

# Contents

<b>Gröbner Bases, Coding, and Cryptography: a Guide to the State-of-Art</b> . . . . .	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
<b>Part 1 Invited Papers</b>	
<b>Gröbner Technology</b> . . . . .	11
Teo Mora	
1 Notation and Definitions . . . . .	11
2 Term-Orderings: Classification and Representation . . . . .	16
3 Buchberger's Theorem and Algorithm . . . . .	19
References . . . . .	24
<b>The FGLM Problem and Möller's Algorithm on Zero-dimensional Ideals</b> . . . . .	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

<b>An Introduction to Linear and Cyclic Codes</b> . . . . .	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
<b>Decoding Cyclic Codes: the Cooper Philosophy</b> . . . . .	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 $F_q$ . . . . .	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 Locator Polynomial . . . . .	85
7 A Newton-Based Decoder . . . . .	88
References . . . . .	90
<b>A Tutorial on AG Code Construction from a Gröbner Basis</b>	
<b>Perspective</b> . . . . .	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

- Automorphisms and Encoding of AG and Order Domain Codes . . . . . 107**
  - John B. Little
  - 1 Introduction . . . . . 107
  - 2 Other Encoding Methods for AG Goppa Codes . . . . . 108
  - 3 Automorphisms and Module Structures . . . . . 109
  - 4 A Systematic Encoding Algorithm . . . . . 110
  - 5 Complexity Comparisons . . . . . 112
  - 6 Automorphisms of Curves and AG Goppa Codes . . . . . 112
  - 7 Examples . . . . . 114
  - References . . . . . 119
  
- Algebraic Geometry Codes from Order Domains . . . . . 121**
  - Olav Geil
  - 1 Introduction . . . . . 121
  - 2 Order Domains with Weight Functions . . . . . 122
  - 3 Codes from Order Domains . . . . . 125
  - 4 One-Point Geometric Goppa Codes . . . . . 132
  - 5 Gröbner Basis Theoretical Tools for the Construction of Order Domains . . . . . 133
  - 6 Gröbner Basis Theoretical Tools for the Code Construction . . . . . 137
  - 7 The Connection to Valuation Theory . . . . . 140
  - References . . . . . 140
  
- The BMS Algorithm . . . . . 143**
  - Shojiro Sakata
  - 1 Introduction . . . . . 143
  - 2 Generating Arrays . . . . . 146
  - 3 BMS Algorithm . . . . . 148
  - 4 Variations . . . . . 154
    - 4.1 Multiarray BMS Algorithm . . . . . 157
    - 4.2 Vectorial BMS Algorithm . . . . . 158
    - 4.3 Non-Homogeneous BMS Algorithm . . . . . 160
    - 4.4 Submodule BMS Algorithm . . . . . 160
    - 4.5 Semigroup BMS Algorithm . . . . . 161
  - 5 Conclusion . . . . . 161
  - Appendix A: Computation of BMS Algorithm
    - Example of Computation . . . . . 161
  - References . . . . . 163
  
- The BMS Algorithm and Decoding of AG Codes . . . . . 165**
  - Shojiro Sakata
  - 1 Introduction . . . . . 166
  - 2 Syndrome Decoding of Dual Codes . . . . . 168
  - 3 Multivariate Polynomial Interpolation and List Decoding of Primal Codes . . . . . 173
  - 4 Other Relevant Decoding Methods of Primal/Dual Codes . . . . . 179

5 Conclusion . . . . .	182
References . . . . .	183
<b>A Tutorial on AG Code Decoding from a Gröbner Basis</b>	
<b>Perspective . . . . .</b>	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
<b>FGLM-Like Decoding: from Fitzpatrick's Approach to Recent</b>	
<b>Developments . . . . .</b>	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
<b>An Introduction to Ring-Linear Coding Theory . . . . .</b>	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

9 Addendum: the Non-commutative Case . . . . .	234
References . . . . .	236
<b>Gröbner Bases over Commutative Rings and Applications</b>	
<b>to Coding Theory . . . . .</b>	<b>239</b>
Eimear Byrne and Teo Mora	
1 Introduction . . . . .	239
2 Gröbner Basis over Commutative Rings: the Lost Lore . . . . .	240
2.1 Notation . . . . .	240
2.2 Zacharias Rings . . . . .	244
2.3 Möller: Gröbner Basis over a Principal Ideal Ring . . . . .	245
2.4 Spear's Theorem . . . . .	247
2.5 Szekeres Ideals . . . . .	247
3 Finite Chain Rings . . . . .	248
4 Solving a Key Equation . . . . .	249
5 Alternant Codes . . . . .	252
5.1 Unique Decoding $C$ for the Hamming Distance . . . . .	253
5.2 Unique Decoding of $C$ for the Lee Distance . . . . .	255
5.3 List Decoding of $C$ for the Hamming Distance . . . . .	256
References . . . . .	258
<b>Overview of Cryptanalysis Techniques in Multivariate Public Key</b>	
<b>Cryptography . . . . .</b>	<b>263</b>
Olivier Billet and Jintai Ding	
1 Introduction . . . . .	263
2 Inversion Attacks . . . . .	264
2.1 Matsumoto–Imai Scheme A and Its Variations . . . . .	265
2.2 Direct Inversion Attacks . . . . .	267
2.3 MinRank . . . . .	269
2.4 Unbalanced Oil and Vinegar . . . . .	272
2.5 Defense Mechanisms . . . . .	273
3 Structural Attacks . . . . .	274
3.1 Isomorphism of Polynomials . . . . .	275
3.2 Two Rounds . . . . .	277
4 Discussion . . . . .	279
References . . . . .	280
<b>A Survey on Polly Cracker Systems . . . . . 285</b>	
Françoise Levy-dit-Vehel, Maria Grazia Marinari, Ludovic Perret and Carlo Traverso	
1 Introduction . . . . .	285
2 The Seminal Paper . . . . .	287
2.1 Barkee's Cryptosystem . . . . .	287
2.2 The Fantomas Attack . . . . .	288
2.3 The Moriarty Attack . . . . .	288
2.4 Bulygin's Attack . . . . .	289

3	CA-Style Cryptosystems . . . . .	290
3.1	Generic Design . . . . .	290
3.2	Graph 3-Coloring . . . . .	291
3.3	Graph Perfect Code . . . . .	291
3.4	Intelligent Linear Algebra Attack . . . . .	292
3.5	EnRoot . . . . .	292
3.6	0-Evaluation Attack . . . . .	293
3.7	3-SAT . . . . .	294
4	Further Attacks . . . . .	295
4.1	Basic CCA (Steinwandt and Geiselmann 2002) . . . . .	295
4.2	Differential Attack . . . . .	296
4.3	The 2-Nomial Attack . . . . .	297
4.4	Further Linear Algebra Attacks . . . . .	298
5	Polly-Two . . . . .	299
6	Non-commutative Gröbner Cryptosystems? No Thanks! . . . . .	300
6.1	Non-commutative Polly Cracker . . . . .	300
6.2	Monoid Algebras . . . . .	301
6.3	Pritchard's Decryption Algorithm . . . . .	302
7	Conclusion . . . . .	303
	References . . . . .	303

## **Block Ciphers: Algebraic Cryptanalysis and Gröbner Bases . . . . . 307**

Carlos Cid and Ralf-Philipp Weinmann

1	Introduction . . . . .	307
2	Design of Block Ciphers . . . . .	308
3	Block Cipher Cryptanalysis . . . . .	310
4	Algebraic Cryptanalysis . . . . .	312
4.1	Polynomial Descriptions of Block Ciphers . . . . .	313
4.2	Field Equations . . . . .	314
4.3	Polynomial Systems over $\mathbb{F}_2$ . . . . .	315
4.4	Equations for Non-linear Components . . . . .	315
4.5	Equations for Inversion over $\mathbb{F}_{2^n}$ . . . . .	316
4.6	Block Cipher Embeddings . . . . .	316
4.7	Direct Construction of Gröbner Bases . . . . .	317
5	Small Scale and Experimental Ciphers . . . . .	318
5.1	Small Scale Variants of the AES . . . . .	318
5.2	Flurry and Curry . . . . .	319
5.3	Other Examples . . . . .	320
6	Experimental Results . . . . .	320
6.1	Small Versions of the AES . . . . .	320
6.2	Flurry and Curry . . . . .	321
6.3	Other Experiments . . . . .	322
7	Attack Strategies . . . . .	322
7.1	Meet-in-the-Middle and Incremental Techniques . . . . .	322
7.2	Differential-Algebraic Cryptanalysis . . . . .	323

8	Alternative Methods for Solving Polynomial Systems . . . . .	324
9	Conclusions . . . . .	325
	References . . . . .	325
<b>Algebraic Attacks on Stream Ciphers with Gröbner Bases . . . . .</b>		<b>329</b>
Frederik Armknecht and Gwenolé Ars		
1	Introduction . . . . .	329
2	Keystream Generators . . . . .	330
3	Algebraic Attacks . . . . .	333
4	Finding Equations . . . . .	336
	4.1 Simple Combiners . . . . .	336
	4.2 Combiners with Memory . . . . .	339
	4.3 Considering Several Equations Simultaneously . . . . .	341
5	Computing Solutions . . . . .	343
	5.1 Minimum Number of Outputs . . . . .	344
	5.2 Time Effort . . . . .	345
6	Conclusions . . . . .	346
	References . . . . .	347
<b>Part 2 Notes</b>		
<b>Canonical Representation of Quasicyclic Codes Using Gröbner</b>		
	<b>Bases Theory . . . . .</b>	<b>351</b>
Kristine Lally		
1	Introduction . . . . .	351
2	Characterisation Using Gröbner Bases Theory . . . . .	352
3	Parity Check Matrix and Dual Code . . . . .	354
4	Recent Application to QC LDPC Codes . . . . .	354
	References . . . . .	355
<b>About the <math>n</math>th-Root Codes: a Gröbner Basis Approach</b>		
	<b>to the Weight Computation . . . . .</b>	<b>357</b>
Marta Giorgetti		
1	General $n$ th-Root Codes . . . . .	357
	1.1 Computing Distance and Weight Distribution for an $n$ th-Root	
	Code . . . . .	358
2	Conclusions and Further Research . . . . .	360
	References . . . . .	360
<b>Decoding Linear Error-Correcting Codes up to Half the Minimum</b>		
	<b>Distance with Gröbner Bases . . . . .</b>	<b>361</b>
Stanislav Bulygin and Ruud Pellikaan		
1	Introduction . . . . .	361
2	Matrix in MDS Form . . . . .	361
3	Decoding up to Half the Minimum Distance . . . . .	362
4	Conclusion and Future Work . . . . .	364
	References . . . . .	364

<b>Gröbner Bases for the Distance Distribution of Systematic Codes . . . . .</b>	<b>367</b>
Eleonora Guerrini, Emmanuela Orsini and Ilaria Simonetti	
1 Preliminaries . . . . .	367
2 Theoretical Results . . . . .	368
3 Numerical Computations . . . . .	370
References . . . . .	371
<b>A Prize Problem in Coding Theory . . . . .</b>	<b>373</b>
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
<b>An Application of Möller's Algorithm to Coding Theory . . . . .</b>	<b>379</b>
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 $\mathfrak{I}$ . . . . .	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
<b>Mattson Solomon Transform and Algebra Codes . . . . .</b>	<b>385</b>
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
<b>Decoding Folded Reed–Solomon Codes Using Hensel-Lifting . . . . .</b>	<b>389</b>
Peter Beelen and Kristian Brander	
1 Introduction . . . . .	389
2 Folded Reed–Solomon Codes . . . . .	390
3 Decoding of Folded Reed–Solomon Codes . . . . .	390
References . . . . .	393
<b>A Note on the Generalisation of the Guruswami–Sudan List Decoding Algorithm to Reed–Muller Codes . . . . .</b>	<b>395</b>
Daniel Augot and Michael Stepanov	
1 Definitions and Notation . . . . .	395



- 2 The Algorithm . . . . . 396
- 3 The Analysis . . . . . 396
- References . . . . . 397
  
- Viewing Multipoint Codes as Subcodes of One-Point Codes . . . . . 399**
- Gretchen L. Matthews
- 1 Introduction . . . . . 399
- 2 Embedding a Multipoint Code in a One-Point Code . . . . . 400
- 3 Examples . . . . . 400
- 4 Conclusion . . . . . 402
- References . . . . . 402
  
- A Short Introduction to Cyclic Convolutional Codes . . . . . 403**
- Heide Gluesing-Luerssen, Barbara Langfeld and Wiland Schmale
- 1 Introduction and Preliminaries . . . . . 403
- 2 How to Define Cyclic Convolutional Codes? . . . . . 404
- 3 Analyzing Cyclic CC’s with Gröbner-type Theory . . . . . 406
- References . . . . . 407
  
- On the Non-linearity of Boolean Functions . . . . . 409**
- Ilaria Simonetti
- 1 Introduction . . . . . 409
- 2 Preliminaries and Notation . . . . . 409
- 3 Computing the Non-linearity . . . . . 411
- References . . . . . 413
  
- Quasigroups as Boolean Functions, Their Equation Systems  
and Gröbner Bases . . . . . 415**
- D. Gligoroski, V. Dimitrova and S. Markovski
- 1 Introduction . . . . . 415
- 2 Quasigroups as Vector Valued Boolean Functions . . . . . 416
- 2.1 Lexicographic Ordering of Finite Quasigroups . . . . . 416
- 2.2 Vector Valued Boolean Functions . . . . . 416
- 2.3 Classification of Quasigroups . . . . . 417
- 3 Systems of Quasigroup Equations and Gröbner Bases . . . . . 418
- References . . . . . 420
  
- A New Measure to Estimate Pseudo-Randomness of Boolean  
Functions and Relations with Gröbner Bases . . . . . 421**
- Danilo Gligoroski, Smile Markovski and Svein Johan Knapskog
- 1 Introduction . . . . . 421
- 2 Normalized Average Number of Terms—NANT . . . . . 422
- 3 NANT and SHA-Family of Hash Functions . . . . . 423
- References . . . . . 425

<b>Radical Computation for Small Characteristics . . . . .</b>	<b>427</b>
Ryutaro Matsumoto	
1 Introduction . . . . .	427
2 Another Radical Computation Method for Positive Characteristic . . . . .	428
3 Comparison of Computational Time and Discussion . . . . .	428
References . . . . .	430