

CoCo : BOUNDED-DEPTH CIRCUITS

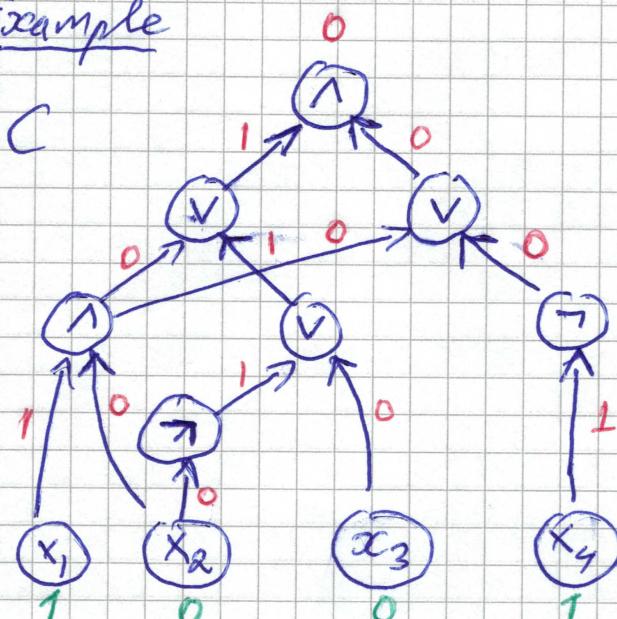
I

Boolean circuits.

- Directed acyclic graph
- Source nodes labelled by variables
- Non-source nodes (gates) labelled by

AND	1
OR	v
NOT	—
- Every gate computes Boolean function of inputs
- Output: value computed by (unique) sink node

Example



$$C(1, 0, 0, 1)$$

Size of circuit:

nodes

(11 for example)

A language is decided by a family of circuits $\{C_n\}_{n \in \mathbb{N}}$ — one circuit C_n for each input length n

P/poly: Class of languages decided by circuits with sizes scaling polynomially

Believe: $NP \notin P/\text{poly}$

To prove this, find language $L \in NP$ that cannot be decided by polynomial-size circuits

Prove lower bounds for functions

$\{f_n : \{0,1\}^n \rightarrow \{0,1\}\}_{n \in \mathbb{N}^+}$ such that

$$f_n(x) = 1 \Leftrightarrow x \in L$$

When we proved Cook-L Levin, we saw that any function $f : \{0,1\}^n \rightarrow \{0,1\}$ computed by circuit C_f of size $O(n \cdot 2^n)$

Can be improved to $O(2^n/n)$

Almost all functions $f : \{0,1\}^n \rightarrow \{0,1\}$ require size $\Omega(2^n/n)$

such functions 2^{2^n} (why?)

Count # circuits of size $\frac{2^n}{10n}$, say

Way fewer.

Shannon's lower bound

III

But best lower bound for explicit functions is $5n - o(n)$

LONG-STANDING OPEN PROBLEM TO IMPROVE THIS 

So look at RESTRICTED CIRCUIT MODELS

- (a) MONOTONE circuits
- (b) BOUNDED-DEPTH circuits
- (c) BOUNDED-DEPTH circuits with "COUNTING GATES"

MONOTONE CIRCUITS

No NOT-gates

Can only compute monotone functions
Switching input bit from 0 to 1 can never flip from 1 to 0

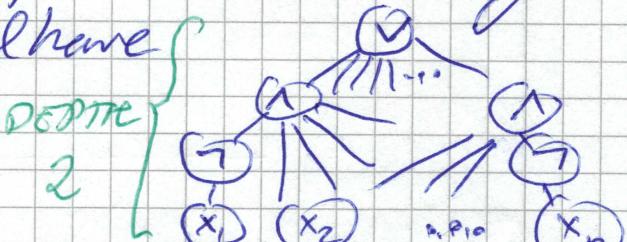
BOUNDED-DEPTH CIRCUITS

Count # alternations AND-OR along any path; restrict to constant # alternations

More convenient model (equivalent)

AND and OR of unbounded arity

Circuit DAG should have
constant depth



COUNTING GATES

$$\text{MOD}_k^n(x_1, \dots, x_n) = \begin{cases} 1 & \text{if } \sum_{i=1}^n x_i \equiv 0 \pmod{k} \\ 0 & \text{otherwise} \end{cases}$$

In constant depth, exactly which gates you have access to can matter a lot

Exponential lower bounds known for

- (a) monotone circuits
- (b) bounded-depth circuits
- (c) bounded depth + some MOD gates

Question right at research frontier

Colo 2023: Presentation of (a)

Colo 2024: Presentation of (b) + (c)

Every Boolean function computable by
CNF/ DNF of exponential size
= depth - 2 circuit

For depth 2, also not too hard to
prove matching lower bounds

But these techniques don't seem to
generalize to depth 3 or larger

AC⁰: Functions / languages computable

by

- polynomial-size circuits
- constant depth
- unbounded fan-in AND- and OR-gates

$$\text{PARITY} = \{x \in \{0, 1\}^* \mid x \text{ has odd \# 1s}\}$$

THEOREM [Furst, Saxe, Sipser '81, Ajtai '83]

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

Will also write

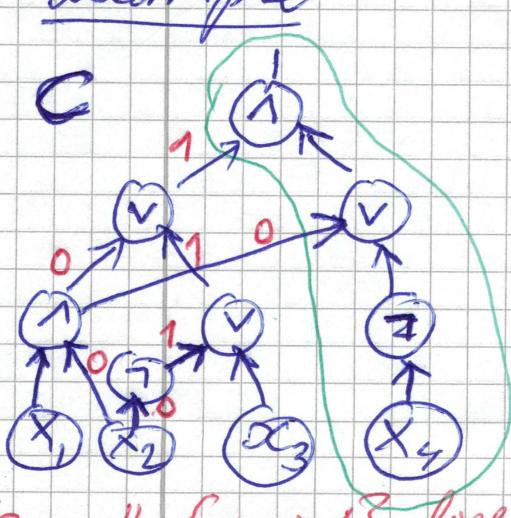
$$\text{PARITY}(x) = 1 \text{ if } x \in \text{PARITY}$$

In fact, circuits of bounded depth for PARITY must have exponential size — proven by Johan Håstad at KTH in Stockholm — but we won't try to prove optimal lower bounds today

Main tool: RANDOM RESTRICTIONS

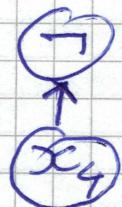
- Pick random subset of variables
- Set to random values 0/1
- Simplify circuit
 - o Replace 1-gate with 0-input by 0
 - o Replace V-gate with 1-input by 1
 - o Replace $g \wedge 1$ by g
 - o Replace $h \vee 0$ by h

Example



$$\text{Let } g = \{x_2 \mapsto 0\}$$

$$C|_g$$



$$\text{For } g' = \{x_2 \mapsto 0, x_4 \mapsto 1\}$$

(But $g'' = \{x_1 \mapsto 1\}$ does not cause such collapse) get constant circuit $C|_{g'} \equiv 0$

Given $f: \mathcal{X} \rightarrow \{0, 1\}$

for $\mathcal{X} = \mathcal{X}_1 \cup \mathcal{X}_2$

and $g: \mathcal{X}_1 \rightarrow \{0, 1\}$

Restricted function $f|_g$ on \mathcal{X}_2 defined by

$$f|_g(x) = f(g, x)$$

OBSERVATION

If C computes f
then $C|_g$ computes $f|_g$

HIGH-LEVEL PROOF IDEA

- ① Suppose \exists circuit C_n for PARITY in polynomial size and constant depth d
- ② Choose random restriction g on all but n^ε variables ($\varepsilon > 0$ depends on d) and simplify $C|_g$
- ③ Prove that since C_n small and shallow, g collapses C_n to $C_n|_g \equiv \text{constant}$
- ④ But $\text{PARITY}|_g$ is still non-constant function (parity or negation of parity)
So $C_n|_g$ should compute this non-constant function

CONTRADICTION ↲

Hence no AC^0 -circuit for PARITY, QED ↳ ↴

SOME NOTATION AND TERMINOLOGY

k -CNF formula: AND of ORs of size $\leq k$

k -DNF formula: OR of ANDs of size $\leq k$

f function, ρ partial assignment = restriction

$f \upharpoonright \rho$ f restricted by ρ

$$f \upharpoonright \rho (\tau) = f(\rho \circ \tau)$$

$\text{Vars}(\rho)$ = sets of variables assigned to 0/1 by ρ

Often write ρ as $\rho: \{0,1\}^n \rightarrow \{0,1,*\}$

$$\rho(x) = \begin{cases} 1 & \text{if } x \in \text{Vars}(\rho) \text{ and } \rho(x) = 1 \\ 0 & \text{if } x \in \text{Vars}(\rho) \text{ and } \rho(x) = 0 \\ * & \text{if } x \notin \text{Vars}(\rho) \end{cases}$$

HÅSTAD'S SWITCHING LEMMA

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

Let ρ uniformly random restriction of

t uniformly chosen variables

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

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

NB! Not the way Hastad stated it!

Not optimal parameters!

But good enough for us today ...

We can change places of DNF and CNF in the switching lemma
 (apply the lemma to $\neg f$ and then negate again)

We will use switching lemma with parameters:

$$k = O(1)$$

$$s = O(1)$$

$$t \approx n - \sqrt{n}$$

Gives

$$\Pr[f \not\models \text{not } s\text{-CNF}] \leq n^{-c}$$

for some constant $c > 0$

PLAN FOR LECTURES ON AC⁰

LARGER BOUNDS

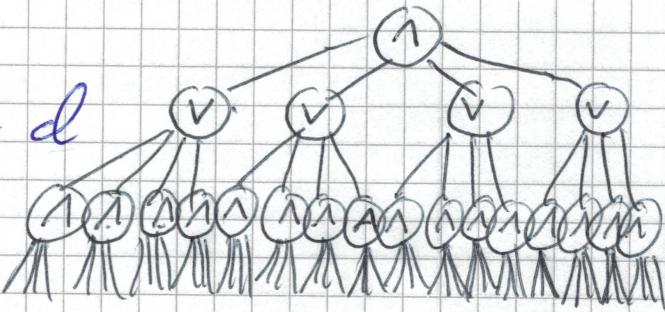
- ① Assume Håstad's Switching Lemma
 Use to prove PARITY \notin AC⁰
- ② Prove Håstad's Switching Lemma

Item ① fairly straightforward (though not if you haven't seen this type of proofs before)

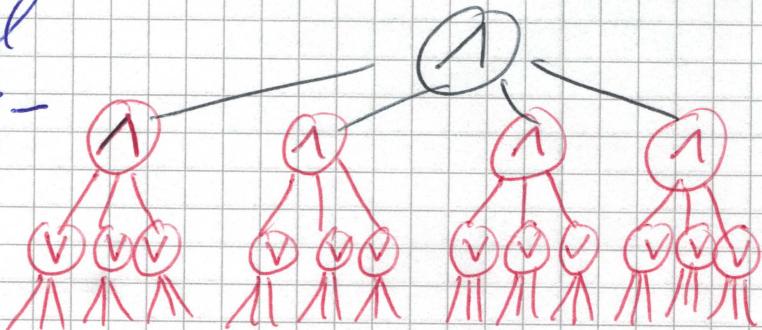
Item ② is hard.

OUTLINE OF ①

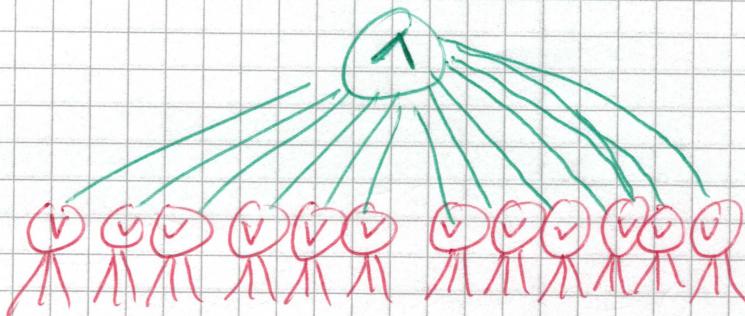
① Suppose circuit of depth d with layers of \wedge and \vee



② Hit with restriction and look at bottom layers - turns DNFs into CNFs with high probability



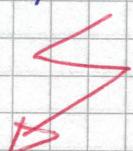
③ But now 2 consecutive layers with same connect - merge and decrease depth from d to $d-1$



④ Repeat this $d-2$ times
 \Rightarrow collapse to k -CNF or k -DNF formula

⑤ Just fix k more variable to make disjunction false or conjunction true
 \Rightarrow fixes value of circuit

⑥ But we still have unassigned variables left that can flip the **CONTRADICTION**



Formal proof of AC^0 & Parity

IX

Start with polynomial-size AC^0 -circuit
of depth d for Parity

Do initial preprocessing to get circuit
with following properties:

- (a) fan-out of all gates is 1
(i.e., circuit DAG is tree; circuit is formula)
- (b) All NOT-gates are right above the
variable input level (i.e., apply to variables
only) and therefore no NOT-gates elsewhere
- (c) AND- and OR-gates alternate — at
each level only 1 or only 1, and
wires only between consecutive layers
- (d) Right above variables and NOT-gates
we have AND-gates with fan-in 1.

LEMMA This preprocessing can be done
without increasing depth by more than $O(1)$
and without blowing up size more than
polynomially

Proof Exercise. (Might potentially appear
on a problem set near you.)

Suppose circuit after preprocessing has depth d and $\leq n^{\frac{1}{6}}$ gates

Let $n_0 = n = \# \text{ variable inputs}$

For $i = 1, 2, \dots, d-2$

- Restrict $n_{i-1} - \sqrt{n_{i-1}}$ variables, leaving $n_i := \sqrt{n_{i-1}}$ unset variables
- Collapse circuit one layer (using Hastad's Switching Lemma)
- While keeping bottom layer at constant fan-in.

$$n_i = \sqrt{n_{i-1}} = \sqrt[2^i]{n}$$

Let $k_i := 10^6 \cdot 2^i (= O(1))$

Show that with high probability after i-th restriction have

- depth - $(d-i)$ circuit
- with fan-in $\leq k_i$ at bottom level

Suppose for concreteness that bottom layer of gates are 1-gates, level above V-gates (the opposite case is entirely symmetric)

By assumption, each V-gate one level up computes k_i -DNF formula

Apply Håstad's Switching Lemma
with parameters

$$\begin{cases} n = n_i = n^{1/2^i} \\ t = n_i - n_{i+1} = n^{1/2^i} - n^{1/2^{i+1}} \\ k = k_i \\ s = k_{i+1} \end{cases}$$

By HSL, for fixed v-gate k_i -DNF
turns into k_{i+1} -CNF except with
probability

$$\left(\frac{n^{1/2^{i+1}} \cdot k_i^{10}}{n^{1/2^i}} \right)^{k_{i+1}/2} \leq \left[\begin{array}{l} \text{pick } \\ K \leq k_d \end{array} \right]^{10 \cdot k_d}$$

$$\leq K \cdot \left(n^{-1/2^{i+1}} \right)^{k_{i+1}/2} \left[\begin{array}{l} \text{this } K \\ \text{so many } \\ \text{gates killed} \end{array} \right]$$

$$\leq K \cdot n^{-\frac{5}{2} \cdot 6}$$

$$\leq \frac{1}{10 \cdot n^6}$$

provided that n
is large enough

If k_i -DNF turns into k_{i+1} -CNF for all v-gates
in next-to-bottom layer, then we
can collapse π -gates with 1-gates
above

\Rightarrow depth decreases by 1
at bottom, have fan-in k_{i+1} ($= O(1)$)
so k_{i+1} -CNFs

In next step, reduce k_{i+1} - CNFs to k_{i+2} - DNFs in the same way

NOTE that to get collapsing argument we only consider the switching lemma once for each gate

So total # switching experiments that can go wrong is = circuit size $\leq n^6$

If there is a circuit gate for which switching does not happen, then we are in bad shape.

Look at random restriction ρ sampled as before

$$\Pr[\rho \text{ fails to collapse } C] \leq$$

$$\leq \Pr[\exists \text{ gate } v \text{ such that no switching for } v]$$

$$\leq \sum_{v \text{ gate}} \Pr[\rho \text{ does not switch } v] \quad \begin{array}{l} \text{UNION BOUND} \\ \Pr[U_i A_i] \\ \leq \sum_i \Pr[A_i] \end{array}$$

$$\leq \underbrace{n^6}_{\# \text{ gates}} \cdot \underbrace{\frac{1}{10 \cdot n^6}}_{\Pr[\text{failure for gate}]} = \frac{1}{10}$$

So whole collapsing process will work with probability $\geq 90\%$

This means, in particular, that

\exists good restriction β^* that will after $d-2$ steps collapse C to k_{d-2} -CNF or k_{d-2} -DNF.

Set additional $k_{d-2} = O(1)$ variables to falsify disjunction or satisfy conjunction $\Rightarrow C$ fixed to constant.

But still $n^{1/2^{d-1}} - k_{d-2} > 0$ variables left, so a correct circuit cannot have collapsed to constant. **Contradiction** ↴

Hence the circuit cannot have been computing PARITY, which proves the lower bound



Proof may be felt complicated, but once you digest the argument it is fairly straightforward (and standard)

The hard part of the lower bound is Håstad's Switching Lemma.

Let's talk about that next

Hastad's SWITCHING LEMMA

XV

Hastad's original proof technique technically quite challenging

Will use a more intuitive proof technique developed by Razborov

Extremely rough description:

Let $|R_t^n| = \{ \text{all restrictions of } t \text{ out of } n \text{ variables} \}$

$B \subseteq R_t^n$ BAD restrictions for which switching does not happen

$$|R_t^n| = \binom{n}{t} 2^t$$

$$\boxed{\Pr[\text{switching fails}] = \frac{|B|}{|R_t^n|}}$$

Show that $|B| \ll |R_t^n|$

Do so by showing that there are very concise ways of describing

$\exists B$ with #GTS $\ll \log_2(|R_t^n|)$

$$\begin{aligned} \text{Hence } |B| &\leq 2^{\#\text{GTS needed}} \ll 2^{\log_2(|R_t^n|)} \\ &= |R_t^n| \end{aligned}$$

TERMINOLOGY

MINTERM partial assignment $f \upharpoonright \beta \equiv 1$
 MAXTERM partial assignment $f \upharpoonright \beta \equiv 0$

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) ~~as~~ (minimal
(to be)

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

Proof. Exercise

Hence, if the switching fails, so that
 $f \upharpoonright \beta$ is not s -CNF, then $f \upharpoonright \beta$ has
a minimal maxterm of size $\geq s+1$

FOCUS on analyzing

$\Pr[f \upharpoonright \beta \text{ has maxterm of size } \geq s+1]$

FIX Boolean function f for the
rest of this argument