EXPLORATIONS OF GEOMETRIC COMBINATORICS IN VECTOR SPACES OVER FINITE FIELDS

A Dissertation presented to

the Faculty of the Graduate School

at the University of Missouri

In Partial Fulfillment of

the Requirements for the Degree of

Doctor of Philosophy

---

by

DERRICK HART

Dr. Alex Iosevich, Dissertation Supervisor

May 2008

The undersigned, appointed by the dean of the Graduate School, have examined the dissertation entitled

EXPLORATIONS OF GEOMETRIC COMBINATORICS
IN VECTOR SPACES OVER FINITE FIELDS

presented by Derrick Hart,

a candidate for the degree of Doctor of Philosophy,

and hereby certify that, in their opinion, it is worthy of acceptance.

Professor Alex Iosevich

Professor William Banks

Professor Dan Edidin

Professor Steve Hofmann

Professor Sergei Kopeikin

ACKNOWLEGDEMENTS

I would like to thank my graduate advisor, Alex Iosevich, for his support throughout the process of writing this dissertation. I would like to thank my masters advisor, Michael Lacey for preparing me for my Ph.D. research. I would also like to thank the members of my graduate committee, Bill Banks, Dan Edidin, Steve Hofmann and Sergei Kopeikin.

Additionally, I would like to thank my loving wife Kathy without whom I could not have completed this dissertation.

TABLE OF CONTENTS

EXPLORATIONS OF GEOMETRIC COMBINATORICS

IN VECTOR SPACES OVER FINITE FIELDS

Derrick Hart

Dr. Alex Iosevich, Dissertation Supervisor

ABSTRACT

Let $\mathbb{F}_q^d$ be the d-dimensional vector space over the finite field with q elements. We study various geometric combinatorics problems in vector spaces over finite fields as well as there arithmetic implications. For example:

- **The Erdős-Falconer distance problem:** How large does $E \subset \mathbb{F}_q^d$ need to be to ensure that

$$|\Delta(E)| = |\{||x-y|| \equiv (x_1-y_1)^2 + \cdots + (x_d-y_d)^2 : x, y \in E\}| \gtrsim q?$$

- **The dot product problem:** How large does $E \subset \mathbb{F}_q^d$ need to be to ensure that

$$|\Pi(E)| = |\{x \cdot y : x, y \in E\}| \gtrsim q?$$

- **The k-point configuration problem:** How large does $E \subset \mathbb{F}_q^d$ need to be to ensure that a congruent copy of every non-degenerate k-point configuration is contained in E?

- **The sum-product problem:** Can the sumset $A + A = \{a + a' : a, a' \in A\}$ and the product set $A \cdot A = \{aa' : a, a' \in A\}$ for $A \subset \mathbb{F}_q$ both be small?

CHAPTER I

INTRODUCTION

1.1 Statement of Purpose

Geometric combinatorics deals with the counting properties of geometric objects. In recent years harmonic analysis, analytic number theory, graph theory, geometric measure theory and ergodic theory have all found common ground in this very old and elegant research area. In many cases the use of finite fields as "model spaces" has yielded many non-trivial insights into the subject. Further exploration has pushed the idea of a finite field "thesis", i.e. the idea that if a certain property or theorem is true in finite fields an analagous statement holds in other spaces, for example $\mathbb{R}^d$, $\mathbb{Z}$. However, a general statement of this magnitude has definite limits. A full understanding of these limitations is necessary in order turn this turn this investigatory process into a well-defined method. Furthermore, the work in this area has helped provide further evidence of finite fields as a mathematical space with many distinct and beautiful properties interesting in their own right. In this dissertation the author studies several key problems in the field of geometric combinatorics in vector spaces over finite fields and their implications.

1.2 Finite Fields

Let $\mathbb{F}_q$ be a finite field of characteristic $q = p^n$, where p is an odd prime. The prime base field of $\mathbb{F}_q$ may then be naturally identified with $\mathbb{Z}_p$. Consider the additive group of $\mathbb{F}_q$.

Definition 1.2.1. For every $a \in \mathbb{F}_q$ define a map $Tr : \mathbb{F}_q \to \mathbb{F}_p$ by

$$Tr(x) = a + a^p + \cdots + a^{p^{n-1}}.$$

Then an additive character of $\mathbb{F}_q$ is of the form

$$\chi(a) = e^{\frac{2\pi i Tr(a)}{p}}.$$

Now we may define $\mathbb{F}_q^d$ to be a d-dimensional vector space over $\mathbb{F}_q$ with respect to a given basis $(e_1, \ldots, e_d)$. With this basis in tow then for $m \in \mathbb{F}_q^d$ we have a complete set of characters $\chi(m \cdot x)$ over $\mathbb{F}_q^d$. Given a subspace $H \subset \mathbb{F}_q^d$ the orthogonality property of characters over finite fields is given by

$$\frac{1}{|H|} \sum_{x \in H} \chi(x \cdot m) = 1 \tag{1.2.2}$$

for $m = 0$ and 0 otherwise.

1.3 Finite Field Fourier Transform

The Fourier transform of a complex-valued function f on $\mathbb{F}_q^d$ with respect to a non-trivial principal additive character χ on $\mathbb{F}_q$ is given by

$$\widehat{f}(m) = q^{-d} \sum_{x \in \mathbb{F}_q^d} f(x)\chi(-x \cdot m).$$

One may immmediately note that that setting $m = 0$ immediately yields the mean

$$\widehat{f}(0) = q^{-d} \sum_{x \in \mathbb{F}_q^d} f(x).$$

Using 1.2.2 quickly yields many standard properties of the Fourier Transform.

Theorem 1.3.1 (Plancherel)**.**

$$\sum_{x \in \mathbb{F}_q^d} f(x)\overline{g(x)} = q^d \sum_{m \in \mathbb{F}_q^d} \hat{f}(m)\overline{\hat{g}(m)}$$

Proof.

$$q^d \sum_{m \in \mathbb{F}_q^d} \hat{f}(m)\overline{\hat{g}(m)} =$$

$$q^{-d} \sum_{m \in \mathbb{F}_q^d} \sum_{x,y} f(x)\overline{g(y)}\chi(m \cdot (y - x)) =$$

$$\sum_{x \in \mathbb{F}_q^d} f(x)\overline{g(x)}$$

□

In the case $f = g$ one has Parseval's equality

Corollary 1.3.2 (Parseval)**.**

$$\sum_{x \in \mathbb{F}_q^d} |f(x)|^2 = q^d \sum_{m \in \mathbb{F}_q^d} |\hat{f}(m)|^2$$

One of the key properties of the Fourier Transform is the ability to reconstruct a function by inverting the Fourier Transform in the following way.

Theorem 1.3.3 (Fourier Inversion)**.**

$$f(x) = \sum_{m \in \mathbb{F}_q^d} \hat{f}(m)\chi(-x \cdot m)$$

Proof.

$$\sum_{m \in \mathbb{F}_q^d} \hat{f}(m)\chi(x \cdot m) =$$

$$q^{-d} \sum_y f(y) \sum_{m \in \mathbb{F}_q^d} \chi((x-y) \cdot m) = f(x)$$

□

For two functions f and g we define convolution to be

$$(f * g)(d) = \sum_{x \in \mathbb{F}_q^d} f(x)g(d-x).$$

Covolution acts as multiplication in the frequency domain

Theorem 1.3.4.

$$\widehat{(f * g)}(m) = q^d \hat{f}(m)\hat{g}(m).$$

Proof.

$$\widehat{(f*g)}(m) =$$

$$= q^{-d} \sum_{y \in F_q^d} \sum_{x \in \mathbb{F}_q^d} f(x) g(y-x) \chi(-m \cdot y)$$

$$= q^{-d} \sum_{x \in \mathbb{F}_q^d} f(x) \sum_{y' \in F_q^d} g(y') \chi(-m \cdot (y+x))$$

$$= q^d \hat{f}(m) \hat{g}(m)$$

□

Given a subset E of $\mathbb{F}_q^d$ we denote the characteristic or indicator function to by $E(x)$. We define the uniformity norm of a function to be $||f||_U = \max_{m \neq 0} |\widehat{f}(m)|$.

1.3.1 Notation

Throughout the paper $X \lesssim Y$ means that there exists $C > 0$ such that $X \leq CY$, $X \gtrsim Y$ means $Y \lesssim X$, and $X \approx Y$ if both $X \lesssim Y$ and $X \gtrsim Y$. Along the same lines, $X \ll Y$ means that $\frac{X}{Y} \to 0$, as $q \to \infty$ $X \gg Y$ means $Y \ll X$, and $X \sim Y$ if $\frac{X}{Y} \to 1$ as $q \to \infty$.

CHAPTER II

GENERALIZED INCIDENCE THEORY

2.1 Introduction

In their 1978 paper, "Problems in harmonic analysis related to curvature", ([52]), Eli Stein and Steve Wainger study a variety of operators defined over hyper-surfaces and other lower dimensional manifolds in $\mathbb{R}^d$. The recurring theme is that the behavior of these operators is governed, to various degrees, by the Gaussian *curvature* of the underlying manifold. This fact allows one to obtain good results for a variety of problems in geometric combinatorics, geometric measure theory and additive number theory. Conversely, one may see that discrete versions of Euclidean operators provide us with coherent models that can be used to achieve progress back in the Euclidean space and other manifolds.

Let P denote a finite point set and L a finite collection of geometric objects. The number of incidences between P and L, denoted by $I(P, L)$ is the number of pairs $(p, l) \in P \times L$ such that p lies on l. Let

$$\mathrm{T}\, f(x) = \int_{\text{family of manifolds indexed by } x} f(y)dy.$$

Suppose that T satisfies better than trivial L_1 or L_2 bounds. Then one can deduce a non-trivial combinatorial incidence theorem for an appropriate finite family of manifolds L and suitably regular point sets. This principle, applied in both Euclidean and finite field settings, has interesting consequences in analytic, combinatorial and number theoretic settings. In this way, *curvature* takes on not only analytic, but also combinatorial and arithmetic manifestations, and the resulting connections provide rich opportunities for exploration.

2.2 Finite Field Incidence Theory

Let $f, g : \mathbb{F}_q^d \to [0, \infty)$ here and in the following sections. Consider the classes of operators

$$\mathrm{A}_t\, g(x) = \sum_{Q(x-y)=t} g(y)$$

and

$$\mathrm{R}_t\, g(x) = \sum_{B(x,y)=t} g(y)$$

where $Q : \mathbb{F}_q^d \to \mathbb{F}_q$ and B is a non-degenerate bilinear form with $B : \mathbb{F}_q^d \times \mathbb{F}_q^d \to \mathbb{F}_q$. In this context we define the corresponding incidence functions

$$\nu(t) = \sum_{x \in \mathbb{F}_q^d} f(x)\, \mathrm{A}_t\, g(x) = \sum_{Q(x-y)=t} f(x)g(y)$$

and

$$\eta(t) = \sum_{x \in \mathbb{F}_q^d} f(x)\, \mathrm{R}_t\, g(x) = \sum_{B(x,y)=t} f(x)g(y).$$

We shall consider these two operators for choices of Q and B that behave very differently in terms of curvature. In the case of $\nu(t)$, we will consider functions Q with high curvature, i.e. the set $M_t = \{x : Q(x) = t\}$ will have good Fourier decay such as in a non-degenerate quadratic form. However, in both cases shall see that we get good control of both $\nu(t)$ and $\eta(t)$ in the sense of small deviation from the mean. Here we employ the methods of [34], [28] to yield an appropriate incidence theorem.

Theorem 2.2.1 (Pointwise Incidence Theorem)**.** *([34],[27],[31]) Suppose that* $M_t =$

$\{x : Q(x) = t\}$. *Then*

$$\nu(t) = |M_t|q^{-d}||f||_1||g||_1 + R(t), \text{ where} \tag{2.2.2}$$

$$|R(t)| \leq q^d||M_t||_U||f||_2||g||_2,$$

$$\eta(t) = ||f||_1||g||_1 q^{-1} + R(t), \text{ where} \tag{2.2.3}$$

$$|R(t)| \leq ||f||_2||g||_2 q^{\frac{d-1}{2}} \text{ if } t \neq 0 \text{ and,}$$

$$|R(0)| \leq ||f||_2 \left(\sum_{y,a \in \mathbb{F}_q^*} g(y)g(ay) \right)^{\frac{1}{2}} q^{\frac{d-1}{2}}.$$

If for any function $\mu(t)$ one has $\mu(t) = M + R(t)$ then using the simple fact that M being larger than the absolute value of $R(t)$ for some t guarantees $\mu(t) > 0$ yields the following useful corollary to Theorem 3.2.2.

Corollary 2.2.4. *([34],[27],[31]) Suppose $L \subset \mathbb{F}_q$ and let $M_t = \{x : Q(x) = t\}, t \in L$. Then if*

$$\frac{||f||_1||g||_1}{||f||_2||g||_2} > q^{2d}\frac{||M_t||_U}{|M_t|}$$

we have that $\nu(t) > 0$ for every $t \in L$.

If $B(x, y)$ be a non-degenerate bilinear form then if

$$\frac{||f||_1||g||_1}{||f||_2||g||_2} > q^{\frac{d+1}{2}}$$

we have that $\eta(t) > 0$ for every $t \in \mathbb{F}_q^*$. If in addition we have that $g(x) \leq C$ then

$$\frac{||f||_1}{||f||_2}||g||_1^{\frac{1}{2}} > C^{\frac{1}{2}}q^{\frac{d}{2}+1}$$

we have that $\eta(t) > 0$ for every $t \in \mathbb{F}_q$.

The last statement follows from the fact that if $g(x) \leq C$ then

$$\sum_{a \in \mathbb{F}_q^*} g(ay) \leq Cq.$$

We shall see during the proof of (2.2.3) that while the $|R(t)|$ may be quite large for specific values of t that for many values of t it should be considerably smaller. In the following theorem one sees that this is indeed true in an L_2 sense.

Theorem 2.2.5 (L_2 Incidence Bound)**.** *([27],[31]) If* $(0,\dots,0) \notin support(f) \equiv E$, *then*

$$\sum_t \eta^2(t) \leq ||f||_2^2 \cdot |E| \cdot ||g||_1^2 \cdot q^{-1} + ||f||_2^2 \cdot q^{2d-1} \sum_{k \neq (0,\dots,0)} |\widehat{g}(k)|^2 |E \cap l_k|,$$

where, $l_k = \{tk : t \in \mathbb{F}_q^*\}$.

In the case of $\nu(t)$ it is indeed possible to obtain a simliar bound for some choices of $Q(x)$. However, this turns out to be more technical and will be discussed in a later section.

Incidence theory in general is very useful in obtaining information about the existence of solutions of equations in large sets. Specifically, setting $f(x) = E(x)$ and $g(x) = F(x)$ for $E, F \subset \mathbb{F}_q^d$ in Corollary 2.2.4 allows us to see when large but otherwise arbitrary sets contain solutions to $Q(x)$ and $B(x,y)$.

We call a set E *Salem* with constant C if

$$||E||_U \leq C\sqrt{|E|}q^{-d}.$$

This property may be thought of as, at least in a general sense, to be the the optimal Fourier decay of a set.

Theorem 2.2.6. *([34],[27],[31]) Let* $E, F \subset \mathbb{F}_q^d$. *If for* $t \in L \subset \mathbb{F}_q$,

$$|E||F| > q^{4d} \left(\frac{||M_t||_U}{|M_t|} \right)^2 \tag{2.2.7}$$

then we have that $\{Q(x-y) : x \in E, y \in F\} = L$.

In particular, if M_t *is Salem for* $t \in L$ *with constant* C *and*

$$|E||F| > C^2 \frac{q^{2d}}{|M_t|} \tag{2.2.8}$$

the we have that $\{Q(x-y) : x \in E, y \in F\} = L$.

Also, if

$$|E||F| > q^{d+1} \tag{2.2.9}$$

we have that $\mathbb{F}_q^* \subset \{B(x,y) : x \in E, y \in F\}$ *and if*

$$|E||F| > q^{d+2} \tag{2.2.10}$$

we have that $\mathbb{F}_q = \{B(x,y) : x \in E, y \in F\}$.

In summary this corollary states that for each t that M_t has any non-trivial fourier decay and for any sets E and F of sufficient size must contain a solution to $Q(x-y) = t$ with $x \in E$ and $y \in F$. Also, in the case of a non-degenerate bilinear form that if E and F are of sufficient size then $B(x,y) = t$ has a solution $x \in E$ and $y \in F$ for every $t \in \mathbb{F}_q$.

Theorem 2.2.5 may be used to give additional information about the solutions to bilinear forms if one of the sets has a particular structure. We say that set E is product-like if for every line through the origin $l_k = \{tk : t \in \mathbb{F}_q^*\}$ one has that $|E \cap l_k| \leq |E|^{\frac{1}{d}}$. The inspiration for this definition of course comes from the fact that the property holds product sets $E = A_1 \times \cdots \times A_d, A_i \subset \mathbb{F}_q$. We notice that in view of the bound on $R(0)$ in 2.2.3 of Theorem 3.2.2 along with the fact that $\sum_{a \in \mathbb{F}_q^*} E(ay) = |E \cap l_y|$ we may under this condition immediately improve 2.2.6 of Corollary 2.2.4 reproving a result of Bourgain ([3]) in $d = 3$ and Cochrane and Pinner ([47]) for $d > 3$.

Corollary 2.2.11. *Let* $E, F \subset \mathbb{F}_q^d$. *If* F *is product-like and*

$$|E|^{1-\frac{1}{d}}|F| > q^{d+1}$$

we have that $\{B(x,y) : x \in E, y \in F\} = \mathbb{F}_q$.

However, this as well as a stronger statement can be shown to follow from the second part of Theorem 2.2.4. Also we say that set E is radial if for every l_k one has that $|E \cap l_k| \leq c$ for some constant c. Theorem 2.2.5 may restated for these sets in the following corollary.

Corollary 2.2.12. *([27],[31]) Let $E, F \subset \mathbb{F}_q^d$ with $(0,\dots,0) \notin E$. If E is product-like then*

$$\sum_t \eta^2(t) \leq |E|^2|F|^2q^{-1} + |E|^{1+\frac{1}{d}}|F|q^{d-1},$$

and if E is radial then

$$\sum_t \eta^2(t) \leq |E|^2|F|^2q^{-1} + c|E||F|q^{d-1}.$$

Now by Cauchy-Schwartz one has that

$$|E|^2|F|^2 = \left(\sum_t \sum_{B(x,y)=t} E(x)E(y)\right)^2 \left(\sum_t \eta(t)\right)^2 \leq |\{B(x,y) : x \in E, y \in F\}| \sum_t \eta(t)^2.$$

Applying this Theorem 2.2.5 immediately yields the fact that for both product-like and radial sets if one is willing to to settle for having a solution $x \in E$ and $y \in F$ for only a positive proportion of t's in the equation $B(x,y) = t$ then one may relax the size condition.

Theorem 2.2.13. *([27],[31]) Let $E, F \subset \mathbb{F}_q^d$ with $(0,\dots,0) \notin E$.*

If E is product-like then

$|\{B(x,y) : x \in E, y \in F\}| \geq \frac{1}{2}q$ *for* $|E|^{1-\frac{1}{d}}|F| \geq q^d$,

$|\{B(x,y) : x \in E, y \in F\}| \geq \frac{1}{2}\frac{|E|^{1-\frac{1}{d}}|F|}{q^{d-1}}$ *for* $|E|^{1-\frac{1}{d}}|F| \leq q^d$.

If E is radial then

$|\{B(x,y) : x \in E, y \in F\}| \geq \frac{1}{2}q$ *for* $|E||F| \geq cq^d$,

$|\{B(x,y) : x \in E, y \in F\}| \geq \frac{1}{2}\frac{|E||F|}{cq^{d-1}}$ *for* $|E||F| \leq cq^d$.

It is of interest that the constant $\frac{1}{2}$ may be increased above if one is will to place a constant C into the size conditions, for example if E is product-like and $|E|^{1-\frac{1}{d}}|F| \geq Cq^d$ then

$$|\{B(x,y) : x \in E, y \in F\}| \geq \frac{C}{1+C}q.$$

2.3 Proofs of Theorem 3.2.2 and 2.2.5

We begin by proving 2.2.2 of Theorem 3.2.2. We first apply fourier inversion to M_t.

$$\begin{aligned}\nu(t) &= \sum_{Q(x-y)=t} f(x)g(y) \\ &= \sum_{x,y} f(x)g(y)M_t(x-y) = \sum_{x,y} f(x)g(y)\sum_m \widehat{M_t}(m)\chi(m(x-y))\end{aligned}$$

Then from the definition of the fourier transform followed by the extraction of the zero frequency.

$$\begin{aligned}\nu(t) &= q^{2d}\sum_m \widehat{f}(-m)\widehat{g}(m)\widehat{M_t}(m) \\ &= |M_t|q^{-d}||f||_1||g||_1 + q^{2d}\sum_{m\neq 0} \widehat{f}(-m)\widehat{g}(m)\widehat{M_t}(m) \\ &= Mean + R(t).\end{aligned}$$

Now,

$$|R(t)| \leq q^{2d}||M_t||_{Uni}\sum_{m\neq 0}|\widehat{f}(-m)\widehat{g}(m)|$$

and applying the Cauchy-Schwartz inequality,

$$|R(t)| \leq q^{2d}||M_t||_{Uni}||\widehat{f}||_2||\widehat{g}||_2 = q^d||M_t||_{Uni}||f||_2||g||_2.$$

The proof is then complete.

We now prove 2.2.3 of Theorem 3.2.2. In this section we set $B(x,y) = x\cdot y$ although the proof goes through without any essential changes if the dot product $x\cdot y$ is replaced by any non-degenerate bi-linear form $B(x,y)$.

We have that

$$\begin{aligned}\eta(t) &= \sum_{x\cdot y=t} f(x)g(y)\\ &= \sum_{x,y} q^{-1}\sum_{s}\chi(s(x\cdot y-t))f(x)g(y)\\ &= ||f||_1||g||_1 q^{-1} + q^{-1}\sum_{x,y}\sum_{s\neq 0}\chi(s(x\cdot y-t))f(x)g(y)\\ &= ||f||_1||g||_1 q^{-1} + R(t).\end{aligned}$$

Using the Cauchy-Schwartz inequality,

$$\begin{aligned}|R(t)|^2 \leq & ||f||_2^2\cdot q^{-2}\sum_{x}\sum_{y,y'}\sum_{s,s'\neq 0} g(y)g(y')\chi(x\cdot(sy-s'y'))\chi(t(s'-s))\\ &= q^{d-2}||f||_2^2\cdot\sum_{sy=s'y'} g(y)g(y')\chi(t(s'-s)).\end{aligned}$$

Now if $t=0$ then,

$$|R(0)|^2 \leq q^{d-2}||f||_2^2\cdot\sum_{sy=s'y'} g(y)g(y') \leq q^{d-1}||f||_2^2\cdot\sum_{\substack{y\in\mathbb{F}_q^d\\ a\in\mathbb{F}_q^*}} g(y)g(ay)$$

Now if $t\neq 0$ then,

$$\begin{aligned}|R(t)|^2 \leq = q^{d-2}||f||_2^2\cdot\sum_{s\neq 0}\sum_{y} g^2(y) + q^{d-2}||f||_2^2\cdot\sum_{\substack{sy=s'y'\\ s\neq s'}} g(y)g(y')\chi(t(s'-s))\\ = q^{d-2}(q-1)||f||_2^2||g||_2^2 + q^{d-2}||f||_2^2\cdot\sum_{\substack{sy=s'y'\\ s\neq s'}} g(y)g(y')\chi(t(s'-s))\\ = q^{d-2}(q-1)||f||_2^2||g||_2^2 + q^{d-2}||f||_2^2\cdot\sum_{\substack{a\neq 0,1\\ b\neq 0}}\sum_{y} g(y)g(ay)\chi(tb(1-a))\\ = ||f||_2^2||g||_2^2 q^{d-2}(q-1) - q^{d-2}||f||_2^2\cdot\sum_{a\neq 0,1}\sum_{y} g(y)g(ay),\end{aligned}$$

and the result follows.

To prove Theorem 2.2.5, apply Cauchy-Schwartz once again to see that

$$\eta^2(t) \leq ||f||_2^2\cdot\sum_{\substack{x,y,y'\\ x\cdot y=x\cdot y'=t}} E(x)g(y)g(y'),$$

where $E = support(f)$.

It follows that

$$\begin{aligned}\sum_t \eta^2(t) \leq & ||f||_2^2 \cdot \sum_{x\cdot y = x\cdot y'} E(x)g(y)g(y') \\ &= ||f||_2^2 q^{-1} \sum_{x,y,y'} \sum_s \chi(s(x\cdot y - x\cdot y'))E(x)g(y)g(y') \\ &= ||f||_2^2 q^{-1}|E|||g||_1^2 + ||f||_2^2 q^{2d-1} \sum_{s\neq 0} \sum_x |\widehat{g}(x)|^2 E(sx) \\ &= ||f||_2^2 q^{-1}|E|||g||_1^2 + ||f||_2^2 q^{2d-1} \sum_x |\widehat{g}(x)|^2 |E\cap l_x|,\end{aligned}$$

as desired.

2.4 Pinned Incidence Theory

It is possible to give a variant of Theorem 2.2.5 which under the assumption of a product structure gives a slight improvement over the corresponding results of Theorem 2.2.13. Furthermore, this technique generalizes to give a L_2 bound for $\nu(t)$ when $Q(x)$ is a non-degenerate quadratic form. In this case for sets with product structure one can match the exponents in Theorem 2.2.13.

Let $\pi_j(x) = (x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_d)$ and define

$$E_z^j = \pi_j(E) \times \{z\},$$

where z is an element of

$$\{z \in \mathbb{F}_q : (x_1, x_2, \ldots, x_{j-1}, z, x_{j+1}, \ldots, x_d) \in E\}.$$

We drop the exponent j in the sequel for the sake of convenience. Let f, g non-negative functions with $support(f) = E_z$ and $B(x,y)$ and $Q(x)$ be non-degenerate bilinear and quadratic forms respectively.

Then we define the corresponding pinned incidence functions to be

$$\eta_{pin}(t) = \sum_{B(x,y)=t} f(x)g(y),$$

and

$$\nu_{pin}(t) = \sum_{Q(x-y)=t} f(x)g(y).$$

For the remainder of this section we will assume for brevitys sake that $B(x,y) = x \cdot y$ and $Q(x) = x \cdot x$. However, both the statement of the Theorems 2.4.1 and 2.4.4 along with their corresponding proofs can be stated under the full assumptions with only minor changes. This changes do not affect the statement of Theorem 2.4.7 Our first result is the following pinned incidence theorem.

Theorem 2.4.1. *([29]) Let f, g are non-negative functions with support$(f) = E_z$. Then, if $(0, \ldots, 0) \notin E_z$, we have*

$$\sum_t \eta_{pin}^2(t) \leq |E_z|||f||_2^2 \cdot ||g||_1^2 \cdot q^{-1} + ||f||_2^2||g||_2^2 q^{d-1}. \tag{2.4.2}$$

Also we have,

$$\sum_t \nu_{pin}^2(t) \leq |E_z|||f||_2^2 \cdot ||g||_1^2 \cdot q^{-1} + q^{d-1}||f||_2^2 \ (g *_d g)(2z) + q^{d-1}||f||_2^2||g||_2^2 \tag{2.4.3}$$

where

$$(g *_d g)(x) = \sum_{\substack{x=y_d+y'_d \\ \pi_d(y)=\pi_d(y')}} g(y)g(y').$$

Letting $g(x) = F(x)$ where $F = B_1 \times \ldots B_d \subset \mathbb{F}_q^d$ one has that

$$(F *_d F)(x) \leq |F|.$$

Then setting $f(x) = E_z(x)$ yields the following theorem.

Theorem 2.4.4. *([29]) Let $F = B_1 \times \ldots B_d$ be product sets of $\mathbb{F}_q^d$. Then, if $(0, \ldots, 0) \notin E_z$ we have that*

$$\sum_t \eta_{pin}^2(t) \leq |E_z|^2|F|^2 q^{-1} + q^{d-1}|E_z||F|. \tag{2.4.5}$$

Also we have,

$$\sum_t \nu_{pin}^2(t) \leq |E_z|^2|F|^2q^{-1} + 2q^{d-1}|E_z||F|. \tag{2.4.6}$$

Assuming product structure on E leads immediately to the following consequence of Theorem 2.4.4.

Theorem 2.4.7. *([29]) Let $B(x,y)$ and $Q(x)$ be non-degenerate bilinear and quadratic forms respectively. If $E = A_1 \times \cdots \times A_d$ and $F = B_1 \times \ldots B_d$ are product sets with $(0,\ldots,0) \notin E$ then,*

$$|\{B(x,y) : x \in E_z, y \in F\}| \geq \tfrac{1}{2}q \qquad \text{for} \quad |E|^{1-\frac{1}{d}}|F| \geq q^d.$$

$$|\{B(x,y) : x \in E_z, y \in F\}| \geq \tfrac{1}{2}\tfrac{|E|^{1-\frac{1}{d}}|F|}{q^{d-1}} \qquad \text{for} \quad |E|^{1-\frac{1}{d}}|F| \leq q^d.$$

$$|\{Q(x-y) : x \in E_z, y \in F\}| \geq \tfrac{1}{3}q \qquad \text{for} \quad |E|^{1-\frac{1}{d}}|F| \geq q^d,$$

$$|\{Q(x-y) : x \in E_z, y \in F\}| \geq \tfrac{1}{3}\tfrac{|E|^{1-\frac{1}{d}}|F|}{q^{d-1}} \qquad \text{for} \quad |E|^{1-\frac{1}{d}}|F| \leq q^d.$$

2.5 Proof of Theorem 2.4.1

We begin by proving 2.4.2 of Theorem 2.4.1. Without loss of generality we may take $j = d$ in the argument below. Then

$$\begin{aligned}\sum_t \eta_z^2(t) \leq & ||f||_2^2 \sum_{x\cdot y = x\cdot y'} E_z(x)g(y)g(y') \\ &= ||f||_2^2||g||_1^2q^{-1} + ||f||_2^2q^{-1}\sum_{s\neq 0}\sum_{\substack{x\in E_z \\ y,y'}} g(y)g(y')\chi(sx\cdot(y-y')) \\ &= Mean + R(t).\end{aligned}$$

Now applying Cauchy-Schwartz in x followed by orthogonality,

$$\begin{aligned}
R(t) =& ||f||_2^2 q^{-1} \sum_{s\neq 0} \sum_{x\in E_z} \left| \sum_{y\in E} g(y)\chi(sx\cdot y)\right|^2 \\
&\leq ||f||_2^2 q^{-1} \sum_{s\neq 0} \sum_{x\in \mathbb{F}_q^{d-1}\times\{z\}} \left| \sum_{y} g(y)\chi(sx\cdot y)\right|^2 \\
&= ||f||_2^2 q^{d-2} \sum_{s\neq 0} \sum_{\pi_d(y)=\pi_d(y')} \chi(sz(y_d - y'_d))g(y)g(y') \\
&= ||f||_2^2 ||g||_2^2 q^{d-1} - ||f||_2^2 q^{d-2} \sum_{\pi_d(y)=\pi_d(y')} g(y)g(y') \\
&\leq ||f||_2^2 ||g||_2^2 q^{d-1}.
\end{aligned}$$

This completes the proof.

Now we prove 2.4.3 of Theorem 2.4.1. Let $\|x\| = x\cdot x$. By Cauchy-Schwartz,

$$\nu_z^2(t) \leq ||f||_2^2 \cdot \sum_{||x-y||=||x-y'||=t} E_z(x)g(y)g(y'),$$

so

$$\begin{aligned}
\sum_t \nu_z^2(t) &\leq ||f||_2^2 \cdot \sum_{||x-y||=||x-y'||} E_z(x)g(y)g(y') \\
&= q^{-1}||f||_2^2 \cdot \sum_s \sum_{x,y,y'} \chi(s(||x-y|| - ||x-y'||))E_z(x)g(y)g(y') \\
&= q^{-1}|E_z|||f||_2^2||g||_1^2 + R(t),
\end{aligned}$$

and

$$R(t) = q^{-1}||f||_2^2 \sum_{s\neq 0} \sum_{x\in E_z} \left| \sum_y g(y)\chi(s(||y|| - 2x\cdot y))\right|^2,$$

since

$$||x-y|| - ||x-y'|| = (||y|| - 2x\cdot y) - (||y'|| - 2x\cdot y').$$

It follows that

$$R(t) \leq q^{-1}||f||_2^2 \sum_{s\neq 0} \sum_{x\in\mathbb{F}_q^{d-1}\times\{z\}} \sum_{y,y'} g(y)g(y')\chi(-2sx\cdot(y-y'))\chi(s(||y||-||y'||))$$

$$= q^{d-2}||f||_2^2 \sum_{s\neq 0} \sum_{\pi_d(y)=\pi_d(y')} g(y)g(y')\chi(-2sz(y_d-y'_d))\chi(s(y_d^2-y'^2_d))$$

$$= q^{d-2}||f||_2^2 \sum_{s} \sum_{\pi_d(y)=\pi_d(y')} g(y)g(y')\chi(-2sz(y_d-y'_d))\chi(s(y_d^2-y'^2_d))$$

$$- q^{d-2}||f||_2^2 \sum_{\pi_d(y)=\pi_d(y')} g(y)g(y')$$

$$= q^{d-1}||f||_2^2 \cdot \sum_{2z(y_d-y'_d)=y_d^2-y'^2_d-\pi_d(y)=\pi_d(y')} g(y)g(y') - q^{d-2}||f||_2^2 \sum_{\pi_d(y)=\pi_d(y')} g(y)g(y')$$

$$\leq q^{d-1}||f||_2^2 \cdot \sum_{\substack{2z=y_d+y'_d \\ y_d\neq y'_d \\ \pi_d(y)=\pi_d(y')}} g(y)g(y') + q^{d-1}||f||_2^2 \sum_{y=y'} g(y)g(y')$$

$$\leq q^{d-1}||f||_2^2\ (g *_d g)(2z) + q^{d-1}||f||_2^2||g||_2^2$$

2.6 Multiple Incidence Theory

It is possible to put Theorem 2.2.6 in a broader context. Consider $k+1$ points $x_0,\dots x_k \in \mathbb{F}_q^d$ and the corresponding system of equations $Q(x_i-y_i)=t_{i,j}$ for $0\leq i,j\leq k$ and $t_{i,j}\in\mathbb{F}_q$. If the sets $M_{t_{i,j}}=\{x : Q(x)=t_{i,j}\}$ have good fourier decay then it is possible to show that there exists a solution this system in sufficiently large subsets of $\mathbb{F}_q^d$.

Let $f_0,\dots f_k : \mathbb{F}_q^d \to [0,1]$ and define the function

$$\mathcal{T}_{l_k}(x_0,\dots,x_k) = \mathcal{T}_{l_{k-1}}(x_0,\dots,x_{k-1})f_k(x_k)M_{t_{1,k}}(x_0-x_k)M_{t_{2,k}}(x_1-x_k)\dots M_{t_{k,k}}(x_{k-1}-x_k),$$

recursively for $l_k = l_{k-1}\cup\{t_{1,k},\dots t_{k,k}\}, t_{i,j}\in\mathbb{F}_q$ where

$$\mathcal{T}_{l_1}(x_0,x_1) = M_{t_{1,1}}(x_0-x_1)f_0(x_0)f_1(x_1).$$

Then define the incidence function

$$\nu_k(l_k) = \sum_{x_0,\dots,x_k} \mathcal{T}_{l_{k-1}}(x_0,\dots,x_{k-1})f_k(x_k)M_{t_{1,k}}(x_0-x_k)\dots M_{t_{k,k}}(x_{k-1}-x_k)$$

where

$$\nu_1(l_1) = \sum_{x_0,\dots,x_k} \mathcal{T}_{l_1}(x_0, x_1) = \sum_{x_0,\dots,x_k} M_{t_{1,1}}(x_0 - x_1) f_0(x_0) f_1(x_1)$$

is the incidence function defined in Section 1.1.

Under these assumptions we prove the following theorem in Section 1.7.

Theorem 2.6.1. *Let $f_0, \dots f_k : \mathbb{F}_q^d \to [0,1]$., such that*

$$\prod_{0\le i\le k-1} ||f_i||_1 \cdot \frac{||f_k||_1^2}{||f_k||_2^2} \gtrsim q^{3kd} \prod_{1\le j\le k} \frac{||M_{t_{j,k}}||_U^2}{|M_{t_{j,k}}|} \prod_{1\le i\le j\le k} \frac{q^d}{|M_{t_{i,j}}|},$$

with a sufficiently large constant. Then for every side length set l_k, $l_k \in (L)^{\binom{k+1}{2}}$ we have that $\nu_k(l_k) > 0$. Furthermore, if

$$\prod_{0\le i\le k-1} ||f_i||_1 \cdot \frac{||f_k||_1^2}{||f_k||_2^2} >> q^{3kd} \prod_{1\le j\le k} \frac{||M_{t_{j,k}}||_U^2}{|M_{t_{j,k}}|} \prod_{1\le i\le j\le k} \frac{q^d}{|M_{t_{i,j}}|},$$

then

$$\nu_k(l_k) \sim \prod_{0\le i\le k} ||f_i||_1 \prod_{1\le i\le j\le k} \frac{|M_{t_{i,j}}|}{q^d}.$$

Theorem 2.6.2. *Let $E_0, \dots E_k \subset \mathbb{F}_q^d$. and the $M_{t_{i,j}}, 1 \le i \le j \le k$ be Salem for $t_{i,j} \in L \subset \mathbb{F}_q^d$, such that*

$$\prod_{0\le i\le k} |E_i| \gtrsim q^{kd} \prod_{1\le i\le j\le k} \frac{q^d}{|M_{t_{i,j}}|}$$

with a sufficiently large constant. Then for every side length set l_k, $l_k \in (L)^{\binom{k+1}{2}}$ we have that $\nu_k(l_k) > 0$. Furthermore, if

$$\prod_{0\le i\le k} |E_i| >> q^{kd} \prod_{1\le i\le j\le k} \frac{q^d}{|M_{t_{i,j}}|}$$

then

$$\nu_k(l_k) \sim \prod_{0\le i\le k} |E_i| \prod_{1\le i\le j\le k} \frac{|M_{t_{i,j}}|}{q^d}.$$

Similarly, consider $k+1$ points $x_0, \dots x_k \in \mathbb{F}_q^d$ and for a nondegenerate bilinear form $B(x,y)$ the corresponding system of equations $B(x_i, y_i) = t_{i,j}$ for $0 \le i, j \le k$

and $t_{i,j} \in \mathbb{F}_q^*$. Associate to each equation the sets $N_{t_{i,j}} = \{x : B(x,y) = t_{i,j}\}$. Then define the function

$$\mathcal{D}_{l_k}(x_0,\dots,x_k) = \mathcal{D}_{l_{k-1}}(x_0,\dots,x_{k-1}) f_k(x_k) N_{t_{1,k}}(x_0,x_k) N_{t_{2,k}}(x_1,x_k)\dots N_{t_{k,k}}(x_{k-1},x_k),$$

recursively for $l_k = l_{k-1} \cup \{t_{1,k},\dots t_{k,k}\}, t_{i,j} \in \mathbb{F}_q^*$ where

$$\mathcal{D}_{l_1}(x_0,x_1) = N_{t_{1,1}}(x_0,x_1) f_0(x_0) f_1(x_1).$$

Then one has the incidence function

$$\eta_k(l_k) = \sum_{x_0,\dots,x_k} \mathcal{D}_{l_{k-1}}(x_0,\dots,x_{k-1}) f_k(x_k) N_{t_{1,k}}(x_0,x_k)\dots N_{t_{k,k}}(x_{k-1},x_k)$$

where

$$\eta_1(l_1) = \sum_{x_0,\dots,x_k} \mathcal{D}_{l_1}(x_0,x_1) = \sum_{x_0,\dots,x_k} N_{t_{1,1}}(x_0,x_1) f_0(x_0) f_1(x_1)$$

is the incidence function defined in Section 1.1.

Theorem 2.6.3. *Let $f_0,\dots f_k : \mathbb{F}_q^d \to [0,1]$., such that*

$$||f_0||_1 \dots ||f_k||_1 \gtrsim q^{kd+\binom{k+1}{2}},$$

with a sufficiently large constant. Then for every side length set l_k, $l_k \in (\mathbb{F}_q^*)^{\binom{k+1}{2}}$ we have that $\eta_k(l_k) > 0$. Furthermore, if

$$||f_0||_1 \dots ||f_k||_1 >> q^{kd+\binom{k+1}{2}},$$

then

$$\eta_k(l_k) \sim ||f_0||_1 \dots ||f_k||_1 q^{-\binom{k+1}{2}}.$$

Theorem 2.6.4. *Let $E_0,\dots E_k \subset \mathbb{F}_q^d$. , such that*

$$|E_0| \dots |E_k| \gtrsim q^{kd+\binom{k+1}{2}}$$

with a sufficiently large constant. Then for every side length set l_k, $l_k \in (\mathbb{F}_q^*)^{\binom{k+1}{2}}$ we have that $\eta_k(l_k) > 0$. Furthermore, if

$$|E_0| \dots |E_k| >> q^{kd+\binom{k+1}{2}}$$

then

$$\eta_k(l_k) \sim |E_0|_1 \dots |E_k|_1 q^{-\binom{k+1}{2}}..$$

2.7 Proof of Theorem 2.6.1

The proof proceeds by induction. The first step is the case $k = 1$ which is given in Section 1.1. Assuming the $(k-1)$st case.

$$\nu_k(l_k) = \sum_{x_0,\dots,x_k} \prod_{0 \le i \le j \le k} f_j(x_j) M_{t_{i,j}}(x_i - x_j).$$

By Fourier inversion, the expression equals

$$\sum_{x_0,\dots,x_k} \sum_{m_0,\dots,m_{k-1}} \prod_{i=1}^{k} \chi((x_{i-1} - x_k) \cdot m_{i-1}) \widehat{M}_{t_{i,k}}(m_{i-1}) \mathcal{T}_{l_{k-1}}(x_0, \dots, x_{k-1}) f_k(x_k)$$

$$= q^{(k+1)d} \sum_{m_0,\dots,m_{k-1}} \widehat{\mathcal{T}}_{l_{k-1}}(-m_0, \dots, -m_{k-1}) \widehat{f_k}(m_0 + \dots + m_{k-1}) \widehat{M}_{t_{1,k}}(m_0) \dots \widehat{M}_{t_{k,k}}(m_{k-1}),$$

where the Fourier transform of $\mathcal{T}_{l_{k-1}}$ is actually the Fourier transform on $\mathbb{F}_q^d \times \dots \times \mathbb{F}_q^d$, k times.

Extracting the zero term and breaking the remaining sum into pieces, this expression equals

$$q^{-dk} \nu_{k-1}(l_{k-1}) \cdot ||f_k||_1 |M_{t_{1,k}}| \dots |M_{t_{k,k}}| +$$

$$q^{(k+1)d} \sum_{\substack{\mathcal{I} \cup \mathcal{I}' = \{0,\dots,k-1\} \\ m_i = 0 \ (i \in \mathcal{I}) \\ m_i \neq 0 \ (i \in \mathcal{I}')}} \widehat{\mathcal{T}}_{l_{k-1}}(-m_0, \dots, -m_{k-1}) \widehat{f_k}(m_0 + \dots + m_{k-1}) \widehat{M}_{t_{1,k}}(m_0) \dots \widehat{M}_{t_{k,k}}(m_{k-1})$$

$$= \text{Mean} + R,$$

where the sum defining R runs over all the partitions of $\{0, \dots, k-1\}$ with the case $\mathcal{I}' = \emptyset$ extracted and used as the main term M above.

We have that

$$|R| \lesssim q^{(k+1)d} \sum_{\substack{\mathcal{I} \cup \mathcal{I}' = \{0,\dots,k-1\} \\ m_i = 0 \ (i \in \mathcal{I}) \\ m_i \neq 0 \ (i \in \mathcal{I}')}}$$

$$\prod_{j\in\mathcal{I}'}||M_{t_{j+1,k}}||_U\cdot q^{-d|\mathcal{I}|}\prod_{h\in\mathcal{I}}|M_{t_{h+1,k}}||\widehat{\mathcal{T}}_{l_{k-1}}(-m_0,\dots,-m_{k-1})||\widehat{f_k}(m_0+\cdots+m_{k-1})|.$$

Then for each term in the sum corresponding to a partition $\mathcal{I}\cup\mathcal{I}'$ we apply Cauchy-Schwarz,

$$\sum_{\substack{m_i=0\ (i\in\mathcal{I})\\ m_i\neq 0\ (i\in\mathcal{I}')}}|\widehat{\mathcal{T}}_{l_{k-1}}(-m_0,\dots,-m_{k-1})||\widehat{f_k}(m_0+\cdots+m_{k-1})|\lesssim A^{1/2}B^{1/2}.$$

Applying Plancherel,

$$\begin{aligned}A\leq\sum_{m_0,\dots,m_{k-1}}|\widehat{\mathcal{T}}_{l_{k-1}}(-m_0,\dots,-m_{k-1})|^2&=q^{-kd}\sum_{x_0,\dots,x_{k-1}}\mathcal{T}_{l_{k-1}}(x_0,\dots,x_{k-1})^2\\&\leq q^{-kd}\nu_{k-1}(l_{k-1})\end{aligned}$$

Now

$$B\leq\sum_{m_i(i\in\mathcal{I}')}\left|\widehat{f_k}\left(\sum_{i\in\mathcal{I}'}m_i\right)\right|^2=q^{|\mathcal{I}'|d}q^{-2d}||f_k||_2^2.$$

This implies that

$$|R|\lesssim q^{(k+1)d}q^{-\frac{kd}{2}}\nu_k(l_k)^{\frac{1}{2}}q^{-d}||f_k||_2$$

$$\sum_{\substack{\mathcal{I}\cup\mathcal{I}'=\{0,\dots,k-1\}\\ m_i=0\ (i\in\mathcal{I})\\ m_i\neq 0\ (i\in\mathcal{I}')}}q^{\frac{|\mathcal{I}'|d}{2}}\prod_{j\in\mathcal{I}'}||M_{t_{j+1,k}}||_U\cdot q^{-d|\mathcal{I}|}\prod_{h\in\mathcal{I}}|M_{t_{h+1,k}}|$$

Since $M_{t_{i,k}}$ can be at best Salem we have that the largest term in the sum occurs when $\mathcal{I}=\emptyset$. We conclude that

$$|R|\lesssim q^{kd}\nu_k(l_k)^{\frac{1}{2}}||f_k||_2\prod_{1\leq j\leq k}||M_{t_{j,k}}||_U$$

The term R is smaller than the Mean if

$$q^{-kd}\nu_{k-1}(l_{k-1})\cdot||f_k||_1\prod_{1\leq j\leq k}|M_{t_{j,k}}|\gtrsim q^{kd}\nu_{k-1}(l_{k-1})^{\frac{1}{2}}||f_k||_2\prod_{1\leq j\leq k}||M_{t_{j,k}}||_U,$$

which in turn gives

$$\nu_{k-1}(l_{k-1})^{\frac{1}{2}}\cdot\frac{||f_k||_1}{||f_k||_2}\gtrsim q^{2kd}\prod_{1\leq j\leq k}\frac{||M_{t_{j,k}}||_U}{|M_{t_{j,k}}|},$$

$$\prod_{0\leq i\leq k-1}||f_i||_1\cdot\frac{||f_k||_1^2}{||f_k||_2^2}\gtrsim q^{3kd}\prod_{1\leq j\leq k}\frac{||M_{t_{j,k}}||_U^2}{|M_{t_{j,k}}|}\prod_{1\leq i\leq j\leq k}\frac{q^d}{|M_{t_{i,j}}|},$$

This completes the proof.

2.8 Proof of Theorem 2.6.3

The proof proceeds by induction. The first step is the case $k = 1$ which is given in Section 1.1. Assuming the $(k-1)$st case.

$$\eta_k(l_k) = \sum_{x_0,\ldots,x_k} \prod_{0\le i\le j\le k} f_j(x_j) N_{t_{i,j}}(x_i, x_j).$$

By orthogonality, the expression equals

$$q^{-k} \sum_{x_0,\ldots,x_k} \sum_{m_0,\ldots,m_{k-1}} \prod_{i=1}^{k} \chi((x_{i-1}\cdot x_k - t_{i,k})\cdot m_{i-1}) \mathcal{D}_{l_{k-1}}(x_0,\ldots,x_{k-1}) f_k(x_k).$$

Extracting the zero frequencies and breaking the remaining sum into pieces, this expression equals

$$q^{-k}\eta_{k-1}(l_{k-1})\cdot ||f_k||_1$$

$$+q^{-k} \sum_{x_0,\ldots,x_k} \mathcal{D}_{l_{k-1}}(x_0,\ldots,x_{k-1}) \sum_{\substack{\mathcal{I}\cup\mathcal{I}'=\{0,\ldots,k-1\} \\ m_i=0\ (i\in\mathcal{I}) \\ m_i\neq 0\ (i\in\mathcal{I}')}} \prod_{j=1}^{k} \chi((x_{j-1}\cdot x_k - t_{j,k})\cdot m_{j-1}) f_k(x_k)$$

$$= \text{Mean} + R,$$

where the inner sum in R runs over all the partitions of $\{0,\ldots,k-1\}$ with the case $\mathcal{I}' = \emptyset$ extracted and used as the main term M above. Then for each term in the sum corresponding to a partition $\mathcal{I}\cup\mathcal{I}'$ we apply Cauchy-Schwarz in $x_0,\ldots,x_{k-1}$,

$$q^{-k} \sum_{x_0,\ldots,x_{k-1}} \mathcal{D}_{l_{k-1}}(x_0,\ldots,x_{k-1}) \sum_{x_k} \sum_{\substack{m_i=0\ (i\in\mathcal{I}) \\ m_i\neq 0\ (i\in\mathcal{I}')}} \prod_{j=1}^{k} \chi((x_{j-1}\cdot x_k - t_{j,k})\cdot m_{j-1}) f_k(x_k)$$

$$= q^{-k} \sum_{x_0,\ldots,x_{k-1}} \mathcal{D}_{l_{k-1}}(x_0,\ldots,x_{k-1}) \sum_{x_k} \sum_{m_i\neq 0\ (i\in\mathcal{I}')} \prod_{j\in\mathcal{I}'}^{k} \chi((x_{j-1}\cdot x_k - t_{j,k})\cdot m_{j-1}) f_k(x_k)$$

$$\le q^{-k} A^{\frac{1}{2}} B^{\frac{1}{2}}$$

$$A = \sum_{x_0,\ldots,x_{k-1}} \mathcal{D}_{l_{k-1}}(x_0,\ldots,x_{k-1})^2 \le \eta_{k-1}(l_{k-1})$$

$$B \le \sum_{x_0,\ldots,x_{k-1}} \left| \sum_{x_k} \sum_{m_i\neq 0\ (i\in\mathcal{I}')} \prod_{j\in\mathcal{I}'}^{k} \chi((x_{j-1}\cdot x_k - t_{j,k})\cdot m_{j-1}) f_k(x_k) \right|^2$$

$$= q^{kd} \sum_{x_k, x'_k} \sum_{\substack{m_i, m'_i \neq 0 \ (i \in \mathcal{I}') \\ m_i x_k = m'_i x'_k}} \prod_{j \in \mathcal{I}'}^{k} \chi(t_{j,k} \cdot (m_{j-1} - m'_{j-1})) f_k(x_k) f_k(x'_k)$$

If $m_i = m'_i$ for any i then $m_i = m'_i$ for every i. Extracting this term in the sum gives

$$B \leq q^{kd+|\mathcal{I}'|} \|f_k\|_2^2 + q^{kd} \sum_{x_k, x'_k} \sum_{\substack{m_i, m'_i \neq 0 \ (i \in \mathcal{I}') \\ m_i \neq m'_i \\ m_i x_k = m'_i x'_k}} \prod_{j \in \mathcal{I}'}^{k} \chi(t_{j,k} \cdot (m_{j-1} - m'_{j-1})) f_k(x_k) f_k(x'_k),$$

then by changing variables,

$$B \leq q^{kd+|\mathcal{I}'|} \|f_k\|_2^2 + q^{kd} \sum_{x_k, x'_k} \sum_{\substack{a_i, b_i \neq 0 \ (i \in \mathcal{I}') \\ x_k = a_i x'_k}} \prod_{j \in \mathcal{I}'}^{k} \chi(t_{j,k} \cdot (b_{j-1}(1 - a_{j-1})) f_k(x_k) f_k(x'_k),$$

which by orthogonality,

$$B \leq q^{kd+|\mathcal{I}'|} \|f_k\|_2^2 + (-1)^{|\mathcal{I}'|} q^{kd} \sum_{x_k, x'_k} \sum_{\substack{a_i, \neq 0 \ (i \in \mathcal{I}') \\ x_k = a_i x'_k}} f_k(x_k) f_k(x'_k),$$

Therefore,

$$\begin{aligned} |B| &\leq q^{kd+|\mathcal{I}'|} \|f_k\|_2^2 + q^{kd} \sum_{x'_k} \sum_{a_0 \neq 0} f_k(a_0 x'_k) f_k(x'_k), \\ &\lesssim q^{kd+k} \|f_k\|_1. \end{aligned}$$

Which gives $|R| \lesssim q^{\frac{kd}{2} - \frac{k}{2}} \|f_k\|_1^{\frac{1}{2}} \eta_{k-1}(l_{k-1})^{\frac{1}{2}}$. Then for the $Mean$ to be greater then $|R|$ one needs

$$q^{-k} \eta_{k-1}(l_{k-1}) \cdot ||f_k||_1 \gtrsim q^{\frac{kd}{2} - \frac{k}{2}} \|f_k\|_1^{\frac{1}{2}} \eta_{k-1}(l_{k-1})^{\frac{1}{2}},$$

which in turn gives,

$$\eta_{k-1}(l_{k-1}) \cdot ||f_k||_1 \gtrsim q^{kd+k},$$

which gives

$$||f_0||_1 \dots ||f_k||_1 \gtrsim q^{kd + \binom{k+1}{2}}.$$

This completes the proof.

CHAPTER III

ERDOS-FALCONER DISTANCE CONJECTURE

3.1 Introduction

The Erdős-Falconer distance conjectures are fundamental problems in geometric combinatorics and measure theory. These conjectures deal with how "dense" a arbitrary subset of a vector space must be to determine a "large" number of distances. The Erdős-Falconer distance problem, in a generalized sense, is a question of how many distances are determined by a set of points. We shall discuss discrete, continuous and finite field formulation of this question and related issues.

3.1.1 The discrete problem

Let E be a finite subset of $\mathbb{R}^d$, $d \geq 2$. Let $\Delta(E) = \{|x-y| : x, y \in E\}$, where $|x| = \sqrt{x_1^2 + \cdots + x_d^2}$. The Erdős distance problem is to determine the smallest possible size of $\Delta(E)$ in terms of the size of E.

Conjecture 3.1.1. *With the notation above, $|\Delta(E)| \gtrapprox |E|^{\frac{2}{d}}$, and taking E to be a piece of the integer lattice shows that one cannot in general do better.*

This problem is far from resolution in any dimension. See, for example, a monograph by Matousek ([44]) and the references contained therein to review the main milestones of the progress towards this conjecture.

3.1.2 The continuous problem

Let $E \subset \mathbb{R}^d$, $d \geq 2$. The Falconer distance problem is to find $s_0 > 0$ such that if the Hausdorff dimension of E is greater than s_0, then the Lebesgue measure of $\Delta(E)$ is positive.

Conjecture 3.1.2. *With the notation above, the Lebesgue measure of* $\Delta(E)$ *is positive provided that the Hausdorff dimension of* E *is greater than* $\frac{d}{2}$.

See [15] for the latest progress and description of techniques. For the connections between the Erdős and Falconer distance problems see, for example, [35].

3.1.3 The finite field problem

In the finite field setting the question turns out to have features of both the Erdős and Falconer distance problems. Let $E \subset \mathbb{F}_q^d$, $d \geq 2$, the d-dimensional vector space over the finite fields $\mathbb{F}_q$. Let $\Delta(E) = \{(x_1 - y_1)^2 + \cdots + (x_d - y_d)^2 : x, y \in E\}$. It is interesting to observe that while the quantity $\|\cdot\|$ is not a distance, in the traditional sense, it is still a natural object in that it is invariant under the action of orthogonal matrices. The first non-trivial result in this context was obtained by Bourgain, Katz and Tao ([7]) using arithmetic-combinatorial methods and the connection of the geometric incidence problem of counting distances with sum-product estimates.

Theorem 3.1.3. *Suppose* $E \subset \mathbb{Z}_p^2$, *where* $p \equiv 3 \mod 4$ *is a prime, and* $|E| \leq p^{2-\epsilon}$. *Then there exists* $\delta = \delta(\epsilon)$ *such that*

$$|\Delta(E)| \geq c|E|^{\frac{1}{2}+\delta}.$$

We note that the conclusion of Theorem 3.1.3 with the exponent $\frac{1}{2}$ follows from the argument due to Erdős ([16]). The condition $|E| \lesssim q^{2-\epsilon}$ addresses the fact that if $E = \mathbb{Z}_p^2$, then $\Delta(E) = \mathbb{Z}_p$ and so $|\Delta(E)| = \sqrt{|E|}$ and no better. The condition $p \equiv 3 \mod 4$ addresses the fact that if conversely $p \equiv 1 \mod 4$, the field $\mathbb{F}_p$ contains an element i such that $i^2 = -1$. This would allow one to take

$$E = \{(t, it) : t \in \mathbb{Z}_p\} \tag{3.1.4}$$

and it is straightforward to check that while $|E| = p$, $|\Delta(E)| = 1$ as all the distances between the elements of the set are identically 0.

In view of the examples cited in the previous paragraph, Iosevich and Rudnev ([34]) formulated the Erdős-Falconer conjecture as follows.

Conjecture 3.1.5. *Let $E \subset \mathbb{F}_q^d$ such that $|E| \geq C_\epsilon q^{\frac{d}{2}+\epsilon}$. Then there exists $c > 0$ such that*

$$|\Delta(E)| \geq cq.$$

In the following section we shall use a Fourier analytic approach to this problem, developed in [34], which led to the following result.

Theorem 3.1.6. *([34]) Suppose that $E \subset \mathbb{F}_q^d$ and $|E| \geq 2q^{\frac{d+1}{2}}$. Then $\Delta(E) = \mathbb{F}_q$.*

Arithmetic examples constructed in [31] show that this result, in general, is sharp. However, we shall argue below that this is not the end of the story. Observe that in the formulation of Conjecture 3.1.5 one asks for the *positive proportion* of distances in $\mathbb{F}_q$, while Theorem 3.1.6 guarantees that *all* distances in $\mathbb{F}_q$ occur, being generated by E. The latter question is closely related to what in the discrete Euclidean setting is known as the Erdős *single distance* conjecture, which says that a single distance in $\mathbb{R}^2$ cannot occur more than $cn^{1+\epsilon}$ times where n is the cardinality of the underlying point set E. It is tempting to strengthen the claim of Conjecture 3.1.5 to cover all distances. However, we shall see below that even the weak form of this conjecture (3.1.5) is not true. This shows that the Theorem (3.1.6) is essentially sharp. This underlines the difference between the finite field setting and the Euclidean setting where the Erdős-Falconer distance conjecture, while far from being proved, is still strongly believed.

3.2 The Single Distance Problem

In this section we prove Theorem 3.1.6. While the literal interpretation of Theorem 3.1.6 is that if $|E| \geq 2q^{(d+1)/2}$ then every distance is realized. It gives an immediate bound on the number of points that determine a single distance.

Corollary 3.2.1 (Single Distance Problem)**.** *Let $E \subset \mathbb{F}_q^d$ such that $|\Delta(E)| = 1$. Then*

$$|E| < \frac{1}{2} q^{\frac{d-1}{2}}.$$

Now for $t \in \mathbb{F}_q$ define

$$\nu(t) = |\{(x, y) \in E \times E : \|x - y\| = t\}|.$$

This counts the number of pairs that give rise to a distance t. Determining the size of this set is equivalent to counting the incidences between the difference of to elements of E and sphere of radius t. That is

$$\nu(t) = \sum_{x,y \in E} S_t(x - y), \tag{3.2.2}$$

where $S_t(\cdot)$ is the indicator function of the set $\{x \in \mathbb{F}_q^d : \|x\| = t\}$.

In view of Corollary 2.2.6 the Fourier decay of the sphere will be central to our discussion. Specifically we give an argument of [34] to show that spheres of non-zero radius are Salem and of appropriate size.

Lemma 3.2.3 (Salem property of the sphere)**.** *Let S_t, $t \in \mathbb{F}_q^*$ be defined as above. If $m \neq (0, \ldots, 0)$ then*

$$|\widehat{S}_t(m)| \leq 2q^{-\frac{d+1}{2}}, \tag{3.2.4}$$

and

$$\widehat{S}_t(0, \ldots, 0) = q^{-d}|S_t| = (1 + o(1))q^{-1}, \tag{3.2.5}$$

Applying Lemma 3.2.3 to Corollary 2.2.6 immediately yields the result. In order to prove Lemma 3.2.3 we first prove the following result.

Lemma 3.2.6. *Then for $m \in \mathbb{F}_q^d$,*

$$\widehat{S}_t(m) = q^{-1}\delta(m) + K^d q^{-\frac{d+2}{2}} \sum_{j \in \mathbb{F}_q^*} \chi\left(\frac{\|m\|}{4j} + tj\right) \kappa^d(-j), \tag{3.2.7}$$

where the notation $\delta(m) = 1$ if $m = (0 \ldots, 0)$ and $\delta(k) = 0$ otherwise. The constant K equals ± 1 or $\pm i$, depending on q, and κ is the quadratic multiplicative character (or the Legendre symbol) of $\mathbb{F}_q^*$.

Proof of Lemma 3.2.6. For any $m \in \mathbb{F}_q^d$, we have

$$\begin{aligned}
\widehat{S}_t(m) &= q^{-d} \sum_{x \in \mathbb{F}_q^d} q^{-1} \sum_{j \in \mathbb{F}_q} \chi(j(\|x\| - t)) \chi(-x \cdot m) \\
&= q^{-1}\delta(m) + q^{-d-1} \sum_{j \in \mathbb{F}_q^*} \chi(-jt) \sum_x \chi(j\|x\|) \chi(-x \cdot m) \qquad (3.2.8) \\
&= q^{-1}\delta(m) + K^d q^{-\frac{d+2}{2}} \sum_{j \in \mathbb{F}_q^*} \chi\left(\frac{\|m\|}{4j} + jt\right) \kappa^d(-j).
\end{aligned}$$

In the line before last we have completed the square, changed j to $-j$, and used d times the Gauss sum

$$\sum_{c \in \mathbb{F}_q} \chi(jc^2) = \kappa(j) \sum_{c \in \mathbb{F}_q} \kappa(c)\chi(c) = \kappa(j) \sum_{c \in \mathbb{F}_q^*} \kappa(c)\chi(c) = K\sqrt{q}\,\kappa(j), \qquad (3.2.9)$$

where $K = \pm i$ or ± 1, depending on q and $\kappa(0) = 0$. See any standard text on finite fields for background and basic results about Gauss sums. Note that we have assumed that $\chi = \chi_1$ is the principal additive character of the field $\mathbb{F}_q$.

We remark that for even d, the sum in the last line of (3.2.8) is the Kloosterman sum, while for odd d the presence of the quadratic character κ would reduce it via the Gauss sum to a "cosine", which is nonzero only if $\theta^2 \equiv \frac{y\|m\|}{4}$ is a square in $\mathbb{F}_q^*$, in which case

$$\sum_{j \in \mathbb{F}_q^*} \chi\left(\frac{\|m\|}{4j} + jy\right) \kappa(-j) = K\sqrt{q}\,\kappa(-\|m\|^2)(\chi(2\theta) + \chi(-2\theta)). \qquad (3.2.10)$$

□

The conclusion of Lemma 3.2.3 now follows from the following classical estimate due to A. Weil ([59]).

Theorem 3.2.11. *Let*

$$K(a) = \sum_{s \neq 0} \chi(as + s^{-1})\psi(s),$$

where, once again, ψ is a multiplicative character on $\mathbb{F}_q^*$. Then

$$|K(a)| \leq 2\sqrt{q}$$

if $a \neq 0$.

3.3 The Distance Problem

In [31] the author along with A. Iosevich, D. Koh, M. Rudnev that the arithmetic of the problem makes the exponent $\frac{d+1}{2}$ best possible in **odd dimensions**, at least in general fields. In even dimensions it is still possible that the correct exponent is $\frac{d}{2}$, in analogy with the Euclidean case. We give these examples here.

Theorem 3.3.1. *([31]) The Conjecture 3.1.5 is false. More precisely, there exists $c > 0$ and $E \subset \mathbb{F}_q^d$, d is odd, such that*

$$|E| \geq cq^{\frac{d+1}{2}} \quad \text{and} \quad \Delta(\mathrm{E}) \neq \mathbb{F}_{\mathrm{q}}.$$

Proof. Proof of Theorem 3.3.1

We begin by proving the following lemma.

Lemma 3.3.2. *We say that $v \in \mathbb{F}_q^d$, $v \neq (0, \ldots, 0)$, is a null vector if $v \cdot v = 0$. If $d \geq 4$ is even, then there exists $\frac{d}{2}$ mutually orthogonal null vectors $v_1, \ldots, v_{\frac{d}{2}}$ in $\mathbb{F}_q^d$.*

To prove the lemma, suppose there exists an element $i \in \mathbb{F}_q$ such that $i^2 = -1$. Consider the collection of vectors

$$v_1 = (1, i, 0, 0, \ldots, 0, 0),\ v_2 = (0, 0, 1, i, \ldots, 0, 0), \ldots, v_{\frac{d}{2}} = (0, 0, \ldots, 0, 0, 1, i).$$

It follows immediately that

$$v_k \cdot v_l = 0$$

for every $k, l = 1, \ldots, \frac{d}{2}$.

If -1 is not a square, then from simple counting there exists a null vector

$$v_1 = (a, b, c, 0 \ldots, 0),$$

with all $a, b, c \in \mathbb{F}_q^*$. Suppose, d is a multiple of 4. Then we may take the null vector

$$v_2 = (0, -c, b, a, \ldots, 0)$$

noting that this vector is orthogonal to

v_1. In this same way we may now take the null vector

$$v_3 = (0, 0, 0, 0, a, b, c, 0, \ldots, 0),$$

and find a corresponding null vector v_4 which is orthogonal to v_3 as well as trivially orthogonal to v_1 and v_2. Continuing in this manner we obtain $\frac{d}{2}$ mutually orthogonal null vectors.

The proof will be complete now if we can also treat the case $d = 6$. In this case Let

$$v_1 = (a, b, c, 0, 0, 0), \quad v_2 = (0, 0, 0, a, b, c) \text{ where } a^2 + b^2 + c^2 = 0.$$

Consider two three-vectors

$$w_1 = (-b/c, a/c, 0) \text{ and } w_2 = (0, -c/a, b/a).$$

Let $s \in \mathbb{F}_q$ be such that

$$e_1 = w_1 + sw_2$$

satisfies $||e_1|| = 1$. Such s exists, by the Lagrange theorem on quadratic forms (or can be verified by direct calculation).

Consider now a six-vector $v_3 = [e_1, w_1]$. By construction, v_3 is orthogonal to both v_1 and v_2. It is also a null vector, as $e_1 \cdot e_1 = 1$, while $w_1 \cdot w_1 = -1$.

This completes the proof of Lemma 3.3.2.

Let $d = 2m + 1$, then from the above lemma there are m mutually orthogonal null vectors $v_1, \ldots, v_m$, such that their dth coordinate is zero. Now let $A \subset \mathbb{F}_q$ be an arithmetic progression of length n and $u = (0, \ldots, 0, 1)$. Consider the set

$$E = \{t_i v_i + au \text{ for } i = 1, \ldots, m : t_i \in \mathbb{F}_q, a \in A\}.$$

We have

$$|E| = q^m \cdot |A| = q^m \cdot n.$$

For any $x, y \in E$ we have from orthogonality that

$$\|x - y\| = \|t_1 u_1 + av - t_2 u_2 - a' v_2\| = (a - a')^2,$$

so $|\Delta(E)| \leq 2n - 1$.

It follows that if we choose $2n = cq$, we have constructed, for any small c, a set E of $\frac{1}{2} c q^{\frac{d+1}{2}}$ generating fewer than cq distances. This completes the proof in the case $d \geq 5$.

If $d = 3$, and -1 is a square, take the null vector $v = (1, i, 0)$ and $u = (0, 0, 1)$. If -1 is not a square, take the null vector $v = (a, b, c)$ such that no entry can be zero, and let $u = (-b, a, 0)$. The proof then proceeds as above. □

3.4 Distance Problem for Product Sets

The example given in Theorem 3.3.1 showing that the $\frac{d+1}{2}$ is sharp in odd dimensions is very radial in nature and this led the author along with A. Iosevich ([29]) to consider classes of sets that possess a certain amount of product structure.

Conjecture 3.4.1. *(Distance Conjecture for Product Sets)*

Let $E \subset \mathbb{F}_q^d, d \geq 2$ be a product-set. If $|E| \gtrsim q^{\frac{d}{2}}$ then

$|\Delta(E)| \gtrsim q.$ (Falconer)

If q is prime then regardless of the size of E,

$|\Delta(E)| \gtrsim |E|^{\frac{2}{d}}.$ (Erdös)

We shall see that if $E \subset \mathbb{F}_q^2$ satisfies $|E| \geq q^{\frac{4}{3}}$ and E is a product set, then $|\Delta(E)| \geq cq$. This is in line with Wolff's result for the Falconer conjecture in the plane which says that the Lebesgue measure of the set of distances determined by a subset of the plane of Hausdorff dimension greater than $\frac{4}{3}$. In higher dimensions one obtains a positive proportion of the distances for products sets of size $\gtrsim q^{\frac{d}{2} + \frac{1}{4} + \frac{1}{4(2d-1)}}$, improving an analog of Erdogan's ([15]) result in Euclidean space for general sets of Hausdorff dimension great than $\frac{d}{2} + \frac{1}{3}$.

This result is an immediately corollary to Theomem 2.4.7 where $Q(x) = x \cdot x = \|x\|$.

Theorem 3.4.2. *[29] Let $E = A_1 \times A_2 \times \cdots \times A_d$, where $E \subset \mathbb{F}_q^d$.*

If $|E| \geq q^{\frac{d}{2}+\frac{1}{4}+\frac{1}{4(2d-1)}}$ *then* $|\Delta(E)| \geq \frac{1}{3}q$.

If $|E| \leq q^{\frac{d}{2}+\frac{1}{4}+\frac{1}{4(2d-1)}}$ *then* $|\Delta(E)| \geq \frac{1}{3}\frac{|E|^{2-\frac{1}{d}}}{q^{d-1}}$.

As one would expect given the existence of subfields this estimate is only non-trivial in the range $|E| > q^{\frac{d}{2}}$. Unfortunately, this estimate also decays as the size of the set gets closer to $\frac{d}{2}$. It is possible to give a combinatorial argument similar to that of Glibichuk [24] which avoids this in sufficiently high dimensions. However, we do not give these arguments here.

3.5 Ubiquity of Simplices

Many problems in combinatorial geometry ask, in one form or another, whether a certain structure must be present in a set of sufficiently large size. Perhaps the most celebrated result of this type is Szemeredi's theorem ([54]) which says that if a subset of the integers has positive density, then it contains an arbitrary large arithmetic progression. The conclusion has recently been extended to the subsets of prime numbers by Green and Tao ([26]). In Euclidean space, a result due to Katznelson and Weiss ([19]) says that a subset of Euclidean space of positive Lebesgue upper density contains every sufficiently large distance. A subsequent result by Bourgain ([4]), says that a subset of $\mathbb{R}^k$ of positive Lebesgue upper density contains an isometric copy of all large dilates of a set of k points spanning a $(k-1)$-dimensional hyperplane. Ergodic theory has been used to show that positive upper density implies that the set contains a copy of a sufficiently large dilate of every convex polygon with finitely many sides. See, for example, a recent survey by Bryna Kra ([41]).

Let $\mathbb{F}_q^d$ be a d-dimensional vector space over a finite field $\mathbb{F}_q$ of odd characteristic. A plausible analogy to Bourgain's result ([4]) in this context would be to consider

whether a subset of positive density contains a isometric copy of a set of $k+1$ points spanning a k-dimensional hyperplane. It turns out however, that the positive density condition is much too strong in the context of vector spaces over finite fields and the same conclusion follows from a much weaker assumption on the size of the underlying set.

Definition 3.5.1. Let a k-simplex be a set of $k+1$ points in general position, which means that no $n+1$ of these points, $n \leq k$, lie in a $(n-1)$-dimensional sub-space of $\mathbb{F}_q^d$. In addition none of the $k+1$ points are a zero distance from each other.

Definition 3.5.2. We say that a linear transformation T on $\mathbb{F}_q^d$ is an isometry if

$$||Tx|| = ||x||.$$

The question we ask in this paper is how large does $E \subset \mathbb{F}_q^d$ need to be in order to be sure that it contains a copy of every k-simplex. Our main result is the following.

Theorem 3.5.3. *[28] Let $E \subset \mathbb{F}_q^d$, $d > \binom{k+1}{2}$, such that $|E| \geq Cq^{\frac{k}{k+1}d}q^{\frac{k}{2}}$ with a sufficiently large constant $C > 0$. Then E contains an isometric copy of every k-simplex.*

Note that we obtain non-trivial results only when $k << \sqrt{d}$. Nevertheless, in that range we are able to dip considerably below the positive density condition on the underlying set E.

The method of proof relies on the fact that orthogonal transformations on $\mathbb{F}_q^d$ are isometries. A "distance representation" of a simplex is then used to reduce Theorem 3.5.3 to an appropriate weighted incidence theorem for spheres and points. The key idea in the proof is to show at each step of an inductive argument that a collection of distances among vertices of a given simplex can not only be realized, but actually occur a "statistically correct" number of times.

Following Section 1.6 consider tbe indicator function of a k-simplex in a subset $E \subset \mathbb{F}_q^d$ on $k+1$ points recursively by setting

$$\mathcal{T}_{l_k}(x_0, \dots, x_k) = \mathcal{T}_{l_{k-1}}(x_0, \dots, x_{k-1}) E(x_k) St_{1,k}(x_0 - x_k) S_{t_{2,k}}(x_1 - x_k) \dots S_{t_{k,k}}(x_{k-1} - x_k),$$

recursively for $l_k = l_{k-1} \cup \{t_{1,k}, \dots t_{k,k}\}, t_{i,j} \in \mathbb{F}_q^*$ where

$$\mathcal{T}_{l_1}(x_0, x_1) = S_{t_{1,1}}(x_0 - x_1) f_0(x_0) f_1(x_1).$$

Then

$$\nu_k(l_k) = \sum_{x_0, \dots, x_k} \mathcal{T}_{l_{k-1}}(x_0, \dots, x_{k-1}) E(x_k) S_{t_{1,k}}(x_0 - x_k) \dots S_{t_{k,k}}(x_{k-1} - x_k)$$

for $l_k = l_{k-1} \cup_{\{} t_{1,k}, \dots t_{k,k}\}, t_{i,j} \in \mathbb{F}_q^*$ where

$$\nu_1(l_1) = \sum_{x_0, \dots, x_k} \mathcal{T}_{l_1}(x_0, x_1) = \sum_{x_0, \dots, x_k} S_{t_{1,1}}(x_0 - x_1) E(x_0) E(x_1).$$

This representation does not, in general, always embody a simplex as $\mathcal{T}_{l_k}^k$ is not guaranteed to be in general position. However, as we show below, "legitimate" k-simplices are equivalent up to an orthogonal transformation.

Lemma 3.5.4. *Let P be a simplex with vertices $V_0, V_1, \dots, V_k$, $V_j \in \mathbb{F}_q^d$. Let P' be another simplex with vertices $V_0', V_1', \dots, V_k'$. Suppose that*

$$||V_i - V_j|| = ||V_i' - V_j'|| \tag{3.5.5}$$

for all i, j. Then there exists an orthogonal, affine transformation O on $\mathbb{F}_q^d$ such that $O(P) = P'$.

Therefore by Theorem 2.6.2 we have the following result which immediately implies Theorem 3.5.3.

Theorem 3.5.6. *[28] Let $E \subset \mathbb{F}_q^d$, $d > \binom{k+1}{2}$, such that $|E| \geq C q^{\frac{k}{k+1} d} q^{\frac{k}{2}}$, with a sufficiently large constant C. Then for every side length set l_k, $l_k \in (\mathbb{F}_q^*)^{\binom{k+1}{2}}$ we have that $\nu_k(l_k) > 0$. Furthermore,*

$$\nu_k(l_k) \sim |E|^{k+1} q^{-\binom{k+1}{2}}.$$

3.5.1 Proof of Lemma 3.5.4

To prove Lemma 3.5.4, let $\pi_r(x)$ denote the rth coordinate of x. There is no harm in assuming that $V_0 = (0, \ldots, 0)$. We may also assume that $V_1, \ldots, V_k$ are contained in $\mathbb{F}_q^k$. The condition (3.5.5) implies that

$$\sum_{r=1}^{k} \pi_r(V_i)\pi_r(V_j) = \sum_{r=1}^{k} \pi_r(V_i')\pi_r(V_j'). \tag{3.5.7}$$

Let T be the linear transformation uniquely determined by the condition

$$T(V_i) = V_i'.$$

In order to prove that T is orthogonal, it suffices to show that

$$||Tx|| = ||x||$$

for any $x \neq (0, \ldots, 0)$.

Since V_js form a basis, by assumption, we have

$$x = \sum_i t_i V_i,$$

so it suffices to show that

$$||x|| = \sum_r \sum_{i,j} t_i t_j \pi_r(V_i)\pi_r(V_j)$$

$$= \sum_r \sum_{i,j} t_i t_j \pi_r(V_i')\pi_r(V_j') = ||Tx||,$$

which follows immediately from (3.5.7).

Observe that we used the fact that orthogonality of T, the condition that $T^t \cdot T = I$ is equivalent to the condition that $||Tx|| = ||x||$. To see this observe that to show that $T^t \cdot T = I$ it suffices to show that $T^t T x = x$ for all non-zero x. This, in turn, is equivalent to the statement that

$$< T^t T x, x >= ||x||,$$

where

$$< x, y >= \sum_{i=1}^{k} x_i y_i.$$

Now,

$$< T^t T x, x >=< Tx, Tx >$$

by definition of the transpose, so the stated equivalence is established. This completes the proof of Lemma 3.5.4.

CHAPTER IV

THE DOT PRODUCT PROBLEM

By analogy with the distance set $\Delta(E)$, let us introduce the set of dot products

$$\Pi(E) = \{x \cdot y = x_1y_1 + \ldots + x_dy_d : x, y \in E\},$$

Theorem 4.0.8. *[27],[31] Let $E \subset \mathbb{F}_q^d$ such that $|E| > q^{\frac{d+1}{2}}$. Then*

$$\mathbb{F}_q^* \subseteq \Pi(E). \tag{4.0.9}$$

Furthermore, if $|E| > q^{\frac{d+2}{2}}$. Then

$$\mathbb{F}_q = \Pi(E). \tag{4.0.10}$$

This result cannot in general be improved in the following sense:

i. Whenever $\mathbb{F}_q$ is a quadratic extension, for any $\epsilon > 0$ there exists $E \subset \mathbb{F}_q^d$ of size $\approx q^{\frac{d+1}{2}-\epsilon}$, such that $|\Pi(E)| = o(q)$. In particular, the set of dot products does not contain a positive proportion of the elements of $\mathbb{F}_q$.

ii. For $d = 4m + 3$, $m \geq 0$, for any $q \gg 1$ and any $t \in \mathbb{F}_q^*$, there exists E of cardinality $\approx q^{\frac{d+1}{2}}$, such that $t \notin \Pi(E)$.

The proof 4.0.9 and 4.0.10 follows immediately from Theorem 2.2.6 is via Fourier analysis. It was pointed out to the authors by Seva Lev that an alternate approach to (4.0.10) is via a graph theoretic result due to Alon and Krivelevich. See, [2] and the references contained therein.

4.0.2 Proof of Theorem 4.0.8

We now turn our attention to proving (i) and (ii) of Theorem 4.0.8. To address the statement (i) of the theorem, let us consider the case $d = 2$ and $q = p^2$, where p is

a power of a large prime. The higher dimensional case follows similarly. Let a be a generator of the cyclic group $\mathbb{F}_q^*$. Then $a^{q-1} = 1$ and a^{p+1} is the generating element for $\mathbb{F}_p^*$ since $p + 1 = \frac{q-1}{p-1}$.

Let A be a proper cyclic subgroup of $\mathbb{F}_q^*$ which properly contains $\mathbb{F}_p^*$. Let s be a divisor of $p + 1$ and let the generating element of A be $\alpha = a^s$. Note that we are taking advantage of the fact that $\mathbb{F}_q^*$ is cyclic. Consider the unit circle

$$\{x \in \mathbb{F}_q^2 : x_1^2 + x_2^2 = 1\},$$

and its subset

$$C_p = \{x \in \mathbb{F}_p^2 : x_1^2 + x_2^2 = 1\}.$$

By elementary number theory (or Lemma 3.2.6), the cardinality of C_p is $p \mp 1$, depending on whether negative one is or is not a square in $\mathbb{F}_p^*$. Clearly, for any $u, v \in C_p$, $u \cdot v \in \mathbb{F}_p$. Let

$$E = \{tu : t \in A, u \in C_p\}. \tag{4.0.11}$$

For any $x, y \in E$, the dot product $x \cdot y$, if nonzero, will lie in A. Indeed, if $x = tu$, $y = \tau v$, according to (4.0.11), then

$$x \cdot y = t\tau(u \cdot v) \in A \cup \{0\},$$

since A contains $\mathbb{F}_p^*$. The cardinality of E is

$$|E| = \frac{p \mp 1}{2}|A| = \frac{p \mp 1}{2} \cdot \frac{q-1}{s},$$

where s is a divisor of $p + 1$. Taking $s = 2$ works and shows that less than half the elements of $\mathbb{F}_q^*$ may be realized as dot products determined by a set of size in excess of $\frac{1}{4} \cdot q^{\frac{3}{2}}$. In order to see that $\{x \cdot y : x, y \in E\}$ does not in general even contain a positive proportion of the elements of $\mathbb{F}_q$ if $|E| \ll q^{\frac{3}{2}}$, we need to produce a sequence of primes, or prime powers, such that $p + 1$ has large divisors. For the reader who does not believe in the existence of infinitely many generalized Fermat primes (those in the form $a^{2^n} + 1$), we can always do it using field extensions as follows.

Consider the family of prime powers

$$\{p^{2k+1} : k = 1, 2 \dots\}$$

and observe that

$$p + 1 \mid p^{2k+1} + 1.$$

This completes the construction demonstrating the claim (i). To take care of the higher dimensional case, simply replace circles by spheres and the same argument goes through.

The claim (ii) of the Corollary will follow immediately from the construction used in the proof of the item (v) of Theorem 4.2.1 (see Section 4.2.3). On any sphere $\{x \in \mathbb{F}_q^d : x_1^2 + \cdots + x_d^2 = r\}$, with $d = 4m + 3$, we can find a set E, with $|E| \gtrsim q^{\frac{d+1}{2}}$, such that the dot product $t = -r$ is not achieved.

4.1 The Dot Product Problem for Product Sets

As with distance sets the example given in Theorem 3.3.1 showing that the $\frac{d+1}{2}$ is sharp is very radial.

Conjecture 4.1.1. *(Dot Product Conjecture for Product Sets) Let $E \subset \mathbb{F}_q^d, d \geq 2$ be a product-set. If $|E| \gtrsim q^{\frac{d}{2}}$ then $|\Pi(E)| \gtrsim q$. If q is prime then regardless of the size of E, $|\Pi(E)| \gtrsim |E|^{\frac{2}{d}}$.*

It is a result due to Glibichuk that [23] that partially proves this for $d \geq 4$.

Theorem 4.1.2. *[23] Let $E \subset \mathbb{F}_q^d, d \geq 4$ be a product set such that $q^{\frac{d}{2}}$ then $|\Pi(E)| \gtrsim q$.*

We have the following result.

Theorem 4.1.3. *[27],[31], [29] Let $E = A_1 \times A_2 \times \cdots \times A_d$, where $E \subset \mathbb{F}_q^d$.*

If $|E| \geq q^{\frac{d}{2}+\frac{1}{4}+\frac{1}{4(2d-1)}}$ *then* $|\Pi(E)| \geq \frac{1}{2}q$.

If $|E| \leq q^{\frac{d}{2}+\frac{1}{4}+\frac{1}{4(2d-1)}}$ *then* $|\Pi(E)| \geq \frac{1}{2}\frac{|E|^{2-\frac{1}{d}}}{q^{d-1}}$.

4.2 Erdos-Falconer Distance Conjecture on a Sphere

We shall see however, that the exponent predicted by Conjecture 3.1.5 does hold for subsets of the sphere in

$$S^{d-1} = S = \{x \in \mathbb{F}_q^d : x_1^2 + \cdots + x_d^2 = 1\}$$

in even dimensions. While it is possible that in some cases this exponent may be further improved for this class of sets under some circumstances, we provide examples showing that if one is after all the distances, and not a positive proportion, then getting a better index is not in general possible. This is geometrically analogous to the general case, for since S^{d-1} is $(d-1)$-dimensional variety in $\mathbb{F}_q^d$, it makes sense that the sharp index should be $\frac{(d-1)+1}{2} = \frac{d}{2}$. The motivation for studying the Erdő-Falconer distance problems for subsets of the sphere is not limited by the consideration that it provides a large set of sets for which Conjecture 3.1.5 holds. For example, Erdős original argument that shows that N points in $\mathbb{R}^2$ determine $\gtrsim N^{\frac{1}{2}}$ distances proceeded as follows. Choose one of the points in the set and draw circles of every possible radius centered at this point such that each circle contains at least one other point of the set. Suppose that the number of such circles is t. If $t \geq N^{\frac{1}{2}}$, we are done. If not, there exists a circle containing $\geq N/t$ points and these points, by an elementary argument, determine $\geq N/2t$ distinct distances. Comparing t and $N/2t$ yields the conclusion. In higher dimension we may proceed by induction with the induction hypothesis being the number of distances determined by points on a sphere. Thus one may view the distribution of distances determined by points on a sphere as a natural and integral component of the general Erdős distance problem.

Theorem 4.2.1. *Let $E \subset \mathbb{F}_q^d$, $d \geq 3$, be a subset of the sphere $S = \{x \in \mathbb{F}_q^d : \|x\| = 1\}$.*

1. *Suppose that $|E| \geq Cq^{\frac{d}{2}}$ with a sufficiently large constant C. Then there exists*

$c > 0$ *such that*

$$|\Delta(E)| \geq cq. \tag{4.2.2}$$

2. *If d is even, then under the same assumptions as above,*

$$\Delta(E) = \mathbb{F}_q. \tag{4.2.3}$$

3. *If d is even, there exists $c > 0$ and $E \subset S$ such that*

$$|E| \geq cq^{\frac{d}{2}} \quad \text{and} \quad \Delta(\mathrm{E}) \neq \mathbb{F}_{\mathrm{q}}. \tag{4.2.4}$$

4. *If d is odd and $|E| \geq Cq^{\frac{d+1}{2}}$ with a sufficiently large constant $C > 0$, then*

$$\Delta(E) = \mathbb{F}_q. \tag{4.2.5}$$

5. *If d is odd, there exists $c > 0$ and $E \subset S$ such that*

$$|E| \geq cq^{\frac{d+1}{2}} \quad \text{and} \quad \Delta(\mathrm{E}) \neq \mathbb{F}_{\mathrm{q}}. \tag{4.2.6}$$

4.2.1 Proof of 4.2.2

Since $E \subset S$,

$$\|x - y\| = (x - y) \cdot (x - y) = 2 - 2x \cdot y,$$

so counting distances on the sphere is the same as counting dot products.

Since now E is a subset of the sphere, it does not contain the origin and

$$|E \cap l_k| \leq 2.$$

Therefore by Theorem 2.2.13 we get the desired conclusion. The case $x \cdot y = 0$ will be addressed further in Section 4.2.2.

4.2.2 Proof of 4.2.3

We now turn to the proof of (4.2.3). We will not distinguish between even and odd d until it becomes necessary. We proceed by writing

$$\nu(t) = |E|^2 q^{-1} + R(t),$$

and apply the Cauchy-Schwartz inequality to $R^2(t)$. This time, however, instead of dominating the sum over E by the sum over $\mathbb{F}_q^d$, we dominate the sum over E by the sum over the sphere S using the assumption that $E \subset S$. This yields

$$\begin{aligned} R^2(t) &\leq q^{-2}|E| \sum_{x \in S} \sum_{s,s' \neq 0} \sum_{y,y' \in E} \chi(sx \cdot y - s'x \cdot y')\chi(t(s'-s)) \\ &= q^{d-2}|E| \sum_{s,s' \neq 0} \chi(t(s'-s)) \sum_{y,y' \in E} \widehat{S}(s'y' - sy) \qquad (4.2.7) \\ &= I + II, \end{aligned}$$

where the term I corresponds to the case $s'y' = sy$. One of the keys to this argument is that since E is a subset of the sphere, $sy = s'y'$ can only happen if $y = \pm y'$ and $s = \pm s'$.

Lemma (3.2.6) below tells us that $\widehat{S}(0, \dots, 0) = q^{-1} +$ lower order terms (unless $d = 2$), and it follows that

$$I \leq q^{d-2}|E|^2. \qquad (4.2.8)$$

To estimate the term II, we have to use the explicit form of the Fourier transform of the discrete sphere. For the reader's convenience we replicate one of the arguments in [34].

We now return to the proof of (4.2.3). From now on, let K, K' stand for complex numbers of modulus 1 that may change from line to line. We now continue with the estimation of the term II in (4.2.7). Namely, we have

$$II = q^{d-2}|E| \sum_{y,y' \in E} \sum_{s,s' \in \mathbb{F}_q^*, s'y' \neq sy} \widehat{S}(s'y' - sy)\chi(t(s'-s)) = III + IIII,$$

where the term III corresponds to the case the case $y = y'$, when $s \neq s'$. Then we have

$$III = q^{d-2}|E| \sum_{y \in E} \sum_{s,s' \in \mathbb{F}_q^*, s \neq s'} \widehat{S}((s'-s)y)\chi(t(s'-s)).$$

Observe that $s' - s$ runs through each value in $\mathbb{F}_q^*$ exactly $q-1$ times. Also, $||y|| = 1$ since $E \subset S$. Therefore, using Lemma 3.2.7, we have

$$\begin{aligned} III &= Kq^{d-2}|E| \textstyle\sum_{y \in E}(q-1)q^{-\frac{d+2}{2}} \sum_{s,j \in \mathbb{F}_q^*} \chi\left(\frac{s^2}{4j} + ts + j\right) \eta^d(j) \\ &= Kq^{d-2}|E| \textstyle\sum_{y \in E}(q-1) \cdot q^{-\frac{d+2}{2}} \sum_{s,j \in \mathbb{F}_q^*} \chi\left(\frac{(s+2jt)^2}{4j} - jt^2 + j\right) \eta^d(j) \quad (4.2.9) \\ &= K\tfrac{q-1}{q} q^{\frac{d-4}{2}} |E| \textstyle\sum_{y \in E} \sum_{j \in \mathbb{F}_q^*} \chi(j - jt^2)\eta^d(j)[-\chi(jt^2) + K'\sqrt{q}\eta(j)], \end{aligned}$$

where the last line follows by (3.2.9).

We now consider the case $t^2 = \|y\| = 1$. We have

$$III_{t^2=1} \approx q^{\frac{d-4}{2}}|E| \sum_{y \in E} \sum_{j \in \mathbb{F}_q^*} \eta^d(j)[-\chi(j) + K\sqrt{q}\eta(j)].$$

Since $\sum_{j \in \mathbb{F}_q^*} \eta(j) = 0$, the worst case scenario is when d is odd. Then the summation in j contributes an extra factor $q-1$ to $K\sqrt{q}$ in the last bracket. If d is even then the summation in j is the Gauss sum, which is smaller by the factor of $\sqrt{q}$. In either case, we have

$$|III_{t^2=1}| \leq 2q^{\frac{d-1}{2}}|E|^2. \quad (4.2.10)$$

If $t^2 \neq 1$, the estimate (4.2.10) improves by factor $\sqrt{q}$, as the worst case scenario is now when d is even, and it only contributes a Gauss sum to the term $K\sqrt{q}$:

$$\sum_{j \in \mathbb{F}_q^*} \chi(j - jt^2)\eta^d(j)[-\chi(jt^2) + K\sqrt{q}\eta(j)]. \quad (4.2.11)$$

Observe however, that in either case, for $d \geq 2$ the estimate for the term III is majorated by (4.2.8).

Finally, let us consider the term $IIII$:

$$IIII = q^{d-2}|E| \sum_{y,y' \in E, y \neq y'} \sum_{s,s' \in \mathbb{F}_q^*} \widehat{S}(s'y' - sy)\chi[t(s'-s)] \tag{4.2.12}$$

Our goal is to prove the following estimate:

$$|IIII = IIII(t)| \ \lesssim \ q^{\frac{d-4}{2}}|E|^3 + q^{\frac{d-2}{2}}|E| \sup_{\tau \in \mathbb{F}_q} |R(\tau)|. \tag{4.2.13}$$

and we are able to do it only for even values of d. (For odd d the estimate will be definitely worse by $\sqrt{q}$ for $t^2 = 1$ and seems to be highly non-trivial for other values of t, see (4.2.20) below.) Note that we can always write $\sup_{\tau \in \mathbb{F}_q} \nu(\tau)$ instead of $\sup_{\tau \in \mathbb{F}_q} |R(\tau)|$, as the regular term $\frac{|E|^2}{q}$ can be absorbed into the first term in (4.2.13).

We verify (4.2.13) below and will now show how it suffices to complete the proof of (4.2.3). Indeed, assuming (4.2.13) and bringing in the estimate (4.2.8), which dominated the terms I, III, we conclude that for all t,

$$R^2(t) \ \lesssim \ q^{d-2}|E|^2 + q^{\frac{d-4}{2}}|E|^3 + q^{\frac{d-2}{2}}|E| \sup_{\tau \in \mathbb{F}_q} |R(\tau)|,$$

which implies that the same estimate holds for $\sup_{\tau \in \mathbb{F}_q} R^2(\tau)$.

Assuming that for some large enough C, we have $Cq^{\frac{d}{2}} \leq |E|$ clearly implies that now

$$|R(t)| \ \leq \ \frac{100}{\sqrt{C}} \frac{|E|^2}{q}, \quad \forall t \in \mathbb{F}_q,$$

where the constant 100 is basically to majorate the number of cases that has been considered. For odd d the last two terms in the latter estimate for R are worse by the factor $\sqrt{q}$ which implies the estimate for all t, thus the claim (ii) of Theorem 4.2.1. As for even d, every dot product $t \in \mathbb{F}_q$ occurs and the claim (iv) of Theorem 4.2.1 follows, provided that we can demonstrate (4.2.13).

4.2.2.1 *Finale of the proof of 4.2.3 – the estimate (4.2.13)*

In the estimates that follow we write

$$\sum_{y,y'} \quad \text{instead of} \quad \sum_{y,y' \in E, y \neq y'} .$$

Let us first extend the summation in (4.2.12) from $s' \in \mathbb{F}_q^*$ to $s' \in \mathbb{F}_q$. If we do so, it follows from Lemma 3.2.7 that we pick up the following term T to $IIII$:

$$\begin{aligned} T &= q^{d-2}|E| \sum_{y,y'} \sum_{s \in \mathbb{F}_q^*} \widehat{S}(sy)\chi(ts) \\ &= Kq^{\frac{d-6}{2}}|E| \sum_{y,y'} \sum_{s,j \in \mathbb{F}_q^*} \chi\left(\frac{s^2}{4j} + ts + j\right) \eta^d(j) \\ &= Kq^{\frac{d-6}{2}}|E| \sum_{y,y'} \sum_{s,j \in \mathbb{F}_q^*} \chi\left(\frac{(s+2jt)^2}{4j} - jt^2 + j\right) \eta^d(j) \\ &= Kq^{\frac{d-6}{2}}|E| \sum_{y,y'} \sum_{j \in \mathbb{F}_q^*} \chi(j - jt^2)\eta^d(j)[-\chi(jt^2) + K'\sqrt{q}\eta(j)] \end{aligned}$$

The analysis of the summation in j now in essence replicates that for the term III, see (4.2.9–4.2.11). If $t^2 \neq 1$ and d is even, using the Gauss sum formula (3.2.9) we obtain

$$|T| \ \leq \ 2q^{\frac{d-4}{2}}|E|^3, \tag{4.2.14}$$

which improves by factor $\sqrt{q}$ if d is odd. If $t^2 = 1$, for even d, the term T satisfies a better (by a factor q) estimate than (4.2.14). However, for odd d we would only get $|T| \leq q^{\frac{d-3}{2}}|E|^3$, which would not give an improvement over the bounds we already have we already have in (**??**). Hence, up to now, the only case we are not able to handle is odd d and $t^2 = 1$.

Thus we will further attempt to establish (4.2.13) for the quantity X, which equals $IIII$, wherein the summation in s' has been extended over the whole field $\mathbb{F}_q$. Using

Lemma 3.2.7 we have, after changing s' to $-s'$, and using $\|y\| = \|y'\| = 1$:

$$X = Kq^{\frac{d-6}{2}}|E| \sum_{y,y'} \sum_{s,j \in \mathbb{F}_q^*, s' \in \mathbb{F}_q} \eta^d(j)\chi\left(\frac{s^2 + 2(y\cdot y')ss' + s'^2 + 4tj(s+s')}{4j} + j\right) \tag{4.2.15}$$

We complete the square under χ as follows

$$s^2 + 2(y\cdot y')ss' + s'^2 + 4tj(s+s') = (s+s')^2 + 4tj(s+s') + 2\alpha s'(s+s'-s')$$

where $\alpha = \alpha(y,y') = y\cdot y' - 1$, and we shall further analyze the possibilities $\alpha \neq 0, -2$ separately: they occur when $y\cdot y' = \pm 1$, respectively.

We rewrite the latter quadratic form as

$$[(s+s') + (2tj + \alpha s')]^2 - 2\alpha s'^2 - (2tj+\alpha s')^2.$$

We now have a new variable $c = (s+s') + (2tj + \alpha s')$, which is in $\mathbb{F}_q$. Since (4.2.15) is symmetric with respect to s and s', we can assume that, in fact, $s \in \mathbb{F}_q$, $s' \in \mathbb{F}_q^*$, so for each s', j the change $s \mapsto c$ is non-degenerate. Changing the notation from $-s'$ to s we therefore have, using the Gauss sum formula

$$\begin{aligned} X &= Kq^{\frac{d-6}{2}}|E| \textstyle\sum_{y,y'} \sum_{s,j\in\mathbb{F}_q^*, c\in\mathbb{F}_q} \eta^d(j)\chi\left(\frac{c^2-(2\alpha+\alpha^2)s^2}{4j} + t\alpha s + j(1-t^2)\right) \\ &= X_1 + X_{-1} + X', \end{aligned} \tag{4.2.16}$$

where X_1 has only summation in y, y' such that $y\cdot y' = 1$ ($\alpha = 0$), X_{-1} has only summation in y, y' such that $y\cdot y' = -1$ ($\alpha = -2$), and X' includes the rest of $y, y' \in E$.

Observe that in either case we already have a Gauss sum in c, so we write

$$X' = Kq^{\frac{d-5}{2}}|E| \sum_{y\cdot y' \neq \pm 1} \sum_{s,j\in\mathbb{F}_q^*} \eta^{d+1}(j)\chi\left(\frac{-a\left(s - \frac{2jt\alpha}{a}\right)^2}{4j} + j\left(\frac{t^2\alpha}{2+\alpha} + (1-t^2)\right)\right), \tag{4.2.17}$$

provided that $a = 2\alpha + \alpha^2 \neq 0$.

Before we proceed with the main term X', let us deal with the cases $\alpha = 0, -2$ which would make the completion of the square in the transition from (4.2.16) to (4.2.17) incorrect.

If $\alpha = 0$, we confront the sum

$$X_1 = Kq^{\frac{d-5}{2}}|E| \sum_{y\cdot y'=1} \sum_{s,j\in\mathbb{F}_q^*} \eta^{d+1}(j)\chi(j(1-t^2)).$$

If d is even, the worst case scenario is $t^2 \neq 1$, when the sum in s and Gauss sum in j contribute the factor $q^{3/2}$. Hence

$$|X_1| \leq 2q^{\frac{d-2}{2}}|E| \sup_{\tau} \nu(\tau), \quad \text{for even } d, \tag{4.2.18}$$

in accordance with (4.2.13). If d is odd, the same, or in fact, better bound holds unless $t^2 = 1$, when (4.2.18) gets worse by factor $\sqrt{q}$.

If $\alpha = -2$, we analyze the sum

$$X_{-1} = Kq^{\frac{d-5}{2}}|E| \sum_{y\cdot y'=-1} \sum_{s,j\in\mathbb{F}_q^*} \eta^{d+1}(j)\chi(j(1-t^2) - 2ts).$$

If d is even, X_{-1} is still bounded by (4.2.18) – the worst case scenario now is $t = 0$; if d is odd, the bound is better than (4.2.18) by factor $\sqrt{q}$.

Finally, we turn to X', the case $a \neq 0$, and once again, the only situation we have not been able to handle so far is d odd and $t^2 = 1$.

Now taking advantage of the Gauss sum in s in (4.2.17) we have

$$\begin{aligned} X' &= Kq^{\frac{d-5}{2}}|E| \textstyle\sum_{y\cdot y'\neq\pm 1} \sum_{j\in\mathbb{F}_q^*} \eta^{d+1}(j)\chi\left(j\left(\frac{t^2\alpha}{2+\alpha} + (1-t^2)\right)\right) \\ &\quad \times \left[-\chi\left(-j\tfrac{t^2\alpha}{2+\alpha}\right) + K'\sqrt{q}\eta(a)\eta(j)\right] \\ &= X_1' + X_2', \end{aligned}$$

according to the two terms in the last bracket.

We have

$$X_1' = Kq^{\frac{d-5}{2}}|E| \sum_{y\cdot y'\neq\pm 1} \sum_{j\in\mathbb{F}_q^*} \eta^{d+1}(j)\chi(j(1-t^2)).$$

For even d, the worst case scenario occurs when $t^2 \neq 1$, the Gauss sum in j then leads to X_1' to be dominated by the first term in (4.2.13). The latter bound will get worse by factor $\sqrt{q}$ only if d is odd and $t^2 = 1$. For the quantity X_2' we obtain:

$$\begin{aligned} X_2' &= Kq^{\frac{d-4}{2}}|E| \textstyle\sum_{y\cdot y'\neq\pm 1} \eta(a) \sum_{j\in\mathbb{F}_q^*} \eta^d(j)\chi\left(\left(1-\frac{2}{2+\alpha}t^2\right)j\right) \\ &= Kq^{\frac{d-4}{2}}|E| \textstyle\sum_{y\cdot y'\neq\pm 1} \eta[(y\cdot y')^2-1] \sum_{j\in\mathbb{F}_q^*} \eta^d(j)\chi\left(\left(1-\frac{2}{y\cdot y'+1}t^2\right)j\right). \end{aligned} \tag{4.2.19}$$

There are two cases here: $y\cdot y' = 2t^2-1$ and otherwise. First consider the latter case. Then if d is even, X_2', subject to this extra constraint, satisfies the estimate (4.2.13), as the summation in j simply yields -1. If d is odd, however, there is a major problem, as then we have

$$\begin{aligned} &q^{\frac{d-4}{2}}|E| \textstyle\sum_{y\cdot y'\neq 2t^2-1,\pm 1} \eta((y\cdot y')^2-1) \sum_{j\in\mathbb{F}_q^*} \eta^d(j)\chi\left(\left(1-\frac{2}{y\cdot y'+1}t^2\right)j\right) \\ &= Kq^{\frac{d-3}{2}}|E| \textstyle\sum_{y\cdot y'\neq 2t^2-1,\pm 1} \eta((y\cdot y')-1)\eta((y\cdot y')+1-2t^2), \end{aligned} \tag{4.2.20}$$

It follows that to improve on the trivial bound $q^{\frac{d-3}{2}}|E|^3$ one would have to establish a cancelation in the multiplicative character sum in (4.2.20).

We finish by adding the constraint $y\cdot y' = 2t^2-1$ to X_2' in (4.2.19). Dealing with this does not represent any difficulty. For even d we have

$$q^{\frac{d-4}{2}}|E| \left| \sum_{\pm 1\neq y\cdot y'=2t^2-1} \eta[(y\cdot y')^2-1] \sum_{j\in\mathbb{F}_q^*} \eta^d(j) \right| \leq q^{\frac{d-2}{2}}|E| \sup_{\tau\in\mathbb{F}_q} \nu(\tau),$$

and zero in the right-hand side for odd d. This proves (4.2.13) and (4.2.3) follows.

4.2.3 Proof of 4.2.4 and 4.2.6

We establish (4.2.6) as the estimate (4.2.4) follows immediately from the same construction.

4.2.3.1 Construction in the case $d \neq 5$:

Suppose that $\mathbb{F}_q$ does not contain $i = \sqrt{-1}$. Let

$$S^2 = \{x \in \mathbb{F}_q^3 : x_1^2 + x_2^2 + x_3^2 = 1\},$$

and let Z_2 denote the maximal subset of S^2 such that $Z_2 \cap (-Z_2) = \emptyset$. Then if $u, v \in S^2$, then $u \cdot v = -1$ if and only if $u = -v$. To see this, without loss of generality let $v = (0, 0, 1)$. Then the condition

$$u \cdot v = -1$$

reduces to

$$u_3 = -1,$$

and

$$u_1^2 + u_2^2 = 0. \tag{4.2.21}$$

Since, by assumption, $\mathbb{F}_q$ does not contain $\sqrt{-1}$, (4.2.21) can only happen if $u_1 = u_2 = 0$, and so $u = -v$. Since $Z_2 \cap (-Z_2) = \emptyset$, the condition $u \cdot v = -1$ in Z_2 is never satisfied.

Let $d = 2k + 1$ with $k \geq 3$. Let H denote sub-space of $\mathbb{F}_q^{2k-2}$ generated by the mutually orthogonal null-vectors given by Lemma 3.3.2. Let

$$E = Z_2 \times H.$$

It follows that

$$|E| \approx q^2 \cdot q^{k-1} = q^{k+1} = q^{\frac{d+1}{2}}.$$

Let (x', x'') and (y', y'') be elements of E. Then

$$(x', x'') \cdot (y', y'') = x' \cdot y' \neq -1.$$

Moreover,

$$||(x', x'')|| = ||x'|| + ||x''|| = ||x'|| = 1,$$

so $E \subset S^{2k}$ where

$$S^{2k} = \{x \in \mathbb{F}_q^{2k+1} : x_1^2 + \cdots + x_{2k+1}^2 = 1\}.$$

This completes the construction in the case $d \neq 5$.

4.2.3.2 Construction in the case $d = 5$

Let

$$u = (a, b, c, 0, 0) \text{ where } a^2 + b^2 + c^2 = 0.$$

Let

$$v = (-b/c, a/c, 0, 0, 0) \text{ and } w = (0, -c/a, b/a, 0, 0).$$

Let $s \in \mathbb{F}_q$ be such that

$$e = v + sw$$

satisfies

$$||e|| = c^2 \text{ for some } c \in \mathbb{F}_q^*.$$

The existence of such a c is verified by a direct calculation. Now let $e' = \frac{e}{c}$, which results in $||e'|| = 1$.

Observe by a direct calculation that

$$u \cdot e = 0 \text{ for all } s \in \mathbb{F}_q.$$

Let Z_2 be as above and let O denote the orthogonal transformation that maps

$$\{(x_1, x_2, x_3, 0, 0) : x_j \in \mathbb{F}_q\}$$

to the three dimensional sub-space of $\mathbb{F}_q^5$ spanned by e', $(0, 0, 0, 1, 0)$ and $(0, 0, 0, 0, 1)$. Let Z_2' denote the image of Z_2 under O.

Define

$$E = \{tu + Z_2' : t \in \mathbb{F}_q\}.$$

Then $|E| \approx q^3$ and for any $t, t' \in \mathbb{F}_q$ and $z, z' \in Z_2'$,

$$(tu + z) \cdot (t'u + z') = tt'u \cdot u + tu \cdot z' + t'u \cdot z + z \cdot z'$$

$$= z \cdot z' \neq -1$$

by construction. This completes the construction in the case $d = 5$.

CHAPTER V

SUMS AND PRODUCTS

5.1 Introduction

A classical problem in additive number theory is to determine, given a finite subset A of a ring, whether both $2A = \{a + a' : a, a' \in A\}$ and $A^2 = \{a \cdot a' : a, a' \in A\}$ can be small in a suitable sense. Let $A \subset \mathbb{R}$. If $A = \{1, 2, \ldots, N\}$, then

$$|A + A| \approx |A|, \text{ and } |A \cdot A| \approx |A|^2,$$

where

$$A + A = \{a + a' : a, a' \in A\}, \quad A \cdot A = \{a \cdot a' : a, a' \in A\}.$$

Similarly, if $A = \{2^n : 1 \leq n \leq N\}$, then

$$|A \cdot A| \approx |A|, \text{ and } |A + A| \approx |A|^2.$$

Erdős and Szemerédi [17] proved the inequality

$$\max(|A + A|, |A \cdot A|) \geq c|A|^{1+\varepsilon}$$

for a small but positive ε, where A is a subset of integers. They conjectured that

$$\max(|A + A|, |A \cdot A|) \geq c|A|^{2-\delta}$$

for any positive δ.

For real numbers the best known bound, due to Jozsef Solymosi, ([49]) says that

$$\max\{|A + A|, |A \cdot A|\} \geq c|A|^{\frac{14}{11}-\epsilon}.$$

In the finite field setting the situation appears to be more complicated due to the fact that the Szemerédi-Trotter incidence theorem, the main tool in Euclidean setting,

does not hold in the same generality and is, in general, much less well understood. It is known, however, via ground breaking work in [7] that if $A \subset \mathbb{F}_q$, q a prime, than if $|A| \leq Cq^{1-\epsilon}$, for some $\epsilon > 0$, then there exists $\delta > 0$ such that

$$\max\{|A+A|, |A \cdot A|\} \gtrsim |A|^{1+\delta}.$$

This bound does not yield a precise relationship between δ and ϵ. In [30] we used Kloosterman sums to establish a concrete value of δ, in certain ranges of $|A|$. More precisely, it is proved that

$$\max\{|A+A|, |A \cdot A|\} \gtrsim \min\left\{q^{\frac{1}{3}}|A|^{\frac{2}{3}}, \frac{|A|^{\frac{3}{2}}}{q^{\frac{1}{4}}}\right\}.$$

This estimate is better than the trivial for $|A| \gtrsim q^{1/2}$ illustrating the fact that in arbitrary finite fields the question is complicated by the occurence of subfields of size $q^{1/2}$ where one can not beat the trivial bound. In the case of prime fields Garaev ([20]) used a combination of combinatorial and exponential sum methods to improve the value of δ and gave non-trivial bounds for all ranges of $|A|$. For large subsets Garaev's argument transfers directly to arbitrary fields.

Theorem 5.1.1. *[20] Let $A \subset \mathbb{F}_q$. Then*

$$\max\{|A+A|, |A \cdot A|\} \gtrapprox \min\left\{q^{\frac{1}{3}}|A|^{\frac{2}{3}}, \frac{|A|^{\frac{5}{3}}}{q^{\frac{1}{3}}}\right\}.$$

Chang gave the following bound.

Theorem 5.1.2. *[10] Let $A \subset \mathbb{F}_q$. Then*

$$\max\{|A+A|, |A \cdot A|\} \gtrsim \min\left\{q^{\frac{1}{3}}|A|^{\frac{2}{3}}, \frac{|A|^{\frac{5}{3}}}{q^{\frac{1}{3}}}\right\}.$$

Garaev subsequently improved this in [21] with the following bound.

Theorem 5.1.3. *[21] Let $A \subset \mathbb{F}_q$. Then*

$$|A+A||A \cdot A| \geq \min\left\{\frac{1}{2}q|A|, \frac{1}{4}\frac{|A|^4}{q}\right\}.$$

This bound in the case $|A| \gtrsim p^{\frac{2}{3}}$ is optimal. For subsets with small cardinalities, in [20] Garaev proved that

$$\max\{|A+A|, |A\cdot A|\} \gtrapprox |A|^{15/14},$$

which was improved by Katz and Shen in [39] to

$$\max\{|A+A|, |A\cdot A|\} \gtrapprox |A|^{14/13}.$$

For another proof of Theorem 5.1.3 see [48].

5.2 Proof of Theorem 5.1.3

Without loss of generality suppose that $0 \notin A$ and

$$N = |\{y = a(x-b) : x \in A+A, a, b \in A, y \in A\cdot A\}|.$$

Since any $(a_1, a_2, a_3) \in A^3$ corresponds to a unique solution $(a_1+a_2, a_2, a_3, a_2a_3)$ to the equation in N we have $|N| \geq |A|^3$.

$$N = \frac{1}{q}\sum_s \sum_{y\in A\cdot A} \chi(-sy) \sum_{\substack{a,b\in A\\ x\in A+A}} \chi(sa(x-b))$$

$$= \frac{|A|^2|A+A||A\cdot A|}{q} + q^2 \sum_{s\neq 0} \widehat{A\cdot A}(-s) \sum_{a\in\mathbb{F}_q} \widehat{A}(a)\widehat{A+A}(-a)A(s^{-1}a) = I + II.$$

and applying Cauchy-Schwartz

$$|II|^2 \leq q^3|A\cdot A| \sum_{s\neq 0} \left| \sum_{a\in\mathbb{F}_q} \widehat{A}(a)\widehat{A+A}(-a)A(s^{-1}a)\right|^2$$

$$\leq q^3|A\cdot A| \sum_{a,a'\in\mathbb{F}_q} |\widehat{A}(a)\widehat{A+A}(-a)||\widehat{A}(a')\widehat{A+A}(-a')|A\times A \cap l_{(a,a')}|$$

$$\leq |A|q^3|A\cdot A| \left| \sum_{a\in\mathbb{F}_q} |\widehat{A}(a)\widehat{A+A}(-a)|\right|^2$$

$$\leq q|A\cdot A||A|^2|A+A|$$

So

$$|A|^3 \leq \frac{|A|^2|A+A||A\cdot A|}{q} + \sqrt{q|A\cdot A||A|^2|A+A|}.$$

5.3 Sums-Product Basis

Given the fact that the sumset and product set can not both be small at the same time a natural question to consider is "'How large does $A \subset \mathbb{F}_q$ need to be to make sure that

$$dA^2 = \underbrace{A^2 + \cdots + A^2}_{d \text{ times}} = \mathbb{F}_q?$$

Define

$$A^2 = A \cdot A = \{a \cdot a' : a, a' \in A\} \text{ and } A + A = \{a + a' : a, a' \in A\}.$$

It is known (see e.g. [3]) that if $d = 3$, this conclusion holds if the number of elements $|A| \geq Cq^{\frac{3}{4}}$, with a sufficiently large constant $C > 0$. It is reasonable to conjecture that if $|A| \geq C_\epsilon q^{\frac{1}{2}+\epsilon}$, then $2A^2 \supseteq \mathbb{F}_q^*$. This result cannot hold, especially in the setting of general finite fields if $|A| = \sqrt{q}$ because A may in fact be a subfield. See also [5], [11], [22], [20], [30], [39], [56], [58] and the references contained therein on recent progress related to this problem and its analogs. For example, Glibichuk and Konyagin, [24](see also [20]), proved that $8A \cdot B = \mathbb{Z}_p$, p prime, provided that $|A||B| > 2p$. This was extended to arbitrary finite fields by Glibichuk in [23].

Theorem 5.3.1. *[23] Let $A, B \subset \mathbb{F}_q$ such that $|A||B| > 2q$ then*

$$8A \cdot B = \mathbb{F}_q.$$

The above-mentioned results were achieved by methods of arithmetic combinatorics.

From Theorem 3.4.2 and Theorem 4.0.8 we have the result.

Theorem 5.3.2. *Let $A_1, \ldots, A_d, B_1, \ldots B_d \subset \mathbb{F}_q^*$.*

If $|A_1| \ldots |A_d||B_1| \ldots |B_d| > q^{d+1}$ then $A_1 \cdot B_1 + \cdots + A_d \cdot B_d \supseteq \mathbb{F}_q^*$.

If $|A_1| \ldots |A_d|(|B_1| \ldots |B_d|)^{1-\frac{1}{d}} \geq q^d$ then $A_1 \cdot B_1 + \cdots + A_d \cdot B_d \geq \frac{1}{2}q$.

This in turn implies the following theorem.

Theorem 5.3.3. *Let* $A \subset \mathbb{F}_q^*$.

If $|A| > q^{\frac{1}{2}+\frac{1}{2d}}$ *then* $dA^2 \supseteq \mathbb{F}_q^*$.

If $|A| \geq q^{\frac{1}{2}+\frac{1}{2(2d-1)}}$ *then* $dA^2 \geq \frac{1}{2}q$.

It follows immediately from Theorem 5.3.3 that in the most interesting particular case $d = 2$, $\mathbb{F}_q^* \subset A^2 + A^2$ if $|A| > q^{\frac{3}{4}}$, and $|A^2 + A^2| \geq \frac{1}{2}q$ if $|A| \geq q^{\frac{2}{3}}$.

REFERENCES

[1] A. Adolphson and S. Sperber, *Exponential sums and Newton polyhedra: cohomology and estimates*, Annals of Mathematics, **130**, (1989), 367-406.

[2] Alon and Krivelevich, *Constructive bounds for a Ramsey-type problem*, Graphs and Combinatorics **13** (1997), 217-225.

[3] J. Bourgain, *Mordell's exponential sum estimate revisited.* Journal of the American Mathematical Society (2005) 18(2):477499.

[4] J. Bourgain, *A Szemerédi type theorem for sets of positive density in* $\mathbb{R}^k$. Isr. J. Math **54** (1986) 307-316.

[5] J. Bourgain, A. A. Glibichuk and S. V. Konyagin, *Estimates for the number of sums and products and for exponential sums in fields of prime order*, J.London Math. Soc. (2) **73** (2006), 380-398.

[6] J. Bourgain and S. Konyagin *Estimates for the number of sums and products and for exponential sums over subgroups in fields of prime order* C. R. Math. Acad. Sci. Paris **337** (2003), no. 2, 75-80.

[7] J. Bourgain, N. Katz and T. Tao, *A sum-product estimate in finite fields, and applications*, Geom. Func. Anal. **14** (2004) 27-57.

[8] M. Chang, *Factorization in generalized arithmetic progressions and applications to the Erdős-Szemerédi sum-product problems*, Geom. Funct. Anal. **13** (2003) 720-736.

[9] M. Chang, *A sum-product estimate in algebraic division algebras*, *Israel J. Math.*, to appear.

[10] M. Chang, *A sum-product estimate for large subsets of* $\mathbb{F}_p$, preprint.

[11] E. Croot, *Sums of the Form* $1/x_1^k + \ldots 1/x_n^k$ *moduloa prime*, Integers **4** (2004).

[12] P. Deligne, *La conjecture de Weil. I. (French)*, Inst. Hautes tudes Sci. Publ. Math. **43**, (1974), 273-307.

[13] G. Elekes and I. Ruzsa, *Few sums, many products*, Studia. Sci. Math. Hungar. **40** (2003) 301-308.

[14] G. Elekes, On the number of sums and products. *ActaArith.*, 81(4) 365–367, 1997.

[15] B. Erdoğan. *A bilinear Fourier extension theorem and applications to the distance set problem.* IMRN (accepted for publication) 2005.

[16] P. Erdös *On sets of distances of n points,* Amer. Math. Monthly. **53** (1946), 248–250.

[17] P. Erdős and E. Szemerédi, On sums and products of integers. In *Studies in pure mathematics*, pages 213–218. Birkhäuser, Basel, 1983.

[18] K. Ford, Sums and products from a finite set of real numbers. *Ramanujan J.*, 2(1-2) 59–66, 1998.

[19] H. Furstenberg, Y. Katznelson, and B. Weiss, *Ergodic theory and configurations in sets of positive density.* In *Mathematics of Ramsey theory*, pages 184-198, Algorithms Combin., **5** , Springer, Berlin, (1990).

[20] M. Garaev, *An explicit sum-product estimate in* $\mathbb{F}_p$, (preprint), (2007).

[21] M. Garaev, *The sum-product estimate for large subsets of prime fields*, (preprint), (2007).

[22] A. Glibichuk, *Combinatorial properties of sets of residues modulo a prime and the Erdos-Graham problem*, Mat. Zametki, **79** (2006), 384-395; translation in: Math. Notes **79** (2006), 356-365.

[23] A. Glibichuk, *Additive properties of product sets in an arbitrary finite field*, preprint.

[24] A. Glibichuk and S. Konyagin, *Additive properties of product sets in fields of prime order*, Centre de Recherches Mathematiques, Proceedings and Lecture Notes, (2006).

[25] B. Green. *Finite field models in additive combinatorics*, arXiv:math.NT/0409420.

[26] B. Green and T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Ann. of Math. (to appear), (2007).

[27] D. Hart and A. Iosevich, *Sums and products in finite fields: an integral geometric viewpoint*,(To appear in Radon transforms, geometry, and wavelets: A special volume of Contemporary Mathematics), 2008.

[28] D. Hart, A. Iosevich, *Ubiquity of simplices in subsets of vector spaces over finite fields*, Analysis Mathematica, **34** (2008), 10 pages.

[29] D. Hart, A. Iosevich, *D. Hart, A. Iosevich, Pinned distance sets, Wolff's exponent in finite fields and sum-product estimates, 8 pages.*, preprint, (2008).

[30] D. Hart, A. Iosevich, J. Solymosi, *Sum-product estimates in finite fields via Kloosterman sums*, Int. Math. Res. Notices (2007) Vol. 2007, article ID rmn007, 14 pages.

[31] D. Hart, A. Iosevich, D. Koh, M. Rudnev, *Averages over hyperplanes, sum-product theory in vector spaces over finite fields and the Erdos-Falconer distance problem*, (preprint), (2007).

[32] A. Iosevich, S. Hofmann, *Circular averages and Falconer/Erdős distance conjecture in the plane for random metrics*, Proc. Amer. Mat. Soc. 133 (2005), 133-143.

[33] A. Iosevich, D. Koh, *Cubic varieties, Erdős-Falconer distance problem and incidence problems in vector spaces over finite fields*, (preprint), (2006).

[34] A. Iosevich, M. Rudnev *Erdős distance problem in vector spaces over finite fields*, Trans. Amer. Math. Soc. (2007).

[35] A. Iosevich, M. Rudnev and I. Uriarte-Tuero. *Theory of dimension for large discrete sets and applications.* Preprint, arxiv.org, 2007.

[36] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, **53** American Mathematical Society, Providence, RI, (2004).

[37] A. A. Karatsuba, *Basic analytic number theory*, Springer-Verlag, 1993.

[38] N. Katz and C. Shen, *Garaev's Inequality in finite fields not of prime order*, (preprint), (2007).

[39] N. Katz and C. Shen, *A slight improvement of Garaev's sum product estimate*, (preprint), (2007).

[40] M. Krivilevich and B. Sudakov, *Pseudo-random graphs*, (preprint), (2007).

[41] B. Kra, *Ergodic methods in additive combinatorics*, Lecture notes from the Montreal Workshop on Additive Combinatorics (2006).

[42] R. Lidl and H. Niederreiter, *Finite fields*,Cambridge Univ. Press (1997).

[43] A. Magyar, *K-point configurations in sets of positive density of $\mathbb{Z}^n$*, preprint.

[44] J. Matousek, *Lectures on Discrete Geometry,* Graduate Texts in Mathematics, Springer **202** (2002).

[45] M. Nathanson, *On sums and products of integers. Proc. Amer. Math. Soc.*, 125(1) 9–16, 1997.

[46] M. Nathanson and G. Tenenbaum, *Inverse theorems and the number of sums and products*, Asterisque **258** (1999) 195-204.

[47] T. Cochrane and C. Pinner, *Sum-product estimates applied to Waring's problem mod p*, preprint.

[48] I. Shparlinski, *On The Solvability of Bilinear Equations in Finite Fields*, (preprint), (2007)

[49] J. Solymosi, *On the number of sums and products*, Bull. London Math. Soc. **37** (2005) 491-494.

[50] J. Solymosi, On sums and products of complex numbers. *J.Théor. Nombres Bordeaux*, (3) 17 (2005) 921-924.

[51] E. Stein, *Harmonic Analysis*, Princeton University Press, (1993).

[52] E. M. Stein and S. Wainger, *Problems in harmonic analysis related to curvature*, Bull. Amer. Math. Soc. **84**, Number 6 (1978).

[53] L. Székely, *Remarks on the chromatic number of geometric graphs.* In *Graphs and other combinatorial topics (Prague, 1982)*, pages 312-315, Algorithms Combin., **59** , Teubner-Texte Math, Leipzig, 1983.

[54] E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression.* Acta. Arith. **27** (1975) 199-245.

[55] T. Tao, *Class notes on additive combinatorics*, UCLA (2005).

[56] T. Tao and V. Vu, Additive Combinatorics, Cambridge University Press (to appear) (2006).

[57] V. Vu, *Sum-Product estimates via directed expanders*, (preprint), (2007).

[58] Le Anh Vinh, *Explicit Ramsey graphs and Erdos distance problem over finite Euclidean and non-Euclidean spaces*, (preprint), arXiv:0711.3508, (2007).

[59] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U.S.A. **34** (1948) 204-207.

VITA

Derrick Hart was born April 4, 1980 in Jefferson City, Missouri. After graduating from School of the Osage High School in 1998, Derrick attended University of Missouri-Columbia in Columbia, Missouri, where he received a Bachelors degree in mathematics. He recieved a masters in mathematics at the Georgia Institute of Technology in 2006 and expects to receive his Doctor of Philosophy degree in May of 2008.