Math 554

Hemanshu Kaul

kaul@iit.edu

Polynomial Method

In a recent survey article of Terence Tao, he describes the polynomial method as

"strategy is to capture the arbitrary set of objects in the zero set of a polynomial whose degree is under control; for instance the degree may be bounded by a function of the number of the objects."

Then we use algebraic tools to understand this zero set

We saw this using linear algebra & dimension of vector spaces.
Now, we will study this approach using abstract algebra.

The famous Hilbert's Nullstellensatz ("theorem of zeros"), a foundational result in algebraic geometry, states:

Theorem [Hilbert 1900] Let $\mathbb{F}$ be an algebraicly closed field & let $f, g_1, \ldots, g_m \in \mathbb{F}[x_1, \ldots, x_n]$ be polynomials such that f vanishes over all common zeros of $g_1, \ldots, g_m$. Then there exist $k \in \mathbb{Z}$ and polynomials $h_1, h_2, \ldots, h_m \in \mathbb{F}[x_1, \ldots, x_n]$ such that

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

We need a form that can be applied to combinatorial/discrete problem in a quantifiable way, and works over any field, especially $\mathbb{R}$ and $\mathbb{F}_q$ which are not algebraicly closed.

We know that a nonzero polynomial of degree d in a single variable has at most d zeros (roots).

<u>Lemma D</u> Let $f \in \mathbb{F}[x_1]$ s.t. $f(x_1) = \sum_{i=0}^{d} c_k x_1^k$ and f has at least $d+1$ roots, then $c_1 = c_2 = \cdots = c_d = 0$, i.e., $f(x_1) = 0$

We know that a nonzero polynomial of degree d in a single variable has at most d zeros (roots).

__Lemma 0__ Let $f \in \mathbb{F}[x_1]$ s.t. $f(x_1) = \sum_{i=0}^{d} c_k x_1^k$ and f has at least $d+1$ roots, then $c_1 = c_2 = \cdots = c_d = 0$, i.e., $f \equiv 0$.

How can we generalize this to n variables?

__Lemma 1__ Let $f \in \mathbb{F}[x_1, \dots, x_n]$. For each i, the degree of f as a polynomial in x_i be at most d_i, and let S_i be a set of d_i+1 distinct values in $\mathbb{F}$.
If $f(x_1, \dots, x_n) = 0$ for $(x_1, \dots, x_n) \in \prod_{i=1}^{n} S_i$, then $f \equiv 0$.

We know that a nonzero polynomial of degree d in a single variable has at most d zeros (roots).

<u>Lemma 0</u> Let $f \in \mathbb{F}[x_1]$ s.t. $f(x_1) = \sum_{i=0}^{d} c_k x_1^k$ and f has at least $d+1$ roots, then $c_1 = c_2 = \cdots = c_d = 0$, i.e., $f \equiv 0$.

How can we generalize this to n variables?

<u>Lemma 1</u> Let $f \in \mathbb{F}[x_1, \ldots, x_n]$. For each i, the degree of f as a polynomial in x_i be at most d_i, and let S_i be a set of d_i+1 distinct values in $\mathbb{F}$.
If $f(x_1, \ldots, x_n) = 0$ for $(x_1, \ldots, x_n) \in \prod_{i=1}^{n} S_i$, then $f \equiv 0$.

Proof by induction on n. $n=1$ is Lemma 0.
For $n>1$, we collect terms to write f as a polyn. in x_n, that is $f(\vec{x}) = \sum_{j=0}^{d_n} f_j(x_1, \ldots, x_{n-1}) x_n^j$ where each f_j is a polyn. of deg. $\leq d_i$ in x_i.

We know that a nonzero polynomial of degree d in a single variable has at most d zeros (roots).

Lemma 0 Let $f \in \mathbb{F}[x_1]$ s.t. $f(x_1) = \sum_{i=0}^{d} c_k x_1^k$ and f has at least $d+1$ roots, then $c_1 = c_2 = \cdots = c_d = 0$, i.e., $f \equiv 0$.

How can we generalize this to n variables?

Lemma 1 Let $f \in \mathbb{F}[x_1, \ldots, x_n]$. For each i, the degree of f as a polynomial in x_i be at most d_i, and let S_i be a set of d_i+1 distinct values in $\mathbb{F}$.
If $f(x_1, \ldots, x_n) = 0$ for $(x_1, \ldots, x_n) \in \prod_{i=1}^{n} S_i$, then $f \equiv 0$.

Proof by induction on n. $n=1$ is Lemma 0.
For $n>1$, we collect terms to write f as a polyn. in x_n, that is $f(\vec{x}) = \sum_{j=0}^{d_n} f_j(x_1, \ldots, x_{n-1}) x_n^j$ where each f_j is a polyn. of deg. $\leq d_i$ in x_i.
For $(x_1, \ldots, x_{n-1})$ in $\prod_{i=1}^{n-1} S_i$, evaluating $f_0, f_1, \ldots, f_{d_n}$ yields a 1-var polyn. in x_n & deg $\leq d_n$.
By ind. hyp., this polyn. is 0 for $x_n \in S_n$. $\therefore f_i = 0$ over $\prod_{i=1}^{n-1} S_i$, so $f \equiv 0$ ∎

We know that a nonzero polynomial of degree d in a single variable has at most d zeros (roots).

<u>Lemma 0</u> Let $f \in \mathbb{F}[x_1]$ s.t. $f(x_1) = \sum_{i=0}^{d} c_k x_1^k$ and f has at least $d+1$ roots, then $c_1 = c_2 = \cdots = c_d = 0$, i.e., $f \equiv 0$.

How can we generalize this to n variables?

<u>Lemma 1</u> Let $f \in \mathbb{F}[x_1, \ldots, x_n]$. For each i, the degree of f as a polynomial in x_i be at most d_i, and let S_i be a set of d_i+1 distinct values in $\mathbb{F}$.
If $f(x_1, \ldots, x_n) = 0$ for $(x_1, \ldots, x_n) \in \prod_{i=1}^{n} S_i$, then $f \equiv 0$.

Can we make this lemma stronger? Instead of controlling the degree in each variable individually, can we do it for total degree of the polynomial?

We know that a nonzero polynomial of degree d in a single variable has at most d zeros (roots).

Lemma 0 Let $f \in \mathbb{F}[x_1]$ s.t. $f(x_1) = \sum_{i=0}^{d} c_k x_1^k$ and f has at least $d+1$ roots, then $c_1 = c_2 = \cdots = c_d = 0$, i.e., $f \equiv 0$.

How can we generalize this to n variables?

Lemma 1 Let $f \in \mathbb{F}[x_1, \ldots, x_n]$. For each i, the degree of f as a polynomial in x_i be at most d_i, and let S_i be a set of d_i+1 distinct values in $\mathbb{F}$.
If $f(x_1, \ldots, x_n) = 0$ for $(x_1, \ldots, x_n) \in \prod_{i=1}^{n} S_i$, then $f \equiv 0$.

Combinatorial Nullstellensatz [Alon 1999, known since 1980s]

If $\prod_{i=0}^{n} x_i^{t_i}$ is a monomial with non-zero coefficient in $f \in \mathbb{F}[x_1, \ldots, x_n]$ where f has degree $\sum_{i=1}^{n} t_i$, and $S_1, \ldots, S_n \subseteq \mathbb{F}$ with $|S_i| > t_i$, $\forall i$, then $f(x) \neq 0$ for some $x \in \prod_{i=1}^{n} S_i$

We know that a nonzero polynomial of degree d in a single variable has at most d zeros (roots).

<u>Lemma 0</u> Let $f \in \mathbb{F}[x_1]$ s.t. $f(x_1) = \sum_{i=0}^{d} c_k x_1^k$ and f has at least $d+1$ roots, then $c_1 = c_2 = \cdots = c_d = 0$, i.e., $f \equiv 0$.

How can we generalize this to n variables?

<u>Lemma 1</u> Let $f \in \mathbb{F}[x_1, \dots, x_n]$. For each i, the degree of f as a polynomial in x_i be at most d_i, and let S_i be a set of d_i+1 distinct values in $\mathbb{F}$.
If $f(x_1, \dots, x_n) = 0$ for $(x_1, \dots, x_n) \in \prod_{i=1}^{n} S_i$, then $f \equiv 0$.

<u>Combinatorial Nullstellensatz [Alon 1999, known since 1980s]</u> any field

If $\prod_{i=0}^{n} x_i^{t_i}$ is a monomial with non-zero coefficient in $f \in \mathbb{F}[x_1, \dots, x_n]$ where f has degree $\sum_{i=1}^{n} t_i$, and $S_1, \dots, S_n \subseteq \mathbb{F}$ with $|S_i| > t_i$, $\forall i$, then $f(x) \not\equiv 0$ for some $x \in \prod_{i=1}^{n} S_i$

Freedom to choose any monomial of highest degree $\sum t_i$. $|S_i|$ is based on our "choice".

Given two sets $A, B \subseteq \mathbb{Z}_n$, define

$$A+B = \{a+b : a \in A, b \in B\} \subseteq \mathbb{Z}_n$$

How large is $|A+B|$ in terms of $|A|$ and $|B|$?

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

then $A+B = \{0, \dots\dots, a+b-2\}$, but "modulo n" means

$|A+B| = \min\{n, a+b-1\}$ (think of $a=2, b=2, n=2$)

If n is not prime, consider $n = 2k$ & $A = \{0, 2, 4, \dots, 2k-2\}$

$B = \{0, 2, 4, \dots, 2k-2\}$

then $A+B = \{0, 2, 4, \dots, 2k-2\}$

so, $|A+B| = n/2 < \min\{n, a+b-1\}$

We can avoid such small size of $A+B$ with n = prime.

Cauchy-Davenport Theorem

1813 1935

Let $A, B \subseteq \mathbb{Z}_p$, p prime, be two nonempty subsets.

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

Cauchy (1813) - Davenport (1935) Theorem

Let $A, B \subseteq \mathbb{Z}_p$, p prime, be two nonempty subsets.
Then $|A+B| \geq \min\{p, |A|+|B|-1\}$

$|\{c-b : b \in B\}| = |B|$ & $|A|+|B| > p$
so by pigeonhole principle,

Proof

If $|A|+|B| \geq p+1$ then for any $c \in \mathbb{Z}_p$, we have $\boxed{A \cap \{c-b : b \in B\} \text{ is non empty}}$

that is, $\exists\, a \in A, b \in B$ s.t. $a = c-b$, i.e, $a+b = c \in \mathbb{Z}_p$

So, $A+B \supseteq \mathbb{Z}_p$.

Hence $A+B = \mathbb{Z}_p$, and $|A+B| = p$ as required.

Cauchy-Davenport Theorem

1813 (Cauchy), 1935 (Davenport)

Let $A, B \subseteq \mathbb{Z}_p$, p prime, be two nonempty subsets.

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

Proof If $|A|+|B| \leq p$ then $|A|+|B|-1 < p$ & we show $|A+B| \geq |A|+|B|-1$

Suppose not, then $\exists\, C \subseteq \mathbb{Z}_p$ s.t. $|C| = |A|+|B|-2$ and $A+B \subseteq C$.

Define $f(x,y) \in \mathbb{Z}_p[x,y]$ as $f(x,y) = \prod_{c \in C}(x+y-c)$, a polyn. of deg. $|C| = |A|+|B|-2$

Let $t_1 = |A|-1$ and $t_2 = |B|-1$, then $\deg(f) = t_1 + t_2$

Claim $\underbrace{[x^{t_1} y^{t_2}]\, f(x,y)}_{\text{coefficient of monomial } x^{t_1} y^{t_2} \text{ in } f(x,y)} = \binom{t_1+t_2}{t_1}$ $\because$ total t_1+t_2 choices using either x or y from each factor

Cauchy-Davenport Theorem

1813 (Cauchy), 1935 (Davenport)

Let $A, B \subseteq \mathbb{Z}_p$, p prime, be two nonempty subsets.

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

<u>Proof</u> If $|A|+|B| \leq p$ then $|A|+|B|-1 < p$ & we show $|A+B| \geqslant |A|+|B|-1$

Suppose not, then $\exists\, C \subseteq \mathbb{Z}_p$ s.t. $|C| = |A|+|B|-2$ and $A+B \subseteq C$.

Define $f(x,y) \in \mathbb{Z}_p[x,y]$ as $f(x,y) = \prod_{c \in C} (x+y-c)$, a polyn. of deg. $|C| = |A|+|B|-2$

Let $t_1 = |A|-1$ and $t_2 = |B|-1$, then $\deg(f) = t_1 + t_2$

<u>Claim</u> $[x^{t_1} y^{t_2}] f(x,y) = \binom{t_1+t_2}{t_1}$ $\because$ total t_1+t_2 choices using either x or y from each factor

<u>claim</u> $\binom{t_1+t_2}{t_1} \not\equiv 0 \pmod p$ $\because$ $t_1+t_2 < p$ & $\dfrac{(t_1+t_2)!}{t_1!\, t_2!}$ no term is greater than p & p is prime

Apply CN with $\mathbb{F} = \mathbb{Z}_p$, $n=2$, $S_1 = A$, $S_2 = B$, giving us

$\exists\, (a,b) \in A \times B$ s.t. $f(a,b) \neq 0$ contradiction since $f(a,b) = 0$ $\forall a \in A, b \in B$.

Combinatorial Nullstellensatz applications

① Design f which is zero over ΠS_i

② Find a coeff $\neq 0$ for an appropriate max degree monomial

Contradiction!

We will see direct applications also where $f(s) \neq 0$ gives $s \equiv$ solution for the problem.

Consider $A, B \subseteq \mathbb{Z}_n$ (n not neccessarily prime)

then $A+B = \mathbb{Z}_n$ if $|A|+|B|>n$

what if $A = B$? e.g. $A = \{0, 1, \dots, a-1\}$, $|A+A| = 2a-1$

Let $2A = A+A = \{a+a' : a, a' \in A\}$

Then Cauchy-Davenport $\Rightarrow$ $|2A| \geq \min\{2a-1, p\}$

Consider $A, B \subseteq \mathbb{Z}_n$ (n not neccessarily prime)

then $A+B = \mathbb{Z}_n$ if $|A|+|B|>n$

What if $A=B$? e.g. $A=\{0,1,\ldots,a-1\}$, $|A+A| = 2a-1$

$\underbrace{|A+A \text{ without sums of the form } x+x}_{\text{only add distinct elements of } A}| = 2a-3$

Let $2A = A+A = \{a+a' : a, a' \in A\}$

Then Cauchy-Davenport $\Rightarrow$ $|2A| \geq \min\{2a-1, p\}$

What if we only add distinct elements of A?

Theorem [Erdős-Heilbronn Conjecture 1964;
Dias da Silva – Hamidoune 1994]

If $A \subseteq \mathbb{Z}_p$, p prime, and C is the set of sums of distinct element of A, then $|C| \geq \min\{2|A|-3, p\}$

Theorem [Erdős-Heilbronn Conjecture 1964; Dias da Silva – Hamidoune 1994]

If $A \subseteq \mathbb{Z}_p$, p prime, and C is the set of sums of distinct element of A, then $|C| \geq \min\{2|A|-3, p\}$

Proof Assume $2|A|-3 < p$ (else we can again give PP argument)

Define $f(x,y) = (x-y) \prod_{c \in C} (x+y-c)$ ($(x-y)$ term ensures distinct elements)

let $|C| = m$, then $\deg(f) = m+1$ & $f(x,y)=0$ for $(x,y) \in A \times A$ s.t. $x+y \in C$

Theorem [Erdős-Heilbronn Conjecture 1964; Dias da Silva – Hamidoune 1994]

If $A \subseteq \mathbb{Z}_p$, p prime, and C is the set of sums of distinct element of A, then $|C| \geq \min\{2|A|-3, p\}$

Proof Assume $2|A|-3 < p$ (else we can again give PP argument)

Define $f(x,y) = (x-y)\prod_{c\in C}(x+y-c)$ ((x-y) term ensures distinct elements)

let $|C| = m$, then $\deg(f) = m+1$ & $f(x,y)=0$ for $(x,y)\in A\times A$ s.t. $x+y\in C$

$$[x^{t-1}y^{m-t+2}]f(x,y) = \binom{m}{t-2} - \binom{m}{t-1} = \left(1-\frac{m-t+2}{t-1}\right)\binom{m}{t-2}$$

where $t = |A|$.

contributions to this coeff. use x or y in each factor

if x from 1st factor then positive contribution

if $-y$ from ——— " ——— negative contribution

Theorem [Erdős-Heilbronn Conjecture 1964; Dias da Silva – Hamidoune 1994]

If $A \subseteq \mathbb{Z}_p$, p prime, and C is the set of sums of distinct element of A, then $|C| \geq \min\{2|A|-3, p\}$

Proof Assume $2|A|-3 < p$ (else we can again give PP argument)

Define $f(x,y) = (x-y) \prod_{c \in C} (x+y-c)$ ($(x-y)$ term ensures distinct elements)

let $|C| = m$, then $\deg(f) = m+1$ & $f(x,y) = 0$ for $(x,y) \in A \times A$ s.t. $x+y \in C$

$[x^{t-1} y^{m-t+2}] f(x,y) = \binom{m}{t-2} - \binom{m}{t-1} = \left(1 - \frac{m-t+2}{t-1}\right)\binom{m}{t-2}$ where $t = |A|$.

If $m \leq 2t-4$ then coeff is positive and $t > m-t+2$ & no factor of p

Then CN $\Rightarrow \exists\, (x,y) \in \underbrace{A \times A}_{x \neq y}$ s.t. $f(x,y) \neq 0$ why? Contradiction!

Hence $m \geq 2t-3$.

Regular Sub-graphs

How many edges are needed to guarantee the existence of a 2-regular subgraph in any graph on n vertices?

Regular Sub-graphs

How many edges are needed to guarantee the existence of a 2-regular subgraph in any graph on n vertices?

n edges. Easy!

Erdős-Sauer asked the same question for 3-regular subgraph

It's conjectured $n^{1+\epsilon}$ (for any $\epsilon > 0$) edges suffice.

Pyber (1985) proved: for large enough n, every graph on n vertices with at least $\Theta(n \log n)$ edges contains a 3-reg subgraph.

Pyber et al. (1995) proved: for every large enough n, $\exists$ graph on n vertices with $\Theta(n \log\log n)$ edges that does not have a 3-reg subgraph.

Regular Sub-graphs

How many edges are needed to guarantee the existence of a 2-regular subgraph in any graph on n vertices?

n edges. Easy!

Erdős-Sauer asked the same question for 3-regular subgraph

They specifically conjectured that every 4-regular graph has a 3-regular subgraph.

Taskinov (1982) & independently Zhang (1986) proved this

Regular Sub-graphs

How many edges are needed to guarantee the existence of a 2-regular subgraph in any graph on n vertices?

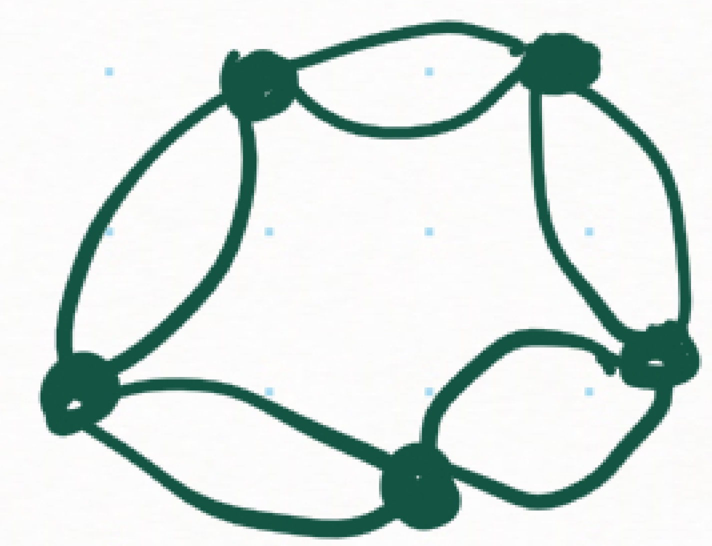
n edges. Easy!

Erdős-Sauer asked the same question for 3-regular subgraph

They specifically conjectured that every 4-regular graph has a 3-regular subgraph.

Taskinov (1982) & independently Zhang (1986) proved this

This claim is false for multigraphs. Consider a "double" odd cycle.



Regular Sub-graphs

How many edges are needed to guarantee the existence of a 2-regular subgraph in any graph on n vertices?

n edges. Easy!

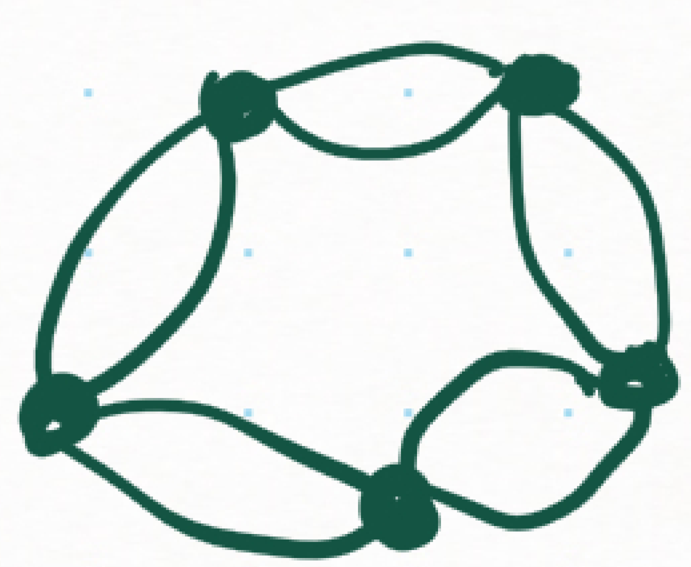
Erdős-Sauer asked the same question for 3-regular subgraphs

They specifically conjectured that every 4-regular graph has a 3-regular subgraph.

Taskinov (1982) & independently Zhang (1986) proved this

This claim is false for multigraphs. Consider a "double" odd cycle.

But if we add even a single extra edge to a 4-regular multigraph, then we will have a 3-regular subgraph.



Theorem [Alon–Friedland–Kalai 1984]

If p is prime, then every loopless multigraph G of average degree $> 2p-2$, and max degree $\leq 2p-1$ contains p-regular subgraph.

Look at $p=3$: $\frac{2m}{n} > 4$, i.e., $m > 2n$, extra edge

compare to 4-regular graph which has $2n$ edges

Theorem [Alon-Friedland-Kalai 1984]

If p is prime, then every loopless multigraph G of average degree $> 2p-2$, and max degree $\leq 2p-1$ contains p-regular subgraph.

Proof Let G have n vertices and m edges. Let $\Gamma(v)$ = set of edges incident to v

We want a polyn. f s.t. $f(x) \neq 0$ means $x \leftrightarrow p$-regular subgraph.

x_e, $e \in E(G)$ be 0-1 variables (indicating whether or not to pick e).

$$f(x) = \prod_{v \in V(G)} \left[1 - \left(\sum_{e \in \Gamma(v)} x_e\right)^{p-1}\right] - \prod_{e \in E(G)} (1 - x_e)$$

$\deg(f) = ?$

Theorem [Alon–Friedland–Kalai 1984]

If p is prime, then every loopless multigraph G of average degree $> 2p-2$, and max degree $\leq 2p-1$ contains p-regular subgraph.

<u>Proof</u> Let G have n vertices and m edges. Let $\Gamma(v)$ = set of edges incident to v

We want a polyn. f s.t. $f(x) \neq 0$ means $x \longleftrightarrow p$-regular subgraph.

x_e, $e \in E(G)$ be 0-1 variables (indicating whether or not to pick e).

$$f(x) = \underbrace{\prod_{v \in V(G)} \left[1 - \left(\sum_{e \in \Gamma(v)} x_e\right)^{p-1}\right]}_{\text{degree} \leq n(p-1)} - \underbrace{\prod_{e \in E(G)} (1 - x_e)}_{\text{degree } m}$$

We know $\frac{2m}{n} > 2p-2$, i.e., $m > n(p-1)$

So $\deg(f) = m$

Theorem [Alon–Friedland–Kalai 1984]

If p is prime, then every loopless multigraph G of average degree $> 2p-2$, and max degree $\leq 2p-1$ contains p-regular subgraph.

<u>Proof</u> Let G have n vertices and m edges. Let $\Gamma(v)$ = set of edges incident to v

We want a polyn. f s.t. $f(x) \neq 0$ means $x \leftrightarrow p$-regular subgraph.

x_e, $e \in E(G)$ be 0-1 variables (indicating whether or not to pick e).

$$f(x) = \prod_{v \in V(G)} \left[1 - \left(\sum_{e \in \Gamma(v)} x_e \right)^{p-1} \right] - \prod_{e \in E(G)} (1 - x_e) \; ; \; \deg(f) = m$$

and $\left[\prod_{e \in E(G)} x_e \right] f(x) = (-1)^{m+1} \neq 0$ (in any field)

Theorem [Alon-Friedland-Kalai 1984]

If p is prime, then every loopless multigraph G of average degree $> 2p-2$, and max degree $\leq 2p-1$ contains p-regular subgraph.

Proof Let G have n vertices and m edges. Let $\Gamma(v)$ = set of edges incident to v

We want a polyn. f s.t. $f(x) \neq 0$ means $x \longleftrightarrow p$-regular subgraph.

x_e, $e \in E(G)$ be 0-1 variables (indicating whether or not to pick e).

$$f(x) = \prod_{v \in V(G)} \left[1 - \left(\sum_{e \in \Gamma(v)} x_e\right)^{p-1}\right] - \prod_{e \in E(G)} (1 - x_e) \; ; \; \deg(f) = m$$

and $\left[\prod_{e \in E(G)} x_e\right] f(x) = (-1)^{m+1} \neq 0$ (in any field)

Apply CN with $S_i = \{0, 1\}$ over $\mathbb{F}_p$.

$\therefore \exists \; s = (s_1, \dots, s_m) \in \{0,1\}^{|E|}$ s.t. $f(s) \neq 0$

Note $s \neq (0, \dots, 0)$ since ?

Theorem [Alon–Friedland–Kalai 1984]

If p is prime, then every loopless multigraph G of average degree $> 2p-2$, and max degree $\leq 2p-1$ contains p-regular subgraph.

Proof Let G have n vertices and m edges. Let $\Gamma(v)=$ set of edges incident to v

We want a polyn. f s.t. $f(x)\neq 0$ means $x \longleftrightarrow p$-regular subgraph.

x_e, $e\in E(G)$ be 0-1 variables (indicating whether or not to pick e).

$$f(x)=\prod_{v\in V(G)}\left[1-\left(\sum_{e\in\Gamma(v)} x_e\right)^{p-1}\right] - \prod_{e\in E(G)}(1-x_e) \; ; \; \deg(f)=m$$

and $\left[\prod_{e\in E(G)} x_e\right] f(x) = (-1)^{m+1} \neq 0$ (in any field)

Apply CN with $S_i=\{0,1\}$ over $\mathbb{F}_p$.

$\therefore \exists\ s=(s_1,\dots,s_m)\in\{0,1\}^{|E|}$ s.t. $f(s)\neq 0$

Note $s\neq(0,\dots,0)$ since $f(0,\dots,0)=0-0=0$

Since some $s_i=1$, $\prod_{j=1}^{m}(1-s_j)=0$. Hence $f(x)=\prod_{v\in V(G)}\left[1-\left(\sum_{e\in\Gamma(v)} x_e\right)^{p-1}\right]\neq 0$ when $x=s$

Theorem [Alon-Friedland-Kalai 1984]

If p is prime, then every loopless multigraph G of average degree $> 2p-2$, and max degree $\leq 2p-1$ contains p-regular subgraph.

Proof Let G have n vertices and m edges. Let $\Gamma(v)$ = set of edges incident to v

we want a polyn. f s.t. $f(x) \neq 0$ means $x \longleftrightarrow p$-regular subgraph.

x_e, $e \in E(G)$ be 0-1 variables (indicating whether or not to pick e).

$$f(x) = \prod_{v \in V(G)} \left[1 - \left(\sum_{e \in \Gamma(v)} x_e\right)^{p-1}\right] - \prod_{e \in E(G)} (1 - x_e)$$

By CN, we found $s \neq (0,..,0)$ in $\{0,1\}^m$ s.t. $f(s) \neq 0$

and $f(x) = \prod_v \left[1 - \left(\sum_{e \in \Gamma(v)} x_e\right)^{p-1}\right] \neq 0$ when $x = s$

Theorem [Alon–Friedland–Kalai 1984]

If p is prime, then every loopless multigraph G of average degree $> 2p-2$, and max degree $\leq 2p-1$ contains p-regular subgraph.

Proof Let G have n vertices and m edges. Let $\Gamma(v)$ = set of edges incident to v

We want a polyn. f s.t. $f(x) \neq 0$ means $x \longleftrightarrow p$-regular subgraph.

x_e, $e \in E(G)$ be 0-1 variables (indicating whether or not to pick e).

$$f(x) = \prod_{v \in V(G)} \left[1 - \Big(\sum_{e \in \Gamma(v)} x_e \Big)^{p-1} \right] - \prod_{e \in E(G)} (1 - x_e)$$

By CN, we found $s \neq (0, \ldots, 0)$ in $\{0,1\}^m$ s.t. $f(s) \neq 0$

and $f(x) = \underbrace{\prod \Big[1 - \Big(\sum_{e \in \Gamma(v)} x_e \Big)^{p-1} \Big]}_{}$ $\neq 0$ when $x = s$, over $\mathbb{F}_p$

prime

$\hookrightarrow$ is not a multiple of p, so each factor is not a multiple of p

So, $\left(\sum x_e\right)^{p-1} \neq 1 \pmod p$ which implies $\sum_{e \in \Gamma(v)} x_e = 0 \pmod p$

Theorem [Alon–Friedland–Kalai 1984]

If p is prime, then every loopless multigraph G of average degree $> 2p-2$, and max degree $\leq 2p-1$ contains p-regular subgraph.

Proof Let G have n vertices and m edges. Let $\Gamma(v)$ = set of edges incident to v

We want a polyn. f s.t. $f(x) \neq 0$ means $x \longleftrightarrow p$-regular subgraph.

x_e, $e \in E(G)$ be 0-1 variables (indicating whether or not to pick e).

$$f(x) = \prod_{v \in V(G)} \left[1 - \Big(\sum_{e \in \Gamma(v)} x_e\Big)^{p-1}\right] - \prod_{e \in E(G)} (1 - x_e)$$

By CN, we found $s \neq (0,\dots,0)$ in $\{0,1\}^m$ s.t. $f(s) \neq 0$

and $f(x) = \prod\left[1 - \Big(\sum_{e \in \Gamma(v)} x_e\Big)^{p-1}\right] \neq 0$ when $x = s$ in $\mathbb{F}_p$

$\Rightarrow \left(\sum x_e\right)^{p-1} \neq 1 \pmod p$ $\Rightarrow$ $\sum_{e \in \Gamma(v)} x_e = 0 \pmod p$

Fermat's Little Thm p prime, $a \not\equiv 0 \pmod p \Rightarrow a^{p-1} \equiv 1 \pmod p$

Theorem [Alon–Friedland–Kalai 1984]

If p is prime, then every loopless multigraph G of average degree $> 2p-2$, and max degree $\leq 2p-1$ contains p-regular subgraph.

<u>Proof</u> Let G have n vertices and m edges. Let $\Gamma(v)$ = set of edges incident to v

We want a polyn. f s.t. $f(x) \neq 0$ means $x \longleftrightarrow p$-regular subgraph.

x_e, $e \in E(G)$ be 0-1 variables (indicating whether or not to pick e).

$$f(x) = \prod_{v \in V(G)} \left[1 - \left(\sum_{e \in \Gamma(v)} x_e\right)^{p-1}\right] - \prod_{e \in E(G)} (1 - x_e)$$

By CN, we found $s \neq (0, \dots, 0)$ in $\{0,1\}^m$ s.t. $f(s) \neq 0$

and $f(x) = \prod_v \left[1 - \left(\sum_{e \in \Gamma(v)} x_e\right)^{p-1}\right] \neq 0$ when $x = s$ in $\mathbb{F}_p$

$\Rightarrow \left(\sum x_e\right)^{p-1} \neq 1 \pmod p$ $\Rightarrow$ $\sum_{e \in \Gamma(v)} x_e = 0 \pmod p$ $\leftarrow$ each degree is a multiple of p

$\sum_{e \in \Gamma(v)} x_e$ = degree(v) in subgraph of G defined by edges w. $x_e \neq 0$.

Theorem [Alon–Friedland–Kalai 1984]

If p is prime, then every loopless multigraph G of average degree $> 2p-2$, and max degree $\leq 2p-1$ contains p-regular subgraph.

Proof Let G have n vertices and m edges. Let $\Gamma(v)$ = set of edges incident to v

We want a polyn. f s.t. $f(x) \neq 0$ means $x \longleftrightarrow$ p-regular subgraph.

x_e, $e \in E(G)$ be 0-1 variables (indicating whether or not to pick e).

$$f(x) = \prod_{v \in V(G)} \Big[1 - \big(\sum_{e \in \Gamma(v)} x_e\big)^{p-1}\Big] - \prod_{e \in E(G)} (1 - x_e)$$

By CN, we found $s \neq (0,..,0)$ in $\{0,1\}^m$ s.t. $f(s) \neq 0$

and $f(x) = \prod_v \Big[1 - \big(\sum_{e \in \Gamma(v)} x_e\big)^{p-1}\Big] \neq 0$ when $x = s$ in $\mathbb{F}_p$

$\Rightarrow \left(\sum x_e\right)^{p-1} \neq 1 \pmod p \Rightarrow \sum_{e \in \Gamma(v)} x_e = 0 \pmod p \to (*)$

$\sum_{e \in \Gamma(v)} x_e$ = degree(v) in H subgraph of G defined by edges w. $x_e \neq 0$.

Since $s \neq \vec{0}$, H is nonempty & H is p-regular by $(*)$ and $\Delta \leq 2p-1$

Theorem [Alon–Friedland–Kalai 1984]

If p is prime, then every loopless multigraph G of average degree $> 2p-2$, and max degree $\leq 2p-1$ contains p-regular subgraph.

<u>Proof</u> Let G have n vertices and m edges. Let $\Gamma(v)$ = set of edges incident to v

we want a polyn. f s.t. $f(x) \neq 0$ means $x \longleftrightarrow$ p-regular subgraph.

x_e, $e \in E(G)$ be 0-1 variables (indicating whether or not to pick e).

FLT

$$f(x) = \prod_{v \in V(G)} \Big[1 - \Big(\underbrace{\sum_{e \in \Gamma(v)} x_e}_{\text{degree of } v} \Big)^{p-1} \Big] - \prod_{e \in E(G)} (1 - x_e)$$

ensure non-empty subgraph & easier application of CN

By CN, we found $s \neq (0, \ldots, 0)$ in $\{0,1\}^m$ s.t. $f(s) \neq 0$

and $f(x) = \prod_v \Big[1 - \Big(\sum_{e \in \Gamma(v)} x_e \Big)^{p-1} \Big] \neq 0$ when $x = s$ in $\mathbb{F}_p$

$\Rightarrow \left(\sum x_e\right)^{p-1} \neq 1 \pmod p$ $\Rightarrow$ $\sum_{e \in \Gamma(v)} x_e = 0 \pmod p$ $\longrightarrow \circledast$

$\sum_{e \in \Gamma(v)} x_e = \text{degree}(v)$ in H subgraph of G defined by edges w. $x_e \neq 0$.

Since $s \neq \vec{0}$, H is nonempty & H is p-regular by $\circledast$ and $\Delta \leq 2p-1$