Registration no: | | | | | | | | | | |

Total Number of Pages: 03 **M.TECH**

ETPC 102

1st Sem MTech Regular/ Back Examination – 2015-16

INFORMATION THEORY, CODING AND CRYPTOGRAPHY

BRANCH(S): ECE

Time: 3 Hours

Max marks: 70

Q.CODE:T1058

Answer Question No.1 which is compulsory and any five from the rest.

The figures in the right hand margin indicate marks.

Q1 Answer the following questions: (2 x 10)

a) Define mutual information between two events. How is it related to self information?

b) A DMS has five messages with source probabilities {0.40, 0.30, 0.15, 0.10, 0.05}. What is the source entropy? What information do you get from the entropy value?

c) Explain the tradeoffs between R_b/W and E_b/N_0 from the bandwidth efficiency diagram.

d) Write down the steps involved in syndrome decoding in linear block codes.

e) For a binary code with blocklength $n=4$, how many vectors are there at a distance 2 or less from any codeword?

f) A code C is defined as $C=\{0000, 0110, 1100, 0011, 1001\}$ over GF(2). Is it a cyclic code? Justify.

g) The generator polynomial matrix of a Convolutional code is given as

$$G(D)=\begin{bmatrix} D+D^2 & D^2 & D+D^2 \\ D^2 & D & D \end{bmatrix}$$

Draw the circuit realization of this encoder using shift register.

h) A channel has the following state transition probability matrix

$$[P(Y|X)]=\begin{bmatrix} 1-p & p & 0 \\ 0 & p & 1-p \end{bmatrix}$$

Draw the channel model. If the source has equally likely messages, compute the probabilities associated with the channel outputs.

i) Write down the three Ungerboeck's TCM design rules.

j) What is public key cryptography? How is it different from private key cryptography?

Q2 a) Determine the differential entropy H(X) of the uniformly distributed random variable X with PDF (4)

$$p(x)=\begin{cases} a^{-1} & (0 \le x \le a) \\ 0 & (\text{otherwise}) \end{cases}$$

for (i) a=1 and (ii) a=1/4.

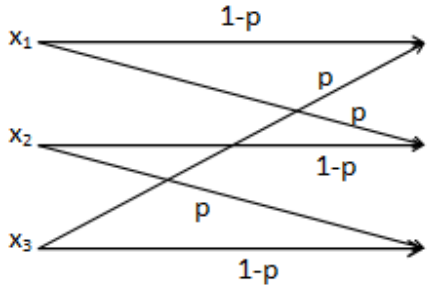
b) A DMS has an alphabet of eight letters, x_i, $i=1,2,\ldots,8$, with probabilities 0.25, 0.20, 0.15, 0.12, 0.10, 0.08, 0.05, and 0.05. (6)

i) Use the Huffman encoding procedure to determine a binary code for the source output.

ii) Determine the average number $\overline{R}$ of binary digits per source letter.

iii) Determine the entropy of the source and compare it with $\overline{R}$.

Q3 a) Determine the capacity of the channel shown in the following figure: (6)



b) State and prove the Kraft inequality. (4)

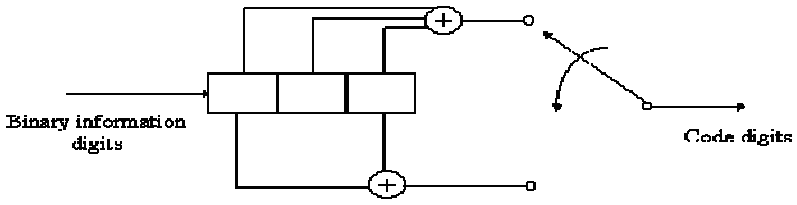
Q4 Consider a systematic block code whose parity-check equations are (10)

$$p_1 = m_1 + m_2 + m_4$$
$$p_2 = m_1 + m_3 + m_4$$
$$p_3 = m_1 + m_2 + m_3$$
$$p_4 = m_2 + m_3 + m_4$$

where m_i are message digits and p_i are check digits (parity bits).

i. Find the generator matrix for this code.
ii. Find the parity check matrix.
iii. How many errors can this code can correct?
iv. Is the vector 10101010 is a codeword?

Q5 For the following 1/3 Convolutional encoder (10)



i. Represent the generator polynomials,
ii. Draw the Trellis diagram(minimum upto 4 states),
iii. Represent the state diagram.
iv. Write down the output sequence for an input sequence of 101011.

Q6 a) Construct the addition and multiplication table for i) $F[x]/(x^2+1)$ defined over GF(2), (4)
ii) $F[x]/(x^2+1)$ defined over GF(3)?

b) Let the polynomial $g(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$ be the generator polynomial of a cyclic code over GF(2) with block length 15. (6)

i. Find the generator matrix **G.**
ii. Find the parity check matrix **H.**
iii. What is the code rate of this code?

Q7 a) What is the need of set partitioning in TCM? Explain the set partitioning of 16 QAM. (5)

b) Using two prime numbers 7 and 11 generate keys (D and E) using RSA algorithm. Find out the ciphertext for a plaintext 5 and decrypt the ciphertext using these keys. (5)

Q8 Write short notes on any (5 x 2)

a) RS code
b) BCH code
c) Data encryption standard