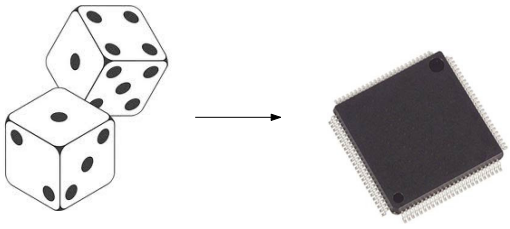
Lecture 9

# Linear Algebra Methods in Combinatorics

**with Applications to Geometry and CS**

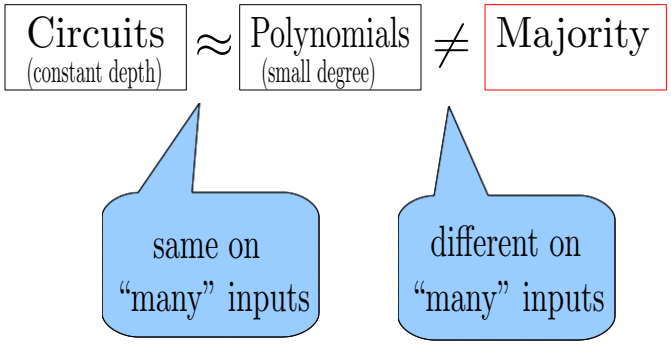


## Previous lecture and this lecture

We want to prove this theorem

**Theorem 1** (Razborov)**.** *Every circuit of depth c (constant) that computes the* ***majority*** *function using AND, OR, NOT, and PARITY gates with* ***unbounded fan-in****, must have* ***exponential size*** *(in the number of bits).*

The structure of the proof is something like this:



We count on how many inputs the two functions differ:

$$diff(f,g) \stackrel{\triangle}{=} |\{y \in \{0,1\}^n| \;\; f(y) \neq g(y)\}|$$

In the previous lecture we have seen this:

| small-degree polynomials $\neq$ $k$-threshold function |
|---|

**Lemma 2** (polynomials vs $k$-threshold)**.** *For $n/2 \leq k \leq n$, every polynomial of degree $\delta \leq 2k-n-1$ must differ from the threshold function on at least $\binom{n}{k}$ inputs.*

In this lecture we shall prove the following:

| constant-depth circuits $\approx$ low-degree polynomials |
|---|

**Lemma 3** (circuits vs polynomials)**.** *For every depth-$d$ circuit with AND, OR, NOT and PARITY gates (of unbounded fan-in) there exists a polynomial $p$ of degree $\delta \leq r^d$ which differs from $C$ on at most $|C|2^n/2^r$ inputs.*

We can already see how these two results imply Theorem 1:

- Take $k = n/2 + \sqrt{n}$ so that $\binom{n}{k} \geq 2^n/\sqrt{n}$.
- Set $r \approx n^{1/2d}$ so that $\delta \leq 2k-n-1$.

Then

$$diff(p,f_k) \leq diff(p,C) + diff(C,f_k)$$

If $C$ computes the threshold function $f_k$ then $diff(C,f_k) = 0$ and the two lemmas tell us

$$\frac{2^n}{\sqrt{n}} \leq diff(p,f_k) \leq diff(p,C) \leq |C|\frac{2^n}{2^r}$$

and thus

$$|C| \geq \frac{2^r}{\sqrt{n}} \approx \frac{2^{n^{1/2d}}}{\sqrt{n}}$$

Since any circuit computing **majority** can be used to compute $f_k$ by adding some "dummy inputs 0":

| Depth-$d$ circuits (using AND, OR, NOT and PARITY gates of unbounded fan-in) that compute the majority function must have size $2^{\Omega(n^{1/2d})}$. |
|---|

# 1 Proof of Lemma 3 – probabilistic argument

We shall approximate every bounded depth circuit by some low-degree polynomial. Suppose the circuit we want to approximate is the AND of $n$ variables

$$p(x) = x_1 \cdots x_n$$

and for this purpose we use this ("strange") polynomial over $\mathbb{F}_2$:

$$\hat{p}(x) = 1 + (1 + x_1) + \cdots + (1 + x_n)$$

The answer is correct for the input $x = \mathbf{1}$

$$p(\mathbf{1}) = 1 = \hat{p}(\mathbf{1})$$

Now pick a **random** subset $R$ of the variables by including the $i^{th}$ variable with probability $1/2$ independently from the other variables and look at

$$\hat{p}_R \stackrel{\triangle}{=} 1 + \sum_{i \in R} (1 + x_i)$$

**Exercise 1.** *Show that,* ***for every input*** $a \neq \mathbf{1}$

$$\Pr_R[\hat{p}_R(a) = 1] = 1/2$$

***Hint:*** *We are in the case* $a_i = 0$ *for some* $i$.

Repeat $r$ times

Pick $r$ subsets $\mathsf{R} = \{R_1, \ldots, R_r\}$ at random independently as above and look at

$$\hat{p}_{\mathsf{R}}(x) \stackrel{\triangle}{=} \hat{p}_{R_1}(x)\hat{p}_{R_2}(x) \cdots \hat{p}_{R_r}(x)$$

Then, **for every input** $a$

$$\Pr_{\mathsf{R}}[\hat{p}_{\mathsf{R}}(a) \neq p(a)] \leq 1/2^r \tag{1}$$

and the **degree of** $\hat{p}_{\mathsf{R}}$ **is at most** $r$.

**Exercise 2.** *Prove (1).*

For every fixed input many polynomials are good
$\Downarrow$
One polynomial is good for many inputs

Our probability space is the set $\Omega$ of all $r$-tuples $\mathsf{R}$ of subsets $R_1, \ldots, R_r$ of variables:

$$\Omega = \underbrace{\{0,1\}^n \times \{0,1\}^n \times \cdots \times \{0,1\}^n}_{r \text{ times}}$$

For every input $a$, we define the random variable $X_a : \Omega \to \mathbb{R}$

$$X_a(\mathsf{R}) = \begin{cases} 1 & \text{if } \hat{p}_{\mathsf{R}}(a) \neq p(a) \\ 0 & \text{otherwise} \end{cases}$$

Consider the sum over all possible inputs $a$

$$X \stackrel{\triangle}{=} \sum_{a \in \{0,1\}^n} X_a$$

By linearity of expectation

$$\mathbb{E}[X] = \sum_a \mathbb{E}[X_a] = \sum_a \Pr[X_a = 1] \leq 2^n/2^r$$

A random variable cannot be always strictly larger than its expectation, that is, there is one $\omega \in \Omega$ such that

$$X(\omega) \leq \mathbb{E}[X]$$

In our case $\omega = \mathsf{R}^*$ meaning that

For every positive integer $r$, there exists a polynomial $\hat{p}_{\mathsf{R}^*}$ of degree at most $r$ which differs from the AND of $n$ variables on at most $2^n/2^r$ inputs.

**Lemma 4** (low degree polynomials)**.** *Let $p(x) \stackrel{\triangle}{=} p_1(x) \cdot p_2(x) \cdots p_m(x)$, where $p_1, \ldots, p_m$ are polynomials of degree at most $d$. For any positive integer $r$, there exists a polynomial $\hat{p}$ such that*

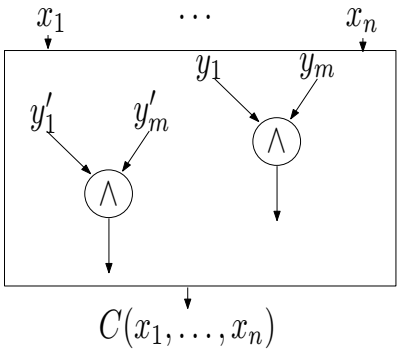
1. *The degree of $\hat{p}$ is at most $rd$*
2. *$\hat{p}$ differs from $p$ on at most $2^n/2^r$ inputs.*

*Proof.* **Exercise!!**. □

## 1.1 Approximate an entire circuit – Lemma 3

Approximating the AND gate is not enough

We first show that one cannot approximate an entire circuit by approximating "locally" every single gate. The output of an AND gate can be also seen as the polynomial $p(y) = y_1 \cdots y_m$ of its "direct inputs in the circuit":




We have seen above how to approximate a single AND gate, which means that there is a polynomial $\hat{p}$ which differs from $y_1 \cdots y_m$ on at most $2^m/2^r$ values. We use this result to approximate an entire circuit.

Lemma 4 $\Rightarrow$ Lemma 3

Each gate outputs some "intermediate" function $g_i(x_1, \ldots, x_n)$ of the **input of the circuit**, and the output of the circuit is the output of the "last" gate

$$C(x) = g_s(x)$$

where $s = |C|$ is the number of gates. If we replace the $i^{th}$ function $g_i(x_1, \ldots, x_n)$ by some other function $\hat{g}_i(x_1, \ldots, x_n)$, then the "new circuit" $\hat{C}$ differs from the previous one on at most $diff(g_i, \hat{g}_i)$ inputs. This argument can be used to derive Lemma 3 from Lemma 4 (**Exercise!!**).