
Error Control Coding

Fundamentals and Applications

Second Edition

Shu Lin

*University of California, Davis
University of Hawaii, Manoa*

Daniel J. Costello

University of Notre Dame



Pearson Education International

Contents

Preface	ix
1 Coding for Reliable Digital Transmission and Storage	1
1.1 Introduction	1
1.2 Types of Codes	3
1.3 Modulation and Coding	5
1.4 Maximum Likelihood Decoding	10
1.5 Types of Errors	13
1.6 Error Control Strategies	14
1.7 Performance Measures	15
1.8 Coded Modulation	21
Bibliography	23
2 Introduction to Algebra	25
2.1 Groups	25
2.2 Fields	31
2.3 Binary Field Arithmetic	37
2.4 Construction of Galois Field $GF(2^m)$	42
2.5 Basic Properties of a Galois Field $GF(2^m)$	47
2.6 Computations Using Galois Field $GF(2^m)$ Arithmetic	54
2.7 Vector Spaces	55
2.8 Matrices	61
Problems	63
Bibliography	65
3 Linear Block Codes	66
3.1 Introduction to Linear Block Codes	66
3.2 Syndrome and Error Detection	72
3.3 The Minimum Distance of a Block Code	76
3.4 Error-Detecting and Error-Correcting Capabilities of a Block Code	78
3.5 Standard Array and Syndrome Decoding	82
3.6 Probability of an Undetected Error for Linear Codes over a BSC	90
3.7 Single-Parity-Check Codes, Repetition Codes, and Self-Dual Codes	94
Problems	95
Bibliography	97
4 Important Linear Block Codes	99
4.1 Hamming Codes	100
4.2 A Class of Single-Error-Correcting and Double-Error-Detecting Codes	102
4.3 Reed–Muller Codes	105
4.4 Other Constructions for Reed–Muller Codes	114

4.5	The Squaring Construction of Codes	119
4.6	The (24, 12) Golay Code	125
4.7	Product Codes	128
4.8	Interleaved Codes	131
	Problems	132
	Bibliography	134
5	Cyclic Codes	136
5.1	Description of Cyclic Codes	136
5.2	Generator and Parity-Check Matrices of Cyclic Codes	143
5.3	Encoding of Cyclic Codes	146
5.4	Syndrome Computation and Error Detection	150
5.5	Decoding of Cyclic Codes	155
5.6	Cyclic Hamming Codes	162
5.7	Error-Trapping Decoding	166
5.8	Improved Error-Trapping Decoding	173
5.9	The (23, 12) Golay Code	175
5.10	Shortened Cyclic Codes	179
5.11	Cyclic Product Codes	184
5.12	Quasi-Cyclic Codes	185
	Problems	188
	Bibliography	192
6	Binary BCH Codes	194
6.1	Binary Primitive BCH Codes	194
6.2	Decoding of BCH Codes	205
6.3	Iterative Algorithm for Finding the Error-Location Polynomial $\sigma(X)$	209
6.4	Simplified Iterative Algorithm for Finding the Error-Location Polynomial $\sigma(X)$	212
6.5	Finding the Error-Location Numbers and Error Correction	215
6.6	Correction of Errors and Erasures	217
6.7	Implementation of Galois Field Arithmetic	217
6.8	Implementation of Error Correction	224
6.9	Weight Distribution and Error Detection of Binary BCH Codes	227
6.10	Remarks	230
	Problems	230
	Bibliography	231
7	Nonbinary BCH Codes, Reed–Solomon Codes, and Decoding Algorithms	234
7.1	q -ary Linear Block Codes	234
7.2	Primitive BCH Codes over $GF(q)$	236
7.3	Reed–Solomon Codes	237
7.4	Decoding of Nonbinary BCH and RS Codes: The Berlekamp Algorithm	241
7.5	Decoding with the Euclidean Algorithm	248
7.6	Frequency-Domain Decoding	255
7.7	Correction of Errors and Erasures	263

Problems	269
Bibliography	270
8 Majority-Logic Decodable and Finite Geometry Codes	273
8.1 One-Step Majority-Logic Decoding	273
8.2 A Class of One-Step Majority-Logic Decodable Codes	282
8.3 Other One-Step Majority-Logic Decodable Codes	290
8.4 Multiple-Step Majority-Logic Decoding	296
8.5 Euclidean Geometry	304
8.6 Euclidean Geometry Codes	309
8.7 Twofold EG Codes	319
8.8 Projective Geometry and Projective Geometry Codes	325
8.9 Remarks	331
Problems	332
Bibliography	335
9 Trellises for Linear Block Codes	338
9.1 Finite-State Machine Model and Trellis Representation of a Code	338
9.2 Bit-Level Trellises for Binary Linear Block Codes	342
9.3 State Labeling	351
9.4 Structural Properties of Bit-Level Trellises	354
9.5 State Labeling and Trellis Construction Based on the Parity-Check Matrix	360
9.6 Trellis Complexity and Symmetry	367
9.7 Trellis Sectionalization and Parallel Decomposition	374
9.8 Low-Weight Subtrellises	380
9.9 Cartesian Product	382
Problems	390
Bibliography	391
10 Reliability-Based Soft-Decision Decoding Algorithms for Linear Block Codes (Contributed by Marc P. C. Fossorier)	395
10.1 Soft-Decision Decoding	395
10.2 Reliability Measures and General Reliability-Based Decoding Schemes	400
10.3 Sufficient Conditions on the Optimality of a Decoded Codeword	402
10.4 Generalized Minimum Distance and Chase Decoding Algorithms	407
10.5 Weighted Erasure Decoding	413
10.6 A Maximum Likelihood Decoding Algorithm Based on Iterative Processing of the Least Reliable Positions	417
10.7 Reduced List Syndrome Decoding Algorithm	419
10.8 Most Reliable Independent Position Reprocessing Decoding Algorithms	422
10.9 Weighted Majority-Logic Decoding	439
10.10 Iterative Reliability-Based Decoding of One-Step Majority-Logic Decodable Codes	442

Problems	447
Bibliography	448
11 Convolutional Codes	453
11.1 Encoding of Convolutional Codes	454
11.2 Structural Properties of Convolutional Codes	486
11.3 Distance Properties of Convolutional Codes	506
Problems	510
Bibliography	513
12 Optimum Decoding of Convolutional Codes	515
12.1 The Viterbi Algorithm	516
12.2 Performance Bounds for Convolutional Codes	525
12.3 Construction of Good Convolutional Codes	538
12.4 Implementation and Performance of the Viterbi Algorithm	544
12.5 The Soft-Output Viterbi Algorithm (SOVA)	558
12.6 The BCJR algorithm	563
12.7 Punctured and Tail-Biting Convolutional Codes	582
Problems	598
Bibliography	602
13 Suboptimum Decoding of Convolutional Codes	605
13.1 The ZJ (Stack) Sequential Decoding Algorithm	606
13.2 The Fano Sequential Decoding Algorithm	620
13.3 Performance Characteristics of Sequential Decoding	626
13.4 Code Construction for Sequential Decoding	640
13.5 Majority-Logic Decoding	645
13.6 Performance Characteristics of Majority-Logic Decoding	670
13.7 Code Construction for Majority-Logic Decoding	677
Problems	685
Bibliography	688
14 Trellis-Based Soft-Decision Decoding Algorithms	691
14.1 The Viterbi Decoding Algorithm	691
14.2 A Recursive Maximum Likelihood Decoding Algorithm	695
14.3 A Suboptimum Iterative Decoding Algorithm Based on a Low-Weight Subtrellis	704
14.4 The MAP Decoding Algorithm	711
14.5 MAP Decoding Based on a Sectionalized Trellis	718
14.6 Max-log-MAP Decoding Algorithm	726
Problems	734
Bibliography	735
15 Concatenated Coding, Code Decomposition, and Multistage Decoding	739
15.1 Single-Level Concatenated Codes	739
15.2 Multilevel Concatenated Codes	743
15.3 A Soft-Decision Multistage Decoding	748
15.4 Decomposition of Codes	750
15.5 An Iterative Multistage MLD Algorithm	754

15.6	Concatenated Coding Schemes with Convolutional Inner Codes	760
15.7	Binary Concatenation	761
	Problems	763
	Bibliography	764
16	Turbo Coding	766
16.1	Introduction to Turbo Coding	767
16.2	Distance Properties of Turbo Codes	783
16.3	Performance Analysis of Turbo Codes	807
16.4	Design of Turbo Codes	814
16.5	Iterative Decoding of Turbo Codes	826
	Problems	844
	Bibliography	847
17	Low-Density Parity-Check Codes	851
17.1	Introduction to LDPC Codes	852
17.2	Tanner Graphs for Linear Block Codes	855
17.3	A Geometric Construction of LDPC Codes	858
17.4	EG-LDPC Codes	860
17.5	PG-LDPC Codes	866
17.6	Decoding of LDPC Codes	871
17.7	Code Construction by Column and Row Splitting	885
17.8	Breaking Cycles in Tanner Graphs	892
17.9	Shortened Finite-Geometry LDPC Codes	898
17.10	Construction of Gallager LDPC Codes	902
17.11	Masked EG-Gallager LDPC Codes	906
17.12	Construction of Quasi-Cyclic Codes by Circulant Decomposition	912
17.13	Construction of LDPC Codes Based on Finite Geometries over $GF(p^s)$	917
17.14	Random LDPC Codes	920
17.15	Irregular LDPC Codes	922
17.16	Graph-Theoretic LDPC Codes	929
17.17	Construction of LDPC Codes Based on Balanced Incomplete Block Designs	935
17.18	Construction of LDPC Codes Based on Shortened RS Codes with Two Information Symbols	938
17.19	Concatenations with LDPC and Turbo Codes	944
	Problems	945
	Bibliography	947
18	Trellis-Coded Modulation	952
18.1	Introduction to Trellis-Coded Modulation	953
18.2	TCM Code Construction	980
18.3	TCM Performance Analysis	992
18.4	Rotationally Invariant TCM	998
18.5	Multidimensional TCM	1015

Problems	1056
Bibliography	1059
19 Block Coded Modulation	1063
19.1 Distance Concepts	1063
19.2 Multilevel Block Modulation Codes	1064
19.3 Multistage Decoding of Multilevel BCM Codes	1075
19.4 Concatenated Coded Modulation	1081
19.5 Product Coded Modulation	1088
19.6 Multilevel Coded Modulation for Unequal Error Protection . . .	1090
Problems	1100
Bibliography	1101
20 Burst-Error-Correcting Codes	1104
20.1 Introduction	1104
20.2 Decoding of Single-Burst-Error-Correcting Cyclic Codes	1105
20.3 Single-Burst-Error-Correcting Codes	1107
20.4 Phased-Burst-Error-Correcting Codes	1118
20.5 Burst-and-Random-Error-Correcting Codes	1119
Problems	1124
Bibliography	1125
21 Burst-Error-Correcting Convolutional Codes	1127
21.1 Bounds on Burst-Error-Correcting Capability	1127
21.2 Burst-Error-Correcting Convolutional Codes	1128
21.3 Interleaved Convolutional Codes	1139
21.4 Burst-and-Random-Error-Correcting Convolutional Codes . . .	1142
Problems	1153
Bibliography	1154
22 Automatic-Repeat-Request Strategies	1156
22.1 Basic ARQ Schemes	1156
22.2 Selective-Repeat ARQ System with Finite Receiver Buffer . . .	1163
22.3 ARQ Schemes with Mixed Modes of Retransmission	1171
22.4 Hybrid ARQ Schemes	1174
22.5 A Class of Half-Rate Invertible Codes	1178
22.6 Type-II Hybrid Selective-Repeat ARQ with Finite Receiver Buffer	1181
22.7 Hybrid ARQ Systems Using Convolutional Codes	1190
22.8 A Concatenated Coded Modulation Hybrid ARQ System	1192
Problems	1197
Bibliography	1198
A Tables of Galois Fields	1204
B Minimal Polynomials of Elements in $GF(2^m)$	1227
C Generator Polynomials of Binary Primitive BCH Codes of Length up to $2^{10} - 1$	1231
Index	1249