ENEE626 Final Exam[1].

1. REED-SOLOMON CODES.

Suppose that $\mathbb{F} = \mathbb{F}_{2^4}$ is the field with a primitive element α that satisfies $\alpha^4 = \alpha + 1$. Consider an RS code $\mathcal{C}$ over $\mathbb{F}$ constructed by evaluating polynomials $f(x), \deg f \le 8$ at the points $\alpha^i, i = 0, \dots, 14$. A codeword $c \in \mathcal{C}$ was transmitted over the channel. The received vector has the form

$$y = (\alpha^{14}, \alpha^9, \alpha^{10}, \alpha^{11}, \alpha^3, \alpha^{12}, 0, \alpha^{13}, \alpha^6, \alpha^{12}, \alpha^3, \alpha^9, \alpha^3, \alpha^{14}, \alpha^6).$$

and $d(c, y) \le 3$. Use any decoder of RS codes (in the lectures, textbooks, online, etc.) to find c. You may use the computer, but please explain all the steps of your decoding.

2. LINEAR CODES, EXIT FUNCTIONS

You are given a linear binary code of length n, dimension k. Let G be a generator matrix; let H be a parity-check matrix. The set of coordinates is denoted by $[n]$. For a subset $E \subset [n]$ we write $H(E), G(E)$ to refer to the corresponding submatrices of H and G. For $i \in [n]$ we write $x_{\sim i} \triangleq (x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n)$. If X is a uniform random codeword, then $H(X) = Rn$, where $H(\cdot)$ is entropy and $R = k/n$ is the code rate.

2.1. Let $\mathcal{C}_E$ be the punctured code (projection of $\mathcal{C}$ on the coordinates indexed by E) and $\mathcal{C}^E$ the shortened code with respect to E (the subcode of $\mathcal{C}$ with zeros in E^c). Prove that $\dim \mathcal{C}_E = k - \dim C^{E^c}$ and $\dim \mathcal{C}^E = |E| - \mathrm{rk}(H(E))$ (recall hw1).

2.2. Define the ith generalized Hamming weight of $\mathcal{C}$ by

$$d_i(\mathcal{C}) \triangleq \min |\operatorname{supp}(\mathcal{D})|$$

where the minimum is over all linear subcodes $\mathcal{D} \subset \mathcal{C}$ such that $\dim(\mathcal{D}) = i$.

Prove that

$$d_i(\mathcal{C}) = \min(|I| : I \subset [n], |I| - \mathrm{rk}(H(I)) \ge i).$$

Prove that $d_i(\mathcal{C}) < d_{i+1}(\mathcal{C}), i = 1, 2, \dots, k-1$.

2.3. Suppose that $\mathcal{C}$ is used to transmit information over a BEC(p). Let X be a random transmitted codeword, and Y a received sequence (i.e., $y_i = x_i$ or $y_i = ?$ for all $i = 1, \dots, n$). Let

$$h_i(p) \triangleq H(X_i | Y_{\sim i}); \quad h(p) \triangleq \frac{1}{n} \sum_{i=1}^{n} h_i(p).$$

In other words, $h_i(p)$ is the uncertainty about x_i given all the other observations except y_i. Below we assume that $p_X(x) = 2^{-k}$ for all $x \in \mathcal{C}$.

2.3(a) Suppose that $\mathcal{C}[n, 1, n]$ is a repetition code. Prove that

$$h(p) = p^{n-1}.$$

Suppose that $\mathcal{C}[n, n-1, 2]$ is a single parity-check code. Prove that

$$h(p) = 1 - (1-p)^{n-1}.$$

2.3(b) Now let $\mathcal{C}$ be a linear code as described in the beginning of Problem 2. Prove that

$$h_i(p) = \sum_{E \subseteq [n] \setminus \{i\}} p^{|E|} (1-p)^{n-1-|E|} (1 + \mathrm{rk}(H(E)) - \mathrm{rk}(H(E \cup \{i\}))).$$

[1] This is a take-home exam. There will be no in-class final exam in CSI2120. Please submit your paper to my office AVW2361 by **Friday Dec. 18, 4pm**. If I am not in the office, slide your paper under my office door. I will be out of town on Dec. 14 (afternoon) to Dec. 17, so if you want to talk to me, do so before I leave.