

# Contents

|          |  |    |
|----------|--|----|
| <b>1</b> | <b>Introduction</b>                                      | 1  |
| 1.1      | Basics of Error-Correcting Codes                         | 1  |
| 1.2      | The Decoding Problem for Error-Correcting Codes          | 4  |
| 1.3      | List Decoding  | 7  |
| 1.3.1    | Definition   | 7  |
| 1.3.2    | Is List Decoding a Useful Relaxation of Unique Decoding? | 8  |
| 1.3.3    | The Challenge of List Decoding                           | 9  |
| 1.3.4    | Early Work on List Decoding                              | 10 |
| 1.4      | Contributions of This Work                               | 10 |
| 1.5      | Background Assumed of the Reader                         | 13 |
| 1.6      | Comparison with Doctoral Thesis Submitted to MIT         | 13 |
| <b>2</b> | <b>Preliminaries and Monograph Structure</b>             | 15 |
| 2.1      | Preliminaries and Definitions                            | 15 |
| 2.1.1    | Basic Definitions for Codes                              | 15 |
| 2.1.2    | Code Families  | 17 |
| 2.1.3    | Linear Codes   | 17 |
| 2.1.4    | Definitions Relating to List Decoding                    | 18 |
| 2.1.5    | Commonly Used Notation                                   | 20 |
| 2.2      | Basic Code Families                                      | 20 |
| 2.2.1    | Reed-Solomon Codes                                       | 20 |
| 2.2.2    | Reed-Muller Codes  | 21 |
| 2.2.3    | Algebraic-Geometric Codes                                | 22 |
| 2.2.4    | Concatenated Codes                                       | 22 |
| 2.2.5    | Number-Theoretic Codes                                   | 23 |
| 2.3      | Detailed Description of Book Chapters                    | 24 |
| 2.3.1    | Combinatorial Results                                    | 24 |
| 2.3.2    | Algorithmic Results                                      | 26 |
| 2.3.3    | Applications   | 28 |
| 2.3.4    | Conclusions  | 29 |
| 2.3.5    | Dependencies Among Chapters                              | 29 |

---

**Part I Combinatorial Bounds**


---

|          |  |    |
|----------|--|----|
| <b>3</b> | <b>Johnson-Type Bounds and Applications to List Decoding .</b> | 33 |
| 3.1      | Introduction . . . . .   | 33 |
| 3.2      | Definitions and Notation . . . . .                             | 34 |
| 3.3      | The Johnson Bound on List Decoding Radius . . . . .            | 35 |
| 3.3.1    | Proof of Theorem 3.1 . . . . .                                 | 37 |
| 3.3.2    | Geometric Lemmas . . . . .                                     | 39 |
| 3.4      | Generalization in Presence of Weights . . . . .                | 41 |
| 3.5      | Notes . . . . .  | 43 |
| <b>4</b> | <b>Limits to List Decodability . . . . .</b>                   | 45 |
| 4.1      | Introduction . . . . .   | 45 |
| 4.2      | Informal Description of Results . . . . .                      | 46 |
| 4.3      | Formal Description of Results . . . . .                        | 47 |
| 4.3.1    | The Result for Non-linear Codes . . . . .                      | 47 |
| 4.3.2    | Definitions . . . . .  | 47 |
| 4.3.3    | Statement of Results . . . . .                                 | 48 |
| 4.4      | Super-constant List Size at Johnson Radius . . . . .           | 50 |
| 4.4.1    | The Basic Construction . . . . .                               | 50 |
| 4.4.2    | Related Constructions . . . . .                                | 55 |
| 4.4.3    | The Technical “Linear-Algebraic” Lemma . . . . .               | 56 |
| 4.5      | Super-polynomial List Size Below Minimum Distance . . . . .    | 60 |
| 4.5.1    | Proof of Theorem 4.10 . . . . .                                | 60 |
| 4.6      | Explicit Constructions with Polynomial-Sized Lists . . . . .   | 62 |
| 4.6.1    | Fourier Analysis and Group Characters . . . . .                | 62 |
| 4.6.2    | Idea Behind the Construction . . . . .                         | 63 |
| 4.6.3    | Proof of Theorem 4.8 . . . . .                                 | 64 |
| 4.6.4    | Proof of Theorem 4.9 . . . . .                                 | 67 |
| 4.6.5    | Proof of Theorem 4.16 . . . . .                                | 68 |
| 4.7      | Super-polynomial List Sizes at the Johnson Bound . . . . .     | 71 |
| 4.7.1    | Proof Idea . . . . .   | 71 |
| 4.7.2    | The Technical Proof . . . . .                                  | 72 |
| 4.7.3    | Unconditional Proof of Tightness of Johnson Bound . . . . .    | 76 |
| 4.8      | Notes and Open Questions . . . . .                             | 76 |
| <b>5</b> | <b>List Decodability Vs. Rate . . . . .</b>                    | 79 |
| 5.1      | Introduction . . . . .   | 79 |
| 5.2      | Definitions . . . . .  | 80 |
| 5.3      | Main Results . . . . .   | 81 |
| 5.3.1    | Basic Lower Bounds . . . . .                                   | 81 |
| 5.3.2    | An Improved Lower Bound for Binary Linear Codes . . . . .      | 85 |
| 5.3.3    | Upper Bounds on the Rate Function . . . . .                    | 88 |
| 5.3.4    | “Optimality” of Theorem 5.8 . . . . .                          | 89 |

|     |                                     |    |
|-----|-------------------------------------|----|
| 5.4 | Prelude to Pseudolinear Codes ..... | 90 |
| 5.5 | Notes .....                         | 91 |

---

## Part II Code Constructions and Algorithms

---

|          |   |            |
|----------|---|------------|
| <b>6</b> | <b>Reed-Solomon and Algebraic-Geometric Codes .....</b>                   | <b>95</b>  |
| 6.1      | Introduction .....  | 95         |
| 6.1.1    | Reed-Solomon Codes .....  | 96         |
| 6.1.2    | Algebraic-Geometric Codes .....   | 97         |
| 6.1.3    | Soft-Decision Decoding Algorithms .....                                   | 98         |
| 6.2      | Reed-Solomon Codes .....  | 98         |
| 6.2.1    | Reformulation of the Problem .....  | 98         |
| 6.2.2    | Informal Description of the Algorithm .....                               | 100        |
| 6.2.3    | Formal Description of the Algorithm .....                                 | 102        |
| 6.2.4    | Correctness of the Algorithm .....  | 103        |
| 6.2.5    | A “Geometric” Example .....   | 105        |
| 6.2.6    | Results for Specific List Sizes .....                                     | 108        |
| 6.2.7    | Runtime of the Algorithm .....  | 111        |
| 6.2.8    | Main Theorems About Reed-Solomon List Decoding ..                         | 113        |
| 6.2.9    | Some Further Consequences .....   | 114        |
| 6.2.10   | Weighted Polynomial Reconstruction and Soft<br>Decoding of RS Codes ..... | 117        |
| 6.3      | Algebraic-Geometric Codes .....   | 121        |
| 6.3.1    | Overview .....  | 121        |
| 6.3.2    | Algebraic-Geometric Codes: Preliminaries .....                            | 122        |
| 6.3.3    | List Decoding Algorithm for Algebraic-Geometric<br>Codes .....            | 126        |
| 6.3.4    | Root Finding over Algebraic Function Fields .....                         | 129        |
| 6.3.5    | An Explicit List Decoding Algorithm .....                                 | 132        |
| 6.3.6    | Analysis of the Algorithm .....   | 134        |
| 6.3.7    | Weighted List Decoding of AG-codes .....                                  | 136        |
| 6.3.8    | Decoding Up to the “ $q$ -ary Johnson Radius” .....                       | 137        |
| 6.3.9    | List Decodability Offered by the Best-Known<br>AG-codes .....             | 138        |
| 6.4      | Concluding Remarks and Open Questions .....                               | 141        |
| 6.5      | Bibliographic Notes .....   | 142        |
| <b>7</b> | <b>A Unified Framework for List Decoding of Algebraic<br/>Codes .....</b> | <b>147</b> |
| 7.1      | Introduction .....  | 147        |
| 7.1.1    | Overview .....  | 148        |
| 7.2      | Preliminaries .....   | 149        |
| 7.3      | Ideal-Based Codes .....   | 151        |
| 7.3.1    | Examples of Ideal-Based Codes .....                                       | 151        |

|          |  |            |
|----------|--|------------|
| 7.4      | Properties of Ideal-Based Codes .....  | 152        |
| 7.4.1    | Axioms and Assumptions .....   | 152        |
| 7.4.2    | Distance Property of Ideal-Based Codes .....                                     | 153        |
| 7.5      | List Decoding Ideal-Based Codes .....  | 153        |
| 7.5.1    | High Level Structure of the Decoding Algorithm .....                             | 154        |
| 7.5.2    | Formal Description of the Decoding Algorithm .....                               | 155        |
| 7.5.3    | Further Assumptions on the Underlying Ring and<br>Ideals .....                   | 156        |
| 7.5.4    | Analysis of the List Decoding Algorithm .....                                    | 156        |
| 7.5.5    | Performance of the List Decoding Algorithm .....                                 | 159        |
| 7.5.6    | Obtaining Algorithms for Reed-Solomon and<br>AG-codes .....                      | 160        |
| 7.6      | Decoding Algorithms for CRT Codes .....  | 161        |
| 7.6.1    | Combinatorial Bounds on List Decoding .....                                      | 162        |
| 7.6.2    | Weighted List Decoding Algorithm .....   | 165        |
| 7.6.3    | Applications to “Interesting” Weight Settings .....                              | 169        |
| 7.7      | GMD Decoding for CRT Codes .....   | 171        |
| 7.8      | Bibliographic Notes .....  | 174        |
| <b>8</b> | <b>List Decoding of Concatenated Codes .....</b>                                 | <b>177</b> |
| 8.1      | Introduction .....   | 177        |
| 8.2      | Context and Motivation of Results .....  | 178        |
| 8.3      | Overview of Results .....  | 179        |
| 8.4      | Decoding Concatenated Codes with Inner Hadamard Code ..                          | 180        |
| 8.4.1    | Reed-Solomon Concatenated with Hadamard Code ...                                 | 184        |
| 8.4.2    | AG-code Concatenated with Hadamard Code .....                                    | 186        |
| 8.4.3    | Consequence for Highly List Decodable Codes .....                                | 187        |
| 8.5      | Decoding a General Concatenated Code with Outer<br>Reed-Solomon or AG-code ..... | 187        |
| 8.5.1    | A Relevant Combinatorial Result .....  | 188        |
| 8.5.2    | The Formal Decoding Algorithm and Its Analysis ...                               | 192        |
| 8.5.3    | Consequence for Highly List Decodable Codes .....                                | 195        |
| 8.6      | Improved Rate Using Tailor-Made Concatenated Code .....                          | 198        |
| 8.6.1    | The Inner Code Construction .....  | 199        |
| 8.6.2    | The Concatenated Code and the Decoding Algorithm .                               | 202        |
| 8.7      | Open Questions .....   | 205        |
| 8.8      | Bibliographic Notes .....  | 206        |
| <b>9</b> | <b>New, Expander-Based List Decodable Codes .....</b>                            | <b>209</b> |
| 9.1      | Introduction .....   | 209        |
| 9.2      | Overview of Results and Techniques .....   | 210        |
| 9.2.1    | Main Results .....   | 210        |
| 9.2.2    | Our Techniques .....   | 213        |
| 9.2.3    | A Useful Definition .....  | 215        |

|           |   |            |
|-----------|---|------------|
| 9.3       | Pseudolinear Codes: Existence Results and Properties . . . . .  | 215        |
| 9.3.1     | Pseudolinear (Code) Families . . . . .  | 216        |
| 9.3.2     | Probabilistic Constructions of Good, List Decodable<br>Pseudolinear Codes . . . . .   | 218        |
| 9.3.3     | Derandomizing Constructions of Pseudolinear Codes . .   | 221        |
| 9.3.4     | Faster Decoding of Pseudolinear Codes over Large<br>Alphabets . . . . .   | 225        |
| 9.4       | The Basic Expander-Based Construction of List Decodable<br>Codes . . . . .  | 227        |
| 9.4.1     | Definition of Required “Expanders” . . . . .  | 228        |
| 9.4.2     | Reduction of List Decoding to List Recoverability<br>Using Dispersers . . . . .   | 228        |
| 9.4.3     | Codes of Rate $\Omega(\varepsilon^2)$ List Decodable to a Fraction<br>( $1 - \varepsilon$ ) of Errors . . . . .                           | 231        |
| 9.4.4     | Better Rate with Sub-exponential Decoding . . . . .   | 234        |
| 9.5       | Constructions with Better Rate Using Multi-concatenated<br>Codes . . . . .  | 235        |
| 9.5.1     | The Basic Multi-concatenated Code . . . . .   | 236        |
| 9.5.2     | Codes of Rate $\Omega(\varepsilon)$ with Sub-exponential List<br>Decoding for a Fraction ( $1 - \varepsilon$ ) of Errors . . . . .        | 239        |
| 9.5.3     | Binary Codes of Rate $\Omega(\varepsilon^3)$ with Sub-exponential<br>List Decoding Up to a Fraction ( $1/2 - \varepsilon$ ) of Errors . . | 242        |
| 9.6       | Improving the Alphabet Size: Juxtaposed Codes . . . . .   | 243        |
| 9.6.1     | Intuition . . . . .   | 244        |
| 9.6.2     | The Actual Construction . . . . .   | 245        |
| 9.7       | Notes . . . . .   | 249        |
| <b>10</b> | <b>List Decoding from Erasures . . . . .</b>  | <b>251</b> |
| 10.1      | Introduction . . . . .  | 251        |
| 10.2      | Overview . . . . .  | 252        |
| 10.3      | Definitions . . . . .   | 253        |
| 10.3.1    | Comment on Combinatorial Vs. Algorithmic Erasure<br>List-Decodability . . . . .   | 254        |
| 10.4      | Relation to Generalized Hamming Weights . . . . .   | 254        |
| 10.5      | Erasure List-Decodability and Minimum Distance . . . . .  | 256        |
| 10.6      | Combinatorial Bounds for Erasure List-Decodability . . . . .  | 257        |
| 10.6.1    | Discussion . . . . .  | 257        |
| 10.6.2    | Lower Bound on $\tilde{R}_L(p)$ . . . . .   | 258        |
| 10.6.3    | Lower Bound on $\tilde{R}_L^{\text{lin}}(p)$ . . . . .  | 259        |
| 10.6.4    | Upper Bound on $\tilde{R}_L(p)$ . . . . .   | 262        |
| 10.6.5    | Improved Upper Bound for $\tilde{R}_L^{\text{lin}}(p)$ . . . . .  | 265        |
| 10.6.6    | Provable Separation Between Erasure List-Decodable<br>Linear and Non-linear Codes . . . . .   | 265        |

|  |     |
|--|-----|
| 10.7 A Good Erasure List-Decodable Binary Code Construction ..           | 265 |
| 10.7.1 Context .....   | 265 |
| 10.7.2 The Formal Result .....   | 266 |
| 10.7.3 Obtaining Near-Linear Encoding and Decoding<br>Times.....         | 268 |
| 10.7.4 The $\varepsilon^2$ “Rate Barrier” for Binary Linear Codes .....  | 270 |
| 10.8 Better Results for Larger Alphabets Using Juxtaposed<br>Codes ..... | 272 |
| 10.8.1 Main Theorem .....  | 272 |
| 10.8.2 Improving the Decoding Time in Theorem 10.22 .....                | 275 |
| 10.9 Concluding Remarks .....  | 276 |
| 10.10 Bibliographic Notes .....  | 277 |

---

### Part III Applications

---

|  |            |
|--|------------|
| <b>11 Linear-Time Codes for Unique Decoding .....</b>  | <b>283</b> |
| 11.1 Context and Introduction .....  | 283        |
| 11.2 Background on Expanders .....   | 284        |
| 11.3 Linear-Time Encodable and Decodable Codes:<br>Construction I .....  | 285        |
| 11.3.1 Codes with Rate $\Omega(\varepsilon^2)$ Decodable Up to a Fraction<br>( $1/2 - \varepsilon$ ) of Errors.....        | 286        |
| 11.3.2 Binary Codes with Rate $\Omega(\varepsilon^4)$ Decodable Up to a<br>Fraction ( $1/4 - \varepsilon$ ) of Errors..... | 288        |
| 11.4 Linear-Time Codes with Near-Optimal Rate .....  | 289        |
| 11.4.1 High-Level View of the Construction .....   | 289        |
| 11.4.2 Linear-Time Codes with Rates Close to 1.....  | 291        |
| 11.4.3 Linear-Time Error-Correcting Codes Meeting the<br>Singleton Bound .....   | 294        |
| 11.5 Linear-Time Encodable Binary Codes Meeting the Zyablov<br>Bound .....   | 297        |
| 11.6 Bibliographic Notes .....   | 298        |
| <b>12 Sample Applications Outside Coding Theory .....</b>  | <b>299</b> |
| 12.1 An Algorithmic Application: Guessing Secrets .....  | 299        |
| 12.1.1 Formal Problem Description .....  | 300        |
| 12.1.2 An Explicit Strategy with $O(\log N)$ Questions .....   | 302        |
| 12.1.3 An Efficient Algorithm to Recover the Secrets .....   | 304        |
| 12.1.4 The Case of More than Two Secrets .....   | 308        |
| 12.1.5 An Efficient “Partial Solution” for the $k$ -Secrets<br>Game .....  | 309        |
| 12.2 Applications to Complexity Theory .....   | 310        |
| 12.2.1 Hardcore Predicates from One-Way Permutations ....  | 311        |
| 12.2.2 Hardness Amplification of Boolean Functions .....   | 313        |

|   |     |
|---|-----|
| 12.2.3 Average-Case Hardness of Permanent .....                             | 315 |
| 12.2.4 Extractors and Pseudorandom Generators .....                         | 315 |
| 12.2.5 Membership Comparable Sets .....                                     | 318 |
| 12.2.6 Inapproximability of NP Witnesses .....                              | 320 |
| 12.3 Applications to Cryptography .....                                     | 324 |
| 12.3.1 Cryptanalysis of Certain Block Ciphers .....                         | 324 |
| 12.3.2 Finding Smooth Integers .....  | 325 |
| 12.3.3 Efficient Traitor Tracing .....                                      | 325 |
| <b>13 Concluding Remarks</b> .....  | 329 |
| 13.1 Summary of Contributions .....   | 329 |
| 13.2 Directions for Future Work .....                                       | 330 |
| 13.2.1 Some Specific Open Questions .....                                   | 330 |
| 13.2.2 Construction of “Capacity-Approaching” List<br>Decodable Codes ..... | 331 |
| <b>A GMD Decoding of Concatenated Codes</b> .....                           | 333 |
| A.1 Proof .....   | 333 |
| <b>References</b> .....   | 337 |
| <b>Index</b> .....  | 349 |

<http://www.springer.com/978-3-540-24051-8>

List Decoding of Error-Correcting Codes

Winning Thesis of the 2002 ACM Doctoral Dissertation  
Competition

Guruswami, V.

2005, XX, 352 p., Softcover

ISBN: 978-3-540-24051-8