Paper Summary: Combinatorial Nullstellensatz

Original work by
Noga Alon
Tel Aviv University

Summarized by
Rachit Garg - CS14B050
IIT Madras

May 15, 2018

Contents

1 Introduction

Combinatorial nullstellensatz is an algebraic tool developed by Noga Alon that can be used to prove results in various fields ranging from combinatorial number theory, graph theory to combinatorics etc. In this summary we summarize the results and comment on the various application of combinatorial nullstellensatz mentioned in the paper.

2 Main Theorem

Combinatorial nullstellensatz is based on the observation of Hilbert's nullstellensatz which states that if F is an algebraically closed field, and f, g_1 , . . . , g_m are polynomials in the ring of polynomials $F[x_1, \ldots, x_n]$, where f vanishes over all common zeros of $g_1, \ldots, g_m$, then there is an integer k and polynomials $h_1, \ldots, h_m$ in $F[x_1, \ldots, x_n]$ so that $f^k = \sum_{i=1}^{n} h_i g_i$. This observation gives rise to the following theorem:

Theorem 2.1. *Let F be an arbitrary field, and let $f = f(x_1, \ldots, x_n)$ be a polynomial in $F[x_1, \ldots, x_n]$. Suppose the degree $deg(f)$ of f is coefficient of $\sum_{i=1}^{n} t_i$, where each t_i is a nonnegative integer, and suppose the coefficient of $\Pi_{i=1}^{n} {x_i}^{t_i}$ in f is nonzero. Then, if $S_1, \ldots, S_n$ are subsets of F with $|S_i| > t_i$, there are $s_1 \in S_1, s_2 \in S_2, \ldots, s_n \in S_n$ so that $f(s_1, \ldots, s_n) \neq 0$.*

3 Applications

3.1 Theorem of Chevalley and Warning

Theorem 3.1. *Let p be a prime, and let $P_1 = P_1(x_1, \ldots, x_n), \ldots, P_m = P_m(x_1, \ldots, x_n)$ be m polynomials in the ring $Z_p[x_1, \ldots, x_n]$. If $n > \sum_{i=1}^{m} deg(P_i)$ and the polynomials P_i have a common zero $(c_1, \ldots, c_n)$, then they have another common zero.*

This theorem was proved by Chevalley in 1935. The interesting observation we make in the proof of this theorem is that the main theorem 2.1, shows that there exists a solution where the polynomial is non zero. To prove we construct a polynomial which must be zero over a fixed space if our assumption is false and then use combinatorial nullstellensatz to arrive at a contradiction.
This method of contradiction is primarily the main idea which is applied to most proofs in the paper.

3.2 Additive number theory

Theorem 3.2. *If p is a prime, and A, B are two nonempty subsets of Z_p , then $|A + B| \geq min\{p, |A| + |B| - 1\}$.*

This result is called the Cauchy-Davenport Theorem, which has numerous applications in Additive Number Theory. Here again we use the same idea of coming up with a construction of a polynomial that has many roots if the assumption is false. This theorem gave a new proof to a lemma of Lagrange in his well known 1770 paper that shows that any integer is a sum of four squares.

3.3 Restricted Sums

We define operation $\oplus$ on sets for a k variate polynomial h as follows:

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

Theorem 3.3. *Let p be a prime and let $h = h(x_0, \ldots, x_k)$ be a polynomial over Z_p . Let $A_0, A_1, \ldots, A_k$ be nonempty subsets of Z_p , where $|A_i| = c_i + 1$ and define $m = \sum_{i=0}^{k} c_i - deg(h)$. If the coefficient of $\prod_{i=0}^{k} x_i^{c_i}$ in*

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

is non zero mod p then,

$$| \oplus_h \sum_{i=0}^{k} A_i| \geq m + 1$$

There are plenty of applications of this theorem in the paper. The proof of the theorem is consistent with the idea of using contradiction on a construction of a polynomial.

3.4 Set additions in vector spaces over prime fields

A triple (r, s, n) of positive integers satisfies the Hopf-Stiefel condition with respect to a prime p if

$\binom{n}{k}$ is divisible by p for every integer k satisfying $n - r < k < s$.

This condition is useful in Topology.
Let $\beta_p(r, s)$ denote the smallest integer n for which the triple (r, s, n) satisfies Hopf-Stiefel condition with respect to a prime p.

Theorem 3.4. *If A and B are two finite nonempty subsets of a vector space V over $GF(p)$, and $|A| = r$, $|B| = s$, then $|A + B| \geq \beta_p(r, s)$.*

In fact this result is sharp for all r and s.

3.5 Graphs and Subgraphs

Theorem 3.5. *For any prime p, any loopless graph $G = (V, E)$ with average degree bigger than $2p - 2$ and maximum degree at most $2p - 1$ contains a p-regular subgraph.*

The proof of this theorem follows a different idea than the previous proofs(earlier proofs used the method of contradiction), here we construct a polynomial that if in a fixed space it has a non zero evaluation then it can be shown to be of a p-regular subgraph. This shows the varied applicability of this tool. One more interesting non trivial application along these lines is the following theorem:

Theorem 3.6. *Let p be a prime, and let $G = (V, E)$ be a graph on a set of $|V| > d(p - 1)$ vertices. Then there is a nonempty subset U of vertices of G such that the number of cliques of d vertices of G that intersect U is 0 modulo p.*

Some versions of these results arise in the study of the minimum possible degree of a polynomial that represents the OR function of n variables.

3.6 Graph Coloring

The technique is applied to study the *choosability* properties of a graph. By choosability we mean the following:
If $G = (V, E)$ is a (finite, directed or undirected) graph, and f is a function that assigns to each vertex v of G a positive integer $f(v)$, we say that G is f-choosable if, for every assignment of sets of integers $S(v) \subset Z$ to all the vertices $v \in V$, where $|S(v)| = f(v)$ for all v, there is a proper vertex coloring $c : V \to Z$ so that $c(v) \in S(v)$ for all $v \in V$. The graph G is k-choosable if it is f-choosable for the constant function $f(v) \equiv k$. The choice number of G, denoted $ch(G)$, is the minimum integer k so that G is k-choosable. Obviously, this number is at least the classical chromatic number $\chi(G)$ of G. The choice number of the line graph of G, which we denote here by $ch'(G)$, is usually called the list chromatic index of G, and it is clearly at least the chromatic index $\chi'(G)$ of G.

Theorem 3.7. *Let G be a graph on $3n$ vertices, whose set of edges is the disjoint union of a Hamilton cycle and n pairwise vertex-disjoint triangles. Then the choice number and the chromatic number of G are both* 3.

Theorem 3.8. *The choice number of every planar bipartite graph is at most* 3.

The above the theorem along with the Four Color Theorem gives the following result:

Theorem 3.9. *For every 2-connected cubic planar graph G, ch'(G) = 3*

It is possible to extend this proof to any d-regular planar multigraph with chromatic index d.

3.7 Permanent Lemma

Lemma 3.10. *Let $A = (a_{ij})$ be an n by n matrix over a field $\mathbb{F}$, and suppose its permanent $Per(A)$ is nonzero (over $\mathbb{F}$). Then for any vector $b = (b_1, b_2, \ldots, b_n) \in \mathbb{F}_n$ and for any family of sets $S_1, S_2, \ldots, S_n$ of $\mathbb{F}$, each of cardinality* 2*, there is a vector $x \in S_1 \times S_2 \times \ldots \times S_n$ such that for every i the i^{th} coordinate of Ax differs from b_i.*

The above lemma follows from the main theorem 2.1. This lemma can be extended to interesting applications where we observe how it can be applied to give equalities rather than inequalities. This technique can be seen in the following theorem:

Theorem 3.11. *For any prime p, any sequence of $2p - 1$ members of Z_p contains a subsequence of cardinality p the sum of whose members is* 0*(in Z_p).*

3.8 Ideals of polynomials and combinatorial properties

Theorem 3.12. *(Li and Li) A graph G does not contain an independent set of $k+1$ vertices if and only if the graph polynomial f_G lies in the ideal generated by all graph polynomials of unions of k pairwise vertex disjoint complete graphs that span its set of vertices.*

Theorem 3.13. *(Kleitman and Lovsz) A graph G is not k colorable if and only if the graph polynomial f_G lies in the ideal generated by all graph polynomials of complete graphs on $k+1$ vertices.*

Theorem 3.14. *(Alon and Tarsi) A graph G on the n vertices $\{1, 2, \ldots, n\}$ is not k colorable if and only if the graph polynomial f_G lies in the ideal generated by the polynomials ${x_i}^k - 1$, $(1 \le i \le n)$.*

Theorem 3.15. *The 3-uniform hypergraph $H = (V, E)$ is not 2-colorable if and only if the polynomial*

$$\prod_{e \in E} [(\sum_{v \in e} x_v)^2 - 9]$$

lies in the ideal generated by the polynomials $\{{x_v}^2 1 : v \in V\}$.

4 Remarks

This paper presented many applications in various fields of mathematics. The proofs in the paper involved the method of contradiction by construction of clever polynomials that algebraically represented the problem. There were a few more ways in which the main theorem 2.1 was modified such as in the permanent lemma where we used the inequality to achieve an equality.

Most proofs presented in the paper algebraic and hence non-constructive in the sense that they supply no efficient algorithm for solving the corresponding algorithmic problems. An interesting extension to this paper would be to find an efficient algorithm to find a point $(s_1, s_2, \ldots, s_n)$ such that the polynomial evaluates to non zero value in theorem 2.1.