GEOMETRIC COMBINATORICS
IN DISCRETE SETTINGS

A Dissertation presented to the

Faculty of the Graduate School

University of Missouri

In Partial Fulfillment of the

Requirements for the Degree

Doctor of Philosophy

by

DAVID COVERT

Dr. Alex Iosevich, Dissertation Supervisor

May 2011

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

GEOMETRIC COMBINATORICS IN FINITE SETTINGS

presented by David Covert, 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 Loukas Grafakos

Professor Steven Hofmann

Professor Sergei Kopeiken

ACKNOWLEDGEMENTS

I would like to thank my family with special thanks to my wife Laura who is everything in my life.

My deepest thanks go to my advisor Professor Alex Iosevich for his support, encouragement, and patience which made this work possible. I would also like to thank the members of my doctoral committee, Professor William Banks, Professor Loukas Grafakos, Professor Steven Hofmann, and Professor Sergei Kopeiken for their support and advice. Finally, I would like to thank my coauthors, especially Derrick Hart and Jonathan Pakianathan, for their help and guidance.

Contents

GEOMETRIC COMBINATORICS

IN DISCRETE SETTINGS

David Covert

Dr. Alex Iosevich, Dissertation Supervisor

ABSTRACT

This thesis is a compilation of work in which the author studies geometric configurations in finite fields and the integers modulo q. The results of this dissertation are threefold. First, we prove a finite field analog of the Furstenberg-Katznelson-Weiss theorem on triangles in $\mathbb{R}^2$. Second, we study volume sets in $\mathbb{F}_q^d$ and discuss some applications to sum-product problems. Finally, we study geometric combinatorics in $\mathbb{Z}/q\mathbb{Z}$. We generalize a result of Hart and Iosevich [27] which has applications to sum-product problems. Finally, we show that the $\mathbb{Z}_q^d$ analogue of a sphere with unital radius is q^{d-1}-dimensional.

Chapter 1

Introduction

1.1 Statement of Purpose

Geometric combinatorics ties together techniques from number theory, harmonic analysis, and combinatorics. A large subset of problems in geometric combinatorics asks one to answer the following question:

Question 1.1. *How "large" must a set be in order to ensure that it contains certain geometric configurations?*

Finite field models were originally studied as a "playground" of sorts for their Euclidean analogues. Using finite field models allows one to gain insight into a problem without having to worry about technical issues such as convergence. Often times, a thorough understanding of a problem in finite fields can translate to a good understanding of its Euclidean analogue. However, there are distinctions to be made between continuous and finite problems. A highly regarded paper of Dvir ([12]), for example, was able to establish the finite field analogue of the Kakeya conjecture, which, roughly speaking, stated that a set in a finite field containing a line in every direction had nearly full cardinality. The Euclidean version remains unsolved for $d \geq 3$. Dvir was able to use to his full advantage, the algebraic nature of finite fields, and he solved the problem by showing that the only low-degree polynomial which could vanish on a Kakeya set was in fact the zero polynomial, which was enough to show that a Kakeya set is sufficiently large. However, this method does not immediately yield a result in the continuous setting. On the other hand, there are obstructions with which one must contend in finite fields that do not appear in Euclidean problems. For example, one must contend with nontrivial spheres with zero radius.

While finite field models have provided insight in how one might solve the analogue in Euclidean space, some finite field problems are interesting in their own right. Furthermore, once one is interested in finite field problems for their own sake, a natural generalization for which one might hope is to replace the finite field with the integers modulo q. In this dissertation, the author will discuss some results in geometric combinatorics arising in problems from finite fields and the integers modulo q.

A large portion of this thesis is based on methods of exponential sums combined with Fourier analytic methods. In particular we use to our advantage the notion of orthogonality. We typically want to find the size of certain algebraic varieties $A_t = \{x \in G^d : f(x) = t\}$, where $t \in G$ is a unit, and where G is a finite abelian group. Utilizing orthogonality, we can then write

$$|A_t| = |G|^{-1} \sum_{x \in G^d} \sum_{s \in G} \chi(s(f(x) - t)),$$

where χ is a nontrivial character on G. We hereby review the basics of Fourier analysis over finite abelian groups for completeness.

1.1.1 Fourier analysis over finite abelian groups

To obtain our results, we relied heavily on Fourier analytic techniques, and we review some properties here. Most of the Fourier analytic machinery can be stated for finite abelian groups or even locally compact abelian groups G (see, for example, [38]), though we need only restrict ourselves to the cases of finite fields and the set of integers modulo q. Here and throughout, G will denote a finite abelian group, and we let $|E|$ denote the cardinality of the set $E \subset G$.

Recall that a character on G is a homomorphism from G to the set $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$. The set of characters $G^\wedge$ has size $|G^\wedge| = |G|$, and it is a group (called the dual group) under the operation $(\chi_1 \cdot \chi_2)(g) = \chi_1(g)\chi_2(g)$, for $\chi_i \in G^\wedge$ and $g \in G$. The inverse of a character $\chi \in G^\wedge$ is the character $\overline{\chi}$, which is the complex conjugate of χ. The character $\chi \equiv 1$ is typically called the trivial character on G, and we refer to all other characters as nontrivial. One of the most basic, and yet most useful properties of characters is their orthogonality:

Lemma 1.2. *Let H be a subgroup of a finite abelian group G and χ a character on G. Then,*

$$\frac{1}{|H|}\sum_{h\in H}\chi(h) = \begin{cases} 1 & \chi_{|H} \textit{ is the trivial character} \\ 0 & \textit{otherwise} \end{cases}$$

In particular, $\dfrac{1}{|G|}\displaystyle\sum_{g\in G}\chi(g) = 1$ *if χ is the trivial character, and zero otherwise.*

We now consider separately the cases of finite fields and integers modulo q.

1.1.2 Finite Fields

Recall that a finite field $\mathbb{F}_q$ must have cardinality $q = p^\ell$, where p is a prime. Viewing $\mathbb{F}_q$ as a field extension of $\mathbb{F}_p$, we recall that the trace function

$$Tr : \mathbb{F}_q \to \mathbb{F}_p \qquad\qquad x \mapsto x + x^p + \cdots + x^{p^{\ell-1}}$$

is linear, and it satisfies $Tr(x^q) = Tr(x)$, for all $x \in \mathbb{F}_q$. There are two types of characters to consider when working with finite fields. First are the characters on the additive group $(\mathbb{F}_q, +)$ which are called additive characters. The additive characters of $\mathbb{F}_q$ are all given by $\chi_c(x) = e_p(cTr(x))$, for some $c \in \mathbb{F}_q$, where $e_n(x) = \exp(2\pi i x/n)$. When $c = 1$, we call $\chi_c = \chi_1$ the canonical additive character of $\mathbb{F}_q$. The second type of characters are those on the multiplicative group $\mathbb{F}_q^\times$, which are simply called multiplicative characters (here and throughout if R is a ring, then we denote the set of units in R by $R^\times$). Let g be an primitive element of $\mathbb{F}_q^\times$. Then every multiplicative character is of the form $\psi_c(g^j) = e_{q-1}(cj)$, where $c \in \{0, \ldots, q-2\}$. Of particular importance is the unique multiplicative character η which annihilates the squares of elements in $\mathbb{F}_q^\times$. Using the notation as above, $\eta(x) = \psi_{\frac{q-1}{2}}(x)$, and when $q = p$ is prime, η is called the Legendre symbol of $\mathbb{F}_p$. We also note that all characters on $\mathbb{F}_q^d$, the d-dimensional vector space over $\mathbb{F}_q$, are of the form $\chi_v(x) = \chi(v \cdot x)$, where $v \in \mathbb{F}_q^d$ and χ is a nontrivial additive character of $\mathbb{F}_q$. We use Lemma 1.2 as follows:

Lemma 1.3 (Orthogonality)**.**

$$q^{-d} \sum_{x \in \mathbb{F}_q^d} \chi(x \cdot m) = \begin{cases} 1 & m = (0, \ldots, 0) \\ 0 & m \neq (0, \ldots, 0) \end{cases} \tag{1.1}$$

1.1.3 Fourier analysis in $\mathbb{F}_q$

Let χ denote a nontrivial additive character of $\mathbb{F}_q$. For a function $f : \mathbb{F}_q^d \to \mathbb{C}$, put

$$\widehat{f}(m) = q^{-d} \sum_{x \in \mathbb{F}_q^d} f(x)\chi(-x \cdot m). \tag{1.2}$$

In turn, Lemma 1.3 has the following consequences:

Lemma 1.4. *Let $f, g : \mathbb{F}_q^d \to \mathbb{C}$. Then,*

$$f(x) = \sum_{m \in \mathbb{F}_q^d} \widehat{f}(m)\chi(x \cdot m) \qquad \textit{(Inversion)} \tag{1.3}$$

$$q^{-d} \sum_{x \in \mathbb{F}_q^d} f(x)\overline{g(x)} = \sum_{m \in \mathbb{F}_q^d} \widehat{f}(m)\overline{\widehat{g}(m)} \qquad \textit{(Parseval's identity)} \tag{1.4}$$

In particular, if $f = g$, then we get Plancherel's identity:

$$q^{-d}\|f\|_2^2 = \|\widehat{f}\|_2^2.$$

Proof. We start with (1.3). We write

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

Similarly for (1.4), we have

$$\begin{aligned}
\sum_{m\in\mathbb{F}_q^d} \widehat{f}(m)\overline{\widehat{g}(m)} &= q^{-2d}\sum_{m\in\mathbb{F}_q^d}\sum_{x\in\mathbb{F}_q^d} f(x)\overline{g(y)}\chi(-x\cdot m)\chi(y\cdot m)\\
&= q^{-2d}\sum_{x,y\in\mathbb{F}_q^d} f(x)\overline{g(y)}\sum_{m\in\mathbb{F}_q^d}\chi(m\cdot(x-y))\\
&= q^{-d}\sum_{x\in\mathbb{F}_q^d} f(x)\overline{g(x)}
\end{aligned}$$

□

1.1.4 Fourier analysis in $\mathbb{Z}_q$

It is customary to write the set of integers modulo q as $\mathbb{Z}/q\mathbb{Z}$, although we have found the notation $\mathbb{Z}_q$ more convenient. The characters on the additive cyclic group $\mathbb{Z}_q$ are all of the form $\chi_c(x) = e_q(cx)$ for $c \in \mathbb{Z}_q$, and we henceforth refer to them as (additive) characters mod q. We will work over the space $\mathbb{Z}_q^d$, the d-fold Cartesian product of the ring $\mathbb{Z}_q$. Since $\mathbb{Z}_q$ is not in general a field, the set $\mathbb{Z}_q^d$ is not in general a vector space. However, $\mathbb{Z}_q^d$ is a free module over $\mathbb{Z}_q$ with rank d, and we will not worry too much about the distinction. All characters on $\mathbb{Z}_q^d$ are of the form $\chi_z(x) = \chi(x\cdot z)$, where $z \in \mathbb{Z}_q$ and χ is a nontrivial character mod q. Let χ denote a character mod

q, and let $f : \mathbb{Z}_q^d \to \mathbb{C}$. Then, in analogy with the finite field case,

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

We also have the following analogies of Lemma 1.3, (1.3), and (1.4).

Lemma 1.5. *Let χ denote a nontrivial character mod q and let $f, g : \mathbb{Z}_q^d \to \mathbb{C}$. Then,*

$$q^{-d} \sum_{x \in \mathbb{Z}_q^d} \chi(x \cdot m) = \begin{cases} 1 & m = (0, \dots, 0) \\ 0 & \textit{otherwise} \end{cases} \qquad \textit{(orthogonality)} \qquad (1.5)$$

$$f(x) = q^{-d} \sum_{m \in \mathbb{Z}_q^d} \widehat{f}(m)\chi(x \cdot m) \qquad \textit{(inversion)} \qquad (1.6)$$

$$q^{-d} \sum_{x \in \mathbb{Z}_q^d} f(x)\overline{g(x)} = \sum_{m \in \mathbb{Z}_q^d} \widehat{f}(m)\overline{\widehat{g}(m)} \qquad \textit{(Parseval's Identity)} \qquad (1.7)$$

Proof. The proof follows line for line as in the finite field case. □

We also note that characters on the multiplicative subgroup $\mathbb{Z}_q^\times$ are called Dirichlet characters $\pmod{q}$, and they will be utilized in the auxiliary lemmas in Chapter 4.

1.1.5 Notations

We will abuse notation and write E for the characteristic function of E. We write $X \lesssim Y$ to mean that there exists some positive constant c so that $X \leq cY$. Similarly, $X \gtrsim Y$ will mean that $Y \lesssim X$, and $X \approx Y$ will mean that both $X \lesssim Y$ and $X \gtrsim Y$ hold simultaneously. We will also write $X \ll Y$ (respectively, $X \gg Y$) to emphasize that $X \leq cY$ (respectively, $X \geq cY$) for a sufficiently small (respectively, large) constant c. Furthermore, we write $X \sim Y$, to mean that with respect to some parameter, we have $\lim X/Y = 1$. Given a ring R, we use $R^{\times}$ to denote the set of units in R. Finally, for a function $f : \mathbb{F}_q^d \to \mathbb{C}$ we write

$$\|f\|_p = \left(\sum_{x \in \mathbb{F}_q^d} |f(x)|^p \right)^{\frac{1}{p}}.$$

Chapter 2

k-point Configurations

2.1 Background

Given a set $E \subset \mathbb{R}^d$, define its distance set as $\Delta(E) = \{|x - y| : x, y \in E\}$, where $|\cdot|$ denotes the usual Euclidean distance. In 1946, Erdős ([15]) posed the following question, now known as the Erdős distance problem.

Question 2.1. *Let $E \subset \mathbb{R}^d$, and let $g(n) = \min\{|\Delta(E)| : |E| = n\}$. What is the best lower bound one can achieve for $g(n)$?*

Remark 2.2. *Erdős showed that $g(n) \gtrsim n^{1/d}$ for all $d \geq 2$, and he conjectured*

$$g(n) \gtrsim \begin{cases} \frac{n}{\sqrt{\log n}} & d = 2 \\ n^{\frac{2}{d}} & d \geq 3 \end{cases}$$

Very recently, Katz and Guth ([25]), were successful in showing that for $d = 2$, one has $g(n) \gtrsim \frac{n}{\log n}$, a very near optimal bound. One can find a nearly complete history of the Erdős distance problem in [22].

Later, Falconer considered a continuous version of the Erdős distance problem. He showed ([17]) that if $E \subset \mathbb{R}^d$ has Hausdorff dimension $\dim_H(E) > \frac{d+1}{2}$, then $\Delta(E)$, the distance set determined by E, has positive Lebesgue measure. He also exhibited a set $F \subset \mathbb{R}^d$ with Hausdorff dimension $\dim_H(F) = \frac{d}{2}$, whose distance set had measure zero. These two findings led to what is now called the Falconer distance conjecture:

Conjecture 2.3. *Suppose that $E \subset \mathbb{R}^d$ has Hausdorff dimension $dim_H(E) > \frac{d}{2}$. Then its distance set, $\Delta(E)$, has positive Lebesgue measure.*

Remark 2.4. *The best know results towards a resolution of the Falconer distance conjecture belong to Wolff ($d = 2$, [47]) and Erdoğan ($d \geq 3$, [14]) who have shown that $\Delta(E)$ has positive Lebesgue measure so long as $\dim_H(E) > \frac{d}{2} + \frac{1}{3}$.*

After carefully considering these two problems concerning distances, one can be led toward generalizations in many directions. For instance, one can study analogues of these statements in finite fields (see, for example [8, 28, 32, 36]). Viewing distances as "2-point configurations", one can also ask what happens for k-point configurations. For example, given a finite set $E \subset \mathbb{R}^d$, what is the minimal number distinct triangles determined by E? A result in a similar spirit is the following result of Furstenberg, Katznelson, and Weiss ([18]).

Theorem 2.5. *Let $E \subset \mathbb{R}^2$ be a set of positive upper Lebesgue measure:*

$$\overline{D}(E) = \limsup_{R\to\infty} \frac{|E \cap B_R|}{|B_R|} > 0,$$

where $|\cdot|$ denotes Lebesgue measure, and B_R is a ball of radius R centered at the origin. Then, given $\delta > 0$ and $T = \{\vec{0}, u, v\} \subset \mathbb{R}^2$, there exists a threshold ℓ_0 such that for all $\ell > \ell_0$, E_δ contains a congruent copy of $\ell T = \{\vec{0}, \ell u, \ell v\}$.

Remark 2.6. *Bourgain ([1]) was able to show that if the given triangle is an arithmetic progression $\{0, u, 2u\}$, then taking the δ-neighborhood of E is in fact necessary to maintain the validity of Theorem 2.5. It is unknown whether the δ-neighborhood of E can be replaced simply by E when the triangle is non-degenerate.*

2.2 Results

Many k-point configuration problems have been studied, notably in finite field geometries (see, for example, [8, 26, 37, 45, 48]). Throughout the remainder of this chapter, however, we will explore a finite field analogue of Theorem 2.5. For ease and clarity, we make the following definitions.

Definition 2.7. *A k-simplex (which we just call a simplex, when the context is clear) is a set of $(k+1)$-points in $\mathbb{F}_q^d$ spanning a k-dimensional subspace.*

We will say that two k-simplices Δ and Δ' are congruent if there exists an orthogonal map $O \in O_d(\mathbb{F}_q)$ and a vector $\tau \in \mathbb{F}_q^d$ such that $\Delta = O(\Delta') + \tau$. Note that this congruence is an equivalence relation, and we then consider the set of resulting equivalence classes

$$T_k(E) = \{\Delta \in E^{k+1}\} \backslash \sim .$$

Note also that $T_k(E)$ can be viewed as a natural subset of $\mathbb{F}_q^{\binom{k+1}{2}}$ (see Lemma 2.10 below). Our main result of this section is the following theorem which appeared in [10]:

Theorem 2.8. *Let $E \subset \mathbb{F}_q^d$ have size $|E| \geq \rho q^d$, where $q^{-\frac{1}{2}} \ll \rho \leq 1$. Then, there exists a constant c so that*

$$|T_d(E)| \geq c\rho^{d-1} q^{\binom{d+1}{2}}.$$

In other words, when $E \subset \mathbb{F}_q^d$ has density ρ as above, the set of d-simplices determined by E has density $\geq c\rho^{d-1}$.

Remark 2.9. *The assumption that $|E| \geq \rho q^d$implies that the number of $(d+1)$-point configurations determined by E (up to congruence) is no less than*

$$\frac{|E|^{d+1}}{\rho q^d \cdot q^{\binom{d}{2}}} \geq \rho^d q^{\binom{d+1}{2}},$$

since the size of the subset of the translation group that maps points in E to a set of size E is no larger than $|E| = \rho q^d$ and the rotation group is of size $\approx q^{\binom{d}{2}}$. Our result shaves off a power of ρ from the trivial estimate.

2.3 Proof of Results

2.3.1 Proof of Theorem 2.8

Here, we roughly state the argument. We prove Theorem 2.8 by first making a reduction to a statistical statement about hinges (the term "hinges" is defined below). Having made this reduction, we next show, using a pigeon-holing argument, that for some $x \in E$, the hinge is large. To finish the argument, we realize a dichotomy. If the number of transformations mapping the hinge to itself is small, then a purely probabilistic argument gives that the number of distinct (incongruent) $(d+1)$-point configurations is what we claim. Otherwise, if the number of transformations mapping the hinge to itself is large, then a purely combinatorial gives the result.

We start with the statistical reduction. We observe that if $|E| \geq \rho q^d$, for ρ as in Theorem 2.8, then it suffices to show that

$$\left|\left\{(a_{i_j})_{1\leq i<j\leq d+1} \in \mathbb{F}_q^{\binom{d+1}{2}} : |R_a(E)| > 0\right\}\right| \geq c\rho^{d-1} q^{\binom{d+1}{2}}, \tag{2.1}$$

where

$$R_a(E) = \{(y^1, \dots, y^{d+1}) \in E \times \cdots \times E : \|y^i - y^j\| = a_{i,j}\},$$

and for $x \in \mathbb{F}_q^d$,

$$\|x\| = x_1^2 + \cdots + x_d^2.$$

This follows immediately from the following simple linear algebra lemma.

Lemma 2.10. *Let V be a simplex with vertices $V_i \in \mathbb{F}_q^d$, where $i = 0, \ldots, k$. Let V' be another simplex with vertices $V_i' \in \mathbb{F}_q^d$ also for $i = 0, \ldots, k$. Suppose further that*

$$\|V_i - V_j\| = \|V_i' - V_j'\| \tag{2.2}$$

for all i, j. Then V and V' are congruent (i.e., they are members of the same equivalence class of $T_k(E)$).

We will postpone the proof of Lemma 2.10. Our main estimate is the following:

Theorem 2.11. *Suppose that $\alpha_i \in \mathbb{F}_q^\times$ for $i = 1, \ldots, d$, and let $E \subset \mathbb{F}_q^d$. Then,*

$$\left|\left\{(x, x^1, \ldots, x^d) \in E \times \cdots \times E : \|x - x^i\| = \alpha_i\right\}\right| = \frac{|E|^{d+1}}{q^d}(1 + o(1)) \qquad (q \to \infty)$$

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

We again postpone the proof of Theorem 2.11.

Remark 2.12. *The threshold $q^{-\frac{1}{2}} \ll \rho \leq 1$ in Theorem 2.8 is a direct consequence of Theorem 2.11. While the exponent $q^{d-\frac{1}{2}}$ is nontrivial, we believe the correct exponent to be closer to $q^{\frac{d+1}{2}}$, although we have been unsuccessful in showing this is true.*

Theorem 2.11 then implies that there exists an element $x \in E$ so that

$$\left|\left\{(x^1, \ldots, x^d) \in E \times \cdots \times E : \|x - x^i\| = \alpha_i\right\}\right| \geq \frac{|E|^d}{q^d}(1 + o(1)). \tag{2.3}$$

Fix a d-tuple $\alpha = (\alpha_i)_{1\leq i\leq d}$ with $\alpha_i \in \mathbb{F}_q^\times$ for $i = 1, \dots, d$. We define the *hinge* $h_{x,\alpha}$ to be the set $\{(x^1, \dots, x^d) \in E \times \cdots \times E : \|x - x^i\| = \alpha_i\}$. Let $M_{x,\alpha} \subset O_d(\mathbb{F}_q)$ denote the set of $d \times d$ orthogonal matrices which map the set $h_{x,\alpha}$ to itself. That is, we set $M_{x,\alpha} = \{O \in O_d(\mathbb{F}_q) : O(h_{x,\alpha}) = h_{x,\alpha}\}$. Finally, put $A_i = \{x^i \in E : \|x - x^i\| = \alpha_i\}$, where the set is indexed in i according to the distance $\alpha_i \in \mathbb{F}_q^\times$.

Using the notation as above, we consider three cases: when $|M_{x,\alpha}|$ is small, when at least one set A_i is small (which we will see forces $|M_{x,\alpha}|$ to be small), and when each A_i and $M_{x,\alpha}$ are large.

In the first case, suppose that $|M_{x,\alpha}| \lesssim \rho q^{\binom{d}{2}}$. Then, (2.3) immediately implies that the number of distinct d-point configurations between the d sets A_i is

$$\geq \frac{|h_{x,\alpha}|}{|M_{x,\alpha}|} \geq \frac{|E|^d q^{-d}(1 + o(1))}{\rho q^{\binom{d}{2}}} \geq c\rho^{d-1} q^{\binom{d}{2}}. \tag{2.4}$$

In the second case, suppose that one of the sets A_i has size $|A_i| \leq \rho q^{d-1}$ for some i. We then utilize the orbit-stabilizer theorem from elementary group theory:

Proposition 2.13 ([34]). *Let a group G act on a set S. Let $Gs = \{gs : g \in G\}$ be the orbit of $s \in S$, and $G_s = \{g : gs = s\}$ the isotropy group of $s \in S$. Then there is a bijection between Gs and G/G_s. Consequently,*

$$|Gs| = (G : G_s) = |G|/|G_s|.$$

We let the group $O_d(\mathbb{F}_q)$ act on $\mathbb{F}_q^d$. Recalling that $|O_d(\mathbb{F}_q)| \approx q^{\binom{d}{2}}$, and since orthogonal maps preserve the length of a certain vector, we get that the size of the orbit of any point is exactly q^{d-1}. Hence, picking some z from the previously mentioned set A_i, we get that the size of the stabilizer group of this element z is

$$|G_z| = \frac{|G|}{|Gz|} \approx \frac{q^{\binom{d}{2}}}{q^{d-1}}.$$

The final element here is to notice that

$$|M_{x,\alpha}| \leq |G_z||A_i| \lesssim \frac{q^{\binom{d}{2}}}{q^{d-1}} \cdot \rho q^{d-1} = \rho q^{\binom{d}{2}},$$

since the number of hinge-preserving orthogonal matrices is no more than the number of orthogonal transformations which fix a given vector $z \in A_i$, times the number of choices for that vector z. Indeed, this forces $|M_{x,\alpha}| \lesssim \rho q^{\binom{d}{2}}$, and we then proceed as in the first case getting the correct amount of distinct d-point configurations by pigeon-holing.

The final case follows by a result of Steven Senger ([10]).

Theorem 2.14. *Let $|A_i| > \rho q^{d-1}$ and $|M_{x,\alpha}| \gtrsim \rho q^{\binom{d}{2}}$. Then, we can find at least $c\rho^{d-1}q^{\binom{d}{2}}$ distinct d-point configurations among the sets A_i.*

We see that in any case, there exist no less than $c\rho^{d-1}q^{\binom{d}{2}}$ many distinct d-point configurations. Since this holds for any fixed vector $\alpha = (\alpha_i)_{i=1}^{d}$, and since there are $q-1$ choices for each $\alpha_i \in \mathbb{F}_q \backslash \{0\}$, then there are at least

$$c\rho^{d-1}q^{\binom{d}{2}}(q-1)^d \geq c\rho^{d-1}q^{\binom{d+1}{2}}$$

many distinct $(d+1)$-point configurations determined by E. This completes the proof of Theorem 2.8 modulo the proofs of Theorem 2.11 and Lemma 2.10.

2.3.2 Proof of Theorem 2.11

To prove Theorem 2.11 we will actually prove the following more general result.

Theorem 2.15. *Let $r > 2$ be an integer, and let $H_{r,\alpha}$ represent the set of $r-$hinges, with distances $\alpha = \{\alpha_i\}_{i=1}^{r-1}$, which are present in E. That is,*

$$H_{r,\alpha} = \{(x, x^1, \dots x^{r-1}) \in E \times \cdots \times E : \|x - x^i\| = \alpha_i\},$$

where $\alpha_i \neq 0$ *for* $i = 1, \ldots, r-1$. *Then,*

$$|H_{r,\alpha}| = \frac{|E|^r}{q^{r-1}}(1 + o(1)),$$

whenever $|E| \gg q^{\frac{2r-5}{2r-4}d + \frac{1}{2r-4}}$

Setting $r = d+1$ in Theorem 2.15 gives Theorem 2.11. in order to complete the proof, we will need the following estimates.

Lemma 2.16. *Let* $S_t = \{x \in \mathbb{F}_q^d : \|x\| = t\}$. *Identify* S_t *with its characteristic function. For* $t \neq 0$,

$$|S_t| = q^{d-1}(1 + o(1)) \tag{2.5}$$

and if also $m \neq (0, \ldots, 0)$,

$$|\widehat{S}_t(m)| \leq 2q^{-\frac{d+1}{2}}. \tag{2.6}$$

As before, we will postpone the proof of Lemma 2.16. We will proceed with the proof of Theorem 2.11, and we induct on r. Before we handle the case $r = 3$ we first observe the following estimate which originally appeared in [32].

Lemma 2.17. *Using the notation as above, we have* $|H_{2,\alpha}| = \frac{|E|^2}{q} + O(q^{\frac{d-1}{2}}|E|)$.

To see this, write

$$\begin{aligned} |H_{2,\alpha}| &= \sum_{x,y} E(x)E(y)S(x-y) \\ &= q^{2d} \sum_{m} \left|\widehat{E}(m)\right|^2 \widehat{S}(m) \\ &= q^{-d}|E|^2|S| + q^{2d} \sum_{m \neq 0} \left|\widehat{E}(m)\right|^2 \widehat{S}(m) \end{aligned}$$

and

$$q^{2d}\left|\sum_{m\neq 0}\left|\widehat{E}(m)\right|^{2}\widehat{S}(m)\right| \leq 2q^{2d}q^{-\frac{d+1}{2}}q^{-d}|E| = 2q^{\frac{d-1}{2}}|E|.$$

We now illustrate the base step. First we write

$$|H_{3,\alpha}| = \sum_{x\in E}|E\cap(x-S)|^{2}.$$

Note that

$$\begin{aligned}|E\cap(x-S)| &= \sum_{y}E(y)S(x-y)\\ &= q^{d}\sum_{m}\widehat{E}(m)\widehat{S}(m)\chi(m\cdot x)\\ &= |E||S|q^{-d} + q^{d}\sum_{m\neq 0}\widehat{E}(m)\widehat{S}(m)\chi(m\cdot x),\end{aligned}$$

which gives

$$\begin{aligned}|H_{3,\alpha}| &= \sum_{x\in E}|E\cap(x-S)|^{2}\\ &= |E|^{3}|S|^{2}q^{-2d} + 2|E||S|q^{d}\sum_{m\neq 0}|\widehat{E}(m)|^{2}|\widehat{S}(m)| + q^{2d}\sum_{x}\left|\sum_{m\neq 0}\widehat{E}(m)\widehat{S}(m)\chi(m\cdot x)\right|^{2}\\ &= |E|^{3}|S|^{2}q^{-2d} + O\left(|E|^{2}|S|q^{-d}q^{(d-1)/2} + q^{3d}\sum_{m\neq 0}|\widehat{E}(m)|^{2}|\widehat{S}(m)|^{2}\right)\\ &= |E|^{3}|S|^{2}q^{-2d} + O\left(|E|^{2}|S|q^{-d}q^{(d-1)/2} + q^{d-1}|E|\right).\end{aligned}$$

If $|E| \gg q^{\frac{d+1}{2}}$ then

$$|H_{3,\alpha}| = |E|^{3}q^{-2}(1+o(1)).$$

For the inductive step, assume that we are in the case $|H_{r,\alpha}| = \frac{|E|^{r}}{q^{r-1}}(1+o(1))$ for

$|E| \gg q^{\frac{2r-5}{2r-4}d+\frac{1}{2r-4}}$. We begin by writing

$$\begin{aligned}
|H_{r+1,\alpha}| &= \sum_{x,x^1,\dots,x^r} H_{r,\alpha}(x,x^1,\dots,x^{r-1})E(x^r)S(x-x^r) \\
&= q^{(r+1)d}\sum_m \widehat{H}_{r,\alpha}(m,0,\dots,0)\widehat{S}(m)\widehat{E}(m) \\
&= q^{-d}|E||S||H_{r,\alpha}| + q^{(r+1)d}\sum_{m\neq 0} \widehat{H}_{r,\alpha}(m,0,\dots,0)\widehat{S}(m)\widehat{E}(m) \\
&= q^{-d}|E||S||H_{r,\alpha}| + R.
\end{aligned}$$

Applying Cauchy-Schwarz gives

$$\begin{aligned}
R^2 &\leq q^{2d(r+1)}\sum_{m\neq 0}|\widehat{S}(m)|^2|\widehat{E}(m)|^2\sum_{m\neq 0}|\widehat{H}_{r,\alpha}(m,0,\dots,0)|^2 \\
&\lesssim q^{2d(r+1)}q^{-d-1}q^{-d}|E|\sum_{m\neq 0}|\widehat{H}_{r,\alpha}(m,0,\dots,0)|^2 \\
&\leq q^{2dr-1}|E|\sum_{m}|\widehat{H}_{r,\alpha}(m,0,\dots,0)|^2
\end{aligned}$$

Also, we have that

$$\begin{aligned}
&\widehat{H}_{r,\alpha}(m,0,\dots,0) \\
&= q^{-rd}\sum_{x,x^1,\dots,x^{r-1}}\chi(x\cdot m)E(x)E(x^1)\dots E(x^{r-1})S(x-x^1)\dots S(x-x^{r-1}) \\
&= q^{-rd+d}\widehat{f}(m)
\end{aligned}$$

where

$$f(x) = E(x)\sum E(x^1)\dots, E(x^{r-1})S(x-x^1)\dots S(x-x^{r-1}) = E(x)|E\cap(x-S)|^{r-1}.$$

Since $|E\cap(x-S)| \leq q^{d-1}$, it follows that

$$\begin{aligned}
A = \sum_m |\widehat{H}_{r,\alpha}(m,0,\dots,0)|^2 &= q^{-2rd+2d}\sum_m|\widehat{f}(m)|^2 \\
&= q^{-2rd+d}\sum_x|f(x)|^2 \\
&\leq q^{-2rd+d}\left(q^{d-1}\right)^{2(r-2)}|H_{3,\alpha}|,
\end{aligned}$$

and therefore,

$$A \lesssim q^{-2rd+d}\left(q^{d-1}\right)^{2(r-2)}|E|^3q^{-2}(1+o(1)).$$

Finally,

$$R^2 \lesssim q^{-3}q^d\left(q^{d-1}\right)^{2(r-2)}|E|^4(1+o(1)) \leq q^{(2r-3)d-2r+1}|E|^4(1+o(1)).$$

This implies that,

$$|H_{r+1,\alpha}| = q^{-d}|E||S||H_{r,\alpha}| + O(q^{d\frac{2r-3}{2}-r+\frac{1}{2}}|E|^2),$$

and we hence get

$$|H_{r+1,\alpha}| = \frac{|E|^{r+1}}{q^r}(1+o(1)),$$

whenever

$$|E| \gg q^{\frac{2r-3}{2r-2}d+\frac{1}{2r-2}}.$$

Finally, to finish the proof of Theorem 2.11, it remains to prove Lemma 2.16. We first need the following well known result on Gauss sums.

Proposition 2.18 ([35]). *Let χ denote a canonical additive character and ψ denote the quadratic multiplicative character on $\mathbb{F}_q$ (or the Legendre symbol, when q is prime). For $a \in \mathbb{F}_q$, we have*

$$\sum_{x\in\mathbb{F}_q}\chi(ax^2) = \eta(a)\sum_{x\in\mathbb{F}_q}\chi(x)\eta(x). \tag{2.7}$$

Furthermore, one has

$$\sum_{x\in\mathbb{F}_q}\chi(x)\psi(x) = \lambda_q\cdot\sqrt{q},$$

where $q = p^\ell$ and

$$\lambda_q = \begin{cases} (-1)^{\ell-1} & p \equiv 1 \text{ mod } 4 \\ (-1)^{\ell-1} i^\ell & p \equiv 3 \text{ mod } 4 \end{cases} \tag{2.8}$$

Proposition 2.19 ([31])**.** *Let χ denote a nontrivial additive character on $\mathbb{F}_q$, and η the quadratic multiplicative character of $\mathbb{F}_q$. Then,*

$$\left| \sum_{x \in \mathbb{F}_q^\times} \chi(ax + bx^{-1}) \right| \leq 2\sqrt{q}, \text{ and} \tag{2.9}$$

$$\left| \sum_{x \in \mathbb{F}_q^\times} \chi(ax + bx^{-1}) \eta(x) \right| \leq 2\sqrt{q} \tag{2.10}$$

Remark 2.20. *The estimate (2.9) was originally due to A. Weil ([46]), and such sums are called Kloosterman sums. The sums appearing in (2.10) were first treated by Salié ([40]), and they are called Salié sums or twisted Kloosterman sums.*

To prove Lemma 2.16, we apply orthogonality to see

$$\begin{aligned} |S_t| = \sum_{x \in \mathbb{F}_q} S_t(x) &= q^{-1} \sum_{s \in \mathbb{F}_q} \sum_{x \in \mathbb{F}_q^d} \chi(sx_1^2) \dots \chi(sx_d^2) \chi(-st) \\ &= q^{d-1} + R(t), \end{aligned}$$

where

$$R(t) = q^{-1} \sum_{s \in \mathbb{F}_q^\times} \sum_{x \in \mathbb{F}_q^d} \chi(sx_1^2) \dots \chi(sx_2^d) \chi(-st).$$

From Proposition 2.18, we have

$$R(t) = q^{\frac{d-2}{2}} \lambda_q^d \sum_{s \in \mathbb{F}_q^\times} \eta^d(s) \chi(-st),$$

where $\lambda_q \in \{\pm 1, \pm i\}$ is explicitly defined in Proposition 2.18 and depends only on q. Now, if d is even, we have

$$R(t) = q^{\frac{d-2}{2}} \lambda_q^d \sum_{s \in \mathbb{F}_q^\times} \chi(-st) = -q^{\frac{d-2}{2}} \lambda_q^d$$

Furthermore, if d is odd, we have

$$\begin{aligned} R(t) &= q^{\frac{d-2}{2}}\lambda_q^d \eta(-t^{-1}) \sum_{s\in\mathbb{F}_q^\times} \eta(s)\chi(s) \\ &= q^{\frac{d-2}{2}}\lambda_q^d \eta(-t^{-1})(\lambda_q q^{\frac{1}{2}} - 1) \end{aligned}$$

In either case, $R(t) = o(q^{d-1})$, and (2.5) follows. For (2.6), write

$$\begin{aligned} \widehat{S}_t(m) &= q^{-d} \sum_{x\in\mathbb{F}_q^d} S_t(x)\chi(-x\cdot m) \\ &= q^{-d-1} \sum_{s\in\mathbb{F}_q} \prod_{i=1}^{d} \sum_{x_i\in\mathbb{F}_q} \chi(sx_i^2)\chi(-x_i m_i)\chi(-st) \\ &= q^{-d-1} \sum_{s\in\mathbb{F}_q^\times} \prod_{i=1}^{d} \sum_{x_i\in\mathbb{F}_q} \chi(sx_i^2 - x_i m_i)\chi(-st) \\ &= q^{-d-1} \sum_{s\in\mathbb{F}_q^\times} \prod_{i=1}^{d} \sum_{x_i\in\mathbb{F}_q} \chi\left(s\left(x_i - \frac{m_i}{2s}\right)^2\right)\chi\left(-\frac{m_i}{4s}\right)\chi(-st) \\ &= q^{-d-1} \sum_{s\in\mathbb{F}_q^\times} \prod_{i=1}^{d} \sum_{x_i\in\mathbb{F}_q} \chi(sx_i^2)\chi\left(-\frac{\|m\|}{4s} - st\right) \\ &= q^{-d-1}\lambda_q^d q^{\frac{d}{2}} \sum_{s\in\mathbb{F}_q^\times} \eta^d(s)\chi\left(-\frac{\|m\|}{4s} - st\right) \end{aligned}$$

Applying Proposition 2.19, we see that $\left|\widehat{S}_t(m)\right| \leq q^{-\frac{d+2}{2}} \cdot 2\sqrt{q} = 2q^{-\frac{d+1}{2}}$, as claimed.

2.3.3 Proof of Lemma 2.10

Let $\pi_r(x)$ denote the r-th coordinate of x. By translating, we may assume that $V_0 = \vec{0}$. We may also assume that $V_1, \ldots, V_k$ are contained in $\mathbb{F}_q^k$. The condition that $\|V_i - V_j\| = \|V_i' - V_j'\|$ for all i, j implies that

$$\sum_{r=1}^{k} \pi_r(V_i)\pi_r(V_j) = \sum_{r=1}^{k} \pi_r(V_i')\pi_r(V_j'). \tag{2.11}$$

Let T be the transformation uniquely defined by $T(V_i) = V_i'$. To show that T is orthogonal it suffices to show that $\|Tx\| = \|x\|$ for all x. By assumption, the V_i's form a basis, so we have

$$x = \sum_i t_i V_i.$$

Thus, by (2.11), we have that

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

giving the result.

Chapter 3

Volume Sets and Applications

3.1 Background

Given a subset A of a ring R, we define its sumset and productset to be

$$A + A = \{a_1 + a_2 : a_i \in A\}, \quad \text{and}$$
$$A \cdot A = \{a_1 \cdot a_2 : a_i \in A\},$$

respectively. A famous and still unresolved question posed by Erdős and Szemerédi ([16]) asks whether the sumset and productset of an arbitrary set of integers A can both be small. Specifically, they conjectured:

Conjecture 3.1. *Given any $\delta > 0$, then there exists a constant C_δ so that*

$$\max\{|A + A|, |A \cdot A|\} \geq C_\delta |A|^{2-\delta},$$

holds for all finite subsets $A \subset \mathbb{Z}$.

In other words, they ask if one can find a nontrivial lower bound on $|A \cdot A| + |A + A|$. The sum-product problem has a very rich history (see, for example [43] or [44] for a nice survey). It has been shown to have connections with geometric incidence theory, first by Elekes ([13]) when he deduced a sum-product bound using the Szemerédi-Trotter theorem on incidences in the plane. As the incidence theory is based in $\mathbb{R}^2$, the results of Elekes and Solymosi, hold also for finite sets of real numbers, with the integers as a special case. This sum-product problem has received much attention over the last few years, and the best results towards a resolution of the Conjecture 3.1 are due to Solymosi ([42]) who showed that when $A \subset \mathbb{R}$ is finite, one has

$$\max\{|A+A|, |A \cdot A|\} \geq \frac{|A|^{\frac{4}{3}}}{4\lceil \log |A| \rceil}.$$

It is also noteworthy to mention that when either the sumset or productset of a set of integers is small, the other is large. See, for example, [7, 42, 43, 44], and the references contained therein. Furthermore, sum-product problems have received much attention in the setting of finite fields. There are, however, two new obstacles with which one must contend in the finite field case. First, incidence theory is simply not as well understood in finite fields, at least in comparison to the continuous case. Since the best known results are based on incidence theory, this presents a rather large problem. One therefore pursues sharper incidence results in hopes of obtaining better sum-product estimates. Secondly, one must also contend with the existence of subfields. For example, when $q = p^2$, the field $\mathbb{F}_q$ contains $\mathbb{F}_p$ as a subfield. Therefore, one usually works with sets satisfying either $|A| \gtrsim q^{\frac{1}{2}+\epsilon}$ or one works with $A \subset \mathbb{F}_p$.

One of the first contributions to the understanding of the sum-product problem in finite fields was a result of Bourgain, Katz, and Tao ([6]), where they showed the following result holds for finite fields with a prime number of elements.

Theorem 3.2. *Let $A \subset \mathbb{F}_p$, where $p \equiv 3$ mod 4, and $p^\delta < |A| < p^{1-\delta}$, for some $\delta > 0$. Then, there exist constants $c = c(\delta)$ and $\epsilon = \epsilon(\delta) > 0$, such that*

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

where $\epsilon \to 0$ as $\delta \to 0$.

Remark 3.3. *When $p \equiv 1 \bmod 4$, there is an element $i \in \mathbb{F}_p$ with $i^2 = -1$. Therefore, one can construct a set $E = \{(t, it) : t \in \mathbb{F}_p\}$ with $\Delta(E) = \{0\}$. Furthermore, if one does not restrict to the case $|A| < p^{1-\delta}$, then $A = \mathbb{F}_p$ can in fact be a subring, and hence $|A + A| = |A \cdot A| = |A|$. Interestingly, the restriction $|A| > p^{\delta}$ has been found to be unnecessary, and it was removed in [5]. The proof of Theorem 3.2 ultimately relied on finding a suitably sharp incidence bound for $\mathbb{F}_p$.*

The first concrete relationship between δ and $\epsilon(\delta)$ in Theorem 3.2 was given by Hart, Iosevich, and Solymosi ([29]) when they showed the following.

Theorem 3.4. *Let $A \subset \mathbb{F}_q$, where q is not necessarily prime. Then,*

$$|A|^3 \lesssim q^{-1}|A + A|^2|A \cdot A||A| + q^{\frac{1}{2}}|A + A||A \cdot A|.$$

In particular, when $q^{\frac{1}{2}} \lesssim |A| \lesssim q^{\frac{7}{10}}$, then one has

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

In a similar spirit, Garaev ([20]) was able to show that for $A \subset \mathbb{F}_p$, one has

$$|A + A||A \cdot A| \gtrsim \min\left\{p|A|, \frac{|A|^4}{p}\right\},$$

and in particular, when $|A| > p^{\frac{2}{3}}$, this implies

$$\max\{|A + A|, |A \cdot A|\} \gtrsim \sqrt{p|A|}.$$

For small subsets of $\mathbb{F}_p$, building upon work of M. Garaev ([19]), Katz and Shen [33], and others, Rudnev has shown ([39]) that one has $\max\{|A+A|, |A \cdot A|\} \geq \frac{|A|^{\frac{12}{11}}}{(\log|A|)^{4/11}}$, whenever $|A| < \sqrt{p}$. Other lines of attack to study the sum-product phenomenon have included studying the size of sets $|dA^2|$ ([27]), or more generally, studying $|f(A)|$, where f is a polynomial in many variables (see, for example, [21, 33, 41] and the references contain therein).

Matrices could also be of assistance to obtain a sum-product result. For example, consider the determinant of a 3×3 matrix with entries in $A \subset \mathbb{F}_q$:

$$\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = aei + bfg + cdh - ceg - bdi - afh \in 3A^3 - 3A^3.$$

It was was this hope of extracting information from the determinant of a $d \times d$ matrix to get a result on the size of dA^d that led to our embarkment on the following project ([9]).

3.2 Results

For $x^i \in \mathbb{F}_q^d$, define $vol(x^1, \dots, x^d) = x^1 \cdot (x^2 \wedge \dots \wedge x^d)$, where $\wedge$ denotes the wedge product

$$u^2 \wedge \dots \wedge u^n = \det(i \quad u^2 \quad \dots \quad u^n),$$

where $i = (i_1, \dots, i_d)$ is the set of coordinate directions in $\mathbb{F}_q^d$, and where $x \cdot y = x_1y_1 + \dots x_dy_d$ is the usual dot product. For a set $E \subset \mathbb{F}_q^d$, we define its *volume set* as

$$vol(E) = \{vol(x^1, \dots, x^d) : x^i \in E, \text{ for } i = 1, \dots, d\}.$$

Definition 3.5. *We say $E \subset \mathbb{F}_q^d$ is Cartesian product-like if given any n-dimensional subspace $H_n \subset \mathbb{F}_q^d$, we have $|E \cap H_n| \lesssim |E|^{\frac{n}{d}}$.*

Our main results are the following:

Theorem 3.6. *Let $E \subset \mathbb{F}_q^3$ be Cartesian product-like. If $|E| \gtrsim q^{\frac{15}{8}}$, then*

$$vol(E) \supset \mathbb{F}_q^\times.$$

Theorem 3.7. *Suppose that $A \subset \mathbb{F}_q$ and $|A| > \sqrt{q}$. If $E = A \times \cdots \times A \subset \mathbb{F}_q^d$, then*

i) $vol(E) = \mathbb{F}_q$, for $d \geq 4$.

ii) $|vol(E)| > \frac{q}{2}$, for $d = 3$.

3.3 Proof of Results

Our main investigative tools is the following incidence theorem:

Lemma 3.8. *Let $B(x,y)$ be any non-degenerate bilinear form on $\mathbb{F}_q^2$. Suppose that $f, g : \mathbb{F}_q^d \to \mathbb{C}$, and put*

$$\nu(t) = \sum_{B(x,y)=t} f(x)g(y).$$

Then, for $t \neq 0$, we have

$$\nu(t) = \|f\|_1\|g\|_1 q^{-1} + O\left(\|f\|_2\|g\|_2 q^{\frac{d-1}{2}}\right). \tag{3.1}$$

Moreover, if we set $E = supp(f)$, then whenever $\vec{0} \notin E$, we have

$$\sum_t \nu(t)^2 \leq \|f\|_2^2\|g\|_1^2|E|q^{-1} + \|f\|_2^2 q^{2d-1} \sum_{k \neq \vec{0}} |\widehat{g}(k)|^2 \, |E \cap \ell_k|, \tag{3.2}$$

where $\ell_k = \{tk : t \in \mathbb{F}_q^{\times}\}$.

Remark 3.9. *Lemma 3.8 has already appeared in [27] and [28], in the realm where $B(x,y) = x \cdot y$ and $f(x) = g(x) = E(x)$, the characteristic function of the set E. Notice that in this scenario (3.1) and (3.2) take the form*

$$\nu(t) = \frac{|E|^2}{q} + O\left(|E|q^{\frac{d-1}{2}}\right), \qquad \textit{and} \tag{3.3}$$

$$\sum_t \nu(t)^2 \leq \frac{|E|^4}{q} + |E|q^{2d-1} \sum_k |\widehat{E}(k)|^2 |E \cap \ell_k|, \tag{3.4}$$

respectively.

Proof. We let χ denote a nontrivial additive character on $\mathbb{F}_q$. As it can be *any* nontrivial additive character, we can replace $B(x, y)$ by the dot-product $x \cdot y$. We write

$$\begin{aligned}
\nu(t) &= \sum_{B(x,y)=t} f(x)g(y) \\
&= q^{-1} \sum_{x,y} \sum_{s \in \mathbb{F}_q} \chi(s(x \cdot y - t)) f(x)g(y) \\
&= \|f\|_1 \|g\|_1 q^{-1} + q^{-1} \sum_{x,y} \sum_{s \in \mathbb{F}_q^\times} \chi(s(x \cdot y - t)) f(x)g(y) \\
&= \|f\|_1 \|g\|_1 q^{-1} + R(t).
\end{aligned}$$

Viewing the term $R(t)$ as a sum in x, and applying Cauchy-Schwarz, we see that

$$\begin{aligned}
R(t)^2 &\leq \|f\|_2^2 q^{-2} \sum_x \sum_{y,y'} \sum_{s,s' \in \mathbb{F}_q^\times} g(y)g(y')\chi(x \cdot (sy - s'y'))\chi(t(s' - s)) \\
&= q^{d-2} \|f\|_2^2 \sum_{\substack{sy=s'y' \\ s,s' \in \mathbb{F}_q^\times}} g(y)g(y')\chi(t(s' - s)) \\
&= q^{d-2} \|f\|_2^2 \sum_{s \in \mathbb{F}_q^\times} \sum_y + q^{d-2} \|f\|_2^2 \sum_{\substack{sy=s'y' \\ s,s' \in \mathbb{F}_q^\times \\ s \neq s'}} g(y)g(y')\chi(t(s' - s)) \\
&= A + B.
\end{aligned}$$

Now,

$$A = q^{d-2} \|f\|_2^2 \|g\|_2^2 (q - 1) \leq q^{d-1} \|f\|_2^2 \|g\|_2^2.$$

Furthermore,

$$\begin{aligned}
B &= q^{d-2} \|f\|_2^2 \sum_{\substack{sy=s'y' \\ s,s' \in \mathbb{F}_q^\times \\ s \neq s'}} g(y)g(y')\chi(t(s' - s)) \\
&= q^{d-2} \|f\|_2^2 \sum_{a \in \mathbb{F}_q^\times \setminus \{1\}} \sum_{b \in \mathbb{F}_q^\times} \sum_y g(y)g(ay)\chi(tb(1 - a)) \\
&= -q^{d-2} \|f\|_2^2 \sum_{a \in \mathbb{F}_q^\times \setminus \{1\}} \sum_y g(y)g(ay)
\end{aligned}$$

For the L^2 estimate, we apply Cauchy-Schwarz once again to see that

$$\nu(t)^2 \leq \|f\|_2^2 \sum_{B(x,y)=B(x,y')=t} E(x)g(y)g(y').$$

Thus,

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

where A is the sum with $s = 0$, and B is the sum with $s \in \mathbb{F}_q^\times$. Thus,

$$A = q^{-1}|E|\|f\|_2^2\|g\|_1^2$$

and

$$\begin{aligned}B &= \|f\|_2^2 q^{2d-1} \sum_{s\in\mathbb{F}_q^\times} \sum_x |\widehat{g}(x)|^2 E(sx) \\ &= \|f\|_2^2 q^{2d-1} \sum_x |\widehat{g}(x)|^2 |E \cap \ell_x| \\ &= \|f\|_2^2 q^{2d-1} \sum_{x\neq\vec{0}} |\widehat{g}(x)|^2 |E \cap \ell_x|,\end{aligned}$$

as E does not contain the origin. □

3.3.1 Proof of Theorem 3.6

Our plan is simply to apply Lemma 3.8 to particular functions f and g. Throughout, we let $E \subset \mathbb{F}_q^3$ be Cartesian product-like. Put $f(x) = E(x)$, and note that $\|f\|_1 = \|f\|_2^2 = |E|$. Put $g_0(x) = |\{(u,v) \in E \times E : u \wedge v = x\}|$, and note that $\|g_0\|_1 = |E|^2$. Furthermore, we put $\nu_0(t) = |\{(x,y,z) \in E \times E \times E : vol(x,y,z) = t\}|$, and we observe the equality

$$\nu_0(t) = \sum_{x\cdot y=t} f(x)g_0(y).$$

Our plan of attack, then, is to show that $\nu_0(t) > 0$ for all values of $t \neq 0$.

Throughout the calculations, the value $g_0(0,0,0)$ is too difficult to handle directly. For this reason, we define a new function $g(x)$ where

$$g(x) = \begin{cases} g_0(x) & x \neq (0,0,0) \\ 0 & x = (0,0,0) \end{cases}$$

and similarly, we set

$$\nu(t) = \sum_{x \cdot y = t} f(x)g(y).$$

To finish the proof of Theorem 3.6, we need the following technical results.

Lemma 3.10. *Let ν_0, ν, g_0, and g be defined as above. Then,*

$$\|g_0\|_1 \approx \|g\|_1 \qquad \textit{and} \qquad \|\nu_0\|_1 \approx \|\nu\|_1$$

Lemma 3.11. *For the function $g(x)$ as above, we have*

$$\|g\|_2 \lesssim \begin{cases} |E|^{\frac{7}{6}} q^{\frac{1}{2}} & q^{\frac{3}{2}} \lesssim |E| \lesssim q^2 \\ |E|^{\frac{5}{3}} q^{-\frac{1}{2}} & |E| \gtrsim q^2 \end{cases}$$

Finally, applying Lemma 3.8 to the functions $f(x)$ and $g(x)$ constructed above yields

$$\nu(t) = q^{-1}\|f\|_1\|g\|_1 + O\left(q^{\frac{d-1}{2}}\|f\|_2\|g\|_2\right)$$

In the case $|E| \lesssim q^2$, we see that

$$\nu(t) = |E|^3 q^{-1} + O(q^{\frac{3}{2}}|E|^{\frac{5}{3}}),$$

and it follows that $\nu(t) > 0$, whenever $|E| \gg q^{\frac{15}{8}}$. In the range $|E| \gtrsim q^2$, we see that

$$\nu(t) = |E|^3 q^{-1} + O(q^{\frac{1}{2}}|E|^{\frac{13}{6}}),$$

and $\nu(t) > 0$ whenever $|E| \gg q^{\frac{9}{5}}$, which is always the case. It then follows that $\nu(t) > 0$ for each $t \neq 0$, and hence $vol(E) \supset \mathbb{F}_q^\times$, so long as $|E| \gg q^{\frac{15}{8}}$. It remains, however, to prove Lemma 3.10 Lemma 3.11.

Proof of Lemma 3.10

The inequalities $\|\nu_0\|_1 \approx \|\nu\|_1$ follows from $\|g_0\|_1 \approx \|g\|_1$. We must therefore demonstrate that there exists constants c_1 and c_2, such that

$$c_1 \sum_x g_0(x) \geq \sum_x g(x) \geq c_2 \sum_x g_0(x).$$

We can clearly take $c_1 = 1$, as $g_0(x) \geq g(x)$ for every x. Since, $\|g_0\|_1 = |E|^2$, it only remains to show that

$$\sum_x g(x) \gtrsim |E|^2,$$

and to do so, it simply suffices to show that $g_0(0,0,0)$ is not the dominant term, and hence its removal does not affect the L^1 bound for g. Therefore, it suffices to show that,

$$g_0(0,0,0) \leq |E|^\alpha$$

for some $\alpha < 2$. However, this follows easily from the fact that

$$\begin{aligned} g_0(0,0,0) &= |\{(u,v) \in E \times E : u \wedge v = (0,0,0)\}| \\ &\leq |E| \max_{\ell \subset \mathbb{F}_q^3} |E \cap \ell| \leq |E|^{\frac{4}{3}}, \end{aligned}$$

since E is Cartesian product-like. Lemma 3.10 then follows.

Proof of Lemma 3.11

Recall we aim to show that function $g(x) = |\{(u,v) \in E \times E : u \wedge v = x\}|$ for $x \neq (0,\dots,0)$ and $g(0) = 0$ has the following L^2 bound:

$$\|g\|_2 \lesssim \begin{cases} |E|^{\frac{7}{6}} q^{\frac{1}{2}} & q^{\frac{3}{2}} \lesssim |E| \lesssim q^2 \\ |E|^{\frac{5}{3}} q^{-\frac{1}{2}} & |E| \gtrsim q^2 \end{cases}$$

Before we proceed, we require the following estimate:

Lemma 3.12. *Let $G(2,3)$ be the set of all 2-dimensional subspaces in $\mathbb{F}_q^3$. Suppose that $E \subset \mathbb{F}_q^3$ is Cartesian product-like. Then,*

$$\sum_{H \in G(2,3)} |E \cap H|^2 \lesssim |E|^2, \tag{3.5}$$

whenever $|E| \gtrsim q^{\frac{3}{2}}$.

Proof. Note that the sum $\sum |E \cap H|^2$ ranging through $H \in G(2,3)$ counts all pairs of mutually orthogonal vectors exactly once, as each pair of orthogonal vectors determines a unique plane $H \in G(2,3)$. If two vectors are not orthogonal, then they both lie on the same line and hence are counted at most $O(q)$ times. Since each line contains at most $c|E|^{\frac{1}{3}}$ points of E, as E is Cartesian product-like, it follows that

$$\sum_{H \in G(2,3)} |E \cap H|^2 \lesssim |E|^2 + q|E|^{1/3} \cdot |E| \lesssim |E|^2,$$

whenever $|E| \gtrsim q^{\frac{3}{2}}$, as claimed. □

To finish the L^2 bound for g, we first notice that

$$\|g\|_2^2 \lesssim \sum_{j \in \mathbb{F}_q^\times} \sum_{H \in G(2,3)} \nu_H^2(t),$$

where if H is determined by the equation $x \cdot y = 0$, we have

$$\nu_H(t) = |\{(y,z) \in (E \cap H) \times (E \cap H) : vol(x,y,z) = t\}|.$$

Applying (3.2) with $d = 2$, we have

$$\begin{aligned}
\|g\|_2^2 &\lesssim \sum_{H \in G(2,3)} \left(|E \cap H|^4 q^{-1} + |E \cap H| q^3 \sum_k |\widehat{E \cap H}|^2 |(E \cap H) \cap \ell_k| \right) \\
&\lesssim \sum_{H \in G(2,3)} \left(\frac{|E \cap H|^4}{q} + \max_\ell |E \cap \ell| |E \cap H| q^3 \sum_k |\widehat{E \cap H}|^2 \right) \\
&\lesssim q^{-1} \sum_{H \in G(2,3)} |E \cap H|^4 + q \max_\ell |E \cap \ell| \sum_{H \in G(2,3)} |E \cap H|^2 \\
&= I + II
\end{aligned}$$

Since E is Cartesian product-like, then $|E\cap H|\lesssim |E|^{\frac{2}{3}}$. Applying Lemma 3.12 gives

$$I\lesssim \begin{cases} q^{-1}|E|^{\frac{4}{3}}|E|^2 & q^{\frac{3}{2}}\lesssim |E|\lesssim q^2 \\ q^{-1}|E|^{\frac{10}{3}} & |E|\gtrsim q^2 \end{cases}$$

This is sufficient as $q^{-1}|E|^{\frac{4}{3}}|E|^2\lesssim q|E|^{\frac{7}{3}}$, when $|E|\lesssim q^2$. Similarly, Lemma 3.12 gives

$$II = q\max_{\ell}|E\cap \ell|\sum_{H\in G(2,3)}|E\cap H|^2\lesssim q|E|^{\frac{1}{3}}|E|^2,$$

as long as $|E|\gtrsim q^{\frac{3}{2}}$, and this completes the proof of Lemma 3.11.

3.3.2 Proof of Theorem 3.7

We require the following preliminary Lemmas (see [6, 23, 24]).

Lemma 3.13. *Suppose that $A\subset \mathbb{F}_q^\times$ is such that $|A|>\sqrt{q}$. Then, there exist elements $\alpha,\beta\in A-A$ such that $|\alpha A\pm\beta A|>\frac{q}{2}$.*

Lemma 3.14. *If $C\subset\mathbb{F}_q^\times$ is such that $|C|>\frac{q}{2}$, then $C\pm C=\mathbb{F}_q$.*

Lemma 3.15. *Suppose that $A\subset\mathbb{F}_q^\times$, $|A|>\sqrt{q}$ and $B=A-A$. Then, $B^2-B^2=\mathbb{F}_q$.*

To prove Lemma 3.15, we must show the set of determinants

$$D=\left\{\begin{vmatrix} x_1 & x_2 \\ x_3 & x_4\end{vmatrix} : x_i\in B\right\}$$

covers $\mathbb{F}_q$. Set $x_1=\alpha, x_2=\beta$ as in Lemma 3.13. Since $x_3,x_4\in B$, we can write $x_3=y_1-y_2$ and $x_4=y_3-y_4$, where $y_i\in A$. Let $C=\alpha A-\beta A$. Then, $D=C-C$, and the result now follows from Lemmas 3.13 and 3.14. To prove the first part of Theorem 3.7, it is enough to prove the result for $d=4$. Now, consider determinants of the form

$$\begin{vmatrix} x_1 & x_2 & x_3 & x_4 \\ y_1 & y_2 & y_3 & y_4 \\ u_1 & u_2 & x_3 & x_4 \\ v_1 & v_2 & y_3 & y_4\end{vmatrix} = \begin{vmatrix} x_1-u_1 & x_2-u_2 & 0 & 0 \\ y_1-v_1 & y_2-v_2 & 0 & 0 \\ u_1 & u_2 & x_3 & x_4 \\ v_1 & v_2 & y_3 & y_4\end{vmatrix} = (x_3y_4-y_3x_4)\begin{vmatrix} x_1-u_1 & x_2-u_2 \\ y_1-v_1 & y_2-v_2\end{vmatrix}.$$

The first part of Theorem 3.7 follows from Lemma 3.15. Finally, when $d = 3$, we have

$$\begin{vmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ u_1 & u_2 & x_3 \end{vmatrix} = x_3 \cdot \begin{vmatrix} x_1 - u_1 & x_2 - u_2 \\ y_1 & y_2 \end{vmatrix} - y_3 \begin{vmatrix} x_1 - u_1 & x_2 - u_2 \\ u_1 & u_2 \end{vmatrix}.$$

Choosing α and β from Lemma 3.13 such that $\alpha = x_1 - u_1$ and $\beta = x_2 - u_2$. Fix y_3, and fix $x_3 \neq 0$. The second half of Theorem 3.7 follows from Lemma 3.13.

Chapter 4

Geometric Configurations in the Integers Modulo q

In this chapter, we turn our attention to geometric combinatorics in the setting of the integers mod q, denoted here by $\mathbb{Z}_q$.

4.1 Background

After studying geometric combinatorics in vector spaces over finite fields, one is naturally led to replace finite fields with the integers modulo q. A few technical obstructions arise, however, in this new setting. First, Gauss sum estimates are much more delicate. For example, when $q \equiv 2 \pmod 4$, the quadratic Gauss sum vanishes completely. To overcome this obstacle (along with many other such obstacles), we typically only consider odd values q.

As discussed in detail in Chapter 3, the sum-product problem has received much attention over the last few decades. We study variants of the sum-product problem in $\mathbb{Z}_q$. In this setting, one is asked to show that when $A \subset \mathbb{Z}_q$ is not a subring, then either the sumset or productset of A is large. Recall that in finite fields, one was forced to deal with the lack of incidence theorems (a rather substantial obstacle) and the existence of subgroups. The situation in $\mathbb{Z}_q$ is even more bleak, as one is forced to also contend with the existence of zero-divisors. The fact that $\mathbb{Z}_q$ is not a field (and hence for $t \in \mathbb{Z}_q^\times$, the equation $x^2 = t$ does not have at most 2 solutions) coupled with the fact that $\mathbb{Z}_q$ is not a unique factorization domain, causes significant technical obstacles in the estimation of Gauss sums. Nonetheless, quite a bit is still known about the sum-product problem in $\mathbb{Z}_q$. For example, Bourgain and Chang have shown ([3]) that if $q = p_1 \dots p_k$, where $p_i > q^{\epsilon_0}$, and $A \subset \mathbb{Z}_q$ satisfies $|A + A| + |A \cdot A| < |A|^{1+\epsilon}$, then either $|A| > q^{1-\delta}$ or else $|\pi_d(A)| < C_{\epsilon_0} q^{\delta}$. Here, $d|q$, $\pi_d : \mathbb{Z}_q \to \mathbb{Z}_d$ is the natural projection, and $\delta = \delta(\epsilon_0, \epsilon) \to 0$ as $\epsilon \to 0$ (see also, [4] for a related result). This result was extended to arbitrary q by Bourgain in [2]. Furthermore, an Elekes-type bound was found by Garaev ([20]), in which he was able to show that if $A \subset \mathbb{Z}_m$ (with $m > 1$), then

$$|A + A||A \cdot A| \gtrsim \left\{ m|A|, \frac{|A|^4}{m} \left(\sum_{\substack{d|m \\ d<m}} \sqrt{d} \right)^{-2} \right\}.$$

The case when m is prime appeared in the same paper and was discussed in the previous chapter. Our line of attack is to study the size of $dA^2 = A \cdot A + \cdots + A \cdot A$, where A is sufficiently large.

4.2 Results

We now discuss our results. We first show a $\mathbb{Z}_q$ analogue of the following theorem of Hart and Iosevich.

Theorem 4.1 ([27]). *Let $E \subset \mathbb{F}_q^d$, and define $\prod(E) = \{x \cdot y : x, y \in E\}$. Then $\prod(E) \subset \mathbb{F}_q^\times$, whenever $|E| > q^{\frac{d+1}{2}}$.*

Given a subset $E \subset \mathbb{Z}_q^d$, we define its *dot-product set* to be defined just as in the finite field case: $\prod(E) = \{x \cdot y : x, y \in E\}$, where $x \cdot y = x_1y_1 + \cdots + x_dy_d$ is the usual dot product. Then, we have the following generalization of Theorem 4.1.

Theorem 4.2. *Suppose $E \subset \mathbb{Z}_q^d$, where $q = p^\ell$, is of size $|E| > \ell q^{\frac{(2\ell-1)d}{2\ell} + \frac{1}{2\ell}}$. Then,*

$$\prod(E) \supset \mathbb{Z}_q^\times.$$

Remark 4.3. *Theorem 4.2 is a generalization of Theorem 4.1 in the sense that when $\ell = 1$, $\mathbb{Z}_p = \mathbb{F}_p$ is a field, and our exponents match exactly. The finite field case has the advantage that even when the field has p^ℓ elements, the analysis goes through unchanged. In the setting of integers mod q, this is not the case.*

Corollary 4.4. *Suppose that $q = p^\ell$ and $A \subset \mathbb{F}_q$, and $|A| > \ell^{\frac{1}{d}} q^{\frac{2\ell-1}{2\ell} + \frac{1}{2\ell d}}$. Then,*

$$\mathbb{Z}_q^\times \subset dA^2 = A \cdot A + \cdots + A \cdot A.$$

In particular, when $d = 2$, $q = p^2$, and $A \subset \mathbb{Z}_q$ with $|A| > q^{7/8}$, one has

$$\mathbb{Z}_q^\times \subset A \cdot A + A \cdot A.$$

Corollary 4.4 follows easily from Theorem 4.2 by setting $E = A \times \cdots \times A$. Theorem 4.2 shows that there exists a constant $B = B(p, \ell) > 0$ so that $|E| > Bq^{\left(\frac{2\ell-1}{2\ell}\right)d}$ implies $\prod(E) \supset \mathbb{Z}_{p^\ell}^\times$. To contrast this result, in [11], we prove the following;

Theorem 4.5. *For $d \geq 3$, there exists a constant $b = b(p) > 0$, such that there exist sets of size $|E| = bq^{\left(\frac{2\ell-1}{2\ell}\right)d}$ and yet $\prod(E) \not\supset \mathbb{Z}_{p^\ell}^\times$*

Remark 4.6. *Theorem 4.5 shows that Theorem 4.2 is best possible up to the factor of $\frac{1}{2\ell}$. In particular, if we fix p and ℓ and let the dimension $d \to \infty$, then our results are sharp asymptotically.*

The second of our results states that the $\mathbb{Z}_q^d$ analogue of a sphere with unital radius is $(d-1)$-dimensional, which again aligns with the finite field case (see (2.5)). More precisely, for $x \in \mathbb{Z}_q^d$, we put $\|x\| = x_1^2 + \cdots + x_d^2$. Clearly, $\|x\|$ is not a metric, although we note that this notion of "length" is invariant under orthogonal transformations. For $t \in \mathbb{Z}_q$, we set $S_t(x) = \{x \in \mathbb{Z}_q^d : \|x\| = t\}$ as d-dimensional sphere of radius t.

Theorem 4.7. *Let $d \geq 2$ and $t \in \mathbb{Z}_q^\times$, where q is odd. Then,*

$$|S_t| = q^{d-1}(1 + o(1)).$$

On the other hand, if n is even, $t \in \mathbb{Z}_n^\times$, $d \equiv 0 \pmod 4$, and $val_2(n) = \alpha$, then

$$|S_t| = O_\alpha\left(n^{d-1}\right).$$

4.3 Proof of Results

4.3.1 Proof of Theorem 4.2

To prove Theorem 4.2, we define the incidence function

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

and we show that $\nu(t) > 0$ for each unit $t \in \mathbb{Z}_q^\times$. We write

$$\begin{aligned}\nu(t) &= q^{-1} \sum_{s \in \mathbb{Z}_q} \sum_{x,y \in E} \chi\left(s(x \cdot y)\right) \chi(-st) \\ &= \nu_\infty(t) + \nu_0(t) + \nu_1(t) + \ldots \nu_{\ell-1}(t),\end{aligned}$$

where $\chi(z) = \exp(2\pi i z/q)$ and

$$\nu_i(t) = q^{-1} \sum_{\substack{s \in \mathbb{Z}_q \\ val_p(s) = i}} \sum_{x,y \in E} \chi\left((s(x \cdot y)\right) \chi(-st).$$

Recall that $val_p(x) = i$ if $p^i | x$, but $p^{i+1} \not| x$, and $val_p(0) = \infty$. It is then plain to see that $\nu_\infty(t) = \frac{|E|^2}{q}$. For the other values $i = 0, \dots, \ell - 1$, notice that s can be written in the form $s = p^i \overline{s}$, where $\overline{s}$ is determined uniquely in $\mathbb{Z}^\times_{p^{\ell-i}}$. Also, viewing the term $\nu_i(t)$ as a sum in the x-variable, applying Cauchy-Schwarz, and extending the sum over $x \in E$ to a sum over $x \in \mathbb{Z}_q^d$, we see that

$$\begin{aligned}
|\nu_i(t)|^2 &\leq |E| q^{-2} \sum_{x \in \mathbb{Z}_q^d} \sum_{y, y' \in E} \sum_{s, s' \in \mathbb{Z}^\times_{p^{\ell-i}}} \chi\left(p^i(sy - s'y')\right) \chi\left(p^i t(s' - s)\right) \\
&\leq |E| q^{d-2} \sum_{\substack{y, y' \in E \\ p^i(sy - s'y') = \vec{0} \\ s, s' \in \mathbb{Z}^\times_{p^{\ell-i}}}} \chi\left(p^i t(s' - s)\right)
\end{aligned}$$

We split the last sum into two parts, I and II, where I corresponds to the sum over the terms where $s = s'$, and II is over the set (s, s'), where $s \neq s'$. We claim that term II is a nonpositive quantity. Accepting this for a moment, we see that

$$\begin{aligned}
I &= |E| q^{d-2} \sum_{\substack{s \in \mathbb{Z}^\times_{p^{\ell-i}} \\ p^i s(y - y') = 0}} E(y) E(y') \\
&= |E| q^{d-2} p^{\ell-i} \left(1 - \frac{1}{p}\right) \sum_{p^i y = p^i y'} E(y) E(y') \\
&\leq |E| q^{d-2} p^{\ell-i} \sum_{\alpha \in \mathbb{Z}_{p^{\ell-i}}} |R_E(\alpha)|^2,
\end{aligned}$$

where $R_E(\alpha) = \{y \in E : y \equiv \alpha \ (mod\ p^{\ell-i})\}$. Since the Kernel K of the map

$$\pi_{p^\ell, p^{\ell-i}} : \mathbb{Z}^d_{p^\ell} \to \mathbb{Z}^d_{p^{\ell-i}}$$

has size p^{id}, it follows that

$$\sum_{\alpha \in \mathbb{Z}_{p^{\ell-i}}} |R_E(\alpha)|^2 \leq |E| p^{id}.$$

Putting everything together, since the term II is nonpositive, it follows that

$$|\nu_i(t)|^2 \leq I \leq |E| q^{d-2} p^{\ell-i} \cdot |E| p^{id}$$

from which it immediately follows that

$$|\nu_i(t)| \leq |E| q^{\frac{d-1}{2}\left(1+\frac{i}{\ell}\right)}.$$

Therefore, for each $t \in \mathbb{Z}_q^\times$, we have

$$\nu(t) = \frac{|E|^2}{q} + \underbrace{\nu_0(t) + \ldots \nu_{\ell-1}(t)}_{:=R(t)},$$

where $|R(t)| \leq \ell |E| q^{\frac{d-1}{2}\left(2-\frac{1}{\ell}\right)}$. Therefore, $\nu(t) > 0$ whenever $|E| > \ell q^{\left(\frac{2\ell-1}{2\ell}\right)d+\frac{1}{2\ell}}$, as claimed. It remains, however, to show that the term II appearing in the bound for $|\nu_i(t)|^2$ is indeed nonpositive. Recall that

$$\begin{aligned} II &= |E| q^{d-2} \sum_{y,y' \in E} \sum_{\substack{s,s' \in \mathbb{Z}_{p^{\ell-i}}^\times \\ p^i(sy-s'y')=0 \\ s \neq s'}} \chi\left(p^i t(s'-s)\right) \\ &= |E| q^{d-2} \sum_{y,y' \in E} \sum_{\substack{p^i(b(ay-y'))=0 \\ a,b \in \mathbb{Z}_{p^{\ell-i}}^\times \\ a \neq 1}} \chi\left(p^i t(b(1-a))\right). \end{aligned}$$

Furthermore, we break up the sum II into two additional pieces according to whether $1-a \in \mathbb{Z}_{p^{\ell-i}} \setminus \{0\}$ is a unit or not:

$$\begin{aligned} II_A &= |E| q^{d-2} \sum_{y,y' \in E} \sum_{\substack{p^i(b(ay-y'))=0 \\ a,b \in \mathbb{Z}_{p^{\ell-i}}^\times \\ 1-a \in \mathbb{Z}_{p^{\ell-i}}^\times}} \chi\left(p^i t(b(1-a))\right) \\ II_B &= |E| q^{d-2} \sum_{y,y' \in E} \sum_{\substack{p^i(b(ay-y'))=0 \\ a,b \in \mathbb{Z}_{p^{\ell-i}}^\times \\ 1-a \notin \mathbb{Z}_{p^{\ell-i}}^\times}} \chi\left(p^i t(b(1-a))\right) \end{aligned}$$

First, and foremost, note that by summing in b and applying orthogonality, we get that

$$
\begin{aligned}
II_A &= |E|q^{d-2} \sum_{y,y' \in E} \sum_{\substack{p^i(b(ay-y'))=0 \\ a,b \in \mathbb{Z}^{\times}_{p^{\ell-i}} \\ 1-a \in \mathbb{Z}^{\times}_{p^{\ell-i}}}} \chi\left(p^i t(b(1-a))\right) \\
&= -|E|q^{d-2} \sum_{y,y' \in E} \sum_{a,1-a \in \mathbb{Z}^{\times}_{p^{\ell-i}}} 1
\end{aligned}
$$

which is negative real quantity. Also, note that if $a \in \mathbb{Z}^{\times}_{p^{\ell-i}}$, but $1-a \notin \mathbb{Z}^{\times}_{p^{\ell-i}}$, then $1-a = p^j s$, for some $0 < j < \ell - i$, where $s \in \mathbb{Z}^{\times}_{p^{\ell-i-j}}$. Thus, we can write

$$
II_B = |E|q^{d-2} \sum_{\substack{y,y' \in E \\ p^i b((1-p^j s)y-y')=0 \\ b \in \mathbb{Z}^{\times}_{p^{\ell-i}}}} \sum_{j=1}^{\ell-i-1} L_j,
$$

where we set

$$
L_j := \sum_{s \in \mathbb{Z}^{\times}_{p^{\ell-i-j}}} \chi(p^{i+j}tbs) = -1,
$$

and we applied orthogonality as we summed in the variable s, as tb is a unit. Therefore, II_B is a negative term, and the claim, hence the proof, follows.

4.3.2 Proof of Theorem 4.7

We will say that a Dirichlet character ψ has conductor m if m is the smallest positive divisor $m|q$ such that $\psi = \psi' \circ \pi_{q,m}$ for some Dirichlet character $\pmod{m}$. Here $\pi_{q,m} : \mathbb{Z}^{\times}_q \to \mathbb{Z}^{\times}_m$ is the natural projection. A Dirichlet character $\pmod{q}$ will be called primitive if it has conductor q. We need the following well known results.

Proposition 4.8 ([31])**.** *Let χ denote a nontrivial additive character of $\mathbb{Z}_n$. For $a \in \mathbb{Z}_n$ with $(a, n) = 1$, we have*

$$G(a, n) := \sum_{x \in \mathbb{Z}_n} \chi(ax^2) = \begin{cases} \varepsilon_n \left(\frac{a}{n}\right) \sqrt{n} & n \equiv \ 1 \ mod \ 2 \\ 0 & n \equiv \ 2 \ mod \ 4 \\ (1+i)\varepsilon_a^{-1} \left(\frac{n}{a}\right) \sqrt{n} & n \equiv \ 0 \ mod \ 4 \ \& \ a \equiv \ 1 \ mod \ 2 \end{cases}$$

where $\left(\frac{\cdot}{c}\right)$ denotes the Jacobi symbol and

$$\varepsilon_n = \begin{cases} 1 & n \equiv 1 \ mod \ 4 \\ i & n \equiv 3 \ mod \ 4 \end{cases}$$

Furthermore, for general values of $a \in \mathbb{Z}_n$, we have

$$G(a, n) = (a, n) G\left(\frac{a}{(a, n)}, \frac{n}{(a, n)}\right).$$

Definition 4.9 (Generalized Gauss Sum)**.** *Let ψ denote a Dirichlet character mod n and $\chi_a(x) = e^{2\pi i a x/n}$. Then, we set*

$$\tau(\psi, \chi_a) = \sum_{x \in \mathbb{Z}_n} \psi(x)\chi_a(x).$$

When $a = 1$, we simply write $\tau(\psi, \chi_1) = \tau(\psi)$.

Proposition 4.10 ([31])**.** *Suppose ψ is a Dirichlet character mod q and $(a, q) = 1$. Then,*

$$\tau(\psi, \chi_a) = \overline{\psi(a)}\tau(\psi).$$

Proof. Since $\psi(a)\overline{\psi(a)} = 1$, and $(a, q) = 1$, we have

$$\tau(\psi, \chi_a) = \overline{\psi(a)} \sum_{x \in \mathbb{Z}_q} \psi(ax)\chi_1(ax) = \overline{\psi(a)} \sum_{y \in \mathbb{Z}_q} \psi(y)\chi_1(y) = \overline{\psi(a)}\tau(\psi).$$

□

Proposition 4.11 ([31]). *Let ψ denote a Dirichlet character mod n which is induced by a primitive character ψ^* modulo n^*. Then,*

$$\tau(\psi) = \mu\left(\frac{n}{n^*}\right)\psi^*\left(\frac{n}{n^*}\right)\tau(\psi^*). \tag{4.1}$$

Here, μ is the Möbius function:

$$\mu(n) = \begin{cases} 1 & n = 1 \\ 0 & n \text{ is not squarefree} \\ (-1)^k & n = p_1 \dots p_k \end{cases}$$

Furthermore, if ψ is a primitive Dirichlet character modulo n, then,

$$|\tau(\psi)| \leq \sqrt{n} \tag{4.2}$$

Corollary 4.12. *Given any Dirichlet character ψ, and $\chi_a(x) = e^{2\pi iax/n}$, we have*

$$|\tau(\psi, \chi_a)| \leq \sqrt{n}.$$

We first show Theorem 4.7 for powers of odd primes. Assume then, that $q = p^\ell$, and let χ denote a nontrivial character additive on $\mathbb{Z}_q$.

$$\begin{aligned} |S_t| = \sum_{x \in \mathbb{Z}_q^d} S_t(x) &= q^{-1} \sum_{s \in \mathbb{Z}_q} \sum_{x \in \mathbb{Z}_q^d} \chi(sx_1^2) \dots \chi(sx_d^2)\chi(-st) \\ &= q^{-1}\left(T_\infty + T_0 + \dots + T_{\ell-1}\right), \end{aligned}$$

where

$$\begin{aligned} T_i &= \sum_{\substack{s \in \mathbb{Z}_q \\ val_p(s)=i}} \sum_{x \in \mathbb{Z}_q^d} \chi(sx_1^2) \dots \chi(sx_d^2)\chi(-st) \\ &= \sum_{\substack{s \in \mathbb{Z}_q \\ val_p(s)=i}} \left(\sum_{x \in \mathbb{Z}_q} \chi(sx^2)\right)^d \chi(-st). \\ &= \sum_{\substack{s \in \mathbb{Z}_q \\ val_p(s)=i}} (G(s,q))^d \chi(-st) \end{aligned}$$

It is clear that $T_\infty = q^d = p^{\ell d}$. For $i = 0, \dots, \ell - 1$, note that if $val_p(s) = i$, then s can be written in the form $s = p^i s'$, where s' is determined uniquely mod $\mathbb{Z}^\times_{p^{\ell-i}}$. Using this fact, along with the bound from Proposition 4.8, we see that

$$\begin{aligned} T_i &= p^{id} \sum_{s \in \mathbb{Z}^\times_{p^{\ell-i}}} (G(s, p^{\ell-i}))^d \chi(-st) \\ &= p^{id} \varepsilon^d_{p^{\ell-i}} \left(p^{\ell-i}\right)^{\frac{d}{2}} \sum_{s \in \mathbb{Z}^\times_{p^{\ell-i}}} \eta\left(s\right)^{d(\ell-i)} \chi(-st) \end{aligned}$$

where $\eta(s) = \left(\frac{s}{p}\right)$ is the Legendre symbol. If $d(\ell - i)$ is even, we see that

$$\begin{aligned} T_i &= p^{\ell \frac{d}{2} + i \frac{d}{2}} \varepsilon^d_{p^{\ell-i}} \sum_{s \in \mathbb{Z}^\times_{p^{\ell-i}}} \chi(-st) \\ &= -p^{\ell \frac{d}{2} + i \frac{d}{2}} \varepsilon^d_{p^{\ell-i}} \sum_{s \notin \mathbb{Z}^\times_{p^{\ell-i}}} \chi(-st), \end{aligned}$$

and hence $|T_i| \le p^{(\ell+i)\frac{d}{2}}(p^{\ell-i-1}) = p^{\ell\left(\frac{d+2}{2}\right) + i\left(\frac{d-2}{2}\right) - 1}$. If $d(\ell - i)$ is odd, then,

$$\begin{aligned} T_i &= p^{(\ell+i)\frac{d}{2}} \varepsilon^d_{p^{\ell-i}} \sum_{s \in \mathbb{Z}^\times_{p^{\ell-i}}} \eta(s)\chi(-st) \\ &= p^{(\ell+i)\frac{d}{2}} \varepsilon^d_{p^{\ell-i}} \left(\underbrace{\sum_{s \in \mathbb{Z}_{p^{\ell-i}}} \eta(s)\chi(-st)}_{\tau(\eta, \chi_{-s})} - \underbrace{\sum_{s \notin \mathbb{Z}_{p^{\ell-i}}} \eta(s)\chi(-st)}_{R} \right). \end{aligned}$$

By Corollary 4.12, $|\tau(\eta, \chi_{-s})| \le \sqrt{p^{\ell-i}}$. Using a crude bound for $|R|$, we see that

$$|T_i| \le p^{(\ell+i)\frac{d}{2}} \left(p^{(\ell-i)\frac{1}{2}} + p^{\ell-i-1} \right).$$

Noting that $\frac{\ell-i}{2} \le \ell - i - 1$ for $i \le \ell - 2$, we have shown that $|T_i| \le 2p^{\ell\frac{d+2}{2} + i\frac{d-2}{2} - 1}$ when $i = 0, \dots, \ell - 2$, and $|T_{\ell-1}| \le 2p^{\ell d - \frac{d-1}{2}}$. Altogether, our estimates show:

$$|T_i| \le |T_{\ell-1}| \le \begin{cases} p^{\ell d - \frac{d}{2}} & d(\ell-1) \text{ is even} \\ 2p^{\ell d - \frac{d-1}{2}} & d(\ell-1) \text{ is odd} \end{cases}$$

Thus, we have $|S_t| = q^{d-1} + q^{-1}(T_0 + \cdots + T_{\ell-1})$, where

$$|T_0 + \cdots + T_{\ell-1}| \leq \sum_{i=0}^{\ell-1} |T_i| \leq \begin{cases} \ell p^{\ell d - \frac{d}{2}} & d(\ell-1) \text{ is even} \\ 2\ell p^{\ell d - \frac{d-1}{2}} & d(\ell-1) \text{ is odd} \end{cases} \tag{4.3}$$

Putting everything together, and recalling that we set $q = p^\ell$, we have that

$$\begin{aligned} |S_t| &= p^{\ell(d-1)} + O\left(q^{-1}\sum_{i=0}^{\ell-1}|T_i|\right) & (4.4) \\ &= q^{d-1} + O\left(\begin{Bmatrix} \ell p^{\ell(d-1)-\frac{d}{2}} & d(\ell-1) \text{ is even} \\ \ell p^{\ell(d-1)-\frac{d-1}{2}} & d(\ell-1) \text{ is odd} \end{Bmatrix}\right) \\ &= p^{\ell(d-1)}(1+o(1)). & (4.5) \end{aligned}$$

The full case follows from the Chinese Remainder Theorem. Recall for $q = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, then $\mathbb{Z}_q, \mathbb{Z}_q^\times$, and $\mathbb{Z}_q^d$ decompose as the following Cartesian products

$$\begin{aligned} &\mathbb{Z}_q \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}, \\ &\mathbb{Z}_q^\times \cong \mathbb{Z}_{p_1^{\alpha}}^\times \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}^\times, & (4.6) \\ &\mathbb{Z}_q^d \cong \mathbb{Z}_{p_1^{\alpha_1}}^d \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}^d. & (4.7) \end{aligned}$$

To find $|S_t|$ for q, one must find the number of solutions in $\mathbb{Z}_q^d$ to the equation

$$f(x) = x_1^2 + \cdots + x_d^2 - t. \tag{4.8}$$

However, (4.6) implies that each unit $t \in \mathbb{Z}_q^\times$ can be written as $t = (t_1, \ldots, t_k)$, where $t_i \in \mathbb{Z}_{p_i^{\alpha_i}}^\times$ is also a unit. Thus (4.7) shows that solving (4.8) in $\mathbb{Z}_q^d$ is equivalent to solving (4.8) in each component $\mathbb{Z}_{p_i^{\alpha_i}}^d$. It follows that for $t = (t_1, \ldots, t_k)$ we have:

$$|S_t| = \prod_{i=1}^{d} |S_{t_i}| = \prod_{i=1}^{d} p_i^{\ell_i(d-1)}(1+o(1)) = q^{d-1}(1+o(1),$$

which proves the first part of Theorem 4.7. We now proceed with the case $q = 2^\alpha$, for dimensions $d \equiv 0 \pmod 4$. As before,

$$|S_t| = q^{d-1} + q^{-1}(T_\infty + T_0 + \cdots + T_{\alpha-1}),$$

where

$$\begin{aligned} T_i &= \sum_{\substack{s\in\mathbb{Z}_q \\ val_2(s)=i}} \left(G(s,2^\alpha)\right)^d \chi(-st) \\ &= 2^{id} \sum_{s\in\mathbb{Z}^{\times}_{2\alpha-i}} G(s,2^{\alpha-i})^d \chi(-st). \end{aligned}$$

Applying Proposition 4.8, we see that

$$\begin{aligned} T_i &= 2^{id}2^{(\ell-i)\frac{1}{2}}(1+i)^d \sum_{s\in\mathbb{Z}^{\times}_{2\alpha-i}} \varepsilon_s^{-d} \left(\frac{2^{\alpha-i}}{s}\right)^d \chi(-st) \\ &= 2^{\alpha\frac{d}{2}+i\frac{d}{2}}(1+i)^d \sum_{s\in\mathbb{Z}^{\times}_{s\alpha-i}} \chi(-st) \\ &= -2^{\alpha\frac{d}{2}+i\frac{d}{2}}(1+i)^d \sum_{s\notin\mathbb{Z}^{\times}_{s\alpha-i}} \chi(-st), \end{aligned}$$

so long as $d \equiv 0 \pmod 4$, and hence $|T_i| \leq 2^{\alpha\frac{d+2}{2}+(i+1)\frac{d-2}{2}}$, which gives

$$|S_t| = q^{d-1} + q^{-1}\sum_{i=0}^{\alpha-1}|T_i| \leq (\alpha+1)q^{d-1}.$$

The conclusion to the second statement in Theorem 4.7 then follows from the same reasoning as in the odd case. Write $n = 2^\alpha m$, where m is odd. Writing $t = (t_1, t_2)$, where $t \in \mathbb{Z}_n^\times, t_1 \in \mathbb{Z}_{2^\alpha}^\times$, and $t_2 \in \mathbb{Z}_m^\times$, we see that

$$|S_t| = |S_{t_1}||S_{t_2}| \leq (\alpha+1)2^{\alpha(d-1)}m^{d-1}(1+o(1)) = O_\alpha(n^{d-1}),$$

as claimed.

Bibliography

[1] J. Bourgain, *A Szemerédi type theorem for sets of positive density*, Israel J. Math. **54** (1986), no. 3, 307-331. 9

[2] J. Bourgain, *Sum-product theorems and exponential sum bounds in residue classes for general modulus*, C. R. Math. Acad. Sci. Paris **344** (2007), no. 6, 349-352. 35

[3] J. Bourgain, M. C. Chang, *Sum-product theorem and exponential sum estimates in residue classes with modulus involving few prime factors,* C. R. Math. Acad. Sci. Paris **339** (2004), no. 7, 463-466. 35

[4] J. Bourgain, M. C. Chang, *Exponential sum estimates over subgroups and almost subgroups of $\mathbb{Z}_Q^*$, where Q is composite with few prime factors,* Geom. Funct. Anal. **16** (2006), no. 2, 327-366. 35

[5] J. Bourgain, A. Glibichuk, S. 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), no. 2, 380-398. 24

[6] J. Bourgain, N. Katz, T. Tao, *A sum-product estimate in finite fields and applications*, GAFA **14** (2004), no 1, 27-57. 23, 32

[7] M. C. Chang *The Erdős-Szemerédi problem on sum set and product set.* Annals of Math. **157** (2003), 939-957. 23

[8] J. Chapman, D. Erdoğan, D. Hart, A. Iosevich, D. Koh, *Pinned distance sets, k-simplices, Wolff's exponent in finite fields and sum-product estimates*, (accepted by Math Z.). 9, 10

[9] D. Covert, D. Hart, A. Iosevich, D. Koh, M. Rudnev, *Generalized incidence theorems, homogeneous forms, and sum-product estimates in finite fields.* European J. Combin. **31**, 206-319, (2010). 25

[10] D. Covert, D. Hart, A. Iosevich, S. Senger, I. Uriarte-Tuero, *A Furstenberg-Katznelson-Weiss type theorem on (d+1)-point configurations in sets of positive density in finite field geometries* (to appear, Discrete Mathematics). 10, 14

[11] D. Covert, A. Iosevich, J. Pakianathan, *Geometric Configurations in the ring of integers modulo q* (in progress). 36

[12] Z. Dvir, *On the size of Kakeya sets in finite fields.* J. Amer. Math Soc., **22**, 1093-1097, (2009). 1

[13] Gy. Elekes, *On the number of sums and products. Acta Arith.* **81** (1997), 365–367. 22

[14] B. Erdoğan, *A bilinear Fourier extension theorem and applications to the distance set problem.* IMRN **23**, 1411-1425 (2005). 9

[15] P. Erdős, *Integral distances*, Bull. Amer. Math. Soc. **51** (1945) 996. 8

[16] P. Erdős and E. Szemerédi, *On sums and products of integers.* Studies in pure mathematics, **213–218**, Birkhäuser, Basel, 1983. 22

[17] K. J. Falconer, *On the Hausdorff dimensions of distance sets*, Mathematatika **32** (1986) 206-212. 8

[18] H. Furstenberg, Y. Katznelson, B. Weiss, *Ergodic theory and configurations in sets of positive density.* Mathematics of Ramsey theory, 184-198, Alg. Combin., 5, Springer, Berlin, (1990) 9

[19] M. Garaev, *An explicit sum-product estimate in Fp*, International Mathematics Research Notices no. **11** (2007), Art. Id.rnm035. (Oxford University Press). 24

[20] M. Garaev, *The sum product estimate for large subsets of prime fields.* Proceedings of the American Mathematical Society **136** (2008), pp. 2735-2739. 24, 35

[21] M. Garaev and C. Y. Shen, *On the size of the set A(A+1)*, Mathematische Zeitschrift **265** (2010), pp. 125-132. 25

[22] J. Garibaldi, A. Iosevich, S. Senger, *Erdős Distance Problem*, AMS Student Library Series, **56**, (2011). 8

[23] A. Glibichuk, *Combinatorial properties of sets of residues modulo a prime and the Erdős–Graham problem.* Mat. Zametki **79** (2006) 384395. Translation in: Math. Notes, **79** (2006), 356365. 32

[24] A. Glibichuk *Additive properties of product sets in an arbitrary finite field,* Additive combinatorics, 279286, CRM Proc. Lecture Notes, 43, Amer. Math. Soc., Providence, RI, 2007. 32

[25] L. Guth and N. Katz *On the Erdős distinct distances problem in the plane.* (preprint) arXiv:1011.4105 (2010). 8

[26] D. Hart, A. Iosevich *Ubiquity of simplices in subsets of vector spaces over finite fields.*, Anal. Math., (2008) volume **34** (1). 10

[27] D. Hart, A. Iosevich, *Sums and products in finite fields: An integral geometric viewpoint.* Contemporary Mathematics: Radon transforms, geometry, and wavelets, **464** (2008). v, 25, 26, 35

[28] D. Hart, A. Iosevich, D. Koh and M. Rudnev, *Averages over hyperplanes, sum-product theory in vector spaces over finite fields and the Erdős-Falconer distance conjecture*, Transactions of the AMS, **363** (2011) 3255-3275. 9, 26

[29] D. Hart, A. Iosevich, S. Solymosi *Sum-product estimates in finite fields via Kloosterman sums*, Int. Math. Res. Notices (2007) Vol. 2007. 24

[30] A. Iosevich, M. Rudnev, *Erdős distance problem in vector spaces over finite fields.* Trans. Amer. Math. Soc. 359 (2007), no. 12, 6127–6142. 9, 15

[31] H. Iwaniec, and E.Kowalski, *Analytic Number Theory*, Colloquium Publications 53 (2004). 19, 41, 42

[32] A. Iosevich and M. Rudnev, *Erdős-Falconer distance problem in vector spaces over finite fields*, Trans. Amer. Math. Soc., 359 (2007), no. 12, 6127–6142 (electronic). 9, 15

[33] N. Katz and C. Y. Shen, *A slight improvement to Garaev's sum product estimate.* Proc. Amer. Math. Soc. **136** (2008), no. 137, 2499-2504. 24, 25

[34] S. Lang, *Algebra*, Addison-Wesley Publishing Company, Menlo Park, California, (1984). 13

[35] R. Lidl, H. Niederreiter, *An Introduction to Finite Fields and Applications*, Cambridge University Press, (1997). 18

[36] A. Magyar, *On distance sets of large sets of integer points.* Israel J. of Math., **164** (2008), no. 1, 251-263. 9

[37] A. Magyar, *k-point configurations in sets of positive density of* $\mathbb{Z}^n$, Duke Math. J., Vol **146**, no. 1 (2009), 1 - 34. 10

[38] W. Rudin, *Fourier Analysis on Groups*, Interscience Tracts in Pure and Applied Math., **No. 12.** Wiley, New York, (1962). 3

[39] M. Rudnev, *An improved sum-product inequality in fields of prime order*, (preprint) arXiv:1011.2738v1 (2010). 24

[40] H. Salié, *Űber die Kloostermanschen summen S(u,v;q)*, Math.Z., 34 (1932), 91-109. 19

[41] C. Y. Shen, *Algebraic methods in sum-product phenomena.* Israel J. Math, (to appear). 25

[42] J. Solymosi, *Bounding multiplicative energy by the sumset.* Advances in Mathematics, Volume **222**, Issue 2, 2009, 402408. 23

[43] T. Tao, *The sum-product phenomenon in arbitrary rings.* Contrib. Discrete Math. **4** (2009), no. 2, 5982 22, 23

[44] T. Tao, V. Vu, *Additive Combinatorics.* Cambridge University Press, (2006). 22, 23

[45] L. A. Vinh, *Triangles in vector spaces over finite fields*, Online J. Anal. Comb. (to appear) (2008). 10

[46] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U. S. A. 34, (1948), 204–207. 19

[47] T. Wolff, *Decay of circular means of Fourier transforms of measures*, International Mathematics Research Notices **10** (1999) 547-567. 9

[48] T. Ziegler, *An application of ergodic theory to a problem in geometric Ramsey theory*, Israel J. Math. **114** (1999) 271-288.

10

VITA

David Covert was born November 4, 1984 in Loring Air Force Base (currently Limestone, Maine). He and his family moved to Buffalo, NY when he was 7. He graduated from Canisius High School in 2002 and Canisius College in 2006 at which time he decided to pursue a Ph.D. in Mathematics at the University of Missouri. David earned a Master's degree in Pure Mathematics from the University of Missouri in May 2009, was married in 2010, and hopes to graduate with his Ph.D. in May 2011.