Lecture 13

Recall In discrete Kakeya set problem, we want to bound the size of a Kakeya set from below.

Suppose it's small $\Rightarrow$ construct a low deg polyn. vanishing on too large set, contradicting to Schwartz-Zippel lem.

Thm [Alon, Combinatorial Nullstellensatz]

Let f be a non-zero n-var. polyn on $\mathbb{F}_p^n$.

Let $S_1, \dots, S_n$ subsets of $\mathbb{F}_p$.

Suppose f has a term $x_1^{k_1} \cdots x_n^{k_n}$ with non-zero coeff. and $\sum_{i=1}^{n} k_i = \deg f$, and $\forall i \in [n]$, $|S_i| > k_i$

$\Longrightarrow$ f cannot vanish on $S_1 \times \cdots \times S_n$.

Pf:

- Induct on $\deg f$
  Base case: $\deg f = 0$ trivial.
- Inductive step, $\deg f > 0$. w.l.o.g. assume $k_1 > 0$

- Supp. f vanishes on $\prod S_i$.

  Take $a \in S_1$, use polyn division to write

$$f(x) = (x_1 - a) g(x) + h(x_2, \dots, x_n)$$

As f vanishes on $\{a\} \times S_2 \times \dots \times S_n$

$\Rightarrow$ h vanishes on $S_2 \times \cdots \times S_n$.

$\Rightarrow$ $(x_1 - a) \cdot g(x)$ vanishes on $S_1 \times \cdots \times S_n$

$\Rightarrow$ g vanishes on $(S_1 \setminus \{a\}) \times S_2 \times \cdots \times S_n$

- f has $x_1^{k_1} \cdots x_n^{k_n}$ w/ non-zero coeff.

which is in $x_1 \cdot g(x)$

$\Rightarrow$ $g(x)$ has $x_1^{k_1 - 1} x_2^{k_2} \cdots x_n^{k_n}$

term w/ $\begin{cases} \text{non-zero coeff.} \\ \deg = \deg g \end{cases}$ $\lightning$ (IH) $\blacksquare$

- Combinatorial Nullstellensatz is useful for lower bounding size of some set. A.

Strategy Suppose $|A|$ is too small.

We find a "low deg" polyn. f vanishing on too large a Cartesian product set, which would contradict Comb. Null.

Def: A, B sets, $A + B = \{a + b : a \in A, b \in B\}$ (sum set)

Thm [Cauchy 1813, Davenport 1935]

Let p be a prime and $A, B \subseteq \mathbb{F}_p$

$\Rightarrow$ $|A + B| \geq \min\{p, |A| + |B| - 1\}$.

Rmk i) best possible: $A = \{0, 1, \dots, a-1\}$
$B = \{0, 1, \dots, b-1\}$

$$A+B = \{0, 1, \dots, a+b-2\}$$

ii) p being a prime is necessary.

divisibility barrier: consider $\mathbb{Z}_{2p}$, $A = B =$ evens

$$A+B = A = B$$

Pf: If $|A| + |B| > p$, then $A+B = \mathbb{F}_p$

Indeed, $\forall\, c \in \mathbb{F}_p$, $c - B = \{c-b : b \in B\}$

$(c-B) \cap A \neq \phi \Rightarrow \exists\, a \in A, b \in B$ s.t.
$c - a = b$ or $c = a+b$ ☺

Assume then $|A| + |B| \leq p \Rightarrow |A| + |B| - 1 < p$

Suppose for contrary that $|A+B| \leq |A| + |B| - 2$
$< p-1$

so $\exists$ set $C \supseteq A+B$ of size
$|A| + |B| - 2$.

Thought process: Need to find 'low-deg' f vanishing on a large product set

want

- natural prod. $= A \times B$ i.e. $f(a,b) = 0$

$$\Rightarrow \prod_{c \in C} (x+y-c)$$

Let $f(x,y) = \prod_{c \in C} (x+y-c)$

- $\deg f = |C| = |A| + |B| - 2$
- f vanishes on $A \times B$ by defn. of f.

Left to check f has term $x^{|A|-1} y^{|B|-1}$ with non-zero coeff.

True: coeff $=$ $\binom{|A|+|B|-2}{|A|-1} \neq 0$ in $\mathbb{F}_p$

b/c $|A|+|B|-2 < p$ & p prime. $\blacksquare$

What about $A \hat{+} A = \{ a + a' : a, a' \in A, a \neq a' \}$? (restricted sumset)

Conjectured by Erdős - Heilbronn

Thm [Dasilva - Hamidoune 94]

Let p prime, $A \subseteq \mathbb{F}_p$, $\Rightarrow$ $A \hat{+} A = \mathbb{F}_p$ or $|A \hat{+} A| \geq 2|A| - 3$

Exer: Prove ↑ using comb. Null.

Next time:

Thm Let $H_1, \dots, H_m$ be hyperplanes in $\mathbb{R}^n$, none of which passing through 0, covering $\{0,1\}^n \setminus 0$

$\Rightarrow$ $m \geq n$.