Problem Set-2

Date : Oct 20 CS229r :Arithmetic Circuits
Due : Nov 17 Fall 2017, Harvard University

---

1. Let $P \in \mathbb{F}[\mathbf{x}]$ be a degree d polynomial which is not identically zero. Let $S \subseteq \mathbb{F}$ be an arbitrary subset such that $|S| \geq d$. For a uniformly random $\mathbf{a} \in S^n$, show that $P(\mathbf{a}) = 0$ with probability at most $\frac{d}{|S|}$.

2. For this problem, we work over a large enough field $\mathbb{F}$. Assume that we have access to an oracle, which takes as input an arithmetic circuit C and correctly tells us if C is identically zero or not. Using this oracle, design an algorithm with the following properties.

   - It takes as input parameters d, n and an arithmetic circuit C of degree d in n variables.
   - If C is not identically zero, then it outputs a point $\mathbf{a} \in \mathbb{F}^n$ such that $C(\mathbf{a}) \neq 0$.
   - It runs in time $\mathsf{poly}(n, d, \text{size}(C))$.

3. Recall the notion of Newton identities we saw in the class. Using Newton identities, show that over fields of characteristic zero, the monomial $x_1 \cdot x_2 \cdots x_n$ can be computed by a depth-4 powering circuit (a depth-4 circuit where every product gate is a powering gate) of size at most $2^{O(\sqrt{n})}\mathsf{poly}(n)$. You might need to use the fact that the number of non-negative integral solutions of $\sum_{i=1}^{n} a_i \cdot i = d$ is $(2^{O(\sqrt{d})})$.

4. Using the ideas in the above problem, show that over fields of characteristic zero, if a homogeneous polynomial of degree d in n variables can be computed by a (possibly non-homogeneous) depth-3 circuit of size s, then it can be computed by a homogeneous depth-5 circuit of size at most $2^{O(\sqrt{d})}\mathsf{poly}(s, d, n)$.

5. Over the field of complex numbers, show that if a homogeneous polynomial P of degree d in n variables can be computed by a circuit of size $\mathsf{poly}(n)$, then it can be computed by a (possibly non-homogeneous) depth-4 circuit of size $n^{O(d^{1/3})}$.