The Combinatorial Nullstellensatz and some applications in classical problems

Orestis Lignos*

Abstract

This article is a short introduction to Alon's Combinatorial Nullstelensatz, as presented in [1]. We present the result and then embark on several applications in a variety of classical problems.

1 Introduction

The Combinatorial Nullstellensatz is a powerfool tool in many problems. Its name is coined after Hilbert's Nullstellensatz:

Theorem 1. (Hilbert's Nullstellensatz) If F is an algebraically closed field and $f, g_1, g_2, \ldots, g_m \in F[x_1, x_2, \ldots, x_n]$ such that f vanishes over all common roots of the g_i, then there is a $k \in \mathbb{N}$ and polynomials $h_i \in F[x_1, x_2, \ldots, x_n]$ such that

$$f^k = h_1 g_1 + h_2 g_2 + \ldots + h_m g_m.$$

We specialize now to the case that $m = n$ and each g_i is a polynomial depending only on the variable x_i. Then it turns out that we may assume that $k = 1$ (see [1] for a proof of this result):

Theorem 2. (Refined Hilbert's Nullstellensatz) If F is a field and $f = f(x_1, x_2, \ldots, x_n)$ and $g_i(x_i) = \prod_{s \in S_i} (x_i - s)$ are as above, then there exist polynomials h_i as above such that $\deg h_i \leq \deg f - \deg g_i$ and

$$f = h_1 g_1 + h_2 g_2 + \ldots + h_n g_n.$$

Armed with this tool, we may proof or main Theorem:

Theorem 3. (Combinatorial Nullstellensatz) If F is a field and $f = f(x_1, x_2, \ldots, x_n) \in F[x_1, x_2, \ldots, x_n]$ is a polynomial with $\deg f = t_1 + t_2 + \ldots + t_n$ for some $t_i \geq 0$ and $S_1, S_2, \ldots, S_n \subseteq F$ such that $|S_i| > t_i$ for each i, then there exist $s_i \in S_i$ such that

$$f(s_1, s_2, \ldots, s_n) \neq 0,$$

provided that the coefficient of $x_1^{t_1} x_2^{t_2} \ldots x_n^{t_n}$ *is non−zero.*

*Department of Mathematics, National and Kapodistrian University of Athens.

Proof. Assume that $f(s_1, s_2, \ldots, s_n) = 0$ for all $s_i \in S_i$. Without loss of generality assume that $|S_i| = t_i + 1$ for each i and let

$$g_i(x_i) = \prod_{s \in S_i} (x_i - s_i)$$

for each i. By Theorem 2 there exist polynomials h_i such that $\deg h_i \leq \deg f - \deg g_i$ and

$$f = h_1 g_1 + h_2 g_2 + \ldots + h_n g_n.$$

However, the coefficient of $x_1^{t_1} x_2^{t_2} \ldots x_n^{t_n}$ in the right hand side is zero because the degree of the right hand side is at most $\deg f = t_1 + t_2 + \ldots + t_n$ and each monomial of degree $\deg f$ is divisible by $x_i^{t_i+1}$ for some i. This contradicts our hypothesis and completes the proof. □

Remark 1.1. The Combinatorial Nullstellensatz may be viewed as a multivariable generalization of the well−known fact that for a nonzero one−variable polynomial of degree k and a set S such that $|S| \geq k + 1$, there is an $s \in S$ such that $f(s) \neq 0$.

2 Restricted sumsets and zero−sum problems

• A *restricted sumset* typically has the form

$$S = \{a_1 + a_2 + \ldots + a_n : a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n \text{ and } P(a_1, a_2, \ldots, a_n) \neq 0\}$$

for some finite nonempty subsets A_i of a field F and a polynomial P over F. When $P(x_1, x_2, \ldots, x_n) = 1$ then $S = A_1 + A_2 \ldots + A_n$, while if $P(x_1, x_2, \ldots, x_n) = \prod_{1 \leq i < j \leq n} (x_j - x_i)$ and $A_i = A$ for all i then S is denoted by $n^\wedge A$.

• *Zero-sum problems* are a class of combinatorial problems concering the structure of a finite abelian group. The typical question here is the following: given an abelian group G and a positive integer n, what is the smallest value of k such that every sequence of elements of G of size k contains n terms that sum to 0?

Example 2.1. (Cauchy−Davenport) If $A, B \subseteq \mathbb{Z}_p$ for some prime p, then

$$|A + B| \geq \min(p, |A| + |B| - 1).$$

Proof. We may assume that $|A| + |B| \leq p$, because otherwise the sets A and $x - B$ have non−empty intersection for each $x \in \mathbb{Z}_p$, and so there exist $a \in A$ and $b \in B$ such that $x = a + b \in A + B$. This proves that

$$|A + B| = p \geq \min(p, |A| + |B| - 1).$$

Now assume that $|A + B| \leq |A| + |B| - 2$. Let $C \subseteq \mathbb{Z}_p$ be a set such that $A + B \subseteq C$ and $|C| = |A| + |B| - 2$ and consider the polynomial

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

Note that by definition there are no $a \in A$ and $b \in B$ such that $P(a,b) \neq 0$. However, the coefficient of $x^{|A|-1}y^{|B|-1}$ is evidently non−zero as it is equal to $\binom{|C|}{|A|-1}$ which is not a multiple of p and $\deg P = |C| = (|A|-1)+(|B|-1)$. Theorem 3 now implies that there exist $a \in A$ and $b \in B$ such that $P(a,b) \neq 0$, a contradiction. □

Example 2.2. (Erdős−Heilbronn conjecture) If $A \subseteq \mathbb{Z}_p$ for some prime p, then

$$|2^{\wedge}A| = |\{a+b : a \in A,\, b \in A,\, a \neq b\}| \geq \min(p, 2|A|-3).$$

Proof. (this proof is due to Peter Scholze) We mimic the above proof. We may assume that $2|A|-3 \leq p$. Indeed, if this is not the case then $2|A| \geq p+4$, and so for each $x \in \mathbb{Z}_p$ the sets A and $x-A$ have cardinality $|A|$ each, implying that it is possible to find $p \in A$, $q = x-p' \in x-A$ such that $p \neq p'$ and $p = q \Longrightarrow x = p+p' \in 2^{\wedge}A$. This proves that $|A+B| = p \geq \min(p, 2|A|-3)$, as desired.

Now assume that $|2^{\wedge}A| \leq 2|A|-3$ and let $C \subseteq \mathbb{Z}_p$ be a set such that $2^{\wedge}A \subseteq C$ and $|C| = 2|A|-3$. Consider the polynomial

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

Note that by definition there are no $a, b \in A$ such that $P(a,b) \neq 0$. However, the coefficient of $x^{|A|-1}y^{|A|-2}$ in $P(x,y)$ is equal to

$$\binom{2|A|-4}{|A|-2} - \binom{2|A|-4}{|A|-1},$$

which can easily be seen that it is not a multiple of p, and so by Theorem 3 we obtain that there exist $a, b \in A$ such that $P(a,b) \neq 0$, a contradiction. □

Example 2.3. (Erdős−Ginzburg−Ziv theorem) Prove that $k = 2n-1$ is the least integer so that the following statement is always true: If $a_1, a_2, \ldots, a_k \in \mathbb{Z}_n$ then there exist $1 \leq i_1 < i_2 < \ldots < i_n \leq k$ such that $a_{i_1} + a_{i_2} + \ldots + a_{i_n} \equiv 0 \pmod{n}$.

Proof. (following the exposition in [2]) It is evident that $k \geq 2n-1$ for any k satisfying the assertion, as we may choose a sequence of $n-1$ zeros and $n-1$ ones.

Now we prove the assertion for $k = 2n-1$. Let us first reduce the problem to the case that n is prime. Assume that we have proven the statement in that case. We proceed by induction on n. The cases $n \in \{1,2\}$ are easy to check. Assume that $n = mp$ for some prime p. By our hypothesis we may successively partition our $2n-1$ numbers into groups of p numbers at a time summing to $0 \pmod{p}$. As $2n-1 \equiv -1 \pmod{p}$, we repeat until we are left with $p-1$ numbers, thus forming $(2n-p)/p = 2m-1$ groups. If the sum of the numbers in the i−th group is equal to pb_i, for $1 \leq i \leq 2m-1$, then applying the inductive hypothesis for $m < n$ we choose m of the b_i so that their sum is a multiple of m. Collecting now all these a_i corresponding to these b_i we prove the result.

It remains to settle the case that $n = p$ for some prime p. Note that if $a_1, a_2, \ldots, a_{2p-1}$ satisfy the statement, then $a_1 - c, a_2 - c, \ldots, a_{2p-1} - c$ satisfy it, too. We may thus assume that $a_{2p-1} = 0$ and moreover that $0 \leq a_i \leq p-1$ for each i. Without loss of generality assume that

$$0 \leq a_1 \leq a_2 \leq \ldots \leq a_{2p-2} \leq p-1.$$

Consider the polynomial

$$P(x_1, x_2, \ldots, x_{p-1}) = \prod_{1 \leq i \leq p-1} (x_1 + x_2 + \ldots + x_{p-1} - i).$$

Then $\deg P = p-1$ and the coefficient of $x_1 x_2 \ldots x_{p-1}$ equals $(p-1)!$ which is not divisible by p. Consider the sets

$$A_1 = \{a_1, a_p\},\ A_2 = \{a_2, a_{p+1}\},\ \ldots,\ A_{p-1} = \{a_{p-1}, a_{2p-2}\}.$$

If each of those sets has cardinality exactly 2, then applying Theorem 3 we obtain that there exists a $k = (k_1, k_2, \ldots, k_{p-1})$ such that $k_i \in A_i$ for each i and $P(k_1, k_2, \ldots, k_{p-1}) \neq 0$. This implies that $k_1 + k_2 + \ldots + k_{p-1} \equiv 0 \pmod{p}$ and so $(k_1, k_2, \ldots, k_{p-1}, a_{2p-1})$ satisfies the conclusion.

Lastly, if $|A_i| = 1$ for some i then $a_i = a_{i+p-1}$ and so $a_i = a_{i+1} = \ldots = a_{i+p-1}$. Therefore $a_i + a_{i+1} + \ldots + a_{i+p-1} = 0$, as desired. □

Remark 2.4. It is possible to prove the above theorem using Cauchy−Davenport. Indeed, we work in the case $n = p$ as above and in the same setting with sets A_i. If $|A_i| \geq 2$ for each i then by Cauchy−Davenport it is easy to see that $|A_1 + A_2 + \ldots + A_{p-1}| = p$ and so there exist $k_i \in A_i$ such that $k_1 + k_2 + \ldots + k_{p-1} = 0 = -a_{2p-2}$.

3 Some combinatorial problems

Example 3.1. (IMO 2007/6) Let n be a positive integer. Consider

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

as a set of $(n+1)^3 - 1$ points in the three−dimensional space. Determine the smallest possible number of planes, the union of which contains S but does not include $(0, 0, 0)$.

Proof. We claim that the answer is $3n$. Note that we may take the $3n$ planes $x = i$, $y = i$, $z = i$ for $1 \leq i \leq n$ to obtain an example. We are left to show that we need at least that many planes.

Assume there exists a choice of $k < 3n$ planes satisfying the conditions. Let the planes be $a_i x + b_i y + c_i z + d_i = 0$ with $d_i \neq 0$ for $1 \leq i \leq k$, and define

$$P(x, y, z) = \prod_{1 \leq i \leq k} (a_i x + b_i y + c_i z + d_i) \text{ and } Q(x, y, z) = \prod_{1 \leq i \leq n} (x - i)(y - i)(z - i).$$

Now let

$$R(x,y,z) = P(x,y,z) - \frac{P(0,0,0)}{Q(0,0,0)}Q(x,y,z),$$

and note that due to our assumption and the construction of the above polynomials R vanishes in each point (p,q,r) with $0 \leq p,q,r \leq n$. However, the coefficient of $x^n y^n z^n$ in the above polynomial is equal to $-\frac{P(0,0,0)}{Q(0,0,0)} \neq 0$, and so we get a contradiction by invoking Theorem 3. □

Example 3.2. (Fedor Petrov) Two numbers are written on each vertex of a convex 2026−gon. Prove that it is possible to remove a number from each vertex so that the remaining numbers on any two adjacent vertices are different.

Proof. Let A_i denote the set of the two numbers written on vertex i, and consider the polynomial

$$P(x_1, x_2, \ldots, x_{100}) = (x_1 - x_2)(x_2 - x_3)\ldots(x_{100} - x_1).$$

The coefficient of $x_1 x_2 \ldots x_{100}$ is evidently non−zero and so by the Combinatorial Nullstellensatz there exists a choice of $x_i \in S_i$ so that $P(x_1, x_2, \ldots, x_{100}) \neq 0$, as desired. □

Example 3.3. (USA TSTST 2012/9 and Theorem 5.1 in [1]) Let n be a positive integer. Suppose we are given $2^n + 1$ distinct sets, each containing finitely many objects. Place each set into one of two categories, the red sets and the blue sets, so that there is at least one set in each category. Prove that there are at least 2^n different sets which can be obtained as the symmetric difference of a red set and a blue set.

Proof. Assume there are k objects in total. We may interpret the problem as working with binary strings of length k. Note that $\mathbb{F}_2^k \simeq \mathbb{F}_{2^k}$. Let R and B denote the families of red and blue sets respectively. Therefore $R, B \subseteq \mathbb{F}_2^k$ and $|R| + |B| = 2^n + 1$, and we wish to prove that $|R+B| \geq 2^n$. Assume otherwise and let $R+B \subseteq C \subseteq \mathbb{F}_2^k$ be a set such that $|C| = 2^n - 1$.

Consider the polynomial

$$P(x,y) = \prod_{v \in c}(x + y - v)$$

over $\mathbb{F}_{2^k}$. Note that P vanishes for all $x \in R$, $y \in B$, and the coefficient of $x^{|R|-1}y^{|B|-1}$ is equal to $\binom{2^n-1}{|R|-1}$, which may easily be seen to be odd using Lucas's theorem. Theorem 3 now gives the desired contradiction. □

References

[1] Noga Alon, *Combinatorial Nullstellensatz*, Combinatorics, Probability and Computing, vol. 8, no. 1-2, 7−29, 1999.

[2] Dragomir Grozev, *Combinatorial Nullstellensatz. Part 2.* , blog post at https://dgrozev.wordpress.com/.