Combinatorics 2017 Fall

week11 note

Teaching by: Professor Xiande Zhang

Reference:

Extremal Combinatorics with applications in Computer Science. 2nd Edition.Stasys Jukna,Springer.

2017/12/05

Theorem1(Nullstellensatz) Let $f \in F[x_1, \cdots, x_n]$, and let $S_1, \cdots, S_n$ be nonempty subsets of F. If $f(x) = 0, \forall x \in S_1 \times \cdots S_n$, then $\exists$polynomials $h_1, h_2, \cdots, h_n \in F[x_1, \cdots, x_n]$ such that $\deg(h_i) \leq deg(f) - |S_i|$ and $f = \sum_{i=1}^{m} h_i \prod_{s \in S_i}(x_i - s)$.

Proof: Let $t_i = |S_i| - 1$, define $g_i(x_i) = \prod_{s \in S_i}(x_i - s) = x_i^{t_i+1} - \sum_{j=0}^{t_i} a_{ij} x_i^j$. Replace each occurrence of $x_i^{t_i+1}$ by $g_i(x_i) + \sum_{j=0}^{t_i} a_{ij} x_i^j$. $f = h_1 g_1(x_1) + f_1, degh_1 \leq degf - |S_1|$ and max deg of $x_1 \leq t_1$. Repeat this procedure for all $x_i^{t_i+1}$, we get $f = \sum_{i=1}^{n} h_i g_i + \bar{f}$, with $degh_i \leq degf - |S_i|$ and maximum degree of x_i in $\bar{f}$ is $\leq t_i, i \in [n]$. Since $\bar{f} = f = 0$ for all $x \in S_1 \times \cdots S_n$, we have $\bar{f} \equiv 0$. Hence $f = \sum h_i g_i$. □

Theorem2(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 $\sum t_i = d$. 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: Assume $|S_i| = t_i + 1, i \in [n]$, Suppose $f(x) = 0$ for all $x \in S_1 \times \cdots S_n$, define $g_i(x_i) = \prod_{s \in S_i}(x_i - s)$ and $h_i(x_i, x_2, \cdots, x_n)$ guaranteed by Nullstellensatz. Hence $degh_i \leq degf - |S_i| = degf - (t_i + 1)$. Since $f(x) = \sum_{i=1}^{n} h_i(x) g_i(x)$, that is $f(x) = \sum_{i=1}^{n} x_i^{t_i+1} h_i(x)$+(terms of degree <degf). By assumption, the $[x_1^{t_1} x_2^{t_2} \cdots x_n^{t_n}] f$ on LHS is nonzero, but it is impossible to have such a monomial on RHS. □

Application of Combinatorial Nullstellensatz

Theorem3(Chevalley-Warning)Let p be a prime and $f_1, \cdots, f_m \in F[x_1, \cdots, x_n]$. If $\sum_{i=1}^{m} degf_i < n$, and $f_1, \cdots, f_m$ have a common root $(c_1, \cdots, c_n)$, then they have another common root.

Proof: Suppose $(c_1, \cdots, c_n)$ is the only common root of $f_1, \cdots, f_m$. Define $f(x_1, \cdots, x_n) = \prod_{i=1}^{m}(1 - f_i(x_1, \cdots, x_n)^{p-1}) - \delta \prod_{j=1}^{n} \prod_{c \in F_p, c \neq c_j}(x_j - c)$, where δ is chosen so that $f(c_1, \cdots, c_n) = 0$.

Hence $\delta = \frac{1}{\prod_{j=1}^{n}\prod_{c\in F_p, c\neq c_j}(c_j-c)} \neq 0$. Given $(s_1,\cdots,s_n)\in F_p^n$ and $(s_1,\cdots,s_n)\neq(c_1,\cdots,c_n)$, then $\exists i\in[m], f_i(s_1,\cdots,s_n)\neq 0$ in F_p. By Fermat's little Theorem, $f_i(s_1,\cdots,s_n)^{p-1}\equiv 1(modp)$,i.e.the first product on RHS is zero. It is easy to check that the second term is also zero. so $f_i(x_1,\cdots,x_n)=0$ for all $(x_1,\cdots,x_n)\in F_p^n$. Now check the degree of f. In the first product,the degree$\leq \sum_{i=1}^{m} degf_i\cdot(p-1) < n(p-1)$. , and the monomial $x_1^{p-1}x_2^{p-1}\cdots x_n^{p-1}$ has coefficient $\delta\neq 0$. Let $S_i = F_p$, then apply Combinatorial Nullstellensatz, $\exists x\in F_p^n, s.t. f(x)\neq 0$, a contradiction. □

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].

Theorem4(Permanent Lemma)Let $b\in F^n$ and $s_1,\cdots,S_n$ be subsets of F, each of cardinality at least 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 $f=\prod_{i=1}^{n}(a_{ij}x_j-b_i)$, need to show $\exists x, s.t. f(x)\neq 0, degf = n.[x_1\cdots x_n]f = per(A)\neq 0$. Since $|S_i|\geq 2, i\in[n]$. then apply Combinatorial Nullstellensatz. □

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.

Theorem6 Let $G=(V,E)$, 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: Associate each edge e with x_e. define $f=\prod_{v\in V}[1-(\sum_{e\in E} a_{v,e}x_e)^{p-1}]-\prod_{e\in E}(1-x_e)$ over F_P, where $a_{v,e}=1$, if $v\in e$ and $a_{v,e}=0$ if $v\notin e$. In the first product, the degree$\leq (p-1)|V| < |E|$. Since $\sum_{v\in V} d(v)=2|E|$, averge degree is $\frac{2|E|}{|V|} > 2p-2 \Longrightarrow (p-1)|V|<|E|$. So degf=$|E|$, and $[\prod_{e\in E} x_e]f=(-1)^{|E|+1}\neq 0$. Now apply Combinatorial Nullstellensatz with $S_i=\{0,1\}, t_e=1, e\in E$. then we get a 0-1 vector $x=(x_e: e\in E) s.t. f(x)\neq 0$. Now consider the spanning subgraph H consisting of all edges $e\in E$ with $x_e=1$. Since $f(0)=0, x\neq 0$, H is non-empty. So the second terms $\prod_{e\in E}(1-x_e)=0$, which means the first term $\prod_{v\in V}[1-(\sum_{e\in E} a_{v,e}x_e)^{p-1}]\neq 0$. By Fermat's little Theorem, $\sum_{e\in E} a_{v,e}x_e\equiv 0(modp), \forall v\in V$. Therefore, $\forall v\in V$, in H $deg(v)\equiv 0(modp)$. Since the maximum degree is smaller than 2p, all positive degrees are precisely p. □

2017/12/08

Sum-set::$A+B=a+b, a\in A, b\in B$, simple set.

Theorem5(Cauchy-Davenport)If p is a prime, and A, B are two non-empty subsets of F_p, then $|A+B|\geq min\{p, |A|+|B|-1\}$.

Proof:

(1) If $|A|+|B|\geq p+1$, then $\forall x\in Z_p, A\cap(x-B)\neq\emptyset. i.e. \forall x\in Z_p, \exists a\in A, b\in B, a=x-b, i.e. x=a+b$, which means $A+B=Z_p$. So $|A+B|\geq p$.

(2) $|A|+|B|\leq p$. Suppose $|A+B|\leq |A|+|B|-2, \exists C\subset Z_p, s.t. A+B\subset C$ and $|C|=|A|+|B|-2$. Define $f(x_1,x_2)=\prod_{c\in C}(x_1+x_2-c)$, then $f(x_1,x_2)=0$ if $(x_1,x_2)\in A\times B$. Let

$t_1 = |A|-1, t_2 = |B|-1$. degf=$t_1+t_2 = |C|$. $[x_1^{t_1}x_2^{t_2}]f = \binom{t_1+t_2}{t_1} = \binom{|A|+|B|-2}{|A|-1}$. Since $|A|+|B|-2 < p$, we have $p \nmid \binom{|A|+|B|-2}{|A|-1}$. Now apply Combinatorial Nullstellensatz with $n = 2$. $S_1 = A, S_2 = B$, we have a pair $(x_1, x_2) \in S_1 \times S_2, s.t. f(x_1, x_2) \neq 0$, a contradiction.□

Zero-sum-sets

Q1 Any sequence $a_1, \cdots, a_n$ of n integers contains a non-empty consecutive subsequence $a_i, a_{i+1}, \cdots, a_{i+m}$ whose sum is divisible by n.

Proof: By pigeonhole, n holes labeled from 0 to $n-1$, consider the n sequence $(a_1), (a_1, a_2), \cdots, (a_1, a_2, \cdots, a_n)$. If the sum of a sequence is $i(mod n)$, then put the sequence in the i-th holes, if $\exists$ a sequence put in the 0-th hole,then done. If not, by P-P, we have two sequences in the same hole, say $(a_1, a_2, \cdots, a_{i-1})$ and $(a_1, a_2, \cdots, a_i, \cdots, a_{i+m})$, then $(a_i, \cdots, a_{i+m})$ with sum divisible by n.

Q2 Given $n > 0$, what is the smallest N,s.t.any sequence of N integers contains a not necessarily consecutive subsequence of n integers whose sum is divisible by n?

e.g. $0, \cdots, 0, 1, \cdots, 1$, $N \leq 2n-1$.

Theorem6 p is a prime, any sequence of 2p-1 integers contains a subsequence of p integers, whose sum is divisible by p(By Cauchy-Davenport Theorem or by Chevalley-Warning Theorem).

Proof: Let $a_1 \leq a_2 \leq \cdots \leq a_{2p-1}$. If $\exists i \in [p-1], s.t. a_i = a_{i+p-1}$, then $a_i + a_{i+1} + \cdots + a_{i+p-1} = pa_i = 0$, done. If not, let $A_i = \{a_i, a_{i+p-1}\}, i \in [p-1]$, then $|A_1 + A_2 + \cdots + A_{p-1}| \geq min\{p, |A_2 + \cdots + A_{p-1}| + 1\} \geq min\{p, A_3 + \cdots + A_{p-1}| + 2\} \geq \cdots \geq min\{p, |A_{p-1}| + p - 2\} = p$. Hence $A_1 + A_2 + \cdots + A_{p-1} = Z_p$, then $-a_{2p-1}$ can be written at a sum of precisely $p-1$ of the first $2p-2$ elements of the sequence. □

Error-correcting codes

Let A be an alphabet, $C \subset A^n$ is called a code, $x \in C$ is called a codeword. The minimum distance, $dist(C) = min\{d_H(x, y) : x \neq y \in C\}$. $\forall x \in C$, the Hamming ball of the radius t centered at x is $B_t(x) = \{y \in A^n : d_H(x, y) \leq t\}$.

Fact: The code C can correct up to t errors $\iff \forall x, x' \in C, B_t(x) \cap B_t(x') = \emptyset$. $\iff \forall x, x' \in C, d_H(x, x') \geq 2t+1, i.e. dist(C) \geq 2t+1$.

Reason: Suppose $x \in C$ is transmitted and $y \in A^n$ is received. If at most t errors occurred, then $d_H(x, y) \leq t$. If $dist(C) \geq 2t+1$, then the only codeword in C with distance $\leq t$ from y is x. So we can correct y to x.

Main problem in coding theory: find large code with large distance.

Theorem1(Singleton bound) If $C \subseteq A^n$ and $d = dist(C) > 0$, then $|C| \leq |A|^{n-d+1}$.

Proof: Deleting the first $d-1$ letters of each codeword, the resulting codewords of length $n-d+1$ must be distinct, since $dist(C)=d$. So $|C| \leq |A|^{n-d+1}$. □

Reed-Solomon code:

$k \leq n \leq q, q$ is a prime power. Let $A=\mathbb{F}_q, |A|=q$. Fix n distinct elements $\alpha_1, \cdots, \alpha_n$ of $\mathbb{F}_q (n \leq q)$. Messages: $w=(w_1, \cdots, w_k) \in \mathbb{F}_q^k$. For each $w \in \mathbb{F}_q^k$, let $P_w(z)=w_1+w_2z+\cdots+w_kz^{k-1}$. $\deg P_w \leq k-1$. The codeword of w is the string $x_w=(P_w(\alpha_1), P_w(\alpha_2), \cdots, P_w(\alpha_n)) \in \mathbb{F}_q^n$. Let $C=\{x_w : w \in A^k\}$ be the resulting q-ary code. Since no two polynomial of degree at most $k-1$ can agree on k or more points, we have $dist(C) \geq n-k+1$. So we have a code $C \subseteq A^n$ of minimum distance $d=n-k+1$ and size $|C|=|A|^k=|A|^{n-d+1}$.

In RS code, we need $q \geq n$. How to reduce the alphabet size.

Binary-Red-Solomon code: replace each element of $\mathbb{F}_q$ by a binary string of length $\lceil \log_2 q \rceil$, let $n'=n\lceil \log_2 q \rceil$. Then we obtain a binary code $C \subseteq \{0,1\}^{n'}$ with length $n'=n\lceil \log_2 q \rceil$, size $|C|=q^k$ and $\text{dist}(C) \geq n-k+1. (n \leq q)$.