

# Contents

<b>Preface</b> . . . . .	ix
<b>1 Block codes for error-correction</b>	
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 . . . . .	13
<b>2 Finite fields</b>	
2.1 Fundamental properties of finite fields . . . . .	19
2.2 The finite field $\mathbb{F}_{2^m}$ . . . . .	22
2.3 Minimal polynomials and factorization of $x^n - 1$ . . . . .	25
2.4 Problems . . . . .	29
<b>3 Bounds on error probability for error-correcting codes</b>	
3.1 Some probability distributions . . . . .	33
3.2 The probability of failure and error for bounded distance decoding . . . . .	34
3.3 Bounds for maximum likelihood decoding of binary block codes . . . . .	37
3.4 Problems . . . . .	39
<b>4 Communication channels and information theory</b>	
4.1 Discrete messages and entropy . . . . .	41
4.2 Mutual information and capacity of discrete channels . . . . .	42
4.2.1 Discrete memoryless channels . . . . .	42
4.2.2 Codes and channel capacity . . . . .	45
4.3 Problems . . . . .	47
<b>5 Reed-Solomon codes and their decoding</b>	
5.1 Basic definitions . . . . .	49
5.2 Decoding Reed-Solomon Codes . . . . .	51
5.3 Vandermonde matrices . . . . .	53
5.4 Another decoding algorithm . . . . .	57
5.5 Problems . . . . .	61

<b>6</b>	<b>Cyclic Codes</b>	
6.1	Introduction to cyclic codes . . . . .	63
6.2	Generator- and parity check matrices of cyclic codes . . . . .	65
6.3	A theorem on the minimum distance of cyclic codes . . . . .	66
6.4	Cyclic Reed-Solomon codes and BCH-codes . . . . .	67
6.4.1	Cyclic Reed-Solomon codes . . . . .	68
6.4.2	BCH-codes . . . . .	68
6.5	Problems . . . . .	70
<b>7</b>	<b>Frames</b>	
7.1	Definitions of frames and their efficiency . . . . .	73
7.2	Frame quality . . . . .	76
7.2.1	Measures of quality . . . . .	76
7.2.2	Parity checks on frames . . . . .	76
7.3	Error detection and error correction . . . . .	77
7.3.1	Short block codes . . . . .	77
7.3.2	Convolutional codes . . . . .	79
7.3.3	Reed-Solomon codes . . . . .	79
7.3.4	Low density codes and ‘turbo’ codes . . . . .	80
7.4	Problems . . . . .	80
<b>8</b>	<b>Convolutional codes</b>	
8.1	Parameters of convolutional codes . . . . .	83
8.2	Tail-biting codes . . . . .	86
8.3	Parity checks and dual codes . . . . .	87
8.4	Distances of convolutional codes . . . . .	89
8.5	Punctured codes . . . . .	90
8.6	Linear systems as encoders . . . . .	91
8.7	Unit memory codes . . . . .	93
8.8	Problems . . . . .	95
<b>9</b>	<b>Maximum likelihood decoding of convolutional codes</b>	
9.1	Finite state descriptions of convolutional codes . . . . .	97
9.2	Maximum likelihood decoding . . . . .	102
9.3	Problems . . . . .	106
<b>10</b>	<b>Combinations of several codes</b>	
10.1	Product codes . . . . .	109
10.2	Concatenated codes (serial encoding) . . . . .	112
10.2.1	Parameters of concatenated codes . . . . .	112
10.2.2	Performance of concatenated codes . . . . .	113
10.2.3	Interleaving and inner convolutional codes . . . . .	114
10.3	Problems . . . . .	116
<b>11</b>	<b>Decoding Reed-Solomon and BCH-codes with the Euclidian algorithm</b>	
11.1	The Euclidian algorithm . . . . .	119

<b>Contents</b>	<b>vii</b>
11.2 Decoding Reed-Solomon and BCH codes . . . . .	121
11.3 Problems . . . . .	125
<b>12 List decoding of Reed-Solomon codes</b>	
12.1 A list decoding algorithm . . . . .	127
12.2 An extended list decoding algorithm . . . . .	130
12.3 Factorization of $Q(x, y)$ . . . . .	132
12.4 Problems . . . . .	135
<b>13 Iterative decoding</b>	
13.1 Low density parity check codes . . . . .	137
13.2 Iterative decoding of LDPC codes . . . . .	138
13.3 Decoding product codes . . . . .	143
13.4 Parallel concatenation of convolutional codes ('turbo codes') . . . . .	145
13.5 Problems . . . . .	149
<b>14 Algebraic geometry codes</b>	
14.1 Hermitian codes . . . . .	151
14.2 Decoding Hermitian codes . . . . .	155
14.3 Problems . . . . .	157
<b>A Communication channels</b>	
A.1 Gaussian channels . . . . .	159
A.2 Gaussian channels with quantized input and output . . . . .	160
A.3 ML Decoding . . . . .	161
<b>B Solutions to selected problems</b>	
B.1 Solutions to problems in Chapter 1 . . . . .	163
B.2 Solutions to problems in Chapter 2 . . . . .	166
B.3 Solutions to problems in Chapter 3 . . . . .	168
B.4 Solutions to problems in Chapter 4 . . . . .	169
B.5 Solutions to problems in Chapter 5 . . . . .	170
B.6 Solutions to problems in Chapter 6 . . . . .	171
B.7 Solutions to problems in Chapter 7 . . . . .	173
B.8 Solutions to problems in Chapter 8 . . . . .	173
B.9 Solutions to problems in Chapter 9 . . . . .	175
B.10 Solutions to problems in Chapter 10 . . . . .	176
B.11 Solutions to problems in Chapter 11 . . . . .	178
B.12 Solutions to problems in Chapter 12 . . . . .	180
B.13 Solutions to problems in Chapter 13 . . . . .	182
B.14 Solutions to problems in Chapter 14 . . . . .	182
<b>C Table of minimal polynomials . . . . .</b>	<b>185</b>
<b>Bibliography . . . . .</b>	<b>187</b>
<b>Index . . . . .</b>	<b>191</b>