Math 137 Section Notes

Noga Alon's Combinatorial Nullstellensatz (Ref: "Comb. Nsts." by Noga Alon)

Warmup:

Prove the Cauchy-Davenport Thm:

Thm 3.3 Let p be a prime number and let $\emptyset \neq A, B \subset \mathbb{Z}/p$. Then the set $A+B$ of sums $a+b$ (w/ $a \in A$, $b \in B$) has size

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

Pf (from first principles)

We induct on $|A|$.

Base case: clear. So assume $|A| \geq 2$. Fix distinct $a, a' \in A$.

For $0 \neq b \in B$, let $V_{ab} = (A+b) \cap (a+B)$

let $W_{ab} = (A+b) \cup (a+B)$

Case 1: $V_{ab} = A+b \ \forall b \in B$. $\Rightarrow A+b \subset a+B \ \forall b$

$\Rightarrow A+B \subset a+B$

Let $x = a-a' \neq 0$.

$\Rightarrow x+B \subset B \iff B = \mathbb{Z}/p$

$\Rightarrow |A+B| = p$

Case 2: $V_{ab} \subsetneq A+b$ for some $b \in B$.

Note: $a+b \in V_{ab} \cap W_{ab}$

$\Rightarrow \#(A+B) \geq \#(V_{ab}+W_{ab}) \geq \min(|V_{ab}|+|W_{ab}|-1, p)$ ← Inductive hypothesis

$\downarrow$

$V_{ab}+W_{ab} \subset (a+b)+A+B$

By PIE,

$|W_{ab}| = |A+b|+|a+B|-|V_{ab}| = |A|+|B|-|V_{ab}|$ $\square$

The Combinatorial Nullstellensatz

Recall: Hilbert's Nullstellensatz (ask someone to do this)

Thm 1.1 Let F be an arbitrary field. Let $f = f(x_1, \ldots, x_n)$ be a poly. in $F[x_1, \ldots, x_n]$. Let $S_1, \ldots, S_n$ be nonempty subsets of F. Define $g_i(x_i) = \prod_{s \in S_i} (x_i - s)$. If f vanishes over all the common zeroes of $g_1, \ldots, g_n$ (i.e, if $f(s_1, \ldots, s_n) = 0 \ \forall s_i \in S_i$), then $\exists \ h_1, \ldots, h_n \in F[x_1, \ldots, x_n]$ s.t. $\deg(g_i) + \deg(h_i) \leq \deg(f)$ and

$$f = \sum_{i=1}^{n} h_i g_i$$

Thm 1.2 Let F and f be as above. Suppose $\deg(f)$ is $\sum_{i=1}^{n} t_i$, where each t_i is a nonneg. int. Suppose coeff. of $\prod_{i=1}^{n} x_i^{t_i}$ is nonzero. Then, if $S_1, \ldots, S_n \subset F$ s.t. $|S_i| > t_i$, there are $s_1 \in S_1, \ldots, s_n \in S_n$ s.t.

$$f(s_1, \ldots, s_n) \neq 0.$$

Lemma 2.1 Let $P \in F[x_1, \ldots, x_n]$. Suppose $\deg_{x_i}(P) \leq t_i \ \forall i$. Let $S_i \subset F$ be a set of $\geq t_i + 1$ distinct elts of F. If

$$P(x_1, \ldots, x_n) = 0 \quad \forall (x_1, \ldots, x_n) \in S_1 \times \cdots \times S_n,$$

then $P \equiv 0$.

Pf (leave as exercise if no time)

Induction. Base case: clear.

Suppose holds for $n-1$. Consider P as a polynomial in x_n

$$P = \sum_{i=0}^{t_n} P_i(x_1, \ldots, x_{n-1}) x_n^i.$$

~~Each~~ ~~P_i~~ ~~has~~ $\deg_{x_j}(P_i) \leq t_j$. $\forall (x_1, \ldots, x_{n-1}) \in S_1 \times \cdots \times S_{n-1}$, the poly in x $P(x_1, \ldots, x_{n-1}, x) = 0 \ \forall x \in S_n \Rightarrow P(x_1, \ldots, x_{n-1}, x) = 0$

$\Rightarrow P_i(x_1, \ldots, x_{n-1}) = 0 \ \forall (x_1, \ldots, x_{n-1}) \in S_1 \times \cdots \times S_{n-1}$

$\Rightarrow P_i \equiv 0 \ \forall i$

$\Rightarrow P \equiv 0.$ $\square$

Proof of Thm 1.1

Define $t_i = |S_i| - 1 \ \forall i$:

$$f(x_1,\dots,x_n) = 0 \quad \forall\ (x_1,\dots,x_n) \in S_1 \times \dots \times S_n.$$

For all i, let

$$g_i(x_i) = \prod_{s \in S_i} (x_i - s) = x_i^{t_i+1} - \sum_{j=0}^{t_i} g_{ij} x_i^j$$

Note: for $x_i \in S_i$, $g_i(x_i) = 0$

$$\Rightarrow x_i^{t_i+1} = \sum_{j=0}^{t_i} g_{ij} x_i^j$$

Let $\bar{f}$ be the poly. obtained by writing f as a lin. comb. of monomials and replacing each occurrence of $x_i^{f_i}$ for $f_i > t_i$.

$\deg_{x_i}(\bar{f}) \le t_i \ \forall i$, and obtained from f by subtracting $h_i g_i$ for

$\deg(h_i) + \deg(g_i) \le \deg(f)$.

Also,

$$\bar{f}(x_1,\dots,x_n) = f(x_1,\dots,x_n) \quad \forall (x_1,\dots,x_n) \in S_1 \times \dots \times S_n$$
$$= 0$$

$\underset{(\text{Lemma } 2.1)}{\Longrightarrow} \ \bar{f} \equiv 0$ $\square$

Pf of Thm 1.2 Wlog assume $|S_i| = t_i + 1$ for all i. Suppose the results is false. Define

$$g_i(x_i) = \prod_{s \in S_i} (x_i - s).$$

By Thm 1.1 there are polynomials $h_1,\dots,h_n \in F[x_1,\dots,x_n]$ satisfying ~~deg hi gi~~ $\deg(g_i) + \deg(h_j) \le \sum_{i=1}^n t_i$ so that $f = \sum_{i=1}^n h_i g_i$. By hypothesis, coeff of $\prod_{i=1}^n x_i^{t_i}$ is $\ne 0$ in f; therefore so is the coeff. on the RHS.

The deg of $h_i g_i$ is at most $\deg(f)$. If $\exists$ monomials of $\deg(f)$ in $h_i g_i$ they are divisible by $x_i^{t_i+1}$

$\Rightarrow$ coefficient of $\prod_{i=1}^n x_i^{t_i}$ in $\sum_i h_i g_i$ is 0, contradiction! $\square$

Applications to Combinatorics

Thm 3.1 (conj. by Artin, 1934; Chevalley, 1935) Let p be a prime; let $P_1, \ldots, P_m \in \mathbb{Z}/p[x_1, \ldots, x_n]$. If $n > \sum_{i=1}^{m} \deg(P_i)$ and the P_i have a common zero $c = (c_1, \ldots, c_n)$, then they have another common zero.

Pf Suppose otherwise. Let

$$f = f(x_1, \ldots, x_n) = \prod_{i=1}^{m} \left(1 - P_i(x_1, \ldots, x_n)^{p-1}\right) - \delta \prod_{j=1}^{n} \prod_{\substack{c \in \mathbb{Z}/p \\ c \neq c_j}} (x_j - c);$$

choose δ s.t. $f(c_1, \ldots, c_n) = 0$.

This determines δ; note $\delta \neq 0$. Moreover,

$$f(s_1, \ldots, s_n) = 0$$

$\forall (s_1, \ldots, s_n) \in \mathbb{Z}/p^n$. By assumption, $\exists P_j$ s.t. $P_j(s_1, \ldots, s_n) \neq 0$, so

assume $(s_1, \ldots, s_n) \neq (c_1, \ldots, c_n)$

$1 - P_j(s_1, \ldots, s_n)^{p-1} = 0$. Since $s_i \neq c_i$ for some i,

$\cancel{\prod_{j=1}^{n} \prod_{\substack{c \in \mathbb{Z}/p \\ c \neq c_j}} (x_j - c)}$ ~~eval at s_i is 0.~~

$$\prod_{\substack{c \in \mathbb{Z}/p \\ c \neq c_i}} (s_i - c) = 0 \Rightarrow f(s_1, \ldots, s_n) = 0$$

Let $t_i = p-1$ for all i; the coeff of $\prod_{i=1}^{n} x_i^{t_i}$ in f is $-\delta$, since the total degree of

$$\prod_{i=1}^{m} \left(1 - P_i(x_1, \ldots, x_n)^{p-1}\right)$$

is $(p-1) \sum_{i=1}^{m} \deg(P_i) < (p-1)n$.

Apply Thm 1.2 w/ $S_i = \mathbb{Z}/p$ $\forall i$; thus there are $s_1, \ldots, s_n \in \mathbb{Z}/p$ s.t. $f(s_1, \ldots, s_n) \neq 0$. Contradiction. □

Thm 3.2 (Cauchy-Davenport, revisited) If p is prime and A and B are nonempty subsets of $\mathbb{Z}/p$, then

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

Pf If $|A|+|B|>p$, the result is trivial

$(\forall g \in \mathbb{Z}/p,\ A \cap (g-B) \neq \emptyset$, so $A+B=\mathbb{Z}/p)$

Thus, assume that $|A|+|B| \leq p$ and that the result is false so that $|A+B| \leq |A|+|B|-2$.

Let $C \subset \mathbb{Z}/p$ be s.t. $A+B \subset C$, $|C|=|A|+|B|-2$.

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

$$f(a,b)=0 \quad \forall a \in A, b \in B$$

Let $t_1=|A|-1$, $t_2=|B|-1$.

The coeff. of $x^{t_1}y^{t_2}$ in f is $\binom{|A|+|B|-2}{|A|-1}$, which is nonzero in $\mathbb{Z}/p$ since $|A|+|B|-2<p$.

Apply Theorem 1.2 $(n=2, S_1=A, S_2=B)$

$\Rightarrow \exists a \in A\ b \in B$ s.t. $f(a,b) \neq 0$. Contradiction $\blacksquare$

Applications to Graph Theory

Recall: A graph G is a set of vertices V and edges E connecting the vertices. If an edge connects 2 vertices, then they are said to be adjacent.

The degree of a vertex $v \in G$ is the # of vertices adjacent to it.

A loop in a graph is an edge connecting a vertex to itself.

A graph is called p-regular if all its vertices have degree p.

Theorem 6.1 For any prime p, any loopless graph $G=(V,E)$ w/average degree $> 2p-2$ and maximum degree $\leq 2p-1$ contains a ~~p-reg~~ p-regular subgraph.

Pf Let $(a_{v,e})_{v\in V, e\in E}$ denote the incidence ~~deg~~ matrix of G, defined by

$a_{v,e}=1$ if $v \in e$;

$a_{v,e}=0$ otherwise.

~~Bes~~ For each edge $e \in G$, consider the ~~var~~ ~~as~~ ~~an~~ variable x_e, and ~~cont~~ consider the polynomial

$$F = \prod_{v\in V}\left(1-\left(\sum_{e\in E} a_{v,e}\, x_e\right)^{p-1}\right) - \prod_{e\in E}(1-x_e)$$

over $\mathbb{F}_p$. ~~The~~

The deg of 1st term: $(p-1)|V| < |E|$ (b/c avg. deg $> 2p-2$)
(recall avg. deg $= \frac{|E|}{|V|} = \frac{\text{avg. \# edges}}{\text{node}}$)

$\Rightarrow \deg(F) = |E|$.

The coeff. of ~~$\prod_{e\in E} x_e$~~ $\prod_{e\in E} x_e$ in F is $(-1)^{|E|+1} \neq 0$.

By Theorem 1.2, $\exists$ values $x_e \in \{0,1\}$ s.t.

$$F((x_e)_{e\in E}) \neq 0.$$

$(x_e)_{e\in E} \neq 0$, since $F(0)=0$.

Additionally, $\underbrace{\sum_{e\in E} a_{v,e} x_e}_{=\deg(v)} = 0 \mod p$ $\forall v$ and $(x_e)_{e\in E}$, o.w. $F((x_e)_{e\in E})=0$.

$\Rightarrow$ subgraph w/ all edges $e \in E$ is ~~p-regular~~ has deg's div by p; since the max deg is $2p-1$ we are done $\square$

Theorem 6.1 can be proved for prime powers too, but open for arbitrary integers (at least I think...)

Def A coloring of a graph G is a way of coloring the vertices of a graph s.t. no two adjacent vertices are of the same color.

A ~~k-coloring~~ a coloring that ~~uses~~ uses k colors.

~~DEFINE GRAPH POLY'S~~

~~Thm 9.2 (Kleitman and Lovász) A graph G is not k-colorable iff the graph polynomial f_G lies in the ideal gen. by all graph polynomials of complete graphs on $k+1$ vertices.~~

Thm 9.3 (Alon and Tarsi) A graph on n vertices is not k-colorable iff the graph polynomial f_G lies in the ideal gen. by the polynomials $x_i^k - 1$, $(1 \leq i, \leq n)$.

Pf If f_G lies in the ideal gen by $x_i^k - 1$, then f_G vanishes when each x_i ~~things~~ is a k^{th} root of unity

$\Rightarrow$ Any coloring of G by the k^{th} roots of unity, $\exists$ (i,j) s.t. $(i,j) \in E$ and $c(v_i) = c(v_j)$

Suppose G not k-colorable. Then f_G vanishes whenever each $g_i(x_i) = x_i^k - 1$ vanishes.

Apply Thm 1.1. $\square$

Def The graph polynomial of $G=(V,E)$, $V=\{v_1, \ldots, v_n\}$

$$f_G = f_G(x_1, \ldots, x_n) = \prod_{\substack{i<j \\ (v_i,v_j)\in E}} (x_i - x_j)$$