What is Combinatorial Nullstellensatz?

Kabir Belgikar

1 Introducing the Theorem

Recall the following basic fact from algebra:

Theorem 1.0: Let F be a field and $f \in F[x]$ a polynomial of degree t. Then, f has at most t roots.

We will prefer to think of this as follows:

Theorem 1.0 (reformulation): Let f be a field and $f \in F[x]$ a polynomial of degree t. Then, for any $S \subseteq F$ with $|S| > t$, there exists an $s \in S$ such that $f(s) \neq 0$ <u>if the coefficient of x^t is non-zero.</u>

Today's main attraction can be thought of as a generalization of this.

Theorem 1.1 (Combinatorial Nullstellensatz): Analogously to before, let F be a field and $f \in F[x_1, ..., x_n]$ a polynomial of degree $t = t_1 + \cdots + t_n$. Then, for any sets $S_1, ..., S_n \subseteq F$ with $|S_i| > t_i$, there exists an $n-$tuple $\mathbf{s} = (s_1, ..., s_n) \in S_1 \times \cdots \times S_n$ such that $f(\mathbf{s}) \neq 0$ <u>given that the coefficient of $x_1^{t_1} \cdots x_n^{t_n}$ is non-zero.</u>

In the original paper (Alon [1], pg.3) on the subject, Noga Alon also called the following theorem Combinatorial Nullstellensatz.

Theorem 1.2: Let F be an arbitrary field, $R \subseteq F$ any sub-ring, and $f \in R[x_1, ..., x_n]$. Let $S_1, ..., S_n \subseteq R$ be non-empty and define $g_i(x_i) = \prod_{s \in S_i}(x_i - s)$. If f vanishes over all the common zeros of $g_1, ..., g_n$ (that is; if $f(\mathbf{s}) = 0$ for all $\mathbf{s} \in S_1 \times \cdots \times S_n$), then there are polynomials $h_1, ..., h_n \in R[x_1, ..., x_n]$ satisfying $\deg(h_i) \leq \deg(f) - \deg(g_i)$ such that $f = \sum_{i=1}^{n} h_i g_i$.

In fact, theorem 1.2 was used to prove theorem 1.1. However, we will only think of theorem 1.1 as Combinatorial Nullstellensatz.

Note the similarities between theorem 1.2 and the more well-known theorem below:

Theorem 1.3 (Hilbert's Nullstellensatz): Let F be an algebraically closed field and $f, g_1, ..., g_m \in F[x_1, ..., x_n]$ such that f vanishes over all common zeroes of $g_1, ..., g_m$. Then, there exists a natural number k and polynomials $h_1, ..., h_m \in F[x_1, ..., x_n]$ such that $f^k = \sum_{i=1}^{n} h_i g_i$.

In essence, theorem 1.2 gives us a stronger conclusion in the special case when $n = m$ and each g_i is a univariate polynomial of the form $\prod_{s \in S_i}(x_i - s)$ (Alon [1], pg.1).

2 Warm up

Here is a problem from the 2007 All-Russian Olympiad ([2]):

Problem: Two distinct numbers are written on each vertex of a regular $100-$gon. Prove one can remove a number from each vertex so that the remaining numbers on any two adjacent vertices differ.

Solution: Let S_i be the set of numbers on the i^{th} vertex and note that $|S_i| = 2$. Consider the polynomial

$$P(c_1, c_2, ..., c_n) := (c_1 - c_2)(c_2 - c_3) \cdots (c_{99} - c_{100})(c_{100} - c_1).$$

Note that the coefficient of $c_1 c_2 \cdots c_{100}$ is 2. Hence, there exists $\mathbf{s} \in S_1 \times \cdots \times S_{100}$ such that $f(\mathbf{s}) \neq 0$ by Combinatorial Nullstellensatz. Since the polynomial doesn't vanish, adjacent vertices must have different numbers. $\square$

3 Applications to Additive Number Theory

Theorem 2.1 (Cauchy-Davenport): If A and B are non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$ with p prime, then $|A + B| \geq \min(p, |A| + |B| - 1)$.

Exercise 1: Prove the above theorem in the case where $\min(p, |A| + |B| - 1) = p$.

Proof: We will suppose $|A| + |B| - 1 < p$. Assume for the sake of contradiction that $|A + B| < |A| + |B| - 1$ and define

$$f(a, b) = \prod_{s \in A+B} (a + b - s).$$

Clearly, f has degree $|A + B|$. Furthermore, note that the coefficient of $a^{|A|-1} b^{|A+B|-|A|+1}$ is $\binom{|A+B|}{|A|-1}$, which is non-zero in $\mathbb{Z}/p\mathbb{Z}$ since $|A + B| < |A| + |B| - 1 < p$. However, using Combinatorial Nullstellensatz with $S_1 = A$ and $S_2 = B$ tells us that there exists $a \in A$ and $b' \in B$ with $f(a', b') \neq 0$. This is a contradiction because f is 0 everywhere on $A \times B$ by construction. $\square$

Note the assumption of primality is crucial. However, Inder Chowla found a generalization to non-prime moduli in 1937 [3].

Theorem 2.2 (Chowla): Let n be a positive integer and $A, B \subseteq \mathbb{Z}/n\mathbb{Z}$ such that $0 \in B$ and $\gcd(b, n) = 1$ for all $b \in B \setminus \{0\}$. Then, $|A + B| \geq \min(n, |A| + |B| - 1)$.

Next, we shall take a look at an application of the Cauchy-Davenport theorem:

Theorem 2.3 (Erdős-Ginzburg-Ziv): Given any $2n-1$ integers, one can pick exactly n whose sum is divisible by n.

Reduction to primes: We will first show that it suffices to prove theorem 2.3 in the case where n is prime. To this end, let $P(n)$ be the statement of the theorem for $n \in \mathbb{N}$. We will prove that $P(a)$ and $P(b)$ implies $P(ab)$. So suppose that we are given integers $x_1, x_2, ..., x_{2ab-1}$. Using $P(a)$, select a numbers $s_{1,1}, s_{1,2}, ..., s_{1,a}$ with sum divisible by a. This leaves us with $2ab - 1 - a$ numbers. Out of these, pick a numbers $s_{2,1}, s_{2,2}, ..., s_{2,a}$ with sum divisible by a. Perform this procedure a total of $2b-1$ times. Note that this is possible since $2ab - 1 - a(2b - 1) = a - 1 \geq 0$ (so we don't run out of numbers). By construction, for any $j \in \{1, 2, ..., 2b - 1\}$,

$$s_{j,1} + s_{j,2} + \cdots + s_{j,a} = ac_j$$

for some $c_j \in \mathbb{N}$. So we end up with $2b - 1$ sums $ac_1, ac_2, ..., ac_{2b-1}$. Using $P(b)$, pick b of these (say $ac_{\ell_1}, ac_{\ell_2}, ..., ac_{\ell_b}$) such that $c_{\ell_1} + \cdots + c_{\ell_b}$ is divisible by b. Each sum consists of a summands and so we have chosen exactly ab numbers. Furthermore, the sum of all our numbers is $a(c_{\ell_1} + \cdots + c_{\ell_b})$ which is plainly divisible by ab. $\square$

The above is rephrased version of the reduction found in [4]. Additionally, [4] also contains a different proof of the theorem that uses the Chevalley-Warning theorem.

Proof of Theorem 2.3: It suffices to prove the statement for an arbitrary prime p. So suppose that we are given $x_1, x_2, ..., x_{2p-1} \in \mathbb{Z}/p\mathbb{Z}$. We may assume that they are ordered so that $x_1 \leq x_2 \leq \cdots \leq x_{2p-1}$. Now define $A_i := \{x_i, x_{i+p-1}\}$ for all $i \in \{1, 2, ..., p - 1\}$. If $|A_i| = 1$ for some i, then $x_i = x_{i+p-1}$, implying that $x_i = x_{i+1} = \cdots = x_{i+p-1}$ since we ordered them. Hence, $x_i + x_{i+1} + \cdots + x_{i+p-1} = px_i = 0$ and so we have found our p numbers. So now suppose that $|A_i| = 2$ for all i. Then, repeated application of Cauchy-Davenport yields $|A_1 + \cdots + A_{p-1}| = p$. In particular, $-x_{2p-1} = a_1 + a_2 + \cdots + a_{p-1}$ where $a_i \in A_i$. Rearranging yields $x_{2p-1} + a_1 + a_2 + \cdots + a_{p-1} = 0$ as desired. $\square$

The above proof was taken from [5].

The following theorem was known as the Erdős-Heilbronn conjecture for about thirty years before it was solved in 1996 by J. A. Dias Da Silva and Y. O. Hamidoune [6]. However, their proof used some very fancy methods. As it happens, Heilbronn was Inder Chowla's advisor [7].

Theorem 2.4: Given S_1, S_2, define $S_1 \dot{+} S_2 = \{s_1 + s_2 : s_1 \in S_1, s_2 \in S \text{ and } s_1 \neq s_2\}$. Then for any $A \subseteq \mathbb{Z}/p\mathbb{Z}$, we have $|A \dot{+} A| \geq \min(p, 2|A| - 3)$.

Proof: We will only consider the case where $2|A| - 3 < p$. Now assume for the sake of contradiction that $|A \dot{+} A| < 2|A| - 3$ and consider the polynomial

$$f(a,b) = (a-b) \prod_{s \in A \dot{+} A} (a+b-s).$$

Observe that f has degree $|A \dot{+} A|+1$. Additionally, note that the coefficient of $a^{|A|-1}b^{|A \dot{+} A|-|A|+2}$ is

$$\binom{|A \dot{+} A|}{|A|-2} - \binom{|A \dot{+} A|}{|A \dot{+} A|-|A|+1} = \frac{|A \dot{+} A|!(2|A|-3-|A \dot{+} A|)}{(|A|-1)!(|A \dot{+} A|-|A|+2)!}.$$

Since this is non-zero by our assumption, Combinatorial Nullstellensatz tells us that f is non-zero somewhere on $A \times A$. However, this is clearly a contradiction. □

The above proof is a modified version of Peter Scholze's solution to corollary 6 on Art of Problem Solving [8]. This is very likely the same person who won a Fields medal in 2018 for his work on Perfectoid Spaces.

4 A Difficult IMO problem

One of the hardest IMO problems to date has been #6 from 2007. Out of approximately 500 participants, only 5 were able to solve it perfectly [9]. One of them was Peter Scholze.

Problem (IMO 2007 #6): Let n be a positive integer. Consider

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

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

Solution: The fewest number of possible planes is $3n$. Consider, for example, the planes given by $x+y+z = \ell$ for $\ell \in \{1,2,...,3n\}$. Assume for the sake of contradiction that fewer planes suffice, say $k < 3n$. Given one of these planes $\mathscr{P}$, let $a_{\mathscr{P}}x + b_{\mathscr{P}}y + c_{\mathscr{P}}z - d_{\mathscr{P}} = 0$ be it's equation. Now define

$$P(x, y, z) := \prod_{\mathscr{P}} (a_{\mathscr{P}}x + b_{\mathscr{P}}y + c_{\mathscr{P}}z - d_{\mathscr{P}})$$
$$Q(x, y, z) := \prod_{j=1}^{n} (x - j)(y - j)(z - j)$$

and consider

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

If $(x, y, z) \in S$, then $P(x, y, z) = Q(x, y, z) = 0$, implying $R(x, y, z) = 0$. Furthermore, simple algebra shows that $R(0, 0, 0) = 0$. Hence, R is 0 everywhere on I^3 where $I = \{0, 1, ..., n\}$.

Now, observe that the coefficient of $x^n y^n z^n$ in P is 0 since $\deg(P) = k < 3n$. However, the coefficient of $x^n y^n z^n$ in Q is 1 and so the coefficient of $x^n y^n z^n$ in R is $-P(0, 0, 0)/Q(0, 0, 0)$. This is non-zero since none of the planes hit the origin (meaning that $d_{\mathscr{P}}$ is always non-zero). Thus, Combinatorial Nullstellensatz tells us that there exists $\alpha, \beta, \gamma \in I$ such that $f(\alpha, \beta, \gamma) \neq 0$. However, this is a contradiction. $\square$

References

[1] ALON, NOGA. "Combinatorial Nullstellensatz." *Combinatorics, Probability and Computing,* vol. 8, no. 1-2, 1999, pp. 7–29., doi:10.1017/S0963548398003411.

[2] Agbdmrbirdyface. "Combinatorial whuuu...?" *Problems of the day,* 26 Nov. 2016, artofproblemsolving.com/community/c282525h1344647. Accessed 29 July 2022.

[3] I. CHOWLA. "A THEOREM ON THE ADDITION OF RESIDUE CLASSES: APPLICATION TO THE NUMBER $\Gamma(k)$ IN WARING'S PROBLEM." *The Quarterly Journal of Mathematics,* Volume os-8, Issue 1, 1937, Pages 99–102, https://doi.org/10.1093/qmath/os-8.1.99

[4] Amit, Alon. "Given $2n - 1$ natural numbers, how can one prove that you can choose n of them such that their sum is a multiple of n?" *Quora*, 21 Mar. 2016, qr.ae/pvMEXA. Accessed 29 July 2022.

[5] Uncudh. "The Erdos-Ginzburg-Ziv Theorem." *Uniformly at Random,* 25 Jan. 2009, uniformlyatrandom.wordpress.com/2009/01/25/the-erdos-ginzburg-ziv-theorem/.

[6] Da Silva, J. A. D., & Hamidoune, Y. O. (1994). *Cyclic Spaces for Grassmann Derivatives and Additive Theory.* Bulletin of the London Mathematical Society, 26(2), 140–146. doi:10.1112/blms/26.2.140

[7] *Mathematics Genealogy Project.* www.genealogy.math.ndsu.nodak.edu/id.php?id=27149.

[8] Scholze, Peter. "nice theorem." *Art of Problem Solving,* 9 Nov. 2004, artofproblemsolving.com/ community/c7h19496p133386. Accessed 29 July 2022.

[9] *International Mathematical Olympiad.* www.imo-official.org/ year_individual_r.aspx?year=2007&column=p6&order=desc&gender=hide&nameform=western.

[10] Yeo, Dominic. "The Combinatorial Nullstellensatz." *Eventually Almost Everywhere,* 25 Nov. 2013, eventuallyalmosteverywhere.wordpress.com/2013/11/25/the-combinatorial-nullstellensatz/.