

Contents

Preface	vii
List of Program Files	xxxi
List of Laboratory Exercises	xxxii
List of Algorithms	xxxiv
List of Figures	xl
List of Tables	xlii
List of Boxes	xliii
Part I Introduction and Foundations	1
1 A Context for Error Correction Coding	2
1.1 Purpose of This Book	2
1.2 Introduction: Where Are Codes?	2
1.3 The Communications System	4
1.4 Basic Digital Communications	9
1.4.1 Binary Phase-Shift Keying	10
1.4.2 More General Digital Modulation	11
1.5 Signal Detection	14
1.5.1 The Gaussian Channel	14
1.5.2 MAP and ML Detection	16
1.5.3 Special Case: Binary Detection	18
1.5.4 Probability of Error for Binary Detection	19
1.5.5 Bounds on Performance: The Union Bound	22
1.5.6 The Binary Symmetric Channel	23
1.5.7 The BSC and the Gaussian Channel Model	25
1.6 Memoryless Channels	25
1.7 Simulation and Energy Considerations for Coded Signals	26
1.8 Some Important Definitions	27
1.8.1 Detection of Repetition Codes Over a BSC	28
1.8.2 Soft-Decision Decoding of Repetition Codes Over the AWGN	32
1.8.3 Simulation of Results	33
1.8.4 Summary	33
1.9 Hamming Codes	34
1.9.1 Hard-Input Decoding Hamming Codes	35
1.9.2 Other Representations of the Hamming Code	36
An Algebraic Representation	37
A Polynomial Representation	37

A Trellis Representation	38
The Tanner Graph Representation	38
1.10 The Basic Questions	39
1.11 Historical Milestones of Coding Theory	40
1.12 A Bit of Information Theory	40
1.12.1 Definitions for Discrete Random Variables	40
Entropy and Conditional Entropy	40
Relative Entropy, Mutual Information, and Channel Capacity	41
1.12.2 Definitions for Continuous Random Variables	43
1.12.3 The Channel Coding Theorem	45
1.12.4 "Proof" of the Channel Coding Theorem	45
1.12.5 Capacity for the Continuous-Time AWGN Channel	49
1.12.6 Transmission at Capacity with Errors	51
1.12.7 The Implication of the Channel Coding Theorem	52
Lab 1 Simulating a Communications Channel	53
Objective	53
Background	53
Use of Coding in Conjunction with the BSC	53
Assignment	54
Programming Part	54
Resources and Implementation Suggestions	54
1.13 Exercises	56
1.14 References	60
Part II Block Codes	61
2 Groups and Vector Spaces	62
2.1 Introduction	62
2.2 Groups	62
2.2.1 Subgroups	65
2.2.2 Cyclic Groups and the Order of an Element	66
2.2.3 Cosets	67
2.2.4 Lagrange's Theorem	68
2.2.5 Induced Operations; Isomorphism	69
2.2.6 Homomorphism	72
2.3 Fields: A Prelude	73
2.4 Review of Linear Algebra	75
2.5 Exercises	80
2.6 References	82
3 Linear Block Codes	83
3.1 Basic Definitions	83
3.2 The Generator Matrix Description of Linear Block Codes	84
3.2.1 Rudimentary Implementation	86
3.3 The Parity Check Matrix and Dual Codes	86
3.3.1 Some Simple Bounds on Block Codes	88
3.4 Error Detection and Correction over Hard-Input Channels	90

3.4.1 Error Detection	90
3.4.2 Error Correction: The Standard Array	90
3.5 Weight Distributions of Codes and Their Duals	95
3.6 Hamming Codes and Their Duals	97
3.7 Performance of Linear Codes	98
3.7.1 Error detection performance	99
3.7.2 Error Correction Performance	100
3.7.3 Performance for Soft-Decision Decoding	103
3.8 Erasure Decoding	104
3.8.1 Binary Erasure Decoding	105
3.9 Modifications to Linear Codes	105
3.10 Best Known Linear Block Codes	107
3.11 Exercises	107
3.12 References	112
4 Cyclic Codes, Rings, and Polynomials	113
4.1 Introduction	113
4.2 Basic Definitions	113
4.3 Rings	114
4.3.1 Rings of Polynomials	115
4.4 Quotient Rings	116
4.5 Ideals in Rings	118
4.6 Algebraic Description of Cyclic Codes	120
4.7 Nonsystematic Encoding and Parity Check	122
4.8 Systematic Encoding	124
4.9 Some Hardware Background	126
4.9.1 Computational Building Blocks	126
4.9.2 Sequences and Power series	127
4.9.3 Polynomial Multiplication	128
Last-Element-First Processing	128
First-Element-First Processing	128
4.9.4 Polynomial division	129
Last-Element-First Processing	129
4.9.5 Simultaneous Polynomial Division and Multiplication	132
First-Element-First Processing	132
4.10 Cyclic Encoding	133
4.11 Syndrome Decoding	137
4.12 Shortened Cyclic Codes	143
Method 1: Simulating the Extra Clock Shifts	144
Method 2: Changing the Error Pattern Detection Circuit	147
4.13 Binary CRC Codes	147
4.13.1 Byte-Oriented Encoding and Decoding Algorithms	150
4.13.2 CRC Protecting Data Files or Data Packets	153
Appendix 4.A Linear Feedback Shift Registers	154
Appendix 4.A.1 Basic Concepts	154
Appendix 4.A.2 Connection With Polynomial Division	157
Appendix 4.A.3 Some Algebraic Properties of Shift Sequences	160

Lab 2 Polynomial Division and Linear Feedback Shift Registers	161
Objective	161
Preliminary Exercises	161
Programming Part: BinLFSR	161
Resources and Implementation Suggestions	161
Programming Part: BinPolyDiv	162
Follow-On Ideas and Problems	162
Lab 3 CRC Encoding and Decoding	162
Objective	163
Preliminary	163
Programming Part	163
Resources and Implementation Suggestions	163
4.14 Exercises	165
4.15 References	170
5 Rudiments of Number Theory and Algebra	171
5.1 Motivation	171
5.2 Number Theoretic Preliminaries	175
5.2.1 Divisibility	175
5.2.2 The Euclidean Algorithm and Euclidean Domains	177
5.2.3 The Sugiyama Algorithm	182
5.2.4 Congruence	184
5.2.5 The ϕ Function	185
5.2.6 Some Cryptographic Payoff	186
Fermat's Little Theorem	186
RSA Encryption	187
5.3 The Chinese Remainder Theorem	188
5.3.1 The CRT and Interpolation	190
The Evaluation Homomorphism	190
The Interpolation Problem	191
5.4 Fields	193
5.4.1 An Examination of \mathbb{R} and \mathbb{C}	194
5.4.2 Galois Field Construction: An Example	196
5.4.3 Connection with Linear Feedback Shift Registers	199
5.5 Galois Fields: Mathematical Facts	200
5.6 Implementing Galois Field Arithmetic	204
5.6.1 Zech Logarithms	204
5.6.2 Hardware Implementations	205
5.7 Subfields of Galois Fields	206
5.8 Irreducible and Primitive polynomials	207
5.9 Conjugate Elements and Minimal Polynomials	209
5.9.1 Minimal Polynomials	212
5.10 Factoring $x^n - 1$	215
5.11 Cyclotomic Cosets	217
Appendix 5.A How Many Irreducible Polynomials Are There?	218
Appendix 5.A.1 Solving for I_m Explicitly: The Moebius Function	222
Lab 4 Programming the Euclidean Algorithm	223

Objective	223
Preliminary Exercises	223
Background	223
Programming Part	223
Lab 5 Programming Galois Field Arithmetic	224
Objective	224
Preliminary Exercises	224
Programming Part	224
5.12 Exercises	225
5.13 References	234
6 BCH and Reed-Solomon Codes: Designer Cyclic Codes	235
6.1 BCH Codes	235
6.1.1 Designing BCH Codes	235
6.1.2 The BCH Bound	237
6.1.3 Weight Distributions for Some Binary BCH Codes	239
6.1.4 Asymptotic Results for BCH Codes	240
6.2 Reed-Solomon Codes	242
6.2.1 Reed-Solomon Construction 1	242
6.2.2 Reed-Solomon Construction 2	243
6.2.3 Encoding Reed-Solomon Codes	244
6.2.4 MDS Codes and Weight Distributions for RS Codes	245
6.3 Decoding BCH and RS Codes: The General Outline	247
6.3.1 Computation of the Syndrome	247
6.3.2 The Error Locator Polynomial	248
6.3.3 Chien Search	248
6.4 Finding the Error Locator Polynomial	250
6.4.1 Simplifications for Binary Codes and Peterson's Algorithm	251
6.4.2 Berlekamp-Massey Algorithm	253
6.4.3 Characterization of LFSR Length in Massey's Algorithm	255
6.4.4 Simplifications for Binary Codes	259
6.5 Non-Binary BCH and RS Decoding	261
6.5.1 Forney's Algorithm	262
6.6 Euclidean Algorithm for the Error Locator Polynomial	266
6.7 Erasure Decoding for Nonbinary BCH or RS codes	267
6.8 Galois Field Fourier Transform Methods	269
6.8.1 Equivalence of the Two Reed-Solomon Code Constructions	274
6.8.2 Frequency-Domain Decoding	275
6.9 Variations and Extensions of Reed-Solomon Codes	276
6.9.1 Simple Modifications	276
6.9.2 Generalized Reed-Solomon Codes and Alternant Codes	277
6.9.3 Goppa Codes	278
6.9.4 Decoding Alternant Codes	280
6.9.5 The McEliece Public Key Cryptosystem	280
Lab 6 Programming the Berlekamp-Massey Algorithm	281
Background	281
Assignment	281

Preliminary Exercises	281
Programming Part	281
Resources and Implementation Suggestions	282
Lab 7 Programming the BCH Decoder	283
Objective	283
Preliminary Exercises	283
Programming Part	283
Resources and Implementation Suggestions	283
Follow-On Ideas and Problems	284
Lab 8 Reed-Solomon Encoding and Decoding	284
Objective	284
Background	284
Programming Part	284
Appendix 6.A Proof of Newton's Identities	285
6.10 Exercises	287
6.11 References	291
7 Alternate Decoding Algorithms for Reed-Solomon Codes	293
7.1 Introduction: Workload for Reed-Solomon Decoding	293
7.2 Derivations of Welch-Berlekamp Key Equation	293
7.2.1 The Welch-Berlekamp Derivation of the WB Key Equation	294
7.2.2 Derivation From the Conventional Key Equation	298
7.3 Finding the Error Values	300
7.4 Methods of Solving the WB Key Equation	302
7.4.1 Background: Modules	302
7.4.2 The Welch-Berlekamp Algorithm	303
7.4.3 Modular Solution of the WB Key Equation	310
7.5 Erasure Decoding with the Welch-Berlekamp Key Equation	321
7.6 The Guruswami-Sudan Decoding Algorithm and Soft RS Decoding	322
7.6.1 Bounded Distance, ML, and List Decoding	322
7.6.2 Error Correction by Interpolation	323
7.6.3 Polynomials in Two Variables	324
Degree and Monomial Order	325
Zeros and Multiple Zeros	328
7.6.4 The GS Decoder: The Main Theorems	330
The Interpolation Theorem	331
The Factorization Theorem	331
The Correction Distance	333
The Number of Polynomials in the Decoding List	335
7.6.5 Algorithms for Computing the Interpolation Step	337
Finding Linearly Dependent Columns: The Feng-Tzeng Algorithm	338
Finding the Intersection of Kernels: The Kötter Algorithm	342
7.6.6 A Special Case: $m = 1$ and $L = 1$	348
7.6.7 The Roth-Ruckenstein Algorithm	350
What to Do with Lists of Factors?	354
7.6.8 Soft-Decision Decoding of Reed-Solomon Codes	358
Notation	358

A Factorization Theorem	360
Mapping from Reliability to Multiplicity	361
The Geometry of the Decoding Regions	363
Computing the Reliability Matrix	364
7.7 Exercises	365
7.8 References	368
8 Other Important Block Codes	369
8.1 Introduction	369
8.2 Hadamard Matrices, Codes, and Transforms	369
8.2.1 Introduction to Hadamard Matrices	369
8.2.2 The Paley Construction of Hadamard Matrices	371
8.2.3 Hadamard Codes	374
8.3 Reed-Muller Codes	375
8.3.1 Boolean Functions	375
8.3.2 Definition of the Reed-Muller Codes	376
8.3.3 Encoding and Decoding Algorithms for First-Order RM Codes	379
Encoding $RM(1, m)$ Codes	379
Decoding $RM(1, m)$ Codes	379
Expediting Decoding Using the Fast Hadamard Transform	382
8.3.4 The Reed Decoding Algorithm for $RM(r, m)$ Codes, $r \geq 1$	384
Details for an $RM(2, 4)$ Code	384
A Geometric Viewpoint	387
8.3.5 Other Constructions of Reed-Muller Codes	391
8.4 Building Long Codes from Short Codes: The Squaring Construction	392
8.5 Quadratic Residue Codes	396
8.6 Golay Codes	398
8.6.1 Decoding the Golay Code	400
Algebraic Decoding of the \mathcal{G}_{23} Golay Code	400
Arithmetic Decoding of the \mathcal{G}_{24} Code	401
8.7 Exercises	403
8.8 References	404
9 Bounds on Codes	406
9.1 The Gilbert-Varshamov Bound	409
9.2 The Plotkin Bound	410
9.3 The Griesmer Bound	411
9.4 The Linear Programming and Related Bounds	413
9.4.1 Krawtchouk Polynomials	415
9.4.2 Character	415
9.4.3 Krawtchouk Polynomials and Characters	416
9.5 The McEliece-Rodemich-Rumsey-Welch Bound	418
9.6 Exercises	420
9.7 References	424

10 Bursty Channels, Interleavers, and Concatenation	425
10.1 Introduction to Bursty Channels	425
10.2 Interleavers	425
10.3 An Application of Interleaved RS Codes: Compact Discs	427
10.4 Product Codes	430
10.5 Reed-Solomon Codes	431
10.6 Concatenated Codes	432
10.7 Fire Codes	433
10.7.1 Fire Code Definition	433
10.7.2 Decoding Fire Codes: Error Trapping Decoding	435
10.8 Exercises	437
10.9 References	438
11 Soft-Decision Decoding Algorithms	439
11.1 Introduction and General Notation	439
11.2 Generalized Minimum Distance Decoding	441
11.2.1 Distance Measures and Properties	442
11.3 The Chase Decoding Algorithms	445
11.4 Halting the Search: An Optimality Condition	445
11.5 Ordered Statistic Decoding	447
11.6 Exercises	449
11.7 References	450
Part III Codes on Graphs	451
12 Convolutional Codes	452
12.1 Introduction and Basic Notation	452
12.1.1 The State	456
12.2 Definition of Codes and Equivalent Codes	458
12.2.1 Catastrophic Encoders	461
12.2.2 Polynomial and Rational Encoders	464
12.2.3 Constraint Length and Minimal Encoders	465
12.2.4 Systematic Encoders	468
12.3 Decoding Convolutional Codes	469
12.3.1 Introduction and Notation	469
12.3.2 The Viterbi Algorithm	471
12.3.3 Some Implementation Issues	481
The Basic Operation: Add-Compare-Select	481
Decoding Streams of Data: Windows on the Trellis	481
Output Decisions	482
Hard and Soft Decoding; Quantization	484
Synchronization Issues	486
12.4 Some Performance Results	487
12.5 Error Analysis for Convolutional Codes	491
12.5.1 Enumerating Paths Through the Trellis	493
Enumerating on More Complicated Graphs: Mason's Rule	496

12.5.2 Characterizing the Node Error Probability P_e and the Bit Error Rate P_b	498
12.5.3 A Bound on P_d for Discrete Channels	501
Performance Bound on the BSC	503
12.5.4 A Bound on P_d for BPSK Signaling Over the AWGN Channel	503
12.5.5 Asymptotic Coding Gain	504
12.6 Tables of Good Codes	505
12.7 Puncturing	507
12.7.1 Puncturing to Achieve Variable Rate	509
12.8 Suboptimal Decoding Algorithms for Convolutional Codes	510
12.8.1 Tree Representations	511
12.8.2 The Fano Metric	511
12.8.3 The Stack Algorithm	515
12.8.4 The Fano Algorithm	517
12.8.5 Other Issues for Sequential Decoding	520
12.8.6 A Variation on the Viterbi Algorithm: The M Algorithm	521
12.9 Convolutional Codes as Block Codes	522
12.10 Trellis Representations of Block and Cyclic Codes	523
12.10.1 Block Codes	523
12.10.2 Cyclic Codes	524
12.10.3 Trellis Decoding of Block Codes	525
Lab 9 Programming Convolutional Encoders	526
Objective	526
Background	526
Programming Part	526
Lab 10 Convolutional Decoders: The Viterbi Algorithm	528
Objective	528
Background	528
Programming Part	528
12.11 Exercises	529
12.12 References	533
13 Trellis Coded Modulation	535
13.1 Adding Redundancy by Adding Signals	535
13.2 Background on Signal Constellations	535
13.3 TCM Example	537
13.3.1 The General Ungerboeck Coding Framework	544
13.3.2 The Set Partitioning Idea	545
13.4 Some Error Analysis for TCM Codes	546
13.4.1 General Considerations	546
13.4.2 A Description of the Error Events	548
13.4.3 Known Good TCM Codes	552
13.5 Decoding TCM Codes	554
13.6 Rotational Invariance	556
Differential Encoding	558
Constellation Labels and Partitions	559
13.7 Multidimensional TCM	561

13.7.1	Some Advantages of Multidimensional TCM	562
13.7.2	Lattices and Sublattices	563
	Basic Definitions	563
	Common Lattices	565
	Sublattices and Cosets	566
	The Lattice Code Idea	567
	Sources of Coding Gain in Lattice Codes	567
	Some Good Lattice Codes	571
13.8	The V.34 Modem Standard	571
Lab 11	Trellis-Coded Modulation Encoding and Decoding	578
	Objective	578
	Background	578
	Programming Part	578
13.9	Exercises	578
13.10	References	580

Part IV Iteratively Decoded Codes 581

14	Turbo Codes	582
14.1	Introduction	582
14.2	Encoding Parallel Concatenated Codes	584
14.3	Turbo Decoding Algorithms	586
14.3.1	The MAP Decoding Algorithm	588
14.3.2	Notation	588
14.3.3	Posterior Probability	590
14.3.4	Computing α_t and β_t	592
14.3.5	Computing γ_t	593
14.3.6	Normalization	594
14.3.7	Summary of the BCJR Algorithm	596
14.3.8	A Matrix/Vector Formulation	597
14.3.9	Comparison of the Viterbi and BCJR Algorithms	598
14.3.10	The BCJR Algorithm for Systematic Codes	598
14.3.11	Turbo Decoding Using the BCJR Algorithm	600
The Terminal State of the Encoders		602
14.3.12	Likelihood Ratio Decoding	602
Log Prior Ratio $\lambda_{p,t}$		603
Log Posterior $\lambda_{s,t}^{(0)}$		605
14.3.13	Statement of the Turbo Decoding Algorithm	605
14.3.14	Turbo Decoding Stopping Criteria	605
The Cross Entropy Stopping Criterion		606
The Sign Change Ratio (SCR) Criterion		607
The Hard Decision Aided (HDA) Criterion		608
14.3.15	Modifications of the MAP Algorithm	608
The Max-Log-MAP Algorithm		608
14.3.16	Corrections to the Max-Log-MAP Algorithm	609
14.3.17	The Soft Output Viterbi Algorithm	610
14.4	On the Error Floor and Weight Distributions	612

14.4.1	The Error Floor	612
14.4.2	Spectral Thinning and Random Interleavers	614
14.4.3	On Interleavers	618
14.5	EXIT Chart Analysis	619
14.5.1	The EXIT Chart	622
14.6	Block Turbo Coding	623
14.7	Turbo Equalization	626
14.7.1	Introduction to Turbo Equalization	626
14.7.2	The Framework for Turbo Equalization	627
Lab 12	Turbo Code Decoding	629
	Objective	629
	Background	629
	Programming Part	629
14.8	Exercises	629
14.9	References	632
15	Low-Density Parity-Check Codes	634
15.1	Introduction	634
15.2	LDPC Codes: Construction and Notation	635
15.3	Tanner Graphs	638
15.4	Transmission Through a Gaussian Channel	638
15.5	Decoding LDPC Codes	640
15.5.1	The Vertical Step: Updating $q_{mn}(x)$	641
15.5.2	Horizontal Step: Updating $r_{mn}(x)$	644
15.5.3	Terminating and Initializing the Decoding Algorithm	647
15.5.4	Summary of the Algorithm	648
15.5.5	Message Passing Viewpoint	649
15.5.6	Likelihood Ratio Decoder Formulation	649
15.6	Why Low-Density Parity-Check Codes?	653
15.7	The Iterative Decoder on General Block Codes	654
15.8	Density Evolution	655
15.9	EXIT Charts for LDPC Codes	659
15.10	Irregular LDPC Codes	660
15.10.1	Degree Distribution Pairs	662
15.10.2	Some Good Codes	664
15.10.3	Density Evolution for Irregular Codes	664
15.10.4	Computation and Optimization of Density Evolution	667
15.10.5	Using Irregular Codes	668
15.11	More on LDPC Code Construction	668
15.11.1	A Construction Based on Finite Geometries	668
15.11.2	Constructions Based on Other Combinatoric Objects	669
15.12	Encoding LDPC Codes	669
15.13	A Variation: Low-Density Generator Matrix Codes	671
15.14	Serial Concatenated Codes; Repeat-Accumulate Codes	671
15.14.1	Irregular RA Codes	673
Lab 13	Programming an LDPC Decoder	674
	Objective	674

Background	674
Assignment	675
Numerical Considerations	675
15.15 Exercises	676
15.16 References	679
16 Decoding Algorithms on Graphs	680
16.1 Introduction	680
16.2 Operations in Semirings	681
16.3 Functions on Local Domains	681
16.4 Factor Graphs and Marginalization	686
16.4.1 Marginalizing on a Single Variable	687
16.4.2 Marginalizing on All Individual Variables	691
16.5 Applications to Coding	694
16.5.1 Block Codes	694
16.5.2 Modifications to Message Passing for Binary Variables	695
16.5.3 Trellis Processing and the Forward/Backward Algorithm	696
16.5.4 Turbo Codes	699
16.6 Summary of Decoding Algorithms on Graphs	699
16.7 Transformations of Factor Graphs	700
16.7.1 Clustering	700
16.7.2 Stretching Variable Nodes	701
16.7.3 Exact Computation of Graphs with Cycles	702
16.8 Exercises	706
16.9 References	708
Part V Space-Time Coding	709
17 Fading Channels and Space-Time Codes	710
17.1 Introduction	710
17.2 Fading Channels	710
17.2.1 Rayleigh Fading	712
17.3 Diversity Transmission and Reception: The MIMO Channel	714
17.3.1 The Narrowband MIMO Channel	716
17.3.2 Diversity Performance with Maximal-Ratio Combining	717
17.4 Space-Time Block Codes	719
17.4.1 The Alamouti Code	719
17.4.2 A More General Formulation	721
17.4.3 Performance Calculation	721
Real Orthogonal Designs	723
Encoding and Decoding Based on Orthogonal Designs	724
Generalized Real Orthogonal Designs	726
17.4.4 Complex Orthogonal Designs	727
Future Work	728
17.5 Space-Time Trellis Codes	728
17.5.1 Concatenation	729
17.6 How Many Antennas?	732

17.7 Estimating Channel Information	733
17.8 Exercises	733
17.9 References	734
A Log Likelihood Algebra	735
A.1 Exercises	737
References	739
Index	750