ERROR CONTROL CODING

From Theory to Practice

Peter Sweeney
University of Surrey, Guildford, UK

JOHN WILEY & SONS, LTD

Contents

1 The Principles of Coding in Digital Communications 1

1.1 Error Control Schemes 1
1.2 Elements of Digital Communication Systems 2
1.3 Source Encoding 2
1.4 Error Control Coding 3
1.5 Modulation 5
1.6 The Channel 7
1.7 Demodulation 8
1.7.1 Coherent demodulation 8
1.7.2 Differential demodulation 9
1.7.3 Soft-decision demodulation 10
1.8 Decoding 11
1.8.1 Encoding and decoding example 12
1.8.2 Soft-decision decoding 14
1.8.3 Alternative decoding approaches 15
1.9 Code Performance and Coding Gain 16
1.10 Information Theory Limits to Code Performance 18
1.11 Coding for Multilevel Modulations 21
1.12 Coding for Burst-Error Channels 22
1.13 Multistage Coding 24
1.14 Error Detection Based Methods 24
1.14.1 ARQ strategies 24
1.14.2 Error concealment 26
1.14.3 Error detection and correction capability of block codes 26
1.15 Selection of Coding Scheme 27
1.15.1 General considerations 27
1.15.2 Data structure 28
1.15.3 Information type 29
1.15.4 Data rate 29
1.15.5 Real time data processing 30
1.15.6 Power and bandwidth constraints 30

1.15.7 Channel error mechanisms 31
1.15.8 Cost 31
1.16 Conclusion 32
1.17 Exercises 33
1.18 References 34

2 Convolutional Codes 35
2.1 Introduction 35
2.2 General Properties of Convolutional Codes 35
2.3 Generator Polynomials 36
2.4 Terminology 37
2.5 Encoder State Diagram 38
2.6 Distance Structure of Convolutional Codes 39
2.7 Evaluating Distance and Weight Structures 39
2.8 Maximum Likelihood Decoding 41
2.9 Viterbi Algorithm 42
2.9.1 General principles 42
2.9.2 Example of viterbi decoding 42
2.9.3 Issues arising 45
2.10 Practical Implementation of Viterbi Decoding 45
2.11 Performance of Convolutional Codes 51
2.12 Good Convolutional Codes 53
2.13 Punctured Convolutional Codes 55
2.14 Applications of Convolutional Codes 56
2.15 Codes for Multilevel Modulations 57
2.16 Sequential Decoding 62
2.17 Conclusion 64
2.18 Exercises 64
2.19 References 66

3 Linear Block Codes 67
3.1 Introduction 67
3.2 Mathematics of Binary Codes 67
3.3 Parity Checks 68
3.4 Systematic Codes 69
3.5 Minimum Hamming Distance of a Linear Block Code 70
3.6 How to Encode – Generator Matrix 70
3.7 Encoding with the Parity Check Matrix 71
3.8 Decoding with the Parity Check Matrix 73
3.9 Decoding by Standard Array 75
3.10 Codec Design for Linear Block Codes 76
3.11 Modifications to Block Codes 78
3.12 Dorsch Algorithm Decoding 81
3.13 Conclusion 83
3.14 Exercises 83
3.15 References 85

4 Cyclic Codes 87
4.1 Introduction 87
4.2 Definition of a Cyclic Code 87
4.3 Example of a Cyclic Code 88
4.4 Polynomial Representation 88
4.5 Encoding by Convolution 89
4.6 Establishing the Cyclic Property 90
4.7 Deducing the Properties of a Cyclic Code 91
4.8 Primitive Polynomials 92
4.9 Systematic Encoding of Cyclic Codes 93
4.10 Syndrome of a Cyclic Code 94
4.11 Implementation of Encoding 94
4.12 Decoding 96
4.13 Decoder Operation 100
4.14 Multiple-Error Correction 100
4.15 Example of Multiple-Error Correction 101
4.16 Shortened Cyclic Codes 103
4.17 Expurgated Cyclic Codes 104
4.18 BCH Codes 106
4.19 Cyclic Codes for Burst-Error Correction 107
4.20 Conclusion 110
4.21 Exercises 110
4.22 References 112

5 Finite Field Arithmetic 113
5.1 Introduction 113
5.2 Definition of a Finite Field 113
5.3 Prime Size Finite Field GF(p) 114
5.4 Extensions to the Binary Field – Finite Field GF(2^m) 115
5.5 Polynomial Representation of Finite Field Elements 117
5.6 Properties of Polynomials and Finite Field Elements 119
5.6.1 Roots of a polynomial 119
5.6.2 Minimum polynomial 120
5.6.3 Order of an element 120
5.6.4 Finite field elements as roots of a polynomial 120
5.6.5 Roots of an irreducible polynomial 120
5.6.6 Factorization of a polynomial 121
5.7 Fourier Transform over a Finite Field 121
5.8 Alternative Visualization of Finite Field Fourier Transform 123
5.9 Roots and Spectral Components 124
5.10 Fast Fourier Transforms 125
5.11 Hardware Multipliers using Polynomial Basis 127
5.12 Hardware Multiplication using Dual Basis 129
5.13 Hardware Multiplication using Normal Basis 131
5.14 Software Implementation of Finite Field Arithmetic 132
5.15 Conclusion 134

5.16 Exercises 135
5.17 References 136

6 BCH Codes 137
6.1 Introduction 137
6.2 Specifying Cyclic Codes by Roots 137
6.3 Definition of a BCH Code 138
6.4 Construction of Binary BCH Codes 138
6.5 Roots and Parity Check Matrices 140
6.6 Algebraic Decoding 143
6.7 BCH Decoding and the BCH Bound 144
6.8 Decoding in the Frequency Domain 146
6.9 Decoding Examples for Binary BCH Codes 147
6.10 Polynomial Form of the Key Equation 149
6.11 Euclid's Method 149
6.12 Berlekamp–Massey Algorithm 151
6.13 Conclusion 152
6.14 Exercises 153
6.15 References 154

7 Reed Solomon Codes 155
7.1 Introduction 155
7.2 Generator Polynomial for a Reed Solomon Code 155
7.3 Time Domain Encoding for Reed Solomon Codes 156
7.4 Decoding Reed Solomon Codes 158
7.5 Reed Solomon Decoding Example 159
7.6 Frequency Domain Encoded Reed Solomon Codes 160
7.7 Further Examples of Reed Solomon Decoding 162
7.8 Erasure Decoding 164
7.9 Example of Erasure Decoding of Reed Solomon Codes 165
7.10 Generalized Minimum Distance Decoding 167
7.11 Welch–Berlekamp Algorithm 168
7.12 Singly Extended Reed Solomon Codes 170
7.13 Doubly Extended Reed Solomon Codes 172
7.14 Conclusion 175
7.15 Exercises 175
7.16 References 176

8 Performance Calculations for Block Codes 177
8.1 Introduction 177
8.2 Hamming Bound 177
8.3 Plotkin Bound 178
8.4 Griesmer Bound 179
8.5 Singleton Bound 180
8.6 Gilbert–Varsharmov Bound 180
8.7 Error Detection 181

8.8 Random-Error Detection Performance of Block Codes 181
8.9 Weight Distributions 182
8.10 Worst Case Undetected Error Rate 184
8.11 Burst-Error Detection 185
8.12 Examples of Error Detection Codes 185
8.13 Output Error Rates using Block Codes 186
8.14 Detected Uncorrectable Errors 188
8.15 Application Example – Optical Communications 190
8.16 Conclusion 192
8.17 Exercises 192

9 Multistage Coding 195
9.1 Introduction 195
9.2 Serial Concatenation 195
9.3 Serial Concatenation using Inner Block Code 196
9.3.1 Maximal length codes 196
9.3.2 Orthogonal codes 197
9.3.3 Reed Muller codes 198
9.3.4 High rate codes with soft-decision decoding 198
9.4 Serial Concatenation using Inner Convolutional Code 199
9.5 Product codes 200
9.6 Generalized Array Codes 203
9.7 Applications of Multistage Coding 206
9.8 Conclusion 208
9.9 Exercises 208
9.10 References 209

10 Iterative Decoding 211
10.1 Introduction 211
10.2 The BCJR Algorithm 211
10.3 BCJR Product Code Example 212
10.4 Use of Extrinsic Information 214
10.5 Recursive Systematic Convolutional Codes 215
10.6 MAP Decoding of RSC Codes 217
10.7 Interleaving and Trellis Termination 220
10.8 The Soft-Output Viterbi Algorithm 222
10.9 Gallager Codes 225
10.10 Serial Concatenation with Iterative Decoding 231
10.11 Performance and Complexity Issues 232
10.12 Application to Mobile Communications 233
10.13 Turbo Trellis-Coded Modulation 233
10.14 Conclusion 235
10.15 Exercises 235
10.16 References 236

Index 239