BOUNDED-DEPTH CIRCUITS WITH MOD-GATES

Polynomial-size bounded-depth circuits with AND-, OR-, and NOT-gates cannot compute PARITY

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

Want to prove lower bounds for stronger class of circuits

- Keep bounded depth
- But allow more types of gates — in constant depth, this can matter a lot

"Counting gates"

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

DEFINITION $\boxed{ACC^0}$

For integers $m_1, \ldots, m_k > 1$, say that

$$L \in \boxed{ACC^0(m_1, \ldots, m_k)}$$

if $\exists$ circuit family $\{C_n\}_{n=1}^{\infty}$ deciding L where C_n has

- gates AND, OR, NOT, $MOD_{m_1}, \ldots, MOD_{m_k}$
- constant depth
- polynomial size

$\boxed{ACC^0}$ = union of $ACC^0(m_1, \ldots, m_k)$ for any $k \in \mathbb{N}^+$ and any $m_1, \ldots, m_k \in \mathbb{N}^+$

Good news and bad news

THEOREM 1 [Razborov '87, Smolensky '87]
For primes p, q, $p \neq q$, $MOD_p \notin ACC^0(q)$

But it is consistent with current state of knowledge that

$$\boxed{NP \subseteq ACC^0(2,3) = ACC^0(6)}$$

Break-through result

THEOREM 2 [Williams '10]
$$NEXP \notin ACC^0$$

So even as simple circuits as ACC^0 brings us right up to the research frontier...

We will prove special case of Theorem 1

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

Proof idea: METHOD OF APPROXIMATIONS

Work in finite field $GF(3) = \mathbb{F}_3 =$
$=$ computing mod 3 with $\{0, 1, 2\}$
$2 \equiv -1 \pmod 3$, so think of $\mathbb{F}_3 = \{-1, 0, 1\}$

1. Show that "small" circuits in $ACC^0(3)$ are well approximated by "low-degree" polynomials in $\mathbb{F}_3[x_1, \ldots, x_n]$
2. Show that PARITY cannot be approximated this way

$\mathbb{F}_3$

+	-1	0	1
-1	1	-1	0
0	-1	0	1
1	0	1	-1

*	-1	0	1
-1	1	0	-1
0	0	0	0
1	-1	0	1

$\mathbb{F}_3[x_1, \ldots, x_n]$ multivariate polynomials
- coefficients in $\mathbb{F}_3$
- evaluated over $\mathbb{F}_3$

$\boxed{\text{FACT 3 Every } \mathbb{F}_3\text{-polynomial that computes parity of } n \text{ variables exactly must have degree } n}$

So if we could strengthen (1) to that small $ACC^0(3)$ - circuits can be represented exactly by low-degree polynomials, then we would be done. But this is not possible (as we shall see soon)

Let us implement step (1) in the proof
We will follow not Arora - Barak, but Ryan Williams (though difference is not huge)

Convenient tool:

DEFINITION 4 A PROBABILISTIC POLYNOMIAL for $f : \{0,1\}^n \to \{0,1\}$ with degree d and error ε is a distribution $\mathcal{D}$ over polynomials of degree $\leq d$ such that

$$\forall x \in \{0,1\}^n \; \Pr_{p \sim \mathcal{D}} \left[p(x) \neq f(x) \right] < \varepsilon$$

Probabilistic polynomial for circuit C: probabilistic polynomial for function f computed by C

LEMMA 5 For all circuits C over gates $\{\wedge, \vee, \neg, MOD_3\}$ of size s and depth d it holds that:

For all $k \in \mathbb{N}^+$

there is a probabilistic polynomial for C over $\mathbb{F}_3$ with

- degree $\leq (2k)^d$
- error $\leq s / 3^k$

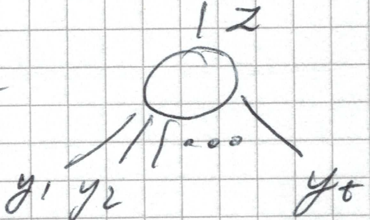
Remarks

(i) In general case with MOD_q-gates would get

- degree $((q-1)k)^d$
- error s / q^k

(ii) Construction of probabilistic polynomial from circuit is efficient — doable in time $\mathrm{poly}(s) \binom{n}{(2k)^d}$ (THOUGH WE WON'T NEED THIS FACT)

Proof of Lemma 5

Replace each gate 

in C by probabilistic polynomial with

- very low degree in inputs $y_1, \ldots, y_t$
- very low error

$\Pr[\text{error at gate}] \leq 1/3^k$

$\Pr[\text{error in circuit} \leq$ [UNION BOUND]

$\sum_{\text{gates}} \Pr[\text{error at gate}] \leq s/3^k$

Approximate each gate by polynomials of degree $\leq 2k$

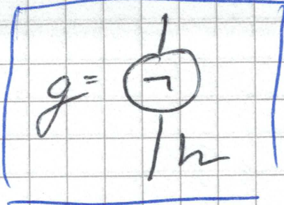
Input wires to gate also approximated by polynomials $\Rightarrow$ degrees multiply in composed polynomial

But depth $\leq d$, so $\boxed{\text{total degree} \leq (2k)^d}$

We need to describe (= approximate) gates g by (probabilistic) polynomials p_g

Note Strictly speaking, gate g represented by distribution $\mathcal{D}_g$ over polynomials p_g but we show how to deal with all polynomials in distribution

(i) NOT-gate



$g = \neg h$

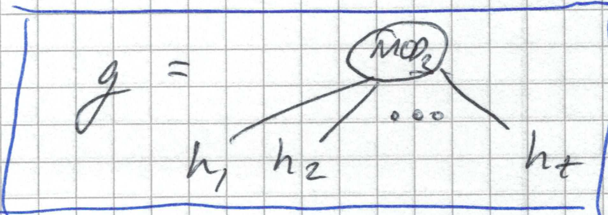
set $\boxed{p_g = 1 - p_h}$

(that is, sample $p_h \sim \mathcal{D}_h$ and then return $1 - p_h$)

No new errors — if p_h correct, then p_g correct

p_g has degree 1 in p_h

(ii) MOD_3-gate



$g = MOD_3(h_1, h_2, \ldots, h_t)$

set $\boxed{p_g = \left(\sum_{i=1}^{t} p_{h_i}\right)^2}$

(that is, sample p_{h_i}:s and return construction)

Now if $a \equiv 0 \pmod 3$ then $a^2 \equiv 0 \pmod 3$
$a \not\equiv 0 \pmod 3$ $a^2 \equiv 1 \pmod 3$
since $(-1)^2 = 1$

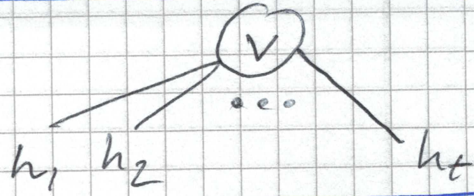
In general:

$$\boxed{\begin{array}{l}\text{FERMAT'S LITTLE THEOREM} \\ a^{p-1} \equiv 1 \pmod p \quad \text{if } p \nmid a\end{array}}$$

No new errors — if p_{h_i} correct, then p_g correct

p_g has degree 2 in p_{h_i} DOES NOT DEPEND ON t

(iii) OR-gate

$g =$ 

Now we have problems...

$\boxed{\bigvee_{i=1}^{t} h_i}$ represented by polynomial

$$\boxed{1 - \prod_{i=1}^{t} (1 - p_{h_i})}$$

Degree $= t$, which can be $\Omega(n)$

far, far too high ☹

LEMMA 6 $\forall k \in \mathbb{N}^+$ $\forall n \in \mathbb{N}^+$

$\exists$ probabilistic polynomial for $\boxed{OR_n}$

over $\mathbb{F}_3$ of

- degree $2k$
- error $1/3^k$

Note: Error probability independent of arity!

Proof Pick uniformly random $v \in \mathbb{F}_3^n$

Set $\boxed{p_1(x_1, \ldots, x_n) = \sum_{i=1}^{n} v_i \cdot x_i}$

Degree-1 polynomial

$$\boxed{OR_n(x_1, \ldots, x_n) = 0 \implies p_1(x) = 0}$$

$$OR_n(x_1, \ldots, x_n) = 1 \implies p_1(x) \in \{-1, 0, 1\}$$

But in this case

$$\boxed{\Pr_v [p_1(x_1, \ldots, x_n) = 0] = 1/3} \quad (*)$$

To see this, fix some coordinate i^* such that $x_{i^*} = 1$

Compute $\sum_{j \neq i^*} v_j \cdot x_j = a$

$a \in \mathbb{F}_3 = \{-1, 0, 1\}$ fixed element

$v_{i^*} \cdot x_{i^*} = v_{i^*}$, since $x_{i^*} = 1$

So $p_1(x_1, \ldots, x_n) = a + v_i$

But v_i uniformly random, and there is exactly one value, namely $-a$, such that $p_1(x_1, \ldots, x_n) = 0$

This proves $(*)$

Set $\boxed{p_2(x_1, \ldots, x_n) = (p_1(x_1, \ldots, x_n))^2 \in \{0,1\}}$

$$\boxed{OR_n(x_1, \ldots, x_n) = 1 \Rightarrow \Pr_v[p_2(x_1, \ldots, x_n) = 1] = 2/3}$$

Pick polynomials $q_1, \ldots, q_k = \left(\sum v_i^{(k)} x_i\right)^2$ in this way

$$\boxed{\begin{aligned} &OR_n(x_1, \ldots, x_n) = 0 \Rightarrow \Pr[\forall_j \; q_j(x_1, \ldots, x_n) = 0] = 1 \\ &OR_n(x_1, \ldots, x_n) = 1 \Rightarrow \Pr[\forall_j \; q_j(x_1, \ldots, x_n) = 0] = 1/3^k \end{aligned}}$$

since vectors $v^{(k)} \in \mathbb{F}_3^n$ chosen independently

Now set

$$\boxed{p(x_1, \dots, x_n) = 1 - \prod_{j=1}^{k} (1 - q_j(x_1, \dots, x_n))}$$

$OR_n(x_1, \dots, x_n) = 0 \Rightarrow p(x_1, \dots, x_n) = 0$ with probability 1

$OR_n(x_1, \dots, x_n) = 1 \Rightarrow$

$$Pr[p(x_1, \dots, x_n) = 1] =$$

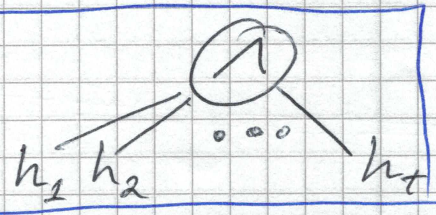
$$= Pr[\exists j \quad q_j(x_1, \dots, x_n) = 1]$$

$$= 1 - 1/3^k$$

So we get $\boxed{\text{degree } 2k}$, $\boxed{\text{error} \leq 1/3^k}$ as claimed, and Lemma 6 follows ☒

(iv) AND-gate

$g =$



Use De Morgan's Laws

$$\boxed{AND(x_1, \dots, x_n) = \neg OR(\neg x_1, \dots, \neg x_n)}$$

so we can take polynomial

$$1 - p(1 - x_1, \dots, 1 - x_n)$$

for p constructed as in case (iii)

Same degree

Same error probability

How this works (1) First sample polynomials p_{h_i} for h_i

(2) Then sample $q_1, \dots, q_k$ & plug in p_{h_i} for x_i

Final probabilistic polynomial = that of output gate

Degree $\leq (2k)^d$ by construction

Error probability

$$\Pr[\text{error in circuit}] \leq \begin{bmatrix}\text{UNION}\\ \text{BOUND}\end{bmatrix}$$

$$\sum_{\text{gates}} \Pr[\text{error at gate}] \leq$$

$$s \cdot 1/3^k$$

Lemma 5 follows $\blacksquare$

But we need real, honest polynomials...

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 of degree $\leq \boxed{(2k)^d}$ such that

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

Note that probability is now over random input $x \in \{0,1\}^n$

Proof For $x \sim \{0,1\}^n$ and $p \sim \mathcal{D}$, define random variable

$$\boxed{X_{p,x} = \begin{cases} 1 & \text{if } C(x) = p(x) \\ 0 & \text{otherwise} \end{cases}}$$

Then

$$\boxed{\sum_{x \in \{0,1\}^n} \mathop{E}_{p \sim \mathcal{D}} \left[X_{p,x} \right] \geq 2^n \left(1 - s/3^k\right)}$$

for distribution $\mathcal{D}$ constructed in proof of Lemma 5

By linearity of expectation

$$\boxed{\mathop{E}_{p \sim \mathcal{D}} \left[\sum_{x \in \{0,1\}^n} X_{p,x} \right] \geq 2^n \left(1 - s/3^k\right)}$$

But then there must exist at least one polynomial p^* in the support of $\mathcal{D}$ with

$$\boxed{\sum_{x \in \{0,1\}^n} X_{p^*,x} \geq 2^n \left(1 - s/3^k\right)}$$

For this p^* we get

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

We have now proven that small, low-depth $ACC^0(3)$-circuits can be well approximated by low-degree polynomials. That is step 1 ✓

Step 2 will be to prove that this is NOT TRUE for the PARITY function.