Lecture 8

Linear Algebra Methods in Combinatorics

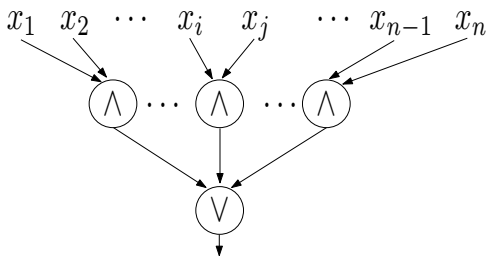
with Applications to Geometry and CS

1 Circuits and simple functions

Consider the simple k-**threshold function** which tells us if the number of bits in input equal to 1 is at least k:

$$f_k(x) \stackrel{\triangle}{=} \begin{cases} 1 & \text{if } x = (x_1, \ldots, x_n) \text{ has } k \text{ entries equal to } 1 \\ 0 & \text{otherwise} \end{cases}$$

The **majority** function tells us if at least half of the bits are set to 1, the case $k = n/2$. This circuit computes the 2-threshold function:



and it has **depth** 2 (maximum number of gates between the input and the output) and **size** $O(n^2)$ (number of gates).

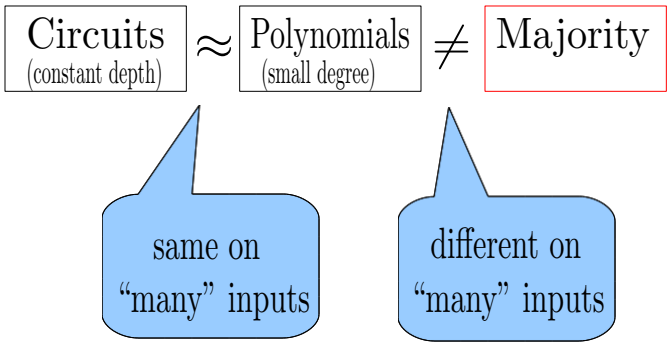
Exercise 1. *Construct a circuit of depth* 2 *to compute the* k*-threshold function, using gates with* ***unbounded*** *fan in. What is the size of the circuit for the majority function* ($k = n/2$)*?*

2 Razborov lower bound

Let us restrict to circuits with **constant depth**. Of course, we need gates with **unbounded fan in**. We can use all "standard gates" (AND, OR, NOT) plus PARITY gates. Here is what happens:

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:



Slightly more formally we count on how many inputs the two functions differ:

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

and prove something like this:

$C =$"circuit" $p =$ "polynomial" $MAJ =$"majority function"

"$size(C)$" $\times$ "small" $\geq diff(C,p)$ and $diff(p, MAJ) \geq$ "large"

So if C computes MAJ then just because "$C = MAJ$"[1] we can conclude

$$\text{"}size(C)\text{"} \geq \frac{\text{"large"}}{\text{"small"}}$$

(Think of "large = exponential" and "small = polynomial" for now.)

Circuits and polynomials. To see the correspondence between circuits and polynomials, consider simple gates:

$$NOT(x_i) \Leftrightarrow 1 + x_i \quad (1)$$
$$XOR(x_1, \ldots, x_n) \Leftrightarrow x_1 + \cdots + x_n \quad (2)$$
$$AND(x_1, \ldots, x_n) \Leftrightarrow x_1 \cdots x_n \quad (3)$$

We consider polynomials in n variables over $\mathbb{F}_2$

For the AND gate (a circuit of depth 1!) the degree of the polynomial is not small. In the next lecture we shall see how to approximate constant-depth circuits with small-degree polynomials.

3 Razborov proof (Part I – linear algebra)

We look at the k-**threshold** function which tells us if the number of 1's in input is at least k. The majority corresponds to "$k = n/2$", but in the sequel we first **look at the case "$k > n/2$"**.[2]

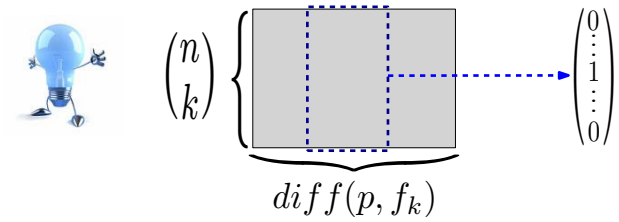
small-degree polynomials $\neq$ k-threshold function

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

[1] That is $MAJ(y) = C(y)$ for all inputs y.

[2] We shall prove that "$k = n/2 + \sqrt{n}$" is hard and then use this for the majority.

Proof Idea. We construct some matrix that "looks like this":

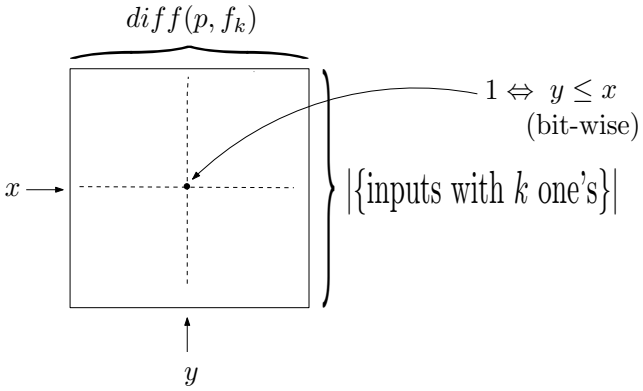


with the key property being that a linear combination of (some) columns generates each vector $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$. Then we simply use the linear algebra bound:

$$e_1, \ldots, e_{\binom{n}{k}} \in \text{span}(\underbrace{c_1, \ldots, c_m}_{\text{columns}})$$

and obtain $\binom{n}{k} \leq m = diff(p, f_k)$ □

Proof of Lemma 2. We shall construct a matrix with rows corresponding to inputs whose number of 1's is k, and columns to the "bad inputs" for our polynomial:



and so we put a "1" is our matrix if and only if the bad input y has a subset of the 1's of the hard input x (in symbol $y \leq x$ means that $x_i \leq y_i$ for all i). Our matrix has the following "magic property":

Claim 3. *We can obtain all vectors e_i by adding a subset of the columns.*

That is

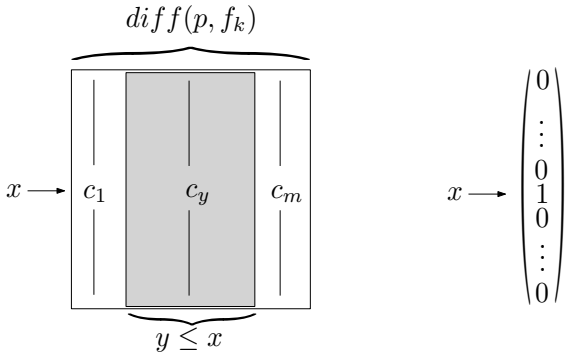
$$e_1, \ldots, e_{\binom{n}{k}} \in \text{span}(c_1, \ldots, c_m)$$

and the linear algebra bound implies

$$\binom{n}{k} \leq m = diff(p, f_k)$$

So it only remains to prove this claim.

Proof of Claim 3. This picture shows which columns to add to obtain the vector e_i having 1 in the position corresponding to x:



Let us look at the sum of these columns. To this end, let

$$DIFF \triangleq \{y| \;\; p(y) \neq f_k(y)\}$$

be the set of inputs where p and f_k are different (so $diff(p, f_k) = |DIFF|$). For any x and x'

$$\sum_{\substack{y \in DIFF \\ y \leq x}} m_{x',y} = \sum_{\substack{y \in DIFF \\ y \leq x,\ y \leq x'}} 1 \quad = \quad \sum_{\substack{y \in DIFF \\ y \leq x,\ y \leq x'}} f_k(y) + p(y) \tag{4}$$

$$= \sum_{\substack{y \in \{0,1\}^n \\ y \leq x,\ y \leq x'}} f_k(y) + p(y) \tag{5}$$

$$= \sum_{\substack{y \in \{0,1\}^n \\ y \leq x,\ y \leq x'}} f_k(y) + \sum_{\substack{y \in \{0,1\}^n \\ y \leq x,\ y \leq x'}} p(y) \tag{6}$$

Equality (4) holds because $f_k(y) + p(y) = 1$ if and only if $f_k(y) \neq p(y)$. Equality (5) holds because, for $y \notin DIFF$, $f_k(y) + p(y) = 0$.

The **first term in (6) produces the identity matrix:**

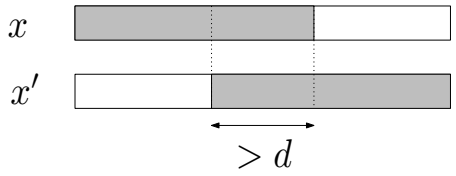
$$\sum_{\substack{y\in\{0,1\}^n \\ y\le x,\ y\le x'}} f_k(y) = \begin{cases} 1 & \text{for } x' = x \\ 0 & \text{for } x' \neq x \end{cases} \tag{7}$$

while **the second term in (6) is always** 0**:**

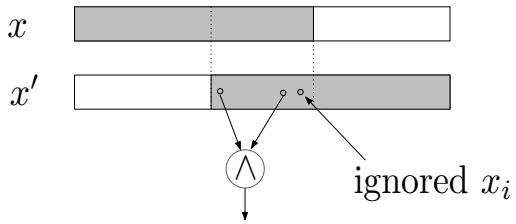
$$\sum_{\substack{y\in\{0,1\}^n \\ y\le x,\ y\le x'}} p(y) = 0 \tag{8}$$

Exercise 2. *Prove (7).*
Hint: *Recall that x and x' have exactly k 1's.*

Equality (11) is due to the fact that the polynomial has degree d, while the number of 1's common to both x and x' is at least $d+1$:



(This is because $k = n/2 + q$ and $d < 2k - n = 2q$.) To see the idea, suppose our polynomial is simply the "AND" of d variables (a **monomial**):



Exercise 3. *Prove (11).*

The claim follows from (7-11). □

The proof of the claim also completes the proof of the main lemma. □

4 What to remember and where to look

We have used (again) this: **linear algebra bound** but this time to prove a **lower bound** (Lemma 2).

Linear Algebra Bound

$$\underbrace{v_1, \ldots, v_n}_{\text{independent}} \in \text{span}(a_1, \ldots, a_m) \Longrightarrow n \leq m$$

Let us see the difference with our previous applications:

- Oddtown, Restricted intersection Theorems (RW), Bollobás Theorem, Two-distance set.

In these cases we prove something like "our objects cannot be too many" (**upper bound**) so we mapped our objects into $v_1, \ldots, v_n$. Today, instead, we have mapped our objects (the "mistakes" of a polynomial p computing f_k) into "$a_1, \ldots, a_m$" and obtained a lower bound.

The other problem for which we have proven a lower bound was the Jigsaw Problem with Graphs in Lecture 3.

The proof of Lemma 2 can be found in [Juk01, Lemma 14.8, p. 174-176].

References

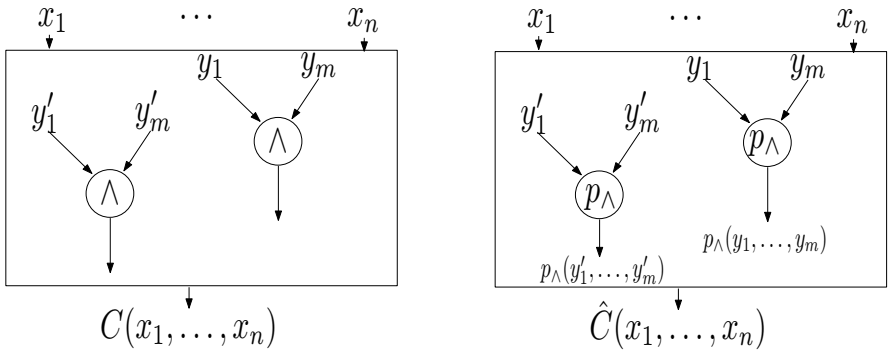
[Juk01] S. Jukna. *Extremal combinatorics: with applications in computer science*. Springer Verlag, 2001.

Exercises
(during next exercise class - 19.4.2018)

We shall discuss and solve together the following exercise:

Exercise 4. *Suppose that for every m there is a low-degree polynomial $p_\wedge$ which **differs** from the AND of m bits **on at most** $2^m/2^r$ of the possible $0/1$-inputs.*

I use this polynomial to "approximate" an entire circuit in the "obvious" way. For each AND gate consider its "direct inputs in the circuit" (left figure below):



(each y_i and y'_i is either the output of another gate or one of the variables) Replace each gate by the polynomial $p_\wedge$ on the "direct inputs" of the gate (see right figure above).

***Claim:** The circuit C and the resulting polynomial $\hat{C}$ differ on **at most** $|C| \cdot 2^n/2^r$ inputs.*

Proof. For each intermediate result (AND gate) in C, there are at most $2^n/2^r$ inputs for which this intermediate result is different in $\hat{C}$. □

*The claim is **false**. Explain why and find a counterexample.*

Exercise Set 8 – FS18
(Linear Algebra Methods in Combinatorics)

You can submit solutions **also by email** by next lecture – **26.4.2018**. These exercises are **non-graded** but you get feedback on your submitted solutions.

Some exercises on Lecture 7.

Exercise 1. *Recall that a family is said* ***critical*** *if the following two conditions hold (see lecture notes):*

CR1: *We need $s+1$ nodes to cover all of its members;*

CR2: *As soon as we remove* ***any one*** *member from the family, then s nodes are enough.*

Bollobás uniform theorem (Theorem 3 in Lecture 7) implies that no r-uniform critical family can have more than $\binom{s+r}{r}$ members. Prove that this result is false for r-uniform families that satisfy ***only CR1****: show that it is possible to construct an* ***arbitrarily large*** *r-uniform family satisfying* ***CR1 only*** *and such that $s+1$ nodes are enough to cover all members of the family.*

Exercise 2. *Let $\mathcal{F}$ be an r-uniform set system of size larger than $\binom{s+r}{r}$. Prove that there exists one $A \in \mathcal{F}$ such that*

$$\mathcal{F}' := \mathcal{F} \setminus A \quad \text{and} \quad \mathcal{F}$$

have the ***same covering number****, that is, they can be both covered by s nodes, and $s-1$ are not enough.*

Exercise 3. *Construct a critical set for $r = 2$ and $s = 2$ matching the bound of Bollobás theorem.*

Some exercises on Lecture 8.

Exercise 4. *Give a formal proof of (11) used in the Proof of Claim 3 in the lecture note. We restate (11) here for convenience:*

If p is a polynomial over $\mathbb{F}_2$ in n variables and of degree at most $2k - n - 1$, then

$$\sum_{\substack{y \in \{0,1\}^n \\ y \leq x,\ y \leq x'}} p(y) = 0$$

where x and x' are two inputs with exactly k 1's, for $k > n/2$, and '$y \leq x$' is the bitwise 'less than or equal' (similarly for $y \leq x'$).

Exercise 5. *In the proof of Claim 3 I'm tempted to take this "**shortcut**":*

For any x and x'

$$\sum_{\substack{y \in DIFF \\ y \leq x}} m_{x',y} = \sum_{\substack{y \in DIFF \\ y \leq x,\ y \leq x'}} 1 \quad = \quad \sum_{\substack{y \in DIFF \\ y \leq x,\ y \leq x'}} f_k(y) + p(y) \tag{9}$$

*The **first term in (9) produces the identity matrix:***

$$\sum_{\substack{y \in DIFF \\ y \leq x,\ y \leq x'}} f_k(y) = \begin{cases} 1 & \text{for } x' = x \\ 0 & \text{for } x' \neq x \end{cases} \tag{10}$$

*while **the second term in (9) is always** 0**:***

$$\sum_{\substack{y \in DIFF \\ y \leq x,\ y \leq x'}} p(y) = 0 \tag{11}$$

By putting the three equations together we get Claim 3.

Explain why this proof is wrong and where it does not work.