COS 522 Complexity — Homework 5.

Boaz Barak

Total of 150 points

Exercise 1 (40 points)**.** Do Exercise 22.5 – alternative proof of the Alphabet reduction lemma using the long code. You can use the result on linearity testing as a black-box, without proof.

Exercise 2 (20 points)**.** For $W \in \mathbb{N}$, let $\mathsf{LABELCOVER}_W$ be the special case of $\mathsf{2CSP}_W$ consisting of formulas where (1) the constraint graph is regular and bipartite, and (2) each of the constraints f_i outputs TRUE iff the two variables u_j, u_k that it depends on satisfy $u_j = g_i(u_k)$ for some function $g_i : [W] \to [W]$. (The latter property is known as the *projection* property.) Using the PCP Theorem as a black-box, show that there is some $W \in \mathbb{N}$ and $\rho < 1$ such that there is a reduction R from any language $L \in \mathbf{NP}$ to $\mathsf{LABELCOVER}_W$ such that $x \in \text{Ł} \implies \mathsf{val}(f(x)) = 1$ and $x \notin L \implies \mathsf{val}(f(x)) \leq \rho$.

Exercise 3 (20 points)**.** Read Section 22.5.1 (pages 475–477) and then show that the linearity testing theorem stated in class (i.e., *for every* $\rho > 1/2$ *and* $f : \{0,1\}^n \to \{0,1\}$ *if* $\Pr_{x,y}[f(x)+f(y) = f(x+y)] \geq \rho$ *then there is a linear function* $L : \{0,1\}^n \to \{0,1\}$ *such that* $\Pr_x[f(x) = L(x)] \geq \rho$) is equivalent to the following statement: for every $f : \{\pm 1\}^n \to \{\pm 1\}$,

$$\mathop{\mathrm{E}}_{x,y \in \{\pm 1\}^n}[f(xy)f(x)f(y)] \leq \max_{\alpha} \hat{f}_\alpha \ ,$$

where the vector xy us the component-wise multiplication of the vectors x and y.

After showing this, read the proof of linearity testing theorem Theorem 22.22 (page 479). (If you want, you can try to prove the theorem yourself— this is not very hard once you express f as a sum of the Fourier basis functions.)

Exercise 4 (40 points)**.** Do exercise 22.12— proof of Goldreich-Levin Theorem. This theorem has many applications in cryptography, derandomization, and learning theory. Note that in (c) f_α should be $\hat{f}_{\alpha\star}$.

Optional exercises. If you didn't do the exercises below last time, you can do them now. Again, they are completely optional, so feel free to skip them if you don't have time.

Exercise 5 (10 points)**.** Do exercise 22.1. Can you see how does the bound improve when you're guaranteed that $|S| < \epsilon n$ rather than only $|S| < n/2$?

Exercise 6 (10 points)**.** Do exercise 22.3. (Bounding the statistical distance of Binomial distributions with close parameter.)

Exercise 7 (10 points)**.** Do Exercise 22.4. For extra 5 points, generalize your proof to show also the Paley-Zygmund Inequality: if Z is a non-negative round variable and $\epsilon > 0$, then $\Pr[Z \geq \epsilon \, \mathrm{E}[Z]] \geq (1-\epsilon)^2 \frac{\mathrm{E}[Z]^2}{\mathrm{E}[Z^2]}$.