Gröbner Bases, Coding, and Cryptography
Gröbner Bases, Coding, and Cryptography
Preface

Massimiliano Sala

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 (D12) 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 some3 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.

2“Gröbner Bases in Cryptography, Coding Theory, and Algebraic Combinatorics”.
3Other 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

Daniel Augot, Emanuele Betti and Emmanuela Orsini

1 An Overview on Error Correcting Codes ............................................ 47
   1.1 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

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

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 ............................... 161
  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
# A Tutorial on AG Code Decoding from a Gröbner Basis Perspective

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

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

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 over Commutative Rings and Applications to Coding Theory

Eimear Byrne and Teo Mora

1. Introduction
2. Gröbner Basis over Commutative Rings: the Lost Lore
   2.1 Notation
   2.2 Zacharias Rings
   2.3 Möller: Gröbner Basis over a Principal Ideal Ring
   2.4 Spear’s Theorem
   2.5 Szekeres Ideals
3. Finite Chain Rings
4. Solving a Key Equation
5. Alternant Codes
   5.1 Unique Decoding $C$ for the Hamming Distance
   5.2 Unique Decoding of $C$ for the Lee Distance
   5.3 List Decoding of $C$ for the Hamming Distance

References

Overview of Cryptanalysis Techniques in Multivariate Public Key Cryptography

Olivier Billet and Jintai Ding

1. Introduction
2. Inversion Attacks
   2.1 Matsumoto–Imai Scheme A and Its Variations
   2.2 Direct Inversion Attacks
   2.3 MinRank
   2.4 Unbalanced Oil and Vinegar
   2.5 Defense Mechanisms
3. Structural Attacks
   3.1 Isomorphism of Polynomials
   3.2 Two Rounds
4. Discussion

References

A Survey on Polly Cracker Systems

Françoise Levy-dit-Vehel, Maria Grazia Marinari, Ludovic Perret and Carlo Traverso

1. Introduction
2. The Seminal Paper
   2.1 Barkee’s Cryptosystem
   2.2 The Fantomas Attack
   2.3 The Moriarty Attack
   2.4 Bulygin’s Attack
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>CA-Style Cryptosystems</td>
<td>290</td>
</tr>
<tr>
<td>3.1</td>
<td>Generic Design</td>
<td>290</td>
</tr>
<tr>
<td>3.2</td>
<td>Graph 3-Coloring</td>
<td>291</td>
</tr>
<tr>
<td>3.3</td>
<td>Graph Perfect Code</td>
<td>291</td>
</tr>
<tr>
<td>3.4</td>
<td>Intelligent Linear Algebra Attack</td>
<td>292</td>
</tr>
<tr>
<td>3.5</td>
<td>EnRoot</td>
<td>292</td>
</tr>
<tr>
<td>3.6</td>
<td>0-Evaluation Attack</td>
<td>293</td>
</tr>
<tr>
<td>3.7</td>
<td>3-SAT</td>
<td>294</td>
</tr>
<tr>
<td>4</td>
<td>Further Attacks</td>
<td>295</td>
</tr>
<tr>
<td>4.1</td>
<td>Basic CCA (Steinwandt and Geiselmann 2002)</td>
<td>295</td>
</tr>
<tr>
<td>4.2</td>
<td>Differential Attack</td>
<td>296</td>
</tr>
<tr>
<td>4.3</td>
<td>The 2-Nomial Attack</td>
<td>297</td>
</tr>
<tr>
<td>4.4</td>
<td>Further Linear Algebra Attacks</td>
<td>298</td>
</tr>
<tr>
<td>5</td>
<td>Polly-Two</td>
<td>299</td>
</tr>
<tr>
<td>6</td>
<td>Non-commutative Gröbner Cryptosystems? No Thanks!</td>
<td>300</td>
</tr>
<tr>
<td>6.1</td>
<td>Non-commutative Polly Cracker</td>
<td>300</td>
</tr>
<tr>
<td>6.2</td>
<td>Monoid Algebras</td>
<td>301</td>
</tr>
<tr>
<td>6.3</td>
<td>Pritchard’s Decryption Algorithm</td>
<td>302</td>
</tr>
<tr>
<td>7</td>
<td>Conclusion</td>
<td>303</td>
</tr>
<tr>
<td>References</td>
<td></td>
<td>303</td>
</tr>
</tbody>
</table>

**Block Ciphers: Algebraic Cryptanalysis and Gröbner Bases**

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

Algebraic Attacks on Stream Ciphers with Gröbner Bases .......... 329
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

Part 2 Notes

Canonical Representation of Quasicyclic Codes Using Gröbner
   Bases Theory ........................................ 351
   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

About the $n$th-Root Codes: a Gröbner Basis Approach
to the Weight Computation ................................ 357
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

Decoding Linear Error-Correcting Codes up to Half the Minimum
   Distance with Gröbner Bases ........................ 361
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
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 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

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
  Introduction ................................................ 389
1 Folded Reed–Solomon Codes ............................ 390
2 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
  Introduction ................................................ 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
## Radical Computation for Small Characteristics

Ryutaroh Matsumoto

1 Introduction ........................................ 427

2 Another Radical Computation Method for Positive Characteristic ........................................ 428

3 Comparison of Computational Time and Discussion ........................................ 428

References ........................................ 430
Gröbner Bases, Coding, and Cryptography: a Guide to the State-of-Art

Massimiliano Sala

1 In the Beginning

Last century saw a number of landmark scientific contributions, solving longstanding problems and opening the path to entirely new subjects. We are interested in three\(^1\) of these:

1. Claude Shannon’s (1948),
2. Claude Shannon’s (1949),
3. Bruno Buchberger’s (1965)

The title of Shannon’s (1948) paper says it all: “A mathematical theory of communication”. It was later reprinted as Shannon and Weaver (1949) with an even more ambitious title: “The Mathematical Theory of Communication”. Although people have exchanged information in speech and writing for centuries, nobody had ever treated the information exchange (or even information itself) in a rigorous mathematical way. In Shannon’s time there was a need for it, since the last century saw a dramatic increase in the amount and speed of information exchange, with the spreading of new media, like radio, television and telephone.

In Shannon (1948), communication theory is the study of some stationary stochastic processes. Random variables describe information sources and probability distributions describe channels, through which information is sent. Noisy channels are modelled and (error correcting) codes are introduced to permit information recovery after the transmission. In particular, the (probabilistic) foundation of Coding Theory was laid.

One year later, another astonishing paper by Shannon appeared: Shannon (1949). For centuries “secret codes” have been used to protect messages from unauthorized readers. Unsurprisingly, the lack of a rigorous model for communication prevented the study of a more specific model for secure communication. Cryptography had been largely regarded as an art, often mixed with esoteric and obscure references. A cipher was considered secure until an attacker could break it. Like a lighthouse in the dark, Shannon’s paper introduces basic definitions and results, which make

\(^1\)Here listed in chronological order.

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

M. Sala et al. (eds.), Gröbner Bases, Coding, and Cryptography, DOI 10.1007/978-3-540-93806-4_1, © Springer-Verlag Berlin Heidelberg 2009
cryptography into a science. Shannon views a cipher as a set of indexed functions from the plain-text space to the cipher-text space, where the index space is the key space. Building on his previous paper, he focuses on the probability distribution of (the use of) the keys and of the plain-texts, on the way they determine the cipher distribution and on how an attacker can use them. The paper is also full of invaluable (and prophetic) remarks, such as: “The problem of good cipher design is essentially one of finding difficult problems ... How can we ever be sure that a system which is not ideal ... will require a large amount of work to break with every method of analysis? ... We may construct our cipher in such a way that breaking it is equivalent to ... the solution of some problem known to be laborious.”

Among the mathematical problems known to be “laborious” (to use Shannon’s terminology), there is one which has always received a lot of interest: how to “solve” a system of polynomial equations. This reduces to a more general problem: how to represent in a “standard” way a (multivariable) polynomial ideal. Even a simple decision problem like ideal membership\(^2\) had no way to be solved and some even believed it was undecidable, after the word problem in group theory was proved so in Novikov (1955, 1958).

However, in 1965 Buchberger’s (1965, 2006) thesis he presented the appropriate framework for the study of polynomial ideals, with the introduction of Gröbner bases. There is no way to summarize in a few pages the surge in computational algebra research originated from Buchberger’s stunning contribution, with uncountable applications in Mathematics, Engineering, Physics and recently even Biology and other sciences. Fortunately, this book deals only with the applications of Gröbner bases to coding theory and cryptography, and in the next section we will hint at them within the book.

2 Until Now

A finite field \(\mathbb{F}\) may not look particularly interesting to mathematicians accustomed to infinite fields. After all, it contains only a finite number of elements. Also, all nonzero elements are exactly the powers of a primitive element, providing a rather dull group structure for its multiplicative elements. Nevertheless, it is a field, which means a lot\(^3\) from the point of view of its polynomial rings and their algebraic varieties. Moreover, it has a very peculiar property: all functions from \(\mathbb{F}^n\) to \(\mathbb{F}\) can be represented as polynomials in \(\mathbb{F}[x_1, \ldots, x_n]\). Here lies the heart of the interaction\(^4\) between Gröbner bases and coding theory/cryptography.

\(^2\)Determining whether a polynomial belongs to an ideal \(I\) given a finite basis for \(I\).

\(^3\)For example, the number of roots of \(p \in \mathbb{F}[x]\) is \(\deg(p)\) (counting multiplicities).

\(^4\)Some recent research has focused on special classes of rings, we will discuss it at the end of Sect. 2.3.
2.1 Classical Coding Theory

After Shannon (1948), coding theory has developed along two main directions:\(^5\) algebraic coding theory and probabilistic coding theory. The rationale behind the (apparently unnatural) introduction of algebra is that it is very difficult to predict (or even to estimate) the performance of codes constructed and decoded in a probabilistic way, while already the pioneeristic work by Hamming (1950) showed how easy it is to construct algebraic codes, with algebraic decoding, whose performance can be easily estimated by the computation of a parameter called the (Hamming) distance. The main objects of study in algebraic coding theory are “codes”, that is, subsets of finite-dimensional vector spaces over \(\mathbb{F}\). There has been extensive study into linear codes (subspaces) and much less into non-linear codes, due to implementation issues. A lot of research has been devoted to cyclic codes, that form a class of linear codes enjoying special algebraic properties, allowing both easier determination of their distance and low-complexity decoders. An introduction to linear and cyclic codes is provided in our chapter (Augot et al. 2009). The two introductory chapters (Mora 2009a, 2009b) lay down our commutative algebra notation, sketch Gröbner basis theory and describe its powerful results for 0-dimensional ideals.\(^6\) The first instance of applications we present is the chapter on the “Cooper philosophy” (Mora and Orsini 2009), where it is showed how to decode efficiently cyclic codes using Gröbner bases. We have a few short notes on linear and non-linear codes, where some Gröbner basis computation is needed:

- Lally (2009) gives a description of quasi-cyclic codes\(^7\) in term of Gröbner bases of polynomial modules,
- Giorgetti (2009) introduces \(n\)th root codes\(^8\) and show how to compute their distance and weight distribution,
- Bulygin and Pellikaan (2009) explains how to decode a (general) linear code,
- Guerrini et al. (2009) explains how to find the distance of (systematic) non-linear codes (and of linear codes as a special case); a variation allows to classify all such codes with some given parameters,
- Kim (2009) presents a prize problem in coding theory about the existence of a code with special parameters (it could be solved by a variation to the methods in Guerrini et al. 2009),
- Borges-Quintana et al. (2009) provides a Gröbner basis description for binary linear codes, allowing their decoding and the calculation of their distance,
- Martinez-Moro and Ruano (2009) presents a new family of linear codes endowed with a natural Gröbner basis description.

---

\(^{5}\)See our note Gluesing-Luerssen et al. (2009) for a hybrid approach.

\(^{6}\)I.e., ideals having a finite number of solutions, as it is always the case in coding and cryptography.

\(^{7}\)A class of linear codes which can be seen as a generalization of cyclic codes.

\(^{8}\)A wide class of linear codes containing cyclic codes.
2.2 AG Codes

In the eighties (Goppa 1981) the so-called AG (short for “Algebraic Geometry”) codes were proposed. These are linear codes obtained as evaluation of function spaces on algebraic curves. Standard results in curve theory yield sharp estimates for their distance. Their geometric structure permits specific decoding algorithms. For problems related to these codes, a polynomial formulation is natural and hence Gröbner bases find a field fertile in applications. Our treatment (chapters) of AG codes is as follows:

- Leonard (2009a) introduces the AG codes, especially the one-point AG codes,
- Little (2009) explains their encoding (with Gröbner bases) and the relation with the curve automorphisms,
- Sakata (2009a) describes the Berlekamp–Massey–Sakata (BMS) algorithm, which can be specialized to decode AG codes, as explained in Sakata (2009b),
- Leonard (2009b) further explores their decoding.

Recently, it has been observed that the classical presentation of AG codes suffers from some limitations, such as the need for a lot of theoretical prerequisites in order to understand theory and the absence of explicit code descriptions. To overcome these difficulties, a new constructive approach has been proposed: the Order Domain codes. These codes and their relation to classical AG codes are discussed in our chapter (Geil 2009). Interestingly, Gröbner bases have turned out to be very convenient tools for their study.

2.3 Coding Miscellanea

Classical decoding algorithms for cyclic and AG codes can be reinterpreted in terms of Gröbner basis computation, as explained in our chapter (Guerrini and Rimoldi 2009), where also list-decoding algorithms are detailed. A list-decoding algorithm is an algorithm that decodes a received message into a list of possible codewords. A probabilistic algorithm is then used to choose the most likely among them. These algorithms are a compromise between algebraic decoding and probabilistic decoding, which is necessary in order to fully exploit the channel capacity without losing the advantage of the algebraic approach. Also the BMS algorithm can be adapted to a list-decoding algorithm (Sakata 2009b).

---

9 Which is their most important subclass, enjoying an easier description. See our note (Matthews 2009) for multi-point AG codes.
10 Historically, this was the first fast algorithm to decode such codes.
11 In comparison to the prerequisites for standard linear code theory.
12 Which would prevent actual use of these codes.
13 See also our notes (Augot and Stepanov 2009; Beelen and Brander 2009).
We report that recently also (linear and cyclic) codes over rings have been studied. For an introduction to this theory see our chapter (Greferath 2009). Also Gröbner basis theory can be adapted to special classes of rings. This is sketched in our chapter (Byrne and Mora 2009), where it is also explained how the Gröbner basis decoding techniques in Guerrini and Rimoldi (2009) are extended to codes over (special) rings.

2.4 Cryptography

After Shannon’s (1949) paper two main kinds of ciphers have been developed: block ciphers and stream ciphers. Block ciphers are closer to Shannon’s original idea of key-indexed transformations from the plain-text space to the cipher-text space, and can be viewed as maps from $\mathbb{F}^n$ to $\mathbb{F}^m$, for some $n, m \geq 1$. Stream ciphers assume the message to come in a (ideally) infinite stream (of field elements in $\mathbb{F}$) and they add element by element the message stream with a key stream produced by the cipher itself. Block ciphers and their relation to Gröbner bases are discussed in our chapter (Cid and Weinmann 2009), while stream ciphers and their relation to Gröbner bases are discussed in chapter (Armknecht and Ars 2009). It is interesting to note that Gröbner basis attacks on some stream ciphers have outmatched all classical attacks and so they are now widely used for assessing the security of keystream generators (Armknecht and Ars 2009). This is not the case for Gröbner basis attacks on block ciphers, yet.

The problem with the ciphers as designed by Shannon is that the two peers need to exchange the key before data transmission. This can be difficult since it requires the presence of a secure channel. In Diffie and Hellman (1976) they solved this problem with an ingenious key exchange protocol and their ideas were adapted to design a cipher based on two keys, a public $K_P$ and a secret $K_S$, such that only a key exchange of $K_P$ in a public channel is required (see e.g. Rivest et al. 1978; McEliece 1978). This branch of cryptography is nowadays called public key (or asymmetric) cryptography (PKC), while traditional cryptography is called symmetric cryptography. Although PKC cannot provide the same security level as symmetric cryptography without a larger computational cost, in many real situations (such as in the Internet) there is little choice. Among the PKC systems brought forward in the last 40 years, there are two families that rely on “laborious” problems in polynomial rings. They are deeply discussed in our chapters (Billet and Ding 2009) and (Levy-dit-Vehel et al. 2009). The ciphers in the latter family are called Polly Cracker systems. Although Gröbner bases are used to attack the systems discussed in both chapters, Gröbner bases are used to build the systems themselves in the Polly Cracker case (which then deserves a deeper analysis).

---

14 Or, rarely, perform more complicate transformations.
As mentioned at the beginning of the section, it is the polynomial nature of all functions from $\mathbb{F}^n$ to $\mathbb{F}$ that allows the use of Gröbner bases in coding and cryptography. A special case is the binary case, i.e. when $\mathbb{F} = \mathbb{F}_2$, since in most applications the encoding/enciphering is binary. Any function from $(\mathbb{F}_2)^n$ to $\mathbb{F}_2$ is called a Boolean function and any function from $(\mathbb{F}_2)^n$ to $(\mathbb{F}_2)^m$ is a vectorial Boolean functions. As expected, their properties are amply studied in connection with cryptography problems.

We present three notes dealing with three different aspects:

- Simonetti (2009) shows how to use Gröbner bases to compute the non-linearity of any Boolean function $f$, which is an important parameter in evaluating the security of using $f$ in building a cipher;
- Gligoroski et al. (2009b) sketches the use of (vectorial) Boolean functions in building hash functions;\footnote{These are cryptographic methods utilized to guarantee the authentication of a pair message/sender.}
- Gligoroski et al. (2009a) uses Gröbner bases to represent a special class of Boolean functions (quasigroups) which are used to construct a PKC system.

3 Final Comments

In the previous sections, I have tried to convey the general plan behind our book and its chapters (notes) division. This book is a collection of papers by many authors, some of them with a very different background.\footnote{There is also a note (Matsumoto 2009) which does not apparently fit with the rest of the book’s material, but which I felt it should be included because it hints at possible new developments.} As such, it cannot be read as a text-book, but the accurate choice of the subjects should allow the reader to have a comprehensive view of the most common applications of Gröbner bases to coding and cryptography. It is especially important to read carefully the introductory chapters and understand their notation. Within every chapter and note, I have done my best to insert all inter-book cross-references that I felt adequate. Still, there are many parts of the theory we have not been able to cover and a lot of further interactions that we have not detailed.

It is my belief (shared by the Board) that this book can be an excellent guide to the subject, both for the researcher wishing to go deeper into some unfamiliar part of the theory and for the student approaching this area.

References

G. L. Matthews, *Viewing multipoint codes as subcodes of one-point codes*, this volume, 2009, pp. 399–402.


T. Mora, *The FGLM problem and Moeller’s algorithm on zero-dimensional ideals*, this volume, 2009a, pp. 27–45.


Part 1
Invited Papers
1 Notation and Definitions

$\mathbb{F}$ denotes an arbitrary field, $\overline{\mathbb{F}}$ denotes its algebraic closure and $\mathbb{F}_q$ denotes a finite field of size $q$ (so $q$ is implicitly understood to be a power of a prime) and $\mathcal{P} := \mathbb{F}[X] := \mathbb{F}[x_1, \ldots, x_n]$ the polynomial ring over the field $\mathbb{F}$.

For any ideal $I \subset \mathcal{P}$ and any extension field $\mathbb{E}$ of $\mathbb{F}$, let $\mathcal{V}_{\mathbb{E}}(I)$ denote the set of the rational points of $I$ over $\mathbb{E}$. We also write $\mathcal{V}(I) = \mathcal{V}_{\mathbb{F}}(I)$.

Let $\mathcal{T}$ be the set of terms in $\mathcal{P}$, id est

$$
\mathcal{T} := \{x_1^{a_1} \cdots x_n^{a_n} : (a_1, \ldots, a_n) \in \mathbb{N}^n\},
$$

which is a multiplicative version of the additive semigroup $\mathbb{N}^n$, the relation between these notations being obvious: given

$$
\alpha := (a_1, \ldots, a_n), \quad \beta := (b_1, \ldots, b_n), \quad \gamma := (c_1, \ldots, c_n)
$$

and the terms

$$
\tau_\alpha := X^\alpha = x_1^{a_1} \cdots x_n^{a_n}, \quad \tau_\beta := X^\beta = x_1^{b_1} \cdots x_n^{b_n}, \quad \tau_\gamma := X^\gamma = x_1^{c_1} \cdots x_n^{c_n},
$$

we have

$$
\tau_\alpha \cdot \tau_\beta = \tau_\gamma \iff a_i + b_i = c_i \textrm{ for each } i \iff \alpha + \beta = \gamma,
$$

$$
\tau_\alpha \mid \tau_\beta \iff a_i \leq b_i \textrm{ for each } i \iff \alpha \leq_{\mathcal{P}} \beta,
$$

where $\langle \cdot \rangle$ is the natural partial ordering over $\mathbb{N}^n$.

The assignment of a finite set of terms

$$
G := \{\tau_1, \ldots, \tau_\nu\} \subset \mathcal{T}, \quad \tau_i = x_1^{a_{i1}} \cdots x_n^{a_{in}}
$$

—or, equivalently of a finite set of integer vectors

$$
\{a^{(1)}, \ldots, a^{(\nu)}\} \subset \mathbb{N}^n, \quad a^{(i)} = (a_{i1}, \ldots, a_{in}) \in \mathbb{N}^n,
$$

defines a partition of $\mathcal{T}$ (resp. $\mathbb{N}^n$) in two parts (see Fig. 1 where $G := \{x_1^6x_2, x_1^4x_2^3, x_1^2x_2^5\} \subset \mathcal{T}$):
Fig. 1 A Gröbner escalier

- $T := \{ \tau \tau_i : \tau \in T, 1 \leq i \leq \nu \} \cong \{ \alpha + a^{(i)} : \alpha \in \mathbb{N}^n, 1 \leq i \leq \nu \} =: \Sigma$ which is a semigroup ideal, id est a subset $T \subset T$ (resp. $\Sigma \subset \mathbb{N}^n$) such that
  
  $\tau \in T, t \in T \implies \tau t \in T$, resp. $a \in \Sigma, b \in \mathbb{N}^n, a \leq_P b \implies b \in \Sigma$;

- $N := T \setminus T \cong \mathbb{N}^n \setminus \Sigma =: \Delta$ which is an order ideal, id est a subset $N \subset T$ (resp. $\Delta \subset \mathbb{N}^n$) such that
  
  $\tau \in T, t \in N, \tau | t \implies \tau \in N$, resp. $a \in \Delta, b \in \mathbb{N}^n, a \geq_P b \implies b \in \Delta$.

Remark that the assignment of
- a finite monomial set $G \subset T$,
- a semigroup ideal $T \subset T$,
- an order ideal $N \subset T$

uniquely characterizes the other data: in fact

- $N$ and $T$ are related by their being complementary in $T$,
- each semigroup ideal $T \subset T$ has a unique minimal basis $G \subset T$ such that $T := \{ \tau \tau_i : \tau \in T, \tau_i \in G \}$; the fact, whose proof is quite involved, that $G$ is finite is known as Dickson’s lemma but actually was already proved by Gordan (1900).

We recall that the well-orderings on $T$ which are a semigroup ordering, id est satisfy

$\tau_1 < \tau_2 \implies \tau \tau_1 < \tau \tau_2$ for each $\tau, \tau_1, \tau_2 \in T$

are called term orderings, even if the old-fashioned notion of admissible ordering can still be found somewhere.

For a free-module $\mathcal{P}^m, m \in \mathbb{N}$, we denote by $\{ e_1, \ldots, e_m \}$ its canonical basis,

$T^{(m)} = \{ t e_i, t \in T, 1 \leq i \leq m \}$

$= \{ x_1^{a_1} \cdots x_n^{a_n} e_i, (a_1, \ldots, a_n) \in \mathbb{N}^n, 1 \leq i \leq m \}$
denotes its monomial $\mathbb{F}$-basis and $<$ denotes a well-ordering on $T^{(m)}$ which is compatible with the term-ordering $<$ on $T$, that is, satisfying
\[ \tau_1 \leq \tau_2, \quad t_1 \leq t_2, \quad \implies \quad \tau_1 t_1 \leq \tau_2 t_2 \]
for each $\tau_1, \tau_2 \in T$, $t_1, t_2 \in T^{(m)}$.

Note that $T^{(1)} = T$.

For each $f = \sum_{\tau \in T^{(m)}} c(f, \tau) \tau \in \mathcal{P}^{m}$, its support is
\[ \text{supp}(f) := \{ \tau \in T^{(m)} : c(f, \tau) \neq 0 \}, \]
its leading term is the term $T_{\prec}(f) := \max_{\prec}(\text{supp}(f))$, its leading coefficient is $\text{lc}_{\prec}(f) := c(f, T_{\prec}(f))$ and its leading monomial is $M_{\prec}(f) := \text{lc}_{\prec}(f)T_{\prec}(f)$.

When $\prec$ is understood we will drop the subscript, as in $T(f) = T_{\prec}(f)$.

For any set $F \subset \mathcal{P}^{m}$, write
\begin{itemize}
  \item $T[F] := T_{\prec}[F] := \{ T(f) : f \in F \}$;
  \item $M[F] := M_{\prec}[F] := \{ M(f) : f \in F \}$;
  \item $T(F) := T_{\prec}(F) := \{ \tau T(f) : \tau \in T, f \in F \}$, a monomial module$^1$;
  \item $N(F) := N_{\prec}(F) := T^{(m)} \setminus T_{\prec}(F)$, an order module$^2$;
  \item $\mathcal{I}(F) = \{ c \}$ the module generated by $F$.
\end{itemize}

Remark that, if $m = 1$, the assignment of $T[F]$ gives the partition $T = T(F) \sqcup N(F)$ discussed above, that the related semigroup ideal $T(F)$ is also denoted $\Sigma(F)$ while the related order ideal $N(F)$ is also denoted $\Delta(F)$ and labelled $\Delta$-set or footprint. When $F$ is the Gröbner basis of the module $\mathcal{I}(F)$ it generates, $N(F)$ is called the Gröbner éscalier (Galligo 1974) of $\mathcal{I}(F)$.

We can now induce a finer partition of $T^{(m)}$ in terms of a module $M \subset \mathcal{P}^{m}$ and a term-ordering $\prec$, by defining (see Fig. 2 where this time we have set $M := \{ x_1^6, x_1^4x_2^3, x_2^5 \} \subset \mathcal{P}$)
\begin{itemize}
  \item $N_{\prec}(M) = T^{(m)} \setminus T_{\prec}(M)$ its Gröbner éscalier;
  \item $B_{\prec}(M) := \{ x_h \tau : 1 \leq h \leq n, \tau \in N_{\prec}(M) \} \setminus N_{\prec}(M)$, its border set;
  \item $J_{\prec}(M) := T_{\prec}(M) \setminus B_{\prec}(M)$,
  \item $G_{\prec}(M) \subset B_{\prec}(M)$ the unique minimal basis of $T_{\prec}(M)$,
  \item $C_{\prec}(M) := \{ \tau \in N_{\prec}(M) : x_h \tau \in T_{\prec}(M), \forall h \}$ its corner set.
\end{itemize}

Under this notation, the following properties are trivially satisfied:

**Lemma 1** It holds
\begin{enumerate}
  \item $T_{\prec}(M) = \{ \tau \in T : \exists g \in M : T_{\prec}(g) = \tau \}$;
  \item $J_{\prec}(M) = \{ \tau \in T_{\prec}(M) : x_i | \tau \implies \frac{\tau}{x_i} \in T_{\prec}(M) \}$;
  \item $B_{\prec}(M) = \{ \tau \in T_{\prec}(M) : \exists x_i | \tau, \frac{\tau}{x_i} \in N_{\prec}(M) \}$;
\end{enumerate}

$^1$Id est a subset $T \subset T^{(m)}$ such that $\tau \in T, t \in T \implies \tau t \in T$.

$^2$Id est a subset $N \subset T^{(m)}$ such that $\tau \in T, \tau t \in N \implies t \in N$. [1]
4. $G ≺ (M) = \{ \tau \in T ≺ (M) : \forall x \mid x, z_j \in N ≺ (M) \}$;
5. $C ≺ (M) = \{ \tau \in N ≺ (M) : \forall i, x \mid x \tau \in B ≺ (M) \}$;
6. $N ≺ (M) = \{ \tau \in T ≺ (M) : \forall x \mid x \tau \in T ≺ (M) \}$;
7. $C ≺ (M) \cup T ≺ (M)$ is a monomial module;
8. $N ≺ (M) \cup G ≺ (M)$ and $N ≺ (M) \cup B ≺ (M)$ are order modules.
9. $\tau \in J ≺ (M) \iff \forall x \mid x \tau \in T ≺ (M)$;
10. $\tau \in B ≺ (M) \setminus G ≺ (M) \iff \exists h, H : z_j \mathrel{\not\subseteq} B ≺ (M) \subset T ≺ (M)$;
11. $\tau \in B ≺ (M) \setminus G ≺ (M) \iff \forall x \mid x \tau \in B ≺ (M)$;
12. $\tau \in N ≺ (M) \cup G ≺ (M) \iff \forall x \mid x \tau \in N ≺ (M)$;
13. $\tau \in T ≺ (M) \cup C ≺ (M) \iff \forall x, x \tau \in T ≺ (M)$;
14. $\tau \in N ≺ (M) \setminus C ≺ (M) \iff \exists h : z_j \mathrel{\not\subseteq} N ≺ (M)$.

**Lemma 2** Let $N$ be a finitely generated $P$-module, $\Phi : P^m \mapsto N$ be any surjective morphism and set $M := \ker(\Phi)$. Then

1. $P^m \cong M \oplus \text{Span}_F(N(M))$;
2. $N \cong \text{Span}_F(N(M))$;
3. for each $f \in P^m$, there is a unique $g := \text{Can}(f, M, \prec) \in \text{Span}_F(N(M))$ such that $f - g \in M$.

Such $g$ is called the canonical form of $f$ w.r.t. $M$ and satisfies also:
(a) $\text{Can}(f_1, M, \prec) = \text{Can}(f_2, M, \prec) \iff f_1 - f_2 \in M$;
(b) $\text{Can}(f, M, \prec) = 0 \iff f \in M$.

**Definition 3** Let $N$ be a finitely generated $P$-module, $\Phi : P^m \mapsto N$ be any surjective morphism and set $M := \ker(\Phi)$.

Let $G \subset M$, $f, h, f_1, f_2 \in P^m$. Then

1. $G$ will be called a Gröbner basis of $M$ if

$$\text{T}(G) = \text{T}(M),$$

that is, $\text{T}(G) := \{ \text{T}(g) : g \in G \}$ generates $\text{T}(M) = \text{T}[M]$. 

---

**Fig. 2** A refined Gröbner escalier
2. For each \( f_1, f_2 \in P^m \) such that 
\[
T(f_1) = t_1 e_{l_1}, \quad T(f_2) = t_2 e_{l_2},
\]
the S-polynomial of \( f_1 \) and \( f_2 \) exists only if \( e_{l_1} = e_{l_2} := \epsilon \), in which case it is 
\[
S(f_1, f_2) := \text{lcm}(f_1, f_2) - \frac{\delta(f_1, f_2)}{t_2} f_2 - \frac{\delta(f_1, f_2)}{t_1} f_1,
\]
where \( \delta := \text{lcm}(t_1, t_2) \); \( \delta \epsilon \) is called the formal term of \( S(f_1, f_2) \).

3. \( f \) has a Gröbner representation \( \sum_{i=1}^{\mu} p_i g_i \) in terms of \( G \) if
\[
f = \sum_{i=1}^{\mu} p_i g_i, \quad p_i \in P, \ g_i \in G, \quad T(p_i)T(g_i) \preceq T(f), \quad \text{for each } i.
\]

4. \( f \) has the (strong) Gröbner representation \( \sum_{i=1}^{\mu} c_i t_i g_i \) in terms of \( G \) if
\[
f = \sum_{i=1}^{\mu} c_i t_i g_i, \quad c_i \in \mathbb{F} \setminus \{0\}, \ t_i \in T, \ g_i \in G,
\]
with \( T(f) = t_1 T(g_1) \succ \cdots \succ t_i T(g_i) \succ \cdots \).

5. \( f \) has the weak Gröbner representation \( \sum_{i=1}^{\mu} c_i t_i g_i \) in terms of \( G \) if
\[
f = \sum_{i=1}^{\mu} c_i t_i g_i, \quad c_i \in \mathbb{F} \setminus \{0\}, \ t_i \in T, \ g_i \in G,
\]
with \( T(f) = t_1 T(g_1) \succeq \cdots \succeq t_i T(g_i) \succeq \cdots \).

6. For any \( f_1, f_2 \in P^m \), whose S-polynomial exists and has \( \delta \epsilon \) as formal term, we say that \( S(f_1, f_2) \) has a quasi-Gröbner representation in terms of \( G \) if it can be written as \( S(g, f) = \sum_{k=1}^{\mu} p_k g_k \), with \( p_k \in P, \ g_k \in G \) and \( T(p_k)T(g_k) \prec \delta \epsilon \) for each \( k \).

7. \( h := \text{NF}(f, G) \) is called a normal form of \( f \) w.r.t. \( G \), if
- \( f - h \in \mathbb{I}(G) \) has a strong Gröbner representation in terms of \( G \) and
- \( h \neq 0 \implies T(h) \notin T(G) \).

8. The reduced Gröbner basis of \( M \) w.r.t. \( \prec \) is the set
\[
\{ \tau \in \text{Can}(\tau, M, \prec) : \tau \in G_\prec(M) \}.
\]

9. The border basis of \( M \) w.r.t. \( \prec \) is the set
\[
\{ \tau \in \text{Can}(\tau, M, \prec) : \tau \in B_\prec(M) \}.
\]

\(^3\)Note that here, unlike in (4), we are not assuming \( i \neq j \implies T(p_i)T(g_i) \neq T(p_j)T(g_j) \); moreover both here, in (4) and in (5) a same element of \( G \) can repeatedly appear.
10. A Gröbner representation of $M$ is the assignment of
- a linearly independent set $q = \{q_1, \ldots, q_s\}$ ($q_1 = 1$), where $s = \#(N(M))$, such that $P^m/M = \text{Span}_F(q)$.
- the set
  \[ M = M(q) := \left\{ (a^{(h)}_{ij}) \in \mathbb{F}^{s^2} \mid 1 \leq h \leq n \right\} \]
  of the $s \times s$ square matrices $(a^{(h)}_{ij})$ defined by the equalities
  \[ x_h q_l = \sum_j a^{(h)}_{lj} q_j, \quad \forall l, j, h, 1 \leq l, j \leq s, 1 \leq h \leq n \]
in $P^m/M = \text{Span}_F(q)$.

11. For each $f \in P$ the Gröbner description of $f$ in terms of a Gröbner representation $(q, M)$ is the unique vector
  \[ \text{Rep}(f, q) := (\gamma(f, q_1, q), \ldots, \gamma(f, q_s, q)) \in \mathbb{F}^s \]
such that $f - \sum j \gamma(f, q_j, q)q_j \in M$.

12. The linear representation of $M$ w.r.t. $\preceq$ is the Gröbner representation $(N_{\preceq}(M), M(N_{\preceq}(M)))$ where $q = N_{\preceq}(M)$.

With these definitions, if $N_{\preceq}(M) = \{\tau_1, \ldots, \tau_s\}$, the Gröbner description
\[ \text{Rep}(f, N_{\preceq}(M)) := (\gamma(f, \tau_1, N_{\preceq}(M)), \ldots, \gamma(f, \tau_s, N_{\preceq}(M))) \]
of $f$ in terms of the linear representation of $M$ w.r.t. $\preceq$ is a convoluted synonym of the notion of canonical form
\[ \text{Can}(f, M, \preceq) = \sum_{j=1}^s \gamma(f, \tau_j, \preceq)\tau_j = \sum_{j=1}^s \gamma(f, \tau_j, N_{\preceq}(M))\tau_j \]
of $f$ in terms of $\preceq$.

## 2 Term-Orderings: Classification and Representation

### Definition 4
A weight function $v_w : T \mapsto \mathbb{R}$ on $T$ and $P$ is the assignment of a vector $w := (w_1, \ldots, w_n) \in \mathbb{R}^n$, $w_i \geq 0$, so that $v_w(X^a) = w \cdot a = \sum_i w_i a_i$.

### Theorem 5 (Erdös 1956)
Each semigroup ordering $<$ on $T$ is characterized by assigning $r \leq n$ linearly independent vectors
\[ w_1, \ldots, w_j := (w_{j1}, \ldots, w_{jn}), \ldots, w_r \in \mathbb{R}^n \]
—or equivalently an $r \times n$ matrix $(w_{ji}) \in \mathbb{R}^{rn}$ of maximal rank—so that for each
\[ \tau_a := X^a, \tau_b := X^b \text{ in } T, \]
we have
\[ \tau_a < \tau_b \iff \exists j: \ w_{j} \cdot a < w_{j} \cdot b \text{ and } w_{i} \cdot a = w_{i} \cdot b \quad \text{for } i < j. \]

Moreover, such an ordering is a well-ordering iff, for each $i$, $X_i > 1$, that is iff, for each $i$, $w_{ji} > 0$, where $j$ denotes the minimal value for which $w_{ji} \neq 0$.

Finally, if $M_1, M_2$ are two $r \times n$ matrices, then they characterize the same ordering $<$ iff there is an invertible $r$-square matrix $A = (a_{ij})$ such that
\[ M_1 = AM_2 \text{ and } a_{ij} = \begin{cases} 0 & \text{if } i < j, \\ 1 & \text{if } i = j. \end{cases} \]

Among the term-orderings we will quote those which have common and practical use, also for applications.

- The **lexicographical (lex)** ordering induced by $X_1 < X_2 < \cdots < X_n$ is defined by
\[ X_1^{a_1} \cdots X_n^{a_n} < X_1^{b_1} \cdots X_n^{b_n} \iff \exists j: \ a_j < b_j \text{ and } a_i = b_i \quad \text{for } i > j; \]
it has good elimination properties since it allows to compute all the elimination ideals $I \cap \mathbb{F}[X_1, \ldots, X_i]$;

**Fact 6** If $G$ is the Gröbner basis of $I \subset \mathbb{F}[X_1, \ldots, X_n]$ w.r.t. lex then, for each $i \leq n$, $G \cap \mathbb{F}[X_1, \ldots, X_i]$ is the Gröbner basis of $I \cap \mathbb{F}[X_1, \ldots, X_i]$ w.r.t. lex.

- Note that the lexicographical ordering depends on a chosen ordering imposed on the variables; recently many authors prefer using the lexicographical ordering induced by $X_1 > X_2 > \cdots > X_n$ which is defined by
\[ X_1^{a_1} \cdots X_n^{a_n} < X_1^{b_1} \cdots X_n^{b_n} \iff \exists j: \ a_j < b_j \text{ and } a_i = b_i \quad \text{for } i < j. \]

- The **reverse lexicographical (rev-lex)** ordering induced by $X_1 < X_2 < \cdots < X_n$ is defined by
\[ X_1^{a_1} \cdots X_n^{a_n} < X_1^{b_1} \cdots X_n^{b_n} \iff \exists j: \ a_j > b_j \text{ and } a_i = b_i \quad \text{for } i < j; \]
it is not a well-ordering since $\cdots < X_i^{d+1} < X_i^d < \cdots < X_1 < 1$.

- The **deg-rev-lex** (degree reverse lexicographical) ordering induced by $X_1 < X_2 < \cdots < X_n$ is the one where terms are first compared by their degree and the ties are solved using rev-lex: it is defined by
\[ X^a < X^b \iff \text{exists } j: \ a_j > b_j \text{ and } a_i = b_i \quad \text{for } 0 \leq i < j, \]
where we set $a_0 := -\sum_i a_i, b_0 := -\sum_i b_i$ and has the following property

\[ a_{ij} := \begin{cases} 0 & \text{if } i < j, \\ 1 & \text{if } i = j. \end{cases} \]

\[ \text{Often shorthanded as } drl. \]