COM S 6810 Theory of Computing	February 12, 2009

Lecture 8: Circuit Lower Bounds II

Instructor: Rafael Pass — *Scribe: Igor Gorodezky*

In this lecture we prove an exponential lower bound on the size of constant-depth circuits computing the parity function. For the remainder of the lecture all circuits will have unbounded fan-in, and we will ignore $\neg$ gates when measuring the size of a circuit.

Define AC_0 to be the class of boolean functions computed by constant-depth, polynomial-size circuits using $\{\neg, \vee, \wedge\}$ gates with unbounded fan-in. Consider the parity function on n bits:

$$\text{PARITY}(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i \mod 2$$

One can show that PARITY can be computed by circuits of depth d and size $O(n2^{n^{1/(d-1)}})$. Naturally, we ask whether PARITY is in AC_0. In this lecture we answer this question in the negative by proving the following lower bound.

Theorem 1 *Any depth d circuit computing* PARITY *has size* $\Omega(2^{n^{1/(2d)}/2})$.

The first exponential lower bound for constant-depth circuits computing PARITY was proved by Yao in 1985 and was strengthened to near-optimality by Håstad in 1986. Here we prove a bound slightly weaker than Håstad's using a technique due to Razborov and Smolensky (1987). We will prove Theorem 1 by, roughly speaking, showing that small constant-depth circuits can be accurately approximated by low degree polynomials while PARITY cannot.

1 The main argument

In this section we state two key lemmas and use them to prove Theorem 1; the proofs of the lemmas are deferred to the next section. The proof of the theorem requires us to consider not only boolean functions but functions (in particular polynomials) over $\mathbb{F}_3^n$, where $\mathbb{F}_3 = \{-1, 0, 1\}$ is the field of order 3.

Our first lemma tells us that a small constant-depth circuit can be accurately approximated by a low degree polynomial over $\mathbb{F}_3^n$.

Lemma 2 *If C is a circuit of depth d and t is arbitrary then there exists a polynomial P over $\mathbb{F}_3^n$ of degree $(2t)^d$ that differs from C on at most a $|C|/2^t$ fraction of inputs.*

If we set $t = n^{1/(2d)}/2$ then Lemma 2 tells us that for any circuit C with $|C| < \frac{1}{100}2^{n^{1/(2d)}/2}$ there exists a degree $\sqrt{n}$ polynomial P over $\mathbb{F}_3^n$ such that $C(\vec{x}) = P(\vec{x})$ for at least 99% of bit strings $\vec{x} \in \{0,1\}^n$.

To prove Theorem 1 it would suffice to show that there cannot exist a degree $\sqrt{n}$ polynomial over $\mathbb{F}_3^n$ that approximates PARITY with such accuracy. This is a silly claim, however, since PARITY is defined as a *linear* function over $\{0,1\}^n$. Therefore our proof proceeds more carefully, using not PARITY itself but a high degree analogue.

Define the parity of a bit string in $\{-1,1\}^n$ to be

$$\widehat{\text{PARITY}}(\hat{x}_1, \dots, \hat{x}_n) = \prod_{i=1}^{n} \hat{x}_i$$

Conveniently, $\widehat{\text{PARITY}}$ has degree n, the maximum possible. Observe that if we map $\{0,1\}$ to $\{-1,1\}$ via $0 \leftrightarrow 1$ and $1 \leftrightarrow -1$ then we can relate PARITY and $\widehat{\text{PARITY}}$ by

$$\widehat{\text{PARITY}}(\hat{x}_1, \dots, \hat{x}_n) = 1 + \text{PARITY}(\hat{x}_1 - 1, \dots, \hat{x}_n - 1) \mod 3 \tag{1}$$

Our second lemma tells us that $\widehat{\text{PARITY}}$ cannot be well approximated by low degree polynomials over $\mathbb{F}_3^n$.

Lemma 3 *Every degree $\sqrt{n}$ polynomial over $\mathbb{F}_3^n$ differs from $\widehat{\text{PARITY}}$ on more than a $\frac{1}{100}$ fraction of inputs.*

The proof of the theorem now follows easily.

Proof of Theorem 1. Assume for the sake of contradiction that PARITY can be computed by a depth d circuit C with $|C| < \frac{1}{100}2^{n^{1/(2d)}/2}$. Then, by the discussion following Lemma 2, there exists a degree $\sqrt{n}$ polynomial P over $\mathbb{F}_3^n$ that agrees with PARITY on at least 99% of input strings in $\{0,1\}^n$.

Using the relation in equation (1), we can convert P into a degree $\sqrt{n}$ polynomial $\hat{P}$ that agrees with $\widehat{\text{PARITY}}$ on at least 99% of input strings in $\{-1,1\}^n$. This contradicts Lemma 3 and completes the proof. ■

2 Proving the lemmas

Proof of Lemma 2. Assume that C uses only $\neg$ and $\vee$ gates; this loses no generality since $x \wedge y = \neg(\neg x \vee \neg y)$ and we agreed not to count $\neg$ gates when measuring circuit size. We will approximate C by simulating its gates with polynomials over $\mathbb{F}_3^n$.

For the moment, fix an input string $\vec{x} \in \{0,1\}^n$. We begin by constructing a degree $(2t)^d$ polynomial P such that $P(\vec{x}) = C(\vec{x})$ with very high probability.

We can simulate each $\neg$ gate with a linear polynomial, since $\neg x = 1 - x$ for $x \in \{0,1\}$. We can naively simulate a $\vee$ gate on input bits $\{b_1, \ldots, b_k\}$ using a polynomial which we will call nOR:

$$\mathrm{nOR}(b_1, \ldots, b_k) = 1 - \prod_{i=1}^{k}(1 - b_i)$$

Clearly nOR cannot be used directly since its degree k might be very high. We can approximate it, however, using low degree polynomials as follows.

Choose $S \subseteq [k]$ uniformly at random and consider

$$q_S = \left(\sum_{j \in S} b_j\right)^2 \mod 3$$

We square the sum to avoid an output of -1. If $b_i = 0$ for all i then $q_S = (b_1 \vee \cdots \vee b_k) = 0$. If $b_i = 1$ for some i then clearly $(b_1 \vee \cdots \vee b_k) = 1$, while $q_S = 1$ with probability at least $1/2$: this is because we can define an injection from the subsets T for which $q_T = 0$ to the subsets S for which $q_S = 1$ by mapping $T \mapsto T \setminus \{b_i\}$ if $b_i \in T$ and otherwise mapping $T \mapsto T \cup \{b_i\}$.

We can amplify this effect by uniformly and independently choosing t subsets $\{S_1, \ldots, S_t\}$ and, writing q_i for q_{S_i}, simulating the $\vee$ gate with $\mathrm{nOR}(q_1, \ldots, q_t)$, which has degree $2t$. Since each q_i fails with probability at most $1/2$, we have

$$\mathrm{Prob}\left(\mathrm{nOR}(q_1, \ldots, q_t) \neq (b_1 \vee \cdots \vee b_k)\right) \leq 2^{-t}$$

Let P be the polynomial produced by approximating gates with polynomials as described above and composing those polynomials as per the circuit layout. Since each gate approximation fails on the (fixed) input $\vec{x}$ with probability at most 2^{-t}, we have

$$\mathrm{Prob}\left(P(\vec{x}) \neq C(\vec{x})\right) \leq |C| 2^{-t} \tag{2}$$

by the union bound, where the probability is over the possible choices of P.

Equation (2) holds for any fixed $\vec{x}$, therefore

$$\mathrm{Exp}\left(|\{\vec{x} \mid P(\vec{x}) \neq C(\vec{x})\}|\right) = \sum_{\vec{x} \in \{0,1\}^n} \mathrm{Prob}\left(P(\vec{x}) \neq C(\vec{x})\right) \leq 2^n \frac{|C|}{2^t}$$

Since the expectation is over P, we conclude that there exists a choice of P that differs from C on at most a $|C| 2^{-t}$ fraction of inputs. ■

Proof of Lemma 3. The proof is a straightforward counting argument. Assume for the sake of contradiction that there exists a degree $\sqrt{n}$ polynomial $\hat{P}$ that agrees with $\widehat{\text{PARITY}}$ on at least 99% of input strings. Thus if $S \subseteq \{-1,1\}^n$ is the set of inputs on which $\hat{P}$ and $\widehat{\text{PARITY}}$ agree, we have $|S| \geq \frac{99}{100}2^n$.

We claim that any function $f : S \to \mathbb{F}_3$ can be computed by a degree $\frac{n}{2}+\sqrt{n}$ polynomial. To see this, start with a polynomial interpolation of f:

$$P_f(\hat{x}_1,\ldots,\hat{x}_n) = \sum_{(\hat{y}_1,\ldots,\hat{y}_n)\in S} \left(f(\hat{y}_1,\ldots,\hat{y}_n) \prod_{i=1}^{n} (-\hat{x}_i\hat{y}_i - 1) \right)$$

Clearly P_f agrees with f on all of S. Moreover, we can replace any monomial in P_f of degree greater than $\frac{n}{2}$ by a polynomial of degree at most $\frac{n}{2}+\sqrt{n}$ as follows. If $\prod_{i\in I}\hat{x}_i$ is a monomial with $|I| > \frac{n}{2}$ then

$$\begin{aligned}
\prod_{i\in I}\hat{x}_i &= \prod_{i\in[n]}\hat{x}_i \prod_{j\in[n]\setminus I}\hat{x}_j \\
&= \widehat{\text{PARITY}}(\hat{x}_1,\ldots,\hat{x}_n) \prod_{j\in[n]\setminus I}\hat{x}_j \\
&= \hat{P}(\hat{x}_1,\ldots,\hat{x}_n) \prod_{j\in[n]\setminus I}\hat{x}_j
\end{aligned}$$

and the claim is proved since $|[n]\setminus I| \leq \frac{n}{2}$.

We conclude that if #pol is the number of degree $\frac{n}{2}+\sqrt{n}$ polynomials over $\mathbb{F}_3^n$, then #pol is at least the number of functions $f : S \to \mathbb{F}_3$. This implies

$$\#\text{pol} \geq 3^{|S|} \geq 3^{\frac{99}{100}2^n}.$$

Since every polynomial is a linear combination of monomials we have $\#\text{pol} = 3^{\#\text{mon}}$ where #mon is the number of monomials of degree at most $\frac{n}{2}+\sqrt{n}$. But

$$\#\text{mon} = \sum_{i=0}^{\frac{n}{2}+\sqrt{n}} \binom{n}{i} < \frac{99}{100}2^n$$

so $\#\text{pol} < 3^{\frac{99}{100}2^n}$, a contradiction. ∎