LECT 06

Note Title 2/25/2007

TODAY : Alternate Proof that Parity $\notin AC^0$.
[SMOLENSKY]

Ingredients
- Finite fields & polynomials
- Linear Algebra
- Randomization.

Why another proof ?

- Quantitatively stronger
- Qualitatively different (not so strongly dependent on properties of AND / OR gates)
- Useful techniques.

General Approach:

- Replace/Approximate gates by nicer functions
  Polynomials over finite fields
- Show circuit becomes simple
  "approximated" by low-degree polynomials
- Show parity is complex
  Can't be "approximated" by low-degree
  polynomials

Issues:

- Which field?
- What is approximation?
- Proving simplicity
  complexity

Which Field?

First Idea: How About $GF(2)$

[addition/multiplication modulo 2]

Unfortunately

$$Parity(x_1 \cdots x_n) = x_1 + x_2 + \cdots x_n$$

↑

Well approximated by degree 1 polynomial ... ☹

Better Idea:

- Use Any Other Field ! (for complexity)
- Use Any Finity Field (for simplicity)

Will Choose $GF(3) = \{-1, 0, 1\}$

Why Other Fields?

What does parity look like over $\mathbb{F}$?

Trick (Fundamental trick of Complexity Theory)

$\{0,1\} \longrightarrow \{1,-1\}$ by linear map $\longleftarrow$

$\Longrightarrow \quad x \longrightarrow 1-2x$

$\Longleftarrow \quad \frac{1+y}{2} \longleftarrow y$

$\text{parity}(x_1 \dots x_n) \longrightarrow \prod_{i=1}^{n} x_i$

$\longleftarrow$ doesn't work over $GF(2)$.

If $p(x_1 \dots x_n)$ computes parity

then $q(x_1 \dots x_n) = 1 - 2p\left(\frac{1+x_1}{2}, \dots \frac{1+x_n}{2}\right)$

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

But $\deg q = \deg p$! $\Rightarrow$ degree of p must be 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 input $x \in S$.

  (simplicity)

- Will prove parity cannot be approximated like this.

  (complexity)

Lemma 1: If C is a circuit of depth d & size S

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

$D \leq$???

& a set $S \subseteq \{0,1\}^n$ of

size $|S| \geq$??? $[(1-\epsilon)2^n]$

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

Idea:
- replace each gate probabilistically with polynomial of degree $k \approx \log \frac{S}{\epsilon}$
- for fixed input x to circuit C, show that polynomial computes gate w.p. $\geq 1 - \exp(-k)$. (prob. taken over poly!)

Conclude:

① C replaced by poly p of degree $\approx (\log \frac{s}{\epsilon})^d$

② for any x p computes C correctly w.p. $(1-\epsilon)$

(EXERCISE) $\Rightarrow$ p computes C correctly on some set S of size $\geq (1-\epsilon)2^n$.

Thus it suffices to show a degree k approximation to OR gate, must compute OR correctly w.p. $1 - \exp(-k)$

Polynomials & Approximate-Or

Exact-Or $(x_1 \cdots x_n)$

$$= 1 - \prod_{i=1}^{n} (1 - x_i)$$

Has degree n ☹

Approx-Or $_{\alpha_1 \cdots \alpha_n}(x_1 \cdots x_n)$ $\quad \alpha_i \in_R \mathbb{F}_q$ ↑ uniform independent

$$= \left(\sum \alpha_i x_i \right)^{q-1}$$

Claim: $\forall x_1 \cdots x_n$

$$\Pr_{\alpha_1 \cdots \alpha_n} \left[\text{APPROX-OR}(x_1 \cdots x_n) = \text{OR}(x_1 \cdots x_n) \right] \geq \frac{q-1}{q}$$

Proof: Obvious if $x_1 \cdots x_n = \bar{0}$; Assume o.w.

& so RHS = 1.

Hence $\left(\sum \alpha_i x_i \right)^{q-1} = 1 \iff \sum \alpha_i x_i \neq 0$

USEFUL GENERAL LEMMA:

[SCHWARTZ, ZIPPEL, DEMILLO-LIPTON]:

Let $p: \mathbb{F}^n \to \mathbb{F}$ be a non-zero polynomial of degree d. Let $S \subseteq \mathbb{F}$ be any finite set.

$$\Pr_{x \in S^n}\left[p(x) = 0\right] \leq \frac{d}{|S|}.$$

Proof: $(n = 1)$: $\Leftrightarrow$ Poly of deg. d has at most d roots

$(n > 1)$ $\Leftarrow$ Induction. (EXERCISE)

Back To Our Setting

$$p(\bar{x}) = \sum \alpha_i x_i$$

Argument ↗ ↖ Coefficients

$$\Pr[p(\bar{x}) = 0] \leq \frac{d}{|S|} = \frac{1}{q}$$

☒ (Proof of Claim & also Lemma 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 $X_1 \cdots X_n$

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

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