# CSS.414.1: Polynomial Methods in Combinatorics

*Instructor: Mrinal Kumar*

*TIFR 2024, Aug-Dec*

Scribe: Soham Chatterjee

sohamchatterjee999@gmail.com
Website: sohamch08.github.io

2024

# Contents


Section 1 Introduction and Targets Page 3

Section 2 Joints Problem Page 4

Section 3 Combinatorial Nullstellensatz Page 4
3.1 Chevally-Warning Theorem 4

Section 4 Sum Sets Page 4
4.1 Sum Sets over Finite Fields 4
4.1.1 Cauchy-Davenport Theorem 4
4.2 Restricted Sum Sets 4
4.2.1 Erdös-Heilbronn Conjecture 4

Section 5 Arithmetic Progression Free Sets in $\mathbb{F}_3^n$ Page 4
5.1 3AP Free sets in $\mathbb{F}_q$ 4

Section 6 3-Tensors and Slice Rank Page 4
6.1 Rank 4
6.2 Generalization to 3-Dimension 4
6.3 Slice Rank of Diagonal 3D Tensor 4

Section 7 Kakeya and Nikodym Problem Page 4
7.1 Lower Bound on Nikodym Sets 4
7.2 Lower Bound on Kakeya Sets 4
7.2.1 Hasse Derivative 4

Section 8 Razborov Smolensky Lower Bound Page 4
8.1 Two Parts of Proving Lower Bound 5
8.2 Approximating Boolean Function with Polynomials 5
8.3 Degree-Error Trade of to Approximate Majority 8

# 1 Introduction and Targets

The content of this course will be the followings:

- Polynomial Methods in Combinatorics/Geometry
  1. Kakeya/Nikodym Problem over finite fields
  2. Joints Problem
  3. Combinatorial Nullstellensatz (CN)
  4. CN proof of Cauchy-Devenport, Erdös-Heilbronn Conjecture
- Polynomial Methods in Algebraic Algorithms
  1. Noisy Polynomial Interpolation (Sudan, Guruswami-Sudan)
  2. Multiplicative noise (Von zur Gathen-Shparlinski)
  3. Coppersmith's Problem (Given an univariate $f(x)\mathbb{Z}[x]$, compute all 'small' integer roots modulo a composite)
- Polynomial Methods in Circuit Complexity
  1. Razborov-Smolensky (Lower Bound for constant depth AND, OR, NOT, $\bmod p$ gates)
  2. Algorithmic consequences (all pairs shortest paths)
  3. Upper bounds on matrix rigidity (Alman-Williams '2015, Dvir-Edelman '2017)
- Polynomial in Property Testing: Polischuk-Speilman Lemma/Variants
- Weil Bounds (Stepanov, Schmidtm Bombieri)
- Rational Approximations of Algebraic Numbers (Thue[1907] - Siegel - Roth[1954])

# 2 Joints Problem

# 3 Combinatorial Nullstellensatz

## 3.1 Chevally-Warning Theorem

# 4 Sum Sets

## 4.1 Sum Sets over Finite Fields

### 4.1.1 Cauchy-Davenport Theorem

## 4.2 Restricted Sum Sets

### 4.2.1 Erdös-Heilbronn Conjecture

# 5 Arithmetic Progression Free Sets in $\mathbb{F}_3^n$

## 5.1 3AP Free sets in $\mathbb{F}_q$

# 6 3-Tensors and Slice Rank

## 6.1 Rank

## 6.2 Generalization to 3-Dimension

## 6.3 Slice Rank of Diagonal 3D Tensor

# 7 Kakeya and Nikodym Problem

**Definition 7.0.1: Kakeya Sets**

In a finite field $\mathbb{F}_q$, $K \subseteq \mathbb{F}^n$ is a Kakeya Set if $\forall\, a \in \mathbb{F}^n$, $\exists\, b \in \mathbb{F}^n$ such that

$$L_{a,b} = \{b + at : t \in \mathbb{F}_q\} \subseteq K$$

i.e. informally it has a line in every direction

Now notice that we can take the whole $\mathbb{F}_q^n$ as the Kakeya Set. We can also remove a point from $\mathbb{F}_q^n$ and it will still be a Kakeya Set. Having defined the Kakeya sets the biggest question which is studied is:

**Question 7.1**

How small can a Kakeya Set be?

## 7.1 Lower Bound on Nikodym Sets

## 7.2 Lower Bound on Kakeya Sets

### 7.2.1 Hasse Derivative

# 8 Razborov Smolensky Lower Bound

The result we will discuss the result that majority is strictly harder than the parity for $AC^0$, since there is no polynomial-size $AC^0$ circuit to compute majority even if we are given parity gates. The result is Razborov's, and the proof technique uses ideas due to both Razborov and Smolensky.

Consider the class $AC^0$ of polynomial size circuits with constant depth with unbounded fan-in. We consider the class $AC^0(\oplus)$ where we are give the parity gates $\oplus$ which outputs 1 if an odd number of its inputs are 1. The main theorem which we will prove in this section is:

**Theorem 8.1** Razborov-Smolensky

For any $d \in \mathbb{N}$ any any depth $d$ $AC^0(\oplus)$ circuit for MAJORITY has size $\geq 2^{\Omega\left(n^{\frac{1}{2d}}\right)}$

## 8.1 Two Parts of Proving Lower Bound

The proof of the above theorem requires two lemmas:

**Lemma 8.1.1**

$\forall\, \epsilon > 0$ and $d \in \mathbb{N}$ the following is true:

If $f : \{0,1\}^n \to \{0,1\}$ can be computed by a size $s$ depth $d$ $AC^0(\oplus)$ circuit then $\exists$ a polynomial $g$ in $n$ variables and $\deg O\left(\log \frac{s}{\epsilon}\right)^d$ such that

$$\mathop{\mathbb{P}}_{a\in\{0,1\}^n}[f(a) = g(a)] \geq 1-\epsilon$$

**Lemma 8.1.2**

For all polynomials $p(x_1, \ldots, x_n)$ with $\deg p = t$,

$$\mathop{\mathbb{P}}_{a\in\{0,1\}^n}[g(a) = \textsc{Maj}(a)] \leq \frac{1}{2} + O\left(\frac{t}{\sqrt{n}}\right)$$

Now first we will show that with these two lemmas we can prove Razborov-Smolensky Lower Bound for MAJORITY function.

**Proof of Theorem 8.1:** Suppose MAJ has a $AC^0(\oplus)$ circuit of size $< 2^{n^{\frac{1}{2d}-\delta}}$

$\xRightarrow{\text{Lemma 8.1.1}}$ $\exists$ polynomial $g$ of degree $n^{\frac{1}{2d}-\delta}$ that approximates MAJ with error 0.1.

$\xRightarrow{\text{Lemma 8.1.2}}$ $\forall$ polynomial $g$ of deg $n^{\frac{1}{2d}-\delta}$ the error is $\geq 1 - \left[\frac{1}{2} + O\left(\frac{n^{\frac{1}{2d}-\delta}}{\sqrt{n}}\right)\right] \geq \frac{1}{2} - -\left[\frac{1}{2} + O\left(\frac{n^{\frac{1}{2d}-\delta}}{\sqrt{n}}\right)\right] \geq \frac{1}{2} - o(1)$

But $\frac{1}{2} - o(1) < 0.1$ is contradiction. ■

**Alternate Proof Theorem 8.1:** Suppose $C$ be an $AC^0(\oplus)$ circuit of size $s$ and depth $d$ computing MAJORITY

$\xRightarrow{\text{Lemma 8.1.1}}$ $\exists$ polynomial $g$ of degree $O\left(\log \frac{s}{\epsilon}\right)^d$ with error probability $\leq \epsilon$.

$\xRightarrow{\text{Lemma 8.1.2}}$ $\forall$ polynomial $g$ of deg $O\left(\log \frac{s}{\epsilon}\right)^d$ the error is $\geq \frac{1}{2} + O\left(\frac{\left(\log \frac{s}{\epsilon}\right)^d}{\sqrt{n}}\right)$.

Hence from these two results and setting $\epsilon = 0.1$ we have

$$\frac{1}{2} + O\left(\frac{\left(\log \frac{s}{\epsilon}\right)^d}{\sqrt{n}}\right) \geq 1-\epsilon \implies (\log 10s)^d \geq \sqrt{n} \implies s \geq 2^{\Omega\left(\frac{1}{2d}\right)}$$

■

Now that we proved our main objective theorem we will focus on proving the 2 lemmas in the following two sections.

## 8.2 Approximating Boolean Function with Polynomials

We first state and prove a lemma showing that every $AC^0(\oplus)$ circuit can be approximated by a low degree polynomial i.e. Lemma 8.1.1. But to prove that we will show a more stronger lemma and then the lemma follows as a simple corollary of this stronger result.

**Lemma 8.2.1**

For all $\mathrm{AC}^0(\oplus)$ circuits $C$ of size $s$ of depth $d$ and $\forall\, \epsilon > 0$ there exists a distribution $\mathscr{D}$ of polynomials $p(x_1, \ldots, x_n) \in \mathbb{F}_2[x_1, \ldots, x_n]$ such that for all $a \in \{0,1\}^n$

$$\mathop{\mathbb{P}}_{p \in \mathscr{D}}[p(a) = C(a)] \geq 1 - \epsilon$$

where $\mathscr{D}$ is supported on polynomials of degree $\leq \left(\log \frac{s}{\epsilon}\right)^d$

First we will show that this lemma implies Lemma 8.1.1.

**Proof of Lemma 8.1.1:** Consider the $|\{0,1\}^n| \times |\operatorname{supp} \mathscr{D}|$ table for each $a \in \{0,1\}^n$, $a$ represents a row in the table. In the table at $(a,i)^{th}$ entry put 1 if $i^{th}$ polynomial $p$ in $\mathscr{D}$ satisfies $p(a) = C(a)$. For rest of the positions put 0.

$\xRightarrow{\text{Lemma 8.2.1}}$ $\forall\, \epsilon > 0$ there exists a distribution $\mathscr{D}$ such that for all $a \in \{0,1\}^n$ such that $\mathop{\mathbb{P}}_{p \in (\mathscr{D})}[p(a) = C(a)] \geq 1 - \epsilon$. Hence in the table for each $a \in \{0,1\}^n$, at least $1 - \epsilon$ many fraction of $|\operatorname{supp}(\mathscr{D})|$ entries in $a^{th}$ row have 1. Therefore there are total at least $(1-\epsilon) \cdot |\{0,1\}^n| \cdot |\operatorname{supp}(\mathscr{D})|$ many 1's in total in the table.

Hence by pigeon hole principle there is at least one column which has at least $(1-\epsilon) \cdot |\{0,1\}^n|$ many 1's. Therefore there is a polynomial $p \in \operatorname{supp}(\mathscr{D})$ which agrees with $C$ in at least $1 - \epsilon$ fraction of total inputs. Hence

$$\mathop{\mathbb{P}}_{a \in \{0,1\}^n}[p(a) = C(a)] \geq 1 - \epsilon$$

■

Now we will prove the Lemma 8.2.1. Now before diving into the proof first let's see how can we approximate the gates in $\mathrm{AC}^0(\oplus)$ circuits with low-degree polynomials. That way we can approximate any $\mathrm{AC}^0(\oplus)$ circuit with low-degree polynomial.

So to for a $\neg x_i$ gate we can have the polynomial $1 - x_i$. For a $\bigoplus_{i=1}^{k} x_i$ we can use the polynomial $\sum_{i=1}^{k} x_i$. So only $\wedge$ and $\vee$ gates are remaining. Now notice if we have a low degree polynomial for $\wedge$ we also have a low degree polynomial for $\vee$ since

$$\bigvee_{i=1}^{n} x_i = \neg\left(\bigwedge_{i=1}^{n} (\neg x_i)\right)$$

So we will try to find a polynomial approximating an $\wedge$ gate of degree $\leq \left(\log \frac{1}{\epsilon}\right)^d$. We can't approximate $\wedge$ by outputting 0 every time since the desired correctness probability must hold for all inputs $x$. Multiplying a random constant-size subset of the bits will not work either, for the same reason.

Naive way to have a polynomial for $\bigvee_{i=1}^{n} x_i$ would be $1 - \prod_{i=1}^{n}(1 - x_i)$. But with this the degree becomes very large.

**Idea.** *Check parity of random subset of* $[n]$. *So we take a random subset* $S \subseteq [n]$ *then we take the polynomial* $p_S = \sum_{i \in S} x_i$.

**Lemma 8.2.2**

If $S$ is a random subset of $[n]$ then

$$\mathop{\mathbb{P}}_{S \subseteq [n]}\left[p_S(x_1, \ldots, x_n) = \bigvee_{i=1}^{n} x_i\right] \geq \frac{1}{2}$$

***Proof:*** If $\overline{x} = (0, \ldots, 0)$ then we have $p_S(x_1, \ldots, x_n) = \bigvee_{i=1}^{n} x_i$. Suppose $\overline{x} \neq (0, \ldots, 0)$. Then only way $p_S(x_1, \ldots, x_n) \neq \bigvee_{i=1}^{n}$ is when $S$ has an even number of 1 bits. So let $T \subseteq [n]$ such that $i \in T \iff x_i = 1$. Then $p_S(\overline{x}) = 0 \iff |S \cap T| \equiv 0 \bmod 2$. Now $|S \cap T| \bmod 2$ can be either 1 or 0. Since $S$ is picked uniform at random the probability therefore the probability that $|S \cap T| \bmod 2 = 0$ is $\frac{1}{2}$. Therefore $\mathop{\mathbb{P}}_{S \subseteq [n], S \neq \emptyset}\left[p_S(x_1, \ldots, x_n) \neq \bigvee_{i=1}^{n} x_i\right] \leq \frac{1}{2}$. Hence we have $\mathop{\mathbb{P}}_{S \subseteq [n]}\left[p_S(x_1, \ldots, x_n) \neq \bigvee_{i=1}^{n} x_i\right] \geq \frac{1}{2}$ ■

Hence we if we pick a subset $S \subseteq [n]$ uniformly at random then with probability $\geq \frac{1}{2}$ we can approximate an $\vee$ gate or an $\wedge$ gate with a polynomial of degree 1. To have error $\frac{1}{2^k}$ we can chose $k$ subsets of $[n]$ uniformly at random $S_1, \dots, S_k$. Then construct the polynomial

$$p_{S_1,\dots,S_k}(x_1, \dots, x_n) = 1 - \prod_{i=1}^{k}\left(1 - p_{S_i}\right) = 1 - \prod_{i=1}^{k}\left(1 - \sum_{j\in S_i} x_j\right)$$

This has error probability $\frac{1}{2^k}$. So we can approximate $\vee$ gate or $\wedge$ gate with $\frac{1}{2^k}$ error probability with a degree $k$ polynomial.

**Proof of Lemma 8.2.1:** So like the above discussion we replace each gate with polynomials starting with leaf and then we proceed to the top:

- For $\neg x_i$ gate replace by $1 - x_i$
- For $\bigoplus_{i=1}^{n} x_i$ gate replace by $\sum_{i=1}^{n} x_i$
- For $\bigvee_{i=1}^{n} x_i$ gate uniformly pick $k$ subsets $S_1, \dots, S_k$ of $[n]$ then construct the polynomial

  $$p_{\vee}(x_1, \dots, x_n) = 1 - \prod_{i=1}^{k}\left(1 - \sum_{j\in S_i} x_j\right)$$

  then the error probability becomes $\frac{1}{2^k}$ by Lemma 8.2.2. For $\bigwedge_{i=1}^{n} x_i$ use the formula $\bigwedge_{i=1}^{n} x_i = \neg\left(\bigvee_{i=1}^{n}(\neg x_i)\right)$ use the process for $\vee$ gates. So

  $$p_{\wedge}(x_1, \dots, x_n) = \prod_{i=1}^{n}\left(1 - \sum_{j\in S_i}(1 - x_j)\right)$$

  Here will choose $k$ later so that we have the necessary total error.

The total polynomial for the circuit is constructed by composing of polynomials with each gate's $S_j$ for $j \in [k]$ sampled from the input wires.

Now degree increases by a factor of $k$ for each $\wedge$ gate or $\vee$ gate. Since the circuit has depth $d$, there can be $\vee$ gates or $\wedge$ gates in at most all depths. Hence degree of the final polynomial becomes $O(k^d)$.

For the error let $\epsilon_l$ denote the errors for each gate at depth $l$. Then for each gate $g$ at depth $l - 1$ we have error for $g$ is $\leq \frac{1}{2^k} + |fanin(g)|\epsilon_l$.

***Claim:*** $\epsilon_d \leq \frac{s}{2^k}$
***Proof:*** We will prove this by induction. For base case $d = 1$ this is trivial. Let this is true for $d - 1$. For $d$ consider all the children of the root gate $v$. Then

$$\epsilon_d \leq \frac{1}{2^k} + \sum_{u\in \mathrm{Child}(v)} \frac{|C_u|}{2^k} = \frac{1 + \sum_{u\in \mathrm{Child}(v)} |C_u|}{2^k} = \frac{|C_v|}{2^k}$$

Hence by mathematical induction we have $\epsilon_d \leq \frac{s}{d}$ ■

Hence the total error is $\frac{s}{2^k}$. We want the error to be at most $\epsilon$. Therefore

$$\frac{s}{2^k} \leq \epsilon \implies k = \log\frac{s}{\epsilon}$$

Hence the degree of the final polynomial approximating the circuit is $\left(\log\frac{s}{\epsilon}\right)^d$. Therefore the support of $\mathscr{D}$ has the polynomials of degree $\leq \left(\log\frac{s}{\epsilon}\right)^d$ ■

## 8.3 Degree-Error Trade of to Approximate Majority

Now we will prove the Lemma 8.1.2. But before that we first make some observations.

**Note:-**

The polynomial which approximates Majority can be made multilinear without changing its evaluation in $\{0,1\}^n$ just by replacing $x_i^k$ by $x_i$ for each variable and for each power.

Now we will show that if Maj has an approximating polynomial of low-degree then every $n-$variable boolean function $f:\{0,1\}^n \to \{0,1\}$ has an approximating polynomial of low degree.

**Theorem 8.3.1** Versatility of Majority

$\forall\, f:\{0,1\}^n \to \{0,1\}$, $\exists\, g,h \in \mathbb{F}_2[x_1,\dots,x_n]$ such that

$$\forall\, x, f(x) = g(x)\cdot \textsc{Maj}(x) + h(x), \text{ where } \deg g, \deg h \le \frac{n}{2}$$

Before proving this theorem first let's see what results we get from this theorem.

**Lemma 8.3.2**

Let $f \in \mathbb{F}_2[x_1,\dots,x_n]$ such that for all $x \in \{0,1\}^n$, $f(x) = \textsc{Maj}(x)$. Then $\deg f \ge \frac{n}{2}$.

***Proof:*** Suppose $\exists\, p \in \mathbb{F}_2[x_1,\dots,x_n]$ such that $\deg p < \frac{n}{2}$ and for all $x \in \{0,1\}^n$ we have $p(x) = \textsc{Maj}(x)$.

$\xRightarrow{\text{Lemma 8.3.1}} \forall\, f:\{0,1\}^n \to \{0,1\}$ such that $f(x) = g(x)\cdot\textsc{Maj}(x) + g(x)$ for all $x \in \{0,1\}^n$. Then the polynomial $f(x) = g(x)\cdot p(x) + h(x)$ for all $x \in \{0,1\}^n$. Then $\deg f \le n-1$. Hence all boolean function of $n-$variables can be computed by a polynomial of degree $\le n-1$.

But number of boolean functions over $n-$variables are $2^{2^n}$. Number of polynomials of $n-$variables of degree $< n$ is $\le 2^{2^n}-1$. Hence there exists a boolean function which can not be computed by polynomial of degree $< n$. Contradiction. ■

Therefore $\deg(\textsc{Maj}) \ge \frac{n}{2}$. Now we will prove Lemma 8.1.2 using the above theorem.

**Proof of Lemma 8.1.2:** Let $p \in \mathbb{F}_2[x_1,\dots,x_n]$ be a polynomial of degree $t$. Let $S \subseteq \{0,1\}^n$ be the set of inputs where $p$ and Maj agree.

$\xRightarrow{\text{Lemma 8.3.1}} \forall\, f:\{0,1\}^n \to \{0,1\}$ there exists $g,h \in \mathbb{F}_2[x_1,\dots,x_n]$ with $\deg g, \deg g \le \frac{n}{2}$ such that $\forall\, z \in \{0,1\}^n$

$$f(a) = g(a)\textsc{Maj}(a) + h(a)$$

Hence every function $f|_S : S \to \{0,1\}^n$ can be computed by the polynomial $g(x)\cdot p(x) + h(x) \in \mathbb{F}_2[x_1,\dots,x_n]$ which has degree $\le \frac{n}{2}+t$.

Let $\mathcal{F}$ be the vector space of all functions $f|_S : S \to \{0,1\}$ for all $f:\{0,1\}^n \to \{0,1\}$ and let $\mathcal{P}$ be the vector space of all polynomials in $\mathbb{F}_2[x_1,\dots,x_n]$ of degree at most $\frac{n}{2}+t$. By the above argument we get that $\forall f|_S \in \mathcal{F}, \exists\, p_f \in \mathcal{P}$ such that $f|_S$ is computed by $\mathcal{P}$. Hence $\dim\mathcal{F} \le \dim\mathcal{P}$. Now

$$\dim\mathcal{P} = \sum_{i=0}^{\frac{n}{2}+t}\binom{n}{i} = \sum_{i=0}^{\frac{n}{2}}\binom{n}{i} + \sum_{i=\frac{n}{2}+1}^{\frac{n}{2}+t}\binom{n}{i} = \frac{1}{2}\,2^n + \sum_{i=\frac{n}{2}+1}^{\frac{n}{2}+t}\binom{n}{i} \le 2^{n-1} + t\frac{2^n}{\sqrt{n}} = 2^n\left(\frac{1}{2}+\frac{t}{\sqrt{n}}\right)$$

Now $\dim\mathcal{F} = |S|$. Hence

$$|S| \le 2^n\left(\frac{1}{2}+\frac{t}{\sqrt{n}}\right) \implies \frac{|S|}{2^n} \le \frac{1}{2}+\frac{t}{\sqrt{n}}$$

Therefore for any polynomial $p \in \mathbb{F}_2[x_1,\dots,x_n]$ with degree $t$ we have $\underset{a\in\{0,1\}^n}{\mathbb{P}}[p(a) = \textsc{Maj}(a)] \le \frac{1}{2} + O\left(\frac{t}{\sqrt{n}}\right)$. ■

**Observation.** *Now let for any $f : \{0,1\}^n \longrightarrow \{0,1\}$, $S_0 = \textsc{Maj}^{-1}(0)$ and $S_1 = \textsc{Maj}^{-1}(1)$. Suppose we can compute the polynomials $u, v \in \mathbb{F}_2[x_1, \dots, x_n]$ with $\deg u, \deg v \leq \frac{n}{2}$ such that $u$,$f$ agree on $S_0$ and $v$, $f$ agree on $S_1$ i.e. $f|_{S_0}$ can be computed by $u$ and $f|_{S_1}$ can be computed by $v$. Then $\forall\ x \in \{0,1\}^n$ we have*

$$f(x) = u(x)(1 - \textsc{Maj}(x)) + v(x)\textsc{Maj}(x)$$

Hence by the observation we can conclude that computing the polynomial for $f$ on $S_0$ or $S_1$ is enough. Now we will prove the Versatility of Majority Theorem.

**Proof of Theorem 8.3.1:** So again assume $S_0 = \textsc{Maj}^{-1}(0)$ and $S_1 = \textsc{Maj}^{-1}(1)$. We want to show that these are interpolating sets for polynomials of degree $\leq \frac{n}{2}$ i.e. $\deg f|_{S_0}, \deg f|_{S_1} \leq \frac{n}{2}$. ■