

# Contents

<b>CHAPTER 1</b>	
<b>Mathematical Background</b>	<b>1</b>
1.1. Algebra	1
1.2. Krawtchouk Polynomials	14
1.3. Combinatorial Theory	17
1.4. Probability Theory	19
<b>CHAPTER 2</b>	
<b>Shannon's Theorem</b>	<b>22</b>
2.1. Introduction	22
2.2. Shannon's Theorem	26
2.3. Comments	29
2.4. Problems	29
<b>CHAPTER 3</b>	
<b>Linear Codes</b>	<b>31</b>
3.1. Block Codes	31
3.2. Linear Codes	33
3.3. Hamming Codes	36
3.4. Majority Logic Decoding	37
3.5. Weight Enumerators	38
3.6. Comments	40
3.7. Problems	40

<b>CHAPTER 4</b>	
<b>Some Good Codes</b>	<b>42</b>
4.1. Hadamard Codes and Generalizations	42
4.2. The Binary Golay Code	43
4.3. The Ternary Golay Code	44
4.4. Constructing Codes from Other Codes	45
4.5. Reed–Muller Codes	47
4.6. Comments	52
4.7. Problems	52
<b>CHAPTER 5</b>	
<b>Bounds on Codes</b>	<b>54</b>
5.1. Introduction; The Gilbert Bound	54
5.2. Upper Bounds	57
5.3. The Linear Programming Bound	64
5.4. Comments	68
5.5. Problems	69
<b>CHAPTER 6</b>	
<b>Cyclic Codes</b>	<b>70</b>
6.1. Definitions	70
6.2. Generator Matrix and Check Polynomial	72
6.3. Zeros of a Cyclic Code	73
6.4. The Idempotent of a Cyclic Code	74
6.5. Other Representations of Cyclic Codes	77
6.6. BCH Codes	80
6.7. Decoding BCH Codes	84
6.8. Reed–Solomon Codes	85
6.9. Quadratic Residue Codes	86
6.10. Comments	89
6.11. Problems	89
<b>CHAPTER 7</b>	
<b>Perfect Codes and Uniformly Packed Codes</b>	<b>91</b>
7.1. Lloyd’s Theorem	91
7.2. The Characteristic Polynomial of a Code	94
7.3. Uniformly Packed Codes	97
7.4. Examples of Uniformly Packed Codes	100
7.5. Nonexistence Theorems	102
7.6. Comments	105
7.7. Problems	106

<b>CHAPTER 8</b>	
<b>Goppa Codes</b>	107
8.1. Motivation	107
8.2. Goppa Codes	108
8.3. The Minimum Distance of Goppa Codes	109
8.4. Asymptotic Behaviour of Goppa Codes	110
8.5. Decoding Goppa Codes	111
8.6. Generalized BCH Codes	112
8.7. Comments	114
8.8. Problems	115
<b>CHAPTER 9</b>	
<b>Asymptotically Good Algebraic Codes</b>	116
9.1. A Simple Nonconstructive Example	116
9.2. Justesen Codes	117
9.3. Comments	120
9.4. Problems	121
<b>CHAPTER 10</b>	
<b>Arithmetic Codes</b>	122
10.1. AN Codes	122
10.2. The Arithmetic and Modular Weight	124
10.3. Mandelbaum–Barrows Codes	128
10.4. Comments	129
10.5. Problems	129
<b>CHAPTER 11</b>	
<b>Convolutional Codes</b>	130
11.1. Introduction	130
11.2. Decoding of Convolutional Codes	134
11.3. An Analog of the Gilbert Bound for Some Convolutional Codes	136
11.4. Construction of Convolutional Codes from Cyclic Block Codes	137
11.5. Automorphisms of Convolutional Codes	140
11.6. Comments	142
11.7. Problems	143
<b>Hints and Solutions to Problems</b>	144
<b>References</b>	163
<b>Index</b>	167