BITS PILANI, DUBAI CAMPUS

Dubai International Academic City

Second Semester 2013 – 2014

Information Theory and Coding, ECE F344/ECE C393

Comprehensive Exam Part I (Open Book)

Duration: 45 minutes

Weightage: 10%

29 May 2014

MAX: 10 Marks

Name:

ID:

**Note: Only answers in space provided will be marked.**

**Question 1:** Simplify the following expression when $X_i$ i=1,2, …, n are statistically independent.

$$H(X_1, X_2, \ldots, X_n) = \sum_{i=1}^{n} H(X_i | X_{i-1}, \ldots, X_1).$$

**Question 2:** Does the probability of error of estimating the transmitted symbol at the receiver increase or decrease as the size of the symbol increase? Justify your answer.

**Question 3:** Given codeword lengths 3, 4, 8 and 16, does an instantaneous code exist? Justify your answer.

**Question 4:** Is it possible that the joint entropy of $X_1$ and $X_2$ is 1.5 while the marginal entropies are 0.5 and .4 respectively. Justify your answer.

**Question 5:** Is it possible for the channel capacity of three cascaded binary symmetric channels is 2 given that the capacity of each individual channel is 1? Justify your answer.

**Question 6:** In optimally designing a communication system, do we first decide the best possible source coding algorithm and then apply the best possible channel coding theorem to the source coded data? Justify your answer

**Question 7:** Draw the diagram of any 2/3 convolution encoder.

**Question 8:** What are **two** advantages of Viterbi decoder over convolution encoders?

**Question 9:** What is the underlying principle of RSA algorithm?

**Question 10:** Explain the difference between **message** and **user** authentication and how each is accomplished.

END OF PART I

BITS PILANI, DUBAI CAMPUS

Dubai International Academic City

Second Semester 2013 – 2014

Information Theory and Coding, ECE F344/ECE C393

Comprehensive Exam Part II (Open Book)

Duration: 2 Hours and 15 minutes | Weightage: 30%

29 May 2014 | MAX: 30 Marks

## Question 1 (3M x 3 = 9 Marks)

The probability of the characters **a** to **h** are given below.

| a | b | c | d | e | f | g | h |
|---|---|---|---|---|---|---|---|
| 0.2 | 0.19 | 0.17 | 0.15 | 0.14 | 0.06 | 0.05 | 0.04 |

1) Obtain the Shannon codewords for each letter.
2) Obtain the SFE codewords for each letter.
3) For the word "hedge", what is
   a. What is the Shannon encoded binary value?
   b. What is the SFE encoded binary value?
   c. What is the binary value if Lempel Ziv algorithm is used?

## Question 2 (0.5M x 4 + 1M = 3 Marks)

The joint entropy of two random variables is given below:

| | Y = 0 | Y = 1 |
|---|---|---|
| X = 0 | 0.25 | 0.35 |
| X = 1 | 0.23 | 0.17 |

1) Calculate the marginal entropies of X and Y.
2) Calculate the joint entropy of X and Y.
3) Calculate the conditional entropy of X given Y.
4) Calculate the conditional entropy of Y given X.
5) Calculate the mutual information of X and Y.

**Question 3 (4 Marks)**

You are given the following information about a binary channel.

Pr[Y=0|X=0] = 1-$p_1$ Pr[Y=1|X=0] = $p_1$

Pr[Y=1|X=1] = 1-$p_2$ Pr[Y=0|X=1] = $p_2$

Determine the capacity of the channel.

**Question 4 (1M + 2M + 0.5M + 0.5M = 4 Marks)**

The generator matrix is given below.

$$G = \begin{bmatrix} 1000101 \\ 0100111 \\ 0010010 \\ 0001010 \end{bmatrix}$$

1) Is G systematic? Justify. Obtain the parity check matrix, H.
2) Obtain all the codewords.
3) If the received vector is 0001010, is there an error in transmission. Justify your answer.
4) If the received vector is 1100000, is there an error in transmission. Justify your answer. Determine the bit that is in error.

**Question 5 (4 Marks)**

Demonstrate, algebraically, the same algorithm works for DES encoding and DES decoding.

**Question 6 (2 x 3M = 6 Marks)**

1) Design a system that *only* provides confidentiality, two levels of authentication and signature
2) Design a system that implements confidentiality, authentication and signature using hash function

************Thank you for a great semester Have a great future ***************

## BITS PILANI, DUBAI CAMPUS

## Dubai International Academic City

## Second Semester 2013 – 2014

## Information Theory and Coding, ECE F344/ECE C393

## Test 2 (Open Book)

**Duration: 50 minutes** **Weightage: 25%**

**27 April 2014** **MAX: 25 Marks**

**Note: Show all working to get full credit.**

### Question 1 (Total: 4 + 2 = 6 Marks)

1) One CRC-6 polynomial is P(x) = $x^6 + x + 1$. The following data is to be transmitted: 1011110111. What is the transmitted data in polynomial format and binary values?
2) Show whether and how errors in bits 1 and 2 of the transmitted data can be detected.

### Question 2 (Total: 1M x 4 = 4 Marks)

$X^{15} - 1 = (x+1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)$

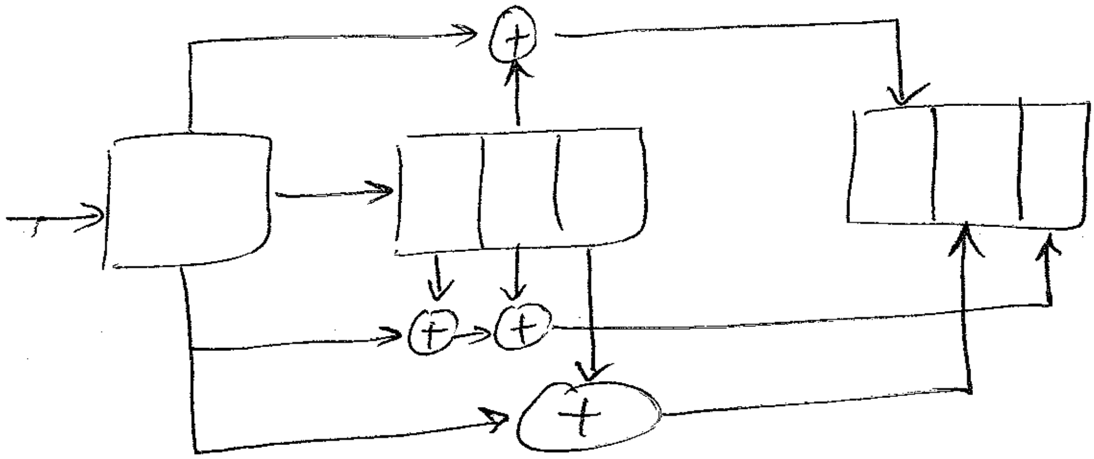
Consider the generator polynomial $g(x) = x^4 + x + 1$ over GF(2).

1) Find the generator matrix G. Is this matrix systematic? Justify your answer.
2) Find the parity check matrix H.
3) What is the maximum number of errors that this code can detect?
4) What is the maximum number of errors that this code can correct?

**Question 3 (Total: 4M + 1M = 5 Marks)**

For the convolution encoder given below, obtain/calculate the following:

1) Table with incoming bit, current state of encoder, next state of encoder and outgoing bits for the following current states only: {000, 001}. Incoming bits of 0 and 1 must be considered.
2) Rate of encoder



**Question 4 (2M + 2M= 4 Marks)**

1) Is the following code cyclic? S = {1100, 1011, 0101}. Obtain a cyclic code from S.
2) Write the Rate Distortion Function for a source that generates 2 bit symbols that independently and normally distributed with a mean 0 and variance $\sigma^3$. Assume a squared error distortion.

**Question 5 (4M + 1Mx2 = 6 Marks)**

1) Given two prime numbers 37 and 97, obtain the public key for the RSA algorithm. Show, with numerical examples, how you would determine the private key for the RSA algorithm.
2) Does the RSA algorithm require a secure key exchange mechanism? Justify your answer.
3) Does DES algorithm require a secure key exchange mechanism? Justify your answer.

# BITS PILANI, DUBAI CAMPUS

## Dubai International Academic City

## Second Semester 2013 – 2014

## Information Theory and Coding, ECE F344/ECE C393

## Test 1 (Open Book)

**Duration: 50 minutes** **Weightage: 20%**

**2 March 2014** **MAX: 20 Marks**

**Note: Show all working to get full credit.**

**Question 1 (Total: 4 Marks)**

.Compute H(X), H(X|Y) and I(X;Y) for p(x,y) given below.

| | Y = 0 | Y = 1 |
|---|---|---|
| X = 0 | 1/7 | 3/7 |
| X = 1 | 2/7 | 1/7 |

**Question 2 (Total: 1M + +1M + 2M = 4 Marks)**

1) As the value of I(X;Y) increases, are X and Y more statistically independent or less statistically independent? Justify your answer.
2) Write an expression for I(X;Y) in terms of Kullback Leibler distances.
3) Extend the Data Processing Inequality to the following random variables W → X → Y → Z. State all the possible inequalities.

**Question 3 (Total: 3 Marks)**

Using the approximate expression for Fano's Inequality, discuss the variation of $P_e$ with the increasing number of possible values for X. What is the significance of this variation?

**Question 4 (Total: = 1M + 3M + 4M + 1M = 9 Marks)**

1) Design an instantaneous code for X = 1, 2, 3, 4, 5, 6.
2) Determine the Huffman code for source values X = 1, 2, 3, 4 with probabilities of 0.25, 0.5, 0.125 and 0.125. Show full working. Compute the number of bits required to transmit {4, 3, 1, 2}.
3) Determine the Arithmetic code for source values X = 1, 2, 3, 4 with probabilities of 0.25, 0.5, 0.125 and 0.125. Assume symbols to be encoded are S = {4, 3, 1, 2}
4) Compare the Huffman and Arithmetic codes obtained in parts (2) and (3).

ITC Test 1 Answering Scheme

Q1) H(X) = -[(4/7)log(4/7) + (3/7)log(3/7)]/log2 = -[-0.13888 - .1577]/0.30103 = 0.98522

H(X|Y) = (3/7) H(1/3,2/3) + (4/7) H(3/4, 1/4) = [(3/7)[-(1/3)log(1/3) – (2/3)log(2/3)] +(4/7)[-(3/4)log(3/4) –(1/4)log(1/4)]]/log2 = [(3/7)[0.15904 + 0.11739] + (4/7)[0.0937 + 0.15051]]/0.30103 = [0.11847 + 0.13955]/.30103 = 0.85712

I(X ;Y) = H(X) - H(X|Y) = 0.1281 bits

Q2)

1) I(X;Y) depends on log(p(x,y)/p(x)p(y)) ➔ I(X;Y) = 0 iff p(x,y) = p(x)p(y) i.e., X and Y are SI. I(X;Y) increases ➔ X and Y less SI.
2) I(X;Y) = D(p(x,y)||p(x)p(y))
3) I(W ;X) >= I(W ;Y) >= I(W;Z)
   I(X ;Y) >= I(X ;Z)

Q3) M= 2, 4, 8, 16 ➔ $P_e$ >= ((H(X|Y)-1)/logM) >= {(H(X|Y)-1, ((H(X|Y)-1)/2, ((H(X|Y)-1)/3, ((H(X|Y)-1)/4…}. Lower bound of $P_e$ decreases with increasing M ➔ lower $P_e$ can be achieved by using larger values of M.