Discrete Kakeya-type problems and small bases

Noga Alon *Boris Bukh* *Benny Sudakov*

Kakeya problem

Definition:

Besicovitch set is a set $U \subset \mathbb{R}^d$ containing a translate of every unit line segment.

Problem: (*Kakeya*)

How small can a Besicovitch set be?

Amazing Fact: (*Besicovitch*)

There are Besicovitch sets of Lebesgue measure zero.

Conjecture:

Every Besicovitch set in $\mathbb{R}^d$ has Minkowski dimension d.

Theorem: (*Bourgain*)

If every set $X \subset \mathbb{Z}/p\mathbb{Z}$ containing a translate of every k-term arithmetic progression is of size at least $c_k p^{1-\epsilon(k)}$ with $\epsilon(k) \to 0$ as $k \to \infty$, then Kakeya conjecture follows.

Universal sets

Definition:

If $\mathcal{F}$ is family of subsets in a group G, then $U \subset G$ is *$\mathcal{F}$-universal* if for every $F \in \mathcal{F}$ there is $g \in G$ such that $gF \subset U$.

For $\mathcal{F} = \{\text{all } k\text{-element sets of } G\}$ $\mathcal{F}$-universal U is said to be *k-universal*.

Observation:

If U is k-universal, then $|U| \geq \frac{1}{2}|G|^{1-1/k}$.

Proof. There are $\binom{|U|}{k}$ k-element subsets of U, and the orbit of a k-set under multiplication by G has size at most $|G|$. Therefore

$$|G|\binom{|U|}{k} \geq \binom{|G|}{k}. \qquad \square$$

Question:

How tight is this lower bound?

Nearly optimal universal sets

Theorem: (*Alon-Bukh-S.*)

For every finite group G there is a k-universal set of size at most $|G|^{1-1/k} \log^{1/k} |G|$.

Remark. For $k \geq \log\log|G|$ this is tight, as $\log^{1/k}|G|$ is bounded by a constant.

Theorem: (*Alon-Bukh-S.*)

- For cyclic G, there is a k-universal set of size $72|G|^{1-1/k}$.
- If G is abelian, there is a k-universal set of size $8^k k|G|^{1-1/k}$.
- If $G = S_n$ is a symmetric group, there is a k-universal set of size $(3k+1)!|G|^{1-1/k}$.

Small bases

Definition:

A set of integers B is a basis for a set of integers A if

$$A \subset B + B = \{b_1 + b_2 \, : \, b_1, b_2 \in B\}.$$

Observation:

- $\{0\} \cup A$ is a basis for A.
- $\{0, 1, 2, \ldots, \sqrt{n}\} \cup \{0, \sqrt{n}, 2\sqrt{n}, \ldots, n\}$ is a basis for $[n] \supset A$.

Thus every $A \subset [n]$ has basis of size at most $\min(|A| + 1, 3\sqrt{n})$.

Theorem: (*Erdős-Newman '77*)

If $m < n^{1/2-\epsilon}$ or $m > n^{1/2+\epsilon}$ then there is a set $A \subset [n]$ of size m such that every basis for A has size at least $c(\epsilon)\min(|A|, \sqrt{n})$.

Sets of size $\sqrt{n}$

Theorem: (*Erdős-Newman '77*)

There is a set $A \subset [n]$ of size $\sqrt{n}$ such that every basis of A has size at least $\sqrt{n}\frac{\log \log n}{\log n}$.

Proof. Every subset of size t can be basis for at most $\binom{t^2}{\sqrt{n}}$ sets A. There are $\binom{n}{\sqrt{n}}$ subsets A, therefore

$$\binom{n}{t}\binom{t^2}{\sqrt{n}} \geq \binom{n}{\sqrt{n}}.$$

□

Problem: (*Erdős-Newman '77*)

Does every $A \subset [n], |A| = \sqrt{n}$ have basis of size $o(\sqrt{n})$?

Small bases for sets of size $\sqrt{n}$

Theorem: (*Alon-Bukh-S.*)

For every subset $A \subset [n]$ of size $\sqrt{n}$ there is a basis B of size
$$|B| \leq 50\sqrt{n}\frac{\log\log n}{\log n}.$$

Sketch of proof. Partition $A = A_1 \cup \dots A_m$ into minimum number of disjoint sets of size at most k, such that each A_i is contained in the interval of length $\sqrt{n}\log n$. Then
$$m = |A|/k + \sqrt{n}/\log n.$$
Let B be a k-universal set for $\{1, 2, \dots, \sqrt{n}\log n\}$ of size $c\left(\sqrt{n}\log n\right)^{1-1/k}$. By definition, for every A_i there is s_i such that $A_i \subset s_i + B$. Then $\{s_1, \dots, s_m\} \cup B$ is a basis for A of size
$$\sqrt{n}/k + \sqrt{n}/\log n + c\left(\sqrt{n}\log n\right)^{1-1/k}.$$
For $k = \frac{\log n}{10\log\log n}$ this is at most $O\left(\sqrt{n}\frac{\log\log n}{\log n}\right)$. □

DEFINITION:

A set $X \subset G$ is a non-doubling if $|XX| \leq 3|X|$.

THEOREM: *(Alon-Bukh-S.)*

If $X \subset G$ is non-doubling, then G contains a k-universal set for X of size $36|X|^{1-1/k} \log^{1/k} |X|$.

Sketch of proof. Choose elements of XX to be in U randomly and independently with $p = \left(\frac{|X|}{2k^3 \log |X|}\right)^{-1/k}$. For every k-element $S \subset X$ and $x \in X$ the set $xS \subset XX$ is not contained in U with probability $1 - p^k$. Since there are $|X|/k^2$ pairwise disjoint sets xS, the probability that U is not k-universal is at most

$$\binom{|X|}{k} \left(1 - p^k\right)^{|X|/k^2} \ll 1. \qquad \square$$

Erdős-Newman in groups

Definition:

Group G of order n satisfies EN-condition if for every $A \subset G$ of size $|A| \leq \sqrt{n}$ there is a basis B of size $|B| \leq 50 \frac{\sqrt{n} \log \log n}{\log n}$.

Theorem: (*Alon-Bukh-S.*)

If group G of order n contains a non-doubling X satisfying

$$\sqrt{n} \log^2 n \leq |X| \leq \sqrt{n} \log^{10} n,$$

then G satisfies EN-condition.

Theorem: (*Alon-Bukh-S.*)

- Every solvable group satisfies EN-condition.
- Every symmetric group S_n satisfies EN-condition.

Bases for powers

Question: (*Wooley*)

Let $P_d = \{1^d, 2^d, \ldots, n^d\}$ for $d \geq 2$. How large must a basis for this set be?

Theorem: (*Erdős-Newman '77*)

There is no basis of size $n^{2/3-\epsilon}$ for squares.

Theorem: (*Alon-Bukh-S.*)

There is no basis of size $n^{3/4-O(1/\sqrt{d})}$ for P_d.

Concluding remarks

Open problems:

- Is there a k-universal set of size $c|G|^{1-1/k}$ for every finite group G?
- Do all finite groups satisfy EN-condition?
- Is it true that every basis for $P_d = \{1^d, 2^d, \ldots, n^d\}$ must have size at least $n^{1-o(1)}$?