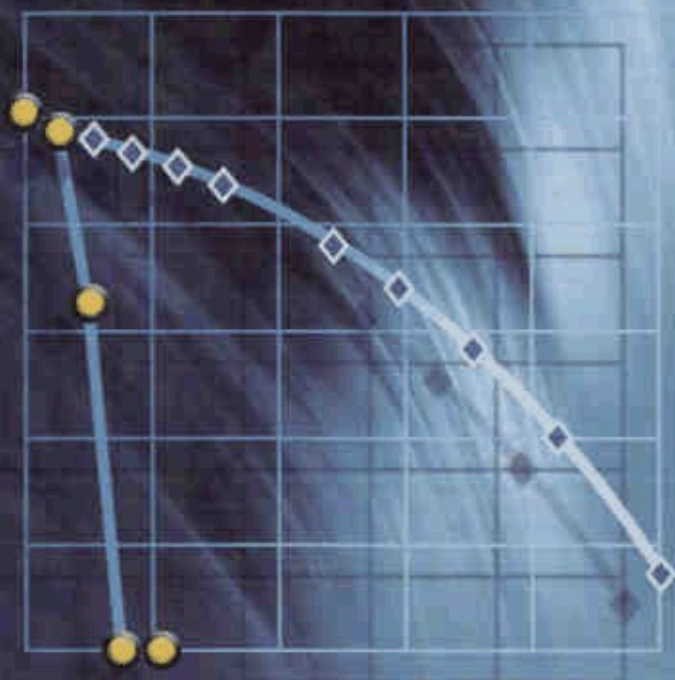


Jorge Castiñeira Moreira
Patrick Guy Farrell

Essentials of Error-Control Coding



Companion Website

 WILEY

Contents

Preface	xiii
Acknowledgements	xv
List of Symbols	xvii
Abbreviations	xxv
1 Information and Coding Theory	1
1.1 Information	3
1.1.1 <i>A Measure of Information</i>	3
1.2 Entropy and Information Rate	4
1.3 Extended DMSs	9
1.4 Channels and Mutual Information	10
1.4.1 <i>Information Transmission over Discrete Channels</i>	10
1.4.2 <i>Information Channels</i>	10
1.5 Channel Probability Relationships	13
1.6 The <i>A Priori</i> and <i>A Posteriori</i> Entropies	15
1.7 Mutual Information	16
1.7.1 <i>Mutual Information: Definition</i>	16
1.7.2 <i>Mutual Information: Properties</i>	17
1.8 Capacity of a Discrete Channel	21
1.9 The Shannon Theorems	22
1.9.1 <i>Source Coding Theorem</i>	22
1.9.2 <i>Channel Capacity and Coding</i>	23
1.9.3 <i>Channel Coding Theorem</i>	25
1.10 Signal Spaces and the Channel Coding Theorem	27
1.10.1 <i>Capacity of the Gaussian Channel</i>	28
1.11 Error-Control Coding	32
1.12 Limits to Communication and their Consequences	34
Bibliography and References	38
Problems	38

2	Block Codes	41
2.1	Error-Control Coding	41
2.2	Error Detection and Correction	41
2.2.1	<i>Simple Codes: The Repetition Code</i>	42
2.3	Block Codes: Introduction and Parameters	43
2.4	The Vector Space over the Binary Field	44
2.4.1	<i>Vector Subspaces</i>	46
2.4.2	<i>Dual Subspace</i>	48
2.4.3	<i>Matrix Form</i>	48
2.4.4	<i>Dual Subspace Matrix</i>	49
2.5	Linear Block Codes	50
2.5.1	<i>Generator Matrix G</i>	51
2.5.2	<i>Block Codes in Systematic Form</i>	52
2.5.3	<i>Parity Check Matrix H</i>	54
2.6	Syndrome Error Detection	55
2.7	Minimum Distance of a Block Code	58
2.7.1	<i>Minimum Distance and the Structure of the H Matrix</i>	58
2.8	Error-Correction Capability of a Block Code	59
2.9	Syndrome Detection and the Standard Array	61
2.10	Hamming Codes	64
2.11	Forward Error Correction and Automatic Repeat ReQuest	65
2.11.1	<i>Forward Error Correction</i>	65
2.11.2	<i>Automatic Repeat ReQuest</i>	68
2.11.3	<i>ARQ Schemes</i>	69
2.11.4	<i>ARQ Scheme Efficiencies</i>	71
2.11.5	<i>Hybrid-ARQ Schemes</i>	72
	Bibliography and References	76
	Problems	77
3	Cyclic Codes	81
3.1	Description	81
3.2	Polynomial Representation of Codewords	81
3.3	Generator Polynomial of a Cyclic Code	83
3.4	Cyclic Codes in Systematic Form	85
3.5	Generator Matrix of a Cyclic Code	87
3.6	Syndrome Calculation and Error Detection	89
3.7	Decoding of Cyclic Codes	90
3.8	An Application Example: Cyclic Redundancy Check Code for the Ethernet Standard	92
	Bibliography and References	93
	Problems	94
4	BCH Codes	97
4.1	Introduction: The Minimal Polynomial	97
4.2	Description of BCH Cyclic Codes	99
4.2.1	<i>Bounds on the Error-Correction Capability of a BCH Code: The Vandermonde Determinant</i>	102

4.3 Decoding of BCH Codes	104
4.4 Error-Location and Error-Evaluation Polynomials	105
4.5 The Key Equation	107
4.6 Decoding of Binary BCH Codes Using the Euclidean Algorithm	108
4.6.1 <i>The Euclidean Algorithm</i>	108
Bibliography and References	112
Problems	112
5 Reed–Solomon Codes	115
5.1 Introduction	115
5.2 Error-Correction Capability of RS Codes: The Vandermonde Determinant	117
5.3 RS Codes in Systematic Form	119
5.4 Syndrome Decoding of RS Codes	120
5.5 The Euclidean Algorithm: Error-Location and Error-Evaluation Polynomials	122
5.6 Decoding of RS Codes Using the Euclidean Algorithm	125
5.6.1 <i>Steps of the Euclidean Algorithm</i>	127
5.7 Decoding of RS and BCH Codes Using the Berlekamp–Massey Algorithm	128
5.7.1 <i>B–M Iterative Algorithm for Finding the Error-Location Polynomial</i>	130
5.7.2 <i>B–M Decoding of RS Codes</i>	133
5.7.3 <i>Relationship Between the Error-Location Polynomials of the Euclidean and B–M Algorithms</i>	136
5.8 A Practical Application: Error-Control Coding for the Compact Disk	136
5.8.1 <i>Compact Disk Characteristics</i>	136
5.8.2 <i>Channel Characteristics</i>	138
5.8.3 <i>Coding Procedure</i>	138
5.9 Encoding for RS codes $C_{RS}(28, 24)$, $C_{RS}(32, 28)$ and $C_{RS}(255, 251)$	139
5.10 Decoding of RS Codes $C_{RS}(28, 24)$ and $C_{RS}(32, 28)$	142
5.10.1 <i>B–M Decoding</i>	142
5.10.2 <i>Alternative Decoding Methods</i>	145
5.10.3 <i>Direct Solution of Syndrome Equations</i>	146
5.11 Importance of Interleaving	148
Bibliography and References	152
Problems	153
6 Convolutional Codes	157
6.1 Linear Sequential Circuits	158
6.2 Convolutional Codes and Encoders	158
6.3 Description in the D -Transform Domain	161
6.4 Convolutional Encoder Representations	166
6.4.1 <i>Representation of Connections</i>	166
6.4.2 <i>State Diagram Representation</i>	166
6.4.3 <i>Trellis Representation</i>	168
6.5 Convolutional Codes in Systematic Form	168
6.6 General Structure of Finite Impulse Response and Infinite Impulse Response FSSMs	170
6.6.1 <i>Finite Impulse Response FSSMs</i>	170
6.6.2 <i>Infinite Impulse Response FSSMs</i>	171

6.7 State Transfer Function Matrix: Calculation of the Transfer Function	172
6.7.1 <i>State Transfer Function for FIR FSSMs</i>	172
6.7.2 <i>State Transfer Function for IIR FSSMs</i>	173
6.8 Relationship Between the Systematic and the Non-Systematic Forms	175
6.9 Distance Properties of Convolutional Codes	177
6.10 Minimum Free Distance of a Convolutional Code	180
6.11 Maximum Likelihood Detection	181
6.12 Decoding of Convolutional Codes: The Viterbi Algorithm	182
6.13 Extended and Modified State Diagram	185
6.14 Error Probability Analysis for Convolutional Codes	186
6.15 Hard and Soft Decisions	189
6.15.1 <i>Maximum Likelihood Criterion for the Gaussian Channel</i>	192
6.15.2 <i>Bounds for Soft-Decision Detection</i>	194
6.15.3 <i>An Example of Soft-Decision Decoding of Convolutional Codes</i>	196
6.16 Punctured Convolutional Codes and Rate-Compatible Schemes	200
Bibliography and References	203
Problems	205
7 Turbo Codes	209
7.1 A Turbo Encoder	210
7.2 Decoding of Turbo Codes	211
7.2.1 <i>The Turbo Decoder</i>	211
7.2.2 <i>Probabilities and Estimates</i>	212
7.2.3 <i>Symbol Detection</i>	213
7.2.4 <i>The Log Likelihood Ratio</i>	214
7.3 Markov Sources and Discrete Channels	215
7.4 The BCJR Algorithm: Trellis Coding and Discrete Memoryless Channels	218
7.5 Iterative Coefficient Calculation	221
7.6 The BCJR MAP Algorithm and the LLR	234
7.6.1 <i>The BCJR MAP Algorithm: LLR Calculation</i>	235
7.6.2 <i>Calculation of Coefficients $\gamma_i(u', u)$</i>	236
7.7 Turbo Decoding	239
7.7.1 <i>Initial Conditions of Coefficients $\alpha_{i-1}(u')$ and $\beta_i(u)$</i>	248
7.8 Construction Methods for Turbo Codes	249
7.8.1 <i>Interleavers</i>	249
7.8.2 <i>Block Interleavers</i>	250
7.8.3 <i>Convolutional Interleavers</i>	250
7.8.4 <i>Random Interleavers</i>	251
7.8.5 <i>Linear Interleavers</i>	253
7.8.6 <i>Code Concatenation Methods</i>	253
7.8.7 <i>Turbo Code Performance as a Function of Size and Type of Interleaver</i>	257
7.9 Other Decoding Algorithms for Turbo Codes	257
7.10 EXIT Charts for Turbo Codes	257
7.10.1 <i>Introduction to EXIT Charts</i>	258
7.10.2 <i>Construction of the EXIT Chart</i>	259
7.10.3 <i>Extrinsic Transfer Characteristics of the Constituent Decoders</i>	261

Bibliography and References	269
Problems	271
8 Low-Density Parity Check Codes	277
8.1 Different Systematic Forms of a Block Code	278
8.2 Description of LDPC Codes	279
8.3 Construction of LDPC Codes	280
8.3.1 <i>Regular LDPC Codes</i>	280
8.3.2 <i>Irregular LDPC Codes</i>	281
8.3.3 <i>Decoding of LDPC Codes: The Tanner Graph</i>	281
8.4 The Sum-Product Algorithm	282
8.5 Sum-Product Algorithm for LDPC Codes: An Example	284
8.6 Simplifications of the Sum-Product Algorithm	297
8.7 A Logarithmic LDPC Decoder	302
8.7.1 <i>Initialization</i>	302
8.7.2 <i>Horizontal Step</i>	302
8.7.3 <i>Vertical Step</i>	304
8.7.4 <i>Summary of the Logarithmic Decoding Algorithm</i>	305
8.7.5 <i>Construction of the Look-up Tables</i>	306
8.8 Extrinsic Information Transfer Charts for LDPC Codes	306
8.8.1 <i>Introduction</i>	306
8.8.2 <i>Iterative Decoding of Block Codes</i>	310
8.8.3 <i>EXIT Chart Construction for LDPC Codes</i>	312
8.8.4 <i>Mutual Information Function</i>	312
8.8.5 <i>EXIT Chart for the SND</i>	314
8.8.6 <i>EXIT Chart for the PCND</i>	315
8.9 Fountain and LT Codes	317
8.9.1 <i>Introduction</i>	317
8.9.2 <i>Fountain Codes</i>	318
8.9.3 <i>Linear Random Codes</i>	318
8.9.4 <i>Luby Transform Codes</i>	320
8.10 LDPC and Turbo Codes	322
Bibliography and References	323
Problems	324
Appendix A: Error Probability in the Transmission of Digital Signals	327
Appendix B: Galois Fields $GF(q)$	339
Answers to Problems	351
Index	357