Applications of the combinatorial Nullstellensatz

Thomas Kalinowski

Discrete Maths seminar

The Theorem

- F an arbitrary field
- $f \in F[x_1, \dots, x_n]$ with $\deg(f) = t_1 + \cdots + t_n$
- coefficient of $\prod_{i=1}^{n} x_i^{t_i}$ nonzero
- $S_1, \dots, S_n \subseteq F$ with $|S_i| > t_i$ for all i

Then there exists $(s_1, \dots, s_n) \in S_1 \times \cdots \times S_n$ with

$$f(s_1, \dots, s_n) \neq 0.$$

Sumsets in vector spaces

Hopf-Stiefel function with respect to a prime p

$$\beta_p(r,s) = \min\{n \,:\, p \mid \binom{n}{k} \text{ for all } k \in \{n-r+1,\dots,s-1\}\}.$$

Theorem

If $A, B \subseteq \mathbb{F}_p^m$ with $|A| = r$ and $|B| = s$, then $|A+B| \geqslant \beta_p(r,s)$.

Proof.

Look at $Q(x,y) = \prod_{c \in A+B} (x+y-c)$ over $\mathbb{F}_q$ for $q = p^m$. □

Subgraphs

- p prime
- $G = (V, E)$ loopless graph
- average degree $> 2p - 2$
- maximum degree $\leqslant 2p - 1$

Then G contains a nontrivial p-regular subgraph.

Proof.

Let $A = (a_{v,e})$ be the incidence matrix of G and stare at

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

Covering the cube with hyperplanes

Let $H_1, \ldots, H_m$ be hyperplanes in $\mathbb{R}^n$ that cover all vertices of the unit cube $\{0,1\}^n$ but one. Then $m \geqslant n$.

Proof.

- W.l.o.g. the origin is the uncovered vertex.
- Let $\langle a_i, x \rangle = b_i$ be the equation for H_i.
- Suppose $m < n$ and consider

$$P = (-1)^{n+m+1} \prod_{j=1}^{m} b_j \prod_{i=1}^{n} (x_i - 1) - \prod_{i=1}^{m} (\langle a_i, x \rangle - b_i). \qquad \square$$

Problem 6 of the IMO 2007

Let n be a positive integer and consider

$$S = \{(x, y, z) \in \{0, 1, 2, \ldots, n\} \ : \ x + y + z > 0\}$$

as a set of $(n+1)^3 - 1$ points in $\mathbb{R}^3$.

Determine the smallest possible number of planes, the union of which contains S but does not include $(0, 0, 0)$.

The Permanent Lemma

- A an $n \times n$ matrix over a field F with $\mathrm{Per}(A) \neq 0$
- $(b_1, \ldots, b_n) \in F^n$
- $S_1, \ldots, S_n \subseteq F$ with $|S_i| = 2$

There exists $x \in S_1 \times \cdots \times S_n$ such that $(Ax)_i \neq b_i$ for all i.

Proof.

$$P = \prod_{i=1}^{n} \left[\sum_{j=1}^{n} a_{ij} x_j - b_i \right]$$

□

Lattice points

Harborth's function (1973)

Let $f(n, d)$ be the smallest number f such that every set of f lattice points in d-dimensional Euclidean space contains n points whose centroid is again a lattice point.

Zero-sum formulation

Any sequence of length $f(n, d)$ in Z_n^d contains a subsequence of length n which sums to 0.

- Easy bound: $f(n, d) \leqslant (n-1)n^d + 1$

Erdős, Ginzburg, Ziv (1961): $f(n,1) = 2n-1$

Proof.

- Easy to reduce to $n = p$ prime.
- Suppose $0 \leqslant a_1 \leqslant \cdots \leqslant a_{2p-1}$
- $a_i \neq a_{i+p-1}$ for all $i \in \{1, \ldots, p-1\}$ (otherwise done),
- $S_i = \{a_i, a_{i+p-1}\}$
- A the $(p-1) \times (p-1)$ all ones matrix
- $\{b_1, \ldots, b_{p-1}\} = Z_p \setminus \{-a_{2p-1}\}$
- Permanent lemma: There exist $\alpha_i \in S_i$ such that

$$\alpha_1 + \cdots + \alpha_{p-1} = -a_{2p-1}.$$

□

The permanent lemma also yields $f(n,2) \leqslant 5n-6$.

The Kemnitz conjecture

- We want to show $f(n, 2) = 4n - 3$.
- "$\geqslant$" is obvious.
- Easy to reduce to $n = p$ prime.

Notation

- Fix an odd prime p, and let $\equiv$ denote congruence modulo p.
- J, X,... : finite sets of lattice points in the plane
- We write $\sum X$ for $\sum_{x \in X} x$.
- $(k \mid X)$: number of k-subsets of X the sum of whose elements is divisible by p

Chevalley-Warning

- F a finite field of characteristic p
- $P_1, \ldots, P_m \in F[x_1, \ldots, x_n]$
- $\sum_{i=1}^{m} \deg(P_i) < n$

Then the number Ω of their common zeros in F^n is divisible by p.

Proof.

- $\Omega \equiv \sum_{y_1,\ldots,y_n \in F} \prod_{j=1}^{m} \left(1 - P_j(y_1, \ldots, y_n)^{q-1}\right)$ where $q = |F|$.
- After expanding the product it is not difficult to check that for every resulting monomial M we have

$$\sum_{y_1,\ldots,y_n \in F} M \equiv 0.$$

□

Congruences

- If $|J| = 3p-3$ then
$$1-(p-1 \mid J)-(p \mid J)+(2p-1 \mid J)+(2p \mid J) \equiv 0.$$
- If $|J| \in \{3p-2, 3p-1\}$ then $1-(p \mid J)+(2p \mid J) \equiv 0$.

Proof.

- Let $J = \{(a_1, b_1), \ldots, (a_{3p-3}, b_{3p-3})\}$ and consider (over $\mathbb{F}_p$)
$$\sum_{i=1}^{3p-3} x_i^{p-1} + x_{3p-2}^{p-1}, \qquad \sum_{i=1}^{3p-3} a_i x_i^{p-1}, \qquad \sum_{i=1}^{3p-3} b_i x_i^{p-1}.$$
- $1+(p-1)^p(p \mid J)+(p-1)^{2p}(2p \mid J)$ zeros with $x_{3p-2}=0$.
- $(p-1)^p(p-1 \mid J)+(p-1)^{2p}(2p-1 \mid J)$ zeros with $x_{3p-2} \neq 0$. $\square$

A consequence of a congruence

If $|J| = 3p - 1$ then $1 - (p \mid J) + (2p \mid J) \equiv 0$.

Corollary (Alon, Dubiner)

If $|J| = 3p$ *and* $\sum J = (0,0)$ *then* $(p \mid J) > 0$*.*

Proof.

- Suppose not and let $J' \subseteq J$ with $|J'| = 3p - 1$.
- By assumption $(p \mid J') = 0$ and therefore $(2p \mid J') \equiv -1$.
- This implies $(2p \mid J) \neq 0$.
- But from $\sum J = (0,0)$ it follows that $(p \mid J) = (2p \mid J)$, contradiction. □

More congruences

If $|X| = 4p - 3$ then

$$\begin{aligned} 1 - (p \mid X) + (2p \mid X) - (3p \mid X) &\equiv 0 \\ (p-1 \mid X) - (2p-1 \mid X) + (3p-1 \mid X) &\equiv 0 \\ 3 - 2(p-1 \mid X) - 2(p \mid X) + (2p-1 \mid X) + (2p \mid X) &\equiv 0. \end{aligned}$$

Proof.

The first two follow from Chevalley-Warning applied to

$$\sum_{i=1}^{4p-3} x_i^{p-1} + \varepsilon x_{4p-2}^{p-1}, \qquad \sum_{i=1}^{4p-3} a_i x_i^{p-1}, \qquad \sum_{i=1}^{4p-3} b_i x_i^{p-1}$$

where $\varepsilon \in \{0, 1\}$. The third one comes from

$$\sum_{J \in \binom{X}{3p-3}} [1 - (p-1 \mid J) - (p \mid J) + (2p-1 \mid J) + (2p \mid J)] \equiv 0. \qquad \square$$

The crucial lemma

If $|X| = 4p - 3$ and $(p \mid X) = 0$, then $(p-1 \mid X) \equiv (3p-1 \mid X)$.

Proof.

- Let χ be the number of partitions $X = A \cup B \cup C$ with parts of size $p-1$, $p-2$ and $2p$, respectively, and

$$\sum A \equiv (0,0), \qquad \sum B \equiv \sum X, \qquad \sum C \equiv (0,0).$$

- We can determine $\chi \pmod p$ in two different ways:
  - $\chi \equiv \sum_A (2p \mid X - A) \equiv \sum_A -1 \equiv -(p-1 \mid X)$
  - $\chi \equiv \sum_B (2p \mid X - B) \equiv \sum_{X-B} -1 \equiv -(3p-1 \mid X)$ $\square$

Putting everything together

- Adding the three congruences

$$\begin{aligned} -1 + (p \mid X) - (2p \mid X) + (3p \mid X) &\equiv 0 \\ (p-1 \mid X) - (2p-1 \mid X) + (3p-1 \mid X) &\equiv 0 \\ 3 - 2(p-1 \mid X) - 2(p \mid X) + (2p-1 \mid X) + (2p \mid X) &\equiv 0. \end{aligned}$$

  and using $(p-1 \mid X) \equiv (3p-1 \mid X)$ gives

$$2 - (p \mid X) + (3p \mid X) \equiv 0.$$

- Therefore $(p \mid X)$ and $(3p \mid X)$ cannot vanish simultaneously.
- But then $(p \mid X) \neq 0$ by the consequence from a congruence.