

## Contents

---

<i>Preface</i>	<i>page xi</i>
<b>1 Introduction</b>	<b>1</b>
Exercises	4
<b>2 Error detection, correction and decoding</b>	<b>5</b>
2.1 Communication channels	5
2.2 Maximum likelihood decoding	8
2.3 Hamming distance	8
2.4 Nearest neighbour/minimum distance decoding	10
2.5 Distance of a code	11
Exercises	14
<b>3 Finite fields</b>	<b>17</b>
3.1 Fields	17
3.2 Polynomial rings	22
3.3 Structure of finite fields	26
3.4 Minimal polynomials	30
Exercises	36
<b>4 Linear codes</b>	<b>39</b>
4.1 Vector spaces over finite fields	39
4.2 Linear codes	45
4.3 Hamming weight	46
4.4 Bases for linear codes	48
4.5 Generator matrix and parity-check matrix	52
4.6 Equivalence of linear codes	56
4.7 Encoding with a linear code	57
4.8 Decoding of linear codes	59

viii	Contents	
4.8.1	Cosets	59
4.8.2	Nearest neighbour decoding for linear codes	61
4.8.3	Syndrome decoding	62
	Exercises	66
<b>5</b>	<b>Bounds in coding theory</b>	<b>75</b>
5.1	The main coding theory problem	75
5.2	Lower bounds	80
5.2.1	Sphere-covering bound	80
5.2.2	Gilbert–Varshamov bound	82
5.3	Hamming bound and perfect codes	83
5.3.1	Binary Hamming codes	84
5.3.2	$q$ -ary Hamming codes	87
5.3.3	Golay codes	88
5.3.4	Some remarks on perfect codes	92
5.4	Singleton bound and MDS codes	92
5.5	Plotkin bound	95
5.6	Nonlinear codes	96
5.6.1	Hadamard matrix codes	98
5.6.2	Nordstrom–Robinson code	98
5.6.3	Preparata codes	99
5.6.4	Kerdock codes	99
5.7	Griesmer bound	100
5.8	Linear programming bound	102
	Exercises	106
<b>6</b>	<b>Constructions of linear codes</b>	<b>113</b>
6.1	Propagation rules	113
6.2	Reed–Muller codes	118
6.3	Subfield codes	121
	Exercises	126
<b>7</b>	<b>Cyclic codes</b>	<b>133</b>
7.1	Definitions	133
7.2	Generator polynomials	136
7.3	Generator and parity-check matrices	141
7.4	Decoding of cyclic codes	145
7.5	Burst-error-correcting codes	150
	Exercises	153

Contents	ix
<b>8 Some special cyclic codes</b>	<b>159</b>
8.1 BCH codes	159
8.1.1 Definitions	159
8.1.2 Parameters of BCH codes	161
8.1.3 Decoding of BCH codes	168
8.2 Reed–Solomon codes	171
8.3 Quadratic-residue codes	175
Exercises	183
<b>9 Goppa codes</b>	<b>189</b>
9.1 Generalized Reed–Solomon codes	189
9.2 Alternant codes	192
9.3 Goppa codes	196
9.4 Sudan decoding for generalized RS codes	202
9.4.1 Generation of the $(\mathcal{P}, k, t)$ -polynomial	203
9.4.2 Factorization of the $(\mathcal{P}, k, t)$ -polynomial	205
Exercises	209
<i>References</i>	215
<i>Bibliography</i>	217
<i>Index</i>	219