

# *Fundamentals of Information Theory, Coding and Cryptography*

## **Table of Contents**

### **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. Source Coding Theorem
- 1.6. Huffman Coding
- 1.7. The Lempel-Ziv Algorithm
- 1.8. Run Length Encoding and the PCX Format
- 1.9. Rate Distortion Function
- 1.10. Optimum Quantizer Design
- 1.11. Introduction to Image Compression
- 1.12. The JPEG Standard for Lossless Compression
- 1.13. The JPEG Standard for Lossy Compression
- 1.14. Concluding remarks
- Problems

#### **2. Channel Capacity and Coding**

- 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. Random selection of codes
- 2.8. 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. Perfect codes
- 3.10. Hamming Codes
- 3.11. Optimal linear codes
- 3.12. Maximum distance separable (MDS) codes
- 3.13. Concluding remarks
- Summary
- 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. Burst error correction
- 4.7. Fire Codes
- 4.8. Golay Codes
- 4.9. Cyclic Redundancy Check (CRC) Codes
- 4.10. Circuit Implementation of Cyclic Codes
- 4.11. 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. Decoding of BCH codes
- 5.7. Reed Solomon Codes
- 5.8. Implementation of Reed Solomon encoders and decoders
- 5.9. Nested Codes
- 5.10. Concluding Remarks
- Problems

## **6. Convolutional Codes**

- 6.1. Introduction to Convolutional Codes
  - 6.2. Tree codes and Trellis codes
  - 6.3. Polynomial description of convolutional codes (Analytical Representation)
  - 6.4. Distance Notions for Convolutional Codes
  - 6.5. The Generating Function
  - 6.6. Matrix description of Convolutional Codes
  - 6.7. Viterbi decoding of Convolutional Codes
  - 6.8. Distance Bounds for Convolutional Codes
  - 6.9. Performance Bounds
  - 6.10. Known good convolutional codes
  - 6.11. Turbo Codes
  - 6.12. Turbo decoding
  - 6.13. Concluding remarks
- Problems

## **7. Trellis Coded Modulation (TCM)**

- 7.1. Introduction to TCM
  - 7.2. The concept of Coded Modulation
  - 7.3. Mapping by set partitioning
  - 7.4. Ungerboeck's TCM Design Rules
  - 7.5. TCM decoder
  - 7.6. Performance Evaluation for AWGN Channel
  - 7.7. Computation of  $d_{free}$
  - 7.8. TCM for Fading Channels
  - 7.9. Concluding remarks
- Problems

## **Part III Coding for Secure Communications**

### **8. Cryptography**

- 8.1. Introduction to cryptography
- 8.2. An overview of encryption techniques
- 8.3. Operations used by encryption algorithms
- 8.4. Symmetric (Secret Key) Cryptography
- 8.5. Data Encryption Standard (DES)
- 8.6. International Data Encryption Algorithm (IDEA)
- 8.7. RC Ciphers
- 8.8. Asymmetric (Public-Key) Algorithms
- 8.9. The RSA Algorithm
- 8.10. Pretty Good Privacy (PGP)
- 8.11. One-way Hashing
- 8.12. Other techniques
- 8.13. Secure Communication using Chaos Functions

8.14.Cryptanalysis  
8.15.Politics Of Cryptography  
8.16.Concluding remarks  
Problems