Gröbner Bases, Coding, and Cryptography
Gröbner Bases, Coding, and Cryptography
In the period February–July 2006 a major research event took place in Linz (Austria): the Special Semester in Gröbner Bases and Related Areas.\(^1\) Organized by RI-CAM (in close cooperation with RISC) and funded by the Austrian Academy of Sciences, it saw the involvement of hundreds of people working in Gröbner bases theory and their applications. In particular, a workshop (D1\(^2\)) was held, co-chaired by Mikhail Klin (algebraic combinatorics), Ludovic Perret (cryptography) and me (coding theory). The aim of the workshop was twofold: to present possible applications of the theory to experts in Gröbner bases (so that they could explore new research fields) and to present Gröbner bases as an attractive tool to people working in other areas. Therefore, the invited talks were mainly tutorials and surveys, while posters and contributed talks outlined specific research results.

Workshop D1 was a success, with a large audience coming from different backgrounds. It was suggested that some\(^3\) of the best D1 presentations related to cryptography and codes would be collected in a book of the RISC Book Series. The invited talks would become book *chapters*. The posters and contributed talks would become short *notes* at the end of the book. I was appointed Managing Editor, with an Editorial Board composed of Teo Mora (Gröbner bases related papers), Ludovic Perret (cryptography), Shojiro Sakata (AG codes) and Carlo Traverso (Gröbner bases and coding). To cover some interesting aspects not presented at Workshop D1, we invited a few more papers and notes.

I would like to thank all of them for their great help and assistance in planning, shaping and editing this book. The Board and I would like to express our gratefulness for their supervision to Bruno Buchberger and the series editor Peter Paule.

\(^1\)http://www.ricam.oeaw.ac.at/specsem/srs/groeb/index.htm.
\(^2\)“Gröbner Bases in Cryptography, Coding Theory, and Algebraic Combinatorics”.
\(^3\)Other D1 presentations will appear in a special issue of Journal of Symbolic Computation, edited by D. Augot, J.-C. Faugère and L. Perret.

M. Sala
Univ. of Trento, Trento, Italy
e-mail: sala@science.unitn.it
Contents

Gröbner Bases, Coding, and Cryptography: a Guide to the State-of-Art ........................................ 1
Massimiliano Sala
1 In the Beginning ........................................ 1
2 Until Now .............................................. 2
   2.1 Classical Coding Theory .......................... 3
   2.2 AG Codes .......................................... 4
   2.3 Coding Miscellanea ............................... 4
   2.4 Cryptography ...................................... 5
3 Final Comments ....................................... 6
References .............................................. 6

Part 1 Invited Papers

Gröbner Technology ..................................... 11
Teo Mora
1 Notation and Definitions ............................. 11
2 Term-Orderings: Classification and Representation ..... 16
3 Buchberger’s Theorem and Algorithm ................. 19
   References .......................................... 24

The FGLM Problem and Möller’s Algorithm on Zero-dimensional Ideals ...................................... 27
Teo Mora
1 Duality ................................................. 27
2 Möller’s Algorithm ..................................... 28
3 The FGLM Problem .................................... 33
4 The FGLM Matrix ..................................... 33
5 Pointers ............................................... 35
6 Point Evaluation ....................................... 38
   6.1 Möller’s Algorithm ............................... 38
   6.2 Cerlienco–Mureddu Correspondence ............... 38
   6.3 Farr–Gao Analysis .................................. 39
   6.4 Points with Multiplicities ......................... 42
   References .......................................... 43
An Introduction to Linear and Cyclic Codes ........................................ 47
Daniel Augot, Emanuele Betti and Emmanuela Orsini
1 An Overview on Error Correcting Codes ........................................ 47
2 Linear Codes ................................................................................. 48
   2.1 Basic Definitions ..................................................................... 48
   2.2 Hamming Distance .................................................................. 49
   2.3 Decoding Linear Codes .......................................................... 52
3 Some Bounds on Codes ................................................................ 54
4 Cyclic Codes ................................................................................ 55
   4.1 An Algebraic Correspondence ................................................ 55
   4.2 Encoding and Decoding with Cyclic Codes ............................. 56
   4.3 Zeros of Cyclic Codes ............................................................. 57
5 Some Examples of Cyclic Codes ..................................................... 58
   5.1 Hamming and Simplex Codes ................................................ 58
   5.2 Quadratic Residue Codes ....................................................... 60
6 BCH Codes .................................................................................. 60
   6.1 On the Optimality of BCH Codes ......................................... 61
7 Decoding BCH Codes ................................................................. 62
8 On the Asymptotic Properties of Cyclic Codes ............................. 66
    References .................................................................................. 67

Decoding Cyclic Codes: the Cooper Philosophy ................................ 69
Teo Mora and Emmanuela Orsini
1 Introduction .................................................................................. 69
2 Decoding Binary BCH Codes ...................................................... 71
3 Gröbner Bases for Cyclic Codes .................................................. 74
   3.1 Decoding Binary Cyclic Codes ............................................. 74
   3.2 Decoding Cyclic Codes over $\mathbb{F}_q$ .................................... 75
   3.3 A New System with the Newton Identities ............................. 76
4 The CRHT Syndrome Variety ....................................................... 77
5 The Gianni–Kalkbrener Shape Theorem ....................................... 78
6 The General Error Locater Polynomial ...................................... 85
7 A Newton-Based Decoder ............................................................ 88
    References .................................................................................. 90

A Tutorial on AG Code Construction from a Gröbner Basis Perspective ......................................................... 93
Douglas A. Leonard
1 Introduction .................................................................................. 93
2 Traditional AG Approach ............................................................ 95
3 Weighted Total-Degree Orders ................................................... 97
4 Hermitian Codes and Affine-Variety Codes ................................. 97
5 Curve Definition .......................................................................... 99
    References .................................................................................. 106
5 Conclusion .................................................. 182
References .................................................. 183

A Tutorial on AG Code Decoding from a Gröbner Basis
Perspective .................................................. 187
Douglas A. Leonard
1 Introduction .............................................. 187
2 Functional Decoding of RS Codes and AG Codes Using Syndromes
   and Error-Locator Ideals ................................ 187
3 Interpolation to Do List Decoding for RS Codes and AG Codes ... 192
References .................................................. 195

FGLM-Like Decoding: from Fitzpatrick’s Approach to Recent
Developments .............................................. 197
Eleonora Guerrini and Anna Rimoldi
1 Introduction .............................................. 197
2 Iterative Computation of Gröbner Basis ....................... 198
3 The Key Equation for Alternant Codes ....................... 201
4 Variations .................................................. 202
5 Some Applications to AG Codes .......................... 203
6 Errors and Erasures for Alternant Codes .................... 204
   6.1 Errors and Erasures .................................. 204
   6.2 Solutions Using Gröbner Bases ..................... 205
7 List Decoding Problem .................................... 207
   7.1 Sudan’s Approach ..................................... 208
   7.2 Improvements on the Interpolation Steps
      for the RS Codes ..................................... 210
   7.3 Method in Sect. 12.2 Applied to List Decoding
      for AG Codes ......................................... 212
   7.4 Hard-Decision List Decoding and List Decoding with Soft
      Information ............................................. 214
8 Conclusions ................................................ 216
References .................................................. 216

An Introduction to Ring-Linear Coding Theory .................. 219
Marcus Greferath
1 Introduction and History .................................. 219
2 Rings and Modules ....................................... 221
   2.1 Some Classes of Rings .............................. 221
3 Weight Functions on Finite Rings and Modules ................ 223
4 Linear and Cyclic Codes ................................ 224
   4.1 Cyclic Linear Codes ................................ 225
5 A Foundational Result: Code Equivalence .................... 225
6 Weight Enumerators and MacWilliams’ Identity ................ 227
7 Code Optimality: Bounds on the Parameters of Codes ........ 230
8 Outlook: the Future of Ring-Linear Coding .................. 233
Gröbner Bases for the Distance Distribution of Systematic Codes ................................ 367
Eleonora Guerrini, Emmanuela Orsini and Ilaria Simonetti

1 Preliminaries ........................................... 367
2 Theoretical Results ................................... 368
3 Numerical Computations .............................. 370
 References ................................................ 371

A Prize Problem in Coding Theory ....................... 373
Jon-Lark Kim
1 Introduction ............................................ 373
2 Related Facts about a Putative Type II \([72, 36, 16]\) Code ...................... 374
3 Future Work .......................................... 375
4 Monetary Prizes ........................................ 376
 References ................................................ 376

An Application of Möller’s Algorithm to Coding Theory ........................................ 379
M. Borges-Quintana, M.A. Borges-Trenard and E. Martínez-Moro
1 Introduction ............................................ 379
2 An Ideal Associated with a Linear Code ........... 379
  2.1 A Second Way of Getting the Data for 1 ......... 380
3 Examples .............................................. 381
  3.1 Working out with a Gröbner Representation .... 381
  3.2 Combinatorial Properties of a Binary Code ... 382
  3.3 Example: the Golay Code ......................... 383
  3.4 GAP Computing Section ......................... 383
 References .............................................. 384

Mattson Solomon Transform and Algebra Codes ............................................. 385
Edgar Martínez-Moro and Diego Ruano
Introduction ............................................. 385
1 Mattson–Solomon Transform ......................... 386
2 Generator Theory ...................................... 386
3 A Note on the Syndrome Variety ..................... 388
 References .............................................. 388

Decoding Folded Reed–Solomon Codes Using Hensel-Lifting .............................. 389
Peter Beelen and Kristian Brander
1 Introduction ............................................ 389
2 Folded Reed–Solomon Codes ........................ 390
3 Decoding of Folded Reed–Solomon Codes .......... 390
 References .............................................. 393

A Note on the Generalisation of the Guruswami–Sudan List Decoding Algorithm to Reed–Muller Codes .......................................................... 395
Daniel Augot and Michael Stepanov
1 Definitions and Notation .............................. 395
Radical Computation for Small Characteristics ................................. 427
   Ryutaroh Matsumoto
   1 Introduction ......................................................... 427
   2 Another Radical Computation Method for Positive Characteristic .............................................. 428
   3 Comparison of Computational Time and Discussion .................................................. 428
   References ............................................................. 430