

Contents

Preface	v
1. Coding and its uses	1
1.1 Messages	1
1.2 Coding	3
1.3 Basic definitions	4
1.4 Coding for economy	7
1.5 Coding for reliability	8
1.6 Coding for security	9
2. Prefix-free codes	13
2.1 The decoding problem	13
2.2 Representing codes by trees	16
2.3 The Kraft-McMillan number	18
2.4 Unique decodability implies $K \leq 1$	21
2.5 Proof of the Counting Principle	24
3. Economical coding	27
3.1 The concept of a source	27
3.2 The optimization problem	30
3.3 Entropy	32
3.4 Entropy, uncertainty, and information	34
3.5 Optimal codes – the fundamental theorems	38
3.6 Huffman’s rule	40
3.7 Optimality of Huffman codes	44

4. Data compression	47
4.1 Coding in blocks	47
4.2 Distributions on product sets	49
4.3 Stationary sources	52
4.4 Coding a stationary source	55
4.5 Algorithms for data compression	58
4.6 Using numbers as codewords	59
4.7 Arithmetic coding	62
4.8 The properties of arithmetic coding	65
4.9 Coding with a dynamic dictionary	67
5. Noisy channels	73
5.1 The definition of a channel	73
5.2 Transmitting a source through a channel	76
5.3 Conditional entropy	78
5.4 The capacity of a channel	81
5.5 Calculating the capacity of a channel	83
6. The problem of reliable communication	89
6.1 Communication using a noisy channel	89
6.2 The extended BSC	94
6.3 Decision rules	96
6.4 Error correction	100
6.5 The packing bound	102
7. The noisy coding theorems	107
7.1 The probability of a mistake	107
7.2 Coding at a given rate	111
7.3 Transmission using the extended BSC	113
7.4 The rate should not exceed the capacity	117
7.5 Shannon's theorem	119
7.6 Proof of Fano's inequality	120
8. Linear codes	123
8.1 Introduction to linear codes	123
8.2 Construction of linear codes using matrices	126
8.3 The check matrix of a linear code	128
8.4 Constructing 1-error-correcting codes	131
8.5 The decoding problem	135

9. Algebraic coding theory	141
9.1 Hamming codes	141
9.2 Cyclic codes	145
9.3 Classification and properties of cyclic codes	149
9.4 Codes that can correct more than one error	153
9.5 Definition of a family of BCH codes	155
9.6 Properties of the BCH codes	158
10. Coding natural languages	163
10.1 Natural languages as sources	163
10.2 The uncertainty of english	165
10.3 Redundancy and meaning	168
10.4 Introduction to cryptography	170
10.5 Frequency analysis	174
11. The development of cryptography	179
11.1 Symmetric key cryptosystems	179
11.2 Poly-alphabetic encryption	180
11.3 The Playfair system	183
11.4 Mathematical algorithms in cryptography	185
11.5 Methods of attack	187
12. Cryptography in theory and practice	191
12.1 Encryption in terms of a channel	191
12.2 Perfect secrecy	195
12.3 The one-time pad	197
12.4 Iterative methods	198
12.5 Encryption standards	201
12.6 The key distribution problem	203
13. The RSA cryptosystem	207
13.1 A new approach to cryptography	207
13.2 Outline of the RSA system	209
13.3 Feasibility of RSA	212
13.4 Correctness of RSA	215
13.5 Confidentiality of RSA	217
14. Cryptography and calculation	221
14.1 The scope of cryptography	221
14.2 Hashing	222
14.3 Calculations in the field \mathbb{F}_p	224
14.4 The discrete logarithm	226

14.5	The ElGamal cryptosystem	228
14.6	The Diffie-Hellman key distribution system	230
14.7	Signature schemes	232
15.	Elliptic curve cryptography	237
15.1	Calculations in finite groups	237
15.2	The general ElGamal cryptosystem	239
15.3	Elliptic curves.....	241
15.4	The group of an elliptic curve	245
15.5	Improving the efficiency of exponentiation	248
15.6	A final word	250
	Answers to odd-numbered exercises	255
	Index	271