DD2445 COMPLEXITY THEORY: LECTURE 17

Boolean circuits again:
- Non-source nodes (gates) labelled by AND, OR, NOT
- Source nodes labelled by variables
- Output: value computed by sink

Size = # nodes
Depth = length of longest path

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

Almost all functions $f : \{0,1\}^n \to \{0,1\}$ are maximally hard — require circuit size $\Omega(2^n/n)$

Best lower bounds for explicit functions $5n - o(n)$

So look at restricted models
(a) monotone circuits (no NOT gates)
(b) Bounded (constant) depth
(c) Bounded depth + "counting gates"

Exponential lower bounds for (a) and (b)
Case (c) is at the research frontier

So get stuck already for fairly weak models...

But quite some exciting developments in last few years (though still for weak models)

Plan for today: Focus on (b).

Every Boolean function computable by CNF / DNF formula of exponential size
– depth-2 circuits

For depth 2 also not too hard to prove exponential lower bounds

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

Recall

AC^0: Circuits with
- constant depth
- Unbounded fan-in AND & OR

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

THM 1 [Furst, Saxe, Sipser '81, Ajtai '83]
PARITY $\notin AC^0$

In fact, circuits of bounded depth must have exponential size — proven by Johan Håstad (but we won't try to prove optimal result today)

MAIN TOOL: RANDOM RESTRICTIONS

Pick random subset of variables

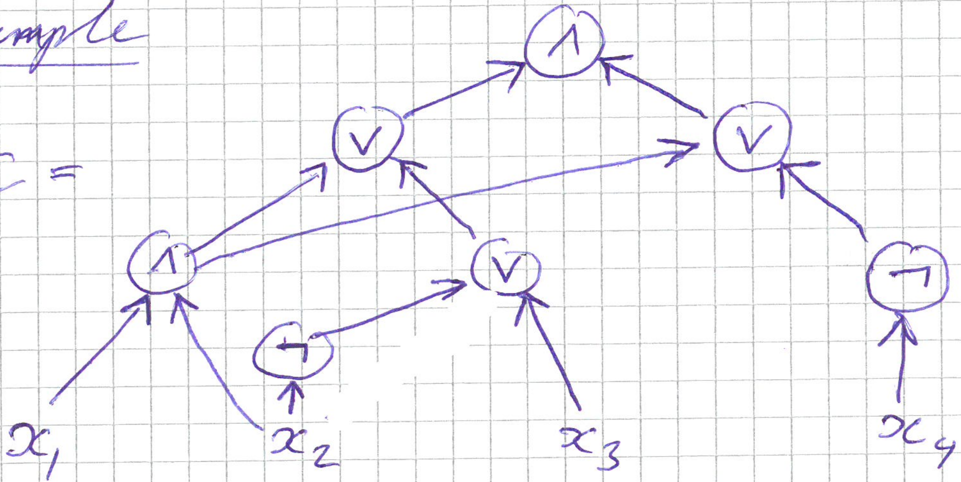
Set to random values 0/1

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

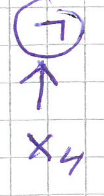
$C =$



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

$C\restriction_\rho$ = Circuit C restricted by ρ

$=$



For $\rho' = \{ x_2 \mapsto 0, x_4 \mapsto 1 \}$ get constant $C\restriction_{\rho'} \equiv 0$.

HIGH-LEVEL IDEA

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

(2) Choose random subset of (most) variables — all except n^ε for $\varepsilon > 0$ depending on d — restrict randomly, and simplify C_n

(3) Since C_n small and shallow circuit, such random restriction will collapse circuit to $C_n \restriction \rho \equiv$ constant

(4) But there are still n^ε unassigned variables, which can all flip value of parity function! ☹

$C \restriction \rho$ should still compute parity, or negation of parity, but not be constant. Contradiction.

Hence, no AC^0-circuits for PARITY, QED $\boxtimes$

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

$f \restriction \rho$ f restricted by ρ

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

$\boxed{Vars(\rho)}$ = set of variables assigned by ρ

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

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

LEMMA (HÅSTAD'S SWITCHING LEMMA)

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

Let ρ uniformly random restriction to t uniformly chosen variables.

Then $\forall s \geq 2$ it holds that

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

NB! - Not the way Håstad stated it

- Not optimal parameters

But good enough for us today...

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

Will use Switching lemma with parameters

$k = O(1)$

$s = O(1)$ $\quad \Rightarrow \Pr\left[f\restriction_{\rho} \text{ not } s\text{-CNF} \right] \lesssim n^{-c}$

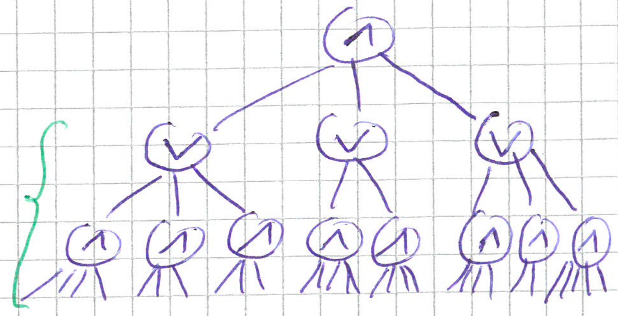
$t \approx n - \sqrt{n}$ $\quad$ for some constant $c > 0$

PLAN FOR REST OF TODAY

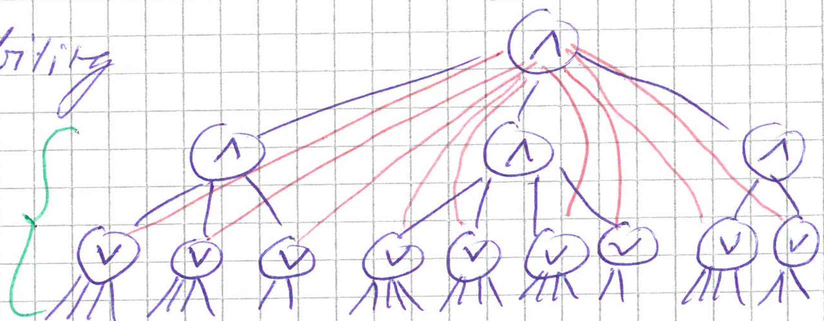
(1) Use switching lemma to prove PARITY $\notin AC^0$
(2) Prove switching lemma

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 by 1 to $d-1$

(iv) Repeat for $d-2$ steps $\Rightarrow$ get k-CNF or k-DNF formula

(v) Just fix k more variables to make disjunction false / conjunction true $\Rightarrow$ fixes value of circuit

(vi) But still unassigned variables left that can flip output value of function — Contradiction

Formal proof of Thm 1

Start with poly-size AC^0 circuit of depth d

Do initial preprocessing to get circuit s.t.

(a) fan-out of all gates is 1 (i.e., circuit DAG is a tree; the circuit is a formula)

(b) all ~~NOT~~ NOT-gates are right above the input level (applied to variables only)

(c) AND- and OR-gates alternate (at each level only $\wedge$ or $\vee$) and wires only between consecutive layers

(d) Right above input literals (variables plus possible negations) have AND-gates with fan-in 1

CLAIM This preprocessing can be done without increasing the depth except by $+O(1)$ and blowing up the size only polynomially

Proof Exercise.

Suppose resulting circuit has depth d and $\leq n^b$ gates

Let $n_0 = n = \#$variables

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
- Keep bottom layer at constant fan-in

VIII

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

Let $k_i = 10\,b \cdot 2^i \quad (= O(1))$

Show that whp after ith restriction have depth-$(d-i)$ circuit with $\leq k_i$ fan-in at bottom level

Suppose for simplicity bottom layer of gates $\wedge$-gates, level above $\vee$-gates (opposite case entirely symmetric)

By assumption each such $\vee$-gate computes k_i-DNF

Use Håstad's switching lemma with

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

For a fixed $\vee$-gate, k_i-DNF turns into k_{i+1}-CNF <u>except</u> with probability

some constant $\leq k_d^{10k_d}$

$$\left(\frac{n^{1/2^{i+1}} \cdot k_i^{10}}{n^{1/2^i}} \right)^{k_{i+1}/2} \leq K \cdot \left(n^{-1/2^{i+1}} \right)^{k_{i+1}/2}$$
$$\leq n^{-\frac{5}{2}b}$$
$$\leq \frac{1}{10\, n^{b}}$$

for n large enough

If this happens for all $\vee$-gates in next-to-bottom layer, can collapse $\wedge$-gates with $\wedge$-gate above

$\Longrightarrow$ depth reduces by 1

fan-in $k_{i+1} = O(1)$

k_{i+1} - CNFs

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

Note that we only consider each gate once, so perform "collapsing experiment" at most n^6 times

Proof fails if $\exists$ circuit gate where collapse does not happen

Look at random restriction ρ sampled as before

$$
\begin{aligned}
&\Pr[\rho \text{ fails to collapse } C] \\
&\leq \Pr[\exists \text{ gate } v \text{ s.t. } \rho \text{ fails to collapse } v] \\
&\leq \sum_{v \text{ gate}} \Pr[\rho \text{ does not collapse } v] \\
&\leq [\text{UNION BOUND}] \quad n^6 \cdot \frac{1}{10 n^6} = \frac{1}{10}
\end{aligned}
$$

So whole process works with 90% probability. Means, in particular, that

$\exists$ one good ρ^* that after $d-2$ steps collapses C to k_{d-2}-CNF or k_{d-2}-DNF.

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

But still $n^{1/2^{d-1}} - k_{d-2} > 0$ variables left, so function is not constant.

Hence the circuit cannot have been computing parity, which proves the lower bound $\blacksquare$

Maybe felt complicated, but once you digest the argument it is straightforward. The hard part of the proof is the switching lemma.

Original proof technique technically fairly complicated

Will use most intuitive technique developed by Razborov

$\boxed{\text{MINTERM}}$ partial assignment ρ fixing $f|_\rho \equiv 1$

$\boxed{\text{MAXTERM}}$ partial assignment ρ fixing $f|_\rho \equiv 0$

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

Every disjunction in k-CNF is (negation of) maxterm of size k

Assume we pick minterms and maxterms minimal

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

Proof Exercise.

Hence, if $f\restriction_\rho$ is not an s-CNF, then it has a ~~maxterm~~ minimal maxterm of size $\geq s+1$

Focus on analyzing this probability

Let us write

$\boxed{R_t} :=$ { all restrictions on t variables }

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

Actually, for which $f\restriction_\rho$ has maxterm of size $\geq s+1$

$\boxed{B} :=$ { bad restrictions ρ for which $f\restriction_\rho$ not s-CNF }

(Note that f is a fixed, known Boolean function for the rest of this argument)

Random restriction ρ will succeed to switch k-DNF f to s-CNF $f\restriction_\rho$ with probability

$$\geq 1 - \frac{|B|}{R_t}$$

We want to prove $|B|$ small compared to $|R_t|$

Do this by constructing one-to-one (injective) mapping

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

for $\ell = O(s \log k)$. Then we get

$$\frac{|B|}{|R_t|} \leq \frac{|R_{t+s} \times \{0,1\}^{\ell}|}{|R_t|} =$$

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

If t close to n, then $\binom{n}{t} \gg \binom{n}{t+s}$

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

$\left[\begin{array}{l} k, s \text{ constants} \\ t \text{ close to } n \end{array}\right]$

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

Looks kind of like what we are after in the switching lemma!

CLAIM C The above handwaving can be worked out to prove the bound (*) in Håstad's switching lemma.

Proof Show that for $t \geq n/2$ it holds that

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

by first proving

$$\binom{n}{t+s} = \binom{n}{t}\binom{n-t}{s} \Big/ \binom{t+s}{t}$$

and then using

$$\left(\frac{n}{k}\right)^k \leq \binom{n}{k} \leq \left(\frac{en}{k}\right)^k$$

The details are left as an exercise.

So we are done if we can construct one-to-one mapping

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

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

No term in k-DNF becomes 1

Some terms might turn 0, but not all

Know $f\restriction_\rho$ has some minimal maxterm π of size $> s$

Since f is k-DNF, this tells us a lot about structure of ρ – can "compress" encoding

XIV

From now on, let $\boxed{\rho\pi}$ denote union of restrictions ρ and π for $Vars(\rho) \cap Vars(\pi) = \emptyset$
(so that $\rho\pi$ is also truth value assignment)

Look at $\rho\pi$ for $\rho \in \mathcal{B}$ and π minimal maxterm of size $> s$

Design mapping from ρ to $\rho\sigma \in R_{s+t}$

Add extra info so that $\rho\pi$ and π can be recovered from $\rho\sigma$
$\Rightarrow$ can also recover ρ uniquely
$\Rightarrow$ mapping is one-to-one

Fix representation of f as k-DNF
- order terms in some fix order
- in each term, order literals in fixed order

$\rho\pi$ sets f to 0 (by construction)
ρ does not (by assumption)

Look at first term (= conjunction) t_1 not falsified by ρ

Let $\boxed{Y_1 := Vars(t_1) \cap Vars(\pi)} \neq \emptyset$

Write $\boxed{\pi_1}$ to denote assignment to Y_1 that coincides with π

Let $\boxed{\sigma_2}$ unique assignment to Y_1 that does not falsify ~~satisfies~~ t_1 — will be part of $\rho\sigma$

Also compute extra information

$\boxed{s_1 := |Vars(\pi_1)|} = |Vars(\sigma_1)|$

Let c_1 be string that contains

- s_1
- indices of these variables in t_1 (according to our fixed order)
- values assigned by π_1

At most k variables in term t_1

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

Continue for $i = 2, 3, \ldots$ At start of step $i+1$ we have defined

$\pi_1, \ldots, \pi_i \subsetneq \pi$

$\sigma_1, \ldots, \sigma_i$

Find first term t_{i+1} not falsified by $\rho\pi_1 \cdots \pi_i$

$Y_{i+1} := (Vars(t_{i+1}) \cap Vars(\pi)) \setminus Vars(\rho\pi_1 \cdots \pi_i)$

π_{i+1} := assignment to Y_{i+1} coinciding with π

σ_{i+1} := unique assignment to Y_{i+1} ~~satisfying~~ not falsifying t_{i+1}

Stop when $\pi_1 \cdots \pi_m$ assigns $\geq s$ variables

Then trim down π_m to get size exactly $= s$

c_{i+1} contains

- $s_{i+1} = |Vars(\pi_{i+1})| = |Vars(\sigma_{i+1})|$
- indices of variables in t_{i+1}
- values assigned by π_{i+1}

Final mapping m

Map $\boxed{\rho}$ to $\boxed{(\rho \overbrace{\sigma_1 \cdots \sigma_m}^{\sigma}, \overbrace{c_1 \cdots c_m}^{c})}$

size of $c = c_1 \cdots c_m$

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

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

WE ARE DONE IF WE CAN:

Argue that m is one-to-one

Given $(\rho\sigma, c)$, want to recover ρ

Note that $\rho\sigma$ is just one big restriction — we have no idea which variables come from where

Find first term t_1 not falsified by $\rho\sigma$

Then ρ doesn't falsify t_1 (but also doesn't satisfy — why?)

σ_1, whatever it is, doesn't falsify t_1 by construction

σ_i for $i > 1$ don't assign to $Vars(t_1)$

Now look up info in $c_1 \in c$

Find variables in t_1 assigned by π_1 & σ_1

Read off values assigned by π_1

Use this info to modify

$$\rho\sigma = \rho\,\sigma_1\,\sigma_2 \cdots \sigma_m$$

to $$\rho\,\pi_1\,\sigma_2 \cdots \sigma_m$$ ← which falsifies term t_1 by construction

Continue — find t_2 first term not falsified by $\rho\,\pi_1\,\sigma_2 \cdots \sigma_m$

Use c_2 to find variables in t_2 and read off assignment π_2

Use this to modify

$$\rho\,\pi_1\,\sigma_2\,\sigma_3 \cdots \sigma_m$$

to $$\rho\,\pi_1\,\pi_2\,\sigma_3 \cdots \sigma_m$$

(which falsifies t_2 by construction)

At the end recover all of

$\rho\,\pi_1 \cdots \pi_m$ and $\pi_1 \cdots \pi_m$

$\Longrightarrow$ read off ρ

$\Longrightarrow$ mapping is one-to-one as claimed

The lemma follows $\blacksquare$