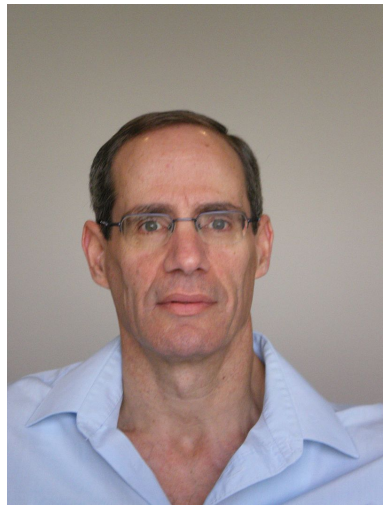
Alon's Combinatorial Nullstellensatz

Thomas Kalinowski

Discrete Maths seminar

The paper

Noga Alon, Combinatorial Nullstellensatz, *Combinatorics, Probability and Computing* **8**, 7–29 (1999)

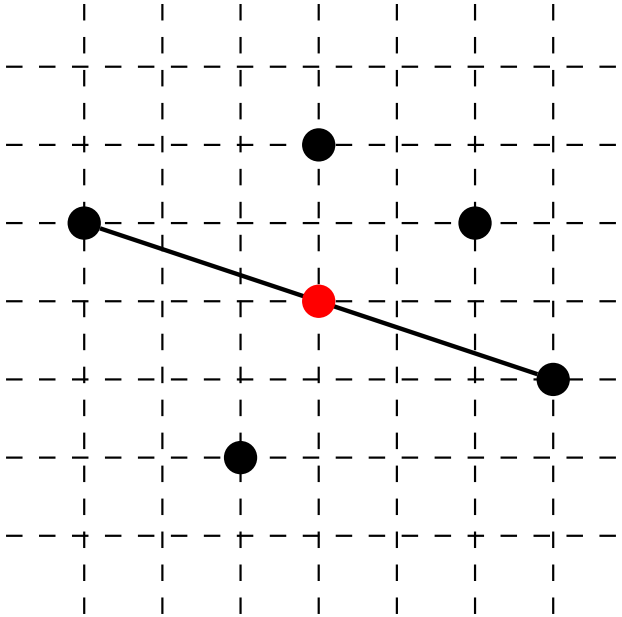


Abstract

We present a general algebraic technique and discuss some of its numerous applications in combinatorial number theory, in graph theory and in combinatorics. These applications include results in additive number theory and in the study of graph colouring problems. Many of these are known results, to which we present unified proofs, and some results are new.

- MathSciNet: 145 citations

A lattice point problem



Among five lattice points there are always two whose midpoint is also a lattice point.

(Pigeon hole argument)

- Harborth (1973): Let $f(n,d)$ be the smallest number f such that among f lattice points in $\mathbb{R}^d$ there are always n whose centroid is a lattice point.
- pigeon hole principle: $f(n,d) \leqslant (n-1)n^d + 1$
- Erdős, Ginzburg, Ziv (1961): $f(n,1) = 2n-1$
- Kemnitz (1983): Conjecture $f(n,2) = 4n-3$
- Alon, Dubiner (1993): $f(n,2) \leqslant 5n-6$ for $n \geqslant 3$
- Reiher (2004): The Kemnitz-conjecture is true.

Additive latin transversals

- G a finite abelian group of odd order.
- $\{a_1, \ldots, a_k\} \subseteq G, \qquad \{b_1, \ldots, b_k\} \subseteq G$

Conjecture (Snevily 1999)

There exists a permutation $\pi \in S_k$ such that the sums $a_i + b_{\pi(i)}$ are distinct.

- Alon (2000): It's true for groups of prime order.
- Dasgupta, Károlyi, Serra, Szegedy (2001): It's true for cyclic groups.
- Arsovski (2011): It's true.

Hilbert's Nullstellensatz

- F an algebraically closed field
- $f, g_1, \ldots, g_m \in F[x_1, \ldots, x_n]$
- f vanishes over all common zeros of $g_1, \ldots, g_m$

Then

$$f^k = \sum_{i=1}^{m} h_i g_i$$

for some integer k and polynomials h_i.

In other words: f vanishes on the variety described by the g_i if and only if f lies in the radical of the ideal generated by the g_i.

Alon's first Nullstellensatz

- F an arbitrary field, $f \in F[x_1, \ldots, x_n]$
- $S_1, \ldots, S_n \subseteq F$, $S_i \neq \emptyset$
- $g_i(x_i) = \prod_{s \in S_i} (x_i - s)$ for $i = 1, \ldots, n$
- $f(s_1, \ldots, s_n) = 0$ for all $(s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$

Then there are $h_1, \ldots, h_m \in F[x_1, \ldots, x_n]$ with

$$f = h_1 g_1 + \cdots + h_n g_n$$

and $\deg(h_i) \leqslant \deg(f) - \deg(g_i)$ for all i.

Alon's second Nullstellensatz

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

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

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

A lemma

- $P = P(x_1, \ldots, x_n)$ polynomial over an arbitrary field F
- $\deg_i(P) \leqslant t_i$ for every i
- $S_i \subseteq F$ with $|S_i| \geqslant t_i + 1$

If P vanishes on $S_1 \times \cdots \times S_n$ then $P \equiv 0$.

Proof by induction on n.

- $n = 1$: A polynomial of degree $\leqslant t$ with $t + 1$ zeros must be the zero polynomial.
- $n > 1$: $P = \sum_{k=0}^{t_n} P_k(x_1, \ldots, x_{n-1}) x_n^k$
  - From the single variable case it follows that all the P_k vanish on $S_1 \times \cdots \times S_{n-1}$.
  - Then $P_k \equiv 0$ for all k, by induction. □

Proof of the first Nullstellensatz

Theorem (short)

If $g_i(x_i) = \prod_{s \in S_i} (x_i - s)$ and f vanishes on $S_1 \times \cdots \times S_n$,

then $f = h_1 g_1 + \cdots + h_n g_n$ with $\deg(h_i) + \deg(g_i) \leqslant \deg(f)$.

Proof.

- For $t_i = |S_i| - 1$ we have $g_i(x_i) = x_i^{t_i+1} - \sum_{j=0}^{t_i} a_{ij} x_i^j$.
- $\bar{f}$ obtained from f by repeatedly replacing $x_i^{t_i+1}$ by $\sum_{j=0}^{t_i} a_{ij} x_i^j$
- $f - \bar{f}$ has the form $h_1 g_1 + \cdots + h_n g_n$ with $\deg(h_i) + \deg(g_i) \leqslant \deg(f)$.
- $\bar{f}$ vanishes on $S_1 \times \cdots \times S_n$ and $\deg_i(\bar{f}) < |S_i|$

$$\Longrightarrow \bar{f} \equiv 0 \text{ by the lemma.} \qquad \square$$

Proof of the second Nullstellensatz

Theorem (short)

If $\deg(f) = t_1 + \cdots + t_n$, the coefficient of $\prod_{i=1}^{n} x_i^{t_i}$ nonzero and $|S_i| > t_i$ then $f(s_1, \ldots, s_n) \neq 0$ for some $\boldsymbol{s} \in S_1 \times \cdots \times S_n$.

Proof.

- Let $|S_i| = t_i + 1$ and $g_i(x_i) = \prod_{s \in S_i} (x_i - s)$
- If f vanishes on $S_1 \times \cdots \times S_n$ then $f = \sum_i g_i h_i$.
- The maximum degree terms on the RHS are divisible by $x_i^{t_i+1}$.
- The coefficient of $\prod_{i=1}^{n} x_i^{t_i}$ on the RHS is zero, contradiction. □

The Chevalley-Warning theorem

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

If the polynomials P_i have a common zero $(c_1, \ldots, c_n)$, then they have another common zero.

Proof.

- $f = \prod_{i=1}^{m} \left[1 - P_i(x_1, \ldots, x_n)^{p-1}\right] - \delta \prod_{j=1}^{n} \prod_{a \in \mathbb{F}_p \setminus \{c_j\}} (x_j - a)$
- δ is chosen such that $f(c_1, \ldots, c_n) = 0$.
- $\deg(f) = n(p-1)$ and the coefficient of $\prod_{j=1}^{n} x_j^{p-1}$ is $-\delta \neq 0$. $\square$

The Cauchy-Davenport theorem

Let p be a prime, $A, B \subseteq \mathbb{F}_p$, $A, B \neq \emptyset$. Then

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

Proof.

- If $|A| + |B| \geqslant p + 1$, then $A \cap (x - B) \neq \emptyset$ for every $x \in \mathbb{F}_p$, and therefore $A + B = \mathbb{F}_p$.
- Suppose $A + B \subseteq C \subseteq \mathbb{F}_p$ with $|C| = |A| + |B| - 2$.
- Put $f(x, y) = \prod_{c \in C} (x + y - c)$.
- Apply the Nullstellensatz with $S_1 = A$ and $S_2 = B$. □

Restricted sums

For a polynomial $h = h(x_0, \ldots, x_k)$ over $\mathbb{F}_p$ and for subsets $A_0, \ldots, A_k \subseteq \mathbb{F}_p$ define

$$\oplus_h \sum_{i=0}^{k} A_i = \{a_0 + \cdots + a_k \ : \ h(a_0, \ldots, a_k) \neq 0\}.$$

Theorem (Alon, Nathanson, Ruzsa 1996)

Let $|A_i| = c_i + 1$ and put $m = \sum_{i=0}^{k} c_i - \deg(h)$. If the coefficient of $\prod_{i=0}^{k} x_i^{c_i}$ in $(x_0 + \cdots + x_n)^m h(x_0, \ldots, x_k)$ is nonzero then

$$\left| \oplus_h \sum_{i=0}^{k} A_i \right| \geqslant m + 1.$$

Proof: $Q(x_0, \ldots, x_k) = h(x_0, \ldots, x_k) \prod_{e \in E} (x_0 + \cdots + x_k - e)$ □

Sums with distinct terms

- $A_0, \ldots, A_k \subseteq \mathbb{F}_p$, $A_i \neq \emptyset$
- $|A_i| \neq |A_j|$ for $0 \leqslant i < j \leqslant k$
- $\sum_{i=0}^{k} |A_i| \leqslant p + \binom{k+2}{2} - 1$

Then

$$\#\{a_0 + \cdots + a_k \ : \ a_i \in A_i, \ a_i \neq a_j \text{ for all } i \neq j\} \geqslant \sum_{i=0}^{k} |A_i| - \binom{k+2}{2} + 1.$$

Theorem (Erdős-Heilbronn conjecture)

$$\#\{a + a' \ : \ a, a' \in A, \ a \neq a'\} \geqslant \min\{p, 2|A| - 3\}.$$

Proof

$A_0, \ldots, A_k \subseteq \mathbb{F}_p, \qquad |A_i| \neq |A_j|, \qquad \sum_{i=0}^{k} |A_i| \leqslant p + \binom{k+2}{2} - 1$

$$\#\{a_0 + \cdots + a_k \ : \ a_i \in A_i,\ a_i \neq a_j \text{ for all } i \neq j\} \geqslant \sum_{i=0}^{k} |A_i| - \binom{k+2}{2} + 1.$$

- $h(x_0, \ldots, x_k) = \prod_{k \geqslant i > j \geqslant 0} (x_i - x_j)$
- $m = \sum_{i=0}^{k} c_i - \deg(h) = \sum_{i=0}^{k} |A_i| - \binom{k+2}{2} < p$
- It remains to be checked that the coefficient of $\prod_{i=0}^{k} x_i^{c_i}$ in

$$(x_0 + \cdots + x_k)^m h(x_0, \ldots, x_k)$$

is nonzero.

The coefficient is nonzero

The coefficient of $\prod_{i=0}^{k} x_i^{c_i}$ in $(x_0 + \cdots + x_k)^m \prod_{k \geqslant i > j \geqslant 0} (x_i - x_j)$ is

$$C = \sum_{\sigma} (-1)^{\sigma} \frac{m!}{(c_0 - \sigma(0))!(c_1 - \sigma(1))! \cdots (c_k - \sigma(k))!}$$

where the sum is over the permutations σ with $\sigma(i) \leqslant c_i$ for all i.
On the other hand

$$\frac{m!}{c_0! \cdots c_k!} \prod_{k \geqslant i > j \geqslant 0} (c_i - c_j) = \frac{m!}{c_0! \cdots c_k!} \det(c_i^j)_{0 \leqslant i,j \leqslant k}$$

$$= \frac{m!}{c_0! \cdots c_k!} \det((c_i)_j)_{0 \leqslant i,j \leqslant k}$$

$$= \frac{m!}{c_0! \cdots c_k!} \sum_{\sigma} (-1)^{\sigma} (c_0)_{\sigma(0)} \cdots (c_k)_{\sigma(k)} = C.$$