IV054 Coding, Cryptography and Cryptographic Protocols
2017 - Exercises I.

1. Consider a binary repetition code of length $n = 2k+1$. Given that probability of a single bit error is p compute probability that a received codeword is incorrectly decoded.

2. Consider the binary code of length 12 defined as

$$\{x_1x_2\cdots x_{12} \mid 3x_1 + x_2 + 3x_3 + x_4 + \ldots + 3x_{11} + x_{12} \equiv 0 \bmod 10\}.$$

   Is it possible to detect all adjacent transposition errors with this code?

3. Decide whether the following codes are equivalent. Prove your answer.

   (a) Binary codes

$$C_1 = \begin{Bmatrix} 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \end{Bmatrix}$$

   and

$$C_2 = \begin{Bmatrix} 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 \end{Bmatrix}.$$

   (b) Ternary codes

$$C_3 = \begin{Bmatrix} 1 & 0 & 2 & 1 \\ 2 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{Bmatrix}$$

   and

$$C_4 = \begin{Bmatrix} 1 & 0 & 0 & 2 \\ 1 & 2 & 0 & 2 \\ 2 & 2 & 2 & 2 \end{Bmatrix}.$$

4. Consider a channel characterized by the following conditional probabilities, where X and Y are the probability distributions of the input and the output, respectively.

$$\begin{aligned} P(Y=0 \mid X=0) &= p \\ P(Y=0 \mid X=1) &= p \\ P(Y=1 \mid X=0) &= 1-p \\ P(Y=1 \mid X=1) &= 1-p, \end{aligned}$$

   for some $0 < p < 1$.

   Let the probability distribution of inputs be $P(X=0) = q$ and $P(X=1) = 1-q$ for some $0 < q < 1$.

   (a) What is the probability of receiving 0 and 1?

   (b) What is the probability that 0 was sent if we received 0?

   (c) What is the probability that 0 was sent if we received 1?

   (d) Is this channel useful?

5. Give an example of a 4-ary $(10, 10, 7)$ code such that each of its words contains exactly one 0, two 1's, three 2's and four 3's.

More on next page >>>

6. Consider a family of codes C_{2n} and the following encoding function:

$$0 \mapsto \overbrace{00\dots0}^{2n \text{ times}}$$
$$1 \mapsto \overbrace{11\dots1}^{2n \text{ times}}$$

Consider a binary symmetric channel with error $p \leq \frac{1}{2}$ and the maximum likelihood decoding strategy, *i.e.* every $k < n$ errors can be corrected.

(a) What are the (n, M, d) parameters of C_{2n}?

(b) What is the probability of correct decoding $P_{corr}(C_{2n})$?

(c) Calculate $\lim_{n\to\infty} P_{corr}(C_{2n})$.

(d) What is the code rate $R(C_{2n})$?

(e) Calculate $\lim_{n\to\infty} R(C_{2n})$.

Hint: $\binom{2n}{n} \leq \frac{4^n}{\sqrt{3n+1}}$.

7. Find a ternary Huffman code for messages $\{0, 1, 2, 3, 4, 5, 6\}$ with the corresponding probability distribution $[\frac{1}{3}, \frac{1}{3}, \frac{1}{9}, \frac{1}{9}, \frac{1}{27}, \frac{1}{27}, \frac{1}{27}]$. Decode the message 2112201221.