Recap

ACC^0$(m_1, \ldots, m_k)$ Constant-depth polynomial-size circuits with AND-, OR-, NOT-, and MOD_{m_i}-gates

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

Notation $x = (x_1, \ldots, x_n) \in \{0,1\}^n$

As usual, dimension n understood from context

Our focus ACC^0(3) — only MOD_3-gates

THEOREM $\boxed{\text{PARITY} \notin ACC^0(3)}$

Proof by Razborov–Smolensky

METHOD OF APPROXIMATIONS

(1) Show small circuits in ACC^0(3) well approximated by low-degree $\mathbb{F}_3$-polynomials

(2) Show that PARITY function cannot be approximated in this way

Did (1) last lecture

COROLLARY 7 For any circuit C over $\{\wedge, \vee, \neg, MOD_3\}$ of size s and depth d and for all $k \in \mathbb{N}^+$ there exists an $\mathbb{F}_3$-polynomial p_C of degree $\leq (2k)^d$ such that

$$\Pr_{x \sim \{0,1\}^n}\left[C(x) \neq p(x) \right] \leq \boxed{s/3^k}$$

Challenge: Exact representation of $\wedge$ and $\vee$ requires high degree

$OR_n(x)$ represented by

$$p(x) = 1 - \prod_{i=1}^{n} (1 - x_i)$$

(and not possible to do lower degree, though we did not prove this)

Solution: For random $v \in \mathbb{F}_3^n$

$\boxed{\left(\sum_{i=1}^{n} v_i x_i\right)^2}$ computes OR_n

with error probability $\boxed{\leq \frac{1}{3}}$ (over v, for all x)

Amplify success probability by taking k copies

$$p'(x) = 1 - \prod_{j=1}^{k} \left(1 - \left(\sum_i v_i^{(j)} \cdot x_i\right)^2\right)$$

has degree $2k$

error $\leq 1/3^k$

This lecture we will prove:

LEMMA 8 There exists constant $\delta > 0$ such that for n large enough it holds for all $\mathbb{F}_3$-polynomials p of degree $\leq \sqrt{n}$ that

$$\boxed{\Pr_{x \sim \{0,1\}^n}\left[p(x) \neq \mathrm{PARITY}(x)\right] \boxed{\geq \delta}}$$

Let us assume Lemma 8 and prove $\text{PARITY} \notin ACC^0(3)$

We know:

(1) For all $C \in ACC^0(3)$ of size s and depth d there is degree-$(2k)^d$ polynomial p such that

$$\Pr_{x \sim \{0,1\}^n}\left[C(x) \neq p(x) \right] \leq s/3^k$$

(2) There exists $\delta > 0$ such that if C computes PARITY, then for all polynomials p of degree $\leq \sqrt{n}$ it holds that

$$\Pr_{x \sim \{0,1\}^n}\left[C(x) \neq p(x) \right] \geq \delta$$

Choose k as large as possible so that

$$(2k)^d \leq \sqrt{n}$$

that is

$$\boxed{k := \frac{n^{\frac{1}{2d}}}{2}}$$

(technically speaking, we should round down to integer, but this doesn't matter and so we will be sloppy)

① and ② together now yield

$$\boxed{\delta \le \Pr_x\left[C(x) \ne p(x)\right] \le s/3^k}$$

or

$$s \ge \delta \cdot 3^k = \delta \cdot 3^{n^{1/2d}/2}$$
$$= \exp(\Omega(n^\gamma))$$

for some constant $\gamma > 0$ as long as $d = O(1)$. ▨

We just need to prove Lemma 8.
To do so, we will make a detour

DETOUR: Useful ways of thinking about Boolean functions

Usually

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

0	false
1	true

Can instead work in $\{-1, +1\}$

1	false
-1	true

$$\boxed{x_i \mapsto (-1)^{x_i}} = y_i \qquad \boxed{\tilde{f} : \{\pm 1\}^n \to \{\pm 1\}}$$

This is an affine transformation

$$y_i = 1 - 2x_i$$
$$x_i = \frac{1 - y_i}{2}$$

$$\tilde{f} = (-1)^f$$

$$\boxed{\widetilde{\mathrm{PARITY}}(y) = \prod_{i=1}^n y_i}$$

$$= \begin{cases} -1 & \text{if odd } \# y_i = -1 \\ +1 & \text{if even } \# y_i = -1 \end{cases}$$

OBSERVATIONS

(1) If $p(x)$ computes $f(x)$, then

$$\boxed{\tilde{p}(y) = 1 - 2p\left(\frac{1-y_1}{2}, \dots, \frac{1-y_n}{2}\right)}$$

computes $\tilde{f}(y)$

Doesn't change degree

(2) W.l.o.g. can represent functions

$$f : \{0,1\}^n \to \mathbb{F}_3$$

and
$$\tilde{f} : \{-1,+1\}^n \to \mathbb{F}_3$$

as $\boxed{\text{MULTILINEAR}}$ (a.k.a. SQUARE-FREE) POLYNOMIALS, i.e., degrees of individual variables ≤ 1

$$x_i \in \{0,1\} \implies x_i^2 = x$$
$$y_i \in \{\pm 1\} \implies y_i^2 = 1$$

FACT 9 Every $f : \{0,1\} \to \mathbb{F}_3$ has UNIQUE REPRESENTATION as multilinear $\mathbb{F}_3$ polynomial

Remark: Nothing special for $\mathbb{F}_3$ – holds for any field.

Proof: Multilinear monomials:

(a) 2^n of them
(b) span space of all functions $\{0,1\}^n \mapsto \mathbb{F}_3$
(c) this space has dimension 2^n

} so basis

For $\alpha \in \{0,1\}^n$, define

$$\boxed{I_\alpha(x) = \prod_{i:\alpha_i=1} x_i \prod_{j:\alpha_j=0} (1-x_j)}$$

$$I_\alpha(x) = \begin{cases} 1 & \text{if } x=\alpha \\ 0 & \text{otherwise} \end{cases}$$

$$\boxed{f(x) = \sum_{\alpha \in \{0,1\}^n} f(\alpha)\cdot I_\alpha(x)}$$

Clearly $I_\alpha(x)$ can be written as linear combination of monomials

Proves (b)

[Can also argue that monomials are linearly independent, but we don't need this since (span) + (dimension correct) $\Rightarrow$ basis]

$$\widetilde{PARITY}(y) = \prod_{i=1}^n y_i$$

Hence $\boxed{PARITY(x) = \dfrac{1 - \prod_{i=1}^n (1-2x_i)}{2}}$

This is the unique multilinear polynomial computing parity. DEGREE n

Clearly has monomial $\prod_{i=1}^n x_i$ — cannot be cancelled by other terms when product expanded

So representing PARITY exactly as $\mathbb{F}_3$ polynomial requires degree n

But we are only able to approximate so not yet done...

$\boxed{\text{END OF DETOUR}}$

Back to proof of Lemma 8

Suppose $p(x)$ approximates PARITY well. Then

$$\tilde{p}(y) = 1 - 2p\left(\frac{1-y_1}{2}, \dots, \frac{1-y_n}{2}\right)$$

approximates $\widetilde{\text{PARITY}}$ exactly as well

And the degree doesn't increase

If $\tilde{p}$ of degree d computes $\widetilde{\text{PARITY}}$ correctly on $\tilde{T} \subseteq \{\pm 1\}^n$ then this can be used to compute all functions

$$\tilde{f} : \{\pm 1\}^n \to \mathbb{F}_3$$

correctly in degree just $\frac{n}{2} + d$

This is surprisingly low degree... Suggesting that $\tilde{T}$ cannot be too large.

Let's first prove our claim formally.

LEMMA 10 Suppose for $\tilde{T} \subseteq \{\pm 1\}^n$ that exists degree-d polynomial $\tilde{p}$ such that

$$\boxed{\forall y \in \tilde{T} \quad \widetilde{PARITY}(y) = \tilde{p}(y)}.$$

Then for all

$$\tilde{f} : \{\pm 1\}^n \to \mathbb{F}_3$$

there is a degree-$\left(\frac{n}{2} + d\right)$ polynomial $\tilde{p}_{\tilde{f}}$ such that

$$\boxed{\forall y \in \tilde{T} \quad \tilde{f}(y) = \tilde{p}_{\tilde{f}}(y)}$$

Proof Note that for any $S \subseteq [n]$ it holds that

$$\boxed{\prod_{i \in S} y_i = \prod_{i \in [n]} y_i \cdot \prod_{i \in [n] \setminus S} y_i} \qquad (+)$$

$$= \prod_{i \in [n] \setminus S} y_i^2 \cdot \prod_{i \in S} y_i$$

$$= 1 \cdot \prod_{i \in S} y_i$$

Note also that the monomials

$$\left\{ \prod_{i \in S} y_i \;\middle|\; S \subseteq [n] \right\} \qquad (\ddagger)$$

form a basis for the space

$$\boxed{\left\{ \{\pm 1\}^n \to \mathbb{F}_3 \right\}}$$

also

Use what we proved before for

$\boxed{\{ \{0,1\}^n \to \{0,1\} \}}$ + affine transformation

Or argue directly with indicator functions

$$\tilde{I}_\beta(y) = \prod_i \left(1 - \frac{(y_i - \beta_i)^2}{4}\right)$$

for $\beta \in \{\pm 1\}^n$

$$\tilde{I}_\beta(y) = \begin{cases} 1 & \text{if } y = \beta \\ 0 & \text{otherwise} \end{cases}$$

So any $\tilde{f} : \{\pm 1\}^n \to \{\pm 1\}$ can be written as

$$\boxed{\tilde{f}(y) = \sum_{S \subseteq [n]} c_S \prod_{i \in S} y_i} \qquad (*)$$

for some constants $c_S \in \mathbb{F}_3$ by (#)

And for set $\tilde{T}$ we have that

$$\boxed{\tilde{p}(y) = \widetilde{PARITY}(y) = \prod_{i=1}^n y_i}$$

so for $y \in \tilde{T}$ we get

$$\boxed{\tilde{f}(y) = \sum_{\substack{S \subseteq [n] \\ |S| \leq n/2}} c_S \prod_{i \in S} y_i + \sum_{\substack{S \subseteq [n] \\ |S| > n/2}} c_S \tilde{p}(y) \prod_{i \notin S} y_i} \quad (**)$$

which is a polynomial of degree $\leq \frac{n}{2} + d$ that computes $\tilde{f}$ correctly on $\tilde{T}$ ∎

Let's continue proof of Lemma 8.

Assume $p: \{0,1\}^n \to \mathbb{F}_3$ polynomial of degree $\leq \sqrt{n}$ that agrees with PARITY on $T \subseteq \{0,1\}^n$

Then $\boxed{\tilde{p}}$ of degree $\leq \sqrt{n}$ agrees with $\widetilde{\text{PARITY}}$ on corresponding set $\boxed{\tilde{T} \subseteq \{\pm 1\}^n}$

And by Lemma 10 we can use $\tilde{p}$ to compute every $f: \{\pm 1\}^n \to \mathbb{F}_3$ correctly on $\tilde{T}$ using just $\left(\frac{n}{2} + \sqrt{n}\right)$-degree polynomial.

Time to look more closely at $\tilde{T}$ and do some counting

$\boxed{\#\text{ distinct functions}}$ when restricted to $\tilde{T}$ is

$$\left| \{ \tilde{T} \to \mathbb{F}_3 \} \right| = 3^{|\tilde{T}|} \qquad (1)$$

Every such function computed correctly on $\tilde{T}$ by distinct multilinear polynomial of degree $\leq \frac{n}{2} + \sqrt{n}$

How many such polynomials are there?

Spoiler alert: Not too many...

So $\tilde{T}$ cannot be too large.

Which is what Lemma 8 says.

CLAIM 22 The number of multilinear monomials of $\boxed{\text{degree} \leq \frac{n}{2} + \sqrt{n}}$ in n variables is

$$\left| \left\{ S \subseteq [n] \;\middle|\; |S| \leq \frac{n}{2} + \sqrt{n} \right\} \right| =$$

$$= \sum_{i=0}^{n/2+\sqrt{n}} \binom{n}{i} \boxed{\leq (1-\delta) 2^n}$$

for some $\delta > 0$ if n large enough

Why is this true?

MORALLY: Flip n coins. How many heads do we expect? $n/2$, of course.
Except we won't get exactly $n/2$

Standard deviation $\approx \sqrt{n}$
Means that with constant probability δ expect to see $\boxed{\geq \frac{n}{2} + \sqrt{n}}$ heads

Number of such outcomes $\geq$

$\geq \delta \cdot (\text{total \# outcomes}) = \delta \cdot 2^n$

But this is exactly the inequality above

PROVABLY Do the calculations...
Several different ways of doing this

Given Claim 11, # multilinear polynomials of degree $\leq \frac{n}{2} + \sqrt{n}$ is

$$(\#\text{coefficient options})^{\#\text{monomials}} \leq$$

$$\leq 3^{(1-\delta) 2^n} \qquad (2)$$

Combining (1) and (2), we get

$$3^{|\tilde{T}|} \leq 3^{(1-\delta) 2^n}$$

$$\boxed{|\tilde{T}| \leq (1-\delta) 2^n}$$

$\tilde{p}$ and $\widetilde{\text{PARITY}}$ disagree outside of $\tilde{T}$, i.e., on $\geq \delta$-fraction of inputs.

Hence, so do p and PARITY, and the lemma follows ∎

DONE WITH PARITY $\notin$ ACC^0(3) !

With similar methods, can prove for any primes $p \neq q$ that

$$\boxed{MOD_p \notin ACC^0(q)}$$

But already for $ACC^0(2,3) = ACC^0(6)$ cannot rule out that $\boxed{NP \subseteq ACC^0(6)}$!

Why is proving circuit lower bounds so hard ?!

One answer:

Razborov-Rudich '97 "Natural Proofs"

But seems mostly fair to say we don't know...