

Student Edition

The Theory of

Information and Coding

Robert McEliece

CAMBRIDGE

Contents

<i>Editor's statement</i>	<i>page</i> viii
<i>Section editor's foreword</i>	ix
<i>Preface to the first edition</i>	x
<i>Preface to the second edition</i>	xii
Introduction	1
Problems	12
Notes	13
Part one: Information theory	
1 Entropy and mutual information	17
1.1 Discrete random variables	17
1.2 Discrete random vectors	33
1.3 Nondiscrete random variables and vectors	37
Problems	44
Notes	49
2 Discrete memoryless channels and their capacity–cost functions	50
2.1 The capacity–cost function	50
2.2 The channel coding theorem	58
Problems	68
Notes	73
3 Discrete memoryless sources and their rate-distortion functions	75
3.1 The rate-distortion function	75
3.2 The source coding theorem	84
Problems	91
Notes	93

4	The Gaussian channel and source	95
4.1	The Gaussian channel	95
4.2	The Gaussian source	99
	Problems	105
	Notes	110
5	The source–channel coding theorem	112
	Problems	120
	Notes	122
6	Survey of advanced topics for part one	123
6.1	Introduction	123
6.2	The channel coding theorem	123
6.3	The source coding theorem	131
Part two: Coding theory		
7	Linear codes	139
7.1	Introduction: The generator and parity-check matrices	139
7.2	Syndrome decoding on q -ary symmetric channels	143
7.3	Hamming geometry and code performance	146
7.4	Hamming codes	148
7.5	Syndrome decoding on general q -ary channels	149
7.6	Weight enumerators and the MacWilliams identities	153
	Problems	158
	Notes	165
8	Cyclic codes	167
8.1	Introduction	167
8.2	Shift-register encoders for cyclic codes	181
8.3	Cyclic Hamming codes	195
8.4	Burst-error correction	199
8.5	Decoding burst-error correcting cyclic codes	215
	Problems	220
	Notes	228
9	BCH, Reed–Solomon, and related codes	230
9.1	Introduction	230
9.2	BCH codes as cyclic codes	234
9.3	Decoding BCH codes, Part one: the key equation	236
9.4	Euclid’s algorithm for polynomials	244
9.5	Decoding BCH codes, Part two: the algorithms	249
9.6	Reed–Solomon codes	253
9.7	Decoding when erasures are present	266

9.8	The (23,12) Golay code	277
	Problems	282
	Notes	292
10	Convolutional codes	293
10.1	Introduction	293
10.2	State diagrams, trellises, and Viterbi decoding	300
10.3	Path enumerators and error bounds	307
10.4	Sequential decoding	313
	Problems	322
	Notes	329
11	Variable-length source coding	330
11.1	Introduction	330
11.2	Uniquely decodable variable-length codes	331
11.3	Matching codes to sources	334
11.4	The construction of optimal UD codes (Huffman's algorithm)	337
	Problems	342
	Notes	345
12	Survey of advanced topics for Part two	347
12.1	Introduction	347
12.2	Block codes	347
12.3	Convolutional codes	357
12.4	A comparison of block and convolutional codes	359
12.5	Source codes	363
<i>Appendices</i>		
A	Probability theory	366
B	Convex functions and Jensen's inequality	370
C	Finite fields	375
D	Path enumeration in directed graphs	380
<i>References</i>		
1	General reference textbooks	384
2	An annotated bibliography of the theory of information and coding	384
3	Original papers cited in the text	386
<i>Index of Theorems</i>		388
<i>Index</i>		390