RECAP

We are proving:

Polynomial-size circuits of constant depth cannot compute the parity of a bit string

$$\boxed{\text{PARITY} \notin AC^0}$$

We showed that this follows from:

HÅSTAD'S SWITCHING LEMMA

Suppose $f: \{0,1\}^n \to \{0,1\}$ can be written as k-DNF formula

Suppose ρ random restriction of t uniformly chosen variables

Then for all $s \geq 2$ it holds that

$$\boxed{\Pr_{\rho}\left[f\restriction_{\rho} \text{ CANNOT be written as } s\text{-CNF} \right] \leq \left(\frac{(n-t)k^{10}}{n} \right)^{s/2}}$$

Recall: NOT AT ALL TRUE in general that k-DNF can also be written as s-CNF for k, s bounded

Can have $k=2$ but $s = \Omega(n)$ (saw example)

But k-DNF hit by suitable random restriction can be written as s-CNF for k, s small — this is what Håstad's Switching Lemma says

TERMINOLOGY

MINTERM partial assignment ρ fixing $f\restriction_\rho \equiv 1$

MAXTERM partial assignment ρ fixing $f\restriction_\rho \equiv 0$

Every conjunction/term in k-DNF formula is minterm of size k

Every disjunction/clause in k-CNF formula is maxterm of size k

We always try to pick minterms and maxterms (to be) minimal (even if not stated explicitly always)

OBSERVATION $\boxed{\text{If}}$ all minimal maxterms of a Boolean function f are of size $\leq s$, $\boxed{\text{then}}$ f can be written as s-CNF formula

Proof. Exercise.

Hence, $\boxed{\text{if}}$ the switching fails, so that $f\restriction_\rho$ is not s-CNF, $\boxed{\text{then}}$ $f\restriction_\rho$ has a minimal maxterm of size $\geq s+1$

FOCUS on analyzing

$$\boxed{\Pr\left[f\restriction_\rho \text{ has maxterm of size } \geq s+1\right]}$$

FIX Boolean function f for the rest of this argument

Let us write

$\boxed{R^n_t}$ = { all restrictions of t out of n variables }

Choose t variables in $\binom{n}{t}$ ways

Assign 0/1 in 2^t ways

$$\boxed{|R^n_t| = \binom{n}{t} 2^t}$$

$\boxed{B}$ = { Bad restrictions $\rho \in R^n_t$ for which $f\restriction_\rho$ has minimal maxterm of size $\geq s+1$ }

Note that if $f\restriction_\rho$ not s-CNF, then $\rho \in B$ (But there are s-CNF formulas with minimal? maxterms of size $\geq s+1$ — exercise.)

Since random restriction ρ is chosen uniformly, ρ will switch k-DNF to s-CNF with probability

$$\geq 1 - \frac{|B|}{|R^n_t|}$$

We want to prove than B is very small compared to $|R^n_t|$

IDEA:

1. Find set S such that $|S| \ll |R^n_t|$
2. Construct one-to-one mapping $m : B \rightarrow S$
3. Then $|B| \leq |S| \ll |R^n_t|$

Slightly more concretely, we will choose

$$\boxed{S = R^n_{t+s} \times \{0,1\}^{\ell}}$$

Plus some extra bits of information

Restriction over $t+s$ variables

for $\ell = O(s \log k)$

$$\boxed{\text{Why is } |S| \ll |R^n_t| \text{ ?}}$$

Intuitively

(a) if t very close to n, then

$$\binom{n}{t} \gg \binom{n}{t+s} \approx \binom{n}{t} / n^s$$

(b) Since s and k constant, multiplying by $2^{O(s \log k)} = k^{O(s)}$ does not change this

THE FORMAL CALCULATIONS will go like

$$\frac{|B|}{|R^n_t|} \leq \frac{|R^n_{t+s} \times \{0,1\}^{\ell}|}{|R^n_t|}$$

$$= \frac{\binom{n}{t+s} 2^{t+s} 2^{O(s \log k)}}{\binom{n}{t} 2^t}$$

$$= \frac{\binom{n}{t+s} \cdot k^{O(s)}}{\binom{n}{t}} \lesssim \left[\begin{array}{l} k, s \text{ constant} \\ t \text{ close to } n \end{array}\right]$$

$$\lesssim \frac{\binom{n}{t} / n^s}{\binom{n}{t}} k^{O(s)} = n^{-\Omega(s)}$$

which looks like what we are after in the statement of Håstad's Switching Lemma!

CLAIM The above handwaving can be worked out to prove the bound in Håstad's Switching Lemma

Proof sketch First, prove

$$\boxed{\binom{n}{t+s}\binom{t+s}{t} = \binom{n}{t}\binom{n-t}{s}} \qquad (1)$$

In how many ways can you choose
- $t+s$ numbers in $[n] = \{1, 2, \ldots, n\}$;
- colour t numbers chosen red;
- colour s numbers chosen blue ?

LHS of (1): First choose $t+s$ numbers, then choose colouring

RHS of (1): First choose t red numbers, then choose s blue numbers among remaining ones

Second, use well-known inequalities

$$\boxed{\left(\frac{n}{k}\right)^k \overset{\text{easy}}{\leq} \binom{n}{k} \leq \left(\frac{en}{k}\right)^k} \qquad (2)$$

Now use (1) and (2) to prove that for $t > n/2$ it holds that

$$\binom{n}{t+s} \leq \binom{n}{t}\left(\frac{e(n-t)}{n}\right)^s$$

The details are left as an exercise $\boxtimes$

THIS MEANS that given this claim, we are done with proof of Håstad's Switching Lemma if we can construct one-to-one mapping

$$\boxed{m : B \longrightarrow R^n_{t+s} \times \{0,1\}^{\ell}}$$

Note that function f fixed

Fix representation of f as k-DNF formula

$$\boxed{F = T_1 \vee T_2 \vee \cdots \vee T_m} \quad \text{for}$$

$$\boxed{T_i = a_{i,1} \wedge a_{i,2} \wedge \cdots \wedge a_{i,k}}$$

Order terms in some order $T_1, T_2, \ldots$

Order literals in each term in some order

Look at $f\restriction_\rho$ for bad $\rho \in B$

- No term T_i satisfied
  (if so, $f\restriction_\rho \equiv 1$, and no maxterms)
- Some terms T_i maybe falsified, but not all
  (if so $f\restriction_\rho \equiv 0$, single maxterm of size 0)
- Some minimal maxterm π of size $> s$

Write $\rho\pi$ for union of restrictions ρ and π when $Vars(\rho) \cap Vars(\pi) = \emptyset$ so that $\rho\pi$ valid truth value assignment

$$\boxed{\begin{aligned} f\restriction_\rho &\not\equiv 0 \\ f\restriction_{\rho\pi} &\equiv 0 \end{aligned}}$$

(by definition of maxterm)

Tells us a lot about structure of ρ !

Define mapping to $\tau \in R^n_{t+s}$

Add extra info so that $\rho\pi$ and π can be recovered from τ

Then can find ρ, so mapping one-to-one

Example $\quad k = s = 3\,,\ \rho \in B$

$$\boxed{\begin{aligned} F = \ & (x_1 \wedge \overline{x_2} \wedge x_4) \\ \vee\ & (x_1 \wedge \overline{x_4} \wedge x_5) \\ \vee\ & (x_2 \wedge \overline{x_3} \wedge \overline{x_4}) \\ \vee\ & (x_3 \wedge x_4 \wedge \overline{x_8}) \\ \vee\ & (x_1 \wedge x_6 \wedge \overline{x_7}) \\ \vee\ & (x_2 \wedge x_7 \wedge x_9) \end{aligned}}$$

3-DNF formula

Suppose $\rho = \{x_1 \mapsto 1, x_2 \mapsto 1, x_3 \mapsto 1\}$

Maxterm of size > 3 is

$$\pi = \{x_4 \mapsto 0, x_5 \mapsto 0, x_6 \mapsto 0, x_7 \mapsto 0\}$$

$$\begin{aligned} F\restriction_\rho = \ & \cancel{(x_1 \wedge \overline{x_2} \wedge x_4)} && \text{falsified by } \rho \\ \vee\ & (\overset{=1}{x_1} \wedge \overline{x_4} \wedge x_5) && \pi \text{ sets } x_5 = 0 \\ & \cancel{\vee\ (x_2 \wedge \overline{x_3} \wedge \overline{x_4})} && \text{falsified by } \rho \\ \vee\ & (\overset{=1}{x_3} \wedge x_4 \wedge \overline{x_8}) && \pi \text{ sets } x_4 = 0 \\ \vee\ & (\overset{=1}{x_1} \wedge x_6 \wedge \overline{x_7}) && \pi \text{ sets } x_6 = 0 \\ \vee\ & (\overset{=1}{x_2} \wedge x_7 \wedge x_9) && \pi \text{ sets } x_7 = 0 \end{aligned}$$

so $F\restriction_{\rho\pi} \equiv 0$ but clearly π minimal

We will use this example to illustrate the mapping

$$m : B \to R^{n}_{t+s} \times \{0,1\}^{\ell}$$

Intuitively, what should the mapping m be ?

Need to use π somehow...

Should we map ρ to $\rho\pi$? (With suitable trimming, to set only $t+s = 6$ variables)

But given $\rho\pi =$

$= \{x_1 \mapsto 1, x_2 \mapsto 1, x_3 \mapsto 1, x_4 \mapsto 0, x_5 \mapsto 0, x_6 \mapsto 0, x_7 \mapsto 0\}$

how do we know which part is ρ and which part is π? We just see that all terms are false!

IDEA: Change π to other assignment σ to same variables that does not falsify terms. Then when we see $\rho\sigma$, we can figure out ρ by

a) looking at which terms are falsified or not

b) using some extra book-keeping notes that provide helpful hints

DEFINITION OF MAPPING

STEP 1 Find first term (= conjunction) T_1 not falsified by ρ

$Y_1 := Vars(T_1) \cap Vars(\pi) \neq \emptyset$

$\pi_1 :=$ subassignment of π to Y_1

$\sigma_1 :=$ unique assignment to Y_1 satisfying literals in T_1

Compute "extra information" c_1 consisting of

- $s_1 := |Y_1|$
- positions of Y_1-variables in T_1
- values to Y_1-variables assigned by π_1

At most k positions in T_1

$\Rightarrow$ $O(s_1 \log k)$ bits needed

Example F

$$T_1 = x_1 \wedge \bar{x}_4 \wedge x_5$$

$$Y_1 = \{x_4, x_5\}$$

$$\pi_1 = \{x_4 \mapsto 0, x_5 \mapsto 0\}$$

$$\sigma_1 = \{x_4 \mapsto 0, x_5 \mapsto 1\}$$

$$c_1 = \text{"}2;\ 2 \mapsto 0,\ 3 \mapsto 0\text{"}$$

STEP $i > 1$

Have computed $Y_j, \pi_j, \sigma_j, c_j$ for $j < i$

$$\rho\pi_1\pi_2 \cdots \pi_{i-1} \subsetneq \rho\pi$$

Find first term T_i not falsified by $\rho\pi_1\pi_2 \cdots \pi_{i-1}$

$Y_i := (Vars(T_i) \cap Vars(\pi)) \setminus Vars(\rho\pi_1 \cdots \pi_{i-1})$

$\pi_i :=$ subassignment of π to Y_i

$\sigma_i :=$ unique assignment to Y_i satisfying literals in T_i

Extra information c_i:

- $s_i = |Y_i|$
- positions of Y_i-variables in T_i
- values to Y_i-variables assigned by π_i

$O(s_i \log k)$ bits

Example F

$T_2 = x_1 \wedge x_6 \wedge \overline{x_7}$

$Y_2 = \{x_6, x_7\}$

$\pi_2 = \{x_6 \mapsto 0, x_7 \mapsto 0\}$

$\sigma_2 = \{x_6 \mapsto 1, x_7 \mapsto 0\}$

$c_2 =$ " $2; \ 2 \mapsto 0, \ 3 \mapsto 0$ "

TERMINATE when $\pi_1, \pi_2 \cdots \pi_m$ assigns $\geq s$ variables

- Trim π_m to get exactly s variables in total
- Update σ_m and c_m accordingly

$\boxed{\text{FINAL MAPPING}}$ of ρ is to

$$\tau = \rho\sigma_1 \cdots \sigma_m \quad \text{plus}$$
$$c = c_1 \cdots c_m$$

$\tau \in R^n_{t+s}$ by construction

Size of $c = c_1 \cdots c_m$ is

$$\leq \sum_{i=1}^{m} O(s_i \log k) = O(s \log k)$$

Can encode $c \in \{0,1\}^{O(s \log k)}$

Example F

Trim to

$$\pi_2 = \{x_6 \mapsto 0\}$$
$$\sigma_2 = \{x_6 \mapsto 1\}$$
$$c_2 = \text{"}1;\ 2 \mapsto 0\text{"}$$

$$\boxed{m(\rho) = (\tau, c)} \quad \text{for}$$

$$\boxed{\tau = \{x_1 \mapsto 1, x_2 \mapsto 1, x_3 \mapsto 1, x_4 \mapsto 0, x_5 \mapsto 1, x_6 \mapsto 1\}}$$

$$\boxed{c = \text{"}2;\ 2 \mapsto 0, 3 \mapsto 0 \mid 1;\ 2 \mapsto 0\text{"}}$$

We are done with proof of Håstad's Switching Lemma if we can prove that

MAPPING m IS ONE-TO-ONE

Given (τ, c), need to recover ρ

By construction, $\rho \subseteq \tau$, but how do we know which part of τ this is?

Example

We have $\tau \in R_6^n$, $\rho \in R_3^n$

$\tau = \{ x_1 = x_2 = x_3 = x_5 = x_6 = 1, x_4 = 0 \}$

Which three variables belong to ρ?

DECODING OF $m(\rho) = (\tau, c)$

STEP 1

Find first term T_1 not falsified by τ

ρ neither falsifies nor satisfies T_1

σ_1 satisfies literals in T_1

σ_i for $i > 1$ does not assign literals in T_1 (by construction)

so same T_1 as in mapping process

Look up in c_1 what Y_1 is

Read off assignment π_1

Use this info to modify

$\tau = \rho \boxed{\sigma_1} \sigma_2 \cdots \sigma_m$ to

$\tau_1 = \rho \boxed{\pi_1} \sigma_2 \cdots \sigma_m$

NOTE τ_1 falsifies T_1

Example

First non-falsified term for τ is

$$x_1 \wedge \overline{x}_4 \wedge x_5$$

$c_1 = $ " 2 ; $2 \mapsto 0$, $3 \mapsto 0$ " says

$$\pi_1 = \{ x_4 \mapsto 0,\ x_5 \mapsto 0 \}$$

$$\tau = \{ x_1 \mapsto 1,\ x_2 \mapsto 1,\ x_3 \mapsto 1,\ x_4 \mapsto 0,\ x_5 \mapsto 1,\ x_6 \mapsto 1 \}$$

$$\tau_1 = \{ x_1 \mapsto 1,\ x_2 \mapsto 1,\ x_3 \mapsto 1,\ x_4 \mapsto 0,\ x_5 \mapsto 0,\ x_6 \mapsto 1 \}$$

STEP $i > 1$

falsifies $T_1, \ldots, T_{i-1}$

We have reconstructed

$$\tau_{i-1} = \rho\, \pi_1 \cdots \pi_{i-1}\, \sigma_i \cdots \sigma_m$$

Find first term T_i not falsified by τ_{i-1}

Must be same T_i as in construction of mapping!

- $\rho\, \pi_1 \cdots \pi_{i-1}$ didn't falsify it
- and σ_i made sure all assigned literals in T_i are true
- No σ_j, $j > i$ assigns variables in this term

Look up in c_i what Y_i is

Read off assignment π_i

Use this information to go from

$$\tau_{i-1} = \rho\, \pi_1 \cdots \pi_{i-1}\, \sigma_i\, \sigma_{i+1} \cdots \sigma_m \quad \text{to}$$

$$\tau_i = \rho\, \pi_1 \cdots \pi_{i-1}\, \pi_i\, \sigma_{i+1} \cdots \sigma_m$$

When this process ends, we have recovered

$\tau_m = \rho\,\pi_1\,\pi_2 \cdots \pi_m$ and all $\pi_1, \ldots, \pi_m$

so we can figure out what ρ is

Since we recovered ρ uniquely, the mapping m is $\boxed{\text{one-to-one}}$ as claimed

Håstad's Switching Lemma follows. $\blacksquare$

$\tau_1 = \{x_1 \mapsto 1, x_2 \mapsto 1, x_3 \mapsto 1, x_4 \mapsto 0, x_5 \mapsto 0, x_6 \mapsto 1\}$

First term not falsified by τ_1 is

$$x_1 \wedge x_6 \wedge x_7$$

$c_2 =$ " $1;\ 2 \mapsto 0$ " says

$\pi_2 = \{x_6 \mapsto 0\}$ so

$\tau_2 = \{\boxed{x_1 \mapsto 1, x_2 \mapsto 1, x_3 \mapsto 1,}\ x_4 \mapsto 0, x_5 \mapsto 0, x_6 \mapsto 0\}$

No more information to process!

ρ has to be what is left when we remove π

$$\rho = \{x_1 \mapsto 1, x_2 \mapsto 1, x_3 \mapsto 1\}$$

PHILOSOPHICAL QUESTION

Why do we prove circuit lower bounds for PARITY ?!

Very simple function — clearly not hard for general circuits!

If we would choose a harder problem, then we could get a stronger lower bound, no?

PARADOX: In order to prove a lower bound for a function, we need to understand this function well, it seems.
So the function cannot be too hard, or else it becomes too hard to prove that the function is hard, even though a strong lower bound should probably be true...

Now we know PARITY $\notin AC^0$

Prove lower bounds for stronger classes of circuits!

- Keep depth $O(1)$
- But add counting gates

$$MOD_m(x) = \begin{cases} 0 & \text{if } \sum_i x_i \equiv 0 \pmod{m} \\ 1 & \text{otherwise} \end{cases}$$

Clearly, with single MOD_2-gate PARITY easy

THIS IS UP NEXT