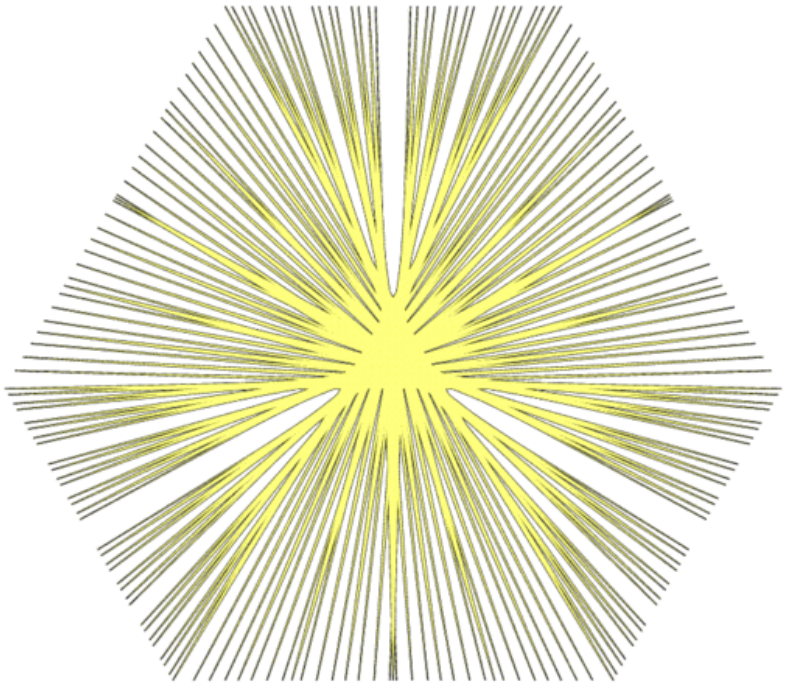
# Algebraic Methods in Combinatorics

*Directed Reading Program, Winter 2025*



*Kakeya Needle Set*

Clara Riachi and Quentin Chiari

Department of Mathematics & Statistics
McGill University

# Contents

# 1 Introduction

This report was completed at McGill University as part of a directed reading project on algebraic methods combinatorics supervised by Gabriel Crudele. The following work is a collection of proofs the authors have learned and rewritten for themselves while being introduced to this topic. This work provides examples of how tools from algebra can be employed to solve problems in combinatorics where a direct approach is possibly more complicated (see 4.2). Most of the material is from the unpublished lecture notes of Natasha Morrison [3], with the exception of the sections 4 and 5 whose contents are mostly from [2].

# 2 Graph Theory

## 2.1 Introduction to Spectral Graph Theory

**Definition 2.1.** A *graph* $G$ is a pair $(V, E)$ where $V$ is a set of vertices and $E$ contains edges between vertices, i.e. elements of the form $xy$ for $x, y \in V$. For any graph $G$ we let $G(V)$ and $G(E)$ denote its set of vertices and edges respectively. Every graph mentioned here will be finite and simple, meaning $|V(G)| < \infty$, there is at most one edge between any two vertices, and edges cannot start and end at the same vertex.

**Definition 2.2.** A graph $G$ is *connected* if there is a path in $G$ between any pair of vertices, i.e. for any $x, y \in V(G)$ there exists $i_1, i_2, ..., i_n \in V(G)$ such that $xi_1, i_1i_2, ..., i_ny \in E(G)$.

**Example 2.2.1.** A *complete graph* $K_n$ with $n$ vertices has an edge between any pair of distinct vertices.

**Example 2.2.2.** A *complete bipartite graph* $K_{a,b}$ has a vertex set $A \cup B$ where $A$ and $B$ are disjoint sets of cardinality $a$ and $b$ respectively, and has an edge $xy$ if and only if $x \in A$ and $y \in B$, or $x \in B$ and $y \in A$. We sometimes denote $K_{a,b}$ as $(A, B)$.

**Definition 2.3.** $N(x) := \{y : yx \in E(G)\}$ is the *neighborhood* of a vertex $x \in V(G)$ for a graph $G$.

**Definition 2.4.** For a graph $G$, the *degree* $d(x)$ of a vertex $x \in V(G)$ is the amount of neighbors $x$ has, meaning $d(x) = |N(x)|$. A graph is said to be *regular* or $d$-regular if every vertex has the same degree $d$.

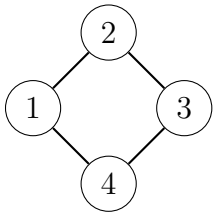



Figure 1: A cycle graph with 4 vertices.

**Definition 2.5.** The *adjacency matrix* $A(G)$ of a graph $G$ is a $|V(G)| \times |V(G)|$ matrix where relabeling the vertices to be integers from 1 to $|V(G)|$,

$$(A(G))_{ij} := \begin{cases} 1 \text{ if } ij \in E(G) \\ 0 \text{ otherwise.} \end{cases} \tag{1}$$

**Example 2.5.1.** The entries of the adjacency matrix of $K_n$ are 1 everywhere except on the diagonal since $K_n$ contains every edge $ij$ where $i \neq j$.

**Example 2.5.2.** The adjacency matrix of the bipartite graph $(\{1,2\},\{3,4\})$ is

$$\begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}.$$

**Remark 2.6.** Since simple graphs do not contain edges starting and ending at the same vertex, the diagonal of their adjacency matrix is 0. Additionally, the adjacency matrix is symmetric since containing the edge $ij$ is the same as containing the edge $ji$.

The spectrum of adjacency matrices provide information on a graph. We give the following example for intuition on dealing with eigenvalues of adjacency matrices. This way of viewing eigenvectors of adjacency matrices works for any graph, but we give a concrete example.

**Example 2.6.1.** Let $G$ be the graph in figure 1 with adjacency matrix

$$A = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}.$$

If we take a vector $x = (x_1, x_2, x_3, x_4)$ to be weights placed on the corresponding vertices of $G$, the $i$th entry of $Ax$ is the addition of weights from the neighbors of $i$ since

$$Ax = x_1 \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} + x_2 \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} + x_3 \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} + x_4 \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} x_2 + x_4 \\ x_1 + x_3 \\ x_2 + x_4 \\ x_1 + x_3 \end{bmatrix}.$$

In this interpretation, any eigenvector of $A$ is a way of distributing weights on the vertices of $G$ such that the addition of weights from neighboring vertices of a vertex is a uniform scalar multiple of the weight on that vertex. With this insight, one can see without much computation that $(1, 1, 1, 1)$ is an eigenvector of $G$, and that the unit vector is an eigenvector of the adjacency matrix for any regular graph.

**Proposition 2.7.** *Let $G$ be a graph with adjacency matrix $A$, and let $\Delta = \max_{x \in V(G)} d(x)$ be the largest degree of a vertex in $G$. Then*

*(i) If $\lambda$ is eigenvalue of $A$, $|\lambda| \leqslant \Delta$.*

*(ii) If $G$ is connected, then $\Delta$ is an eigenvalue of $A$ if and only if $G$ is regular.*

*(iii) If $G$ is connected, then $-\Delta$ is an eigenvalue of $A$ if and only if $G$ is regular and bipartite.*

*Proof.* (i) Let $v = (v_1, ..., v_n)$ be an eigenvector for $A$ with eigenvalue $\lambda$ and $i$ be such that $|v_i| = \max_{j \leqslant n} |v_j|$. Then rescaling $v$ so that $v_i = 1$ we have

$$|\lambda| = |(Av)_i| = \left| \sum_{j \in N(i)} v_j \right| \leqslant \Delta |v_i| = \Delta.$$

(ii) Suppose $G$ is connected. If $\Delta$ is an eigenvalue of $G$ with eigenvector $v = (v_1, ..., v_n)$, if we pick $i$ and rescale $v$ as in (i),

$$\Delta = (Av)_i = \sum_{j \in N(i)} v_j, \tag{2}$$

but since $1 = v_i = \max_{j \leqslant n} |v_j|$ and $|N(i)| \leqslant \Delta$, $v_j = 1$ for all $j \in N(i)$ and $d(i) = \Delta$. Applying this argument to the vertices in $N(i)$ and repeating,

since $G$ is connected we get that each vertex has degree $\Delta$ so $G$ is regular. On the other hand, if $G$ is regular then the unit vector is an eigenvector with eigenvalue $\Delta$.

(iii) Suppose $G$ is connected. If $-\Delta$ is an eigenvalue of $G$ with eigenvector $v = (v_1, ..., v_n)$, the argument in (ii) using $-\Delta$ instead of $\Delta$ in (2) gives that $v_j = -1$ for all $j \in N(i)$ and $d(i) = \Delta$. Furthermore, for $j \in N(i)$ the argument in (ii) gives that for $k \in N(j)$, $v_k = 1$ and $d(k) = \Delta$. Since $G$ is connected, we may repeat this argument to get that $G$ is regular and that for any vertex $x$, if $y \in N(x)$ then $v_y = -v_x$. Therefore letting $X = \{x : v_x = 1\}$ and $Y = \{y : v_y = -1\}$, we get that $G = (X, Y)$ so $G$ is bipartite. On the other hand, if $G = (A, B)$ is regular, $v = (v_1, ..., v_n)$ such that

$$v_i = \begin{cases} 1 \text{ if } i \in A \\ -1 \text{ if } i \in B \end{cases}$$

is an eigenvector for $A$. Indeed,

$$(Av)_i = \begin{cases} -\Delta \text{ if } i \in A \\ \Delta \text{ if } i \in B \end{cases},$$

so $v$ has eigenvalue $-\Delta$. □

**Proposition 2.8.** *Let $A$ be a real symmetric matrix and $u_1, ..., u_n$ an orthonormal eigenbasis for $A$ such that $Au_i = \lambda_i u_i$ for any $i = 1, ..., n$. Then for any $x = \sum_{i=1}^{n} c_i u_i \in \mathbb{R}^n$, we have*

$$x^T Ax = \sum_{i=1}^{n} \lambda_i c_i^2 \text{ and } x^T x = \sum_{i=1}^{n} c_i^2.$$

*Proof.*

$$\begin{aligned}
x^T Ax &= \Big(\sum_{i=1}^{n} c_i u_i^T\Big)\Big(A \cdot \sum_{j=1}^{n} c_j u_j\Big) \\
&= \Big(\sum_{i=1}^{n} c_i u_i^T\Big)\Big(\sum_{j=1}^{n} c_j A_{ij} u_j\Big) \\
&= \Big(\sum_{i=1}^{n} c_i u_i^T\Big)\Big(\sum_{j=1}^{n} c_j \lambda_j u_j\Big) \\
&= \Big(\sum_{i=1}^{n}\sum_{j=1}^{n} c_i c_j \lambda_j u_i^T u_j\Big) \\
&= \Big(\sum_{i=1}^{n}\sum_{j=1}^{n} c_i c_j \lambda_j \delta_{ij}\Big) \quad \text{since } u_i, u_j \text{ are orthonormal} \\
&= \sum_{i=1}^{n} \lambda_i c_i^2 \qquad\qquad \text{all other terms vanish for } i \neq j
\end{aligned}$$

$$\begin{aligned}
x^T x &= \Big(\sum_{i=1}^{n} c_i u_i^T\Big)\Big(\sum_{i=1}^{n} c_j u_j\Big) \\
&= \Big(\sum_{i=1}^{n}\sum_{j=1}^{n} c_i c_j \delta_{ij}\Big) \\
&= \sum_{i=1}^{n} c_i^2
\end{aligned}$$

□

**Definition 2.9.** A *decomposition* of a graph $G$ is a set of subgraphs $G_1, ..., G_k$ whose sets of edges are pairwise disjoint and $\bigcup_i G_i(E) = G$

In the following proof we see that the adjacency matrix is not the only useful matrix

**Theorem 2.1.** *(Graham-Pollak Theorem) Let $K_n$ be a complete graph with a decomposition $G_1, ..., G_k$ where each $G_t$ is a complete bipartite graph. Then $k \geqslant n - 1$.*

*Proof.* Suppose $V(K_n) = \{1, ..., n\}$ and for each $t \leqslant k$ let $G_t = (X_t, Y_t)$. Also, let $M_t$ be an $n \times n$ matrix defined by

$$(M_t)_{i,j} := \begin{cases} 1 \text{ if } i \in X_t, j \in Y_t \\ 0 \text{ otherwise} \end{cases} .$$

Note that every non-zero row of any $M_t$ is 1 where the label of the column is the same as the label of a vertex in $Y_t$, and thus they are all the same. Hence each $M_t$ has rank 1. Because $\text{rank}(A + B) \leqslant \text{rank}(A) + \text{rank}(B)$, if $n - 1 \leqslant \text{rank}(M) \leqslant k$ then we are done.

Let $M' : \mathbb{R}^n \to \mathbb{R}^{n+1}$ be obtained from adding a row of ones to $M$. Supposing towards a contradiction that $\text{rank}(M) \leqslant n - 2$, we have that $\text{rank}(M') \leqslant n - 1$, and by rank-nullity theorem $\ker(M') \geqslant 0$ so there exists a nonzero vector $x \in \mathbb{R}^n$ such that $M'x = 0$, and by considering the row of ones we see that

$$Mx = 0 \text{ and } \left( \sum_{i=1}^{n} x_i = 0 \iff J_n x = 0 \right) \tag{3}$$

where $J_n$ is the $n \times n$ matrix with 1 in every entry. Notice that for $i \neq j$, if $(M)_{i,j} = 0$ then since $K_n$ is complete and $G_1, ..., G_k$ is a decomposition, the edge $ij$ lies in some $G_t$ where $i \notin X_t$, so $(M)_{j,i} = 1$. Observing that $M + M^T = J_n - I_n$, where $I_n$ is the $n \times n$ identity matrix, the following calculation leads to a contradiction

$$\begin{aligned} 0 = x^T Mx + (Mx)^T x = x^T Mx + \left( x_1 + \begin{pmatrix} (M)_{1,1} \\ \vdots \\ (M)_{1,n} \end{pmatrix} ... + x_n \begin{pmatrix} (M)_{n,1} \\ \vdots \\ (M)_{n,n} \end{pmatrix} \right)^T \\ = x^T (M + M^T) x = x^T (J_n - I_n) x \\ = -\sum_{i=1}^{n} x_i^2 < 0, \end{aligned}$$

where the last equality comes from (3). □

## 2.2 Expander Graphs

**Definition 2.10.** A graph is said to be a $\delta$-expander if for every partition $V(G) = A \cup B$ with $|A| \leqslant |B|$, it satisfies $e(A, B) \geqslant \delta |A|$.

In other words, regardless of how one chooses to split an expander graph into two parts, there will always be a large number of edges emanating from the smaller part to the other so that one can quickly reach some part of the graph starting at any vertex.

We write $\sum_{i\sim_G j}$ to denote the sum over all edges $ij$ in $G$, where each edge contributes exactly once. That is, if the edge $(i,j)$ is in the sum, then the edge $(j,i)$ is not.

**Lemma 2.2.** *Let $G$ be an $n$-vertex $d$-regular graph whose adjacency matrix $A$ has eigenvalues $\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_n$. Then for any $x_1, \ldots, x_n \in \mathbb{R}$,*

$$\sum_{i\sim j}(x_i - x_j)^2 \leqslant (d - \lambda_n)\sum_{i=1}^{n} x_i^2 \qquad (1)$$

*Moreover, if $\sum x_i = 0$, then*

$$(d - \lambda_2)\sum_{i=1}^{n} x_i^2 \leqslant \sum_{i\sim j}(x_i - x_j)^2 \qquad (2)$$

*Proof.* (1) Let $u_1, \ldots, u_n$ be an orthonormal eigenbasis for $A$ such that $Au_i = \lambda_i u_i$ and $u_1 = \frac{1}{\sqrt{n}}(1, \ldots, 1)^T$. Note that $G$ being $d$-regular implies that we can choose the all-ones unit vector $u_1$ to be an eigenvector of $A$, and it has eigenvalue $d$. By algebraic expansion, we see that

$$\sum_{i\sim_G j}(x_i - x_j)^2 = \sum_{i\sim_G j} x_i^2 - 2\sum_{i\sim_G j} x_i x_j + \sum_{i\sim_G j} x_j^2 = d\sum_{i=1}^{n} x_i^2 - \sum_{i,j} A_{ij}x_i x_j \quad (\dagger)$$

One may ask why there is no factor of 2 in front of the $d$ coefficient when equating $\sum_{i\sim_G j} x_i^2 + \sum_{i\sim_G j} x_j^2 = d\sum_{i=1}^{n} x_i^2$. The key is that we must be consistent about what $\sum_{i\sim_G j} f(i,j)$ means when $f$ is a function that depends on only one of the indices. Define

$$\sum_{i\sim_G j} f(i,j) := \frac{1}{2}\sum_{i,j} A_{ij} f(i,j)$$

where

$$A_{ij} = \begin{cases} 1 & \text{if } (i,j) \text{ is an edge} \\ 0 & \text{otherwise} \end{cases}$$

Here each edge $\{i, j\}$ appears twice in the sum $\sum_{i,j} A_{ij} f(i, j)$: once as $(i, j)$ and once as $(j, i)$. The factor $1/2$ ensures each edge contributes exactly once. Applying this interpretation to our case, we have

$$\sum_{i \sim_G j} x_i^2 = \frac{1}{2} \sum_{i,j} A_{ij} x_i^2 = \frac{1}{2} \sum_{i=1}^{n} x_i^2 \sum_{j=1}^{n} A_{ij} = \frac{1}{2} \sum_{i=1}^{n} x_i^2 \cdot d = \frac{d}{2} \sum_{i=1}^{n} x_i^2$$

$$\sum_{i \sim_G j} x_j^2 = \frac{1}{2} \sum_{i,j} A_{ij} x_j^2 = \frac{1}{2} \sum_{j=1}^{n} x_j^2 \sum_{i=1}^{n} A_{ij} = \frac{1}{2} \sum_{j=1}^{n} x_j^2 \cdot d = \frac{d}{2} \sum_{i=1}^{n} x_i^2$$

where $\sum_{j=1}^{n} A_{ij}$ is the row sum of the $i^{th}$ row of the adjacency matrix $A$, and this sum represents the degree of vertex $i$ in the graph $G$. We can thus see why their sum only has a factor of $d$. In addition, $2 \sum_{i \sim_G j} x_i x_j = \sum_{i,j} A_{ij} x_i x_j$ By the result of (†), we notice that proving (1) can be reduced to showing that

$$\sum_{i,j} A_{ij} x_i x_j \geqslant \lambda_n \sum_{i=1}^{n} x_i^2$$

To that end, let $\mathbf{x} = (x_1, \ldots, x_n)^T = \sum_i c_i u_i$, for $c_i \in \mathbb{R}$. We have

$$\begin{aligned}
\sum_{i,j} A_{ij} x_i x_j &= x^T A x \quad \text{quadratic form} \\
&= \sum_{i=1}^{n} \lambda_i c_i^2 \quad \text{Proposition 2.8} \\
&\geqslant \lambda_n \sum_{i=1}^{n} c_i^2 \quad \lambda_n \text{ is the smallest eigenvalue} \\
&= \lambda_n x^T x \quad \text{Proposition 2.8}
\end{aligned}$$

This completes the proof of (1).
To prove (2), (†) tells us that it suffices to show

$$\sum_{i,j} A_{ij} x_i x_j \leqslant \lambda_2 x^T x$$

Suppose $\sum_{i=1}^{n} x_i = 0$. This means

$$\langle \mathbf{x}, u_1 \rangle = 0 \iff \langle c_1 u_1 + \cdots + c_n u_n, u_1 \rangle = 0 \iff c_1 = 0$$

Again, by Proposition 2.8, we have

$$\sum_{i,j} A_{ij}x_ix_j = x^TAx \overset{c_1=0}{=} \sum_{i=2}^{n} \lambda_i c_i^2 \overset{\lambda_2 \geqslant \lambda_i \forall i}{\leqslant} \lambda_2 \sum_{i=2}^{n} c_i^2 = \lambda_2 x^T x$$

which proves (2). □

**Theorem 2.3.** *Let $G$ be a $d$-regular graph with second largest eigenvalue $\lambda_2$. Then $G$ is a $\frac{d-\lambda_2}{2}$-expander.*

*Proof.* We must show for any $A, B$ that partition $V(G)$ with $|A| \leqslant |B|$, that $e(A,B) \geqslant \frac{d-\lambda_2}{2}|A|$. So let $A \cup B$ be such a partition. Then $|A| + |B| = n$. Define a vector $\mathbf{x}$ where

$$x_i = \begin{cases} n - |A| & \text{if } i \in A, \\ -|A| & \text{if } i \notin A \iff i \in B. \end{cases}$$

Consider $\sum_{i \sim_G j}(x_i - x_j)^2$. The only nonzero terms that contribute to the sum are those edges having one endpoint in $A$ and the other in $B$, and each such edge contributes $(x_i - x_j)^2 = (n - |A| - (-|A|))^2 = n^2$. So we can see that

$$\sum_{i \sim_G j} (x_i - x_j)^2 = n^2 e(A,B)$$

We also have

$$\sum_{i=1}^{n} x_i^2 = \sum_{i=1}^{|A|}(n-|A|)^2 + \sum_{i=|A|+1}^{n} (-|A|)^2 = |A|(n-|A|)^2 + (n-|A|)|A|^2 = |A|(n-|A|)n$$

Now observe that the sum of coordinates of $\mathbf{x}$ satisfies

$$\sum_i x_i = (n - |A|)|A| + (-|A|)(n - |A|) = 0,$$

so we can apply part (2) of Lemma 2.2 to obtain

$$\sum_{i \sim_G j} (x_i - x_j)^2 = n^2 e(A,B) \geqslant (d - \lambda_2) \sum_{i=1}^{n} x_i^2 = (d - \lambda_2)|A|(n - |A|)n.$$

Since $|A| \leqslant |B|$ and $|A| + |B| = n$, we have $|A| \leqslant n/2$ then $|B| = n - |A| \geqslant n - n/2 = n/2$, and dividing both sides by $n^2$ completes the proof. □

# 3 Discrete Geometry

## 3.1 Points on a Line

**Theorem 3.1.** *Let $k > n$ and let $A_1, ..., A_k \subseteq \{1, ..., n\}$ be non-empty. Then there exist non-empty disjoint sets $I, J \subseteq \{1, ..., k\}$ such that $\bigcup_{i \in I} A_i = \bigcup_{j \in J} A_j$.*

*Proof.* Let $S = \{v_1, ..., v_k\}$ be a collection of vectors in $\mathbb{R}^n$ such that each $v_i = (a_{i1}, ..., a_{in})$ where

$$a_{ij} = \begin{cases} 1 \text{ if } j \in A_i \\ 0 \text{ if } j \notin A_i \end{cases}.$$

Since $k > n$, $S$ is linearly dependent, so there exists $D \subseteq \{1, ..., k\}$ and a collection of $\alpha_i \in \mathbb{R}$ which are not all zero such that $\sum_{i \in D} \alpha_i v_i = 0$. We take $I := \{i : \alpha_i > 0\}$ and $J := \{j : \alpha_j > 0\}$ and observe that

$$\sum_{i \in I} \alpha_i v_i = \sum_{j \in J} (-\alpha_j) v_j.$$

Then for any $p \in \bigcup_{i \in I} A_i$, by the definition of the vectors in $S$ and the definition of $I$, the $p$th coordinate of $\sum_{i \in I} \alpha_i v_i$ is positive, and by the equation above we have that $p \in \bigcup_{j \in J} A_j$. We apply the same argument in the other direction to get that $\bigcup_{i \in I} A_i = \bigcup_{j \in J} A_j$. □

With a slightly stronger assumption, we slighlty modify this technique to get a stronger result.

**Theorem 3.2.** *Let $k > n + 1$ and let $A_1, ..., A_k \subseteq \{1, ..., n\}$ be non-empty. Then there exist non-empty disjoint sets $I, J \subseteq \{1, ..., k\}$ such that both $\bigcup_{i \in I} A_i = \bigcup_{j \in J} A_j$ and $\bigcap_{i \in I} A_i = \bigcap_{j \in J} A_j$.*

*Proof.* Let $S = \{v_1, ..., v_k\}$ be a collection of vectors in $\mathbb{R}^n$ such that each $v_i = (a_{i1}, ..., a_{in})$ where

$$a_{ij} = \begin{cases} 1 \text{ if } j \in A_i \\ 0 \text{ if } j \notin A_i \end{cases}.$$

Also, let $S' = \{u_1, ..., u_k\}$ be a collection of vectors in $\mathbb{R}^{n+1}$ where each $u_i$ is the same as $v_i$ for its $n$ first coordinates and 1 for its $n + 1$ coordinate.

Since $k > n$, $S$ is linearly dependent, so there exists $D \subseteq \{1, ..., k\}$ and a collection of $\alpha_i \in \mathbb{R}$ which are not all zero such that $\sum_{i\in D} \alpha_i v_i = 0$. We take $I := \{i : \alpha_i > 0\}$ and $J := \{j : \alpha_j > 0\}$ so using the same proof as in theorem 3.1 we have that $\bigcup_{i\in I} A_i = \bigcup_{j\in J} A_j$.

It remains to show that $\bigcap_{i\in I} A_i = \bigcap_{j\in J} A_j$. Note that $\sum_{i\in D} \alpha_i u_i = 0$, and since the last coordinate of every $u_i$ is 1, $\sum_{i\in D} \alpha_i = 0$. Hence for some $t \in \mathbb{R}$,

$$\sum_{i\in I} \alpha_i = \sum_{j\in J} (-\alpha_j) = t.$$

Then the $p$th coordinate of $\sum_{i\in I} \alpha_i v_i$ is $t$ if and only if $p \in \bigcap_{i\in I} A_i$, but $p \in \bigcap_{j\in J} A_j$ if and only if the $p$th coordinate of $\sum_{j\in J} \alpha_j v_j$ is $t$. Since if the $p$th coordinate of is $\sum_{i\in I} \alpha_i v_i$ is $t$, the same is true of $\sum_{j\in J} \alpha_j v_j$, so we have that $\bigcap_{i\in I} A_i = \bigcap_{j\in J} A_j$. □

## 3.2 Convex Geometry

**Definition 3.1.** A set $S \subseteq \mathbb{R}^n$ is *convex* if the line between any two points in $S$ lies in $S$. In other words, $S$ is convex if for any $x, y \in \mathbb{R}^n$, $tx + (1-t)y \in S$ for all $t \in [0, 1]$.

The *convex hull* of $S$, denoted $\text{conv}(S)$, is the smallest convex set containing the points of $S$. By this we mean that for any convex set $C \supseteq S$, $\text{conv}(S) \subseteq C$.

A *convex combination* of a finite set $S$ is a point of the form $\sum_{s\in S} \alpha_s s$ where $\alpha_s \geqslant 0$ for all $s \in S$ and $\sum_{s\in S} \alpha_s = 1$. A convex combination can be thought of as a weighted average of points.

**Proposition 3.2.** *For any finite set $S \subseteq \mathbb{R}^n$, conv$(S)$ is the set of all convex combinations of points in $S$, denoted cc$(S)$.*

*Proof.* For any point $s \in S$, taking $\alpha_s = 1$ we see that $s \in cc(S)$, so $S \subseteq cc(S)$. Additionally, for any $x_1 = \sum_{s\in S} \alpha_{s,1} s$ and $x_2 = \sum_{s\in S} \alpha_{s,2} s$ in $cc(S)$, the points on the line $tx_1 + (1-t)x_2$ are convex combinations of $S$ for each $t \in [0, 1]$, so $cc(S)$ is convex. Indeed, for any $t \in [0, 1]$,

$$tx_1 + (1-t)x_2 = \sum_{s\in S} (t\alpha_{s,1} + (1-t)\alpha_{s,2})s,$$

$t\alpha_{s,1} + (1-t)\alpha_{s,2} \geqslant 0$ for every $s \in S$, and

$$\sum_{s\in S} (t\alpha_{s,1} + (1-t)\alpha_{s,2}) = t\sum_{s\in S} \alpha_{s,1} + (1-t)\sum_{s\in S} \alpha_{s,2} = 1.$$

It remains to show that $cc(S) \subseteq \text{conv}(S)$. Letting $S = \{s_1, ..., s_n\}$, we proceed by induction on $n$. For $n = 1$, take $\alpha_1 = 1$ so $\alpha_1 s_1 = s_1 \in S$. Assume that for $n = k - 1$, $cc(S) \subseteq S$. Let $x = \sum_{i=1}^{k} \alpha_i s_i$ be convex combination where we take without loss of generality that $\alpha_n \neq 1$. Then

$$\alpha_n = 1 - \sum_{i=1}^{n-1} \alpha_i \implies \sum_{i=1}^{n-1} \frac{\alpha_i}{1 - \alpha_n} = 1$$

and $\alpha_i/(1 - \alpha_n) \geqslant 0$ for any $i$, so by the induction hypothesis we have that

$$\sum_{i=1}^{n-1} \frac{\alpha_i}{1 - \alpha_n} s_i \in \text{conv}(S).$$

Therefore,

$$x = \sum_{i=1}^{n} \alpha_i s_i = (1 - \alpha_n) \sum_{i=1}^{n-1} \frac{\alpha_i}{1 - \alpha_n} s_i + \alpha_n s_n,$$

which is a point on a line between two points in $\text{conv}(S)$, so $x \in \text{conv}(S)$. □

**Theorem 3.3.** *(Radon) Let $A = \{x_1, ..., x_k\} \in \mathbb{R}^n$ such that $k \geqslant n + 2$, then there exist disjoint sets $I, J \subseteq \{1, ..., k\}$ such that*

$$conv(\{x_i : i \in I\}) \cap conv(\{x_j : j \in J\}) \neq \varnothing.$$

*Proof.* For each $i \in \{1, ..., k\}$ let $y_i = (x_i, 1) \in \mathbb{R}^{n+1}$. Since $k \geqslant n + 2$ we have that there exists a collection of constants $\alpha_i$ which are not all 0 such that

$$\sum_{i=1}^{k} \alpha_i y_i = 0.$$

From the last row we get that $\sum_{i=1}^{n} \alpha_i = 0$.

Let $I = \{i : a_i > 0\}$, $J = \{j : a_j < 0\}$. Then

$$\sum_{i \in I} \alpha_i y_i = \sum_{j \in J} (-\alpha_j) y_j,$$

and from the last row we may let $t := \sum_{i \in I} \alpha_i = -\sum_{j \in J} \alpha_j > 0$. Then if we drop the last entry of the $y_j$s and divide by $t$ we have that

$$p := \sum_{i \in I} \frac{\alpha_i}{t} x_i = \sum_{j \in J} \frac{-\alpha_j}{t} x_j.$$

Noting that $\sum_{i\in I}\alpha_i/t = \sum_{j\in J}(-\alpha_j)/t = 1$ and $\alpha_i/t, -\alpha_j/t > 0$ for every $i \in I$ and $j \in J$, we have that

$$p \in cc(\{x_i : i \in I\}) \cap cc(\{x_j : j \in J\}) = \text{conv}(\{x_i : i \in I\}) \cap \text{conv}(\{x_j : j \in J\}).$$

□

**Theorem 3.4.** *(Helly) Let $k \geqslant n+1$ and let $C_1, .., C_k \subseteq \mathbb{R}^n$ be convex sets such that any $n+1$ of them intersect. Then $\bigcap_{i=1}^{k} C_i \neq \varnothing$*

*Proof.* We proceed by induction on $k$. For $k = n+1$, by assumption we have that $\bigcap_{i=1}^{n+1} c_i \neq \varnothing$. Assume that for $k-1 > n+1$, the intersection of $k-1$ convex subsets of $\mathbb{R}^n$ where $n+1$ of them intersect is non-empty. Then for any $i \in \{1, ..., k\} := [k]$, there exists a point $x_i \in \bigcap_{j\in[k]\setminus\{i\}} C_j$. Therefore we may let $A = \{x_1, ..., x_k\}$ be a collection of points such that $x_i \in C_j$ for every $i \neq j$. Since $k \geqslant n+2$, by theorem 3.3 there exist disjoint sets $I, J \subseteq [k]$ such that

$$\text{conv}(\{x_i \in A : i \in I\}) \cap \text{conv}(\{x_j \in A : j \in J\})$$

contains a point $x$. By definition of $A$, for each $j \in J$, $\{x_i \in A : i \in I\} \subseteq C_j$ and since $C_j$ is convex, $\text{conv}(\{x_i \in A : i \in I\}) \subseteq C_j$. By the same argument, for each $i \in I$, $\text{conv}(\{x_j \in A : j \in J\}) \subseteq C_i$. Taking $I$ and $J$ disjoint such that $I \cup J = [k]$ does not change the theorem, and doing this we get that $x \in \bigcap_{i=1}^{k} C_i \neq \varnothing$. □

# 4 Polynomial Methods

## 4.1 Basic Results

**Lemma 4.1.** *Let $\mathbb{F}$ be a field and $f \in \mathbb{F}[x]$ a polynomial of degree at most $d$. For any $x_1 \in \mathbb{F}$ there exists a polynomial $f_1 \in \mathbb{F}[x]$ of degree at most $d-1$ and $r \in \mathbb{F}$ such that*

$$f(x) = f_1(x)(x - x_1) + r.$$

*Proof.* We proceed by induction on $d$. For $d = 0$ $f$ is constant and we take $f_1(x) = 0$ and $r = f$. Let $k \in \mathbb{N}$ assume the hypothesis holds for $k-1$. Write $f(x) = \sum_{n=1}^{k} a_n x^n$ and let $g(x) = f(x) - (x - x_1)(a_k x^{k-1})$. The terms

of degree $k$ in $g$ cancel so $g$ has degree at most $k-1$. For $x_1 \in \mathbb{F}$, by the assumption we have that there exist $g_1$ of degree at most $k-2$ and $r \in \mathbb{F}$ such that

$$g(x) = g_1(x)(x - x_1) + r.$$

Then,

$$f(x) = (g_1(x) + a_k x^{k-1})(x - x_1) + r.$$

□

**Lemma 4.2.** *Let $\mathbb{F}$ be a finite field and $f \in \mathbb{F}[x]$ a polynomial of degree at most $d$. Then if $f \in \mathbb{F}[x]$ has more than $d$ roots, it is the 0 polynomial.*

*Proof.* We proceed by induction on $d$. For $d = 0$, $f$ is constant so if it has a root $f$ must be 0. Let $k \in \mathbb{N}$ and assume the hypothesis for $d = k - 1$. Let $f$ have distinct roots $x_1, ..., x_{d+1}$. Then by lemma 4.1 we have that for $f_1$ of degree at most $d - 1$,

$$f(x) = f_1(x)(x - x_{d+1})$$

where we have $r = 0$ since $f(x_{d+1}) = 0$. Then $f_1(x)$ has roots $x_1, ..., x_d$, but by the assumption $f_1$ is the 0 polynomial hence $f$ is the zero polynomial. □

The below lemma tells us that a nonzero polynomial of small degree can't have too many zeroes:

**Lemma 4.3.** *(Schwartz-Zippel) Let $\mathbb{F}$ be a finite field with $q$ elements. A non-zero polynomial $f(x_1, ..., x_n) = \sum_{t \in \mathbb{Z}^n} c_1 x_1^{t_1} + \cdots + c_n x_n^{t_n}$ of degree at most $d$ over $\mathbb{F}_q$ has at most $dq^{n-1}$ roots.*

*Proof.* By induction on the number of variables $n$. For $n = 1$, a univariate polynomial has at most $d = dq^{1-1}$ roots over $\mathbb{F}$. So let $n > 1$ and consider a multivariate polynomial $f(x_1, ..., x_n)$ of degree at most $d$ over $\mathbb{F}$. Note that $\mathbb{F}^n = \mathbb{F}^{n-1} \times \mathbb{F}$. For $y = (x_1, ..., x_{n-1}) \in \mathbb{F}^{n-1}$ and $z \in \mathbb{F}$, write

$$f(y, z) = g_0(y) + g_1(y)z + \cdots + g_t(y)z^t$$

where each $g_i(y)$ is a polynomial in $n - 1$ variables of degree at most $d - i$ (because the degree $\deg(g_i(y)) + i$ of each term $g_i(y)z^i$ must not exceed the

degree $d$ of $f(y,z)$), $t$ is the highest power of $z$ appearing in $f(y,z)$. We now partition the roots based on (two cases) whether or not $g_t(y) = 0$ (if $g_t(y) = 0$ then $f(y,z)$ has lower degree in $z$). We have

$$\begin{aligned}|\{(y,z) \in \mathbb{F}^n : f(y,z) = 0\}| = &|\{(y,z) : f(y,z) = 0, g_t(y) = 0\}| \\ &+|\{(y,z) : f(y,z) = 0, g_t(y) \neq 0\}|\end{aligned}$$

We can upper bound the first summand:

$$|\{(y,z) : f(y,z) = 0, g_t(y) = 0\}| \leqslant q|\{y : g_t(y) = 0\}| \leqslant q(d-t)q^{n-2} = (d-t)q^{n-1}$$

by the inductive hypothesis since $g_t(y)$ is a polynomial of degree at most $d-t$ in $n-1$ variables. Also, for each $y$, $z$ has $q$ possible choices. Now, for each $y \in \mathbb{F}^{n-1}$ such that $g_t(y) \neq 0$, we have that $f(y,z)$ is a univariate nonzero polynomial of degree $t$. By the base case, it has at most $t$ roots. Thus, we obtain

$$|\{(y,z) : f(y,z) = 0 \text{ and } g_t(y) \neq 0\}| \leqslant tq^{n-1}$$

Summing the two bounds yields

$$|\{(y,z) : f(y,z) = 0 \text{ and } g_t(y) \neq 0\}| \leqslant dq^{n-1}$$

□

**Lemma 4.4.** *Let $\mathbb{F}$ be a field. The vector space $V$ of polynomials in $\mathbb{F}[x_1, ..., x_n]$ of degree at most $d$ has dimension $\binom{n+d}{n}$.*

*Proof.* A basis for $V$ consists of polynomials $x_1^{t_1}x_2^{t_2}...x_n^{t_n}$ where $\sum_{i=1}^n t_i \leqslant d$ and $t_i \geqslant 0$ for all $i$. This basis is in 1-1 correspondence with $\{t_1 + t_2 + ... + t_n : \sum_{i=1}^n t_i \leqslant d, t_i \geqslant 0\}$ which has the same cardinality as $\{t_1 + t_2 + ... + t_n + t_{n+1} : \sum_{i=1}^{n+1} t_i = d, t_i \geqslant 0\}$. We proceed by the stars and bars method. If we take $n + d$ slots and place $n$ '+' signs in them, we are left with $d$ slots within which we place bars. The number of bars between consecutive '+' signs or between '+' signs and the first and last slots corresponds to a value of $t_i$ since we have $d$ bars. For example, for $d = 6$ and $n = 3$, the string $|| + ||| + +|$ corresponds with $t_1 = 2, t_2 = 3, t_3 = 0, t_4 = 1$. Since there are $\binom{n+d}{n}$ such strings, $\dim V = \binom{n+d}{n}$. □

**Lemma 4.5.** *Let $\mathbb{F}$ be a field and let $S \subseteq \mathbb{F}^n$ such that $|S| < \binom{n+d}{n}$, then there exists a non-zero polynomial $f \in \mathbb{F}[x_1, ..., x_n]$ of degree at most $d$ which vanishes on $S$.*

*Proof.* By lemma 4.4, the vector space $V$ of polynomials in $\mathbb{F}[x_1, ..., x_n]$ of degree at most $d$ has dimension $\binom{n+d}{n}$. Let $E : V \to \mathbb{F}^{|S|}$ such that $E(f) = (f(s))_{s\in S}$. $E$ is linear since for $\alpha, \beta \in \mathbb{F}$ and $f, g \in V$ ,

$$E(\alpha f + \beta g) = (\alpha f(s) + \beta g(s))_{s\in S} = \alpha(f(s))_{s\in S} + \beta(g(s))_{s\in S}.$$

By rank-nullity theorem we have that

$$\dim V - \dim(\mathrm{Im}E) = \dim(\ker E),$$

but since $\dim(\mathrm{Im}E) \leqslant \dim \mathbb{F}^{|S|} < \binom{n+d}{n} = \dim V$, $\dim(\ker E) > 0$ so there exists a non-zero polynomial in $V$ vanishing on $S$. □

**Lemma 4.6.** *Let $\mathbb{F}$ be a finite field and $n \geqslant 2$. Then for any set $S \subseteq \mathbb{F}^n$ there exists a non-zero polynomial $f \in \mathbb{F}[x_1, ..., x_n]$ vanishing on $S$ with degree at most $n|S|^{1/n}$.*

*Proof.* Let $d \in \mathbb{N}$ such that $d \leqslant n|S|^{1/n}$ and $n|S|^{1/n} - d < 1$. Since $n \geqslant 2$ we have that $n^n > n!$, so

$$|S| < \left(\frac{d+1}{n}\right)^n < \frac{(d+n)(d+n-1)...(d+1)d!}{n!d!} = \binom{n+d}{n}.$$

Then by lemma 4.5 there exists a nonzero polynomial of degree at most $n|S|^{1/n}$ vanishing on $S$. □

## 4.2 The Finite Field Kakeya Problem

**Definition 4.1.** Let $\mathbb{F}$ be a finite field. For $a \in \mathbb{F}^n$ and $b \in \mathbb{F}^n \backslash \{0\}$ a *line* $L_{a,b} \subseteq \mathbb{F}^n$ is defined as

$$L_{a,b} := \{a + t \cdot b : t \in \mathbb{F}\}.$$

We say that $L_{a,b}$ is a line centered at $a$ with the *direction* $b$. We also let $L_x$ denote a line containing a point $x \in \mathbb{F}^n$.

**Remark 4.2.** Let $\mathbb{F}$ be a finite field. If $L_{a,b}$ and $L_{c,d}$ are distinct lines in $\mathbb{F}^n$, there is at most one point where they intersect.

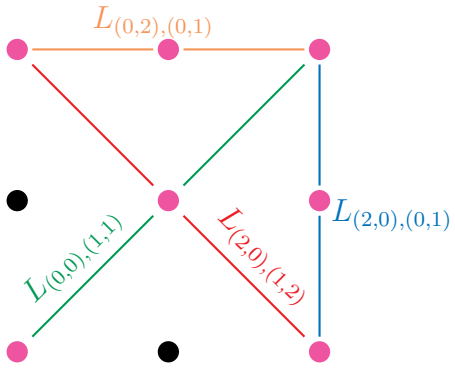



Figure 2: A Kakeya set in $\mathbb{Z}/3\mathbb{Z}^2$ colored in rhodamine where some lines it contains are colored and labeled. We have one line for each direction.

*Proof.* Suppose for contradiction that there exist two distinct points in $L_{a,b} \cap L_{c,d}$, then there exist $t_1, t_2, t_3, t_4 \in \mathbb{F}$ such that $t_1 \neq t_3$ and $t_2 \neq t_4$ where

$$\begin{cases} a + t_1 \cdot b = c + t_2 \cdot d \\ a + t_3 \cdot b = c + t_4 \cdot d \end{cases} \implies (t_2 - t_4) \cdot d = (t_1 - t_3) \cdot b \implies d = (t_1 - t_3)(t_2 - t_4)^{-1} \cdot b.$$

Letting $\lambda = (t_1 - t_3)(t_2 - t_4)^{-1}$ we have

$$a - c = t_2 \cdot d - t_1 \cdot b = (t_2\lambda - t_1) \cdot b,$$

so for any $t \in \mathbb{F}$,

$$a + t \cdot b = c + (t_2\lambda - t_1)\lambda^{-1} \cdot d + t\lambda^{-1} \cdot d = c + (t_2\lambda - t_1 + t)\lambda^{-1} \cdot d,$$

which means $L_{a,b} = L_{c,d}$, contradiction. □

**Definition 4.3.** Let $\mathbb{F}$ be a finite field. A set $K \subseteq \mathbb{F}^n$ is a *Kakeya set* if it contains a line in every direction. In other words, for every $b \in \mathbb{F}^n \backslash \{0\}$ there exists $a \in K$ such that $L_{a,b} \subseteq K$. See figure 2 for an example.

In $\mathbb{R}^n$, Kakeya sets are compact sets containing unit line segments in every direction. In [5], Wolff introduced a conjecture on the cardinality of Kakeya sets in finite fields as an analogue of the Kakeya conjecture, which asks about the size of Kakeya sets in $\mathbb{R}^n$ with respect to Hausdorff and Minkowski dimension. Several years later, Dvir resolved this conjecture in [1] by using polynomial methods. We provide some methods of obtaining bounds on the size of Kakeya sets in finite fields without the polynomial method in comparison with Dvir's proof.

**Proposition 4.4.** *(Counting Method) Let $\mathbb{F}_q$ be a finite field with $q$ elements and $K \subseteq \mathbb{F}_q^n$ a Kakeya set. Then if $n > 1$, $|K| \geqslant (1/2)q^2$.*

*Proof.* We can count the elements in $K$ as follows. For $n > 1$, we have $q$ choices for the first component of the direction of a line in $K$ so there are at least $q$ distinct lines in $K$. Pick a line in $K$, this has $q$ points, then by remark 4.2 there is another line with $q-1$ points not in the first, and repeating this till we've picked $q$ distinct lines we get that $K$ has at least $q + (q-1) + ... + 1 = (1/2)q^2$ points. □

**Proposition 4.5.** *(Bush Method) Let $\mathbb{F}_q$ be a finite field with $q$ elements and $K \subseteq \mathbb{F}_q^n$ a Kakeya set. Then $|K| \geqslant (q^n-1)^{\frac{1}{2}}$.*

*Proof.* Let $\lambda \in \mathbb{F}_q \backslash \{0\}$, then for any line $L_{a,b} \subseteq K$, we also have that $L_{a,\lambda \cdot b} = L_{a,b}$. Since we have $q^n - 1$ choices for a direction $b$ and $q-1$ directions are a scalar multiple of $b$, K contains at least $(q^n-1)/(q-1)$ distinct lines. Then, by the pigeonhole principle, there exists $x \in K$ which lies in at least $(q^n-1)(q-1)^{-1}/|K|$ distinct lines. By remark 4.2, these lines only intersect at $x$, and if there are many of these lines one may picture this as a bush. Each line through $x$ has $q-1$ points disjoint from any other line through $x$, hence

$$|K| \geqslant \frac{q^n-1}{(q-1)|K|}(q-1)+1 \implies |K|^2 \geqslant q^n - 1 \implies |K| \geqslant (q^n-1)^{\frac{1}{2}}.$$

□

**Theorem 4.7.** *(Finite Field Kakeya Theorem (Dvir)) Let $\mathbb{F}_q$ be a finite field with $q$ elements and $K \subseteq \mathbb{F}_q^n$ a Kakeya set. Then for some constant $c_n > 0$ depending only on $n$,*

$$|K| \geqslant c_n q^n.$$

*Proof.* It will suffice to prove the following claim.

**Claim 4.7.1.** *Let $f \in \mathbb{F}_q[x_1, ..., x_n]$ be a non-zero polynomial with degree at most $q-1$. Then there exists $a \in K$ such that $f(a) \neq 0$.*

We proceed by contradiction. If there exists $K$ such that $|K| < \binom{n+q-1}{n}$, then by lemma 4.5 there exists a non-zero $f \in \mathbb{F}_q[x_1, ..., x_n]$ with degree at

most $q-1$ vanishing on $K$, which contradicts claim 4.7.1. Hence we would have that

$$|K| \geqslant \binom{n+q-1}{n} = \frac{(n+q-1)(n-1+q-1)\cdot\ldots\cdot(q-1)!}{n!(q-1)!} \geqslant \frac{q^n}{n!},$$

and choosing $c_n = 1/n!$ we are done.

We now prove claim 4.7.1. Suppose that $f \in \mathbb{F}[x_1, \ldots, x_n]$ is a non-zero polynomial of degree $< q$ that vanishes on $S$. We will show that $f \equiv 0$, and thus obtain a contradiction. Let $d = \deg(f)$ and write $f = \sum_{i=0}^{d} f_i$, where for each $i$, $f_i$ is the polynomial containing all the monomials of $f$ of degree $i$. In particular, $f_d \neq 0$. For every $b \in \mathbb{F}^n \backslash \{0\}$, there exists $a = a(b) \in \mathbb{F}^n$ such that the polynomial $f(a+tb) = 0$ for all $t \in \mathbb{F}$ (as $S$ is a Kakeya set). So define $g_{a,b} : \mathbb{F} \to \mathbb{F}$ such that for $t \in \mathbb{F}$, we have $g_{a,b}(t) := f(a+tb)$. Then $g_{a,b} \in \mathbb{F}[x]$ is a polynomial of degree at most $d < q$ (by assumption) that vanishes on $\mathbb{F}$. But by lemma 4.2, $g_{a,b}(t) \equiv 0$. The coefficient of $t^d$ in $g_{a,b}(t)$ is $f_d(b)$ (check). So we have $f_d(b) = 0$ for all $b \in \mathbb{F}^n \backslash \{0\}$. So $f_d$ has at least $q^n - 1$ roots in $\mathbb{F}$. As $d < q$, we have $dq^{n-1} < q^n - 1$, and so this contradicts the Schwartz–Zippel lemma. □

Dvir's proof demonstrates how the polynomial method can provide a quick proof to a combinatorial problem which might otherwise be rather difficult.

## 4.3 The Finite Field Nikodym Problem

Closely related to Kakeya sets are Nikodym sets, which in $\mathbb{R}^2$ are subsets of the unit square with area 1 where for each point there is a line intersecting the set at only that point. Nikodym sets also have a finite field analogue. The finite field Nikodym problem asks about the size of Nikodym sets in finite field, and the method to approaching this is similar to that of the Kakeya problem.

**Definition 4.6.** Let $\mathbb{F}$ be a finite field. A set $N \subseteq \mathbb{F}^n$ is a *Nikodym set* if for each point $x \in N$ there is a line $L_x$ through $x$ such that $L_x \backslash \{x\} \subseteq N$.

The complement of a Nikodym set in $\mathbb{R}^2$ in the square has measure 0, though it is not easy to see that it must have Hausdorff dimension 2 (see chapter 9 of [4]). If one thinks about $\mathbb{F}_q^n$ as an $n$ dimensional grid with $q$ points on each side, see figure 3, a Nikodym set in $\mathbb{F}_q^n$ will be at a 'distance'

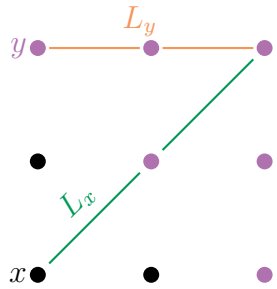



Figure 3: A Nikodym set $N$ in $\mathbb{Z}/3\mathbb{Z}^2$ colored in orchid where $x$ and $y$ are examples of points such that $L_x \backslash \{x\} \subseteq N$ and $L_y \backslash \{y\} \subseteq N$.

of at most 1 of any point in $\mathbb{F}_q^n$, and the complement of the Nikodym set will have a line through it only intersecting the complement at that point. This resembles the Euclidean version of Nikodym sets, though the condition on their size has been removed since in a finite field knowing the size of a set also reveals the size of its complement.

**Theorem 4.8.** *Let $\mathbb{F}_q$ be a finite field with $q$ elements and $N \subseteq \mathbb{F}_q^n$ a Nikodym set. Then for some constant $c_n > 0$ depending only on $n$,*

$$|N| \geqslant c_n q^n.$$

To prove this theorem, we will first need the vanishing lemma.

**Lemma 4.9.** *(Vanishing lemma) Let $\mathbb{F}$ be a finite field. If a polynomial $f \in \mathbb{F}[x_1, ..., x_n]$ of degree at most $d$ vanishes at $d+1$ points on a line, then it vanishes at all points on that line.*

*Proof of lemma 4.9.* Suppose $f \in \mathbb{F}[x_1, ..., x_n]$ of degree at most $d$ vanishes on $d+1$ points of the line $L_{a,b}$. Letting $g(t) = f(a+tb) \in \mathbb{F}[x]$ we have that $g$ is a polynomial of degree at most $d$. Since $f$ has $d+1$ roots on $L_{a,b}$, $g$ has more than $d$ roots, hence by lemma 4.2 $g$ is the zero polynomial so $f$ vanishes at all points on $L_{a,b}$. □

*Proof of theorem 4.8.* Assume by contradiction that $|N| < (10n)^{-n} q^n$. Then by lemma 4.6 there exists a non-zero polynomial $f \in \mathbb{F}[x_1, ..., x_n]$ vanishing on $N$ with degree at most $n|N|^{1/n} < 10^{-n} q < q - 1$. Then for any $x \in \mathbb{F}^n$ since $N$ is a Nikodym set there exists a line $L_x$ through $x$ such that $L_x \backslash \{x\} \subseteq N$. $f$ vanishes on the $q-1$ points of $L_x \backslash \{x\}$, so by the vanishing

lemma (lemma 4.9) $f$ vanishes on all points of $L_x$. Because $x$ was arbitrary, $f$ vanishes on all points of $\mathbb{F}_q^n$, but this alone does not guarantee that $f$ is the zero polynomial. Indeed, $x^{p-1}-1$ vanishes on $\mathbb{F}_q$ without being the zero polynomial. However, since we also know that $f$ has degree at most $q-1$, the following claim will show that $f$ is the zero polynomial, leading us to a contradiction.

**Claim 4.9.1.** *If $f \in \mathbb{F}_q[x_1, ..., x_n]$ has degree at most $q-1$ and vanishes on $\mathbb{F}_q^n$, then $f$ is the zero polynomial.*

*Proof.* We proceed by induction on n. For $n = 1$, $f$ has $q$ roots so by lemma 4.2 $f$ is the zero polynomial. For $k \in \mathbb{N}$, assume the hypothesis for $k-1$ and let $f$ of degree at most $q-1$ vanish on $\mathbb{F}_q^k$. For $x_1, ..., x_k \in \mathbb{F}$, let $F \in \mathbb{F}[x]$ such that

$$F_{x_1,..,x_k}(x_k) = f(x_1, .., x_k) = \sum_{i=1}^{q-1} g_i(x_1, .., x_{k-1}) x_k^i$$

where $x_1, ..., x_{k-1}$ are fixed and each $g_i \in \mathbb{F}[x_1, ..., x_{k-1}]$ is a polynomial of degree at most $q-1$. Since $f$ has degree at most $q-1$ and vanishes on all $q$ values of $x_k$, by lemma 4.2 $f$ is the zero polynomial. Then each $g_i$ vanishes on $\mathbb{F}_q^{k-1}$ so by the assumption they are also zero polynomials. Hence, $f$ is the 0 polynomial. □

□

# 5 Harmonic Analysis and the Kakeya Problem

## 5.1 The Loomis-Whitney Inequality

The Loomis-Whitney inequality is a combinatorial and geometric inequality about Euclidean space with many consequences in Analysis.
Let $X$ be a set of unit cubes in the unit cubical lattice in $\mathbb{R}^n$ with volume $|X|$. Let $\pi_j$ be the projection onto the coordinate hyperplane perpendicular to the $x_j$-axis. We would like to bound $|X|$ given that $\pi_j(X)$ is 'small' for all $j$. Informally, this is asking: if a set $X$ appears small when viewed from any angle, is it actually small as a whole?

**Theorem 5.1** (Loomis-Whitney)**.** *If* $|\pi_j(X)| \leqslant A$ *for all* $1 \leqslant j \leqslant n$*, then* $|X| \leqslant A^{\frac{n}{n-1}}$*.*

The original proof uses induction and Holder's inequality repeatedly to obtain the bound.
The below proof by induction does not give a sharp upper bound but is fairly straightforward and not too computational.

*Proof.* Define a column of cubes to be the set of cubes obtained by starting at any cube and taking all the cubes that lie along a line parallel to the $x_j$-axis, for some $1 \leqslant j \leqslant n$. We require the following lemma:

**Lemma 5.2.** *If* $|\pi_j(X)| \leqslant B$ *for all* $j$*, then there exists a column of cubes with between 1 and* $B^{\frac{1}{n-1}}$ *cubes of the set* $X$*.*

*Proof.* Suppose for the sake of contradiction that every column has $> B^{\frac{1}{n-1}}$ cubes of the set $X$. This implies, in particular, that there are $> B^{\frac{1}{n-1}}$ along some line parallel to the $x_1$-axis. Call this line $A_1$. If a point $p$ lies on the line $A_1$ and inside a cube of $X$, then the line passing through $p$ parallel to the $x_2$-axis must intersect $> B^{\frac{1}{n-1}}$ cubes of $X$. The plane $A_2$ containing the line $A_1$ and parallel to the $(x_1, x_2)$-plane must intersect $> (B^{\frac{1}{n-1}})^2 = B^{\frac{2}{n-1}}$ cubes of $X$. If we continue in this manner, each time sweeping along dimensions, we can find an $(n-1)$-dimensional plane $A_{n-1}$ which is parallel to the $(x_1, \cdots, x_{n-1})$-plane and intersects $> (B^{\frac{1}{n-1}})^{n-1} = B$ cubes of $X$. However, this would imply that $|\pi_n(X)| > B$, which contradicts the assumption that $|\pi_j(X)| \leqslant B$ for all $1 \leqslant j \leqslant n$. □

The Loomis-Whitney inequality then follows from this lemma by induction.

**Corollary 5.3.** *If* $\sum_j |\pi_j(X)| \leqslant B$*, then* $|X| \leqslant \sum_{b=1}^{B} b^{\frac{1}{n-1}}$*. Therefore,* $|X| \leqslant B^{\frac{n}{n-1}}$*.*

*Proof.* We prove this by induction on $B$, the total size of all projections. The base case $B = 1$ is trivial since if the sum of all projection sizes is at most 1, then $X$ can contain at most 1 cube. For the inductive step, consider the set $X$ and identify its smallest column (the column containing the fewest cubes). Let $X'$ denote the set $X$ with this smallest column completely removed. The key insight is that removing any column reduces the projection size in at least one direction. Specifically, if we remove a column parallel to

the $x_j$-axis, then $|\pi_j(X')|$ becomes strictly smaller than $|\pi_j(X)|$. Therefore, $\sum_j |\pi_j(X')| \leqslant \sum_j |\pi_j(X)| - 1 \leqslant B - 1$. By the inductive hypothesis applied to the smaller set $X'$, we have:

$$|X'| \leqslant \sum_{b=1}^{B-1} b^{\frac{1}{n-1}}$$

Now we need to account for the column we removed. By Lemma 5.2, since $\sum_j |\pi_j(X)| \leqslant B$, there exists some column containing at most $B^{\frac{1}{n-1}}$ cubes. Since we chose the smallest column to remove, it certainly contains at most $B^{\frac{1}{n-1}}$ cubes. Combining these facts:

$$|X| = |X'| + (\text{size of removed column}) \leqslant \sum_{b=1}^{B-1} b^{\frac{1}{n-1}} + B^{\frac{1}{n-1}} = \sum_{b=1}^{B} b^{\frac{1}{n-1}}$$

The final inequality $|X| \leqslant B^{\frac{n}{n-1}}$ follows because the sum $\sum_{b=1}^{B} b^{\frac{1}{n-1}}$ can be bounded by the integral $\int_1^B x^{\frac{1}{n-1}} dx$, which evaluates to approximately $\frac{n-1}{n} B^{\frac{n}{n-1}}$. □

□

# 6 Acknowledgements

We would like to thank Hazem Hassan, Sasha Bell, Yanees Dobberstein, and all those involved in organizing this semester's Directed Reading Program. We are particularly thankful for our mentor Gabriel Crudele for his guidance, insights, and passion involved in making our project a success.

# References

[1] Zeev Dvir. "On the size of Kakeya sets in finite fields." In: *Journal of the American Mathematical Society* (2009), pp. 1093–1097.

[2] Larry Guth. *Polynomial Methods in Combinatorics*. American Mathematical Society, 2016.

[3] Natasha Morrison. "Algebraic Methods in Combinatorics". Not Publically Available. 2021.

[4] Christopher D. Sogge. *Fourier Integrals in Classical Analysis (2nd ed.)* Cambridge University Press, 2017.

[5] Thomas Wolff. "Recent work connected with the Kakeya problem." In: *Prospects in mathematics : invited talks on the occasion of the 250th anniversary of Princeton university* (1999), pp. 129–162.