ASSIGNMENT 5

Exercise 1 (List decoding from erasures)**.** We say that a code is (p, L)-erasure list-decodable if for any vector $\mathbf{y} \in \{0, 1, *\}^n$ (where $*$ denotes the erasure symbol) with at most pn erasures, there are at most L codewords that agree with $\mathbf{y}$ in the unerased positions. For any vector $\mathbf{c}$ and $T \subset [n]$, let $\mathbf{c}_T$ denote the restriction of $\mathbf{c}$ to T, i.e., it is the $|T|$-length vector $(c_i : i \in T)$. Formally, a code $\mathcal{C} \subset \mathbb{F}_2^n$ is (p, L)-erasure list-decodable if for every $T \subset [n]$ with $|T| \geq (1-p)n$, and $\mathbf{y}' \in \{0, 1\}^{|T|}$, we have

$$|\{\mathbf{c} \in \mathcal{C} : \mathbf{c}_T = \mathbf{y}'\}| \leq L.$$

Prove the following:

1. If $\mathcal{C}$ has minimum distance d, then it is $\left(\frac{d-1}{n}, 1\right)$-list decodable.
2. For every $\epsilon > 0$, there exists a (p, L)-erasure list decodable code of rate

$$R \geq \frac{L}{L+1}(1-p) - \frac{1}{L} - \epsilon$$

   Hint: Use random codes. For a fixed $T, \mathbf{y}'$, compute the probability that the codeword for a fixed message is equal to $\mathbf{y}$ when restricted to T. Do this for $L+1$ messages. Then take a union bound over messages, $\mathbf{y}$', and T.

3. For every $\epsilon > 0$, there exists a linear (p, L)-erasure list-decodable code of rate

$$R \geq \frac{J-1}{J}(1-p) - \frac{1}{J-1} - \epsilon$$

   where $J = \lceil \log_2(L+1) \rceil$.

4. Show that if a code of rate $1 - p + \epsilon$ is (p, L)-erasure list-decodable, then $L = 2^{\Omega(n)}$.

Exercise 2 (Random graphs are good expanders)**.** In this exercise, we will show that a randomly chosen bipartite graph is a good expander with high probability. Recall that a bipartite graph with n left vertices, m right vertices, and left degree D is a (γ, α) expander if for all subsets S of left vertices with $|S| \leq \gamma n$, we have $|N(S)| > \alpha|S|$. Here, $N(S)$ denotes the set of neighbours of S.

Let us 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 for all sufficiently large n, and $m > 3n/4$, $D > 32$, $\gamma = 1/10$, $\alpha = 5D/8$

$$\Pr[\mathcal{G} \text{ is not a } (\gamma, \alpha) \text{ expander}] = o(1).$$

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

2. Argue that

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

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 $o(1)$.

Exercise 3. Let $\mathcal{G}$ be an $(n, m, D, \gamma, \alpha)$ expander graph. Let $\alpha = D(1-\epsilon)$ 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 4. Let $\mathcal{G}$ be an $(n, m, D, \gamma, D(1-\epsilon))$ expander. We will now show that the minimum distance of the corresponding expander code is $\geq 2\gamma(1-\epsilon)n$. We will prove this by contradiction. For the sake of contradiction, suppose that c^n is a nonzero codeword of Hamming weight less than $2\gamma(1-\epsilon)n$.

- Label the set of left vertices of $\mathcal{G}$ using c^n, and let S be the set of vertices labelled 1. Note that $|S|$ is equal to the Hamming weight of c^n. What is the size of $U(S)$?

- Pick $Q \subset S$ such that $|Q| = \gamma n$. Compute the size of $U(Q)$ and $N(S \backslash Q)$ and argue that $|U(S)| > 0$.

Exercise 5 (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? Use this to find the worst-case computational complexity assuming that the number of errors is less than $\gamma(1-2\epsilon)n$.