

# Contents

<b>Preface</b>	<b>v</b>
----------------	----------

## **Part I: Coding Theory**

<b>1 Introduction to Coding Theory</b>	<b>1</b>
1.1 Introduction . . . . .	1
1.2 Basic assumptions . . . . .	2
1.3 Correcting and detecting error patterns . . . . .	4
1.4 Information rate . . . . .	6
1.5 The effects of error correction and detection . . . . .	7
1.6 Finding the most likely codeword transmitted . . . . .	8
1.7 Some basic algebra . . . . .	10
1.8 Weight and distance . . . . .	11
1.9 Maximum likelihood decoding . . . . .	12
1.10 Reliability of MLD . . . . .	16
1.11 Error-detecting codes . . . . .	18
1.12 Error-correcting codes . . . . .	22
<b>2 Linear Codes</b>	<b>27</b>
2.1 Linear codes . . . . .	27
2.2 Two important subspaces . . . . .	28
2.3 Independence, basis, dimension . . . . .	30
2.4 Matrices . . . . .	35
2.5 Bases for $C = \langle S \rangle$ and $C^\perp$ . . . . .	37
2.6 Generating matrices and encoding . . . . .	41
2.7 Parity-check matrices . . . . .	45
2.8 Equivalent codes . . . . .	48
2.9 Distance of a linear code . . . . .	52
2.10 Cosets . . . . .	53
2.11 MLD for linear codes . . . . .	57
2.12 Reliability of IMLD for linear codes . . . . .	62

<b>3</b>	<b>Perfect and Related Codes</b>	<b>65</b>
3.1	Some bounds for codes . . . . .	65
3.2	Perfect codes . . . . .	70
3.3	Hamming codes . . . . .	72
3.4	Extended codes . . . . .	75
3.5	The extended Golay code . . . . .	77
3.6	Decoding the extended Golay code . . . . .	79
3.7	The Golay code . . . . .	82
3.8	Reed-Muller codes . . . . .	84
3.9	Fast decoding for $RM(1, m)$ . . . . .	88
<b>4</b>	<b>Cyclic Linear Codes</b>	<b>91</b>
4.1	Polynomials and words . . . . .	91
4.2	Introduction to cyclic codes . . . . .	96
4.3	Generating and parity check matrices for cyclic codes . . . . .	101
4.4	Finding cyclic codes . . . . .	104
4.5	Dual cyclic codes . . . . .	109
<b>5</b>	<b>BCH Codes</b>	<b>111</b>
5.1	Finite fields . . . . .	111
5.2	Minimal polynomials . . . . .	115
5.3	Cyclic Hamming codes . . . . .	118
5.4	BCH codes . . . . .	120
5.5	Decoding 2 error-correcting BCH code . . . . .	122
<b>6</b>	<b>Reed-Solomon Codes</b>	<b>127</b>
6.1	Codes over $GF(2^r)$ . . . . .	127
6.2	Reed-Solomon codes . . . . .	129
6.3	Decoding Reed-Solomon codes . . . . .	135
6.4	Transform approach to Reed-Solomon codes . . . . .	141
6.5	Berlekamp-Massey algorithm . . . . .	148
6.6	Erasures . . . . .	153
<b>7</b>	<b>Burst Error-Correcting Codes</b>	<b>159</b>
7.1	Introduction . . . . .	159
7.2	Interleaving . . . . .	163
7.3	Application to compact discs . . . . .	170
<b>8</b>	<b>Convolutional Codes</b>	<b>173</b>
8.1	Shift registers and polynomials . . . . .	173
8.2	Encoding convolutional codes . . . . .	179
8.3	Decoding convolutional codes . . . . .	186
8.4	Truncated Viterbi decoding . . . . .	193

<b>9 Reed-Muller and Preparata Codes</b>	<b>205</b>
9.1 Reed-Muller codes . . . . .	205
9.2 Decoding Reed-Muller codes . . . . .	208
9.3 Extended Preparata codes . . . . .	213
9.4 Encoding extended Preparata codes . . . . .	219
9.5 Decoding extended Preparata codes . . . . .	222

**Part II: Cryptography**

<b>10 Classical Cryptography</b>	<b>227</b>
10.1 Encryption schemes . . . . .	228
10.2 Symmetric-key encryption . . . . .	230
10.3 Feistel ciphers and DES . . . . .	238
10.3.1 The New Data Seal . . . . .	240
10.3.2 The Data Encryption Standard . . . . .	243
10.4 Notes . . . . .	249
<b>11 Topics in Algebra and Number Theory</b>	<b>253</b>
11.1 Algorithms, complexity, and modular arithmetic . . . . .	253
11.2 Quadratic residues . . . . .	260
11.3 Primality testing . . . . .	264
11.4 Factoring and square roots . . . . .	267
11.4.1 Pollard’s rho . . . . .	267
11.4.2 Random squares . . . . .	269
11.4.3 Square roots . . . . .	271
11.5 Discrete logarithms . . . . .	274
11.5.1 Baby-step giant-step . . . . .	274
11.5.2 Index calculus . . . . .	275
11.6 Notes . . . . .	277
<b>12 Public-key Cryptography</b>	<b>279</b>
12.1 One-way and hash functions . . . . .	280
12.2 RSA . . . . .	284
12.3 Provable security . . . . .	290
12.4 ElGamal . . . . .	293
12.5 Cryptographic protocols . . . . .	297
12.5.1 Diffie-Hellman key agreement . . . . .	298
12.5.2 Zero-knowledge proofs . . . . .	299
12.5.3 Coin-tossing and mental poker . . . . .	301
12.6 Notes . . . . .	305
<b>A The Euclidean Algorithm</b>	<b>307</b>

<b>B</b>	<b>Factorization of <math>1 + x^n</math></b>	<b>311</b>
<b>C</b>	<b>Example of Compact Disc Encoding</b>	<b>313</b>
<b>D</b>	<b>Solutions to Selected Exercises</b>	<b>317</b>
	<b>Bibliography</b>	<b>335</b>
	<b>Index</b>	<b>343</b>