Indian Institute of Technology Kharagpur
Information and Coding Theory (MA41024/MA60020)
Assignment - 3, Spring Semester 2021-22

Last date of submission ($\star$-marked questions): April 10, 2022

1. Determine the channel capacity of the channels whose channel matrices are given by

   (a) $M = \begin{bmatrix} 2/3 & 1/3 & 0 \\ 1/3 & 1/3 & 1/3 \\ 0 & 1/3 & 2/3 \end{bmatrix}, \mathcal{X} = \mathcal{Y} = \{0, 1, 2\}$

   (b) $M = \begin{bmatrix} 1/2 & 1/2 & 0 \\ 0 & 1/2 & 1/2 \\ 1/2 & 0 & 1/2 \end{bmatrix}, \mathcal{X} = \mathcal{Y} = \{0, 1, 2\}$

   (c) $M = \begin{bmatrix} p & 1-p & 0 & 0 \\ 1-p & p & 0 & 0 \\ 0 & 0 & q & 1-q \\ 0 & 0 & 1-q & q \end{bmatrix}, \mathcal{X} = \mathcal{Y} = \{0, 1, 2, 3\}$

2. $\star$ Let X and Y denote the input and output random variables for a channel. Define the error probability that two outcomes x and y are different as

$$P_e = \sum_x \sum_{y \neq x} P(x, y).$$

   Then consider the joint random variable $\mathbf{X}^L = (X_1, X_2, \ldots, X_L)$ where X_l is a copy of X, $1 \leq l \leq L$. Then show that

$$\frac{1}{L} \sum_{l=1}^{L} \mathcal{H}(P_{e,l}) \leq \mathcal{H}(\langle P_e \rangle),$$

   where $\langle P_e \rangle = \sum_{l=1}^{L} P_{e,l}/L$ and $P_{e,l}$ denotes the error probability for $x_l \neq y_l$ for the joint random variable $(\mathbf{X}^L, \mathbf{Y}^L)$.

3. Determine the parity-check matrix H for the $(15, 11)$ Hamming code. Encode and decode the messages 11111100000 and 111000111000111 respectively.

4. Determine the codes corresponding to the parity-check matrices

(a) $H = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}$

(b) $H = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}$

Also find the generator matrices for both the codes in systematic form.

5. Consider the generator matrix of an (n, k) code given by

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Determine n, k and the minimum distance of the code.

6. $\star$ Let $u = (u_1, u_2, \ldots, u_n)$, $v = (v_1, v_2, \ldots, v_n)$ and $w = (w_1, w_2, \ldots, w_n)$ be elements of the vector space $\{0, 1\}^n$. Then verify if the following are true. Justify your answer.

   (a) $d(u, v) = wt(u + v)$

   (b) if $u \cdot v = (u_1v_1, u_2v_2, \ldots, u_nv_n)$ then $d(u, v) = wt(u) + wt(v) - 2\,wt(u \cdot v)$

   (c) if u, v have even wrights then $u + v$ has even weight

   (d) $d(u, v) \leq d(u, w) + d(w, v)$

   (e) $wt(u + v) \geq wt(u) - wt(v)$

7. Let us denote a (n, k) linear blockcode with minimum distance d as $[n, k, d]$ code. Suppose G_1 and G_2 are generator matrices corresponding to $[n_1, k_1, d_1]$ and $[n_2, k_2, d_2]$ codes. Then what are the parameters of the code corresponding to the generator matrix $G = [G_1 | G_2]$ and $G = \begin{bmatrix} G_1 & 0 \\ 0 & G_2 \end{bmatrix}$.?

8. Prove the following:

   (a) if C is a linear code and $u \notin C$ then $C \cup (u + C)$ is a linear code

   (b) $(C^\perp)^\perp = C$

9. Determine codewords for the $n = 7$ binary cyclic code generated by $g(x) = 1 + x + x^3$.

10. Prove that $g(x) = 1 + x^2 + x^4 + x^6 + x^7 + x^{10}$ is a generator polynomial for a $(21, 11)$ cyclic code. Determine the check polynoial of the code.

11. $\star$ Let C denote the binary $[n, k, d]$ cyclic code with the generator polynomial $g(x)$. Then prove that $x^{n-k} g(1/x)$ is a generator polynomial for some code $\overline{C}$. Determine the minimum distance of $\overline{C}$.

All the Best!!