Assignment 9, Complexity Theory, SoSe 15

Markus Bläser, Holger Dell, Karteek Sreenivasaiah
http://www-cc.cs.uni-saarland.de/course/47/

Due: July 1, 2015, 11:00

Exercise 9.1 a) Prove the following: Any arithmetic circuit of size s computes polynomials of degree at most 2^{s-1}.

b) Construct an arithmetic circuit of size s that computes a polynomial of degree 2^{s-1}

c) Consider a circuit of size s and let c be an upper bound for the absolute values of the constants in C. Assume we evaluate the circuit at a point $(a_1, \ldots, a_n)$ with $|a_\nu| \leq d$, $1 \leq \nu \leq n$. Then $|C(a_1, \ldots, a_n)| \leq O(\max\{c, d\}^{2^s})$.

Exercise 9.2 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

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

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.)

Definition 1 *A family H of functions $h : \Sigma^n \to \Sigma^m$ is called a family of k-wise uniform (or k-wise independent) hash functions if for all mutually distinct $x_1, \ldots, x_k \in \Sigma^n$ and all $a_1, \ldots, a_k \in \Sigma^m$ we have*

$$\Pr_{h\sim H}\Big(\forall i.h(x_i) = a_i\Big) = \frac{1}{|\Sigma|^{km}}$$

Exercise 9.3 Let $\Sigma = \mathrm{GF}(q)$ be the finite field with q elements and let k be a positive integer. Let H be the set of all polynomials over Σ that have degree less than k, that is, each function has the form $h(x) = \sum_{i=0}^{k-1} c_i x^i$. Prove that H is a k-wise uniform family of hash functions.