CS 599B: Math for TCS, Spring 2022

Homework 2

Due: 10:00PM, Friday March 25, 2022 on Gradescope.

Instructions. Solutions must be typeset, with LaTeX strongly preferred. You are encouraged to collaborate on the homework problems with each other in small groups (2-4 people). Collaboration may include brainstorming or exploring possible solutions together on a whiteboard, but should not include one person telling the others how to solve a problem. You must also write up the solutions independently (in your own words) and acknowledge your collaborators at the beginning of the first page.

You may freely use without proof any results proved in class, in Mark's lecture notes posted on the class webpage, or in the main body of the texts assigned as reading. Note that this excludes results that appear in the texts as problems and exercises. You may, of course, use such results but you have to prove them first.

Problem 1 (Tightness of Braverman's Theorem)**.** For $n \in \mathbb{N}$ and $\varepsilon > 0$, let $r = \log n$ and $t = \log(2/\varepsilon)$. Consider the function $f = \mathrm{OR}_t \circ \mathrm{XOR}_r^{\otimes t}$. We will regard this as a function $f : \{-1,1\}^n \to \{-1,1\}$, but note that it depends only on the first $rt = (\log n)\log(2/\varepsilon)$ inputs.

a) Show that f is computed by a DNF with $s = n\log(2/\varepsilon)$ terms.

b) Show that $\mathbb{E}_{x\sim\{-1,1\}^n}[f(x)] = -1+\varepsilon$. (Note in particular that this means the Fourier spectrum of f is (2ε)-concentrated on degree 0.)

c) Show that there is an $(rt-1)$-wise independent distribution $\mathcal{D}$ such that $\mathbb{E}_{x\sim\mathcal{D}}[f(x)] = -1$. (Combined with part (b), this separates sandwiching approximations from ℓ_2 approximations.)

d) Conclude that for some constant $c > 0$, depth-2 circuits of size s are *not* fooled by $(c\log s \cdot \log(1/\varepsilon))$-wise independence.

e) Generalize this argument to show that for every $d \in \mathbb{N}$, there exists a constant c_d such that depth-d circuits of size s are not fooled by $(c_d(\log s)^{d-1}\cdot\log(1/\varepsilon))$-wise independence. Hint: You can use without proof the fact that XOR_r is computed by a depth-d circuit of size $2^{r^{1/(d-1)}}\mathrm{poly}(r)$; but I encourage you to think about how to prove this fact!

Problem 2 (Closeness to k-wise independence)**.** In this problem, you will explore the relationships between various forms of "almost" k-wise independence and their consequences for derandomization.

a) Suppose $X \in \{-1,1\}^n$ is δ-almost k-wise independent as in Lecture 9, Definition 10. Show that low-degree parities of X are approximately unbiased: for every $|S| \le k$, we have $|\mathbb{E}[\chi_S(X)]| \le 2\delta$.

b) Use part (a) to show that if X is δ-almost k-wise independent, then there exists an actual k-wise independent distribution Y such that $TV(X,Y) \leq \delta \cdot O(n^k)$. Hint: Take a convex combination of X with distributions that look like $P_S = \mathcal{U}(\{x \in \{-1,1\}^n \mid \chi_S(x) = 1\})$.

c) Use part (b) and Braverman's Theorem to show that $\varepsilon^{\log^{O(d)} s}$-biased distributions ε-fool size-s, depth-d circuits. (You can assume that the size s of a circuit is larger than its number of inputs n.)

d) Show that if $X \in \{-1,1\}^n$ is k-wise independent for even k, then $H_\infty(X) \geq k \log(2\sqrt{n}/k)$. Hint: You can use without proof the result of Exercise Set 4, Problem 1 on the Chernoff bound with limited independence. You might also want to use the fact that if X is k-wise independent, then so is $X \oplus y$ for every constant $y \in \{-1,1\}^n$.

e) Use part (d) to show that part (b) is nearly tight in the following sense: For $k \leq n^{1/4}$, there exists an $n^{-O(k)}$-almost k-wise independent distribution X such that $TV(X,Y) \geq 1/2$ for every k-wise independent Y. Hint: How close can a distribution with high min-entropy be to one with small support?

Problem 3 (Error reduction for polynomials)**.**

a) Let k be odd, and let $A_k(x) = \sum_{S\subseteq[k]} a_s \chi_S(x)$ be the Fourier representation of MAJ_k. Show that if $\rho \in \{-1,1,\star\}$ is a restriction there exists $b \in \{\pm 1\}$ with $\rho_i = b$ for more than $k/2$ indices i, then $A_k|_\rho$ is the constant polynomial b.

b) An ε-probabilistic polynomial for a function $f : \{-1,1\}^n \to \{-1,1\}^n$ is a distribution $\mathcal{P}$ over degree-d polynomials $p : \{-1,1\}^n \to \mathbb{R}$ such that for all $x \in \{-1,1\}^n$,

$$\Pr_{p\sim\mathcal{P}}[p(x) \neq f(x)] \leq \varepsilon.$$

Show that if $\mathcal{P}$ is a 1/3-probabilistic polynomial for f of degree d, then for $k = O(\log(1/\varepsilon))$, the distribution $\mathcal{Q}$ over polynomials q defined by $q(x) = A_k(p_1(x), \ldots, p_k(x))$ where $p_1, \ldots, p_k$ are sampled i.i.d. from $\mathcal{P}$ is an ε-probabilistic polynomial for f of degree $kd = O(d \log(1/\varepsilon))$.