cs579: Computational Complexity	Assigned: *Mon., Mar. 26, 2018*

Problem Set #5

Prof. Michael A. Forbes — Due: *Mon., Apr. 9, 2018 (3:30pm)*

1. Let $\mathbb{F}$ be a field (such as the real or complex numbers), and let $\mathbb{F}[x_1, \ldots, x_n]$ be the ring of n-variate polynomials. A monomial $\overline{x}^{\overline{a}} = x_1^{a_1} \cdots x_n^{a_n}$ has *(total) degree* $a_1 + \cdots + a_n$ (denoted deg) and *individual degree* $\max_i a_i$ (denoted ideg). The *(total) degree* and *individual degree* of a polynomial $f(\overline{x}) = \sum_{\overline{a}} \alpha_{\overline{a}} \overline{x}^{\overline{a}}$ (with $\alpha_{\overline{a}} \in \mathbb{F}$) are the maximum of the respective degrees over all monomials $\overline{x}^{\overline{a}}$ where $\alpha_{\overline{a}} \neq 0$.

   It is a basic fact in algebra that a non-zero univariate polynomial $f(x)$ of degree $\leq d$ has at most d roots, that is, points α in $\mathbb{F}$ where $f(\alpha) = 0$. The *Schwartz-Zippel Lemma* is a generalization to non-zero multivariate polynomials $f \in \mathbb{F}[x_1, \ldots, x_n]$, showing that for any set $S \subseteq \mathbb{F}$, the number of roots in $S^n = \{(\alpha_1, \ldots, \alpha_n) : \alpha_i \in S\}$ is small. One can phrase this result about the probability that a uniformly random point in S^n is a root of f.

   (a) (Schwartz version) Show that for non-zero $f \in \mathbb{F}[x_1, \ldots, x_n]$

   $$\Pr_{\overline{\alpha} \leftarrow S^n}[f(\overline{\alpha}) = 0] \leq \frac{\deg f}{|S|} \ .$$

   Find a polynomial where this bound is tight.

   (b) (Zippel version) Show that for non-zero $f \in \mathbb{F}[x_1, \ldots, x_n]$,

   $$\Pr_{\overline{\alpha} \leftarrow S^n}[f(\overline{\alpha}) = 0] \leq 1 - \left(1 - \frac{\operatorname{ideg} f}{|S|}\right)^n \ .$$

   Find a polynomial where this bound is tight.

2. (Arora-Barak 12.7) Let $f : \{0,1\}^n \to \{0,1\}$ be a boolean function. The *degree* of f over a field $\mathbb{F}$ (denoted $\deg_{\mathbb{F}} f$) is the minimum degree of a polynomial $p \in \mathbb{F}[x_1, \ldots, x_n]$ such that $f(\overline{x}) = p(\overline{x})$ for all $\overline{x} \in \{0,1\}^n$. Show that for any field $\mathbb{F}$, $\deg_{\mathbb{F}} f \leq D(f)$, where $D(f)$ is the deterministic decision-tree complexity of f. Conclude that $\deg_{\mathbb{F}} f \leq n$ for any n-variate boolean function.

3. (Arora-Barak 12.5) Let $f : \{0,1\}^n \to \{0,1\}$ be a boolean function. For any field $\mathbb{F}$, show that there is a *unique* polynomial $p \in \mathbb{F}[x_1, \ldots, x_n]$ with $\operatorname{ideg} p \leq 1$, such that $f(\overline{x}) = p(\overline{x})$ for all $\overline{x} \in \{0,1\}^n$.

4. (Arora-Barak 13.13) Let $G = (V, E)$ be an undirected graph. Consider the following communication problem. Alice receives a clique $C \subseteq V$ in G, while Bob receives an independent set $I \subseteq V$. They must then communicate to compute $|C \cap I|$ (note that this is either 0 or 1). Prove a $O(\log^2 |V|)$ upper bound on the deterministic communication complexity of this problem.

Some hints.

1. Induction on the number of variables. Split $\overline{x} = (y, \overline{z})$, and decompose $f(y, \overline{z}) = \sum_{i=0}^{d} f_i(\overline{z}) y^i$, where $f_d(\overline{z})$ is a non-zero polynomial. When picking $\overline{\alpha} = (\beta, \overline{\gamma})$ at random, condition on whether $f_d(\overline{\gamma})$ is zero or non-zero.

3. Use the solutions and ideas of problems 1 and 2.

4. Proceed in $O(\log |V|)$ rounds of $O(\log |V|)$ communication. Suppose $v \in C \cap I$, condition on the degree of this vertex (large vs small).