

Contents

Preface *ix*

1. INTRODUCTION *1*

- 1.1 The Discrete Communication Channel *2*
- 1.2 History of Error-Control Coding *3*
- 1.3 Applications *4*
- 1.4 Elementary Concepts *6*
- 1.5 Elementary Codes *11*
- Problems *14*

2. INTRODUCTION TO ALGEBRA *16*

- 2.1 The Binary Field and the Hexadecimal Field *16*
- 2.2 Groups *20*
- 2.3 Rings *25*
- 2.4 Fields *27*
- 2.5 Vector Spaces *29*
- 2.6 Linear Algebra *34*
- Problems *41*
- Notes *44*

3. LINEAR BLOCK CODES	45
3.1 Structure of Linear Block Codes	46
3.2 Matrix Description of Linear Block Codes	47
3.3 The Standard Array	51
3.4 Hamming Codes	54
3.5 Perfect and Quasi-Perfect Codes	56
3.6 Simple Modifications to a Linear Code	56
3.7 Reed-Muller Codes	58
Problems	62
Notes	64
4. THE ARITHMETIC OF GALOIS FIELDS	65
4.1 The Integer Ring	66
4.2 Finite Fields Based on the Integer Ring	68
4.3 Polynomial Rings	69
4.4 Finite Fields Based on Polynomial Rings	76
4.5 Primitive Elements	80
4.6 The Structure of Finite Fields	84
Problems	90
Notes	92
5. CYCLIC CODES	93
5.1 Viewing a Code from an Extension Field	94
5.2 Polynomial Description of Cyclic Codes	96
5.3 Minimal Polynomials and Conjugates	101
5.4 Matrix Description of Cyclic Codes	107
5.5 Hamming Codes as Cyclic Codes	109
5.6 Cyclic Codes for Correcting Double Errors	112
5.7 Cyclic Codes for Correcting Burst Errors	114
5.8 The Binary Golay Code	119
5.9 Quadratic Residue Codes	123
Problems	128
Notes	129
6. CIRCUITS FOR IMPLEMENTATION OF CYCLIC CODES	130
6.1 Logic Circuits for Finite Field Arithmetic	131
6.2 Digital Filters	133
6.3 Shift-Register Encoders and Decoders	137
6.4 The Meggitt Decoder	140
6.5 Error Trapping	147
6.6 Shortened Cyclic Codes	153
6.7 A Meggitt Decoder for the Golay Code	156
Problems	158
Notes	159

7. BOSE-CHAUDHURI-HOCQUENGHEM CODES	161
7.1 Definition of the Codes	162
7.2 The Peterson-Gorenstein-Zierler Decoder	166
7.3 Reed-Solomon Codes	174
7.4 Synthesis of Autoregressive Filters	176
7.5 Fast Decoding of BCH Codes	183
7.6 Decoding of Binary BCH Codes	191
7.7 Decoding with the Euclidean Algorithm	193
7.8 Nested Codes	198
7.9 Justesen Codes	201
Problems	204
Notes	206

8. CODES BASED ON SPECTRAL TECHNIQUES	207
8.1 Fourier Transforms in a Galois Field	208
8.2 Conjugacy Constraints and Idempotents	211
8.3 Spectral Description of Cyclic Codes	215
8.4 Extended Reed-Solomon Codes	220
8.5 Extended BCH Codes	224
8.6 Alternant Codes	228
8.7 Performance of Alternant Codes	231
8.8 Goppa Codes	233
8.9 Preparata Codes	242
Problems	246
Notes	247

9. ALGORITHMS BASED ON SPECTRAL TECHNIQUES	248
9.1 Spectral Techniques for Decoding	249
9.2 Correction of Erasures and Errors	256
9.3 Decoding of Extended Reed-Solomon Codes	260
9.4 Decoding of Extended BCH Codes	263
9.5 Decoding in the Time Domain	264
9.6 Decoding Beyond the BCH Bound	268
9.7 Decoding of Alternant Codes	272
9.8 Computation of the Finite Field Transforms	275
Problems	280
Notes	281

10. MULTIDIMENSIONAL SPECTRAL TECHNIQUES	282
10.1 Product Codes	283
10.2 The Chinese Remainder Theorems	285
10.3 Decoding of Product Codes	289

10.4	Multidimensional Spectra	294
10.5	Fast BCH Codes	298
10.6	Decoding of Multidimensional Codes	300
10.7	Large Codes in Small Fields	302
	Problems	306
	Notes	306
11.	FAST ALGORITHMS	308
11.1	Linear Convolution and Cyclic Convolution	309
11.2	Fast Convolution Algorithms	311
11.3	Fast Fourier Transforms	317
11.4	Agarwal-Cooley Convolutions	323
11.5	The Winograd Fast Fourier Transform	326
11.6	An Accelerated Berlekamp-Massey Algorithm	331
11.7	A Recursive Berlekamp-Massey Algorithm	336
11.8	Accelerated Decoding of BCH Codes	340
11.9	Convolution in Surrogate Fields	342
	Problems	345
	Notes	345
12.	CONVOLUTIONAL CODES	347
12.1	Tree Codes and Trellis Codes	348
12.2	Polynomial Description of Convolutional Codes	353
12.3	Error Correction and Distance Notions	359
12.4	Matrix Description of Convolutional Codes	361
12.5	Some Simple Convolutional Codes	364
12.6	Syndrome Decoding Algorithms	368
12.7	Convolutional Codes for Correcting Burst Errors	373
12.8	The Viterbi Decoding Algorithm	377
12.9	Trellis Searching Algorithms	382
	Problems	388
	Notes	389
13.	CODES AND ALGORITHMS FOR DECODING WITH MAJORITY LOGIC	391
13.1	Decoding with Majority Logic	392
13.2	Circuits for Majority Decoding	395
13.3	Affine Permutations for Cyclic Codes	399
13.4	Cyclic Codes Based on Permutations	403
13.5	Convolutional Codes for Majority Decoding	407
13.6	Generalized Reed-Muller Codes	410
13.7	Euclidean Geometry Codes	415
13.8	Projective Geometry Codes	424

**14. COMPOSITION AND PERFORMANCE OF
ERROR-CONTROL CODES** 430

14.1 Weight Distributions	431	
14.2 Probabilities of Decoding Error and Decoding Failure		439
14.3 Weight Distributions for Convolutional Codes	442	
14.4 Bounds on Minimum Distance for Block Codes	444	
14.5 Bounds on Minimum Distance for Convolutional Codes		452
Problems	455	
Notes	456	

15. EFFICIENT SIGNALING FOR NOISY CHANNELS 457

15.1 The Bandpass Gaussian Channel	458	
15.2 Bit Energy and Bit Error Rate	461	
15.3 Soft-Decision Decoding of Block Codes	464	
15.4 Soft-Decision Decoding of Convolutional Codes		473
15.5 Sequential Decoding	479	
Problems	481	
Notes	482	

References 483

Index 493