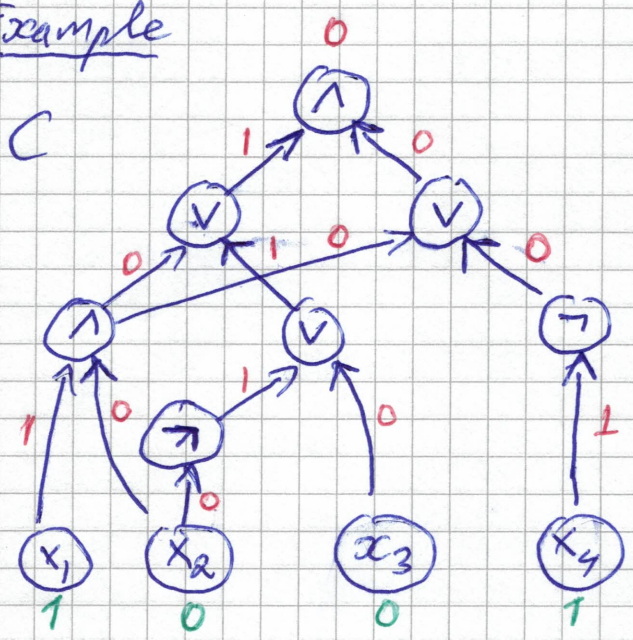
CoCo: BOUNDED-DEPTH CIRCUITS

Boolean circuits:

- Directed acyclic graph
- Source nodes labelled by variables
- Non-source nodes (gates) labelled by
  - AND $\wedge$
  - OR $\vee$
  - NOT $\neg$
- Every gate computes Boolean function of inputs
- Output: value computed by (unique) sink node

Example



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

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: $\boxed{NP \not\subseteq P/poly}$

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

Prove lower bounds for functions $\{f_n : \{0,1\}^n \to \{0,1\}\}_{n \in \mathbb{N}^+}$ such that

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

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

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

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

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

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

Way fewer. **Shannon's lower bound**

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 f from 1 to 0

BOUNDED-DEPTH CIRCUITS

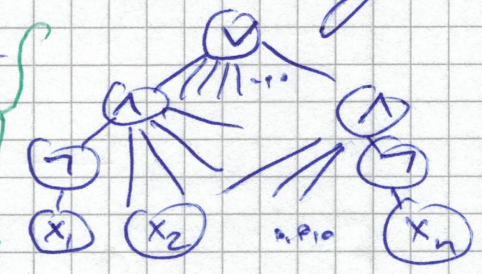
Count # alternations AND-OR along any path; restrict to constant # alternations

More convenient model (equivalent)

AND and OR of unbounded arity

Circuit DAG should have constant depth

DEPTH 2



COUNTING GATES

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

In constant depth, exactly which gates you have access to can make 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

CoCo 2023: Presentation of (a)
CoCo 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

AC^0: Functions / languages computable by
- polynomial-size circuits
- constant depth
- unbounded fan-in AND- and OR-gates

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

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

$PARITY \notin AC^0$

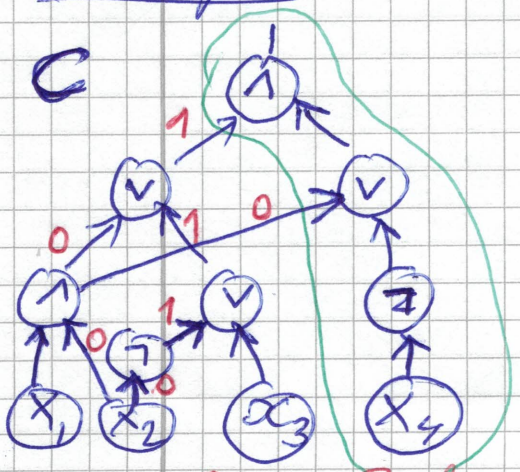
Will also write $PARITY(x) = 1$ if $x \in PARITY$

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

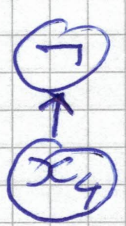
- Pick random subset of variables
- Set to random values 0/1
- Simplify circuit
  - Replace $\wedge$-gate with 0-input by 0
  - Replace $\vee$-gate with 1-input by 1
  - Replace $g \wedge 1$ by g
  - Replace $h \vee 0$ by h

Example



Let $\rho = \{x_2 \mapsto 0\}$

$C|_\rho$



For $\rho' = \{x_2 \mapsto 0, x_4 \mapsto 1\}$ get constant circuit $C|_{\rho'} \equiv 0$

(But $\rho'' = \{x_1 \mapsto 1\}$ does not cause such collapse)

Given $f : X \to \{0,1\}$

for $x = x_1 \cdot x_2$

and $\rho : X_1 \to \{0,1\}$

Restricted function $f\restriction_\rho$ on X_2 defined by

$$f\restriction_\rho(x) \equiv f(\rho, x)$$

OBSERVATION

If C computes f
then $C\restriction_\rho$ computes $f\restriction_\rho$

HIGH-LEVEL PROOF IDEA

(1) Suppose $\exists$ circuit C_n for PARITY in polynomial size and constant depth d

(2) Choose random restriction ρ on all but n^ε variables ($\varepsilon > 0$ depends on d) and simplify $C\restriction_\rho$

(3) Prove that since C_n small and shallow, ρ collapses C_n to $C_n\restriction_\rho \equiv$ constant

(4) But PARITY$\restriction_\rho$ is still non-constant function (parity or negation of parity) so $C_n\restriction_\rho$ 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

$f|_\rho$ f restricted by ρ

$$f|_\rho(\tau) = f(\rho \circ \tau)$$

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

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

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

HÅSTAD'S SWITCHING LEMMA

Suppose $f: \{0,1\}^n \to \{0,1\}$ 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

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

NB! Not the way Håstad stated it!
Not optimal parameters!
But good enough for us today ...

DETOUR: Note that it is VERY FALSE in general that k-DNF can be written as s-CNF for k, s bounded

Consider 2-DNF formula

$$F = (x_1 \wedge x_2) \vee (x_3 \wedge x_4) \vee (x_5 \wedge x_6) \vee \cdots \vee (x_{2n-1} \wedge x_{2n})$$

Write as CNF formula F' with clauses of minimal size k

Suppose F' contains k-clause

$$a_1 \vee a_2 \vee \cdots \vee a_k$$

Then falsifying these k literals guarantees that F' is false, and hence also that F is false

But that is impossible except if clause contains one variable from every term $(x_{2i-1} \wedge x_{2i})$

So F cannot be written as k-CNF formula for $k < n$

What Håstad's Switching Lemma says is that after applying a random restriction ρ, it holds that $F|_\rho$ can be rewritten as an s-CNF formula for s small with high probability

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

$$Pr\left[f|_\rho \text{ not } s\text{-CNF} \right] \leq n^{-c}$$

for some constant $c > 0$

PLAN FOR LECTURES ON AC^0 LOWER BOUNDS

(1) Assume Håstad's Switching Lemma
Use to prove PARITY $\notin AC^0$

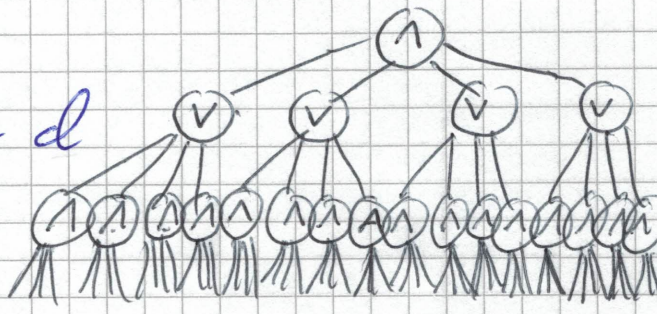
(2) Prove Håstad's Switching Lemma

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

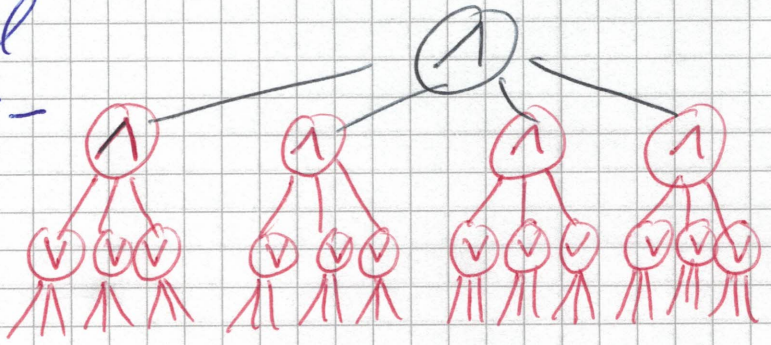
Item (2) is hard.

OUTLINE OF (1)

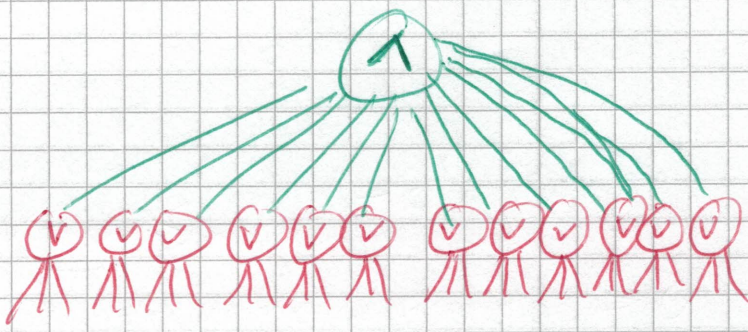
(i) Suppose circuit of depth d with layers of $\wedge$ and $\vee$



(ii) Hit with restriction and look at bottom layers – turns DNFs into CNFs with high probability



(iii) But now 2 consecutive layers with same connective – merge and decrease depth from d to $d-1$



(iv) Repeat this $d-2$ times
⇒ collapse to k-CNF or k-DNF formula

(v) Just fix k more variable to make disjunction false or conjunction true
⇒ fixes value of circuit

(vi) But we still have unassigned variables left that can flip the parity CONTRADICTION

Formal proof of AC^0 & PARITY

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 there are no NOT-gates elsewhere

(c) AND- and OR-gates alternate — at each level only $\wedge$ or only $\vee$, 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 $\leq n^6$ gates

Let $n_0 = n$ = # variable inputs

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

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

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

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

Show that with high probability after ith restriction have

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

Suppose for concreteness that bottom layer of gates are $\wedge$-gates, level above $\vee$-gates (the opposite case is entirely symmetric)

By assumption, each $\vee$-gate one level up computes k_i-DNF formula

Apply Håstad's Switching Lemma with parameters

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

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

$$\left(\frac{n^{1/2^{i+1}} \cdot k_i^{10}}{n^{1/2^i}} \right)^{k_{i+1}/2} \leq$$

[pick $K \leq k_d^{10 \cdot k_d}$]

$$\leq K \cdot \left(n^{-1/2^{i+1}} \right)^{k_{i+1}/2}$$

[this K ~~guys~~ gets killed]

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

$$\leq \frac{1}{10\, n^b}$$

provided that n is large enough

If k_i-DNF turns into k_{i+1}-CNF for all $\wedge$-gates in next-to-bottom layer, then we can collapse new $\wedge$-gates with $\wedge$-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 ~~foo~~ which switching does not happen, then we are in bad shape.

Look at random restriction ρ sampled as before

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

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

$$\leq \sum_{v \text{ gate}} \Pr[\rho \text{ does not switch } v]$$

UNION BOUND

$$\Pr[\bigcup_i A_i] \leq \sum_i \Pr[A_i]$$

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

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

This means, in particular, that

$\exists$ good restriction ρ^* 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 maybe 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

HÅSTAD'S SWITCHING LEMMA

Håstad's original proof technique technically quite challenging

Will follow more intuitive proof developed by Razborov

Very rough description

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

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

$f|_\rho$ is not s-CNF

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

We want to show that $|B| << |R_t^n|$

Use encoding argument: Show that there are very concise ways of describing $\rho \in B$ uniquely

If so, B cannot be too large

Find small set S, $|S| << |R_t^n|$

Construct one-to-one mapping

$$m : B \to S$$

Then $|B| \leq |S| << |R_t^n|$

$\rho \in B$
- assigns t variables
- fails to turn $f \wedge \rho$ into s-CNF

Use this to construct $\tau \in R^n_{t+s}$

$|R^n_t| =$ choose t variables in $\binom{n}{t}$ ways
assign them in 2^t ways

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

When t is close to n,

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

If we could map $\rho \in B$ to $\tau \in R^n_{t+s}$ in one-to-one fashion, we are done!

Doesn't quite work — in order to recover ρ from τ need $O(s \log k)$ extra bits of information

Will construct mapping

$$m : B \to R^n_{t+s} \times \{0,1\}^{O(s \log k)}$$

that is one-to-one. And we can show that $|R^n_{t+s} \times \{0,1\}^{O(s \log k)}| = \binom{n}{t+s} 2^{t+s} \cdot k^{O(s)} \ll$
$\ll |R^n_t|$. MORE ABOUT THIS NEXT TIME...