Combinatorics 2018 Fall

Taught by: Professor Xiande Zhang

2018.12.13

Key words: Combinatorial Nullstellensatz, Sumset, Zero-Sum Set

Recall (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 $|S_i| \geqslant t_i + 1$, $i \in [n]$, then $\exists\, x \in S_1 \times \cdots \times S_n$ *s.t.* $f(x) \neq 0$.

Theorem 6. Let $G = (V, E)$. G has no loops but multiple edges are allowed. Let p be a prime. If average degree of $G > 2p-2$, max degree of $G \leqslant 2p-1$, then G contains a p-regular subgraph.

proof: Associate $\forall\, e \in E$ with a variable x_e.
Define $f = \prod_{v \in V} [1 - (\sum_{e \in E} a_{v,e} x_e)^{p-1}] - \prod_{e \in E} (1 - x_e) \in \mathbb{F}_p[x_1, \cdots, x_{|E|}]$, where $a_{v,e} = 1$ if $v \in e$ and $a_{v,e} = 0$ if $v \notin e$.
Note that degree in the first product is $(p-1)|V|$, and degree in the second product is $|E|$. By Handshaking Lemma, average degree $\frac{\sum_{v \in V} d(v)}{|V|} = \frac{2|E|}{|V|} > 2p - 2 \Longrightarrow (p-1)|V| < |E|$. So $deg(f) = |E|$, and $[\prod_{e \in E} x_e]f = (-1)^{|E|+1} \neq 0$.
Apply Combinatorial Nullstellensatz with $S_i = \{0, 1\}$, $t_e = 1$ for $\forall\, e \in E \Longrightarrow \exists\, x = (x_e)_{e \in E} \in \{0, 1\}^{|E|}$ *s.t.* $f(x) \neq 0$.
Now consider the subgraph H consisting of all edges $e \in E$ with $x_e = 1$. If $x = (0, \cdots, 0)$, $f(x) = 0$. So $x \neq (0, \cdots, 0)$. $\Longrightarrow H$ is not empty.

So

$$0 \neq f(x) = \prod_{v \in V} [1 - (\sum_{e \in E} a_{v,e} x_e)^{p-1}],$$

which implies $(\sum_{e \in E} a_{v,e} x_e)^{p-1} \neq 1$ for $\forall\ v \in V$.
By Fermat's Little Theorem, $\sum_{e \in E} a_{v,e} x_e \equiv 0 \pmod p$ for $\forall\ v \in V$.
$\Longrightarrow \sum_{e \in E : v \in e} x_e = \sum_{e \in E} a_{v,e} x_e \equiv 0 \pmod p$ for $\forall\ v \in V$
$\Longrightarrow$ Each vertex has degree $0 \pmod p$ in H.
Since the maximum degree $\leqslant 2p-1$, all positive degrees are precisely p, *i.e.* H is p-regular. $\square$

Additive Combinatorics

Definition (Sumset). $A + B = \{a + b : a \in A, b \in B\}$.

Theorem 7 (Cauchy-Davenport). If p is a prime, and A, B are two non-empty subsets of $\mathbb{F}_p$, then $|A+B| \geqslant \min\{p, |A|+|B|-1\}$.

proof:

(1) If $|A| + |B| - 1 \geqslant p$, then $|A| + |B| \geqslant p + 1$, which implies $|A \cap B| \neq \emptyset$.
For $\forall\ x \in \mathbb{F}_p$, $|\{x\} - B| = |B|$. So $A \cap (\{x\} - B) \neq \emptyset$.
$\Longrightarrow \exists\ a \in A$, $a \in \{x\} - B$.
$\Longrightarrow \exists\ b \in B$, $a = x - b$, *i.e.* $x = a + b$.
$\Longrightarrow A + B = \mathbb{F}_p$. So $|A + B| \geqslant p$.

(2) If $|A| + |B| - 1 \leqslant p - 1$, then $|A| + |B| \leqslant p$. We need to show $|A + B| \geqslant |A| + |B| - 1$.
Assume $|A + B| \leqslant |A| + |B| - 2 \leqslant p - 2$, then $\exists\ C \subset \mathbb{F}_p$ with $|C| = |A| + |B| - 2$ *s.t.* $A + B \subset C$.
Define $f = \prod_{c \in C} (x_1 + x_2 - c) \in \mathbb{F}_p[x_1, x_2]$, then $f(x_1, x_2) = 0$ for $\forall\ (x_1, x_2) \in A \times B$ and $deg(f) = |C| = |A| + |B| - 2$.
Let $t_1 = |A| - 1$, $t_2 = |B| - 1$, then $[x_1^{t_1} x_2^{t_2}] f = \binom{|C|}{|A|-1} =$

$\binom{|A|+|B|-2}{|A|-1} \not\equiv 0 \pmod p$.
By Combinatorial Nullstellensatz, $\exists\,(x_1,x_2) \in A \times B$ *s.t.* $f(x_1,x_2) \neq 0$, a contradiction. $\square$

Zero-Sum Set

Question 1. 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 $0 \pmod n$.

proof: Assume there are n holes labeled from 0 to $n-1$.
Consider n sequences: $(a_1), (a_1, a_2), \cdots, (a_1, a_2, \cdots, a_n)$. If the sum of a sequence is $i \pmod n$, put it into the i-th hole.
If the 0-th hole is not empty, we're done.
Suppose not. Then by Pigeonhole Principle, there are two sequences in the same hole, say, $(a_1, \cdots, a_{i-1})$ and $(a_1, \cdots, a_{i-1}, a_i, \cdots, a_{i+m})$, which means they have the same sum $\pmod n$. Then the subsequence $(a_i, \cdots, a_{i+m})$ has sum $0 \pmod n$. $\square$

Question 2. Given $n > 0$, what is the smallest N such that any sequence of N integers contains a subsequence of n integers (not necessarily consecutive) whose sum is $0 \pmod n$?

Example. Consider $(a_1, \cdots, a_{2n-2})$ where $a_i = 0$ for $i = 1, \cdots, n-1$ and $a_i = 1$ for $i = n, \cdots, 2n-2$. $\Longrightarrow N > 2n-2$.

Theorem 8. p is a prime, then any integer sequence of length $2p-1$ contains a subsequence of length p whose sum is $0 \pmod p$.

proof 1: Assume $a_1 \leqslant a_2 \leqslant \cdots \leqslant a_{2p-1}$.
If $\exists\, i \in [p-1]$ such that $a_i = \cdots = a_{i+p-1}$, we're done.
Suppose not. Define $A_i = \{a_i, a_{i+p-1}\}$ for $i \in [p-1]$. Then by Cauchy-Davenport Theorem, we have $|A_1 + A_2 + \cdots + A_{p-1}| \geqslant \min \{p, |A_2 + \cdots + A_{p-1}| + 1\} \geqslant \min \{p, |A_3 + \cdots + A_{p-1}| + 2\} \geqslant \cdots \geqslant$

$\min\{p, |A_{p-1}| + p - 2\} = p$. Hence $A_1 + A_2 + \cdots + A_{p-1} = \mathbb{F}_p$. So $\exists\ a_{i_j} \in A_j$ such that $-a_{2p-1} = a_{i_1} + a_{i_2} + \cdots + a_{i_{p-1}}$. $\square$

proof 2: Define $f_1 = \sum_{i=1}^{2p-1} a_i x_i^{p-1}$ and $f_2 = \sum_{i=1}^{2p-1} x_i^{p-1} \in \mathbb{F}_p[x_1, \cdots, x_{2p-1}]$, then $f_1(0) = f_2(0) = 0$, and $deg(f_1) + deg(f_2) = 2(p-1) < 2p-1$. So $\exists\ x = (x_1, \cdots, x_{2p-1}) \neq 0$ such that $f_1(x) = f_2(x) = 0$. Here, we use the fact that if $f_1, \cdots, f_m \in F[x_1, \cdots, x_n]$, $\sum_{i=1}^{m} deg(f_i) < n$, and $(c_1, \cdots, c_n)$ is a common root of all f_i, then $\exists$ another common root.
Let $I = \{i \in [2p-1] : x_i \neq 0\}$. Then $f_2(x) = 0 \Longrightarrow |I| \equiv 0 \pmod{p}$ $\Longrightarrow |I| = p$, and $f_1(x) = 0 \Longrightarrow \sum_{i \in I} a_i \equiv 0 \pmod{p}$. $\square$

Theorem 8' (generalization of Theorem 8). n is an integer, then any integer sequence of length $2n-1$ contains a subsequence of length n whose sum is $0 \pmod{n}$.

proof: Prove by induction on the number of primes in n.
If $n = p$, we're done. ($i.e.$ Theorem 8)
Assume $n = pm \geqslant 2p$, and Theorem 8' holds for m.
Consider sequence $a_1, \cdots, a_{2p-1}$, and apply Theorem 8 for p, we get $I_1 \subset \{a_1, \cdots, a_{2p-1}\}$ with $|I_1| = p$ and $\sum_{i \in I_1} a_i \equiv 0 \pmod{p}$.
Now consider sequence $\{a_1, \cdots, a_{2p-1}\} \backslash I_1, a_{2p}, \cdots, a_{2n-1}$, and apply Theorem 8 for p again, we get I_2 with $|I_2| = p$, $I_2 \cap I_1 = \emptyset$ and $\sum_{i \in I_2} a_i \equiv 0 \pmod{p}$.
Repeat this process until we can't do it any more, we get disjoint $I_1, \cdots, I_l$ with $|I_j| = p$ and $\sum_{i \in I_j} a_i \equiv 0 \pmod{p}$ for $\forall\ j \in [l]$.
Claim: $l \geqslant 2m - 1$.
Proof of Claim: If $l \leqslant 2m-2$, then $(2n-1) - lp \geqslant (2pm-1) - (2m-2)p = 2p-1$, which means we can get I_{l+1}, a contradiciton.
Let $b_j = \dfrac{\sum_{i \in I_j} a_i}{p}$ for $j \in [l]$, then b_j is an integer.
Since $l \geqslant 2m-1$, by assumption, $\exists\ J \subset [2m-1]$ with $|J| = m$ such that $\sum_{j \in J} b_j \equiv 0 \pmod{m}$.

$$\implies \sum_{j\in J}\sum_{i\in I_j}\frac{a_i}{p} = \sum_{j\in J} b_j \equiv 0 \pmod{m}$$
$$\implies \sum_{j\in J}\sum_{i\in I_j} a_i \equiv 0 \pmod{pm} \quad i.e. \quad \sum_{j\in J}\sum_{i\in I_j} a_i \equiv 0 \pmod{n} \qquad \square$$