

Contents

Preface	page ix
1 Introduction	1
1.1 Communication systems	1
1.2 Channel coding	3
1.3 Block codes	5
1.4 Decoding	7
1.5 Levels of error handling	11
Problems	17
Notes	22
2 Linear Codes	26
2.1 Definition	26
2.2 Encoding of linear codes	28
2.3 Parity-check matrix	29
2.4 Decoding of linear codes	32
Problems	36
Notes	47
3 Introduction to Finite Fields	50
3.1 Prime fields	50
3.2 Polynomials	51
3.3 Extension fields	56
3.4 Roots of polynomials	59
3.5 Primitive elements	60
3.6 Field characteristic	62
3.7 Splitting field	64
3.8 Application: double error-correcting codes	66
Problems	70
Notes	90

4	Bounds on the Parameters of Codes	93
4.1	The Singleton bound	94
4.2	The sphere-packing bound	95
4.3	The Gilbert–Varshamov bound	97
4.4	MacWilliams’ identities	99
4.5	Asymptotic bounds	104
4.6	Converse Coding Theorem	110
4.7	Coding Theorem	115
	Problems	119
	Notes	136
5	Reed–Solomon and Related Codes	147
5.1	Generalized Reed–Solomon codes	148
5.2	Conventional Reed–Solomon codes	151
5.3	Encoding of RS codes	152
5.4	Concatenated codes	154
5.5	Alternant codes	157
5.6	BCH codes	162
	Problems	163
	Notes	177
6	Decoding of Reed–Solomon Codes	183
6.1	Introduction	183
6.2	Syndrome computation	184
6.3	Key equation of GRS decoding	185
6.4	Solving the key equation by Euclid’s algorithm	191
6.5	Finding the error values	194
6.6	Summary of the GRS decoding algorithm	195
6.7	The Berlekamp–Massey algorithm	197
	Problems	204
	Notes	215
7	Structure of Finite Fields	218
7.1	Minimal polynomials	218
7.2	Enumeration of irreducible polynomials	224
7.3	Isomorphism of finite fields	227
7.4	Primitive polynomials	227
7.5	Cyclotomic cosets	229
	Problems	232
	Notes	240

<i>Contents</i>	vii
8 Cyclic Codes	242
8.1 Definition	242
8.2 Generator polynomial and check polynomial	244
8.3 Roots of a cyclic code	247
8.4 BCH codes as cyclic codes	250
8.5 The BCH bound	253
Problems	256
Notes	265
9 List Decoding of Reed–Solomon Codes	266
9.1 List decoding	267
9.2 Bivariate polynomials	268
9.3 GRS decoding through bivariate polynomials	269
9.4 Sudan’s algorithm	271
9.5 The Guruswami–Sudan algorithm	276
9.6 List decoding of alternant codes	280
9.7 Finding linear bivariate factors	284
9.8 Bounds on the decoding radius	289
Problems	291
Notes	295
10 Codes in the Lee Metric	298
10.1 Lee weight and Lee distance	298
10.2 Newton’s identities	300
10.3 Lee-metric alternant codes and GRS codes	302
10.4 Decoding alternant codes in the Lee metric	306
10.5 Decoding GRS codes in the Lee metric	312
10.6 Berlekamp codes	314
10.7 Bounds for codes in the Lee metric	316
Problems	321
Notes	327
11 MDS Codes	333
11.1 Definition revisited	333
11.2 GRS codes and their extensions	335
11.3 Bounds on the length of linear MDS codes	338
11.4 GRS codes and the MDS conjecture	342
11.5 Uniqueness of certain MDS codes	347
Problems	351
Notes	361

12 Concatenated Codes	365
12.1 Definition revisited	366
12.2 Decoding of concatenated codes	367
12.3 The Zyablov bound	371
12.4 Justesen codes	374
12.5 Concatenated codes that attain capacity	378
Problems	381
Notes	392
13 Graph Codes	395
13.1 Basic concepts from graph theory	396
13.2 Regular graphs	401
13.3 Graph expansion	402
13.4 Expanders from codes	406
13.5 Ramanujan graphs	409
13.6 Codes from expanders	411
13.7 Iterative decoding of graph codes	414
13.8 Graph codes in concatenated schemes	420
Problems	426
Notes	445
14 Trellis and Convolutional Codes	452
14.1 Labeled directed graphs	453
14.2 Trellis codes	460
14.3 Decoding of trellis codes	466
14.4 Linear finite-state machines	471
14.5 Convolutional codes	477
14.6 Encoding of convolutional codes	479
14.7 Decoding of convolutional codes	485
14.8 Non-catastrophic generator matrices	495
Problems	501
Notes	518
Appendix: Basics in Modern Algebra	521
Problems	522
Bibliography	527
List of Symbols	553
Index	559