

Steven Roman

# Coding and Information Theory

With 31 Illustrations



Springer

# Contents

*Sections marked with an asterisk are optional.*

<b>Preface</b>	<b>vii</b>
<b>Introduction</b>	<b>1</b>
<b>Part 1 Information Theory</b>	
<b>Chapter 1</b>	
<b>Entropy</b>	<b>11</b>
<b>1.1 Entropy of a Source</b>	<b>11</b>
The Entropy Function $H(p_1, \dots, p_n)$	12
The Units of Entropy	16
The Entropy of a Random Variable; Joint Entropy	18
<b>1.2 Properties of Entropy</b>	<b>22</b>
The Range of the Entropy Function	23
A Grouping Axiom for Entropy	23
Properties of Joint Entropy	23
The Convexity of the Entropy Function	26
Entropy as an Expected Value	28
<b>1.3 Additional Properties of Entropy</b>	<b>30</b>
The Entropy of Countably Infinite Distributions	30
Typical Sequences	33

## Chapter 2

<b>Noiseless Coding</b>	<b>39</b>
<b>2.1 Variable Length Encoding</b>	<b>39</b>
Strings and Codes	39
Average Codeword Length	40
Fixed and Variable Length Codes	41
Unique Decipherability	41
Instantaneous Codes; The Prefix Property	43
Kraft's Theorem	44
McMillan's Theorem	47
<b>2.2 Huffman Encoding</b>	<b>52</b>
An Example of Huffman Encoding	52
Motivation for the General Case	54
The General Case	56
Huffman's Algorithm	59
<b>2.3 The Noiseless Coding Theorem</b>	<b>62</b>
Extensions of a Source	64

## Chapter 3

<b>Noisy Coding</b>	<b>69</b>
<b>3.1 The Discrete Memoryless Channel and Conditional Entropy</b>	<b>69</b>
Discrete Memoryless Channels	69
Conditional Entropy	72
Some Special Channels	76
<b>3.2 Mutual Information and Channel Capacity</b>	<b>81</b>
Mutual Information	81
A Summary of Properties	83
The Capacity of a Channel	84
<b>3.3 The Noisy Coding Theorem</b>	<b>89</b>
The Channel	91
The Decision Scheme	92
The Probability of a Decision Error	93
The Rate of a Code	95
The Noisy Coding Theorem	96
The Weak Converse of the Noisy Coding Theorem	98
The Strong Converse of the Noisy Coding Theorem	101
<b>3.4 Proof of the Noisy Coding Theorem and Its Strong Converse</b>	<b>105</b>
More on the Probability of Error	106
Proof of the Noisy Coding Theorem	107
Proof of the Strong Converse	111

## Part 2 Coding Theory

### Chapter 4

<b>General Remarks on Codes</b>	<b>119</b>
<b>4.1 Error Detection and Correction</b>	<b>119</b>
Block Codes	119
The Channel	119
Burst Errors	122
The Decision Scheme	122
Probabilities Associated with Error Detection	123
Probabilities Associated with Error Correction	123
The Noisy Coding Theorem	126
<b>4.2 Minimum Distance Decoding</b>	<b>129</b>
Minimum Distance Decoding	129
t-Error-Correcting and t-Error-Detecting Codes	131
Using a Code for Simultaneous Error Correction/Detection	132
The Relationship Between Minimum Distance and the Probability of Error	134
The Packing and Covering Radii of a Code	136
Perfect and Quasi-Perfect Codes	138
<b>4.3 Families of Codes</b>	<b>143</b>
Systematic Codes	143
Finite Fields	143
Equivalence of Codes	144
Types of Codes	145
Linear Codes	145
Nonlinear Codes	149
Families of Codes	150
Repetition Codes	150
Hamming Codes	150
Golay Codes	151
Reed-Muller Codes	151
BCH Codes and Reed-Solomon Codes	152
Quadratic Residue Codes	152
Goppa Codes	153
Justesen Codes	154
Perfect Codes	154
Obtaining New Codes from Old Codes	154
Extending a Code	155
Puncturing a Code	155
Expunging a Code	156
Augmenting a Code	156

Shortening a Code	157
The $(u, u+v)$ -Construction	158
The Automorphism Group of a Code	158
• Transitive Permutation Groups	159
<b>4.4 Codes and Designs</b>	<b>163</b>
t-Designs	163
The Intersection Numbers of a t-Design	165
Designs and Codes	167
<b>4.5 The Main Coding Theory Problem</b>	<b>170</b>
Overview	170
Elementary Results	170
A Lower Bound on $A_q(n, d)$	171
Upper Bounds on $A_q(n, d)$	171
Elementary Results	172
Small Values of $A_q(n, d)$	173
A Lower Bound on $A_q(n, d)$	173
Upper Bounds on $A_q(n, d)$	174
The Singleton Bound	174
The Sphere-Packing Bound	175
• The Numbers $A(n, d, w)$	176
• The Johnson Bound	178
The Plotkin Bound	181
• Equality in the Plotkin Bound – Hadamard codes	183
• The Elias Bound	188
<b>Chapter 5</b>	
<b>Linear Codes</b>	<b>197</b>
<b>5.1 Linear Codes and Their Duals</b>	<b>197</b>
The Generator Matrix of a Linear Code	197
The Dual of a Linear Code	199
Syndrome Decoding	202
The Probability of Correct Decoding	205
The Probability of Error Detection	206
Majority Logic Decoding	206
Self-Dual Codes	208
• The Number of Binary Self-Dual Codes	210
Burst Error Detection and Correction	212
<b>5.2 Weight Distributions</b>	<b>216</b>
Characters	216
The Group Algebra	218
The Transform of an Element of the Group Algebra	219
Weight Enumerators and Weight Distributions	220

The Krawtchouk Polynomials	222
Linear Codes	223
Moments of the Weight Distribution	225
• Distance Distributions	226
• The Four Fundamental Parameters of a Code	228
• The Linear Programming Bound	230
<b>5.3 Maximum Distance Separable Codes</b>	<b>235</b>
The Trivial MDS Codes	235
Characterizations of MDS Codes	235
Existence of Nontrivial MDS Codes	237
The Weight Distribution of an MDS Code	239
MDS Codes from Vandermonde Matrices	240
<b>5.4 Invariant Theory and Self-Dual Codes</b>	<b>245</b>
Introduction	245
Invariant Theory	246
The Weight Enumerator of a Self-Dual Code	250
The Weight Enumerator of an Even Self-Dual Code	251

## Chapter 6

<b>Some Linear Codes</b>	<b>253</b>
<b>6.1 Hamming and Golay Codes</b>	<b>253</b>
Hamming Codes	253
Decoding with a Hamming Code	254
A Nonlinear Code with the Hamming Parameters	256
Hamming Codes and Designs	256
Simplex Codes	256
Golay Codes	258
The Binary Golay Code $\mathcal{G}_{24}$	258
Decoding the Binary Golay Code $\mathcal{G}_{24}$	260
The Binary Golay Code $\mathcal{G}_{23}$	262
The Ternary Golay Codes	262
Perfect Codes	263
The Nordstrom-Robinson Code	263
<b>6.2 Reed-Muller Codes</b>	<b>267</b>
Boolean Functions and Boolean Polynomials	267
Boolean Functions	267
Boolean Polynomials	268
The Vector Spaces $\mathcal{B}_m$ and $\mathcal{B}_m$	269
Reed-Muller Codes	270
The Reed-Muller Codes as $(u, u+v)$ -Constructions	272
The Dual of $\mathcal{R}(r, m)$	274
Euclidean Geometry	275
A Geometric Look at the Reed-Muller Codes	276
Decoding the Reed-Muller Codes	278

## Chapter 7

<b>Finite Fields and Cyclic Codes</b>	<b>285</b>
<b>7.1 Basic Properties of Finite Fields</b>	<b>285</b>
A Characterization of Finite Fields	286
The Subfields of a Finite Field	287
The Multiplicative Structure of a Finite Field	288
Describing the Elements of a Finite Field	289
<b>7.2 Irreducible Polynomial over Finite Fields</b>	<b>296</b>
The Splitting Field of an Irreducible Polynomial	296
The Nature of the Roots of an Irreducible Polynomial	297
Computing Minimal Polynomials	299
The Automorphism Group of $F_{q^n}$	300
• Normal Bases	301
• Linearized Polynomials	302
• The Number of Irreducible Polynomials	304
<b>7.3 The Roots of Unity</b>	<b>308</b>
Roots of Unity	308
Primitive Field Elements and Primitive Roots of Unity	309
A Method for Factoring $X^n - 1$	310
The Order of an Irreducible Polynomial	312
Computing the Order of an Irreducible Polynomial	314
The Cyclotomic Polynomials	315
<b>7.4 Cyclic Codes</b>	<b>320</b>
The Generator Polynomial of a Cyclic Code	321
The Check Polynomial of a Cyclic Code	325
The Zeros of a Cyclic Code	327
Hamming Codes as Cyclic Codes	328
The Idempotent Generator of a Cyclic Code	331
Minimal Cyclic Codes	333
Finding Generating Idempotents	335
A Formula for Primitive Idempotents	336
<b>7.5 More on Cyclic Codes</b>	<b>342</b>
Mattson-Solomon Polynomials	342
Encoding with a Cyclic Code	344
A Nonsystematic Method	344
A Systematic Method	344
Decoding with a Cyclic Code	345
Error Trapping	347
Burst Error Detection and Correction with Cyclic Codes	349
Interleaving	349

## Chapter 8

<b>Some Cyclic Codes</b>	<b>353</b>
<b>8.1 BCH Codes</b>	<b>353</b>
The BCH Bound	353
BCH Codes	354
Binary BCH Codes	356
The Automorphisms of Binary BCH Codes	358
The True Minimum Distance of a BCH Code	360
The Quality of BCH Codes	362
Double-Error-Correcting BCH Codes	362
Decoding BCH Codes	363
No Errors	363
Exactly One Error	363
Exactly Two Errors	363
The General Case	365
<b>8.2 Reed-Solomon and Justesen Codes</b>	<b>369</b>
Reed-Solomon Codes	369
Properties of the Reed-Solomon Codes	370
The Reed-Solomon Codes are MDS Codes	370
The Dual of a Reed-Solomon Code	370
Extending a Reed-Solomon Code	371
Obtaining a Binary Code from a $2^m$ -ary Code	372
Burst Error Correction	374
Idempotents of Reed-Solomon Codes	375
Encoding Reed-Solomon Codes	376
Decoding Reed-Solomon Codes	377
Asymptotically Good Codes	379
Finding Good Families of Codes	379
Concatenation of Codes	380
Justesen Codes	381
An Asymptotically Good Family of Justesen Codes	382
<b>8.3 Alternant Codes and Goppa Codes</b>	<b>386</b>
Alternant Codes	386
Goppa Codes	389
The Parameters of $\Gamma(G,L)$	390
Binary Goppa Codes	393
Fast Decoding of Alternant Codes	395
The Euclidean Algorithm	396
Decoding of Alternant Codes – The Initial Setup	398
Decoding of Alternant Codes – The Decoding Step	401
<b>8.4 Quadratic Residue Codes</b>	<b>407</b>
Quadratic Residues	407
Quadratic Residue Codes	409

The Golay Codes as Quadratic Residue Codes	412
The Square Root Bound	412
The Idempotents of a Binary Quadratic Residue Code	414
Duals of the Quadratic Residue Codes	417
The Extended Quadratic Residue Codes	417

## Appendix

<b>Preliminaries</b>	<b>421</b>
<b>A.1 Algebraic Preliminaries</b>	<b>421</b>
Groups	421
Euler's Formula	422
Cyclic Groups	423
Rings and Fields	425
Homomorphisms	425
Ideals	426
Factor Rings	426
The Characteristic of a Ring	427
Extension Fields	428
The Prime Field	429
Simple Extensions	429
The Roots of Polynomials	430
Splitting Fields	430
Polynomials	430
The Division Algorithm and its Consequences	430
The Euclidean Algorithm	431
Irreducible Polynomials	431
Common Roots	432
The Minimal Polynomial	433
Multiple Roots	433
<b>A.2 Möbius Inversion</b>	<b>435</b>
Partially Ordered Sets	435
The Incidence Algebra of a Partially Ordered Set	436
Classical Möbius Inversion	440
Multiplicative Version of Möbius Inversion	441
<b>A.3 Binomial Inequalities</b>	<b>442</b>
Inequalities Involving a Single Binomial Coefficient	443
Inequalities Involving Sums of Binomial Coefficients	445
Bounds on the Volume of a Sphere	446
<b>A.4 More on Finite Fields</b>	<b>449</b>
Computing Minimal Polynomials	449
An Algorithm for Factoring Polynomials	452
Finding Primitive Polynomials	456

<b>Tables</b>	<b>459</b>
Monic Irreducible Polynomials	459
Primitive Polynomials	463
Finite Field Tables	464
Factorization of $x^n - 1$	468
Krawtchouk Polynomials	469
<b>References</b>	<b>475</b>
<b>Symbol Index</b>	<b>479</b>
<b>Index</b>	<b>481</b>