

Contents

1	Block Codes for Error Correction	1
1.1	Linear codes and vector spaces	1
1.2	Minimum distance and minimum weight	4
1.3	Syndrome decoding and the Hamming bound	8
1.4	Weight distributions	11
1.5	Problems	14
2	Finite Fields	21
2.1	Fundamental properties of finite fields	21
2.2	Polynomials over finite fields	24
2.2.1	Reed–Solomon codes over $\mathbb{F}_p$	26
2.3	The finite field $\mathbb{F}_{2^m}$	27
2.3.1	Quadratic polynomials over $\mathbb{F}_{2^m}$	29
2.4	Minimal polynomials and factorization of $x^n - 1$	30
2.5	Geometries over finite fields	35
2.5.1	Affine planes	35
2.5.2	Projective planes	36
2.6	Problems	37
3	Communication Channels and Error Probability	41
3.1	Probability and entropy	41
3.1.1	Probability distributions	41
3.1.2	Discrete messages and entropy	42
3.2	Mutual information and capacity of discrete channels	43
3.2.1	Discrete memoryless channels	43
3.2.2	Approximations for long sequences	46
3.3	Error probabilities for specific codes	47
3.3.1	The probability of failure and error for bounded distance decoding	47
3.3.2	Bounds for maximum likelihood decoding of binary block codes	50
3.4	Long codes and channel capacity	53
3.5	Problems	56
4	Reed–Solomon Codes and Their Decoding	61
4.1	Basic definitions	61
4.2	Decoding Reed–Solomon codes	63
4.3	A list decoding algorithm	66

4.4	Another decoding algorithm	69
4.5	Problems	74
5	Cyclic Codes	77
5.1	Introduction to cyclic codes	77
5.2	Generator and parity check matrices of cyclic codes	79
5.3	Cyclic Reed–Solomon codes and BCH codes	80
5.3.1	Cyclic Reed–Solomon codes	81
5.3.2	BCH codes	81
5.4	Cyclic codes from $PG(2, \mathbb{F}_{2^m})$	83
5.5	Problems	87
6	Frames	93
6.1	Definitions of frames and their efficiency	93
6.2	Frame quality	95
6.2.1	Measures of quality	95
6.2.2	Parity checks on frames	96
6.2.3	Header protection codes	97
6.3	Short block codes in frames	97
6.3.1	Reed Solomon codes and long BCH codes	99
6.4	Problems	100
7	Maximum Likelihood Decoding and Convolutional Codes	103
7.1	Definitions of convolutional codes	103
7.2	Codewords and minimum weights	107
7.3	Maximum likelihood decoding	111
7.4	Maximum likelihood decoding of block codes and tail-biting codes	115
7.5	Punctured codes	117
7.6	Correctable error patterns and unit memory codes	118
7.7	Problems	121
8	Combinations of Several Codes	125
8.1	Product codes	125
8.2	Products of Reed–Solomon and binary codes (concatenated codes)	129
8.2.1	Parameters of concatenated codes	129
8.2.2	Inner convolutional codes	131
8.3	Graph codes	133
8.3.1	Graphs and their adjacency matrices	133
8.3.2	Codes on graphs	134
8.3.3	RS codes on planes	136
8.4	Problems	138

9	Decoding Reed–Solomon and BCH Codes	141
9.1	Syndrome calculation	141
9.2	The Euclidean algorithm	144
9.3	Reed–Solomon and BCH decoding with the Euclidian algorithm	146
9.4	Finding the error positions	148
9.5	Calculation of error values	149
9.6	Problems	152
10	Iterative Decoding	153
10.1	Low density parity check codes	153
10.2	Bit flipping	154
10.2.1	Generalized syndromes	155
10.2.2	A bit-flipping algorithm	155
10.2.3	Decoding of projective geometry codes	156
10.3	Decoding by message passing	157
10.4	Decoding product codes by iterated (serial) decoding	162
10.5	Decoding of graph codes	165
10.6	Parallel decoding	166
10.6.1	Message passing in graph codes	166
10.6.2	Parallel encoding and decoding of product codes	167
10.6.3	Parallel encoding and decoding of convolutional codes	168
10.7	Problems	170
11	Algebraic Geometry Codes	173
11.1	Hermitian codes	173
11.2	Decoding Hermitian codes	178
11.3	Problems	180
A	Some Results from Linear Algebra	181
A.1	Vandermonde matrices	181
A.2	A useful theorem	184
B	Communication Channels	185
B.1	Gaussian channels	185
B.2	Gaussian channels with quantized input and output	186
B.3	ML Decoding	187
C	Tables of minimal polynomials	189
D	Solutions to Selected Problems	193
D.1	Solutions to problems in Chapter 1	193
D.2	Solutions to problems in Chapter 2	196
D.3	Solutions to problems in Chapter 3	198
D.4	Solutions to problems in Chapter 4	200

D.5 Solutions to problems in Chapter 5	202
D.6 Solutions to problems in Chapter 6	203
D.7 Solutions to problems in Chapter 7	204
D.8 Solutions to problems in Chapter 8	205
D.9 Solutions to problems in Chapter 9	206
D.10 Solutions to problems in Chapter 10	208
D.11 Solutions to problems in Chapter 11	209
Index	213