

# Contents

1.1. Ternary Codes . . . . .	34
1.2. Nonexistence Theorems . . . . .	37
1.3. Comments . . . . .	38
1.4. Problems . . . . .	39
CHAPTER 2	
2.1. Codes over $\mathbb{Z}_2$ . . . . .	40
Quadratic Codes . . . . .	41
Binary Codes Derived from Codes over $\mathbb{Z}_2$ . . . . .	42
Galois Rings over $\mathbb{Z}_2$ . . . . .	43
Cyclic Codes over $\mathbb{Z}_2$ . . . . .	44
Problems . . . . .	45
2.2. Codes over $\mathbb{Z}_3$ . . . . .	46
2.3. Codes over $\mathbb{Z}_4$ . . . . .	47
2.4. Codes over $\mathbb{Z}_{2^m}$ . . . . .	48
2.5. Comments . . . . .	49
2.6. Problems . . . . .	50
CHAPTER 3	
3.1. Linear Codes . . . . .	51
Preface to the Third Edition . . . . .	V
Preface to the Second Edition . . . . .	VII
Preface to the First Edition . . . . .	IX
CHAPTER 4	
4.1. Block Codes . . . . .	1
Definitions . . . . .	1
Combinatorial Properties of Block Codes . . . . .	14
Comments . . . . .	17
Problems . . . . .	19
CHAPTER 5	
5.1. Linear Codes over $\mathbb{Z}_2$ . . . . .	22
Shannon's Theorem . . . . .	22
2.1. Introduction . . . . .	22
2.2. Shannon's Theorem . . . . .	27
2.3. On Coding Gain . . . . .	29
2.4. Comments . . . . .	31
2.5. Problems . . . . .	32
CHAPTER 6	
6.1. Linear Codes over $\mathbb{Z}_3$ . . . . .	33
3.1. Block Codes . . . . .	33
3.2. Linear Codes . . . . .	35
3.3. Hamming Codes . . . . .	38

3.4. Majority Logic Decoding . . . . .	39
3.5. Weight Enumerators . . . . .	40
3.6. The Lee Metric . . . . .	42
3.7. Comments . . . . .	44
3.8. Problems . . . . .	45
<b>CHAPTER 4</b>	
<b>Some Good Codes . . . . .</b>	<b>47</b>
4.1. Hadamard Codes and Generalizations . . . . .	47
4.2. The Binary Golay Code . . . . .	48
4.3. The Ternary Golay Code . . . . .	51
4.4. Constructing Codes from Other Codes . . . . .	51
4.5. Reed–Muller Codes . . . . .	54
4.6. Kerdock Codes . . . . .	60
4.7. Comments . . . . .	61
4.8. Problems . . . . .	62
<b>CHAPTER 5</b>	
<b>Bounds on Codes . . . . .</b>	<b>64</b>
5.1. Introduction: The Gilbert Bound . . . . .	64
5.2. Upper Bounds . . . . .	67
5.3. The Linear Programming Bound . . . . .	74
5.4. Comments . . . . .	78
5.5. Problems . . . . .	79
<b>CHAPTER 6</b>	
<b>Cyclic Codes . . . . .</b>	<b>81</b>
6.1. Definitions . . . . .	81
6.2. Generator Matrix and Check Polynomial . . . . .	83
6.3. Zeros of a Cyclic Code . . . . .	84
6.4. The Idempotent of a Cyclic Code . . . . .	86
6.5. Other Representations of Cyclic Codes . . . . .	89
6.6. BCH Codes . . . . .	91
6.7. Decoding BCH Codes . . . . .	98
6.8. Reed–Solomon Codes . . . . .	99
6.9. Quadratic Residue Codes . . . . .	103
6.10. Binary Cyclic Codes of Length $2n$ ( $n$ odd) . . . . .	106
6.11. Generalized Reed–Muller Codes . . . . .	108
6.12. Comments . . . . .	110
6.13. Problems . . . . .	111
<b>CHAPTER 7</b>	
<b>Perfect Codes and Uniformly Packed Codes . . . . .</b>	<b>112</b>
7.1. Lloyd’s Theorem . . . . .	112
7.2. The Characteristic Polynomial of a Code . . . . .	115

7.3. Uniformly Packed Codes . . . . .	118
7.4. Examples of Uniformly Packed Codes . . . . .	120
7.5. Nonexistence Theorems . . . . .	123
7.6. Comments . . . . .	127
7.7. Problems . . . . .	127
<b>CHAPTER 8</b>	
<b>Codes over <math>\mathbb{Z}_4</math> . . . . .</b>	<b>128</b>
8.1. Quaternary Codes . . . . .	128
8.2. Binary Codes Derived from Codes over $\mathbb{Z}_4$ . . . . .	129
8.3. Galois Rings over $\mathbb{Z}_4$ . . . . .	132
8.4. Cyclic Codes over $\mathbb{Z}_4$ . . . . .	136
8.5. Problems . . . . .	138
<b>CHAPTER 9</b>	
<b>Goppa Codes . . . . .</b>	<b>139</b>
9.1. Motivation . . . . .	139
9.2. Goppa Codes . . . . .	140
9.3. The Minimum Distance of Goppa Codes . . . . .	142
9.4. Asymptotic Behaviour of Goppa Codes . . . . .	143
9.5. Decoding Goppa Codes . . . . .	144
9.6. Generalized BCH Codes . . . . .	145
9.7. Comments . . . . .	146
9.8. Problems . . . . .	147
<b>CHAPTER 10</b>	
<b>Algebraic Geometry Codes . . . . .</b>	<b>148</b>
10.1. Introduction . . . . .	148
10.2. Algebraic Curves . . . . .	149
10.3. Divisors . . . . .	155
10.4. Differentials on a Curve . . . . .	156
10.5. The Riemann–Roch Theorem . . . . .	158
10.6. Codes from Algebraic Curves . . . . .	160
10.7. Some Geometric Codes . . . . .	162
10.8. Improvement of the Gilbert–Varshamov Bound . . . . .	165
10.9. Comments . . . . .	165
10.10. Problems . . . . .	166
<b>CHAPTER 11</b>	
<b>Asymptotically Good Algebraic Codes . . . . .</b>	<b>167</b>
11.1. A Simple Nonconstructive Example . . . . .	167
11.2. Justesen Codes . . . . .	168
11.3. Comments . . . . .	172
11.4. Problems . . . . .	172

<b>CHAPTER 12</b>	<i>Logic Decoding</i>
<b>Arithmetic Codes</b>	173
12.1. AN Codes	173
12.2. The Arithmetic and Modular Weight	175
12.3. Mandelbaum-Barrows Codes	179
12.4. Comments	180
12.5. Problems	180
<b>CHAPTER 13</b>	<i>Generalizations</i>
<b>Convolutional Codes</b>	181
13.1. Introduction	181
13.2. Decoding of Convolutional Codes	185
13.3. An Analog of the Gilbert Bound for Some Convolutional Codes	187
13.4. Construction of Convolutional Codes from Cyclic Block Codes	188
13.5. Automorphisms of Convolutional Codes	191
13.6. Comments	193
13.7. Problems	194
<b>Hints and Solutions to Problems</b>	195
<b>References</b>	218
<b>Index</b>	223

**CHAPTER 6***Cyclic Codes*

8-1 Definitions

8-2 Generator Matrix and Check Polynomial

8-3 Zeros of a Cyclic Code

8-4 The Identifying of a Cyclic Code

8-5 Cyclic Representations of Cyclic Codes

8-6 BCH Codes

8-7 Decoding BCH Codes

8-8 Reed-Solomon Codes

8-9 Quadratic Residue Codes

8-10 Binary Cyclic Codes of Length  $2^m$  (odd  $m$ )

8-11 Generalized Reed-Muller Codes

8-12 Comments

8-13 Problems

**CHAPTER 7***Perfect Codes and Uniformly Packed Codes*

7-1 Perfect Codes

7-2 Lloyd's Method

7-3 The Characteristics Properties of Perfect Codes

7-4 Problems

**CHAPTER 8***Asymptotically Good V-Bespice Codes*

8-1 Asymptotic Codes

8-2 A Simple Asymptotic Example

8-3 Column Properties

8-4 The Characteristics Properties of Asymptotic Codes

8-5 Problems