UNIVERSITY OF CALIFORNIA SAN DIEGO

Connections between additive combinatorics, graph theory, and incidence geometry

A dissertation submitted in partial satisfaction of the
requirements for the degree
Doctor of Philosophy

in

Mathematics

by

Mozhgan Mirzaei

Committee in charge:

Professor Andrew Suk, Chair
Professor Shachar Lovett
Professor Jonathan Novak
Professor Brendon Rhoades
Professor Jacques Verstraëte

2020

The dissertation of Mozhgan Mirzaei is approved, and it is acceptable in quality and form for publication on microfilm and electronically:

_____

_____

_____

_____

_____

_____

Chair

University of California San Diego

2020

DEDICATION

To Khashayar.

TABLE OF CONTENTS

LIST OF FIGURES

ACKNOWLEDGEMENTS

I wish to thank Andrew Suk for his advice and guidance in writing this thesis. I would like to thank Shachar Lovett, Jonathan Novak, Brendon Rhoades, and Jacques Verstraëte for serving on my thesis committee. I also want to thank Thang Pham, for being an outstanding collaborator and friend.

A huge thanks to my dear parents Leila and Reza, and to my sisters Maryam and Mahgol, for their endless love, consistent encouragement, support, and understanding throughout all my life. I also like to thank my best friend Fereshteh over the years that certainly made her marks on my life for being the greatest friend one could ever hope for and for always being there for me even though life had kept us mostly apart. Last but not the least, I am beyond words of gratitude for the constant of my life, Khashayar, for being the better half of me, and for his unbelievable amount of love, encouragement and support.

Chapter 1 is a version of the material appearing in "*On Grids in Point-Line Arrangements in the Plane*," *In 35th International Symposium on Computational Geometry* (SoCG 2019) (Vol. 129, p. 50), co-authored with Andrew Suk. The author was one of the primary investigators and authors of this paper.

Chapter 2 is a version of the material in "*Constructions of Point-Line Arrangements in the Plane with Large Girth*", co-authored with Andrew Suk and Jacques Verstraëte, which has been submitted for publication. The author was one of the primary investigators and authors of this paper.

Chapter 3 is a version of the material appearing in "*A Positive Fraction Mutually Avoiding Sets Theorem*", *Discrete Mathematics*, Vol. 343, Issue 3, 2020, co-authored with Andrew Suk. The author was one of the primary investigators and authors of this paper.

Chapter 4 is a version of the material appearing in "*A Note on Conditional Expanders over Prime Fields*," which will appear in Discrete Mathematics. The author was the primary investigator and author of this paper.

Chapter 5 is a version of the material appearing in "*Exponential Sum Estimates over Prime Fields*", *International Journal of Number Theory,* Vol. 16, No. 02, pp. 291-308, 2020, co-authored with Doowon Koh, Thang Pham, and Chun-Yen Shen. The author was one of the primary investigators and authors of this paper.

Chapter 6 is a version of the material in "*Moderate Expanders over Rings*," co-authored with Dao Nguyen Van Anh, Le Quang Ham, Doowon Koh, Hossein Mojarrad, and Thang Pham, which has been submitted for publication. The author was one of the primary investigators and authors of this paper.

VITA

2020	Ph. D. in Mathematics, University of California San Diego.
2014	B. S. in Mathematics, Sharif University of Technology.

PUBLICATIONS

M. Mirzaei, A. Suk, J. Verstrate, *Constructions of Point-Line Arrangements in the Plane with Large Girth*, submitted for publication.

D. Anh, L. Ham, D. Koh, M. Mirzaei, H. Mojarrad, and T. Pham, *Moderate Expanders over Rings,* submitted for publication.

M. Mirzaei, *A Note on Conditional Expanders over Prime Fields, to appear in Discrete Mathematics*, 2020.

M. Mirzaei, A. Suk, *A Positive Fraction Mutually Avoiding Sets Theorem, Discrete Mathematics*, Vol. 343, Issue 3, 2020.

D. Koh, M. Mirzaei, T. Pham, C. Shen, *Exponential Sum Estimates over Prime Fields*, *International Journal of Number Theory,* Vol. 16, No. 02, pp. 291-308, 2020,

M. Mirzaei, A. Suk, *On Grids in Point-Line Arrangements in the Plane, In 35th International Symposium on Computational Geometry* (SoCG 2019) (Vol. 129, p. 50). Schloss DagstuhlLeibniz-Zentrum fuer Informatik.

ABSTRACT OF THE DISSERTATION

Connections between additive combinatorics, graph theory, and incidence geometry

by

Mozhgan Mirzaei
Doctor of Philosophy in Mathematics

University of California San Diego, 2020

Professor Andrew Suk, Chair

This dissertation studies problems in extremal combinatorics, combinatorial number theory, and discrete geometry, and the interplay between these three areas.

One of the Erdős-like cornerstones in incidence geometry from which many other results follow, is the celebrated Szemerédi-Trotter Theorem which states that any arrangement of n points and n lines in the plane determines $O(n^{4/3})$ incidences, and this bound is tight. In this thesis, we study the effect of forbidding grids and short even cycles on the incidence graphs of point-line arrangements in the plane.

Let A and B be two disjoint finite sets of points in the plane such that their

union contains no three points on a line. We say that A *avoids* B if no straight line determined by a pair of points in A intersects the convex hull of B. A and B are called mutually avoiding if A avoids B and B avoids A. Aronov et al. showed that any set of n points in general position in the plane contains a pair of mutually avoiding sets, each of size at least $\Omega(\sqrt{n})$. Moreover, they proved that any set of n points in general position in $\mathbb{R}^d$ contains a pair of mutually avoiding sets, each of size at least $\Omega\left(n^{\frac{1}{d^2-d+1}}\right)$. In this thesis, we give a generalized version of mutually avoiding set theorem in the plane.

Given an algebraic structure R and a subset $A \subset R$, define the sum set and the product set of A to be $A + A = \{a + b : a, b \in A\}$ and $A \cdot A = \{a \cdot b : a, b \in A\}$ respectively. Showing under what conditions at least one of $|A + A|$ or $|A \cdot A|$ is large has a long history of study that continues to the present day. By employing recent developments on the energy of polynomials over finite fields, we give the best-known lower bounds on $\max\{|A + A|, |f(A, A)|\}$, when A is a small subset of $\mathbb{F}_p$, and f is a quadratic non-degenerate polynomial in $\mathbb{F}_p[x, y]$.

Chapter 1

On grids in point-line arrangements in the plane

1.1 Introduction

Given a finite set P of points in the plane and a finite set $\mathcal{L}$ of lines in the plane, let $I(P, \mathcal{L}) = \{(p, \ell) \in P \times \mathcal{L} : p \in \ell\}$ be the set of incidences between P and $\mathcal{L}$. The *incidence graph* of $(P, \mathcal{L})$ is the bipartite graph $G = (P \cup \mathcal{L}, I)$, with vertex parts P and $\mathcal{L}$, and $E(G) = I(P, \mathcal{L})$. If $|P| = m$ and $|\mathcal{L}| = n$, then the celebrated theorem of Szemerédi and Trotter [89] states that

$$|I(P, \mathcal{L})| \leq O(m^{2/3}n^{2/3} + m + n). \tag{1.1}$$

Moreover, this bound is tight which can be seen by taking the $\sqrt{m} \times \sqrt{m}$ integer lattice and bundles of parallel "rich" lines (see [64]). It is widely believed that the extremal configurations maximizing the number of incidences between m points and n lines in the plane exhibit some kind of lattice structure. The main goal of this thesis is to show that such extremal configurations must contain large *natural grids*.

Let P and P_0 (respectively, $\mathcal{L}$ and $\mathcal{L}_0$) be two sets of points (respectively, lines) in the plane. We say that the pairs $(P, \mathcal{L})$ and $(P_0, \mathcal{L}_0)$ are *isomorphic* if their incidence graphs are isomorphic. Solymosi made the following conjecture (see page 291 in [11]).

Conjecture 1.1. *For any set of points P_0 and for any set of lines $\mathcal{L}_0$ in the plane, the maximum number of incidences between n points and n lines in the plane containing no subconfiguration isomorphic to $(P_0, \mathcal{L}_0)$ is $o(n^{\frac{4}{3}})$.*

In [87], Solymosi proved this conjecture in the special case that P_0 is a fixed set of points in the plane, no three of which are on a line, and $\mathcal{L}_0$ consists of all of their connecting lines. However, it is not known if such configurations satisfy the following stronger conjecture.

Conjecture 1.2. *For any set of points P_0 and for any set of lines $\mathcal{L}_0$ in the plane, there is a constant $\varepsilon = \varepsilon(P_0, \mathcal{L}_0)$, such that the maximum number of incidences between n points and n lines in the plane containing no subconfiguration isomorphic to $(P_0, \mathcal{L}_0)$ is $O(n^{4/3-\varepsilon})$.*

Our first theorem is the following.

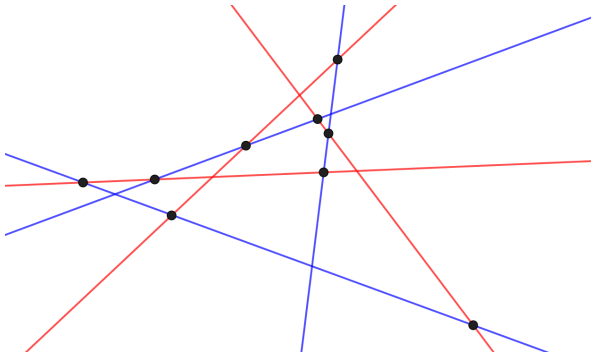

Figure 1.1: An example with $|\mathcal{L}_a| = |\mathcal{L}_b| = 3$ and $|P| = 9$.

Theorem 1.3. *For fixed $t > 1$, let $\mathcal{L}_a$ and $\mathcal{L}_b$ be two sets of t lines in the plane, and let $P_0 = \{\ell_a \cap \ell_b : \ell_a \in \mathcal{L}_a, \ell_b \in \mathcal{L}_b\}$ such that $|P_0| = t^2$. Then there is a constant $c = c(t)$ such that any arrangement of m points and n lines in the plane that does not contain a subconfiguration isomorphic to $(P_0, \mathcal{L}_a \cup \mathcal{L}_b)$ determines at most $c(m^{\frac{2t-2}{3t-2}} n^{\frac{2t-1}{3t-2}} + m^{1+\frac{1}{6t-3}} + n)$ incidences.*

See the Figure 1.1. As an immediate corollary, we prove Conjecture 1.2 in the following special case.

Corollary 1.4. *For fixed $t > 1$, let $\mathcal{L}_a$ and $\mathcal{L}_b$ be two sets of t lines in the plane, and let $P_0 = \{\ell_a \cap \ell_b : \ell_a \in \mathcal{L}_a, \ell_b \in \mathcal{L}_b\}$. If $|P_0| = t^2$, then any arrangement of n points and n lines in the plane that does not contain a subconfiguration isomorphic to $(P_0, \mathcal{L}_a \cup \mathcal{L}_b)$ determines at most $O(n^{\frac{4}{3}-\frac{1}{9t-6}})$ incidences.*

In the other direction, we prove the following.

Theorem 1.5. *Let $\mathcal{L}_a$ and $\mathcal{L}_b$ be two sets of 2 lines in the plane, and let $P_0 = \{\ell_a \cap \ell_b : \ell_1 \in \mathcal{L}_a, \ell_b \in \mathcal{L}_b\}$ such that $|P_0| = 4$. For $n > 1$, there exists an arrangement of n*

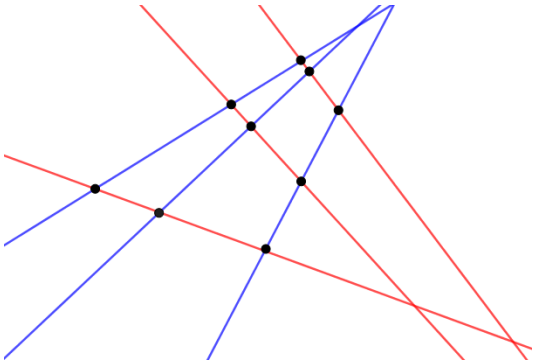

Figure 1.2: An example of a natural 3×3 grid.

points and n lines in the plane that does not contain a subconfiguration isomorphic to $(P_0, \mathcal{L}_a \cup \mathcal{L}_b)$, and determines at least $\Omega(n^{1+\frac{1}{14}})$ incidences.

Given two sets $\mathcal{L}_a$ and $\mathcal{L}_b$ of t lines in the plane, and the point set $P_0 = \{\ell_a \cap \ell_b : \ell_a \in \mathcal{L}_a, \ell_b \in \mathcal{L}_b\}$, we say that $(P_0, \mathcal{L}_a \cup \mathcal{L}_b)$ forms a *natural $t \times t$ grid* if $|P_0| = t^2$, and the convex hull of P_0, $conv(P_0)$, does not contain the intersection point of any two lines in $\mathcal{L}_a$ and does not contain the intersection point of any two lines in $\mathcal{L}_b$. See Figure 1.2.

Theorem 1.6. *For fixed $t > 1$, there is a constant $\varepsilon = \varepsilon(t)$, such that any arrangement of n points and n lines in the plane that does not contain a natural $t \times t$ grid determines at most $O(n^{\frac{4}{3}-\varepsilon})$ incidences.*

Let us remark that $\varepsilon = \Omega(1/t^2)$ in Theorem 1.6, and can be easily generalized to the off-balanced setting of m points and n lines.

We systemically omit floor and ceiling signs whenever they are not crucial for the sake of clarity of our presentation. All logarithms are assumed to be base 2. For $N > 0$, we let $[N] = \{1, \ldots, N\}$.

1.2 Proof of Theorem 1.3

In this section we will prove Theorem 1.3. We first list several results that we will use. The first lemma is a classic result in graph theory.

Lemma 1.7 (Kövari-Sós-Turán [49]). *Let $G = (V, E)$ be a graph that does not contain a complete bipartite graph $K_{r,s}$ $(1 \leq r \leq s)$ as a subgraph. Then $|E| \leq c_s |V|^{2-\frac{1}{r}}$, where $c_s > 0$ is constant which only depends on s.*

The next lemma we will use is a partitioning tool in discrete geometry known as *simplicial partitions*. We will use the dual version which requires the following definition. Let $\mathcal{L}$ be a set of lines in the plane. We say that a point p *crosses* $\mathcal{L}$ if it is incident to at least one member of $\mathcal{L}$, but not incident to all members in $\mathcal{L}$.

Lemma 1.8 (Matousek [58]). *Let $\mathcal{L}$ be a set of n lines in the plane and let r be a parameter such that $1 < r < n$. Then there is a partition on $\mathcal{L} = \mathcal{L}_1 \cup \cdots \cup \mathcal{L}_r$ into r parts, where $\frac{n}{2r} \leq |\mathcal{L}_i| \leq \frac{2n}{r}$, such that any point $p \in \mathbb{R}^2$ crosses at most $O(\sqrt{r})$ parts $\mathcal{L}_i$.*

Proof of Theorem 1.3. Set $t \geq 2$. Let P be a set of m points in the plane and let $\mathcal{L}$ be a set of n lines in the plane such that $(P, \mathcal{L})$ does not contain a subconfiguration isomorphic to $(P_0, \mathcal{L}_a \cup \mathcal{L}_b)$.

If $n \geq m^2/100$, then (2.1) implies that $|I(P, \mathcal{L})| = O(n)$ and we are done. Likewise, if $n \leq m^{\frac{t}{2t-1}}$, then (2.1) implies that $|I(P, \mathcal{L})| = O(m^{1+\frac{1}{6t-3}})$ and we are done. Therefore, let us assume $m^{\frac{t}{2t-1}} < n < m^2/100$. In what follows, we will show

that $|I(P,\mathcal{L})| = O(m^{\frac{2t-2}{3t-2}}n^{\frac{2t-1}{3t-2}})$. For sake of contradiction, suppose that $I(P,\mathcal{L}) \geq cm^{\frac{2t-2}{3t-2}}n^{\frac{2t-1}{3t-2}}$, where c is a large constant depending on t that will be determined later.

Set $r = \lceil 10n^{\frac{4t-2}{3t-2}}/m^{\frac{2t}{3t-2}} \rceil$. Let us remark that $1 < r < n/10$ since we are assuming $m^{\frac{t}{2t-1}} < n < m^2/100$. We apply Lemma 1.8 with parameter r to $\mathcal{L}$, and obtain the partition $\mathcal{L} = \mathcal{L}_1 \cup \cdots \cup \mathcal{L}_r$ with the properties described above. Note that $|\mathcal{L}_i| > 1$. Let G be the incidence graph of $(P,\mathcal{L})$. For $p \in P$, consider the set of lines in $\mathcal{L}_i$. If p is incident to exactly one line in $\mathcal{L}_i$, then delete the corresponding edge in the incidence graph G. After performing this operation between each point $p \in P$ and each part $\mathcal{L}_i$, by Lemma 1.8, we have deleted at most $c_1 m\sqrt{r}$ edges in G, where c_1 is an absolute constant. By setting c sufficiently large, we have

$$c_1 m\sqrt{r} = \sqrt{10}c_1 m^{\frac{2t-2}{3t-2}}n^{\frac{2t-1}{3t-2}} < (c/2)m^{\frac{2t-2}{3t-2}}n^{\frac{2t-1}{3t-2}}.$$

Therefore, there are at least $(c/2)m^{\frac{2t-2}{3t-2}}n^{\frac{2t-1}{3t-2}}$ edges remaining in G. By the pigeonhole principle, there is a part $\mathcal{L}_i$ such that the number of edges between P and $\mathcal{L}_i$ in G is at least

$$\frac{cm^{\frac{2t-2}{3t-2}}n^{\frac{2t-1}{3t-2}}}{2r} = \frac{cm^{\frac{4t-2}{3t-2}}}{20n^{\frac{2t-1}{3t-2}}}.$$

Hence, every point $p \in P$ has either 0 or at least 2 neighbors in $\mathcal{L}_i$ in G. We claim

that $(P, \mathcal{L}_i)$ contains a subconfiguration isomorphic to $(P_0, \mathcal{L}_a \cup \mathcal{L}_b)$. To see this, let us construct a graph $H = (\mathcal{L}_i, E)$ as follows. Set $V(H) = \mathcal{L}_i$. Let $Q = \{q_1, \ldots, q_w\} \subset P$ be the set of points in P that have at least two neighbors in $\mathcal{L}_i$ in the graph G. For $q_j \in Q$, consider the set of lines $\{\ell_1, \ldots, \ell_s\}$ from $\mathcal{L}_i$ incident to q_j, such that $\{\ell_1, \ldots, \ell_s\}$ appears in clockwise order. Then we define $E_j \subset \binom{\mathcal{L}_i}{2}$ to be a matching on $\{\ell_1, \ldots, \ell_s\}$, where

$$E_j = \begin{cases} \{(\ell_1, \ell_2), (\ell_3, \ell_4), \ldots, (\ell_{s-1}, \ell_s)\} & \text{if } s \text{ is even.} \\ \\ \{(\ell_1, \ell_2), (\ell_3, \ell_4), \ldots, (\ell_{s-2}, \ell_{s-1})\} & \text{if } s \text{ is odd.} \end{cases}$$

Set $E(H) = E_1 \cup E_2 \cup \cdots \cup E_w$. Note that E_j and E_k are disjoint, since no two points are contained in two lines. Since $|E_j| \geq 1$, we have

$$|E(H)| \geq \frac{cm^{\frac{4t-2}{3t-2}}}{60n^{\frac{2t-1}{3t-2}}}.$$

Since

$$|V(H)| = |\mathcal{L}_i| \leq \frac{m^{\frac{2t}{3t-2}}}{5n^{\frac{t}{3t-2}}},$$

this implies

$$|E(H)| \geq \frac{c}{60 \cdot 25}(V(H))^{2-\frac{1}{t}}.$$

By setting $c = c(t)$ to be sufficiently large, Lemma 1.7 implies that H contains a copy of $K_{t,t}$. Let $\mathcal{L}_1', \mathcal{L}_2' \subset \mathcal{L}_i$ correspond to the vertices of this $K_{t,t}$ in H, and let $P' = \{\ell_1 \cap \ell_2 \in P : \ell_1 \in \mathcal{L}_1', \ell_2 \in \mathcal{L}_2'\}$. We claim that $(P', \mathcal{L}_1' \cup \mathcal{L}_2')$ is isomorphic to $(P_0, \mathcal{L}_a \cup \mathcal{L}_b)$. It suffices to show that $|P'| = t^2$. For the sake of contradiction, suppose $p \in \ell_1 \cap \ell_2 \cap \ell_3$, where $\ell_1, \ell_2 \in \mathcal{L}_1'$ and $\ell_3 \in \mathcal{L}_2'$. This would imply $(\ell_1, \ell_3), (\ell_2, \ell_3) \in E_j$ for some j which contradicts the fact that $E_j \subset \binom{\mathcal{L}_i}{2}$ is a matching. Same argument follows if $\ell_1 \in \mathcal{L}_1'$ and $\ell_2, \ell_3 \in \mathcal{L}_2'$. This completes the proof of Theorem 1.3. □

1.3 Natural Grids

Given a set of n points P and a set of n lines $\mathcal{L}$ in the plane, if $|I(P, \mathcal{L})| \geq cn^{\frac{4}{3}-\frac{1}{9k-6}}$, where c is a sufficiently large constant depending on k, then Corollary 1.4 implies that there are two sets of k lines such that each pair of them from different sets intersects at a unique point in P. Therefore, Theorem 1.6 follows by combining Theorem 1.3 with the following lemma.

Lemma 1.9. *There is a natural number c such that the following holds. Let $\mathcal{B}$ be a set of ct^2 blue lines in the plane, and let $\mathcal{R}$ be a set of ct^2 red lines in the plane such*

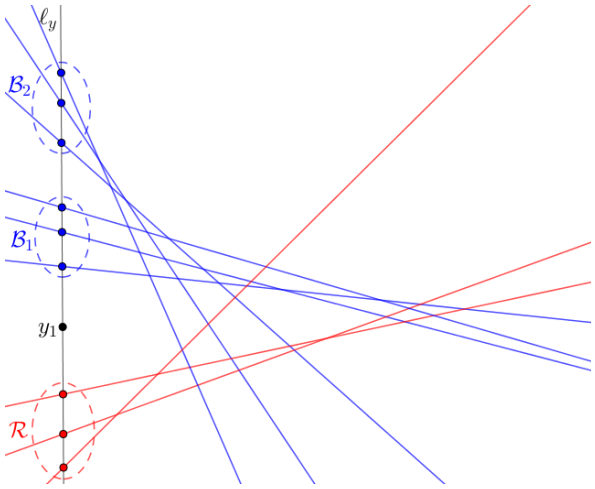

Figure 1.3: Sets $\mathcal{R}, \mathcal{B}_1, \mathcal{B}_2$ in the proof of Lemma 1.9.

that for $P = \{\ell_1 \cap \ell_2 : \ell_1 \in \mathcal{B}, \ell_2 \in \mathcal{R}\}$ *we have* $|P| = c^2t^4$. *Then* $(P, \mathcal{B} \cup \mathcal{R})$ *contains a natural* $t \times t$ *grid.*

To prove Lemma 1.9, we will need the following lemma which is an immediate consequence of Dilworth's Theorem.

Lemma 1.10. *For* $n > 0$, *let* $\mathcal{L}$ *be a set of* n^2 *lines in the plane, such that no two members intersect the same point on the* y*-axis. Then there is a subset* $\mathcal{L}' \subset \mathcal{L}$ *of size* n *such that the intersection point of any two members in* $\mathcal{L}'$ *lies to the left of the* y*-axis, or the intersection point of any two members in* $\mathcal{L}'$ *lies to the right of the* y*-axis.*

Proof. Let us order the elements in $\mathcal{L} = \{\ell_1, \ldots, \ell_{n^2}\}$ from bottom to top according to their y-intercept. By Dilworth's Theorem [22], $\mathcal{L}$ contains a subsequence of n lines whose slopes are either increasing or decreasing. In the first case, all intersection points are to the left of the y-axis, and in the latter case, all intersection points are to the right of the y-axis. □

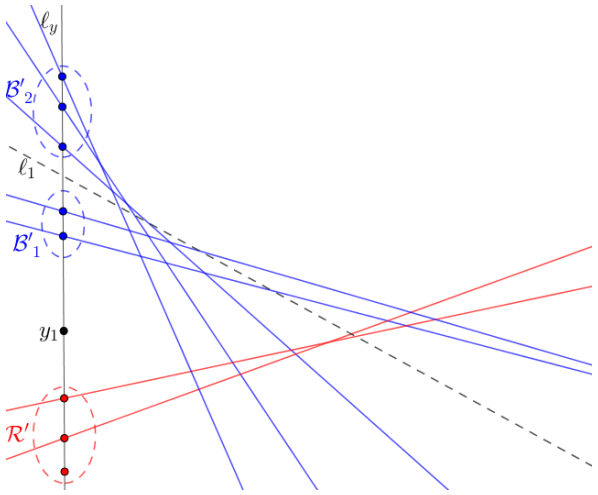

Figure 1.4: An example for the line ℓ_1.

Proof of Lemma 1.9. Let $(P, \mathcal{B} \cup \mathcal{R})$ be as described above, and let ℓ_y be the y-axis. Without loss of generality, we can assume that all lines in $\mathcal{B} \cup \mathcal{R}$ are not vertical, and the intersection point of any two lines in $\mathcal{B} \cup \mathcal{R}$ lies to the right of ℓ_y. Moreover, we can assume that no two lines intersect at the same point on ℓ_y.

We start by finding a point $y_1 \in \ell_y$ such that at least $|\mathcal{B}|/2$ blue lines in $\mathcal{B}$ intersect ℓ_y on one side of the point y_1 (along ℓ_y) and at least $|\mathcal{R}|/2$ red lines in $\mathcal{R}$ intersect ℓ_y on the other side. This can be done by sweeping the point y_1 along ℓ_y from bottom to top until $ct^2/2$ lines of the first color, say red, intersect ℓ_y below y_1. We then have at least $ct^2/2$ blue lines intersecting ℓ_y above y_1. Discard all red lines in $\mathcal{R}$ that intersect ℓ_y above y_1, and discard all blue lines in $\mathcal{B}$ that intersect ℓ_y below y_1. Hence, $|\mathcal{B}| \geq ct^2/2$.

Set $s = \lfloor ct^2/4 \rfloor$. For the remaining lines in $\mathcal{B}$, let $\mathcal{B} = \{b_1, \ldots, b_{2s}\}$, where the elements of $\mathcal{B}$ are ordered in the order they cross ℓ_y, from bottom to top. We partition $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$ into two parts, where $\mathcal{B}_1 = \{b_1, \ldots, b_s\}$ and $\mathcal{B}_2 = \{b_{s+1}, \ldots, b_{2s}\}$. By

applying an affine transformation, we can assume all lines in $\mathcal{R}$ have positive slope and all lines in $\mathcal{B}_1 \cup \mathcal{B}_2$ have negative slope. See Figure 1.3.

Let us define a 3-partite 3-uniform hypergraph $H = (\mathcal{R} \cup \mathcal{B}_1 \cup \mathcal{B}_2, E)$, whose vertex parts are $\mathcal{R}, \mathcal{B}_1, \mathcal{B}_2$, and $(r, b_i, b_j) \in \mathcal{R} \times \mathcal{B}_1 \times \mathcal{B}_2$ is an edge in H if and only if the intersection point $p = b_i \cap b_j$ lies above the line r. Note, if b_i and b_j are parallel, then $(r, b_i, b_j) \notin E$. Then a result of Fox et al. on semi-algebraic hypergraphs implies the following (see also [13] and [30]).

Lemma 1.11 (Fox et al. [29], Theorem 8.1)**.** *There exists a positive constant α such that the following holds. In the hypergraph above, there are subsets $\mathcal{R}' \subseteq \mathcal{R}, \mathcal{B}'_1 \subseteq \mathcal{B}_1, \mathcal{B}'_2 \subseteq \mathcal{B}_2$, where $|\mathcal{R}'| \geq \alpha|\mathcal{R}|, |\mathcal{B}'_1| \geq \alpha|\mathcal{B}_1|, |\mathcal{B}'_2| \geq \alpha|\mathcal{B}_2|$, such that either $\mathcal{R}' \times \mathcal{B}'_1 \times \mathcal{B}'_2 \subseteq E$, or $(\mathcal{R}' \times \mathcal{B}'_1 \times \mathcal{B}'_2) \cap E = \emptyset$.*

We apply Lemma 1.11 to H and obtain subsets $\mathcal{R}', \mathcal{B}'_1, \mathcal{B}'_2$ with the properties described above. Without loss of generality, we can assume that $\mathcal{R}' \times \mathcal{B}'_1 \times \mathcal{B}'_2 \subset E$, since a symmetric argument would follow otherwise. Let ℓ_1 be a line in the plane such that the following holds.

1. The slope of ℓ_1 is negative.

2. All intersection points between $\mathcal{R}'$ and $\mathcal{B}'_1$ lie above ℓ_1.

3. All intersection points between $\mathcal{R}'$ and $\mathcal{B}'_2$ lie below ℓ_1.

See Figure 1.4.

Line ℓ_1 defined above exists.

Proof. Let U be the upper envelope of the arrangement $\bigcup_{\ell \in \mathcal{R}'} \ell$, that is, U is the closure of all points that lie on exactly one line of $\mathcal{R}'$ and strictly above exactly the $|\mathcal{R}'| - 1$ lines in $\mathcal{R}'$.

Let P_1 be the set of intersection points between the lines in $\mathcal{B}'_1$ with U. Likewise, we define P_2 to be the set of intersection points between the lines in $\mathcal{B}'_2$ with U. Since U is x-monotone and convex the set P_2 lies to the left of the set P_1. Then the line ℓ_1 that intersects U between P_1 and P_2 and intersects ℓ_y between $\mathcal{B}'_1$ and $\mathcal{B}'_2$ satisfies the conditions above. □

Now we apply Lemma 1.10 to $\mathcal{R}'$ with respect to the line ℓ_1, to obtain $\sqrt{\alpha c/2} \cdot t$ members in $\mathcal{R}'$ such that every pair of them intersects on one side of ℓ_1. Discard all other members in $\mathcal{R}'$. Without loss of generality, we can assume that all intersection points between any two members in $\mathcal{R}'$ lie below ℓ_1, since a symmetric argument would follow otherwise. We now discard the set $\mathcal{B}'_2$.

Notice that the order in which the lines in $\mathcal{R}'$ cross $b \in \mathcal{B}'_1$ will be the same for any line $b \in \mathcal{B}'_1$. Therefore, we order the elements in $\mathcal{R}' = \{r_1, \ldots, r_m\}$ with respect to this ordering, from left to right, where $m = \lceil \sqrt{\alpha c/2} \cdot t \rceil$. We define ℓ_2 to be the line obtained by slightly perturbing the line $r_{\lfloor m/2 \rfloor}$ such that:

1. The slope of ℓ_2 is positive.

2. All intersection points between $\mathcal{B}'_1$ and $\{r_1, \ldots, r_{\lfloor m/2 \rfloor}\}$ lie above ℓ_2.

3. All intersection points between $\mathcal{B}'_1$ and $\{r_{\lfloor m/2 \rfloor + 1}, \ldots, r_m\}$ lie below ℓ_2.

See the Figure 1.5.

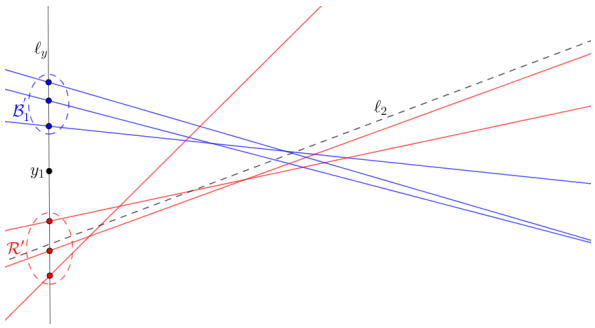

Figure 1.5: An example for the line ℓ_2.

Finally, we apply Lemma 1.10 to $\mathcal{B}'_1$ with respect to the line ℓ_2, to obtain at least $\sqrt{\alpha c} \cdot t/2$ members in $\mathcal{B}'_1$ with the property that any two of them intersect on one side of ℓ_2. Without loss of generality, we can assume that any two such lines intersect below ℓ_2 since a symmetric argument would follow. Set $\mathcal{B}^* \subset \mathcal{B}'_1$ to be these set of lines. Then $\mathcal{B}^* \cup \{r_1, \ldots, r_{\lfloor m/2 \rfloor}\}$ and their intersection points form a natural grid. By setting $c = c(t)$ to be sufficiently large, we obtain a natural $t \times t$ grid. □

1.4 Lower Bound Construction

In this section, we will prove Theorem 1.5. First, let us recall the definitions of Sidon and k-fold Sidon sets.

Let A be a finite set of positive integers. Then A is a *Sidon set* if the sum of all pairs are distinct, that is, the equation $x+y = u+v$ has no solutions with $x, y, u, v \in A$, except for trivial solutions given by $u = x, y = v$ and $x = v, y = u$. We define $s(N)$ to be the size of the largest Sidon set $A \subset \{1, \ldots, N\}$. Erdős and Turán proved the

following.

Lemma 1.12 (See [28] and [74]). *For $N > 1$, we have $s(N) = \Theta(\sqrt{N})$.*

Let us now consider a more general equation. Let $u_1, \ldots, u_4$ be integers such that $u_1 + u_2 + u_3 + u_4 = 0$, and consider the equation

$$u_1x_1 + u_2x_2 + u_3x_3 + u_4x_4 = 0. \tag{1.2}$$

We are interested in solutions to (1.2) with $x_1, x_2, x_3, x_4 \in \mathbb{Z}$.

Suppose $(x_1, x_2, x_3, x_4) = (a_1, a_2, a_3, a_4)$ is an integer solution to (1.2). Let $d \leq 4$ be the number of distinct integers in the set $\{a_1, a_2, a_3, a_4\}$. Then we have a partition on the indices

$$\{1, 2, 3, 4\} = T_1 \cup \cdots \cup T_d,$$

where i and j lie in the same part T_ν if and only if $x_i = x_j$. We call (a_1, a_2, a_3, a_4) a *trivial* solution to (1.2) if

$$\sum_{i \in T_\nu} u_i = 0, \qquad \nu = 1, \ldots, d.$$

Otherwise, we will call (a_1, a_2, a_3, a_4) a *nontrivial* solution to (1.2).

In [53], Lazebnik and Verstraëte introduced k-fold Sidon sets which are defined as follows. Let k be a positive integer. A set $A \subset \mathbb{N}$ is a *k-fold Sidon set* if each

equation of the form

$$u_1x_1 + u_2x_2 + u_3x_3 + u_4x_4 = 0, \tag{1.3}$$

where $|u_i| \leq k$ and $u_1 + \cdots + u_4 = 0$, has no nontrivial solutions with $x_1, x_2, x_3, x_4 \in A$. Let $r(k, N)$ be the size of the largest k-fold Sidon set $A \subset \{1, \ldots, N\}$.

Lemma 1.13. *There is an infinite sequence* $1 = a_1 < a_2 < \cdots$ *of integers such that*

$$a_m \leq 2^8 k^4 m^3,$$

and the system of equations (1.3) has no nontrivial solutions in the set $A = \{a_1, a_2, \ldots\}$. *In particular, for integers* $N > k^4 \geq 1$, *we have* $r(k, N) \geq ck^{-4/3}N^{1/3}$, *where* c *is a positive constant.*

The proof of Lemma 1.13 is a slight modification of the proof of Theorem 2.1 in [74]. For the sake of completeness, we include the proof here.

Proof. We put $a_1 = 1$ and define a_m recursively. Given $a_1, \ldots, a_{m-1}$, let a_m be the smallest positive integer satisfying

$$a_m \neq -\Big(\sum_{i \in S} u_i\Big)^{-1} \sum_{1 \leq i \leq 4, i \notin S} u_i x_i, \tag{1.4}$$

for every choice u_i such that $|u_i| \leq k$, for every set $S \subset \{1, \ldots, 4\}$ of subscripts such that $\Big(\sum_{i \in S} u_i\Big) \neq 0$, and for every choice of $x_i \in \{a_1, \ldots, a_{m-1}\}$, where $i \notin S$. For

a fixed S with $|S| = j$, this excludes $(m-1)^{4-j}$ numbers. Since $|u_i| \leq k$, the total number of excluded integers is at most

$$(2k+1)^4 \sum_{j=1}^{3} \binom{4}{j} (m-1)^{4-j} = (2k+1)^4 (m^4 - (m-1)^4 - 1) < 2^8 k^4 m^3.$$

Consequently, we can extend our set by an integer $a_m \leq 2^8 k^4 m^3$. This will automatically be different from from $a_1, \ldots, a_{m-1}$, since putting $x_i = a_j$ for all $i \notin S$ in (1.4) we get $a_m \neq a_j$. It will also satisfy $a_m > a_{m-1}$ by minimal choice of a_{m-1}.

We show that the system of equations (1.3) has no nontrivial solutions in the set $\{a_1, \ldots, a_m\}$. We use induction on m. The statement is obviously true for $m = 1$. We establish it for m assuming for $m-1$. Suppose that there is a nontrivial solution (x_1, x_2, x_3, x_4) to (1.3) for some u_1, u_2, u_3, u_4 with the properties described above. Let S denote the set of those subscripts for which $x_i = a_m$. If $\sum_{i \in S} u_i \neq 0$, then this contradicts (1.4). If $\sum_{i \in S} u_i = 0$, then by replacing each occurrence of a_m by a_1, we get another nontrivial solution, which contradicts the induction hypothesis. □

For more problems and results on Sidon sets and k-fold Sidon sets, we refer the interested reader to [53, 74, 16].

We are now ready to prove Theorem 1.5.

Proof of Theorem 1.5. We start by applying Lemma 1.12 to obtain a Sidon set $M \subset [n^{1/7}]$, such that $|M| = \Theta(n^{1/14})$. We then apply Lemma 1.13 with $k = n^{1/7}$ and

$N = \frac{1}{4}n^{11/14}$, to obtain a k-fold Sidon set $A \subset [N]$ such that

$$|A| \geq cn^{1/14},$$

where c is defined in Lemma 1.13. Without loss of generality, let us assume $|A| = cn^{1/14}$.

Let $P = \{(i,j) \in \mathbb{Z}^2 : i \in A, 1 \leq j \leq n^{13/14}\}$, and let $\mathcal{L}$ be the family of lines in the plane of the form $y = mx + b$, where $m \in M$ and b is an integer such that $1 \leq b \leq n^{13/14}/2$.

Hence, we have

$$|P| = |A| \cdot n^{13/14} = \Theta(n),$$
$$|\mathcal{L}| = |M| \cdot \frac{n^{13/14}}{2} = \Theta(n).$$

Notice that each line in $\mathcal{L}$ has exactly $|A| = cn^{1/14}$ points from P since $1 \leq b \leq n^{13/14}/2$. Therefore,

$$|I(P, \mathcal{L})| = |\mathcal{L}||A| = \Theta(n^{1+1/14}).$$

Claim. *There are no four distinct lines $\ell_1, \ell_2, \ell_3, \ell_4 \in \mathcal{L}$ and four distinct points $p_1, p_2, p_3, p_4 \in P$ such that $\ell_1 \cap \ell_2 = p_1, \ell_2 \cap \ell_3 = p_2, \ell_3 \cap \ell_4 = p_3, \ell_4 \cap \ell_1 = p_4$.*

Proof. For the sake of contradiction, suppose there are four lines $\ell_1, \ell_2, \ell_3, \ell_4$ and four points p_1, p_2, p_3, p_4 with the properties described above. Let $\ell_i = m_i x + b_i$ and let

$p_i = (x_i, y_i)$. Therefore,

$$\ell_1 \cap \ell_2 = p_1 = (x_1, y_1),$$

$$\ell_2 \cap \ell_3 = p_2 = (x_2, y_2),$$

$$\ell_3 \cap \ell_4 = p_3 = (x_3, y_3),$$

$$\ell_4 \cap \ell_1 = p_4 = (x_4, y_4).$$

Hence,

$$p_1 \in \ell_1, \ell_2 \implies (m_1 - m_2)x_1 + b_1 - b_2 = 0,$$

$$p_2 \in \ell_2, \ell_3 \implies (m_2 - m_3)x_2 + b_2 - b_3 = 0,$$

$$p_3 \in \ell_3, \ell_4 \implies (m_3 - m_4)x_3 + b_3 - b_4 = 0,$$

$$p_4 \in \ell_4, \ell_1 \implies (m_4 - m_1)x_4 + b_4 - b_1 = 0.$$

By summing up the four equations above, we get

$$(m_1 - m_2)x_1 + (m_2 - m_3)x_2 + (m_3 - m_4)x_3 + (m_4 - m_1)x_4 = 0.$$

By setting $u_1 = m_1 - m_2, u_2 = m_2 - m_3, u_3 = m_3 - m_4, u_4 = m_4 - m_1$, we get

$$u_1x_1 + u_1x_2 + u_3x_3 + u_4x_4 = 0, \tag{1.5}$$

where $u_1 + u_2 + u_3 + u_4 = 0$ and $|u_i| \leq n^{1/7}$. Since $x_1, \ldots, x_4 \in A$, (x_1, x_2, x_3, x_4) must be a trivial solution to (1.5). The proof now falls into the following cases, and let us note that no line in $\mathcal{L}$ is vertical.

Case 1. Suppose $x_1 = x_2 = x_3 = x_4$. Then ℓ_i is vertical and we have a contradiction.

Case 2. Suppose $x_1 = x_2 = x_3 \neq x_4$ and $u_1 + u_2 + u_3 = 0$ and $u_4 = 0$. Then ℓ_1 and ℓ_4 have the same slope which is a contradiction. The same argument follows if $x_1 = x_2 = x_4 \neq x_3$, $x_1 = x_3 = x_4 \neq x_2$, or $x_2 = x_3 = x_4 \neq x_1$.

Case 3. Suppose $x_1 = x_2 \neq x_3 = x_4$, $u_1 + u_2 = 0$, and $u_3 + u_4 = 0$. Since $p_1, p_2 \in \ell_2$ and $x_1 = x_2$, this implies that ℓ_2 is vertical which is a contradiction. A similar argument follows if $x_1 = x_4 \neq x_2 = x_3$, $u_1 + u_4 = 0$, and $u_2 + u_3 = 0$.

Case 4. Suppose $x_1 = x_3 \neq x_2 = x_4$, $u_1 + u_3 = 0$, and $u_2 + u_4 = 0$. Then $u_1 + u_3 = 0$ implies that $m_1 + m_3 = m_2 + m_4$. Since M is a Sidon set, we have either $m_1 = m_2$ and $m_3 = m_4$ or $m_1 = m_4$ and $m_2 = m_3$. The first case implies that ℓ_1 and ℓ_2 are parallel

which is a contradiction, and the second case implies that ℓ_2 and ℓ_3 are parallel, which is again a contradiction. □

This completes the proof of Theorem 1.5. □

1.5 Concluding Remarks

- An old result of Erdős states that every n-vertex graph that does not contain a cycle of length $2k$, has $O_k(n^{1+1/k})$ edges. It is known that this bound is tight when $k = 2, 3$, and 5, but it is a long standing open problem in extremal graph theory to decide whether or not this upper bound can be improved for other values of k. Hence, Erdős's upper bound of $O(n^{5/4})$ when $k = 4$ implies Theorem 1.3 when $t = 2$ and $m = n$. It would be interesting to see if one can improve the upper bound in Theorem 1.3 when $t = 2$. For more problems on cycles in graphs, see [91].

- The proof of Lemma 1.9 is similar to the proof of the main result in [1]. The main difference is that we use the result of Fox et al. [29] instead of the Ham-Sandwich Theorem. We also note that a similar result was established by Dujmović and Langerman (see Theorem 6 in [23]).

Chapter 1 is a version of the material appearing in "*On Grids in Point-Line Arrangements in the Plane*," *In 35th International Symposium on Computational Geometry* (SoCG 2019) (Vol. 129, p. 50), co-authored with Andrew Suk. The author

was one of the primary investigators and authors of this paper.

Chapter 2

Constructions of point-line arrangements in the plane with large girth

2.1 Introduction

Let $k \geq 2$ be a fixed integer and let C_{2k} denote a cycle of length $2k$. If a graph contains cycles, then the length of the shortest cycle is called the *girth* of the graph and is denoted by g. A graph is C_{2k}-free if it contains no subgraph isomorphic to C_{2k}. The *Turán number* (n, C_{2k}) denotes the maximum number of edges in a C_{2k}-free graph on n vertices. An unpublished result of Erdős, which was also proved by Bondy and

Simonovits in [6], shows that

$$(n, C_{2k}) = O\left(n^{1+1/k}\right).$$

In the other direction, one can use the probabilistic method to show that

$$(n, C_{2k}) \geq (n, \{C_3, C_4, \ldots, C_{2k+1}\}) \geq \Omega(n^{1+1/2k}).$$

For $k \in \{2, 3, 5\}$, it is known that $(n, C_{2k}) = \Theta\left(n^{1+1/k}\right)$(see [12, 24] for $k = 2$ and [4, 50, 95] for $k \in \{3, 5\}$). It is a long standing open problem to determine the order of magnitude of (n, C_{2k}) for $k \notin \{2, 3, 5\}$. Erdős and Simonovits [25] conjectured that $(n, C_{2k}) = \Theta\left(n^{1+1/k}\right)$ for all $k \geq 2$. For $k = 4$, the current best lower bound is due to Benson [4] and Singleton [86], who showed $(n, C_8) \geq \Omega(n^{6/5})$. For large k, the densest known C_{2k}-free graphs on n vertices are the constructions of Ramanujan graphs due to Margulis [57] Lubotzky, Phillips, and Sarnak [54], Lazebnik, Ustimenko and Woldar [52], and Dahan and Tillich [21]. The constructions provide $n^{1+\delta}$ edges where $\delta \sim \frac{6}{7k}$ as $k \to \infty$.

In this thesis, we study the analogous problem for the point-line incidences in the plane. Given a finite set P of points in the plane and a finite set $\mathcal{L}$ of lines in the plane, let $I(P, \mathcal{L}) = \{(p, \ell) \in P \times \mathcal{L} : p \in \ell\}$ be the set of incidences between P and $\mathcal{L}$. The *incidence graph* of $(P, \mathcal{L})$ is the bipartite graph $G = (P \cup \mathcal{L}, I)$, with vertex parts P and $\mathcal{L}$, and $E(G) = I(P, \mathcal{L})$. If $|P| = m$ and $|\mathcal{L}| = n$, then the celebrated theorem

of Szemerédi and Trotter [89] states that

$$|I(P, \mathcal{L})| = O\left(m^{2/3}n^{2/3} + m + n\right). \tag{2.1}$$

Moreover, this bound is tight which can be seen by taking the $\sqrt{m} \times \sqrt{m}$ integer lattice and bundles of parallel "rich" lines (see [64]). Thus, the number of incidences between any arrangement of n points and n lines is at most $O(n^{4/3})$, which is significantly better than $ex(n, C_4) = \Theta(n^{3/2})$. Therefore, we make the following conjecture.

Conjecture 2.1. *Let $k \geq 3$ be an integer. Let P be a set of n points in the plane, let $\mathcal{L}$ be a set of n lines in the plane, and $I = I(P, \mathcal{L})$. If the incidence graph $G = (P \cup \mathcal{L}, I)$ is C_{2k}-free, then $|I(P, L)| = o(n^{1+1/k})$.*

Solymosi proved Conjecture 2.1 for $k = 3$, but it is still an open problem for $k \geq 4$.

In this thesis, we apply a simple technique of realizing point-line incidence graphs arising from finite geometries as point-line incidence graphs in the Euclidean plane. As expected, we obtain some loss on the number of edges. Our first result is stated below, which is obtained by applying this technique to a well-known construction of Lazebnik and Ustimenko [51] of a large graph with large girth.

Theorem 2.2. *Let $k \geq 3$ be an odd integer. For $n > 1$, there exists an arrangement of n points P and n lines $\mathcal{L}$ in the plane such that their incidence graph $G = (\mathcal{P} \cup \mathcal{L}, I)$ has girth $g \geq k + 5$ and determines at least $\Omega(n^{1+\frac{4}{k^2+6k-3}})$ incidences.*

For $k = 5$, we obtain a slightly better bound by applying this technique to

Wenger graphs.

Theorem 2.3. *There exists an arrangement of n points $\mathcal{P}$ and n lines $\mathcal{L}$ in the plane such that their incidence graph $G = (\mathcal{P} \cup \mathcal{L}, I)$ is C_{10}-free and determines at least $\Omega(n^{1+1/15})$ incidences.*

We systemically omit floor and ceiling signs whenever they are not crucial for the sake of clarity of our presentation.

2.2 Proof of Theorem 2.2

In [51], Lazebnik and Ustimenko gave the following construction of a q-regular bipartite graph $D(q,k) = (U \cup V, E)$ on $2q^k$ vertices with girth $g \geq k+5$, where q is a prime power and $k \geq 3$ is an odd integer. The vertex set of $D(q,k)$ is $U \cup V$, where $U = V = \{0, 1, \ldots, q-1\}^k$. In order to define $E \subset U \times V$, we will label the coordinates of $u \in U$ and $v \in V$ as follows.

$$u = \left(u_1, u_{1,1}, u_{1,2}, u_{2,1}, u_{2,2}, u'_{2,2}, u_{2,3}, u_{3,2}, u_{3,3} \ldots, u'_{i,i}, u_{i,i+1}, u_{i+1,i}, u_{i+1,i+1}, \ldots\right).$$

and

$$v = \left(v_1, v_{1,1}, v_{1,2}, v_{2,1}, v_{2,2}, v'_{2,2}, v_{2,3}, v_{3,2}, v_{3,3}, \ldots, v'_{i,i}, v_{i,i+1}, v_{i+1,i}, v_{i+1,i+1}, \ldots\right),$$

Note that we only consider the first k such coordinates. For example when $k = 5$, we

have $u = (u_1, u_{1,1}, u_{1,2}, u_{2,1}, u_{2,2})$, $v = (v_1, v_{1,1}, v_{1,2}, v_{2,1}, v_{2,2})$. Then $uv \in E$ if and only if the following $k-1$ equations are satisfied:

$$
\begin{aligned}
v_{1,1} - u_{1,1} &= v_1 u_1 && \bmod q \\
v_{1,2} - u_{1,2} &= v_{1,1} u_1 && \bmod q \\
v_{2,1} - u_{2,1} &= v_1 u_{1,1} && \bmod q \\
& \left.\begin{aligned}
v_{i,i} - u_{i,i} &= v_1 u_{i-1,i} && \bmod q \\
v'_{i,i} - u'_{i,i} &= u_1 v_{i,i-1} && \bmod q \\
v_{i,i+1} - u_{i,i+1} &= u_1 v_{i,i} && \bmod q \\
v_{i+1,i} - u_{i+1,i} &= v_1 u'_{i,i} && \bmod q
\end{aligned}\right\} && i \geq 2.
\end{aligned}
$$

where $u'_{1,1} = u_{1,1}, v'_{1,1} = v_{1,1}$.

For example, if $k = 5$, $uv \in E$ if and only if the following 4 equations are satisfied.

$$
\begin{aligned}
v_{1,1} - u_{1,1} &= v_1 u_1 && \bmod q \\
v_{1,2} - u_{1,2} &= v_{1,1} u_1 && \bmod q \\
v_{2,1} - u_{2,1} &= v_1 u_{1,1} && \bmod q \\
v_{2,2} - u_{2,2} &= v_1 u_{1,2} && \bmod q.
\end{aligned}
$$

In [51], Lazebnik and Ustimenko proved the following.

Theorem 2.4 (Theorem 3.3 in [51]). *For an odd integer $k \geq 3$, the bipartite graph*

$D(k,q)$ described above has girth $g \geq k+5$.

We will use this construction to prove Theorem 2.2.

Proof of Theorem 2.2. Let $k \geq 3$, and $n > 1$ be sufficiently large such that $\lfloor n^{\frac{4}{k^2+6k-3}} \rfloor \geq 1$. By Bertrand's postulate theorem, there is a prime number q such that $4n^{\frac{8}{k}} < q < 8n^{\frac{8}{k}}$. Then let $D(q,k) = (U \cup V, E)$ be defined as above. Let $U' \subset U$ and $V' \subset V$ such that $u \in U'$ if

$$\begin{aligned} &0 \leq u_1 \leq n^{\frac{4}{k^2+6k-3}}, \\ &0 \leq u_{i,j} \leq n^{\frac{4(i+j)}{k^2+6k-3}} \qquad i,j \geq 1, \\ &0 \leq u'_{i,j} \leq n^{\frac{4(i+j)}{k^2+6k-3}} \qquad i,j \geq 1. \end{aligned}$$

and $v \in V'$ if

$$\begin{aligned} &0 \leq v_1 \leq 2n^{\frac{4}{k^2+6k-3}}, \\ &0 \leq v_{i,i+1} \leq 4n^{\frac{4(2i+1)}{k^2+6k-3}}, \\ &0 \leq v_{i+1,i} \leq 3n^{\frac{4(2i+1)}{k^2+6k-3}}, \qquad i \geq 1, \\ &0 \leq v'_{i,i} \leq 4n^{\frac{4(2i)}{k^2+6k-3}}, \\ &0 \leq v_{i,i} \leq 3n^{\frac{4(2i)}{k^2+6k-3}}. \end{aligned}$$

Then let $E' \subset U' \times V'$ such that $uv \in E'$ if and only if the following $k-1$ equations are satisfied

$$
\left.
\begin{aligned}
v_{1,1} - u_{1,1} &= v_1 u_1 \\
v_{1,2} - u_{1,2} &= v_{1,1} u_1 \\
v_{2,1} - u_{2,1} &= v_1 u_{1,1} \\
v_{i,i} - u_{i,i} &= v_1 u_{i-1,i} \\
v'_{i,i} - u'_{i,i} &= u_1 v_{i,i-1} \\
v_{i,i+1} - u_{i,i+1} &= u_1 v_{i,i} \\
v_{i+1,i} - u_{i+1,i} &= v_1 u'_{i,i}
\end{aligned}
\right\} \quad i \geq 2. \tag{2.1}
$$

The bipartite graph $G = (U' \cup V', E')$ is a subgraph of $D(q,k)$, and therefore, it has girth $g \geq k+5$. It suffices to show that $|E'| = \Omega(n^{1+\frac{4}{k^2+6k-3}})$ and to realize G as an incidence graph of points and lines in the plane.

Set $P = U' \subset \mathbb{Z}^k$. Then we have

$$
\begin{aligned}
|P| &= n^{\frac{4}{k^2+6k-3}} \cdot n^{\frac{4(2)}{k^2+6k-3}} \cdot \left(\prod_{i=3}^{\frac{k-3}{2}-1} n^{\frac{4i}{k^2+6k-3}} \right) \cdot n^{\frac{4(\frac{k-3}{2})}{k^2+6k-3}} \\
&= n^{\frac{4}{k^2+6k-3}\left(1+2+2(3)+\ldots+2\left(\frac{k+3}{2}-1\right)+\frac{k+3}{2}\right)} \\
&= n.
\end{aligned}
$$

We define a set of $|V'|$ lines $\mathcal{L}$ in $\mathbb{R}^k$ as follows. For each $v \in V'$, let ℓ_v be the solution space to the following system of $k-1$ equations over k variables.

$$
\begin{aligned}
v_{1,1} - x_{1,1} &= v_1 x_1 \\
v_{1,2} - x_{1,2} &= v_{1,1} x_1 \\
v_{2,1} - x_{2,1} &= v_1 x_{1,1} \\
&\left.\begin{aligned}
v_{i,i} - x_{i,i} &= v_1 x_{i-1,i} \\
v'_{i,i} - x'_{i,i} &= x_1 v_{i,i-1} \\
v_{i,i+1} - x_{i,i+1} &= x_1 v_{i,i} \\
v_{i+1,i} - x_{i+1,i} &= v_1 x'_{i,i}
\end{aligned}\right\} \quad i \geq 2.
\end{aligned} \tag{2.2}
$$

Set $\mathcal{L} = \{\ell_v : v \in V'\}$. It is easy to see that the $k-1$ equations above are independent and therefore, ℓ_v is a line in $\mathbb{R}^k$. Moreover, each line is unique by the following claim.

Claim. *If $v, w \in V'$ are distinct, then $\ell_v \neq \ell_w$.*

Proof. Let v and w be two distinct members of V', where

$$v = (v_1, v_{1,1}, v_{1,2}, v_{2,1}, v_{2,2}, v'_{2,2}, v_{2,3}, v_{3,2}, v_{3,3}, \ldots, v'_{i,i}, v_{i,i+1}, v_{i+1,i}, v_{i+1,i+1}, \ldots),$$

$$w = (w_1, w_{1,1}, w_{1,2}, w_{2,1}, w_{2,2}, w'_{2,2}, w_{2,3}, w_{3,2}, \ldots, w'_{i,i}, w_{i,i+1}, w_{i+1,i}, w_{i+1,i+1}, \ldots).$$

Without loss of generality, we can assume $u_1 \neq w_1$, as otherwise, we can show inductively that both vectors u and v have the same coordinates. For any point $u \in P$,

$$u = (u_1, u_{1,1}, u_{1,2}, u_{2,1}, u_{2,2}, u'_{2,2}, u_{2,3}, u_{3,2}, u_{3,3}, \ldots, u'_{i,i}, u_{i,i+1}, u_{i+1,i}, u_{i+1,i+1}, \ldots),$$

there is a unique solution to the following system of k equations.

$$\left.\begin{aligned} v_{i,i} - u_{i,i} &= v_1 u_{i-1,i} \\ v'_{i,i} - u'_{i,i} &= u_1 v_{i,i-1} \\ v_{i,i+1} - u_{i,i+1} &= u_1 v_{i,i} \\ v_{i+1,i} - u_{i+1,i} &= v_1 u'_{i,i} \end{aligned}\right\} \quad i \geq 2.$$

$$\begin{aligned} w_{1,1} - u_{1,1} &= w_1 u_1 \\ v_{1,1} - u_{1,1} &= v_1 u_1 \\ v_{1,2} - u_{1,2} &= v_{1,1} u_1 \end{aligned}$$

Hence, both v and w correspond to distinct lines. □

Therefore, we have

$$\begin{aligned} |\mathcal{L}| &= \Theta\left(n^{\frac{4}{k^2+6k-3}} \cdot n^{\frac{4(2)}{k^2+6k-3}} \cdot \left(\prod_{i=3}^{\frac{k-3}{2}-1} n^{\frac{4i}{k^2+6k-3}} \right) \cdot n^{\frac{4(\frac{k-3}{2})}{k^2+6k-3}} \right) \\ &= \Theta\left(n^{\frac{4}{k^2+6k-3}\left(1+2+2(3)+\ldots+2\left(\frac{k+3}{2}-1\right)+\frac{k+3}{2}\right)} \right) \\ &= \Theta(n). \end{aligned}$$

Notice that every point $u \in P$ is incident to at least $2n^{\frac{4}{k^2+6k-3}}$ lines in $\mathcal{L}$. Indeed, consider the $k-1$ equations (2.2). There are $2n^{\frac{4}{k^2+6k-3}}$ choices for v_1. For fixed $u \in U$, by fixing v_1 and by equation (2.1), we obtain $v_{1,1}$ sch that $0 \leq v_{1,1} = v_1 u_1 + u_{1,1} \leq 3n^{\frac{8}{k^2+6k-3}}$. By repeating the same argument the rest of the coordinates of v will be determined uniquely.

Hence, we have a set of $\Theta(n)$ points P and $\Theta(n)$ lines in $\mathbb{R}^k$ such that $|I(P,k)| = \Omega(n^{1+\frac{4}{k^2+6k-3}})$. Projecting points P and lines $\mathcal{L}$ into the plane completes the proof of Theorem 2.2. □

2.3 Proof of Theorem 2.3

Let $k \in \{2,3,5\}$. In [95], Wenger gave the following construction of a C_{2k}-free and p-regular bipartite graph $H_k(p) = (U \cup V, E)$ on $2p^k$ vertices, where p is a prime power. First we briefly discuss the Wenger's construction. The vertex set of $H_k(p)$ is $U \cup V$, where $U = V = \{0, \ldots, p-1\}^k$. In order to define $E \subset U \times V$, we will label the coordinates of $u \in U$ and $v \in V$ as follows.

$$u = (u_0, u_1, \ldots, u_{k-1}) \qquad \text{and} \qquad v = (v_0, v_1, \ldots, v_{k-1}).$$

Then $uv \in E$ if and only if the following $k-1$ equations are satisfied:

$$v_j = u_j + u_{j+1}v_{k-1} \mod p \qquad j = 0, \ldots, k-2.$$

In [95], Wenger proved the following.

Theorem 2.5. *For $k \in \{2,3,5\}$, the bipartite graph $H_k(p)$ described above is C_{2k}-free.*

We will use this construction to prove Theorem 2.3.

Proof of Theorem 2.3. Let $k \geq \{2,3,5\}$ and $n > 1$ be sufficiently large such that $\lfloor n^{\frac{2}{k^2+2k}} \rfloor \geq 1$. By Bertrand's postulate theorem, there is a prime number p such that

$2^{2k}n^{\frac{2}{k}} < p < 2^{2k+1}n^{\frac{2}{k}}$. Then let $H_k(p) = (U \cup V, E)$ be defined as above. Let $U' \subset U$ and $V' \subset V$ such that $u \in U'$ if

$$\begin{aligned} 0 \leq u_i &\leq 2^{2(k-i-1)}n^{\frac{2(k-i)}{k(k+1)}} && 0 \leq i \leq k-2, \\ 0 \leq u_i &\leq n^{\frac{2}{k(k+1)}} && i = k-1, \end{aligned}$$

and $v \in V'$ if

$$\begin{aligned} 2^{2(k-i-1)-1}n^{\frac{2(k-i)}{k(k+1)}} \leq v_i &\leq 2^{2(k-i-1)}n^{\frac{2(k-i)}{k(k+1)}} && 0 \leq i \leq k-2, \\ n^{\frac{2}{k(k+1)}} \leq v_i &\leq 2n^{\frac{2}{k(k+1)}} && i = k-1. \end{aligned}$$

Let $E' \subset U' \times V'$ such that $uv \in E'$ if and only if the following $k-1$ equations are satisfied:

$$v_j = u_j + u_{j+1}v_{k-1} \qquad j = 0, \ldots, k-2. \tag{2.2}$$

The bipartite graph $G = (U' \cup V', E')$ is a subgraph of $H_k(p)$, and therefore, it is C_{2k}-free. It suffices to show that $|E'| \geq \Omega(n^{1+\frac{2}{k^2+k}})$ and to realize G as the incidence graph of points and lines in the plane.

Let $P = U' \subset \mathbb{Z}^k$. Then we have

$$|P| = \prod_{i=0}^{k-1} 2^{2(k-i-1)} n^{\frac{2(k-i)}{k(k+1)}} = 2^{k(k-1)} n = \Theta_k(n).$$

We define a set of $|V'|$ lines $\mathcal{L}$ in $\mathbb{R}^k$ as follows. For each $v \in V'$, let ℓ_v be the solution space to the following system of $k-1$ equations over k variables.

$$x_i + v_{k-1} x_{i+1} - v_i = 0 \qquad\qquad j = 0, \ldots, k-2. \tag{2.3}$$

Set $\mathcal{L} = \{\ell_v : v \in V'\}$. It is easy to see that the $k-1$ equations above are independent and therefore, ℓ_v is a line in $\mathbb{R}^k$. Moreover, we have the following claim.

Claim. *If $v, w \in V'$ are distinct, then $\ell_v \neq \ell_w$.*

Proof. Let v and w be two distinct members of V', where

$$v = (v_1, \ldots, v_{k-1}) \quad \text{and} \quad w = (w_1, \ldots, w_{k-1}).$$

Without loss of generality, we can assume $u_1 \neq w_1$, as otherwise, we can show inductively that both vectors u and v have the same coordinates. For any point $u =$

$(u_1, u_2, \ldots, u_{k-1}) \in P$, there is a unique solution to the following system of k equations.

$$\begin{aligned} x_1 + w_{k-1}x_2 - w_1 &= 0 \\ x_i + v_{k-1}x_{i+1} - v_1 &= 0 \qquad\qquad 0 \le i \le k-2. \end{aligned}$$

Hence, both v and w correspond to distinct lines. □

Therefore, we have

$$|\mathcal{L}| = \frac{1}{2^{k-1}} \prod_{i=0}^{k-1} 2^{2(k-i-1)} n^{\frac{2(k-i)}{k(k+1)}} = 2^{k^2-1} n = \Theta_k(n).$$

Notice that every line $\ell_v \in \mathcal{L}$ is incident to at least $n^{\frac{2}{k^2+k}}$ points in P. Indeed, consider $k-1$ equations 2.3. There are $n^{\frac{2}{k^2+k}}$ choices for u_{k-1}. For fixed $v \in V'$, by fixing u_{k-1} and by equation 2.2, we obtain $u_{k-2} = v_{k-2} - u_{k-1}v_{k-1}$, such that

$$0 \le u_{k-2} \le 2^2 n^{\frac{4}{k(k+1)}},$$

since

$$2n^{\frac{4}{k(k+1)}} \le v_{k-2} \le 2^2 n^{\frac{4}{k(k+1)}} \qquad \text{and} \qquad -2n^{\frac{4}{k(k+1)}} \le -u_{k-1}v_{k-1} \le 0.$$

By repeating the same argument the other coordinates of u will be determined uniquely.

Thus we have a set of $\Theta(n)$ points P and $\Theta(n)$ lines in $\mathbb{R}^k$ such that $|I(P,k)| = \Omega(n^{1+\frac{2}{k^2+k}})$. Projecting points P and lines $\mathcal{L}$ into the plane completes the proof of Theorem. □

2.4 Concluding Remarks

As a corollary of Theorem 2.2 for $k = 3$, we get that there exists an arrangement of n points and n lines in the plane with no C_6 in the incidence graph while determining $\Omega(n^{1+\frac{1}{6}})$ incidences. It is worth mentioning that one can follow the construction of Theorem 1.5 in [60] to get a construction of an arrangement of n points and n lines in the plane where their incidence graph is C_6-free while it determines $\Omega(n^{1+\frac{1}{7}})$ incidences.

Chapter 2 is a version of the material in "*Constructions of Point-Line Arrangements in the Plane with Large Girth*", co-authored with Andrew Suk and Jacques Verstraëte, which has been submitted for publication. The author was one of the primary investigators and authors of this paper.

Chapter 3

A positive fraction mutually avoiding sets theorem

3.1 Introduction

Let P be an n-element point set in the plane in general position, that is, no three members are collinear. For $k > 0$, we say that P contains a *crossing family* of size k if there are k segments whose endpoints are in P that are pairwise crossing. Crossing families were introduced in 1994 by Aronov, Erdős, Goddard, Kleitman, Kluggerman, Pach, and Schulman [1], who showed that for any given set of n points in the plane in general position, there exists a crossing family of size at least $\sqrt{n/12}$. They raised the following problem (see also Chapter 9 in [11]).

Problem 3.1 ([1])**.** *Does there exist a constant $c > 0$ such that every set of n points*

in the plane in general position contains a crossing family of size at least cn?

There have been several results on crossing families over the past several decades [32, 66, 76]. Very recently, Pach, Rudin, and Tardos showed that any set of n points in general position in the plane determines $n^{1-o(1)}$ pairwise crossing segments. More precisely, they proved the following theorem.

Theorem 3.2 ([65]). *Any set P of n points in general position in the plane determines at least $n/2^{O(\sqrt{\log n})}$ pairwise crossing segments.*

The result of Aronov et al. on crossing families was actually obtained by finding point sets that are *mutually avoiding*. Let A and B be two disjoint point sets in the plane. We say that A *avoids* B if no line subtended by a pair of points in A intersects the convex hull of B. The sets A and B are *mutually avoiding* if A avoids B and B avoids A. In other words, A and B are mutually avoiding if and only if each point in A "sees" every point in B in the same clockwise order, and vice versa. Hence two mutually avoiding sets A and B, where $|A| = |B| = k$, would yield a crossing family of size k. In Figure 1, two mutually avoiding sets $A = \{a_1, a_2, a_3, a_4\}$ and $B = \{b_1, b_2, b_3, b_4\}$ yield a crossing family of size four.

Theorem 3.3 ([1]). *Any set of n points in the plane in general position contains a pair of mutually avoiding sets, each of size at least $\sqrt{n/12}$.*

It was shown by Valtr [90] that this bound is best possible up to a constant factor. In this note, we give a fractional version of Theorem 3.3.

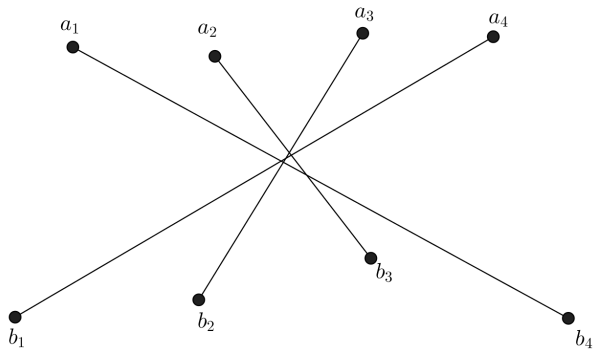

Figure 3.1: Two mutually avoiding sets A and B.

Theorem 3.4. *For every $k > 0$ there is a constant $\varepsilon_k > 0$ such that every sufficiently large point set P in the plane in general position contains $2k$ disjoint subsets $A_1, \ldots, A_k, B_1, \ldots, B_k$, each of size at least $\varepsilon_k|P|$, such that every pair of sets $A = \{a_1, \ldots, a_k\}$ and $B = \{b_1, \ldots, b_k\}$, with $a_i \in A_i$ and $b_i \in B_i$, are mutually avoiding. Moreover, $\varepsilon_k = \Omega(1/k^4)$.*

As an immediate corollary, we establish the following fractional version of the crossing families theorem.

Theorem 3.5. *For every $k > 0$ there is a constant $\varepsilon_k > 0$ such that every sufficiently large point set P in the plane in general position contains $2k$ subsets $A_1, \ldots, A_k$, $B_1, \ldots, B_k$, each of size at least $\varepsilon_k|P|$, such that every segment that joins a point from A_i and B_{k+1-i} crosses every segment that joins a point from A_{k+1-i} and B_i, for $1 \leq i \leq k$. Moreover, $\varepsilon_k = \Omega(1/k^4)$.*

Let us remark that if we are not interested in optimizing ε_k in the theorems above, one can combine the well-known same-type lemma due to Barany and Valtr [2]

(see section 3.8) with Theorem 3.3 to establish Theorems 3.4 and 3.5 with $\varepsilon_k = 2^{-O(k^4)}$. Hence, the main advantage in the theorems above is that ε_k decays only polynomially in k. We will however, use this approach in higher dimensions with a more refined same-type lemma.

Higher dimensions. Mutually avoiding sets in $\mathcal{R}^d$ are defined similarly. A point set P in $\mathcal{R}^d$ is in *general position* if no $d+1$ members of P lie on a common hyperplane. Given two point sets A and B in $\mathcal{R}^d$, we say that A *avoids* B if no hyperplane generated by a d-tuple in A intersects the convex hull of B. The sets A and B are *mutually avoiding* if A avoids B and B avoids A. Aronov et al. proved the following.

Theorem 3.6 ([1])**.** *For fixed $d \geq 3$, any set of n points in $\mathcal{R}^d$ in general position contains a pair of mutually avoiding subsets each of size $\Omega_d(n^{1/(d^2-d+1)})$.*

In the other direction, Valtr showed in [90] that by taking a $k \times \cdots \times k$ grid, where $k = \lfloor n^{1/d} \rfloor$, and slightly perturbing the n points so that the resulting set is in general position, one obtains a point set that does not contain mutually avoiding sets of size $cn^{1-1/d}$, where $c = c(d)$.

Our next result is a fractional version of Theorem 3.6.

Theorem 3.7. *For $d \geq 3$ and $k \geq 2$, there is a constant $\varepsilon_{d,k}$, such that every sufficiently large point set P in $\mathcal{R}^d$ in general position contains $2k$ subsets $A_1, \ldots, A_k, B_1, \ldots, B_k$, each of size at least $\varepsilon_k|P|$, such that every pair of sets $A = \{a_1, \ldots, a_k\}$ and $B = \{b_1, \ldots, b_k\}$, with $a_i \in A_i$ and $b_i \in B_i$, are mutually avoiding. Moreover, $\varepsilon_{d,k} = 1/k^{c_d}$ where $c_d > 0$ depends only on d.*

Similar to Theorem 3.4, $\varepsilon_{d,k}$ in Theorem 3.7 also decays only polynomially in k for fixed $d \geq 3$. However, c_d does have a rather bad dependency on d, $c_d \approx 2^{O(d)}$.

Finally, we establish a result on crossing families in higher dimensions which was also observed by Aronov et al. in [1].

3.2 Proof of Theorem 3.4

Proof. In this section we give the proof of Theorem 3.4 which closely follows an argument of Pór and Valtr in [69]. Let $k > 2$ and let P be a set of n points in the plane in general position where $n > (1500k)^4$. It follows from Theorem 1.2 that among any $12(40k+1)^2$ points P, it is always possible to find two mutually avoiding sets $A \subseteq P$ and $B \subseteq P$ each of size at least $40k+1$. It follows that P contains at least

$$\frac{\binom{n}{12(40k+1)^2}}{\binom{n-(80k+2)}{12(40k+1)^2-(80k+2)}} = \frac{\binom{n}{80k+2}}{\binom{12(40k+1)^2}{80k+2}} \tag{3.1}$$

pairs of mutually avoiding sets, each set of size $40k+1$. Note that (3.1) follows from the equality

$$\frac{\binom{m}{a}}{\binom{m-b}{a-b}} = \frac{\binom{m}{b}}{\binom{a}{b}},$$

for positive integers m, a, b where $1 \leq b \leq a \leq m$.

Let A and B be a pair of mutually avoiding sets each of size $40k+1$. For $b \in B$,

label the points in A with $a_1, \ldots, a_{40k+1}$ in radial clockwise order with respect to b. Likewise, for $a \in A$, label the points in B with $b_1, \ldots, b_{40k+1}$ in radial counterclockwise order with respect to a. We say that the pair (A', B') *supports* the pair (A, B) if $A' = \{a_i \in A; i \equiv 1 \bmod 4\}$ and $B' = \{b_i \in B; i \equiv 1 \bmod 4\}$. Clearly, $|A'| = |B'| = 10k + 1$.

Since P has at most $\binom{n}{10k+1}^2$ pairs of disjoint subsets with size $10k + 1$ each, there is a pair of subsets (A', B') such that $A', B' \subset P, |A'| = |B'| = 10k + 1$, and (A', B') supports at least

$$\begin{aligned}
\frac{\binom{n}{80k+2}}{\binom{12(40k+1)^2}{80k+2}\binom{n}{10k+1}^2} &> \frac{\left(\frac{n}{80k+2}\right)^{80k+2}}{\left(\frac{12(40k+1)^2 e}{80k+2}\right)^{80k+2}\left(\frac{ne}{10k+1}\right)^{20k+2}} \\
&> \frac{n^{60k}}{e^{100k+4}12^{80k+2}(50k)^{141k}} \\
&> \frac{n^{60k}}{(430k)^{141k}}
\end{aligned}$$

mutually avoiding pairs (A, B) in P, where $|A| = |B| = 40k + 1$. Notice that for the first inequality, we use the inequality $\left(\frac{m}{r}\right)^r < \binom{m}{r} < \left(\frac{me}{r}\right)^r$, where $1 < r < m$. To see why the second inequality holds, we claim that

$$\frac{(10k+1)^{20k+2}}{(40k+1)^{160k+4}} > \frac{1}{(50k)^{141k}} \quad \text{as long as } k > 2.$$

To prove the claim, we need to show that

$$(50k)^{141k} > (40k+1)^{140k+2}\left(\frac{40k+1}{10k+1}\right)^{20k+2}.$$

Since $k > 2$, $(40k+1)^{140k+2}\left(\frac{40k+1}{10k+1}\right)^{20k+2} < (40k+1)^{141k}(\frac{40k+1}{10k+1})^{21k}$. Therefore, it is enough to show

$$(50k)^{141}(10k+1)^{21} > (40k+1)^{162}.$$

It is easy to check that $50^{141}10^{21} > (40.5)^{162}$ (since $k > 2,\ 40k+1 < 40.5k$) and this completes the proof of the claim. For the last inequality, it is easy to observe that $e^{100k+4}12^{80k+2}(50)^{141k} < (430)^{141k}$, for $k > 2$. Note that

$$e^{100k} < \left(\frac{43}{5}\right)^{46.5k} \quad \text{and} \quad 12^{80k} < \left(\frac{43}{5}\right)^{92.5k}.$$

Therefore,

$$e^{100k}12^{80k}12^2e^4 < \left(\frac{43}{5}\right)^{46.5k}\left(\frac{43}{5}\right)^{92.5k}\left(\frac{43}{5}\right)^{5} < \left(\frac{43}{5}\right)^{141k}.$$

Set $A' = \{a'_1, \ldots, a'_{10k+1}\}$ and $B' = \{b'_1, \ldots, b'_{10k+1}\}$. For any two consecutive points $a'_i, a'_{i+1} \in A', 1 \leq i \leq 10k$, consider the region $\mathcal{A}_i$ produced by the intersection of regions bounded by the lines $b'_1a'_i, b'_1a'_{i+1}$ and $b'_{10k}a'_i, b'_{10k}a'_{i+1}$. Similarly, we define the region $\mathcal{B}_i$ produced by the intersection of regions bounded by the lines $a'_1b'_i, a'_1b'_{i+1}$ and $a'_{10k}b'_i, a'_{10k}b'_{i+1}$ for $1 \leq i \leq 10k$. Therefore, we have $20k$ regions

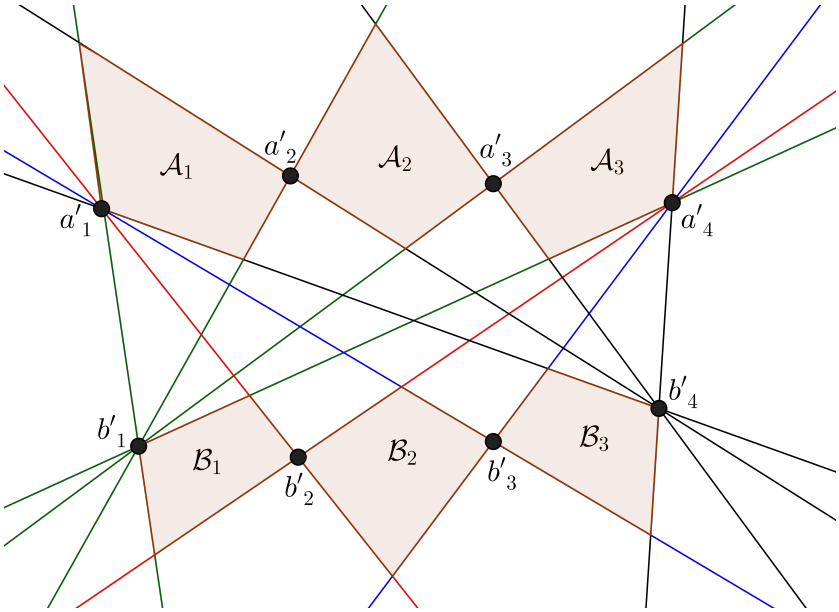

Figure 3.2: Regions and their support.

$\mathcal{A}_1, \ldots, \mathcal{A}_{10k}, \mathcal{B}_1, \ldots, \mathcal{B}_{10k}$. In Figure 3.2, the regions $\mathcal{A}_i$ and $\mathcal{B}_i$ defined by support $A' = \{a'_1, a'_2, a'_3, a'_4\}$ and $B' = \{b'_1, b'_2, b'_3, b'_4\}$. Let us remark that $4 \neq 10k+1$ for $k \in \mathbb{Z}$. The purpose of this figure is to give some intuition on how the regions A_i and B_i are formed.

Let A and B be a pair of mutually avoiding sets each of size $40k+1$. If (A', B') supports (A, B), where $A' = \{a'_1, \ldots, a'_{10k+1}\}$ and $B' = \{b'_1, \ldots, b'_{10k+1}\}$, then $A = A' \cup A_1 \cup \cdots \cup A_{10k}$ and $B = B' \cup B_1 \cup \cdots \cup B_{10k}$, where $|A_i| = |B_i| = 3$ for all $1 \leq i \leq 10k$, and A_i lies in region $\mathcal{A}_i$ and B_i lies in region $\mathcal{B}_i$.

For $i = 1, \ldots, 10k$, let α_i, respectively β_i, denote the number of points of P lying in the interior of $\mathcal{A}_i$, respectively $\mathcal{B}_i$. It follows from Observation 2.1 that (A', B') supports at most $\prod_{i=1}^{10k} \binom{\alpha_i}{3} \prod_{i=1}^{10k} \binom{\beta_i}{3}$ pairs of mutually avoiding sets (A, B), each of size $40k+1$. Therefore,

$$\frac{n^{60k}}{(430k)^{141k}} \leq \prod_{i=1}^{10k} \binom{\alpha_i}{3} \prod_{i=1}^{10k} \binom{\beta_i}{3} \leq \prod_{i=1}^{10k} (\alpha_i \beta_i)^3.$$

Without loss of generality, let us relabel the regions $\mathcal{A}_1, \ldots, \mathcal{A}_{10k}, \mathcal{B}_1, \ldots, \mathcal{B}_{10k}$ so that $\alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_{10k}$ and $\beta_1 \leq \beta_2 \leq \cdots \leq \beta_{10k}$.

Claim. *There exists an i such that $1 \leq i \leq 9k$, and $\alpha_i, \beta_i \geq \frac{n}{(1320k)^4}$.*

Proof. For the sake of contradiction, suppose for each i, $1 \leq i \leq 9k$, we have $\alpha_i < \frac{n}{(1320k)^4}$. Therefore,

$$\begin{aligned}
\frac{n^{20k}}{(430k)^{47k}} \leq \prod_{i=1}^{10k} \alpha_i \beta_i &= \prod_{i=1}^{9k} \alpha_i \left(\prod_{i=9k+1}^{10k} \alpha_i \prod_{i=1}^{10k} \beta_i) \right) \\
&\leq \left(\frac{n}{(1320k)^4} \right)^{9k} \left(\frac{\Sigma_{i=9k+1}^{10k} \alpha_i + \Sigma_{i=1}^{10k} \beta_i}{11k} \right)^{11k} \\
&< \left(\frac{n}{(1320k)^4} \right)^{9k} \left(\frac{n}{11k} \right)^{11k} \\
&= \frac{n^{20k}}{(1320k)^{36k} (11k)^{11k}}.
\end{aligned}$$

Hence, we have

$$\frac{n^{20k}}{(430k)^{47k}} < \frac{n^{20k}}{(1320k)^{36k} (11k)^{11k}}. \tag{3.2}$$

After simplifying (3.2), we get $\frac{1320^{36}11^{11}}{430^{47}} < 1$ which is a contradiction as $\frac{1320^{36}11^{11}}{430^{47}} \approx 1.054$. Thus, there exists an i, $1 \leq i \leq 9k$, with $\alpha_i \geq \frac{n}{(1320k)^4}$. With a similar calculation, there exists an i, $1 \leq i \leq 9k$ with $\beta_i \geq \frac{n}{(1320k)^4}$. □

By setting $A_i^* = P \cap \mathcal{A}_{9k+i}$ and $B_i^* = P \cap \mathcal{B}_{9k+i}$, for $1 \leq i \leq k$, we have $2k$ subsets $A_1^*, \ldots, A_k^*, B_1^*, \ldots, B_k^*$, each of size at least $\frac{n}{(1320k)^4}$, such that every pair of subsets $\{a_1, \ldots, a_k\}$ and $\{b_1, \ldots, b_k\}$, where $a_i \in A_i^*$ and $b_i \in B_i^*$, is mutually avoiding. □

3.3 Mutually avoiding sets in higher dimensions

In this section we will prove Theorem 3.7. Let $P = (p_1, \ldots, p_n)$ be an n-element point sequence in $\mathbb{R}^d$ in general position. The *order type* of P is the mapping $\chi : \binom{P}{d+1} \to \{+1, -1\}$ (positive orientation, negative orientation), assigning each $(d+1)$-tuple of P its orientation. More precisely, by setting $p_i = (a_{i,1}, a_{i,2}, \ldots, a_{i,d}) \in \mathbb{R}^d$,

$$\chi(\{p_{i_1}, p_{i_2}, \ldots, p_{i_{d+1}}\}) = sgn\ det \begin{bmatrix} 1 & 1 & \ldots & 1 \\ a_{i_1,1} & a_{i_2,1} & \ldots & a_{i_{d+1},1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i_1,d} & a_{i_2,d} & \ldots & a_{i_{d+1},d} \end{bmatrix},$$

where $i_1 < i_2 < \cdots < i_{d+1}$.

Hence two point sequences $P = (p_1, \ldots, p_n)$ and $Q = (q_1, \ldots, q_n)$ have the same order-type if and only if they are "combinatorially equivalent." See [34] and [59] for more background on order-types.

Given k disjoint subsets $P_1, \ldots, P_k \subset P$, a *transversal* of $(P_1, \ldots, P_k)$ is any k-element sequence $(p_1, \ldots, p_k)$ such that $p_i \in P_i$ for all i. We say that the k-tuple $(P_1, \ldots, P_k)$ has *same-type transversals* if all of its transversals have the same order-type. In 1998, Bárány and Valtr proved the following same-type lemma.

Lemma 3.8 ([2])**.** *Let $P = (p_1, \ldots, p_n)$ be an n-eLemmaent point sequence in $\mathcal{R}^d$ in general position. Then for $k > 0$, there is an $\varepsilon = \varepsilon(d, k)$, such that one can find disjoint subsets $P_1, \ldots, P_k \subset P$ such that $(P_1, \ldots, P_k)$ has same-type transversals and $|P_i| \geq \varepsilon n$.*

Their proof shows that $\varepsilon = 2^{-O(k^{d-1})}$. This was later improved by Fox, Pach, and Suk [30] who showed that Lemmama 3.8 holds with $\varepsilon = 2^{-O(d^3 k \log k)}$. We will use the following result, which was communicated to us by Jacob Fox, which shows that Lemmama 3.8 holds with ε decaying only polynomially in k for fixed $d \geq 3$.

Lemma 3.9. *Lemma 3.8 holds for $\varepsilon = k^{-c_d}$, where c_d depends only on d.*

The proof of Lemma 3.9 is a simple application of the following regularity lemma due to Fox, Pach, and Suk. A partition on a finite set P is called *equitable* if any two parts differ in size by at most one.

Lemma 3.10 (Theorem 1.3 in [30])**.** *For $d > 0$, there is a constant $c = c(d)$ such that the following holds. For any $\varepsilon > 0$ and for any n-element point sequence $P = (p_1, \ldots, p_n)$ in $\mathcal{R}^d$, there is an equitable partition $P = P_1 \cup \cdots \cup P_K$, with $1/\varepsilon < K < (1/\varepsilon)^c$, such that all but at most $\varepsilon\binom{K}{d+1}$ $(d+1)$-tuples of parts $(P_{i_1}, \ldots, P_{i_{d+1}})$ have same-type transversals.*

Let us note that $K > 1/\varepsilon$ follows by first arbitrarily partitioning P into $\lceil 1/\varepsilon \rceil$ parts, such that any two parts differ in size by at most one, and then following the proof of Theorem 1.3 in [30].

The next lemma we will use is Turán's Theorem for hypergraphs. Given an r-uniform hypergraph $\mathcal{H}$, let $ex(n, \mathcal{H})$ denote the maximum number of edges in any $\mathcal{H}$-free r-uniform hypergraph on n vertices.

Lemma 3.11 (de Caen [15])**.** *Let K_k^r denote the complete r-uniform hypergraph on k vertices. Then*

$$ex(n, K_k^r) \leq \left(1 - \frac{1}{\binom{k-1}{r-1}} + o(1)\right) \binom{n}{r}.$$

Proof of Lemma 3.9. Let $P = (p_1, \ldots, p_n)$ be an n-element point sequence in $\mathcal{R}^d$ in general position. Set $\varepsilon = 1/(2k)^d$, and apply Lemma 3.10 to P with parameter ε to obtain the equitable partition $P = P_1 \cup \cdots \cup P_K$ with the desired properties. Hence $|P_i| \geq n/(2k)^{d \cdot c}$, where c is defined in Lemma 3.10. Since all but at most $\varepsilon \binom{K}{d+1}$ $(d+1)$-tuples of parts $(P_{i_1}, \ldots, P_{i_{d+1}})$ have same-type transversals, we can apply Lemma 3.11 to obtain k parts $P'_1, \ldots, P'_k \in \{P_1, \ldots, P_K\}$ such that all $(d+1)$-tuples $(P'_{i_1}, \ldots, P'_{i_{d+1}})$ in $\{P'_1, \ldots, P'_k\}$ have same-type transversals. □

Proof of Theorem 3.7. Let $k > 0$ and let P be an n-element point set in $\mathcal{R}^d$ in general position. We will order the elements of $P = \{p_1, \ldots, p_n\}$ by increasing first coordinate, breaking ties arbitrarily. Let $c' = c'(d)$ be a sufficiently large constant that will be

determined later. We apply Lemma 3.9 to P with parameter $k' = \lceil k^{c'} \rceil$ to obtain subsets $P_1, \ldots, P_{k'} \subset P$ such that $|P_i| \geq k^{-c_d c'} n$, where c_d is defined in Lemma 3.9, such that all $(d+1)$-tuples $(P_{i_1}, \ldots, P_{i_{d+1}})$ have same-type transversals. Let P' be a k'-element subset obtained by selecting one point from each subset P_i. By applying Theorem 3.6 to P', we obtain subsets $A, B \subset P'$ such that A and B are mutually avoiding, and $|A|, |B| \geq \Omega((k')^{1/(d^2-d+1)})$. By choosing $c' = c'(d)$ sufficiently large, we have $|A|, |B| \geq k$. Let $\{a_1, \ldots, a_k\} \subset A$ and $\{b_1, \ldots, b_k\} \subset B$. Then the subsets $A_1, \ldots, A_k, B_1, \ldots, B_k \in \{P_1, \ldots, P_{k'}\}$, where $a_i \in A_i$ and $b_i \in B_i$, are as required in the theorem. □

3.3.1 Crossing Families in Higher Dimensions

Let P be an n-element point set in $\mathcal{R}^d$ in general position. A $(d-1)$-*simplex* in P is a $(d-1)$-dimensional simplex generated by taking the convex hull of d points in P. We say that two $(d-1)$-simplices *strongly cross* in P if their interiors intersect and they do not share a common vertex. A *crossing family* of size k in P is a set of k pairwise strongly crossing $(d-1)$-simplices in P.

In [1], Aronov et al. stated that Theorem 3.6 implies that every point set P in $\mathcal{R}^d$ in general position contains a polynomial-sized crossing family, that is, a collection of $(d-1)$-simplices in P such that any two strongly cross. Since they omitted the details, below we provide the construction of a crossing family using mutually avoiding sets in $\mathbb{R}^d$.

Let $d \geq 2$ and let P be a set of n points in $\mathcal{R}^d$ in general position. Then P contains a crossing family of size $\Omega(\sqrt{n})$ for $d = 2$, and of size $\Omega_d(n^{\frac{1}{2\prod_{i=3}^{d}(i^2-i+1)}})$ for $d \geq 3$.

Proof. We proceed by induction on d. The base case $d = 2$ follows from Theorem 3.3: a pair of mutually avoiding sets A and B in the plane, each of size $\Omega(\sqrt{n})$, gives rise to a crossing family of size $\Omega(\sqrt{n})$. For the inductive step, assume the statement holds for all $d' < d$.

Let P be a set of n points in $\mathcal{R}^d$ in general position. By Theorem 3.6, there is a pair of mutually avoiding sets A and B such that $|A| = |B| = k = \Omega_d(n^{\frac{1}{d^2-d+1}})$. Let $A = \{a_1, \ldots, a_k\}$ and $B = \{b_1, \ldots, b_k\}$. Since $conv(A) \cap conv(B) = \emptyset$, by the separation theorem (see Theorem 1.2.4 in [59]), there is a hyperplane $\mathcal{H}$ such that A lies in one of the closed half-spaces determined by $\mathcal{H}$, and B lies in the opposite closed half-space.

For each $a_i \in A$, let a_ib be the line generated by points a_i and $b \in B$. Then set $B_i = \{a_ib \cap \mathcal{H} : b \in B\}$. Since P is in general position, B_i is also in general position in $\mathcal{H}$ for each i. Moreover, since A and B are mutually avoiding, B_i has the same order-type as B_j for every $i \neq j$. Indeed, for any d-tuple $b_{i_1}, b_{i_2}, \ldots, b_{i_d} \in B$, every point in A lies on the same side of the hyperplane generated by $b_{i_1}, b_{i_2}, \ldots, b_{i_d}$. Hence the orientation of the corresponding d-tuple in $B_i \subset \mathcal{H}$ will be the same as the orientation of the corresponding d-tuple in $B_j \subset \mathcal{H}$ for $i \neq j$. Therefore, let us just consider $B_1 \subset \mathcal{H}$. By the induction hypothesis, there exists a crossing family of

$(d-2)$-simplices of size

$$k' = \Omega_d\left(k^{\frac{1}{2\prod_{i=3}^{d-1}(i^2-i+1)}}\right) = \Omega_d\left(n^{\frac{1}{2\prod_{i=3}^{d}(i^2-i+1)}}\right),$$

in $B_1 \subset \mathcal{H}$. Let $\mathcal{S} = \{\mathcal{S}_1, \ldots, \mathcal{S}_{k'}\}$ be our set of pairwise crossing $(d-2)$-simplices in $B_1 \subset \mathcal{H}$ and let $\mathcal{S}' = \{\mathcal{S}'_1, \ldots, \mathcal{S}'_{k'}\}$ be the corresponding $(d-2)$-simplices in B (which may or may not intersect).

Set $\mathcal{S}^*_i = (a_i \cup \mathcal{S}'_i)$. Then $\mathcal{S}^*_1, \ldots, \mathcal{S}^*_{k'}$ is a set of k' pairwise crossing $(d-1)$-simplices in $\mathcal{R}^d$. Indeed, consider $\mathcal{S}^*_i$ and $\mathcal{S}^*_j$. If $\mathcal{S}'_i \cap \mathcal{S}'_j \neq \emptyset$, then we are done. Otherwise, we would have $\mathcal{S}'_j \cap \mathcal{S}^*_i \neq \emptyset$ or $\mathcal{S}'_i \cap \mathcal{S}^*_j \neq \emptyset$ since B_i and B_j have the same order type and $\mathcal{S}_i \cap \mathcal{S}_j \neq \emptyset$. More precisely, let r_i be a ray from a_i through an intersection point of $\mathcal{S}_i$ and $\mathcal{S}_j$. The ray r_i intersects both $\mathcal{S}'_i$ and $\mathcal{S}'_j$ by the definition of $\mathcal{S}_i$ and $\mathcal{S}_j$. Without loss of generality assume r_i intersects $\mathcal{S}_i$ first. It follows that $\mathcal{S}'_i \cap \mathcal{S}^*_j \neq \emptyset$. □

Chapter 3 is a version of the material appearing in "*A Positive Fraction Mutually Avoiding Sets Theorem*", *Discrete Mathematics*, Vol. 343, Issue 3, 2020, co-authored with Andrew Suk. The author was one of the primary investigators and authors of this paper.

Chapter 4

Exponential sum estimates over prime fields

4.1 Introduction

Let $\mathbb{F}_p$ be a prime field, and χ be a non-trivial multiplicative character of $\mathbb{F}_p^*$. Let $\delta > 0$ be a real number. The Paley graph conjecture states that for any two sets $A, B \subset \mathbb{F}_p$ with $|A|, |B| > p^\delta$, there exists $\gamma = \gamma(\delta)$ such that the following estimate holds:

$$\left| \sum_{a \in A, b \in B} \chi(a+b) \right| < p^{-\gamma} |A||B|, \tag{4.1}$$

for any sufficiently large prime p and any non-trivial character χ.

If $|A| > p^{\frac{1}{2}+\delta}$ and $|B| > p^\delta$, the conjecture has been confirmed by Karatsuba in [45, 44, 46]. In other ranges, the conjecture remains widely open, even in the balance

case $|A| = |B| \sim p^{1/2}$.

In [17], it is shown that if we have a restricted condition on the size of the sumset $B + B$, then the inequality (4.1) is true. The precise statement is as follows.

Theorem 4.1 ([17]). *Let δ and K be positive numbers. Let A, B be sets in $\mathbb{F}_p^*$ with $p > p(\delta, K)$ large enough and χ a non-trivial multiplicative character of $\mathbb{F}_p^*$. Suppose that*

$$|A| > p^{\frac{4}{9}+\delta},$$

$$|B| > p^{\frac{4}{9}+\delta},$$

$$|B + B| < K|B|.$$

Then there exists $\gamma = \gamma(\delta, K) > 0$ such that

$$\left| \sum_{a \in A, b \in B} \chi(a + b) \right| < p^{-\gamma}|A||B|.$$

In a recent work, Shkredov and Volostnov [83] improved this theorem in the case $A = B$ using a Croot-Sisask lemma on almost periodicity of convolutions of characteristic functions of sets [20]. For the sake of completeness, we will state their result in a general form as follows.

Theorem 4.2 ([83]). *Let δ, K and L be positive numbers. Let A, B be sets in $\mathbb{F}_p^*$ with $p > p(\delta, K, L)$ large enough and χ a non-trivial multiplicative character of $\mathbb{F}_p^*$. Suppose*

that

$$|A| > p^{\frac{12}{31}+\delta},$$

$$|B| > p^{\frac{12}{31}+\delta},$$

$$|A + A| < K|A|,$$

$$|A + B| < L|B|.$$

Then we have

$$\left|\sum_{a\in A, b\in B} \chi(a+b)\right| < \sqrt{\frac{L\log 2K}{\delta \log p}}|A||B|.$$

Using recent advances in additive combinatorics, it has been indicated by Shkredov and Shparlinski [82] that if we study the sums with more variables, then the problem becomes much easier. Namely, given four sets $\mathcal{T}, \mathcal{U}, \mathcal{V}, \mathcal{W}$ in $\mathbb{F}_p^*$ and two sequences of weights $\alpha = (\alpha_t)_{t\in\mathcal{T}}$, $\beta = (\beta_{u,v,w})_{u,v,w\in\mathcal{U}\times\mathcal{V}\times\mathcal{W}}$ with

$$\max_{t\in\mathcal{T}} |\alpha_t| \leq 1, \quad \max_{(u,v,w)\in\mathcal{U}\times\mathcal{V}\times\mathcal{W}} |\beta_{uvw}| \leq 1,$$

they considered the following sum

$$S_\chi(\mathcal{T}, \mathcal{U}, \mathcal{V}, \mathcal{W}, \alpha, \beta, f) := \sum_{t\in\mathcal{T}, u\in\mathcal{U}, v\in\mathcal{V}, w\in\mathcal{W}} \alpha_t \beta_{uvw} \chi(t + f(u, v, w)),$$

where $f(x, y, z)$ is a polynomial in three variables in $\mathbb{F}_p[x, y, z]$.

Throughout this chapter, we denote the cardinality of $\mathcal{T},\mathcal{U},\mathcal{V},\mathcal{W} \subset \mathbb{F}_p$ by T,U,V,W, respectively. We use $X \ll Y$ if $X \leq CY$ for some constant $C > 0$ independent of the parameters related to X and Y, and write $X \gg Y$ for $Y \ll X$. The notation $X \sim Y$ means that both $X \ll Y$ and $Y \ll X$ hold. In addition, we use $X \lesssim Y$ to indicate that $X \ll (\log Y)Y$.

For the specific cases $f(x,y,z) = x + yz$ and $f(x,y,z) = x(y+z)$, Shkredov and Shparlinski [82] deduced the following result.

Theorem 4.3 ([82]). *For $\mathcal{U},\mathcal{V},\mathcal{W},\mathcal{T} \subset \mathbb{F}_p^*$, let $M = \max\{U,V,W\}$. If $f(x,y,z) = x + yz$ or $f(x,y,z) = x(y+z)$, then for any fixed integer $n \geq 1$, we have*

$$|S_\chi(\mathcal{T},\mathcal{U},\mathcal{V},\mathcal{W},\alpha,\beta,f)| \ll$$

$$\left((UVW)^{1-\frac{1}{4n}} + M^{\frac{1}{2n}}(UVW)^{1-\frac{1}{2n}}\right) \cdot \begin{cases} T^{\frac{1}{2}}p^{\frac{1}{2}} & \text{if } n = 1 \\ Tp^{\frac{1}{4n}} + T^{\frac{1}{2}}p^{\frac{1}{2n}} & \text{if } n \geq 2. \end{cases}$$

We note that this theorem is an improvement of the work of Hanson [35]. In order to indicate the strength of Theorem 4.3, the following interesting cases were considered by Shkredov and Shparlinski [82].

1. If $U \sim V \sim W \sim T \sim N$, then by setting $n = 1$, we have

$$|S_\chi(\mathcal{T},\mathcal{U},\mathcal{V},\mathcal{W},\alpha,\beta,f)| \ll N^{\frac{11}{4}}p^{\frac{1}{2}},$$

which is non-trivial whenever $N \geq p^{\frac{2}{5}+\epsilon}$ for some $\epsilon > 0$.

2. Suppose that $T \geq p^{\epsilon}$ for some $\epsilon > 0$ and $U \sim V \sim W \sim N$. Taking $n = \lfloor \frac{2}{\epsilon} \rfloor + 1$, we have

$$|S_{\chi}(\mathcal{T},\mathcal{U},\mathcal{V},\mathcal{W},\alpha,\beta,f)| \ll N^{3-\frac{3}{4n}} T p^{\frac{1}{4n}},$$

which is non-trivial as long as $N \geq p^{\frac{1}{3}+\delta}$ for some $\delta > 0$.

One can see [66, 26, 9, 31, 35, 43, 83, 56, 55, 85] and references therein for related results.

4.1.1 Statement of main results

The main purpose of this thesis is to extend Theorem 4.3 to a general form. More precisely, we consider any quadratic polynomial $f(x, y, z)$ which is not in the form of $g(h(x) + k(y) + l(z))$ for some polynomials g, h, k, l in one variable. We will also study the case of polynomials f in two variables. Our first result is as follows.

Theorem 4.4. *Let $f \in \mathbb{F}_p[x, y, z]$ be a quadratic polynomial that depends on each variable and that does not have the form $g(h(x) + k(y) + l(z))$. For $\mathcal{U}, \mathcal{V}, \mathcal{W} \subset \mathbb{F}_p^*$, let $\Omega = \max\{U^{-1}, V^{-1}, W^{-1}\}$ and let $\mathcal{T} \subset \mathbb{F}_p^*$. Then the following statements hold:*

1. *If $UVW \ll p^2$, then we have*

$$|S_{\chi}(\mathcal{T},\mathcal{U},\mathcal{V},\mathcal{W},\alpha,\beta,f)| \ll \left((UVW)^{1-\frac{1}{4n}} + UVW\Omega^{\frac{1}{n}}\right) \cdot \begin{cases} T^{\frac{1}{2}} p^{\frac{1}{2}} & \text{if } n = 1 \\ T p^{\frac{1}{4n}} + T^{\frac{1}{2}} p^{\frac{1}{2n}} & \text{if } n \geq 2. \end{cases}$$

2. If $UVW \gg p^2$, then we have

$$|S_\chi(\mathcal{T},\mathcal{U},\mathcal{V},\mathcal{W},\alpha,\beta,f)| \ll \left(\frac{UVW}{p^{1/2n}} + UVW\Omega^{\frac{1}{n}}\right)\cdot \begin{cases} T^{\frac{1}{2}}p^{\frac{1}{2}} & \text{if } n=1 \\ Tp^{\frac{1}{4n}} + T^{\frac{1}{2}}p^{\frac{1}{2n}} & \text{if } n\geq 2. \end{cases}$$

As an immediate consequence of Theorem 4.4, we get the following corollaries.

Let $f \in \mathbb{F}_p[x,y,z]$ be a quadratic polynomial defined in Theorem 4.4. Let $\mathcal{U},\mathcal{V},\mathcal{W},\mathcal{T} \subset \mathbb{F}_p^*$ such that $U \sim V \sim W \sim N$ and $T \geq p^\epsilon$ for some $\epsilon > 0$. Then the following statements hold:

1. If $p^{\frac{1}{3}+\delta} \ll N \ll p^{\frac{2}{3}}$ for some $\delta > 0$ and $n > \lfloor \frac{1}{2\epsilon} \rfloor + 1$, then we have

$$|S_\chi(\mathcal{T},\mathcal{U},\mathcal{V},\mathcal{W},\alpha,\beta,f)| \ll N^{3-\frac{3}{4n}}Tp^{\frac{1}{4n}}.$$

2. If $N \gg p^{\frac{2}{3}}$ and $n > \lfloor \frac{1}{2\epsilon} \rfloor + 1$, then we have

$$|S_\chi(\mathcal{T},\mathcal{U},\mathcal{V},\mathcal{W},\alpha,\beta,f)| \ll \frac{N^3T}{p^{1/4n}}.$$

Let $f \in \mathbb{F}_p[x,y,z]$ be a quadratic polynomial defined in Theorem 4.4. For $\mathcal{U},\mathcal{V},\mathcal{W},\mathcal{T} \subset \mathbb{F}_p^*$ with $U \sim V \sim W \sim T \sim N$, we have the following conclusions:

1. Suppose that $p^{\frac{2}{5}+\delta} \ll N \ll p^{\frac{2}{3}}$ for some $\delta > 0$, then we have

$$|S_\chi(\mathcal{T},\mathcal{U},\mathcal{V},\mathcal{W},\alpha,\beta,f)| \ll N^{11/4}p^{1/2} \ (n=1).$$

2. Suppose that $N \gg p^{2/3}$, then we have

$$|S_\chi(\mathcal{T},\mathcal{U},\mathcal{V},\mathcal{W},\alpha,\beta,f)| \ll N^{7/2} \ (n=1).$$

Now we address the results for two variable quadratic polynomial $f \in \mathbb{F}_p[x,y]$. Let χ be a non-trivial multiplicative character of $\mathbb{F}_p^*$. Given three sets $\mathcal{T},\mathcal{U},\mathcal{V}$ in $\mathbb{F}_p^*$, a polynomial $f \in \mathbb{F}_p[x,y]$, and two sequences of weights $\alpha = (\alpha_t)_{t\in\mathcal{T}}, \beta = (\beta_{u,v})_{u,v\in\mathcal{U}\times\mathcal{V}}$ with

$$\max_{t\in\mathcal{T}} |\alpha_t| \le 1, \quad \max_{(u,v)\in\mathcal{U}\times\mathcal{V}} |\beta_{uv}| \le 1,$$

we define

$$S_\chi(\mathcal{T},\mathcal{U},\mathcal{V},\alpha,\beta,f) = \sum_{t\in\mathcal{T},u\in\mathcal{U},v\in\mathcal{V}} \alpha_t\beta_{uv}\chi(t+f(u,v)).$$

We are interested in finding an upper bound of the sum $S_\chi(\mathcal{T},\mathcal{U},\mathcal{V},\alpha,\beta,f)$. In particular, we deduce strong results on this problems in the case when $f \in \mathbb{F}_p[x,y]$ is a quadratic polynomial which is not of the form $g(\alpha x+\beta y)$ for some polynomial g in one variable. Relating this problem for two variable polynomials to that of three variable polynomials, we are able to prove the following result for two variable polynomials.

Theorem 4.5. *Let $f \in \mathbb{F}_p[x,y]$ be a quadratic polynomial which depends on each variable and which does not take the form $g(ax+by)$. Given $\mathcal{U},\mathcal{V},\mathcal{T} \subset \mathbb{F}_p^*$ with $|\mathcal{U}-\mathcal{V}| \sim kU$ for some parameter $k>0$, the following two statements hold:*

1. *If $V^2|\mathcal{U}-\mathcal{V}| \ll p^2$, then we have*

$$|S_\chi(\mathcal{T},\mathcal{U},\mathcal{V},\alpha,\beta,f)| \lesssim$$
$$\left(k^{\frac{3}{4n}} \cdot \frac{UV}{U^{1/4n}V^{1/2n}} + k^{\frac{1}{n}} \cdot \frac{UV}{V^{1/n}}\right) \cdot \begin{cases} T^{\frac{1}{2}}p^{\frac{1}{2}} & \text{if } n=1 \\ Tp^{\frac{1}{4n}} + T^{\frac{1}{2}}p^{\frac{1}{2n}} & \text{if } n \geq 2. \end{cases}$$

2. *If $V^2|\mathcal{U}-\mathcal{V}| \gg p^2$, then we have*

$$|S_\chi(\mathcal{T},\mathcal{U},\mathcal{V},\alpha,\beta,f)| \lesssim$$
$$\left(k^{\frac{1}{n}} \cdot \frac{UV}{p^{1/2n}} + k^{\frac{1}{n}} \cdot \frac{UV}{V^{1/n}}\right) \cdot \begin{cases} T^{\frac{1}{2}}p^{\frac{1}{2}} & \text{if } n=1 \\ Tp^{\frac{1}{4n}} + T^{\frac{1}{2}}p^{\frac{1}{2n}} & \text{if } n \geq 2. \end{cases}$$

As a consequence of Theorem 4.5 for $k=1$, we have the following corollary. Let $f \in \mathbb{F}_p[x,y]$ be a quadratic polynomial defined as in Theorem 4.5. Assume that $\mathcal{U},\mathcal{V},\mathcal{T} \subset \mathbb{F}_p^*$ with $|\mathcal{U}-\mathcal{V}| \sim U$, $U \sim V \sim N$, and $T \geq p^\epsilon$ for some $\epsilon > 0$. Then the following statements hold:

1. Suppose that $p^{\frac{1}{3}+\epsilon'} \ll N \ll p^{\frac{2}{3}}$ for some $\epsilon' > 0$ and $n > \lfloor 1/2\epsilon \rfloor + 1$. Then we have

$$|S_\chi(\mathcal{T},\mathcal{U},\mathcal{V},\alpha,\beta,f)| \lesssim N^{2-\frac{3}{4n}} T p^{\frac{1}{4n}}.$$

2. Suppose that $N \gg p^{2/3}$ and $n > \lfloor 1/2\epsilon \rfloor + 1$. Then we have

$$|S_\chi(\mathcal{T},\mathcal{U},\mathcal{V},\alpha,\beta,f)| \lesssim \frac{N^2 T}{p^{1/4n}}.$$

The rest of this chapter is organized as follows: in Section 2 we prove Theorem 4.4, and in Section 3 we present the proof of Theorem 4.5.

4.2 Proof of Theorem 4.4

The following result is our main step in the proof of Theorem 4.4. This is the unbalanced energy version of Theorem 1.1 in [68].

Theorem 4.6. *Suppose that $f \in \mathbb{F}_p[x,y,z]$ is a quadratic polynomial which depends on each variable and which does not take the form $g(h(x)+k(y)+l(z))$. For $\mathcal{U},\mathcal{V},\mathcal{W} \subset \mathbb{F}_p^*$ with $UVW \ll p^2$, let E be the number of tuples $(u,v,w,u',v',w') \in (\mathcal{U}\times\mathcal{V}\times\mathcal{W})^2$ such that $f(u,v,w) = f(u',v',w')$. Then we have*

$$E \ll (UVW)^{3/2} + \max\{V^2W^2, V^2U^2, U^2W^2\}.$$

Proof. Let $f(x,y,z)$ be a quadratic polynomial that is not of the form $g(h(x)+k(y)+l(z))$. Then f has at least one of the mixed terms xy, yz, xz, because otherwise f would be in the form of $h(x)+k(y)+l(z)$. Moreover, we may assume that f does not have any constant term, because the value E is independent of the constant term in $f(x,y,z)$. Therefore, we may assume that $f(x,y,z) = axy+bxz+cyz+r(x)+s(y)+t(z)$ where one of $a,b,c \in \mathbb{F}_p$ is not zero, and r,s,t are polynomials in one variable with degree at most two and no constant terms. Furthermore, from the symmetric property of $f(x,y,z)$ we only need to prove Theorem 5.8 for the following three cases:

Case 1: $f(x,y,z) = axy+bxz+r(x)+s(y)+t(z)$ with $a \neq 0$ and $\deg(t) = 2$.

Case 2: $f(x,y,z) = axy+bxz+r(x)+s(y)+t(z)$ with $a \neq 0$ and $\deg(t) = 1$.

Case 3: $f(x,y,z) = axy+bxz+r(x)+s(y)$ with $a,b \neq 0$.

Case 4: $f(x,y,z) = axy+bxz+cyz+r(x)+s(y)+t(z)$ with $a,b,c \neq 0$.

Notice that if one or two of the three mixed terms does not appear in the polynomial $f(x,y,z)$ (i.e. **Case 1, 2** or **3**), then the statement of Theorem 5.8 follows immediately from Lemma 4.7, 4.8 and 4.9 below. On the other hand, if the polynomial $f(x,y,z)$ has all the three mixed terms (i.e. **Case 4**), then Theorem 5.8 is a direct consequence of Lemma 4.10. Hence, the proof of Theorem 5.8 is complete if we have the following four lemmas whose proofs will be given in the subsection below.

Lemma 4.7. *Let $f(x,y,z) = axy+bxz+r(x)+s(y)+t(z)$ be a quadratic polynomial in $\mathbb{F}_p[x,y,z]$ that depends on each variable with $a \neq 0$ and $\deg(t) = 2$. If $\mathcal{U}, \mathcal{V}, \mathcal{W} \subset \mathbb{F}_p^*$*

with $UVW \ll p^2$, *then we have*

$$E \ll (UVW)^{3/2} + \max\{U, V\}(UVW),$$

where E *denotes the number of tuples* $(x, y, z, x', y', z') \in (\mathcal{U} \times \mathcal{V} \times \mathcal{W})^2$ *such that* $f(x, y, z) = f(x', y', z')$.

Lemma 4.8. *Let* $f(x, y, z) = axy + bxz + r(x) + s(y) + t(z)$ *be a quadratic polynomial in* $\mathbb{F}_p[x, y, z]$ *that depends on each variable with* $a \neq 0$ *and* $\deg(t) = 1$. *Then for* $\mathcal{U}, \mathcal{V}, \mathcal{W} \subset \mathbb{F}_p^*$ *with* $UVW \ll p^2$, *we have*

$$E \ll (UVW)^{3/2} + \max\{V^2W^2, V^2U^2, U^2W^2\},$$

where E *is the number of tuples* $(x, y, z, x', y', z') \in (\mathcal{U} \times \mathcal{V} \times \mathcal{W})^2$ *such that* $f(x, y, z) = f(x', y', z')$.

Lemma 4.9. *Let* $f(x, y, z) = axy + bxz + r(x) + s(y)$ *be a quadratic polynomial in* $\mathbb{F}_p[x, y, z]$ *that depends on each variable with* $a, b \neq 0$. *Then for* $\mathcal{U}, \mathcal{V}, \mathcal{W} \subset \mathbb{F}_p^*$ *with* $UVW \ll p^2$, *we have*

$$E \ll (UVW)^{3/2} + \max\{U, V\}(UVW),$$

where E *is the number of tuples* $(x, y, z, x', y', z') \in (\mathcal{U} \times \mathcal{V} \times \mathcal{W})^2$ *such that* $f(x, y, z) =$

$f(x', y', z')$.

Lemma 4.10. *Let $f(x, y, z) = axy + bxz + cyz + r(x) + s(y) + t(z)$ be a quadratic polynomial in $\mathbb{F}_p[x, y, z]$ with $a, b, c \neq 0$ which depends on each variable and which does not take the form $g(h(x) + k(y) + l(z))$. If $\mathcal{U}, \mathcal{V}, \mathcal{W} \subset \mathbb{F}_p^*$ with $UVW \ll p^2$, then*

$$E \ll (UVW)^{3/2} + \max\{V^2W^2, V^2U^2, U^2W^2\},$$

where E denotes the number of tuples $(x, y, z, x', y', z') \in (\mathcal{U} \times \mathcal{V} \times \mathcal{W})^2$ such that $f(x, y, z) = f(x', y', z')$.

□

Proofs of Lemmas 4.7, 4.8, 4.9, and 4.10

In order to estimate the energy E given in four lemmas above, we use the point-plane incidence bound due to Rudnev [71]. A short proof can be found in [97].

Theorem 4.11 (Rudnev)**.** *Let $\mathcal{R}, \mathcal{S}$ denote a set of points in $\mathbb{F}_p^3$ and a set of planes in $\mathbb{F}_p^3$, respectively. Suppose that $|\mathcal{R}| \ll |\mathcal{S}|$ and $|\mathcal{R}| \ll p^2$. In addition, assume that there is no line that contains k points of $\mathcal{R}$ and is contained in k planes of $\mathcal{S}$. Then we have*

$$\mathcal{I}(\mathcal{R}, \mathcal{S}) := |\{(p, \pi) : p \in \mathcal{R}, \pi \in \mathcal{S}\}| \ll |\mathcal{R}|^{1/2}|\mathcal{S}| + k|\mathcal{S}|.$$

We also need the following Lemma.

Lemma 4.12 (Kővari–Sós–Turán theorem, [5]). *Let $G = (A \cup B, E(G))$ be a $K_{2,t}$-free bipartite graph. Then the number of edges between A and B is bounded by*

$$|E(G)| \ll t^{1/2}|A||B|^{1/2} + |B|.$$

Proof of Lemma 4.7 Let E be the number of tuples $(x, y, z, x', y', z') \in (\mathcal{U}\times\mathcal{V}\times\mathcal{W})^2$ such that $f(x, y, z) = f(x', y', z')$, where the quadratic polynomial f takes the form in **Case 1**. This implies that

$$ayx - ax'y' + (bxz + r(x) + t(z) - s(y')) = bx'z' + r(x') + t(z') - s(y).$$

This relation can be viewed as an incidence between the point $(x, y', bxz+r(x)+t(z)-s(y'))$ in $\mathbb{F}_p^3$ and the plane defined by $ayX - ax'Y + Z = bx'z' + r(x') + t(z') - s(y)$. Let $\mathcal{R}$ be the following point set:

$$\mathcal{R} := \{(x, y', bxz + r(x) + t(z) - s(y')) : (x, y', z) \in \mathcal{U} \times \mathcal{V} \times \mathcal{W}\} \subset \mathbb{F}_p^3,$$

and $\mathcal{S}$ be the following plane set

$$\mathcal{S} := \{ayX - ax'Y + Z = bx'z' + r(x') + t(z') - s(y) : (x', y, z') \in \mathcal{U} \times \mathcal{V} \times \mathcal{W}\}.$$

For each fixed $(u, v, w) \in \mathcal{R}$, at most two elements (x, y', z) in $\mathcal{U} \times \mathcal{V} \times \mathcal{W}$ reproduce the (u, v, w), because $\deg(t) = 2$. In fact, we can take $x = u, y' = v$, and z values are

solutions to

$$t(z) + buz + r(u) - s(v) = w.$$

By the same argument, we see that each fixed plane in $\mathcal{S}$ can be determined by at most two elements $(x', y, z') \in \mathcal{U} \times \mathcal{V} \times \mathcal{W}$. Also notice that each element in $\mathcal{U} \times \mathcal{V} \times \mathcal{W}$ determines a point in $\mathcal{R}$ and a plane in $\mathcal{S}$. Hence, we have that

$$|\mathcal{R}| \sim |\mathcal{S}| \sim UVW \quad \text{and} \quad E \sim \mathcal{I}(\mathcal{R}, \mathcal{S}).$$

This shows that our problem is reducing to estimate of $\mathcal{I}(\mathcal{R}, \mathcal{S})$. To bound this, we apply Rudnev's point-plane incidence theorem. Since $|\mathcal{R}| \sim UVW$, the condition $|\mathcal{R}| \ll p^2$ in Theorem 4.11 is clearly satisfied from our assumption that $UVW \ll p^2$. Now, we count the number of collinear points in $\mathcal{R}$. Let $\mathcal{R}'$ be the projection of $\mathcal{R}$ onto the first two coordinates. It is clear that $\mathcal{R}' = \mathcal{U} \times \mathcal{V}$. Thus any line contains at most $\max\{U, V\}$ points unless it is vertical. In the case of vertical lines, we can see that no plane in $\mathcal{S}$ contains such lines, because the z-coordinate of normal vectors of planes in $\mathcal{S}$ is one. Therefore, we can apply Theorem 4.11 with $k = \max\{U, V\}$. In other words, we obtain

$$E \ll (UVW)^{3/2} + \max\{U, V\}(UVW).$$

This completes the proof of Lemma 4.7. $\square$.

Proof of Lemma 4.8 Since $\deg(t) = 1$, without loss of generality, we assume that $t(z) = mz$ for some $m \in \mathbb{F}_p^*$ and so $f(x, y, z) = axy + bxz + r(x) + s(y) + mz$. As in the proof of Lemma 4.7, we define the set $\mathcal{R}$ of points and the set $\mathcal{S}$ of planes as follows:

$$\mathcal{R} := \{(x, y', bxz + r(x) + mz - s(y')) : (x, y', z) \in \mathcal{U} \times \mathcal{V} \times \mathcal{W}\} \subset \mathbb{F}_p^3,$$

$$\mathcal{S} := \{ayX - ax'Y + Z = bx'z' + r(x') + mz' - s(y) : (x', y, z') \in \mathcal{U} \times \mathcal{V} \times \mathcal{W}\}.$$

The only reason we need to prove Lemma 4.8 is that if $u = -m/b \in \mathcal{U}$, then the triples $(-m/b, v, w) \in \mathcal{R}$ can be determined by many triples $(x, y', z) \in \mathcal{U} \times \mathcal{V} \times \mathcal{W}$. For this case, we need to do some more technical steps. If $-m/b \notin \mathcal{U}$, then Lemma 4.8 follows immediately from the same argument as in the proof of Lemma 4.7. Thus we may assume that $u = -m/b \in \mathcal{U}$. As above, we first need to estimate the sizes of $\mathcal{R}$ and $\mathcal{S}$. For $(u, v, w) \in \mathcal{R}$ and $(x, y', z) \in \mathcal{U} \times \mathcal{V} \times \mathcal{W}$, we consider the following system of three equations:

$$u = x,\ v = y',\ w = buz + r(u) + mz - s(v).$$

If $u \in \mathcal{U}$ satisfies $bu = -m$, i.e. $u = -m/b \in \mathcal{U}$, then we have

$$u = x,\ v = y',\ w = r(u) - s(v) \quad \text{for all} \ \ z \in \mathcal{W}. \tag{4.2}$$

Let $\mathcal{R}_1$ be the set of points $(u, v, w) \in \mathcal{R}$ with $u = -m/b$. Then $\mathcal{R}_1$ is a set with V points, since for any $v = y' \in \mathcal{V}$, w is determined uniquely. By (4.2) and the definition of $\mathcal{R}_1$, notice that each point in $\mathcal{R}_1$ is determined by W triples $(x, y', z) \in \mathcal{U} \times \mathcal{V} \times \mathcal{W}$. Let $\mathcal{R}_2 = \mathcal{R} \setminus \mathcal{R}_1$. Also notice that each point in $\mathcal{R}_2$ is determined by exactly one triple $(x, y', z) \in \mathcal{U} \times \mathcal{V} \times \mathcal{W}$.

By the similar argument, we can partition the set of planes $\mathcal{S}$ into two sets $\mathcal{S}_1$ and $\mathcal{S}_2$ with $\mathcal{S}_2 = \mathcal{S} \setminus \mathcal{S}_1$ so that $|\mathcal{S}_1| = V$, each plane in $\mathcal{S}_1$ is determined by W triples $(x', y, z') \in \mathcal{U} \times \mathcal{V} \times \mathcal{W}$, and each plane in $\mathcal{S}_2$ is determined by exactly one triple $(x', y, z') \in \mathcal{U} \times \mathcal{V} \times \mathcal{W}$.

From the above observations, it follows that each incidence between $\mathcal{R}_1$ and $\mathcal{S}_2$, or between $\mathcal{R}_2$ and $\mathcal{S}_1$ contributes to E by W, each incidence between $\mathcal{R}_1$ and $\mathcal{S}_1$ contributes to E by W^2, and each incidence between $\mathcal{R}_2$ and $\mathcal{S}_2$ contributes to E by one. Namely, we have

$$E \ll W^2 \cdot \mathcal{I}(\mathcal{R}_1, \mathcal{S}_1) + W \cdot \mathcal{I}(\mathcal{R}_1, \mathcal{S}_2) + W \cdot \mathcal{I}(\mathcal{R}_2, \mathcal{S}_1) + \mathcal{I}(\mathcal{R}_2, \mathcal{S}_2).$$

Since $|\mathcal{R}_1| = |\mathcal{S}_1| = V$, it is clear that

$$I(\mathcal{R}_1, \mathcal{S}_1) \ll V^2.$$

To bound $I(\mathcal{R}_2, \mathcal{S}_2)$, recall that each element of $\mathcal{R}_2$ and $\mathcal{S}_2$ is determined by exactly one element $(x, y, z) \in \mathcal{U} \times \mathcal{V} \times W$ with $x \neq -m/b$. Hence, by the same

argument as in the proof of Lemma 4.7, we see that

$$I(\mathcal{R}_2, \mathcal{S}_2) \ll (UVW)^{3/2} + \max\{U, V\}(UVW).$$

To bound $I(\mathcal{R}_1, \mathcal{S}_2)$, we will use Lemma 4.12. Let G denote the bipartite graph with vertex sets $\mathcal{S}_2$ and $\mathcal{R}_1$ such that there is an edge between a point in $\mathcal{R}_1$ and a plane in $\mathcal{S}_2$ if the point lies on the plane. Since $|\mathcal{R}_1| = V$, each line contains at most V points in $\mathcal{R}_1$, and so any two planes in $\mathcal{S}_2$ support at most V points in common. Thus letting $A := \mathcal{R}_1$ and $B := \mathcal{S}_2$ and applying Lemma 4.12, we obtain that

$$I(\mathcal{R}_1, \mathcal{S}_2) = |E(G)| \ll V^{1/2}V(UVW)^{1/2} + UVW = U^{1/2}W^{1/2}V^2 + UVW.$$

Similarly, we also have

$$I(\mathcal{R}_2, \mathcal{S}_1) \ll U^{1/2}W^{1/2}V^2 + UVW.$$

In other words, we have proved that

$$\begin{aligned} E &\ll (UVW)^{3/2} + \max\{U, V, W\}(UVW) + V^2W^2 + U^{1/2}V^2W^{3/2} \\ &\ll (UVW)^{3/2} + V^2W^2 + V^2U^2 + U^2W^2 \\ &\ll (UVW)^{3/2} + \max\{V^2W^2, V^2U^2, U^2W^2\}. \end{aligned}$$

This completes the proof of Lemma 4.8. $\square$.

Proof of Lemma 4.9: Since $f(x,y,z) = axy + bxz + r(x) + s(y)$ with $a, b \neq 0$, as in the proof of Lemma 4.7, we can define the set $\mathcal{R}$ of points and the set $\mathcal{S}$ of planes as follows:

$$\mathcal{R} := \{(x, y', bxz + r(x) - s(y')) : (x, y', z) \in \mathcal{U} \times \mathcal{V} \times \mathcal{W}\} \subset \mathbb{F}_p^3,$$

$$\mathcal{S} := \{ayX - ax'Y + Z = bx'z' + r(x') - s(y) : (x', y, z') \in \mathcal{U} \times \mathcal{V} \times \mathcal{W}\}.$$

Since $b \neq 0$ and $\mathcal{U} \subset \mathbb{F}_p^*$, we have

$$|\mathcal{R}| = |\mathcal{S}| = UVW \quad \text{and} \quad E = \mathcal{I}(\mathcal{R}, \mathcal{S}).$$

By the same argument as in the proof of Lemma 4.7, we conclude that

$$E \ll (UVW)^{3/2} + \max\{U, V\}(UVW),$$

as desired. $\square$.

Proof of Lemma 4.10: Now we would like to estimate E which is the number of tuples $(x, y, z, x', y', z') \in (\mathcal{U} \times \mathcal{V} \times \mathcal{W})^2$ satisfying the equation

$$f(x, y, z) = f(x', y', z'), \tag{4.3}$$

where $f(x,y,z) = axy + bxz + cyz + r(x) + s(y) + t(z)$ is a quadratic polynomial in $\mathbb{F}_p[x,y,z]$ with $a,b,c \neq 0$. Without loss of generality, we may assume that

$$f(x,y,z) = axy + bxz + cyz + dx^2 + ey^2 + gz^2 + hx + iy + jz,$$

where $a,b,c \neq 0$ and $d,e,g,h,i,j \in \mathbb{F}_q$. We adapt the argument as in the proof of Lemma 2.3 in [68]. Since the polynomial $f(x,y,z)$ is not in the form of $g(h(x)+k(y)+l(z))$, one of the following equations is not satisfied:

$$4de = a^2,\ 4dg = b^2,\ 4eg = c^2,\ hc = ja = ib.$$

Otherwise, we could write

$$f = \left(\sqrt{d}x + \sqrt{e}y + \sqrt{g}z + \frac{h}{2\sqrt{d}}\right)^2 - \frac{h^2}{4d},$$

if all of d,e,g are squares in $\mathbb{F}_q$. On the other hand, if all of d,e,g are not squares in $\mathbb{F}_q$, we could write

$$f = \frac{1}{deg}\left(d\sqrt{eg}x + e\sqrt{dg}y + g\sqrt{de}z + \frac{h\sqrt{eg}}{2}\right)^2 - \frac{h^2}{4d},$$

since the equations $4de = a^2, 4dg = b^2, 4eg = c^2$ imply that de, dg, eg are squares in $\mathbb{F}_q$, and e,d,g are nonzeros.

By permuting the variables, we may assume that one of the following equations

does not hold:

$$4eg = c^2,\ ib = ja.$$

The equation (4.3) is rewritten as

$$\begin{aligned}(ay+bz)x - x'(ay'+bz') + dx^2 - e(y')^2 - cy'z' - g(z')^2 + hx - iy' - jz' \\ = d(x')^2 - ey^2 - cyz - gz^2 + hx' - iy - jz.\end{aligned}$$

This relation can be viewed as an incidence between the point $(x, ay'+bz', dx^2-e(y')^2-cy'z'-g(z')^2+hx-iy'-jz')$ in $\mathbb{F}_p^3$ and the plane defined by

$$(ay+bz)X - x'Y + Z = d(x')^2 - ey^2 - cyz - gz^2 + hx' - iy - jz.$$

Let $\mathcal{R}$ be the following set of points

$$\mathcal{R} = \{(x, ay'+bz', dx^2-e(y')^2-cy'z'-g(z')^2+hx-iy'-jz') : (x, y', z') \in \mathcal{U}\times\mathcal{V}\times\mathcal{W}\},$$

and $\mathcal{S}$ be the following set of planes

$$\mathcal{S} = \{(ay+bz)X-x'Y+Z = d(x')^2-ey^2-cyz-gz^2+hx'-iy-jz : (x', y, z) \in \mathcal{U}\times\mathcal{V}\times\mathcal{W}\}.$$

It is clear that E is bounded from above by the number of incidences between $\mathcal{R}$ and $\mathcal{S}$. In the next step, we estimate the sizes of $\mathcal{R}$ and $\mathcal{S}$. Indeed, for a given point

$(u, v, w) \in \mathcal{R}$, we now count the number of triples $(x, y', z') \in \mathcal{U} \times \mathcal{V} \times \mathcal{W}$ such that

$$u = x, \quad v = ay' + bz', \quad w = dx^2 - e(y')^2 - cy'z' - g(z')^2 + hx - iy' - jz'.$$

These equations yield that

$$w = du^2 - e(y')^2 - cy' \left(\frac{v - ay'}{b} \right) - g \left(\frac{v - ay'}{b} \right)^2 + hu - iy' - j \left(\frac{v - ay'}{b} \right),$$

or

$$\begin{aligned} \left(b^2e - abc + a^2g\right)(y')^2 + \left(bcv - 2agv + ib^2 - jab\right)y' \\ + \left(b^2w - b^2du^2 + gv^2 - b^2hu + bjv\right) \\ = 0. \end{aligned}$$

We consider the following two cases:

Case 1: If either $b^2e - abc + a^2g$ or $bcv - 2agv + ib^2 - jab$ is non-zero, then at most two solutions y' of the above equation exist, and z' value is determined in terms of v and y'.

Case 2: If both $b^2e - abc + a^2g$ and $bcv - 2agv + ib^2 - jab$ are zero, then we

will have the following system:

$$b^2e-abc+a^2g=0, \quad (bc-2ag)v+(ib-ja)b=0, \quad b^2w-b^2du^2+gv^2-b^2hu+bjv=0. \tag{4.4}$$

In this case, we need to do some more technical steps.

In the case when $bc-2ag=0$, the second equation above tells us that $ib=ja$. Therefore, it follows from the first equation that $4eg=c^2$, which contradicts our assumptions at the beginning of the proof.

Thus we must have $bc-2ag\neq 0$. This gives us $v=-(ib^2-jab)/(bc-2ag)$. For this value of v and any $u\in\mathcal{U}, w$ is determined uniquely by the third equation of (4.4). Therefore, there are at most U points $(u,v,w)\in\mathcal{R}$ which satisfy three equations above. We denote the set of these points by $\mathcal{R}_2\subset\mathcal{R}$. Let $\mathcal{R}_1=\mathcal{R}\setminus\mathcal{R}_2$. We have $|\mathcal{R}_2|=U$ and $|\mathcal{R}_1|\sim UVW$. Note that any point in $\mathcal{R}_1$ corresponds to at most two points in $\mathcal{U}\times\mathcal{V}\times\mathcal{W}$ and any point in $\mathcal{R}_2$ corresponds to at most $\max\{V,W\}$ points $(x,y',z')\in\mathcal{U}\times\mathcal{V}\times\mathcal{W}$.

Likewise, we can also show that the plane set $\mathcal{S}$ can be partitioned into two sets $\mathcal{S}_1$ and $\mathcal{S}_2$, where each plane in $\mathcal{S}_1$ corresponds to at most two points in $\mathcal{U}\times\mathcal{V}\times\mathcal{W}$, and each plane in $\mathcal{S}_2$ corresponds to at most $\max\{V,W\}$ points in $\mathcal{U}\times\mathcal{V}\times\mathcal{W}$.

Set $N:=\max\{V,W\}$. We observe that an incidence between $\mathcal{R}_2$ and $\mathcal{S}_1$, or between $\mathcal{R}_1$ and $\mathcal{S}_2$, contributes at most N to E, and an incidence between$\mathcal{R}_2$ and $\mathcal{S}_2$

contributes at most N^2 to E. Hence, we obtain

$$E \ll \mathcal{I}(\mathcal{R}_1, \mathcal{S}_1) + N \cdot \mathcal{I}(\mathcal{R}_1, \mathcal{S}_2) + N \cdot \mathcal{I}(\mathcal{R}_2, \mathcal{S}_1) + N^2 \cdot \mathcal{I}(\mathcal{R}_2, \mathcal{S}_2). \tag{4.5}$$

Since $|\mathcal{R}_2|, |\mathcal{S}_2| \ll U$, we have $\mathcal{I}(\mathcal{R}_2, \mathcal{S}_2) \leq U^2$. To bound $\mathcal{I}(\mathcal{R}_1, \mathcal{S}_1)$, we will apply Theorem 4.11. Before doing this, we need to give an upper bound on the number of collinear points in $\mathcal{R}$.

One can cover the set $\mathcal{R}$ by U planes defined by the equations $x = x_0, x_0 \in U$. By a direct computation, one can check that for each plane $x = x_0$, the points of $\mathcal{R}$ on this plane lie on either a line or a parabola, and for distinct $y' \in V$, we have distinct parabolas or lines.

If a line l does not lie on any of those planes, then it intersects $\mathcal{R}$ in at most U points. Suppose that l lies on the plane $x = x_0$. Then there are two possibilities. If l is the same as a line determined by some $y' \in V$, then it contains W points. If it is not that case, then l supports at most $2V$ points from $\mathcal{R}$, since a line intersects a parabola or a line in at most two points. In other words, we can say that the maximal number of collinear points in $\mathcal{R}$ is at most $U + 2V + W$. By Theorem 4.11, we have

$$\mathcal{I}(\mathcal{R}_1, \mathcal{S}_1) \ll (UVW)^{3/2} + \max\{U, V, W\}(UVW).$$

To bound $I(\mathcal{R}_1, \mathcal{S}_2)$ and $I(\mathcal{R}_2, \mathcal{S}_1)$, we use Lemma 4.12 again. Let G be the bipartite graph with vertex sets $\mathcal{S}_2$ and $\mathcal{R}_1$ such that there is an edge between a point

and a plane if the point lies on the plane. We showed that no $\max\{U, V, W\}+1$ points of $\mathcal{R}_1$ lie on a line. Hence, any two planes of $\mathcal{S}_2$ contain at most $\max\{U, V, W\}$ points of $\mathcal{R}_1$ in common. Thus, we get

$$\mathcal{I}(\mathcal{R}_1, \mathcal{S}_2) = |E(G)| \ll (\max\{U, V, W\})^{1/2} \cdot U \cdot (UVW)^{1/2} + UVW.$$

Using a similar argument, we get

$$\mathcal{I}(\mathcal{R}_2, \mathcal{S}_1) \ll (\max\{U, V, W\})^{1/2} \cdot U \cdot (UVW)^{1/2} + UVW.$$

Putting all bounds together, it follows from (4.5) that

$$E \ll (UVW)^{3/2} + M(UVW) + NM^{\frac{1}{2}}U^{\frac{3}{2}}V^{\frac{1}{2}}W^{\frac{1}{2}} + N(UVW) + N^2U^2, \tag{4.6}$$

where $N = \max\{V, W\}$ and $M = \max\{U, V, W\}$. A direct computation shows that each of the second, third, fourth, and fifth terms in the RHS of the equation (4.6) is dominated by

$$V^2W^2 + V^2U^2 + U^2W^2.$$

Hence, we have

$$\begin{aligned} E &\ll (UVW)^{3/2} + V^2W^2 + V^2U^2 + U^2W^2 \\ &\ll (UVW)^{3/2} + \max\{V^2W^2, V^2U^2, U^2W^2\}, \end{aligned}$$

which completes the proof of Lemma 4.10. □

In addition to Theorem 5.8, the following lemma also plays an important role in providing the complete proof of the first part of Theorem 4.4.

Lemma 4.13 ([82], Lemma 2.3)**.** *For $\mathcal{T} \subset \mathbb{F}_p^*$ with size T and a sequence of weights $\alpha = (\alpha_t)_{t\in\mathcal{T}}$ with $\max_{t\in\mathcal{T}} |\alpha_t| \leq 1$, and for any fixed integer $n \geq 1$, we have*

$$\sum_{\lambda\in\mathbb{F}_p} \left|\sum_{t\in\mathcal{T}} \alpha_t \chi(\lambda + t)\right|^{2n} \ll \begin{cases} Tp & \text{if } n = 1 \\ \\ T^{2n}p^{1/2} + T^n p & \text{if } n \geq 2. \end{cases}$$

To prove the second part of Theorem 4.4, we use following point-plane incidence theorem due to Vinh ([92]).

Theorem 4.14 ([92], Theorem 5)**.** *Suppose that $\mathcal{R}$ is a collection of points in $\mathbb{F}_q^d$, and $\mathcal{S}$ is a collection of hyperplanes in $\mathbb{F}_q^d$, with $d \geq 2$. Then we have*

$$\mathcal{I}(\mathcal{R}, \mathcal{S}) := |\{(p, \pi) : p \in \mathcal{R}, \pi \in \mathcal{S}\}| \ll \frac{|\mathcal{R}||\mathcal{S}|}{q} + q^{(d-1)/2}|\mathcal{R}|^{1/2}|\mathcal{S}|^{1/2}.$$

Using Theorem 5.8 and the argument in [82], we are now ready to give a proof of Theorem 4.4.

Proof of Theorem 4.4: Since $\max_{(u,v,w)\in\mathcal{U}\times\mathcal{V}\times\mathcal{W}} |\beta_{uvw}| \leq 1$, we have

$$|S_\chi(\mathcal{T},\mathcal{U},\mathcal{V},\mathcal{W},\alpha,\beta,f)| \leq \sum_{u\in\mathcal{U},v\in\mathcal{V},w\in\mathcal{W}} \left|\sum_{t\in\mathcal{T}} \alpha_t \chi(t+f(u,v,w))\right|.$$

For $\lambda \in \mathbb{F}_p$, let $N(\mathcal{U},\mathcal{V},\mathcal{W},\lambda)$ be the number of solutions of the equation

$$f(u,v,w) = \lambda,$$

with $(u,v,w) \in \mathcal{U}\times\mathcal{V}\times\mathcal{W}$. One can check that

$$\sum_{\lambda\in\mathbb{F}_p} N(\mathcal{U},\mathcal{V},\mathcal{W},\lambda) = UVW,$$

and

$$\sum_{\lambda\in\mathbb{F}_p} N(\mathcal{U},\mathcal{V},\mathcal{W},\lambda)^2 = E,$$

where E is the number of tuples $(u,v,w,u',v',w') \in (\mathcal{U}\times\mathcal{V}\times\mathcal{W})^2$ such that $f(u,v,w) = f(u',v',w')$.

Thus we have

$$|S_\chi(\mathcal{T},\mathcal{U},\mathcal{V},\mathcal{W},\alpha,\beta,f)| \leq \sum_{\lambda\in\mathbb{F}_p} N(\mathcal{U},\mathcal{V},\mathcal{W},\lambda) \left|\sum_{t\in\mathcal{T}} \alpha_t \chi(t+\lambda)\right|.$$

Using the Hölder inequality, we have

$$|S_\chi(\mathcal{T},\mathcal{U},\mathcal{V},\mathcal{W},\alpha,\beta,f)|^{2n} \leq \left(\sum_{\lambda\in\mathbb{F}_p}\left|\sum_{t\in\mathcal{T}}\alpha_t\chi(t+\lambda)\right|^{2n}\right)\cdot\left(\sum_{\lambda\in\mathbb{F}_p}N(\mathcal{U},\mathcal{V},\mathcal{W},\lambda)^{\frac{2n}{2n-1}}\right)^{2n-1}$$

$$\leq \left(\sum_{\lambda\in\mathbb{F}_p}N(\mathcal{U},\mathcal{V},\mathcal{W},\lambda)\right)^{2n-2}\cdot\left(\sum_{\lambda\in\mathbb{F}_p}N(\mathcal{U},\mathcal{V},\mathcal{W},\lambda)^2\right)\cdot\left(\sum_{\lambda\in\mathbb{F}_p}\left|\sum_{t\in\mathcal{T}}\alpha_t\chi(t+\lambda)\right|^{2n}\right)$$

$$= (UVW)^{2n-2}\cdot E\cdot\left(\sum_{\lambda\in\mathbb{F}_p}\left|\sum_{t\in\mathcal{T}}\alpha_t\chi(t+\lambda)\right|^{2n}\right).$$

It follows from Theorem 5.8 and Lemma 4.13 that if $UVW \ll p^2$, then

$$|S_\chi(\mathcal{T},\mathcal{U},\mathcal{V},\mathcal{W},\alpha,\beta,f)| \ll$$

$$(UVW)^{\frac{2n-2}{2n}}\left((UVW)^{\frac{3}{2}}+\max\{V^2W^2,V^2U^2,U^2W^2\}\right)^{\frac{1}{2n}}\cdot\begin{cases}T^{\frac{1}{2}}p^{\frac{1}{2}} & \text{if } n=1\\ Tp^{\frac{1}{4n}}+T^{\frac{1}{2}}p^{\frac{1}{2n}} & \text{if } n\geq 2.\end{cases}$$

$$\ll\left((UVW)^{1-\frac{1}{4n}}+UVW\Omega^{\frac{1}{n}}\right)\cdot\begin{cases}T^{\frac{1}{2}}p^{\frac{1}{2}} & \text{if } n=1\\ Tp^{\frac{1}{4n}}+T^{\frac{1}{2}}p^{\frac{1}{2n}} & \text{if } n\geq 2.\end{cases}$$

This completes the proof of the first part of Theorem 4.4.

Next we prove the second part of Theorem 4.4. Suppose that $UVW \gg p^2$. Instead of Rudnev's point-plane incidence theorem (Theorem 4.11), one can follow the proof of Theorem 5.8 with Vinh's point-plane incidence theorem (Theorem 4.14). Then we see that

$$E \ll (UVW)^2/p+\max\{V^2W^2,V^2U^2,U^2W^2\}.$$

With this bound of E, we have

$$|S_\chi(\mathcal{T},\mathcal{U},\mathcal{V},\mathcal{W},\alpha,\beta,f)| \ll \left(\frac{UVW}{p^{1/2n}} + UVW\Omega^{\frac{1}{n}}\right) \cdot \begin{cases} T^{\frac{1}{2}}p^{\frac{1}{2}} & \text{if } n=1 \\ Tp^{\frac{1}{4n}} + T^{\frac{1}{2}}p^{\frac{1}{2n}} & \text{if } n \geq 2, \end{cases}$$

which completes the proof of the second part of Theorem 4.4. Thus the proof of Theorem 4.4 is complete. □

4.3 Proof of Theorem 4.5

In the proof of Theorem 4.5, we make use of the following result which can be obtained by applying Theorem 5.8.

Theorem 4.15. *Let $f \in \mathbb{F}_p[x,y]$ be a quadratic polynomial that depends on each variable and that does not have the form $g(ax+by)$. For $\mathcal{U},\mathcal{V} \subset \mathbb{F}_p^*$, let E be the number of tuples $(u,v,u',v') \in (\mathcal{U}\times\mathcal{V})^2$ such that $f(u,v) = f(u',v')$. Suppose that $V^2|\mathcal{U}-\mathcal{V}| \ll p^2$. Then we have*

$$E \lesssim V|\mathcal{U}-\mathcal{V}|^{3/2} + |\mathcal{U}-\mathcal{V}|^2.$$

Proof. For any $t \in f(\mathcal{U},\mathcal{V})$, let m_t be the number of pairs $(u,v) \in \mathcal{U}\times\mathcal{V}$ such that $f(u,v) = t$. It is clear that $m_t \leq UV$ for all $t \in f(\mathcal{U},\mathcal{V})$. It follows that

$$E = \sum_{t\in f(\mathcal{U},\mathcal{V})} m_t^2 = \sum_j \sum_{t\in f(\mathcal{U},\mathcal{V}),2^j\leq m_t<2^{j+1}} m_t^2 \ll \sum_{j=0}^{\log(UV)} 2^{2j+2}k_{2^j}, \tag{4.7}$$

where k_{2^j} denotes the cardinality of the set $D_j := \{t \in f(\mathcal{U},\mathcal{V})\colon m_t \geq 2^j\}$. We now bound k_{2^j} as follows.

Let $h(x,y,z) = f(x-z,y)$. Since $f(x,y)$ is not of the form $g(ax+by)$, by a direct computation, we have $h(x,y,z)$ satisfies the conditions of Theorem 5.8. We now consider the following equation

$$h(x,y,z) = t, \tag{4.8}$$

where $x \in \mathcal{V}, z \in \mathcal{V}-\mathcal{U}, y \in \mathcal{V}, t \in D_j \subset f(\mathcal{U},\mathcal{V})$. Let $N(h)$ be the number of solutions of this equation. It is easy to see that $N(h) \geq 2^j k_{2^j} V$. By Cauchy-Schwarz inequality, we have

$$\begin{aligned} N(h) &\ll k_{2^j}^{1/2} \left|\{(x,y,z,x',y',z') \in (\mathcal{V}\times\mathcal{V}\times(\mathcal{V}-\mathcal{U}))^2 : h(x,y,z) = h(x',y',z')\}\right|^{1/2} \\ &\ll k_{2^j}^{1/2} \left(V^{3/2}|\mathcal{U}-\mathcal{V}|^{3/4} + |\mathcal{U}-\mathcal{V}|V\right), \end{aligned}$$

where the second inequality follows from Theorem 5.8 with the condition $V^2|\mathcal{U}-\mathcal{V}| \ll p^2$. Putting the lower bound and the upper bound of $N(h)$ together we get

$$2^j k_{2^j} V \ll k_{2^j}^{1/2} \left(V^{3/2}|\mathcal{U}-\mathcal{V}|^{3/4} + |\mathcal{U}-\mathcal{V}|V\right).$$

This gives us

$$k_{2^j} \ll \frac{V|\mathcal{U}-\mathcal{V}|^{3/2} + |\mathcal{U}-\mathcal{V}|^2}{2^{2j}}.$$

Combining this estimate with the inequality (4.7), we see that

$$E \ll \left(V|\mathcal{U}-\mathcal{V}|^{3/2}+|\mathcal{U}-\mathcal{V}|^2\right)\sum_{j=0}^{\log(UV)} 1 \lesssim V|\mathcal{U}-\mathcal{V}|^{3/2}+|\mathcal{U}-\mathcal{V}|^2.$$

This concludes the proof of Theorem 4.15. □

Proof of Theorem 4.5: The proof of Theorem 4.5 is similar to Theorem 4.4 except that we use Theorem 4.15 instead of Theorem 5.8. For the completeness, we will include the detailed proof here.

Since $\max_{(u,v)\in\mathcal{U}\times\mathcal{V}}|\beta_{uv}| \le 1$, we have

$$|S_\chi(\mathcal{T},\mathcal{U},\mathcal{V},\alpha,\beta,f)| \le \sum_{u\in\mathcal{U},v\in\mathcal{V},w\in\mathcal{W}}\left|\sum_{t\in\mathcal{T}}\alpha_t\chi(t+f(u,v))\right|.$$

For $\lambda\in\mathbb{F}_p$, let $N(\mathcal{U},\mathcal{V},\lambda)$ be the number of solutions of the equation

$$f(u,v)=\lambda,$$

with $(u,v)\in\mathcal{U}\times\mathcal{V}$. It is easy to see

$$\sum_{\lambda\in\mathbb{F}_p}N(\mathcal{U},\mathcal{V},\lambda)=UV, \quad \text{and} \quad \sum_{\lambda\in\mathbb{F}_p}N(\mathcal{U},\mathcal{V},\lambda)^2=E,$$

where E is defined as in Theorem 4.15. Thus we have

$$|S_\chi(\mathcal{T},\mathcal{U},\mathcal{V},\alpha,\beta,f)| \leq \sum_{\lambda\in\mathbb{F}_p} N(\mathcal{U},\mathcal{V},\lambda)\left|\sum_{t\in\mathcal{T}}\alpha_t\chi(t+\lambda)\right|.$$

Using the Hölder inequality, we have

$$\begin{aligned}
&|S_\chi(\mathcal{T},\mathcal{U},\mathcal{V},\alpha,\beta,f)|^{2n} \leq \\
&\left(\sum_{\lambda\in\mathbb{F}_p}\left|\sum_{t\in\mathcal{T}}\alpha_t\chi(t+\lambda)\right|^{2n}\right)\cdot\left(\sum_{\lambda\in\mathbb{F}_p}N(\mathcal{U},\mathcal{V},\lambda)^{\frac{2n}{2n-1}}\right)^{2n-1} \ll \\
&\left(\sum_{\lambda\in\mathbb{F}_p}N(\mathcal{U},\mathcal{V},\lambda)\right)^{2n-2}\cdot\left(\sum_{\lambda\in\mathbb{F}_p}N(\mathcal{U},\mathcal{V},\lambda)^2\right)\cdot\left(\sum_{\lambda\in\mathbb{F}_p}\left|\sum_{t\in\mathcal{T}}\alpha_t\chi(t+\lambda)\right|^{2n}\right) = \\
&(UV)^{2n-2}\cdot E\cdot\left(\sum_{\lambda\in\mathbb{F}_p}\left|\sum_{t\in\mathcal{T}}\alpha_t\chi(t+\lambda)\right|^{2n}\right).
\end{aligned}$$

By Theorem 4.15 and Lemma 4.13, we see that if $V^2|\mathcal{U}-\mathcal{V}| \sim kUV^2 \ll p^2$, then

$$\begin{aligned}
&|S_\chi(\mathcal{T},\mathcal{U},\mathcal{V},\alpha,\beta,f)| \lesssim \\
&\left(k^{\frac{3}{4n}}\cdot\frac{UV}{U^{1/4n}V^{1/2n}}+k^{\frac{1}{n}}\cdot\frac{UV}{V^{1/n}}\right)\cdot\begin{cases}T^{1/2}p^{1/2} & \text{if } n=1\\ Tp^{1/4n}+T^{1/2}p^{1/2n} & \text{if } n\geq 2.\end{cases}
\end{aligned}$$

This proves the first part of Theorem 4.5.

To prove the second part of Theorem 4.5, assume that $V^2|\mathcal{U}-\mathcal{V}| \gg p^2$. We can follow the proof of Theorem 4.15 with Vinh's point-plane incidence theorem (Theorem

4.14) to obtain $E \ll V^2|\mathcal{U}-\mathcal{V}|^2/p + |\mathcal{U}-\mathcal{V}|^2$. With this bound of E, we have

$$|S_\chi(\mathcal{T},\mathcal{U},\mathcal{V},\alpha,\beta,f)| \lesssim \left(k^{1/n}\cdot\frac{UVW}{p^{1/2n}} + k^{1/n}\cdot\frac{UVW}{V^{1/n}}\right)\cdot\begin{cases} T^{1/2}p^{1/2} & \text{if } \ n=1 \\ \\ Tp^{1/4n} + T^{1/2}p^{1/2n} & \text{if } \ n\geq 2, \end{cases}$$

which completes the proof of the second part of Theorem 4.5. $\square$

Chapter 4 is is a version of the material appearing in "*A Note on Conditional Expanders over Prime Fields*," which will appear in Discrete Mathematics. The author was the primary investigator and author of this paper.

Chapter 5

Conditional expanders over prime fields

5.1 Introduction

Let A be a set of integers. The sum and product sets are defined as follows:

$$A + A = \{a + b \colon a, b \in A\}$$

$$A \cdot A = \{ab \colon a, b \in A\}.$$

Throughout this chapter, by $X \gg Y$, we mean $X \geq C_1 Y$ for some absolute constant C_1, and $X \sim Y$ means that $X \gg Y$ and $Y \gg X$, by $X \gtrsim Y$ we mean $X \gg (\log Y)^{-C_2} Y$ for some absolute constant C_2.

Erdős and Szemerédi [27] proved that for any finite set $A \subset \mathbb{Z}$, we have

$$\max\{|A+A|, |A \cdot A|\} \gg |A|^{1+\varepsilon}$$

for some positive constant ε. In the setting of finite fields, a similar result has been derived by Bourgain, Katz, and Tao [10]. They showed that for any set $A \subset \mathbb{F}_p$, where p is a prime and $p^\delta < |A| < p^{1-\delta}$ for some $\delta > 0$, one has

$$\max\{|A+A|, |A \cdot A|\} \geq C_\delta |A|^{1+\varepsilon},$$

for some $\varepsilon = \varepsilon(\delta) > 0$. We note here that in the result of Bourgain, Katz, and Tao [10], it is difficult to determine the relation between ε and δ.

Hart, Iosevich, and Solymosi [41] developed Fourier analysis tools to obtain a bound over arbitrary finite fields that gives an explicit dependence of ε on δ as follows.

Theorem 5.1 (**Hart-Iosevich-Solymosi,** [41])**.** *Let $\mathbb{F}_q$ be an arbitrary finite field of order q, and let $A \subset \mathbb{F}_q$. Suppose $|A+A| = m$ and $|A \cdot A| = n$, then we have*

$$|A|^3 \leq \frac{cm^2 n|A|}{q} + cq^{1/2}mn, \tag{5.1}$$

for some positive constant c.

By a direct computation, Theorem 5.1 is non-trivial when $|A| \gg q^{1/2}$. For

$|A| \sim q^{7/10}$, we have the best growth

$$\max\{|A+A|, |A\cdot A|\} \gg |A|^{8/7}.$$

Using exponential sums, Garaev [33] obtained the following improvement.

Theorem 5.2 (**Garaev**, [33]). *Let $\mathbb{F}_p$ be a prime field of order p and A be a set in $\mathbb{F}_p$.*

1. *If $p^{1/2} \ll |A| \ll p^{2/3}$, then*

$$\max\{|A+A|, |A\cdot A|\} \gg \frac{|A|^2}{p^{1/2}}.$$

2. *If $|A| \gg p^{2/3}$, then*

$$\max\{|A+A|, |A\cdot A|\} \gg (p|A|)^{1/2}.$$

Hence, if $|A| = p^\alpha$, then we have

$$\max\{|A+A|, |A\cdot A|\} \gg |A|^{1+\alpha'},$$

where $\alpha' = \frac{1}{4} - \frac{1}{2}\frac{1}{\alpha} - \frac{3}{2}$. If α is very small, say $\alpha \le 18/35$, then Rudnev, Shakan, and Shkredov [72] proved the following.

Theorem 5.3 (**Rudnev-Shakan-Shkredov**, [72]). *Let $\mathbb{F}_p$ be a prime field of order p. Let A be a set in $\mathbb{F}_p$. Suppose that $|A| \ll p^{\frac{18}{35}}$, then we have*

$$\max\{|A+A|, |A \cdot A|\} \gg |A|^{1+\frac{2}{9}-o(1)}.$$

This theorem improves the earlier exponents 39/32 due to Chen, Kerr, and Mohammadi [19] and 6/5 due to Roche-Newton, Rudnev, and Shkredov [70]. Let $\mathbb{F}_p$ be a prime field. A polynomial $f(x,y) \in \mathbb{F}_p[x,y]$ is *degenerate* if it is of the form $Q(L(x,y))$ where Q is a one-variable polynomial and L is a linear form in x and y.

A more general statement of Theorem 5.2 has been established by Vu [94]. In particular, let $f(x,y)$ be a non-degenerate polynomial of degree d in $\mathbb{F}_p[x,y]$, and A a set in $\mathbb{F}_p$, we have

$$\max\{|A+A|, |f(A,A)|\} \gg \min\left\{\frac{|A|^{3/2}}{dp^{1/4}}, \frac{p^{1/3}|A|^{2/3}}{d^{1/3}}\right\}.$$

This statement tells us that if the size of $A+A$ is small, then the size of $f(A,A)$ is large. Note that the non-degenerate condition of f is necessary since otherwise we might have $\max\{|A+A|, |f(A,A)|\} \sim |A|$ when A is an arithmetic progression.

In the case $f(x,y) = xy$, this result is slight weaker than Theorem 5.2. This result is only non-trivial when $|A| \geq p^{1/2}$. When $|A| < p^{1/2}$, Bukh and Tsimerman [14]

derived the following estimate for quadratic non-degenerate polynomials

$$\max\{|A+A|, |f(A,A)|\} \gg |A|^{1+\epsilon}, \tag{5.2}$$

for some $\epsilon > 0$.

This bound has been quantified and improved over the years. More precisely, Koh, Mojarrad, Pham, and Valculescu [48] proved the following theorem.

Theorem 5.4 (**Koh-Mojarrad-Pham-Valculescu**, [48])**.** *Let $\mathbb{F}_p$ be a prime field of order p, and let $f(x,y) \in \mathbb{F}_p[x,y]$ be a non-degenerate quadratic polynomial. For $A \subset \mathbb{F}_p$ with $|A| \ll p^{5/8}$, we have*

$$\max\{|A+A|, |f(A,A)|\} \gg |A|^{6/5}.$$

Notice that the case $f(x,y) = x^2 + y^2$ was first proved by Pham, Vinh and De Zeeuw in [68]. We refer the interested reader to [78] for similar results in the setting of $\mathbb{R}$.

In this thesis, we employ the theory of higher energies developed in [80, 81, 72, 77], namely E_4-*energy*, to give a better exponents as follows.

Theorem 5.5. *Let $f(x,y) \in \mathbb{F}_p[x,y]$ be a non-degenerate quadratic polynomial. For $A \subset \mathbb{F}_p$ with $|A| \ll p^{1/2}$ we have*

$$\max\{|A+A|, |f(A,A)|\} \gtrsim |A|^{\frac{6}{5}+\frac{4}{305}}.$$

As in the Euclidean setting, it is expected that when A is not too large, then $\max\{|A+A|, |f(A,A)|\} \gg |A|^{2-\epsilon}$ for any $\epsilon > 0$. We will discuss about the limitations of methods in [72, 77] for our settings in Remarks 5.2 and 5.2. We also refer the interested reader to [42] for an application of E_4-*energy* in a variant of the distance problem over prime fields.

5.2 Proof of Theorem 5.5

For $A, B \subset \mathbb{F}_p$, let $E_4^+(A,B)$ be the number of tuples $(a_1,a_2,a_3,a_4,b_1,b_2,b_3,b_4) \in A^4 \times B^4$ such that

$$a_1 - b_1 = a_2 - b_2 = a_3 - b_3 = a_4 - b_4.$$

For $A \subset \mathbb{F}_p$, we define

$$d_4^+(A) := \sup_{B \neq \emptyset} \frac{E_4^+(A,B)}{|A||B|^3}.$$

Note that $d_4^+(A) \geq \frac{E_4^+(A,A)}{|A|^4} \geq \frac{|A|^4}{|A|^4} = 1$.

It has been observed in [77] that the sup is taken over all sets B with $|B| \leq |A|^{3/2}$. Indeed, if $|B| \geq |A|^{3/2}$, then

$$d_4^+(A) = \sup_{B \neq \emptyset} \frac{E_4^+(A,B)}{|A||B|^3} \leq \frac{|A|^4|B|}{|A||B|^3} \leq 1,$$

a contradiction.

In [77], Shakan and Shkredov proved that

$$d_4^+(A) \ll \frac{|A \cdot A|^2}{|A|^2} \tag{5.3}$$

whenever $|A| \leq p^{3/5}$. They also derived the following lemma, which says that small energy implies large sumset.

Lemma 5.6 ([77])**.** *For $A \subset \mathbb{F}_p$, we have*

$$d_4^+(A) \gtrsim \frac{|A|^{48/13}}{|A+A|^{35/13}}.$$

It has been indicated in [77] that the best one can hope for the lower bound of $d_4^+(A)$ is as follows:

$$d_4^+(A) \gtrsim \frac{|A|^3}{|A+A|^2}.$$

Combining this with the bound (5.3), one gets $\max\{|A+A|, |AA|\} \gg |A|^{5/4}$. This is still far away from the conjecture. In this thesis, we will give an upper bound of $d_4^+(A)$ in terms of $|f(A,A)|$ for any non-degenerate quadratic polynomial f as follows.

Lemma 5.7. *Let $f(x,y) \in \mathbb{F}_p[x,y]$ be a non-degenerate quadratic polynomial. For $A \subset \mathbb{F}_p$ with $|A| \ll p^{1/2}$, we have*

$$d_4^+(A) \lesssim \frac{|f(A,A)|^2}{|A|^2}.$$

To prove lemma 5.7, we use the following result in [47].

Theorem 5.8 ([47]). *Let $f \in \mathbb{F}_p[x,y,z]$ be a quadratic polynomial that depends on each variable and that does not have the form $g(h(x)+k(y)+l(z))$. For $A,B,C \subset \mathbb{F}_p$ with $|A||B||C| \ll p^2$, let E be the number of tuples $(a,b,c,a',b',c') \in (A\times B\times C)^2$ such that $f(a,b,c)=f(a',b',c')$. Then we have*

$$E \ll (|A||B||C|)^{3/2} + (|A|+|B|+|C|)(|A||B||C|) + |B|^2|C|^2.$$

Proof of Lemma 5.7: Let $B \subset \mathbb{F}_p$ be a set maximizing $d_4^+(A)$. By a dyadic decomposition, there exist a number $t>0$ and a set $D_t := \{x\colon r_{A-B}(x) \geq t\}$ such that

$$E_4^+(A,B) \lesssim |D_t|t^4.$$

Without loss of generality, we assume that $f(x,y)=ax^2+by^2+cxy+dx+ey$ with $a\neq 0$. Let $f'(u,v,w) := f(u+v,w)$.

Since $f(x,y)$ is a non-degenerate polynomial, by an elementary calculation (similar to the proof of Lemma 5.1 in [48]), we have $f'(x,y,z)$ is not of the form $g'(h'(x)+k'(y)+l'(z))$ for some polynomials g',h',k',l'.

Consider the following equation

$$f'(u,v,w)=t', \tag{5.4}$$

with $u \in D_t, v \in B, w \in A, t' \in f(A,A)$.

It easy to check that the number of solutions of the equation (5.4) is at least $|D_t|t|A|$. Now by the Cauchy-Schwarz inequality, we have

$$|D_t|t|A| \ll |f(A,A)|^{1/2}E^{1/2}, \tag{5.5}$$

where E is the number of tuples $(u,v,w,u',v',w') \in (D_t \times B \times A)^2$ such that

$$f'(u,v,w) = f'(u',v',w').$$

Suppose $|D_t||A||B| \ll p^2$. We now consider the following cases:

Case 1: If $|D_t| \leq |B|$, then Theorem 5.8 with $A := D_t, B := B, C := A$ gives

$$E \ll (|D_t||B||A|)^{3/2} + (|D_t| + |B| + |A|)(|D_t||B||A|) + |B|^2|A|^2.$$

Case 2: If $|D_t| \geq |B|$, then Theorem 5.8 with $A := B, B := D_t, C := A$ gives

$$E \ll (|B||D_t||A|)^{3/2} + (|B| + |D_t| + |A|)(|B||D_t||A|) + |D_t|^2|A|^2.$$

These cases can be handled in the same way. Therefore, without loss of generality, we assume that we are in the first case, i.e. $|D_t| \leq |B|$ (i. e. $|D_t|^2|A||B| \leq |D_t|^{3/2}|A||B|^{3/2}$).

We also can assume that $|B| \leq |D_t||A|$ (i. e. $|B|^2|D_t||A| \leq |B|^{3/2}(|D_t||A|)^{3/2}$),

otherwise, using the fact that $|D_t|t \leq |D_t||A| \leq |B|$, we have

$$\frac{|D_t|t^4}{|A||B|^3} \leq \frac{|B|t^3}{|A||B|^3} \leq 1 \leq \frac{|f(A,A)|^2}{|A|^2}.$$

Similarly, we assume that $|A| \leq |D_t||B|$ (i. e. $|A|^2|D_t||B| \leq |A|^{3/2}(|D_t||B|)^{3/2}$). Furthermore, $|D_t| \leq |B|$ and $|B| \leq |A|^{3/2}$ implies that $|D_t|^5 \leq |B|^2|B|^3 \leq |A|^3|B|^3$. With these assumptions, we obtain

$$E \ll (|D_t||A||B|)^{3/2} + (|B||A|)^2.$$

Without loss of generality, let us assume $(|D_t||A||B|)^{3/2} \geq (|B||A|)^2$. (As otherwise, $|D_t|^3 \leq |B||A|$. Hence $\frac{|D_t|t^4}{|A||B|^3} \leq \frac{t^4}{|D_t|^2|B|^2} \leq \frac{t^4}{|D_t|^4} \leq 1 \leq \frac{|f(A,A)|^2}{|A|^2}$, and we are done.) Therefore,

$$|D_t|t^4 \ll \frac{|f(A,A)|^2|B|^3}{|A|},$$

and we are done by the definition of $d_4^+(A)$.

Now suppose $|D_t||A||B| \gg p^2$. We can use the point-plane incidence bound due to Vinh [92] for large sets in the proofs of Lemmas 2.2 and 2.3 in [68] to obtain an upper bound of E. More precisely, we are able to obtain the following version of Lemma 5.1 in [48] for large sets.

Lemma 5.9. *Let $\mathbb{F}_p$ be a prime field. Let $f(x,y,z) \in \mathbb{F}_p[x,y,z]$ be a quadratic polynomial that depends on each variable and is not of the form $g(h(x)+k(y)+l(z))$. Let*

$A, B, C \subset \mathbb{F}_p$, *then we have*

$$\left|\left\{(x,y,z,x',y',z') \in (A\times B\times C)^2 : f(x,y,z) = f\left(x',y',z'\right)\right\}\right| \leq \frac{(|A||B||C|)^2}{p} + p|A||B||C|.$$

. We consider the following two case Therefore, by Lemma 5.9 assuming $|D_t||A||B| \gg p^2$, we have the following upper bound on E

$$E \ll \frac{|D_t|^2|A|^2|B|^2}{p}.$$

Substituting this inequality to (5.5) we get

$$pt^2 \leq |f(A,A)||B|^2. \tag{5.6}$$

Since $|A| \leq p^{1/2}$ and $|B| \leq |A|^{3/2}$, we have

$$|B|^2|f(A,A)| \leq |A||B|^{4/3}|f(A,A)| \ll \frac{p}{|A|}\cdot|B|^{2/3}\cdot\frac{|f(A,A)|^{4/3}}{|A|^{1/3}}.$$

Therefore, it follows from (5.6) that

$$pt^2 \ll p\frac{|B|^{4/3}|f(A,A)|^{4/3}}{|A|^{4/3}}$$
$$\Rightarrow t^3 \ll \frac{|B|^2|f(A,A)|^2}{|A|^2}.$$

And, since $|D_t|t \leq |A||B|$,

$$E_4(A,B) \lesssim |D_t|t^4 = (|D_t|t)\cdot t^3 \ll |A||B|.\frac{|B|^2|f(A,A)|^2}{|A|^2} = \frac{|B|^3|f(A,A)|^2}{|A|}.$$

Theorem 5.5 follows by combining Lemma 5.6 and Lemma 5.7.

It is clear that if $f(x,y) = xy$, then Theorem 5.5 is weaker than Theorem 5.3. In our general setting, the main difficulty arises when we want to give an upper bound for $E_2^+(A, A-A)$ in terms of $|f(A,A)|$, where $E_2^+(A,B)$ is the number of tuples $(a_1,a_2,b_1,b_2) \in A^2 \times B^2$ such that $a_1 - b_1 = a_2 - b_2$. For all non-degenerate quadratic polynomials, it seems very difficult to give such an upper bound, but for some special families of polynomials it is possible. For instance, if $f(x,y) = g(x)(h(x)+y)$ is a function defined on $\mathbb{F}_p^* \times \mathbb{F}_p^*$, where $g, h\colon \mathbb{F}_p^* \to \mathbb{F}_p^*$ are arbitrary functions, then one can follow the proof of [61, Theorem 1.6] to derive the following Lemma:

Lemma 5.10. *Let $f(x,y) = g(x)(h(x)+y)$ be a function defined on $\mathbb{F}^* \times \mathbb{F}^*$, where $g, h\colon \mathbb{F}^* \to \mathbb{F}^*$ are arbitrary functions. Define $m = \mu(g)$. For any subsets $A, B, C \subset \mathbb{F}_p^*$,*

suppose that $|f(A,B)||A||C| \ll p^2$*, then we have*

$$E_2^+(B,C) \ll |A|^{-2}\left(|f(A,B)|^{3/2}|A|^{3/2}|C|^{3/2} + k|f(A,B)|A||C|\right),$$

where $k \leq \max\{|A|,|C|,|f(A,B)|\}$.

Proof. We have

$$E_2^+(B,C) = \#\{(b,c,b',c') \colon b+c = b'+c'\} \ll |A|^{-2}N,$$

where N is the number of tuples $(a,b,c,a',b',c') \in A \times B \times C \times A \times B \times C$ such that

$$g(a)^{-1} \cdot g(a)(h(a)+b) + (c - h(a)) = g(a')^{-1} \cdot g(a')(h(a')+b') + (c' - h(a')).$$

Define the point set $\mathcal{R}$ as

$$\mathcal{R} = \left\{\left(g(a)^{-1}, c - h(a), g(a')(h(a')+b')\right) : a,a' \in A, b' \in B, c \in C\right\},$$

and the collection of planes $\mathcal{S}$ as

$$\mathcal{S} = \left\{g(a)(h(a)+b)X + Y - g(a')^{-1}Z = c' - h(a') \colon a,a' \in A, b \in B, c' \in C\right\}.$$

It is clear that $|\mathcal{R}| = |\mathcal{S}| \leq |f(A,B)||A||C|$, and $E \leq I(\mathcal{R},\mathcal{S})$. To apply Theorem 4.11, we need to find an upper bound on k which is the maximum number of

collinear points in $\mathcal{R}$. The projection of $\mathcal{R}$ into the first two coordinates is the set $\mathcal{T} = \{(g(a)^{-1}, c - h(a)) : a \in A, c \in C\}$. The set $\mathcal{T}$ can be covered by at most $|A|$ lines of the form $x = g(a)^{-1}$ with $a \in A$, where each line contains $|C|$ points of $\mathcal{T}$. Therefore, a line in $\mathbb{F}^3$ contains at most $\max\{|A|, |C|\}$ points of $\mathcal{R}$, unless it is vertical, in which case it contains at most $|f(A, B)|$ points. So we get

$$k \leq \max\{|A|, |C|, |f(A, B)|\}.$$

Since $|\mathcal{R}| \ll p^2$, we can apply Theorem 4.11 to obtain

$$I(\mathcal{R}, \mathcal{S}) \leq |f(A, B)|^{3/2}|A|^{3/2}|C|^{3/2} + k|f(A, B)|A||C|. \tag{5.7}$$

This concludes the proof of the lemma. □

Chapter 5 is a version of the material appearing in "*Exponential Sum Estimates over Prime Fields*", *International Journal of Number Theory,* Vol. 16, No. 02, pp. 291-308, 2020, co-authored with Doowon Koh, and Thang Pham, and Chun-Yen Shen. The author was one of the primary investigators and authors of this paper.

Chapter 6

Moderate Expanders over Rings

6.1 Introduction

Let $\mathbb{F}_q$ be an arbitrary finite field of order q, where q is a prime power. We first recall the following definition from [38].

Let $f\colon \mathbb{F}_q^l \to \mathbb{F}_q$.

- The function f is called a strong expander with the exponent ϵ if for all $A \subset \mathbb{F}_q$ with $|A| \gg q^{1-\epsilon}$, we have $|f(A,\ldots,A)| \geq q-k$, for some fixed positive constant k.

- The function f is called a moderate expander with the exponent ϵ if for all $A \subset \mathbb{F}_q$ with $|A| \gg q^{1-\epsilon}$, we have $|f(A,\ldots,A)| \gg q$.

- The function f is called a weak expander with parameters $0 < \epsilon < 1$ and $0 < \delta < 1$ if for all $A \subset \mathbb{F}_q$ with $|A| \gg q^{1-\epsilon}$, we have $|f(A,\ldots,A)| \geq |A|^{\delta} q^{1-\delta}$.

Throughout this chapter, we use $X \ll Y$ if $X \leq CY$ for some constant $C > 0$ independent of the parameters related to X and Y, and write $X \gg Y$ for $Y \ll X$. The notation $X \sim Y$ means that both $X \ll Y$ and $Y \ll X$ hold. In addition, we use $X \lesssim Y$ to indicate that $X \ll (\log Y)^{C'} Y$ for some constant $C' > 0$.

Over the past 10 years, there has been an intensive progress on seeking moderate expanders with biggest exponents. For instance, the followings are moderate expanders with the exponent $\frac{1}{3}$: $x + yz$ [84], $x + (y-z)^2$ and $x(y+z)$ [93], $(x-y)^2 + (z-t)^2$ [18], $xy + zt$ [36], $xy + z + t$ [75]. We also know that $(x-y)(z-t)$ is a moderate expander with the exponent $\frac{1}{3}$ in [3], which has been slightly improved to $\frac{1}{3} + \frac{1}{13542}$ in [62].

Using spectral graph theory techniques, Vinh [93] proved that the polynomial $xy+(z-t)^2$ is a moderate expander with the exponent $\frac{3}{8} = \frac{1}{3}+\frac{1}{24}$. To the best knowledge of the authors, this is the only known moderate expander with the exponent $\frac{3}{8}$ over arbitrary finite fields in the literature.

In the setting of prime fields, Rudnev, Shkredov, and Stevens [73] also proved that the function $\frac{xy-z}{x-t}$ is a moderate expander with the exponent $\frac{17}{42} = \frac{1}{3} + \frac{1}{14}$ over prime fields.

In this note, we provide a large class of moderate expanders with the exponents $\frac{3}{8}$ and $\frac{5}{13}$ over arbitrary finite fields and prime fields, respectively. Our main ingredients are an energy result due to the third, fourth, sixth listed authors and Shen (2019) and a theorem on two-variable expanding functions given by Hegyvári and Hennecart (2009). Using the same approach, we derive similar results in the setting of finite local and principal rings.

We will see in our first result that there are actually many moderate expanders with the exponent $\frac{3}{8}$ over arbitrary finite fields.

Let $m(x)$ and $n(x)$ be polynomials with integer coefficients. We say that $m(x)$ and $n(x)$ are affinely independent if there is no $(\lambda, \beta) \in \mathbb{Z} \times \mathbb{Z}$ such that $m(x) = \lambda \cdot n(x) + \beta$ or $n(x) = \lambda \cdot m(x) + \beta$. Our first result is as follows.

Theorem 6.1. *Let $\mathbb{F}_q$ be an arbitrary finite field. Let $f \in \mathbb{F}_q[x, y, z]$ be a quadratic polynomial that depends on each variable and that does not have the form $g(h(x)+k(y)+l(z))$. Let $m(x)$ and $n(x)$ be affinely independent polynomials with bounded degrees. Define $Q(u, v) := m(u) + u^k n(v)$, and $F(u, v, y, z) := f(Q(u, v), y, z)$, where k is a fixed positive integer. For $A \subset \mathbb{F}_q$ with $|A| \gg q^{\frac{5}{8}}$, we have*

$$|F(A, A, A, A)| \gg q.$$

The following 4-variable polynomials are moderate expanders with the exponent $\frac{3}{8}$ over arbitrary finite fields:

$$u(u+v)y + z, \quad u(u+v) + yz, \quad u(u+v)(y+z)$$

$$y\left(u(u+v) + z\right), \quad \left(u(u+v) - y\right)^2 + z, \quad (y-z)^2 + u(u+v).$$

Proof. This follows directly from Theorem 6.1 with the following polynomials:

$xy+z,\ x+yz,\ x(y+z),\ y(x+z),\ (x-y)^2+z,\ (y-z)^2+x$, respectively. □

In the setting of prime fields, using recent new results in incidence geometry, one can prove that polynomials in Theorem 6.1 are moderate expanders with bigger exponents.

Theorem 6.2. *Let $\mathbb{F}_p$ be a prime field. Let $f \in \mathbb{F}_p[x,y,z]$ be a quadratic polynomial that depends on each variable and that does not have the form $g(h(x)+k(y)+l(z))$. Let $m(x)$ and $n(x)$ be affinely independent polynomials with bounded degrees. Define $Q(u,v) := m(u)+u^k n(v)$, and $F(u,v,y,z) := f(Q(u,v),y,z)$, where k is a fixed positive integer. For $A \subset \mathbb{F}_p$ with $|A| \gg p^{\frac{8}{13}}$, we have*

$$|F(A,A,A,A)| \gg p.$$

The following 4-variable polynomials are moderate expanders with the exponent $\frac{5}{13}$ over prime fields:

$$u(u+v)y+z, \quad u(u+v)+yz, \quad u(u+v)(y+z)$$

$$y\left(u(u+v)+z\right), \quad \left(u(u+v)-y\right)^2+z, \quad (y-z)^2+u(u+v).$$

Proof. This follows directly from Theorem 6.2 with the following polynomials:

$xy+z,\ x+yz,\ x(y+z),\ y(x+z),\ (x-y)^2+z,\ (y-z)^2+x$, respectively. □

An extension to finite local and principal rings: A ring $\mathcal{R}$ is *local* if $\mathcal{R}$ has a unique maximal ideal that contains every proper ideal of $\mathcal{R}$. A finite valuation ring $\mathcal{R}$ is a finite ring that is local and principle.

Let $\mathcal{R}$ be a finite valuation ring of order q^r, where $q = p^n$ is an odd prime number. Throughout this thesis, we assume $\mathcal{R}$ is commutative, and also it has an identity. Let $\mathcal{R}^\times$ denote the set of units in $\mathcal{R}$. Likewise, let $\mathcal{R}^0$ denote the set of non-units in $\mathcal{R}$. Since $\mathcal{R}$ has a unique maximal ideal that contains every proper ideals of $\mathcal{R}$, we have a non-unit $z \in \mathcal{R}$ so that the maximal ideal is generated by z. Let (z) denote the maximal ideal of $\mathcal{R}$. Throughout, q and r will denote the structural parameters associated to $\mathcal{R}$. For the maximal ideal (z), r is the smallest positive integer such that $z^r = 0$, and also q is the size of the residue field $\mathcal{R}/(z)$. We assume q is an odd prime number. Hence, 2 is a unit in $\mathcal{R}$. For more details on finite valuation rings, we refer the reader to [63].

Here are some examples of finite valuation rings.

(1) Finite fields $\mathbb{F}_q, q = p^n$ for some $n > 0$.

(2) Finite rings $\mathbb{Z}/p^r\mathbb{Z}$, where p is a prime.

(3) $\mathbb{F}_q[x]/\left(f^r\right)$, where $f \in \mathbb{F}_q[x]$ is an irreducible polynomial.

(4) $\mathcal{O}/\left(p^r\right)$ where $\mathcal{O}$ is the ring of integers in a number field and $p \in \mathcal{O}$ is a prime.

In general, there are many zero divisors in $\mathbb{R}$, so it seems difficult to extend Theorem 6.1 to the setting of finite valuation rings. However, we are able to put

Corollary 6.1 in this setting.

Theorem 6.3. *Let $\mathbb{R}$ be a finite valuation ring of order q^r, and A be a set in $\mathbb{R}$.*

Let $F_1(u,v,y,z) = u(u+v)y+z$, $F_2(u,v,y,z) = u(u+v)+yz$, $F_3(u,v,y,z) = u(u+v)(y+z)$, $F_4(u,v,y,z) = y\left(u(u+v)+z\right)$, $F_5(u,v,y,z) = \left(u(u+v)-y\right)^2+z$, and $F_6(u,v,y,z) = (y-z)^2+u(u+v)$. Suppose that $|A| \gg q^{\frac{8r-3}{8}}$, then, for each $i \in \{1,\dots,6\}$, we have

$$|F_i(A,A,A,A)| \gg q^r.$$

6.2 Moderate expanders over arbitrary finite fields (proof of Theorem 6.1)

Using a point-plane incidence bound due to Rudnev [71], the third, fourth, sixth listed authors and Shen [47] proved the following general theorem on the energy of a polynomial in three variables over prime fields.

Theorem 6.4 ([47])**.** *Suppose that $f \in \mathbb{F}_p[x,y,z]$ is a quadratic polynomial which depends on each variable and which does not take the form $g(h(x)+k(y)+l(z))$. For $U,V,W \subset \mathbb{F}_p^\times$ with $|U||V||W| \ll p^2$, let E be the number of tuples $(u,v,w,u',v',w') \in (U\times V\times W)^2$ such that $f(u,v,w) = f(u',v',w')$. Then we have*

$$E \ll (|U||V||W|)^{3/2} + \max\{|V|^2|W|^2, |V|^2|U|^2, |U|^2|W|^2\}.$$

One can follow the proof of this theorem in [47] identically and use Vinh's point-plane incidence bound [92] in the place of Rudnev's point-plane incidence bound and the Kövari-Sós-Turán theorem to obtain a version over arbitrary finite fields. For simplicity, we omit the proof.

Theorem 6.5. *Suppose that $f \in \mathbb{F}_q[x,y,z]$ is a quadratic polynomial which depends on each variable and which does not take the form $g(h(x)+k(y)+l(z))$. For $U,V,W \subset \mathbb{F}_q^\times$, let E be the number of tuples $(u,v,w,u',v',w') \in (U \times V \times W)^2$ such that $f(u,v,w) = f(u',v',w')$. If $|U||V||W| \geq q^2$, then*

$$E \ll \frac{|U|^2|V|^2|W|^2}{q} + \max\{|V|^2|W|^2, |V|^2|U|^2, |U|^2|W|^2\}.$$

The next corollary is a direct application of the Cauchy-Schwarz inequality and Theorem 6.5.

Suppose that $f \in \mathbb{F}_q[x,y,z]$ is a quadratic polynomial which depends on each variable and which does not take the form $g(h(x)+k(y)+l(z))$. If $U,V,W \subset \mathbb{F}_q^\times$ with $|U||V||W| \gg q^2$, then

$$|f(U,V,W)| \gg \min\left\{q,\ |U|^2,\ |V|^2,\ |W|^2\right\}.$$

Proof. By the Cauchy-Schwarz inequality, we have

$$|f(U,V,W)| \geq \frac{|U|^2|V|^2|W|^2}{E},$$

where E denotes the number of tuples $(u,v,w,u',v',w') \in (U \times V \times W)^2$ such that $f(u,v,w) = f(u',v',w')$. Hence, the corollary follows by applying Theorem 6.5 to the above inequality.

□

Let $m(x)$ and $n(x)$ be affinely independent polynomials. Suppose that the degrees of m and n are bounded. In [39], Hegyvári and Hennecart proved that the polynomial $Q(u,v) = m(u) + u^k n(v)$ is an expander. More precisely, for $A \subset \mathbb{F}_p$ with $|A| \leq p^{1-\epsilon}$ for some $0 < \epsilon < 1$, we have

$$|Q(A,A)| \gg |A|^{1+\epsilon'},$$

where $\epsilon' > 0$ depending on ϵ.

Using the point-line incidence bound for large sets over arbitrary finite fields due to Vinh [92], and the point-line incidence bound for small Cartesian product sets over prime fields due to Stevens and De Zeeuw [97], the following is a consequence of [39, Theorem 4] due to Hegyvári and Hennecart.

Lemma 6.6 ([39])**.** *Let $m(x)$ and $n(x)$ be affinely independent polynomials. Suppose that the degrees of m and n are bounded. Define $Q(u,v) := m(u) + u^k n(v)$.*

1. *For $A \subset \mathbb{F}_q$, we have*

$$|Q(A,A)| \gg \min\left\{q, \frac{|A|^2}{q^{1/2}}\right\}.$$

2. *For $A \subset \mathbb{F}_p$ with $|A| \leq p^{2/3}$, we have*

$$|Q(A,A)| \gg |A|^{5/4}.$$

We note here that if $Q(u,v) = u^2 + uv$, then Lemma 6.6 (1) was first obtained by Shkredov in [79].

We are now ready to prove Theorem 6.1.

Proof of Theorem 6.1. Since $|A| > 2$, without loss of generality, we may assume that $0 \notin A$. We define $U := \{Q(a,b) \colon a, b \in A\}$. It follows from Lemma 6.6 that

$$|U| \gg \min\left\{q, \frac{|A|^2}{q^{1/2}}\right\}.$$

Let $U^* = U \setminus \{0\}$. We also have

$$|U^*| \gg \min\left\{q, \frac{|A|^2}{q^{1/2}}\right\}.$$

When $|A| \gg q^{5/8}$, this inequality implies that $|A||A||U^*| \gg q^2$. Thus we can apply Corollary 6.2 so that

$$|F(A,A,A,A)| = |f(U,A,A)| \geq |f(U^*,A,A)| \gg \min\left\{q,\ |U^*|^2,\ |A|^2\right\} \gg q,$$

under the assumption $|A| \gg q^{5/8}$. This completes the proof of the theorem. $\square$

6.3 Moderate expanders over prime fields (proof of Theorem 6.2)

As in the previous section, the following corollary is a direct application of Theorem 6.4 and the Cauchy-Schwarz inequality.

Suppose that $f \in \mathbb{F}_p[x, y, z]$ is a quadratic polynomial which depends on each variable and which does not take the form $g(h(x) + k(y) + l(z))$. For $U, V, W \subset \mathbb{F}_p^\times$ with $|U||V||W| \ll p^2$, we have

$$|f(U, V, W)| \gg \min\left\{(|U||V||W|)^{1/2},\ |U|^2,\ |V|^2,\ |W|^2\right\}.$$

We are now ready to prove Theorem 6.2.

Proof of Theorem 6.2. Since $|A| > 2$, without loss of generality, we may assume that $0 \notin A$.

Set $U := \{Q(a, b) \colon a, b \in A\}$. It follows from Lemma 6.6 that

$$|U| \gg |A|^{5/4},$$

under the condition $|A| \leq p^{2/3}$.

Since $\frac{8}{13} \leq \frac{2}{3}$, for our purpose, there is no harm to assume that $|A| \leq p^{\frac{2}{3}}$ in the rest of the proof.

Let $U^* = U \setminus \{0\}$. We also have $|U^*| \gg |A|^{5/4}$.

Set $V = W = A$. It is not hard to see that $F(A, A, A, A) = f(U, V, W)$.

If $|U||A|^2 \gg p^2$, then it follows from Corollary 6.2 that $|F(A, A, A, A)| \gg p$ and we are done.

Therefore, we assume that $|U||A|^2 \ll p^2$, and apply Corollary 6.3 to get

$$|F(A, A, A, A)| = |f(U, V, W)| \geq |f(U^*, V, W)| \gg \min\left\{(|U^*||A|^2)^{1/2},\ |A|^2,\ |U^*|^2\right\}.$$

Using the fact that $|U^*| \gg |A|^{5/4}$, the theorem follows. □

6.4 Moderate expanders over finite valuation rings (proof of Theorem 6.3)

In order to prove Theorem 6.3, the following results play crucial roles. Recall that $\mathbb{R}$ denotes the finite valuation ring of order q^r.

The first result is a point-line incidence bound over finite valuation rings due to Pham and Vinh [67], where a line over $\mathcal{R}$ is defined of the form $ax + by + c = 0$ with $(a, b, c) \notin (\mathcal{R}^0)^3$.

Theorem 6.7. *Let P be a set of points in $\mathbb{R}^2$ and L be a set of lines in $\mathbb{R}^2$. The*

number of incidences between P and L, denoted by $I(P,L)$, satisfies

$$I(P,L) \leq \frac{|P||L|}{q^r} + q^{r-\frac{1}{2}}\sqrt{|P||L|}.$$

The second result is due to Yazici in [96].

Lemma 6.8. *Let X, Y, Z be sets in $\mathbb{R}$. We have*

$$|XY + Z| \gg \min\left\{q^r, \frac{|X||Y||Z|}{q^{2r-1}}\right\}.$$

Our next two lemmas are consequences of Theorem 6.7.

Lemma 6.9. *Let X, Y, Z be sets in $\mathbb{R}$. If $|X| \geq 2q^{r-1}$, then*

$$|X(Y + Z)| \gg \min\left\{q^r, \ \frac{|X||Y||Z|}{q^{2r-1}}\right\}.$$

Proof. Since $|X| \geq 2q^{r-1}$ and $|\mathbb{R}^0| = q^{r-1}$, without loss of generality we may assume that $X \subset \mathbb{R}^\times$. Let $T = X(Y + Z)$ and let us consider the following equation

$$y = a(x + c)$$

with $a \in X, x \in Y, c \in Z$, and $y \in T$. Let N denote the number of solutions of the

above equation. It is clear that

$$|X||Y||Z| \leq N. \tag{6.1}$$

We now find an upper bound of N. Let L be a collection of lines of the form $y = a(x+c)$ with $a \in X$ and $c \in Z$. In addition, define P as the set of points (x, y) with $x \in Y$ and $y \in T$. Since $a \in \mathbb{R}^\times$, the lines in L are distinct. It is clear that $|L| = |X||Z|$ and $|P| = |Y||T|$. It is not hard to see that $N = I(P, L)$ which is the number of incidences between L and P. Hence, using Theorem 6.7, we have

$$N \leq \frac{|X||Y||Z||T|}{q^r} + q^{r-\frac{1}{2}}\sqrt{|X||Y||Z||T|}.$$

Combining the above inequality with (6.1), we have

$$|T| = |X(Y+Z)| \gg \min\left\{q^r, \frac{|X||Y||Z|}{q^{2r-1}}\right\},$$

as required. □

Lemma 6.10. *Let X, Y, Z be sets in $\mathbb{R}$. We have*

$$|(X-Y)^2 + Z| \gg \min\left\{q^r, \frac{|X||Y||Z|}{q^{2r-1}}\right\}.$$

Notice that Lemma 6.10 will also be used to give a new distance result in the p-adic perspective in the next section.

Proof. We consider the following equation

$$(x-y)^2 + z = t,$$

where $x \in X, y \in Y, z \in Z, t \in T := (X-Y)^2 + Z$.

Let N be the number of solutions of this equation. We can see that $N \geq |X||Y||Z|$.

Define $P := X \times T$ and C being the set of curves of the form $t = (x-a)^2 + c$ with $a \in Y$ and $c \in Z$. It is clear that N is bounded by the number of incidences between points in P and curves in C.

Let φ be a map from $\mathbb{R}^2$ to $\mathbb{R}^2$, which maps the point (x,t) to $(x, t-x^2)$. It is clear that φ is a bijection. Under this map, the curve $t = (x-a)^2 + c$ in C will be sent to the line $t' = -2xa + c + a^2$. Furthermore, we also have that the number of incidences between P and C is equal to the number of incidences between the point set $\varphi(P)$ and the line set $\varphi(C)$.

Applying Theorem 6.7, we have

$$N \leq \frac{|P||C|}{q^r} + q^{\frac{2r-1}{2}}\sqrt{|P||C|},$$

where we have used the fact that $|\varphi(P)| = |P|, |\varphi(C)| = |C|$.

By using $|P| = |X||T|, |C| = |Y||Z|$, and $N \geq |X||Y||Z|$, we obtain the desired estimate. □

The following result is very important in the proof of Theorem 6.3.

Lemma 6.11. *Let A be a set in $\mathbb{R}$. Suppose that $|A| \geq 2q^{r-1}$, then we have*

$$|\{a(a+b)\colon a,b \in A\}| \gg \min\left\{q^r, \frac{|A|^2}{q^{\frac{2r-1}{2}}}\right\}.$$

Proof. Since $|A| \gg q^{r-1} = |(z)|$, we may assume that $A \subset \mathbb{R}^\times$. Let N be the size of the set $\{a^2+ab\colon a,b \in A\}$. By the Cauchy-Schwarz inequality, we have

$$N \geq \frac{|A|^4}{E},$$

where E is the number of quadruples $(a,b,a',b') \in A^4$ such that

$$a^2+ab = a'^2+a'b'.$$

Let L be the set of lines of the form $ax-a'y = a'^2-a^2$ with $a,a' \in A$, and P be the set of points (b,b') with $b,b' \in A$. It is not hard to see that $|L| = |P| = |A|^2$. We have $E = I(P,L)$.

Let L' be the subset of L that contains lines $ax-a'y = a'^2-a^2$ with $a'^2-a^2 \in \mathbb{R}^0$. Since $|\mathbb{R}^0| = q^{r-1}$ and $A \subset R^\times$, we have the number of pairs $(a,a') \in A^2$ such that $a'^2-a^2 \in \mathbb{R}^0$ is bounded by $2q^{r-1}|A|$. On the other hand, for each such pair (a,a') and each $b \in A$, the number of $b' \in A$ satisfying $a^2+ab = a'^2+a'b'$ is at most one. Thus, $I(P,L') \leq 2|A|^2q^{r-1}$.

It is not hard to check that the lines in $L \setminus L'$ are distinct.

Applying Theorem 6.7 we have

$$I(P, L \setminus L') \leq \frac{|P||L|}{q^r} + q^{r-\frac{1}{2}}\sqrt{|P||L|} = \frac{|A|^4}{q^r} + q^{r-\frac{1}{2}}|A|^2.$$

By an elementary calculation, we have

$$E = I(P, L \setminus L') + I(P, L') \ll \frac{|A|^4}{q^r} + q^{r-\frac{1}{2}}|A|^2,$$

which implies that

$$N \gg \min\left\{q^r, \frac{|A|^2}{q^{\frac{2r-1}{2}}}\right\},$$

and the theorem follows. □

We are now ready to prove Theorem 6.3.

Proof of Theorem 6.3. Since $|A| \gg q^{r-\frac{3}{8}} > |(z)| = q^{r-1}$, without loss of generality, we assume that A is a subset of $\mathbb{R}^\times$.

We now start with the case of $F_1 = u(u+v)y + z$.

Set $X = \{u(u+v) \colon u, v \in A\}, Y = Z = A$. It follows from Lemma 6.11 that

$$|X| \gg \min\left\{q^r, \frac{|A|^2}{q^{\frac{2r-1}{2}}}\right\}.$$

On the other hand, it is not hard to see that

$$|F_1(A,A,A,A)| = |XA+A|.$$

Lemma 6.8 tells us that

$$|XA+A| \gg \min\left\{q^r,\ \frac{|A|^2}{q^{r-1}},\ \frac{|A|^4}{q^{\frac{6r-3}{2}}}\right\} \gg q^r,$$

whenever $|A| \gg q^{\frac{8r-3}{8}}$. This completes the proof in the case of F_1.

For any F_i with $2 \leq i \leq 6$, the proof is almost the same as that for F_1 except that we have to use Lemma 6.9 or Lemma 6.10 instead of Lemma 6.8 with switching the roles of X, Y, and Z if necessary. □

Chapter 6 is a version of the material in "*Moderate Expanders over Rings*," co-authored with Dao Nguyen Van Anh, Le Quang Ham, Doowon Koh, Hossein Mojarrad, and Thang Pham, which has been submitted for publication. The author was one of the primary investigators and authors of this paper.

Bibliography

[1] B. Aronov, P. Erdős, W. Goddard, D. Kleitman, M. Klugerman, J. Pach, L. Schulman, Crossing families, *Combinatorica* **14** (1994), 127–134.

[2] I. Bárány, P. Valtr, A positive fraction Erdős-Szekeres theorem, *Discrete Comput. Geom.* **19** (1998), 335–342.

[3] M. Bennett, D. Hart, A. Iosevich, J. Pakianathan, M. Rudnev. Group actions and geometric combinatorics in $\mathbb{F}_q^d$, Forum Mathematicum (Vol. 29, No. 1, pp. 91-110). De Gruyter.

[4] C. T. Benson, *Minimal regular graphs of girths eight and twelve*. Canadian Journal of Mathematics **18** (1966), 1091-1094.

[5] B. Bollobas, *Modern Graph Theory*, Springer-Verlag, 1998.

[6] J. A. Bondy, and M. Simonovits, *Cycles of even length in graphs*. Journal of Combinatorial Theory, Series B 16, **2** (1974), 97-105.

[7] J. Bourgain, *On exponential sums in finite fields,* Bolyai Soc. Math. Stud., 21, János Bolyai Math. Soc., Budapest, 2010, 219–24.

[8] J. Bourgain and M. Z. Garaev, *On a variant of sum-product estimates and explicit exponential sum bounds in prime fields*, Math. Proc. Cambridge Phil. Soc., 146 (2009), 1–2.

[9] J. Bourgain and A. Glibichuk, *Exponential sum estimates over a subgroup in an arbitrary finite field*, J. DAnalyse Math., 115 (2011), 51–70.

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

[11] P. Brass, W. Moser, J. Pach, *Research Problems in Discrete Geometry*. Berlin, Germany: Springer-Verlag, 2005.

[12] W. G. Brown, *On graphs that do not contain a thomsen graph.* Canadian Mathematical Bulletin 9, **3** (1966), 281-285.

[13] B. Bukh, and A. Hubard. *Space crossing numbers.* Combin. Probab. Comput. 21, **3** (2012), 358–373.

[14] B. Bukh, J. Tsimerman, *Sumproduct estimates for rational functions*, Proceedings of the London Mathematical Society, **104**(1) (2012), 1-26.

[15] D. de. Caen, Extension of a theorem of Moon and Moser on complete subgraphs. Ars Combinatoria **16**(1983), 5–10.

[16] J. Cilleruelo, and C. Timmons, *k-fold sidon sets.* Electron. J. Combin. 21, **4**(2014), 4–12.

[17] M.C. Chang, On a question of Davenport and Lewis and new character sum bounds in finite fields, Duke Math. J. **145**(3)(2008), 409-442.

[18] J. Chapman, M. B. Erdogan, D. Hart, A. Iosevich, D. Koh, *Pinned distance sets, k-simplices, Wolffs exponent in finite fields and sum-product estimates*, Math. Z., **271**(1-2):63–93, 2012.

[19] C. Chen, B. Kerr, A. Mohammadi, *A new sum-product estimate in prime fields*, arXiv:1807.10998, 2018.

[20] E. Croot, O. Sisask, A probabilistic technique for finding almost periods of convolutions, Geom. Funct. Anal., **20:6** (2010), 1367–1396.

[21] X. Dahan, *Regular graphs of large girth and arbitrary degree.* Combinatorica 34, **4** (2014), 407-426.

[22] R. P. Dilworth, *A decomposition theorem for partially ordered sets.* Ann. of Math. (1950), 161–166.

[23] V. Dujmović, and S. Langerman, *A center transversal theorem for hyperplanes and applications to graph drawing.* Discrete Comput. Geom. 49, *1* (2013), 74–88.

[24] P. Erdős, A. Rényi, V. and Sós, *On a problem of graph theory.* Studia Sci. Math. Hungar **1** (1966), 215-235.

[25] P. Erdős, and M. Simonovits, *Compactness results in extremal graph theory.* Combinatorica 2, **3** (1982), 275-288.

[26] P. Erdős, G. Szekeres, A combinatorial problem in geometry, *Compositio Math.* **2** (1935), 463–470.

[27] P. Erdős, E. Szemerédi, *On sums and products of integers*, Studies in Pure Mathematics. To the memory of Paul Turan, Basel: Birkhäuser Verlag, pp. 213-218, 1983.

[28] P. Erdős, and P. Turán, *On a problem of sidon in additive number theory, and on some related problems.* J. Lond. Math. Soc. (2) 1, **4** (1941), 212–215.

[29] J. Fox, M. Gromov, V. Lafforgue, A. Naor, and J. Pach, *Overlap properties of geometric expanders*. J. Reine Angew. Math. 2012, **671** (2012), 49–83.

[30] J. Fox, J. Pach, and A. Suk. *A polynomial regularity lemma for semialgebraic hypergraphs and its applications in geometry and property testing*. SIAM J. Comput. 45, **6** (2016), 2199–2223.

[31] J. B. Friedlander and H. Iwaniec, *Estimates for character sums*, Proc. Amer. Math. Soc., 119 (1993), 365–372.

[32] R. Fulek, A. Suk, On disjoint crossing families in geometric graphs, *Electronic Notes in Discrete Mathematics* **38** (2011), 367–375.

[33] M. Z. Garaev, *The sum-product estimate for large subsets of prime fields*, Proc. Amer. Math. Soc., **136**(2008), 2735–2739.

[34] J. E. Goodman and R. Pollack, Allowable sequences and order-types in discrete and computational geometry, In J. Pach editor, New Trends in Discrete and Computational Geometry, **10** (1993), Springer, Berlin etc., 103134.

[35] B. Hanson, *Estimates for characters sums with various convolutions*, Acta Arithmetica, **179**(2017), 133–146.

[36] D. Hart, A. Iosevich, *Sums and products in finite fields: an integral geometric viewpoint*. In Radon Transforms, Geometry, and Wavelets, AMS Contemporary Mathematics **464**(2008)129–136, 2008.

[37] D. Hart, A. Iosevich, D. Koh, M. Rudnev, *Averages over hyperplanes, sum-product theory in vector spaces over finite fields and the Erdős-Falconer distance conjecture*, Trans. Amer. Math. Soc., **363** (2011), 3255–3275.

[38] D. Hart, L. Li, C-Y. Shen, *Fourier analysis and expanding phenomena in finite fields*, Proceedings of the American Mathematical Society, **141**(2) (2013): 461–473.

[39] N. Hegyvári, F. Hennecart, *Explicit constructions of extractors and expanders*, Acta Arithmetica, **140** (2009), 233–249.

[40] N. Hegyvári, F. Hennecart, *Conditional expanding bounds for two-variable functions over prime fields*, European J. Combin., **34**(2013), 1365–1382.

[41] D. Hart, A. Iosevich, J. Solymosi, *Sum-product estimates in finite fields via Kloosterman sums*, Int. Math. Res. Not. **5**, (2007) Art. ID rnm007.

[42] A. Iosevich, D. Koh, T. Pham, *A new perspective on the distance problem over prime fields*, arXiv:1905.04179, 2019.

[43] A. Iosevich, B. Murphy, J. Pakianathan, *The square root law and structure of finite rings*, Moscow Journal of Combinatorics and Number Theory **7**(2017), 38–72.

[44] A. A. Karatsuba, *Distribution of power residues and non-residues in additive sequences,* Soviet Math. Dokl., **11** (1970), 235–236.

[45] A. A. Karatsuba, *The distribution of values of Dirichlet characters on additive sequences*, Soviet Math. Dokl., **44:1** (1992), 145–148.

[46] A. A. Karatsuba, *Arithmetic problems in the theory of Dirichlet char- acters*, Russ. Math. Surv., **63:4** (2008), 43–92.

[47] D. Koh, M. Mirzaei, T., Pham, C., Shen, *Exponential Sum Estimates over Prime Fields*, International Journal of Number Theory, **16** (02) (2020), 291-308.

[48] D. Koh, H. Mojarrad, T. Pham, C. Valculescu, *Four-variable expanders over the prime fields*, Proceedings of the American Mathematical Society, **146** (12) (2018), 5025–5034.

[49] T. Kovári, V. Sós, and P. Turán, *On a problem of K. Zarankiewicz.* In Colloq. Math. **1**(1954), 50–57.

[50] F. Lazebnik, and V. A. Ustimenko, *New examples of graphs without small cycles and of large size.* European Journal of Combinatorics **14**, 5 (1993), 445–460.

[51] F. Lazebnik, V.A. and Ustimenko, *Explicit construction of graphs with an arbitrary large girth and of large size.* Discrete Applied Mathematics **60**, 1-3 (1995), 275-284.

[52] F. Lazebnik, V.A. Ustimenko, and A. J. Woldar, *A new series of dense graphs of high girth.* Bulletin of the American mathematical society 32, *1* (1995), 73–79.

[53] F. Lazebnik, and J. Verstraëte. *On hypergraphs of girth*

five. Electron. J. Combin. **10** (2003), 1–25.

[54] A. Lubotzky, R. Phillips, and P. Sarnak, *Ramanujan graphs.* Combinatorica, *8* 261–277.

[55] S. Macourt, *Incidence Results and Bounds Of Trilinear and Quadrilinear Exponential Sums*, SIAM Journal on Discrete Mathematics, **32**(2) (2018): 815–825.

[56] S. Macourt, I. D. Shkredov, I. Shparlinski, *Multiplicative energy of shifted subgroups and bounds on exponential sums with trinomials in finite fields*, arXiv:1701.06192 (2017).

[57] G. A. Margulis, *Explicit constructions of graphs without short cycles and low density codes*. Combinatorica 2, **1** (1982), 71–78.

[58] J. Matoušek, *Efficient partition trees.* Discrete Comput. Geom. 8, **3** (1992), 315–334.

[59] J. Matoušek, Lectures on discrete geometry, Springer-Verlag New York, Inc., 2002.

[60] M. Mirzaei, and A. Suk, *On grids in point-line arrangements in the plane*. In 35th International Symposium on Computational Geometry, **129** (2019), 29–40.

[61] H. Mojarrad, T. Pham, *Conditional expanding bounds for two-variable functions over arbitrary fields*, Journal of Number Theory, **186** (2018), 137–146.

[62] B. Murphy, G. Petridis, *Products of Differences over Arbitrary Finite Fields*, arXiv:1705.06581 (2017).

[63] B. Nica, *Unimodular graphs and Eisenstein sums,* Journal of Algebraic Combinatorics **45**(2)(2017), 423-454.

[64] J. Pach, and P. K. Agarwal, *Combinatorial geometry*, John Wiley & Sons, **37** (2011).

[65] J. Pach, N. Rubin, G. Tardos, Planar point sets determine many pairwise crossing segments. *STOC* 2019, 1158–1166.

[66] J. Pach, J. Solymosi, Halving lines and perfect cross-matchings, *Contemporary Mathematics* **223** (1999), 245–250.

[67] T. Pham and Le Anh Vinh, *Some combinatorial number theory problems over finite valuation rings*, Illinois J. Math. Volume 61, Number 1-2 (2017), 243–257.

[68] T. Pham, L. A. Vinh, F. De Zeeuw, *Three-variable expanding polynomials and higher-dimensional distinct distances*, Combinatorica, **39**(2) (2019), 411–426.

[69] A. Pór, P. Valtr, The partitioned version of the Erdős-Szekeres theorem. Discrete and Computational Geometry, **28** (2002), no. 4, 625–637.

[70] O. Roche-Newton, M. Rudnev, and I.D. Shkredov, *New sum-product type estimates over finite fields*, Advances in Mathematics **293** (2016), 589–605.

[71] M. Rudnev, *On the number of incidences between points and planes in three dimensions*, Combinatorica, **38** (2018), no. 1, 219–254.

[72] M. Rudnev, G. Shakan, I. Shkredov, *Stronger sum-product inequalities for small sets*, arXiv:1808.08465 (2018).

[73] M. Rudnev, I. Shkredov, S. Stevens, *On the energy variant of the sum-product conjecture*, accepted in Revista Matemática Iberoamericana, 2018.

[74] I. Z. Ruzsa, *Solving a linear equation in a set of integers I.* Acta Arith. 65, **3** (1993), 259–282.

[75] A. Sárközy, *On sums and products of residues modulo p*, Acta Arith., **118** (4)(2005), 403–409,.

[76] P. Schnider, A generalization of crossing families. 33rd European Workshop on Computational Geometry (EuroCG '17), Malm, Sweden, 2017, 273–276.

[77] G. Shakan, and I. D. Shkredov, *Breaking the* $6/5$ *threshold for sums and products modulo a prime*, arXiv:1806.07091 (2018).

[78] C. Shen, *Algebraic methods in sum-product phenomena*, Israel J. Math. **188**(1) (2012), 123–130.

[79] I. D. Shkredov, *On monochromatic solutions of some nonlinear equations in* $\mathbb{Z}_p$ Mat. Zametki, **88**(4) (2010):625–634.

[80] I.D. Shkredov, *Some new results on higher energies*, Transactions of MMS, **74**(1) (2013), 35–73.

[81] I.D. Shkredov, *Energies and structure of additive sets*, Electronic Journal of Combinatorics, **21**(3) (2014), #P3.44, 1–53.

[82] I.D. Shkredov and I. Shparlinski, *On some multiple character sums*, Mathematika, **63** (2017), 553–560.

[83] I. D. Shkredov, A. Volostnov, *Sums of multiplicative characters with additive convolutions*, Proceedings of the Steklov Institute of Mathematics **296**(1) (2017): 256–269.

[84] I. E. Shparlinski, *On the solvability of bilinear equations in finite fields*, Glasg. Math. J., **50**(3):523 529, 2008.

[85] I. Shparlinski, *On sums of Kloosterman and Gauss sums*, accepted in Trans. Amer. Math. Soc., 2018.

[86] R. Singleton, *On minimal graphs of maximum even girth.* Journal of Combinatorial Theory 1, **3** (1966), 306–332.

[87] Solymosi, J. Dense arrangements are locally very dense I. SIAM J. Discrete Math. 20, 3 (2006), 623–627.

[88] S. Stevens, F. De Zeeuw, *An improved pointline incidence bound over arbitrary fields*, Bulletin of the London Mathematical Society, **49**(5) (2017), 842–858.

[89] E. Szemerédi, and W. T. Trotter, *Extremal problems in discrete geometry.* Combinatorica 3, **3-4** (1983), 381–392.

[90] P. Valtr, On mutually avoiding sets, *The Mathematics of Paul Erdős II.* Springer Berlin Heidelberg, 1997. 324–328.

[91] J. Verstraëte, *Extremal problems for cycles in graphs.* In Recent Trends in Combinatorics. Springer, (2016), 83–116.

[92] L. A. Vinh, *The Szemerédi–Trotter type theorem and the sum-product estimate in finite fields*, European Journal of Combinatorics, **32**(8) (2011): 1177–1181.

[93] L. A. Vinh, *On four-variable expanders in finite fields*, SIAM Journal on Discrete Mathematics, **27**(4)(2013): 2038-2048.

[94] V. Vu, *Sum-product estimates via directed expanders*, Math. Res. Lett. **15** (2008), no. 2, 375-388.

[95] R. Wenger, *Extremal graphs with no C_4's, C_6's, or C_{10}'s.* Journal of Combinatorial Theory, Series B 52, **1** (1991), 113–116.

[96] E. Yazici, *Sum-product type estimates for subsets of finite valuation rings*, Acta Arithmetica, **185**(1) (2018).

[97] F. de Zeeuw: *A short proof of Rudnevs point-plane incidence bound*, arXiv: 1612.02719 (2016).