Exercise Set 9 – FS18
(Linear Algebra Methods in Combinatorics)

These exercises will be **graded**. Please write your solutions using **LaTeX** and send them no later than **6.5.2018 (time 23:59)** to barbara.geissmann@inf.ethz.ch.

This exercise is about lecture 7:

Exercise 1 (2 Points). *Bollobás theorem says that, for every positive integers s and r, no critical family can have more than $\binom{r+s}{r}$ members. Prove that this result is always tight, that is, for every r and s there exists a critical family with $\binom{r+s}{r}$ members.*

Note: *for every r and s describe how the family is defined and prove that it is critical with respect to these parameters.*

Two exercises on the proof of Razborov Theorem (proof of Lemma 2 in Lecture 8):

Exercise 2 (1 Point). *Let f and g be two Boolean functions in n variables and let $X \subseteq \{0,1\}^n$ be a subset of inputs such that*

$$\forall x, x' \in X \qquad \sum_{\substack{y \in \{0,1\}^n \\ y \leq x,\ y \leq x'}} f(y) + g(y) = \begin{cases} 1 & \text{for } x' = x \\ 0 & \text{for } x' \neq x \end{cases}$$

Prove that f and g must differ in at least $|X|$ inputs.

Note: *Here $y \leq x$ means that $y_i \leq x_i$ for $i = 1, \ldots, n$ (similarly for $y \leq x'$).*

Exercise 3 (2 Points). *Let p be a polynomial in n variables (over $\mathbb{F}_2$) of degree at most d. Prove that, for any $x, x' \in \{0,1\}^n$ that have more than d 1's in common (i.e. $|\{i|\ x_i = 1 = x'_i\}| > d$), the following identity holds:*

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

Note: *Here $y \leq x$ means that $y_i \leq x_i$ for $i = 1, \ldots, n$ (similarly for $y \leq x'$).*

An exercise on proving lower bounds via the linear algebra bound:

Exercise 4 (1 Point). *In Lecture 3 we have shown the following* ***lower bound*** *for a "jigsaw puzzle with graph": the number m of bipartite graphs that "cover" the complete graph on n nodes must satisfy $m \geq n-1$. Show how you can do the same proof directly from the linear algebra bound,* ***without using the rank inequality****.*

<u>Details:</u> We have the bipartite graphs and (see the proof) each of them corresponds to a matrix A_i of rank 1. The matrix $S = A_1 + \cdots + A_m$ has rank at least $n-1$. Given these things (you don't need to reprove them), show that $m \geq n-1$ by applying the linear algebra bound:

$$\underbrace{v_1, \ldots, v_k}_{independent} \in span(a_1, \ldots, a_l) \Longrightarrow k \leq l$$

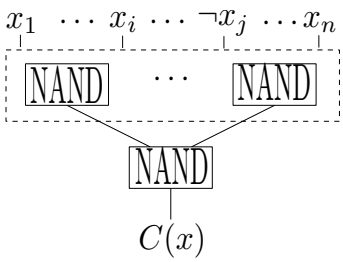
What are the v_i's, why are them independent, and what are the a_i's?

Another exercise on circuits vs polynomials:

Exercise 5 (3 Points). *We consider polynomials in n variables over $\mathbb{F}_2$. Suppose we have proven this result saying that certain polynomials p can be approximated well by some lower-degree polynomial $\hat{p}$:*

> ***Theorem.*** Let $p(x) \triangleq p_1(x) \cdot p_2(x) \cdots p_m(x)$, 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.

Consider an arbitrary depth-2 circuit C using only NAND gates of unbounded fan-in and of size s (the number of NAND gates is s):



(The gates on the top level can be connected to any subset of literals – input variables or their negations. For the sake of simplicity, the negations of the variables are given for free – we do not count these NOT gates in the size of the circuit.)

Prove that, for every positive integer r*, there exists a polynomial* $\hat{p}$ *of degree at most* r^2 *which differs from the output of the circuit on at most* $s2^n/2^r$ *inputs. (**Hint:** look at what happens for a circuit consisting of a single NAND gate – a depth-1 circuit.)*