Assignment 7, Complexity Theory, WiSe 16/17

Markus Bläser, Anurag Pandey, Harry Zisopoulos
http://www-cc.cs.uni-saarland.de/course/56/

Due: Jan 12, 2016

Exercise 7.1 a) Let C be an arithmetic circuit computing a polynomial $p(X_1, \ldots, X_n)$ such that the degree of any variable is $< d$. Let Y be a new variable and let $q(Y) = p(Y, Y^d, Y^{d^2}, \ldots, Y^{d^n})$. Prove that q is nonzero iff p is nonzero.
(It might be easier to show that there is a bijection between the monomials of p and q.)

b) Prove that if C has size s, then there is a circuit C' of size $\mathrm{poly}(s)$ computing q.

c) An arithmetic circuit is called variable-free, if every leaf is labeled with a constant. Such a variable-free circuit just computes a number. Prove that ACIT is polynomial-time reducible to the identity testing of variable-free circuits.

Exercise 7.2 Let C be a circuit computing a multilinear polynomial $p(X_1, \ldots, X_n)$, that is, every variable has degree ≤ 1.

a) Let Y be a new variable. Choose $e_i \in \{1, \ldots, 2n\}$ uniformly at random and set $r(Y) = p(Y^{e_1}, \ldots, Y^{e_n})$. Prove that if p is nonzero, then r is nonzero with probability $\geq 1/2$. What is (an upper bound for) the degree of r?

b) Use the previous item to design a randomized algorithm for identity testing of multilinear polynomials.

Exercise 7.3 The characteristic polynomial of a matrix A is defined as $c_A(X) = \det(A - X \cdot I)$ where I is the identity matrix. Let $c_A(X) = s_{A,0}X^n + s_{A,1}X^{n-1} + \cdots + s_{A,n}$.

a) Show that

$$s_{A,0} = (-1)^n$$
$$s_{A,k} = \frac{1}{k}\sum_{i=1}^{k}(-1)^{i-1}s_{A,k-i}\,\mathrm{trace}(A^i), \qquad 1 \leq k \leq n.$$

b) Show that $s_{A,n} = \det A$.

c) Show that there is a logarithmic space uniform family of Boolean circuits of polynomial size and polylogarithmic depth that computes the determinant of a matrix A. (Assume that A has dimension $n \times n$ and entries with $p(n)$ bits for some polynomial p.)