The method of approximations

- Parity $\not\in AC^0$ (Second proof).

Highlights
- Method of approximations.
- Algebra + randomness.
- Exponential lower bounds.

- Introduced by Alexander Razborov.
- Replace circuits by “simpler” circuits that compute function on many (most) inputs.
- Typically done piecewise - replace gates by approximating gates.
- Prove underlying function is complex, and so simple functions can’t compute it.

Smolensky notions

- functions $\rightarrow$ polynomials (over which domain?).
- Parity has high-degree.
- Can’t even be approximated by low-degree.
- Circuits have low-degree.

The key insight

- Let field be $\mathbb{Z}_3 = \{-1, 0, 1\}$.
- Embed binary world by the map $0 \rightarrow 1$ and $1 \rightarrow -1 (i \rightarrow (-1)^i)$.
- Addition becomes multiplication; so parity becomes product: $\oplus(y_1, \ldots, y_n) = \prod_i y_i$.
- Claim: Parity is hard to compute is algebraic world, even with addition (over $\mathbb{Z}_3$) thrown in for free.
Lemma 1: If $f : \{0, 1\}^n \to \{0, 1\}$ is computed by a depth $d$ circuit of size $s$, then there exists a set $S \subseteq \{0, 1\}^n$ of size $|S| \geq 3/42^n$ such that $f : S \to \{0, 1\}$ computed by a polynomial over $\mathbb{Z}_3$ of degree $(\log s)^{O(d)}$.

Lemma 2: If there exists a degree polynomial $D : \mathbb{Z}_3^n \to \mathbb{Z}_3$ such that $p(x) = \Theta(x)$ for all $x \in S$, then every Boolean function $f : S \to \{0, 1\}$ is computed by polynomials of degree $n/2 + D$.

Lemma 3: Any set of functions generating all $f : S \to \{0, 1\}$ must have at least $|S|$ members.

- Assume parity has depth $d$, size $s$ circuit.
- By Lemma 1, parity is computed by polynomial of degree $(\log s)^{O(d)}$ on set $S$ of size $3/42^n$.
- By Lemma 2, every Boolean function on $S$ is a polynomial of degree $n/2 + (\log s)^{O(d)}$. Thus this set of functions is contained in a vector space over $\mathbb{Z}_3$ of dimension at most $\sum_{i=0}^{n/2+(\log s)^{O(d)}} \binom{n}{i} \leq 2^{n-1} + (\log s)^{O(d)} 2^n / \sqrt{n} < 3/42^n$. (Provided $s \leq 2^n^{O(1/d)}$.)
- By Lemma 3, this space of functions has dimension at least $|S| \geq 3/42^n$.

Proof of Lemma 3

- Let $\delta_x(y) = 1$ if $x = y$ and 0 o.w..
- The functions $\{\delta_x : S \to \{0, 1\} | x \in S\}$ are linearly independent.
- Simple linear algebra.
Proof of Lemma 2

- Will switch back and forth between 0/1 and ±1.
- Suppose \( \oplus : S \to \{0, 1\} \) is represented by a polynomial \( q : \mathbb{R}^n \to \mathbb{R} \). Let \( T \subseteq \{+1, -1\}^n \) be the associated set. Then \( \prod_{i=1}^{n} x_i = 1-2q((1-x_1)/2, \ldots, (1-x_n)/2) \) on the set \( T \).

- Consider Boolean function \( f : S \to \{0, 1\} \). Let \( g : T \to \{+1, -1\} \) be associated function. Represent \( g \) by a polynomial in its arguments. \( p(x) = \sum A_i x_i + \sum B_j C_j \) where \( A_i \)'s are terms of degree less than \( n/2 \) and \( B_j \)'s are terms of degree greater than \( n/2 \). Let \( C_j = \prod_{i=1}^{n} x_i/B_j \). Then \( p'(x) = \sum A_i + q(x) \sum B_j C_j \) also represents \( g \) and is a polynomial of degree at most \( n/2 + D \).
- The polynomial \( r(x) = (1 + p(1 - 2x))/2 \) represents \( f \).

Proof of Lemma 1

- This is the hard lemma. (Though the linear algebra is also very novel.)
- But is seen again and again in complexity.
- Basic idea: Fix input \( x_1, \ldots, x_n \) and randomly replace every gate by a polynomial of low-degree. Show the resulting circuit still computes the original value with probability at least 3/4.
- Use the probabilistic method to conclude there exists a collection of polynomials which computes the original function on 3/4ths of the input.

Prob. polynomial for the OR function

Naive answer: \( OR(y_1, \ldots, y_k) = 1 - \prod_{i=1}^{k} (1 - y_i) \). Answer is always right. But degree is \( k \) - too much.

Step 1: Get the answer right w.p. 1/2 with polynomials of degree 2.

Basic idea: pick \( a_1, \ldots, a_k \in \mathbb{Z}_3 \) at random.
\( p_a(y) = \sum_{i=1}^{k} a_i y_i \).

Claim 1: \( p_a(0) = 0 \).

Claim 2: \( \Pr[p_a(y) = 0] \leq 1/3 \).

Proof: Let \( Q(z) = \sum y_i z_i \). \( Q \) is a non-zero polynomial of degree 1 in its argument. Evaluation at random \( z = a \) leaves it non-zero.
The polynomial $p_a^2$ is always 0 or 1 and computes the OR function on any fixed input w.p. 2/3.

Pick $a_1, \ldots, a_l$, and take the OR of polynomials $p_{a_i}$.

Gives degree $2\ell$ polynomial that is right w.p. $1 - (2/3)^\ell$.

What we gained? Will pick $\ell = \log s$ to make degrees logarithmically smaller than fan-in.

What we lost? Not guaranteed to be right.

Conclusions

- Algebra, arithmetization, randomness very powerful tools.
- Work in situations where there’s no mention of them in problem statement.
- Many more examples in course.
- Unfortunately, know little else?

- Replace every gate by degree $2\ell$ poly randomly.
- Resulting circuit computes a polynomial of degree $(2\ell)^d$.
- Prob. it gets the output wrong (for fixed input) is at most $s(1/3)^\ell$.
- Lemma follows.