TTIC/CMSC 31150 Mathematical Toolkit	**Spring 2013**

Homework 2

Madhur Tulsiani Due: June 7, 2013

Note: *You may discuss these problems in groups. However, you must write up your own solutions and mention the names of the people in your group. Also, please do mention any books or papers you refer to.*

1. **Gaussian Random Variables.** Prove the following very useful facts about Gaussian random variables:

   (a) Let $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$ be two vectors. Let $\mathbf{g} \in \mathbb{R}^n$ be a random vector such that each coordinate g_i of $\mathbf{g}$ is distributed as a Gaussian random variable with mean 0 and variance 1, and any two coordinates g_i, g_j (for $i \neq j$) are independent. Then show that

   $$\mathop{\mathbb{E}}_{\mathbf{g}}\left[\langle \mathbf{u}, \mathbf{g} \rangle \cdot \langle \mathbf{v}, \mathbf{g} \rangle\right] \quad = \quad \langle \mathbf{u}, \mathbf{v} \rangle \ .$$

   (b) Let g be a Gaussian random variable with mean 0 and variance 1. Show that for any $t \in \mathbb{R}$, we have

   $$\mathbb{E}\left[e^{tg}\right] \quad = \quad e^{t^2/2} \, .$$

   Comparing coefficients of t^{2k} on both sides, use this to show that for any $k \in \mathbb{N}$,

   $$\mathbb{E}\left[g^{2k}\right] \quad = \quad \frac{(2k)!}{2^k \cdot k!} \, .$$

   (c) **(Optional Problem - will not be graded)** Let g_1, g_2, g_3 and g_4 be (not necessarily independent) Gaussian random variables with mean 0. Consider the function $\mathbb{E}_{g_1,g_2,g_3,g_4}\left[e^{t_1 g_1 + t_2 g_2 + t_3 g_3 + t_4 g_4}\right]$ in the variables t_1, t_2, t_3, t_4 and use it to show that

   $$\mathbb{E}\left[g_1 g_2 g_3 g_4\right] \quad = \quad \mathbb{E}\left[g_1 g_2\right] \cdot \mathbb{E}\left[g_3 g_4\right] + \mathbb{E}\left[g_1 g_3\right] \cdot \mathbb{E}\left[g_2 g_4\right] + \mathbb{E}\left[g_1 g_4\right] \cdot \mathbb{E}\left[g_2 g_3\right] \ .$$

   This shows that for *any* four Gaussian random variables, the expectation of their product can be expressed in terms of their pairwise correlations! This is a special case of what is known as Wick's theorem, which can also be proved by the above method.

2. **Spectra of Bipartite Graphs.** Let $G = (U, V, E)$ be a d-regular bipartite graph with adjacency matrix A, where U, V represent the two sides of the graph.

   (a) Prove that for the graph to be regular, we must have $|U| = |V|$.

   (b) Prove that $-d$ is an eigenvalue of A and find the corresponding eigenvector.

   (c) Prove that for every eigenvalue μ of A, $-\mu$ is also an eigenvalue of A.

3. **Expander Mixing Lemma.** This is an extremely useful result that lets one calculate the number of edges between sets S and T in a graph. One can give an estimate that depends only on the number of vertices in S and T, with an error term that is very small for expander graphs. For a graph $G = (V, E)$ and two subsets $S, T \subseteq V$, let $e(S, T)$ denote the number of edges (i, j) such that $i \in S$ and $j \in T$ (you can assume that $S \cap T = \emptyset$ so that each edge is counted exactly once).

   (a) Let G be a *random* graph in which each edge is chosen to be present with probability d/n. Then show that

   $$\mathbb{E}\left[e(S,T)\right] \;=\; \frac{d}{n} \cdot |S| \cdot |T| \,.$$

   (b) Let G be a connected d-regular graph and A be its adjacency matrix with eigenvalues $d = \mu_1 \geq \mu_2 \geq \cdots \geq \mu_n$. Let $\mu = \max\{\mu_2, -\mu_n\}$.

      i. Let $\mathbb{1}_S$ be a vector which is 1 on vertices in S and 0 elsewhere. For $\mathbb{1}_T$ defined similarly, show that

      $$e(S,T) \;=\; \mathbb{1}_S^T A \mathbb{1}_T .$$

      ii. Let $\mathbf{u}$ be the (unit-length) eigenvector of A with eigenvalue d. Calculate the components of $\mathbb{1}_S$ and $\mathbb{1}_T$ along $\mathbf{u}$ and perpendicular to $\mathbf{u}$.

      iii. Use the above to show that

      $$\left| e(S,T) - \frac{d}{n} \cdot |S| \cdot |T| \right| \;\leq\; \mu \cdot \sqrt{|S| \cdot |T|} \,.$$

4. **More on Linearity Testing.** In class we analyzed a test for checking if a function $f : \{0,1\}^n \to \{0,1\}$ is close to a linear function $\ell_a(x) = a \cdot x \mod 2$ for some $a \in \{0,1\}^n$. The test was to select $x, y \in \{0,1\}^n$ at random and test if

   $$f(x) + f(y) \;=\; f(x+y) \mod 2 \,.$$

   (We shall omit writing "mod 2" in the rest of the problem) The analysis of the linearity test proceeded by defining a function $g(x) = (-1)^{f(x)}$ and showing that the probability that the test accepted was equal to

   $$\mathop{\mathbb{P}}_{x,y}\left[f(x) + f(y) = f(x+y)\right] \;=\; \frac{1}{2} + \frac{1}{2}\sum_{S \subseteq [n]} \left(\widehat{g}(S)\right)^3 ,$$

   and we concluded that if the test accepts with probability at least $1 - \eta$, then there exists an $S \subseteq [n]$ such that $\widehat{g}(S) \geq 1 - \eta$. This gave a linear function $\ell_a(x) = a \cdot x$ such that $\mathbb{P}_x\left[f(x) = \ell_a(x)\right] \geq 1 - \eta$.

   The above test requires $2n$ random bits for choosing x and y. In this problem, we will reduce the number of random bits using ε-biased sets. Recall that a set $\mathcal{F} \subseteq \{0,1\}^n$ is called ε-biased, if for all $S \subseteq [n]$, $S \neq \emptyset$, we have $\left|\mathbb{E}_{y \in \mathcal{F}}\left[\chi_S(y)\right]\right| \leq \varepsilon$. We also discussed that there exist ε-biased sets of small size (at most $(n/\varepsilon)^2$). We can sample y uniformly from an ε-biased set using $\log(|\mathcal{F}|)$ bits.

   We will now consider the following variant of the above linearity test: Sample x uniformly from $\{0,1\}^n$ and y from an ε-biased set $\mathcal{F}$. Then accept if and only if $f(x) + f(y) = f(x+y)$. Note that the test is the same as before, except that y is now sampled from an ε-biased set.

(a) Extend the analysis from the previous linearity test to show that the probability of acceptance of the modified test is equal to

$$\frac{1}{2} + \frac{1}{2} \mathop{\mathbb{E}}_{y \in \mathcal{F}} \left[\sum_{S,T \subseteq [n]} (\widehat{g}(S))^2 \cdot \widehat{g}(T) \cdot \chi_S(y) \cdot \chi_T(y) \right].$$

(b) The Cauchy-Schwartz inequality states that for any two functions h_1 and h_2, we have $\mathbb{E}_x [h_1(x) \cdot h_2(x)] \leq \left(\mathbb{E}_x \left[(h_1(x))^2\right]\right)^{1/2} \cdot \left(\mathbb{E}_x \left[(h_2(x))^2\right]\right)^{1/2}$. Use this to show that the probability of acceptance is at most

$$\frac{1}{2} + \frac{1}{2} \left(\mathop{\mathbb{E}}_{y \in \mathcal{F}} \left[\left(\sum_{S \subseteq [n]} (\widehat{g}(S))^2 \cdot \chi_S(y) \right)^2 \right] \right)^{1/2}.$$

(c) Use the fact that $\mathcal{F}$ is an ε-biased set to conclude that

$$\mathop{\mathbb{E}}_{y \in \mathcal{F}} \left[\left(\sum_{S \subseteq [n]} (\widehat{g}(S))^2 \cdot \chi_S(y) \right)^2 \right] \leq \sum_{S \subseteq [n]} (\widehat{g}(S))^4 + \varepsilon .$$

(d) Combine the above parts to conclude that if the test accepts with probability at least $1 - \eta$, then there exists $S \subseteq [n]$, such that $|\widehat{g}(S)| \geq 1 - 4\eta - \varepsilon$.