ECT306	INFORMATION THEORY AND CODING	CATEGORY	L	T	P	CREDIT
		PCC	3	1	0	4

Preamble: This course aims to lay down the foundation of information theory introducing both source coding and channel coding. It also aims to expose students to algebraic and probabilistic error-control codes that are used for reliable transmission.

Prerequisite: MAT 201 Linear Algebra and Calculus, MAT 204 Probability, Random Process and Numerical Methods, ECT 204 Signals and Systems.

Course Outcomes: After the completion of the course the student will be able to

CO 1	Explain measures of information – entropy, conditional entropy, mutual information
CO 2	Apply Shannon's source coding theorem for data compression.
CO 3	Apply the concept of channel capacity for characterize limits of error-free transmission.
CO 4	Apply linear block codes for error detection and correction
CO 5	Apply algebraic codes with reduced structural complexity for error correction
CO 6	Understand encoding and decoding of covolutional and LDPC codes

Mapping of course outcomes with program outcomes

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12
CO 1	3	3										
CO 2	3	3	2	3	3							
CO 3	3	3	2	3	3	2						2
CO 4	3	3	2	3	3	2						2
CO 5	3	3	2	3	3	2						2
CO 6	3	3	2	3	3	2						2

Assessment Pattern

Bloom's Category	**Continuous Assessment Tests**		**End Semester Examination**
	1	**2**	
Remember	10	10	20
Understand	30	30	60
Apply	10	10	20
Analyse			
Evaluate			
Create			

Mark distribution

Total Marks	**CIE**	**ESE**	**ESE Duration**
150	50	100	3 hours

Continuous Internal Evaluation Pattern:

Attendance	: 10 marks
Continuous Assessment Test (2 numbers)	: 25 marks
Assignment/Quiz/Course project	: 15 marks

End Semester Examination Pattern: There will be two parts; Part A and Part B. Part A contain 10 questions with 2 questions from each module, having 3 marks for each question. Students should answer all questions. Part B contains 2 questions from each module of which student should answer any one. Each question can have maximum 2 sub-divisions and carry 14 marks.

Course Level Assessment Questions

Course Outcome 1 (CO1): Entropy, Mutual Information

1. Prove that entropy of a discrete random variable is upper bounded by logarithm of alphabet size.
2. Prove that I(X:Y|Z) is always greater than or equal to 0.

Course Outcome 2 (CO2): Source Coding

1. State and prove Kraft's inequality for uniquely decodable codes.
2. Describe operational meaning of entropy in the light of Shannons's source coding theorem.

Course Outcome 3 (CO2): Channel Capacity

1. Derive the expression for capacity of binary symmetric channel.
2. Define differential entropy and derive its expression for a Gaussian distributed random variable with zero mean value and variance σ2.
3. Explain the inferences from Shannon Hartley theorem with the help of spectral efficiency versus SNR per bit graph.

Course Outcome 4 (CO4): Linear Block Codes

1. Construct a table for GF(23) based on the primitive polynomial, p(x) = 1 + *x* + *x*3.
2. Find generator and parity check matrix in systematic format of the (6,3) linear block code for the given parity matrix.

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

3. Explain standard array decoding of linear block codes.

Course Outcome 4 (CO4): Algebraic codes

1. Draw and explain the decoder circuit of (n, k) cyclic codes.
2. Give the properties of BCH codes.

Course Outcome 5 (CO5): Convlutional and LDPC Codes

1. Obtain the output codeword corresponding to the information sequence (1 1 0 1 1) for a convolutional encoder with rate ½ and constraint length 4, for generator sequences, g(1) = (1011) and g(2)
   = (1111).
2. Explain the message-passing decoding algorithm for LDPC codes with respect to binary erasure channel.

SYLLABUS

Module 1 – Entropy, Sources and Source Coding

Entropy, Properties of Entropy, Joint and Conditional Entropy, Mutual Information, Properties of Mutual Information.

Discrete memoryless sources, Source code, Average length of source code, Bounds on average length, Uniquely decodable and prefix-free source codes. Kraft Inequality (with proof), Huffman code. Shannon's source coding theorem (both achievability and converse) and operational meaning of entropy.

Module 2 – Channels and Channel Coding

Discrete memoryless channels. Capacity of discrete memoryless channels. Binary symmetric channels (BSC), Binary Erasure channels (BEC). Capacity of BSC and BEC. Channel code. Rate of channel code. Shannon's channel coding theorem (both achievability and converse without proof) and operational meaning of channel capacity.

Modeling of Additive White Gaussian channels. Continuous-input channels with average power constraint. Differential entropy. Differential Entropy of Gaussian random variable. Relation between differential entropy and entropy. Shannon-Hartley theorem (with proof – mathematical subtlities regarding power constraint may be overlooked).

Inferences from Shannon Hartley theorem – spectral efficiency versus SNR per bit, power-limited and bandwidth-limited regions, Shannon limit, Ultimate Shannon limit.

Module 3 – Introduction to Linear Block Codes

Overview of Groups, Rings, Finite Fields, Construction of Finite Fields from Polynomial rings, Vector spaces.

Block codes and parameters. Error detecting and correcting capability. Linear block codes. Two simple examples -- Repetition code and single parity-check code. Generator and parity-check matrix. Systematic form.

Maximum likelihood decoding of linear block codes. Bounded distance decoding. Syndrome. Standard array decoding.

Module 4 – A Few Important Classes of Algebraic codes
Cyclic codes. Polynomial and matrix description. Interrelation between polynomial and matrix view point. Systematic encoding. Decoding of cyclic codes.

(Only description, no decoding algorithms) Hamming Codes, BCH codes, Reed-Solomon Codes.

Module 5 – Convolutional and LDPC Codes
Convolutional Codes. State diagram. Trellis diagram. Maximum likelihood decoding. Viterbi algorithm.

Low-density parity check (LDPC) codes. Tanner graph representation. Message-passing decoding for transmission over binary erasure channel.

Text Books and References

1. "Elements of Information Theory", Joy A Thomas, Thomas M Cover, Wiley-Interscience.
2. "Information Theory, Inference and Learning Algorithms", David JC McKay, Cambridge University Press
3. "Principles of digital communication", RG Gallager, Cambridge University Press
4. "Digital Communication Sysmtes", Simon Haykin, Wiley.
5. "Introduction to Coding Theory", Ron M Roth, Cambrdige University Press
6. Shu Lin & Daniel J. Costello. Jr., Error Control Coding : Fundamentals and Applications, 2nd Edition.
7. Modern Coding Theory, Rüdiger Urbanke and TJ Richardson, Cambdridge University Press.

Course Contents and Lecture Schedule

No	Topic	No. of Lectures
1	**Entropy, Sources and Source Coding**	
1.1	Entropy, Properties of Entropy, Joint and Conditional Entropy	2
1.2	Mutual Information, Properties of Mutual Information	2
1.3	Discrete memoryless sources, Source code, Average length of source code, Bounds on average length	2
1.4	Uniquely decodable and prefix-free source codes. Kraft Inequality (with proof)	2
1.5	Huffman code. Shannon's source coding theorem and operational meaning of entropy	2
2	**Channels and Channel Coding**	
2.1	Discrete memoryless channels. Capacity of discrete memoryless channels	1
2.2	Binary symmetric channels (BSC), Binary Erasure channels (BEC). Capacity of BSC and BEC.	2

2.3	Channel code. Rate of channel code. Shannon's channel coding theorem (without proof) and operational meaning of channel capacity.	2
2.4	Modeling of Additive White Gaussian channels. Continuous-input channels with average power constraint.	1
2.5	Differential entropy. Differential Entropy of Gaussian random variable. Relation between differential entropy and entropy	2
2.6	Shannon-Hartley theorem and its proof	1
2.7	Inferences from Shannon Hartley theorem – spectral efficiency versus SNR, power-limited and bandwidth-limited regions, Shannon limit, Ultimate Shannon limit.	2
3	**Introduction to Linear Block Codes**	
3.1	Overview of Groups, Rings, Finite Fields, Construction of Finite Fields from Polynomial rings, Vector spaces.	5
3.2	Block codes and parameters. Error detecting and correcting capability	1
3.3	Linear block codes. Generator and parity-check matrix. Systematic form. Two simple examples -- Repetition code and single parity-check code. General examples.	2
3.5	Maximum likelihood decoding of linear block codes. Bounded distance decoding. Syndrome. Standard array decoding.	3
4	**A Few Important Classes of Algebraic codes**	
4.1	Cyclic codes. Polynomial and matrix description. Interrelation between polynomial and matrix view point. Systematic encoding. Decoding of cyclic codes.	4
4.2	Hamming Codes,	1
4.3	BCH codes, Reed-Solomon Codes.	2
5	**Convolutional and LDPC Codes**	
5.1	Convolutional Codes.	1
5.2	State diagram. Trellis diagram.	2
5.3	Maximum likelihood decoding. Viterbi algorithm	
5.4	Low-density parity check (LDPC) codes. Tanner graph representation Message-passing decoding for transmission over binary erasure channel.	2

.

ECT 306 Information Theory and Coding

Simulation Assignments

The following simulation assignments can be done with Python/MATLAB/ SCILAB/LabVIEW

1. **Source Coding - Huffman Code**
    1. Generate Huffman code for the source with symbol probabilities {1/2, 1/3, 1/6}.
    2. Find the entropy, average codeword length and efficiency of the code.
    3. Create the second order extended source by taking probabilities of 9 symbols in the extended source as the product of every possible combinations of two symbols from the original source.
    4. Generate Huffman code for the extended source symbols and find the entropy, average codeword length and efficiency of the code.
    5. Compare the two efficiencies and appreciate the Shannon's source coding theorem.

2. **Binary Symmetric Channel**
    1. Create a 2 x 2 matrix, P(Y/X) for binary symmetric channel with channel transition probability, $p < 0.5$.
    2. Let the input symbol probabilities corresponding to symbol 0 and 1 be α and (1 - α) respectively. For different values of α ranging from 0 to 1, find the joint probability matrix, P(X,Y) and output probability, P(Y)
    3. Find mutual information, I(X; Y) = H(Y) – H(Y/X) for each value of α. Plot the I(X; Y) versus α graph and observe the channel capacity.

3. **Linear Block Code (LBC)**
    1. Create the k x n generator matrix, G of (n, k) LBC.
    2. Generate all possible codewords by multiplying the message vector of length, k with G.
    3. Calculate the Hamming weight of all codewords and obtain the minimum distance, dmin of the code.
    4. Find its error correcting and detecting capability.

5. **Cyclic Code – Encoder & Decoder**
    1. Realize the encoder circuit for (7, 4) cyclic code in Fig. 4.2 in page 96 in *Error Control Coding: Fundamentals and Applications by Shu Lin & Daniel J. Costello. Jr.*

2. Create a random binary vector of length 4 as input message vector and generate the codeword.
3. Create binary vector of length 7 with Hamming weight 1 as error vector and add it to the encoder output to generate the receiver output.
4. Realize the decoder circuit for (7, 4) cyclic code in Fig. 4.9 in page 107 in *Error Control Coding: Fundamentals and Applications by Shu Lin & Daniel J. Costello. Jr.*
5. Observe the encoder and decoder outputs for different message vectors and error vectors and find the error correcting capability of the code.

6. **Convolutional Code**

1. Implement (2,1,3) convolutional encoder in Fig. 10.1 in page 288 in *Error Control Coding: Fundamentals and Applications by Shu Lin & Daniel J. Costello. Jr.*
2. Give a message vector, u of arbitrary length as input to the encoder.
3. Generate the output code sequence.

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

ECT 306 INFORMATION THEORY AND CODING

Time: 3 hours **Max. Marks:100**

PART A

Answer ***all*** questions. Each question carries ***3 marks***.

1. A source emits one f four symbols, s_0, s_1, s_2, s_3 with probabilities 1/3, 1/6, 1/4 and 1/4 respectively. The successive symbols emitted by the source are statistically independent. Calculate the entropy of the source.
2. Identify the instantaneous codes from the code sets listed below.

Symbol	Code I	Code II	Code III	Code IV
s_0	0	0	0	00
s_1	10	01	01	01
s_2	110	001	011	10
s_3	1110	0010	110	110
s_4	1111	0011	111	111

3. State Shannon's channel coding theorem. What is its significance in digital communication system?
4. An analog signal band limited to 'B' Hz is sampled at Nyquist rate. The samples are quantized into 4 levels. The quantization levels are assumed to be independent and occur with probabilities: p1= p4 = 1/8, p2 = p3 = 3/8. Find the information rate of the source assuming B = 100Hz.
5. List the properties of group. Give an example.
6. Show that C = {0000, 1100, 0011, 1111} is a linear code. What is its minimum distance?
7. Explain generation of systematic cyclic code using polynomial description.
8. List the features of Reed Solomon code.
9. Draw a (3,2,1) convolutional encoder with generator sequences, $g_1^{(1)}=(11), g_1^{(2)}=(01), g_1^{(3)}=(11)$ and $g_2^{(1)}=(01), g_2^{(2)}=(10), g_2^{(3)}=(10)$.
10. Draw the tanner graph of rate 1/3 LDPC code for the given parity check matrix.

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

PART B

Answer ***any one*** question from each module. Each question carries 14 marks.

MODULE I

11 (a) The joint probability of a pair of random variables is given below. Determine H(X, Y), H(X/Y), H(Y/X) and I(X,Y). Verify the relationship between joint, conditional and marginal entropies.

$$P(X, Y) = \begin{bmatrix} 1/3 & 1/3 \\ 0 & 1/3 \end{bmatrix}$$

(10 marks)

11 (b) Explain uniquely decodable and prefix-free property of source code. (4 marks)

12 (a) Find the binary Huffman code for the source with probabilities {1/3, 1/5, 1/5, 2/15, 2/15}. Also find the efficiency of the code. (9 marks)

12 (b) Prove that H(Y) ≥ H(Y/X). (5 marks)

MODULE II

13 (a) A voice grade channel of the telephone network has a bandwidth of 3.4 KHz. Calculate channel capacity of the telephone channel for signal to noise ratio of 30 dB. Also determine the minimum SNR required to support information transmission through the telephone channel at the rate of 4800 bits/sec.

(7 marks)

13 (b) Derive the expression for channel capacity for binary erasure channel. (7 marks)

14 (a) A binary channel has the following noise characteristic.

$$P(Y/X) = \begin{bmatrix} 2/3 & 1/3 \\ 1/3 & 2/3 \end{bmatrix}$$

If the input symbols are transmitted with probabilities 3/4 and 1/4 respectively, find I(X;Y). Also compute channel capacity and what are the input symbol probabilities that correspond to the channel capacity. (9 marks)

14 (b) State Shannon Hartley theorem and explain the significance of Shannon limit. (6 marks)

MODULE III

15 (a) The parity check matrix of (7,4) linear block code is given as

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

Compute the minimum distance of the code and find its error detection and correcting capability. Suppose that the received codeword, r = (1001111). Determine whether the received codeword is in error? If so, form the decoding table and obtain the correct codeword. (9 marks)

16 (b) List the properties of vector space. Define subspace. (5 marks)

17 (a)The parity bits of a (8, 4) linear systematic block code are generated by

$c5 = d1+d2+d4$
$c6 = d1+d2+d3$
$c7 = d1+d3+d4$
$c8 = d2+d3+d4$

(+ sign denotes modulo-2 addition)

where d1, d2, d3 and d4 are message bits and c5, c6, c7 and c8 are parity bits. Find generator matrix G and parity check matrix H for this code. Draw the encoder circuit (7 marks)

17 (b) Explain the construction of finite field from polynomial ring with the help of an ex-ample. (7 marks)

MODULE IV

18 (a) Consider a (7, 4) cyclic code with generator polynomial, $g(x) = 1 + x + x^3$. Express the generator matrix and parity-check matrix in systematic and non-systematic form (8 Marks)

18 (b) Find the generator polynomial for single, double and triple error correcting BCH code of block length, n = 15. (6 marks)

19 (a) Draw syndrome circuit for a (7,4) cyclic code generated by $g(x)=1+x+x^3$. If the re-ceived vector r is [0010110] what is the syndrome of r? Explain the circuit with a table showing the contents of the syndrome register. (8 Marks)

19 (b) What are the features of Hamming code? Find the parity check matrix for (15, 11) Hamming code. (6 marks)

MODULE V

20 (a) Draw the state diagram of a convolution encoder with rate 1/3 and constraint length 3 for generator sequences $g^{(1)} = (1\ 0\ 0)$, $g^{(2)} = (1\ 0\ 1)$, $g^{(3)} = (1\ 1\ 1)$. (7 marks)

20 (b) Explain message passing decoding algorithm for LDPC codes with the help of an example. (7 marks)

21 For a (2,1,2) convolutional encoder with generator sequences $g^{(1)} = (1\ 1\ 1)$ and $g^{(2)} = (1\ 0\ 1)$. Draw Trellis and perform Viterbi decoding on this trellis for the received sequence {01, 10, 10, 11, 01, 01, 11} and obtain the estimate of the transmitted se-quence. (14 marks)