Telecom Paris ACCQ204, Coding Theory

ASSIGNMENT 5

Exercise 1 (List decodability of linear codes)**.** Show that with high probability, a random (binary) linear code obtained by choosing an $nR \times n$ generator matrix uniformly at random is (p, L)-list decodable as long as

$$R \leq 1 - H(p) - \frac{1}{\lceil \log_2(L+1) \rceil}.$$

Hint: Argue that any set of $L+1$ vectors in $\mathbb{F}_2^k$ contains at least $\lceil \log_2(L+1) \rceil$ linearly independent vectors. If two messages are linearly independent, then what can you say about the corresponding codewords of the random linear code?

Exercise 2 (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

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

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