Algebraic Techniques in TCS (Fall'21) Assigned: October 6, 2021

Homework 2

Instructor: *Josh Alman* Due: October 19, 2021 at 3:59 pm

Collaboration on homework is encouraged. However, you must write up solutions by yourself and understand everything that you hand in. For each question on the problem set, please write a list of everyone you collaborated on that problem with. You may not seek out answers from other sources without permission.

On all the problems, you may use without proof the following result we discussed in class, which follows from the Chernoff bound:

Lemma 1. *There is a constant $c > 0$ such that, for every $\varepsilon \in (0, 1/2)$, and every sufficiently large integer n, we have*

$$\sum_{i=0}^{\frac{n}{2} - c\sqrt{n \log(1/\varepsilon)}} \binom{n}{i} \leq \varepsilon \cdot 2^n.$$

1 Low-dimensional Orthogonal Vectors

Recall the Orthogonal Vectors problem: Given as input $2n$ vectors $x_1, \ldots, x_n, y_1, \ldots, y_n \in \{0,1\}^d$ in d dimensions, determine whether there are $i, j \in \{1, 2, \ldots, n\}$ such that $\langle x_i, y_j \rangle = 0$, where the inner product is taken over $\mathbb{Z}$.

In this problem we'll design an algorithm for the Orthogonal Vectors problem by using a closely-related matrix $R_d \in \{0,1\}^{2^d \times 2^d}$ defined recursively as follows:

$$R_1 := \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix},$$

and for $d \geq 2$,

$$R_d := \begin{bmatrix} R_{d-1} & R_{d-1} \\ R_{d-1} & 0 \end{bmatrix}.$$

(a) Prove that there is a bijection $f : \{0,1\}^d \to \{1, 2, \ldots, 2^d\}$ such that, for any $x, y \in \{0,1\}^d$, we have $R_d[f(x), f(y)] = 1$ if and only if $\langle x, y \rangle = 0$ (over $\mathbb{Z}$).

(b) For any field $\mathbb{F}$, give and prove the correctness of an algorithm which performs $O(d \cdot 2^d)$ field operations for the following problem: Given as input a vector $v \in \mathbb{F}^{2^d}$, output the vector $R_d \times v$. Hint: use recursion!

(c) Design and prove the correctness of an algorithm for the Orthogonal Vectors problem for $2n$ vectors in d dimensions whose running time is $(d \cdot 2^d + n) \cdot \text{polylog}(n)$.

2 Harder Versions of Easy Problems

In class we discussed how the determinant of an $n \times n$ matrix can be computed using $O(n^{2.373})$ operations. We also discussed how a perfect matching in an n-node graph can be detected in time $O(n^{2.373})$. In this problem, we will explore variants on these problems which appear to be much harder: computing the *permanent* of a matrix, and *counting* the number of perfect matchings in a bipartite graph. (Both of these problems are complete for the complexity class $\#P$, which gives evidence that one cannot improve much on the algorithms we will design in this problem.)

Recall that for an $n \times n$ matrix A, the permanent of A is defined as

$$\text{perm}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} A[i, \sigma(i)],$$

which is similar to the determinant except we have removed the $\text{sgn}(\sigma)$ term. For a vector $b \in \{0,1\}^n$, let $|b|$ denote the number of 1s in b, i.e., $|b| = \sum_{i=1}^{n} b[i]$.

(a) Prove that for any field $\mathbb{F}$ and any matrix $A \in \mathbb{F}^{n \times n}$, we have

$$\text{perm}(A) = \sum_{b \in \{0,1\}^n} (-1)^{n-|b|} \prod_{i=1}^{n} \langle b, a_i \rangle,$$

where $a_i \in \mathbb{F}^n$ denotes the ith column of A. Hint: think of this formula as a polynomial in the entries of A, and determine the coefficient of each monomial.

(b) Give and prove the correctness of a deterministic algorithm running in time $2^n \cdot \text{poly}(n)$ which, given as input an undirected bipartite graph G with n nodes in each bipartition (so, $2n$ nodes in total), counts the number of perfect matchings in G.

3 SUPERMAJORITY

Define the function $SMAJ : \{0,1\}^n \to \{0,1\}$, by

$$SMAJ(x_1, \ldots, x_n) = \begin{cases} 1 & \text{if } \sum_{i=1}^{n} x_i \geq \frac{2n}{3}, \\ 0 & \text{if } \sum_{i=1}^{n} x_i < \frac{2n}{3}. \end{cases}$$

(a) Prove that for every positive integer n, there is a polynomial $p : \mathbb{R}^n \to \mathbb{R}$ of degree $O(1)$ which has $|\{x \in \{0,1\}^n \mid p(x) = SMAJ(x)\}| \geq \frac{2}{3} \cdot 2^n$.

(b) Prove that for sufficiently large n, the function $SMAJ$ does *not* have a probabilistic polynomial of degree $o(\sqrt{n})$ and error $1/3$ over $\mathbb{R}$.

4 The Probabilistic Degree of OR

Fix any positive integer n and any $\varepsilon \in [2^{-n}, 1/4]$. In class, we saw that OR has a probabilistic polynomial of degree $\lceil \log(1/\varepsilon) \rceil$ and error ε over $\mathbb{F}_2$. Here we'll prove that this is very close to tight.

(a) Prove that OR does not have a probabilistic polynomial of degree $< n$ and error $< 2^{-n}$ over $\mathbb{F}_2$.

(b) Prove that for any any $\varepsilon \in [2^{-n}, 1/4]$, OR does not have a probabilistic polynomial of degree $\leq \log(1/\varepsilon) - 2$ and error ε over $\mathbb{F}_2$.

(c) (BONUS) Find a positive integer n, and an $\varepsilon \in [2^{-n}, 1/4]$ such that there is a probabilistic polynomial of degree $< \lceil \log(1/\varepsilon) \rceil$ and error ε for OR over $\mathbb{F}_2$.

5 The Probabilistic Degree of PARITY

Recall the function $PARITY : \{0,1\}^n \to \{0,1\}$, given by

$$PARITY(x_1, \ldots, x_n) = \begin{cases} 0 & \text{if } \sum_{i=1}^n x_i \equiv 0 \pmod 2, \\ 1 & \text{if } \sum_{i=1}^n x_i \equiv 1 \pmod 2. \end{cases}$$

In this problem, we will prove that the ε-error probabilistic degree of PARITY over $\mathbb{R}$ is $\Theta(\sqrt{n \log(1/\varepsilon)})$.

(a) Prove that for positive integer n and real $\varepsilon \in (0, 1/3)$, there is a polynomial $p : \mathbb{R}^n \to \mathbb{R}$ of degree $O(\sqrt{n \log(1/\varepsilon)})$ such that $|\{x \in \{0,1\}^n \mid p(x) = PARITY(x)\}| \geq (1-\varepsilon)2^n$.

(b) Prove that for positive integer n and real $\varepsilon \in (0, 1/3)$, there is a probabilistic polynomial of degree $O(\sqrt{n \log(1/\varepsilon)})$ and error ε over $\mathbb{R}$ for $PARITY$. Hint: On input $x \in \{0,1\}^n$, pick a random $y \in \{0,1\}^n$, and consider $p(x \oplus y)$, where p is the polynomial from part a, and $\oplus$ denotes coordinate-wise addition mod 2.

(c) Suppose n is an even integer, and there is a polynomial $q : \mathbb{R}^n \to \mathbb{R}$ of degree d, and a set $S \subseteq \{0,1\}^n$, such that $q(x) = PARITY(x)$ for all $x \in S$. Prove that for any function $f : \{0,1\}^n \to \{0,1\}$, there is a polynomial $r : \mathbb{R}^n \to \mathbb{R}$ of degree $\leq \frac{n}{2} + d$ such that $r(x) = f(x)$ for all $x \in S$.

Note: Just as in class, it follows from part c that there is a constant $a > 0$ such that, for sufficiently large positive integer n and real $\varepsilon \in (0, 1/3)$, there is no probabilistic polynomial of degree $\leq a \cdot \sqrt{n \log(1/\varepsilon)}$ and error ε over $\mathbb{R}$ for $PARITY$.