Circuit Complexity and Natural Proofs

NOEL ARTECHE
(Lund University)

META-COMPLEXITY PROJECT – ILLC, Amsterdam
(January 2024)

Plan for today

PART I : Circuit lower bounds
— what they are and what we unconditionally know

PART II : The Natural Proofs Barrier
— and efforts to overcome it

Why care about circuits?

(Well, P vs. NP obviously?)

Theorem. (Baker-Gill-Solovay, 1975)
There exist oracles A and B such that:
(i) $P^A = NP^A$
(ii) $P^B \neq NP^B$.

"P vs. NP DOES NOT relativize"

"computation in our universe is local but Turing machines are opaque"

"we need a simple, concrete, transparent model"

Our friend : the CIRCUIT

- ✓ Transparent (obvious complexity : SIZE, DEPTH)
- ✓ Concrete (no imaginary infinite tapes)
- ✓ Simple (just a labelled graph)

Our ~~friend~~ enemy: the CIRCUIT ($P/poly$)

✓ Transparent (obvious complexity: SIZE, DEPTH)

✓ Concrete (no imaginary infinite tapes)

✓ Simple (just a labelled graph)

✗ Sneaky (non-uniformity)

✗ Messy (nobody wants to program a graph)

✗ Hard (some of the hardest open combinatorics problems ever conceived)

Some reminders

A language $L \subseteq \{0,1\}^*$ is in P/poly if there is a sequence of circuits $\{C_n\}_{n \in \mathbb{N}}$ s.t.

- C_n computes $L_n := \{x \in \{0,1\}^n \mid x \in L\}$
- $|C_n| \leq n^{O(1)}$.

⚠ Recall $P \subsetneq P/poly$!

non-uniform unless mentioned otw.

Other classes that matter: $\left.\begin{matrix} SIZE(n^k) \\ DEPTH(f(n)) \end{matrix}\right\}$

GOOD NEWS : Our enemy is weak! Almost all of the time!

Theorem. (Shannon, 1949)
All but a $o(1)$ fraction of all Boolean function require circuit size $\geq 2^n/n$.

BAD NEWS : Absolutely no idea which functions are truly hard!

The best size lower bound for $f \in NP$ is like $3.1n$ (or $5n - o(1)$)
For formulas, $\sim n^3$

The Problem of Explicit Constructions

Provide a concrete function (e.g. in NP) that requires high circuit complexity.

↳ Even better: provide an efficient algorithm A that describes such a function.

$$A(1^n) = f$$

f: truth table over $\log n$ bits requiring circuit complexity $> n/\log n$ (cf. $2^n/n$)

This would imply

$NP \not\subseteq P/poly \Rightarrow P \neq NP$!

But what about MCSP?

$$MCSP := \{ (f, s) \mid \text{the truth table } f \text{ has circuits of size} \leq s \}$$

The Holy Grail of Meta-Complexity: $SAT \leq_p MCSP$

i.e. a poly-time $R(\varphi) = (f_\varphi, s_\varphi)$ so that

$$\varphi \in SAT \quad \text{iff} \quad (f_\varphi, s_\varphi) \in MCSP$$

Then,

$$R\left(\bigvee_{i=1}^{n} x_i \wedge \neg x_i \right) = (f_n, s_n)$$

is solving* the problem of explicit constructions

* unless R is really weird...

Making life easier

a) Choose a REALLY HARD FUNCTION!

↳ Like in NEXP, or 3-EXP or something...

Not very concrete...

Kannan's Theorem

[Actually, we know for all $k \in \mathbb{N}$,
there exists $L \in \Sigma_2 P \setminus SIZE(n^k)$

↳ But it is NOT a very concrete function...

b) Choose a REALLY STUPID CIRCUIT MODEL!

↳ Don't allow negations (ie. monotone circuits)
or restrict depth to constant (i.e. AC^0).

The Fable of Circuit Complexity

(a.k.a. the circuit complexity program ca. 1980)

Recall:

- NC^i: fan-in 2, depth $O(\log^i n)$
- AC^i: unbounded fan-in, depth $O(\log^i n)$

$$AC^0 \subseteq AC^0[p] \subseteq ACC^0 \subseteq TC^0 \subseteq NC^1 \subseteq L \subseteq NL \subseteq AC^1 \subseteq NC^2 \subseteq P \subseteq NP$$

- $AC^i[p]$: AC^i with MOD_p gates

$$ACC^i := \bigcup_{p \in \mathbb{N}} AC^i[p]$$

Structural Complexity vs. Concrete Complexity

Razborov 1985
Andreev 1985
Alon-Boppana 1987

MONOTONE CIRCUITS

$NP \not\subseteq mP$

Concrete hard function example:
- $Clique_{n,k}$
- Perfect Matching

Furst-Saxe-Sipser 1981
Ajtai 1983
Håstad 1986

CONSTANT-DEPTH CIRCUITS

$NP \not\subseteq AC^0$

Concrete hard function example:
PARITY
(a.k.a. MOD 2)

Razborov 1986
Smolensky 1986

CONSTANT-DEPTH CIRCUITS WITH COUNTING MOD p

$NP \not\subseteq AC^0[p]$

Concrete hard function example:
MOD q
(for $p \neq q$ primes)

Razborov 1985
Andreev 1985
Alon-Boppana 1987

MONOTONE CIRCUITS

$NP \not\subseteq mP$

Concrete hard function example:
- $Clique_{n,k}$
- Perfect Matching

Removing negations : Monotone Circuits (mP)

The $\wedge$ and $\vee$ functions are **monotone** :

$$x \leq y \implies f(x) \leq f(y)$$

$1001 \leq 1011 \implies f(1001) = 0 \mapsto f(1011) \neq 0$ ✓

$1001 \leq 1011 \implies f(1001) = 1 \mapsto f(1011) = 0$ ✗

Prop. If C is a monotone circuit, then the function computed by it must be monotone.

↳ **Corollary.** Parity $\notin$ mP. (But that's not very interesting...)

Q : Are there interesting functions computable by Monotone Circuits?

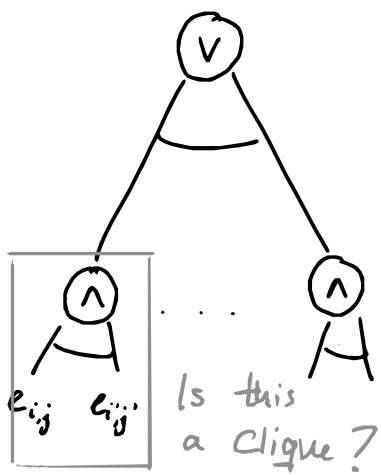
Q: Are there interesting functions computable by MONOTONE CIRCUITS?

YES!

The $\text{Clique}_{n,k}$ function is monotone, concrete and it's NP-complete!

Encode a graph $G = ([n], E)$ with n^2 variables $e_{i,j}$, such that $e_{i,j} = 1$ iff $(i,j) \in E$.

$$\text{Clique}_{n,k}(G) = \bigvee_{\substack{S \subseteq [n] \\ |S| = k}} \bigwedge_{\substack{i,j \in S \\ i \neq j}} e_{i,j}$$



The trivial circuit has size $\Theta(n^k)$...
and you cannot do much better!

Theorem. (Razborov '85, Alon-Boppana '87)
For $k \leq \log n$, every monotone circuit computing $\text{Clique}_{n,k}$ requires size $n^{\Omega(k)}$.

Corollary. For $k = \log n$, $n^{\Omega(\log n)}$ is SUPER-POLYNOMIAL!
So this is a super-polynomial lower bound for a concrete function in NP, as long as we disallow negation!

PROOF TECHNIQUE: Razborov's METHOD of APPROXIMATIONS.

The Method of Approximations

Let C be a small circuit for $f : \{0,1\}^n \to \{0,1\}$.

1) Replace $\wedge$ and $\vee$ in C by the "approximants": $\tilde{\wedge}$, $\tilde{\vee}$.

2) Argue that $\tilde{\wedge}, \tilde{\vee}$ make few mistakes!

3) So $\tilde{C}$ must be very closely approximating f!

4) But actually $\tilde{\wedge}, \tilde{\vee}$ are so stupid that $\tilde{C}$ has a lot of structure... we can rule out small $\tilde{C}$ circuits unconditionally!

↳ CONTRADICTION! C must be large. QED

Q: Can we turn GENERAL CIRCUITS into MONOTONE ones (i.e. removing negation + some clean-up)?

No!

Theorem. (Tardos '88)
PERFECT MATCHING requires monotone circuits of super-polynomial size, but it is in P.
That is,

$$\mathrm{Mon} \cap \mathrm{P} \not\subseteq \mathrm{mP}.$$

This does work for SLICE FUNCTIONS...
but we don't know how to prove anything for those...

"The Mystery of Negation" (Jukna, ch. 10)

① Negation are weirdly useful...

Example: triangle detection $\equiv$ $\text{Clique}_{n,3}$

↳ Monotone circuit size $\Omega(n^3)$.

But with negation... $O(n^{2.37\ldots})$!

② Negation break the method of approximation.

Theorem. (Razborov 1989)

Any lower bound for GENERAL CIRCUITS proven via the APPROXIMATION METHOD is of at most $O(n^2)$.

Razborov 1985
Andreev 1985
Alon-Boppana 1987

MONOTONE CIRCUITS

$NP \not\subseteq mP$

Concrete hard function example:
- $Clique_{n,k}$
- Perfect Matching

Razborov 1985
Andreev 1985
Alon-Boppana 1987

MONOTONE CIRCUITS

$NP \not\subseteq mP$

Concrete hard function example:
- $Clique_{n,k}$
- Perfect Matching

Furst-Saxe-Sipser 1981
Ajtai 1983
Håstad 1986

CONSTANT-DEPTH CIRCUITS

$NP \not\subseteq AC^0$

Concrete hard function example:
PARITY
(a.k.a. MOD 2)

Constant-depth circuits : AC^0

For $x \in \{0,1\}^n$, $\text{PARITY}(x) := \sum_{i=1}^{n} x_i \pmod 2$.

Theorem (Furst-Saxe-Sipser '81, Ajtai '83, Håstad '86)
Every depth-d circuit computing PARITY requires size $2^{\Omega(n^{1/d})}$. Thus, $\text{PARITY} \notin AC^0$.

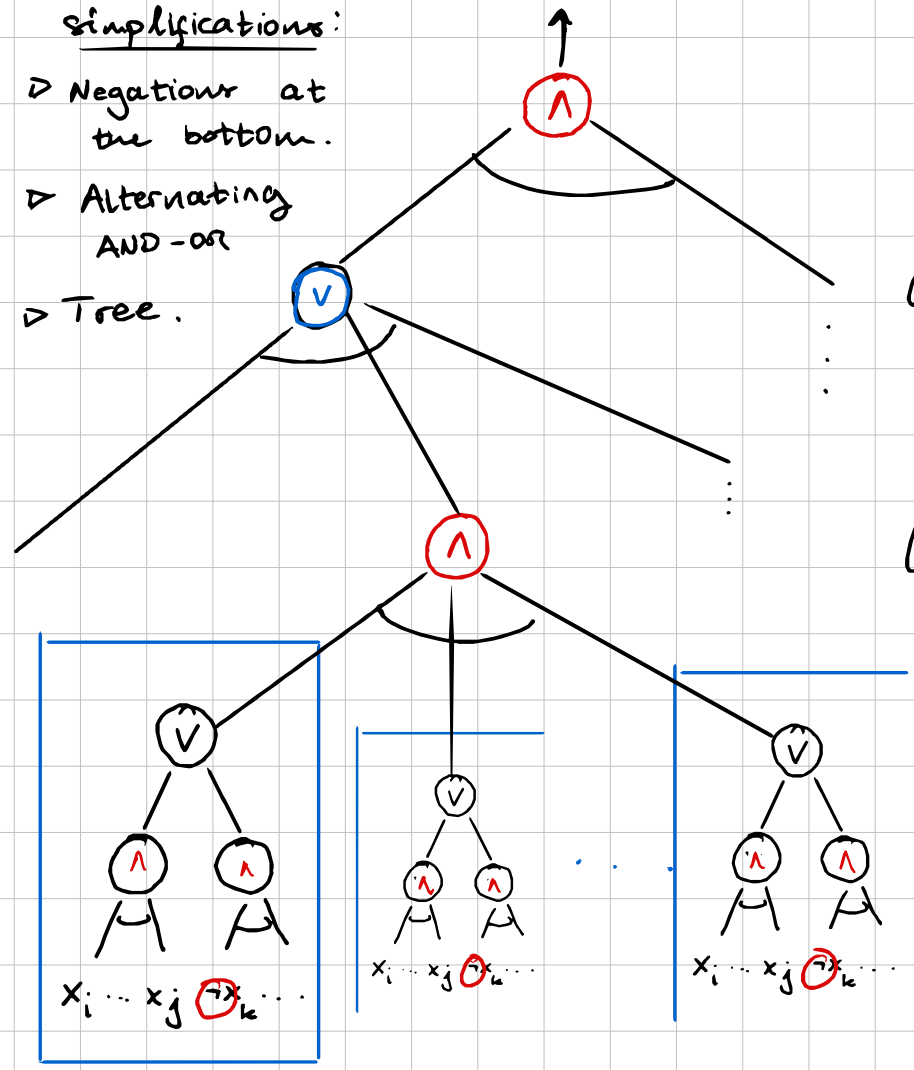
PROOF TECHNIQUE : "the method of RANDOM RESTRICTIONS".

↓

key Ingredient : Switching Lemma

Some inoffensive simplifications:

- ▷ Negations at the bottom.
- ▷ Alternating AND-OR
- ▷ Tree.



(depth 0)

(depth 1)

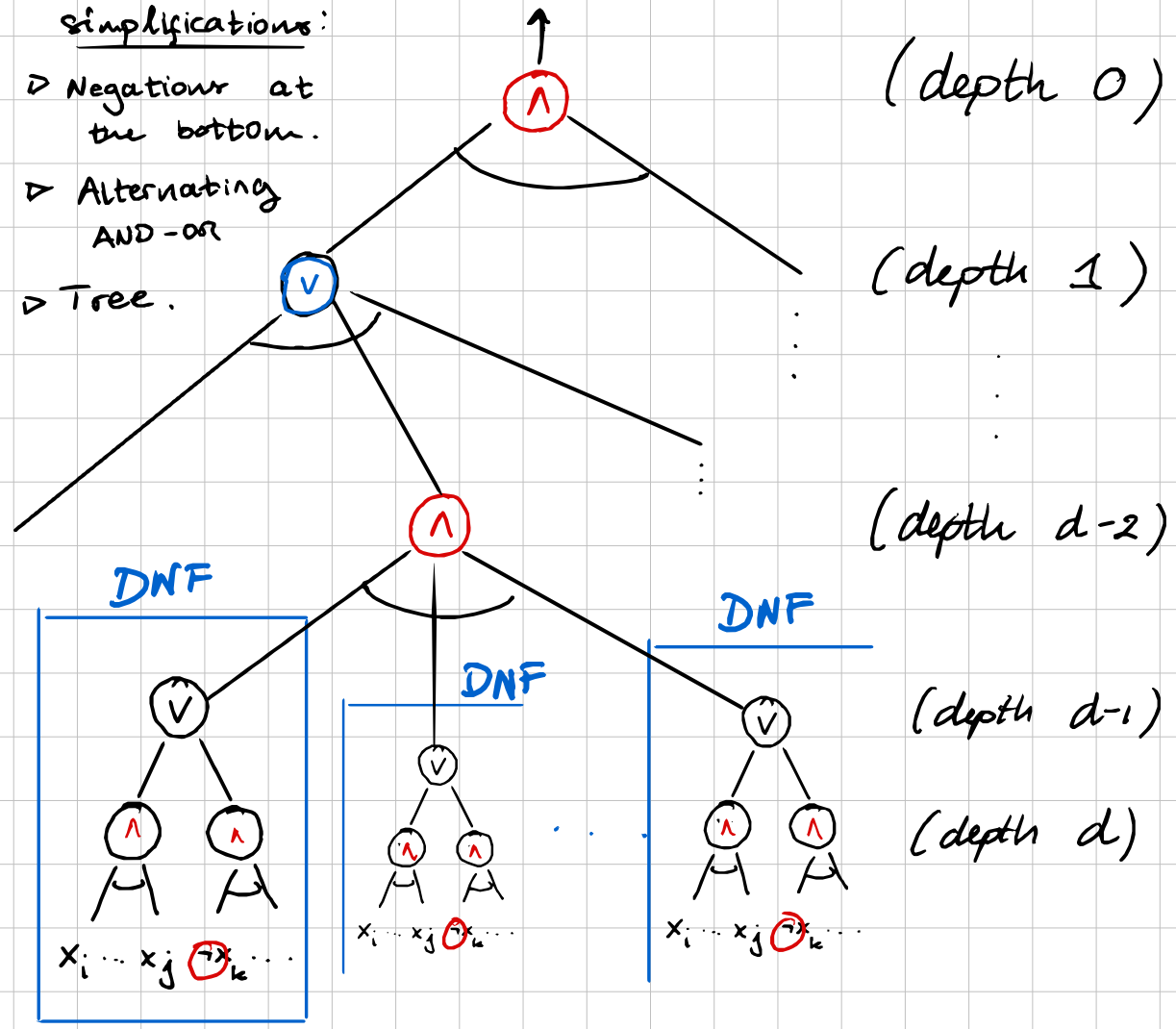
(depth d-2)

(depth d-1)

(depth d)

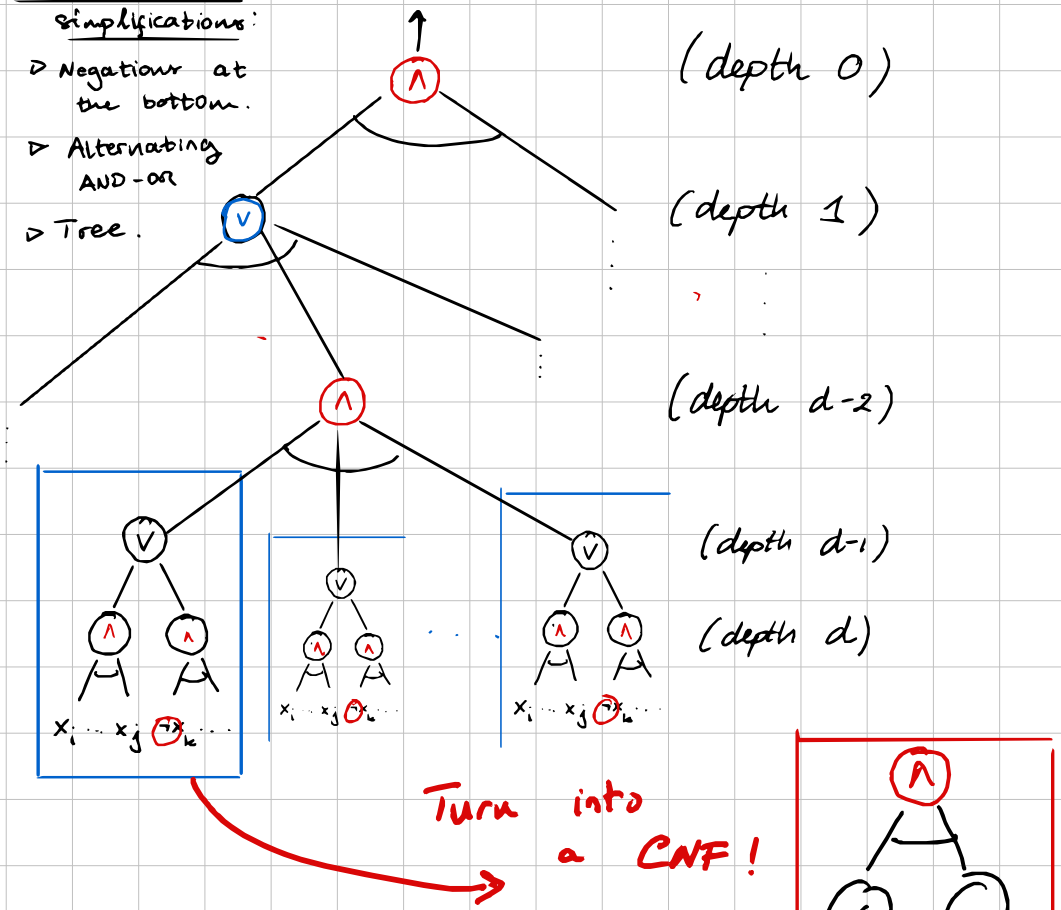
Some inoffensive simplifications:

- Negations at the bottom.
- Alternating AND-OR
- Tree.



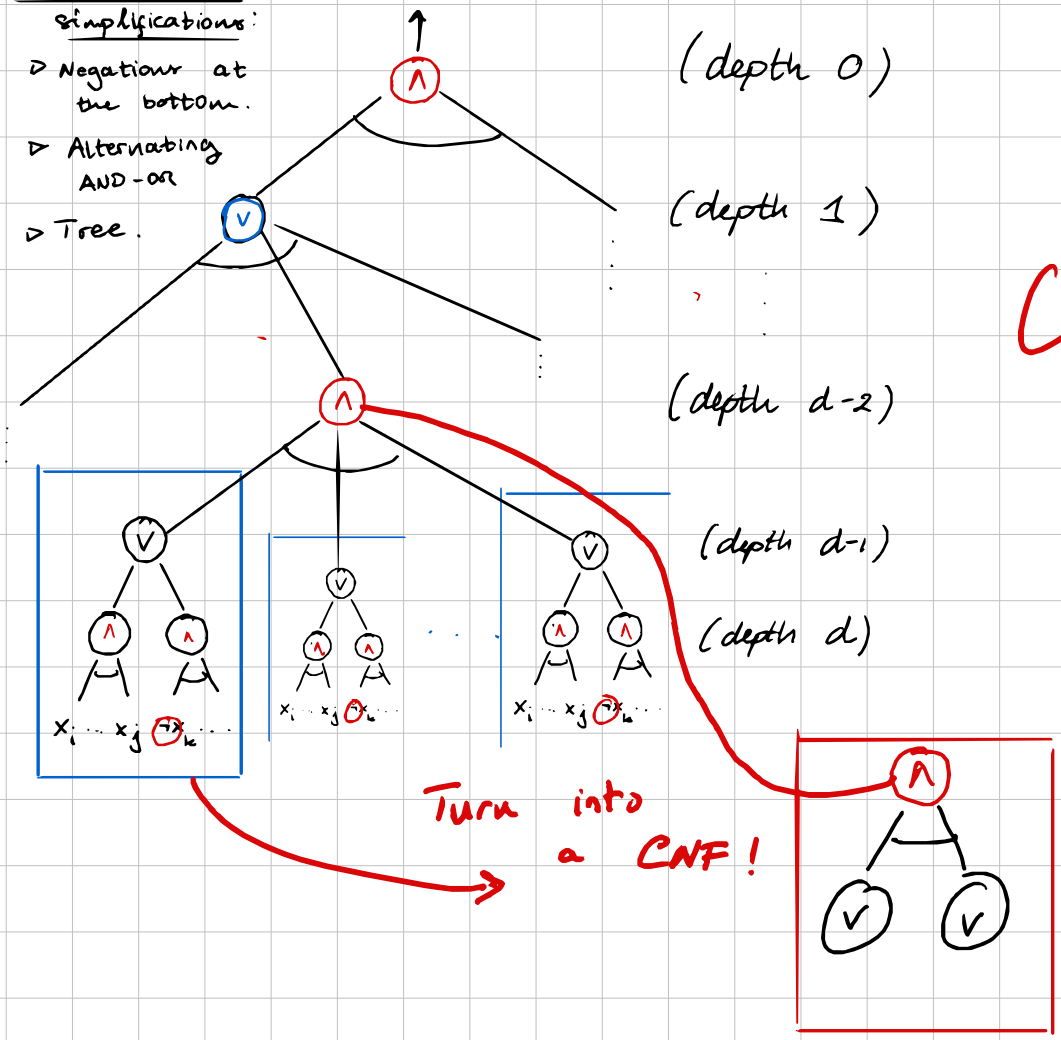
Some inoffensive simplifications:

- Negations at the bottom.
- Alternating AND-OR
- Tree.



Some inoffensive simplifications:

- Negations at the bottom.
- Alternating AND-OR
- Tree.



CNF φ $\xrightarrow{?}$ DNF $\varphi' \equiv \varphi$

n variables $\quad$ n variables

In general, φ' may grow too large.

But we could fix some values and simplify...

Håstad's Switching Lemma. (1986)

Let φ be a k-DNF over n variables, and let $R \subseteq \{0,1,*\}^n$ be the set of partial restrictions assigning at most $\alpha \cdot n$ variables, for $\alpha \leq 1/7$.

Then,

$$\Pr_{\rho \sim R}\left[\varphi|_\rho \text{ has a } k\text{-CNF of size } s\right] \geq 1 - (7\alpha k)^s$$

Theorem. If C is an AC^0 circuit, then there exists a strictly partial restriction that makes the circuit constant.

⚠ But PARITY is NOT mode constant by fixing a small number of inputs!

Corollary. PARITY $\notin AC^0$.

Nice corollary for logicians

↳ DESCRIPTIVE COMPLEXITY

An input $x \in \{0,1\}^n$ can be encoded into the first-order structure $A(x) := ([n], X, <)$ where

- $X(i)$ is true iff $x_i = 1$
- $<$ is the usual order on $[n]$

A language $L \subseteq \{0,1\}^*$ is in **FO** if there is a first-order sentence φ such that for all $x \in \{0,1\}^*$,

$$x \in L \iff A(x) \models \varphi.$$

Fact. $\mathbf{AC^0} = \mathbf{FO}$.

↑ uniform

Corollary. PARITY $\notin$ FO.

↳ i.e. PARITY is not expressible in first-order logic

↳ **Theorem.** (Murray-Williams '17)

If MCSP is NP-hard under uniform AC^0-reductions, then NP $\not\subseteq$ P/poly and P = BPP.

↓

But SAT is NP-hard under such reductions!

↓

"reductions describable in first-order logic"

Razborov 1985
Andreev 1985
Alon-Boppana 1987

MONOTONE CIRCUITS

$NP \not\subseteq mP$

Concrete hard function example:
- $Clique_{n,k}$
- Perfect Matching

Furst-Saxe-Sipser 1981
Ajtai 1983
Håstad 1986

CONSTANT-DEPTH CIRCUITS

$NP \not\subseteq AC^0$

Concrete hard function example:
PARITY
(a.k.a. MOD 2)

Razborov 1985
Andreev 1985
Alon-Boppana 1987

MONOTONE CIRCUITS

$NP \not\subseteq mP$

Concrete hard function example:
- $Clique_{n,k}$
- Perfect Matching

Furst-Saxe-Sipser 1981
Ajtai 1983
Håstad 1986

CONSTANT-DEPTH CIRCUITS

$NP \not\subseteq AC^0$

Concrete hard function example:
PARITY
(a.k.a. MOD 2)

Razborov 1986
Smolensky 1986

CONSTANT-DEPTH CIRCUITS WITH COUNTING MOD p

$NP \not\subseteq AC^0[p]$

Concrete hard function example:
MOD q
(for $p \neq q$ primes)

Constant-depth with counter : $AC^0[p]$

Theorem. (Razborov - Smolensky '86)
Let p and q be two distinct primes.
Then, $MOD_q \notin AC^0[p]$.

So, in particular, $AC^0[2]$ cannot count mod 3.

⚠ If p is not a prime or a prime power, then we know nothing... As far as we know, $NP \subseteq AC^0[6]$ is possible!

PROOF TECHNIQUE : the METHOD of APPROXIMATIONS (again)!

The Frontier

Razborov 1985
Andreev 1985
Alon-Boppana 1987

MONOTONE CIRCUITS

$NP \not\subseteq mP$

Concrete hard function example:
- $Clique_{n,k}$
- Perfect Matching

Furst-Saxe-Sipser 1981
Ajtai 1983
Håstad 1986

CONSTANT-DEPTH CIRCUITS

$NP \not\subseteq AC^0$

Concrete hard function example:
PARITY
(a.k.a. MOD 2)

Razborov 1986
Smolensky 1986

CONSTANT-DEPTH CIRCUITS WITH COUNTING MOD p

$NP \not\subseteq AC^0[p]$

Concrete hard function example:
MOD q
(for $p \neq q$ primes)

?

CONSTANT-DEPTH CIRCUITS WITH ALL COUNTERS

$NP \not\subseteq ACC^0$

where

$ACC^0 := \bigcup_{p \in \mathbb{N}} AC^0[p]$

Part II

The Natural Proofs Barrier

and Beyond

'Modus operandi' of circuit complexity

1. Choose a circuit model C.
2. Choose a concrete candidate function f.
3. Identify a WEAKNESS of C.
4. The function f is not affected by the weakness.

Q: Which WEAKNESSES did we exploit so far?

Remember!

Theorem. If C is an AC^0 circuit, then there exists a strictly partial restriction that makes the circuit constant.

WEAKNESS!

⚠ But PARITY is NOT made constant by fixing a small number of inputs!

WEAKNESS = COMBINATORIAL PROPERTY

Razborov-Rudich '94: "Too simple" combinatorial properties cannot yield strong lower bounds!

What is "too simple" about a property P?

1. "Easy to detect"
   ↳ You can decide in polynomial time whether a function satisfies P, given its truth table.

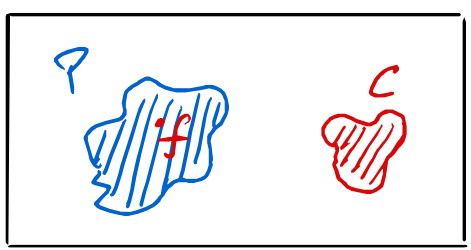
2. "Pretty common"
   ↳ There's a large amount of functions satisfying P — it's nothing very rare.

What is ~~"too simple"~~ NATURAL about a property P?

CONSTRUCTIVENESS

1. ~~"Easy to detect"~~
   ↳ You can decide in polynomial time whether a function satisfies P, given its truth table.

2. ~~"Pretty common"~~ LARGENESS
   ↳ There's a large amount of functions satisfying P — it's nothing very rare.



The space of all n-bit functions $\{0,1\}^{2^n}$
↳ 2^{2^n} possible functions

Natural Properties

A property $\mathcal{P}$ is a NATURAL PROPERTY USEFUL AGAINST $\mathbf{SIZE}(n^k)$ if it satisfies

(i) CONSTRUCTIVENESS. Given a 2^n-sized truth table for f, deciding whether $\mathcal{P}(f) = 1$ can be done in time $2^{O(n)}$ — so polynomial time!

(ii) LARGENESS. $\Pr_{f \sim \{0,1\}^{2^n}} [\mathcal{P}(f) = 1] \geq 1/\text{poly}(2^n)$

(iii) USEFULNESS. $f \in \mathbf{SIZE}(n^k) \Rightarrow \mathcal{P}(f) = 0$.

In general, a property $\mathcal{P}$ could be **$\mathcal{C}$-natural and useful against $\mathcal{D}$.**

(e.g. The weakness for AC^0 circuits is AC^0-natural and useful against AC^0

Razborov-Rudich '94: "All known circuit lower bounds NATURALIZE"

↳ you can find a corresponding natural property in the proof

However...

Theorem. Suppose there exists a subexponentially-secure one-way function. Then, there is NO P/poly-natural property useful against P/poly.

↳ (!) Unconditional impossibility for DISCRETE LOG!

Key Idea: A natural property is a DISTINGUISHER!

"What we are saying, subject to the truth of the cryptographic conjecture, is this: Any proof that some function does not have small circuits must either seize on some very specialized property of the function, or it must define a very complicated property, one outside the bounds of most mathematical experience."

— Razborov and Rudich, 1994

NO LARGENESS

NO CONSTRUCTIVENESS

Life after natural proofs...?

"We do not conclude that researchers should give up on proving serious lower bounds. Quite the contrary, [...] we hope to focus research on a more fruitful direction.

Pessimism will only be warrented if a long period of time passes without the discovery of a nonnaturalizing lower bound."

— Razborov & Rudich, '94

Barriers as logical independence

(!) Most lower bound arguments are provable within "poly-time reasoning" : $S^1_2 \subseteq PA$.

Theorem. (Razborov, 1996)

$S^2_2(\alpha) \nvdash$ "NP $\not\subseteq$ P/poly".

Theorem. (Razborov-Rudich '94, Krajíček '11)
Suppose strong OWF exist. Then, for any "reasonable" subsystem $T \subseteq PA$ with propositional feasible interpolation,

$T \nvdash$ "NP $\not\subseteq$ P/poly".

Theorem. (Razborov 2003/2015 – Annals of Mathematics)
The k-DNF Resolution proof system cannot prove "NP $\not\subseteq$ P/poly".

Some unnatural lower bounds

1. Santhanam 2007 : $\forall k \in \mathbb{N}$: $\mathrm{prMA} \not\subseteq \mathrm{SIZE}(n^k)$
   cf. $\mathrm{NP} \not\subseteq \mathrm{SIZE}(n^k)$

2. Diagonalization !

3. The Algorithmic Method

   ↳ Williams 2009 : $\mathrm{NEXP} \not\subseteq \mathrm{ACC}^0$

   (but $\mathrm{NP} \not\subseteq \mathrm{AC}^0[6]$ still open !)

Recap

- Circuit lower bounds are about "explicit construction"
- In the 80's the circuit complexity program had some success via COMBINATORIAL LOWER BOUNDS:

$$AC^0 \subsetneq AC^0[p] \subsetneq ACC^0 \subseteq \ldots \subseteq P \quad \text{and} \quad \mathbf{mNP} \not\subseteq \mathbf{mP}$$

- The Natural Proofs barrier tells us WHY progress stalled and $NP \not\subseteq P/poly$ seems far!
- Meta-complexity (i.e. MCSP) is, at its core, about the structural questions of circ. comp.