

Contents

	<i>Preface</i>	<i>page</i> xiii
1	Coding and Capacity	1
	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

vi	Contents	
	2.7 Finite Geometries	70
	2.7.1 Euclidean Geometries	70
	2.7.2 Projective Geometries	76
	2.8 Graphs	80
	2.8.1 Basic Concepts	80
	2.8.2 Paths and Cycles	84
	2.8.3 Bipartite Graphs	86
	Problems	88
	References	90
	Appendix A	92
3	Linear Block Codes	94
	3.1 Introduction to Linear Block Codes	94
	3.1.1 Generator and Parity-Check Matrices	95
	3.1.2 Error Detection with Linear Block Codes	98
	3.1.3 Weight Distribution and Minimum Hamming Distance of a Linear Block Code	99
	3.1.4 Decoding of Linear Block Codes	102
	3.2 Cyclic Codes	106
	3.3 BCH Codes	111
	3.3.1 Code Construction	111
	3.3.2 Decoding	114
	3.4 Nonbinary Linear Block Codes and Reed–Solomon Codes	121
	3.5 Product, Interleaved, and Concatenated Codes	129
	3.5.1 Product Codes	129
	3.5.2 Interleaved Codes	130
	3.5.3 Concatenated Codes	131
	3.6 Quasi-Cyclic Codes	133
	3.7 Repetition and Single-Parity-Check Codes	142
	Problems	143
	References	145
4	Convolutional Codes	147
	4.1 The Convolutional Code Archetype	147
	4.2 Algebraic Description of Convolutional Codes	149
	4.3 Encoder Realizations and Classifications	152
	4.3.1 Choice of Encoder Class	157
	4.3.2 Catastrophic Encoders	158
	4.3.3 Minimal Encoders	159
	4.3.4 Design of Convolutional Codes	163
	4.4 Alternative Convolutional Code Representations	163
	4.4.1 Convolutional Codes as Semi-Infinite Linear Codes	164
	4.4.2 Graphical Representations for Convolutional Code Encoders	170

	Contents	vii
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
5	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

viii	Contents	
6	Computer-Based Design of LDPC Codes	257
6.1	The Original LDPC Codes	257
6.1.1	Gallager Codes	257
6.1.2	MacKay Codes	258
6.2	The PEG and ACE Code-Design Algorithms	259
6.2.1	The PEG Algorithm	259
6.2.2	The ACE Algorithm	260
6.3	Protograph LDPC Codes	261
6.3.1	Decoding Architectures for Protograph Codes	264
6.4	Multi-Edge-Type LDPC Codes	265
6.5	Single-Accumulator-Based LDPC Codes	266
6.5.1	Repeat–Accumulate Codes	267
6.5.2	Irregular Repeat–Accumulate Codes	267
6.5.3	Generalized Accumulator LDPC Codes	277
6.6	Double-Accumulator-Based LDPC Codes	277
6.6.1	Irregular Repeat–Accumulate–Accumulate Codes	278
6.6.2	Accumulate–Repeat–Accumulate Codes	279
6.7	Accumulator-Based Codes in Standards	285
6.8	Generalized LDPC Codes	287
6.8.1	A Rate-1/2 G-LDPC Code	290
	Problems	292
	References	295
7	Turbo Codes	298
7.1	Parallel-Concatenated Convolutional Codes	298
7.1.1	Critical Properties of RSC Codes	299
7.1.2	Critical Properties of the Interleaver	300
7.1.3	The Puncturer	301
7.1.4	Performance Estimate on the BI-AWGNC	301
7.2	The PCCC Iterative Decoder	306
7.2.1	Overview of the Iterative Decoder	308
7.2.2	Decoder Details	309
7.2.3	Summary of the PCCC Iterative Decoder	313
7.2.4	Lower-Complexity Approximations	316
7.3	Serial-Concatenated Convolutional Codes	320
7.3.1	Performance Estimate on the BI-AWGNC	320
7.3.2	The SCCC Iterative Decoder	323
7.3.3	Summary of the SCCC Iterative Decoder	325
7.4	Turbo Product Codes	328
7.4.1	Turbo Decoding of Product Codes	330
	Problems	335
	References	337

	Contents	ix
8	Ensemble Enumerators for Turbo and LDPC Codes	339
	8.1 Notation	340
	8.2 Ensemble Enumerators for Parallel-Concatenated Codes	343
	8.2.1 Preliminaries	343
	8.2.2 PCCC Ensemble Enumerators	345
	8.3 Ensemble Enumerators for Serial-Concatenated Codes	356
	8.3.1 Preliminaries	356
	8.3.2 SCCC Ensemble Enumerators	358
	8.4 Enumerators for Selected Accumulator-Based Codes	362
	8.4.1 Enumerators for Repeat–Accumulate Codes	362
	8.4.2 Enumerators for Irregular Repeat–Accumulate Codes	364
	8.5 Enumerators for Protograph-Based LDPC Codes	367
	8.5.1 Finite-Length Ensemble Weight Enumerators	368
	8.5.2 Asymptotic Ensemble Weight Enumerators	371
	8.5.3 On the Complexity of Computing Asymptotic Ensemble Enumerators	376
	8.5.4 Ensemble Trapping-Set Enumerators	379
	Problems	383
	References	386
9	Ensemble Decoding Thresholds for LDPC and Turbo Codes	388
	9.1 Density Evolution for Regular LDPC Codes	388
	9.2 Density Evolution for Irregular LDPC Codes	394
	9.3 Quantized Density Evolution	399
	9.4 The Gaussian Approximation	402
	9.4.1 GA for Regular LDPC Codes	403
	9.4.2 GA for Irregular LDPC Codes	404
	9.5 On the Universality of LDPC Codes	407
	9.6 EXIT Charts for LDPC Codes	412
	9.6.1 EXIT Charts for Regular LDPC Codes	414
	9.6.2 EXIT Charts for Irregular LDPC Codes	416
	9.6.3 EXIT Technique for Protograph-Based Codes	417
	9.7 EXIT Charts for Turbo Codes	420
	9.8 The Area Property for EXIT Charts	424
	9.8.1 Serial-Concatenated Codes	424
	9.8.2 LDPC Codes	425
	Problems	426
	References	428
10	Finite-Geometry LDPC Codes	430
	10.1 Construction of LDPC Codes Based on Lines of Euclidean Geometries	430
	10.1.1 A Class of Cyclic EG-LDPC Codes	432
	10.1.2 A Class of Quasi-Cyclic EG-LDPC Codes	434

x	Contents	
	10.2 Construction of LDPC Codes Based on the Parallel Bundles of Lines in Euclidean Geometries	436
	10.3 Construction of LDPC Codes Based on Decomposition of Euclidean Geometries	439
	10.4 Construction of EG-LDPC Codes by Masking	444
	10.4.1 Masking	445
	10.4.2 Regular Masking	446
	10.4.3 Irregular Masking	447
	10.5 Construction of QC-EG-LDPC Codes by Circulant Decomposition	450
	10.6 Construction of Cyclic and QC-LDPC Codes Based on Projective Geometries	455
	10.6.1 Cyclic PG-LDPC Codes	455
	10.6.2 Quasi-Cyclic PG-LDPC Codes	458
	10.7 One-Step Majority-Logic and Bit-Flipping Decoding Algorithms for FG-LDPC Codes	460
	10.7.1 The OSMLG Decoding Algorithm for LDPC Codes over the BSC	461
	10.7.2 The BF Algorithm for Decoding LDPC Codes over the BSC	468
	10.8 Weighted BF Decoding: Algorithm 1	469
	10.9 Weighted BF Decoding: Algorithms 2 and 3	472
	10.10 Concluding Remarks	477
	Problems	477
	References	481
11	Constructions of LDPC Codes Based on Finite Fields	484
	11.1 Matrix Dispersions of Elements of a Finite Field	484
	11.2 A General Construction of QC-LDPC Codes Based on Finite Fields	485
	11.3 Construction of QC-LDPC Codes Based on the Minimum-Weight Codewords of an RS Code with Two Information Symbols	487
	11.4 Construction of QC-LDPC Codes Based on the Universal Parity-Check Matrices of a Special Subclass of RS Codes	495
	11.5 Construction of QC-LDPC Codes Based on Subgroups of a Finite Field	501
	11.5.1 Construction of QC-LDPC Codes Based on Subgroups of the Additive Group of a Finite Field	501
	11.5.2 Construction of QC-LDPC Codes Based on Subgroups of the Multiplicative Group of a Finite Field	503
	11.6 Construction of QC-LDPC Code Based on the Additive Group of a Prime Field	506
	11.7 Construction of QC-LDPC Codes Based on Primitive Elements of a Field	510
	11.8 Construction of QC-LDPC Codes Based on the Intersecting Bundles of Lines of Euclidean Geometries	512
	11.9 A Class of Structured RS-Based LDPC Codes	516
	Problems	520
	References	522

	Contents	xi
12	LDPC Codes Based on Combinatorial Designs, Graphs, and Superposition	523
	12.1 Balanced Incomplete Block Designs and LDPC Codes	523
	12.2 Class-I Bose BIBDs and QC-LDPC Codes	524
	12.2.1 Class-I Bose BIBDs	525
	12.2.2 Type-I Class-I Bose BIBD-LDPC Codes	525
	12.2.3 Type-II Class-I Bose BIBD-LDPC Codes	527
	12.3 Class-II Bose BIBDs and QC-LDPC Codes	530
	12.3.1 Class-II Bose BIBDs	531
	12.3.2 Type-I Class-II Bose BIBD-LDPC Codes	531
	12.3.3 Type-II Class-II QC-BIBD-LDPC Codes	533
	12.4 Construction of Type-II Bose BIBD-LDPC Codes by Dispersion	536
	12.5 A Trellis-Based Construction of LDPC Codes	537
	12.5.1 A Trellis-Based Method for Removing Short Cycles from a Bipartite Graph	538
	12.5.2 Code Construction	540
	12.6 Construction of LDPC Codes Based on Progressive Edge-Growth Tanner Graphs	542
	12.7 Construction of LDPC Codes by Superposition	546
	12.7.1 A General Superposition Construction of LDPC Codes	546
	12.7.2 Construction of Base and Constituent Matrices	548
	12.7.3 Superposition Construction of Product LDPC Codes	552
	12.8 Two Classes of LDPC Codes with Girth 8	554
	Problems	557
	References	559
13	LDPC Codes for Binary Erasure Channels	561
	13.1 Iterative Decoding of LDPC Codes for the BEC	561
	13.2 Random-Erasure-Correction Capability	563
	13.3 Good LDPC Codes for the BEC	565
	13.4 Correction of Erasure-Bursts	570
	13.5 Erasure-Burst-Correction Capabilities of Cyclic Finite-Geometry and Superposition LDPC Codes	573
	13.5.1 Erasure-Burst-Correction with Cyclic Finite-Geometry LDPC Codes	573
	13.5.2 Erasure-Burst-Correction with Superposition LDPC Codes	574
	13.6 Asymptotically Optimal Erasure-Burst-Correction QC-LDPC Codes	575
	13.7 Construction of QC-LDPC Codes by Array Dispersion	580
	13.8 Cyclic Codes for Correcting Bursts of Erasures	586
	Problems	589
	References	590
14	Nonbinary LDPC Codes	592
	14.1 Definitions	592
	14.2 Decoding of Nonbinary LDPC Codes	593
	14.2.1 The QSPA	593
	14.2.2 The FFT-QSPA	598

xii	Contents	
	14.3 Construction of Nonbinary LDPC Codes Based on Finite Geometries	600
	14.3.1 A Class of q^m -ary Cyclic EG-LDPC Codes	601
	14.3.2 A Class of Nonbinary Quasi-Cyclic EG-LDPC Codes	607
	14.3.3 A Class of Nonbinary Regular EG-LDPC Codes	610
	14.3.4 Nonbinary LDPC Code Constructions Based on Projective Geometries	611
	14.4 Constructions of Nonbinary QC-LDPC Codes Based on Finite Fields	614
	14.4.1 Dispersion of Field Elements into Nonbinary Circulant Permutation Matrices	615
	14.4.2 Construction of Nonbinary QC-LDPC Codes Based on Finite Fields	615
	14.4.3 Construction of Nonbinary QC-LDPC Codes by Masking	617
	14.4.4 Construction of Nonbinary QC-LDPC Codes by Array Dispersion	618
	14.5 Construction of QC-EG-LDPC Codes Based on Parallel Flats in Euclidean Geometries and Matrix Dispersion	620
	14.6 Construction of Nonbinary QC-EG-LDPC Codes Based on Intersecting Flats in Euclidean Geometries and Matrix Dispersion	624
	14.7 Superposition–Dispersion Construction of Nonbinary QC-LDPC Codes	628
	Problems	631
	References	633
15	LDPC Code Applications and Advanced Topics	636
	15.1 LDPC-Coded Modulation	636
	15.1.1 Design Based on EXIT Charts	638
	15.2 Turbo Equalization and LDPC Code Design for ISI Channels	644
	15.2.1 Turbo Equalization	644
	15.2.2 LDPC Code Design for ISI Channels	648
	15.3 Estimation of LDPC Error Floors	651
	15.3.1 The Error-Floor Phenomenon and Trapping Sets	651
	15.3.2 Error-Floor Estimation	654
	15.4 LDPC Decoder Design for Low Error Floors	657
	15.4.1 Codes Under Study	659
	15.4.2 The Bi-Mode Decoder	661
	15.4.3 Concatenation and Bit-Pinning	666
	15.4.4 Generalized-LDPC Decoder	668
	15.4.5 Remarks	670
	15.5 LDPC Convolutional Codes	670
	15.6 Fountain Codes	672
	15.6.1 Tornado Codes	673
	15.6.2 Luby Transform Codes	674
	15.6.3 Raptor Codes	675
	Problems	676
	References	677
	<i>Index</i>	681