Combinatorial Nullstellensatz

Evan Chen
chen.evan6@gmail.com

Berkeley Math Circle
September 17, 2013

Definition. A *field* is a structure in which one can add, subtract, multiply, and divide[1]. The operations are commutative and associative, and multiplication is distributive.

For example, the real numbers $\mathbb{R}$ and the rational numbers $\mathbb{Q}$ are a field. For any prime number p, $\mathbb{Z}_p$ is a field as well. Here $\mathbb{Z}_p$ denotes the integers modulo p.

Definition. Let $R[x_1, x_2, \dots, x_n]$ denote the set of polynomials in n variables $x_1, \dots, x_n$, with coefficients in R.

Thus $\mathbb{R}[x, y]$ is the set of real polynomials in x and y. This includes, say, $x^2 + \pi x^3 y$.

Fact (Fermat's Little Theorem)**.** Let p be a prime, and suppose x is an integer not 0 modulo p. Then

$$x^{p-1} \equiv 1 \pmod{p}.$$

1 Combinatorial Nullstellensatz

Consider the following "theorem":

Theorem 0. Let $f \in F[x]$ be a polynomial of degree t. If $S \subseteq F$ satisfies $|S| \geq t + 1$, then

$$\exists s \in S : f(s) \neq 0.$$

Combinatorial nullstellensatz generalizes this to multiple variables:

Theorem 1 (Combinatorial Nullstellensatz)**.** Let $f \in F[x_1, x_2, \dots, x_n]$ be a polynomial of degree $t_1 + \dots + t_n$. If $S_1, S_2, \dots, S_n$ are nonempty subsets of F such that $|S_i| \geq t_i + 1$ for all i, then there exists $s_1 \in S_1$, $s_2 \in S_2$, ..., $s_n \in S_n$ for which

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

as long as the coefficient of $x_1^{t_1} x_2^{t_2} \dots x_n^{t_n}$ is nonzero.

Note the extra condition at the end! The above theorems follows from the lemma:

Lemma 2. *Let $f \in F[x_1, \dots, x_n]$ be a polynomial, and $S_1, S_2, \dots, S_n$ be nonempty subsets of F. If $f(s_1, s_2, \dots, s_n) = 0$ for all $s_1 \in S_1, s_2 \in S_2, \dots, s_n \in S_n$ then there exist polynomials $h_1, h_2, \dots, h_n \in F[x_1, x_2, \dots, x_n]$ for which $f = \sum_{i=1}^{n} \left(h_i \cdot \prod_{s_i \in S_i} (x_i - s_i) \right)$.*

[1] Except for dividing by zero.

2 Problems

In what follows, p will denote an odd prime.

1. (Russia MO 2007/5) Two distinct numbers are written on each vertex of a convex 100-gon. Prove one can remove a number from each vertex so that the remaining numbers on any two adjacent vertices differ.

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

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

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 $(0, 0, 0)$.

3. (Cauchy-Davenport) If A and B are subsets of $\mathbb{Z}_p$, then

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

4. (Erdős-Heilbronn Conjecture) Let A be a subset of $\mathbb{Z}_p$. Then

$$|\{x + y \mid x, y \in A, x \neq y\}| \geq \min(p, 2|A| - 3).$$

5. (Chevalley-Warning) Let $f_1, f_2, \cdots, f_k$ be polynomials in $\mathbb{Z}_p[x_1, x_2, \cdots, x_n]$ with $\sum_{i=1}^k \deg f_i < n$. Show that if the polynomials f_i have a common zero $(c_1, c_2, \cdots, c_n)$, then they have another common zero.

6. (Alon) Show that any loopless graph with average degree at least $2p - 2$ and maximum degree at most $2p - 1$ contains a p-regular subgraph.

7. (Shirazi-Verstraëte) Let $G = (V, E)$ be a graph. For each vertex $v \in V$ we are given a *bad set* $B(v)$ of positive integers.
   (i) Prove that if $\sum_{v \in V} |B(v)| < |E|$, then there exists a nontrivial subgraph H for which $\deg_H v \notin B(v)$ for any v.
   (ii) Now suppose we allow $0 \in B(v)$ as well. Prove that if, $|B(v)| \leq \frac{1}{2} \deg v$ for any v, then we can still find such an H (not necessarily nontrivial).

8. (Alon, Knuth) Let $n \geq 2$ be even and let $v_1, v_2, \ldots, v_k \in \{\pm 1\}^n$ be vectors of length n such that any $v \in \{\pm 1\}^n$ is orthogonal to at least one of the v_i. Prove that $k \geq n$ and that this estimate is sharp.

3 Further Links

- Alon's original paper: `http://www.tau.ac.il/~nogaa/PDFS/null2.pdf`
- Slides from a presentation I gave: `http://db.tt/G4xx3fdJ`
- `http://www.math.uiuc.edu/~jobal/teach/nullstellensatz.pdf`