Combinatorics 2017 Fall

week11 note

Teaching by: Professor Xiande Zhang

2017.11.28

Recall Fisher's Inequality: Let $A_1, \cdots, A_m$ be subsets of X such that $|A_i \cap A_j| = k$ for all $i \neq j \in [m]$, then $m \leq n$.

Def: Let $\mathscr{F} \subset 2^X$, and $L \subset \{0, 1, \cdots\}$ be a finite set of integers. say $\mathscr{F}$ is $L-$intersecting if $|A \cap B| \in L$ for all $A \neq B \in \mathscr{F}$. Note that Fisher's inequality tells that $|\mathscr{F}| \leq n$, if $|L| = 1$.

Thm1:(Frankl-Wilson) If $\mathscr{F}$ is an $L-$intersecting family of subsets of an $n-$elements set.then $|\mathscr{F}| \leq \sum_{i=0}^{|L|} \binom{n}{i}$. [Ex:Show the bound is best possible.]

Def:A function space is the set of all functions from $\Omega \to F$. A set of functions $f_1, f_2, \cdots, f_m$ is linearly independence if $\exists \lambda_i \ s.t. \lambda_1 f_1 + \lambda_2 f_2 + \cdots + \lambda_m f_m = 0$, then $\lambda_i = 0, i \in [m]$.

Lemma1:(Independence criterion) If $i \in [m]$, Let $f_i : \Omega \to F$,(where F is a field) be functions and $v_i \in \Omega$. such that

(i) $f_i(v_i) \neq 0, \forall i \in [m]$.

(ii) $f_i(v_j) = 0, \forall 1 \leq j < i \leq m$.

Then $f_1, \cdots, f_m$ are linearly independent in the function space F^Ω.

proof: If there is a nontrivial linear relation

$$\lambda_1 f_1 + \lambda_2 f_2 + \cdots + \lambda_m f_m = 0$$

Suppose i is the smallest index such that $\lambda_i \neq 0$. then

$$0 = \lambda_{i+1} f_{i+1}(v_i) + \lambda_{i+2} f_{i+2}(v_i) + \cdots + \lambda_n f_n(v_i) = -\lambda_i f_i(v_i) \neq 0$$

$\square$

proof of Thm1: Consider $\{f(x_1, \cdots, x_n)$ polynomials with degree $\leq d$ $\}$,then each of f is combination of $x_1^{t_1} \cdots x_n^{t_n}$, with $t_1 + \cdots + t_n \leq d$. Suppose $\mathscr{F} = \{A_1, \cdots, A_m\}$,with $|A_1| \leq \cdots \leq |A_m|$,and $L = \{l_1, \cdots l_s\}$. That is,$\forall i \neq j, \exists k \in [s], s.t. |A_i \cap A_j| = l_k$, Let v_i be the indicator vector of $A_i, i \in [m]$, then $< v_i, v_j >= |A_i \cap A_j|$. For $i = 1, \cdots, m$. define f_i with n variables by

$$f_i : \mathbb{R}^n \to \mathbb{R}.$$

$$f_i(x) = \prod_{k: l_k < |A_i|} (< v_i, x > - l_k).$$

if $j < i$, then $f_i(v_j) = 0$ and $f_i(v_i) \neq 0, i \in [m]$. Then $f_1, \cdots, f_m$ are linearly independent over $\mathbb{R}$.
f_i are polynomials of degree at most s. so $x_1^{r_1} \cdots x_n^{r_n}$ with $r_1 + \cdots + r_n \leq s$ are basic monomials,which has in total $\sum_{i=0}^{s} \binom{i+n-1}{i} = \binom{s+n}{s}$, but we can do it better! define new polynomials $\bar{f}_i$ form f_i by replacing all term x_i^k by x_i since v_i are $0-1$ vectors.we have $\bar{f}_i(v_i) = f_i(v_j), \forall i, j$ so $\bar{f}_i, \cdots, \bar{f}_m$ are linearly independent.who lie in a space with basis $x_1^{r_1} \cdots x_n^{r_n}$ with $r_1 + \cdots + r_n \leq s$ and $r_i \in \{0, 1\}$. so $m \leq \sum_{i=0}^{s} \binom{n}{i}$. $\square$

Thm2: Let p be a prime and $L \subset \mathbb{Z}_p = \{0, 1, \cdots, p-1\}$.Assume $\mathscr{F} = \{A_1, \cdots A_m\} \subset 2^{[n]}$ such that

(a) $|A_i| \notin L \pmod{p}, \forall i \in [m]$.

(b) $|A_i \cap A_j| \in L \pmod{p}, \forall i \neq j$.

Then $|\mathscr{F}| \leq \sum_{i=0}^{|L|} \binom{n}{i}$
[Hint:define $f_i(x) = \prod_{l \in L} (< v_i, x > - l) \pmod{p}, i \in [m]$.]

Recall Ramsey number $R(s,t)$

1. $R(t,t) > (t-1)^2$.
2. $R(s,t) > \Omega(t^3)$ 1972,Zsigmond Nagy
3. $R(t,t) > \Omega(2^{\frac{t}{2}})$.
4. $R(t,t) > t^{\Omega(\ln t/\ln\ln t)}$. 1977,Frankl, 1981 F&Wlison.

A graph is Ramsey graph with respect t, if it has no clique of size t and no independent set of size t.

Thm3: For any prime p,there is a graph G on $n = \binom{p^3}{p^2-1}$ vertices s.t. the size of maximum clique or maximum independent set is $\leq \sum_{i=0}^{p-1}\binom{p^3}{i}$.

proof: Let $G=(V,E)$ be as follows

- $V = \binom{[p^3]}{p^2-1}$
- for $A, B \in V, A \sim B$ iff $|A\cap B| \neq p-1 \pmod p$.

consider the clique $A_1, \cdots, A_m \in V, |A_i| = p^2-1 = p-1 \pmod p$, $|A\cap B| \neq p-1 \pmod p$ means $|A\cap B| \in L \pmod p$. where $L = \{0,1,\cdots p-2\} \subset \mathbb{Z}_p$.
By Thm2,we have $m \leq \sum_{i=0}^{p-1}\binom{p^3}{i}$.
Now consider an independent set $B_1,\cdots,B_s, |B_i\cap B_j| = p-1 \pmod p$,
so $|B_i \cap B_j| \in \{p-1, 2p-1, \cdots, p(p-1)-1\} = L^* \subset \mathbb{Z}_{\geq 0}$. and $|L^*| = p-1$, By Thm1, we have $s \leq \sum_{i=0}^{p-1}\binom{p^3}{i}$. $\square$

Colloary4: $R(t+1,t+1) > t^{\Theta(\ln t/\ln\ln t)}$.

proof: Let $t = \sum_{i=0}^{p-1}\binom{p^3}{i}, V = \binom{p^3}{p^2-1}$.

Recall $(\frac{n}{k})^k \leq \binom{n}{k} \leq (\frac{en}{k})^k$
$t \approx \binom{p^3}{p} \approx (p^2)^p = p^{2p}, V \approx \binom{p^3}{p^2} \approx p^{p^2},$
$\ln t \approx 2p \ln p = O(p \ln p), \ln\ln t \approx \ln p.$
$\Rightarrow p = \Theta(\frac{\ln t}{\ln\ln t}), V \approx (p^{2p})^{p/2} \approx t^{\theta(\ln t/\ln\ln t)}.$ $\square$

Recall a vector space over a field$(\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{F}_q)$

Thm5:(Odd/Even Town) Let $\mathscr{F} \subset 2^{[n]}, s.t. |A|$ is odd for all $A \in \mathscr{F}$, and $|A \cap B|$ is even for $A \neq B \in \mathscr{F}$, Then $|\mathscr{F}| \leq n$.

proof:$\forall A \in \mathscr{F}$, let e_A be the indictor vector of A,consider e_A as a vector in $\mathbb{F}_2^n$, Then

$$
\begin{aligned}
&< e_A, e_A >= 1, \quad \forall A \in \mathscr{F} \\
&< e_A, e_B >= 0, \quad \forall A \neq B \in \mathscr{F}
\end{aligned}
$$

Let $\mathscr{F} = m$,we will show vectors $e_A A \in \mathscr{F}$ are linearly independent in $\mathbb{F}_2^n$. If $\alpha_A \in \{0,1\}, s.t. \sum_{A \in \mathscr{F}} \alpha_A e_A = 0$
$\Rightarrow < e_A, \sum_{A \in \mathscr{F}} \alpha_A e_A >= 0 \quad \Rightarrow \alpha_A = 0$
This shows $e_A, A \in \mathscr{F}$ are linearly independent,so $|\mathscr{F}| \leq n$. $\square$

Colloary6:$R(t+1, t+1) > \binom{t}{3}$.

proof: Let $G = (V, E)$ be as follows
$V = \binom{[t]}{3}, A \sim B$, iff $|A \cap B| = 1$,
Consider a clique $A_1, \cdots, A_m.|A_i \cap A_j| = 1$ by Fisher's inequality, $m \leq t$.
Condsider an independent set $B_1, \cdots B_s$
$|B_i| = 3 \quad Odd, |B_i \cap B_j| = 0 \text{ or } 2 \quad Even.$
By Odd/Even Thm,$s \leq t$ $\square$

2017.12.1

<u>Graham-Pollak Thm:</u>
Biclique:i.e. a complete bipartite graph $K_{A,B}$ with vertex set $A \cup B$, and edge set $A \times B$.
<u>Def:</u>Let G be a graph and $G_1, \cdots, G_t$ be subgraph of G,say $G_1, \cdots, G_t$ is an edge-decomposition of G if each edge of G occurs in exactly one subgraph of G_i.

<u>Thm1:</u>(Graham-Pollak Thm) The edges of K_n can not be decomposed into fewer than $n-1$ edge-disjoint bicliques.
[Best possible:define K_{A_i,B_i} with $A_i = \{i\}, B_i = \{i+1, \cdots, n\}, i = 1, \cdots, n-1$, then $K_{A_i,B_i}, i \in [n-1]$ form a decomposition].

<u>proof:</u>Associate each vertex i of K_n with an indeterminate x_i and each edges $i \sim j$ with $x_i x_j$, Let $S(x) = \sum\limits_{1 \leq i < j \leq n} x_i x_j$. suppose $K_{A_i,B_i}, i \in [t]$ is an edge decomposition of K_n.$\forall i \in [t]$, Let $L_i(x) = \sum\limits_{j \in A_i} x_j$, $R_i(x) = \sum\limits_{j \in B_i} x_j$, then $L_i(x) \cdot R_i(x) = (\sum\limits_{j \in A_i} x_j)(\sum\limits_{j \in B_i} x_j) = \sum\limits_{\{i,j\} \in K_{A_i,B_i}} x_i x_j$. and $S(x) = \sum\limits_{i=1}^{t} L_i(x) \cdot R_i(x)$.
Let $T(x) = (\sum\limits_{i=1}^{n} x_i)^2 - 2\sum\limits_{i<j} x_i x_j = (\sum\limits_{i=1}^{n} x_i)^2 - 2S(x) = (\sum\limits_{i=1}^{n} x_i)^2 - 2\sum\limits_{i=1}^{t} L_i(x) \cdot R_i(x)$.
consider $t+1$ linear equations over $\mathbb{R}$.$L_i(x) = 0, i \in [t], \sum\limits_{i=1}^{n} x_i = 0$,If $t \leq n-2$, then it has a nonzero solution $x \in \mathbb{R}^n$, Put this vector into equation $T(x) = (\sum\limits_{i=1}^{n} x_i)^2 - 2\sum\limits_{i=1}^{t} L_i(x) \cdot R_i(x)$, we have $LRH = T(x) \neq 0$. Contradiction! $\square$

Fix a field F, Let $F[x_1, \cdots x_n]$ ={multivariate polynomial $f : F^n \to F$}.
A polynomial f vanishes on $E \subset F^n$ if $f(x_1, \cdots, x_n) = 0, \forall (x_1, \cdots, x_n) \in E$.

A point $(x_1, \cdots, x_n) \in F^n$ with $f(x_1, \cdots x_n) = 0$ is a root of f.

A polynomial f is a zero polynomial if all coefficients are 0.

Reacll:univeriate case $f(x) \neq 0, deg(f) = d$,then f has $\leq d$ roots.

1. If $0 \neq f$ vanishes on a subset S,then $|S| \leq deg(f)$.
2. If $\nexists f \neq 0$ that vanishes on S,then $|S| > deg(f)$.

Lemma1: Given $E \subset F^n$ of size $|E| < \binom{n+d}{d}$,there exists a $0 \neq f \in F[x_1, \cdots, x_n]$ with $deg(f) \leq d$ that vanishes on E.

proof: Let $V_d = \{f \in F[x_1, \cdots, x_n], deg(f) \leq d\}$, then dimension of V_d is $\binom{n+d}{d}$.
Let F^E be the set of vectors of length $|E|$,where each component of a vector $u \in F^E$ has value in F and is indexed by an element in E,that is $u = (u_x)_{x \in E}$, and $u_x \in F$.
Consider the evaluation map $V_d \to F^E, f \mapsto (f(a))_{a \in E}$. since dimension of F^E is $|E| < \binom{n+d}{d} = dim(V_d)$.
We have the map is non-injective.i.e.$\exists f_1 \neq f_2$, such that $(f_1(a))_{a \in E} = (f_2(a))_{a \in E}$,then $f = f_1 - f_2$ vanishes on E $\square$

Lemma2:$\forall 0 \neq f(x_1, \cdots, x_n) \in \mathbb{F}_q[x_1, \cdots, x_n]$ with $deg(f) = d$,has at most dq^{n-1} roots.($d \leq q$,if $d > q$ trivial.)

proof: Assume $n \geq 2$, Write $f = g + h$,where g is homogenous of degree d,and $deg(h) \leq d - 1$. Since $f \neq 0, g \neq 0, \exists \omega \in \mathbb{F}_q^n \backslash \{0\}, g(\omega) \neq 0$.
$\forall u \in \mathbb{F}_q^n$, Let $L_u = \{u + t\omega : t \in \mathbb{F}_q\}, |L_u| = q$
If $v \notin L_u$ then $L_u \cap L_v = \phi$. Hence $\mathbb{F}_q^n$ is partitioned into $q^n/q = q^{n-1}$ lines.It remains to show that the number of roots of f on each line is at most d.

$\forall u \in \mathbb{F}_q^n$,define a univariate polynomial $p_u(t) = f(u + t\omega)$,then $deg(p_u) \leq d$. since the coefficient t^d in $p_u(t)$ is $g(\omega) \neq 0, p_u(t) \neq 0$. so $p_u(t)$ has at most d roots in L_u, implying that f has at most root in L_u. since we have q^{n-1} lines,f has at most dq^{n-1} roots in $\mathbb{F}_q^n$ $\square$

Lemma3:$\forall S \subset F, |S| \geq d, \forall 0 \neq f \in F[x_1, \cdots, x_n]$ of degree d can have at most $d|S|^{n-1}$ roots in S^n.

proof: Induction on n, the number of variables in f.
$n = 1$ is true,let $n \geq 2$. write f according to the powers of $x_n.f = f_0 + f_1 x_n + \cdots + f_t x_n^t, t \leq d. f_t \neq 0$. and $f_i, i = 0, 1, \cdots, t$ are polynomials in $F[x_1, \cdots, x_{n-1}]$.
Now estimate the number of points $(a, b) \in S^{n-1} \times S, s.t. f(a, b) = 1$.

1. $f_t(a) = 0. deg(f_t) \leq d - t$,by assumption, f_t at most $(d-t)|S|^{n-2}$ roots in $|S|^{n-1}$,so there are at most $(d-t)|S|^{n-1}$ points $(a, b) \in S^{n-1} \times S$,for which $f(a, b) = 0$ and $f_t(a) = 0$.
2. $f_t(a) \neq 0$ Fix a point $a \in S^{n-1}$ satisfying $f_t(a) \neq 0$.then $g_a(x_n) = f(a, x_n)$ is of degree t ,So $g_a(x_n)$ has at most t roots,since there are at most $|S|^{n-1}$ such points a,the number of points $(a, b) \in S^{n-1} \times S$,for which $f(a, b) = 0$ and $f_t(a) \neq 0$. is at most $t|S|^{n-1}$.

Together, there are $\leq d|S|^{n-1}$ points $(a, b) \in S^{n-1} \times S$,for which $f(a, b) = 0$ $\square$

Combinatorial Nullstellensatz

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 is zero polynomial.

proof: By induction.$n = 1$ is true,Assume that the lemma holds for $n - 1$,we prove it for $n (n \geq 2)$. Write f as a polynomial in $x_n, f = \sum_{i=0}^{t_n} f_i(x_1, \cdots, x_{n-1}) x_n^i$. where in each f_i,the maximum degree of x_i is $t_j, j \in [n-1]$.
For each fixed $(n-1)-$tuple $(x_1, \cdots, x_{n-1}) \in S_1 \times \cdots \times S_{n-1}$,Let $g(x_n) = f(x_1, \cdots, x_{n-1}, x_n)$ vanishes on S_n,Hence $g(x_n) \equiv 0$ That is all coefficients $f_i(x_1, \cdots, x_{n-1})$ of $g(x_n)$ is zero, for all $(x_1, \cdots, x_{n-1}) \in$

$S_1 \times \cdots \times S_{n-1}$, Hence by induction hypothesis,$f_i \equiv 0, \forall i$, which implies that $f \equiv 0$. $\square$