7. Polynomial Methods

7.1. Combinatorial Nullstellensatz

Thm (Alon, Tarsi 92)

Let $\mathbb{F}$ be a field

$f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ (polynomials with n variables $x_1, x_2, \ldots, x_n$)

Suppose that $\deg(f) = d = \sum_{i=1}^{n} d_i$

and the (coefficient of $\prod_{i=1}^{n} x_i^{d_i}$) $\neq 0$

Let $L_1, L_2, \ldots, L_n$ be the subsets of $\mathbb{F}$ with $|L_i| > d_i$

Then there exist $a_1 \in L_1, a_2 \in L_2, \ldots, a_n \in L_n$ such that $f(a_1, a_2, \ldots, a_n) \neq 0$.

Proof Induction on n.

Trivial if $n \leq 1$ $\Rightarrow$ So we may assume $n > 1$.

We may assume $|L_n| = d_n + 1$

Let $f_n(x_n) = \prod_{t \in L_n} (x_n - t)$ ← degree $d_n + 1$.

By expanding f_n, we can write

$$f_n(x_n) = x_n^{d_n+1} - h_n(x_n)$$

where $h_n(x_n)$ is a polynomial of degree $\leq d_n$.

Now, we reduce f to get $\tilde{f}$
by replacing $x_n^{d_n+1}$ with $h_n(x_n)$ repeatedly.

Observe that $f_n(x)=0$ if $x \in L_n$
$\Rightarrow x^{d_n+1} = h_n(x)$ if $x \in L_n$.

Then $f(x_1, x_2, \dots, x_n) = \tilde{f}(x_1, x_2, \dots, x_n)$
whenever $x_n \in L_n$.

The coefficient of $x_1^{d_1} x_2^{d_2} \cdots x_n^{d_n}$ in f
$=$ the coefficient of $x_1^{d_1} x_2^{d_2} \cdots x_n^{d_n}$ in $\tilde{f}$

Now we write

$$\tilde{f} = \sum_{i=0}^{d_n} g_i(x_1, x_2, \dots, x_{n-1}) x_n^i$$

then the degree of g_{d_n} is $d_1+d_2+\cdots+d_{n-1}$.
By the induction hypothesis
there exist $a_1 \in L_1$, $a_2 \in L_2$, $\dots$, $a_{n-1} \in L_{n-1}$
such that
$g_{d_n}(a_1, a_2, \dots, a_{n-1}) \neq 0$.

Fix $a_1, \dots, a_{n-1}$
Then $\tilde{f}$ is a polynomial of degree d_n

$\Rightarrow$ So there is $a_n \in L_n$
such that $\tilde{f}(a_1, a_2, \dots, a_n) \neq 0$. $\square$

7.2. Cauchy-Davenport inequality

Γ : abelian group. $\oplus$ $A, B \subseteq \Gamma$

$\Rightarrow A+B = \{x+y : x \in A,\ y \in B\}$.

Thm (Cauchy 1813 – Davenport 1935)

Let p be a prime. $A, B \neq \phi$

$A, B \subseteq \mathbb{Z}_p = \{0, 1, \cdots, p-1\}$

Then

$$|A+B| \geq \min(p,\ |A|+|B|-1)$$

For instance $A = \{0, 1, \cdots, a-1\}$ (a)

$B = \{0, 1, \cdots, b-1\}$ (b)

$\Rightarrow A+B = \{0, 1, \cdots, a+b-2\}$ (a+b-1)

$|A+B| = |A|+|B|-1$ tight

Proof 1: Induction on $\min(|A|, |B|)$.

By symmetry, we may assume $|A| \leq |B|$.

and $|A| \geq 2$

We may assume $A \cap B = \phi$ or $A \cap B = A$

Otherwise let $A' = A \cap B$

$B' = A \cup B$.

$A' + B' \subseteq A + B$.

$|A'|+|B'| = |A|+|B|$.

$\Rightarrow$ If $0 < |A'| < |A|$ then the conclusion follows

so we may assume $|A| = |A|$

$\Rightarrow A \cap B = A$

If we multiply $g \neq 0$ to both A and B

$A' = gA$, $B' = gB$ $\quad |A'+B'| = |A+B|$

Thus by multiplying $(a-b)^{-1}$ for some $a, b \in A$ we may assume

A contains 2 consecutive elements $a,\ a+1 \in A$.

By adding $-a$ to all of A we may assume $a = 0$

$0,\ 1 \in A$

Since $B \neq \mathbb{Z}_p$ (otherwise trivial) there exist $b \in B$ such that $b+1 \notin B$.

By adding $-b$ to all elements of B we may assume $0 \in B$, $1 \notin B$. $(b \to 0)$

$\Rightarrow \phi \neq A \cap B \neq A$ $\Rightarrow$ Contradiction.

($0 \in A$, $1 \notin B$)

Proof 2. The result is trivial if $|A|+|B| > p$

If $|A|+|B| > p$, then for $g \in \mathbb{Z}_p$

A and $g - B$

have a common element.

$a = g - b \Rightarrow a + b = g$.

So, we may assume $|A|+|B| \le p$.

Suppose $|A+B| \le |A|+|B|-2$.

Let $C \subseteq \mathbb{Z}_p$ such that

$A+B \subseteq C$

$|C| = |A|+|B|-2$

Let us define

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

Let $d_1 = |A|-1$, $d_2 = |B|-1$

The coeff of $x^{d_1} y^{d_2}$ in $f = \binom{d_1+d_2}{d_1} \not\equiv 0 \pmod p$

$d_1+d_2 < p$

By the Combinatorial Nullstellensatz

there exist $a \in A$, $b \in B$

such that $f(a+b) \neq 0$

$\Rightarrow a+b \notin C \Rightarrow A+B \not\subseteq C$ Contradiction.

Corollary. If $A_1, A_2 \dots, A_t \subseteq \mathbb{Z}_p$, then

$$|A_1+A_2+\dots+A_t| \ge \min\left(p, \sum_{i=1}^{t} |A_i| - (t-1)\right)$$

7.3. Restricted sum sets

$$A \hat{+} B = \{ a+b : a \in A,\ b \in B,\ a \neq b \}$$

Erdős-Heilbronn conjectured in 1964

$$|A \hat{+} A| \geq \min(p,\ 2|A|-3)$$

for $A \subseteq \mathbb{Z}_p$

Proved by Dias da Silva, Hamidoune 1994

(Proof by Alon, Nathanson, Ruzsa 1995)

We prove that if $|A| \neq |B|$

then $|A \hat{+} B| \geq \min(p,\ |A|+|B|-2)$

(we can take A, $A-\{x\}$

$A \hat{+} (A-\{x\}) = A \hat{+} A$)

We may assume $|A|+|B|-2 < p$.

Otherwise for all $g \in \mathbb{Z}_p$

A, $g-B$

If $|A|+|B| \geq p+2$, then

$$|A \cap (g-B)| \geq 2$$

$$\begin{cases} a_1 = g-b_1 \Rightarrow a_1 = b_1 \\ a_2 = g-b_2 \Rightarrow a_2 = b_2 \\ a_1 \neq a_2 \end{cases}$$

$$\left(\begin{array}{l} a_1+b_1 = a_2+b_2 = g \\ 2a_1 = 2a_2 = g \\ 2(a_1-a_2) = 0 \\ a_1 = a_2 \end{array} \right) \Rightarrow A \hat{+} B = Z_p$$

Now, suppose that $|A \hat{+} B| \leq |A| + |B| - 3$.

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

where $C \subseteq Z_p$ $\quad C \supseteq A \hat{+} B$

$$|C| = |A| + |B| - 3.$$

The degree of f is $|C|+1 = |A|+|B|-2$.

The coefficient of $x^{|A|-1} y^{|B|-1}$ in f

is exactly $\underbrace{\binom{|C|}{|A|-2}}_{x \cdot x^{|A|-2} y^{|B|-1}} - \underbrace{\binom{|C|}{|A|-1}}_{y \cdot x^{|A|-1} y^{|B|-2}}$

$$= \frac{|C|!}{(|A|-2)!\,(|B|-1)!} - \frac{|C|!}{(|A|-1)!\,(|B|-2)!}$$

$$= \frac{(|A|-1) - (|B|-1)}{(|A|-1)!\,(|B|-1)!}\,|C|!$$

$$= \frac{|A| - |B|}{(|A|-1)!\,(|B|-1)!}\,|C|! \not\equiv 0 \pmod{p}$$

By the Combinatorial Nullstellensatz there exist $a \in A$ $b \in B$

$$f(a, b) \neq 0.$$

$$\Rightarrow a+b \notin C \quad a \neq b$$

$$\Rightarrow a+b \notin A \hat{+} B$$

Contradiction.

7.4. Distinct Sums

Thm (Alon 2000)
Let p be an odd prime. $k < p$.
Let $a_1, a_2, \dots, a_k, b_1 \dots b_k$: numbers

If $b_1, b_2, \dots b_k$ are distinct
then there exists a permutation π of $\{1, \dots, k\}$ such that
$a_1 + b_{\pi(1)}, a_2 + b_{\pi(2)}, \dots, a_k + b_{\pi(k)}$ are all distinct.

Proof.
Let

$$f(x_1, x_2, \dots, x_k) = \prod_{1 \le i < j \le k} (x_j - x_i) \prod_{1 \le i < j \le k} (x_j + a_j - x_i - a_i)$$

be a polynomial over $GF(p)$.
Take

$$L_i = \{ b_1, b_2 \dots b_k \} \text{ for all } 1 \le i \le n.$$

$f(x_1, x_2, \dots x_k) \not\equiv 0$

$\Rightarrow$ $x_i \neq x_j$ for $i \neq j$
$x_j + a_j \neq x_i + a_i$ for all $i \neq j$

Want to show:
$\exists\, x_i \in L_i$ such that $f(x_1, x_2 \dots x_k) \neq 0$.

We want the coefficient of $\prod_{i=1}^{k} x_i^{k-1}$ is nonzero.

degree of $f = k(k-1) = \deg$

$= $ coefficient of $\prod_{i=1}^{k} x_i^{k-1}$ in $\left(\prod_{i<j}(x_j - x_i)\right)^2$

$$\prod_{i<j}(x_j - x_i) = \det \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ x_1 & x_2 & x_3 & \cdots & x_k \\ x_1^2 & x_2^2 & & & x_k^2 \\ \vdots & & & & \vdots \\ x_1^{k-1} & x_2^{k-1} & \cdots & & x_k^{k-1} \end{pmatrix} = \sum_{\sigma \text{ perm of } \{1,\dots,k\}} \operatorname{sign}(\sigma) \prod x_i^{\sigma(i)-1}$$

How do we get $\prod_{i=1}^{k} x_i^{k-1}$ in $\left(\prod (x_j - x_i)\right)^2$?

$$\left(\sum_{\sigma} \operatorname{sign}(\sigma) \prod x_i^{\sigma(i)-1}\right)\left(\sum_{\tau} \operatorname{sign}(\tau) \prod x_i^{\tau(i)-1}\right)$$

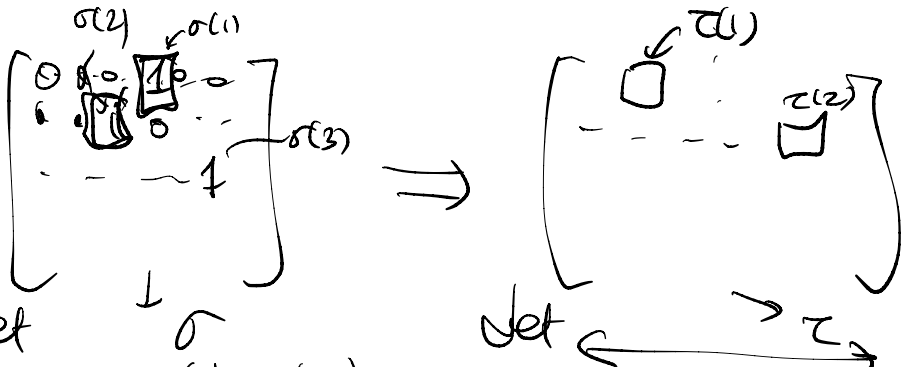
$$x_i^{\sigma(i)-1} \cdot x_i^{\tau(i)-1} \rightsquigarrow x_i^{k-1}$$

$$(\sigma(i)-1) + (\tau(i)-1) = k-1$$

Want: $\tau(i) = k+1-\sigma(i)$.

$\Rightarrow \tau$ is the reverse of σ

$$\operatorname{sign}(\sigma)\operatorname{sign}(\tau) = \begin{cases} (-1)^{k/2} & \text{if } k \text{ even} \\ (-1)^{(k-1)/2} & \text{if } k \text{ odd} \end{cases}$$



The coefficient of $\left(\prod_{i=1}^{k} x_i^{(k-1)}\right)$ in

$$\sum_{\substack{\sigma \\ \tau(i)=k+1-\sigma(i)}} \underbrace{\operatorname{sign}(\sigma)\operatorname{sign}(\tau)}_{\text{constant } \pm 1} \; x_i^{k-1}$$

$$\Rightarrow \boxed{(\pm 1)\cdot k!} \neq 0 \pmod p$$

Since $k < p$

By the Combinatorial Nullstellensatz, there exist $b_{\pi(i)} \in L_i$ for all i such that $f(b_{\pi(1)}, b_{\pi(2)}, \ldots, b_{\pi(k)}) \neq 0$.

7.5. The permanent lemma

$$\text{per}(A) = \sum_{\pi : \text{permutation of } \{1,\dots,n\}} \prod_{i=1}^{n} a_{i,\pi(i)}$$

$$\text{per}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = ad + bc$$

Thm (permanet lemma)

- A: $n \times n$ matrix over a field $\mathbb{F}$
- $\text{per}(A) \neq 0$.

$b \in \mathbb{F}^n$

Then for every family of sets $L_1, L_2, \dots, L_n$ of size 2 in $\mathbb{F}$, there exists a vector $x \in L_1 \times L_2 \times \cdots \times L_n$ such that

$$(Ax)_i \neq b_i$$

↑ i^{th} coordinate

for all $i = 1, 2, \dots, n$.

Proof. Let $A = (a_{ij})_{n \times n}$ $\quad 1 \le i, j \le n$

$$f(x_1, x_2, \dots, x_n) = \prod_{i=1}^{n} \left(\sum_{j=1}^{n} a_{ij} x_j - b_i \right)$$

The degree of $f = n$

The coefficient of $x_1 x_2 \cdots x_n$ is exactly $\text{per}(A)$.

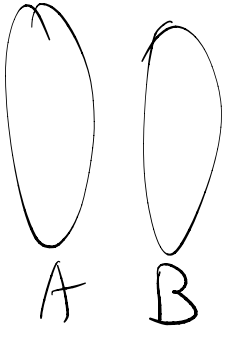
By the combinatorial Nullstellensatz, there exist $x_1, x_2, \ldots x_n$ such that

$$f(x_1, x_2, \ldots, x_n) \neq 0.$$

$x_i \in L_i$. □

Cor. Let G be a bipartite graph with the bipartition (A, B).

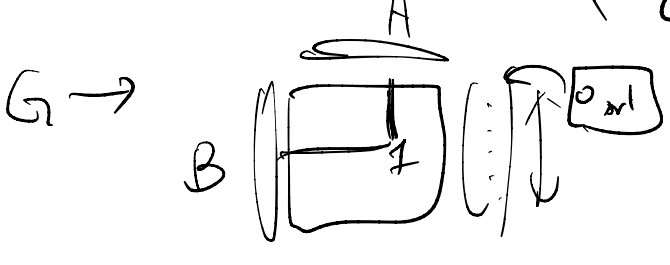
$|A| = |B| = n$.



Assume G has at least 1 perfect matching.

For every sequence of integers $d_1, d_2, \ldots, d_n$, there exists a subset X of A such that

#nbrs of (the i^{th} vertex of B) in X $\neq d_i$



7.6. Chevalley-Warning Theorem

Thm (Chevalley-Warning 1935)

Let $\mathbb{F}$ be a field with $|\mathbb{F}| = p$, p a prime.
Let $f_1, f_2, \dots, f_m$ be polynomials in $\mathbb{F}[x_1, x_2, \dots, x_n]$.
If $\sum_{i=1}^{m} \deg(f_i) < n$, then
the number of common zeros of $f_1, f_2, \dots, f_m$ is divisible by p.

Proof (Alon 1995)

Fermat's Little theorem

$$x^{p-1} \equiv 1 \pmod p \quad \text{if } x \not\equiv 0 \pmod p$$

Let N be the number of common roots.

Then

$$N \equiv \sum_{x_1, x_2, \dots, x_n \in \mathbb{F}} \prod_{i=1}^{m} \left(1 - f_i(x_1, \dots, x_n)^{p-1}\right) \pmod p$$

By expanding the right-hand side

we get a linear combination of monomials of the form

$$\prod_{i=1}^{n} x_i^{t_i}$$

of deg $< (p-1)n$

$$\Rightarrow \sum_{i=1}^{n} t_i < (p-1)n$$

$$\Rightarrow \text{for some } i,\ t_i \leq p-2.$$

Key fact: $\sum_{n=0}^{p-1} n^t \equiv 0 \pmod p$ if $t \leq p-2$

Let g be a primitive root so that $1, g, g^2, g^3, \ldots, g^{p-2}$ are distinct

$$\Rightarrow \sum_{n=0}^{p-1} n^t = \sum_{i=0}^{p-2} g^{ti} = \frac{(g^t)^{p-1}-1}{g^t-1}$$

$$= \left(g^{\frac{p-1}{t}}-1\right)\left(g^{t}-1\right)^{-1}$$

$$\equiv 0 \pmod{p}$$

$$\sum X_1^{t_1} X_2^{t_2} \cdots X_n^{t_n} = \sum_{j \neq i} \prod X_j^{t_j} \underbrace{\left(\sum_{X_i \in \mathbb{F}} X_i^{t_i}\right)}_{=0}$$

$$\therefore N \equiv 0 \pmod{p} \qquad \square$$

Corollary

Let $\mathbb{F}$ be a field with $|\mathbb{F}| = p$, p a prime. Let $f_1, f_2, \cdots, f_m$ be polynomials in $\mathbb{F}[x_1, x_2, \cdots, x_n]$.

If $\sum_{i=1}^{m} \deg(f_i) < n$, then the number of common roots $\neq 1$.

Proof of this corollary by Combinatorial Nullstellensatz.

Suppose not. Let $(c_1, c_2 \ldots c_n)$ be the unique common root.

We define

$$f(x_1, x_2, \ldots x_n) = \prod \left(1 - f_i(x_1, \ldots, x_n)^{p-1}\right) - \delta \prod_{j=1}^{n} \prod_{\substack{c \in \mathbb{F} \\ c \neq c_j}} (x_j - c)$$

where we choose δ so that

$$f(c_1, c_2, \ldots c_n) = 0.$$

observe that $\delta \neq 0$

$\Rightarrow f(x_1, x_2, \ldots, x_n) = 0$

for all $x_i \in \mathbb{F}$.

The degree of $f = n(p-1)$

(The coefficient of $x_1^{p-1} x_2^{p-1} \cdots x_n^{p-1}$) $= -\delta \neq 0$.

By the combinatorial Nullstellensatz

there exist $x_1, x_2, \ldots x_n \in \mathbb{F}$

such that $f(x_1, x_2, \ldots x_n) \neq 0$

Contradiction

□.

7.7. Zero-sum sets

Exercise: If $a_1, a_2, \ldots, a_n$ are integers then there exists a nonempty subset I of $\{1, \ldots, n\}$ such that $\sum_{i \in I} a_i$ is divisible by n.

a_1
$a_1 + a_2$
$a_1 + a_2 + a_3$
$\vdots$
$a_1 + a_2 + a_3 + \cdots + a_n$

Q: Can we always find a subset I of $|I| = n$ so that $n \mid \sum_{i \in I} a_i$?

$0, 0, 0, \ldots, 0$ ($n-1$) $1, 1, \ldots, 1$ ($n-1$)

$2n-2$

impossible.

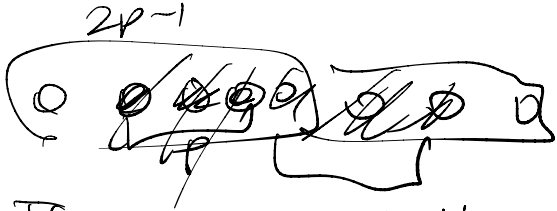
Thm (Erdős, Ginzburg, Ziv 1961)
If $a_1, a_2, \ldots a_{2n-1}$ are integers, then there exists a subset I of size n such that $\sum_{i \in I} a_i$ is divisible by n.

Claim: We may assume n is a prime.

Suppose not. Induction on n.

$n = mp$ for some prime p.

$m > 1$.



If we repeatedly take a set I_i of size p with $\sum_{i \in I} a_i \equiv 0 \pmod p$ ℓ times then #remaining integers

$= 2n-1 - \ell p = 2mp - \ell p - 1$

$= (2m-\ell)p - 1$

If $(2m-\ell)p - 1 \geq 2p-1$ then we can get one more I_i.

So, we may choose

$$\ell = 2m-1$$

$\therefore$ We have $2m-1$ disjoint subsets

$I_1, I_2, \cdots, I_{2m-1}$

of $\{1, 2, \cdots, 2n-1\}$

such that $\sum_{i \in I_j} a_i \equiv 0 \pmod{p}$ for all j.

Then there exists $J \subseteq \{1, 2, \cdots 2m-1\}$

$|J| = m$ such that

$$\sum_{j \in J} \left(\frac{\sum_{i \in I_j} a_i}{p} \right) \equiv 0 \pmod{m}$$

by the induction hypothesis

$\Rightarrow$ Let $K = \bigcup_{j \in J} I_j$

$|K| = mp = n$.

$$\sum_{i \in K} \frac{a_i}{p} \equiv 0 \pmod{m}$$

$$\Rightarrow \sum a_i \equiv 0 \pmod{n}$$

□

So, from now on, we may assume $n = p$ for a prime p.

1st Proof using the permanent lemma:

Let $0 \le a_1 \le a_2 \le \dots \le a_{2p-1} < p$

We may assume that

$$a_i < a_{i+p-1}$$

(otherwise $a_i = a_{i+1} = \dots = a_{i+p-1}$)

Let $J = (p-1) \times (p-1)$ all-1 matrix.

Let $L_i = \{a_i, a_{i+p-1}\}$.

Let $b_1, b_2, \dots, b_{p-1}$ be the list of elements $\not\equiv -a_{2p-1} \pmod p$

$\operatorname{per}(J) = (p-1)! \not\equiv 0 \pmod p$

By the permanent lemma, there exists $x_i \in L_i$ so that

$$(Ax)_i \neq b_i$$

$\Rightarrow$ sum of $p-1$ distinct a_j's $\neq -b_i$ for all i

$\Rightarrow$ this sum $\equiv -a_{2p-1} \pmod p$

$$a_{2p-1} + \sum_{i=1}^{p} x_i \equiv 0 \pmod{p}$$ □

2nd proof:

$a_1 \le a_2 \le \cdots \le a_{2p-1}$

We may assume $a_i < a_{i+p-1}$

$A_i = \{a_i, a_{i+p-1}\}$

$$|A_1 + A_2 + \cdots + A_{p-1}| \ge \min\left(p, \sum_{i=1}^{p} (|A_i| - (p-2))\right)$$

↑ Cauchy-Davenport

$$= \min(p, 2(p-1) - p - 2)$$

$$= p.$$

$$\Rightarrow -a_{2p-1} \in A_1 + A_2 + \cdots + A_{p-1}$$

□

3rd proof using the Chevalley-Warning thm.

Consider 2 polynomials

$$\begin{cases} \sum_{i=1}^{2p-1} a_i x_i^{p-1} \equiv 0 \pmod p \\ \sum x_i^{p-1} \equiv 0 \pmod p \end{cases}$$

Sum of degree $= 2(p-1) < 2p-1$ = # variables.

$x_1 = x_2 = \cdots = x_{2p-1} = 0$ is a common root.

$\Rightarrow$ there is another common root $(y_1, y_2, \cdots, y_{2p-1})$

$\sum y_i^{p-1} \equiv 0 \Rightarrow$ # nonzero y_i's $\equiv 0 \pmod p$

$\sum a_i y_i^{p-1} \equiv 0 \pmod p \Rightarrow$ # nonzero y_i's $= p$.

$\Rightarrow$ Sum of p of a_i's $\equiv 0 \pmod p$

□