Today

- Parity $\notin$ AC^0 (Second proof).
- Highlights
  - Method of approximations.
  - Algebra + randomness.
  - Exponential lower bounds.

The method of approximations

- 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: $\tilde{\oplus}(y_1, \ldots, y_n) = \prod_i y_i$.
- Claim: Parity is hard to compute is algebraic world, even with addition (over $\mathbb{Z}_3$) thrown in for free.

Main Lemmas

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 $p : \mathbb{Z}_3^n \to \mathbb{Z}_3$ such that $p(x) = \bigoplus(x)$ 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.

Using lemmas to prove theorem

- 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 $s \leq 2^{n^{\Omega(1/d)}}$.)
- By Lemma 3, this space of functions has dimension at *least* $|S| \geq 3/42^n$.

- We have a contradiction

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 $\bigoplus : S \rightarrow \{0,1\}$ is represented by a polynomial $q : \mathbb{R}^n \rightarrow \mathbb{R}$. 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 $f : S \rightarrow \{0,1\}$. Let $g : T \rightarrow \{+1,-1\}$ be associated function. Represent g by a polynomial in its arguments. $p(\mathbf{x}) = \sum_i \alpha_i A_i + \sum_j \beta_j B_j$ where A_i 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 $p'(\mathbf{x}) =$

$\sum_i \alpha_i A_i + q(\mathbf{x}) \sum_j \beta_j C_j$ also represents g and is a polynomial of degree at most $n/2 + D$.

- The polynomial $r(\mathbf{x}) = (1 + p(1-2\mathbf{x}))/2$ 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 $3/4$ths 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. $p_{\mathbf{a}}(\mathbf{y}) = \sum_{i=1} a_i y_i$.

Claim 1: $p_{\mathbf{a}}(\mathbf{0}) = 0$.

Claim 2: $\Pr_{\mathbf{a}}[p_{\mathbf{a}}(\mathbf{y}) = 0] \leq 1/3$.

Proof: Let $Q(\mathbf{z}) = \sum_{i=1}^k y_i z_i$. Q is a non-zero polynomial of degree 1 in its argument. Evaluation at random $\mathbf{z} = \mathbf{a}$ leaves it non-zero.

Prob. polynomial for the OR function (contd.)

The polynomial $p_{\mathbf{a}}^2$ is always 0 or 1 and computes the OR function on any fixed input w.p. $2/3$.

Pick $\mathbf{a}_1, \ldots, \mathbf{a}_l$, and take the OR of polynomials $p_{\mathbf{a}_i}$.

Gives degree 2ℓ 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.

Prob. polynomial for circuit

- Replace every gate by degree 2ℓ 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.

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?