Assignment 6

Exercise 1 (Random graphs are good expanders)**.** In this exercise, we will show the existence of good expander through a probabilistic method. Recall that a bipartite graph with n left vertices, m right vertices, and left degree D is an $(n, m, D, \gamma, \alpha)$ expander if for all subsets S of left vertices with $|S| \leq \gamma n$, we have $|N(S)| > \alpha|S|$ where $N(S)$ denotes the set of neighbours of S.

We will prove the following: Fix $0 < \varepsilon < 1$, $n \geq m$, $q > 1$, and let D be (implicitly) defined as the solution of

$$D = \frac{\log_{1/(1-\varepsilon)}\left(\frac{qe^{1/\varepsilon+1}Dn}{m}\right)}{\varepsilon}.$$

Let $\alpha = (1-\varepsilon)D$, and let $\gamma = \frac{m}{nDe^{1/\varepsilon}}$. Then, there exist expander graphs with parameters $(n, m, D, \gamma, (1-\varepsilon)D)$.

Pick a random graph in the following manner: For each left vertex, pick D neighbours uniformly at random from the set of all $\binom{m}{D}$ subsets of right vertices. This is done independently for each vertex. Call the resulting random graph $\mathcal{G}$. We want to show that if the parameters are chosen as above then

$$\Pr[\mathcal{G} \text{ is not an } (n, m, D, \gamma, \alpha) \text{ expander}] < 1.$$

1. Choose any set of left vertices S and set of right vertices T, with $|S| = s \leq \gamma n$ and $|T| = t \leq \alpha s$. Compute the probability that $N(S) \subset T$.

2. Argue that

   $$\Pr[\mathcal{G} \text{ is not an } (n, m, D, \gamma, \alpha) \text{ expander}] = \Pr[\exists S \subset \mathcal{L}, T \subset \mathcal{R} : |S| \leq \gamma n, |T| \leq \alpha|S|,\ N(S) \subset T]$$

   where $\mathcal{L}, \mathcal{R}$ denote the set of left and right vertices respectively.

3. Use the first two parts to get an upper bound on the probability that $\mathcal{G}$ is not an expander.

4. Using the bound $\binom{a}{b} \leq \left(\frac{ea}{b}\right)^b$, prove that as long as $m > 3n/4$, $D > 32$, $\gamma = 1/10$, $\alpha = 5D/8$, the probability that $\mathcal{G}$ is not an expander is < 1.

Exercise 2 (Minimum distance)**.** Let $\mathcal{G}$ be an $(n, m, D, \gamma, D(1-\epsilon))$ be an expander graph for some $0 < \epsilon < 1/2$. Given any set of left vertices S, a right vertex v is said to be a unique neighbour of S if it is adjacent to exactly one vertex in S. Let $U(S)$ denote the set of unique neighbours of S.

1. Fix any set of left vertices S such that $|S| \leq \gamma n$. How many edges leave S? Using this, compute an upper bound on the number of vertices in $N(S)$ that have more than one incident edge from S.

2. Use the above to argue that $|U(S)| \geq D(1-2\epsilon)|S|$.

3. Use the second part to argue that the minimum distance of the corresponding expander code is at least γn.

   Hint: Choose any nonzero codeword and label the left vertices by the codeword bits. Let S be the support set of vertices labelled 1. What can you say about $U(S)$?

Exercise 3 (Encoding/decoding complexity of expander codes)**.** Expander codes have low encoding and decoding complexity.

- What is the encoding complexity of an expander code?
- What is the computational complexity in each iteration of decoding an expander code? Justify first that it can be made $O(n^2)$, then improve your method to make it $O(n)$.