# Announcements

- Presentations on April 17 : Upload video by April 12
  Presentations on April 24 : Upload video by April 19

  Videos: 20 mins
  Class Presentation: 10 mins plus 5-10 mins discussion

- 1-on-1 office hours to discuss your presentation: Today 5-7 pm and next Thurs 5-7 pm

- HW2 posted

- Scribe Notes: 1st draft due one week after lecture

Today:

Upper Bounds for Random + semi-Random CNFs

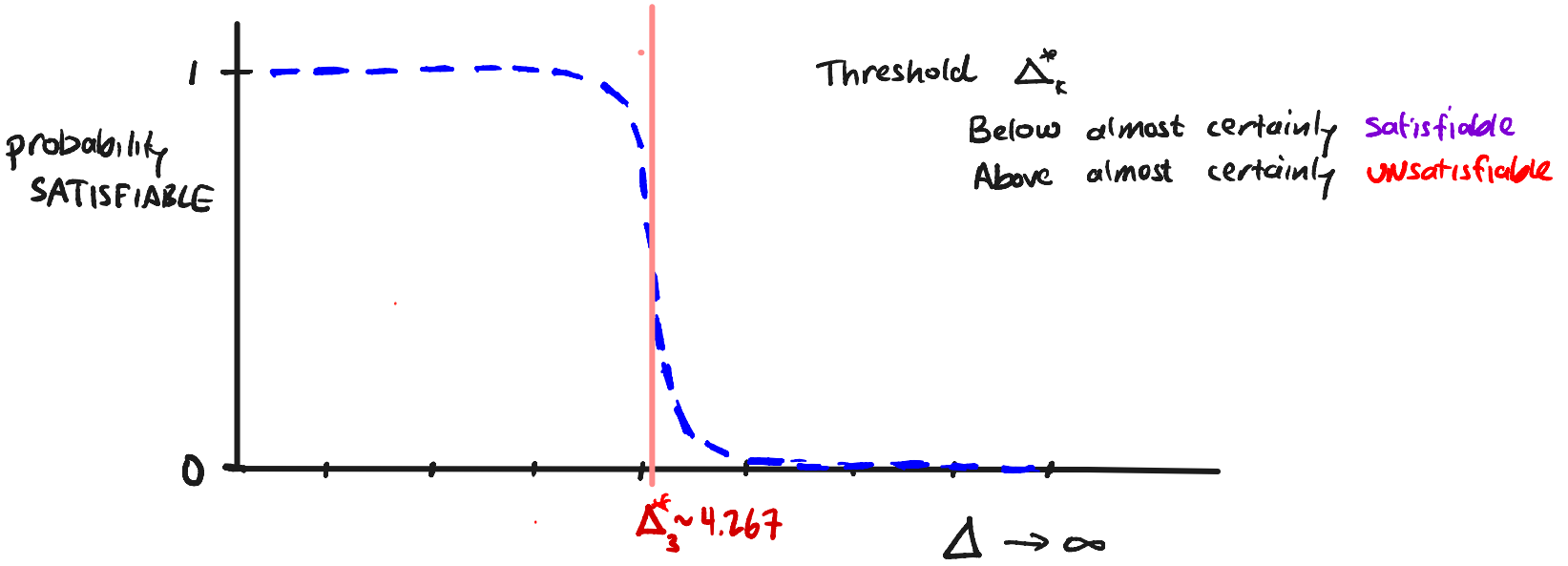
Applications: Lower Bounds for LDC's, LCC's

Other Nontrivial Upper Bounds and Open Q's

# RANDOM K-CNFs

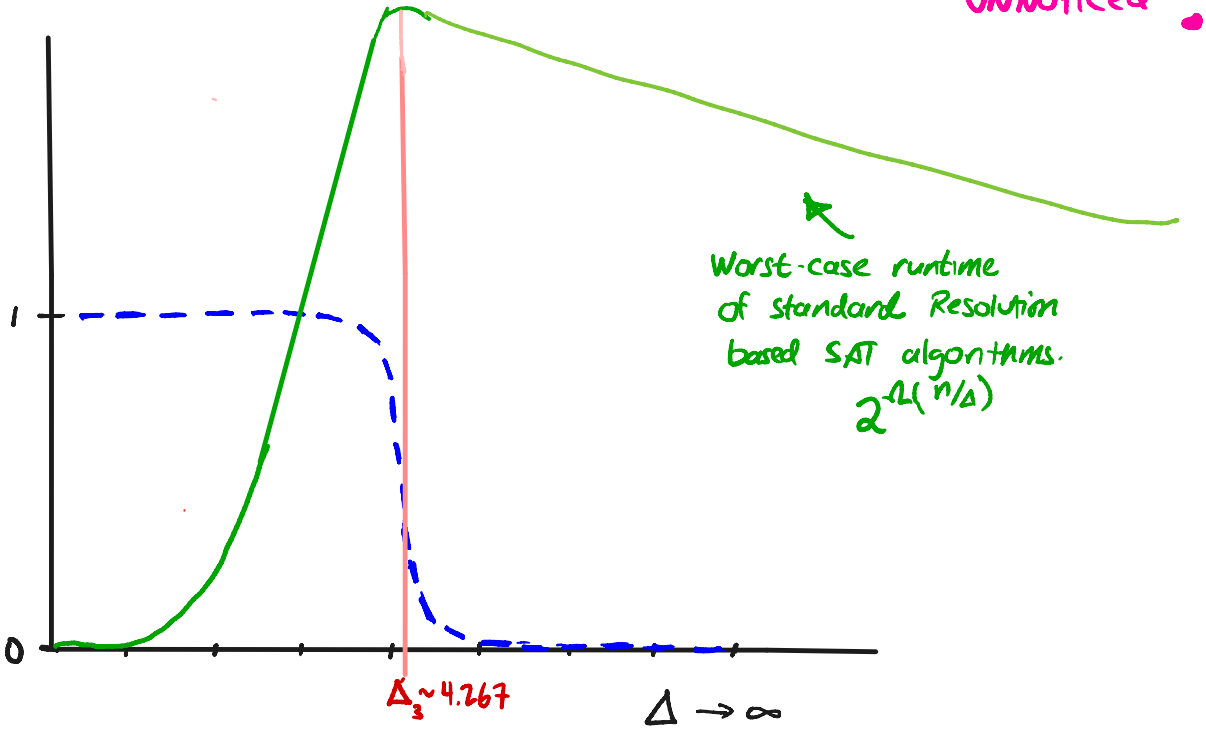
$f \sim \mathcal{F}(\Delta, n, k)$: pick $m = \Delta n$ clauses of width $k$

for $\Delta > 0$ suff large $f \sim \mathcal{F}(\Delta, n, k)$ UNSAT w.h.p.



# Resolution-Based Algorithms for random KCNF

passing transition point $\Delta_k^*$ goes absolutely unnoticed !



# MOTIVATION

1. Structural properties relate to our understanding

2. Natural distributions as benchmark for SAT algorithms

3. Lower bounds for particular proof systems (RES, SOS) give unconditional inapproximability for large family of algorithms

# WHY IS IT SO HARD TO CERTIFY UNSAT OF RANDOM f?

Counting argument doesn't seem to work:

Circuit complexity:

$2^{poly(n)}$ circuits of poly size $\ll$ $2^{2^n}$ Boolean functions

Proof complexity

# of proofs of size $s$ $\approx$ # UNSAT formulas

# Hypotheses of Feige, Krajicek/Razborov

**Defn** (Refutation algorithm) Algorithm $A$ is a refutation algorithm for random kSAT, $f \sim \mathcal{F}(\Delta, n, k)$ if:
- $A$ outputs YES with probability $> 1/2$
- $A$ outputs NO if $Q$ is satisfiable

**Feige's Hypothesis:** $\exists \Delta > \Delta_k^*$ such that

There is NO polytime refutation algorithm for $f \sim \mathcal{F}(\Delta, n, k)$:

**Krajicek/Razborov Hypothesis:** $\exists \Delta > \Delta_k^*$ such that

No proof system can efficiently refute $f \sim \mathcal{F}(\Delta, n, k)$:

# UPPER BOUNDS FOR RANDOM SAT

| | Poly-size UB |
|---|---|
| Resolution | $m > n^2/\log n$ [Beame, Kautz, Pi, Saks] ( $n^{k-1}/\log n$ ) |
| * $TC^0$ Frege | $m \sim n^{1.4}$ [Feige, Kim, Ofek] [Müller, Tzameret] |

← Poly sized refutations exist but NO known poly time algorithm to find refutation

# LOWER BOUNDS FOR RANDOM SAT

| | Poly-size UB | Expontial LB |
|---|---|---|
| Resolution | $m > n^2/\log n$ $k=3$ [Beame, Karp, P, Saks] | $m < n^{1.5}$ [Chvatal, Szemeredi] $k=O(1)$ [Beame, Karp, P, Saks] [Ben-Sasson, Wigderson] |
| Nullsatz | | $m = O(n)$ [Grigoriev] $k=O(1)$ |
| Poly Calculus | | $m = O(n)$ $k=O(1)$ [Buss, Grigoriev, Impagliazzo, P] |
| SOS | | $m = O(n)$ $k=O(1)$ [Gresoriev, Schoenebeck] |
| Cutting Planes | | $k = \Theta(\log n)$ $m = \text{poly}(n)$ [Fleming, Pankratov, P, Robere/Hrubes, Pudlak] |
| TC° Frege | $m \sim n^{1.4}$ [Feige, Kim, Ofek] [Müller, Tzameret] | ? |

# Random + Semi-Random 3SAT

**Random KSAT** : Pick $k$-uniform hypergraph $H$ over $\{x_1, \ldots x_n\}$ at random.

For each edge $C \in H$, randomly choose signs $b_1, \ldots b_k \in \{-1, 1\}$ of each literal.

whether variables in $C$ occurs positively or negatively

**Semi-random KSAT** :

Fix arbitrary 3-hypergraph $H$ over $\{x_1, \ldots x_n\}$, with $m$ edges.

For each edge $C \in H$ randomly choose $b_1, b_2, b_3 \in \{-1, 1\}$

hypergraph not random, only signs are random

[Feige-Kim-Ofek]:

**Theorem** whp there exists polysize Frege refutations for semirandom 3SAT instance, for $m \geq n^{1.4}$ clauses

Guruswami, Kothari, Manohar '22

# Refuting Semi-Random 3SAT

**Theorem** whp there exists polysize Frege refutations for semirandom 3SAT instance, for $m \geq n^{1.4}$ clauses

[Feige, Kim, Ofek]
[Guruswami Kothari, Manohar '22]

## Proof Plan:

I. Reduce weak refutation for semirandom 3SAT to (semi)-strong refutation for 3XOR via Feige XOR trick:

Weak vs Strong refutation of UNSAT CNF f:

weak refutation: proves $val(f) < 1$ $\quad val(f) = \max_{\alpha}$ [fraction of clauses satisfied by $\alpha$]

strong refutation: proves $val(f) < 1-\varepsilon$, $\varepsilon > \frac{1}{\sqrt{n}}$

# Refuting Semi-Random 3SAT

**Theorem** whp there exists polysize Frege refutations for semirandom 3SAT instance, for $m \geq n^{1.4}$ clauses

[Feige, Kim, Ofek]
[Guruswami Kothari, Manohar '22]

## Proof Plan:

I. Reduce weak refutation for semirandom 3SAT to (semi)-strong refutation for 3XOR via Feige XOR trick:

**Theorem 2** Strong refutations for semi-random 3XOR with $m = n^{1.4}$ (show $val(f) < 1 - \frac{1}{n^2}$ whp) implies weak refutations of semi-random 3SAT, $m = n^{1.4}$

II. **Theorem 1**: $\exists$ strong refutations of semi-random 3XOR via Moore hypergraph bound.

# Semi-strong Refutation for 3XOR

**Theorem 1**

Let $H = \{C_1, \ldots, C_m\}$ be arbitrary 3-uniform hypergraph over $[n]$

Let $\psi_H$ be semi-random 3XOR given by 3XOR constraints:

$$\psi_{H,\vec{b}} \stackrel{d}{=} \left\{ \oplus_2\{\text{vars}(C_1)\} = b_1, \ldots \oplus_2\{\text{vars}(C_m)\} = b_m \right\}$$

For $m \geq 100\, n \left(\frac{n}{\ell}\right)^{1/2}$, whp over $\vec{b} \in \{0,1\}^m$

$\text{val}(\psi_{H,\vec{b}}) \stackrel{d}{=}$ max fraction of satisfied constraints of $\psi_{H,\vec{b}} \leq 1 - O\left(\frac{1}{\ell \log n}\right)$

- To refute Ksat via strong KXOR refutations, we will set $\ell \sim n^{1/s}$

# Hypergraph Moore Bound

$k=2$ (ordinary graphs): Any graph with $\geq \frac{nd}{2}$ edges has a cycle of length $\lesssim 2\log_{d-1} n$

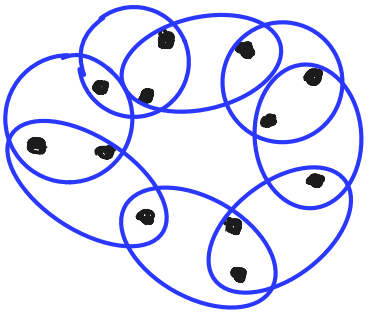
# Hypergraph Moore Bound

$k=2$ (ordinary graphs): Any graph with $\geq \frac{nd}{2}$ edges has a cycle of length $\leq 2\log_{d-1} n$ [Alon-Hoory-Linial 2002]

Generalization to $k$-uniform hypergraphs: ($k=3$ here)

A "cycle" is an even cover: set of $k$-edges $\mathcal{H}' \subseteq \mathcal{H}$ such that every vertex is contained in an even number of edges in $\mathcal{H}'$

$k=3$



# Hypergraph Moore Bound

**Feige conjecture (2008):**

$\forall \ell > 0$, Every $k$-uniform hypergraph $H$ with $m \gtrsim n\left(\frac{n}{\ell}\right)^{\left(\frac{k}{2}-1\right)}$ edges contains an even cover of length $\lesssim \ell \log_2 n$

↑

Proven up to polylog $n$ factors

Guruswami - Kothari - Manohar '21
Hsieh - Kothari - Mohanty '22
H-K-M-Correlu-Sudakov '24

(We will sketch a simple proof time-permitting)

# Semi-strong Refutation for semi-random 3XOR

**Theorem 1**

Let $H = \{C_1, \ldots, C_m\}$ be arbitrary 3-uniform hypergraph over $[n]$

Let $\Psi_H$ be semi-random 3XOR given by 3XOR constraints:

$$\Psi_{H,\vec{b}} \triangleq \{ \oplus_2\{vars(C_1)\} = b_1, \ldots \oplus_2\{vars(C_m)\} = b_m \}$$

For $m \geq 100\, n (\frac{n}{\ell})^{1/2}$, whp over $\vec{b} \in \{0,1\}^m$

$val(\Psi_{H,\vec{b}}) \triangleq$ max fraction of satisfied constraints of $\Psi_{H,\vec{b}} \leq 1 - O(\frac{1}{\ell \log n})$

Proof: $H$ satisfies conditions of even cover Theorem (Moore bound)

(1) Find $\ell \log n$ length even cover.

(2) Remove all hyperedges in cover, Let $H' = H$ - even cover
$H'$ still has $100 m_0 - \ell \log n \geq m_0$ edges

(3) Repeatedly apply even cover theorem, partitioning $.99 m_0$ hyperedges of $H$ into disjoint even covers, each of size $\leq \ell \log n$

(4) since each even cover is linearly independent, $\sim \frac{1}{2}$ of the even covers will be unsatisfiable (RHS of equations will sum to 1 mod 2)

$\therefore$ in total at least $\frac{1}{2}\left(\frac{99 m_0}{\ell \log n}\right)$ constraints must be falsified

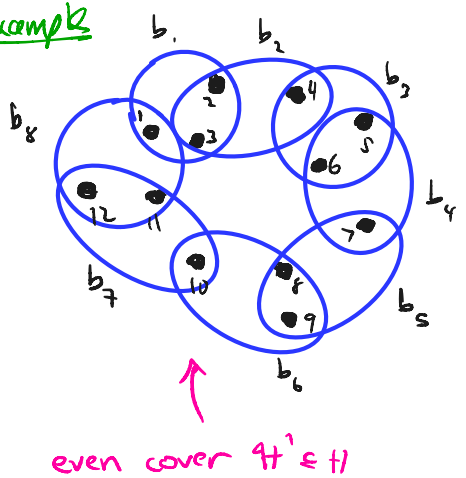
$\therefore$ whp $val(\Psi_H) \leq 1 - O(\frac{1}{\ell \log n})$ ∎

(4) since each even cover is linearly independent, $\sim \frac{1}{2}$ of the even covers will be unsatisfiable (RHS of equations will sum to 1 mod 2)

$\therefore$ in total at least $\frac{1}{2}\left(\frac{99 m_0}{\ell \log n}\right)$ constraints must be falsified

$\therefore$ whp $val(\varphi_H) \leq 1 - O\left(\frac{1}{\ell \log n}\right)$

Example




even cover $q_H^{-1} \in H$

$$
\begin{aligned}
x_1 + x_2 + x_3 &= b_1 \\
x_2 + x_3 + x_4 &= b_2 \\
x_4 + x_5 + x_6 &= b_3 \\
x_5 + x_6 + x_7 &= b_4 \\
x_7 + x_8 + x_9 &= b_5 \\
x_8 + x_9 + x_{10} &= b_6 \\
x_{10} + x_{11} + x_{12} &= b_7 \\
x_{11} + x_{12} + x_1 &= b_8
\end{aligned}
$$

UNSat iff $b_1 \oplus b_2 \oplus \ldots + b_m = 1 \mod 2$

# Proof of Hypergraph Moore Bound ($k=4$)

**Hypergraph Moore Bound:**
Every $k$-uniform hypergraph $H$ with $m \sim n\left(\frac{n}{\ell}\right)^{\left(\frac{k}{2}-1\right)}$ edges contains an even cover of length $\leq \ell \log_2 n$

Warmup: $\ell = 1$. Let's show every 4-uniform $H$ with $\geq n^2$ edges contains a $\sim \log n$ length even cover

Pf Let $G_H$ be a graph on $\binom{n}{2}$ vertices. $V = \{(i,j) \mid i<j<n\}$

edge $((i,j),(k,\ell)) \in G_H$ iff $\{i,j,k,\ell\} \in H$ and $i,j \neq k,\ell$

edges in $G_H$ in 1-1 correspondence to hyperedges in $H$

cycles in $G_H$ in 1-1 correspondence with an even cover in $H$

$\therefore$ follows by graph moore bound

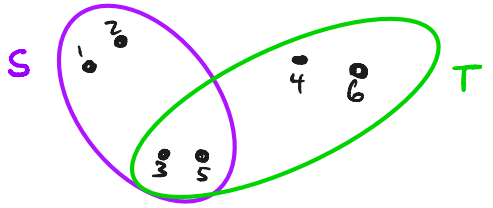
# Proof of Hypergraph Moore Bound ($k=4$)

Let $H$ be a 4-uniform hypergraph with $\geq n\left(\frac{1}{\ell}\right)^{\frac{k}{2}-1} \cdot \log n = \frac{n^2}{\ell} \log n$ edges.

Let $K_\ell(H)$ be the level-$\ell$ Kikuchi graph of $H$:

Vertices of $K_\ell(H)$: all $\binom{[n]}{\ell}$ $\ell$-subsets of $[n]$

Edges of $K_\ell(H)$: $(S,T)$ is an edge iff $S \oplus T \in H$




$(S,T) \in$ edge $(K_\ell(H))$

iff $\{1,2,4,6\} \in H$

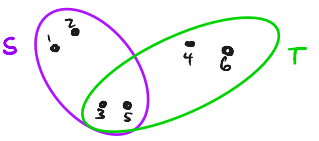
# Proof of Hypergraph Moore Bound ($k=4$)

Let $H$ be a 4-uniform hypergraph with $\geq n\left(\frac{n}{\ell}\right)^{\frac{k}{2}-1} \cdot \log n = \frac{n^2}{\ell}\log n$ edges.

Let $K_\ell(H)$ be the level-$\ell$ Kikuchi graph of $H$:

Vertices of $K_\ell(H)$ : all $\binom{[n]}{\ell}$ $\ell$-subsets of $[n]$

Edges of $K_\ell(H)$ : $(S,T)$ is an edge iff $S \oplus T \in H$



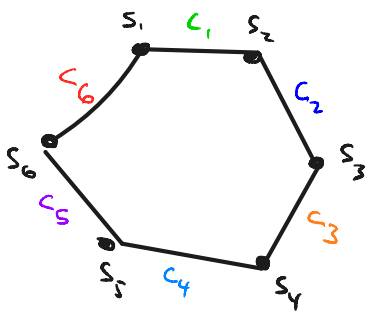

color edge $(S,T)$ in $K_\ell(H)$ by $C = S \oplus T$

**Claim**

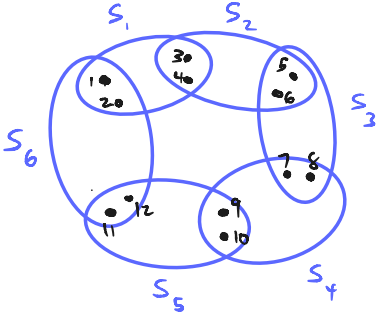
A closed walk in $K_\ell(H)$ where some color appears an odd # of times $\rightarrow$ even cover in $H$

(even cover = set of $C_i$'s that occur an odd # of times in walk)

$k=4$
$\ell=4$




closed walk in $K_\ell(H)$




$S_1 \oplus S_2 = C_1 = \{1,2,5,6\}$

$S_2 \oplus S_3 = C_2 = \{3,4,7,8\}$

$S_3 \oplus S_4 = C_3 = \{5,6,9,10\}$

$S_4 \oplus S_5 = C_4 = \{7,8,11,12\}$

$S_5 \oplus S_6 = C_5 = \{9,10,1,2\}$

$S_6 \oplus S_1 = C_6 = \{11,12,1,2\}$

even cover in $H$

# Proof of Hypergraph Moore Bound ($k=4$)

Thus it suffices to prove the following Lemma:

**MAIN LEMMA:** Let $H$ be 4-uniform hypergraph with $\geq \frac{n^2}{\ell} \log n$ edges. Let $g = K_2(H)$ be colored Kikuchi graph for $H$. Then $g$ has a closed walk of length $\leq \ell \log n$ where each color on walk occurs exactly once.

rainbow walk

**Lemma** Let $g$ have $nd$ edges. Then $g$ contains a subgraph $g' \leq g$ with minimum degree $d' \geq d/4$ and at least $nd/2$ edges.

# Proof of Hypergraph Moore Bound ($k=4$)

**MAIN LEMMA:** Let $H$ be 4-uniform hypergraph with $\geq \frac{n^2}{\ell}\log n$ edges.
Let $q = K_\ell(H)$ be colored Kikuchi graph for $H$. Then $q$ has a closed walk of length $\leq \ell \log n$ where each color on walk occurs exactly once.
(rainbow walk)

**Pf** (double count rainbow paths of length $\ell$ in $q$)

$G$ has $N = \binom{[n]}{\ell}$ vertices

Edges: each $c \in H$ contributes $\binom{4}{2}\binom{n-4}{\ell-2}$ edges to $G$.

$\therefore$ $G$ has $\geq \frac{n^2}{\ell}\binom{n}{\ell-2}\log n \geq 20N\log N$ edges, so avg degree $\sim 20\log N \sim 20\ell\log n$

Assume fsoc that $G$ contains no short closed rainbow walks.

Let $G' \subseteq G$ be subgraph guaranteed by Lemma, mindegree $d' \geq 5\log N$

Let $q = \log N \sim \ell \log n$

(i) # of length-$q$ rainbow paths in $G \geq N d' \cdot (d'-1)\cdot(d'-2)\cdot\ldots\cdot(d'-(q-1)) \geq N(.9d')^q = (1.8d')^q$

(ii) # length-$q$ rainbow paths $\leq N^2 \cdot q! \approx 4^q \cdot q^q = (4q)^q$ ← if $\exists$ a closed rainbow walk then set of colors on every rainbow walk must use same set of $q$ colors

$u \bullet \sim\sim \bullet v$

Contradiction since $4q < 1.8d'$

**Theorem 2** | Semi-strong KXOR Refutations $\longrightarrow$ Weak KSAT Refutations

**Semirandom KSAT:**

Fix arbitrary 3-hypergraph $H$ over $\{x_1 \ldots x_n\}$, with $m$ edges.

For each edge $C \in H$ randomly choose $b_1^C, b_2^C, b_3^C \in \{-1,1\}$

For each clause $(C, b_1, b_2, b_3)$ its Fourier representation over $\mathbb{F}_2$ $(x_i \in \{-1,1\})$ is:

$$P(C,b_1,b_2,b_3) \stackrel{d}{=} \frac{7}{8} + \frac{1}{8}\left(b_1x_1 + b_2x_2 + b_3x_3 + b_1b_2x_1x_2 + b_1b_3x_1x_3 + b_2b_3x_2x_3 + b_1b_2b_3x_1x_2x_3\right)$$

**Example:** $C = \{x_1, x_2, x_3\}$ $b_1 = b_2 = b_3 = -1$ so clause is $(x_1 \vee x_2 \vee x_3)$

Fourier representation $= \frac{7}{8} + \frac{1}{8}\left(-x_1 - x_2 - x_3 - x_1x_2 - x_1x_3 - x_2x_3 - x_1x_2x_3\right)$

**Defn**

Let $\psi_H = \{(C_1, b^{C_1}), (C_2, b^{C_2}), \ldots (C_m, b^{C_m})\}$ be a semirandom 3SAT

Then $val(\psi) = \frac{1}{m} \cdot \max_{x \in \{-1,1\}^n} \sum_{i=1}^{m} P(C_i, b^{C_i})$ ← $val(\psi)$ is max fraction of satisfied clauses in $\psi$

**Defn**

Let $\psi_H = \{ (C_1, b^{c_1}), (C_2, b^{c_2}), \ldots (C_m, b^{c_m}) \}$ be a semirandom 3SAT

Then $val(\psi) = \max_{x \in \{-1,1\}^n} \underbrace{\frac{1}{m} \sum_{i=1}^{m} P(C_i, b^{c_i})}_{P}$ ← $val(\psi)$ is max fraction of satisfied clauses in $\psi$

write $P$ as sum of 8 polynomials:

$P_0$ = all constant terms
$P_1$ = all linear terms
$P_2$ = all quadratic terms
$P_3$ = all degree 3 terms (3XORs)

$$val(\psi) \leq \underbrace{\max_x P_0}_{\frac{7}{8}} + \underbrace{\max_x P_1}_{\frac{1}{8} \cdot O(\sqrt{n/m}\sqrt{\log n})} + \underbrace{\max_x P_2}_{\frac{1}{8} \cdot O(\sqrt{n/m}\sqrt{\log n})} + \underbrace{\max_x P_3}_{\frac{1}{8}(1 - O(\frac{1}{\ell \log n}))}$$

we'll show:

$$val(\psi) \le \underbrace{\max_x P_0}_{\frac{7}{8}} + \underbrace{\max_x P_1}_{\frac{1}{8}\cdot O\left(\sqrt{n/m}\sqrt{\log n}\right)} + \underbrace{\max_x P_2}_{\frac{1}{8}\cdot O\left(\sqrt{n/m}\sqrt{\log n}\right)} + \underbrace{\max_x P_3}_{\frac{1}{8}\left(1-O\left(\frac{1}{\ell \log n}\right)\right)}$$

we'll show:

Assuming these upper bounds, and $m = O(n\sqrt{\frac{n}{\ell}}\log n)$

$$val(\psi) \le \frac{7}{8} + \left(\frac{\ell}{n}\right)^{1/4} + \frac{1}{8}\left(1-O\left(\frac{1}{\ell \log n}\right)\right) = 1 + \left(\frac{\ell}{n}\right)^{1/4} - O\left(\frac{1}{\ell \log n}\right)$$

this is $< 1$ if $\left(\frac{\ell}{n}\right)^{1/4} \ll \frac{1}{\ell \log n}$.

This happens if $\ell^{5/4} \ll n^{1/4}$, so setting $\ell \le n^{1/5}$ achieves this.

Choosing $\ell = n^{1/5}$ gives $m = n^{1.4}$.

So it is left to prove the claimed upper bounds.

## Degree 3 terms (3XOR2 part)

upper bound on $\mathrm{val}(P_3)$ follows by Theorem 1 !

UPPER bounds for linear part ($P_1$) and quadratic part ($P_2$) is easier.
We sketch proofs of these next.

## Linear terms

Say $x_i$ occurs in $n_i$ many clauses.
Because signs are random, the coefficient in front of $x_i$ has expectation $\sim \frac{\sqrt{n_i}}{m}$

$$\therefore P_1 = \frac{1}{m} \sum_i \sqrt{n_i}\, x_i$$

$$\therefore \max_{x \in \{-1,1\}^n} P_i \le \frac{n}{m} \frac{1}{n} \sum_i \sqrt{n_i} \le \frac{n}{m} \sqrt{\frac{1}{n} \sum_i n_i} = \frac{n}{m} \sqrt{\frac{m}{n}} = O\left(\sqrt{\frac{n}{m}}\right)$$

(Cauchy-Swartz)

## Quadratic terms

Key idea: we can write quadratic part as $\frac{1}{m} x^T \left( \sum_{c \in H} a_c A_c \right) x$

where $A_c$ = $n \times n$ matrix with 1 in $(i,j)$ iff $x_i, x_j \in C$

$a_c$ = coefficient of $x_i x_j$ in Fourier expansion of clause $(C, b^C)$

Note nonzero entries of $\sum_c a_c A_c$ are determined by $H$, but sign ($\pm 1$) is random.

$\therefore \frac{1}{m} x^T \left( \sum_c a_c A_c \right) x \leq \frac{n}{m} \left\| \sum_c a_c A_c \right\|_2$ since $\|x\|_2 = \sqrt{n}$

By Matrix Khintchine (Matrix Chernoff bound):

$$\left\| \sum_c a_c A_c \right\|_2 \leq \left( \sum_c A_c^2 \right)^{1/2} \sqrt{\log m} \leq \sqrt{\frac{m}{n}} \sqrt{\log n}$$

assuming $H$ is random. more complicated arg if $H$ not random.

$\therefore \max_x p_2 \leq \frac{n}{m} \left\| \sum_c a_c A_c \right\|_2 \leq \frac{n}{m} \sqrt{\frac{m}{n}} \sqrt{\log n} = \sqrt{\frac{n}{m}} \sqrt{\log n}$

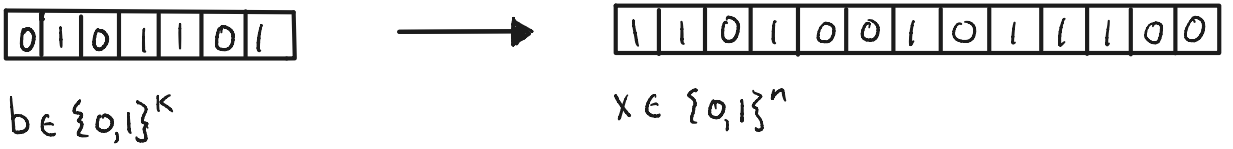
## Remarks

(1) The whole proof can be formalized in poly sized Frege pf.
The hard part (Theorem 1) actually formalized in much weaker system – poly-size PC refutation

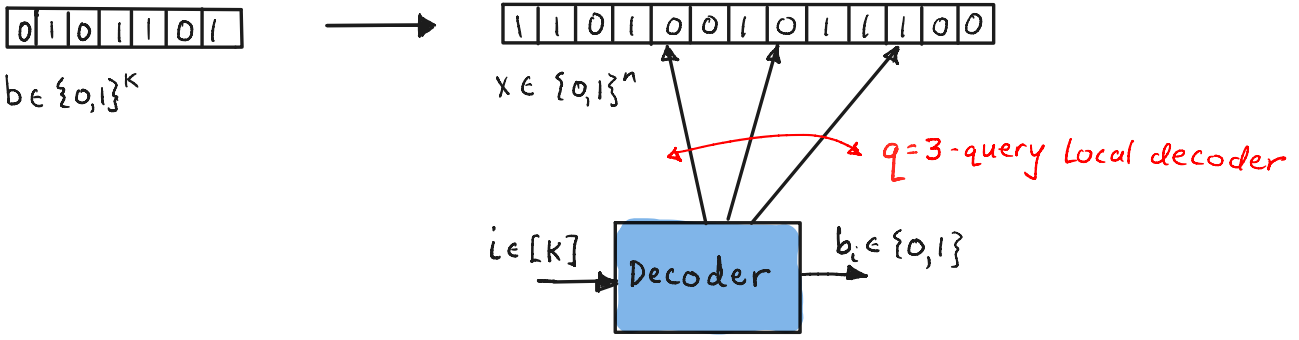
(2) No improvements to $m \geq n^{1.4}$ given in original FKO paper.

(3) Strong LBs for Resolution refutations:
for $m \leq n^{5/4 - \varepsilon}$ 3clauses, Resolution refutations require exponential size

Application: **Locally Decodable Codes**



# Locally Decodable Codes

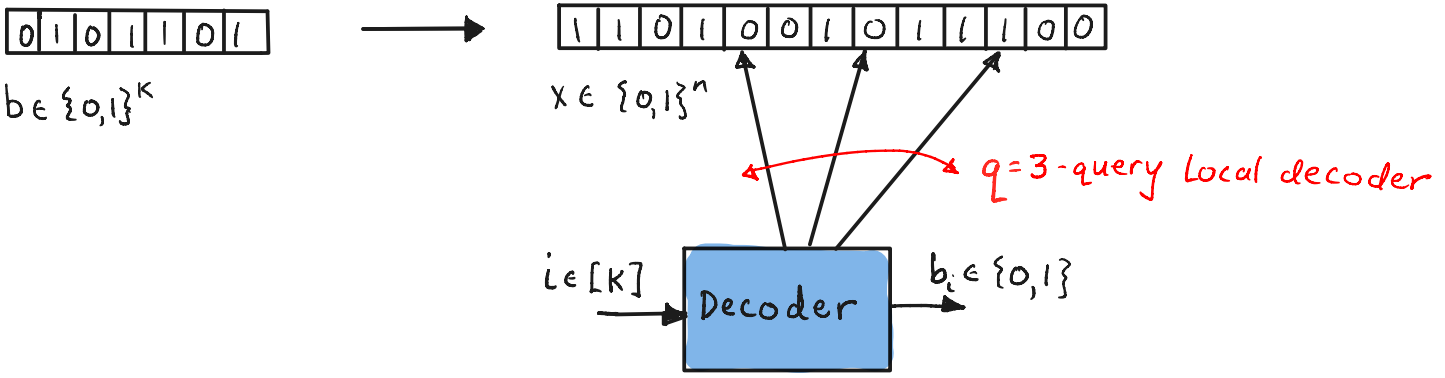



$(q, \varepsilon, \delta)$-LDC: given received word $x$ with $\leq \delta$ fraction of errors, for any position $i$, $\text{Decoder}(i, x) = x_i$ with probability $\geq 1 - \varepsilon$

Applications: PCP's, Private Information Retrieval, secret sharing, worst-to-avg case reductions, Distributed computation, ...

Open: Does there exist $q = O(1)$ LDC with $n = \text{poly}(K)$?

# Locally Decodable Codes



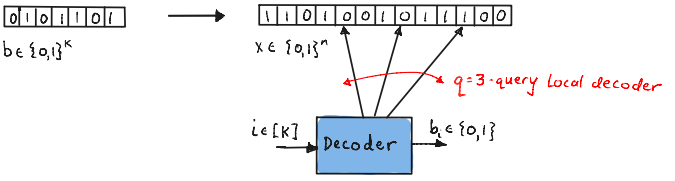

**Best construction** $K \longrightarrow 2^{K^\varepsilon}$ "Matching Vector Codes" [Yek'08, Efr09, DGY'11]

***New Lower Bounds***

$n = \Omega(K^3)$ for 3-query LDC's [AGKM23] (see references at end)

$n = 2^{\Omega(K)}$ for linear 3-query LCC's [Kothari, Manohar '23]

# SEMI-RANDOM XORs & LDC LOWER BOUNDS

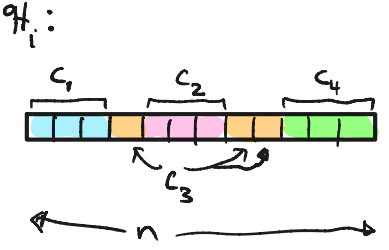



* Breakthrough Lower Bounds: formalized as system of semi-random XOR constraints: $\mathcal{F} = \{F_\beta \in \{0,1\}^K : F_\beta\}$

## Normal Form [Yek'08]

$\exists$ 3-uniform hypergraph matchings $\mathcal{H}_1, \ldots, \mathcal{H}_K$, each $\mathcal{H}_i$ over $\{1, \ldots, n\}$

Decoding: on $i \in [K]$ pick random $C \in \mathcal{H}_i$, output $\sum_{v \in C} x_v \bmod 2$




System of XORs: $\forall \beta \in \{0,1\}^K$: $F_\beta = \{\forall i \in [K], C \in \mathcal{H}_i : \sum_{v \in C} x_v = \beta_i\}$

**Lemma:** $F_\beta$ highly UNSAT for random $\beta$ $\Rightarrow$ LB $\Omega(n)$ for LDC's

Proof based on ideas in semirandom CSP refutations

# Other Nontrivial Upper Bounds

[Razborov 95] Formalized "$f \in C$" by propositional CNF

Proved standard Lower Bounds : { PARITY $\notin AC^0$ ; Clique $\notin$ monotone P/poly }

have polysize EF proofs

[Buss 06], [Alsenberg, Bonet, Buss] Proved several combinatorial properties believed to be hard for Frege have efficient Frege proofs

[Buss, Kabanets, Kolokolova, Koucky] : Proved existence of expander graphs can be proven with polysized EF proofs

[Pich] : PCP Theorem has polysize EF proofs

# References (1)


1. Buss, Kabanets, Kolokolova, Koucky
   Expander construction in $VNC^1$

2. Pich.
   Logical Strength of complexity theory and a formal. of PCP theorem in Bounded Arithmetic.
   Logical Methods in CS, 11 (2:8): 1-38, 2015

3. Razborov 95
   Bounded Arithmetic and lower Bounds in complexity Theory
   Feasible Mathematics II, 1995, 344-356

4. [Buss 06]
   Polynomial-size Frege + Resolution proofs of st-connectivity + Hex tautologies
   TCS 357, 2006

5. [Aisenberg, Bonet, Buss] Quasipolynomial size proofs of Frankl's Theorem on the trace of sets. JSL, 2016

References (2)


6. [Feige, Kim, Ofek] Witnesses for non-satisfiability of dense random 3CNF formulas 47th STOC, 2006

7. [Guruswami, Kothari, Manohar]
Algorithms & Certificates for Boolean CSP refutation;
"Smoothed is no harder than random" STOC 2022

8. [AGKM 23]: Alrabiah, Guruswami, Kothari Manohar
A near cubic lower bound for 3-query locally Decodable Codes from semirandom CSP refutation STOC 2023