Combinatorics 2018 Fall

Taught by: Professor Xiande Zhang

2018.12.10

Key words: Combinatorial Nullstellensatz

Recall:

- $0 \neq f \in \mathbb{F}_q[x_1, \cdots, x_n]$, deg$f$=$d$, then f has $\leq dq^{n-1}$ roots in $\mathbb{F}_q^n$
- $0 \neq f \in F[x_1, \cdots, x_n]$, deg$f$=$d$, then f has $\leq d|S|^{n-1}$ roots in S^n

Lemma4: Let $f \in F[x_1, \cdots, x_n]$ be a polynomial,and let t_i be the maximum degree of x_i in f. Let $S_i \subset F$ with $|S_i| \geq t_i + 1$. If $f(x) = 0, \forall x \in S_1 \times \cdots \times S_n$, then $f \equiv 0$.

proof :.
Induction on n. $n = 1$ is true.
Assume the claim holds for $n-1$ variables. Write $f = f_0 + f_1 x_n^1 + f_2 x_n^2 + \cdots + f_{t_n} x_n^{t_n}$, where $f_i \in F[x_1, \cdots, x_{n-1}]$. In each f_i, the maximum degree of x_j is $\leq t_j,\ j \in [n-1],\ i \in \{0, 1, \cdots, t_n\}$.
For any given $a \in S_1 \times S_2 \times \cdots S_{n-1}$. Let $g_a(x_n) = f(a, x_n)$, $\deg(g_a) = t_n$. $\forall x_n \in S_n, g_a(x_n) = f(a, x_n) = 0$ and $|S_n| \geq t_n + 1 \Longrightarrow g_a \equiv 0$
$g_a(x_n) = f_0(a) + f_1(a)x_n^1 + \cdots + f_{t_n}(a)x_n^{t_n} \Longrightarrow f_0(a) = f_1(a) = \cdots = f_{t_n}(a) = 0, \forall a \in S_1 \times S_2 \times \cdots S_{n-1}$.
By assumption, $f_i = 0, i \in [n-1] \Longrightarrow f = 0$ $\square$

Thm1:(Nullstellensatz) Let $f \in F[x_1, \cdots, x_n]$, and let $S_1, \cdots, S_n$ be nonempty subsets of F and $f(x) = 0, \forall x \in S_1 \times \cdots \times S_n$, then exist polynomials $h_1, \cdots h_n \in F[x_1, \cdots x_n]$ such that $deg(h_i) \leq$

$deg(f) - |S_i|$ and $f = \sum\limits_{i-1}^{n} h_i \prod\limits_{s \in S_i} (x_i - s.)$

proof :.

Let $t_i = |S_i| - 1$, and $g_i(x_i) = \prod\limits_{s \in S_i} (x_i - s) = x_i^{t_i+1} - \sum\limits_{j=0}^{t_i} a_{ij} x_i^j$.

In f, replace x_1^d $(d \geq t_1 + 1)$ by $x_1^{d-(t_1+1)}(g_1(x_1) + \sum\limits_{j=0}^{t_1} a_{1j} x_1^j)$, we get $f = h_1(x_1, \cdots, x_n) g_1(x_1) + f_1$, where max deg of x_1 in f_1 is $\leq t_1$ and degh_1 $\leq$deg$f$-$|S_1|$. Repeat this step for $x_i^{t_i+1}$, $i \in [2, n]$, we get $f = \sum\limits_{i=1}^{n} h_i g_i + \bar{f}$. In $\bar{f}$, each x_j has deg $\leq t_j$ and $\bar{f} = f = 0, \forall x \in S_1 \times \cdots S_n \implies \bar{f} \equiv 0$. $\square$

Thm2:(Combinatorial Nullstellensatz) Let $f \in F[x_1, \cdots, x_n]$ be a polynomial of degree d. Suppose $[x_1^{t_1} x_2^{t_2} \cdots x_n^{t_n}] f \neq 0$ and $\sum_{i=1}^{n} t_i = d$. If $S_i \subset F$ with $|S_i| \geq t_i + 1, i \in [n]$, then $\exists x \in S_1 \times \cdots S_n$ for which $f(x) \neq 0$.

proof :.

By contradiction. Assume $|S_i| = t_i + 1, i \in [n]$ and $f(x) = 0$ for all $x \in S_1 \times \cdots S_n$. By **Thm1**, write $f = \sum_{i=1}^{n} h_i g_i$, where deg$h_i \leq d - |S_i|$ and $g_i(x_i) = \prod_{s \in S_i}(x_i - s)$, then $f(x) = \sum_{i=1}^{n} h_i(x) x_i^{t_i+1}$+(terms of degree $< d$). By assumption, $[x_1^{t_1} x_2^{t_2} \cdots x_n^{t_n}] f$ on LHS is nonzero, but it is impossible to have such a monomial on RHS. $\square$

Application of Combinatorial Nullstellensatz

Thm3: (Chevalley-Warning) Let p be a prime and $f_1, \cdots, f_m \in \mathbb{F}_p[x_1, \cdots, x_n]$. If $\sum_{i=1}^{m}$deg$f_i < n$, and $f_1, \cdots, f_m$ have a common root $(c_1, \cdots, c_n)$, then they have another common root.

proof :.

By contradiction. Assume $(c_1, \cdots, c_n)$ is the only common root. Define $f(x_1, \cdots, x_n) = \prod\limits_{i=1}^{m} (1 - f_i(x_1, \cdots, x_n)^{p-1}) - \delta \prod\limits_{j=1}^{n} \prod\limits_{c \in F_p, c \neq c_j} (x_j - c)$, where δ is chosen s.t. $f(c_1, \cdots, c_n) = 0$. i.e. $\delta = \frac{1}{\prod\limits_{j=1}^{n} \prod_{c \in F_p, c \neq c_j} (c_j - c)}$

$\forall (s_1, \cdots, s_n) \in \mathbb{F}_p^n$ and $(s_1, \cdots, s_n) \neq (c_1, \cdots, c_n)$,
$\exists i \in [m]$ s.t. $f_i(s_1, \cdots, s_n) \neq 0$ in $\mathbb{F}_p$. By Fermat's little Theorem, $f_i(s_1, \cdots, s_n)^{p-1} \equiv 1 (mod p) \implies$ the first product on RHS is zero. It is easy to check that the second term is also zero, so $f_i(x_1, \cdots, x_n) = 0$, $\forall (x_1, \cdots, x_n) \in \mathbb{F}_p^n$.
Now check the degree of f. In the first product,the degree$\leq \sum_{i=1}^{m} deg f_i \cdot (p-1) < n(p-1) \implies \deg f = n(p-1)$, and the monomial $x_1^{p-1} x_2^{p-1} \cdots x_n^{p-1}$ has coefficient $-\delta \neq 0$. Let $S_i = \mathbb{F}_p$, then apply Combinatorial Nullstellensatz, $\exists x \in F_p^n, s.t. f(x) \neq 0$, a contradiction. $\square$

Recall: $A = (a_{ij})_{n \times n}$, $per(A) = \sum_{(i_1, \cdots, i_n)} a_{1,i_1} a_{2,i_2} \cdots a_{n,i_n}$, where $(i_1, \cdots, i_n)$ runs over all permutations of [n].

Thm4: (Permanent Lemma) Let $b \in F^n$ and $S_1, \cdots, S_n$ be subsets of F, and $|S_i| \geq 2$. If the $per(A) \neq 0$, then there $\exists x \in S_1 \times \cdots S_n$ such that Ax differs from b in all coordinates.

proof :.
Define $f = \prod_{i=1}^{n} (\sum\limits_{i=1}^{n} a_{ij} x_j - b_i)$, need to show $\exists x, s.t. f(x) \neq 0$.
$\deg f = n$ and $[x_1 \cdots x_n] f = per(A) \neq 0$. Since $|S_i| \geq 2, i \in [n]$, then apply Combinatorial Nullstellensatz. $\square$

Corollary5: If $per(A) \neq 0$, then for any $b \in F^n$, there is a subset of columns of A whose sum differs from b in all coordinates.
Hint: Let $S_i = \{0, 1\}$

Thm6: Let $G = (V, E)$ be a graph, no loops but multiple edges allowed. p is a prime, if average degree $> 2p-2$, max degree $\leq 2p-1$, then G contains a p-regular subgraph.

proof :.
To be continued. $\square$