
EFFICIENT ALGORITHMS FOR ALGEBRAIC RELATIONS

YOUNES GRACE

INTERNSHIP OF MASTER 2 IN

APPLIED ALGEBRA IN CRYPTOGRAPHY

AT



WITH THE SUPERVISORS:
M. NALDI SIMONE, M. NEIGER VINCENT

SEPTEMBER 2018

Table of contents

Introduction	5
1 Algebraic Relations	7
1.1 Problem Definition	7
1.2 Examples	8
1.2.1 Rational Reconstruction	8
1.2.2 Bivariate Hermite-Padé Approximation	8
1.2.3 Modular Inversion	8
1.2.4 Bivariate Interpolation	9
2 Preliminaries	11
2.1 Polynomials, Ideals, Modules	11
2.2 Gröbner Bases	13
2.2.1 Introduction	13
2.2.2 Ideals	13
2.2.3 Modules	16
2.3 Algebras of Dimension 0	21
2.3.1 Some Geometry	21
2.3.2 0-Dimensional Ideals	21
3 Main problem and Previous Work	23
3.1 Algorithmic Problem	23
3.2 Existing Algorithm	24
4 Contribution and Perspectives	27
4.1 Proposition	27
Bibliography	35

Introduction

We propose to study the design of fast algorithms for the computation of algebraic relations [1]. This fundamental problem can be interpreted as the resolution of linear systems which have some structure [2], that one wishes to exploit in order to obtain more efficient algorithms. In the case of multivariate polynomial relations, improving the bounds of complexity is an open question, actively studied by the community of symbolic computation that tackles it from different angles: Gröbner bases [3], linear recurrences [4],... If progress has been obtained, however no solution known yet is entirely satisfying. Indeed, in the fastest algorithms that have been proposed, the basic bricks as the fast polynomials and matrices products are either not fully used and appear difficult to incorporate, or used but in methods that only weakly exploit the structure of the problem.

Recent advances for the computation of algebraic relations in the univariate case [5] suggest the possibility of improvements in the case of several variables. First of all it will be a question to study this on specific instances; thus, a first milestone could be the case of a generic equation, which makes it possible to know structural information on the relations already found. This particular case is already concentrating of the algorithmic difficulties of calculating relations, and improvements in complexity bounds would have important spillovers for example in polynomial optimization and in decoding algorithms of error correcting codes.

The algebraic relation problem is finding a list of polynomials (p_1, \dots, p_m) that satisfies $p_1 f_1 + \dots + p_m f_m = 0$ for some given elements f_1, \dots, f_m in a space where we can multiply by polynomials. We will often have degree constraints on p_i , or we will want to compute a representative set of relations, for example a Gröbner basis. The complexity of this computation depends mainly on a dimension D related to the number of linear parameters in the relations sought. The best bound of known complexity is of the order of $\mathcal{O}(nD^3)$ [3], where n , the number of variables, is usually negligible compared to D .

Under this bound, the dominant term D^3 seems to be improvable in many interesting situations. This is the case for the Padé Approximation and the multivariate interpolation, which are involved in the decoding Reed-Solomon and geometric codes [6], in cryptology in the computation of algebraic immunity [7], and in the computation of the kernel of multi-level Hankel structured matrices (polynomial optimization [8], linear recurrences [4]).

In the univariate case, iterative fast algorithms exist for the approximation [9], then have been

accelerated to reach a quasi-linear complexity in D thanks to divide and conquer techniques [10]. The spectrum of structures that are already known to be dealt with under a satisfying bound of complexity, has recently been extended from the point of view of one-variable relations [5] and that of structured matrices at one structure level [11]. This raises the question of how similar improvements could be performed in the multivariate case.

In the first chapter entitled *Algebraic Relations* we define the problem we aim to solve. Then we give examples of some interesting problems that can be solved by computing algebraic relations.

In the second chapter entitled *Preliminaries* we recall some definitions and important theorems about ideals, polynomials and modules. Then we introduce Gröbner bases in particular (ideals) and general (modules) cases. In brief, a Gröbner basis of an ideal I is a set of generators for I with some additional properties. The advantage of using Gröbner bases is the reduction of many questions about ideals or modules in polynomials rings to questions about monomial ideals or monomial modules which is easier and somehow faster (algorithmic point of view). After having a good knowledge about Gröbner bases and being familiar with the notions of modules, we will be able to address the third and the last chapter.

The third chapter entitled *Main Problem and Previous Work* explains the context of our work at the algorithmic level. So we give an existing algorithm that studied the same problem (Algebraic relations) iteratively [12] and by which we got inspired to construct our algorithm in the last chapter.

Finally in *Contributions and Perspectives* we will give a proposition that we wish it will help us to design algorithms that improve the known complexity terminals. In fact, existing algorithms for multivariate relations [4, 13, 3] follow an iterative approach similar to that used for univariate relations. It is then righteous to want to take advantage of multivariate divide and conquer techniques that have allowed great advances in the univariate case. This last case suggests that we can obtain complexities of the order of $\mathcal{O}(nD^2)$, a gain of a factor D in relation to the cubic complexities mentioned above.

Algebraic Relations

1.1 Problem Definition

Let \mathbb{K} be a field, and let R denote $\mathbb{K}[x_1, \dots, x_n]$, the set of multivariate polynomials in (x_1, \dots, x_n) over \mathbb{K} , and $R^{m \times r}$ denote the set of $m \times r$ (multivariate) polynomial matrices.

MULTIVARIATE RELATIONS

Let us consider a submodule $\mathcal{M} \subseteq R^r$ and let some elements $f_1, \dots, f_m \in R^r / \mathcal{M}$ be represented as a matrix $F \in R^{m \times r}$ such that each row of this matrix corresponds to an f_i . Then, the kernel of the module morphism

$$\begin{aligned} \varphi_{\mathcal{M},f}: \quad R^m &\longrightarrow R^r / \mathcal{M} \\ (p_1, \dots, p_m) &\longmapsto p_1 f_1 + \dots + p_m f_m \end{aligned}$$

consists of relations between the f_i 's. So we write it as

$$\mathcal{R}(\mathcal{M}, F) = \{p \in R^{1 \times m} \mid pF \in \mathcal{M}\},$$

Example 1.1.1. Let $r = 2$ and $\mathcal{M} = \langle x^3, y^3 \rangle \times \langle x^3, y^3 \rangle$. Let $f_1 = (2xy + x^2y, xy)$, $f_2 = (x^2y^2 + x^3, xy^2 + 4)$ and $f_3 = (xy + x^2 + 4, x + y + y^2) \in R^2 / \mathcal{M}$. Then the problem is to find $(p_1, p_2, p_3) \in R^{1 \times 3}$ that verifies:

$$\begin{pmatrix} p_1 & p_2 & p_3 \end{pmatrix} \begin{pmatrix} 2xy + x^2y & xy \\ x^2y^2 + x^3 & xy^2 + 4 \\ xy + x^2 + 4 & x + y + y^2 \end{pmatrix} \in \mathcal{M}$$

□

Hereafter, the elements of $\mathcal{R}(\mathcal{M}, F)$ are called relations of $\mathcal{R}(\mathcal{M}, F)$ and our problem is finding such elements. In some situations, one is interested to solve the problem by finding just one relation with given degree constraints. In others, the goal is to construct a fast algorithm for finding a relation with degree constraints via the computation of a whole (Gröbner) basis for a monomial order (defined in the next chapter) chosen according to these constraints.

1.2 Examples

These examples are inspired from [14] and [9].

1.2.1 Rational Reconstruction

Let $A \in \mathbb{K}[x]$ be a polynomial of degree $D > 0$ and $B \in \mathbb{K}[x]$ of degree $< D$. For $k \in \{1, \dots, n\}$, the rational reconstruction of B modulo A is finding a couple of polynomials $(U, V) \in \mathbb{K}[x]^2$ that verifies under some degree constraints, see [14, section 5.7]:

$$\gcd(V, A) = 1 \text{ and } \frac{U}{V} \equiv B \pmod{A}$$

This is equivalent to finding a couple of polynomials $(U, V) \in R^2$ that verifies the equation $U - BV \equiv 0 \pmod{A}$ which means :

$$\begin{pmatrix} U & V \end{pmatrix} \begin{pmatrix} 1 \\ -B \end{pmatrix} \in \langle A \rangle$$

This is a relation with $n = 1$ variables, $r = 1$, $m = 2$ and $\mathcal{M} = \langle A \rangle$.

1.2.2 Bivariate Hermite-Padé Approximation

We suppose $R = \mathbb{K}[x, y]$. Let $F = (f_1, \dots, f_m)^\top \in R^m / \langle x^d, y^d \rangle$ for some d . We need to find a non-zero vector $P = (p_1, \dots, p_m) \in R^m$ that verifies under some degree constraints:

$$\begin{pmatrix} p_1 & \dots & p_m \end{pmatrix} \begin{pmatrix} f_1 \\ \vdots \\ f_m \end{pmatrix} = 0 \pmod{\langle x^d, y^d \rangle}$$

This is a relation with $n = 2$ variables and $\mathcal{M} = \langle x^d, y^d \rangle$.

1.2.3 Modular Inversion

We consider a polynomial ring R with n variables and an ideal I . For an element $f \in R$ we need to find an element g (if it exists) such that

$$fg = 1 \pmod{I}.$$

which is equivalent to finding the vector $(g, 1)$ that verifies

$$\begin{pmatrix} g & 1 \end{pmatrix} \begin{pmatrix} f \\ -1 \end{pmatrix} = 0 \pmod{I}$$

which is a relation modulo the ideal I .

1.2.4 Bivariate Interpolation

This problem is fundamental in numerical analysis. It consists in constructing a function which goes through a given set of points in the plane. So we consider having $(x_1, y_1), \dots, (x_D, y_D) \in \mathbb{K}^2$. So we aim to find a polynomial $Q(x, y) \in \mathbb{K}[x, y]$ such that:

$$Q(x_i, y_i) = 0 \quad \forall i \in \{1, \dots, D\}.$$

There exist some trivial polynomials verifying this, like for example:

$$M(x) = \prod_{i=1}^D (x - x_i) \text{ and } M' = y - L(x) \text{ while } L(x_i) = y_i.$$

Hence we denote by I the ideal $\langle M(x), y - L(x) \rangle$. Hereafter, for some cases, we need to find Q with small degree and balanced in x and y , for example

$$\deg_x(Q) \leq \sqrt{D} \text{ and } \deg_y(Q) \leq \sqrt{D},$$

verifying: $Q = Q_0(x) + Q_1(x)y + \dots + Q_l(x)y^l$. We obtain then :

$$\begin{aligned} Q(x_i, y_i) = 0 \quad \forall i &\iff \sum_{k=0}^l Q_k(x)y^k = 0 \pmod{I} \\ &\iff \begin{pmatrix} Q_0 & \dots & Q_l \end{pmatrix} \begin{pmatrix} 1 \\ L(x) \\ \vdots \\ L(x)^l \end{pmatrix} = 0 \pmod{\langle M(x) \rangle} \end{aligned}$$

This is a relation with $n = 2$ variables modulo $\mathcal{M} = \langle M(x) \rangle$.

□

Chapter 2

Preliminaries

Before passing to chapter 3 and chapter 4, which will represent the main of our work, we will first recall some definitions about polynomials ideal and modules. In fact, we will consider a multivariate polynomial ring $R = \mathbb{K}[x_1, \dots, x_n]$, with $n \geq 2$, over which most ideals and modules do not have a basis, that is, a set of R -linearly independent elements generating them. Yet we will study the fact that they always have a finite generating set. Adding some specific properties to such generating sets, we obtain a Gröbner basis depending on a specific monomial order. We will give definitions for both particular (ideals) and general (modules) cases with some useful examples that may help in the comprehension.

2.1 Polynomials, Ideals, Modules

Definition 2.1.1. An *ideal* in a commutative ring A is an additive subgroup I such that if $a \in A$ and $s \in I$, then $as \in I$.

An ideal I is said to be generated by a subset $S \subset A$ if every element $t \in I$ can be written in the form

$$t = \sum_i a_i s_i \text{ with } a_i \in A \text{ and } s_i \in S.$$

We shall write (S) for the ideal generated by a subset $S \subset A$; if S consists of finitely many elements s_1, \dots, s_n , we usually write (s_1, \dots, s_n) in place of (S) .

By convention, an ideal generated by the empty set is 0 . An ideal is *principal* if it can be generated by one element.

We establish some terminology about polynomials and we consider a field \mathbb{K} .

Definition 2.1.2. We denote by $R = \mathbb{K}[x_1, \dots, x_n]$ the polynomial ring with coefficients in \mathbb{K} . An element in this ring is a *polynomial*.

Definition 2.1.3. A *monomial* is a polynomial of the form $x_1^{\alpha_1} \dots x_n^{\alpha_n}$ with $\alpha_i \in \mathbb{N}$ for all $i \in [1, n]$. We denote it as well by x^α with $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$. The total degree of x^α is $|\alpha| = \alpha_1 + \dots + \alpha_n$.

By convention, the element 1 is regarded as the empty product: it is the unique monomial of total degree 0.

A *term* is a scalar times a monomial and every polynomial P can be written uniquely as a finite sum of nonzero terms:

$$P = \sum_{\alpha} a_{\alpha} x^{\alpha}$$

with $a_{\alpha} \in \mathbb{K}$.

In this case, the total degree of a nonzero multivariate polynomial P is:

$$\deg(P) = \sup\{|\alpha| / a_{\alpha} \neq 0\}.$$

Let $I \subset \mathbb{K}[x]$ be an ideal in a univariate polynomial ring, and $f \in I$ be an element of lowest degree then the Euclid's algorithm for dividing polynomials shows that f divides every element of I . Thus $\mathbb{K}[x]$ is a *principal ideal domain*, a domain in which every ideal can be generated by one element, see [15]. We have to mention that the situation in the multivariate case is more complex.

Example 2.1.1. Let $I = \langle x, y \rangle \subset \mathbb{K}[x, y]$ be an ideal generated by x and y . If there exists a nonzero generator $f \in \mathbb{K}[x, y]$ such that $I = \langle f \rangle$ then both x and y must be multiples of f , which implies that $f \in \mathbb{K}$; as a consequence we obtain that $I = \mathbb{K}[x, y]$, which is not the case. Hence I is not principle.

We suppose then that there exists a generating set $\{f_1, \dots, f_s\}$ of I consisting of $s \geq 2$ polynomials. Then, f_1 and f_2 are not $\mathbb{K}[x, y]$ -linearly independent, since a nontrivial combination $\alpha f_1 + \beta f_2 = 0$ is given by $\alpha = f_2$ and $\beta = -f_1$.

We can say that if an ideal $I \in R$ is not principle, then it does not have a basis (generating set which elements are R -linearly independent). Here is another example encountered in interpolation problems such as the one in the subsection 1.2.4.

Example 2.1.2. Let $\{(x_j, y_{j,1}, \dots, y_{j,r}) \in \mathbb{K}^{r+1}, 1 \leq j \leq D\}$, be a set of points with x_1, \dots, x_D pairwise distinct. Then,

$$I = \{Q \in \mathbb{K}[x, y_1, \dots, y_r] \mid Q(x_j, y_{j,1}, \dots, y_{j,r}) = 0 \text{ for all } 1 \leq j \leq D\}$$

is an ideal. Let $M(x) = (x - x_1) \dots (x - x_D)$, and for each $k \in \{1, \dots, r\}$ let $L_k(x)$ be in $\mathbb{K}[x]$ such that $L_k(x_j) = y_{j,k}$ for $1 \leq j \leq D$. Then,

$$I = \langle M(x), y_1 - L_1(x), \dots, y_r - L_r(x) \rangle.$$

As in the previous example, one can easily prove that I is not principal, and that it does not have a basis. Hereafter, we will see that every ideal in R has a finite generating set.

For modules, we start by some basic definitions:

Definition 2.1.4. For any ring A , an A -module M is an abelian group with an action of A characterized by the following map:

$$\begin{aligned} A \times M &\longrightarrow M \\ (r, m) &\longrightarrow rm \end{aligned}$$

such that it satisfies for all $r, s \in A$ and $m, n \in M$ the associativity, the distributivity and the identity, see [15]

We want to consider modules over the multivariate polynomial ring R (as mentioned above). Before going more into detail about module bases (Gröbner bases), we need to mention that R is not a principal ideal domain as soon as $n \geq 2$, and as a consequence, there will exist some R -modules that don't have any bases that consists of R -linearly independent elements. But we will learn from the next section that submodules of R^m , for any $m \in \mathbb{N}$, always have a generating set. So in the next section we represent the notion of Gröbner bases which is fundamentally relying on a chosen *monomial order*. We first give definitions for $m = 1$, where the R -submodules of R are exactly the ideals of R then we develop ideas to obtain definitions for $m > 1$.

2.2 Gröbner Bases

2.2.1 Introduction

The method of Gröbner bases is a solid technique for solving problems in commutative algebra (polynomial ideal theory, algebraic geometry) and very attractive tool in computer algebra. Gröbner bases provide a uniform approach for solving problems that can be expressed in terms of systems of multivariate polynomial equations. It happens that many practical problems, e.g. in operational research (graph theory), can be transformed into sets of polynomial equations, thus solved using Gröbner bases method as in [16].

2.2.2 Ideals

Monomial order - Monomial ideal

If we wish to order the monomials of a polynomial, what properties should this order have to obtain the leading term as the greatest term with respect to this order? It is important that a monomial $x^\alpha \neq 1$ be chosen as a leading term before the monomial 1, otherwise the reductions will not end. Moreover, the terms of a polynomial should not change order upon multiplying by a monomial. These requirements lead to the following definition:

Definition 2.2.1. A total order $>$ on the monomials of $R = \mathbb{K}[x_1, \dots, x_n]$ is called a monomial order if:

1. $x^\alpha > 1$, for every monomial $x^\alpha \neq 1$
2. If $x^\alpha > x^\beta$, then for every monomial x^γ , $x^{\alpha+\gamma} > x^{\beta+\gamma}$.

For the next definition, one can verify [17] for detailed information.

Definition 2.2.2. We give some specific orders:

- The *lexicographic order*: It is the order $>_{lex}$ such that $x^\alpha >_{lex} x^\beta$ iff the first non-zero entry of the vector $\alpha - \beta$ is positive.
- The *graded lexicographic order*: It is the order $>_{deglex}$ such that $x^\alpha >_{deglex} x^\beta$ iff $\deg x^\alpha > \deg x^\beta$, or $\deg x^\alpha = \deg x^\beta$ and the first non-zero entry of $\alpha - \beta$ is positive.
- The *graded reverse lexicographic order*: It is the order $>_{degrevlex}$ such that $x^\alpha >_{degrevlex} x^\beta$ iff $\deg x^\alpha > \deg x^\beta$, or $\deg x^\alpha = \deg x^\beta$ and the last non-zero entry of $\alpha - \beta$ is negative.

In each case above, we have $x_1 > x_2 > \dots > x_n$.

For $R = \mathbb{K}[x_1, x_2, x_3]$, the graded reverse lexicographic order satisfies

$$x_1^2 > x_1x_2 > x_2^2 > x_1x_3 > x_2x_3 > x_3^2,$$

while the graded lexicographic order has

$$x_1^2 > x_1x_2 > x_1x_3 > x_2^2 > x_2x_3 > x_3^2.$$

We have a unique difference between these two orders, which is that the middle two monomials have changed order. Hence, it is important to know that the properties of Gröbner bases using these two orders are completely different. As a first glimpse of the difference, notice that the last variable x_3 divides the last three monomials in the reverse lexicographic case, whereas the last three monomials in the graded lexicographic order don't impact x_1 . This will imply that the properties (and also the size) of the corresponding Gröbner bases will be different. (The following results can be checked from [16] and [18])

Definition 2.2.3. (Initial term) Given a monomial order $>$ on R , if $f = c_1x^{\alpha_1} + \dots + c_sx^{\alpha_s}$, where $c_i \neq 0$ are constants, and $x^{\alpha_1} > \dots > x^{\alpha_s}$, the initial term, or leading term of f is $in_{>}(f) = c_1x^{\alpha_1}$. For convenience, we also define $in(0) = 0$.

If the monomial order is understood, we abbreviate the notation to $in(f)$.

Definition 2.2.4. (Initial ideal) For an ideal $I \subset R$ and a monomial order $>$ on R , the monomial ideal generated by $\{in(f) \mid f \in I\}$ is the ideal of initial terms denoted by $in_{>}(I)$.

Definition 2.2.5. (Gröbner bases) For an ideal $I \subset R$ and a monomial order $>$ on R , a subset $G = \{g_1, \dots, g_s\}$ of I is called a Gröbner basis of I with respect to $>$, if the monomial ideal $in_{>}(I)$ is generated by $\{in(g_1), \dots, in(g_s)\}$.

A Gröbner basis G is called minimal if the leading terms of the elements in G minimally generate $in(I)$: that is, $in(g_i)$ never divides $in(g_j)$, as long as $i \neq j$. The Gröbner basis G is called reduced if in addition, no term in the polynomial g_i is divisible by $in(g_j)$, whenever $i \neq j$, and that each g_i is monic: the leading monomial $in(g_i)$ has coefficient one.

Hence, the solution set of $f_1 = \dots = f_r = 0$ is empty if $1 \in I = (f_1, \dots, f_r)$.

This result can be used to show that Gröbner bases exist.

Lemma 2.2.1. Let S be a set of monomials in $\mathbb{K}[x_1, \dots, x_n]$. If x^α divides x^β with respect to an order $x^\alpha \leq x^\beta$, then there are only finitely many minimal elements of S . In particular, every monomial ideal in $\mathbb{K}[x_1, \dots, x_n]$ is finitely generated (as shown in [19, lemma 2.20]).

This is “**Gordan’s Lemma**” and it is often called “**Dickson’s lemma**”.

Corollary 2.2.1. A monomial order $>$ is a well ordering on the set of monomials. i.e. every set S of monomials has a minimal element with respect to $>$.

Corollary 2.2.2. For every ideal $I \subset R$ and every monomial order $>$, the ideal $in_{>}(I)$ is finitely generated. In particular, every ideal has a (finite) Gröbner basis.

Corollary 2.2.3. If $J \subset I \subset R$ are ideals, and $>$ is a monomial order, and if $in(I) = in(J)$, then $I = J$.

This next result is important for applications. In fact, instead of showing that a set G generates I , it is easier to prove that it is its Gröbner basis.

Corollary 2.2.4. If $G = \{g_1, \dots, g_s\}$ is a Gröbner basis of the ideal I , then G generates I .

Corollary 2.2.5. (Hilbert bases theorem) Let $I \subset R = \mathbb{K}[x_1, \dots, x_n]$ be an ideal. Then I is finitely generated.

Proposition 2.2.1. Let G be a Gröbner basis with respect to the monomial order $<$. A basis of the \mathbb{K} -vector space R/I is given by the monomials that don’t belong to the monomial ideal $in_{>}(G)$ generated by $\{in_{>}(g) \mid g \in G\}$

Algorithms for computing a Gröbner basis

The first applications of Gröbner bases, and one of Buchberger’s original motivations for defining it, is to decide whether a specific polynomial $f \in R$ is in an ideal I .

To study the membership problem, we first need to find the remainder of f (modulo a given Gröbner basis) by using the division algorithm.

Definition 2.2.6. (Remainder) Let $G = \{g_1, \dots, g_s\}$ be a set of non-zero polynomials. Define the remainder, \bar{f}^G , of $f \in R$ by G by the formula:

$$\bar{f}^G = \begin{cases} \overline{f - ag_i}^G, & \text{if } i \text{ is least such that } ag_i = in(h); \\ \overline{f - in(f)}^G, & \text{otherwise, if } h \neq 0; \\ 0, & \text{if } f = 0. \end{cases}$$

In the first case, we choose the least i such that $in(g_i)$ divides $in(f)$ (if there are several).

If G is a Gröbner basis, then the choice of i does not affect the final answer.

Proposition 2.2.2. (Ideal membership) Let $I \subset R$ be an ideal, and let G be a finite subset of I . Then

1. G is a Gröbner basis of I if and only if for every $f \in I$, $\bar{f}^G = 0$.
2. If G is a Gröbner basis of I , then two polynomials $f_1, f_2 \in R$ are equal modulo I if and only if $\bar{f}_1^G = \bar{f}_2^G$.

Definition 2.2.7. Given two non-zero polynomials g and h , where $\text{in}(g) = ax^\alpha$ and $\text{in}(h) = bx^\beta$, we define the s -polynomial $S(g, h)$ by $S(g, h) = bx^\lambda g - ax^\gamma h$, where $x^\lambda x^\alpha = x^\gamma x^\beta$, and the $g.c.d.$ $(x^\lambda, x^\gamma) = 1$.

This way of uncovering new leading terms is sufficient to find all the possible new ones, and hence a Gröbner basis. This result of Buchberger leads to his algorithm for computing a Gröbner basis.

Proposition 2.2.3. (Buchberger) Let $I \subset R$ be an ideal, and let $G \subset I$ be a finite subset, consisting of non-zero polynomials. Then

G is a Gröbner basis if and only if for every pair of elements $g, f \in G$, $\overline{S(g, f)}^G = 0$.

So if we want to compute a Gröbner basis, we start by computing the remainder of the s -polynomial of every couple of polynomials. If we get a zero remainder, we continue to the next couple. Otherwise, if we get a non-zero remainder, then we have a new leading term. So we add this element to our growing Gröbner basis G . This process must end because the initial ideal is finitely generated.

Algorithm 2.2.1. Buchberger's algorithm

input: A set $\{f_1, \dots, f_r\} \subset R$.

output: a Gröbner basis G of the ideal generated by $\{f_1, \dots, f_r\}$.

begin

$G := \{f_1, \dots, f_r\}$

$Pairs := \{(f_i, f_j) \mid 1 \leq i < j \leq r\}$

while $Pairs \neq \emptyset$ **do**

$(g_i, g_j) :=$ remove an element from $Pairs$

$s := S(g_i, g_j)$

$h := \bar{s}^G$

if $h \neq 0$ **then**

$Pairs := Pairs \cup \{(h, g) \mid g \in G\}$.

$G := G \cup \{h\}$

return G

end.

2.2.3 Modules

Now we consider the general case of R -submodules of R^m for $m \geq 1$. Generally, as what is mentioned previously, such submodules don't have a basis. Yet, it follows from the Hilbert bases theorem that they are finitely generated. So we will compute generating sets for submodules of R^m .

Monomials modules

For $i \in \{1, \dots, m\}$ we denote by c_i the coordinate vector $(0, \dots, 0, 1, 0, \dots, 0) \in R^m$ with 1 at index i , which form a basis of the free R -module R^m . Hence, a **monomial** in R^m is an element of the form $X = x^\alpha c_i$ for some $i \in \{1, \dots, m\}$. We will say that such X involves the bases element c_i . A **monomial submodule** of R^m is a submodule generated by elements of this form.

A **term** in R is a monomial multiplied by a scalar. Since the monomials form a vector space bases for R^m , every element $f \in R^m$ is uniquely expressible as a finite sum of nonzero terms involving distinct monomials which we call the terms of f [15]. We will call the monomials appearing in these terms, the monomials of f .

We have to mention that in our theory we will not consider the distinction between monomials and terms since \mathbb{K} is a field.

If u, v are monomials of R , $a, b \in \mathbb{K}$, and $b \neq 0$, then we say the term auc_i is divisible by the term bvc_j if $i = j$ and u divisible by v in R .

We discuss now the module membership. Let $M \subset R^m$ a submodule generated by the monomials X_1, \dots, X_t : A monomial X belongs to M iff it is divisible by at least one of the X_i . More generally, the membership problem is easy to solve for a monomial submodule: any element in R^m belongs to M iff each of its monomials belongs to M .

Let's consider a set of monomial generators for M . To get what is called the unique minimal set of monomials generating M we may remove from the set any element that are divisible by others.

Monomial orders and initial modules

Definition 2.2.8. Let's consider a pair of monomials f and $g \in R^m$ and $h \neq 1$ a monomial in R . A **monomial order** on R^m is a total order $<$ on the set of monomials in R^m such that,

$$f < g \implies f < hf < hg.$$

Now we give definitions of monomial orders over modules : **Term-Over-Position** and **Position-Over-Term**. They are two natural extensions of monomial orders over the polynomial ring R to monomial orders on R^m . We also include a shifted variant of term-over-position orders.

Definition 2.2.9. We start with $<$ to be a monomial order on R . Consider the module R^m with its canonical basis $\{c_1, \dots, c_m\}$, and let S_1, \dots, S_m, f, g be monomials in R and $S = (S_1, \dots, S_m)$. Then, $<$ induces the following monomial orders on R^m :

- $<_{POT}$ order: $fc_j <_{pot} gc_k \iff j < k$ or $j = k$ and $f < g$;
- $<_{TOP}$ order: $fc_j <_{top} gc_k \iff f < g$ or $f = g$ and $j < k$;
- Shifted $<_{TOP}$ order: $fc_j <_{S-top} gc_k \iff fS_j < gS_k$ or $fS_j = gS_k$ and $j < k$.

Example 2.2.1. In this exemple, we consider $r = m = 2$. For any monomial order $<$ on $R = \mathbb{K}[x_1, x_2]$ and any monomials f, g of R , we have $(f, 0) <_{pot} (0, g)$ and $(f, 0) <_{top} (0, f)$. Furthermore, $(f, 0) <_{pot} (g, 0)$ and $(f, 0) <_{top} (g, 0)$ are both equivalent to $f < g$.

For $<_{top}^{lex}$ we have:

$$(0, x_1) \prec_{\text{top}}^{\text{lex}} (x_1^2 x_3^3, 0) \prec_{\text{top}}^{\text{lex}} (0, x_1^3 x_2^2) \prec_{\text{top}}^{\text{lex}} (x_1^3 x_2^5, 0) \prec_{\text{top}}^{\text{lex}} (0, x_1^3 x_2^5),$$

and for $\prec_{\text{pot}}^{\text{lex}}$ we have:

$$(x_1^2 x_2^3, 0) \prec_{\text{pot}}^{\text{lex}} (x_1^3 x_2^5, 0) \prec_{\text{pot}}^{\text{lex}} (0, x_1) \prec_{\text{pot}}^{\text{lex}} (0, x_1^3 x_2^2) \prec_{\text{pot}}^{\text{lex}} (0, x_1^3 x_2^5).$$

□

Initial module

Let f be an element of R^m . We denote by $\text{in}_>(f)$ the initial term of f , which is the term of f whose monomial is the greatest with respect to a given monomial order $<$. We extend this notion to any subset $\mathcal{F} \subset R^m$ of polynomials:

$$\text{in}_>(\mathcal{F}) = \{\text{in}_>(f), f \in \mathcal{F}\}.$$

We have the same thing for a module \mathcal{M} :

$$\text{in}_>(\mathcal{M}) = \{\text{in}_>(f), f \in \mathcal{M}\}.$$

For example, the $<_{\text{lex}}$ -initial term of $f = 3x_1^3 x_2^5 + 5x_1^3 x_2^2 + 2x_1^2 x_2^3 \in K[x_1, x_2]$ is $\text{in}_{<_{\text{lex}}}(f) = 3x_1^3 x_2^5$.

The following theorem is a generalization of proposition 2.2.1.

Theorem 2.2.1. (Macaulay) *Let $R = \mathbb{K}[x_1, \dots, x_n]$, $m \in \mathbb{N}^*$ and \mathcal{M} be an R -submodule of R^m . For any monomial order $<$ on R^m , the set \mathcal{E} of all monomials that don't belong to $\text{in}_>(\mathcal{M})$ forms a basis of R^m/\mathcal{M} as a \mathbb{K} -vector space*

We can find a proof in [15, Section 15.2]

Example 2.2.2. Following the notation of Example 2.1.1, we show that

$$I = \{Q \in \mathbb{K}[x, y_1, \dots, y_r] \mid Q(x_j, y_{j,1}, \dots, y_{j,r}) = 0 \text{ for all } 1 \leq j \leq D\} = \langle M(x), y_1 - L_1(x), \dots, y_r - L_r(x) \rangle$$

is such that the quotient ring $\mathcal{M} = \mathbb{K}[x, y_1, \dots, y_r]/I$ has a finite dimension D as \mathbb{K} -vector space, and more precisely, that it admits $\{1, x, \dots, x^{D-1}\}$ as a vector space basis.

First, the monomials $1, x, \dots, x^{D-1}$ are \mathbb{K} -linearly independent in \mathcal{M} . In fact, let us consider a linear combination $p(x) = p_0 + p_1 x + \dots + p_{D-1} x^{D-1}$ for some $p_0, \dots, p_{D-1} \in \mathbb{K}$. If this combination is zero in the quotient, this means that $p(x) \in I$, and therefore $p(x_1) = \dots = p(x_D) = 0$. Thus $p(x)$ is a univariate polynomial of degree less than D which has at least D pairwise distinct roots: it must be zero. Hence $p_0 = \dots = p_{D-1} = 0$.

Then, the conclusion follows from the remark that for any $f \in \mathbb{K}[x, y_1, \dots, y_r]$, we have $f(x, y_1, \dots, y_r) = f(x, L_1, \dots, L_r) + g$ for some $g \in I$. Considering the univariate polynomial $p(x)$ which is the remainder in the (univariate) division of $f(x, L_1, \dots, L_r)$ by $M(x)$, we obtain that the image of f in the quotient \mathcal{M} is the same as that of p , which is a \mathbb{K} -linear combination of the monomials $1, x, \dots, x_{D-1}$.

Gröbner bases

As above, let $R = \mathbb{K}[x_1, \dots, x_n]$, $m \in \mathbb{N}^*$ and \mathcal{M} be an R -submodule of R^m . Based on *Theorem 2.2.1*, any polynomial $f \in R^m$ can be uniquely written as $f = g + h$, where $g \in \mathcal{M}$ and h is a \mathbb{K} -linear combination of monomials not in $\text{in}_>(\mathcal{M})$. This is a generalized case of what we've already explained in definition 2.2.6.

Also, there exists an algorithm that undergoes the multivariate division with remainder, relying on a specific monomial order. Given $f \in R^m$ and a generating set $\{f_1, \dots, f_s\}$ of the submodule \mathcal{M} , this algorithm outputs the quotients $\{q_1, \dots, q_s\} \in R^m$ and the remainder h where none of its terms belongs to $\langle \text{in}_>(f_1), \dots, \text{in}_>(f_s) \rangle$. So f can be written as $f = q_1 f_1 + \dots + q_s f_s + h$. For more details, one may refer to [15, Section 15.3]

We have to mention that the remainder h as defined above is not always unique. This leads us to a specific type of generating set of \mathcal{M} , called Gröbner basis, that are the generalization of ideals case.

Definition 2.2.10. (Gröbner bases) Let $>$ be a monomial order on R^m and let \mathcal{M} be an R -submodule of R^m . A generating set $\{f_1, \dots, f_s\}$ of \mathcal{M} is said to be a Gröbner basis of \mathcal{M} with respect to $>$, if the initial module of \mathcal{M} is generated by $\{\text{in}_>(f_1), \dots, \text{in}_>(f_s)\}$. Hence we can write:

$$\{f_1, \dots, f_s\} \subset \mathcal{M} \text{ is a Gröbner basis of } \mathcal{M} \text{ w.r.t } > \iff \text{in}_>(\mathcal{M}) = \langle \text{in}_>(f_1), \dots, \text{in}_>(f_s) \rangle$$

The next result will be useful to prove that two sets of polynomials generate the same module, by only comparing their initial modules. This also prove the importance of reducing the study of a module to the study of its initial module.

Lemma 2.2.2. If $\mathcal{N} \subseteq \mathcal{M} \subseteq R^m$ are two submodules verifying $\text{in}_>(\mathcal{N}) = \text{in}_>(\mathcal{M})$, the $\mathcal{N} = \mathcal{M}$.

To find the proof, one can check [15, Lemma 15.5].

As a consequence of what is already said, we can say that:

Corollary 2.2.6. Any submodule \mathcal{M} of R^m has a Gröbner basis w.r.t a monomial order $>$.

In fact, the initial module of \mathcal{M} is finitely generated and it is written as $\text{in}_>(\mathcal{M}) = \langle g_1, \dots, g_s \rangle$, with $\{g_1, \dots, g_s\}$ is a set of monomials in $\text{in}_>(\mathcal{M})$. On the other hand, there exists a set of elements $\{f_1, \dots, f_s\} \subset \mathcal{M}$ such that $\text{in}_>(f_i) = g_i \forall i \in \{1, \dots, s\}$, and therefore $\text{in}_>(\mathcal{M}) = \langle g_1, \dots, g_s \rangle \subseteq \text{in}_>(\langle f_1, \dots, f_s \rangle) \subseteq \text{in}_>(\mathcal{M})$ which implies $\text{in}_>(\mathcal{M}) = \text{in}_>(\langle f_1, \dots, f_s \rangle)$ and then, by the previous lemma, $\mathcal{M} = \langle f_1, \dots, f_s \rangle$.

Corollary 2.2.7. A set of elements $\{f_1, \dots, f_s\} \subset \mathcal{M}$ is a Gröbner basis of \mathcal{M} if and only if $\{\text{in}_>(f_1), \dots, \text{in}_>(f_s)\}$ generates $\text{in}_>(\mathcal{M})$.

One can check [15, Theorem 15.8] to study another Gröbner bases test called Buchberger's criterion.

Considering then a Gröbner basis of a submodule \mathcal{M} , we can transform it into a minimal one by removing elements whose initial term is divisible by the initial term of another element, *i.e.*:

Definition 2.2.11. $\{f_1, \dots, f_s\} \subset R^m$ is a minimal Gröbner basis of \mathcal{M} w.r.t a monomial order $>$ if $in_{>}(f_i)$ is monic for all i , and for all $i \neq j$, $in_{>}(f_i)$ does not divide $in_{>}(f_j)$.

There is a specific minimal Gröbner basis of \mathcal{M} w.r.t to a monomial order $>$ called the *reduced Gröbner basis*:

Definition 2.2.12. $\{f_1, \dots, f_s\} \subset R^m$ is a reduced Gröbner basis of \mathcal{M} if it satisfies:

1. for $1 \leq i \leq s$, $in_{>}(f_i)$ is monic;
2. for $1 \leq i \leq s$, $in_{>}(f_i)$ does not divide any term of f_j for $j \neq i$.

Using these properties, we can easily transform any Gröbner basis of a submodule \mathcal{M} into a reduced one.

Example 2.2.3. As in Examples 2.1.1 and 2.2.2, consider the ideal

$$I = \{Q \in \mathbb{K}[x, y_1, \dots, y_r] \mid Q(x_j, y_{j,1}, \dots, y_{j,r}) = 0 \text{ for all } 1 \leq j \leq D\}$$

of $\mathbb{K}[x, y_1, \dots, y_r]$, and let $M(x) = (x - x_1) \dots (x - x_D)$. $L_k(x) \in \mathbb{K}[x]$ is such that $L_k(x_j) = y_{j,k}$ for $1 \leq j \leq D$ and $k \in \{1, \dots, r\}$. Furthermore, let $<_{lex}$ stand for the lexicographic order on $\mathbb{K}[x, y_1, \dots, y_r]$, where the variables are ordered arbitrarily with $x <_{lex} y_j$ for all j . Then,

$$\{M(x), y_1 - L_1(x), \dots, y_r - L_r(x)\}$$

is the reduced $<_{lex}$ -Gröbner basis of I .

Lemma 2.2.3. Let \mathcal{M} be a submodule of R^m , $<$ be a monomial module over R^m and $G = \{f_1, \dots, f_s\} \subseteq \mathcal{M}$. Then:

G is a Gröbner basis of \mathcal{M} w.r.t $>$ $\iff \forall f \in \mathcal{M}, \exists g_1, \dots, g_s \in R$ s.t. $f = g_1 f_1 + \dots + g_s f_s$
and $in_{>}(f) = \max \{in_{>}(g_i f_i), 1 \leq i \leq s\}$.

We mention that one of the motivations of studying Gröbner bases is the advantages we get regarding computations in the quotient R^m/\mathcal{M} or equivalently the computation of the remainder of an element $f \in R^m$ modulo \mathcal{M} . This idea will be generalized in the next chapter. In the next lemma we summarize properties about division with remainder

Lemma 2.2.4. Let \mathcal{M} be a submodule of R^m and $>$ a monomial module over R^m . Let $G = \{f_1, \dots, f_s\} \subseteq \mathcal{M}$ be a Gröbner basis of \mathcal{M} w.r.t $>$. For any $f \in R^m$, the *algorithm of multivariate division with remainder* computes $g_1, \dots, g_s \in R$ and $h \in R^m$ such that:

$$f = g_1 f_1 + \dots + g_s f_s + h, \text{ with } h \text{ is the remainder of } f \text{ modulo } \mathcal{M} \text{ having no monomial in } in_{>}(\mathcal{M}).$$

2.3 Algebras of Dimension 0

We discuss in this section the following idea: studying the quotient R/I leads to solving systems of polynomial equations that generate an ideal $I \subset R = \mathbb{K}[x_1, \dots, x_n]$. This also helps to find geometrical facts of the solutions: number of the roots of the system, finding them, discussing their multiplicity, ... [19] Throughout this section, we assume that \mathbb{K} is algebraically closed.

2.3.1 Some Geometry

One can check [16] for more details.

Definition 2.3.1. Given any set S of polynomials in R , we denote by $V(S)$ the zero set, or variety of S :

$$V(S) = \{(p_1, \dots, p_n) \in \mathbb{K}^n \mid f(p_1, \dots, p_n) = 0 \text{ for all } f \in S\}.$$

For example, if $I = (x_1 + x_2 - 1, x_1 - x_2 + 2) \subset \mathbb{C}[x_1, x_2]$, then

$$V(I) = V(\{x_1 + x_2 - 1, x_1 - x_2 + 2\}) = \{(-1/2, 3/2)\} \in \mathbb{C}^2.$$

Notice that if I is the ideal generated by S , then $V(S) = V(I)$.

We denote by $A^n(\mathbb{K})$, or simply A^n if \mathbb{K} is understood, an affine n -space over \mathbb{K} . We call the subsets $V(I)$ of A^n , the **algebraic sets**.

Definition 2.3.2. Given a subset $X \subset A^n$, define the ideal of X to be

$$I(X) = \{f \in R \mid f(p) = 0 \text{ for all } p \in X\}.$$

We can notice that, given an algebraic set X , it is easy to see that $V(I(X)) = X$. If X is not an algebraic set, then $\bar{X} := V(I(X))$ strictly contains X . We call \bar{X} the Zariski-closure of X . It is not always true that $I(V(J)) = J$. For example, $V(x^3) = V(x^2) = V(x)$ and $I(V(x^2)) = (x)$. Hilbert's Nullstellensatz describes precisely when equality does hold:

Theorem 2.3.1. (Hilbert's Nullstellensatz) If $J \subset R$ is an ideal, then

$$I(V(J)) = \{f \in R \mid f^N \in J, \text{ for some sufficiently large } N\}.$$

In particular, $V(J) = \emptyset$ if and only if $J = (1)$.

2.3.2 0-Dimensional Ideals

We mention that the variety $V(I)$ of an ideal $I \subset R$ is of dimension 0, if it is a non-empty, finite set. In this case we can say that I is 0-dimensional (of dimension 0) [19].

Theorem 2.3.2. We have equivalence between the following conditions, for any ideal $I \neq R$:

1. I is 0-dimensional.
2. For any $i \in \{1, \dots, n\}$, $\mathbb{K}[x_i] \cap I \neq 0$.

3. The dimension of $\mathcal{A} = R/I$, seen as a \mathbb{K} -vector space, is finite.

One can find the proof in [19, Theorem 4.3]

Remark 2.3.1. According to proposition 1.2.1, the vector space \mathcal{A} always has a monomial bases.

In all what follows, we consider by I a 0-dimensional ideal of $R = \mathbb{K}[x_1, \dots, x_n]$, \mathcal{A} the \mathbb{K} -vector space R/I , D its dimension, $(x^\alpha)_{\alpha \in E}$ (where $E \subset \mathbb{N}^n$ of dimension D) a monomial bases of \mathcal{A} , $V(I)$ the algebraic variety $\{\mathcal{C}_1, \dots, \mathcal{C}_d\}$ defined by I . For every $i \in \{1, \dots, d\}$, $\mathcal{C}_i = (\mathcal{C}_{i,1}, \dots, \mathcal{C}_{i,n}) \in \bar{\mathbb{K}}^n$

Based on what we've already mentioned, every x^α is associated with a multi-index α . Hence, there exists a one-to-one function between monomials of R and \mathbb{N}^n . In case $n = 2$, the following figure represents an example of a basis $(x^\alpha)_{\alpha \in E}$. The monomials represented over the grey area (in figure 2.1) can be reduced, modulo the ideal I , to a linear combination of x^α for $\alpha \in E$.

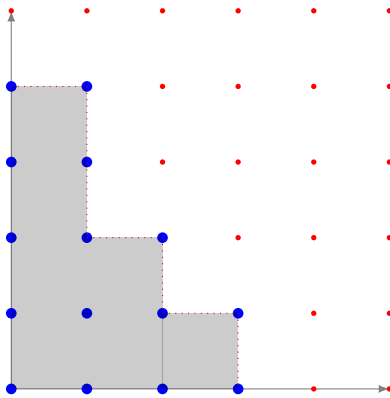


Figure 2.1: Monomial basis of a quotient algebra

Example 2.3.1. Let $f_1(x_1, x_2) = 13x_1^2 + 8x_1x_2 + 4x_2^2 - 8x_1 - 8x_2 + 2$ and $f_2 = x_1^2 + x_1x_2 - x_1 - 1/6$. $I = \langle f_1, f_2 \rangle$ is a 0-dimensional ideal since it is easy to prove that the vector space $\mathcal{M} = \mathbb{K}[x_1, x_2]/I$ is of dimension 4 and of basis $\langle 1, x_1, x_2, x_1x_2 \rangle$.

Finally we give a proposition before passing to the next chapter.

Proposition 2.3.1. Let G be a Gröbner bases of an ideal I with respect to a monomial order $<$. The ideal I is 0-dimensional if and only if for every $i \in \{1, \dots, n\}$, there exist $(g_i, m_i) \in G \times \mathbb{N}^*$ such that $in_{>}(g_i) = x_i^{m_i}$.

We can now move on to a new chapter after having a look at the tools needed to understand the last two. In the next chapter we will get into the main problem that we did our studies on, then we will give a quick idea about a previous work done by Henry O'KEEFFE and Patrick FITZPATRICK before moving on to the last chapter **Contribution and Perspectives**.

Main problem and Previous Work

3.1 Algorithmic Problem

As we have already mentioned in the introduction, our goal is to design algorithms that improve the known complexity bounds. Moreover, existing algorithms for multivariate relations follow an iterative approach, similar to the ones used for univariate relations. Hence, it is reasonable to get inspired by the divide and conquer techniques, that have added great benefits (in complexity terms) to univariate cases.

Particular attention will be paid to the particularities of the output of the algorithms designed, and to the speed of the algorithm according to these particularities.

First of all, getting back to the multivariate relations in chapter 1, the set

$$\mathcal{R}(\mathcal{M}, F) = \{p \in R^{1 \times m} \mid pF \in \mathcal{M}\},$$

which is the kernel of the module morphism

$$\begin{aligned} \varphi_{\mathcal{M}, f} : \quad R^m &\longrightarrow R^r / \mathcal{M} \\ (p_1, \dots, p_m) &\longmapsto p_1 f_1 + \dots + p_m f_m \end{aligned}$$

consists of relations between the f_i 's. Hence, it is a submodule of the R -module R^m .

For this module, some applications require only the computation of a single relation satisfying some degree constraints while others require to compute a Gröbner basis.

While these two outputs are computed with a similar cost in the univariate case, it is conceivable that a difference in complexity may appear in the multivariable case.

Example 3.1.1. We consider a multivariate polynomial ring $\mathbb{K}[x, y]$ with respect to the graded reverse lexicographic monomial order $>$, that satisfies $x^2y > xy^2 > x^2 > xy > y^2 > x > y$ and an ideal $I = \langle x^3, y^3 \rangle \subset \mathbb{K}[x, y]$.

We suppose having two polynomials $u = u_0 + u_1y + u_2x + u_3y^2 + u_4xy + u_5x^2$ and $v = v_0 + v_1y + v_2x + v_3y^2 + v_4xy + v_5x^2 \in \mathbb{K}[x, y]/I$.

Purpose: Finding two polynomials $f = f_0 + f_1y + f_2x + f_3y^2 + f_4xy + f_5x^2$ and $g = g_0 + g_1y + g_2x + g_3y^2 + g_4xy + g_5x^2 \in \mathbb{K}[x, y]/I$, satisfying $fu + vg \equiv 0 \pmod{I}$.

Developing the equation we obtain:

$$\begin{aligned}
fu + vg &= (f_0u_0 + g_0v_0) + \\
& y(f_1u_0 + f_0u_1 + g_1v_0 + g_0v_1) + \\
& x(f_0u_2 + f_2u_0 + g_2v_0 + g_0v_2) + \\
& y^2(f_0u_3 + f_3u_0 + g_0v_3 + g_3v_0 + u_1f_1 + v_1g_1) + \\
& xy(f_0u_4 + f_2u_1 + f_1u_2 + u_0f_4 + g_0v_4 + g_2v_1 + g_1v_2 + v_0g_4) + \\
& x^2(f_0u_5 + f_2u_2 + f_5u_0 + u_0f_4 + g_0v_5 + g_2v_2 + g_5v_0) + \\
& y^2x(f_1u_4 + f_2u_3 + f_3u_2 + u_1f_4 + g_1v_4 + g_2v_3 + g_3v_2 + v_1g_4) + \\
& x^2y(f_1u_5 + f_2u_4 + f_4u_2 + u_1f_5 + g_1v_5 + g_2v_4 + g_4v_2 + v_1g_5) \equiv 0 \pmod I
\end{aligned}$$

This is equivalent to the matrix writing:

$$\underbrace{\begin{pmatrix}
u_0 & 0 & 0 & 0 & 0 & 0 & v_0 & 0 & 0 & 0 & 0 & 0 \\
u_1 & u_0 & 0 & 0 & 0 & 0 & v_1 & v_0 & 0 & 0 & 0 & 0 \\
u_2 & 0 & u_0 & 0 & 0 & 0 & v_2 & 0 & v_0 & 0 & 0 & 0 \\
u_3 & u_1 & 0 & u_0 & 0 & 0 & v_3 & v_1 & 0 & v_0 & 0 & 0 \\
u_4 & u_2 & u_1 & 0 & u_0 & 0 & v_4 & v_2 & v_1 & 0 & u_0 & 0 \\
u_5 & 0 & u_2 & 0 & 0 & u_0 & v_5 & 0 & v_2 & 0 & 0 & v_0 \\
0 & u_4 & u_3 & u_2 & u_1 & 0 & 0 & v_4 & v_3 & v_2 & v_1 & 0 \\
0 & u_5 & u_4 & 0 & u_2 & u_1 & 0 & v_5 & v_4 & 0 & v_2 & v_1
\end{pmatrix}}_A \begin{pmatrix}
f_0 \\
f_1 \\
f_2 \\
f_3 \\
f_4 \\
f_5 \\
g_0 \\
g_1 \\
g_2 \\
g_3 \\
g_4 \\
g_5
\end{pmatrix} \equiv 0 \pmod I.$$

So some are interested in computing the kernel of the matrix A and others in computing a Gröbner basis of the solution module $\mathcal{R}(\mathcal{M}, F)$ with $F = \begin{pmatrix} u \\ v \end{pmatrix}$ and $\mathcal{M} = I$.

Remark 3.1.1. The matrix A figuring in the previous example is called a multiHenkel matrix (with two levels) and it's a kind of the structured matrices. These matrices are distinguished by having repetitive elements or elements satisfying certain relations. Officially, a $n \times n$ structured matrix is typically defined by $\mathcal{O}(n)$ elements, instead of n^2 for a dense matrix. Moreover, it can be multiplied by a vector with $\tilde{\mathcal{O}}(n)$ arithmetic operations, instead of $\mathcal{O}(n^2)$ operations for a dense matrix. So the benefit of using these kind of matrices is reducing computing time when n is a very large number.

3.2 Existing Algorithm

We explain now an existing algorithm for computing a Gröbner basis of a solution module recursively, which will inspire us to build another recursive algorithm for such computation but for some special modular cases.

Let $R = \mathbb{K}[x_1, \dots, x_n]$ be the multivariate polynomial ring over a field \mathbb{K} . Taking a particular case from [12], we consider $(p_1, \dots, p_m) \in R^m$ to be a solution of the congruence

$$\sum_{i=1}^m p_i f_i \equiv 0 \pmod{I}$$

where $f_i \in R$ for $i \in \{1, \dots, m\}$, and I is an ideal in R . We denote by F the vector $(f_1, \dots, f_m)^\top \in R^m$. As we already said in the first chapter, the set of solution vectors (p_1, \dots, p_m) forms a submodule of R^m , denoted by $\mathcal{R}(I, F)$. Under suitable conditions on the ideal I , and with an appropriate monomial order, we shall construct a Gröbner basis of $\mathcal{R}(I, F)$, using an algorithm which recursively determines Gröbner bases of submodules in a descending sequence terminating in $\mathcal{R}(I, F)$.

Here's the explanation:(one can find the proof and more details in [12, Section 3])

The incremental step

The incremental step will be applied to the ideals I_l and I_{l+1} in R with $I_l \supseteq I_{l+1}$ such that for each $s = 1, \dots, n$ there exists $\beta_s \in \mathbb{K}$ satisfying

$$(x_s - \beta_s)I_l \subseteq I_{l+1}. \quad (3.1)$$

(In the following interpretations, we considered β_s to be 0 for all s in $\{1, \dots, n\}$ since we're working only on monomial ideals).

We also require an \mathbb{K} -homomorphism

$$\alpha : I_l \longrightarrow \mathbb{K} \quad (3.2)$$

with $\ker(\alpha) = I_{l+1}$.

If \mathcal{W} is an ordered set then $\mathcal{W}[j]$ denotes its j^{th} element, and if $\mathcal{W}[j]$ is a vector then $\mathcal{W}[j]_i$ denotes its i^{th} component.

Theorem 3.2.1. *Let $I_l \supseteq I_{l+1}$ be ideals in R satisfying (3.1) and (3.2). Let $\mathcal{R}(I_l, F)$ be the submodule of R^m of solution vectors (p_1, \dots, p_m) of*

$$\sum_{i=1}^m p_i f_i \equiv 0 \pmod{I_l},$$

and let $\mathcal{R}(I_{l+1}, F) \subseteq \mathcal{R}(I_l, F)$ be the submodule of $\mathcal{R}(I_l, F)$ of elements satisfying

$$\sum_{i=1}^m p_i f_i \equiv 0 \pmod{I_{l+1}}.$$

If \mathcal{W} is an ordered minimal Gröbner basis of $\mathcal{R}(I_l, F)$ relative to a given term order $>$ then a Gröbner basis \mathcal{W}' of $\mathcal{R}(I_{l+1}, F)$ relative to $>$ can be constructed as follows:

Define: $\alpha_j := \alpha(\sum_{i=1}^m \mathcal{W}[j]_i f_i)$ for $j \in \{1, \dots, |\mathcal{W}|\}$.

If $\alpha_j = 0$ for all j then $\mathcal{W}' = \mathcal{W}$.

Else

$$j^* := \text{least } j \text{ for which } \alpha_j \neq 0$$

$$\mathcal{W}_1 = \{\mathcal{W}[j] : j < j^*\};$$

$$\mathcal{W}_2 = \{x_s \mathcal{W}[j^*] : 1 \leq s \leq n\};$$

$$\mathcal{W}_3 = \{\mathcal{W}[j] - (\alpha_j / \alpha_{j^*}) \mathcal{W}[j^*] : j > j^*\}$$

$$\mathcal{W}' = \mathcal{W}_1 \cup \mathcal{W}_2 \cup \mathcal{W}_3$$

Chapter 4

Contribution and Perspectives

Many questions in system and coding theory can be formulated as the solution of a system of polynomial congruences in one or more variables. For this reason our goal is to construct an algorithm solving this kind of problem, based on Gröbner bases.

Henry O'KEEFFE and Patrick FITZPATRICK have constructed an algorithm which recursively determines Gröbner bases of submodules. Hence, inspired by this algorithm we have reached these following results that can be useful for some special cases.

4.1 Proposition

We consider two $\mathbb{K}[X]$ -submodules $\mathcal{M}_1, \mathcal{M}_2 \subseteq \mathbb{K}[X]^r$, while X represents x_1, \dots, x_n for some $n \in \mathbb{N}^*$. Let $F = \begin{pmatrix} f_1 & \dots & f_m \end{pmatrix}^\top \in \mathbb{K}[X]^{m \times r}$.

We suppose that $\mathcal{R}(\mathcal{M}_1, F) = \langle P \rangle$, $\mathcal{R}(\mathcal{M}_2, G) = \langle Q \rangle$ for some $P \in \mathbb{K}[X]^{p \times m}$ and $Q \in \mathbb{K}[X]^{q \times p}$ and $G = PF \in \mathbb{K}[X]^{p \times r}$.

If $\mathcal{M}_2 \subset \mathcal{M}_1$ then

$$\mathcal{R}(\mathcal{M}_2, F) = \langle QP \rangle$$

PROOF: First of all, it is obvious that $QP.F \in \mathcal{M}_2$. So it remains to prove that:

$$\forall V \in \mathbb{K}[X]^m \text{ s.t. } V.F \in \mathcal{M}_2, \exists \rho \in \mathbb{K}[X]^q \text{ s.t. } V = \rho.QP$$

Since $\mathcal{R}(\mathcal{M}_1, F) = \langle P \rangle$, we have :

$$(*) PF \in \mathcal{M}_1 \text{ and } \forall U \in \mathbb{K}[X]^m \text{ s.t. } U.F \in \mathcal{M}_1, \exists \lambda \in \mathbb{K}[X]^p \text{ s.t. } U = \lambda.P$$

Likewise, since $\mathcal{R}(\mathcal{M}_2, G) = \langle Q \rangle$, we have :

$$(**) Q.PF \in \mathcal{M}_2 \text{ and } \forall W \in \mathbb{K}[X]^p \text{ s.t. } W.PF \in \mathcal{M}_2, \exists \gamma \in \mathbb{K}[X]^q \text{ s.t. } W = \gamma.Q$$

Finally, let $V \in \mathbb{K}[X]^m$

$$\begin{aligned}
VF \in \mathcal{M}_2 & \xrightarrow{\mathcal{M}_2 \subset \mathcal{M}_1} VF \in \mathcal{M}_1 \\
& \xrightarrow{(*)} V = \lambda.P \quad \text{for some } \lambda \in \mathbb{K}[X]^p \\
& \implies \lambda.PF \in \mathcal{M}_2 \\
& \xrightarrow{(**)} \lambda = \gamma.Q \quad \text{for some } \gamma \in \mathbb{K}[X]^q \\
& \implies V = \gamma.QP
\end{aligned}$$

□

We aim now solving the multivariate relation problem in the bivariate ring $R = \mathbb{K}[x, y]$ modulo the ideal $I = \langle x, y \rangle$ i.e finding a Gröbner basis of the solution module $\mathcal{R}(I, F)$ for any $F \in R^{r \times 1}$ (as defined in the first chapter).

Afterwards we will be able to construct a recursive algorithm to solve the same problem for a special ideal form $\langle x^d, y^d \rangle$.

Lemma 4.1.1. Let $F = (f_1, \dots, f_r)^\top \in R^{r \times 1}$. We consider the ideal $I = \langle x, y \rangle$ in the polynomial ring $R = \mathbb{K}[x, y]$, a \mathbb{K} -homomorphism

$$\begin{aligned}
\alpha : \quad R & \longrightarrow \mathbb{K} \\
f(x, y) & \longrightarrow f(0, 0)
\end{aligned}$$

with $\ker(\alpha) = I$ and an identity matrix W in $R^{r \times r}$.

The Gröbner basis of the solution module $\mathcal{R}(I, F)$, denoted by W' , can be constructed using the function $fitz1(F)$ defined as follows:

Define: $\alpha_j = f_j \bmod \langle x, y \rangle$ for $j \in \{1, \dots, r\}$.

If $\alpha_j = 0$ for all j then $W' = W$.

Else

$$j^* := \text{least } j \text{ for which } \alpha_j \neq 0$$

$$W' = \{W[j] : j < j^*\} \cup \{xW[j^*], yW[j^*]\} \cup \{W[j] - (\alpha_j/\alpha_{j^*})W[j^*] : j > j^*\}$$

Example 4.1.1. Let $\mathbb{K} = \mathbb{F}_{13}$ and $R = \mathbb{K}[x, y]$. We suppose that $f_1 = x^4 - 2x^3y^5$, $f_2 = x + y + 2$, $f_3 = x^2 + 5xy + 10$, $f_4 = x + 7$, $f_5 = y + 6$ and $F = (f_1, \dots, f_5)$. So applying the algorithm, we obtain that the Gröbner basis of the solution module $\mathcal{R}(I, F)$ for $I = \langle x, y \rangle$ is represented by the following matrix:

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & x & 0 & 0 & 0 \\ 0 & y & 0 & 0 & 0 \\ 0 & -5 & 1 & 0 & 0 \\ 0 & 3 & 0 & 1 & 0 \\ 0 & -3 & 0 & 0 & 1 \end{pmatrix}.$$

After obtaining this basis, we consider the ideal $I_2 = \langle x^2, y \rangle$. We want to compute a basis of $\mathcal{R}(I_2, F)$ using the previous proposition so we start by computing PF and a basis Q of $\mathcal{R}(I_2, PF)$:

$$PF = \begin{pmatrix} x^4 - 2x^3y^5 \\ x^2 + xy + 2x \\ xy + y^2 + 2y \\ x^2 - 5x - 5y + 5xy \\ 4x + 3y \\ -3x - 2y \end{pmatrix}$$

Actually, for computing a Gröbner basis for $\mathcal{R}(I_2, PF)$, we used the same algorithm as Fitzpatrick considering the sequence of ideals: $I_1 = \langle x, y \rangle \supset I_2 = \langle x^2, y \rangle$ and the \mathbb{K} -homomorphism

$$\begin{aligned} \alpha_1 : R &\longrightarrow \mathbb{K} \\ f(x, y) &\longrightarrow f'_x(0, 0) \end{aligned}$$

the coefficient of x in $f(x, y)$.

What helped during the computation is that the Gröbner basis of $\mathcal{R}(I, PF)$ is the identity matrix $\in R^{6 \times 6}$, for having $PF = 0 \pmod I$. Hence the computation went this way:

$$Q = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & x & 0 & 0 & 0 & 0 \\ 0 & y & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & -4 & 0 & 1 & 0 & 0 \\ 0 & -2 & 0 & 0 & 1 & 0 \\ 0 & -5 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Finally we compute QP :

$$QP = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & x^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & y & 0 & 0 & 0 \\ 0 & -4x - 5 & 1 & 0 & 0 \\ 0 & -2x + 3 & 0 & 1 & 0 \\ 0 & -5x - 3 & 0 & 0 & 1 \end{pmatrix}.$$

QP then is a generating set of $\mathcal{R}(I_2, F)$.

In the following lemma, we want to exploit the Fitzpatrick algorithm as well:

Lemma 4.1.2. Let $F = (f_1, \dots, f_r)^\top \in R^{r \times 1}$ and I be a monomial ideal in the polynomial ring $R = \mathbb{K}[x, y]$. We consider then a decreasing set of ideals starting by $I_1 = \langle x, y \rangle$ and ending by $I_n = I$, satisfying

$$xI_l \subseteq I_{l+1} \text{ and } yI_l \subseteq I_{l+1}$$

along with $n - 1$ \mathbb{K} -homomorphisms $\alpha_1, \dots, \alpha_{n-1}$ such that:

$$\alpha_n : I_n \longrightarrow \mathbb{K}$$

with $\ker(\alpha_n) = I_{n+1}$ and an identity matrix W in $R^{r \times r}$.

We define then the function $fitz2(I_n, F)$ as follow:

Define: $\alpha_j = \alpha_{n-1}(f_j)$ for $j \in \{1, \dots, r\}$.

If $\alpha_j = 0$ for all j then $W' = W$.

Else

$$j^* := \text{least } j \text{ for which } \alpha_j \neq 0$$

$$W' = \{W[j] : j < j^*\} \cup \{xW[j^*], yW[j^*]\} \cup \{W[j] - (\alpha_j/\alpha_{j^*})W[j^*] : j > j^*\}$$

This function outputs a Gröbner basis of the module $\mathcal{R}(I_n, F)$ if the Gröbner basis of $\mathcal{R}(I_{n-1}, F)$ equals to the identity matrix W .

Theorem 4.1.1. *The following algorithm computes a generating set of $\mathcal{R}(I_n, F)$ and represents a function $REL(I_n, F)$:*

If: $n > 1$

$$P = REL(I_{n-1}, F)$$

Return: $fitz2(I_n, PF).P$

Else:

Return: $fitz1(F)$

PROOF: If $REL(I_n, F)$ outputs a generating set of the module $\mathcal{R}(I_n, F)$, then by the proposition we have

$$\left. \begin{array}{l} REL(I_{n-1}, F) = (P) \\ REL(I_n, PF) = (Q) \end{array} \right\} \implies REL(I_n, F) = (QP)$$

Which means:

$$REL(I_n, F) = REL(I_n, REL(I_{n-1}, F)F)REL(I_{n-1}, F)$$

But $REL(I_{n-1}, REL(I_{n-1}, F)F) = W$, the identity matrix, hence

$$REL(I_n, REL(I_{n-1}, F)F) = fitz2(I_n, REL(I_{n-1}, F)F)$$

and the proof holds.

Example 4.1.2. We continue example 4.1.1, we try this algorithm to compute a generating set of $\mathcal{R}(I_3, F)$ with $I_3 = \langle x^2, xy, y^2 \rangle \subset I_2 = \langle x^2, y \rangle$ and we consider the \mathbb{K} -homomorphism

$$\begin{array}{lcl} \alpha_2 : & I_2 & \longrightarrow \mathbb{K} \\ & f(x, y) & \longrightarrow f'_y(0, 0) \end{array}$$

the coefficient of y in $f(x, y)$.

To compute a generating set of $\mathcal{R}(I_3, F)$ using the proposition, we start by the matrix multiplication:

$$QPF = \begin{pmatrix} x^4 - 2x^3y^5 \\ x^3 + x^2y + 2x^2 \\ 0 \\ xy + y^2 + 2y \\ -3x^2 + xy - 4y \\ -2x^2 - 2xy + 3y \\ -5x^2 - 5xy - 2y \end{pmatrix}.$$

Then we compute Q' , a generating set for $\mathcal{R}(I_3, QPF)$, using $fitz2(I_3, QPF)$ since $\mathcal{R}(I_2, QPF)$ is generated by the identity matrix W :

$$Q' = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & x & 0 & 0 & 0 \\ 0 & 0 & 0 & y & 0 & 0 & 0 \\ 0 & 0 & 0 & -4 & 1 & 0 & 0 \\ 0 & 0 & 0 & 5 & 0 & 1 & 0 \\ 0 & 0 & 0 & 4 & 0 & 0 & 1 \end{pmatrix}.$$

Finally we compute $Q'QP$ (hence we end up computing $fitz2(I_3, REL(I_2, F)F)REL(I_2, F)$)

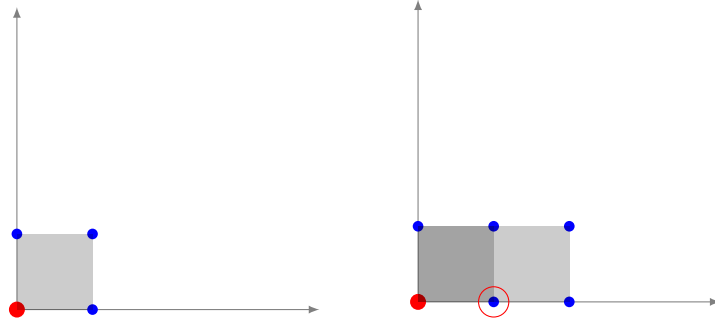
$$Q'QP = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & x^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & xy & 0 & 0 & 0 \\ 0 & y^2 & 0 & 0 & 0 \\ 0 & -4y - 4x - 5 & 1 & 0 & 0 \\ 0 & 5y - 2x + 3 & 0 & 1 & 0 \\ 0 & 4y - 5x - 3 & 0 & 0 & 1 \end{pmatrix}.$$

$Q'QP$ then is a generating set of $\mathcal{R}(I_3, F)$.

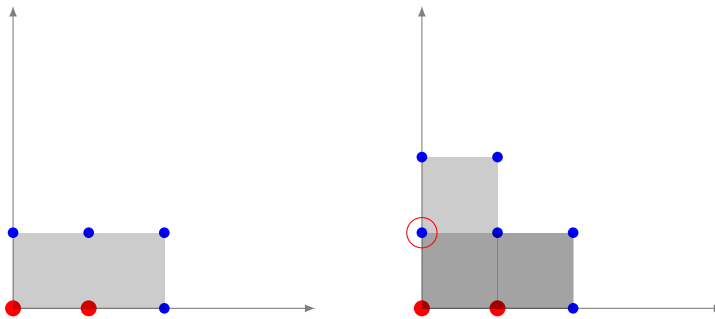
Remark 4.1.1. While proceeding the computation, we choose α_i for $i \in \{1, \dots, n-1\}$, with $\alpha_n : I_n \rightarrow \mathbb{K}$ and $\ker(\alpha_n) = I_{n+1}$, as follows: We draw the staircases of both I_n and I_{n+1} then we consider by α_n the coefficient of the added monomial between them, except the border.

For example:

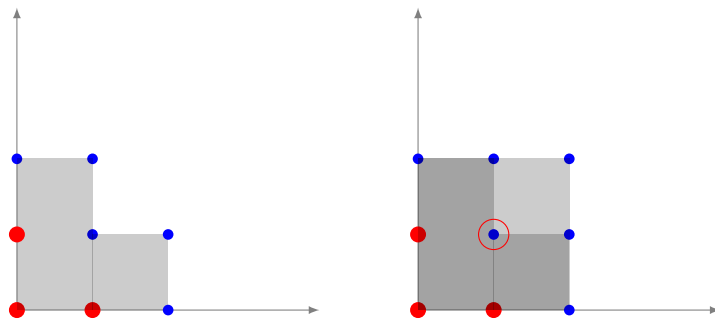
For $i = 1$, $I_1 = \langle x, y \rangle$ and $I_2 = \langle x^2, y \rangle$



and $\alpha_1 : R \rightarrow \mathbb{K}$ is the coefficient of x in $f(x, y)$.
 For $i = 2$, $I_2 = \langle x^2, y \rangle$ and $I_3 = \langle x^2, xy, y^2 \rangle$



and $\alpha_2 : R \rightarrow \mathbb{K}$ is the coefficient of y in $f(x, y)$.
 For $i = 3$, $I_3 = \langle x^2, xy, y^2 \rangle$ and $I_4 = \langle x^2, y^2 \rangle$



and $\alpha_3 : R \rightarrow \mathbb{K}$ is the coefficient of xy in $f(x, y)$.
 And so on...

Remark 4.1.2. We can think about some perspectives that could be useful for further studies:

1. In the matrix above $(Q'QP)$ we see that there is a line 0: cleaning the QP product would be more effective.

2. How to make sure the product is a Gröbner basis? Can we efficiently reduce it to reduced Gröbner basis?

Bibliography

- [1] David Eisenbud. *The geometry of syzygies: a second course in algebraic geometry and commutative algebra*, volume 229. Springer Science & Business Media, 2005.
- [2] Victor Y Pan. *Structured matrices and polynomials: unified superfast algorithms*. Springer Science & Business Media, 2012.
- [3] Maria Grazia Marinari, H. Michael Moeller, and Teo Mora. Gröbner bases of ideals defined by functionals with an application to ideals of projective points. *Applicable Algebra in Engineering, Communication and Computing*, 4(2):103–145, 1993.
- [4] Jérémy Berthomieu, Brice Boyer, and Jean-Charles Faugère. Linear algebra for computing gröbner bases of linear recursive multidimensional sequences. *Journal of Symbolic Computation*, 83:36–67, 2017.
- [5] Vincent Neiger and Vu Thi Xuan. Computing canonical bases of modules of univariate relations. In *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation, ISSAC '17*, pages 357–364, New York, NY, USA, 2017. ACM.
- [6] Venkatesan Guruswami and Madhu Sudan. Improved decoding of reed-solomon and algebraic-geometric codes. In *Foundations of Computer Science, 1998. Proceedings. 39th Annual Symposium on*, pages 28–37. IEEE, 1998.
- [7] Frederik Armknecht, Claude Carlet, Philippe Gaborit, Simon Künzli, Willi Meier, and Olivier Ruatta. Efficient computation of algebraic immunity for algebraic and fast algebraic attacks. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 147–164. Springer, 2006.
- [8] Jean-Bernard Lasserre, Monique Laurent, Bernard Mourrain, Philipp Rostalski, and Philippe Trébuchet. Moment matrices, border bases and real radical computation. *Journal of Symbolic Computation*, 51:63–85, 2013.
- [9] Marc Van Barel and Adhemar Bultheel. A general module theoretic framework for vector M-Padé and matrix rational interpolation. *Numerical Algorithms*, 3(1):451–461, 1992.

- [10] Bernhard Beckermann and George Labahn. A uniform approach for the fast computation of matrix-type padé approximants. *SIAM Journal on Matrix Analysis and Applications*, 15(3):804–823, 1994.
- [11] Alin Bostan, C-P Jeannerod, Christophe Moulleron, and É Schost. On matrices with displacement structure: Generalized operators and faster algorithms. *SIAM Journal on Matrix Analysis and Applications*, 38(3):733–775, 2017.
- [12] Henry O’keeffe and Patrick Fitzpatrick. Recursive construction of gröbner bases for the solution of polynomial congruences. In *Codes, Systems, and Graphical Models*, pages 299–309. Springer, 2001.
- [13] Jean-Charles Faugere, Patrizia Gianni, Daniel Lazard, and Teo Mora. Efficient computation of zero-dimensional gröbner bases by change of ordering. *Journal of Symbolic Computation*, 16(4):329–344, 1993.
- [14] Alin Bostan, Frédéric Chyzak, Marc Giusti, Romain Lebreton, Grégoire Lecerf, Bruno Salvy, and Éric Schost. *Algorithmes efficaces en calcul formel*. published by the Authors, 2017.
- [15] David Eisenbud. Commutative algebra, volume 150 of graduate texts in mathematics, 1995.
- [16] Mike Stillman. Gröbner bases: a tutorial. 1999.
- [17] David Cox, John Little, and Donal O’shea. *Ideals, varieties, and algorithms*, volume 3. Springer, 2007.
- [18] Diane Maclagan, Rekha R Thomas, Sara Faridi, Leah Gold, AV Jayanthan, Amit Khetan, and Tony Puthenpurakal. Computational algebra and combinatorics of toric ideals. *Commutative algebra and combinatorics*, 4, 2005.
- [19] Mohamed Elkadi and Bernard Mourrain. *Introduction à la résolution des systèmes polynomi-*
aux, volume 59. Springer Science & Business Media, 2007.