## Contents

**Preface**

**1** Coding and Capacity

1.1 Digital Data Communication and Storage 1

1.2 Channel-Coding Overview 3

1.3 Channel-Code Archetype: The (7,4) Hamming Code 4

1.4 Design Criteria and Performance Measures 7

1.5 Channel-Capacity Formulas for Common Channel Models 10

1.5.1 Capacity for Binary-Input Memoryless Channels 11

1.5.2 Coding Limits for M-ary-Input Memoryless Channels 18

1.5.3 Coding Limits for Channels with Memory 21

Problems 24

References 26

**2** Finite Fields, Vector Spaces, Finite Geometries, and Graphs 28

2.1 Sets and Binary Operations 28

2.2 Groups 30

2.2.1 Basic Concepts of Groups 30

2.2.2 Finite Groups 32

2.2.3 Subgroups and Cosets 35

2.3 Fields 38

2.3.1 Definitions and Basic Concepts 38

2.3.2 Finite Fields 41

2.4 Vector Spaces 45

2.4.1 Basic Definitions and Properties 45

2.4.2 Linear Independence and Dimension 46

2.4.3 Finite Vector Spaces over Finite Fields 48

2.4.4 Inner Products and Dual Spaces 50

2.5 Polynomials over Finite Fields 51

2.6 Construction and Properties of Galois Fields 56

2.6.1 Construction of Galois Fields 56

2.6.2 Some Fundamental Properties of Finite Fields 64

2.6.3 Additive and Cyclic Subgroups 69
### Contents

2.7 Finite Geometries
   2.7.1 Euclidean Geometries
   2.7.2 Projective Geometries

2.8 Graphs
   2.8.1 Basic Concepts
   2.8.2 Paths and Cycles
   2.8.3 Bipartite Graphs

Problems

References

Appendix A

### 3 Linear Block Codes

3.1 Introduction to Linear Block Codes
   3.1.1 Generator and Parity-Check Matrices
   3.1.2 Error Detection with Linear Block Codes
   3.1.3 Weight Distribution and Minimum Hamming Distance of a Linear Block Code
   3.1.4 Decoding of Linear Block Codes

3.2 Cyclic Codes

3.3 BCH Codes
   3.3.1 Code Construction
   3.3.2 Decoding

3.4 Nonbinary Linear Block Codes and Reed–Solomon Codes

3.5 Product, Interleaved, and Concatenated Codes
   3.5.1 Product Codes
   3.5.2 Interleaved Codes
   3.5.3 Concatenated Codes

3.6 Quasi-Cyclic Codes

3.7 Repetition and Single-Parity-Check Codes

Problems

References

### 4 Convolutional Codes

4.1 The Convolutional Code Archetype

4.2 Algebraic Description of Convolutional Codes

4.3 Encoder Realizations and Classifications
   4.3.1 Choice of Encoder Class
   4.3.2 Catastrophic Encoders
   4.3.3 Minimal Encoders
   4.3.4 Design of Convolutional Codes

4.4 Alternative Convolutional Code Representations
   4.4.1 Convolutional Codes as Semi-Infinite Linear Codes
   4.4.2 Graphical Representations for Convolutional Code Encoders
4.5 Trellis-Based Decoders 171
  4.5.1 MLSD and the Viterbi Algorithm 172
  4.5.2 Differential Viterbi Decoding 177
  4.5.3 Bit-wise MAP Decoding and the BCJR Algorithm 180
4.6 Performance Estimates for Trellis-Based Decoders 187
  4.6.1 ML Decoder Performance for Block Codes 187
  4.6.2 Weight Enumerators for Convolutional Codes 189
  4.6.3 ML Decoder Performance for Convolutional Codes 193

Problems 195

References 200

Low-Density Parity-Check Codes 201
5.1 Representations of LDPC Codes 201
  5.1.1 Matrix Representation 201
  5.1.2 Graphical Representation 202
5.2 Classifications of LDPC Codes 205
  5.2.1 Generalized LDPC Codes 207
5.3 Message Passing and the Turbo Principle 208
5.4 The Sum–Product Algorithm 213
  5.4.1 Overview 213
  5.4.2 Repetition Code MAP Decoder and APP Processor 216
  5.4.3 Single-Parity-Check Code MAP Decoder and APP Processor 217
  5.4.4 The Gallager SPA Decoder 218
  5.4.5 The Box-Plus SPA Decoder 222
  5.4.6 Comments on the Performance of the SPA Decoder 225
5.5 Reduced-Complexity SPA Approximations 226
  5.5.1 The Min-Sum Decoder 226
  5.5.2 The Attenuated and Offset Min-Sum Decoders 229
  5.5.3 The Min-Sum-with-Correction Decoder 231
  5.5.4 The Approximate Min* Decoder 233
  5.5.5 The Richardson/Novichkov Decoder 234
  5.5.6 The Reduced-Complexity Box-Plus Decoder 236
5.6 Iterative Decoders for Generalized LDPC Codes 241
5.7 Decoding Algorithms for the BEC and the BSC 243
  5.7.1 Iterative Erasure Filling for the BEC 243
  5.7.2 ML Decoder for the BEC 244
  5.7.3 Gallager's Algorithm A and Algorithm B for the BSC 246
  5.7.4 The Bit-Flipping Algorithm for the BSC 247
5.8 Concluding Remarks 248

Problems 248

References 254
## Contents

### 6 Computer-Based Design of LDPC Codes

6.1 The Original LDPC Codes
   - 6.1.1 Gallager Codes
   - 6.1.2 MacKay Codes

6.2 The PEG and ACE Code-Design Algorithms
   - 6.2.1 The PEG Algorithm
   - 6.2.2 The ACE Algorithm

6.3 Protograph LDPC Codes
   - 6.3.1 Decoding Architectures for Protograph Codes

6.4 Multi-Edge-Type LDPC Codes

6.5 Single-Accumulator-Based LDPC Codes
   - 6.5.1 Repeat–Accumulate Codes
   - 6.5.2 Irregular Repeat–Accumulate Codes
   - 6.5.3 Generalized Accumulator LDPC Codes

6.6 Double-Accumulator-Based LDPC Codes
   - 6.6.1 Irregular Repeat–Accumulate–Accumulate Codes
   - 6.6.2 Accumulate–Repeat–Accumulate Codes

6.7 Accumulator-Based Codes in Standards

6.8 Generalized LDPC Codes
   - 6.8.1 A Rate-1/2 G-LDPC Code

Problems

References

### 7 Turbo Codes

7.1 Parallel-Concatenated Convolutional Codes
   - 7.1.1 Critical Properties of RSC Codes
   - 7.1.2 Critical Properties of the Interleaver
   - 7.1.3 The Puncturer
   - 7.1.4 Performance Estimate on the BI-AWGNC

7.2 The PCCC Iterative Decoder
   - 7.2.1 Overview of the Iterative Decoder
   - 7.2.2 Decoder Details
   - 7.2.3 Summary of the PCCC Iterative Decoder
   - 7.2.4 Lower-Complexity Approximations

7.3 Serial-Concatenated Convolutional Codes
   - 7.3.1 Performance Estimate on the BI-AWGNC
   - 7.3.2 The SCCC Iterative Decoder
   - 7.3.3 Summary of the SCCC Iterative Decoder

7.4 Turbo Product Codes
   - 7.4.1 Turbo Decoding of Product Codes

Problems

References
Contents

10.2 Construction of LDPC Codes Based on the Parallel Bundles of Lines in Euclidean Geometries
10.3 Construction of LDPC Codes Based on Decomposition of Euclidean Geometries
10.4 Construction of EG-LDPC Codes by Masking
  10.4.1 Masking
  10.4.2 Regular Masking
  10.4.3 Irregular Masking
10.5 Construction of QC-EG-LDPC Codes by Circulant Decomposition
10.6 Construction of Cyclic and QC-LDPC Codes Based on Projective Geometries
  10.6.1 Cyclic PG-LDPC Codes
  10.6.2 Quasi-Cyclic PG-LDPC Codes
10.7 One-Step Majority-Logic and Bit-Flipping Decoding Algorithms for FG-LDPC Codes
  10.7.1 The OSMLG Decoding Algorithm for LDPC Codes over the BSC
  10.7.2 The BF Algorithm for Decoding LDPC Codes over the BSC
10.8 Weighted BF Decoding: Algorithm 1
10.9 Weighted BF Decoding: Algorithms 2 and 3
10.10 Concluding Remarks
Problems
References

11 Constructions of LDPC Codes Based on Finite Fields
11.1 Matrix Dispersions of Elements of a Finite Field
11.2 A General Construction of QC-LDPC Codes Based on Finite Fields
11.3 Construction of QC-LDPC Codes Based on the Minimum-Weight Codewords of an RS Code with Two Information Symbols
11.4 Construction of QC-LDPC Codes Based on the Universal Parity-Check Matrices of a Special Subclass of RS Codes
11.5 Construction of QC-LDPC Codes Based on Subgroups of a Finite Field
  11.5.1 Construction of QC-LDPC Codes Based on Subgroups of the Additive Group of a Finite Field
  11.5.2 Construction of QC-LDPC Codes Based on Subgroups of the Multiplicative Group of a Finite Field
11.6 Construction of QC-LDPC Code Based on the Additive Group of a Prime Field
11.7 Construction of QC-LDPC Codes Based on Primitive Elements of a Field
11.8 Construction of QC-LDPC Codes Based on the Intersecting Bundles of Lines of Euclidean Geometries
11.9 A Class of Structured RS-Based LDPC Codes
Problems
References
12 LDPC Codes Based on Combinatorial Designs, Graphs, and Superposition

12.1 Balanced Incomplete Block Designs and LDPC Codes

12.2 Class-I Bose BIBDs and QC-LDPC Codes
   12.2.1 Class-I Bose BIBDs
   12.2.2 Type-I Class-I Bose BIBD-LDPC Codes
   12.2.3 Type-II Class-I Bose BIBD-LDPC Codes

12.3 Class-II Bose BIBDs and QC-LDPC Codes
   12.3.1 Class-II Bose BIBDs
   12.3.2 Type-I Class-II Bose BIBD-LDPC Codes
   12.3.3 Type-II Class-II QC-BIBD-LDPC Codes

12.4 Construction of Type-II Bose BIBD-LDPC Codes by Dispersion

12.5 A Trellis-Based Construction of LDPC Codes
   12.5.1 A Trellis-Based Method for Removing Short Cycles from a Bipartite Graph
   12.5.2 Code Construction

12.6 Construction of LDPC Codes Based on Progressive Edge-Growth Tanner Graphs

12.7 Construction of LDPC Codes by Superposition
   12.7.1 A General Superposition Construction of LDPC Codes
   12.7.2 Construction of Base and Constituent Matrices
   12.7.3 Superposition Construction of Product LDPC Codes

12.8 Two Classes of LDPC Codes with Girth 8

Problems

References

13 LDPC Codes for Binary Erasure Channels

13.1 Iterative Decoding of LDPC Codes for the BEC

13.2 Random-Erasure-Correction Capability

13.3 Good LDPC Codes for the BEC

13.4 Correction of Erasure-Bursts

13.5 Erasure-Burst-Correction Capabilities of Cyclic Finite-Geometry and Superposition LDPC Codes
   13.5.1 Erasure-Burst-Correction with Cyclic Finite-Geometry LDPC Codes
   13.5.2 Erasure-Burst-Correction with Superposition LDPC Codes

13.6 Asymptotically Optimal Erasure-Burst-Correction QC-LDPC Codes

13.7 Construction of QC-LDPC Codes by Array Dispersion

13.8 Cyclic Codes for Correcting Bursts of Erasures

Problems

References

14 Nonbinary LDPC Codes

14.1 Definitions

14.2 Decoding of Nonbinary LDPC Codes
   14.2.1 The QSPA
   14.2.2 The FFT-QSPA
14.3 Construction of Nonbinary LDPC Codes Based on Finite Geometries
   14.3.1 A Class of $q^m$-ary Cyclic EG-LDPC Codes
   14.3.2 A Class of Nonbinary Quasi-Cyclic EG-LDPC Codes
   14.3.3 A Class of Nonbinary Regular EG-LDPC Codes
   14.3.4 Nonbinary LDPC Code Constructions Based on Projective Geometries

14.4 Constructions of Nonbinary QC-LDPC Codes Based on Finite Fields
   14.4.1 Dispersion of Field Elements into Nonbinary Circulant Permutation Matrices
   14.4.2 Construction of Nonbinary QC-LDPC Codes Based on Finite Fields
   14.4.3 Construction of Nonbinary QC-LDPC Codes by Masking
   14.4.4 Construction of Nonbinary QC-LDPC Codes by Array Dispersion

14.5 Construction of QC-EG-LDPC Codes Based on Parallel Flats in Euclidean Geometries and Matrix Dispersion

14.6 Construction of Nonbinary QC-EG-LDPC Codes Based on Intersecting Flats in Euclidean Geometries and Matrix Dispersion

14.7 Superposition–Dispersion Construction of Nonbinary QC-LDPC Codes

Problems
References

15 LDPC Code Applications and Advanced Topics

15.1 LDPC-Coded Modulation
   15.1.1 Design Based on EXIT Charts

15.2 Turbo Equalization and LDPC Code Design for ISI Channels
   15.2.1 Turbo Equalization
   15.2.2 LDPC Code Design for ISI Channels

15.3 Estimation of LDPC Error Floors
   15.3.1 The Error-Floor Phenomenon and Trapping Sets
   15.3.2 Error-Floor Estimation

15.4 LDPC Decoder Design for Low Error Floors
   15.4.1 Codes Under Study
   15.4.2 The Bi-Mode Decoder
   15.4.3 Concatenation and Bit-Pinning
   15.4.4 Generalized-LDPC Decoder
   15.4.5 Remarks

15.5 LDPC Convolutional Codes

15.6 Fountain Codes
   15.6.1 Tornado Codes
   15.6.2 Luby Transform Codes
   15.6.3 Raptor Codes

Problems
References

Index