Title : Combinatorial Nullstellensatz and Applications
Paper by Noga Alon

$0 \neq f(x) \in F(x)$, degree t

f can't have more than t zeroes

Given $S \subset F$ with $|S| > t$, $\exists\ s \in S$ s.t. $f(s) \neq 0$

Lemma : $0 \neq f \in F[x_1, x_2, \ldots, x_n]$ (Lemma 2.1 in Alon's paper)

deg of $x_i \leq t_i$

$S_1 \times S_2 \times \ldots \times S_n \subset F \times F \times \ldots \times F$, $|S_i| > t_i$

$\exists\ (s_1, \ldots, s_n)$ s.t. $f(s_1, s_2, \ldots, s_n) \neq 0$

Theorem (Comb. Null) : $f \in F[x_1, x_2, \ldots, x_n]$ (Thm 1.2 in Alon's paper)

$\deg f = \sum_{i=1}^{n} t_i$

Coeff of $x_1^{t_1} x_2^{t_2} \ldots x_n^{t_n}$ is nonzero

$S_1, \ldots, S_n \subset F$, $|S_i| > t_i$

Then $\exists\ (s_1, \ldots, s_n) \in S_1 \times \ldots \times S_n$

s.t. $f(s_1, s_2, \ldots, s_n) \neq 0$

"A polynomial of a certain degree cannot vanish over a large set of nos."

Apps to Graph Theory, Number Theory, Enumerative Combinatorics

Thm asserting something is true :
Pf by Contradiction → construct a polynomial of smaller degree that vanishes over a large enough set

Thm guaranteeing existence of something :
Construct a poly of small degree, our search space corresponds to pt. where poly is looking at a large enough set of values, we are guaranteed a non-vanishing pt.

(I) Cauchy - Davenport Theorem

(Thm 3.2 in Alon's paper)

$A, B \subset \mathbb{Z}_p$. $A+B := \{a+b \mid a \in A, b \in B\}$

Then $|A+B| \geq \min\{p, |A|+|B|-1\}$

($|A|+|B|-1$ can be attained by for eg $A = \{0\}$, $B = \{1, 2, \ldots, p-1\}$)

Proof: Then asserts

$|A|+|B| > p \Rightarrow |A+B| = p \Rightarrow A+B = \mathbb{Z}_p$

$g \in \mathbb{Z}_p$. $|g-A| + |B| = |A|+|B| > p$

$b \in (g-A) \cap B \neq \phi$ $\quad g-a = b \in B$

So assume $|A|+|B| \leq p$. Want $|A+B| \geq |A|+|B|-1$

Suppose $|A+B| \leq |A|+|B|-2 = (|A|-1)+(|B|-1)$

$C \neq A+B$, $C \supseteq A+B$, $|C| = |A|+|B|-2$

$f(x,y) = \prod_{c \in C}(x+y-c)$ vanishes $\forall (x,y) \in A \times B$

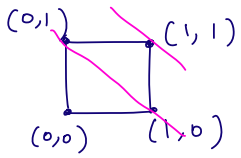
$\deg = |C| = (|A|-1)+(|B|-1)$

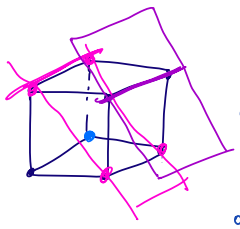
Coeff of $x^{|A|-1} y^{|B|-1}$: $\binom{|A|+|B|-2}{|A|-1}$, $\neq 0$ in $\mathbb{Z}_p$ since $|A|+|B|-2 < p$

So $\exists$ non-zero pt in $A \times B$. Contradiction!

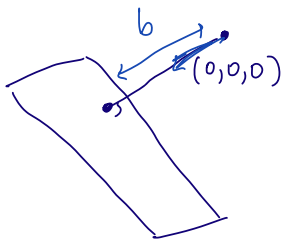
Theorem: Let $H_1, H_2, \ldots, H_m$ be hyperplanes in $\mathbb{R}^n$ that cover all vertices of $[0,1]^n$ but one. Then $m \geq n$. (Thm 6.3 in Alon's paper)

Proof:





(all but one vertex condition is imp — o/w $\{0,1\}^3$ for eg can be covered with 2 planes)



unit vector in this direction: a

$$a \cdot x = b \qquad (x = (x_1, x_2, \ldots x_n))$$

$H_1, H_2, \ldots, H_m$ covers all but $(0, 0, \ldots, 0)$

$x = (x_1, \ldots, x_n)$. H_i : $(a_i \cdot x) = b_i$

Suppose $m < n$.

Will construct a polynomial of degree n that vanishes on $\{0,1\}^n$

$$(-1)^m \prod_{j=1}^{m} b_j \prod_{i=1}^{n}(1-x_i) - \prod_{i=1}^{m}\left[(a_i \cdot x) - b_i\right]$$

(3) need this part to still vanish on non-zero pts

(2) Want poly to vanish at $(0,0,\ldots,0)$ too

deg n

(1) Each pt lies on some H_i

deg $m < n$

Coeff of $x_1^1 x_2^1 \ldots x_n^1 \neq 0$

So cannot vanish on $\{0,1\} \times \{0,1\} \times \ldots \times \{0,1\}$. Contradiction

III. **Theorem:** (Thm 6.1 in Alon's paper)

$G = (V, E)$ loopless graph. p prime.

Avg. degree $> 2p-2$

Max. degree $\leq 2p-1$

Then G has a p-regular subgraph

Recall: $\sum_{v \in V} \deg v = 2|E| = 2n$ } Hypothesis $\Rightarrow$ $2|E| > (2p-2)|V|$ $\Leftrightarrow |E| > (p-1)|V|$

In $\mathbb{F}_p$, $a^{p-1} \equiv 1 \mod p$ if $a \not\equiv 0 \mod p$

$0 \mod p$ if $a \equiv 0 \mod p$

Proof: "Existence" proof. So will construct poly, will be interested in when the poly value is non-zero

$|E| = n$

$e_1, e_2, \ldots, e_n$

Subgraph $\rightsquigarrow$ collection of edges

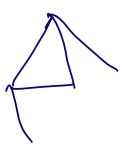
Variables $x_{e_1}, x_{e_2}, \ldots, x_{e_n}$. Look at values in $\{0,1\}^n$

$\{0,1\} \times \{0,1\} \times \cdots \times \{0,1\}$

For an edge e, $x_e = 1$ if $e \in$ subgraph

0 if $e \notin$ subgraph

Restriction:



If v is incident on an edge in the subgraph, then $\deg v = p$ in the subgraph

i.e. $\forall\, v \in V$, v is incident on exactly 0 or p of the edges in the subgraph

$\forall\, (v,e) \in (V,E)$, $a_{v,e} := 1$ if v incident on e

0 o/w

For fixed v, $\sum_{e \in \text{subgraph}} a_{v,e} = 0$ or p

$$\sum_{e \in E} a_{v,e} x_e = 0 \bmod p$$

$\leq \deg v < 2p$

Field : $\mathbb{F}_p$

$$\left(\sum_{e \in E} a_{v,e} x_e\right)^{p-1} = \begin{cases} 1 & \text{if sum is non-zero} \\ 0 & \text{if sum is } 0 \end{cases}$$

→ This is the case we want

$$f(x_{e_1}, \ldots, x_{e_n}) = \prod_{v \in V} \left(1 - \left(\sum_{e \in E} a_{v,e} x_e\right)^{p-1}\right) - \prod_{e \in E}(1 - x_e)$$

① Want non-zero value

② Want non-zero $\forall v$

③ Want to guarantee that all x_e are not 0

$\deg (p-1)|V| < |E|$

$\deg |E|$, coeff of $x_{e_1}^{1} x_{e_2}^{1} \cdots x_{e_n}^{1} \neq 0$

So, $\exists (s_1, s_2, \ldots, s_n) \in \{0,1\}^n$ s.t. $f(s_1, s_2, \ldots, s_n) \neq 0$