

Contents

Part I Theoretical Performance of Error-Correcting Codes

| | | |
|----------|---|-----------|
| 1 | Bounds on Error-Correction Coding Performance | 3 |
| 1.1 | Gallager's Coding Theorem | 3 |
| 1.1.1 | Linear Codes with a Binomial Weight Distribution | 7 |
| 1.1.2 | Covering Radius of Codes | 13 |
| 1.1.3 | Usefulness of Bounds | 13 |
| 1.2 | Bounds on the Construction of Error-Correcting Codes | 13 |
| 1.2.1 | Upper Bounds | 15 |
| 1.2.2 | Lower Bounds | 19 |
| 1.2.3 | Lower Bounds from Code Tables | 21 |
| 1.3 | Summary | 21 |
| | References | 22 |
| 2 | Soft and Hard Decision Decoding Performance | 25 |
| 2.1 | Introduction | 25 |
| 2.2 | Hard Decision Performance | 26 |
| 2.2.1 | Complete and Bounded Distance Decoding | 26 |
| 2.2.2 | The Performance of Codes on the Binary Symmetric Channel | 28 |
| 2.3 | Soft Decision Performance | 30 |
| 2.3.1 | Performance Assuming a Binomial Weight Distribution | 35 |
| 2.3.2 | Performance of Self-dual Codes | 39 |
| 2.4 | Summary | 40 |
| | References | 41 |
| 3 | Soft Decision and Quantised Soft Decision Decoding | 43 |
| 3.1 | Introduction | 43 |
| 3.2 | Soft Decision Bounds | 43 |

| | | |
|-----|--|----|
| 3.3 | Examples | 49 |
| 3.4 | A Hard Decision Dorsch Decoder and BCH Codes | 53 |
| 3.5 | Summary | 57 |
| | References | 57 |

Part II Code Construction

| | | |
|----------|--|------------|
| 4 | Cyclotomic Cosets, the Mattson–Solomon Polynomial, Idempotents and Cyclic Codes | 61 |
| 4.1 | Introduction | 61 |
| 4.2 | Cyclotomic Cosets | 61 |
| 4.3 | The Mattson–Solomon Polynomial | 69 |
| 4.4 | Binary Cyclic Codes Derived from Idempotents | 73 |
| 4.4.1 | Non-Primitive Cyclic Codes Derived from Idempotents | 75 |
| 4.5 | Binary Cyclic Codes of Odd Lengths from 129 to 189 | 78 |
| 4.6 | Summary | 78 |
| | References | 99 |
| 5 | Good Binary Linear Codes | 101 |
| 5.1 | Introduction | 101 |
| 5.2 | Algorithms to Compute the Minimum Hamming Distance of Binary Linear Codes | 103 |
| 5.2.1 | The First Approach to Minimum Distance Evaluation. | 103 |
| 5.2.2 | Brouwer’s Algorithm for Linear Codes | 104 |
| 5.2.3 | Zimmermann’s Algorithm for Linear Codes and Some Improvements. | 106 |
| 5.2.4 | Chen’s Algorithm for Cyclic Codes | 107 |
| 5.2.5 | Codeword Enumeration Algorithm | 111 |
| 5.3 | Binary Cyclic Codes of Lengths $129 \leq n \leq 189$ | 114 |
| 5.4 | Some New Binary Cyclic Codes Having Large Minimum Distance. | 115 |
| 5.5 | Constructing New Codes from Existing Ones | 118 |
| 5.5.1 | New Binary Codes from Cyclic Codes of Length 151. | 121 |
| 5.5.2 | New Binary Codes from Cyclic Codes of Length ≥ 199 | 124 |
| 5.6 | Concluding Observations on Producing New Binary Codes. | 124 |
| 5.7 | Summary | 134 |
| | Appendix | 135 |
| | References | 135 |

| | | |
|----------|---|-----|
| 6 | Lagrange Codes | 137 |
| 6.1 | Introduction | 137 |
| 6.2 | Lagrange Interpolation | 137 |
| 6.3 | Lagrange Error-Correcting Codes | 139 |
| 6.4 | Error-Correcting Codes Derived from the Lagrange Coefficients | 142 |
| 6.5 | Goppa Codes | 143 |
| 6.6 | BCH Codes as Goppa Codes | 147 |
| 6.7 | Extended BCH Codes as Goppa Codes | 151 |
| 6.8 | Binary Codes from MDS Codes | 160 |
| 6.9 | Summary | 164 |
| | References | 165 |
| 7 | Reed–Solomon Codes and Binary Transmission | 167 |
| 7.1 | Introduction | 167 |
| 7.2 | Reed–Solomon Codes Used with Binary Transmission-Hard Decisions | 168 |
| 7.3 | Reed–Solomon Codes and Binary Transmission Using Soft Decisions | 171 |
| 7.4 | Summary | 176 |
| | References | 178 |
| 8 | Algebraic Geometry Codes | 181 |
| 8.1 | Introduction | 181 |
| 8.2 | Motivation for Studying AG Codes | 181 |
| 8.2.1 | Bounds Relevant to Algebraic Geometry Codes | 182 |
| 8.3 | Curves and Planes | 186 |
| 8.3.1 | Important Theorems and Concepts | 189 |
| 8.3.2 | Construction of AG Codes | 192 |
| 8.4 | Generalised AG Codes | 195 |
| 8.4.1 | Concept of Places of Higher Degree | 195 |
| 8.4.2 | Generalised Construction | 196 |
| 8.5 | Summary | 202 |
| | References | 202 |
| 9 | Algebraic Quasi Cyclic Codes | 205 |
| 9.1 | Introduction | 205 |
| 9.2 | Background and Notation | 206 |
| 9.2.1 | Description of Double-Circulant Codes | 207 |
| 9.3 | Good Double-Circulant Codes | 209 |
| 9.3.1 | Circulants Based Upon Prime Numbers Congruent to ± 3 Modulo 8 | 209 |
| 9.3.2 | Circulants Based Upon Prime Numbers Congruent to ± 1 Modulo 8: Cyclic Codes | 211 |
| 9.4 | Code Construction | 215 |

| | | |
|-----------|---|------------|
| 9.4.1 | Double-Circulant Codes from Extended Quadratic Residue Codes | 218 |
| 9.4.2 | Pure Double-Circulant Codes for Primes ± 3 Modulo 8 | 220 |
| 9.4.3 | Quadratic Double-Circulant Codes | 222 |
| 9.5 | Evaluation of the Number of Codewords of Given Weight and the Minimum Distance: A More Efficient Approach | 227 |
| 9.6 | Weight Distributions | 230 |
| 9.6.1 | The Number of Codewords of a Given Weight in Quadratic Double-Circulant Codes | 231 |
| 9.6.2 | The Number of Codewords of a Given Weight in Extended Quadratic Residue Codes | 240 |
| 9.7 | Minimum Distance Evaluation: A Probabilistic Approach | 244 |
| 9.8 | Conclusions | 247 |
| 9.9 | Summary | 249 |
| | Appendix | 249 |
| | References | 287 |
| 10 | Historical Convolutional Codes as Tail-Biting Block Codes | 289 |
| 10.1 | Introduction | 289 |
| 10.2 | Convolutional Codes and Circulant Block Codes. | 291 |
| 10.3 | Summary | 297 |
| | References | 298 |
| 11 | Analogue BCH Codes and Direct Reduced Echelon Parity Check Matrix Construction | 299 |
| 11.1 | Introduction | 299 |
| 11.2 | Analogue BCH Codes and DFT Codes | 299 |
| 11.3 | Error-Correction of Bandlimited Data | 304 |
| 11.4 | Analogue BCH Codes Based on Arbitrary Field Elements | 304 |
| 11.5 | Examples | 306 |
| 11.5.1 | Example of Simple (5, 3, 3) Analogue Code. | 306 |
| 11.5.2 | Example of Erasures Correction Using (15, 10, 4) Binary BCH code. | 307 |
| 11.5.3 | Example of (128, 112, 17) Analogue BCH Code and Error-Correction of Audio Data (Music) Subjected to Impulsive Noise | 309 |
| 11.6 | Conclusions and Future Research. | 312 |
| 11.7 | Summary | 313 |
| | References | 314 |

| | |
|---|-----|
| 12 LDPC Codes | 315 |
| 12.1 Background and Notation | 315 |
| 12.1.1 Random Constructions | 318 |
| 12.1.2 Algebraic Constructions | 320 |
| 12.1.3 Non-binary Constructions | 321 |
| 12.2 Algebraic LDPC Codes | 322 |
| 12.2.1 Mattson–Solomon Domain Construction of Binary Cyclic LDPC Codes | 327 |
| 12.2.2 Non-Binary Extension of the Cyclotomic Coset-Based LDPC Codes | 332 |
| 12.3 Irregular LDPC Codes from Progressive Edge-Growth Construction. | 337 |
| 12.4 Quasi-cyclic LDPC Codes and Protographs | 344 |
| 12.4.1 Quasi-cyclic LDPC Codes | 345 |
| 12.4.2 Construction of Quasi-cyclic Codes Using a Protograph | 347 |
| 12.5 Summary | 351 |
| References | 352 |

Part III Analysis and Decoders

| | |
|--|-----|
| 13 An Exhaustive Tree Search for Stopping Sets of LDPC Codes | 357 |
| 13.1 Introduction and Preliminaries | 357 |
| 13.2 An Efficient Tree Search Algorithm | 358 |
| 13.2.1 An Efficient Lower Bound | 359 |
| 13.2.2 Best Next Coordinate Position Selection | 363 |
| 13.3 Results | 364 |
| 13.3.1 WiMax LDPC Codes | 365 |
| 13.4 Conclusions | 365 |
| 13.5 Summary | 365 |
| References | 366 |
| 14 Erasures and Error-Correcting Codes | 367 |
| 14.1 Introduction | 367 |
| 14.2 Derivation of the PDF of Correctable Erasures | 368 |
| 14.2.1 Background and Definitions | 368 |
| 14.2.2 The Correspondence Between Uncorrectable Erasure Patterns and Low-Weight Codewords | 368 |
| 14.3 Probability of Decoder Error | 372 |
| 14.4 Codes Whose Weight Enumerator Coefficients Are Approximately Binomial | 373 |
| 14.5 MDS Shortfall for Examples of Algebraic, LDPC and Turbo Codes | 377 |

| | | |
|-----------------------------|--|------------|
| 14.5.1 | Turbo Codes with Dithered Relative Prime (DRP) | |
| | Interleavers | 386 |
| 14.5.2 | Effects of Weight Spectral Components | 390 |
| 14.6 | Determination of the d_{min} of Any Linear Code | 395 |
| 14.7 | Summary | 396 |
| | References | 397 |
| 15 | The Modified Dorsch Decoder | 399 |
| 15.1 | Introduction | 399 |
| 15.2 | The Incremental Correlation Dorsch Decoder | 400 |
| 15.3 | Number of Codewords that Need to Be Evaluated to Achieve Maximum Likelihood Decoding | 406 |
| 15.4 | Results for Some Powerful Binary Codes | 407 |
| 15.4.1 | The (136, 68, 24) Double-Circulant Code. | 407 |
| 15.4.2 | The (255, 175, 17) Euclidean Geometry (EG) Code. | 412 |
| 15.4.3 | The (513, 467, 12) Extended Binary Goppa Code | 413 |
| 15.4.4 | The (1023, 983, 9) BCH Code. | 414 |
| 15.5 | Extension to Non-binary Codes | 414 |
| 15.5.1 | Results for the (63, 36, 13) $GF(4)$ BCH Code. | 416 |
| 15.6 | Conclusions | 417 |
| 15.7 | Summary | 418 |
| | References | 418 |
| 16 | A Concatenated Error-Correction System Using the $u u + v$ Code Construction | 421 |
| 16.1 | Introduction | 421 |
| 16.2 | Description of the System | 422 |
| 16.3 | Concatenated Coding and Modulation Formats | 430 |
| 16.4 | Summary | 430 |
| | References | 430 |
| Part IV Applications | | |
| 17 | Combined Error Detection and Error-Correction | 435 |
| 17.1 | Analysis of Undetected Error Probability. | 435 |
| 17.2 | Incremental-Redundancy Coding System. | 438 |
| 17.2.1 | Description of the System. | 438 |
| 17.3 | Summary | 449 |
| | References | 450 |
| 18 | Password Correction and Confidential Information Access System | 451 |
| 18.1 | Introduction and Background. | 451 |
| 18.2 | Details of the Password System. | 453 |

| | | |
|-----------|--|------------|
| 18.3 | Summary | 463 |
| | References | 463 |
| 19 | Variations on the McEliece Public Key Cryptosystem | 465 |
| 19.1 | Introduction and Background. | 465 |
| 19.1.1 | Outline of Different Variations of the Encryption System | 465 |
| 19.2 | Details of the Encryption System. | 468 |
| 19.3 | Reducing the Public Key Size | 487 |
| 19.4 | Reducing the Cryptogram Length Without Loss of Security . . . | 498 |
| 19.5 | Security of the Cryptosystem. | 502 |
| 19.5.1 | Probability of a $k \times k$ Random Matrix Being Full Rank | 503 |
| 19.5.2 | Practical Attack Algorithms | 505 |
| 19.6 | Applications. | 506 |
| 19.7 | Summary | 508 |
| | References | 509 |
| 20 | Error-Correcting Codes and Dirty Paper Coding | 511 |
| 20.1 | Introduction and Background. | 511 |
| 20.2 | Description of the System | 511 |
| 20.3 | Summary | 519 |
| | References | 519 |
| | Index | 521 |

Error-Correction Coding and Decoding

Bounds, Codes, Decoders, Analysis and Applications

Tomlinson, M.; Tjhai, C.J.; Ambroze, M.A.; Ahmed, M.;

Jibril, M.

2017, XX, 522 p. 134 illus., 82 illus. in color., Hardcover

ISBN: 978-3-319-51102-3