CAMBRIDGE

Cambridge University Press
978-0-521-81711-0 — Codes, Cryptology and Curves with Computer Algebra
Ruud Pellikaan , Xin-Wen Wu , Stanislav Bulygin , Relinde Jurrius
Table of Contents
More Information

Contents

Preface *page* xi

1 Error-correcting Codes 1
Ruud Pellikaan and Xin-Wen Wu

1.1 Block Codes 2
1.2 Linear Codes 11
1.3 Parity Checks and Dual Code 18
1.4 Decoding and the Error Probability 27
1.5 Equivalent Codes 39
1.6 Notes 48

2 Code Constructions and Bounds on Codes 49
Ruud Pellikaan and Xin-Wen Wu

2.1 Code Constructions 49
2.2 Bounds on Codes 70
2.3 Asymptotic Bounds 87
2.4 Notes 94

3 Weight Enumeration 96
Relinde Jurrius, Ruud Pellikaan and Xin-Wen Wu

3.1 Weight Enumerator 96
3.2 Extended Weight Enumerator 109
3.3 Generalized Weight Enumerator 125
3.4 Error Probability 135
3.5 Notes 139

4 Cyclic Codes 141
Ruud Pellikaan

4.1 Cyclic Codes 141

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-81711-0 — Codes, Cryptology and Curves with Computer Algebra
Ruud Pellikaan , Xin-Wen Wu , Stanislav Bulygin , Relinde Jurrius
Table of Contents
More Information

4.2 Finite Fields 155
4.3 Defining Zeros 169
4.4 Bounds on the Minimum Distance 173
4.5 Improvements of the BCH Bound 180
4.6 Locator Polynomials and Decoding Cyclic Codes 185
4.7 Notes 199

5 Polynomial Codes 200
Ruud Pellikaan

5.1 RS Codes and their Generalizations 200
5.2 Subfield Subcodes and Trace Codes 215
5.3 Some Families of Polynomial Codes 225
5.4 Reed–Muller Codes 233
5.5 Notes 241

6 Algebraic Decoding 243
Ruud Pellikaan and Xin-Wen Wu

6.1 Decoding by Key Equation 243
6.2 Error-correcting Pairs 253
6.3 List Decoding by Sudan's Algorithm 259
6.4 Notes 275

7 Complexity and Decoding 277
Stanislav Bulygin, Ruud Pellikaan and Xin-Wen Wu

7.1 Complexity 277
7.2 Decoding Complexity 286
7.3 Difficult Problems in Coding Theory 297
7.4 Notes 302

8 Codes and Related Structures 303
Relinde Jurrius and Ruud Pellikaan

8.1 Graphs and Codes 304
8.2 Matroids and Codes 309
8.3 Finite Geometry and Codes 319
8.4 Geometric Lattices and Codes 330
8.5 Characteristic Polynomial 343
8.6 Combinatorics and Codes 361
8.7 Notes 365

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-81711-0 — Codes, Cryptology and Curves with Computer Algebra
Ruud Pellikaan , Xin-Wen Wu , Stanislav Bulygin , Relinde Jurrius
Table of Contents
More Information

9 Cryptology 368
Stanislav Bulygin

9.1 Symmetric Encryption Schemes and Block Ciphers 368
9.2 Stream Ciphers and Linear Feedback Shift Registers 385
9.3 Authentication, Orthogonal Arrays and Codes 392
9.4 Secret Sharing 402
9.5 Asymmetric Encryption Schemes 406
9.6 Encryption Schemes from Error-correcting Codes 417
9.7 Notes 425

10 Gröbner Bases for Coding and Cryptology 430
Stanislav Bulygin

10.1 Polynomial System Solving 431
10.2 Decoding Codes with Gröbner Bases 444
10.3 Algebraic Cryptanalysis 456
10.4 Notes 464

11 Codes on Curves 467
Ruud Pellikaan

11.1 Algebraic Curves 467
11.2 Codes from Algebraic Curves 492
11.3 Order Functions 503
11.4 Evaluation Codes 513
11.5 Notes 522

12 Coding and Cryptology with Computer Algebra 524
Stanislav Bulygin

12.1 SINGULAR 524
12.2 MAGMA 527
12.3 GAP 530
12.4 SAGE 531
12.5 Error-correcting Codes with Computer Algebra 532
12.6 Cryptography with Computer Algebra 553
12.7 Gröbner Bases with Computer Algebra 559

References 565
Index 586

© in this web service Cambridge University Press www.cambridge.org