LECT 06

Note Title

TODAY: Alternate Proof that Parity $\notin AC^0$

[RAZBOROV, SMOLENSKY]

Ingredients

- finite fields & polynomials
- linear Algebra
- Randomization

Why another proof?

- Quantitatively stronger (than [F.S.S.])
- Qualitatively different (not so reliant on properties of AND/OR gates)
- Useful techniques

General Approach:

- Replace / Approximate Boolean Gates By Nicer Functions (polynomials over fields)
- Show Circuit Becomes Simple
  ("approximated" by low degree polynomials)
- Show Parity Is Complex
  (can't be "approximated" by low. deg. poly.)

Issues:

- Which field ?
- What is approximation ?
- What is simple
- Proving parity is complex

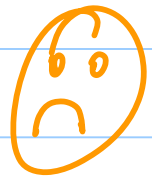
Which field ?

First Idea: How about $GF(2)$?
[addition / multiplication mod 2]

Unfortunately Parity is simple

$$\text{Parity}(x_1 \dots x_n) = x_1 + x_2 + \dots x_n$$

↑ degree 1 !



BETTER IDEA:

- Use any other finite (*) field
  - Parity becomes complex
  - AC^0 becomes simple
- Will use $GF(3) = \{-1, 0, 1\}$

(*) finite nos not necessary, just easier.
See talk by Braverman tomorrow !!

Why other fields?

- What does Parity look like over $\mathbb{F}$?
- Fundamental trick of Boolean analysis

$$\{0,1\} \longleftrightarrow \{-1,1\}$$

by linear maps

$$x \longmapsto 1-2x$$

$$\frac{1-y}{2} \longmapsto y$$

$$\text{Parity}(x_1 \dots x_n) \longleftrightarrow \prod_{i=1}^{n} y_i \quad \text{[Magic!]}$$

if $p(x_1 \dots x_n)$ computes $\text{Parity}(x_1 \dots x_n)$

then $q(y_1 \dots y_n) \triangleq 1 - 2p\left(\frac{1-y_1}{2}, \dots, \frac{1-y_n}{2}\right)$

computes $\prod_{i=1}^{n} y_i$

$\deg(q) \leq \deg(p) \Rightarrow \deg(p) \geq n$ 

Approximation?

- Will find large subset $S \subseteq \{0,1\}^n$ s.t. AC^0 circuit $C : \{0,1\}^n \to \{0,1\}$ equals low degree poly $P : \mathbb{F}_3^n \to \mathbb{F}_3$ for every $x \in S$

  (simplicity)

- Will prove Parity cannot be approximated like this (complexity)

Lemma 1: if C is a circuit of depth d & size s

$\exists$ poly $p: \mathbb{F}_2^n \to \mathbb{F}_3$ of degree

$D \leq$???

& set $S \subseteq \{0,1\}^n$ of size $|S| \geq$??? $(1-\epsilon)\cdot 2^n$

s.t. $\forall x \in S, \quad p(x) = C(x)$

Idea:
- Replace each gate of circuit prob. by a polynomial of deg $k \approx \log \frac{s}{\epsilon}$
- for fixed input $x \in \{0,1\}^n$ show that Poly "computes" gate(x) w.p. $1 - \exp(-k)$

("computes": if inputs correct per $C(x)$, then output would be right!)

- Conclude:

① C replaced by poly p of deg $\approx k^d$

$\approx \left(\log \frac{1}{\epsilon}\right)^d$

② for any $x \in \{0,1\}^n$

$\Pr_p[p(x) = C(x)] \geq (1-\epsilon)\cdot 2^n$

③ $\Rightarrow \exists\ p,\ S \subseteq \{0,1\}^n,\ |S| \geq (1-\epsilon)\cdot 2^n$

s.t. $\forall x \in S,\ p(x) = C(x)$.

Exercise

Thus it suffices to show

Lemma 1.1: $\exists$ distribution on deg k poly p

s.t. $\forall z_1 \dots z_t$ $\Pr_p[p(z_1 \dots z_t) = \mathrm{OR}(z_1 \dots z_t)] \geq 1 - \exp(-k)$

Polynomials & Approximate-OR

- Exact-OR $(z_1 \cdots z_t) = 1 - \prod_{j=1}^{t} (1 - z_i)$

  Degree = t ☹

- Approximate-OR$_{\alpha_1 \cdots \alpha_t}(z_1 \cdots z_t)$

  $= \left(\sum \alpha_i z_i \right)^{q-1}$ $\quad \alpha_i \in \mathbb{F}_q$ ↑ uniform independent

  - Degree = $q-1$ independent of t ☺

  - Correct?

Claim: $\forall z_1 \cdots z_t \quad \Pr_{\alpha_1 \cdots \alpha_t} [\text{APPROX-OR}(z_1 \cdots z_t) = \text{OR}(z_1 \cdots z_t)] \geq \frac{q-1}{q}$

Proof: Obvious if $z_1 \cdots z_t = 0 \cdots 0$;

Else RHS = 1;

$\left(\sum \alpha_j z_j \right)^{q-1} = 1 \iff \sum \alpha_j z_j \neq 0$;

Useful General Lemma

[SCHWARTZ, ZIPPEL, DEMILLO LIPTON]

Let $f: \mathbb{F}^n \to \mathbb{F}$ be a non-zero deg D polynomial. Let $H \subseteq \mathbb{F}$ be any finite set

$$\Pr_{\alpha \leftarrow H^n}\left[f(\alpha) = 0 \right] \leq \frac{D}{|H|}$$

Proof: $n = 1 \Leftarrow \#\{\text{roots of } f\} \leq D$

$n > 1 \Leftarrow$ Induction (Exercise)

Back to our Claim:

$$f(\alpha) = \sum z_i \cdot \alpha_i$$

z_i: coeff. of f

Not all $z_i = 0 \Rightarrow f \neq 0$; deg of $f = 1$

$$\Rightarrow \Pr_{\alpha}\left[f(\alpha) = 0 \right] \leq \frac{1}{q}$$ ☒

Now can combine k APPROX-OR with k-wise EXACT-OR to get Lemma 1.1 ☒

Complexity of Parity

Lemma 2:

If P approximates parity : $\{0,1\}^n \to \{0,1\}$

on set S with $|S| \geq (1-\epsilon)\cdot 2^n$

then $\deg(P) \geq \Omega\left(\left(\frac{1}{2}-\epsilon\right)\sqrt{n}\right)$

(By Fundamental Trick of Complexity) ⇕

Lemma 2': if q approximates $\prod_{i=1}^{n} x_i$ on

set $T \subseteq \{-1,+1\}^n$ with $|T| \geq (1-\epsilon)2^n$

then $\deg(q) \geq \Omega\left(\left(\frac{1}{2}-\epsilon\right)\sqrt{n}\right)$.

Proof: Counting:

Set of functions from $S \to \mathbb{F}$

$\leq$ " polynomials "

functions $\geq |\mathbb{F}|^{|S|}$ obviously

$= 3^{|S|}$ (if $|\mathbb{F}| = 3$)

- But can write any function from $S \to \mathbb{F}$ as a polynomial

$$P(x_1 \cdots x_n) = \sum_{\vec{d}} c_{\vec{d}}\, x_1^{d_1} x_2^{d_2} \cdots x_n^{d_n}$$

- Can replace d_i by $d_i \pmod 2$ since $S \subseteq \{-1, 1\}^n$ & for

... (continued on next page)

(KEY IDEA)

if $\sum d_i > \frac{n}{2}$ then replace

$x_1^{d_1} \cdots x_n^{d_n}$ by $x_1^{(d_1+1) \bmod 2} \cdots x_n^{(d_n+1) \pmod 2} \cdot q(x_1 \cdots x_n)$

Resulting polynomial has terms of degree

$\uparrow$ in each var, & total degree $\leq \frac{n}{2} + D$

$$\#\text{ coefficients} \leq \sum_{i=1}^{\frac{n}{2}+D} \binom{n}{i} \leq 2^{n-1} + \frac{D \cdot 2^n}{\sqrt{n}}$$

$$\#\text{ polynomials} \leq 3^{\left(2^{n-1} + \frac{D \cdot 2^n}{\sqrt{n}}\right)}$$

To ensure #poly $\geq$ #functions need

$$2^{n-1} + \frac{D \cdot 2^n}{\sqrt{n}} \geq |S| \geq (1-\epsilon) 2^n$$

$$\Rightarrow D \geq \sqrt{n} \cdot \left(\frac{1}{2} - \epsilon\right) \quad \cdots \quad \boxtimes$$

(LEMMA 2)

Putting things together

Set $\epsilon = \frac{1}{4}$ & get

$$(\log s)^d \geq \sqrt{n}$$

$$\Rightarrow \log s \geq n^{\frac{1}{2d}}$$

$$\Rightarrow s \geq 2^{n^{\frac{1}{2d}}}$$

Conclusions: • Exponential Lower Bound On Parity.

• Could throw in $\oplus \pmod 3$ gates for free

• Major Open Question: Lower Bound for $\oplus_5$ using $\oplus_6$ gates.

Probability Background

Events

$$Pr[E_1 \cup E_2] \leq Pr[E_1] + Pr[E_2]$$

$$Pr[E_1 \cap E_2] = Pr[E_1] \cdot Pr[E_2]$$

↑ ↑ if these are independent

Random Variables

$$E[X_1 + X_2] = E[X_1] + E[X_2]$$

$$E[X_1 \cdot X_2] = E[X_1] \cdot E[X_2]$$

↑ ↑ if they are independent.

Tail Bounds (Convert Exp. ⇒ Prob.)

Markov: Assumes non-negative variable.

$$Pr[X \geq kE[X]] \leq \frac{1}{k}$$

Chebychev Assumes (identical) pairwise ind. variables $X_1 \ldots X_n$

$$Pr\left[\left(\frac{\sum x_i}{n} - E(x_i)\right)^2 \geq \epsilon \cdot Var(x_i)\right] \leq \frac{1}{\epsilon \cdot n}$$

CHERNOFF-HOEFFDING

ASSUMES BOUNDED IDENTICAL INDEPENDENT VARIABLES $X_1 \cdots X_n$

$$Pr\left[\left| \frac{\sum x_i}{n} - E(x_i) \right| \geq \epsilon \sqrt{VAR(x_i)} \right]$$

$$= \exp(-\epsilon^2 n) .$$