In which we introduce the basic idea of Combinatorial Nullstellensatz and study several examples.

Combinatorial Nullstellensatz [AT99] is a beautiful algebraic technique in the study of combinatorics. It stemmed from the *Hilbert's Nullstellensatz* which established the relations between algebra and geometry. In this post, I will first give a brief introduction to Hilbert's Nullstellensatz. Then, state two important theorem in combinatorial Nullstellensatz and use them to prove several interesting examples.

1 Hilbert's Nullstellensatz

We consider an algebraically closed field F [1] and a set of polynomials $g_1, \ldots, g_m \in F[x]$, where $x = (x_1, \ldots, x_n) \in F^n$ is a n-dimensional variable. It is then natural to ask: *Is these polynomials have common zeros?* When n is small, you probably can try to find all the roots of each polynomial and check whether there's a common root. However, can will have a more systematical way? That is, is there any theorem/algorithm that can help us assert whether $P_1, \ldots, P_m$ have a common root?

You're right, this is exactly what Hilbert's Nullstellensatz did! Formally, Hilbert's Nullstellensatz provided the following dichotomy:

Theorem 1 (weak Nullstellensatz) *Given the above conditions, exactly one of the following holds.*

- $\exists x \in F^n$ *such that* $g_1(x) = \cdots = g_m(x) = 0$.
- $\exists h_1, \ldots, h_m \in F[x]$ *such that* $h_1 g_1 + \cdots + h_m g_m = 1$.

Even more, we can extend the weak Nullstellensatz to the following strong Nullstellensatz.

Theorem 2 (strong Nullstellensatz) *Given the above conditions and a polynomial* $f \in F[x]$*, exactly one of the following holds.*

- $\exists x \in F^n$ *such that* $g_1(x) = \cdots = g_m(x) = 0$ *but* $f(x) \neq 0$.
- $\exists h_1, \ldots, h_m \in F[x]$ *and non-negative integer* r *such that* $h_1 g_1 + \cdots + h_m g_m = f^r$.

Here we omit the proof for simplicity. Readers who are interested is recommended to see the blog post from Terence Tao.

The critical message here is that the Hilbert's Nullstellensatz provided a nice dichotomy for a set of polynomials. Namely, they are either sharing a common zero or can be written in a inner-produce like equation. The latter turns out to be quite useful in lots of applications, e.g. the Combinatorial Nullstellensatz.

[1] For instance, $\mathbb{C}$. Note that the real $\mathbb{R}$ is not algebraically closed.

2 Combinatorial Nullstellensatz

When we restricted the conditions above as follow, one can yield the so called combinatorial Nullstellensatz.

- $m = n$
- Given nonempty sets $S_1, \ldots, S_n$ in F, take $g_i = \prod_{s \in S_i}(x_i - s)$

Theorem 3 *With the above conditions, if f vanishes over all common zeros of $g_1, \ldots, g_n$, then $\exists h_1, \ldots, h_m \in F[x]$ such that $deg(h_i) \leq deg(f) - deg(g_i)$ $\forall i \in [n]$ and $f = \sum_{i \in [n]} h_i g_i$.*

Theorem 3 provided a necessary condition for polynomial f to be simultaneously zero with $g_1, \ldots, g_n$. With the construction of $g_1, \ldots, g_n$, we can further show the following useful theorem for asserting the existence of nonzero solution over the set $S_1 \times \cdots \times S_n$.

Theorem 4 (combinatorial Nullstellensatz) *With the conditions above and. Suppose $deg(f) = \sum_{i \in [n]} t_i$ and the coefficients of $\prod_{i \in [n]} x^{t_i}$ is nonzero for some $t_i < |S_i|$. Then, $\exists s_1 \in S_1, \ldots, s_n \in S_n$ such that $f(s_1, \ldots, s_n) \neq 0$.*

With Theorem 4, it turns out that a large amount of theorems in combinatorics can be proven in an unexpected and elegant way.

3 Come classical examples

3.1 Polynomials in prime field

The first example considers polynomials in finite field Z_p where p is a prime.

Theorem 5 *Let $P_1, \ldots, P_m \in Z_p[x_1, \ldots, x_n]$. If $n > \sum_{i \in [n]} deg(P_i)$ and these polynomials share a common root $(r_1, \ldots, r_n) \in Z_p^n$, then there exists another common root.*

Proof: Define the following polynomial.

$$f(x_1, \ldots, x_n) = \prod_{i \in [m]} (1 - P_i(x_1, \ldots, x_n)^{p-1}) - \delta \prod_{j \in [n]} \prod_{r \in Z_p, r \neq r_j} (x_j - r) \tag{1}$$

, where δ is chosen so that $f(r_1, \ldots, r_n) = 0$. Note that δ is nonzero. Suppose the theorem statement is wrong, i.e. for any $(s_1, \ldots, s_n) \in Z_p^n \backslash \{(r_1, \ldots, r_n)\}$, $\exists i \in [m]$ such that $P_i(s_1 \ldots, s_n) \neq 0$. Observe that

- By Fermat's little theorem, $P_i(s_1, \ldots, s_n)^{p-1} = 1$. As a result, $f(s_1, \ldots, s_n) = 0$.
- As $n > \sum_{i \in [m]} deg(P_i)$, the degree of g is dominant by the second term and is $n(p-1)$.
- Take $t_i = p - 1$ and $S_1 = \cdots = S_n = Z_p$, we have $|S_i| > t_i$. Moreover, the coefficient of $\prod_{i \in [n]} x^{t_i}$ is $\delta \neq 0$.

Thus, by Theorem 4, we know that $\exists (s_1, \ldots, s_n) \in Z_p^n$ such that $f(s_1, \ldots, s_n) \neq 0$. As $f(r_1, \ldots, r_n) = 0$, $(s_1, \ldots, s_n) \neq (r_1, \ldots, r_n)$. Moreover, as the evaluation of the second term is 0, we must have $P_i(s_1, \ldots, s_n) = 0$. Otherwise, the evaluation of the first term is also zero, which is a contradiction. □

3.2 Cauchy-Davenport Theorem

The Cauchy-Davenport theorem, which was first proved by Cauchy in 1813 and later being proved with combinatorial Nullstellensatz in 1995 by Alon et. al., has numerous applications in additive number theory. Here, let's see how to prove it with our cute algebraic technique.

Theorem 6 (Cauchy-Davenport) *If p is a prime and A, B are two nonempty subsets of Z_p, then $|A+B| \geq \min\{p, |A|+|B|-1\}$.*

PROOF: First, if $|A|+|B| > p$, then it is easy to show that $A+B = Z_p$. Now, consider the case where $|A|+|B| \leq p$ and assume the theorem is wrong, i.e. $|A+B| \leq |A|+|B|-2$. Thus, we can take $C \subset Z_p$ such that $A+B \subseteq C$ and $|C| = |A|+|B|-2 < p$. Define polynomial f as follow:

$$f(x,y) = \prod_{c \in C}(x+y-c) \tag{2}$$

Directly from the definition we have $f(a,b) = 0, \forall a \in A, b \in B$. However, as we take $t_1 = |A|-1$ and $t_2 = |B|-1$, the coefficient of $x^{t_1}y^{t_2}$ is $\binom{|A|+|B|-2}{|A|-1} \neq 0$. As a result, by Theorem 4, $\exists a, \in A$ and $b \in B$ such that $f(a,b) \neq 0$, which is a contradiction. □

An interesting application of Cauchy-Davenport theorem is to prove the well-known fact proved by Lagrange that any rational number can be written as sum of four squares. Maybe I will introduce this result in the future.

4 Some examples in graph theory

4.1 Regular subgraph of almost regular graph

In [AFK84], Alon et. al. discussed the existence of regular subgraph in an almost regular graph. The following theorem proved with combinatorial Nullstellensatz showed that when we consider prime order, the regular subgraph will exist. As a remark, for general order, the problem is still open.

Theorem 7 *For any prime p, any graph $G = (V, E)$ with*

- *average degree ¿ $2p-2$, and*
- *maximum degree at most $2p-1$*

contains a p-regular subgraph.

PROOF: Let $A = (A_{v,e})_{v \in V, e \in E}$ denote the incident matrix among V and E. Associate each edge $e \in E$ with variables x_e taking value in $\{0,1\}$, i.e. $t_e = 2$. Define the following polynomial over Z_p.

$$f(x_e | e \in E) = \prod_{v \in V}[1 - (\sum_{e \in E} A_{v,e}x_e)^{p-1}] - \prod_{e \in E}(1-x_e) \tag{3}$$

First, compute the degree of f: $deg(f) = \max\{p-1, |E|\}$, where $2|E| > 2p-1$ by the assumption. We have $deg(f) = |E| = \sum_{e \in E} t_e$. As the coefficient of g is $(-1)^{|E|+1} \neq 0$, by Theorem 4, $\exists\{s_e | e \in E\} \in \{0,1\}^{|E|}$ such that $f(s_e | e \in E) \neq 0$.

- If $\{s_e | e \in E\}$ are all zero, then $f(\{s_e | e \in E\}) = 0$, which is a contradiction.
- If $\{s_e | e \in E\}$ are not all zero, take $G' = (V, E')$ to be the subgraph of G that consists the edge with nonzero solution. That is, $E' = \{e \in E | s_e \neq 0\}$. Note that as the second term of f will become 0, $\forall v \in V$, $\sum_{e \in E} A_{v,e} x_e = deg_{G'}(v) \equiv 0 (\text{mod } p)$. From the assumption, we know that the degree of $v \in V$ will thus be either 0 or p.

Finally, take the vertices having degree p in G', we yield a p-regular subgraph of G. □

References

[AFK84] Noga Alon, Shmuel Friedland, and Gil Kalai. Regular subgraphs of almost regular graphs. *Journal of Combinatorial Theory, Series B*, 37(1):79–91, 1984.

[AT99] Noga Alon and M Tarsi. Combinatorial nullstellensatz. *Combinatorics Probability and Computing*, 8(1):7–30, 1999.