Contents

Introduction xi

1 Strategic Issues 1
  1.1 Why Code? 1
  1.2 Data Errors 1
    1.2.1 Binary Symmetric Channel 1
    1.2.2 Burst Channel 1
    1.2.3 Binary Erasure Channel 2
  1.3 Software Notes 2

2 Mathematical Tools for Coding 5
  2.1 Modulo Arithmetic 5
    2.1.1 Modulo-2 Arithmetic 6
  2.2 Finite Fields 9
    2.2.1 Groups 9
    2.2.2 Fields 11
  2.3 Introduction to Polynomials 13
  2.4 Extension Fields 16
  2.5 Binary Extension Fields: Manual Construction 20
    2.5.1 Constructing the Field 22
    2.5.2 Representing the Field Elements 24
  2.6 Computer Methods for Galois Fields 26
    2.6.1 Representing Field Elements 27
  2.7 More About Polynomials 30
  2.8 Cyclotomic Cosets 33
  2.9 Finding Minimal Polynomials 36

3 Block and Cyclic Codes 41
  3.1 Introduction 41
  3.2 Linear Block Codes 44
3.2.1 Encoding for Linear Block Codes 44
3.2.2 Constructing the Generator Matrix 47
3.2.3 Parity-Check Matrix 47
3.3 Cyclic Codes 49
3.4 Manual Encoding Methods for Cyclic Codes 51
3.5 Modifications to Cyclic Codes 52
  3.5.1 Extended Codes 53
  3.5.2 Punctured Codes 54
  3.5.3 Expurgated Codes 54
  3.5.4 Augmented Codes 55
  3.5.5 Shortened Codes 56
  3.5.6 Lengthened Codes 56
3.6 Hamming Codes 56
  3.6.1 Shortened Hamming Codes 58

4 BCH and Reed-Solomon Codes 61
  4.1 BCH Codes 61
    4.1.1 Genesis of the Codes 62
    4.1.2 Types of BCH Codes 63
    4.1.3 Critical Features 63
    4.1.4 Constructing the Generator Polynomial 68
    4.1.5 Algorithmic Approach 71
    4.1.6 Computer Approach 73
  4.2 Nonbinary BCH Codes 79
  4.3 Reed-Solomon Codes 82

5 Encoders and Decoders 85
  5.1 Division Method for Encoding Cyclic Codes 85
    5.1.1 Hardware Implementation 85
    5.1.2 Software Implementation 88
  5.2 Standard Array 89
    5.2.1 Hazards in Standard Array Decoding 92
  5.3 Syndromes for BCH Codes 93
  5.4 Peterson-Berlekamp Method 97
  5.5 Error Location 102

6 Convolutional Codes 105
  6.1 Canonical Example 105
    6.1.1 Convolutional Encoder Viewed as a Moore Machine 106
6.1.2 Convolutional Encoder Viewed as a Mealy Machine 106
6.1.3 Moore Machines vs. Mealy Machines 109
6.1.4 Notation and Terminology 112
6.2 Tree Representation of a Convolutional Encoder 116
6.3 Trellis Representation of a Convolutional Encoder 119
6.4 Distance Measures 123

7 Viterbi Decoding 127
  7.1 Introduction to Viterbi Decoding 127
  7.2 Viterbi Decoding Failures 141
    7.2.1 Minimum Free Distance 146
    7.2.2 Weight Distribution 147
    7.2.3 Information Sequence Weight 147
  7.3 Viterbi Decoding with Soft Decisions 147
  7.4 Practical Issues 152
    7.4.1 Decoding Depth 153

8 Sequential Decoding 155
  8.1 Stack Decoding Algorithm 155
    8.1.1 Fano Metric 161
  8.2 Software for Stack Decoding 168
    8.2.1 Implementing the Stack 171
    8.2.2 Received Symbol Buffering 177
    8.2.3 State Table 179
  8.3 Fano Decoding Algorithm 180

Appendices
A Minimal Polynomials of Elements in GF(2^m) for Chapter 2 191
B Stack Tables for Example 8.1 197
C Stack Tables for Example 8.2 207
D Stack Tables for Example 8.3 215
E Software 227
  Index 245
  About the Author 251
  Disk Warranty 260