Contents

List of Figures  
List of Tables  
Preface  
Acknowledgments  

1 Coding for Reliable Digital Information Transmission and Storage  
1.1 Introduction  
1.2 Categories of Error-Correcting Codes  
1.3 Modulation and Demodulation  
1.4 Hard-Decision and Soft-Decision Decodings  
1.5 Maximum A Posteriori and Maximum Likelihood Decodings  
1.6 Channel Capacity on Transmission Rate  
1.7 Classification of Channel Errors  
1.8 Error-Control Strategies  
1.9 Measures of Performance  
1.10 Contents of the Book  
References  

2 Some Elements of Modern Algebra and Graphs  
2.1 Groups  
2.1.1 Basic Definitions and Concepts  
2.1.2 Finite Groups  
2.1.3 Subgroups and Cosets  
2.2 Finite Fields  
2.2.1 Basic Definitions and Concepts  
2.2.2 Prime Fields  
2.2.3 Finite Fields with Orders of Prime Powers  
2.3 Polynomials over Galois Field GF(2)  
2.4 Construction of Galois Field GF(2^m)  
2.5 Basic Properties and Structures of Galois Field GF(2^m)  
2.6 Computations over Galois Field GF(2^m)  
2.7 A General Construction of Finite Fields  

v
## Contents

2.8 Vector Spaces over Finite Fields  
2.8.1 Basic Definitions and Concepts  
2.8.2 Vector Spaces over Binary Field GF(2)  
2.8.3 Vector Spaces over Nonbinary Field GF(q)  
2.9 Matrices over Finite Fields  
2.9.1 Concepts of Matrices over GF(2)  
2.9.2 Operations of Matrices over GF(2)  
2.9.3 Matrices over Nonbinary Field GF(q)  
2.9.4 Determinants  
2.10 Graphs  
2.10.1 Basic Definitions and Concepts  
2.10.2 Bipartite Graphs  
Problems  
References  

### 3 Linear Block Codes  
3.1 Definitions  
3.2 Generator and Parity-Check Matrices  
3.3 Systematic Linear Block Codes  
3.4 Error Detection with Linear Block Codes  
3.5 Syndrome and Error Patterns  
3.6 Weight Distribution and Probability of Undetected Error  
3.7 Minimum Distance of Linear Block Codes  
3.8 Decoding of Linear Block Codes  
3.9 Standard Array for Decoding Linear Block Codes  
3.9.1 A Standard Array Decoding  
3.9.2 Syndrome Decoding  
3.10 Shortened and Extended Codes  
3.11 Nonbinary Linear Block Codes  
Problems  
References  

### 4 Binary Cyclic Codes  
4.1 Characterization of Cyclic Codes  
4.2 Structural Properties of Cyclic Codes  
4.3 Existence of Cyclic Codes  
4.4 Generator and Parity-Check Matrices of Cyclic Codes  
4.5 Encoding of Cyclic Codes in Systematic Form  
4.6 Syndrome Calculation and Error Detection  
4.7 General Decoding of Cyclic Codes  
4.8 Error-Trapping Decoding for Cyclic Codes  
4.9 Shortened Cyclic Codes  
4.10 Hamming Codes  
4.11 Cyclic Redundancy Check Codes  
4.12 Quadratic Residue Codes  
Problems  
References
Contents

4.13 Quasi-cyclic Codes 161
  4.13.1 Definitions and Fundamental Structures 161
  4.13.2 Generator and Parity-Check Matrices in Systematic Circulant Form 163
  4.13.3 Encoding of QC Codes 164
  4.13.4 Generator and Parity-Check Matrices in Semi-systematic Circulant Form 168
  4.13.5 Shortened QC Codes 176

4.14 Nonbinary Cyclic Codes 176

4.15 Remarks 177

Problems 177

References 182

5 BCH Codes 185

5.1 Primitive Binary BCH Codes 185

5.2 Structural Properties of BCH Codes 190

5.3 Minimum Distance of BCH Codes 192

5.4 Syndrome Computation and Error Detection 196

5.5 Syndromes and Error Patterns 198

5.6 Error-Location Polynomials of BCH Codes 199

5.7 A Procedure for Decoding BCH Codes 200

5.8 Berlekamp–Massey Iterative Algorithm 201

5.9 Simplification of Decoding Binary BCH Codes 205

5.10 Finding Error Locations and Error Correction 211

5.11 Nonprimitive Binary BCH Codes 212

5.12 Remarks 216

Problems 216

References 218

6 Nonbinary BCH Codes and Reed–Solomon Codes 220

6.1 Nonbinary Primitive BCH Codes 221

6.2 Decoding Steps of Nonbinary BCH Codes 224

6.3 Syndrome and Error Pattern of Nonbinary BCH Codes 225

6.4 Error-Location Polynomial of Nonbinary BCH Codes 226

6.5 Error-Value Evaluator 231

6.6 Decoding of Nonbinary BCH Codes 232

6.7 Key-Equation 235

6.8 Reed–Solomon Codes 235
  6.8.1 Primitive Reed–Solomon Codes 236
  6.8.2 Nonprimitive Reed–Solomon Codes 237

6.9 Decoding Reed–Solomon Codes with Berlekamp–Massey Iterative Algorithm 238

6.10 Euclidean Algorithm for Finding GCD of Two Polynomials 243

6.11 Solving the Key-Equation with Euclidean Algorithm 247

6.12 Weight Distribution and Probability of Undetected Error of Reed–Solomon Codes 251
Contents

6.13 Remarks 252
Problems 252
References 255

7 Finite Geometries, Cyclic Finite-Geometry Codes, and Majority-Logic Decoding 258
7.1 Fundamental Concepts of Finite Geometries 259
7.2 Majority-Logic Decoding of Finite-Geometry Codes 261
7.3 Euclidean Geometries over Finite Fields 266
  7.3.1 Basic Concepts and Properties 266
  7.3.2 A Realization of Euclidean Geometries 269
  7.3.3 Subgeometries of Euclidean Geometries 275
7.4 Cyclic Codes Constructed Based on Euclidean Geometries 277
  7.4.1 Cyclic Codes on Two-Dimensional Euclidean Geometries 278
  7.4.2 Cyclic Codes on Multi-Dimensional Euclidean Geometries 284
7.5 Projective Geometries 288
7.6 Cyclic Codes Constructed Based on Projective Geometries 292
7.7 Remarks 296
Problems 297
References 300

8 Reed–Muller Codes 303
8.1 A Review of Euclidean Geometries over GF(2) 304
8.2 Constructing RM Codes from Euclidean Geometries over GF(2) 305
8.3 Encoding of RM Codes 311
8.4 Successive Retrieval of Information Symbols 314
8.5 Majority-Logic Decoding through Successive Cancellations 319
8.6 Cyclic RM Codes 324
8.7 Remarks 325
Problems 326
References 327

9 Some Coding Techniques 331
9.1 Interleaving 332
9.2 Direct Product 334
9.3 Concatenation 341
  9.3.1 Type-1 Serial Concatenation 342
  9.3.2 Type-2 Serial Concatenation 344
  9.3.3 Parallel Concatenation 346
9.4 \(|u|u + v|-Construction 347
9.5 Kronecker Product 348
9.6 Automatic-Repeat-Request Schemes 353
  9.6.1 Basic ARQ Schemes 353
  9.6.2 Mixed-Mode SR-ARQ Schemes 358
  9.6.3 Hybrid ARQ Schemes 359
Problems 362
References 363
Contents

10 Correction of Error-Bursts and Erasures 367
  10.1 Definitions and Structures of Burst-Error-Correcting Codes 368
  10.2 Decoding of Single Burst-Error-Correcting Cyclic Codes 370
  10.3 Fire Codes 373
  10.4 Short Optimal and Nearly Optimal Single Burst-Error-Correcting Cyclic Codes 376
  10.5 Interleaved Codes for Correcting Long Error-Bursts 377
  10.6 Product Codes for Correcting Error-Bursts 379
  10.7 Phased-Burst-Error-Correcting Codes 380
    10.7.1 Interleaved and Product Codes 380
    10.7.2 Codes Derived from RS Codes 380
    10.7.3 Burton Codes 381
  10.8 Characterization and Correction of Erasures 382
    10.8.1 Correction of Errors and Erasures over BSECs 383
    10.8.2 Correction of Erasures over BECs 385
    10.8.3 RM Codes for Correcting Random Erasures 388
  10.9 Correcting Erasure-Bursts over BBECs 390
    10.9.1 Cyclic Codes for Correcting Single Erasure-Burst 391
    10.9.2 Correction of Multiple Random Erasure-Bursts 394
  10.10 RS Codes for Correcting Random Errors and Erasures 394
Problems 402
References 403

11 Introduction to Low-Density Parity-Check Codes 406
  11.1 Definitions and Basic Concepts 407
  11.2 Graphical Representation of LDPC Codes 410
  11.3 Original Construction of LDPC Codes 414
    11.3.1 Gallager Codes 415
    11.3.2 MacKay Codes 416
  11.4 Decoding of LDPC Codes 416
    11.4.1 One-Step Majority-Logic Decoding 418
    11.4.2 Bit-Flipping Decoding 422
    11.4.3 Weighted One-Step Majority-Logic and Bit-Flipping Decodings 425
  11.5 Iterative Decoding Based on Belief-Propagation 427
    11.5.1 Message Passing 428
    11.5.2 Sum-Product Algorithm 429
    11.5.3 Min-Sum Algorithm 436
  11.6 Error Performance of LDPC Codes with Iterative Decoding 439
    11.6.1 Error-Floor 439
    11.6.2 Decoding Threshold 441
    11.6.3 Overall Performance and Its Determinating Factors 442
  11.7 Iterative Decoding of LDPC Codes over BECs 446
  11.8 Categories of LDPC Code Constructions 449
  11.9 Nonbinary LDPC Codes 450
Problems 453
References 456
# Contents

12 Cyclic and Quasi-cyclic LDPC Codes on Finite Geometries 464

12.1 Cyclic-FG-LDPC Codes 465
12.2 A Complexity-Reduced Iterative Algorithm for Decoding Cyclic-FG-LDPC Codes 472
12.3 QC-EG-LDPC Codes 480
12.4 QC-PG-LDPC Codes 487
12.5 Construction of QC-EG-LDPC Codes by CPM-Dispersion 489
12.6 Masking Techniques 493
12.7 Construction of QC-FG-LDPC Codes by Circulant-Decomposition 496
12.8 A Complexity-Reduced Iterative Algorithm for Decoding QC-FG-LDPC Codes 503
12.9 Remarks 509
Problems 511
References 513

13 Partial Geometries and Their Associated QC-LDPC Codes 518

13.1 CPM-Dispersions of Finite-Field Elements 518
13.2 Matrices with RC-Constrained Structure 520
13.3 Definitions and Structural Properties of Partial Geometries 522
13.4 Partial Geometries Based on Prime-Order Cyclic Subgroups of Finite Fields and Their Associated QC-LDPC Codes 524
13.5 Partial Geometries Based on Prime Fields and Their Associated QC-LDPC Codes 531
13.6 Partial Geometries Based on Balanced Incomplete Block Designs and Their Associated QC-LDPC Codes 538
13.6.1 BIBDs and Partial Geometries 538
13.6.2 Class-1 Bose \((N, M, t, r, 1)\)-BIBDs 541
13.6.3 Class-2 Bose \((N, M, t, r, 1)\)-BIBDs 549
13.7 Remarks 556
Problems 556
References 559

14 Quasi-cyclic LDPC Codes Based on Finite Fields 562

14.1 Construction of QC-LDPC Codes Based on CPM-Dispersion 563
14.2 Construction of Type-I QC-LDPC Codes Based on Two Subsets of a Finite Field 564
14.3 Construction of Type-II QC-LDPC Codes Based on Two Subsets of a Finite Field 576
14.4 Masking-Matrix Design 580
14.4.1 Type-1 Design 580
14.4.2 Type-2 Design 582
14.4.3 Type-3 Design 584
14.5 A Search Algorithm for \(2 \times 2/3 \times 3\) SM-Constrained Base Matrices for Constructing Rate-1/2 QC-LDPC Codes 586
14.6 Designs of \(2 \times 2\) SM-Constrained RS Base Matrices 590
## Contents

14.7 Construction of Type-III QC-LDPC Codes Based on RS Codes  592
14.8 Construction of QC-RS-LDPC Codes with Girths at Least 8  598
14.9 A Special Class of QC-RS-LDPC Codes with Girth 8  603
14.10 Optimal Codes for Correcting Two Random CPM-Phased Erasure-Bursts  608
14.11 Globally Coupled LDPC Codes  612
14.12 Remarks  619
Problems  619
References  623

15 Graph-Theoretic LDPC Codes  628
15.1 Protograph-Based LDPC Codes  629
15.2 A Matrix-Theoretic Method for Constructing Protograph-Based LDPC Codes  640
15.3 Masking Matrices as Protomatrices  655
15.4 LDPC Codes on Progressive Edge-Growth Algorithms  670
15.5 Remarks  676
Problems  677
References  679

16 Collective Encoding and Soft-Decision Decoding of Cyclic Codes of Prime Lengths in Galois Fourier Transform Domain  684
16.1 Cyclic Codes of Prime Lengths and Their Hadamard Equivalents  685
16.2 Composing, Cascading, and Interleaving a Cyclic Code of Prime Length and Its Hadamard Equivalents  688
   16.2.1 Composing  688
   16.2.2 Cascading and Interleaving  689
16.3 Galois Fourier Transform of ICC Codes  692
16.4 Structural Properties of GFT-ICC Codes  694
16.5 Collective Encoding of GFT-ICC-LDPC Codes  696
16.6 Collective Iterative Soft-Decision Decoding of GFT-ICC-LDPC Codes  698
16.7 Analysis of the GFT-ISDD Scheme  700
   16.7.1 Performance Measurements  700
   16.7.2 Complexity  701
16.8 Joint Decoding of RS Codes with GFT-ISDD Scheme  701
16.9 Joint Decoding of BCH Codes with GFT-ISDD Scheme  706
16.10 Joint Decoding of QR Codes with GFT-ISDD Scheme  709
16.11 Code Shortening and Rate Reduction  710
   16.11.1 Shortened GFT-ICC Codes  710
   16.11.2 Reductions of Code Rate  713
16.12 Erasure Correction of GFT-ICC-RS-LDPC Codes  715
16.13 Remarks  717
Problems  717
References  719
Contents xii

17 Polar Codes 721
  17.1 Kronecker Matrices and Their Structural Properties 721
  17.2 Kronecker Mappings and Their Logical Implementations 724
  17.3 Kronecker Vector Spaces and Codes 735
  17.4 Definition and Polarized Encoding of Polar Codes 738
  17.5 Successive Information Retrieval from a Polarized Codeword 741
  17.6 Channel Polarization 744
    17.6.1 Some Elements of Information Theory 745
    17.6.2 Polarization Process 747
    17.6.3 Channel Polarization Theorem 760
  17.7 Construction of Polar Codes 766
  17.8 Successive Cancellation Decoding 768
    17.8.1 SC Decoding of Polar Codes of Length $N = 2$ 770
    17.8.2 SC Decoding of Polar Codes of Length $N = 4$ 773
    17.8.3 SC Decoding of Polar Codes of Length $N = 2^f$ 778
  17.9 Remarks 779

Problems 780
References 781

Appendix A Factorization of $X^n + 1$ over GF(2) 784

Appendix B A $2 \times 2/3 \times 3$ SM-Constrained Masked Matrix Search Algorithm 785

Appendix C Proof of Theorem 14.4 786

Appendix D The $2 \times 2$ CPM-Array Cycle Structure of the Tanner Graph of $C_{RS,n}(2, n)$ 791

Appendix E Iterative Decoding Algorithm for Nonbinary LDPC Codes 793
  E.1 Introduction 793
  E.2 Algorithm Derivation 794
    E.2.1 VN Update 795
    E.2.2 CN Update: Complex Version 795
    E.2.3 CN Update: Fast Hadamard Transform Version 796
  E.3 The Nonbinary LDPC Decoding Algorithm 800

Index 802