Birla Institute of Technology and Science Pilani (Rajasthan)

EEE G612 Coding Theory and Practice
First Semester 2022-23

Date : 27/12/2022 **Comprehensive Exam** **Max. Marks: 80**

Name: ________________________________ID No. ________________ **Time: 3 hrs**

Instructions:

1) This is an open book exam. Only 1 A4 size handwritten cheat sheet is allowed.

2) Show all the steps clearly. If I cannot interpret it, I cannot grade it.

Q.1) Consider the wireless system given as,

$$y = [\,1 + j \quad 3 + 4j\,]\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + n$$

Indicate the step by step processing at the transmitter and receiver for above system using Alamouti codes and show how the input signal can be recovered. **[10 Marks]**

Q.2) Consider a Trellis encoder that uses a rate 2/3 convolution code to transmit 2 information bits per modulation interval as shown in Fig. 1a. The first flip flop is used for storing the input, while rest are the part of encoding logic circuit. The encoder performs TCM using an 8-ary PAM whose constellation diagram is as shown in Fig. 1b. Answer the following. **[4+4+2 = 10 Marks]**

(i) Show the optimal set partitioning for the 8-ary PAM scheme.

(ii) Draw the Trellis diagram showing waveform assignment and state transitions following the Ungerboeck's design rules.

(iii) Calculate the free distance of this TCM scheme, given that the minimum Euclidean distance between non-parallel paths of the Trellis is 6.

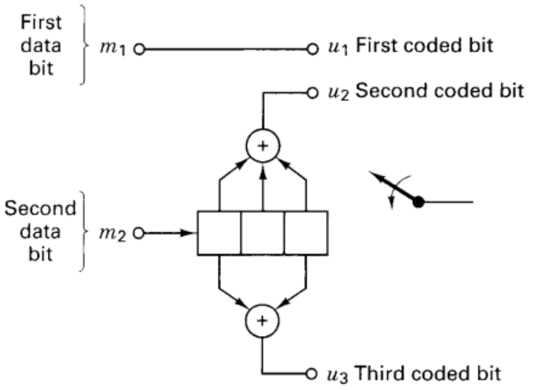

Fig. 1a

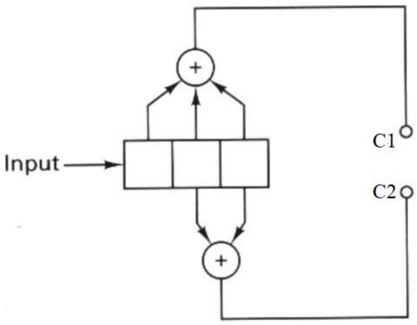

Fig. 2

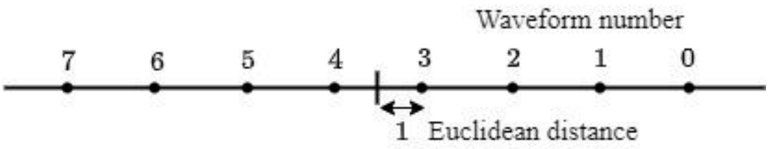

Fig. 1b

Q.3) Given rate 1/2 binary convolutional encoder as shown in Fig. 2. Consider that the first flip flop is used for storing the input, while rest are the part of encoding logic circuit. **[5+4+4+2 = 15 Marks]**

(i) Draw the state transition diagram, also indicating the input bit and the corresponding output bits.

(ii) Draw the modified state diagram showing the branch gains in terms of Hamming weight of the output bits.

(iii) Derive the expression for augmented generating function.

(iv) What is the free distance of this encoder?

Q.4) The generator polynomial for a (15,5) binary cyclic redundancy code is given as, $g(X) = 1 + X + X^2 + X^5 + X^8 + X^{10}$. Answer the following. **[5+2+3+2+3 = 15 Marks]**

(i) If $g(X)$ is used to encode a message sequence $m = 11011$, what is the resulting code word polynomial $C(X)$ that can be transmitted?

(ii) Consider that the transmitted code word is corrupted by error pattern $e(X) = X^8 + X^{10} + X^{13}$. What is the received code word polynomial?

(iii) What is the syndrome polynomial formed by using $g(X)$ and the received code word polynomial?

(iv) Prove that the syndrome polynomial formed by using (a) $g(X)$ and the received code word polynomial, and (b) $g(X)$ and $e(X)$ are the same.

(v) Consider that this (15,5) cyclic redundancy code is a triple-error correcting code. If we want to simultaneously correct 2 erasures and still perform error correction, how much error correction would have to be sacrificed ?

Q.5a) A Z-channel has binary input and output such that a 0 is transmitted correctly, while a 1 is the noisy input. The transition probabilities $p(y/x)$ are given by matrix P as shown below. If the input probability $p(x = 1) = q$, find the capacity of the Z-channel and the maximizing input probability distribution. **[6 Marks]**

$$P = \begin{bmatrix} 1 & 0 \\ 1/2 & 1/2 \end{bmatrix}$$

Q.5b) Consider two parallel AWGN channels with input X_i and output Y_i such that $Y_i = X_i + Z_i$, $i \in [1,2]$, and $Z_1 \sim \mathrm{N}\ (0, \sigma_1)$ and $Z_2 \sim N\ (0, \sigma_2)$ are independent Gaussian random variables. It is required to allocate power to the two parallel channels subject to a total cost constraint $\beta_1 P_1 + \beta_2 \mathrm{P}_2 \leq \beta$, where P_i is the power allocated to the *i-th* channel and β_i is the cost per unit power in that channel. Let β_i be fixed and $P_i \geq 0$ be chosen subject to cost constraint β. **[5+4 = 9 Marks]**

(i) Obtain the optimal power allocation that maximizes the total capacity of parallel channels.

(ii) Explain how will the power allocation take place. State the condition when the channel stops acting like a single channel and starts acting like a pair of channels.

Q.6a) There are 6 bottles of wine, out of which one bottle has gone bad (tastes terrible). From inspection of the bottles it is determined that the probability p_i of *i-th* bottle being bad is given by $(p_1, p_2, p_3, p_4, p_5, p_6) = (8/23, 6/23, 4/23, 2/23, 2/23, 1/23)$. Tasting will determine the bad wine. Suppose you taste the wines one at a time. Choose the order of tasting to minimize the expected number of tastings required to determine the bad bottle. Remember, if the first 5 wines pass the test you don't have to taste the last. **[2+1+4+1 = 8 Marks]**

(i) What is the expected number of tastings required?

(ii) Which bottle should be tasted first?

Now you get smart. For the first sample, you mix two of the wines in a fresh glass and sample the mixture. You proceed, mixing and tasting, stopping when the bad bottle has been determined. **(iii)** What is the minimum expected number of tastings required to determine the bad wine? **(iv)** What mixture should be tasted first?

Q.6b) Consider symmetric cryptographic algorithms. **[5+2 = 7 Marks]**

(i) Explain the key steps and working of the DES encryption and decryption

(ii) It is required to test the security of $character\ +\ x$ encrypting technique in which each alphabet of the plaintext is shifted by x to produce the cipher text. Consider the plaintext to be a word of English language. How many different attempts must be made to crack this code in the worst case? Assuming it takes a computer 1 ms to check out one value of the shift, how soon can this code be cracked.

---END---