Monotone Circuit Lower Bounds from Resolution.

high level plan:
(1) prove monotone circuit l.b.
(2) Argument and technical lemmas to prove on Friday

$$
\begin{tikzcd}
\text{Cutting Planes} \arrow[d] & & \text{monotone (real) circuit} \arrow[ll, "\text{monotone}"', "\text{interpolation}"] \\
\text{Resolution} \arrow[urr, "\text{lifting}"'] & &
\end{tikzcd}
$$

Thm. If a CNF formula F is hard to refute in the Resolution
[GGKS] proof system, then there is a (related) monotone
function with F that requires large monotone (real) circuits.

Search problems: $S \subseteq I \times O$; total: $\forall i \in I: \exists o: (i,o) \in S$.

Fix a CNF F.

Falsified Clause search problem: S_F:

input: an n-variable truth assignment α

output: a falsified clause C of F; $C(\alpha) = 0$.

$\rightsquigarrow$ total problem for an unsat CNF F.

$f(x) \leq f(y)$ if $\forall i \in [n]: x_i \leq y_i$.

Fix a monotone function $f: \{0,1\}^n \to \{0,1\} \rightsquigarrow$ mKW(f):

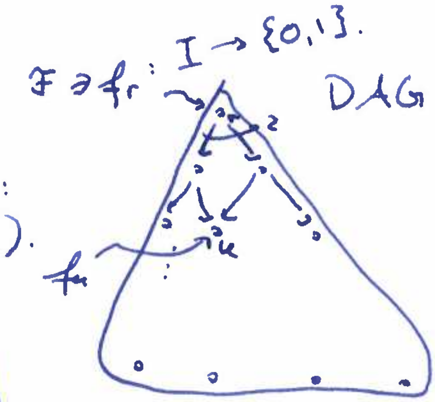
mKW: input: $\alpha \in f^{-1}(1)$; $\beta \in f^{-1}(0)$.

output: $i \in [n]$ such that $1 = \alpha_i > \beta_i = 0$.

~~mon-formula(f) = 2^{Ω(mKW)}~~

mon-d(f) = mKW(f).

Let $\mathcal{F}$ be a family of functions $I \to \{0,1\}$.
An $\mathcal{F}$-dag solves $S \subseteq I \times O$ if:



- Root: fan-in 0; $f_r \equiv 1$.

- Non-leaves: node v with children u, u':

$$f_v^{-1}(1) \subseteq f_u^{-1}(1) \cup f_{u'}^{-1}(1).$$

- Leaves: each leaf v is labelled with an output $o_v \in O$, and

$$f_v^{-1}(1) \subseteq S^{-1}(o_v)$$

"consistency"

Consider $I = X \times Y$.

$$\mathcal{F} := \{ U \times V : U \subseteq X; V \subseteq Y \}.$$

These are the rectangle-DAGs.

rect-dag(S) := least size of a rectangle-dag solving S.

Thm: ~~$mC(f) = mKW(f)$.~~
[Pud'10, Sok'17]

$$mC(f) = \text{rect-dag}(mKW(f)).$$

Let $\mathcal{F}_c$ be ~~all rectangles~~ family of functions

$$X \times Y \to \{0,1\}$$

that can be computed by (tree-like) communication protocols of cost $c = \text{poly}\log(n)$.

- Can simulate resolution; CP with bounded coeffs.

- Any $\mathcal{F}_c$-dag can be simulated by a rect-dag with a blow-up of size at most 2^c.

$\Rightarrow$ not much loss when studying rect-dags.

3

Resolution: $I = \{0,1\}^n$

$\mathcal{F} :=$ conjunctions of literals over n input vars.

resolution size $=$ conj-dag$(S) :=$ least size of any conj-dag solving S.

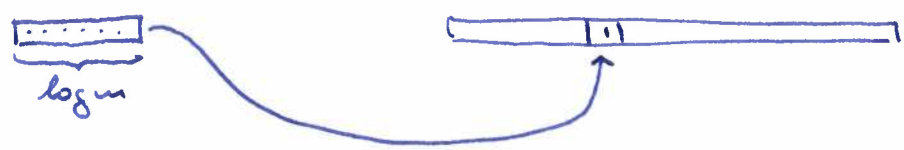
$$w(S) := \max_{\pi} \max_{C \in \pi} \text{width}(C).$$

mention xor!

For any bipartition $X \times Y = \{0,1\}^n$:

$$\text{rect-dag}(\underset{\substack{\uparrow \\ \text{over} \\ \text{bipartition}}}{S'}) \le \text{conj-dag}(S) \le n^{O(w(S))}.$$

indexing gadget $\text{IND}_m : \underbrace{[m]}_{\text{Alice}} \times \underbrace{\{0,1\}^m}_{\text{Bob}} \to \{0,1\}$



$$\text{Ind}_m(x,y) = y_x.$$

$$S \circ \text{Ind}_m^n : [m]^n \times (\{0,1\}^m)^n \times O$$

given $x \in [m]^n$ to Alice;

$y \in \{0,1\}^{m \cdot n}$ to Bob

find $(z, o) \in S$

for $z := \text{Ind}_m^n(x,y) = (\text{Ind}(x_1,y_1), \ldots, \text{Ind}(x_n,y_n))$

Thm. Let $m = n^c$ for c large enough. For any $S \subseteq \{0,1\}^n \times O$

$$\text{~~rect~~ triangle-dag}(S \circ \text{Ind}_m^n) = n^{\Theta(w(S))}$$

$\to$ Can lift large resolution width to $n^{\Omega(w(S))}$ CP-size l.b.

<u>Cor.</u> <u>3XOR-SAT</u> requires monotone circuits of size $2^{n^{\Omega(1)}}$.

$\hookrightarrow m = O(1) \Rightarrow 2^{\Omega(n)}$.

[GKRS] $\to$ in NC^2; but not computable by a small monotone circuit.

dsu $\to$ $\{0,1\}^N \to \{0,1\}$

over $\underset{N}{\underset{\shortparallel}{2n^3}}$ input bits

the input encodes a 3-XOR instance I over n variables:

each bit indicates whether a 3-XOR equation appears.

output 1 iff the encoded instance I is unsat.

$\to$ monotone function

<u>idea:</u> argue that $S_{Tseitin} \circ \mathrm{Ind}_m^n$ reduces to $mKW(3\text{XOR-SAT})$

Fix a Tseitin formula F ~~over~~ with constraints $C_1, \dots, C_t$ over variables $z_1, \dots, z_n$.

$\sum z_i \equiv_2 1$

want: reduction from

$$S_{Tseitin} \circ \mathrm{Ind}_m^n \subseteq [m]^n \times (\{0,1\}^m)^n \times [t]$$

$$\Downarrow$$

$$mKW(\underbrace{3\text{XOR-SAT}}_{f}) \subseteq f^{-1}(1) \times f^{-1}(0) \times [N]$$

$N := 2 \cdot (mn)^3$

<u>Alice:</u> $(x_1, \dots, x_n) \in [m]^n$. Define 3-XOR instance over vars

$$\{ v_{ij} : (i,j) \in [n] \times [m] \}:$$

same formula as F but over variables $v_{1x_1}, \dots, v_{nx_n}$.

$\to$ the ~~given input~~ constructed formula is a 1-input for 3XOR-SAT.

$\Updownarrow$ unsat

<u>Bob:</u> $y \in (\{0,1\}^m)^n$. Construct a 3-XOR instance over the same variables v_{ij}. Add all possible 3-XOR constraints <u>consistent</u> with y.

$\to y$ is a satisfying assignment.

$\to$ the constructed formula is a 0-input for 3XOR-SAT.

Argue that any solution to $mKW(3\text{XOR-SAT})$ gives a solution to $S_{Tseitin} \circ \mathrm{Ind}_m^n$.

Any solution is a constraint present in Alice's 3-XOR instance but not in Bob's.

$\Rightarrow C(y) = 0$; otherwise Bob would have added C.

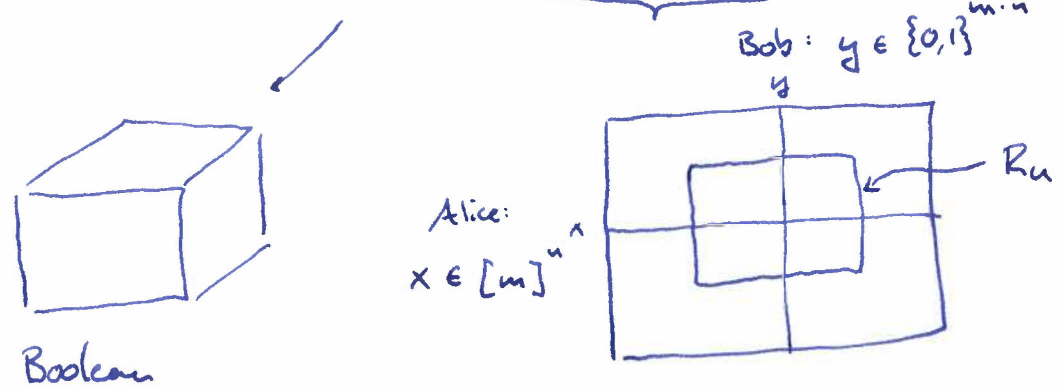
Since the constraint is over variables $v_{1x_1}, \dots, v_{nx_n}$

$\Rightarrow$ also falsified by $z = \mathrm{Ind}_m^n(x, y)$.

Want to prove: given a rectangle-dag Π solving $S \circ G$ of size $|\Pi| = n^d$, then $w(S) \le O(d)$.

$g_m^n := \mathrm{Ind}_m^n$

$S \qquad \{0,1\}^n \longleftarrow \underbrace{(\{0,1\}^m)^n \times [m]^n}_{} = \mathrm{Ind}_m \qquad S \circ G$



Boolean hypercube.

low-width refutation. $\rightsquigarrow$ small Π

$\Rightarrow$ want to relate a rectangle with large sub-cubes.
co-dim $\le O(d)$.

---

idea: maintain a subrectangle $R' \subseteq R_u$ which is "structured"

- "structured" $\longrightarrow$ corresponds to a sub-cube of co-dim $\le O(d)$.
- need to be able to find another such structured rectangle in ~~one~~ the corresponding child.

---

what is this invariance that we want to maintain?

Structured Rectangles.

partial assignment to $z = \mathrm{Ind}^n(x,y)$

$R \subseteq [m]^n \times (\{0,1\}^m)^n$ is ρ-like if the image of R under $G := \mathrm{Ind}^n$ is the subcube of n-bit assignments consistent with ρ;

at least one (x,y)-tuple for every consistent.

$$R \text{ is } \rho\text{-like} \iff G(R) = C_\rho^{-1}(1).$$

Clause falsified by all extensions of ρ. $\leftrightarrow$ conjunction sat by all extensions of ρ

Good property but hard to maintain;
$\to$ will ~~try~~ to maintain that X is ~~very~~ almost uniform and Y is large. Will imply ρ-like!

The min-entropy corresponds to the bits required to write down the most likely event of a random variable;

$$H_\infty(X) = \min_x \log\left(\frac{1}{\Pr[X=x]}\right)$$

$X \sim_{u.a.r.} \{0,1\}^k$
$\to H_\infty(x) = k$

$X = (0,\dots,0)$
$\to H_\infty(x) = 0$

$x \to$ $\frac{1}{4}$: 0, $\frac{1}{2}$: 1, $\frac{1}{8}$: 2, $\frac{1}{8}$: 3
$\to H_\infty(x) = 1$

$\to$ will want to maintain large min-entropy;
even something stronger: that no marginal has low min-entropy.

$\to$ distribution with last bit fixed: large min-entropy but annoying as the final bit is determined.

A random variable $X \in [m]^J$ is δ-dense if for every nonempty $I \subseteq J$ X_I has min-entropy $H_\infty(X_I) \geq \delta \cdot |I| \cdot \log m$

marginal distribution

$\overbrace{x_1 \mid x_2 \mid \quad \mid \quad \mid \quad \mid \quad \mid x_{|J|}}^{I}$ J close to uniform

$R := X \times Y \subseteq [m]^n \times (\{0,1\}^m)^n$

A rectangle R is ρ-structured if

1) $X_{\mathrm{dom}(\rho)}$ is fixed, and every $z \in G(R) \subseteq C_\rho^{-1}(1)$.
u.a.r. over X; non-*; $\rho^{-1}(\{0,1\})$; y is chosen appropriately $\leftrightarrow$ y fixed on the index

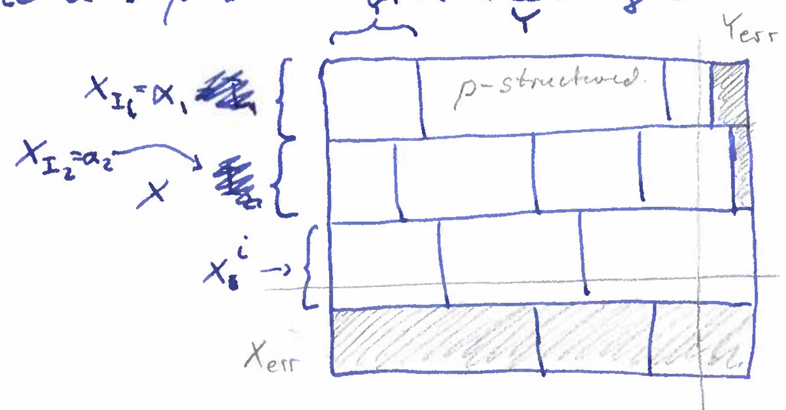
2) $X_{\mathrm{free}(\rho)}$ is 0.9-dense. every marginal close to uniform.
$\rho^{-1}(*)$

3) Y is large: $H_\infty(Y) \geq mn - n^3$.
$\to |Y| \geq 2^{mn-n^3}$

Ultimately we will maintain ~~that~~ a ρ-structured rectangle.

Lemma. ~~that~~ If $X \times Y$ ~~be~~ is ρ-structured, $m \geq n^c$ then $X \times Y$ is ρ-like, and, furthermore, there is a $x \in X$ such that $\{x\} \times Y$ is ρ-like.

Remains to explain how to go from a rectangle $R = X \times Y$ on from Π to a ρ-structured rectangle.



$Y^{i,\gamma}$: on I_i the gadget $g^{I_i}(\alpha_i, y_{I_i}) = \gamma$.

R1: 1) Let $I_i \subseteq [n]$ be maximal such that X_{I_i} has min-entropy rate < 0.95; let $\alpha_i \in [m]^{I_i}$ witness this

$\rightarrow \Pr[X_{I_i} = \boxed{\alpha_i}] > m^{-0.95|I_i|}$

$\cdot\ X^i_\gamma := \{x : x_{I_i} = \alpha_i\}$

2) Remove X^i_γ from R

R2: For each X^i_γ; $\gamma \in \{0,1\}^{I_i}$, define $Y^{i,\gamma} := \{y : g^{I_i}(\alpha_i, y_{I_i}) = \gamma\}$.

output: $\{R^{i,\gamma} := X^i \times \underbrace{Y^{i,\gamma}}_{\neq \emptyset}\}$

Rectangle Lemma: $|\Pi| = n^d$

Fix $k \leq n \log n$ ($2 \cdot d \cdot \log n$). Given a rectangle R, let $R = \dot\bigcup R_i$ be the rectangles from above partition scheme. Then there are error set $X^{err} \subseteq [m]^n$ and $Y^{err} \subseteq \{0,1\}^{m \cdot n}$ both of density $\leq 2^{-k}$ ($\leq n^{-2d}$) such that for every i either

- R^i is ρ^i structured for ρ^i of width $O(k/\log n)$
- R^i is covered by error rows/cols; $R^i \subseteq X_{err} \times \{0,1\}^{mn} \cup [m]^n \times Y_{err}$.

Finally, for every $x \in [m]^n \setminus X_{err}$ there is a subset $I_x \subseteq [n]$: $|I_x| \leq O(k/\log n)$ such that every structured R^i intersecting $\{x\} \times \{0,1\}^{mn}$ has $\mathrm{dom}(\rho^i) \subseteq I_x$.

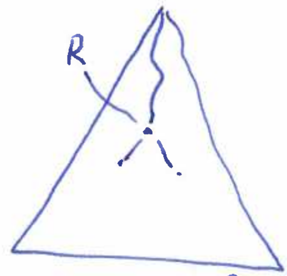
Given a rectangle-dag π solving $S \circ G$ with $|\pi| = n^d$, then $w(S) \leq O(d)$.

$\to$ want to create a width d res. refutation from π.

Let us ignore error sets for now.

Want to create a prosecution strategy in width $\leq O(d)$.

$k := 2d \log n$



idea: · walk down π; start at the root.

· for each rectangle R reached maintain a ρ-structured rectangle

what is queried

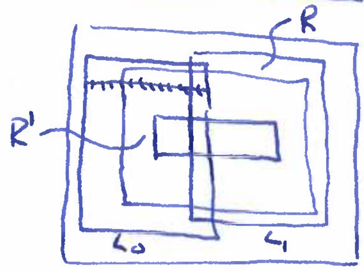
width $\leq d$

$\to R' \subseteq R$. from the partition.

1) Why can we start at the root?

2) How do we go to a child in π?

3) Why are we done in a leaf?



(1) Root: the partition is everything; $\rho = *^n \Rightarrow$ all good.

(2) step: Suppose the game is in state $\rho_{R'}$; R' is $\rho_{R'}$ structured.

want to move to ρ_L-structured subrectangle $L_b^* \subseteq L$. of a child. Want to remain in width $O(d)$.

· $R' =: X' \times Y'$ is $\rho_{R'}$-structured $\Rightarrow \exists x^* \in X'$: $\{x^*\} \times Y'$ is $\rho_{R'}$-like.

· $L_b = \dot{\bigcup} L_b^i$ from partition scheme.

$\exists I_b^* \subseteq [n]'$

$\to$ all L_b^i that intersect row x^* satisfy:

· L_b^i is ρ^i-structured

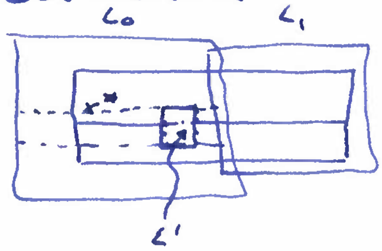
· $\mathrm{dom}(\rho^i) \subseteq I_b^*$.

$\Rightarrow$ query $J := (I_0^* \cup I_1^*) \setminus \mathrm{dom}(\rho_{R'})$. (in S)

$\to z_J$ be that answer.

note: $\mathrm{dom}(\underbrace{z_J \cup \rho_{R'}}_{\rho^*}) \leq O(d)$.

Because R' is $\rho_{R'}$-like and ρ^* is an extension:



$\rightsquigarrow \exists\, y^* \in Y'$: $\quad G(x^*, y^*) = \rho^*$

· Suppose $(x^*, y^*) \in L_0$.

· Consider $\quad L'$ from partition such that $(x^*, y^*) \in L_0$.)

· L' is $\rho_{L'}$-structured

· $\mathrm{dom}(\rho_{L'}) \subseteq I_1^*$.

· Forget everything except $\mathrm{dom}(\rho_{L'})$.

<u>(3) Leaf case:</u> Suppose we have game state ρ; R': ρ-struct.

The leaf node is labeled by o: $\quad R' \subseteq (S \circ G)^{-1}(o)$.

$\longleftrightarrow \quad G(R') \subseteq S^{-1}(o)$.

$\qquad \| \leftarrow$ lemma ρ-like

$C_\rho^{-1}(1)$

<u>Error:</u> traverse π in topological order from bottom to top;
$R_1, \dots, R_{n^d}$; $\quad X^*_{err} = Y^*_{err} = \emptyset$.
Consider R_i.

· update $R_i \leftarrow R_i \setminus (X^*_{err} \times \{0,1\}^{mn} \cup [m]^n \times Y^*_{err})$

keep the good rectangles.

· apply partition scheme. Call X_{err}; Y_{err} the errors.

· $X^*_{err} \leftarrow X^*_{err} \cup X_{err}$; $\; Y^*_{err} \leftarrow Y^*_{err} \cup Y_{err}$.

$\rightsquigarrow$ same proof as before on $(X \setminus X^*_{err}) \times (Y \setminus Y^*_{err})$.

(1) <u>Root</u>: density of error $\leq n^d \cdot n^{-2d} \ll 1\%$.

$\rightarrow R_{n^d}$ (with errors removed)

is still the output.

(2) <u>Step</u>: Just note that the error sets shrink as we walk down the proof; same argument.

- Constant gadget size?
- lifting theorem for "complicated" objects such as intersection of triangles?
  $\rightsquigarrow$ Res-lin; Res(CP) $\approx$ DAG-like Stabbing Planes
- nondeterministic lifting theorem for NOF protocols
  $\rightsquigarrow$ semi-algebraic proof system over polynomials.