ENGINEERING & MANAGEMENT EXAMINATIONS, DECEMBER - 2008

INFORMATION THEORY, CODING AND CRYPTOGRAPHY

SEMESTER - 7

Time : 3 Hours] [Full Marks : 70

GROUP - A

(Multiple Choice Type Questions)

1. Choose correct answer from the given alternatives for any *ten* of the following : $10 \times 1 = 10$

i) A (7, 4) Linear Block Code with minimum distance guarantees error detection of

a) ≤ 4 bits b) ≤ 3 bits

c) ≤ 2 bits d) None of these. ☐

ii) Gaussian channel is characterised by a distribution represented by

a) $p(x) = \frac{1}{\sqrt{2\pi\sigma}} e^{-x^2/2\sigma^2}$

b) $p(x) = \frac{1}{\sqrt{2\pi\sigma}} e^{-x^2/2\sigma^2}$

c) $p(x) = \frac{\sqrt{2\pi}}{\sigma} e^{-x^2/2\sigma^2}$

d) $p(x) = \sqrt{2\pi\sigma}\ e^{-x^2/\sqrt{2\sigma^2}}$. ☐

iii) The binary Hamming Codes have the property that

a) $(n, k) = (2^m + 1, 2^m - 1 - m)$

b) $(n, k) = (2^m - 1, 2^m - 1 + m)$

c) $(n, k) = (2^m - 1, 2^m - 1 - m)$

d) $(n, k) = (2^{m-1}, 2^{m-1} - m)$ ☐

iv) Which of the following expression is incorrect ?

a) $H(y/x) = H(x, y) - H(x)$

b) $I(x, y) = H(x) - H(y/x)$

c) $H(x, y) = H(x, y) + H(y)$

d) $I(x, y) = H(y) - H(y/x)$. ☐

v) For GF (2^3), the elements in the set are

a) { 1, 2, 3, 4, 5, 6, 7 } b) { 0, 1, 2, 3, 4, 5, 6 }
c) { 0, 1, 2, 3 } d) { 0, 1, 2, 3, 4, 5, 6, 7 }. ☐

vi) Entropy represents

a) amount of information b) rate of information
c) measure of uncertainty d) probability of message. ☐

vii) 100110 ⊕ 011011, when ⊕ represent modulo-2 addition for binary number, yields

a) 100111 b) 111101
c) 000001 d) 011010. ☐

viii) In a binary system, the coding efficiency increases on probability of occurrence of *O*, approaches 0·5.

a) True
b) False. ☐

ix) A polynomial is called monic if

a) odd terms are unity b) even terms are unity
c) leading coefficient is unity d) leading coefficient is zero. ☐

x) If $m = 4$, then what will be the length of the BCH Code ?

a) 16 b) 15
c) 17 d) none of these. ☐

xi) Consider the Code C = { 0000, 0101, 1010, 1111 } for which compute the minimum distance is

a) 1 b) 2
c) 3 d) 4. ☐

xii) The generator polynomial of a cyclic code is a factor of

a) $X^n + 1$ b) $X^{(n+1)} + 1$
c) $X^{(n+2)} + 1$ d) none of these. ☐

xiii) Consider the parity check matrix $H = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$ and the received vector r = (001110). Then the syndrome is given by

a) (110) b) (100)
c) (111) d) (101). ☐

GROUP – B

(Short Answer Type Questions)

Answer any *three* of the following. $3 \times 5 = 15$

2. a) Draw the block diagram of a typical message information communication system. 2

   b) Define Forward Error Correction and Automatic Request for Retransmission. 3

3. a) What is systematic format of a code word. 2

   b) Explain 'Source Coding' and 'Channel Coding'. 3

4. a) A code has the parity check matrix

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

   Assuming that a vector (111011) is received,

   Determine whether the received vector is a valid code. 3

   b) If 'not', determine what is the probable code vector originally transmitted. If 'yes', conform. 2

5. a) Discuss the scheme of syndrome decoding of BCH Codes. 4

   b) What is the distance of t-error correcting Reed-Solomon Code. 1

6. a) Consider the primitive polynomial $p(Z) = Z^4 + Z + 1$ over GF (2). Use this to construct the expansion field GF (16). 3

   b) Let $\alpha = 7$ be the primitive element, the element of GF (16) as a power of α and find out the corresponds minimal polynomial. 2

7. a) What do you mean by Quantum Cryptography ? 2

   b) Write some application of cryptography in network security. 2

   c) What is Steganography. 1

GROUP – C
(Long Answer Type Questions)

Answer any *three* questions. 3 × 15 = 45

8. a) Consider a systematic (8, 4) code whose parity-check equations are

$$v_0 = u_1 + u_2 + u_3$$

$$v_1 = u_0 + u_1 + u_2$$

$$v_2 = u_0 + u_1 + u_3$$

$$v_3 = u_0 + u_2 + u_3.$$

where v_0, v_1, v_2 and v_3 are message digits and v_0, v_1, v_2, v_3 are parity-check digits.

Find the generator and parity-check matrix for the code.

— Show that minimum distance of the code is 4. 4 + 1 = 5

b) Design the syndrome circuit for which the parts-generate matrix is given by

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$ 5

c) Prove the following :

If C be an (n, k) linear code units parity-check matrix H. For each code vector of Hamming weight l, these exists l columns of H such that the vector sum of these l columns is equal to the zero vector. Conversely, if there exists l columns of H whose vector sum is the zero vector, there exists a code vector of Hamming weight l is C. 3 + 2 = 5

9. a) In a (7, 4) cyclic code, if the generator polynomial $g(x) = 1 + x + x^3$, find the generator matrix and convert it into systematic form. 3

b) Find the parity polynomial and show that the polynomial divides $X^n + 1$. 3

c) Consider the message vector polynomial $u(x) = 1 + x^2 + x^3$ and find the encoding circuit and complete code vector. 4

d) Now, find the error pattern and coset leaders for code vector v = (1001011) and received vector r = (1011011). 5

10. a) Explain the terms and their significance : Entropy, Mutual information and Self-information and Channel capacity. 4 × 2

b) State the Channel capacity of a white, band-limited Gaussian channel.

Derive an expression of noisy channel when bandwidth tends to be very long. 3 + 4

11. A discrete memoryless source has five symbols x_1, x_2, x_3, x_4 and x_5 with probabilities of occurrence $P(x_1) = 0{\cdot}4$, $P(x_2) = 0{\cdot}19$, $P(x_3) = 0{\cdot}16$, $P(x_4) = 0{\cdot}15$ and $P(x_5) = 0{\cdot}1$.

Construct the Huffman Code and determine

a) entropy

b) average code length

c) code efficiency. 5 + 4 + (2 + 2 + 2)

12. Explain with block diagram, the secrecy and authentication algorithm is secured.

Given N = 119 and public key $P_u = 5$, find the private key P_r. Also calculate the ciphertext C. In the Diffic-Hellman key exchange algorithm let the prime number $q = 353$ and its primitive root $\alpha = 3$. For A and B select their secret keys $X_A = 97$ and $X_B = 233$. Compute the public key Y_A and Y_B. 6 + 4 + 5

13. a) Given the polynomial $p(X) = X^3 + X + 1$. Construct the field GF (2^3) 5

b) Construct a double error-correcting BCH Code over GF (2^3) and determine the value of n and k. 5

c) Construct the (15, 7) double error correcting BCH code and code word $C(X) = X^8 + X^7 + X^6 + X^4 + 1$. Determine the outcome of a decoder when $C(X)$ incurs the error pattern $e(X) = X^7 + X^2 + 1$. 5

14. Write short notes on the following :

a) For a valid and correctly received code word,

$$CH^T = 0.$$

When C is the code word and H is the parity-check matrix. 5

b) RSA algorithm. 5

c) Shannon's theorems (three) in communication. 1 + 2 + 2

END