ACC0 circuit Lower Bound

Arka Ray Nabarun Deka

25th December, 2020

Brief History

- In 1981, Frust, Saxe and Sipser showed a lower bound for circuits computing the parity function, which implied that Parity was not in the class $\mathbf{AC}^0$.
- Once this result came out, a natural question to ask was, what happens if we give more power to the $\mathbf{AC}^0$ circuits. In particular, what if we allow the circuits to have more general gates, for example, some MOD_m gate.

Brief History

- Razborov proved the first lower bound for such a class of circuits (called $\mathbf{ACC}^0[q]$) using his 'Method of Approximation', by showing PARITY $\notin \mathbf{ACC}^0[q]$.
- Smolensky generalized this lower bound to a much larger class of functions (i.e, MOD_p) using similar methods.

Definitions

Modular Gates

For any integer m, the MOD_m gate outputs 0 if the sum of its inputs is 0 modulo m and 1 otherwise.

Class $\mathbf{ACC}^0$

For integers $m_1, m_2, \ldots, m_k$, a language L is said to be in the class $\mathbf{ACC}^0[m_1, m_2, \ldots, m_k]$ if L can be decided by a circuit family $\{C_n\}_{n\in\mathbb{N}}$ such that for every $n \in \mathbb{N}$, C_n is a polynomial size and constant depth circuit, with unbounded fan-in, consisting of $\vee, \wedge, \neg$, MOD_{m_1}, MOD_{m_2}, $\ldots$, MOD_{m_k} gates.

Definitions

Class $\mathbf{ACC}^0$

The class $\mathbf{ACC}^0$ consists of all languages L that is in $\mathbf{ACC}^0[m_1, m_2, \ldots, m_k]$ for some $k \geq 0$ and $m_1, m_2, \ldots, m_k \geq 1$.

Method of Approximation

Razborov used a technique called method of approximation to show circuit lower bounds. This method is used to show that a language L does not belong to some class $\mathcal{C}$ by showing :

- For any language L' in $\mathcal{C}$, there is a "good approximation".
- The language L does not have a "good approximation".

PARITY $\notin$ $\mathbf{ACC}^0[q]$

Theorem (Razborov)

PARITY $\notin$ $\mathbf{ACC}^0[q]$ for any odd prime q

Proof: The proof has two major steps.
Step 1: In the first step, we show that for a Boolean function f on n inputs that can be computed by a depth d circuit of size s containing MOD_q gates, there is a polynomial p of degree $((q-1)l)^d$ which agrees with f on $1 - s/2^l$ fraction of inputs.
Step 2: In the second step, we show that no polynomial of degree atmost $\sqrt{n}$ agrees with PARITY on more than $49/50$ fraction of its inputs.

Step 1

In this step, we want to prove the following theorem :

Theorem 1

If $f : \{0,1\}^n \to \{0,1\}$ can be computed by a depth d and size s circuit containing MOD_q gates, then, for any integer $l \geq 1$, there exists a polynomial $p(x) \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ of degree $((q-1)l)^d$ such that

$$\Pr_x[f(x) \neq p(x)] \leq \frac{s}{2^l}$$

Here, $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$ is the ring of polynomials on n variables over the field $\mathbb{F}_q$. $\mathbb{F}_q$ is the field of integers modulo q.

Proof of Theorem 1

Observe that :

- $\text{NOT}(x) = 1 - x$
- $MOD_q(x_1, x_2, \ldots, x_n) = (x_1 + x_2 + \cdots + x_n)^{(q-1)}$
- $\text{AND}(x) = 1 - \text{OR}(1 - x)$

The NOT function can be evaluated by a linear polynomial, while the MOD_q function can be computed by a polynomial of degree $q - 1$, regardless of n. The key observation, made by Razborov, is that AND and OR can be approximated by low degree polynomials.

Approximating OR

We will now look at how OR can be approximated by low degree polynomials. If we can approximate OR by a polynomial, then we can approximate AND also, by using the formula $\text{AND}(x) = 1 - \text{OR}(1 - x)$

Approximating OR

Lemma 1

Let S be a subset of $[n]$ chosen uniformly at random. Let $x \in \{0,1\}^n$ be any non-zero vector. Then,

$$\Pr_S\left[\sum_{i\in S} x_i \neq 0\right] \geq 1/2$$

where the summation is over the field $\mathbb{F}_q$

Proof : $x \neq 0^n$. Hence, there exists $j_0 \in [n]$ such that $x_{j_0} = 1$. Think of choosing S as follows: first choose a subset S' of $[n]\setminus\{j_0\}$ uniformly at random. And then with probability half, add j_0 to S'. Now, let $\sum\limits_{i\in S'} x_i = c$.

Approximating OR

Regardless of what c is, with probability half, we choose to add j_0 to S', in which case, $\sum_{i \in S} x_i = c + 1$, and with probability half we choose to not add j_0 to S', in which case $\sum_{i \in S} x_i = c$. Now, both c and $c + 1$ cannot simultaneously be zero. Hence,

$$\Pr_S \left[\sum_{i \in S} x_i \neq 0 \right] \geq \frac{1}{2}$$

Approximating OR

Lemma 2

There is a $(q-1)l$ degree polynomial p over $\mathbb{F}_q$ such that

$$\Pr_{x\in\{0,1\}^n}[\mathrm{OR}(x) \neq p(x)] \leq 1/2^l$$

Proof : Pick l subsets of $[n]$ independently and uniformly at random, call this collection of subsets $\mathcal{S} = \{S_1, S_2, \ldots, S_l\}$.
Consider the polynomial

$$p_{\mathcal{S}}(x) = 1 - \prod_{i=1}^{l}(1 - (\sum_{j\in S_i} x_j)^{q-1})$$

For a fixed $x \in \{0,1\}^n$, by Lemma 1,

$$\Pr_{\mathcal{S}}[p_{\mathcal{S}}(x) \neq \mathrm{OR}(x)] \leq 1/2^l$$

Approximating OR

Now consider the indicator random variable:

$$I_{x,\mathcal{S}} := \mathbb{1}(p_{\mathcal{S}}(x) \neq \mathrm{OR}(x))$$

Expected number of points where $p_{\mathcal{S}}(x) \neq \mathrm{OR}(x)$ is,

$$\mathop{\mathbb{E}}_{\mathcal{S}}\left[\sum_{x\in\{0,1\}^n} I_{x,\mathcal{S}}\right] = \sum_{x\in\{0,1\}^n} \mathbb{E}\left[I_{x,\mathcal{S}}\right] \leq 2^n.(1/2^l)$$

Hence, there exists some $\mathcal{S}$ such that

$$\sum_{x\in\{0,1\}^n} I_{x,\mathcal{S}} \leq 2^n.(1/2^l)$$

Approximating OR

For this choice of $\mathcal{S}$, we get,

$$\Pr_{x \in \{0,1\}^n}[p_{\mathcal{S}}(x) \neq OR(x)] \leq 2^{n-l}/2^n = 2^{-l}$$

$p_{\mathcal{S}}(x)$ is the required polynomial.

Completing Step 1

Theorem 1

If $f : \{0,1\}^n \to \{0,1\}$ can be computed by a depth d and size s circuit containing MOD_q gates, then, for any integer $l \geq 1$, there exists a polynomial $p(x) \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ of degree $((q-1)l)^d$ such that

$$\Pr_x[f(x) \neq p(x)] \leq s/2^l$$

Here, $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$ is the ring of polynomials on n variables over the field $\mathbb{F}_q$. $\mathbb{F}_q$ is the field of integers modulo q.

Now, we prove our theorem. Let f be computed by a depth d and size s circuit C. In C, replace each gate with the corresponding $(q-1)l$ degree polynomial. So, the resulting polynomial, p, that approximates f :

- has degree $((q-1)l)^d$
- By using union bound, we get that

$$\Pr_x[f(x) \neq p(x)] \leq s/2^l$$

Completing Step 1

Theorem 1 holds for any integer l. We choose our l to be

$$(q-1)l = n^{1/2d}$$

With this choice of l, we get:

Corollary 1

If $f : \{0,1\}^n \to \{0,1\}$ can be computed by a depth d and size s circuit containing MOD_q gates, then, there exists a polynomial $p(x) \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ of degree $\sqrt{n}$ such that

$$\Pr_x[f(x) \neq p(x)] \leq s/(2^{\frac{n^{1/2d}}{q-1}})$$

Here, $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$ is the ring of polynomials on n variables over the field $\mathbb{F}_q$. $\mathbb{F}_q$ is the field of integers modulo q.

Step 2

In step 2, we want to prove the following theorem:

Theorem 2

Any polynomial $p(x) \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ of degree at most $\sqrt{n}$ can agree with the PARITY function on at most 49/50 fraction of its inputs (where the inputs are coming from the set $\{0,1\}^n$).

Step 2

Theorem 2

Any polynomial $p(x) \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ of degree at most $\sqrt{n}$ can agree with the PARITY function on at most $49/50$ fraction of its inputs (where the inputs are coming from the set $\{0, 1\}^n$).

Proof : Let $p(x) \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ be a polynomial of degree at most $\sqrt{n}$ that agrees with PARITY on a set $G' \subseteq \{0, 1\}^n$. We want to show that $|G'| \leq (49/50)2^n$.
We first do the following change of variables:

$$y_i = 1 + (q - 2)x_i \bmod q$$

This change of variables sends $0 \rightarrow 1$ and $1 \rightarrow (q - 1)$ in $\mathbb{F}_q$. Under this change of variables, G' is transformed to a subset $G \subseteq \{1, q - 1\}^n$, such that $|G'| = |G|$.

Step 2

Consider the polynomial

$$g(y_1, y_2, \ldots, y_n) := 1 + (q-2)p((q-2)^{-1}(y_1 - 1), \ldots, (q-2)^{-1}(y_n - 1))$$

Observe that g is also a polynomial over $\mathbb{F}_q$ of degree at most $\sqrt{n}$.
The key observation here is that on the set G

$$g(y_1, y_2, \ldots, y_n) = \prod_{i=1}^{n} y_i$$

This statement is saying that a polynomial of degree $\sqrt{n}$ is agreeing with a polynomial of degree n on a set G. Hence, intuitively, this set G cannot be the entire set $\{1, (q-1)\}^n$.

Step 2

Our goal is to show that $|G| \leq (49/50).2^n$. For this, we will need the following two lemmas:

Lemma 3

Any function $S : \mathbb{F}_q^n \rightarrow \mathbb{F}_q$ can be written as a polynomial g_S.

Lemma 4

Let $G \subseteq \{1, q-1\}^n$. For each function $S : G \rightarrow \mathbb{F}_q$ there exists a polynomial $g_S(x_1, x_2, \dots, x_n)$ over $\mathbb{F}_q$ whose terms are monomials of the form $c. \prod_{i \in I} x_i$ with $|I| \leq n/2 + \sqrt{n}$ such that g_S agrees with S on the set G.

Step 2

Assuming the lemmas, let us see how theorem 2 follows. Let

$$\mathcal{F}(G) := \{S \mid S : G \to \mathbb{F}_q\}$$

By lemma 4, we know that for each function $S : G \to \mathbb{F}_q$, there exists a "special" polynomial g_S. Hence, $|\mathcal{F}(G)|$ is bounded above by the total number of "special" polynomials. Also, $|\mathcal{F}(G)| = q^{|G|}$. Therefore,

$$q^{|G|} \leq \#(\text{"special" polynomials})$$

Step 2

We now have to compute the number of "special" polynomials. Let

$$\mathcal{M} := \{\prod_{i \in I} x_i \mid |I| \leq n/2 + \sqrt{n}\}$$

Each "special" polynomial can be written as:

$$g_S(x_1, x_2, \ldots, x_n) = \sum_{m \in \mathcal{M}} c_m.m$$

where c_m's are coefficients from $\mathbb{F}_q$. Hence,

$$\#(\text{"special" polynomials}) = q^{|\mathcal{M}|}$$

Step 2

We get,

$$q^{|G|} \leq q^{|\mathcal{M}|}$$
$$\implies |G| \leq |\mathcal{M}|$$

We can compute $|\mathcal{M}|$ as :

$$|\mathcal{M}| = \sum_{i=1}^{n/2+\sqrt{n}} \binom{n}{i} \leq (49/50).2^n$$

We get the final bound by using bounds on tails of binomial distribution.

Step 2

Theorem 2

Any polynomial $p(x) \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ of degree at most $\sqrt{n}$ can agree with the PARITY function on at most $49/50$ fraction of its inputs (where the inputs are coming from the set $\{0, 1\}^n$).

Hence, we get that $|G'| = |G| \leq (49/50).2^n$, which proves Theorem 2.

Proof of Lemmas

We now prove the lemmas 3 and 4.

Lemma 3

Any function $S : \mathbb{F}_q^n \to \mathbb{F}_q$ can be written as a polynomial g_S.

Proof : Fix a $b \in \mathbb{F}_q^n$. Let $b = b_1 b_2 \dots b_n$. We will construct a polynomial h_b such that

$$h_b(x) = \begin{cases} 1 & x = b \\ 0 & x \neq b \end{cases}$$

For each $i \in [n]$, define a polynomial $f_{b,i}$ as

$$f_{b,i}(x_1, x_2, \dots, x_n) := \prod_{a \in \mathbb{F}_q \setminus \{b_i\}} (x_i - a).(b_i - a)^{-1}$$

Proof of Lemmas

Observe that

$$f_{b,i}(x_1, x_2, \ldots, x_n) = \begin{cases} 1 & x_i = b_i \\ 0 & x_i \neq b_i \end{cases}$$

Now, define h_b as

$$h_b(x_1, x_2, \ldots, x_n) := \prod_{i=1}^{n} f_{b,i}(x_1, x_2, \ldots, x_n)$$

For any function $S : \mathbb{F}_q^n \to \mathbb{F}_q$, consider the polynomial

$$g_S(x_1, x_2, \ldots, x_n) := \sum_{y \in \mathbb{F}_q^n} S(y).h_y(x_1, x_2, \ldots, x_n)$$

It is clear that $g_S(x) = S(x)$.

Proof of Lemmas

Lemma 4

Let $G \subseteq \{1, q-1\}^n$. For each function $S : G \to \mathbb{F}_q$ there exists a polynomial $g_S(x_1, x_2, \ldots, x_n)$ over $\mathbb{F}_q$ whose terms are monomials of the form $c.\prod_{i \in I} x_i$ with $|I| \leq n/2 + \sqrt{n}$ such that g_S agrees with S on the set G.

Proof: Fix a function $S : G \to \mathbb{F}_q$. We can extend S to a function $\hat{S} : \mathbb{F}_q^n \to \mathbb{F}_q$. By Lemma 3, there is a polynomial $g_{\hat{S}} = \hat{S}$. $g_{\hat{S}}$ agrees with S on the set G. Observe that in $\mathbb{F}_q$,

$$1^2 = (q-1)^2 = 1$$

For any term $c.\prod_{i \in I} x_i^{p_i}$ in $g_{\hat{S}}$, replace it with the term $c.\prod_{i \in I} x_i^{r_i}$ where $r_i = p_i \bmod 2$ to get a new polynomial g_S. From our observation, we can see that g_S still agrees with S on the set G.

Proof of Lemmas

The terms of g_S look like $c.\prod_{i\in I} x_i$. If for any term, $|I| > n/2$, we can write that term as:

$$c.\prod_{i\in I} x_i = c.\prod_{i=1}^{n} x_i.\prod_{i\in \bar{I}} x_i = c.g(x_1, x_2, \ldots, x_n).\prod_{i\in \bar{I}} x_i$$

where $\bar{I} = [n]\backslash I$. We could replace $c.\prod_{i=1}^{n} x_i$ with $g(x_1, \ldots, x_n)$ because we know that they agree on the set G. The polynomial g_S obtained after this modification still agrees with S on the set G. Furthermore, every term of g_S is now a monomial of the form c. $\prod_{i\in I} x_i$ where $|I| \leq n/2 + \sqrt{n}$. Hence, we get Lemma 4.

Completing the Proof

Theorem (Razborov)

PARITY $\notin$ $\mathbf{ACC}^0[q]$ for any odd prime q

Let $\{C_n\}_{n \in \mathbb{N}}$ be a circuit family that decides PARITY such that for every $n \in \mathbb{N}$, C_n is a circuit on n inputs of size s_n and constant depth d with unbounded fan-in, and consists of $\wedge, \vee, \neg$ and MOD_q gates.

Completing the Proof

Corollary 1

If $f : \{0,1\}^n \to \{0,1\}$ can be computed by a depth d and size s circuit containing MOD_q gates, then, there exists a polynomial $p(x) \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ of degree $\sqrt{n}$ such that

$$\Pr_x[f(x) \neq p(x)] \leq s/(2^{n^{1/2d}/q-1})$$

Here, $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$ is the ring of polynomials on n variables over the field $\mathbb{F}_q$. $\mathbb{F}_q$ is the field of integers modulo q.

Fix $n \in \mathbb{N}$. By Corollary 1, there exists a polynomial p_n of degree $\sqrt{n}$ such that

$$\Pr_x[f(x) \neq p_n(x)] \leq s_n/(2^{n^{1/2d}/q-1})$$

equivalently,

$$\Pr_x[f(x) = p_n(x)] \geq 1 - s_n/(2^{n^{1/2d}/q-1})$$

Completing the Proof

Theorem 2

Any polynomial $p(x) \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ of degree atmost $\sqrt{n}$ can agree with the PARITY function on atmost $49/50$ fraction of its inputs (where the inputs are coming from the set $\{0,1\}^n$).

By Theorem 2, we also have,

$$(49/50) \geq \Pr_x[f(x) = p_n(x)]$$

Hence, we get

$$49/50 \geq 1 - s_n/(2^{n^{1/2d}/q-1}) \quad (1)$$

$$\implies s_n/(2^{n^{1/2d}/q-1}) \geq 1/50 \quad (2)$$

$$\implies s_n \geq (1/50).(2^{n^{1/2d}/q-1}) \quad (3)$$

Completing the Proof

Theorem (Razborov)

PARITY $\notin \mathbf{ACC}^0[q]$ for any odd prime q

Thus, we see that for every $n \in \mathbb{N}$, the size of the circuit C_n cannot be polynomial in n. Hence, PARITY $\notin \mathbf{ACC}^0[q]$.

Concluding Remarks

- The result presented in this presentation is the result proved by Razborov. Later on, Smolensky generalises this proof to prove that not only PARITY, but MOD_p is not in $\mathbf{ACC}^0[q]$ for distinct primes p and q.
- The method of approximation used by Razborov is a very general technique that has been used to prove various other circuit lower bounds.

References

- Section 13.2 : Circuits with "Counters": **ACC** of the draft of 'Computational Complexity : A Modern Approach' by Sanjeev Arora and Boaz Barak.
  Link: http://theory.cs.princeton.edu/complexity/book.pdf
- Lecture 5 : 'Razborov-Smolensky Lower Bounds for Constant Depth Circuit with MOD_p gates' given by Yuan Li as part of the Chicago Center for Theory of Computing Summer REU Program 2014.
  Link: http://people.cs.uchicago.edu/ yuanli/Lec5.pdf