Ch7 Polynomial Methods

§7.1 Combinatorial Nullstellensatz

Thm (Alon, Tarsi 92)

$\mathbb{F}$: field, $f \in \mathbb{F}[x_1, \cdots, x_n]$

Suppose $\deg(f) = d = \sum_{i=1}^{n} d_i$, and the coef. of $\prod_{i=1}^{n} x_i^{d_i} \neq 0$.

Let $L_1, \cdots, L_n$ be subsets of $\mathbb{F}$ w/ $|L_i| > d_i$, then $\exists\ a_i \in L_i$, $i \in [n]$ s.t. $f(a_1, \cdots, a_n) \neq 0$

Pf/ Induction on n.

1° $n=1$, trivial

2° $n>1$, also assume $|L_n| = d_n + 1$,

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

Expanding f_n, we have

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

$\deg(h_n) \leq d_n$

Now, we reduce $f \to \tilde{f}$ by replacing

$x_n^{d_n+1} \to h_n(x_n)$ repeatedly.

Observe that $f_n(x) = 0$ if $x \in L_n$, i.e.,

$x^{d_n+1} = h_n(x)$ if $x \in L_n$

Then $f(x_1, \sim, x_n) = \tilde{f}(x_1, \sim, x_n)$, if $x_n \in L_n$

and coef. of $\prod_{i \in [n-1]} x_i^{d_i}$ remains the same.

Now we write $\tilde{f}$ as

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

$$\Rightarrow \deg(g_{d_n}) = d_1 + \cdots + d_{n-1}$$

$\xrightarrow{IP\ (\text{Induction hypo.})}$ $\exists\ a_1 \in L_1, \sim, a_{n-1} \in L_{n-1}$ s.t.

$\exists a_{n1}, \dots, a_{n,n-1}$ s.t. $\tilde{f}|_{a_{n1}, \dots, a_{n,n-1}}$ is a polynomial of degree d_n

$\Rightarrow \exists a_{nn} \in L_n$ s.t. $\tilde{f}(a_{n1}, \dots, a_{nn}) = \tilde{f}|_{a_{n1}, \dots, a_{n,n-1}}(a_{nn}) \neq 0$,

as $|L_n| = d_n + 1 > d_n$. ∎

§7.2 Cauchy-Davenport Thm.

Γ: Abelian Group, $A, B \subseteq \Gamma$

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

Thm (C^{1813} - D^{1935})

p: Prime, $A, B \subseteq \mathbb{Z}_p$

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

Tight. $A = \{0, \dots, a-1\}$, $B = \{0, \dots, b-1\}$

$\Rightarrow A+B = \{0, \dots, a+b-2\} \Rightarrow |A+B| = |A|+|B|-1$

Pf 1 (Induction on $\min\{|A|, |B|\}$)

WLOG, assume $2 \leq |A| \leq |B|$.

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

exercise Let $A' = A \cap B$, $B' = A \cup B$, then

$A'+B' \subseteq A+B$ and $|A'|+|B'| = |A|+|B|$.

If we multiply q to to both A and B, $A' = qA$, $B' = qB$, and $|A'+B'| = |A+B|$.

Thus, by multiplying $(a-b)^{-1}$ for some $a, b \in A$ we may assume A contains 2 consecutive elements K, $K+1$ ($b = (a-b)K$, $a = (a-b)K+1$)

Moreover, adding $-K$ to A, we may assume $A \supseteq \{0, 1\}$.

Also assume $B \neq \mathbb{Z}_p$ (trivial otherwise)

$\Rightarrow \exists\, b \in B$ s.t. $b+1 \notin B$

Similarly, adding $-b$ to B $\overset{WLOG}{\Rightarrow} 0 \in B$, $1 \notin B$

$\Rightarrow A \cap B \neq A$ ($A \cap B \ni 0$, $A \cap B \not\ni 1$).

contradiction!

□

Pf 2 (Using Comb. Nullstellensatz)

Trivial if $|A|+|B|>p$.

$|A|+|B|>p \Rightarrow \forall g \in \mathbb{Z}_p,\ A \cap (g-B) \neq \emptyset$

So WMA $|A|+|B| \leq p$. Suppose $|A+B| \leq |A|+|B|-2$

Let $C \subseteq \mathbb{Z}_p$ s.t. $A+B \subseteq C$ w/ $|C| = |A|+|B|-2$

Define $f(x,y) = \prod_{c \in C} (x+y-c)$, Let $d_1 = |A|-1$, $d_2 = |B|-1$

Coef. of $x^{d_1} y^{d_2}$ is $\binom{d_1+d_2}{d_1} \neq 0 \pmod p$

as $d_1+d_2 < p$

By Comb. Nullstellensatz, $\exists\ a \in A, b \in B$

s.t. $f(a,b) \neq 0 \Rightarrow a+b \notin C$, contradiction!

w/ $A+B \subseteq C$

Cor $A_1, \dots, A_t \subseteq \mathbb{Z}_p$, then

$$|A_1+\dots+A_t| \geq \min\left(p, \sum_{i \in [t]} |A_i| - (t-1)\right)$$

§7.3 Restricted Sum sets

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

Conj (Erdös-Heilbronn 1964)

$|A \hat{+} A| \geq \min(p, 2|A|-3)$, $\forall A \subseteq \mathbb{Z}_p$

First Pf/ (Dias da Silva & Hamidoune 1994)

Pf/ (Alon, Nathanson, Ruzsa 1995, using CN)

Actually more generally, we prove that

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

(take $B = A - \{x\}$ for the original Conj.)

WMA $|A|+|B|-2 \leq p$, otherwise,

i.e. $|A|+|B| \geq p+3$, then

$|A \cap (g-B)| \geq 3$, i.e., we have

$a_i = g - b_i$, $i \in [3]$

In order to make $|A \hat{+} B| < p$, we need to have some $g \in \mathbb{Z}_p$ s.t.

$$\begin{cases} a_1 = b_1, \ a_1 + b_1 = 2a_1 = g \\ a_2 = b_2, \ a_2 + b_2 = 2a_2 = g \\ a_3 = b_3, \ a_3 + b_3 = 2a_3 = g \end{cases}$$

$$\Rightarrow 2(a_1 - a_2) = 2(a_2 - a_3) = 0$$

$$\Rightarrow a_1 = a_2 \quad (\text{actually, WMA } |A| + |B| - 2 < p)$$

(As a_3 is not needed)

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

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

$A \hat{+} B \subseteq C \subseteq \mathbb{Z}_p$, $|C| = |A| + |B| - 3$.

$\deg(f) = |C| + 1 = |A| + |B| - 1$ ✗

Coef. $x^{|A|-1} y^{|B|-1}$ is $\binom{|C|}{|A|-2} - \binom{|C|}{|A|-1} = \frac{(|A| - |B|)\,|C|!}{(|A|-1)!\,(|B|-1)!}$

By CN, $\exists\ a \in A, b \in B$ s.t. $f(a,b) \neq 0$,

i.e. $a+b \notin C$, $a \neq b$, contradiction w/ $A \dot{+} B \subseteq C$!

§7.4 Distinct Sums

Thm (Alon 2000)

$p > 2$: prime, $k < p$

$(a_i)_{i \in [k]}, (b_i)_{i \in [k]}$: Numbers

If $(b_i)_{i \in [k]}$ are distinct, then $\exists\, \pi \in S_k$

s.t. $(a_i + b_{\pi(i)})_{i \in [k]}$ are distinct.

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

be a polynomial over $GF(p) = \mathbb{F}_p$

Take $L_i = \{b_1, \cdots, b_k\}$ for all $i \in [k]$,

$f(x_1, \cdots, x_k) \neq 0 \Leftrightarrow \begin{cases} x_1, \cdots, x_k \text{ are distinct} \\ (x_i + a_i)_{i \in [k]} \text{ are distinct} \end{cases}$

NTS, $\exists\, x_i \in L_i$ for all $i \in [k]$ s.t.

$f(x_1, \cdots, x_k) \neq 0$

We want coef. of $\prod_{i=1}^{k} x_i^{k-1} \neq 0$ i.f

which the same as the coef. of

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

$$\prod_{i<j}(x_j - x_i) = \det\begin{pmatrix} 1 & \cdots & 1 \\ x_1 & \cdots & x_k \\ \vdots & & \vdots \\ x_1^{k-1} & \cdots & x_k^{k-1} \end{pmatrix} = \sum_{\sigma \in S_k} \operatorname{sign}(\sigma) \prod_{i=1}^{k} x_i^{\sigma(i)-1}$$

$$\left(\sum_{\sigma \in S_k} \operatorname{sign}(\sigma) \prod_{i=1}^{k} x_i^{\sigma(i)-1}\right)\left(\sum_{\sigma' \in S_k} \operatorname{sign}(\sigma') \prod_{i=1}^{k} x_i^{\sigma'(i)-1}\right)$$

Want: $(\sigma(i)-1) + (\sigma'(i)-1) = k-1$, i.e.,

$\sigma'(i) = k+1-\sigma(i) \iff \sigma' = \sigma^{-1}$

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

So, the interesting coef. is

$\sum_{\sigma \in S_k} \operatorname{sign}(\sigma)\operatorname{sign}(\sigma') = \pm k! \not\equiv 0 \pmod{p}$

$\overset{CN}{\Rightarrow}$ Completing the proof. $\square$

§7.5 The Permanent Lemma

Def/ $\operatorname{per}(A) := \sum_{\pi \in S_n} \prod_{i=1}^{n} a_{i\pi(i)}$

(Compare w/ determinant)

Thm (The Permanent Lemma)

$A \in \mathbb{F}^{n \times n}$, $\operatorname{per}(A) \neq 0$, $b \in \mathbb{F}^n$, then

$\forall$ 2-family $L_1, \dots, L_n$ in $\mathbb{F}$, $\exists x \in L_1 \times \cdots \times L_n$

s.t. $(Ax)_i \neq b_i$, $\forall i \in [n]$

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

$\deg(f) = n$, and

coef. of $x_1 \cdots x_n$ in f is $\operatorname{per}(A) \neq 0$

By CN, $\exists (x_i \in L_i)_{i \in [n]}$ s.t. $f(x_1, \dots, x_n) \neq 0$

Cor G: bipartite graph w/ partitions $|A| = |B| = n$

Assume that G has ≥ 1 perfect matching.

For $\forall$ sequence of integers $d_1, \cdots, d_n$,

$\exists X \subseteq A$ s.t. # nbrs of i-th vtx of B in $X \neq d_i$. $\forall i \in [n]$

§7.6 Chevalley-Warning Thm.

Thm (C-W 1935)

$\mathbb{F}$: field of $|\mathbb{F}| = p$, let $f_1, \dots, f_m \in \mathbb{F}[x_1, \dots, x_n]$

If $\sum_{i=1}^{m} \deg(f_i) < n$, then # common zeros of $f_1 \cdots f_m$ is divisible by p.

Pf (Alon 95', using Fermat's Little Thm.)

$x^{p-1} \equiv 1 \pmod p$ if $x \neq 0 \pmod p$

Let N be the number of common roots, then

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

Expanding RHS, we get a linear combination of monomials of the form $\prod_{i=1}^{n} x_i^{t_i}$ of $\deg < (p-1)\cdot n$

$\Rightarrow \exists\, i \in [n]$ s.t. $t_i \leq p-2$

Key fact: $\sum_{x \in \mathbb{F}} x^t \equiv 0 \pmod p$ if $t \leq p-2$

To see this, let g be a primitive root, i.e.

$1, g, \dots, g^{p-2}$ are all distinct

$$\Rightarrow \sum_{x \in \mathbb{F}} x^t = \sum_{i=0}^{p-2} g^{it} = (g^t)^{p-1} - 1 / g^t - 1 \equiv 0 \pmod{p}$$

For each term in the form of

$\sum_{x_1, \dots, x_n} x_1^{t_1} \cdots x_n^{t_n}$, sup se $t_i \leq p-2$, we rewrite

$$\sum_{x_1, \dots, x_n} x_1^{t_1} \cdots x_n^{t_n} = \sum \prod_{j \neq i} x_j^{t_j} \left(\sum_{x_i \in \mathbb{F}} x_i^{t_i} \right) \equiv 0 \pmod{p}$$

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

Cor

$\mathbb{F}$: field wl $|\mathbb{F}| = p$, let $f_1, \dots, f_m \in \mathbb{F}[x_1, \dots, x_n]$

If $\sum_{i=1}^{m} \deg(f_i) < n$, then # common zeros of $f_1, \dots, f_m \neq 1$

Pf (of Cor, using CN, Alon)

Suppose NOT, let $(c_1, \dots, c_n)$ be the unique common root.

Let $f(x_1, \dots, x_n) := \prod (1 - f_i^{p-1}(x_1, \dots, x_n)) - \delta \prod_{j=1}^{n} \prod_{c \in \mathbb{F}, c \neq c_j} (x_j - c)$,

where we choose $\delta \neq 0$ s.t. $f(c_1, \dots, c_n) = 0$.

$\Rightarrow f(x_1, \dots, x_n) = 0$, $\forall x_1, \dots, x_n \in \overline{\mathbb{F}}$.

$\deg(f) = n(p-1)$, and

coef. of $x_1^{p-1} \cdots x_n^{p-1} = \delta \neq 0$ in f

$\overset{CN}{\Longrightarrow} \exists x_1, \dots, x_n \in \overline{\mathbb{F}}$ s.t. $f(x_1, \dots, x_n) \neq 0$, contradiction!

§7.7 Zero-Sum Sets

Motivative Exercise $a_1, \cdots, a_n \in \mathbb{Z}$

$\Rightarrow \exists\, I \subseteq [n], I \neq \phi$ s.t. $\sum_{i \in I} a_i \equiv 0 \pmod{n}$

Consider $\sum_{i=1}^{j} a_i$ for $j = 1, \cdots, n$, by pigeonhole

Q: Can we always find $|I| = n$ s.t. $n \mid \sum_{i \in I} a_i$?

Impossible case w/ $(2n-2)$, where $(n-1)$ 1's and $(n-1)$ 0's

Thm (Erdös, Ginzburg, Ziv 1961)

$(a_i)_{i \in [2n-1]} \in \mathbb{Z} \Rightarrow \exists\, I \subseteq [2n-1], |I| = n$ s.t.

$n \mid \sum_{i \in I} a_i$

Claim: We may assume n is a prime.

To see this, let $n = mp$, p prime, $m > 2$ and suppose the proposition holds for $n' < n$. Note that $p < n$, so we can repeatedly remove p

elements whose sum $\equiv 0 \pmod p$. As $2m-1 = 2mp-1$, we can do this ~~for~~ $(2m-1)$ times and get $I_1, \dots, I_{2m-1}$, disjoint, p-uniform.

Use IH again, $\exists J \in [2m-1]$ w/ $|J| = m$ s.t. $\sum_{j\in J} \left(\sum_{i\in I_j} a_i/p\right) \equiv 0 \pmod m$.

Now let $K = \bigcup_{j\in J} I_j$, $|K| = mp = n$, we have $\sum_{i\in K} a_i/p \equiv 0 \pmod m \Rightarrow \sum_{i\in K} a_i \equiv 0 \pmod n$

Now, WMA $n=p$ is a prime.

Pf 1 (using the permanent Lemma)

Let $0 \le a_1 \le a_2 \le \dots \le a_{2p-1} < p$, WMA $a_i < a_{i+p-1}, \forall i$, otherwise $a_i = a_{i+1} = \dots = a_{i+p-1}$ and their sum $\equiv 0 \pmod p$

Let J be the $(p-1)\times(p-1)$ all-1 matrix, and let $L_i = \{a_i, a_{i+p-1}\}$, $i \in [p-1]$

let $b_1, \dots, b_{p-1}$ be the list of elements $\neq -a_{2p-1}$

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

Pf $\Rightarrow \exists\, x_i \in L_i,\ i \in [p-1]$ s.t. $(Jx)_i \neq b_i$

$\Rightarrow \sum_{i\in[p-1]} x_i = -a_{2p-1},\ \sum_{i\in[p-1]} x_i + a_{2p-1} = 0$

□

Pf 2 (Using Cauchy-Davenport Thm.)

Sanely, let $a_1 \le a_2 \le \dots \le a_{2p-1}$, $a_i < a_{i+p-1}$

Let $A_i = \{a_i, a_{i+p-1}\}$, $i \in [p-1]$

$\overset{CD}{\Rightarrow} |A_1 + \dots + A_{p-1}| \ge \min\left(p, \sum_{i\in[p-1]} |A_i| - (p-2)\right)$

$= p$

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

□

Pf 3 (Using CW Thm.)

Consider 2 polynomials

$$\sum_{i=1}^{2p-1} a_i x_i^{p-1}, \quad \sum_{i=1}^{2p-1} x_i^{p-1}$$

the sum of their degrees $= 2(p-1) < 2p-1$.

and $(0, \sim, 0)$ is a common root

$\overset{CW}{\Longrightarrow}$ $\exists$ another common root $(Y_1, \sim, Y_{2p-1}) \neq 0$

Then we have $\sum Y_i^{p-1} \equiv 0 \Rightarrow$ $\#\{Y_i \neq 0\} \equiv 0$

$\Rightarrow$ $\#\{Y_i \neq 0\} = p$;

Also, $\sum_i a_i Y_i^{p-1} = \sum_{i: Y_i \neq 0} a_i \equiv 0$ ☐