathrm{ord}\, z}$ and $\widehat{u} = q^u$. Let τ be some fixed integer, and let $\lambda_1, \dots, \lambda_s$ be fixed non-zero elements of $\mathbb{K}_\infty$, not all in $\mathbb{F}_q(t)$-rational ratio. Suppose also that the equation*

$$\lambda_1 z_1^k + \cdots + \lambda_s z_s^k = 0 \tag{2.8}$$

has a non-trivial solution $\mathbf{z}$ in $\mathbb{K}_\infty^s$. Then, for all sufficiently large positive real numbers P, the number of $\mathbb{F}_q[t]$-solutions $N(P; \boldsymbol{\lambda})$ of

$$\langle \lambda_1 x_1^k + \cdots + \lambda_s x_s^k \rangle < \widehat{\tau}, \tag{2.9}$$

with $\langle x_i \rangle \leq \widehat{P}$ $(1 \leq i \leq s)$, satisfies

$$N(P, \boldsymbol{\lambda}) \gg \widehat{P}^{s-k}. \tag{2.10}$$

Here, the implicit constant depends on $\boldsymbol{\lambda}, \tau, k, s,$ and q.

With the exception of Section 2.6, which investigates the solvability of $\lambda_1 z_1^k + \cdots + \lambda_s z_s^k = 0$ in $\mathbb{K}_\infty$, the remainder of this chapter is devoted to proving Theorem 2.2. In order to analyze the integral in (2.7), we split up the subset of $\mathbb{K}_\infty$ for which the integrand is non-zero into two parts. Let

$$S_1(P) = (\mathrm{Log}\, \widehat{P})^{1/8}.$$

Define the *major arc* by

$$\mathfrak{M} = \{\alpha \in \mathbb{K}_\infty : \langle \alpha \rangle < S_1(P) \widehat{P}^{-k}\}$$

and the *minor arc* by

$$\mathfrak{m} = \{\alpha \in \mathbb{K}_\infty : S_1(P) \widehat{P}^{-k} \leq \langle \alpha \rangle < \widehat{\tau}^{-1}\}.$$

Theorem 2.2 is proved by demonstrating that for large enough values of P, one has

$$\int_{\mathfrak{m}} F_1(\alpha)F_2(\alpha)f_3(\alpha)\cdots f_s(\alpha)\chi_\tau(\alpha)\,d\alpha = o(\widehat{P}^{s-k}) \tag{2.11}$$

and

$$\int_{\mathfrak{M}} F_1(\alpha)F_2(\alpha)f_3(\alpha)\cdots f_s(\alpha)\chi_\tau(\alpha)\,d\alpha \gg \widehat{P}^{s-k}. \tag{2.12}$$

We prove (2.11) in Section 2.4 (see Lemma 2.7) by combining mean value estimates with a Weyl-type estimate. The mean value estimates depend on the efficient differencing arguments in [28], and the Weyl-type estimate proved in Section 2.3 stems from the ideas of Bentkus, Götze, and Freeman in [3], [10], and [11]. We prove (2.12) in Section 2.5 (see Lemma 2.10) by using a line of attack similar to that of [23] and [28].

By multiplying each side of (2.9) by $\langle t^{-j}\rangle$ for some sufficiently large integer j, we may assume that $\widehat{\tau} < 1$ and $0 < \langle \lambda_i\rangle < 1$ for $1 \le i \le s$. Since $\lambda_1, \dots, \lambda_s$ are not all in $\mathbb{F}_q(t)$-rational ratio, there is no loss of generality in supposing that $\lambda_2/\lambda_1 \notin \mathbb{K}$.

2.3 A Weyl-Type Estimate

In this section, we mimic the work in Section 2 of [47] to show that when $\alpha \in \mathfrak{m}$, one has $|F_1(\alpha)F_2(\alpha)| = o(\widehat{P}^2)$. Recall that $\mathfrak{n}$ denotes the set of elements α of $\mathbb{T}$ satisfying the property that whenever a and g are elements of $\mathbb{A}$ such that $\langle g\alpha - a\rangle < \widehat{P}^{1-k}$ and $g \neq 0$, then $\langle g\rangle > \widehat{P}$. By Lemma A.5, there exists a small positive constant $\nu = \nu(q,k)$ such that

$$\sup_{\alpha\in\mathfrak{n}} |F(\alpha)| \ll \widehat{P}^{1-\nu}.$$

Our first lemma demonstrates that good Diophantine approximations are produced by large Weyl sums.

Lemma 2.3. *There is a positive constant c, depending at most on k and q, with the following property. Suppose that P is a real number, sufficiently large in terms of k and q, and suppose that δ is a positive number with $\widehat{P}^{-\nu/2} \le \delta \le 1$. Then, whenever $|F(\alpha)| \ge \delta\widehat{P}$, there exist a and g in $\mathbb{A}$ such that $(a,g) = 1$, $1 \le \langle g\rangle \le c\delta^{-k}$, and $\langle g\alpha - a\rangle \le c\delta^{-k}\widehat{P}^{-k}$.*

Proof. Suppose that α is an element of $\mathbb{K}_\infty$ such that $|F(\alpha)| \ge \delta\widehat{P}$, where δ satisfies the hypothesis of the lemma. By Lemma 3 of [23], there exists a unique choice of a and g in $\mathbb{A}$ such that g is monic, $(a,g) = 1$, $1 \le \langle g\rangle \le \widehat{P}^{k-1}$, and $\langle g\alpha - a\rangle < \widehat{P}^{1-k}$.

Suppose that $\langle g\rangle > \widehat{P}$. It follows that $\alpha \in \mathfrak{n}$, implying that $|F(\alpha)| \ll \widehat{P}^{1-\nu}$. When P is sufficiently large in terms of k and q, one has

$$|F(\alpha)| < \frac{1}{2}\widehat{P}^{1-\nu/2} \le \frac{1}{2}\delta\widehat{P},$$

which would contradict our hypothesis on δ. Hence, we may assume that $\langle g\rangle \le \widehat{P}$. In the latter circumstance, by Lemma A.1, we have

$$F(\alpha) \ll \widehat{P}(\langle g\rangle + \widehat{P}^k\langle g\alpha - a\rangle)^{-1/k}.$$

Thus, there exists a positive constant c such that

$$|F(\alpha)| \le c^{1/k}\widehat{P}(\langle g\rangle + \widehat{P}^k\langle g\alpha - a\rangle)^{-1/k}.$$

By recalling that $\delta\widehat{P} \le |F(\alpha)|$, we conclude that

$$\langle g\rangle + \widehat{P}^k\langle g\alpha - a\rangle \le c\delta^{-k},$$

and the lemma follows. □

We now use the hypothesis that $\lambda_2/\lambda_1 \notin \mathbb{K}$ to begin our study of the product $F_1(\alpha)F_2(\alpha)$ of Weyl sums.

Lemma 2.4. *Suppose that S is a fixed real number with $0 < S < \widehat{\tau}^{-1}$. Then, one has*

$$\lim_{P\to\infty} \sup_{S\le\langle\alpha\rangle<\widehat{\tau}^{-1}} \widehat{P}^{-2}|F_1(\alpha)F_2(\alpha)| = 0.$$

Proof. Suppose that the lemma fails. We can then find a real number δ in $(0,1)$, a sequence $(P_n)_{n=1}^{\infty}$ of real numbers that increases monotonically to infinity, and a sequence $(\alpha_n)_{n=1}^{\infty}$ of elements in $\mathbb{K}_\infty$ such that for all n, we have that $S \le \langle\alpha_n\rangle < \widehat{\tau}^{-1}$ and $|F_1(\alpha_n;P_n)F_2(\alpha_n;P_n)| \ge \delta\widehat{P}_n^2$. Since $|F_i(\alpha_n;P_n)| \le \widehat{P}_n$ for $i \in \{1,2\}$, one has $|F_i(\alpha_n;P_n)| \ge \delta\widehat{P}_n$ for $i \in \{1,2\}$. When n is large enough, say $n \ge r$, we have that $\widehat{P}_n^{-\nu/2} \le \delta$ and that $P = P_n$ is sufficiently large in the context of Lemma 2.3. By Lemma 2.3, for $i \in \{1,2\}$ and $n \ge r$, there exist elements a_{in} and g_{in} in $\mathbb{A}$ such that $(a_{in}, g_{in}) = 1$, $1 \le \langle g_{in}\rangle \le c\delta^{-k}$, and

$$\langle g_{in}\lambda_i\alpha_n - a_{in}\rangle \le c\delta^{-k}\widehat{P}_n^{-k}.$$

It follows from the inequality for $\langle g_{in}\rangle$ that there are only finitely many possibilities for such g_{in}. For $i \in \{1,2\}$ and $n \ge r$, by noting that

$$\langle a_{in}\rangle \le \langle g_{in}\lambda_i\alpha_n\rangle + c\delta^{-k}\widehat{P}^{-k} \ll 1,$$

we conclude that there are only finitely many choices for a_{in}. Thus, there are only finitely many possibilities for the 4-tuples $(a_{1n}, g_{1n}, a_{2n}, g_{2n})$, and some 4-tuple, say (a_1, g_1, a_2, g_2), occurs infinitely often.

When $i \in \{1,2\}$ and $n \ge r$, we have

$$\Big\langle \alpha_n - \frac{a_{in}}{g_{in}\lambda_i}\Big\rangle \le \langle g_{in}\lambda_i\rangle^{-1} c\delta^{-k}\widehat{P}_n^{-k} \ll \widehat{P}_n^{-k}, \tag{2.13}$$

and this implies that

$$\Big\langle \frac{a_{1n}}{g_{1n}\lambda_1} - \frac{a_{2n}}{g_{2n}\lambda_2}\Big\rangle \ll \widehat{P}_n^{-k}.$$

Since $(a_{1n}, g_{1n}, a_{2n}, g_{2n}) = (a_1, g_1, a_2, g_2)$ for infinitely many values of n, we conclude that

$$\frac{a_1}{g_1\lambda_1} = \frac{a_2}{g_2\lambda_2}.$$

If $a_1 \neq 0$, then

$$\frac{\lambda_2}{\lambda_1} = \frac{a_2 g_1}{a_1 g_2} \in \mathbb{K},$$

which provides a contradiction. If $a_1 = 0$, by (2.13), there exists some large integer m with $\langle \alpha_m \rangle < S$, contradicting the fact that $S \leq \langle \alpha_n \rangle < \widehat{\tau}^{-1}$ for all $n \in \mathbb{N}$. This completes the proof of the lemma. □

We now are in a position to prove our Weyl-type estimate.

Lemma 2.5. *Suppose that $S(P)$ is a function on $(0, \infty)$ that increases monotonically to infinity and satisfies $1 \leq S(P) \leq \widehat{P}$. Then, there exists a function $T(P)$ on $(0, \infty)$, depending only on λ_1, λ_2, k, q, τ, and $S(P)$, that increases monotonically to infinity, satisfies $1 \leq T(P) \leq S(P)$, and satisfies the property that*

$$\sup_{\substack{\alpha \\ S(P)\widehat{P}^{-k} \leq \langle \alpha \rangle < \widehat{\tau}^{-1}}} |F_1(\alpha)F_2(\alpha)| \ll \widehat{P}^2 T(P)^{-\nu/(2k)}. \tag{2.14}$$

Proof. By Lemma 2.4, for each natural number n, we can find a positive number P_n such that if $P \geq P_n$ and $1/n \leq \langle \alpha \rangle < \widehat{\tau}^{-1}$, then

$$\widehat{P}^{-2}|F_1(\alpha)F_2(\alpha)| \leq \frac{1}{n}.$$

Furthermore, we can choose $(P_n)_{n=1}^{\infty}$ to be an increasing sequence with $S(P_n) \geq n$ for all n. Define $T(P)$ by setting

$$T(P) = \begin{cases} n, & \text{when } P_n \leq P < P_{n+1}, \\ 1, & \text{when } P < P_1. \end{cases}$$

If $P \geq P_n$ and $T(P)^{-1} \leq \langle \alpha \rangle < \widehat{\tau}^{-1}$, then

$$\widehat{P}^{-2}|F_1(\alpha)F_2(\alpha)| \leq \frac{1}{n}.$$

This implies that

$$\sup_{\substack{\alpha \\ T(P)^{-1} \leq \langle \alpha \rangle < \widehat{\tau}^{-1}}} |F_1(\alpha)F_2(\alpha)| \leq \widehat{P}^2 T(P)^{-1}. \tag{2.15}$$

Suppose now that P is sufficiently large in the context of Lemma 2.3. Note that $S(P)\widehat{P}^{-k} \leq T(P)^{-1}$, and assume that

$$S(P)\widehat{P}^{-k} \leq \langle \alpha \rangle < T(P)^{-1}$$

and

$$|F_1(\alpha)| \geq T(P)^{-\nu/(2k)}\widehat{P}.$$

Since

$$\widehat{P}^{-\nu/2} \leq T(P)^{-\nu/(2k)} \leq 1,$$

by applying Lemma 2.3 with $\delta = T(P)^{-\nu/(2k)}$, there exist elements a and g of $\mathbb{A}$ such that $(a, g) = 1$, $1 \leq \langle g \rangle \leq cT(P)^{\nu/2}$, and

$$\langle g\lambda_1\alpha - a \rangle \leq cT(P)^{\nu/2}\widehat{P}^{-k}.$$

Hence, by the triangle inequality,

$$\langle a \rangle \ll \langle g\lambda_1\alpha \rangle + T(P)^{\nu/2}\widehat{P}^{-k} \ll T(P)^{-1+\nu/2} + T(P)^{\nu/2}\widehat{P}^{-k}.$$

Since

$$\lim_{P\to\infty} \left(T(P)^{-1+\nu/2} + T(P)^{\nu/2}\widehat{P}^{-k} \right) = 0,$$

it follows that $a = 0$ for large enough values of P. This implies that

$$\langle \alpha \rangle \ll \langle g\lambda_1 \rangle^{-1} cT(P)^{\nu/2}\widehat{P}^{-k} \ll T(P)^{\nu/2}\widehat{P}^{-k},$$

and thus, for large enough values of P, we see that

$$\langle \alpha \rangle < T(P)\widehat{P}^{-k} \leq S(P)\widehat{P}^{-k}.$$

This contradicts the fact that $\langle \alpha \rangle \geq S(P)\widehat{P}^{-k}$. For P sufficiently large in terms of λ_1, λ_2, k, q, and $S(P)$, we have therefore shown that whenever

$$S(P)\widehat{P}^{-k} \leq \langle \alpha \rangle < T(P)^{-1},$$

then

$$|F_1(\alpha)| < \widehat{P}T(P)^{-\nu/(2k)}.$$

Hence,

$$\sup_{\substack{\alpha \\ S(P)\widehat{P}^{-k} \leq \langle \alpha \rangle < T(P)^{-1}}} |F_1(\alpha)F_2(\alpha)| \ll \widehat{P}^2 T(P)^{-\nu/(2k)}. \tag{2.16}$$

The lemma now follows by combining (2.15) with (2.16). □

2.4 The Minor Arc

In order to complete our work on the minor arc, we first need to establish a mean value estimate for the smooth Weyl sum $f(\alpha)$.

Lemma 2.6. *Suppose that $u > 2k-2$ is accessible to the exponent k and that $s \geq u+5$. One has*

$$\int_{\mathbb{T}} |f(\alpha)|^{s-2}\, d\alpha \ll \widehat{P}^{s-2-k}.$$

Proof. Let $v = [s/2] - 2$. By considering the underlying Diophantine equations, we note that

$$\int_{\mathbb{T}} |f(\alpha)|^{2v+2} d\alpha \ll \int_{\mathbb{T}} |F(\alpha)^2 f(\alpha)^{2v}|\, d\alpha.$$

Since $2v \geq s-5 \geq u$, we may apply Lemma A.3 to establish that

$$\int_{\mathbb{T}} |F(\alpha)^2 f(\alpha)^{2v}|\, d\alpha \ll \widehat{P}^{2v+2-k},$$

and this implies that

$$\int_{\mathbb{T}} |f(\alpha)|^{2v+2}\, d\alpha \ll \widehat{P}^{2[s/2]-2-k}.$$

For even values of s, the proof of the lemma is now complete. If s is odd, the lemma follows by noting that

$$\int_{\mathbb{T}} |f(\alpha)|^{s-2}\, d\alpha \le \widehat{P} \int_{\mathbb{T}} |f(\alpha)|^{2v+2}\, d\alpha \ll \widehat{P}^{2[s/2]-1-k}. \qquad \square$$

We are now in a position to show that the minor arc contribution is $o(\widehat{P}^{s-k})$, thereby confirming (2.11).

Lemma 2.7. *One has*

$$\int_{\mathfrak{m}} F_1(\alpha)F_2(\alpha)f_3(\alpha)\cdots f_s(\alpha)\chi_\tau(\alpha)\, d\alpha = o(\widehat{P}^{s-k}).$$

Proof. By Hölder's inequality,

$$\int_{\mathfrak{m}} F_1(\alpha)F_2(\alpha)f_3(\alpha)\cdots f_s(\alpha)\chi_\tau(\alpha)\, d\alpha \ll \Big(\sup_{\alpha\in\mathfrak{m}} |F_1(\alpha)F_2(\alpha)|\Big) \prod_{i=3}^{s} I_i^{1/(s-2)}, \tag{2.17}$$

where

$$I_i = \int_{\langle\alpha\rangle<\widehat{\tau}^{-1}} |f_i(\alpha)|^{s-2}\, d\alpha$$

for $3 \le i \le s$. Note that $f(\alpha+g) = f(\alpha)$ for all $\alpha \in \mathbb{T}$ and $g \in \mathbb{A}$. By Lemma 2.6, one has

$$\begin{aligned}\int_{\langle\alpha\rangle<\widehat{\tau}^{-1}} |f(\alpha)|^{s-2}\, d\alpha &= \sum_{\langle x\rangle<\widehat{\tau}^{-1}} \int_{\langle\alpha-x\rangle<1} |f(\alpha)|^{s-2}\, d\alpha \\ &= \sum_{\langle x\rangle<\widehat{\tau}^{-1}} \int_{\mathbb{T}} |f(\alpha)|^{s-2}\, d\alpha \ll \widehat{P}^{s-2-k}.\end{aligned}$$

For $3 \le i \le s$, since $\langle\lambda_i\rangle < 1$, we see that

$$I_i = \langle\lambda_i\rangle^{-1} \int_{\langle\alpha\rangle<\langle\lambda_i\rangle\widehat{\tau}^{-1}} |f(\alpha)|^{s-2}\, d\alpha \ll \int_{\langle\alpha\rangle<\widehat{\tau}^{-1}} |f(\alpha)|^{s-2}\, d\alpha \ll \widehat{P}^{s-2-k}. \tag{2.18}$$

By applying Lemma 2.5 with $S(P) = S_1(P)$, we obtain the bound

$$\sup_{\alpha \in \mathfrak{m}} |F_1(\alpha)F_2(\alpha)| = o(P^2). \tag{2.19}$$

The result now follows by combining (2.17), (2.18), and (2.19). □

2.5 The Major Arc

We now wish to find an asymptotic for the major arc contribution. Let

$$\mathcal{F}(\alpha) = F_1(\alpha)F_2(\alpha)f_3(\alpha)\cdots f_s(\alpha)$$

and

$$\mathcal{G}(\alpha) = F_1(\alpha)\cdots F_s(\alpha).$$

Since $S_1(P)\widehat{P}^{-k} \le \widehat{\tau}^{-1}$, one has

$$\int_{\mathfrak{M}} \mathcal{F}(\alpha)\chi_\tau(\alpha)\, d\alpha = \hat{\tau} \int_{\mathfrak{M}} \mathcal{F}(\alpha)\, d\alpha.$$

We first wish to compare this integral to the *singular integral*

$$J_{s,k} = \int_{\langle\alpha\rangle < \widehat{P}^{1-k}} \mathcal{G}(\alpha)\, d\alpha.$$

To do this, let $\rho(u)$ denote the Dickman function, which is defined as the unique continuous function on $[0,\infty)$ that satisfies the differential-difference equation $u\rho'(u) = -\rho(u-1)$ $(u > 1)$ with the initial condition $\rho(u) = 1$ $(0 \le u \le 1)$.

Lemma 2.8. *One has*

$$\int_{\mathfrak{M}} \mathcal{F}(\alpha)\, d\alpha - \rho(P/R)^{s-2}J_{s,k} \ll \widehat{P}^{s-k}(\operatorname{Log}\widehat{P})^{-1/(8k)}.$$

Proof. Let P be large enough so that $P \ge 1$ and

$$2P/\log(2P) < R = \eta P < P - \log(P).$$

For $3 \le i \le s$, we deduce from Lemma A.2 that

$$\begin{aligned} f_i(\alpha) - \rho(P/R)F_i(\alpha) &\ll \widehat{P}(\operatorname{Log}\widehat{P})^{-1/2}(1+\widehat{P}^k\langle\lambda_i\alpha\rangle) \\ &\ll \widehat{P}(\operatorname{Log}\widehat{P})^{-3/8} \end{aligned}$$

for $\alpha \in \mathfrak{M}$. Hence,

$$\mathcal{F}(\alpha) - \rho(P/R)^{s-2}\mathcal{G}(\alpha) \ll \widehat{P}^s(\operatorname{Log}\widehat{P})^{-3/8}$$

for $\alpha \in \mathfrak{M}$. Furthermore, by noting that the measure of $\mathfrak{M}$ is $O(\widehat{P}^{-k}(\operatorname{Log}\widehat{P})^{1/8})$, one has

$$\int_{\mathfrak{M}} \mathcal{F}(\alpha)\,d\alpha - \rho(P/R)^{s-2}\int_{\mathfrak{M}} \mathcal{G}(\alpha)\,d\alpha \ll \widehat{P}^{s-k}(\operatorname{Log}\widehat{P})^{-1/4}.$$

By Lemma A.1, whenever $1 \le i \le s$ and $\langle\alpha\rangle \le \widehat{P}^{1-k}$, we have the bound

$$F_i(\alpha) \ll \widehat{P}(1+\widehat{P}^k\langle\lambda_i\alpha\rangle)^{-1/k} \ll \widehat{P}(1+\widehat{P}^k\langle\alpha\rangle)^{-1/k}.$$

Therefore,

$$\int_{\mathfrak{M}} \mathcal{G}(\alpha)\,d\alpha - J_{s,k} \ll P^s\int_{\mathfrak{T}}(1+\widehat{P}^k\langle\alpha\rangle)^{-s/k}\,d\alpha,$$

where $\mathfrak{T} = \{\alpha \in \mathbb{K}_\infty : S_1(P)\widehat{P}^{-k} \le \langle\alpha\rangle\}$. Let $V = \log_q(S_1(P))$. Since the measure of the set of points α in $\mathbb{T}$ with $\langle\alpha\rangle = q^m$ is less than q^{m+1}, we deduce that

$$\begin{aligned} \int_{\mathfrak{M}} \mathcal{G}(\alpha)\,d\alpha - J_{s,k} &\ll \widehat{P}^s \sum_{V-kP\le m} q^{m+1}(1+q^{kP+m})^{-s/k} \\ &\ll \widehat{P}^{s-k}\widehat{V}^{1-s/k} \ll \widehat{P}^{s-k}(\operatorname{Log}P)^{-1/(8k)}. \end{aligned}$$

We have now established that

$$\int_{\mathfrak{M}} \mathcal{F}(\alpha)\,d\alpha - \rho(P/R)^{s-2}J_{s,k} \ll \widehat{P}^{s-k}(\operatorname{Log}\widehat{P})^{-1/(8k)}. \qquad \square$$

Since $0 < \eta < 1$ and $R = \eta P$, it follows that $\rho(P/R) \gg 1$. Thus, we are left to show that $J_{s,k} \gg \widehat{P}^{s-k}$ in order to get an asymptotic lower bound of the desired form for the major arc contribution. To do this, we use ingredients from the proof of Lemma 16 in [23].

Lemma 2.9. *For sufficiently large values of P, one has $J_{s,k} \gg \widehat{P}^{s-k}$.*

Proof. By Lemma 1 of [23],

$$J_{s,k} = \int_{\langle\alpha\rangle<\widehat{P}^{1-k}} F_1(\alpha)\cdots F_s(\alpha)\,d\alpha = \widehat{P}^{1-k}W, \tag{2.20}$$

where W denotes the number of s-tuples $(x_1, x_2, \dots, x_s)$ in $\mathbb{A}^s$ with

$$\langle\lambda_1 x_1^k + \cdots + \lambda_s x_s^k\rangle < \widehat{P}^{k-1} \tag{2.21}$$

and $\langle x_i\rangle \le \widehat{P}$ for $1 \le i \le s$.

By our hypothesis in Theorem 2.2, we know that there exists a non-trivial solution $\mathbf{z} \in \mathbb{K}_\infty^s$ for (2.8). Choose r such that $\langle\lambda_r z_r^k\rangle$ is maximal. Let $d = \operatorname{ord}\lambda_r$ and $w = \operatorname{lead}(\lambda_r)$. For $1 \le i \le s$, we define a_i by

$$a_i = \begin{cases} \operatorname{lead}(z_i), & \text{when } \langle\lambda_i z_i^k\rangle = \langle\lambda_r z_r^k\rangle, \\ 0, & \text{otherwise.} \end{cases}$$

For $1 \le i \le s$, let

$$m_i = \left\lfloor \frac{d - \operatorname{ord}\lambda_i + k\operatorname{ord} z_r}{k} \right\rfloor,$$

and let $n = [P] - \max_{1\le i\le s} m_i$. Suppose that P is large enough so that $n + m_i > 0$ for $1 \le i \le s$. For $1 \le i \le s$, let x_i be an element of $\mathbb{A}$ with $x_i = a_i t^{n+m_i} + y_i$, where $y_i \in \mathbb{A}$ and $\operatorname{ord} y_i < n + m_i$. Let

$$x_r = a_r t^{n+m_r} + b_{n+m_r-1}t^{n+m_r-1} + \cdots + b_0,$$

where each b_i is an element of $\mathbb{F}_q$, and define the coefficients $c_l \in \mathbb{F}_q$ via the relation

$$\lambda_1 x_1^k + \cdots + \lambda_s x_s^k = \sum_{l=-\infty}^{\infty} c_l t^l.$$

The inequality (2.21) is satisfied when $c_l = 0$ for all $l \ge (k-1)P$. For $1 \le i \le s$, observe that

$$\operatorname{ord}\lambda_i + k(n + m_i) \le d + k(n + m_r)$$

with equality holding whenever $\langle \lambda_i z_i^k \rangle = \langle \lambda_r z_r^k \rangle$. Thus, the coefficient $c_l = 0$ for all $l > d + k(n + m_r)$. Furthermore, our choice of $(a_1, \dots, a_s)$ guarantees that $c_{d+k(n+m_r)} = 0$. When

$$d + (k-1)(n+m_r) \le l < d + k(n+m_r),$$

one has

$$c_l = kwa_r^{k-1} b_{l-d-(k-1)(n+m_r)} + h_l,$$

where h_l is an element of $\mathbb{F}_q$ depending at most on $\boldsymbol{\lambda}$, $\mathbf{a}$, b_i with

$$i > l - d - (k-1)(n+m_r),$$

and y_j with $j \neq r$.

Let y_j be arbitrarily selected for each $j \neq r$. Since $kwa_r^{k-1} \neq 0$, we can choose b_{n+m_r-1} so that $c_{d+k(n+m_r)-1} = 0$. Similarly, we can now choose b_{n+m_r-2} so that $r_{d+k(n+m_r)-2} = 0$. Continuing in this manner, it is possible to choose x_r in such a way that $c_l = 0$ for all

$$l \ge d + (k-1)(n+m_r).$$

Since d is negative, one has

$$d + (k-1)(n+m_r) < (k-1)P,$$

and it follows that (2.21) holds for $(x_1, \dots, x_s)$. Since y_j was arbitrarily selected for $j \neq r$, for sufficiently large values of P, it follows that $W \gg \widehat{P}^{s-1}$, and from (2.20), we conclude that $J_{s,k} \gg \widehat{P}^{s-k}$. □

By combining Lemmas 2.8 and 2.9, we obtain the following result, which confirms (2.12).

Lemma 2.10. *For sufficiently large values of P, one has*

$$\int_{\mathfrak{M}} F_1(\alpha)F_2(\alpha)f_3(\alpha)\cdots f_s(\alpha)\chi_\tau(\alpha)\,d\alpha \gg \widehat{P}^{s-k}.$$

2.6 The Solvability of $\lambda_1 z_1^k + \cdots + \lambda_s z_s^k = 0$ in $\mathbb{K}_\infty$

Let $\psi(q,k)$ denote the minimum integer such that for all $n > \psi(q,k)$ and any choice of $a_1,\dots,a_n \in \mathbb{F}_q$, the equation $a_1y_1^k + \cdots + a_ny_n^k = 0$ has a non-zero solution $\mathbf{y} \in \mathbb{F}_q^n$. We now use the function $\psi(q,k)$ to discuss the solvability of $\lambda_1 z_1^k + \cdots + \lambda_s z_s^k = 0$ in $\mathbb{K}_\infty$, which is a necessary hypothesis in Theorems 2.1 and 2.2.

Lemma 2.11. *Let $\lambda_1,\dots,\lambda_s$ be non-zero elements of $\mathbb{K}_\infty$. Whenever* $\mathrm{char}(\mathbb{F}_q) \nmid k$ *and $s > k\psi(q,k)$, there exists a non-trivial solution $\mathbf{z} \in \mathbb{K}_\infty^s$ of the equation $\lambda_1 z_1^k + \cdots + \lambda_s z_s^k = 0$.*

Proof. Suppose that $s > k\psi(q,k)$. Note that for any $l_1,\dots,l_s \in \mathbb{Z}$, we have

$$\lambda_1 z_1^k + \cdots + \lambda_s z_s^k = (\lambda_1 t^{-kl_1})(z_1 t^{l_1})^k + \cdots + (\lambda_s t^{-kl_s})(z_s t^{l_s})^k. \tag{2.22}$$

Hence, without loss of generality, we may assume that $0 \le \operatorname{ord}\lambda_i < k$ for each $1 \le i \le s$, and we can find an integer w with $0 \le w < k$ such that $\operatorname{ord}\lambda_i = w$ for at least $\lceil s/k \rceil$ distinct choices of i with $1 \le i \le s$. By multiplying the equation $\lambda_1 z_1^k + \cdots + \lambda_s z_s^k = 0$ by t^{-w}, using (2.22) if necessary, and rearranging the indices if required, there is no loss of generality in supposing that $\operatorname{ord}\lambda_i = 0$ $(1 \le i \le n)$ and $\operatorname{ord}\lambda_j < 0$ $(n < j \le s)$, where $n \ge s/k > \psi(q,k)$. Therefore, there exist elements $y_1,\dots,y_n \in \mathbb{F}_q$, not all zero, such that

$$\mathrm{lead}(\lambda_1)y_1^k + \cdots + \mathrm{lead}(\lambda_n)y_n^k = 0.$$

By reordering the indices if necessary, we may assume that $y_1 \neq 0$. Let $z_i = y_i$ $(2 \le i \le n)$ and $z_j = 0$ $(n < j \le s)$. Consider the function

$$f(z) = \lambda_1 z^k + \lambda_2 z_2^k + \lambda_3 z_3^k + \cdots + \lambda_s z_s^k.$$

Since $\operatorname{ord} f(y_1) < 0$ and $\operatorname{ord} f'(y_1) = \operatorname{ord}(k\lambda_1 y_1^{k-1}) = 0$, a variant of Hensel's lemma implies that there exists an element $z_1 \in \mathbb{K}_\infty$ such that $\operatorname{ord}(z_1 - y_1) < 0$ and $f(z_1) = 0$. The lemma now follows. □

By Chevalley's theorem (see Theorem 1 of Section 10.2 in [22]), we see that $\psi(q,k) \leq k$. When $q > k^4$, it follows from the work of Weil (see [45]) that $\psi(q,k) \leq 2$. Furthermore, when $(k, q-1) = 1$, the mapping $x \mapsto x^k$ from $\mathbb{F}_q$ to $\mathbb{F}_q$ is a bijection, implying that $\psi(q,k) = 1$. We summarize the results of this section in the following lemma.

Lemma 2.12. *Suppose that* $\operatorname{char}(\mathbb{F}_q) \nmid k$, *and let* $\lambda_1, \dots, \lambda_s$ *be non-zero elements of* $\mathbb{K}_\infty$. *The equation* $\lambda_1 z_1^k + \cdots + \lambda_s z_s^k = 0$ *has a non-trivial solution* $\mathbf{z} \in \mathbb{K}_\infty^s$ *whenever one of the following three conditions are met:*

1. $s \geq k^2 + 1$,
2. $q > k^4$ *and* $s \geq 2k + 1$,
3. $(k, q-1) = 1$ *and* $s \geq k + 1$.

CHAPTER III

A Generalization of Roth's Theorem in Function Fields

3.1 Overview

Let $\mathbb{F}_q[t]$ denote the ring of polynomials over the finite field $\mathbb{F}_q$. For $N \in \mathbb{N}$, let $\mathcal{S}_N$ denote the subset of $\mathbb{F}_q[t]$ containing all polynomials of degree strictly less than N. For an integer $s \geq 3$, let $\mathbf{r} = (r_1, \ldots, r_s)$ be a vector of non-zero elements of $\mathbb{F}_q$ satisfying $r_1 + \cdots + r_s = 0$. A solution $\mathbf{x} = (x_1, \ldots, x_s) \in \mathcal{S}_N^s$ of $r_1x_1 + \cdots + r_sx_s = 0$ is said to be *trivial* if $x_{j_1} = \cdots = x_{j_l}$ for some subset $\{j_1, \ldots, j_l\} \subseteq \{1, \ldots, s\}$ with $r_{j_1} + \cdots + r_{j_l} = 0$. Otherwise, we say a solution $\mathbf{x}$ is *non-trivial*. Let $D_{\mathbf{r}}(\mathcal{S}_N)$ denote the maximal cardinality of a set $A \subseteq \mathcal{S}_N$ which contains no non-trivial solution of $r_1x_1 + \cdots + r_sx_s = 0$ with $x_i \in A$ $(1 \leq i \leq s)$.

We will now state the main result of this chapter.

Theorem 3.1. *For $N \in \mathbb{N}$,*

$$D_{\mathbf{r}}(\mathcal{S}_N) \ll \frac{|\mathcal{S}_N|}{(\log_q |\mathcal{S}_N|)^{s-2}} = \frac{q^N}{N^{s-2}}.$$

Here the implicit constant depends only on $\mathbf{r}$.

Before proving Theorem 3.1, we recall the Fourier analysis of $\mathbb{F}_q[t]$. Let $\mathbb{K} = \mathbb{F}_q(t)$ be the field of fractions of $\mathbb{F}_q[t]$, and let $\mathbb{K}_\infty = \mathbb{F}_q((1/t))$ be the completion of $\mathbb{K}$ at ∞. We may write each element $\alpha \in \mathbb{K}_\infty$ in the shape $\alpha = \sum_{i \leq v} a_i t^i$ for some $v \in \mathbb{Z}$

and $a_i = a_i(\alpha) \in \mathbb{F}_q$ $(i \le v)$. If $a_v \neq 0$, we define $\operatorname{ord}\alpha = v$, and we write $\langle\alpha\rangle$ for $q^{\operatorname{ord}\alpha}$. We adopt the conventions that $\operatorname{ord} 0 = -\infty$ and $\langle 0\rangle = 0$. For a real number R, we let $\widehat{R}$ denote q^R. Hence, if x is a polynomial in $\mathbb{F}_q[t]$, then $\langle x\rangle < \widehat{N}$ if and only if the degree of x is strictly less than N. Consider the compact additive subgroup $\mathbb{T}$ of $\mathbb{K}_\infty$ defined by $\mathbb{T} = \big\{\alpha \in \mathbb{K}_\infty : \langle\alpha\rangle < 1\big\}$. Given any Haar measure $d\alpha$ on $\mathbb{K}_\infty$, we normalize it in such a manner that $\int_{\mathbb{T}} 1\, d\alpha = 1$. Thus, if $\mathfrak{M}$ is the subset of $\mathbb{K}_\infty$ defined by $\mathfrak{M} = \big\{\alpha \in \mathbb{K}_\infty :\ \operatorname{ord}\alpha < -N\big\}$, then the measure of $\mathfrak{M}$, $\operatorname{mes}(\mathfrak{M})$, is equal to $\widehat{N}^{-1}$.

We are now equipped to define the exponential function on $\mathbb{F}_q[t]$. Suppose that the characteristic of $\mathbb{F}_q$ is p. Let $e(z)$ denote $e^{2\pi i z}$, and let $\operatorname{tr} : \mathbb{F}_q \to \mathbb{F}_p$ denote the familiar trace map. There is a non-trivial additive character $e_q : \mathbb{F}_q \to \mathbb{C}^\times$ defined for each $a \in \mathbb{F}_q$ by taking $e_q(a) = e(\operatorname{tr}(a)/p)$. This character induces a map $e : \mathbb{K}_\infty \to \mathbb{C}^\times$ by defining, for each element $\alpha \in \mathbb{K}_\infty$, the value of $e(\alpha)$ to be $e_q(a_{-1}(\alpha))$. It is often convenient to refer to $a_{-1}(\alpha)$ as being the residue of α, an element of $\mathbb{F}_q$ that we denote by $\operatorname{res}\alpha$. In this guise, we have $e(\alpha) = e_q(\operatorname{res}\alpha)$. The orthogonality relation underlying the Fourier analysis of $\mathbb{F}_q[t]$, established in [23, Lemma 1], takes the shape

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

This chapter is based on the author and Yu-Ru Liu's submitted manuscript [26].

3.2 Proof of Theorem 3.1

For $N \in \mathbb{N}$ and $s \ge 3$, let $\mathbf{r} = (r_1, \dots, r_s)$, $\mathcal{S}_N$, and $D_{\mathbf{r}}(\mathcal{S}_N)$ be defined as in Section 3.1. Write $d_{\mathbf{r}}(N) = D_{\mathbf{r}}(\mathcal{S}_N)/|\mathcal{S}_N|$. For convenience, in what follows, we write $D(\mathcal{S}_N)$ in place of $D_{\mathbf{r}}(\mathcal{S}_N)$ and $d(N)$ in place of $d_{\mathbf{r}}(N)$. Hence, to prove Theorem 3.1, it is equivalent to show that $d(N) \ll 1/N^{s-2}$.

For a set $A \subseteq \mathcal{S}_N$, let $T(A) = T_{\mathbf{r}}(A)$ denote the number of solutions of $r_1x_1 + \cdots + r_sx_s = 0$ with $x_i \in A$ $(1 \le i \le s)$. Let 1_A be the characteristic function of A, i.e., $1_A(x) = 1$ if $x \in A$ and $1_A(x) = 0$ otherwise. Define

$$f_i(\alpha) = \sum_{\langle x \rangle < \widehat{N}} 1_A(x) e(\alpha r_i x) = \sum_{x \in A} e(\alpha r_i x).$$

Then, by the orthogonality relation for the exponential function, we have

$$T(A) = \int_{\mathbb{T}} f_1(\alpha) f_2(\alpha) \cdots f_s(\alpha)\, d\alpha. \tag{3.1}$$

We estimate $T(A)$ by dividing $\mathbb{T}$ into two parts: the major arc $\mathfrak{M}$ defined by $\mathfrak{M} = \{\alpha : \operatorname{ord}\alpha < -N\}$ and the minor arc $\mathfrak{m} = \mathbb{T} \setminus \mathfrak{M} = \{\alpha : -N \le \operatorname{ord}\alpha < 0\}$.

Lemma 3.2. *Suppose that $A \subseteq \mathcal{S}_N$ contains no non-trivial solution of $r_1x_1 + \cdots + r_sx_s = 0$ with $x_i \in A$ $(1 \le i \le s)$. Then, we have*

$$\sup_{\alpha \in \mathfrak{m}} \left| f_i(\alpha) \right| \le d(N-1)\widehat{N} - |A|.$$

Proof. For $\alpha \in \mathfrak{m}$, let $W = W(\alpha, r_i) = \left\{ y \in \mathcal{S}_N \colon e(\alpha r_i y) = 1 \right\}$. Since $\operatorname{ord} r_i = 0$ and $-N \le \operatorname{ord}\alpha < 0$, we can write $\operatorname{ord}(\alpha r_i) = -l$ and $\alpha r_i = \sum_{j \le -l} b_j t^j$ with $-N \le -l \le -1$, $b_j \in \mathbb{F}_q$ $(j \le -l)$, and $b_{-l} \ne 0$. Then, for $y = c_{N-1}t^{N-1} + \cdots + c_0 \in \mathcal{S}_N$, the polynomial $y \in W$ if and only if

$$\operatorname{res}(\alpha r_i y) = b_{-l}c_{l-1} + b_{-l-1}c_l + \cdots + b_{-N}c_{N-1} = 0.$$

Therefore, we have that $W \simeq \mathbb{F}_q^{N-1}$ as a vector space over $\mathbb{F}_q$.

Since $\operatorname{ord}(\alpha r_i) \ge -N$, by [23, Lemma 7], we have

$$\sum_{\langle x \rangle < \widehat{N}} e(\alpha r_i x) = 0.$$

Hence,

$$\operatorname{card}(W) \cdot |f_i(\alpha)| = \left| \sum_{y \in W} \sum_{\langle x \rangle < \widehat{N}} d(N-1) e(\alpha r_i x) - \sum_{y \in W} \sum_{\langle x \rangle < \widehat{N}} 1_A(x) e(\alpha r_i x) \right|.$$

For $y \in W$, since $e(\alpha r_i y) = 1$ and $y \in \mathcal{S}_N$, we have by a change of variables that

$$\sum_{\langle x \rangle < \widehat{N}} 1_A(x) e(\alpha r_i x) = \sum_{\langle x \rangle < \widehat{N}} 1_A(x) e(\alpha r_i (x+y)) = \sum_{\langle x \rangle < \widehat{N}} 1_A(x-y) e(\alpha r_i x).$$

It now follows that

$$\begin{aligned} \operatorname{card}(W) \cdot |f_i(\alpha)| &= \Big| \sum_{\langle x \rangle < \widehat{N}} \Big(\sum_{y \in W} d(N-1) - \sum_{y \in W} 1_A(x-y) \Big) e(\alpha r_i x) \Big| \\ &\leq \sum_{\langle x \rangle < \widehat{N}} \Big| \sum_{y \in W} d(N-1) - \sum_{y \in W} 1_A(x-y) \Big| \\ &= \sum_{\langle x \rangle < \widehat{N}} \Big| d(N-1) \cdot \operatorname{card}(W) - \operatorname{card}\big(W \cap (x-A)\big) \Big|. \end{aligned}$$

Since $r_1 + \cdots + r_s = 0$ and A contains no non-trivial solution of $r_1 x_1 + \cdots + r_s x_s = 0$ with $x_i \in A$ $(1 \leq i \leq s)$, the set $W \cap (x - A)$ also contains no non-trivial solution of the same equation. Since $W \simeq \mathcal{S}_{N-1}$ as a vector space over $\mathbb{F}_q$ and $r_i \in \mathbb{F}_q$ $(1 \leq i \leq s)$, any invertible $\mathbb{F}_q$-linear transformation from W to $\mathcal{S}_{N-1}$ maps $W \cap (x-A)$ to a subset of $\mathcal{S}_{N-1}$ which contains no non-trivial solution of $r_1 x_1 + \cdots + r_s x_s = 0$. This implies that $\operatorname{card}(W \cap (x-A)) \leq d(N-1) \cdot \operatorname{card}(W)$. We may now conclude that

$$\begin{aligned} \operatorname{card}(W) \cdot |f_i(\alpha)| &\leq \sum_{\langle x \rangle < \widehat{N}} \Big(d(N-1) \cdot \operatorname{card}(W) - \operatorname{card}\big(W \cap (x-A)\big) \Big) \\ &= d(N-1) \cdot \operatorname{card}(W) \cdot \widehat{N} - \operatorname{card}(W) \cdot \operatorname{card}(A). \end{aligned}$$

Thus, if $\alpha \in \mathfrak{m}$, we have

$$|f_i(\alpha)| \leq d(N-1) \cdot \widehat{N} - |A|.$$

This completes the proof of the lemma. □

Now, we are ready to prove Theorem 3.1.

Proof. (of Theorem 3.1) Suppose that $A \subseteq \mathcal{S}_N$ contains no non-trivial solution of $r_1 x_1 + \cdots + r_s x_s = 0$ with $x_i \in A$ $(1 \leq i \leq s)$. We suppose further that $|A|/|\mathcal{S}_N| =$

$d(N)$. By (3.1), we have

$$\begin{aligned} T(A) &= \int_{\mathbb{T}} f_1(\alpha) f_2(\alpha) \cdots f_s(\alpha)\, d\alpha \\ &= \int_{\mathfrak{M}} f_1(\alpha) f_2(\alpha) \cdots f_s(\alpha)\, d\alpha + \int_{\mathfrak{m}} f_1(\alpha) f_2(\alpha) \cdots f_s(\alpha)\, d\alpha. \end{aligned} \tag{3.2}$$

If $\alpha \in \mathfrak{M}$ and $x \in \mathcal{S}_N$, we have $e(\alpha r_i x) = 1$. It follows that

$$\int_{\mathfrak{M}} f_1(\alpha) f_2(\alpha) \cdots f_s(\alpha)\, d\alpha = |A|^s \cdot \mathrm{mes}(\mathfrak{M}) = d(N)^s\, \widehat{N}^{s-1}. \tag{3.3}$$

By the orthogonality relation for the exponential function,

$$\int_{\mathbb{T}} |f_1(\alpha)|^2\, d\alpha = |A| = \int_{\mathbb{T}} |f_2(\alpha)|^2\, d\alpha.$$

Hence, by Cauchy's inequality and Lemma 3.2, we have

$$\begin{aligned} &\left| \int_{\mathfrak{m}} f_1(\alpha) f_2(\alpha) \cdots f_s(\alpha)\, d\alpha \right| \\ &\le \sup_{\alpha \in \mathfrak{m}} \left| f_3(\alpha) \cdots f_s(\alpha) \right| \left(\int_{\mathbb{T}} |f_1(\alpha)|^2\, d\alpha \right)^{1/2} \left(\int_{\mathbb{T}} |f_2(\alpha)|^2\, d\alpha \right)^{1/2} \\ &\le d(N) \big(d(N-1) - d(N) \big)^{s-2}\, \widehat{N}^{s-1}. \end{aligned} \tag{3.4}$$

By combining (3.2), (3.3), and (3.4), we obtain

$$\begin{aligned} T(A) &\ge \int_{\mathfrak{M}} f_1(\alpha) f_2(\alpha) \cdots f_s(\alpha)\, d\alpha - \left| \int_{\mathfrak{m}} f_1(\alpha) f_2(\alpha) \cdots f_s(\alpha)\, d\alpha \right| \\ &\ge \Big(d(N)^s - d(N) \big(d(N-1) - d(N) \big)^{s-2} \Big)\, \widehat{N}^{s-1}. \end{aligned}$$

Since A contains no non-trivial solution of $r_1 x_1 + \cdots + r_s x_s = 0$ with $x_i \in A$ $(1 \le i \le s)$, there exists a constant $B = B(\mathbf{r})$ such that

$$T(A) \le B|A|^{s-2} = B d(N)^{s-2} \widehat{N}^{s-2}.$$

Combining the above two inequalities, we have

$$d(N)^s - B d(N)^{s-2} \widehat{N}^{-1} - d(N) \big(d(N-1) - d(N) \big)^{s-2} \le 0. \tag{3.5}$$

We now claim that there exists a constant $C = C(\mathbf{r}) \geq 1$ such that for all $N \in \mathbb{N}$,

$$d(N) \leq \frac{C^{s-2}}{N^{s-2}}.$$

This statement follows by induction on N. Since $d(N) \leq 1$, the cases where $N \leq C$ are trivial. Let $N > C$, and suppose that $d(N-1) \leq C^{s-2}(N-1)^{2-s}$. We now verify that $d(N) \leq C^{s-2}N^{2-s}$. Since $N^{s-1}(2^N)^{-1/2} \to 0$ as $N \to \infty$, without loss of generality, we may assume that $C^{s-2} \geq B^{1/2}N^{s-1}(2^N)^{-1/2}$ for all $N \in \mathbb{N}$. Hence, if $d(N)^2 \leq BN^2\widehat{N}^{-1}$, since $\widehat{N} \geq 2^N$, we have

$$d(N) \leq B^{1/2}N\widehat{N}^{-1/2} \leq B^{1/2}N(2^N)^{-1/2} \leq C^{s-2}N^{2-s},$$

which gives the desired conclusion. Thus, in what follows, we assume that $d(N)^2 > BN^2\widehat{N}^{-1}$. Since $Bd(N)^{s-2}\widehat{N}^{-1} < d(N)^sN^{-2}$ and $N \geq 2$, by (3.5), we have

$$d(N)^s2^{-1} < d(N)^s(1-N^{-2}) < d(N)\big(d(N-1)-d(N)\big)^{s-2}.$$

Let $E = E(\mathbf{r})$ be the unique positive number satisfying $E^{s-2} = 2^{-1}$. By the induction hypothesis for $d(N-1)$, the above inequality implies that

$$Ed(N)^{\frac{s-1}{s-2}} + d(N) < d(N-1) \leq \frac{C^{s-2}}{(N-1)^{s-2}}. \tag{3.6}$$

We note that without loss of generality, we can assume that $C \geq E^{-1}(2^{s-1}-2)$. Then by the binomial theorem, we have

$$\begin{aligned} N^{s-1} &= (N-1)^{s-1} + \binom{s-1}{1}(N-1)^{s-2} + \binom{s-1}{2}(N-1)^{s-3} + \cdots + \binom{s-1}{s-1} \\ &\leq (N-1)^{s-1} + (N-1)^{s-2}(2^{s-1}-1) \\ &\leq (N-1)^{s-1} + (N-1)^{s-2}(CE+1). \end{aligned}$$

Then, it follows that

$$\frac{C^{s-2}}{(N-1)^{s-2}} \leq E\left(\frac{C^{s-2}}{N^{s-2}}\right)^{\frac{s-1}{s-2}} + \frac{C^{s-2}}{N^{s-2}}.$$

We note that $Ex^{\frac{s-1}{s-2}} + x$ is an increasing function of x. Thus, by combining the above inequality with (3.6), we conclude that $d(N) \leq C^{s-2}N^{2-s}$. This completes the proof of Theorem 3.1. $\square$

CHAPTER IV

A Generalization of Roth's Theorem in Finite Abelian Groups

4.1 Overview

For a natural number $s \geq 3$, let $\mathbf{r} = (r_1, \ldots, r_s)$ be a vector of non-zero integers satisfying $r_1 + \cdots + r_s = 0$. Given a finite Abelian group M, we can write

$$M \simeq \mathbb{Z}/k_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/k_n\mathbb{Z},$$

where $\mathbb{Z}/k_i\mathbb{Z}$ is a cyclic group $(1 \leq i \leq n)$ and $k_i | k_{i-1}$ $(2 \leq i \leq n)$. We denote by $c(M) = n$ the number of constituents $\mathbb{Z}/k_i\mathbb{Z}$ of M. Moreover, we say that M is *coprime to* $\mathbf{r}$ provided that $(r_i, k_1) = 1$ for $1 \leq i \leq s$.

A solution $\mathbf{x} = (x_1, \ldots, x_s) \in M^s$ of $r_1x_1 + \cdots + r_sx_s = 0$ is said to be *trivial* if $x_{j_1} = \cdots = x_{j_l}$ for some subset $\{j_1, \ldots, j_l\} \subseteq \{1, \ldots, s\}$ with $r_{j_1} + \cdots + r_{j_l} = 0$. Otherwise, we say that a solution $\mathbf{x}$ is *non-trivial*. For a finite Abelian group M coprime to $\mathbf{r}$, let $D_{\mathbf{r}}(M)$ denote the maximal cardinality of a set $A \subseteq M$ which contains no non-trivial solution of $r_1x_1 + \cdots + r_sx_s = 0$ with $x_i \in A$ $(1 \leq i \leq s)$. Also, for $n \in \mathbb{N}$, we denote by $d_{\mathbf{r}}(n)$ the supremum of $D_{\mathbf{r}}(M)/|M|$ as M ranges over all finite Abelian groups M with $c(M) \geq n$ and M coprime to $\mathbf{r}$.

We will now state the main result of this chapter.

Theorem 4.1. *Let* $\mathbf{r} = (r_1, \ldots, r_s)$ *be a vector of non-zero integers satisfying* $r_1 + \cdots + r_s = 0$. *There exists an effectively computable constant* $C(\mathbf{r}) > 0$ *such that for* $n \in \mathbb{N}$,

$$d_{\mathbf{r}}(n) \leq \frac{C(\mathbf{r})^{s-2}}{n^{s-2}}.$$

In the following corollary, we provide an application of Theorem 4.1.

Corollary 4.2. *Let* p *be an odd prime and* $q = p^h$ *for some* $h \in \mathbb{N}$. *For* $n \in \mathbb{N}$, *let* $PG(n, q)$ *denote the projective space of dimension* n *over the finite field* $\mathbb{F}_q$ *of* q *elements. For* $v \in \mathbb{N}$ *with* $v > 1$, *let* $\mathcal{M}_v(n, q)$ *denote the maximum cardinality of a set* $A \subseteq PG(n, q)$ *for which no* $(v + 1)$ *points in* A *are linearly dependent over* $\mathbb{F}_q$. *Then, there exists an effectively computable constant* $\tilde{C}(p, v) > 0$ *such that*

$$\mathcal{M}_v(n, q) \leq \frac{\tilde{C}(p, v)}{h^{v-1}} \cdot \sum_{j=1}^{n} \frac{q^j}{j^{v-1}} + 1.$$

Before proving Theorem 4.1 and Corollary 4.2, we introduce the Fourier transform on a finite Abelian group M. Let $\widehat{M}$ denote the character group of M. The *Fourier transform* of a function $g : M \to \mathbb{C}$ is the function $\widehat{g} : \widehat{M} \to \mathbb{C}$ defined by

$$\widehat{g}(\chi) = \sum_{x \in M} g(x)\, \chi(-x).$$

Then, we have *Parseval's identity*,

$$\sum_{\chi \in \widehat{M}} |\widehat{g}(\chi)|^2 = |M| \sum_{x \in M} |g(x)|^2.$$

This chapter is based on the author and Yu-Ru Liu's preliminary manuscript [25].

4.2 Proof of Theorem 4.1

Let $r_1, \ldots, r_s$ be non-zero integers with $r_1 + \cdots + r_s = 0$. For $n \in \mathbb{N}$, let M be a finite Abelian group coprime to $\mathbf{r}$ with $c(M) \geq n$. For convenience, in what follows,

we write $D(M)$ in place of $D_{\mathbf{r}}(M)$ and $d(n)$ in place of $d_{\mathbf{r}}(n)$. For a set $A \subseteq M$, we denote by $T(A) = T_{\mathbf{r}}(A)$ the number of solutions of

$$r_1x_1 + \cdots + r_sx_s = 0$$

with $x_i \in A$ $(1 \le i \le s)$. For $1 \le i \le s$, let $r_iA = \{r_ix \colon x \in A\}$, and let 1_{r_iA} be the characteristic function of r_iA, i.e., $1_{r_iA}(x) = 1$ if $x \in r_iA$ and $1_{r_iA}(x) = 0$ otherwise. Let $f_i = \widehat{1_{r_iA}}$. We note that since M is coprime to $\mathbf{r}$, the map from M to M defined by $x \mapsto r_ix$ is a bijection. Thus, for $\chi \in \widehat{M}$, we have

$$f_i(\chi) = \sum_{x \in M} 1_{r_iA}(x)\chi(-x) = \sum_{x \in A} \chi(-r_ix) \qquad (1 \le i \le s).$$

It follows that

$$\begin{aligned} \sum_{\chi \in \widehat{M}} f_1(\chi)f_2(\chi)\cdots f_s(\chi) &= \sum_{x_1 \in A} \cdots \sum_{x_s \in A} \sum_{\chi \in \widehat{M}} \chi\big(-(r_1x_1 + \cdots + r_sx_s)\big) \\ &= |M|\, T(A). \end{aligned} \tag{4.1}$$

Moreover, we define

$$h(\chi) = \sum_{x \in M} d(n-1)\chi(-x).$$

Hence, $h(\chi) = d(n-1)|M|$ if $\chi = \chi_0$ and $h(\chi) = 0$ otherwise. The function $h(\chi)$ is a good approximation for $f_i(\chi)$. More precisely, we have the following lemma.

Lemma 4.3. *Let M be a finite Abelian group coprime to $\mathbf{r}$ with $c(M) \ge n$. Suppose that $A \subseteq M$ contains no non-trivial solution of $r_1x_1 + \cdots + r_sx_s = 0$ with $x_i \in A$ $(1 \le i \le s)$. Then we have*

$$\sup_{\chi \in \widehat{M}} |h(\chi) - f_i(\chi)| = d(n-1)|M| - |A|.$$

In particular, since $h(\chi) = 0$ for $\chi \ne \chi_0$, it follows that

$$\sup_{\chi \ne \chi_0} \big|f_i(\chi)\big| \le d(n-1)|M| - |A|.$$

Proof. Let $\chi \in \widehat{M}$ and $W = \ker(\chi)$. Since $\chi(M)$ is a cyclic group and $M \cong \chi(M) \oplus W$, we may conclude that $c(W) \geq c(M) - 1 \geq (n-1)$. Note that

$$\operatorname{card}(W) \cdot |h(\chi) - f_i(\chi)| = \left| \sum_{y \in W} \sum_{x \in M} d(n-1)\chi(-x) - \sum_{y \in W} \sum_{x \in M} 1_{r_i A}(x)\chi(-x) \right|.$$

Since $y \in \ker(\chi)$, by a change of variables, we have

$$\sum_{x \in M} 1_{r_i A}(x)\chi(-x) = \sum_{x \in M} 1_{r_i A}(x)\chi(-(x+y)) = \sum_{x \in M} 1_{r_i A}(x-y)\chi(-x).$$

Hence, it follows that

$$\begin{aligned} \operatorname{card}(W) \cdot |h(\chi) - f_i(\chi)| &= \left| \sum_{x \in M} \left(\sum_{y \in W} d(n-1) - \sum_{y \in W} 1_{r_i A}(x-y) \right) \chi(-x) \right| \\ &\leq \sum_{x \in M} \left| \sum_{y \in W} d(n-1) - \sum_{y \in W} 1_{r_i A}(x-y) \right| \\ &= \sum_{x \in M} \Big| d(n-1) \cdot \operatorname{card}(W) - \operatorname{card}\big(W \cap (x - r_i A)\big) \Big|. \end{aligned}$$

We note that since A contains no non-trivial solution of $r_1 x_1 + \cdots + r_s x_s = 0$ with $x_i \in A$ $(1 \leq i \leq s)$, the set $W \cap (x - r_i A)$ also contains no non-trivial solution of the same equation. Furthermore, the fact that M is coprime to $\mathbf{r}$ implies that W is coprime to $\mathbf{r}$. Since $c(W) \geq (n-1)$, we have $\operatorname{card}\big(W \cap (x - r_i A)\big) \leq d(n-1) \cdot \operatorname{card}(W)$. We may conclude that

$$\begin{aligned} \operatorname{card}(W) \cdot |h(\chi) - f_i(\chi)| &\leq \sum_{x \in M} \Big(d(n-1) \cdot \operatorname{card}(W) - \operatorname{card}\big(W \cap (x - r_i A)\big) \Big) \\ &= d(n-1) \cdot \operatorname{card}(W) \cdot \operatorname{card}(M) - \operatorname{card}(W) \cdot \operatorname{card}(A). \end{aligned}$$

Hence, we have

$$|h(\chi) - f_i(\chi)| \leq d(n-1)|M| - |A|.$$

We note that for $\chi = \chi_0$, one has

$$|h(\chi_0) - f_i(\chi_0)| = d(n-1)|M| - |A|.$$

This completes the proof of the lemma. $\square$

Now, we are ready to prove Theorem 4.1.

Proof. (of Theorem 4.1) Let M be a finite Abelian group coprime to $\mathbf{r}$ with $c(M) \geq n$. Suppose that $A \subseteq M$ contains no non-trivial solution of $r_1x_1 + \cdots + r_sx_s = 0$ with $x_i \in A$ $(1 \leq i \leq s)$. Furthermore, let $d^*(n) = |A|/|M|$.

By (4.1), we have

$$\begin{aligned} |M|\,T(A) &= \sum_{\chi \in \widehat{M}} f_1(\chi) f_2(\chi) \cdots f_s(\chi) \\ &= f_1(\chi_0) f_2(\chi_0) \cdots f_s(\chi_0) + \sum_{\chi \neq \chi_0} f_1(\chi) f_2(\chi) \cdots f_s(\chi). \end{aligned} \tag{4.2}$$

We note that

$$f_1(\chi_0) f_2(\chi_0) \cdots f_s(\chi_0) = |A|^s = d^*(n)^s |M|^s. \tag{4.3}$$

Also, by Cauchy's inequality and Lemma 4.3, we have

$$\begin{aligned} &\Big| \sum_{\chi \neq \chi_0} f_1(\chi) f_2(\chi) \cdots f_s(\chi) \Big| \\ &\leq \sup_{\chi \neq \chi_0} \big| f_3(\chi) \cdots f_s(\chi) \big| \left(\sum_{\chi \neq \chi_0} |f_1(\chi)|^2 \right)^{1/2} \left(\sum_{\chi \neq \chi_0} |f_2(\chi)|^2 \right)^{1/2} \\ &\leq \big(d(n-1) - d^*(n) \big)^{s-2} |M|^{s-2} \left(\sum_{\chi \in \widehat{M}} |f_1(\chi)|^2 \right)^{1/2} \left(\sum_{\chi \in \widehat{M}} |f_2(\chi)|^2 \right)^{1/2}. \end{aligned}$$

By Parseval's identity,

$$\sum_{\chi \in \widehat{M}} |f_1(\chi)|^2 = |M| \sum_{x \in M} |1_{r_1 A}(x)|^2 = |M||A|.$$

The same equality also holds if we replace f_1 by f_2. Thus, from the above estimates, we have

$$\Big| \sum_{\chi \neq \chi_0} f_1(\chi) f_2(\chi) \cdots f_s(\chi) \Big| \leq d^*(n) \big(d(n-1) - d^*(n) \big)^{s-2} |M|^s. \tag{4.4}$$

By combining (4.2), (4.3), and (4.4), it follows that

$$\begin{aligned} T(A) &\geq \frac{1}{|M|} f_1(\chi_0) f_2(\chi_0) \cdots f_s(\chi_0) - \frac{1}{|M|} \left| \sum_{\chi \neq \chi_0} f_1(\chi) f_2(\chi) \cdots f_s(\chi) \right| \\ &\geq \left(d^*(n)^s - d^*(n) \left(d(n-1) - d^*(n) \right)^{s-2} \right) |M|^{s-1}. \end{aligned}$$

Since A contains no non-trivial solution of $r_1 x_1 + \cdots + r_s x_s = 0$ with $x_i \in A$ $(1 \leq i \leq s)$, there exists a constant $B = B(\mathbf{r})$ such that

$$T(A) \leq B|A|^{s-2} = B d^*(n)^{s-2} |M|^{s-2}.$$

Combining the above two estimates, we have

$$d^*(n)^s - B d^*(n)^{s-2} |M|^{-1} - d^*(n) \big(d(n-1) - d^*(n) \big)^{s-2} \leq 0. \tag{4.5}$$

We now claim that there exists a constant $C = C(\mathbf{r}) \geq 1$ such that for all $n \in \mathbb{N}$,

$$d(n) \leq \frac{C^{s-2}}{n^{s-2}}. \tag{4.6}$$

This statement follows by induction on n. Since $d(n) \leq 1$, the cases where $n \leq C$ hold trivially. Let $n > C$, and suppose that $d(n-1) \leq C^{s-2}(n-1)^{2-s}$. We now verify that $d^*(n) \leq C^{s-2} n^{2-s}$, and since this inequality holds for any valid choice of A and M, we may conclude that $d(n) \leq C^{s-2} n^{2-s}$. Let F be any real number with $F > 1$. We split the proof into two cases:

(1) Suppose that $d^*(n)^2 \leq FB|M|^{-1}$. Since $|M| \geq 2^n$, we have $d^*(n) \leq (FB2^{-n})^{1/2}$. Hence, if $(FB2^{-m})^{1/2} m^{s-2} \leq C^{s-2}$ for all $m > C$, one has that $d^*(n) \leq C^{s-2} n^{2-s}$. For $m > 0$, the function $2^{-m/2} m^{s-2}$ obtains its global maximum of $(2s-4)^{s-2} (e \log 2)^{2-s}$ when $m = (2s-4)/\log 2$. Therefore, this case follows provided that

$$C \geq (FB)^{1/(2s-4)} \left(\frac{2s-4}{e \log 2} \right).$$

(2) Suppose that $d^*(n)^2 > FB|M|^{-1}$. Since $F^{-1}d^*(n)^s > Bd^*(n)^{s-2}|M|^{-1}$, by (4.5), we have

$$(1-F^{-1})d^*(n)^s < d^*(n)(d(n-1)-d^*(n))^{s-2}.$$

Let $E = E(F)$ be the unique positive number satisfying $E^{s-2} = (1-F^{-1})$. By the induction hypothesis for $d(n-1)$, the above inequality implies that

$$Ed^*(n)^{\frac{s-1}{s-2}} + d^*(n) < d(n-1) \leq \frac{C^{s-2}}{(n-1)^{s-2}}.$$

Since $Ex^{\frac{s-1}{s-2}} + x$ is an increasing function of x, to prove that $d^*(n) \leq C^{s-2}n^{s-2}$, it suffices to show that

$$\frac{C^{s-2}}{(n-1)^{s-2}} \leq E\left(\frac{C^{s-2}}{n^{s-2}}\right)^{\frac{s-1}{s-2}} + \frac{C^{s-2}}{n^{s-2}}.$$

We note that the above inequality is equivalent to

$$\frac{n^{s-1}}{(n-1)^{s-2}} - n \leq CE. \tag{4.7}$$

For $m > 1$,

$$\frac{m^{s-1}}{(m-1)^{s-2}} - m$$

is a decreasing function of m. Since $n > C$, to prove (4.7), it is enough to show that

$$\frac{C^{s-1}}{(C-1)^{s-2}} - C \leq CE.$$

The above inequality is satisfied whenever

$$C \geq \frac{(E+1)^{1/(s-2)}}{(E+1)^{1/(s-2)}-1}.$$

Hence, provided that C is large enough in terms of $\mathbf{r}$, it follows by induction that (4.6) holds for all $n \in \mathbb{N}$. This completes the proof of Theorem 4.1. □

Remark 4.4. We see from the above proof that our constant $C = C(\mathbf{r})$ can be computed explicitly. For any value of E such that $0 < E < 1$, we may choose C to be

$$\max\left\{\left(\frac{B}{1-E^{s-2}}\right)^{1/(2s-4)}\left(\frac{2s-4}{e\log 2}\right),\ \frac{(E+1)^{1/(s-2)}}{(E+1)^{1/(s-2)}-1}\right\},$$

where $B = B(\mathbf{r})$ is chosen as in the proof of Theorem 1. For any choice of $\mathbf{r} = (r_1, \ldots, r_s)$, one can numerically choose E to minimize the above expression. We note that

$$\lim_{s\to\infty}\left(\frac{(E+1)^{1/(s-2)}}{(E+1)^{1/(s-2)}-1} - \frac{s-2}{\log(E+1)} - \frac{1}{2}\right) = 0.$$

Thus, for fixed B, the constant C can be chosen in such a way that it grows like a linear function in s.

Remark 4.5. If the vector $\mathbf{r} = (r_1, \ldots, r_s) \in \mathbb{Z}^s$ satisfies the condition that there is no proper subset $\{j_1, \ldots, j_l\} \subsetneq \{1, \ldots, s\}$ with $r_{j_1} + \cdots + r_{j_l} = 0$, then a solution $\mathbf{x} = (x_1, \ldots, x_s) \in A^s$ is trivial if and only if $x_1 = \cdots = x_s$. Hence, $T(A) = |A|$, and in place of (4.5), we obtain the inequality

$$d^*(n)^s - d^*(n)|M|^{2-s} - d^*(n)\big(d(n-1) - d^*(n)\big)^{s-2} \leq 0.$$

By an argument similar to the proof of Theorem 4.1, for any value of E such that $0 < E < 1$, we may choose C to be

$$\max\left\{\left(\frac{1}{1-E^{s-2}}\right)^{\frac{1}{(s-1)(s-2)}}\left(\frac{s-1}{e\log 2}\right),\ \frac{(E+1)^{1/(s-2)}}{(E+1)^{1/(s-2)}-1}\right\}.$$

We note that in this case, the constant C depends only on s. Moreover, we can change the constant E as n varies in our proof, i.e., $E = E(n)$ can be chosen to be a function of n. Table 4.1 lists valid choices of $C(s)$ for small values of s.

Remark 4.6. One can also optimize the choice of $C = C(\mathbf{r})$ by utilizing the inequality in (4.5) directly. Consider the special case that $\mathbf{r} = (1, -2, 1)$ and G is a finite Abelian

Table 4.1: Values of the Constant $C(s)$ in Remark 4.5

s	3	4	5	6	7	8	9	10	11
$C(s)$	2.050	3.138	4.766	6	7.598	9	10.436	12	13.277

group of odd order with $c(G) \geq n$. Since a solution $\mathbf{x} = (x_1, x_2, x_3)$ is trivial if and only if $x_1 = x_2 = x_3$, we can take $B(\mathbf{r}) = 1$ in this case. Since $|G| \geq 3^n$, by (4.5), we have

$$d^*(n)^2 + d^*(n) - 3^{-n} \leq d(n-1).$$

We note that for $n \geq 3$,

$$\frac{2}{n-1} \leq \left(\frac{2}{n}\right)^2 + \frac{2}{n} - 3^{-n}.$$

Since $x^2 + x - 3^{-n}$ is an increasing function of x, by induction, we can show that $d(n) \leq 2/n$ for all $n \in \mathbb{N}$. In other words, when $\mathbf{r} = (1, -2, 1)$, we can take $C(\mathbf{r}) = 2$.

4.3 Proof of Corollary 4.2

Let p be an odd prime and $q = p^h$ for some $h \in \mathbb{N}$. For $n \in \mathbb{N}$, let $PG(n, q)$ denote the projective space of dimension n over $\mathbb{F}_q$. For $v \in \mathbb{N}$ with $v > 1$, define $\mathcal{M}_v(n, q)$ to be the maximum cardinality of a set $A \subseteq PG(n, q)$ for which no $(v+1)$ points in A are linearly dependent over $\mathbb{F}_q$. We can similarly define $\widetilde{\mathcal{M}}_v(n, q)$ as the maximum cardinality of a set $B \subseteq \mathbb{F}_q^n \oplus \{1\} \subseteq PG(n, q)$ for which no $(v+1)$ points in B are linearly dependent over $\mathbb{F}_q$.

Corollary 4.7. *There exists an effectively computable constant $\tilde{C}(p, v) > 0$ such that*

$$\widetilde{\mathcal{M}}_v(n, q) \leq \frac{\tilde{C}(p, v) q^n}{(nh)^{v-1}}.$$

Proof. Let $r_1, \ldots, r_{v-1}$ be any integers that are not divisible by p. Since $p \geq 3$, there exists an $r_v \in \mathbb{Z}$ such that $p \nmid r_v$ and $r_1 + \cdots + r_v \not\equiv 0 \pmod{p}$. By taking $r_{v+1} = -(r_1 + \cdots + r_v)$, we have shown that there exists a vector $\mathbf{r} = (r_1, \ldots, r_{v+1})$ of integers not divisible by p that satisfies $r_1 + \cdots + r_{v+1} = 0$.

Suppose that $B \subseteq \mathbb{F}_q^n \oplus \{1\}$ and no $(v+1)$ points in B are linearly dependent over $\mathbb{F}_q$. Let $\mathbf{r} = (r_1, \ldots, r_{v+1})$ be a vector of integers not divisible by p that satisfies $r_1 + \cdots + r_{v+1} = 0$. If B contains a non-trivial solution of $r_1x_1 + \cdots + r_{v+1}x_{v+1} = 0$ with $x_i \in B$ $(1 \leq i \leq v+1)$, then there are $(v+1)$ points in B that are linearly dependent over $\mathbb{F}_q$. Hence, by viewing $\mathbb{F}_q^n$ as a finite Abelian group with nh constituents, we can derive from Theorem 4.1 that

$$\widetilde{\mathcal{M}}_v(n,q) \leq \frac{C(\mathbf{r})^{v-1}\, q^n}{(nh)^{v-1}}. \tag{4.8}$$

Define

$$\tilde{C}(p,v) = \inf_{\mathbf{r}} \left\{C(\mathbf{r})^{v-1}\right\},$$

where $\mathbf{r}$ runs through all vectors $(r_1, \ldots, r_{v+1})$ of integers not divisible by p with $r_1 + \cdots + r_{v+1} = 0$. Then, by (4.8), the corollary follows. □

We are now ready to prove Corollary 4.2, which states that

$$\mathcal{M}_v(n,q) \leq \frac{\tilde{C}(p,v)}{h^{v-1}} \cdot \sum_{j=1}^{n} \frac{q^j}{j^{v-1}} + 1.$$

Proof. (of Corollary 4.2) We note that an element of $PG(n,q)$ can be written either as $(y,1)$ with $y \in \mathbb{F}_q^n$ or as $(z,0)$ with $z \in PG(n-1,q)$. Thus, for $n \geq 1$, we have

$$\mathcal{M}_v(n,q) \leq \widetilde{\mathcal{M}}_v(n,q) + \mathcal{M}_v(n-1,q). \tag{4.9}$$

We note that

$$\mathcal{M}_v(1,q) \leq \widetilde{\mathcal{M}}_v(1,q) + 1. \tag{4.10}$$

By (4.9), (4.10), and Corollary 4.7, we have

$$\mathcal{M}_v(n,q) \leq \sum_{j=1}^{n} \widetilde{\mathcal{M}}_v(j,q) + 1 \leq \frac{\tilde{C}(p,v)}{h^{v-1}} \cdot \sum_{j=1}^{n} \frac{q^j}{j^{v-1}} + 1.$$

The corollary now follows. □

CHAPTER V

The Manin Conjecture for $x_0y_0 + \cdots + x_sy_s = 0$

5.1 Overview

We consider the variety defined by $x_0y_0 + \cdots + x_sy_s = 0$ in $\mathbb{P}^s(\mathbb{Q}) \times \mathbb{P}^s(\mathbb{Q})$. This is a flag variety with anticanonical height function

$$H(\mathbf{x}, \mathbf{y}) = \max_{0 \le i,j \le s} |x_i y_j|^s, \tag{5.1}$$

where we choose representatives $\mathbf{x} = (x_0, \ldots, x_s) \in \mathbb{Z}^{s+1}$ and $\mathbf{y} = (y_0, \ldots, y_s) \in \mathbb{Z}^{s+1}$ with $\gcd(x_0, \ldots, x_s) = \gcd(y_0, \ldots, y_s) = 1$. Let

$$N(B) = \#\{(\mathbf{x}, \mathbf{y}) \in \mathbb{P}^s(\mathbb{Q}) \times \mathbb{P}^s(\mathbb{Q}) \,:\, \mathbf{x} \cdot \mathbf{y} = 0,\ x_0 \cdots x_s y_0 \cdots y_s \neq 0, \tag{5.2}$$
$$\text{and } H(\mathbf{x}, \mathbf{y}) < B\}.$$

For the variety $x_0y_0 + \cdots + x_sy_s = 0$, the Manin conjecture predicts that $N(B) \sim \kappa B \log B$, where κ is a constant.

We first need to define some notation. Let $\mathbf{x} = (x_0, \ldots, x_s)$ and $\mathbf{y} = (y_0, \ldots, y_s)$ be vectors lying in $\mathbb{R}^{s+1}$. For the sake of concision, we write $\mathbf{x}_i$ for $(x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_s)$ and likewise $\mathbf{y}_i$ for $(y_0, \ldots, y_{i-1}, y_{i+1}, \ldots, y_s)$. Furthermore, for any vector $\mathbf{u}$, we define $\|\mathbf{u}\|_\infty = \max |u_i|$, where the maximum is taken over all components u_i of $\mathbf{u}$. Let

$$\mathcal{X}_1 = \{(\mathbf{x}_0, \mathbf{y}_0) \in \mathbf{R}^{2s} \,:\, \|\mathbf{x}_0\|_\infty \le 1,\ \|\mathbf{y}_0\|_\infty \le 1, \text{ and } |\mathbf{x}_0 \cdot \mathbf{y}_0| \le 1\}.$$

We define the *local density at infinity* to be

$$\sigma_\infty = \int_{\mathcal{X}_1} d\mathbf{x}_0\, d\mathbf{y}_0, \tag{5.3}$$

and the *singular series* to be

$$\mathfrak{S} = \sum_{q=1}^{\infty} \frac{\phi(q)}{q^{s+1}}.$$

Note that for $s \geq 2$, we have $\mathfrak{S} \ll 1$.

In this chapter, we prove the following theorem.

Theorem 5.1. *For $s \geq 2$ and $B \geq 2$, we have*

$$N(B) = \left(\frac{s+1}{2s}\right) \zeta(s)^{-2} \sigma_\infty \mathfrak{S} B \log B + O(B).$$

Let

$$\mathcal{W} = \{(\mathbf{x}, \mathbf{y}) \in (\mathbb{Z} \setminus \{0\})^{2s+2} \,:\, y_0 > 0,\ \|\mathbf{y}\|_\infty \leq y_0 \leq B^{1/2}, \text{ and } \|\mathbf{x}\|_\infty \leq B/y_0\}$$

and

$$N_0(B) = \#\{(\mathbf{x}, \mathbf{y}) \in \mathcal{W} \,:\, \mathbf{x} \cdot \mathbf{y} = 0\}.$$

In order to verify Theorem 5.1, we prove the following theorem.

Theorem 5.2. *For $s \geq 2$ and $B \geq 2$, one has*

$$N_0(B) = \frac{1}{2} \sigma_\infty \mathfrak{S} B^s \log B + O(B^s).$$

Let $e(\alpha) = \exp(2\pi\alpha)$ and

$$\mathcal{F}(\alpha) = \sum_{(\mathbf{x},\mathbf{y}) \in \mathcal{W}} e(\alpha \mathbf{x} \cdot \mathbf{y}). \tag{5.4}$$

Let $\delta > 0$ be a small positive constant with $\delta < 1/10$, and let $Q = B^\delta$. We define

$$\mathfrak{M}(a, q) = \{\alpha \in \mathbb{R} : |\alpha - a/q| \leq B^{-1} Q\}.$$

The *major arcs* are defined to be

$$\mathfrak{M} = \bigcup_{\substack{1 \le a \le q \le Q \\ (a,q)=1}} \mathfrak{M}(a,q),$$

and the *minor arcs* are

$$\mathfrak{m} = \left[B^{-1}Q, 1 + B^{-1}Q\right) \setminus \mathfrak{M}.$$

Note that when $1 \le a_1 \le q_1 \le Q$ and $1 \le a_2 \le q_2 \le Q$ with $(a_1, q_1) = (a_2, q_2) = 1$, we have $\mathfrak{M}(a_1, q_1) \cap \mathfrak{M}(a_2, q_2) \neq \emptyset$ if and only if $a_1 = a_2$ and $q_1 = q_2$. Thus, the major arcs $\mathfrak{M}(a, q)$ that constitute $\mathfrak{M}$ are disjoint. Since

$$\int_{\mathbb{T}} e(\alpha n)\, d\alpha = \begin{cases} 1, & \text{when } n = 0, \\ 0, & \text{when } n \in \mathbb{Z}\backslash\{0\}, \end{cases}$$

where $\mathbb{T} = [0, 1)$, we have

$$N_0(B) = \int_{B^{-1}Q}^{1+B^{-1}Q} \mathcal{F}(\alpha)\, d\alpha.$$

In order to prove Theorem 5.2, it now suffices to demonstrate that for $B \ge 2$, one has

$$\int_{\mathfrak{m}} \mathcal{F}(\alpha)\, d\alpha = O(B^{s+\epsilon}Q^{-1}) \tag{5.5}$$

and

$$\int_{\mathfrak{M}} \mathcal{F}(\alpha)\, d\alpha = \frac{1}{2}\sigma_\infty \mathfrak{S} B^s \log B + O(B^s). \tag{5.6}$$

We prove (5.5) in Section 5.2 and (5.6) in Section 5.3. In Section 5.4, we derive Theorem 5.1 from Theorem 5.2.

This chapter is based on the author's preliminary manuscript [36].

5.2 The Minor Arcs

Our goal for this section is to prove (5.5). We first record a reciprocal sum estimate and a version of Hua's inequality. In this section, we write $\|\alpha\|$ for the fractional part of α.

Lemma 5.3. *Suppose that X and Y are real numbers with $X \geq 1$ and $Y \geq 1$. Also, suppose that $a \in \mathbb{Z}$, $q \in \mathbb{N}$, and $\alpha \in \mathbb{R}$ satisfy $|\alpha - a/q| \leq q^{-2}$ and $(a,q) = 1$. Then,*

$$\sum_{1 \leq y \leq Y} \min\Big(\frac{XY}{y}, \|\alpha y\|^{-1}\Big) \ll XY\Big(\frac{1}{q} + \frac{1}{X} + \frac{q}{XY}\Big)\log(2Yq).$$

Proof. See [44, Lemma 2.2]. □

Lemma 5.4. *One has*

$$\#\{(x,x',y,y') \in \mathbb{Z}^4 \,:\, 1 \leq |xy| = |x'y'| \leq B\} \ll B^{1+\epsilon}. \tag{5.7}$$

Proof. For a natural number n, let $\tau_2(n)$ denote the number of positive integers that divide n. A standard divisor function estimate (see, for example, the argument on page 10 of [7]) shows that $\tau_2(n) \ll n^{\epsilon}$, and hence,

$$\begin{aligned}\#\{(x,x',y,y') \in \mathbb{Z}^4 \,:\, 1 \leq |xy| = |x'y'| \leq B\} &\ll \sum_{1 \leq n \leq B} (\tau_2(n))^2 \\ &\ll \sum_{1 \leq n \leq B} n^{\epsilon} \ll B^{1+\epsilon}.\end{aligned}$$

□

With greater effort, in fact, one may obtain an upper bound for the left hand side of (5.7) of the shape $O(B\big(\log B)^3\big)$ (see [21, Lemma 2.5]). We are now in a position to show that the minor arc contribution is $O(B^{s+\epsilon}Q^{-1})$, thereby confirming (5.5). One difficulty that arises in the proof is that $\mathcal{F}(\alpha)$ does not naturally break apart into a product of s exponential sums owing to dependencies on y_0. In order to get around this, we employ a standard argument from the theory of Fourier analysis

to de-interlace the pairs (x_i, y_i) (see the appendix due to Montgomery in [48]). We define

$$g(\alpha, \gamma, \eta) = \sum_{\substack{x,y \\ 1 \le |xy| \le B}} e(\alpha xy - \gamma x - \eta y).$$

Let

$$D_R(\gamma) = \sum_{1 \le |z| \le R} e(\gamma z),$$

and note that for positive real numbers R and S with $RS \le B$, we have

$$\int_{\mathbb{T}^2} g(\alpha, \gamma, \eta) D_R(\gamma) D_S(\eta)\, d\gamma\, d\eta = \sum_{\substack{1 \le |x| \le R \\ 1 \le |y| \le S}} e(\alpha xy). \tag{5.8}$$

Lemma 5.5. *For $s \ge 2$, one has*

$$\int_{\mathfrak{m}} \mathcal{F}(\alpha)\, d\alpha = O(B^{s+\epsilon} Q^{-1}).$$

Proof. Denote by $\boldsymbol{\gamma} = (\gamma_1, \dots, \gamma_s)$ and $\boldsymbol{\eta} = (\eta_1, \dots, \eta_s)$ vectors lying in $\mathbb{T}^s$. Let

$$\mathcal{G}(\alpha, \boldsymbol{\gamma}, \boldsymbol{\eta}) = \sum_{\substack{1 \le y_0 \le B^{1/2} \\ 1 \le |x_0| \le B/y_0}} e(\alpha x_0 y_0) \prod_{i=1}^{s} g(\alpha, \gamma_i, \eta_i) D_{y_0}(\gamma_i) D_{B/y_0}(\eta_i).$$

By using (5.8), we are able to rewrite $\mathcal{F}(\alpha)$ as

$$\mathcal{F}(\alpha) = \int_{\mathbb{T}^s} \int_{\mathbb{T}^s} \mathcal{G}(\alpha, \boldsymbol{\gamma}, \boldsymbol{\eta})\, d\boldsymbol{\gamma}\, d\boldsymbol{\eta}. \tag{5.9}$$

Let

$$\mathcal{C} = \left[B^{-2s-2}, 1 - B^{-2s-2}\right]^s.$$

Using trivial estimates, we find that

$$g(\alpha, \gamma, \eta) \ll \sum_{\substack{x,y \\ 1 \le |xy| \le B}} 1 \ll \sum_{1 \le y \le B} B/y \ll B \log B \tag{5.10}$$

and

$$D_{y_0}(\gamma) D_{B/y_0}(\eta) \ll y_0(B/y_0) = B$$

uniformly in α, γ, and η. Hence, we have

$$\mathcal{G}(\alpha, \boldsymbol{\gamma}, \boldsymbol{\eta}) \ll B^{2s+1}(\log B)^{s+1} \ll B^{2s+2} \tag{5.11}$$

uniformly in α, $\boldsymbol{\gamma}$, and $\boldsymbol{\eta}$. The measure of $(\mathbb{T}^s \times \mathbb{T}^s) \setminus (\mathcal{C} \times \mathcal{C})$ equals the volume of the boundary shell, which is $O(B^{-2s-2})$. Hence, together with (5.9) and (5.11), we obtain

$$\int_{\mathfrak{m}} \mathcal{F}(\alpha)\, d\alpha = \int_{\mathfrak{m}} \int_{\mathcal{C}} \int_{\mathcal{C}} \mathcal{G}(\alpha, \boldsymbol{\gamma}, \boldsymbol{\eta})\, d\boldsymbol{\gamma}\, d\boldsymbol{\eta}\, d\alpha + O(1). \tag{5.12}$$

When $\gamma \notin \mathbb{Z}$ and $R \geq 1$, one finds by summing the geometric progressions that

$$D_R(\gamma) = \frac{e(\gamma) - e(\lfloor R+1 \rfloor \gamma) + e(-\lfloor R \rfloor \gamma) - 1}{1 - e(\gamma)}. \tag{5.13}$$

Let

$$\mathbf{D}^*(\boldsymbol{\gamma}, \boldsymbol{\eta}) = \prod_{i=1}^{s} \left(\frac{1}{1 - e(\gamma_i)} \right) \left(\frac{1}{1 - e(\eta_i)} \right).$$

By applying (5.13), we find that there exists a complex number $\rho(B, y_0, \boldsymbol{\gamma}, \boldsymbol{\eta})$, independent of x_0 and of modulus at most 4^{2s}, such that

$$\prod_{i=1}^{s} D_{y_0}(\gamma_i) D_{B/y_0}(\eta_i) = \rho(B, y_0, \boldsymbol{\gamma}, \boldsymbol{\eta}) \mathbf{D}^*(\boldsymbol{\gamma}, \boldsymbol{\eta}) \tag{5.14}$$

for all $(\boldsymbol{\gamma}, \boldsymbol{\eta}) \in \mathcal{C}^2$. Hence, for all $(\boldsymbol{\gamma}, \boldsymbol{\eta}) \in \mathcal{C}^2$, we may write

$$\mathcal{G}(\alpha, \boldsymbol{\gamma}, \boldsymbol{\eta}) = \mathbf{D}^*(\boldsymbol{\gamma}, \boldsymbol{\eta}) h(\alpha, B, \boldsymbol{\gamma}, \boldsymbol{\eta}) \left(\prod_{j=1}^{s} g(\alpha, \gamma_j, \eta_j) \right), \tag{5.15}$$

where

$$h(\alpha, B, \boldsymbol{\gamma}, \boldsymbol{\eta}) = \sum_{1 \leq y_0 \leq B^{1/2}} \rho(B, y_0, \boldsymbol{\gamma}, \boldsymbol{\eta}) \sum_{1 \leq |x_0| \leq B/y_0} e(\alpha x_0 y_0).$$

By the triangle inequality, we find that

$$\begin{aligned} h(\alpha, B, \boldsymbol{\gamma}, \boldsymbol{\eta}) &\leq 4^{2s} \sum_{1 \leq y_0 \leq B^{1/2}} \left| \sum_{1 \leq |x_0| \leq B/y_0} e(\alpha x_0 y_0) \right| \\ &\ll \sum_{1 \leq y_0 \leq B^{1/2}} \max\left(B/y_0, \|\alpha y_0\|^{-1} \right) \end{aligned}$$

uniformly in $\boldsymbol{\gamma}$ and $\boldsymbol{\eta}$. By Dirichlet's approximation theorem, for every $\alpha \in \mathbb{R}$, there exist elements $a, q \in \mathbb{Z}$ such that $1 \leq q \leq BQ^{-1}$, $(a,q) = 1$, and $|\alpha - a/q| < q^{-1}B^{-1}Q$. If $\alpha \in \mathfrak{m}$, for such a choice of a and q, we must have that $q > Q$ and $|\alpha - a/q| < q^{-1}B^{-1}Q \leq q^{-2}$. Therefore, an application of Lemma 5.3 with $X = Y = B^{1/2}$ implies that

$$h(\alpha, B, \boldsymbol{\gamma}, \boldsymbol{\eta}) \ll BQ^{-1} \log B \tag{5.16}$$

uniformly in $\boldsymbol{\gamma}, \boldsymbol{\eta}$, and $\alpha \in \mathfrak{m}$. From (5.10), (5.15), and (5.16), we may conclude that

$$\begin{aligned} &\int_{\mathfrak{m}} \int_{\mathcal{C}} \int_{\mathcal{C}} \mathcal{G}(\alpha, \boldsymbol{\gamma}, \boldsymbol{\eta})\, d\boldsymbol{\gamma}\, d\boldsymbol{\eta}\, d\alpha \\ &\ll B^{s-1}Q^{-1}(\log B)^{s-1} \int_{\mathcal{C}} \int_{\mathcal{C}} \big|\mathbf{D}^*(\boldsymbol{\gamma}, \boldsymbol{\eta})\big| \int_{\mathfrak{m}} \prod_{j=1}^{2} |g(\alpha, \gamma_j, \eta_j)|\, d\alpha\, d\boldsymbol{\gamma}\, d\boldsymbol{\eta}. \end{aligned} \tag{5.17}$$

On making use of orthogonality, it follows from Lemma 5.4 that

$$\int_{\mathbb{T}} |g(\alpha, \gamma, \eta)|^2\, d\alpha \ll \sum_{\substack{x,x',y,y' \\ 1 \leq |xy| = |x'y'| \leq B}} 1 \ll B^{1+\epsilon}.$$

Hence, by Schwarz's inequality, we find that

$$\int_{\mathfrak{m}} \prod_{j=1}^{2} |g(\alpha, \gamma_j, \eta_j)|\, d\alpha \leq \prod_{j=1}^{2} \Big(\int_{\mathbb{T}} |g(\alpha, \gamma_j, \eta_j)|^2\, d\alpha \Big)^{1/2} \ll B^{1+\epsilon}.$$

From (5.17), we now have that

$$\int_{\mathfrak{m}} \int_{\mathcal{C}} \int_{\mathcal{C}} \mathcal{G}(\alpha, \boldsymbol{\gamma}, \boldsymbol{\eta})\, d\boldsymbol{\gamma}\, d\boldsymbol{\eta}\, d\alpha \ll B^{s+\epsilon}Q^{-1} \int_{\mathcal{C}} \int_{\mathcal{C}} \big|\mathbf{D}^*(\boldsymbol{\gamma}, \boldsymbol{\eta})\big|\, d\boldsymbol{\gamma}\, d\boldsymbol{\eta}. \tag{5.18}$$

Observe that

$$\int_{B^{-2s-2}}^{1-B^{-2s-2}} \frac{d\beta}{1 - e(\beta)} \ll \int_{B^{-2s-2}}^{1-B^{-2s-2}} \frac{d\beta}{\|\beta\|} \ll \log B,$$

which implies that

$$\int_{\mathcal{C}} \int_{\mathcal{C}} \big|\mathbf{D}^*(\boldsymbol{\gamma}, \boldsymbol{\eta})\big|\, d\boldsymbol{\gamma}\, d\boldsymbol{\eta} \ll (\log B)^{2s} \ll B^{\epsilon}. \tag{5.19}$$

Combining (5.12), (5.18), and (5.19) yields the upper bound

$$\int_{\mathfrak{m}} \mathcal{F}(\alpha)\, d\alpha \ll B^{s+\epsilon} Q^{-1}.$$

This completes the proof of the lemma. □

5.3 The Major Arcs

In order to prove (5.6), we first prove an auxiliary lemma. Throughout this section, when $\alpha \in \mathfrak{M}(a,q)$, we write $\beta = \alpha - a/q$.

Lemma 5.6. *When $\alpha \in \mathfrak{M}(a,q)$, $y \in \mathbb{Z}$, and $X \geq 1$, we have*

$$\sum_{1 \leq |x| \leq X} e(\alpha x y) = q^{-1} \sum_{u=1}^{q} e\left(\frac{a}{q} u y\right) \int_{-X}^{X} e(\beta x y)\, dx + O(q(1 + |\beta| X y)).$$

Proof. By splitting the sum into arithmetic progressions modulo q, we have

$$\begin{aligned}
\sum_{1 \leq |x| \leq X} e(\alpha x y) &= \sum_{u=1}^{q} e\left(\frac{a}{q} u y\right) \sum_{\substack{|x| \leq X \\ x \equiv u \pmod q}} e(\beta x y) + O(1) \\
&= \sum_{u=1}^{q} e\left(\frac{a}{q} u y\right) \sum_{\substack{r \in \mathbb{Z} \\ |qr+u| \leq X}} e(\beta (qr+u) y) + O(1) \qquad (5.20) \\
&= \sum_{u=1}^{q} e\left(\frac{a}{q} u y\right) \sum_{q^{-1}(-X-u) \leq r \leq q^{-1}(X-u)} e(\beta (qr+u) y) + O(1).
\end{aligned}$$

The inner sum may be replaced with an integral by noting that from the mean value theorem,

$$\begin{aligned}
\sum_{q^{-1}(-X-u) \leq r \leq q^{-1}(-X-u)} e(\beta (qr+u) y) &= \int_{(-X-u)/q}^{(X-u)/q} e(\beta (qr+u) y)\, dr \\
&\quad + O\Big(1 + q^{-1} X \max_{q^{-1}(-X-u) \leq r \leq q^{-1}(X-u)} |\beta q y|\Big) \\
&= q^{-1} \int_{-X}^{X} e(\beta x y)\, dx + O(1 + |\beta X y|).
\end{aligned}$$

Therefore, we may conclude from (5.20) that

$$\sum_{1 \leq |x| \leq X} e(\alpha x y) = q^{-1} \sum_{u=1}^{q} e\left(\frac{a}{q} u y\right) \int_{-X}^{X} e(\beta x y)\, dx + O\big(q(1 + |\beta X y|)\big).$$ □

Define

$$\mathcal{V}_1 = \{\mathbf{y} \in \mathbb{Z}^{s+1} \,:\, 1 \le |y_1|, \dots, |y_s| \le y_0 \le B^{1/2}\}$$

and

$$\mathcal{X}_2 = \{\mathbf{x} \in \mathbb{R}^{s+1} \,:\, \|\mathbf{x}\|_\infty \le B/y_0\}.$$

Let

$$S(a, q, \mathbf{y}) = \sum_{\mathbf{x} \,(\mathrm{mod}\, q)} \left(\frac{a}{q}\mathbf{x} \cdot \mathbf{y}\right) \tag{5.21}$$

and

$$T(\mathbf{y}) = \int_{-B^{-1}Q}^{B^{-1}Q} \int_{\mathcal{X}_2} e(\beta \mathbf{x} \cdot \mathbf{y})\, d\mathbf{x}\, d\beta. \tag{5.22}$$

Lemma 5.7. *For $s \ge 2$, one has*

$$\int_{\mathfrak{M}} \mathcal{F}(\alpha)\, d\alpha = \sum_{\substack{1 \le a \le q \le Q \\ (a,q)=1}} \sum_{\mathbf{y} \in \mathcal{V}_1} q^{-1-s} S(a, q, \mathbf{y}) T(\mathbf{y}) + O(B^s).$$

Proof. For $\alpha \in \mathfrak{M}(a, q)$, by Lemmas 5.6, we have that

$$\mathcal{F}(\alpha) = \sum_{\mathbf{y} \in \mathcal{V}_1} J(\alpha, y_0, y_0) \cdots J(\alpha, y_0, y_s),$$

where

$$J(\alpha, y_0, y) = q^{-1} \sum_{u=1}^{q} e\left(\frac{a}{q} uy\right) \int_{-B/y_0}^{B/y_0} e(\beta x y)\, dx + O(q(1 + |\beta| B)).$$

Note that for $\alpha \in \mathfrak{M}(a, q)$, we have

$$q(1 + |\beta| B) \ll qQ.$$

In addition, the trivial estimate $|e(z)| \le 1$ for $z \in \mathbb{R}$ yields

$$q^{-1} \sum_{u=1}^{q} e\left(\frac{a}{q} uy\right) \int_{-B/y_0}^{B/y_0} e(\beta x y)\, dx \ll B/y_0.$$

Therefore, we may write

$$\int_{\mathfrak{M}} \mathcal{F}(\alpha)\, d\alpha - \sum_{\substack{1\le a\le q\le Q\\(a,q)=1}} \sum_{\mathbf{y}\in\mathcal{V}_1} q^{-1-s} S(a,q,\mathbf{y}) T(\mathbf{y}) \ll E_1 + E_2,$$

where

$$E_1 = \sum_{\substack{1\le a\le q\le Q\\(a,q)=1}} \sum_{\mathbf{y}\in\mathcal{V}_1} \int_{-B^{-1}Q}^{B^{-1}Q} (qQ)^{s+1}\, d\beta$$

and

$$E_2 = \sum_{\substack{1\le a\le q\le Q\\(a,q)=1}} \sum_{\mathbf{y}\in\mathcal{V}_1} \int_{-B^{-1}Q}^{B^{-1}Q} (qQ)(B/y_0)^s\, d\beta.$$

Noting that the measure of the domain of integration is $O(B^{-1}Q)$, we observe that

$$E_1 \ll B^{-1}Q^{s+2} \sum_{1\le q\le Q} q^{s+2} \sum_{1\le y_0\le B^{1/2}} y_0^s \ll B^{(s-1)/2}Q^{2s+5},$$

and

$$E_2 \ll B^{s-1}Q^2 \sum_{1\le q\le Q} q^2 \sum_{1\le y_0\le B^{1/2}} 1 \ll B^{s-1/2}Q^5.$$

Recalling that we chose Q to be B^δ and $\delta < 1/10$, we may conclude that $E_1 + E_2 \ll B^s$. This completes the proof of the lemma. □

Let

$$\mathcal{X}_3(\mathbf{y}) = \{\mathbf{x}_0 \in \mathbb{R}^s \,:\, \|\mathbf{x}_0\|_\infty \le 1 \text{ and } |x_1y_1/y_0 + \cdots + x_sy_s/y_0| \le 1\}. \tag{5.23}$$

Lemma 5.8. *For $s \ge 2$, one has*

$$T(\mathbf{y}) = B^s y_0^{-1-s} \int_{\mathcal{X}_3(\mathbf{y})} d\boldsymbol{x}_0 + O\left(\frac{B^s}{Q^s|y_0\cdots y_s|}\right).$$

Proof. Let

$$G(\mathbf{x},\mathbf{y}) = x_0 + x_1\frac{y_1}{y_0} + \cdots + x_s\frac{y_s}{y_0}$$

and

$$\mathcal{X}_4 = \{\mathbf{x} \in \mathbb{R}^{s+1} \,:\, \|\mathbf{x}\|_\infty \le 1\}.$$

By a change of variables in the right hand side of (5.22), namely $\mathbf{x} \to (B/y_0)\mathbf{x}$ and $\beta \to B^{-1}\beta$, we have

$$T(\mathbf{y}) = B^s y_0^{-1-s} \int_{-Q}^{Q} \int_{\mathcal{X}_4} e(\beta G(\mathbf{x}, \mathbf{y}))\, d\mathbf{x}\, d\beta.$$

Since

$$\int_C^D e(\gamma x)\, dx \ll \min(|D - C|, |\gamma|^{-1}),$$

for $\gamma \neq 0$, it follows that when $y_i \neq 0$ for $0 \leq i \leq s$, we have

$$\int_{|\beta|>Q} \int_{\mathcal{X}_4} e(\beta G(\mathbf{x}, \mathbf{y}))\, d\mathbf{x}\, d\beta \ll \int_{|\beta|>Q} \frac{y_0^s}{|\beta^{s+1} y_1 \cdots y_s|}\, d\beta \ll \frac{y_0^s}{Q^s |y_1 \cdots y_s|}.$$

Therefore, we have

$$T(\mathbf{y}) = B^s y_0^{-1-s} \int_{-\infty}^{\infty} \int_{\mathcal{X}_4} e(\beta G(\mathbf{x}, \mathbf{y}))\, d\mathbf{x}\, d\beta + O\left(\frac{B^s}{Q^s |y_0 \cdots y_s|}\right).$$

Let

$$\mathcal{X}_5(\mathbf{y}, u) = \{\mathbf{x}_0 \in \mathbb{R}^s \,:\, \|\mathbf{x}_0\|_\infty \leq 1 \text{ and } |u - (x_1 y_1/y_0 + \cdots + x_s y_s/y_0)| \leq 1\}.$$

Observing that

$$\int_{-\lambda}^{\lambda} e(\beta u)\, d\beta = \frac{\sin(2\pi\lambda u)}{\pi u}$$

for $u \neq 0$ and making a change of variables, namely

$$x_0 \to (u - x_1 y_1/y_0 - \cdots - x_s y_s/y_0),$$

we may conclude that

$$\begin{aligned} \int_{-\infty}^{\infty} \int_{\mathcal{X}_4} e(\beta G(\mathbf{x}, \mathbf{y}))\, d\mathbf{x}\, d\beta &= \lim_{\lambda\to\infty} \int_{\mathcal{X}_4} \frac{\sin(2\pi\lambda G(\mathbf{x}, \mathbf{y}))}{\pi G(\mathbf{x}, \mathbf{y})}\, d\mathbf{x} \\ &= \lim_{\lambda\to\infty} \int_{-s-1}^{s+1} \psi_2(\mathbf{y}, u) \frac{\sin(2\pi\lambda u)}{\pi u}\, du, \end{aligned} \tag{5.24}$$

where

$$\psi_2(\mathbf{y}, u) = \int_{\mathcal{X}_5(\mathbf{y},u)} d\mathbf{x}_0.$$

We note that if u is not in the interval

$$\big[-1-(|y_1|+\cdots+|y_s|)/y_0,\, 1+(|y_1|+\cdots+|y_s|)/y_0\big],$$

then $\mathcal{X}_5(\mathbf{y},u)$ is empty, and hence $\psi_2(\mathbf{y},u)=0$. The latter values of u consequently make no contribution in the last integral in (5.24). By the Fourier Integral Theorem, we have that

$$\int_{-\infty}^{\infty}\int_{\mathcal{X}_4} e(\beta G(\mathbf{x},\mathbf{y}))\,d\mathbf{x}\,d\beta=\psi_2(\mathbf{y},0).$$

On noting from (5.23) that $\mathcal{X}_5(\mathbf{y},0)=\mathcal{X}_3(\mathbf{y})$, it now follows that

$$\psi_2(\mathbf{y},0)=\int_{\mathcal{X}_3(\mathbf{y})} d\mathbf{x}_0,$$

which completes the proof of our lemma. □

It is convenient to have available the following technical lemma in order to more concisely estimate the major arc contribution in Lemma 5.10.

Lemma 5.9. *Let* $I_0=[-1,1]$ *and*

$$I(z,y_0,K)=\{x\in\mathbb{R}\,:\,|xz/y_0-K|\le 1\}.$$

Suppose that $0\le|y|-1\le|y'|\le|y|\le y_0$. *Then, for any real number* K, *one has*

$$\left|\int_{I_0\cap I(y',y_0,K)} dx-\int_{I_0\cap I(y,y_0,K)} dx\right|\le 4/|y|.$$

Proof. Since

$$\left|\int_{I_0\cap I(y',y_0,K)} dx-\int_{I_0\cap I(y,y_0,K)} dx\right|\le 2$$

it suffices to prove this lemma under the assumption that $|y|>2$. By symmetry, we may also assume that $1<y'\le y\le y_0$ and $K\ge 0$. Observe that for $z>0$, we have

$$I(z,y_0,K)=\left[\frac{y_0(K-1)}{z},\frac{y_0(K+1)}{z}\right].$$

We now divide our work into two cases: $0 \leq K \leq 1$ and $K > 1$.

(i) Suppose that $0 \leq K \leq 1$. The relation $1 < y' \leq y \leq y_0$ implies that

$$\frac{y_0(K-1)}{y'} \leq \frac{y_0(K-1)}{y} \leq 0 < 1 \leq \frac{y_0(K+1)}{y} \leq \frac{y_0(K+1)}{y'}.$$

Hence,

$$I_0 \cap I(y, y_0, K) \subseteq I_0 \cap I(y', y_0, K),$$

and so

$$\int_{I_0 \cap I(y,y_0,K)} dx \leq \int_{I_0 \cap I(y',y_0,K)} dx.$$

Furthermore, we have that

$$\int_{I_0 \cap I(y,y_0,K)} dx = 1 + \min\left(1, \frac{y_0(1-K)}{y}\right)$$

and that

$$\int_{I_0 \cap I(y',y_0,K)} dx = 1 + \min\left(1, \frac{y_0(1-K)}{y'}\right).$$

If

$$1 \leq \frac{y_0(1-K)}{y},$$

then

$$\int_{I_0 \cap I(y,y_0,K)} dx = 2 = \int_{I_0 \cap I(y',y_0,K)} dx.$$

If, on the other hand,

$$\frac{y_0(1-K)}{y} < 1,$$

then

$$\begin{aligned} 0 \leq \int_{I_0 \cap I(y',y_0,K)} dx - \int_{I_0 \cap I(y,y_0,K)} dx &= \min\left(1, \frac{y_0(1-K)}{y'}\right) - \frac{y_0(1-K)}{y} \\ &\leq \frac{y_0(1-K)}{y'} - \frac{y_0(1-K)}{y} \\ &= \frac{y_0(1-K)(y-y')}{yy'} \leq \frac{y_0(y/y_0)}{yy'} \\ &= 1/y' \leq 2/y. \end{aligned}$$

(ii) Now suppose that $K > 1$. The relation $1 < y' \leq y \leq y_0$ implies that

$$0 < \frac{y_0(K-1)}{y} \leq \frac{y_0(K-1)}{y'}$$

and

$$1 \leq \frac{y_0(K+1)}{y} \leq \frac{y_0(K+1)}{y'}.$$

Therefore,

$$I_0 \cap I(y', y_0, K) \subseteq I_0 \cap I(y, y_0, K),$$

which implies that

$$\int_{I_0 \cap I(y', y_0, K)} dx \leq \int_{I_0 \cap I(y, y_0, K)} dx.$$

Also, we see that

$$\int_{I_0 \cap I(y, y_0, K)} dx = 1 - \min\left(1, \frac{y_0(K-1)}{y}\right)$$

and

$$\int_{I_0 \cap I(y', y_0, K)} dx = 1 - \min\left(1, \frac{y_0(K-1)}{y'}\right).$$

If

$$1 \leq \frac{y_0(K-1)}{y},$$

then

$$\int_{I_0 \cap I(y, y_0, K)} dx = 0 = \int_{I_0 \cap I(y', y_0, K)} dx.$$

If, on the other hand,

$$\frac{y_0(K-1)}{y} < 1,$$

then

$$\begin{aligned} 0 \le \int_{I_0 \cap I(y,y_0,K)} dx - \int_{I_0 \cap I(y',y_0,K)} dx &= \min\left(1, \frac{y_0(K-1)}{y'}\right) - \frac{y_0(K-1)}{y} \\ &\le \frac{y_0(K-1)}{y'} - \frac{y_0(K-1)}{y} \\ &= \frac{y_0(K-1)(y-y')}{yy'} \le \frac{y_0(y/y_0)}{yy'} \\ &= 1/y' \le 2/y. \end{aligned}$$

This completes the proof of our lemma. □

Lemma 5.10. *For $s \ge 2$, one has*

$$\int_{\mathfrak{M}} \mathcal{F}(\alpha)\, d\alpha = \frac{1}{2}\sigma_\infty \mathfrak{S} B^s \log B + O(B^s).$$

Proof. Let

$$\mathcal{V}_2(q) = \{\mathbf{y} \in \mathbb{Z}^{s+1} \,:\, 1 \le |y_1|, \dots, |y_s| \le y_0 \le B^{1/2} \text{ and } q | \gcd(y_0, \dots, y_s)\}$$

and

$$\mathcal{V}_3(q) = \{\mathbf{y} \in \mathbb{Z}^{s+1} \,:\, 1 \le |y_1|, \dots, |y_s| \le y_0 \le q^{-1}B^{1/2}\}.$$

Note that from (5.21),

$$S(a,q,\mathbf{y}) = \sum_{\mathbf{x} \,(\mathrm{mod}\, q)} \Big(\frac{a}{q}\mathbf{x} \cdot \mathbf{y}\Big) = \begin{cases} q^{s+1}, & \text{when } q \mid \gcd(y_0, \dots, y_s), \\ 0, & \text{when } q \nmid \gcd(y_0, \dots, y_s). \end{cases}$$

By Lemmas 5.7 and 5.8, we have

$$\begin{aligned}\int_{\mathfrak{M}} \mathcal{F}(\alpha)\, d\alpha - B^s \sum_{\substack{1\le a\le q\le Q\\(a,q)=1}} \sum_{\mathbf{y}\in\mathcal{V}_2(q)} y_0^{-1-s} \int_{\mathcal{X}_3(\mathbf{y})} d\mathbf{x}_0 \\ &\ll B^s + B^s Q^{-s} \sum_{\substack{1\le a\le q\le Q\\(a,q)=1}} \sum_{\mathbf{y}\in\mathcal{V}_2(q)} |y_0\cdots y_s|^{-1} \\ &\ll B^s + B^s Q^{-s} \sum_{1\le q\le Q} q^{-s} \sum_{\mathbf{y}\in\mathcal{V}_3(q)} |y_0\cdots y_s|^{-1} \\ &\ll B^s,\end{aligned}$$

and hence, in view of the definitions of $\mathcal{V}_2(q)$, $\mathcal{V}_3(q)$, and $\mathcal{X}_3(\mathbf{y})$, one has

$$\int_{\mathfrak{M}} \mathcal{F}(\alpha)\, d\alpha = B^s \sum_{\substack{1\le a\le q\le Q\\(a,q)=1}} q^{-1-s} \sum_{\mathbf{y}\in\mathcal{V}_3(q)} y_0^{-1-s} \int_{\mathcal{X}_3(\mathbf{y})} d\mathbf{x}_0 + O(B^s). \tag{5.25}$$

Let

$$\begin{aligned}\mathcal{X}_6(y_0) = \{(\mathbf{x}_0,\mathbf{y}_0)\in\mathbb{R}^{2s} : &\|\mathbf{x}_0\|_\infty \le 1,\ \|\mathbf{y}_0\|_\infty \le y_0, \text{ and} \\ &|x_1y_1/y_0 + \cdots + x_sy_s/y_0| \le 1\}.\end{aligned}$$

Observe that for $K\in\mathbb{R}$ and $y_0\ge 1$, by Lemma 5.9 and the mean value theorem, we have

$$\begin{aligned}\sum_{1\le|y|\le y_0} \int_{\substack{|x|\le 1\\ |xy/y_0-K|\le 1}} dx - \int_{\substack{|x|\le 1,\,|y|\le y_0\\ |xy/y_0-K|\le 1}} dx\, dy &\ll \sum_{1\le|y|\le y_0} 4/|y| \\ &\ll \log(2y_0).\end{aligned}$$

We may iteratively apply the above inequality s times to exchange our sum over y_i for an integral over y_i for each $1\le i\le s$. By carrying out this procedure and noting that

$$\int_{\mathcal{X}_3(\mathbf{y})} d\mathbf{x}_0 \le 2^s,$$

we obtain that

$$\sum_{\mathbf{y}\in\mathcal{V}_3(q)} y_0^{-1-s}\int_{\mathcal{X}_3(\mathbf{y})} d\mathbf{x}_0 - \sum_{y_0\le q^{-1}B^{1/2}} y_0^{-1-s}\int_{\mathcal{X}_6(y_0)} d\mathbf{x}_0\, d\mathbf{y}_0 \ll \sum_{y_0\le q^{-1}B^{1/2}} \frac{\log y_0}{y_0^2}$$

$$\ll 1. \tag{5.26}$$

Furthermore, by making the change of variables $\mathbf{y}_0 \to y_0\mathbf{y}_0$ and recalling (5.3), one has

$$\sum_{y_0\le q^{-1}B^{1/2}} y_0^{-1-s}\int_{\mathcal{X}_6(y_0)} d\mathbf{x}_0\, d\mathbf{y}_0 = \sigma_\infty \sum_{y_0\le q^{-1}B^{1/2}} y_0^{-1}. \tag{5.27}$$

Combining (5.25), (5.26), and (5.27), we have now shown that

$$\begin{aligned}\int_{\mathfrak{M}} \mathcal{F}(\alpha)\, d\alpha &= \sigma_\infty B^s \sum_{\substack{1\le a\le q\le Q\\(a,q)=1}} q^{-1-s} \sum_{y_0\le q^{-1}B^{1/2}} y_0^{-1} + O\left(B^s \sum_{1\le q\le Q} q^{-s}\right)\\ &= \sigma_\infty B^s \sum_{\substack{1\le a\le q\le Q\\(a,q)=1}} q^{-1-s}\left(\frac{1}{2}\log B - \log q + O(1)\right) + O(B^s).\\ &= \frac{1}{2}\sigma_\infty B^s \log B \sum_{1\le q\le Q} \frac{\phi(q)}{q^{s+1}} + O(B^s).\end{aligned}$$

On observing that

$$\sum_{1\le q\le Q} \frac{\phi(q)}{q^{s+1}} = \mathfrak{S} + O(Q^{1-s}),$$

we now find that

$$\int_{\mathfrak{M}} \mathcal{F}(\alpha)\, d\alpha = \frac{1}{2}\sigma_\infty \mathfrak{S} B^s \log B + O(B^s). \qquad \square$$

Theorem 5.2 now follows from Lemmas 5.5 and 5.10.

5.4 The Proof of Theorem 5.1

Now that we have completed our proof of Theorem 5.2, we are able to derive Theorem 5.1. Let

$$\mathcal{U}(B) = \{(\mathbf{x},\mathbf{y}) \in (\mathbb{Z}\setminus\{0\})^{2s+2} \,:\, \mathbf{x}\cdot\mathbf{y} = 0 \text{ and } \max_{i,j} |x_i y_j| \le B\}$$

and $N_1(B) = \#\mathcal{U}(B)$. We first prove two auxiliary lemmas. Then, we derive an asymptotic formula for $N_1(B)$, and we conclude by applying our asymptotic formula for $N_1(B)$ in combination with Möbius inversion to prove Theorem 5.1.

Lemma 5.11. *For $s \geq 2$, one has*

$$\#\left\{(\mathbf{x},\mathbf{y}) \in \left(\mathbb{Z} \cap [-B^{1/2}, B^{1/2}]\right)^{2s+2} \,:\, \mathbf{x}\cdot\mathbf{y} = 0\right\} \ll B^s.$$

Proof. Note that

$$xy = \frac{1}{4}\big((x+y)^2 - (x-y)^2\big)$$

and that the mapping $L : \mathbb{Z}^2 \to \mathbb{Z}^2$, defined by $L(x,y) = (x+y, x-y)$, is injective. Hence, by setting $(u_i, v_i) = (x_i + y_i, x_i - y_i)$, the set

$$\left\{(\mathbf{x},\mathbf{y}) \in \left(\mathbb{Z} \cap [-B^{1/2}, B^{1/2}]\right)^{2s+2} \,:\, \mathbf{x}\cdot\mathbf{y} = 0\right\}$$

injects into the set

$$\left\{(\mathbf{u},\mathbf{v}) \in \left(\mathbb{Z} \cap [-2B^{1/2}, 2B^{1/2}]\right)^{2s+2} \,:\, (u_0^2 - v_0^2) + \cdots + (u_s^2 - v_s^2) = 0\right\}.$$

The size of the above set is equal to

$$\int_{\mathbb{T}} |H(B)|^{2s+2}\, d\alpha,$$

where

$$H(B) = \sum_{0 \leq z \leq 2B^{1/2}} e(\alpha z^2).$$

Since $(2s+2) \geq 6$, it follows from Chapter 2 of [44] that

$$\int_{\mathbb{T}} |H(B)|^{2s+2}\, d\alpha \ll \left(2B^{1/2}\right)^{2s} \ll B^s.$$

The lemma now follows. □

Lemma 5.12. *For $s \geq 2$, $B \geq 2$, and $i \in \{0, \dots, s\}$, one has*

$$\#\{(\mathbf{x}, \mathbf{y}) \in \mathcal{U}(B) \, : \, |y_i| = \max_j |y_j| \leq B^{1/2} \text{ and } \max_{0 \leq k < i} |y_k| < |y_i|\}$$
$$= \sigma_\infty \mathfrak{S} B^s \log B + O(B^s).$$

Proof. One can follow the argument of our proof of Theorem 5.2 mutatis mutandis to show that

$$\#\{(\mathbf{x}, \mathbf{y}) \in \mathcal{U}(B) \, : \, y_i = \max_j |y_j| \leq B^{1/2} \text{ and } \max_{0 \leq k < i} |y_k| < y_i\}$$
$$= \frac{1}{2} \sigma_\infty \mathfrak{S} B^s \log B + O(B^s).$$

The lemma now follows by noting that

$$\mathbf{x} \cdot \mathbf{y} = 0 \quad \Leftrightarrow \quad \mathbf{x} \cdot (-\mathbf{y}) = 0$$

in order to account for both positive and negative values of y_i. □

Lemma 5.13. *For $s \geq 2$ and $B \geq 2$, one has*

$$N_1(B) = (2s+2) \sigma_\infty \mathfrak{S} B^s \log B + O(B^s).$$

Proof. We first split the set $\mathcal{U}(B)$ into $2s+2$ regions. Note that for each point in this set, either $\max_i |x_i| \leq B^{1/2}$ or $\max_j |y_j| \leq B^{1/2}$. The $2s+2$ regions that we consider are $\mathfrak{K}_0, \dots, \mathfrak{K}_s, \mathfrak{L}_0, \dots, \mathfrak{L}_s$, where

$$\mathfrak{K}_i = \{(\mathbf{x}, \mathbf{y}) \in \mathcal{U}(B) : |x_i| = \max_j |x_j| \leq B^{1/2} \text{ and } \max_{0 \leq k < i} |x_k| < |x_i|\}$$

and

$$\mathfrak{L}_i = \{(\mathbf{x}, \mathbf{y}) \in \mathcal{U}(B) : |y_i| = \max_j |y_j| \leq B^{1/2} \text{ and } \max_{0 \leq k < i} |y_k| < |y_i|\}.$$

Observe that when $0 \leq k < l \leq s$, we have $\mathfrak{K}_k \cap \mathfrak{K}_l = \emptyset = \mathfrak{L}_k \cap \mathfrak{L}_l$. Furthermore, for $k, l \in \{0, \dots, s\}$, the intersection of $\mathfrak{K}_k$ and $\mathfrak{L}_l$ lies inside the set

$$\{(\mathbf{x}, \mathbf{y}) \in \left(\mathbb{Z} \cap [-B^{1/2}, B^{1/2}]\right)^{2s+2} \, : \, \mathbf{x} \cdot \mathbf{y} = 0\},$$

and so by Lemma 5.11, the size of $\mathfrak{K}_k \cap \mathfrak{L}_l$ is $O(B^s)$.

By applying Lemma 5.12, we see that each of our $2s+2$ regions $\mathfrak{K}_0, \ldots, \mathfrak{K}_s, \mathfrak{L}_0, \ldots, \mathfrak{L}_s$ is of size

$$\sigma_\infty \mathfrak{S} B^s \log B + O(B^s).$$

Hence, we have

$$N_1(B) = (2s+2)\sigma_\infty \mathfrak{S} B^s \log B + O(B^s). \qquad \square$$

We now prove Theorem 5.1.

Proof. (of Theorem 5.1)

Recall the definitions of $H(\mathbf{x}, \mathbf{y})$ and $N(B)$ in (5.1) and (5.2), respectively. When counting the points that contribute to $N(B)$ and $N_1(B)$, note that the height of a solution differs by a power of s. Furthermore, for $(\mathbf{x}, \mathbf{y}) \in \mathbb{P}^s(\mathbb{Q}) \times \mathbb{P}^s(\mathbb{Q})$, the definition of our anticanonical height function $H(\mathbf{x}, \mathbf{y})$ assumes that $\gcd(x_0, \ldots, x_s) = \gcd(y_0, \ldots, y_s) = 1$. Also, for $(\mathbf{x}, \mathbf{y}) \in \mathbb{P}^s(\mathbb{Q}) \times \mathbb{P}^s(\mathbb{Q})$, we have $(\mathbf{x}, \mathbf{y}) = (\mathbf{x}, -\mathbf{y}) = (-\mathbf{x}, \mathbf{y}) = (-\mathbf{x}, -\mathbf{y})$. Let $M(B) = N(B^s)$. Hence,

$$N_1(B) = 4 \sum_{i=1}^{\infty} \sum_{j=1}^{\infty} M\left(\frac{B}{ij}\right),$$

and by Möbius inversion, we have that

$$\begin{aligned} M(B) &= \frac{1}{4} \sum_{i=1}^{\infty} \sum_{j=1}^{\infty} \mu(i)\mu(j) N_1\left(\frac{B}{ij}\right) \\ &= \left(\frac{s+1}{2}\right) \sigma_\infty \mathfrak{S} \sum_{\substack{i,j \\ ij \le B}} \mu(i)\mu(j) \left(\frac{B}{ij}\right)^s \log\left(\frac{B}{ij}\right) + O\left(\sum_{\substack{i,j \\ ij \le B}} \frac{B^s}{i^s j^s}\right) \\ &= \left(\frac{s+1}{2}\right) \sigma_\infty \mathfrak{S} B^s \log B \sum_{\substack{i,j \\ ij \le B}} \frac{\mu(i)\mu(j)}{i^s j^s} + O\left(B^s \sum_{\substack{i,j \\ ij \le B}} \frac{\log(ij)}{i^s j^s}\right). \end{aligned}$$

Note that

$$B^s \sum_{\substack{i,j \\ ij \le B}} \frac{\log(ij)}{i^s j^s} \ll B^s$$

and that

$$\begin{aligned}
\sum_{\substack{i,j \\ ij \le B}} \frac{\mu(i)\mu(j)}{i^s j^s} &= \left(\sum_{1 \le i \le B^{1/2}} \frac{\mu(i)}{i^s} \right)^2 + O\left(\sum_{1 \le k \le B} \frac{1}{k^s} \sum_{l > B^{1/2}} \frac{1}{l^s} \right) \\
&= \left(\zeta(s)^{-1} + O\big(B^{(1-s)/2}\big) \right)^2 + O\big(B^{(1-s)/2}\big). \\
&= \zeta(s)^{-2} + O(B^{(1-s)/2}).
\end{aligned}$$

Hence, we have

$$M(B) = \left(\frac{s+1}{2} \right) \zeta(s)^{-2} \sigma_\infty \mathfrak{S} B^s \log B + O(B^s),$$

which implies that

$$N(B) = M(B^{1/s}) = \left(\frac{s+1}{2s} \right) \zeta(s)^{-2} \sigma_\infty \mathfrak{S} B \log B + O(B).$$

This completes the proof of Theorem 5.1. □

APPENDIX

APPENDIX A

Statement of Results Used in Chapter II

In this appendix, we provide statements of the lemmas used in Chapter II which are from the preprints [28] and [27] of Liu and Wooley. The notation here will be consistent with that of Chapter II, and we will assume that $\mathrm{char}(\mathbb{F}_q) \nmid k$.

Let

$$U(a,g) = \sum_{\langle r\rangle < \langle g\rangle} e(ar^k/g).$$

Lemma A.1. *(i) Suppose that $\alpha \in \mathbb{T}$ and that $\alpha = a/g + \beta$ with $a, g \in \mathbb{F}_q[t]$, $0 \le \langle a\rangle < \langle g\rangle \le \widehat{P}$, and $\langle\beta\rangle < \langle g\rangle^{-1}\widehat{P}^{1-k}$. Then, $F(\alpha;P) = \langle g\rangle^{-1}U(a,g)F(\beta;P)$.*
(ii) When $\langle\beta\rangle < \widehat{P}^{1-k}$, one has $F(\beta;P) \ll \widehat{P}(1+\widehat{P}^k\langle\beta\rangle)^{-1/k}$.
(iii) When $(a,g) = 1$, one has $U(a,g) \ll \langle g\rangle^{1-1/k}$.

Proof. This is Lemma 4.1 of [28]. □

Lemma A.2. *Let P and R be positive numbers with $P \ge 1$ and $2P/\log(2P) < R < P - \log P$. Suppose that $\alpha \in \mathbb{T}$, that a and g are elements of $\mathbb{F}_q[t]$ with g monic and $(a,g) = 1$, and write $\beta = \alpha - a/g$. Then, whenever $\langle g\rangle \le \widehat{R}$ and $\langle\beta\rangle < \widehat{P}^{1-k}$, one has*

$$f(\alpha;P,R) - \langle g\rangle^{-1}U(a,g)\rho(P/R)F(\beta;P) \ll \langle g\rangle\widehat{P}(\log\widehat{P})^{-1/2}(1+\widehat{P}^k\langle\beta\rangle).$$

Proof. This is Lemma 4.3 of [28]. □

Lemma A.3. *Suppose that $u > 2k-2$ is accessible to the exponent k and that v is an integer with $2v \geq u$. Then, we have*

$$\int_{\mathbb{T}} |F(\alpha)^2 f(\alpha)^{2v}|\, d\alpha \ll \widehat{P}^{2v+2-k}.$$

Proof. This is Lemma 6.2 of [28]. □

Lemma A.4. *There exists a positive absolute constant C such that if*

$$u + 5 \geq s_{q,k} + Ck\sqrt{\operatorname{Log}\operatorname{Log} k}/\operatorname{Log} k,$$

then u is accessible to the exponent k.

Proof. This is a combination of Theorem 9.4, Corollary 13.3, and Lemma 14.1 of [28]. □

Lemma A.5. *There exists a small positive constant $\nu = \nu(q,k)$ such that*

$$\sup_{\alpha \in \mathfrak{n}} |F(\alpha)| \ll \widehat{P}^{1-\nu}.$$

Proof. This is a theorem in [27]. □

BIBLIOGRAPHY

BIBLIOGRAPHY

[1] V. V. Batyrev and Y. Tschinkel, *Manin's conjecture for toric varieties*, J. Alg. Geom. **7** (1998), 1553.

[2] V. V. Batyrev and Y. Tschinkel, *Rational points on some Fano cubic bundles*, C. R. Acad. Sci. Paris **323** (1996), 41-46.

[3] V. Bentkus and F. Götze, *Lattice point problems and distribution of values of quadratic forms,* Ann. Math. **150** (1999), 977-1027.

[4] J. Bourgain, *On triples in arithmetic progression*, Geom. Funct. Anal. **9** (1999), 968-984.

[5] R. de la Bretèche and T. D. Browning, *On Manin's conjecture for singular del Pezzo surfaces of degree four, I*, Mich. Math. J. **55** (2007), 51-80.

[6] R. de la Bretèche and T. D. Browning, *On Manin's conjecture for singular del Pezzo surfaces of degree four, II*, Math. Proc. Cambridge Phil. Soc. **143** (2007), 579-605.

[7] H. Davenport, *Analytic methods for Diophantine equations and Diophantine inequalities*, 2nd ed., Cambridge Univ. Press, Cambridge, 2005.

[8] H. Davenport and H. Heilbronn, *On indefinite quadratic forms in five variables,* J. London Math. Soc. **21** (1946), 185-193.

[9] J. Franke, Y. Manin, and Y. Tschinkel, *Rational points of bounded height on Fano varieties*, Invent. Math. **95** (1989), 421-435.

[10] D. E. Freeman, *Asymptotic lower bounds and formulas for Diophantine inequalities,* Number Theory for the Millennium, Vol. 2 (Urbana, IL, 2000), A. K. Peters, Natick, MA, 2002, 57-74.

[11] D. E. Freeman, *Asymptotic lower bounds for Diophantine inequalities,* Mathematika **47** (2000), 127-159.

[12] W. T. Gowers, *A new proof of Szemerédi's theorem*, Geom. Funct. Anal. **11** (2001), 465-588.

[13] W. T. Gowers, *A new proof of Szemerédi's theorem for arithmetic progressions of length four*, Geom. Funct. Anal. **8** (1998), 529-551.

[14] B. J. Green, *Roth's theorem in the primes*, Ann. Math. **161** (2005), 1609-1636.

[15] B. J. Green and T. C. Tao, *The primes contain arbitrarily long arithmetic progressions*, to appear in Ann. Math.

[16] G. H. Hardy and J. E. Littlewood, *A new solution of Waring's problem*, Q. J. Math. **48** (1919), 272-293.

[17] D. R. Heath-Brown, *A new form of the circle method, and its application to quadratic forms*, J. Reine Angew. Math. **481** (1996), 149-206.

[18] D. R. Heath-Brown, *Integer sets containing no arithmetic progressions*, J. London Math. Soc. **35** (1987), 385-394.

[19] J. Hirschfeld and L. Storme, The packing problem in statistics, coding theory and finite projective spaces: update 2001. *Finite geometries*, Dev. Math. 3, Kluwer Acad. Publ., Dordrecht (2001), 201-246.

[20] C.-N. Hsu, *Diophantine inequalities for the non-Archimedean line* $\mathbb{F}_q((1/T))$, Acta Arith. **97** (2001), 253-267.

[21] L. K. Hua, *Additive theory of prime numbers*, Amer. Math. Soc., Providence, 1965.

[22] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, 2nd ed., Springer, New York, 1990.

[23] R. M. Kubota, *Waring's problem for* $\mathbb{F}_q[x]$, Dissertationes Math. (Rozprawy Mat.) **117** (1974), 60pp.

[24] S. Lang, *On Quasi Algebraic Closure*, Ann. Math. **55** (1952), 373-390.

[25] Y.-R. Liu and C. V. Spencer, *A generalization of Roth's theorem in finite Abelian groups* (in preparation).

[26] Y.-R. Liu and C. V. Spencer, *A generalization of Roth's theorem in function fields* (submitted).

[27] Y.-R. Liu and T. D. Wooley, *Vinogradov's mean value theorem in function fields* (in preparation).

[28] Y.-R. Liu and T. D. Wooley, *Waring's problem in function fields* (submitted).

[29] G. A. Margulis, *Discrete subgroups and ergodic theory*, Number Theory, Trace Formulas and Discrete Groups (Oslo, 1987), Academic Press, Boston, 1989, 377-398.

[30] R. Meshulam, *On subsets of finite Abelian groups with no 3-term arithmetic progressions*, J. Combin. Theory Ser. A **71** (1995), 168-172.

[31] A. Oppenheim, *The minima of indefinite quaternary quadratic forms*, Proc. Nat. Acad. Sci. **15** (1929), 724727.

[32] E. Peyre, *Hauteurs et mesures de Tamagawa sur les variétés de Fano*, Duke Math. J. **79** (1995), 101-218.

[33] M. Robbiani, *On the number of rational points of bounded height on smooth bilinear hypersurfaces in biprojective space*, J. Lond. Math. Soc. **63** (2001), 33-51.

[34] M. Rosen, *Number theory in function fields*, GTM **210**, Springer (2002).

[35] R. F. Roth, *On certain sets of integers*, J. London Math. Soc. **28** (1953), 104-109.

[36] C. V. Spencer, *The Manin-Peyre conjecture for* $x_0y_0 + \cdots + x_ny_n = 0$ (in preparation).

[37] C. V. Spencer, *Diophantine inequalities in function fields* (submitted).

[38] C. V. Spencer and T. D. Wooley, *Diophantine inequalities and quasi-algebraically closed fields* (in preparation).

[39] L. Storme, J. Thas, and S. Vereecke, *New upper bounds for the sizes of caps in finite projective spaces*, J. Geom. 73 (2002), 176-193.

[40] E. Szemerédi, *Integer sets containing no arithmetic progressions*, Acta Math. Hungar. **56** (1990), 155-158.

[41] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. Math. **141** (1995), 553-572.

[42] J. L. Thunder, *Asymptotic estimates for rational points of bounded height on flag varieties*, Comp. Math. **88** (1993), 155-186.

[43] C. C. Tsen, *Divisionalgebren über Funktionenkörper*, Gött. Nach. (1933), 335-339.

[44] R. C. Vaughan, *The Hardy-Littlewood method*, 2nd ed., Cambridge Univ. Press, Cambridge, 1997.

[45] A. Weil, *Numbers of solutions of equations in finite fields,* Bull. Amer. Math. Soc. **55** (1949), 497-508.

[46] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Ann. Math. **141** (1995), 443-551.

[47] T. D. Wooley, *On Diophantine inequalities: Freeman's asymptotic formula,* Bonner Math. Schriften **360** (2003), Article 30, 32pp.

[48] T. D. Wooley, *Breaking classical convexity in Waring's problem: sums of cubes and quasi-diagonal behaviour*, Invent. Math. **122** (1995), 421-451.