Discrete analogues of the Kakeya set conjecture: The cases of Finite Fields and $\mathbb{Z}/N\mathbb{Z}$ for square-free N

John Green

January 25, 2021

References

- M. Dhar, Z. Dvir. *Proof of the Kakeya set conjecture over rings of integers modulo square-free N*. arXiv:2011.11225.
- Z. Dvir, S. Kopparty, S. Saraf, M. Sudan. *Extensions to the Method of Multiplicities, with applications to Kakeya Sets and Mergers*. SIAM Journal on Computing, 2013.
- J. Hickman, J. Wright. *The Fourier Restriction and Kakeya Problems over Rings of Integers Modulo N*. Discrete Analysis, 2018.

I have also written some notes with further discussion/details, these can be found on the webpage.

Motivation (1)

Recall: A Kakeya set in $\mathbb{R}^n$ is a set K containing a line in each direction.

Conjecture

Every Kakeya set in $\mathbb{R}^n$ has Hausdorff dimension n.

Sufficient to prove that every Kakeya set has non-zero s-dimensional Hausdorff measure for each $s < n$. Would also be sufficient to prove this just for $s = n$, but this is known to be false.

Motivation (2)

Arguments using Additive Combinatorics have proven useful. This has lead to increased interest in discrete analogues, which have found interest in their own right.

We'll mostly be interested in $\mathbb{Z}/N\mathbb{Z}$. In this case Hausdorff dimension is not meaningful, so how should we replace it?

If we suppose that, independently of N, Kakeya sets K_N in $(\mathbb{Z}/N\mathbb{Z})^n$ approximate a Kakeya set K in $\mathbb{R}^n$, comparison with the Hausdorff dimension approximated at scale $1/N$ shows that the natural replacement for s-dimensional measure is $|K_N|/N^s$.

Motivation (3)

The natural analogue of the Kakeya conjecture is then:

Conjecture

For each $\varepsilon > 0$, there exists $C = C(n, \varepsilon)$ independent of N so that any Kakeya set K in $(\mathbb{Z}/N\mathbb{Z})^n$ satisfies $|K| \geq CN^{n-\varepsilon}$.

We expect to be unable to get estimates $|K| \geq C_n N^n$, but we can in the Finite Field case - we will explain why later.

Overview

- Finite Fields (Dvir, Kopparty, Saraf and Sudan)
  - Preliminaries and Polynomial method
  - Proof of the sharp result
- $\mathbb{Z}/N\mathbb{Z}$ for square-free N (Dhar and Dvir)
  - Further preliminaries and discussion
  - Proof of the main result

Finite Fields - Main Theorem

A Kakeya set K in $\mathbb{F}_q^n$ is a set for which given any non-zero vector $b \in \mathbb{F}_q^n$, there is an $a \in \mathbb{F}_q^n$ such that the line $L = \{a + tb : t \in \mathbb{F}_q\}$ is contained in K.

Theorem

If $K \subseteq \mathbb{F}_q^n$ is a Kakeya set, then $|K| \geq \frac{q^n}{(2-\frac{1}{q})^n}$.

Immediately, we have that $|K| \geq C_n |\mathbb{F}_q|^n$ for any finite field.

Notation

For multiindices $\alpha \in \mathbb{N}_0^n$ we write $|\alpha| = \alpha_1 + \ldots + \alpha_n$. Upper case X and Y will denote vectors $(x_1, \ldots, x_n)$, $(y_1, \ldots, y_m)$, etc. By X^α we mean $x_1^{\alpha_1} \ldots x_n^{\alpha_n}$.

By H_P we denote the homogeneous part of P of highest degree.

For multiindices α and β we denote

$$\binom{\alpha}{\beta} = \prod_{i=1}^{n} \binom{\alpha_i}{\beta_i}.$$

This is the coefficient of $X^\beta Y^{\alpha-\beta}$ in the expansion of $(X+Y)^\alpha$.

Hasse Derivatives - Definition

Definition

Given $P \in \mathbb{F}[X]$, the α^{th} Hasse derivative of P, denoted $P^{(\alpha)}$, is the polynomial which is the coefficient of Y^α in the expansion of $P(X+Y)$, that is,

$$P(X+Y) = \sum_\alpha P^{(\alpha)}(X) Y^\alpha.$$

The multiplicity of P at a point A, denoted $\text{mult}(P, A)$, is defined to be the largest integer M for which $P^{(\alpha)}(A) = 0$ for all α with $|\alpha| < M$. For vectors $P = (P_1, \ldots, P_m) \in \mathbb{F}[X]^m$, set $\text{mult}(P, A) = \min_i \{\text{mult}(P_i, A)\}$.

Hasse Derivatives - Properties

Proposition

Let $P, Q \in \mathbb{F}[X]$, $\alpha, \beta \in \mathbb{N}_0^n$, $\lambda, \mu \in \mathbb{F}$. *Then:*

- $P(A) = 0$ *if and only if* $mult(P, A) \geq 1$.
- $\lambda P^{(\alpha)} + \mu Q^{(\alpha)} = (\lambda P + \mu Q)^{(\alpha)}$.
- *If* P *is homogeneous of degree* d, *then* $P^{(\alpha)}$ *is homogeneous of degree* $d - |\alpha|$ *or* $P^{(\alpha)} = 0$.
- $(H_P)^{(\alpha)} = H_{P^{(\alpha)}}$ *or* $(H_P)^{(\alpha)} = 0$.
- $\left(P^{(\alpha)}\right)^{(\beta)} = \binom{\alpha}{\beta} P^{(\alpha+\beta)}$.
- *If* $A \in \mathbb{F}^n$ *is such that* $mult(P, A) = m$, *then* $mult(P^{(\alpha)}, A) \geq m - |\alpha|$.

Proofs of some statements (1)

Write $P = H_P + R$, so that $H_P^{(\alpha)} = P^{(\alpha)} - R^{(\alpha)}$.
If this is non-zero, it must be homogeneous of degree $\deg P - |\alpha|$, hence $P^{(\alpha)} - R^{(\alpha)} = H_{P^{(\alpha)} - R^{(\alpha)}}$. However, the degree of $R^{(\alpha)}$ is strictly less than $\deg P - |\alpha|$, so we must have

$$P^{(\alpha)} = P^{(\alpha)} - R^{(\alpha)} = H_{P^{(\alpha)} - R^{(\alpha)}} = H_{P^{(\alpha)}}.$$

Proofs of some statements (2)

Expand $P(X+Y+Z)$ in two different ways. Firstly,

$$\begin{aligned} P(X+(Y+Z)) &= \sum_{\alpha} P^{(\alpha)}(X)(Y+Z)^{\alpha} \\ &= \sum_{\alpha} \sum_{\beta+\gamma=\alpha} P^{(\alpha)}(X) \binom{\alpha}{\beta} Y^{\gamma} Z^{\beta} \\ &= \sum_{\beta,\gamma} P^{(\beta+\gamma)}(X) \binom{\beta+\gamma}{\beta} Y^{\gamma} Z^{\beta}. \end{aligned}$$

Also, we may write

$$P((X+Y)+Z) = \sum_{\beta} P^{(\beta)}(X+Y) Z^{\beta} = \sum_{\beta} \sum_{\gamma} \left(P^{(\beta)}\right)^{(\gamma)} (X) Y^{\gamma} Z^{\beta}.$$

Multiplicities under composition (1)

Given $P \in \mathbb{F}[X]^m, Q \in \mathbb{F}[Y]^n$, consider the polynomial $P(Q(Y))$. We have:

Proposition

For any A, $mult(P \circ Q, A) \geq mult(P, Q(A)) mult(Q - Q(A), A)$. In particular, since $mult(Q - Q(A), A) \geq 1$, we have $mult(P \circ Q, A) \geq mult(P, Q(A))$.

Let $m_1 = \text{mult}(P, Q(A))$ and $m_2 = \text{mult}(Q - Q(A), A)$. Note that $m_2 \geq 1$. If $m_1 = 0$ we are done, so assume $m_1 \geq 1$, so that $P(Q(A)) = 0$.

Multiplicities under composition (2)

$$
\begin{aligned}
P(Q(A+Y)) &= P\left(Q(A) + \sum_{\alpha \neq 0} Q^{(\alpha)}(A) Y^{\alpha}\right) \\
&= P\left(Q(A) + \sum_{|\alpha| \geq m_2} Q^{(\alpha)}(A) Y^{\alpha}\right) \\
&= P\left(Q(A) + R(Y)\right) \\
&= P(Q(A)) + \sum_{\beta \neq 0} P^{(\beta)}(Q(A)) R(Y)^{\beta} \\
&= \sum_{|\beta| \geq m_1} P^{(\beta)}(Q(A)) R(Y)^{\beta}
\end{aligned}
$$

Each Y^{α} in R has $|\alpha| \geq m_2$, and $R(Y)$ is raised β with $\beta \geq m_1$, so we conclude that $P(Q(A+Y))$ is of the form $\sum_{|\gamma| \geq m_1 m_2} c_{\gamma} Y^{\gamma}$.

Multiplicities under composition (3)

Corollary

For $A, B \in \mathbb{F}^n$, the single variable polynomial $P_{A,B}(T) := P(A + TB)$ has $mult(P_{A,B}, t) \geq mult(P, A + tB)$ for each $t \in \mathbb{F}$.

The strengthened Schwartz-Zippel lemma (1)

Lemma

Let $P \in \mathbb{F}[X]$ be a non-zero polynomial of degree at most d. Then for any finite $S \subseteq \mathbb{F}$, we have

$$\sum_{A \in S^n} mult(P, A) \leq d|S|^{n-1}.$$

Proof (1/4).

We induct on n. For $n = 1$, we must show that the sum of multiplicities at each point of S is at most d. It is enough to show that if $\text{mult}(P, A) = m$ then $(X - A)^m$ divides P. We have $P(A + Y) = \sum_\alpha P^{(\alpha)}(A) Y^\alpha$ and $P^{(\alpha)}(A) = 0$ for all $\alpha < m$. Thus Y^m divides $P(A + Y)$, and setting $Y = X - A$ concludes this case. □

The strengthened Schwartz-Zippel lemma (2)

Proof (2/4).

Suppose $n > 1$. Write

$$P(x_1, \ldots, x_n) = \sum_{j=0}^{t} P_j(x_1, \ldots, x_{n-1}) x_n^j,$$

where $0 \leq t \leq d$, P_t is non-zero and $\deg P_j \leq d - j$. For $a_1, \ldots, a_{n-1} \in S$, denote $m_{a_1,\ldots,a_{n-1}} = \mathrm{mult}(P_t, (a_1, \ldots, a_{n-1}))$. We show that

$$\sum_{a_n \in S} \mathrm{mult}(P, (a_1, \ldots, a_n)) \leq m_{a_1,\ldots,a_{n-1}} |S| + t.$$

□

The strengthened Schwartz-Zippel lemma (3)

Proof (3/4).

Let $\alpha \in \mathbb{N}_0^{n-1}$ be such that $|\alpha| = m_{a_1,\dots,a_{n-1}}$ and $P_t^{(\alpha)} \neq 0$. Then we have

$$P^{(\alpha,0)}(x_1,\dots,x_n) = \sum_{j=0}^{t} P_j^{(\alpha)}(x_1,\dots,x_{n-1})x_n^j$$

and hence $P^{(\alpha,0)}$ is non-zero (since $P_t^{(\alpha)} \neq 0$). Then

$$\begin{aligned} \mathrm{mult}(P,(a_1,\dots,a_n)) &\leq |(\alpha,0)| + \mathrm{mult}(P^{(\alpha,0)}(x_1,\dots,x_n),(a_1,\dots,a_n)) \\ &\leq m_{a_1,\dots,a_{n-1}} + \mathrm{mult}(P^{(\alpha,0)}(a_1,\dots,a_{n-1},x_n),a_n). \end{aligned}$$

Summing over $a_n \in S$, and applying the $n = 1$ case to $P^{(\alpha,0)}(a_1,\dots,a_{n-1},x_n)$ (which has degree t), we get the inequality. □

The strengthened Schwartz-Zippel lemma (4)

Proof (4/4).

We may now bound

$$\sum_{a_1,\ldots,a_n \in S} \text{mult}(P,(a_1,\ldots,a_n)) \leq \left(\sum_{a_1,\ldots,a_{n-1} \in S} m_{a_1,\ldots,a_{n-1}} \right) |S| + |S|^{n-1} t.$$

By the inductive hypothesis, the sum in brackets is bounded by $(d-t)|S|^{n-2}$, which completes the proof. □

Corollary

Let $P \in \mathbb{F}_q[X]$ be a polynomial of degree at most d. If $\sum_{A \in \mathbb{F}_q^n} \text{mult}(P,A) > dq^{n-1}$, then $P = 0$.

Polynomial method (1)

Notation. We denote the dimensions of the space of homogeneous polynomials of degree d in n variables over $\mathbb{F}$ and the space of polynomials of degree at most d in n variables by

$$\delta_{n,d} = \binom{d+n-1}{n-1} = \binom{d+n-1}{d} \text{ and } \Delta_{n,d} = \binom{d+n}{n} = \binom{d+n}{d}$$

respectively. We have:

Proposition

Given a set $K \subseteq \mathbb{F}^n$ and non-negative integers m, d such that $\Delta_{n,m-1}|K| < \Delta_{n,d}$, there exists a non-zero polynomial $P \in \mathbb{F}[X]$ of total degree at most d such that $mult(P, A) \geq m$ for every $A \in K$.

Polynomial method (2)

Proof.

For a given A, $\mathrm{mult}(P, A) \geq m$ means that the rank 1 linear function $P \mapsto P^{(\alpha)}(A) = 0$ for each multiindex α with $|\alpha| < m$. This imposes $\Delta_{n,m-1}$ linear constraints on P. Since the total number of linear constraints is $\Delta_{n,m-1}|K|$, which is strictly less than the dimension of the space of polynomials of degree at most d in n variables, so there is a non-zero polynomial of degree d vanishing to multiplicity m at every point of K. □

Proof of Finite Field bound (1)

Proof (1/4).

Let l be a large multiple of q and let $m = 2l - l/q$, $d = lq - 1$.
Note that $d < lq$ and thus $(m - l)q = ql - l > d - l$.
We will prove by contradiction that $|K| \geq \Delta_{n,d}/\Delta_{n,m-1}$, so let us assume that $\Delta_{n,m-1}|K| < \Delta_{n,d}$. By the previous proposition, there exists a non-zero polynomial $P \in \mathbb{F}[X]$ of degree $d^* \leq d$ such that $\text{mult}(P, A) \geq m$ for each $A \in K$.
Note that $d^* \geq l$ since $m \geq l$ and, since P vanishes to multiplicity m at some A but is non-zero, there must be monomials of degree greater than m in the expansion of $P(A + (X - A))$. □

Proof of Finite Field bound (2)

Proof (2/4).

We show that H_P vanishes to multiplicity l at each point $B \in \mathbb{F}_q^n$. Let α be such that $|\alpha| < l$. Denote $Q = P^{(\alpha)}$, and let $d' \leq d^* - |\alpha|$ be the degree of Q.

Pick A such that $\{A + tB : t \in \mathbb{F}_q\} \subseteq K$. Then for all $t \in \mathbb{F}_q$, $\text{mult}(Q, A + tB) \geq m - |\alpha|$.

Since $|\alpha| < l$ and $(m - l)q > d - l \geq d^* - l$, we get $(m - |\alpha|)q = (m - l)q + (|\alpha| - l)q > d^* - l + (|\alpha| - l)q = d^* - |\alpha| + (l - |\alpha|)(q - 1) > d^* - |\alpha|$.

Let $Q_{A,B}(T)$ be the polynomial $Q(A + TB)$. Then $\text{mult}(Q_{A,B}, t) \geq \text{mult}(Q, A + tB) \geq m - |\alpha|$. Since $(m - |\alpha|)q > d^* - |\alpha| \geq d' \geq \deg Q_{A,B}$, the $n = 1$ case of the corollary of the Schwartz-Zippel lemma implies $Q_{A,B} = 0$. □

Proof of Finite Field bound (3)

Proof (3/4).

Therefore the coefficient of $T^{d'}$ in $Q_{A,B}$ is 0. It is easily checked that this coefficient is equal to $H_Q(B)$, so $H_Q(B) = 0$. Thus $(H_P)^{(\alpha)}(B) = (H_Q(B) \text{ or } 0) = 0$. Since this is true for all α with $|\alpha| < l$, we have $\text{mult}(H_P, B) \geq l$. □

Proposition

If a homogeneous polynomial $P \in \mathbb{F}_q[X]$ of degree at most $lq - 1$ in n variables vanishes to multiplicity at least m at each point of a line L in direction B, then it vanishes to multiplicity at least l at B.

Proof of Finite Field bound (4)

Proof (4/4).

By the corollary of the Schwartz-Zippel lemma, noting that $lq^n > d^* q^{n-1}$, we conclude that $H_P = 0$, which in turn means $P = 0$, a contradiction. Thus

$$|K| \geq \binom{d+n}{n} / \binom{m+n-1}{n} = \binom{lq-1+n}{n} / \binom{2l-l/q+n-1}{n}$$
$$= \frac{\prod_{i=1}^{n}(lq-1+i)}{\prod_{i=1}^{n}(2l-l/q-1+i)} = \frac{\prod_{i=1}^{n}(q-1/l+i/l)}{\prod_{i=1}^{n}(2-1/q-1/l+i/l)}$$

Letting $l \to \infty$ gives the result. □

The Kakeya set bound for square-free N

Q. Why is the Finite Field bound so good?
The issue is that of the scales available in each case. In the Euclidean case, the usual distance gives a range of infinitely many scales which are ubiquitous in many arguments. In the Finite Field case, there are no natural notions of distance that provide any more scales than the trivial discrete distance. In the setting of $\mathbb{Z}/N\mathbb{Z}$, the divisors of N provide a range of scales to work with.

Theorem

Let $N = p_1 \ldots p_r$ be a square-free integer with distinct prime factors $p_1, \ldots, p_r$. Then for each Kakeya set $K \subseteq (\mathbb{Z}/N\mathbb{Z})^n$, we have

$$|K| \geq \frac{N^n}{\prod_{i=1}^{r}(2 - 1/p_i)^n}.$$

Definitions and preliminaries (1)

Let $\mathbb{PF}_q^{n-1}$ be the projective space of $\mathbb{F}_q$, the non-zero vectors identified up to scaling. A Kakeya set in $\mathbb{F}_q^n$ is a set containing a line in each such direction.

Recall the Chinese remainder theorem - if m and n are coprime, then $\mathbb{Z}/mn\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ are isomorphic as rings. For square-free $N = p_1 \dots p_r$, we have $\mathbb{Z}/N\mathbb{Z} \cong \mathbb{F}_{p_1} \times \dots \times \mathbb{F}_{p_r}$, where $\mathbb{F}_{p_i}$ denotes the Finite Field $\mathbb{Z}/p_i\mathbb{Z}$. By this we identify $(\mathbb{Z}/N\mathbb{Z})^n$ with $\mathbb{F}_{p_1}^n \times \dots \times \mathbb{F}_{p_r}^n$.

Definition

Set $R = \mathbb{Z}/N\mathbb{Z}$. We define the projective space of directions $\mathbb{P}R^{n-1} := \mathbb{PF}_{p_1}^{n-1} \times \dots \times \mathbb{PF}_{p_r}^{n-1}$. A Kakeya set in R is a set containing a line in each direction.

Definitions and preliminaries (2)

Idea. We define a matrix A associated to K with rank comparable to $|K|$. We construct a matrix C such that $CA = B$, a known, well-understood matrix. Lower bounding this rank gives a lower bound on K.
For Finite Fields, the "line matrix " is enough for obtaining bounds q^{n-1}, which can be improved using a tensor power trick. In general we construct a more complicated matrix using the polynomial method, but we will still make use of the line matrix.

Definition

Given a Kakeya set $S \subseteq R^n$, for each direction $b \in \mathbb{P}R^{n-1}$ choose a line $L(b) \subseteq S$ in direction b. Define the line matrix M_S with rows and columns indexed by $\mathbb{P}R^{n-1}$ and R^n respectively, with rows the indicator vectors of $L(b)$.

Definitions and preliminaries (3)

Proposition

For any field $\mathbb{F}$, M_S of a Kakeya set has rank at least $|S'|/|R|$, where S' is the set of indices corresponding to non-zero columns of M_S. Also, S' is itself a Kakeya set.

Proof.

Pick a non-zero line $L_1 = L(b_1)$. Given lines $L_1 = L(b_1), \ldots, L_{t-1} = L(b_{t-1})$, the cardinality of their union is at most $|R|(t-1)$. If $|R|(t-1) < |S'|$, there is a column corresponding to a point which does not intersect $L_1, \ldots, L_{t-1}$, but does intersect some $L_t(b_t)$. Hence if we cannot add another such line to the collection, the final number t of lines satisfies $|R|t \geq |S'|$. □

Linear Algebra results (1)

Proposition

Let U and V be finite dimensional vector spaces over $\mathbb{F}$, $u_1, \ldots, u_n \in U$ linearly independent, and for each i let $v_1^{(i)}, \ldots, v_m^{(i)} \in V$ be linearly independent. Then the tensors $u_i \otimes v_j^{(i)}$ form a linearly independent collection of size nm in $U \otimes V$.

Proof (1/2).

Let $w_1, \ldots, w_l$ be a basis of V and write $v_j^{(i)} = \sum_{k=1}^{l} \lambda_{i,j,k} w_k$. Note that the $u_i \otimes w_k$ form a linearly independent collection in $U \otimes V$. Suppose that for some scalars $\alpha_{i,j}$ we have

$$\sum_{i=1}^{n} \sum_{j=1}^{m} \alpha_{i,j} u_i \otimes v_j^{(i)} = 0.$$

□

Linear Algebra results (2)

Proof (2/2).

$$\sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{k=1}^{l}\alpha_{i,j}\lambda_{i,j,k}u_i\otimes w_k = 0$$

and so by linear independence of the $u_i \otimes w_k$, we have that for each i, k,

$$\sum_{j=1}^{m}\alpha_{i,j}\lambda_{i,j,k} = 0$$

Multiplying by w_k and summing over k gives

$$\sum_{k=1}^{l}\sum_{j=1}^{m}\alpha_{i,j}\lambda_{i,j,k}w_k = \sum_{j=1}^{m}\alpha_{i,j}v_j^{(i)} = 0$$

for each i, so by independence of the $v_j^{(i)}$, we have $\alpha_{i,j} = 0$. □

Linear Algebra results (3)

Definition

Given an $m \times n$ matrix A and a $r \times s$ matrix B, the Kronecker product $A \otimes B$ is the $mr \times ns$ block matrix given by

$$\begin{bmatrix} a_{1,1}B & \cdots & a_{1,n}B \\ \vdots & \ddots & \vdots \\ a_{m,1}B & \cdots & a_{m,n}B \end{bmatrix}.$$

Proposition

Let $A = (a_{i,j})$ be an $m \times n$ matrix, $B = (b_{i,j})$ an $r \times s$ matrix, $X = (x_{i,j})$ an $n \times p$ matrix and $Y = (y_{i,j})$ an $s \times t$ matrix. Then $(A \otimes B)(X \otimes Y) = (AX) \otimes (BY)$.

Linear Algebra results (4)

Proof.

Index rows in $(A \otimes B)$ by pairs (i_1, i_2) corresponding to rows of A and B, and columns by pairs (j_1, j_2) corresponding to those of A and B. The $((i_1, i_2), (j_1, j_2))$ entry of $A \otimes B$ is $a_{i_1,j_1} b_{i_2,j_2}$. We have that the $((i_1, i_2), (k_1, k_2))$ entry of $(A \otimes B)(X \otimes Y)$ is given by

$$\sum_{(j_1,j_2)} a_{i_1,j_1} b_{i_2,j_2} x_{j_1,k_1} y_{j_2,k_2} = \left(\sum_{j_1} a_{i_1,j_1} x_{j_1,k_1} \right) \left(\sum_{j_2} b_{i_2,j_2} y_{j_2,k_2} \right).$$

The right hand side is precisely the $((i_1, i_2), (k_1, k_2))$ entry of $(AX) \otimes (BY)$. □

Linear Algebra results (5)

Definition

Given a finite set $T = \{A_1, \ldots, A_n\}$ of matrices having the same number of columns we let crank(T) be the rank of the matrix obtained by concatenating all the elements A_i in T along their columns. Equivalently, it is the dimension of the space spanned by $\cup_{i=1}^{n}\{r : r \text{ is a row in } A_i\}$.

Proposition

Given $m \times n$ matrices $A_1, \ldots, A_r$ and an $n \times p$ matrix B we have $crank\{A_i\}_{i=1}^{r} \geq crank\{A_iB\}_{i=1}^{r}$.

Linear Algebra results (6)

Proposition

Given matrices $A_1, \ldots, A_r$ of size $m_1 \times n_1$ such that $crank\{A_i\}_{i=1}^r \geq k_1$ and matrices $B_{i,j}$ for $1 \leq i \leq r$ and $1 \leq j \leq s$ of size $m_2 \times n_2$ such that $crank\{B_{i,j}\}_{j=1}^s \geq k_2$ for each i we have,

$$crank\{A_i \otimes B_{i,j} : 1 \leq i \leq r, 1 \leq j \leq s\} \geq k_1 k_2.$$

Proof.

Let U be an independent subset of $\cup_{i=1}^r \{u : u \text{ is a row in } A_i\}$ of size k_1 and for each $1 \leq i \leq r$ let V_i be an independent subset of $\cup_{j=1}^s \{v : v \text{ is a row in } B_{i,j}\}$ of size k_2. By the previous tensor product bound we have that $\cup_{i=1}^r \{u \otimes v : u \in U, v \in V_i\}$ is a linearly independent set of size $k_1 k_2$. □

One more preliminary... (1)

Lemma

Let K be a Kakeya set in R^n where $R = \mathbb{Z}/N\mathbb{Z}$ for a square-free integer $N = p_1 \dots p_r$. Then $K^m \subseteq R^{mn}$ is a Kakeya set in R^{mn}.

Proof (1/2).

Let $b \in \mathbb{P}R^{mn-1}$ be some direction and choose a representative $(b_1, \dots, b_m) \in (R^n)^m$ of this direction. Let $b_i^{(j)}$ denote the $\mathbb{F}_{p_j}^n$ component of b_i obtained through the Chinese remainder theorem.

For each i let $L_i \subseteq K$ be a line in some direction c_i that agrees with $b_i^{(j)}$ whenever it is non-zero. We claim that $L_1 \times \dots \times L_m$ contains a line in direction $(b_1, \dots, b_m)$. □

One more preliminary... (2)

Proof (2/2).

We have $L_i = \{a_i + tc_i : t \in R\}$ for some a_i. Let $L = \{(a_1, \ldots, a_m) + t(b_1, \ldots, b_m) : t \in R\}$, a line in direction b.
Now, $L_1 \times \ldots \times L_m$ contains all points of the form $(a_1 + t_1c_1, \ldots, a_m + t_mc_m)$ where $t_i \in R$.
Under the isomorphism given by the Chinese remainder theorem, choose t_i to be equal to t in the j^{th} entry when $b_i^{(j)}$ is non-zero, and 0 in the other entries. Then $t_ic_i = tb_i$ for each i, and we have $(a_1 + t_1c_1, \ldots, a_m + t_mc_m) = (a_1, \ldots, a_m) + t(b_1, \ldots, b_m)$, so K^m contains a line in direction b and we are done. □

The Evaluation maps

Definition

Let m, n be natural numbers, and $U \subseteq \mathbb{F}^n$. We will consider vectors in $\mathbb{F}^{|U|\Delta_{n,m-1}}$ with entries indexed by (A, α) where A runs through U and α runs through the set of multiindices with $|\alpha| < m$. We define

$$\mathrm{EVAL}_U^m : \mathbb{F}[X] \to \mathbb{F}^{|U|\Delta_{n,m-1}}$$

to be the linear map which sends a polynomial P to $(P^{(\alpha)}(A))_{(A,\alpha)}$. Here $P^{(\alpha)}$ is the α^{th} Hasse derivative.

The Decoding matrix (1)

Lemma

Let $\mathbb{F}_q$ be a Finite Field, and let $l, n, m \in \mathbb{N}_0$ be such that $q|l$, $m = 2l - l/p$, and let $L \subseteq \mathbb{F}_q^n$ be a line in the direction $b \in \mathbb{PF}_q^{n-1}$. Then we can construct a $\Delta_{n,l-1} \times q^n \Delta_{n,m-1}$ matrix C_L^l such that, for a homogeneous $P \in \mathbb{F}_q[X]$ of degree $lq - 1$ we have

$$C_L^l \cdot EVAL_{\mathbb{F}_q^n}^m(P) = EVAL_b^l(P).$$

Moreover, following the notation from the previous definition, the only non-zero columns of C_L^l are the ones corresponding to (X, α) for which $X \in L$.

The Decoding matrix (2)

Proof.

We have noted that for homogenous polynomials P of degree $lq-1$ we have

$$\text{EVAL}_L^m(P)=0 \Rightarrow \text{EVAL}_b^l(P)=0$$

where $m=2l-l/q$.

Recall: whenever A and B are linear maps from $\mathbb{F}^k$ to some other (possibly different) vector spaces, we have that if for each $v \in \mathbb{F}^k$, $Av=0$ implies $Bv=0$, then there exists C such that $CA=B$.

Thus there is a matrix C' such that

$$C' \cdot \text{EVAL}_L^m(P)=\text{EVAL}_b^l(P).$$

We now add in zero columns to C' to correspond to (X,α) for $X \in \mathbb{F}_q^n \setminus L$, and we see that the resulting matrix C_L^l has the desired properties. □

Proof of the Kakeya bound (1)

Proof (1/8).

We will use induction over r. For $r = 1$, this is just the Finite Field bound. Suppose now that $r > 1$ and the result holds for $N_0 = p_2 \dots p_r$. We will prove the result for $N = p_1 \dots p_r$. Denote $R = \mathbb{Z}/N\mathbb{Z}$, $R_0 = \mathbb{Z}/N_0\mathbb{Z}$ and $p = p_1$ so that $R \cong \mathbb{F}_p \times R_0$.

Where we consider polynomials or do Linear Algebra in the proof, we will work over $\mathbb{F}_p$.

Let K be a Kakeya set in R^n. Every direction $b \in \mathbb{P}R^{n-1}$ is represented by $(b_1, b_2) \in \mathbb{P}\mathbb{F}_p^{n-1} \times \mathbb{P}R_0^{n-1}$. Through the Chinese remainder theorem, we see that a line $L \subseteq R^n$ in direction $b = (b_1, b_2)$ is a product of lines $L_1 \subseteq \mathbb{F}_p^n$ in direction b_1 and $L_2 \subseteq R_0^n$ in direction b_2. □

Proof of the Kakeya bound (2)

Proof (2/8).

Let I_L denote the indicator row vector of L, with entries $I_L(X)$ indexed by points of $X \in R^n$, and similarly for I_{L_1} and I_{L_2}. Identifying $X \in R^n$ with $(X_1, X_2) \in \mathbb{F}_p^n \times R_0^n$ by Chinese remainder theorem, we have $I_L(X) = I_{L_1}(X_1) I_{L_2}(X_2) = I_{L_1} \otimes I_{L_2}(X)$, the Kronecker product of I_{L_1} and I_{L_2}.

For each direction $b \in \mathbb{P}R^{n-1}$ we have at least one line in K in that direction. Pick one for each b and denote it by $L(b)$ contained in K. We may write it as a product $L_1(b) \times L_2(b)$ of lines in $\mathbb{F}_p^n$ and R_0^n in directions b_1 and b_2 respectively. □

Proof of the Kakeya bound (3)

Proof (3/8).

Fix an l divisible by p, set $m = 2l - l/p$, and for $b \in \mathbb{P}R^{n-1}$ consider the decoding matrix $C^l_{L_1(b)}$ over the field $\mathbb{F}_p$. We will show that

$$|K|\Delta_{n,m-1} \geq \text{crank}\{C^l_{L_1(b)} \otimes I_{L_2(b)}\}_{b \in \mathbb{P}R^{n-1}}.$$

For each b, the columns in $C^l_{L_1(b)}$ are indexed by $(X, \alpha) \in \mathbb{F}_p^n \times \mathbb{N}_0^n$ with $|\alpha| < m$, hence the columns in $C^l_{L_1(b)} \otimes I_{L_2(b)}$ are indexed by $(X, \alpha) \in R^n \times \mathbb{N}_0^n$ with $|\alpha| < m$.
The non-zero columns of $C^l_{L_1(b)}$ correspond to points $X \in L_1(b)$, so the non-zero columns in $C^l_{L_1(b)} \otimes I_{L_2(b)}$ correspond to $X \in L(b) \subseteq K$. Hence the columns of the concatenated matrix are non-zero only if they correspond to (X, α) for which $X \in K$. For each such X there are $\Delta_{n,m-1}$ such columns, which gives the bound. □

Proof of the Kakeya bound (4)

Proof (4/8).

Let E be a matrix representing the linear map $\mathrm{EVAL}^{m}_{\mathbb{F}_p^n}$ restricted to the space of polynomials that are homogeneous of degree $lp-1$. Given a direction $b_1 \in \mathbb{PF}_p^{n-1}$, let D_{b_1} be the matrix representing the linear map $\mathrm{EVAL}^{l}_{b_1}$ restricted to space of homogeneous polynomials of degree $lp-1$. Then we have $C^{l}_{L_1(b)}E = D_{b_1}$. Let $I_{N_0^n}$ be an identity matrix of size $N_0^n \times N_0^n$.

$$\begin{aligned}
\mathrm{crank}\{C^{l}_{L_1(b)} \otimes I_{L_2(b)}\}_{b\in \mathbb{P}R^{n-1}} &\geq \mathrm{crank}\{(C^{l}_{L_1(b)} \otimes I_{L_2(b)})(E \otimes I_{N_0^n})\}_{b\in \mathbb{P}R^{n-1}} \\
&= \mathrm{crank}\{(C^{l}_{L_1(b)}E) \otimes I_{L_2(b)}\}_{b\in \mathbb{P}R^{n-1}} \\
&= \mathrm{crank}\{D_{b_1} \otimes I_{L_2(b_1,b_2)}\}_{(b_1,b_2)\in \mathbb{PF}_p^{n-1}\times \mathbb{P}R_0^{n-1}}.
\end{aligned}$$

□

Proof of the Kakeya bound (5)

Proof (5/8).

First, we show that $\text{crank}(\{D_{b_1}\}_{b_1 \in \mathbb{PF}_p^{n-1}}) \geq \delta_{n,lp-1}$. Let us consider the matrix D obtained by concatenating these matrices. This is precisely the matrix for the map $\text{EVAL}^{l}_{\mathbb{PF}_p^{n-1}}$ restricted to the space of homogeneous polynomials of degree $lp - 1$. We claim that this map is injective, so that its rank is equal to the dimension of its domain, which is $\delta_{n,lp-1}$.

If some homogeneous polynomial P lies in the kernel of this map, then all its Hasse derivatives of order less than l vanish over $\mathbb{PF}_p^{n-1}$. Since P is homogenous, so are its Hasse derivatives, hence P and its Hasse derivatives of order less than l vanish everywhere. By the extended Schwartz-Zippel lemma, as $(lp-1)p^{n-1} < lp^n$, we have $P = 0$. □

Proof of the Kakeya bound (6)

Proof (6/8).

Next we show that for each $b_1 \in \mathbb{PF}_p^{n-1}$ we have

$$\mathrm{crank}\{I_{L_2(b_1,b_2)}\}_{b_2 \in \mathbb{P}R_0^{n-1}} \geq \frac{N_0^{n-1}}{\prod_{i=2}^{r}(2-1/p_i)^n}.$$

Here we use the inductive hypothesis - observe that for fixed b_1 the union of the $L_2(b_1, b_2)$ is a Kakeya set S in R_0^n. The crank of the set of indicator vectors is just the rank of the line matrix M_S over $\mathbb{F}_p$. Hence this is bounded below by $|S'|/|R_0|$, which by the induction hypothesis is at least the desired lower bound.

These two lower bounds combine to give... □

Proof of the Kakeya bound (7)

Proof (7/8).

$$|K|\Delta_{n,m-1} \geq \frac{N_0^{n-1}}{\prod_{i=2}^{r}(2-1/p_i)^n}\delta_{n,lp-1}$$

$$|K|\binom{2l-l/p+n-1}{n} \geq \frac{N_0^{n-1}}{\prod_{i=2}^{r}(2-1/p_i)^n}\binom{lp+n-2}{n-1}.$$

Let l be a square multiple of p. Apply our bound to $K^{\sqrt{l}}$ to get

$$|K|^{\sqrt{l}}\binom{2l-l/p+n\sqrt{l}-1}{n\sqrt{l}} \geq \frac{N_0^{n\sqrt{l}-1}}{\prod_{i=2}^{r}(2-1/p_i)^{n\sqrt{l}}}\binom{lp+n\sqrt{l}-2}{n\sqrt{l}-1}.$$

□

Proof of the Kakeya bound (8)

Proof (8/8).

$$|K|^{\sqrt{l}} \geq \frac{N_0^{n\sqrt{l}-1}}{\prod_{i=2}^{r}(2-1/p_i)^{n\sqrt{l}}} \frac{(lp+n\sqrt{l}-2)\dots(lp-1)}{(2l-l/p+n\sqrt{l}-1)\dots(2l-l/p-1)} n\sqrt{l}.$$

Take the $\sqrt{l}^{\text{th}}$ root on both sides and let $l \to \infty$ to get

$$|K| \geq \frac{p^n N_0^n}{(2-1/p)\prod_{i=2}^{r}(2-1/p_i)^n}$$

which is the desired result. □

Aside - Some Analytic Number Theory (1)

Let $\omega(N)$ denote the number of distinct prime factors of N.

Lemma

$\omega(N) = O(\log(N)/\log\log(N))$ *as* $N \to \infty$

Proof (1/2).

By Stirling's formula (the ratio of $k!$ and $\sqrt{2\pi k}(k/e)^k$ approaches 1 as $k \to \infty$), we have $k! \geq (k/e)^k = e^{k\log(k)-k}$ for sufficiently large k. Take logs and set $k = \omega(N)$ to get $\omega(N)\log(\omega(N)) - \omega(N) \leq \log(\omega(N)!)$.
Write $N = p_1^{a_1}\dots p_r^{a_r}$ where $r = \omega(N)$ and p_i are prime numbers satisfying $p_1 < \dots < p_r$. Clearly $i < p_i$ for each i, so $r! < p_1 \dots p_r \leq N$, hence $\omega(N)! \leq N$.
Thus $\omega(N)\log(\omega(N)) - \omega(N) \leq \log(N)$. □

Aside - Some Analytic Number Theory (2)

Proof (2/2).

Rearranging gives $\omega(N) \leq \log(N)/(\omega(N)-1) \leq \log(N)$ for large $\omega(N)$.
Alternatively, we could rearrange as
$\omega(N)\log(\omega(N)) \leq \log(N) + \omega(N) \leq 2\log(N)$.
Now let $C > 2$ and suppose that there are infinitely many N with $\omega(N) \geq C\log(N)/\log\log(N)$. Then for these N we have

$$[C\log(N)/\log\log(N)] \cdot [\log(C\log(N)/\log\log(N))] \leq \omega(N)\log(\omega(N)) \leq 2\log(N).$$

Rearranging and then taking exponentials gives

$$C\log(N)/\log\log(N) \leq (\log(N))^{2/C}.$$

Rearranging gives $C(\log(N))^{1-(2/C)}/\log\log(N) \leq 1$ for infinitely many N, but as $N \to \infty$ the left hand side goes to infinity, a contradiction. $\square$

Wrapping up

Since $\omega(N) \leq C \log(N)/\log\log(N)$, and we know $|K| \geq N^n 2^{-rn}$, we have

$$|K| \geq CN^{n(1-1/\log\log(N))}$$

hence for any $\varepsilon > 0$ we have

$$|K| \geq C_{n,\varepsilon} N^{n-\varepsilon}$$

as conjectured.