Lecture 15. Combinatorial Nullstellensatz

Problem. Suppose that the planes $P_1 \dots P_m$ in $\mathbb{R}^3$ avoids $(0,0,0)$.

but cover all $(n+1)^3-1$ points in $\{0,1,\dots,n\}^3$. then $m \geq ?$

Upper bound: $3n$ suffice. $x-i$, $y-j$. $z-k$. $1 \leq i.j.k \leq n$.

Lower bound: suppose m planes. consider their product $p(x.y.z)$.

Define partial difference $\Delta p(x) = p(x+1) - p(x)$. $= p'(\xi)$ for some ξ.

If p has degree d. then for all $N > d$. $\Delta^N p(x)$

$\Delta p(x) = p(x+1) - p(x)$. $\Delta^2 p(x) = p(x+2) - 2p(x+1) + p(x)$.

By induction. $\Delta^N p(x) = \sum_{k=0}^{N} (-1)^{N-k} \binom{N}{k} p(x+k)$

Similarly. $\Delta_x^n \Delta_y^n \Delta_z^n p(x.y.z)$

$$= \sum_{i=0}^{n} \sum_{j=0}^{n} \sum_{j=0}^{n} (-1)^{3n-i-j-k} \binom{n}{i}\binom{n}{j}\binom{n}{k} p(x+i, y+j, z+k).$$

Plugging in $(x.y.z) = (0,0,0)$. $\Delta_x^n \Delta_y^n \Delta_z^n p(0,0,0) = (-1)^{3n} p(0,0,0)$

Thus $\Delta_x^n \Delta_y^n \Delta_z^n p(0,0,0) \neq 0$. p has degree $\geq 3n$. $\square$

Remark. This problem comes from IMO 07 P6. The most difficult

problem in IMO from 2007 to 2017. with average score 0.15/7.

The proof was given by Peter Scholze. IMO 07 rank 2.

Theorem (Combinatorial Nullstellensatz) by Noga Alon.

Let $f(x_1 \cdots x_n)$ be a polynomial of degree d over a field $\mathbb{F}$.

Suppose that the coefficient of the monomial $x_1^{t_1} \cdots x_n^{t_n}$ in f is

nonzero and $t_1 + \cdots + t_n = d$. If $S_1, \ldots, S_n$ are finite subsets of

$\mathbb{F}$ with $|S_i| \geq t_i + 1$. then there exists $x \in S_1 \times \cdots \times S_n$. s.t. $f(x) \neq 0$.

Proof of IMO 07 P6 by combinatrial nullstellensatz.

Suppose $< 3n$ planes. $p(x, y, z) = \prod_{i=1}^{m} (a_i x + b_i y + c_i z + d_i)$

$p(0,0,0) \neq 0 \Rightarrow \prod d_i \neq 0$. Let $D = \prod d_i / (n!)^3$. and

$$q(x, y, z) = p(x, y, z) - D \prod_{i=1}^{n} (x - i) \prod_{j=1}^{n} (y - j) \prod_{k=1}^{n} (z - k).$$

$D \neq 0$ and $m < 3n \Rightarrow q(x, y, z)$ has degree $3n$. and the

coefficient of $x^n y^n z^n \neq 0$. but $q(x, y, z)$ vanishes on $\{0, \ldots, n\}^3$. □

To prove CN. we first introduce Nullstellensatz.

Theorem (Nullstellensatz. theorem of zero points).

Let $f \in \mathbb{F}[x_1 \cdots x_n]$ and $S_1 \cdots S_n$ be nonempty subsets of $\mathbb{F}$.

If f vanishes on $S_1 \times \cdots \times S_n$ then there are polynomials $h_1 \cdots h_m$

$\in \mathbb{F}[x_1 \cdots x_n]$ such that $\deg(h_i) \leq \deg(f) - |S_i|$, and

$$f(x_1 \dots x_n) = \sum_{i=1}^{n} h_i(x_1 \dots x_n) \prod_{s \in S_i} (x_i - s).$$

Proof (by Noga Alon). Define $d_i = |S_i| - 1$. consider polynomials.

$$g_i(x_i) = \prod_{s \in S_i} (x_i - s) = x_i^{d_i+1} - \sum_{j=0}^{d_i} a_{ij} x_i^j.$$

Note that. if $x_i \in S_i$. then $g_i(x_i) = 0$. namely $x_i^{d+1} = \sum_{j=0}^{d_i} a_{ij} x_i^j$.

Let $\hat{f}$ be the polynomial obtained by repeatedly replacing each x^{t_i} where $t_i > d_i$. by a linear combination of small powers of x_i.

Clearly. $\hat{f}(x) = f(x)$ if $x \in S_1 \times S_2 \times \cdots S_n$.

Also. $\hat{f}$ is obtained from f by subtracting from it products of the form $h_i g_i$. where $\deg(h_i) \le \deg(f) - \deg(g_i) = \deg(f) - |S_i|$

So $\hat{f}(x) = f(x) - \sum_{i=1}^{n} h_i(x) g_i(x)$. Since $\hat{f}$ has degree at most d_i in x_i but vanishes on $S_1 \times \cdots \times S_n$ with $|S_i| = d_i + 1$. by a generalized Schwartz-Zippel lemma. $\hat{f} \equiv 0$. Thus $f = \sum h_i g_i$ □

Proof of Combinatorial Nullstellensatz.

We may assume $|S_i| = t_i + 1$. Suppose the result does not hold.

Define $g_i(x_i) = \prod_{s \in S_i} (x_i - s)$. Let $h_1 \dots h_n$ be the polynomials guaranteed by Nullstellensatz. Hence. $f(x_1 \dots x_n) = \sum_{i=1}^{n} h_i \cdot g_i$. and

$\deg(h_i) \le \deg(f) - \deg(g_i) = \deg(f) - (t_i+1)$. Note that

$$f(x) = \sum_{i=1}^{n} x_i^{t_i+1} h_i(x) + (\text{terms of degree} < \deg(f)).$$

By assumption. the coefficient of monomial $\prod_{i=1}^{n} x_i^{t_i}$ is nonzero.

However there is no such term on the RHS. Contradiction. □

Theorem (Chevalley - Warning)

Let p be a prime. and $f_1 \dots f_m$ be polynomials in $\mathbb{F}_p[x_1 \dots x_n]$.

If $\sum_{i=1}^{m} \deg(f_i) < n$ then the number of common zeros of $f_1 \dots f_m$

is divisible by p. In particular. the number of common zeros is not 1.

Proof (by Noga Alon). By Fermat's Little Theorem. $a^{p-1} \equiv 1 \mod p$

for all $a \in \mathbb{F}_p$, $a \neq 0$. So the number N of common zeros is

$$N = \sum_{x_1 \dots x_n \in \mathbb{F}_p} \prod_{j=1}^{m} \left(1 - f_j(x_1 \dots x_n)^{p-1}\right) \quad (\text{in } \mathbb{F}_p)$$

$$= \sum_{x_1 \dots x_n \in \mathbb{F}_p} g(x_1 \dots x_n) \quad \text{for some polynomial } g.$$

For each monomial $\prod_{i=1}^{n} x_i^{t_i}$ in g. we claim that $\sum_{x_1 \dots x_n \in \mathbb{F}_p} \prod x_i^{t_i} = 0$.

To prove this. consider the primitive root r of p. Then

$\mathbb{F}_p = \{0, r, r^2, \dots, r^{p-1}\}$. So for every t. $\sum_{x \in \mathbb{F}_p} x^t = \sum_{j=1}^{p-1} r^{jt}$

$= \sum_{j=1}^{p-1} (r^t)^j = ((r^t)^p - 1)/(r^t - 1) - 1 = 0$. Thus $N = 0$. □

Theorem (Permanent Lemma). Let $b \in \mathbb{F}^n$ and $S_1 \dots S_n$ be subsets of $\mathbb{F}$ with $|S_i| \geq 2$. If $\mathrm{Per}(A) \neq 0$ where $A \in \mathbb{F}^{n \times n}$, then there exists a vector $x \in S_1 \times \cdots \times S_n$ such that Ax differs from b in all coordinates.

Remark. In particular, let $S_i = \{0,1\}$. There exists a subset of columns of A whose sum differs from b in all coordinates.

Proof. Let $A = (a_{ij})$ and polynomial $f = \prod_{i=1}^{n} \left(\sum_{j=1}^{n} a_{ij} x_j - b_i \right)$ be of degree n. The coefficient of $x_1 \cdots x_n$ in f is precisely $\mathrm{per}(A) \neq 0$.

The result follows directly from the Combinatorial Nullstellensatz. □

Regular subgraphs.

Theorem (Alon, Friedland & Kalai, 1984). Let $G = (V, E)$ be a graph. Assume that G has no self-loops but parallel edges are allowed.

Let p be a prime. If G has average degree $> 2p-2$ and maximum degree $\leq 2p-1$, then G contains a p-regular subgraph.

Proof. Associate each edge e with a variable x_e. Consider the polynomial

$$f = \prod_{v \in V} \left[1 - \left(\sum_{e \in E} a_{v,e} x_e \right)^{p-1} \right] - \prod_{e \in E} (1 - x_e) \qquad a_{v,e} = \mathbb{1}_{[v \in e]}$$

Note that average degree $= 2|E|/V > 2p-2$. So f has degree $|E|$, and the coefficient of $\prod_{e\in E} x_e$ is $(-1)^{|E|+1} \neq 0$.

Apply the Combinatorial Nullstellensatz with $S_e = \{0,1\}$ and $t_e = 1$.

We have a $(0,1)$-vector $x = (x_e : e \in E)$ such that $f(x) \neq 0$.

First $x \neq \vec{0}$, since $f(\vec{0}) = 0$. So $\prod_{e\in E}(1-x_e) = 0$, which implies that $\prod_{v\in V}\left[1-\left(\sum_{e\in E} a_{v,e}\, x_e\right)^{p-1}\right] \neq 0$. By Fermat's Little Theorem, $\left(\sum_{e\in E} a_{v,e}\, x_e\right)^{p-1} = 1$ if $\sum_{e\in E} a_{v,e}\, x_e \neq 0$. Thus for all v,

$\sum_{e\in E} a_{v,e}\, x_e = 0 \pmod p$. Let H be the subgraph consisting of edges with $x_e = 1$. H is not empty and every positive degree in H is p, since the maximum degree in $G < 2p$. □

Definition (sum-set): $A + B = \{a+b : a \in A,\ b \in B\}$.

Question: How large is $|A+B|$? upper bound $|A|\cdot|B|$ trivial lower bound? $A = [n]$, $B = [m]$, $|A+B| = n+m-1$

cannot be smaller. consider $\min A + B$ and $\max B + A$.

Theorem (Cauchy–Davenport theorem).

Let p be a prime, and A, B be two nonempty subsets of $\mathbb{Z}_p$.

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

Proof. If $|A|+|B| > p$ then the result is trivial.

For every $c \in \mathbb{Z}_p$, A and $c-B$ intersects. So $A+B = \mathbb{Z}_p$.

Now assume $|A|+|B| \leq p$ and suppose $|A+B| \leq |A|+|B|-2$.

Choose a set $C \supseteq A+B$ such that $C \subseteq \mathbb{Z}_p$ and $|C| = |A|+|B|-2$.

Consider the polynomial $f(x,y) = \prod_{c \in C}(x+y-c)$. $\deg(f) = |C|$.

The coefficient of $x^{|A|-1}y^{|B|-1}$ is $\binom{|A|+|B|-2}{|A|-1}$, which is nonzero

in $\mathbb{Z}_p$, since $|A|+|B|-2 < p$. However, $f(a,b) = 0$ for all

$a \in A$ and $b \in B$, which contradicts the Combinatorial Nullstellensatz. □

Theorem (Vosper). Let A, B be two subsets of $\mathbb{Z}_p$ such that $|A|, |B|$

≥ 2, and $|A|+|B| < p$. If $|A+B| = |A|+|B|-1$, then A, B

are two arithmetic progressions with the same difference.

Zero-sum sets: Any sequence of length n contains a nonempty

consecutive subsequence whose sum is divisible by n. (Pigeonhole).

Question: How about n nonconsecutive subsequence? (fixed size)

The sequence $0, 0, \ldots, 0, 1, 1, \ldots 1$ of $n-1$ 0 and $n-1$ 1 shows $N \geq 2n-1$.

Theorem (Erdős-Ginzburg-Ziv, 1961) Any sequence of $2n-1$ integers contains a subsequence of length n whose sum is divisible by n.

Proof (based on Cauchy-Davenport). First assume $n = p$ is a prime.

Let $a_1 \leq \cdots \leq a_{2p-1}$. If $a_i = a_{i+p-1}$ for some i. then $a_i + \cdots + a_{i+p-1}$ is the desired subsequence. Otherwise define $A_i = \{a_i, a_{i+p-1}\}$.

By applying Cauchy-Davenport repeatedly. we conclude that

$$|A_1 + A_2 + \cdots + A_{p-1}| \geq \min\{p, |A_2 + \cdots + A_{p-1}| + 1\}.$$

$$\geq \min\{p, |A_3 + \cdots + A_{p-1}| + 2\}$$

$$\geq \cdots \geq \min\{p, |A_{p-1}| + p - 2\} = p.$$

Hence every number in $\mathbb{Z}_p$ is the sum of precisely $p-1$ of the first $2p-2$ elements of the sequence. In particular. consider $-a_{2p-1}$

For general n. prove by induction on the number of primes in the prime factorization of n. Suppose $n = pm$. By the prime case. each subset of $2p-1$ members of the sequence contains a p-element subset whose sum is $0 \bmod p$. Find $l \geq 2m-1$ disjoint p-element subsets $I_1 \ldots I_l$. Now define $b_i = \sum_{j \in I_i} \frac{a_j}{p}$. b_i is an integer.

Apply induction hypothesis on $\{b_i : i \in [2m-1]\}$ and we're done. $\square$

Proof (by Noga Alon, 1995). Again, only prove the prime case $n = p$.

consider the following system of two polynomials in $2p-1$ variables of degree $p-1$ over $\mathbb{F}_p$: $\sum_{i=1}^{2p-1} a_i x_i^{p-1} = 0$, $\sum_{i=1}^{2p-1} x_i^{p-1} = 0$.

Since $2(p-1) < 2p-1$ and $x_1 = \cdots = x_{2p-1} = 0$ is a common root.

By Chevalley-Warning theorem, there is another common root $y \neq 0$ such that $\sum_{i=1}^{2p-1} a_i y_i^{p-1} = 0$ and $\sum_{i=1}^{2p-1} y_i^{p-1} = 0$. If $y_i \neq 0$, then $y_i^{p-1} = 1$. Thus $\{a_i : y_i \neq 0\}$ is the desired subsequence. $\square$