Course Title: Coding Theory

Course Developer: Ranjan Bose, IIT Delhi

Part I Information Theory and Source Coding

1. Source Coding

1.1. Introduction to Information Theory
1.2. Uncertainty and Information
1.3. Average Mutual Information and Entropy
1.4. Information Measures for Continuous Random Variables
1.5. Relative Entropy
1.6. Source Coding Theorem
1.7. Huffman Coding
1.8. Shannon-Fano-Elias Coding
1.9. Arithmetic coding
1.10. The Lempel-Ziv Algorithm
1.11. Run Length Encoding
1.12. Rate Distortion Function
1.13. Optimum Quantizer Design
1.14. Entropy Rate of a Stochastic Process
1.15. Introduction to Image Compression
1.16. The JPEG Standard for Lossless Compression
1.17. The JPEG Standard for Lossy Compression
1.18. Concluding remarks
Problems

2. Reliable Communication through Noisy Channels

2.1. Introduction
2.2. Channel models
2.3. Channel Capacity
2.4. Channel Coding
2.5. Information Capacity Theorem
2.6. The Shannon Limit
2.7. Channel capacity for MIMO systems
2.8. Random selection of codes
2.9. Network Information Theory
2.10. Concluding remarks
Problems

Part II Error Control Coding (Channel Coding)

3. Linear Block Codes

3.1. Introduction to error correcting codes
3.2. Basic Definitions
3.3. Matrix description of linear block codes
3.4. Equivalent codes
3.5. Parity check matrix
3.6. Decoding of a linear block code
3.7. Syndrome decoding
3.8. Error probability after decoding (Probability of error correction)
3.9. Weight Distributions of codes
3.10. Perfect codes
3.11. Hamming Codes
3.12. Low Density Parity Check (LDPC) Codes
3.13. Optimal linear codes
3.13 Maximum distance separable (MDS) codes
3.14 Bounds on Minimum Distance
3.15 Space Time Block Codes
3.16 Concluding remarks
Problems

4. Cyclic Codes

4.1. Introduction to cyclic codes
4.2. Polynomials
4.3. The division algorithm for polynomials
4.4. A method for generating cyclic codes
4.5. Matrix description of cyclic codes
4.6. Quasi-cyclic codes and shortened cyclic codes
4.7. Burst error correction
4.8. Fire Codes
4.9. Golay Codes
4.10. Cyclic Redundancy Check (CRC) Codes
4.11. Circuit Implementation of Cyclic Codes
4.12. Concluding remarks
Problems

5. Bose Chaudhuri Hocquenghem (BCH) Codes

5.1. Introduction to BCH codes
5.2. Primitive elements
5.3. Minimal polynomials

5.4. Generator Polynomials in terms of Minimal Polynomials
5.5. Some examples of BCH codes
5.6. Weight Distributions of BCH Codes
5.7. Decoding of BCH codes
5.8. Reed Solomon Codes
5.9. Implementation of Reed Solomon encoders and decoders
5.10. Performance of RS codes over real channels
5.11. Nested Codes
5.12. Concluding Remarks
Problems

6. Space Time Codes

6.1. Introduction to Space-Time Codes
6.2. Anatomy of a Space Time Block Code
6.3. Space Time Code design Criteria
6.4. Real Orthogonal Design
6.5. Generalized Real Orthogonal Design
6.6. Complex Orthogonal Design
6.7. Quasi-orthogonal Space Time Block Codes
6.8. STBC design Targets and Performance
6.9. Concluding Remarks
Problems

Part III Codes on Graph

7. Convolutional Codes

7.1. Introduction to Convolutional Codes
7.2. Tree codes and Trellis codes
7.3. Polynomial description of convolutional codes (Analytical Representation)
7.4. Distance Notions for Convolutional Codes
7.5. The Generating Function
7.6. Matrix description of Convolutional Codes
7.7. Viterbi decoding of Convolutional Codes
7.8. Distance Bounds for Convolutional Codes
7.9. Performance Bounds
7.10. Known good convolutional codes
7.11. Turbo Codes
7.12. Turbo decoding
7.13. Interleaver Design for Turbo Codes
7.14. Concluding remarks
Problems

8. Trellis Coded Modulation (TCM)

8.1. Introduction to TCM
8.2. The concept of Coded Modulation
8.3. Mapping by set partitioning
8.4. Ungerboeck's TCM Design Rules
8.5. TCM decoder
8.6. Performance Evaluation for AWGN Channel
8.7. Computation of d_{free}
8.8. TCM for Fading Channels
8.9. Space Time Trellis Codes
8.10. Concluding remarks
Problems

Part III Coding for Secure Communications

9. Cryptography

9.1. Introduction to cryptography
9.2. An overview of encryption techniques
9.3. Operations used by encryption algorithms
9.4. Symmetric (Secret Key) Cryptography
9.5. Data Encryption Standard (DES)
9.6. International Data Encryption Algorithm (IDEA)
9.7. RC Ciphers
9.8. Asymmetric (Public-Key) Algorithms
9.9. The RSA Algorithm
9.10. Pretty Good Privacy (PGP)
9.11. One-way Hashing
9.12. Other techniques
9.13. Elliptic Curve Cryptography
9.14. Diffie-Hellman key agreement protocol
9.15. Secure Communication using Chaos Functions
9.16. Quantum Cryptography
9.17. Biometric Encryption
9.18. Cryptanalysis
9.19. Politics Of Cryptography
9.20. Concluding remarks
Problems

10. Physical Layer Security

10.1. Introduction to Physical Layer Security
10.2. Shannon's Notion of Security
10.3. The Wiretap Model