8-2014

Grobner Bases: Degree Bounds and Generic Ideals

Juliane Golubinski Capaverde
Clemson University, julianegc@gmail.com

Gröbner Bases: Degree Bounds and Generic Ideals

A Dissertation
Presented to
the Graduate School of
Clemson University

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy
Mathematical Sciences

---

by
Juliane Golubinski Capaverde
August 2014

Accepted by:
Dr. Shuhong Gao, Committee Chair
Dr. Michael Burr
Dr. Gretchen Matthews
Dr. Hui Xue

Abstract

In this thesis, we study two problems related to Gröbner basis theory: degree bounds for general ideals and Gröbner bases structure for generic ideals. We start by giving an introduction to Gröbner bases and their basic properties and presenting a recent algorithm by Gao, Volny and Wang.

Next, we survey degree bounds for the ideal membership problem, the effective Nullstellensatz, and polynomials in minimal Gröbner bases. We present general upper bounds, and bounds for several classes of special ideals. We provide classical examples showing some of these bounds cannot be improved in general. We present a comprehensive study of a result by Lazard, that gives a bound on the degree of Gröbner bases after a generic change of variables. The maximum degree of minimal generators of the initial ideal obtained this way is related to the regularity of the ideal, an important concept in algebraic geometry. We give a complete proof of Lazard's bound, filling in the details omitted in his paper.

Finally, we study Gröbner bases structure for generic ideals. It was conjectured by Moreno-Socías that the initial ideal of generic ideals is almost reverse lexicographic, which implies a conjecture by Fröberg on Hilbert series of generic algebras. In the literature, these conjectures were attacked using indirect methods. We use a direct incremental approach, based on a method by Gao, Guan and Volny. We show how a Gröbner basis for the ideal $\langle I, g\rangle$ can be obtained from that of I when adding a generic polynomial g, using properties of the standard basis of I. For a generic ideal $I = \langle f_1, \ldots, f_n\rangle$ in $K[x_1, \ldots, x_n]$, with $\deg f_i = d_i$, we are able to give a complete description of the ideal of leading terms of I in the case where $d_i \geq \left(\sum_{j=1}^{i-1} d_j\right) - i - 2$. As a result, we obtain a partial answer to Moreno-Socías Conjecture: the initial ideal of I is almost reverse lexicographic if the degrees of generators satisfy the condition above. This result slightly improves a result by Cho and Park. We hope this approach can be strengthened to prove the conjecture in full.

Dedication

This dissertation is dedicated to my future husband, Diego. I give my deepest expression of love and appreciation for the encouragement that you gave and the sacrifices you made during this graduate program. Thank you for the support and company during these though years.

Acknowledgments

Foremost, I would like to express my gratitude to my advisor Dr. Shuhong Gao for the support of my Ph.D study and research. I also would like to thank the rest of my thesis committee: Dr. Michael Burr, Dr. Gretchen Matthews, and Dr. Hui Xue, for their insightful comments.

I want to thank to CAPES/Brasil, Fulbright and Clemson University for their financial support granted through doctoral fellowship.

A special thanks to my family. Words cannot express how grateful I am to my mother and father for all of the sacrifices that they have made on my behalf, and to my sister for the constant support. At the end I would like express appreciation to my beloved fiance Diego, for the love, kindness and support he has shown during the entire process.

Table of Contents

Chapter 1

Introduction

Polynomial rings and their ideals are fundamental in many areas of mathematics, and efficient computation in polynomial ideal theory is important, not only in mathematics, but also in applications in sciences and engineering. Gröbner bases play a fundamental role in the algorithmic treatment of problems in polynomial ideals; they are the foundation for most computations in commutative algebra and algebraic geometry. Buchberger introduced Gröbner bases in 1965 [12]. Although the ideas behind the concept had appeared in others' works since the beginning of the 20th century, Buchberger's main contribution is that he gave the first algorithm for computing Gröbner bases. His algorithm makes actual implementations feasible, and leads to solutions to a large number of algorithmic problems related to multivariate polynomials. Since then, many improvements to Buchberger's algorithm have been proposed, as well as new algorithms, in an effort to compute Gröbner bases efficiently.

In Chapter 2, we give an introduction to Gröbner bases theory. We start with Gröbner bases for ideals, and then give the generalization to submodules. We present Buchberger's algorithm, and also a recent algorithm by Gao, Volny and Wang [26] that computes a Gröbner bases for an ideal and for its syzygy module simultaneously.

Another question that arises is: what is the complexity of computing Gröbner bases? Even with the best algorithms currently available, there are examples of ideals for which the computation of Gröbner bases takes a long time or consumes an enormous amount of storage space. One of the reasons for this is that the degrees of the polynomials generated during computations can be quite large. Thus, the maximal degree of polynomials occurring in computations is a good measure to

estimate the complexity of computational problems in polynomial ideal theory, and much work has been done in the search for upper bounds on such degrees.

A general upper bound for Gröbner bases degree has been given in [18, 41]. For $I = \langle f_1, \ldots, f_r \rangle$ an ideal in $K[x_1, \ldots, x_n]$, with $\deg f_i \leq d$ for $1 \leq i \leq r$, and any monomial order, the reduced Gröbner basis for I consists of polynomials whose total degree is bounded by

$$2\left(\frac{d^2}{2} + d\right)^{2^{n-1}}.$$

Mayr and Meyer [39] proved that the ideal membership problem has doubly exponential complexity. This result also gives a lower bound for the complexity of computing Gröbner basis. Although this bound raises questions about the applicability of Gröbner bases, it also contrasts with the fact that Gröbner bases are being successfully used in practice. Therefore, there is great interest in further investigating what causes the double exponential behavior, and establishing better bounds for families of ideals satisfying specific conditions. In Chapter 3, we survey degree bounds for Gröbner bases and other related problems, including the ideal membership problem and the effective Nullstellensatz. We also include classical examples showing that some of these bounds cannot be improved in general.

In [36], Lazard proved a bound on the degree of Gröbner bases, after a generic linear change of variables with respect to the graded reverse lexicographic order, for ideals satisfying certain conditions. This bound is linear in the degrees of the generators and the number of variables. More precisely, let $I = \langle f_1, \ldots, f_r \rangle$ be a homogeneous ideal in $K[x_0, \ldots, x_n]$, with $\deg f_i = d_i$, and suppose $d_1 \geq \cdots \geq d_r$. For I such that $\dim(I) = 0$ or $\operatorname{depth}(A) \geq \dim(I)$, Lazard proved that, after a generic change of variables, the elements of the reduced Gröbner basis with respect to the graded reverse lexicographical order have degree bounded by

$$d_1 + \cdots + d_{r+1} - n + \operatorname{depth}(A),$$

where $A = K[x_0, \ldots, x_n]/I$. The result also holds for any ideal if $n \leq 2$. The proof of this bound in [36] is missing some details. We give a complete proof of the bound, including the proof of an important result from [37] that gives the foundation for the result. Lazard conjectured the bound holds in general; however, this is now known not to be true. The initial ideal obtained after a generic

change of variables is called a *generic initial ideal*. The maximum degree of minimal generators of a generic initial ideal is related to the regularity of the ideal, which is considered a refined measure of the complexity of an ideal. Examples of ideals with high regularity are known, and they provide counterexamples for Lazard's conjecture.

In Chapter 4, we study the Gröbner bases structure of ideals generated by generic sequences of polynomials. Roughly speaking, we would like to know what the Gröbner basis of the ideal should look like if we choose the coefficients of its generators at random. We are particularly interested in two conjectures concerning these ideals. One is a famous conjecture by Fröberg [23]: Suppose $I = \langle f_1, \ldots, f_r \rangle$ is generated by homogeneous generic polynomials of degrees $d_1, \ldots, d_r$. He conjectured the Hilbert series of R/I is given by

$$S_{R/I}(z) = \left| \frac{\prod_{i=1}^{r}(1 - z^{d_i})}{(1-z)^n} \right|.$$

The second conjecture, by Moreno-Socías [43], is related to the initial ideal with respect to the reverse lexicographic order. He conjectured such initial ideals are *almost reverse lexicographic*, meaning that if m is a minimal generator of the initial ideal, then any monomial of the same degree and larger than m must be in the initial ideal as well. Pardue [45] and Cho and Park [14] proved that the Moreno-Socías Conjecture implies the Fröberg Conjecture. Partial answers have been given to both conjectures, usually using indirect methods. We attack the problem using a direct approach, based on an incremental method by Gao, Guan and Volny [25]. We show how a Gröbner basis for the generic ideal $\langle I, g \rangle$ can be obtained from the Gröbner basis of I when a generic polynomial g is added, employing properties of the standard basis of I. We give a description of the initial ideal of $I = \langle f_1, \ldots, f_n \rangle$ in the case the degrees $d_1, \ldots, d_n$ satisfy $d_i \geq \left(\sum_{j=1}^{i-1} d_j \right) - i - 2$. Our construction shows that Moreno-Socías Conjecture is true for these ideals, thus we give a partial answer to the conjecture. Our result is somewhat more general then the one given by Cho and Park in [14], where they showed Moreno-Socías to be true for degrees satisfying $d_i > \left(\sum_{j=1}^{i-1} d_j \right) - i + 1$. We expect that our method can be strengthened to fully prove the conjecture.

Chapter 2

Gröbner Bases

In Section 2.1, we introduce the concept of Gröbner basis and a few basic properties. In Section 2.2, we present Buchberger's algorithm, which was the first algorithm for computing Gröbner bases. In Section 2.3, we generalize the definition of Gröbner bases and the results of the previous sections to submodules. In Section 2.4, we present a recent algorithm, called GVW [26], that computes, simultaneously, a Gröbner bases for an ideal $I = \langle f_1, \ldots, f_m \rangle$ and the syzygy module of $f_1, \ldots, f_m$. In the last section, we introduce Hilbert functions and their connection with Gröbner bases.

Our main references for the first sections of this chapter are the books [1, 8, 16], where the interested reader can find the details omitted here and also learn more. Throughout the chapter, R denotes the polynomial ring $K[x_1, \ldots, x_n]$ over a field K.

2.1 Monomial orders and Gröbner bases

In the polynomial ring in one variable $K[x]$ over a field K, to decide whether a polynomial f is in the ideal generated by a set of polynomials $\{f_1, \ldots, f_r\}$, we first find their greatest common divisor using the Euclidean Algorithm. The polynomial f is in the ideal generated by $f_1, \ldots, f_r$ if, and only if, the remainder of the division of f by $\gcd(f_1, \ldots, f_r)$ is zero. Gröbner bases theory can be seen as a generalization of this procedure to multivariate polynomials. Given a finite set of multivariate polynomials with coefficients in a field, one can compute a new set of polynomials, a Gröbner basis, that generates the same ideal, with the property that a given polynomial is in the

ideal if, and only if, its normal form with respect to the Gröbner basis is zero. This normal form is computed using a procedure similar to the division algorithm of the univariate case, with the Gröbner basis playing the role of the gcd.

Our first step towards the generalization mentioned above is to extend the division algorithm to the multivariate case. Let us recall how it works in the univariate case. Let $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in K[x]$ be a nonzero polynomial, where $a_n \neq 0$. The leading term of f, denoted $\mathrm{lt}(f)$, is the term with the highest power of x, and the leading coefficient of f, $\mathrm{lc}(f)$, is the coefficient that appears in the leading term, that is, $\mathrm{lt}(f) = a_n x^n$ and $\mathrm{lc}(f) = a_n$. Given two polynomials f and g in $K[x]$, in the first step of the division algorithm we compute $h = f - \frac{\mathrm{lt}(f)}{\mathrm{lt}(g)} g$. The idea is to subtract from f an appropriate multiple of g so that the leading term of f is cancelled. Then we repeat this process using the polynomial h, until the power of x in the leading term of the resulting polynomial is less than the one in the leading term of g.

In order to generalize this procedure to the multivariate case, we need to establish an order for the terms in R, so we can define the leading term of a multivariate polynomial. We will follow here the convention that a *monomial* in R is a product of powers of the form $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$, with $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}_{\geq 0}$. To shorten the notation, we will write $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, for $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n$. A *term* is a monomial with a coefficient, that is, a term t has the form $t = cx^\alpha$, where $c \in K$. The *degree* of a monomial x^α is given by $\deg(x^\alpha) = \sum_{i=1}^n \alpha_i$.

Definition 2.1.1. A *monomial order* on the monomials of R is a total order $>$ satisfying

(i) $>$ is a well-ordering;

(ii) if $x^\alpha > x^\beta$, then $x^\alpha x^\gamma > x^\beta x^\gamma$ for all monomials x^γ.

For monomials in one variable, the only order satisfying this conditions is the natural one: $1 < x < x^2 < x^3 < \cdots$. In the multivariate case, however, there are infinitely many ways to order monomials. In the following examples we give two commonly used monomial orders.

Example 2.1.2 (Lexicographic order)**.** Given monomials x^α and x^β, $x^\alpha > x^\beta$ if and only if $\alpha_i > \beta_i$ for some $1 \leq i \leq n$, and $\alpha_j = \beta_j$ for all $1 \leq j < i$. ♢

A monomial order is said to be *degree compatible*, or *graded*, if $\deg(x^\alpha) > \deg(x^\beta)$ implies $x^\alpha > x^\beta$, for any monomials $x^\alpha, x^\beta \in R$.

Example 2.1.3 (Graded reverse lexicographic order)**.** Usually called *grevlex* order for short, this monomial order is defined as follows: for monomials x^α and x^β, $x^\alpha > x^\beta$ if and only if $\deg(x^\alpha) > \deg(x^\beta)$, or $\deg(x^\alpha) = \deg(x^\beta)$ and $\alpha_i < \beta_i$ for some $1 \leq i \leq n$, and $\alpha_j = \beta_j$ for all $i < j \leq n$. $\diamondsuit$

Every polynomial $f \in R$ can be written as a sum $f = \sum_{i=1}^{t} c_i x^{\alpha_i}$, with $c_i \in K$ and $x^{\alpha_1} > x^{\alpha_2} > \cdots > x^{\alpha_t}$. In this case, the *leading monomial*, *leading term* and *leading coefficient* of f are x^{α_1}, $c_1 x^{\alpha_1}$ and c_1, respectively, and are denoted by $\mathrm{lm}(f)$, $\mathrm{lt}(f)$ and $\mathrm{lc}(f)$.

Example 2.1.4. Consider the following monomials in $\mathbb{Q}[x_1, x_2, x_3]$: $x_1x_2x_3^2$, x_1^3, and x_2^4. Let us see how these monomials are ordered according to each of the monomial orders from the examples above.

(i) Lexicographic order: $x_1^3 > x_1x_2x_3^2 > x_2^4$

(ii) Grevlex order: $x_2^4 > x_1x_2x_3^2 > x_1^3$

Thus, the polynomial $f = 4x_1x_2x_3^2 + x_1^3 - 5x_2^4$ has distinct leading terms with respect to each monomial order.

	$\mathrm{lt}(f)$	$\mathrm{lm}(f)$	$\mathrm{lc}(f)$
Lexicographic	x_1^3	x_1^3	1
Grevlex	$-5x_2^4$	x_2^4	-5

$\diamondsuit$

Fix a monomial order. Now that we know how to choose the leading monomials, we may divide (or reduce) a polynomial by another polynomial, or a set of polynomials. The idea is the same as the univariate case: we cancel terms in the dividend using the leading terms of the divisors, so that the terms introduced are smaller than the cancelled ones. The differences are that in this case we may use more than one divisor, and we may cancel terms of the dividend other than the leading term.

Let $f \in R$ and $F = \{f_1, \ldots, f_m\} \subset R$. We say f is *reducible* by F if any of the terms of f is divisible by an element of $\{\mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_m)\}$. If $\mathrm{lm}(f)$ is divisible by an element of $\{\mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_m)\}$, then f is said *top-reducible* by F. If f is not reducible (resp. not top-reducible) by F, then we say f is reduced (resp. top-reduced) with respect to F.

If f is top-reducible by $F = \{f_1, \ldots, f_m\}$, then $\mathrm{lm}(f)$ is divisible by $\mathrm{lm}(f_{i_1})$, for some $1 \leq i_1 \leq m$. We then compute

$$h_1 = f - \frac{\mathrm{lt}(f)}{\mathrm{lt}(f_{i_1})} f_{i_1}.$$

The leading term of f is cancelled in this operation, and the leading monomial of the resulting polynomial h_1 is strictly smaller then $\mathrm{lm}(f)$. If $\mathrm{lm}(h_1)$ is divisible by $\mathrm{lm}(f_{i_2})$, for some $1 \leq i_2 \leq m$, then we repeat the operation to get

$$h_2 = h_1 - \frac{\mathrm{lt}(h_1)}{\mathrm{lt}(f_{i_2})} f_{i_2}.$$

This process is repeated until the resulting polynomial

$$h_N = f - \frac{\mathrm{lt}(f)}{\mathrm{lt}(f_{i_1})} f_{i_1} - \cdots - \frac{\mathrm{lt}(h_{i_{N-1}})}{\mathrm{lt}(f_{i_N})} f_{i_N}$$

is top-reduced with respect to F. We then proceed to cancel lower terms in h_N, using the same type of operation, until no term is divisible by leading terms of polynomials in F. In the end of this process, that is called reduction, we obtain a polynomial r which is reduced with respect to F, and satisfies

$$f = q_1 f_1 + \cdots + q_m f_m + r. \tag{2.1}$$

We say r is a remainder for f with respect to F.

To see that the reduction process must terminate, note that, at each step, we subtract a polynomial tf_i, where t is a term, such that the leading monomial of tf_i is strictly smaller than the leading monomial of the polynomial subtracted in the previous step. Thus, if the reduction process did not terminate, we would have an infinite strictly decreasing sequence of monomials, contradicting the fact that the monomial order is a well-ordering.

Example 2.1.5. Let $f = x_1^2 + x_1x_2 + x_2^3$, $f_1 = x_1 + x_2^2$, and $f_2 = x_1x_2 + x_2$ be polynomials in $\mathbb{Q}[x_1, x_2]$. Using the lexicographic order, we have $\mathrm{lm}(f_1) = x_1$ and $\mathrm{lm}(f_2) = x_1x_2$, so f is reducible by $F = \{f_1, f_2\}$. We reduce f by F as follows:

Step 1	$f - x_1 f_1 = -x_1x_2^2 + x_1x_2 + x_2^3$
Step 2	$(-x_1x_2^2 + x_1x_2 + x_2^3) - (-x_2^2)f_1 = x_1x_2 + x_2^4 + x_2^3$
Step 3	$(x_1x_2 + x_2^4 + x_2^3) - x_2 f_1 = x_2^4$

Since x_2^4 is not divisible by either $\mathrm{lm}(f_1)$ or $\mathrm{lm}(f_2)$, we have that x_2^4 is reduced with respect to F, and so it is a remainder for f with respect to F.

Now note that, at step 2 in the reduction above, $\mathrm{lm}(-x_1x_2^2+x_1x_2+x_2^3) = -x_1x_2^2$ is divisible by both $\mathrm{lm}(f_1)$ and $\mathrm{lm}(f_2)$. We chose to use f_1 in the reduction, but we could have used f_2. In this case we would have the following:

Step 1	$f - x_1f_1 = -x_1x_2^2 + x_1x_2 + x_2^3$
Step 2	$(-x_1x_2^2 + x_1x_2 + x_2^3) - (-x_2)f_2 = x_1x_2 + x_2^3 + x_2^2$
Step 3	$(x_1x_2 + x_2^3 + x_2^2) - f_2 = x_2^3 + x_2^2 - x_2$

We obtain a distinct remainder $x_2^3 + x_2^2 - x_2$. ♢

As we can see from Example 2.1.5, in general, the remainder obtained from the reduction of a polynomial is not unique.

Now suppose we reduce f by a set of polynomials F and get a remainder $r = 0$. Then by (2.1), $f \in \langle F\rangle$. However, the converse is not true.

Example 2.1.6. Let $f = x_1x_2 + x_1, f_1 = x_1x_2^2 + 1, f_2 = x_1^2x_2 - x_1 \in \mathbb{Q}[x_1, x_2]$, and fix the lexicographic order. Then f is reduced with respect to $F = \{f_1, f_2\}$, so that a remainder for f with respect to F is f itself. However, it is easy to see that $f = x_1f_1 - x_2f_2 \in \langle F\rangle$. ♢

In Example 2.1.6 we can see that even though $f \in \langle F\rangle$, its remainder is not zero, because the leading terms of f_1 and f_2 do not divide the terms in f. In general, if $f \in I = \langle F\rangle$, since any remainder r of f with respect to F satisfies an equation of the form (2.1), it follows that $r \in I$. To have zero remainders after reduction, we need to be able to reduce all leading terms of I using the leading terms of the divisors.

Given a set $F \subset R$, we denote by $\mathrm{lm}(F)$ the ideal generated by leading monomials of elements of F. For an ideal I, $\mathrm{lm}(I)$ is called the *leading term ideal* of I, or the *initial ideal* of I, sometimes also denoted as $\mathrm{in}(I)$.

Example 2.1.7. Let $f \in R$ and $I = \langle f\rangle$. Since $\mathrm{lm}(fg) = \mathrm{lm}(f)\,\mathrm{lm}(g)$, we have $\mathrm{lm}(I) = \langle \mathrm{lm}(f)\rangle$. ♢

Example 2.1.8. Let $I = \langle x_1^2 - x_2, x_1 - x_2\rangle \subset \mathbb{Q}[x_1, x_2]$. Fix the lexicographic order. Then

$$\langle \mathrm{lm}(x_1^2 - x_2), \mathrm{lm}(x_1 - x_2)\rangle = \langle x_1^2, x_1\rangle = \langle x_1\rangle.$$

Now,

$$x_2^2 - x_2 = (x_1^2 - x_2) - (x_1 + x_2)(x_1 - x_2) \in I$$

but

$$\mathrm{lm}(x_2^2 - x_2) = x_2^2 \notin \langle x_1 \rangle.$$

$\diamondsuit$

Example 2.1.8 shows that, in general, $I = \langle F \rangle$ does not imply $\mathrm{lm}(I) = \mathrm{lm}(F)$. The inclusion $\mathrm{lm}(F) \subseteq \mathrm{lm}(I)$ clearly holds.

Definition 2.1.9. Fix a monomial order for R. Given an ideal I in R, we say that a finite subset $G \subset I$ is a *Gröbner basis* for I if $\mathrm{lm}(G) = \mathrm{lm}(I)$. We say simply that G is a Gröbner basis if G is a Gröbner basis for the ideal generated by G.

Example 2.1.10. Consider the polynomials $f_1 = x_2 - x_3^2$ and $f_2 = x_1 - x_3^3$ in $\mathbb{Q}[x_1, x_2, x_3]$. Let $F = \{f_1, f_2\}$ and $I = \langle F \rangle$. Choosing the lexicographic order, we have $\mathrm{lm}(f_1) = x_2$ and $\mathrm{lm}(f_2) = x_1$. Suppose there is $f \in I$ such that $\mathrm{lm}(f) \notin \mathrm{lm}(F) = \langle x_1, x_2 \rangle$. Then, $\mathrm{lm}(f) = x_3^m$ for some $m \geq 0$, which implies $f \in \mathbb{Q}[x_3]$.

On the other hand, since $f \in I$, there exist $h_1, h_2 \in \mathbb{Q}[x_1, x_2, x_3]$ such that

$$f = h_1 f_1 + h_2 f_2.$$

Since x_1 does not appear in f, setting $x_1 = x_3^3$ gives

$$f(x_3) = h_1(x_3^3, x_2, x_3) \cdot (x_2 - x_3^2).$$

This implies that $(x_2 - x_3^2)$ divides f, contradicting the fact the only variable that appears in f is x_3. We conclude that F is a Gröbner basis with respect to the lexicographic order.

However, using the grevlex order, we have $\mathrm{lm}(f_1) = x_3^2$, and $\mathrm{lm}(x_3^3)$, so $\mathrm{lm}(F) = \langle x_3^2 \rangle$. Take $f = x_3 \cdot f_1 - f_2 \in I$. Then $\mathrm{lm}(f) = x_2 x_3 \notin \mathrm{lm}(F)$. Thus, F is not a Gröbner basis with respect to the grevlex order. $\diamondsuit$

Proposition 2.1.11. *Every nonzero ideal of R has a Gröbner basis.*

Proof. Let $I \subseteq R$ be an ideal. By Hilbert Basis Theorem, the ideal $\mathrm{lm}(I)$ has a finite set of generators,

say $\mathrm{lm}(I) = \langle h_1, \ldots, h_t \rangle$. Now, for each $1 \leq i \leq t$, since $h_i \in \mathrm{lm}(I)$, h_i can be expressed as

$$h_i = \sum_{j=1}^{\ell} g_j \, \mathrm{lm}(f_j),$$

for some $g_j \in R$ and $f_j \in I$. Expanding the g_j's, we see that every term in h_i is divisible by the leading monomial of an element in I, and so every term in h_i is itself the leading monomial of a polynomial in I. Let $S = \{m_1, \ldots, m_r\}$ be the set of all monomials that appear in $h_1, \ldots, h_t$. Then for each $1 \leq i \leq r$, $m_i = \mathrm{lm}(p_i)$, for some $p_i \in I$. Thus, $\{p_1, \ldots, p_r\}$ is a Gröbner basis for I. □

The following properties already allow us to glimpse the importance of Gröbner bases. For a proof, see [16, Chap. 2, §6, Proposition 1], for example.

Proposition 2.1.12. *Let $I \subseteq R$ be an ideal, and G be a Gröbner basis for I. Then*

(i) *The remainder of any polynomial $f \in R$ with respect to G is unique.*

(ii) *$f \in I$ if and only if the remainder of f with respect to G is zero.*

Given a Gröbner basis G and a polynomial f in R, we define the *normal form* of f with respect to G, denoted by $N_G(f)$, to be the remainder of f after reduction by G.

It follows from Proposition 2.1.12(ii) that a Gröbner basis for I is indeed a basis of the ideal. It also follows that, given a Gröbner bases for the ideal, one can easily determine ideal membership.

Example 2.1.10 (Continued)**.** Let $f = x_1^4 + x_1x_2 - x_3^{12} \in \mathbb{Q}[x_1, x_2, x_3]$. Reducing f by F using the lexicographic order we have

Step 1	$f - x_1^3 f_2 = x_1^3 x_3^3 + x_1x_2 - x_3^{12}$
Step 2	$(x_1^3 x_3^3 + x_1x_2 - x_3^{12}) - x_1^2 x_3^3 f_2 = x_1^2 x_3^6 + x_1x_2 - x_3^{12}$
Step 3	$(x_1^2 x_3^6 + x_1x_2 - x_3^{12}) - x_1 x_3^6 f_2 = x_1x_2 + x_1x_3^9 - x_3^{12}$
Step 4	$(x_1x_2 + x_1x_3^9 - x_3^{12}) - x_2 f_2 = x_1x_3^9 + x_2x_3^3 - x_3^{12}$
Step 5	$(x_1x_3^9 + x_2x_3^3 - x_3^{12}) - x_3^9 f_2 = x_2x_3^3$
Step 6	$(x_2x_3^3) - x_3^3 f_1 = x_3^5$

Thus, the normal form of f with respect to F is $x_3^5 \neq 0$, and therefore $f \neq I$, as F is a Gröbner basis with respect to the lexicographic order.

Using the grevlex order, x_1x_2 is a remainder of f with respect to F, as $f = (x_3^9 + x_1x_3^6 + x_1^2x_3^3 + x_1^3)f_2 + x_1x_2$ and x_1x_2 is reduced. But we cannot conclude that $f \notin I$ from this nonzero remainder, because F is not a Gröbner basis with respect to the grevlex order. $\diamondsuit$

Let I be an ideal, and suppose G is a Gröbner basis for I. Given $f, g \in R$, we say f is *congruent* to g modulo I, denoted $f \equiv g \pmod{I}$, if $f - g \in I$. This congruence is an equivalence relation on R. The set of equivalence classes is denoted by R/I. The elements of R/I are of the form $f + I$, and are called *cosets* of I. R/I is a commutative ring with the usual operations of addition and multiplication inherited from R, called the *quotient ring* of R by I. It is also a vector space over K.

Proposition 2.1.13. *Let I be an ideal in R, and let G be a Gröbner basis for I. If $f, g \in R$, then $f \equiv g \pmod{I}$ if, and only if, $N_G(f) = N_G(g)$. Thus, $\{N_G(h) : h \in R\}$ is a set of coset representatives of R/I.*

Fix a monomial order. For an ideal $I \subset R$, we define

$$\mathrm{B}(I) = \{x^\alpha : x^\alpha \notin \mathrm{lm}(I)\}.$$

Proposition 2.1.14. *Let I be an ideal in R. Then the set of cosets of monomials in $\mathrm{B}(I)$ is a basis of R/I as a K-vector space.*

The set of monomials $\mathrm{B}(I)$ is called the *standard basis* of I.

Example 2.1.10 (Continued)**.** As we have shown earlier, $F = \{x_2 - x_3^2, x_1 - x_3^3\}$ is a Gröbner basis for $I = \langle F \rangle$ with respect to the lexicographic order. Thus,

$$\mathrm{lm}(I) = \mathrm{lm}(F) = \langle x_1, x_2 \rangle \subset \mathbb{Q}[x_1, x_2, x_3].$$

It follows that

$$\mathrm{B}(I) = \{x_3^\ell : \ell \geq 0\}.$$

So, R/I is an infinite dimensional $\mathbb{Q}$-vector space. $\diamondsuit$

2.2 Buchberger Algorithm

One of the key results about Gröbner bases is Theorem 2.2.2, called the Buchberger Criterion. It gives an easy way to check whether a basis is a Gröbner basis, and naturally leads to an algorithm to compute a Gröbner basis starting with any basis of an ideal.

Let $F = \{f_1, \ldots, f_r\} \subset R$ and $I = \langle F \rangle$. For F to be a Gröbner basis, the leading monomial of every element $f \in I$ must be divisible by $\mathrm{lm}(f_i)$, for some $1 \leq i \leq r$. Since every $f \in I$ can be written as $f = \sum_{i=1}^{r} h_i f_i$, for some $h_i \in R$, an obstacle may be the cancellation of the largest of the $\mathrm{lm}(h_i)\,\mathrm{lm}(f_i)$. One way this can happen is the following.

Definition 2.2.1. Let $f, g \in R$ be nonzero polynomials, and let $m = \mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))$. The polynomial

$$S(f,g) = \frac{m}{\mathrm{lt}(f)} f - \frac{m}{\mathrm{lt}(g)} g$$

is called the *S-polynomial* of f and g.

S-polynomials are the simplest way that cancellation of leading terms can occur. As it turns out, they are actually the only type of cancellation we need to account for.

Theorem 2.2.2. *Let $G \subset R$ be a set of nonzero polynomials. Then G is a Gröbner basis if and only if $S(f,g)$ reduces to zero modulo G, for all $f, g \in G$.*

We need a couple of preliminary lemmas before we can prove Theorem 2.2.2.

Lemma 2.2.3. *Suppose $f_1, \ldots, f_r \in R$ are such that $\mathrm{lm}(f_i) = x^\alpha$ for all $1 \leq i \leq r$. Let $f = \sum_{i=1}^{r} c_i f_i$, with $c_i \in K$ for $1 \leq i \leq r$. If $\mathrm{lm}(f) < x^\alpha$, then f is a linear combination, with coefficients in K, of $S(f_i, f_j)$, $1 \leq i < j \leq r$.*

Proof. Let $a_i = \mathrm{lc}(f_i)$. Then $f_i = a_i x^\alpha + \text{lower terms}$, and, by assumption, $\sum_{i=1}^{r} c_i a_i = 0$. Now,

$$S(f_i, f_j) = \frac{1}{a_i} f_i - \frac{1}{a_j} f_j,$$

so

$$\begin{aligned} f &= c_1 f_1 + \cdots + c_r f_r \\ &= c_1 a_1 \left(\frac{1}{a_1} f_1\right) + \cdots + c_r a_r \left(\frac{1}{a_r} f_r\right) \end{aligned}$$

$$
\begin{aligned}
&= c_1a_1\left(\frac{1}{a_1}f_1 - \frac{1}{a_2}f_2\right) + (c_1a_1 + c_2a_2)\left(\frac{1}{a_2}f_2 - \frac{1}{a_3}f_3\right) + \cdots + \\
&\quad (c_1a_1 + \cdots + c_{r-1}a_{r-1})\left(\frac{1}{a_{r-1}}f_{r-1} - \frac{1}{a_r}f_r\right) + (c_1a_1 + \cdots + c_ra_r)\frac{1}{a_r}f_r \\
&= c_1a_1S(f_1, f_2) + (c_1a_1 + c_2a_2)S(f_2, f_3) + \cdots + (c_1a_1 + \cdots + c_{r-1}a_{r-1})S(f_{r-1}, f_r)
\end{aligned}
$$

as $c_1a_1 + \cdots + c_ra_r = 0$. □

Lemma 2.2.4. *Let $f, g \in R$ and suppose that $\operatorname{lm}(x^\alpha f) = \operatorname{lm}(x^\beta g)$, for some monomials $x^\alpha, x^\beta \in R$. Then there exists a monomial x^γ such that*

$$S(x^\alpha f, x^\beta g) = x^\gamma S(f, g).$$

Proof. Let $x^\delta = \operatorname{lm}(x^\alpha f) = \operatorname{lm}(x^\beta g)$. Then

$$S(x^\alpha f, x^\beta g) = x^\delta \left(\frac{f}{\operatorname{lt}(f)} - \frac{g}{\operatorname{lt}(g)}\right).$$

Let $x^\mu = \operatorname{lcm}(\operatorname{lm}(f), \operatorname{lm}(g))$; then $\mu_i \leq \delta_i$, and, taking $\gamma = \delta - \mu$, we have

$$S(x^\alpha f, x^\beta g) = x^\gamma S(f, g).$$

□

Proof of Theorem 2.2.2. If G is a Gröbner basis, then, by Proposition 2.1.12, $S(f, g)$ reduces to zero with respect to G, for all $f, g \in G$, since $S(f, g) \in I$.

Conversely, assume $S(p, q)$ reduces to zero with respect to G, for all $p, q \in G$. Let $f \in I = \langle G \rangle$. Then f can be written as a sum

$$f = \sum_{g \in G} h_g g$$

with $h_g \in R$, and, since each polynomial h_g is a sum of terms, we can write

$$f = \sum_{\alpha} \sum_{g \in G} c_{\alpha,g} x^\alpha g \tag{2.2}$$

with $c_{\alpha,g} \in K$.

Let $x^\delta = \max\{x^\alpha \operatorname{lm}(g) : c_{\alpha,g} \neq 0\}$. By the well-ordering property of the monomial order,

we can choose an expression of the form (2.2) with x^δ minimum. Let

$$f^* = \sum_{x^\alpha \operatorname{lm}(g)=x^\delta, g\in G} c_{\alpha,g} x^\alpha g,$$

so that $f = f^* + \text{smaller terms}$. Suppose that $\operatorname{lm}(f^*) < x^\delta$. By Lemma 2.2.3, there are constants $b_{ij} \in K$ such that

$$f^* = \sum_{i,j} b_{ij} S(x^{\alpha_i} g_i, x^{\alpha_j} g_j)$$

with $g_i, g_j \in G$ and $\operatorname{lm}(S(x^{\alpha_i} g_i, x^{\alpha_j} g_j)) < x^\delta$ for all i, j. By Lemma 2.2.4, for each pair i, j, there is a γ_{ij} such that

$$S(x^{\alpha_i} g_i, x^{\alpha_j} g_j) = x^{\gamma_{ij}} S(g_i, g_j).$$

Thus,

$$f^* = \sum_{i,j} b_{ij} x^{\gamma_{ij}} S(g_i, g_j)$$

and, since $\operatorname{lm}(S(x^{\alpha_i} g_i, x^{\alpha_j} g_j)) < x^\delta$, it follows that

$$\operatorname{lm}(x^{\gamma_{ij}} S(g_i, g_j)) = x^{\gamma_{ij}} \operatorname{lm}(S(g_i, g_j)) < x^\delta.$$

By assumption, $S(g_i, g_j)$ reduces to zero modulo G, so we can write

$$S(g_i, g_j) = \sum_{g\in G} q_g g$$

with $\operatorname{lm}(q_g g) \le \operatorname{lm}(S(g_i, g_j))$. Since each q_g is a sum of terms, we can write

$$S(g_i, g_j) = \sum_{\beta} \sum_{g\in G} d_{\beta,g} x^\beta g$$

with $x^\beta \operatorname{lm}(g) \le \operatorname{lm}(S(g_i, g_j))$. Thus,

$$x^{\gamma_{ij}} S(g_i, g_j) = \sum_{\beta} \sum_{g\in G} d_{\beta,g} x^{\beta+\gamma_{ij}} g$$

with $x^{\beta+\gamma_{ij}} \operatorname{lm}(g) \le \operatorname{lm}(x^{\gamma_{ij}}) S(g_i, g_j) = x^{\gamma_{ij}} \operatorname{lm}(S(g_i, g_j)) < x^\delta$. It follows that f^*, and hence f, can

be written in the form

$$\sum_{\mu} \sum_{g \in G} c'_{\mu,g} x^{\mu} g$$

with each monomial in $x^{\mu}g$ smaller than x^{δ}, contradicting the minimality of x^{δ}. □

Algorithm 2.2.1 Buchberger's Algorithm

Input: $F = \{f_1, \ldots, f_m\} \subset R$ and a term order for R.
Output: A Gröbner basis for $I = \langle F \rangle$.
$G := F$
$S = \{\{p, q\} : p, q \in G, p \neq q\}$
while S is not empty **do**
  Select $\{p, q\} \in S$
  $S := S \backslash \{\{p, q\}\}$
  Compute a remainder h of $S(p, q)$ with respect to G
  if $h \neq 0$ **then**
    $S := S \cup \{\{g, h\} : g \in G\}$
    $G := G \cup \{h\}$
  end if
end while
return G

Theorem 2.2.5. *Algorithm 2.2.1 constructs a Gröbner basis for the ideal $I = \langle F \rangle$ in finitely many steps.*

We point out that Algorithm 2.2.1 is only a rudimentary version of Buchberger's Algorithm. We present the algorithm in this form for the sake of clarity, but it is not a practical version. The following example illustrates Buchberger's Algorithm.

Example 2.2.6. Let $f_1 = x_1^2 x_2 + x_3$, $f_2 = x_1 x_3 + x_2 \in \mathbb{Q}[x_1, x_2, x_3]$ ordered by the lexicographic order. We apply Buchberger's Algorithm to find a Gröbner basis of the ideal $I = \langle f_1, f_2 \rangle$. We start with

$$G = \{f_1, f_2\}, \quad S = \{\{f_1, f_2\}\}.$$

We find $S(f_1, f_2) = x_3 f_1 - x_1 x_2 f_2 = -x_1 x_2^2 + x_3^2$, which is reduced with respect to G, so $h = -x_1 x_2^2 + x_3^2 \neq 0$. Let $f_3 = -x_1 x_2^2 + x_3^2$, and update G and S:

$$G = \{f_1, f_2, f_3\}, \quad S = \{\{f_1, f_3\}, \{f_2, f_3\}\}.$$

Next, we compute $S(f_1, f_3) = x_2 f_1 + x_1 f_3 = x_1 x_3^2 + x_2 x_3$. We can see that $S(f_1, f_3) = x_3 f_2$, so that

$h = 0$, and we have

$$G = \{f_1, f_2, f_3\}, \quad S = \{\{f_2, f_3\}\}.$$

Continue with the S-polynomial $S(f_2, f_3) = x_2^2 f_2 + x_3 f_3 = x_2^3 + x_3^3$, which is reduced with respect to G, that is, $h \neq 0$. Let $f_4 = x_2^2 + x_3^3$. G and S are updated:

$$G = \{f_1, f_2, f_3, f_4\}, \quad S = \{\{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}\}.$$

Now, $S(f_1, f_4) = x_2^2 f_1 - x_1^2 f_4 = -x_1^2 x_3^3 + x_2^2 x_3$, and using f_2 to reduce $S(f_1, f_4)$ we have $S(f_1, f_4) = (x_1 x_3^2 - x_2 x_3) f_2$, that is, $S(f_1, f_4)$ reduces to zero. So

$$G = \{f_1, f_2, f_3, f_4\}, \quad S = \{\{f_2, f_4\}, \{f_3, f_4\}\}.$$

In the following step we compute $S(f_2, f_4) = x_2^2 f_2 - x_1 x_3 f_4 = -x_1 x_3^4 + x_2^3$. Using f_2 and then f_4 to cancel terms, $S(f_2, f_4)$ reduces to zero. At this point we have

$$G = \{f_1, f_2, f_3, f_4\}, \quad S = \{\{f_3, f_4\}\}.$$

We then process the last pair in S. The S-polynomial $S(f_3, f_4) = x_2 f_3 + x_1 f_4 = x_1 x_3^3 + x_2 x_3^2$ equals $x_3^2 f_2$, so it reduces to zero with respect to G. At this point $S = \emptyset$, and the algorithm returns the Gröbner basis $G = \{f_1, f_2, f_3, f_4\}$.

Note that

$$\mathrm{lm}(I) = \mathrm{lm}(G) = \langle x_1^2 x_2, x_1 x_3, x_1 x_2^2, x_2^2 \rangle = \langle x_1^2 x_2, x_1 x_3, x_2^2 \rangle.$$

It follows that f_3 may be removed from from G. The subset $\{f_1, f_2, f_4\} \subset G$ is still a Gröbner basis for I. $\diamondsuit$

We note that Algorithm 2.2.1 does not specify a rule for selecting a pair $\{p, q\} \in SP$ and computing its S-polynomial. Often pairs are selected in a way such that $S(p, q)$ is computed first if $\mathrm{lcm}(\mathrm{lm}(p), \mathrm{lm}(q))$ is minimum among all pairs with respect to the monomial order being used. This procedure is known as the *normal selection strategy*. Experimental evidence shows that it works well for graded monomial orders [27].

Buchberger's algorithm is based on the computation of S-polynomials and their reduction. As the computation progresses, a large proportion of the S-polynomials reduce to zero, which requires a huge amount of computation but adds no new information, as this S-polynomials will not be added to the basis. One way to improve the algorithm's performance is detect that some S-polynomials reduce to zero without actually reducing them. The following result is an example of criterion used to avoid the reduction of S-polynomials that reduce to zero. For a proof, see [16, Proposition 4, Chapter 2, § 9].

Proposition 2.2.7 (Buchberger's first criterion)**.** *Let $G \subset R$ be a finite set, and suppose $f, g \in G$ are such that*

$$\operatorname{lcm}(\operatorname{lm}(f), \operatorname{lm}(g)) = \operatorname{lm}(f) \cdot \operatorname{lm}(g).$$

Then $S(f, g)$ reduces to zero modulo G.

2.3 Gröbner bases for modules

The theory of Gröbner bases for polynomial ideals presented in the previous sections can be generalized to submodules of free R-modules of finite rank. This generalization is attained by mimicking the steps of the case of ideals. As a consequence, we are able to compute with submodules in a similar way as with ideals.

First, we briefly review basic concepts and results from the theory of modules. For a detailed exposition of the material, see [4].

Let A be a commutative ring and $(M, +)$ a abelian group. M is an A-module if there exists a binary operation (scalar multiplication) $A \times M \longrightarrow M$, $(a, \mathbf{m}) \mapsto a\mathbf{m}$, such that, for all $a, b \in A$ and $\mathbf{m}, \mathbf{n} \in M$,

(i) $a(\mathbf{m} + \mathbf{n}) = a\mathbf{m} + a\mathbf{n}$,

(ii) $(a + b)\mathbf{m} = a\mathbf{m} + b\mathbf{m}$,

(iii) $a(b\mathbf{m}) = (ab)\mathbf{m}$,

(iv) $1\mathbf{m} = \mathbf{m}$.

The concept of modules is similar to that of vector spaces, except that scalars are in a ring, not necessarily a field.

Example 2.3.1. (i) Any ideal I of A is an A-module. In particular, A itself is an A-module.

(ii) If $A = K$ is a field, then A-modules are the same as K-vector spaces.

(iii) The product $A^m = \{(a_1, \ldots, a_m) : a_i \in A\}$ is an A-module.

$\diamondsuit$

Let M and M' be A-modules. A function $\varphi : M \longrightarrow M'$ is an A-module homomorphism if

$$\begin{aligned} \varphi(\mathbf{m}_1 + \mathbf{m}_2) &= \varphi(\mathbf{m}_1) + \varphi(\mathbf{m}_2) \\ \varphi(a\mathbf{m}_1) &= a\varphi(\mathbf{m}_1) \end{aligned}$$

for all $a \in A$ and $\mathbf{m}_1, \mathbf{m}_2 \in M$. If φ is a bijection, then it is an A-module isomorphism, and in this case we write $M \cong M'$.

A submodule of an A-module M is a subset of M which is an A-module . Let $\mathbf{m}_1, \ldots, \mathbf{m}_s \in M$. Then

$$N = \{a_1\mathbf{m}_1 + \cdots + a_s\mathbf{m}_s : a_1, \ldots, a_s \in A\} \subseteq M$$

is a submodule of M, called *submodule generated* by $\mathbf{m}_1, \ldots, \mathbf{m}_s$, denoted by $\langle \mathbf{m}_1, \ldots, \mathbf{m}_s \rangle$.

Let $\varphi : M \longrightarrow M'$ be an A-module homomorphism. The *kernel* of φ is the set

$$\ker(\varphi) = \{m \in M : \varphi(m) = 0\}.$$

$\ker(\varphi)$ is a submodule of M. The *image* of φ, $\operatorname{im}\varphi = \varphi(M)$, is a submodule of M'.

Example 2.3.2 (Syzygy module)**.** Let $A = R$ be the polynomial ring, and let $I = \langle f_1, \ldots, f_m \rangle \subset R$. Define

$$\begin{aligned} \varphi : R^m &\longrightarrow R \\ (h_1, \ldots, h_m) &\longmapsto h_1 f_1 + \cdots + h_m f_m \end{aligned}$$

Then φ is an R-module homomorphism, with $\operatorname{im}(\varphi) = I$. The kernel of φ is the submodule of R^m formed by all vectors $(h_1, \ldots, h_m)$ that satisfy

$$h_1 f_1 + \cdots + h_m f_m = 0.$$

Such an element is called a *syzygy* of $f_1, \ldots, f_m$. $\ker(\varphi)$ is called the *syzygy* module of $f_1, \ldots, f_m$, denoted by $\mathrm{Syz}(f_1, \ldots, f_m)$. $\diamondsuit$

M is said to be a *free* A-module if M has a basis, that is, a linearly independent set of generators. We say M is a free A-module of rank m if m is the number of elements in the basis. So, $M = A\mathbf{m}_1 + \cdots + A\mathbf{m}_m$, for some $\mathbf{m}_1, \ldots, \mathbf{m}_m \in M$, and every element $\mathbf{m} \in M$ can be written in a unique way as $\mathbf{m} = a_1\mathbf{m}_1 + \cdots + a_m\mathbf{m}_m$, with $a_1, \ldots, a_m \in A$. We say simply that M is a free A-module of *finite rank* if M has a finite basis.

The product A^m is a free A-module of rank m. The set $\{\mathbf{e}_1, \ldots, \mathbf{e}_m\}$, where $\mathbf{e}_i$ is the vector with the i-th entry equal to 1 and the others equal to zero, is a basis of A^m, called *standard basis*. If M is a free A-module of rank m, then $M \cong A^m$.

The ring A is said to be Noetherian if every ideal in A is finitely generated. The polynomial ring $R = K[x_1, \ldots, x_n]$, for instance, is Noetherian, by the Hilbert Basis Theorem. If A is Noetherian, then every submodule of A^r is finitely generated. A-modules with this property are also called Noetherian.

We now let $A = R$. Our goal is to generalize the theory of Gröbner bases to submodules of free R-modules of finite rank. In what follows, we restrict our discussion to the modules R^m, for $m > 0$, as any free R-module of finite rank is isomorphic to one of these modules. We outline the generalization with the definitions and main results, and refer the reader to [1, Chapter 3] for the details.

A *monomial* in R^m is an element of the form $x^\alpha \mathbf{e}_i$, where x^α is a monomial in R, and $\mathbf{e}_i$ is a standard basis element.

We say a monomial $x^\alpha \mathbf{e}_i$ divides $x^\beta \mathbf{e}_j$ if $i = j$ and x^α divides x^β. In this case, we define the quotient by

$$\frac{x^\beta \mathbf{e}_i}{x^\alpha \mathbf{e}_i} = x^{\beta-\alpha} \in R.$$

Similarly, a term in R^m has the form $cx^\alpha \mathbf{e}_i$, with $c \in K$.

We define monomial orders in R^m analogously to the polynomial case.

Definition 2.3.3. A *monomial order* on the monomials of R^m is a total order $>$ satisfying

(i) $>$ is a well-ordering.

(ii) If $\mathbf{x} > \mathbf{y}$, then $x^\alpha \mathbf{x} > x^\alpha \mathbf{y}$, for any monomials $\mathbf{x}, \mathbf{y} \in R^m$ and $x^\alpha \in R$.

Fix a monomial order in R^m. For all nonzero $\mathbf{f} \in R^m$, we can write

$$\mathbf{f} = a_1\mathbf{x}_1 + \cdots + a_r\mathbf{x}_r,$$

where $a_i \in K\backslash\{0\}$ and $\mathbf{x}_i \in R^m$ is a monomial, for $1 \leq i \leq r$, with $\mathbf{x}_1 > \mathbf{x}_2 > \cdots > \mathbf{x}_r$. Then we define:

(i) the *leading monomial* of $\mathbf{f}$ by $\mathrm{lm}(\mathbf{f}) = \mathbf{x}_1$;

(ii) the *leading term* of $\mathbf{f}$ by $\mathrm{lt}(\mathbf{f}) = a_1\mathbf{x}_1$;

(iii) the *leading coefficient* of $\mathbf{f} = a_1$.

Given a monomial order $>_R$ in R, there are two natural ways of obtaining monomial orders in R^m, which are frequently used. We fix an ordering for the elements of the basis of R^m: $\mathbf{e}_1 < \cdots < \mathbf{e}_m$.

Example 2.3.4 (TOP)**.** Let $x^\alpha\mathbf{e}_i, x^\beta\mathbf{e}_j \in R^m$ be monomials. We say $x^\alpha\mathbf{e}_i < x^\beta\mathbf{e}_j$ if, and only if, $x^\alpha <_R x^\beta$, or $x^\alpha = x^\beta$ and $i < j$. This order is called TOP for "term over position", since it first compares the monomials in R, and then the position in the vector. ♢

Example 2.3.5 (POT)**.** Let $x^\alpha\mathbf{e}_i, x^\beta\mathbf{e}_j \in R^m$ be monomials. We say $x^\alpha\mathbf{e}_i < x^\beta\mathbf{e}_j$ if, and only if, $i < j$, or $i = j$ and $x^\alpha <_R x^\beta$. This order is called POT for "position over term", since it first compares the position of monomials in the vector, and then breaks ties using the monomial order in R. ♢

Example 2.3.6. Let $R = \mathbb{Q}[x_1, x_2]$ and $\mathbf{f} = (7x_1x_2^3 - 4x_2^2, 10x_1^2x_2^2, x_1^3 - x_1x_2) \in R^3$. Then $\mathbf{f}$ is the sum of terms

$$\mathbf{f} = 7x_1x_2^3\mathbf{e}_1 - 4x_2^2\mathbf{e}_1 + 10x_1^2x_2^2\mathbf{e}_2 + x_1^3\mathbf{e}_3 - x_1x_2\mathbf{e}_3.$$

Fix the grevlex order on R. Then using the TOP order on R^3 we have

$$x_1^2x_2^2\mathbf{e}_2 > x_1x_2^3\mathbf{e}_1 > x_1^3\mathbf{e}_3 > x_1x_2\mathbf{e}_3 > x_2^2\mathbf{e}_1,$$

so that

$$\mathrm{lm}(\mathbf{f}) = x_1^2x_2^2\mathbf{e}_2, \quad \mathrm{lt}(\mathbf{f}) = 10x_1^2x_2^2\mathbf{e}_2, \quad \mathrm{lc}(\mathbf{f}) = 10.$$

Now, using the POT order,

$$x_1^3\mathbf{e}_3 > x_1x_2\mathbf{e}_3 > x_1^2x_2^2\mathbf{e}_2 > x_1x_2^3\mathbf{e}_1 > x_2^2\mathbf{e}_1,$$

which gives

$$\mathrm{lm}(\mathbf{f}) = x_1^3\mathbf{e}_3, \quad \mathrm{lt}(\mathbf{f}) = x_1^3\mathbf{e}_3, \quad \mathrm{lc}(\mathbf{f}) = 1.$$

♢

We continue following the steps from Section 2.1 with the concept of reduction. Let $\mathbf{g} \in R^m$ and let $F = \{\mathbf{f}_1, \ldots, \mathbf{f}_s\}$ be a set of nonzero elements in R^m. Then $\mathbf{g}$ is said to be *reduced* with respect to F if either $\mathbf{g} = \mathbf{0}$ or no monomial in $\mathbf{g}$ is divisible by any of $\mathrm{lm}(\mathbf{f}_i)$, for $1 \leq i \leq s$. Otherwise, $\mathbf{g}$ is said to be *reducible* by F. The reduction process we described for the polynomial case works exactly the same way in the context of modules: when reducing $\mathbf{g}$ by $F = \{\mathbf{f}_1, \ldots, \mathbf{f}_s\}$, we cancel terms in $\mathbf{g}$ using the leading terms of $\mathbf{f}_i$'s until all terms are reduced. As before, reduction produces a reduced element $\mathbf{r}$ such that

$$\mathbf{g} = q_1\mathbf{f}_1 + \cdots + q_s\mathbf{f}_s + \mathbf{r}, \tag{2.3}$$

where $q_i \in R$.

Example 2.3.7. Consider again the ring $R = \mathbb{Q}[x_1, x_2]$ and the element $\mathbf{f} = (7x_1x_2^3 - 4x_2^2, 10x_1^2x_2^2, x_1^3 - x_1x_2) \in R^3$ from Example 2.3.6. Let

$$\begin{aligned} \mathbf{f}_1 &= (x_1x_2 + 2x_1, 0, x_2^2), \\ \mathbf{f}_2 &= (0, x_2 - 1, x_1 - x_2) \end{aligned}$$

be in R^3. We fix the POT order on R^3 with the grevlex order on R, and reduce $\mathbf{f}$ by $F = \{\mathbf{f}_1, \mathbf{f}_2\}$ as follows. Since $\mathrm{lt}(\mathbf{f}) = x_1^3\mathbf{e}_3$ is divisible by $\mathrm{lt}(\mathbf{f}_2) = x_1\mathbf{e}_3$, we compute

$$\begin{aligned} \mathbf{h}_1 &= \mathbf{f} - \frac{\mathrm{lt}(\mathbf{f})}{\mathrm{lt}(\mathbf{f}_2)}\mathbf{f}_2 \\ &= (7x_1x_2^3 - 4x_2^2, 10x_1^2x_2^2, x_1^3 - x_1x_2) - x_1^2(0, x_2 - 1, x_1 - x_2) \end{aligned}$$

$$= \quad (7x_1x_2^3 - 4x_2^2, 10x_1^2x_2^2 - x_1^2x_2 + x_1^2, x_1^2x_2 - x_1x_2).$$

$\mathrm{lt}(\mathbf{h}_1) = x_1^2x_2\mathbf{e}_3$ is still divisible by $\mathrm{lt}(\mathbf{f}_2)$, so we may reduce by $\mathbf{f}_2$ again.

$$\begin{aligned}
\mathbf{h}_2 &= \mathbf{h}_1 - \frac{\mathrm{lt}(\mathbf{h}_1)}{\mathrm{lt}(\mathbf{f}_2)}\mathbf{f}_2 \\
&= (7x_1x_2^3 - 4x_2^2, 10x_1^2x_2^2 - x_1^2x_2 + x_1^2, x_1^2x_2 - x_1x_2) - x_1x_2(0, x_2 - 1, x_1 - x_2) \\
&= (7x_1x_2^3 - 4x_2^2, 10x_1^2x_2^2 - x_1^2x_2 - x_1x_2^2 + x_1^2 + x_1x_2, x_1x_2^2 - x_1x_2).
\end{aligned}$$

$\mathrm{lt}(\mathbf{h}_2) = x_1x_2^2\mathbf{e}_3$ is divisible by both $\mathrm{lt}(\mathbf{f}_1)$ and $\mathrm{lt}(\mathbf{f}_2)$, so we choose $\mathbf{f}_1$ to continue the reduction.

$$\begin{aligned}
\mathbf{h}_3 &= \mathbf{h}_2 - \frac{\mathrm{lt}(\mathbf{h}_2)}{\mathrm{lt}(\mathbf{f}_1)}\mathbf{f}_1 \\
&= (7x_1x_2^3 - 4x_2^2, 10x_1^2x_2^2 - x_1^2x_2 - x_1x_2^2 + x_1^2 + x_1x_2, x_1x_2^2 - x_1x_2) - x_1(x_1x_2 + 2x_1, 0, x_2^2) \\
&= (7x_1x_2^3 - x_1^2x_2 - 2x_1^2 - 4x_2^2, 10x_1^2x_2^2 - x_1^2x_2 - x_1x_2^2 + x_1^2 + x_1x_2, -x_1x_2).
\end{aligned}$$

$\mathrm{lt}(\mathbf{h}_3) = -x_1x_2\mathbf{e}_3$ is divisible by $\mathrm{lt}(\mathbf{f}_2) = x_1\mathbf{e}_3$

$$\begin{aligned}
\mathbf{h}_4 &= \mathbf{h}_3 - \frac{\mathrm{lt}(\mathbf{h}_3)}{\mathrm{lt}(\mathbf{f}_2)}\mathbf{f}_2 \\
&= (-x_1^2 + 7x_1x_2^3 - 2x_1^2 - 4x_2^2, 10x_1^2x_2^2 - x_1^2x_2 - x_1x_2^2 + x_1^2 + x_1x_2, -x_1x_2) \\
&\quad +x_2(0, x_2 - 1, x_1 - x_2) \\
&= (7x_1x_2^3 - x_1^2x_2 - 2x_1^2 - 4x_2^2, 10x_1^2x_2^2 - x_1^2x_2 - x_1x_2^2 + x_1^2 + x_1x_2 + x_2^2 - x_2, -x_2^2).
\end{aligned}$$

$\mathrm{lt}(\mathbf{h}_4) = -x_2^2\mathbf{e}_3$ is divisible by $\mathrm{lt}(\mathbf{f}_1) = x_2^2\mathbf{e}_3$

$$\begin{aligned}
\mathbf{h}_5 &= \mathbf{h}_4 - \frac{\mathrm{lt}(\mathbf{h}_4)}{\mathrm{lt}(\mathbf{f}_1)}\mathbf{f}_1 \\
&= (7x_1x_2^3 - x_1^2x_2 - 2x_1^2 - 4x_2^2, 10x_1^2x_2^2 - x_1^2x_2 - x_1x_2^2 + x_1^2 + x_1x_2 + x_2^2 - x_2, -x_2^2) \\
&\quad +(x_1x_2 + 2x_1, 0, x_2^2) \\
&= (7x_1x_2^3 - x_1^2x_2 - 2x_1^2 + x_1x_2 - 4x_2^2 + 2x_1, 10x_1^2x_2^2 - x_1^2x_2 - x_1x_2^2 + x_1^2 + x_1x_2 + x_2^2 - x_2, 0).
\end{aligned}$$

At this point, all terms in $\mathbf{h}_5$ are reduced by F, as they contain the standard basis elements $\mathbf{e}_1$ and $\mathbf{e}_2$, while the leading terms of $\mathbf{f}_1$ and $\mathbf{f}_2$ contain $\mathbf{e}_3$. Thus $\mathbf{r} = \mathbf{h}_5$ is a remainder of $\mathbf{f}$ with respect to F. $\diamondsuit$

For a set $S \subseteq R^m$, we define $\mathrm{lm}(S) = \langle \mathrm{lm}(\mathbf{f}) : \mathbf{f} \in S \rangle$, called the *submodule of leading terms* of S. We are now ready to define Gröbner bases of submodules of R^m.

Definition 2.3.8. Fix a monomial order on R^r, and let M be a submodule of R^m. A finite subset $G \subset M$ is a Gröbner basis for M if $\mathrm{lm}(G) = \mathrm{lm}(M)$. We say simply that G is a Gröbner basis if G is a Gröbner basis for the submodule it generates.

The following properties follow analogously to the ideal case:

(i) If G is a Gröbner basis for the submodule $M \subset R^m$, then $M = \langle G \rangle$.

(ii) Every nonzero submodule of R^m has a Gröbner basis.

(iii) If G is a Gröbner basis, then the remainder of $\mathbf{f}$ with respect to G is unique, for all $\mathbf{f} \in R^m$.

(iv) Given $\mathbf{f} \in R^m$ and a Gröbner basis G, $\mathbf{f} \in \langle G \rangle$ if, and only if, the remainder of $\mathbf{f}$ with respect to G is zero.

Now we generalize the notion of S-polynomial. For this, we need to define the least common multiple of two monomials in R^m. Given $x^\alpha \mathbf{e}_i$ and $x^\beta \mathbf{e}_j$ in R^m, we define

$$\mathrm{lcm}(x^\alpha \mathbf{e}_i, x^\beta \mathbf{e}_j) = \begin{cases} \mathbf{0}, \text{ if } i \neq j \\ \mathrm{lcm}(x^\alpha, x^\beta)\mathbf{e}_i, \text{ if } i = j. \end{cases}$$

Let $\mathbf{f}, \mathbf{g} \in R^m$ be nonzero. The *S-vector* of $\mathbf{f}$ and $\mathbf{g}$ is defined by

$$S(\mathbf{f}, \mathbf{g}) = \frac{\mathbf{m}}{\mathrm{lt}(\mathbf{f})}\mathbf{f} - \frac{\mathbf{m}}{\mathrm{lt}(\mathbf{g})}\mathbf{g},$$

where $\mathbf{m} = \mathrm{lcm}\, \mathrm{lm}(\mathbf{f}), \mathrm{lm}(\mathbf{g})$.

Proposition 2.3.9. *Let G be a finite set of nonzero elements in R^m. G is a Gröbner basis if, and only if, $S(\mathbf{f}, \mathbf{g})$ reduces to zero with respect to G, for all $\mathbf{f}, \mathbf{g} \in G$.*

The proof is analogous to the proof of Theorem 2.2.2. From this result we obtain the analog of Buchberger Algorithm for computing Gröbner bases of submodules.

Algorithm 2.3.1 Buchberger's Algorithm for Submodules

Input: $F = \{\mathbf{f}_1, \ldots, \mathbf{f}_m\} \subset R^m \backslash \{\mathbf{0}\}$ and a term order for R^m.
Output: A Gröbner basis for $M = \langle F \rangle$.
$G := F$
$SP = \{\{\mathbf{p}, \mathbf{q}\} : \mathbf{p}, \mathbf{q} \in G, \mathbf{p} \neq \mathbf{q}\}$
while SP is not empty **do**
  Select $\{\mathbf{p}, \mathbf{q}\} \in SP$
  $SP := SP \backslash \{\{\mathbf{p}, \mathbf{q}\}\}$
  Compute a remainder $\mathbf{h}$ of $S(\mathbf{p}, \mathbf{q})$ with respect to G
  if $\mathbf{h} \neq \mathbf{0}$ **then**
    $SP := SP \cup \{\{\mathbf{g}, \mathbf{h}\} : \mathbf{g} \in G\}$
    $G := G \cup \{\mathbf{h}\}$
  end if
end while
return G

2.4 GVW Algorithm

As we already mentioned in Section 2.2, in Buchberger's algorithm, several reductions of S-polynomials must be performed, many of which are unnecessary in the sense that the S-polynomials reduce to zero. Since reductions are time consuming, there has been extensive effort in finding more efficient algorithms by avoiding unnecessary reductions. Buchberger gave two criteria for detecting useless S-polynomials in [13, 11], one of which is the so called Buchberger's First Criterion (Proposition 2.2.7). Gebauer and Möller [46] interpreted one of Buchberger's criteria in terms of syzygies: finding useless S-polynomial amounts to finding redundant generators in a generating set of certain syzygies. Möller, Mora and Traverso [42] extend this idea, and construct a Gröbner basis and a basis of the syzygy module simultaneously. An S-polynomial is not considered if the corresponding syzygy is a linear combination of the syzygies already known. However, the efficiency of their algorithm is not satisfactory, as a lot of extra computation is required to uncover useless S-polynomials, and many unnecessary reductions are not detected. Faugère [21] introduced the algorithm F5, that uses two new criteria based on the idea of signatures and rewriting rules. By means of computer experiments, F5 was shown to be many times faster than previous algorithms.

We now describe a recent algorithm given in [26], that computes not only a Gröbner basis for the ideal, but also for the syzygy module of the original generators. Their key result is Theorem 2.4.2, which gives a condition that can be tested without performing any reduction.

Let $I = \langle f_1, \ldots, f_m \rangle$ be an ideal in R. Consider the R-module $R^m \times R$, and its submodule $M = \{(\mathbf{u}, v) \in R^m \times R \mid \mathbf{u}\mathbf{f}^{\mathrm{T}} = v\}$, with $\mathbf{f} = (f_1, \ldots, f_m)$. Let $\{\mathbf{e}_1, \ldots, \mathbf{e}_m\}$ standard basis of

R^m. Note that the R-module M is generated by $(\mathbf{e}_1, f_1), (\mathbf{e}_2, f_2), \ldots, (\mathbf{e}_m, f_m)$. Fix any compatible monomial orders $>_1$ on R and $>_2$ on R^m, that is, $>_1$ and $>_2$ are such that $x^\alpha <_1 x^\beta$ if and only if $x^\alpha \mathbf{e}_i <_2 x^\beta \mathbf{e}_i$ for all $1 \leq i \leq m$.

Given $(\mathbf{u}, v) \in R^m \times R$, we define the *signature* of $(\mathbf{u}, v)$ to be $\mathrm{lm}(\mathbf{u})$. A pair $(\mathbf{u}_1, v_1)$ is said to be *top-reducible* by $(\mathbf{u}_2, v_2)$, $v_2 \neq 0$, if $v_1 \neq 0$, $\mathrm{lm}(v_2)$ divides $\mathrm{lm}(v_1)$, and $\mathrm{lm}(t\mathbf{u}_2) \leq \mathrm{lm}(\mathbf{u}_1)$, where $t = \mathrm{lm}(v_1)/\mathrm{lm}(v_2)$. In this case, the *top-reduction* is

$$(\mathbf{u}_1, v_1) - ct(\mathbf{u}_2, v_2) = (\mathbf{u}_1 - ct\mathbf{u}_2, v_1 - ctv_2)$$

where $c = \frac{\mathrm{lc}(v_1)}{\mathrm{lc}(v_2)}$. So by performing a top-reduction we decrease the leading monomial of the v-part, without increasing the signature. The top-reduction is called *regular* if the signature stays the same, and it is called *super* if the signature decreases. If $v_2 = 0$, then $(\mathbf{u}_1, v_1)$ is top-reducible by $(\mathbf{u}_2, 0)$ if $\mathrm{lm}(\mathbf{u}_2)$ divides $\mathrm{lm}(\mathbf{u}_1)$. In this case the top-reduction is called super.

Definition 2.4.1. Let G be a subset of M. Then G is a *strong Gröbner basis* for M if every nonzero pair in M is top-reducible by some pair in G.

A strong Gröbner basis $G = \{(\mathbf{u}_1, v_1), (\mathbf{u}_2, v_2), \ldots, (\mathbf{u}_k, v_k)\}$ has the property that $G_0 = \{\mathbf{u}_i : v_i = 0, 1 \leq i \leq k\}$ is a Gröbner basis for the syzygy module of $\mathbf{f} = (f_1, \ldots, f_m)$, and $G_1 = \{v_i : 1 \leq i \leq k\}$ is a Gröbner basis for $I = \langle f_1, \ldots, f_m \rangle$.

Also, a strong Gröbner basis for M is a Gröbner basis for M in the classical sense as a submodule of R^{m+1}, with $\mathrm{lm}(\mathbf{u}, v) = \mathrm{lm}(v)\mathbf{e}_{m+1}$ if $v \neq 0$ and $\mathrm{lm}(\mathbf{u}, v) = \mathrm{lm}(\mathbf{u})$, if $v = 0$.

We now define J-pairs, which will play a role similar to that of S-polynomials in Buchberger's algorithm. Let $p_1 = (\mathbf{u}_1, v_1)$ and $p_2 = (\mathbf{u}_2, v_2)$ be two pairs in $R^m \times R$ with both v_1 and v_2 nonzero. Let

$$t = \mathrm{lcm}(\mathrm{lm}(v_1), \mathrm{lm}(v_2)), \quad t_1 = \tfrac{t}{\mathrm{lm}(v_1)}, \quad t_2 = \tfrac{t}{\mathrm{lm}(v_2)}, \quad c = \tfrac{\mathrm{lc}(v_1)}{\mathrm{lc}(v_2)}, \quad T = \max\{t_1 \,\mathrm{lm}(\mathbf{u}_1), t_2 \,\mathrm{lm}(\mathbf{u}_2)\}.$$

Assume, without loss of generality, that $T = t_1 \,\mathrm{lm}(\mathbf{u}_1)$. If $\mathrm{lm}(t_1\mathbf{u}_1 - ct_2\mathbf{u}_2) = T$, then the *J-pair* of p_1 and p_2 is defined to be $t_1 p_1$, and T is the *J-signature* of p_1 and p_2. When $\mathrm{lm}(t_1\mathbf{u}_1 - ct_2\mathbf{u}_2) < T$, we do not define a J-pair for p_1 and p_2.

Note that if $\mathrm{lm}(t_1\mathbf{u}_1 - ct_2\mathbf{u}_2) = T$, then the J-pair $t_1 p_1$ is regular top-reducible by p_2, and

the regular top-reduction yields the pair

$$t_1 p_1 - c t_2 p_2 = (t_1 \mathbf{u}_1 - c t_2 \mathbf{u}_2, t_1 v_1 - c t_2 v_2)$$

whose v-part we recognize as the S-polynomial of v_1 and v_2.

Let $G \subset R^m \times R$. A pair $(\mathbf{u}, v)$ is said to be regular top-reducible by G if it is regular top-reducible by at least one pair in G. A pair $(\mathbf{u}, v)$ is said to be *eventually super top-reducible* by G if there is a sequence of regular top-reductions of $(\mathbf{u}, v)$ by pairs of G that reduce $(\mathbf{u}, v)$ to $(\mathbf{u}', v')$ that is not regular top-reducible by G but is super top-reducible by at least one pair in G. Finally, a pair $(\mathbf{u}, v)$ is said to be *covered* by G if there is a pair $(\mathbf{u}_i, v_i) \in G$ such that $\mathrm{lm}(\mathbf{u}_i)$ divides $\mathrm{lm}(\mathbf{u})$ and $t\,\mathrm{lm}(v_i) < \mathrm{lm}(v)$, where $t = \frac{\mathrm{lm}(\mathbf{u})}{\mathrm{lm}(\mathbf{u}_i)}$.

Theorem 2.4.2. *Let $G \subset M$ be such that, for any monomial $T \in R^m$, $T = t\,\mathrm{lm}(\mathbf{u})$ for some pair $(\mathbf{u}, v) \in G$ and some monomial $t \in R$. Then the following are equivalent:*

(i) *G is a strong Gröbner basis for M.*

(ii) *Every J-pair of G is eventually super top-reducible by G.*

(iii) *Every J-pair of G is covered by G.*

Proof. To see that (i) implies (ii), assume G is a strong Gröbner basis for M, and let $p = (\mathbf{u}, v)$ be a J-pair of G. Then $p \in M$, and so it is top-reducible by some pair in G. We perform regular top-reductions on p until we get $p' = (\mathbf{u}', v')$ which is no longer regular top-reducible. Since $p' \in M$, it is top-reducible by G, and hence must be super top-reducible by G. Thus p is eventually super top-reducible by G.

Now assume (ii) holds. Let $p = (\mathbf{u}, v)$ be a J-pair of G. Then there is a sequence of regular top-reductions that produce $p_0 = (\mathbf{u}_0, v_0) \in M$ not regular top-reducible by G but super top-reducible by some pair $(\mathbf{u}_1, v_1) \in G$. Since regular top-reductions do not change the signatures, $\mathrm{lm}(\mathbf{u}_0) = \mathrm{lm}(\mathbf{u})$. Furthermore, $\mathrm{lm}(\mathbf{u}_1) | \mathrm{lm}(\mathbf{u}_0) = \mathrm{lm}(\mathbf{u})$. Let $t = \frac{\mathrm{lm}(\mathbf{u})}{\mathrm{lm}(\mathbf{u}_1)}$. If $v_1 = 0$, then $t\,\mathrm{lm}(v_1) = 0 < \mathrm{lm}(v)$, thus p is covered. If $v_1 \neq 0$, then $t\,\mathrm{lm}(v_1) = \mathrm{lm}(v_0) < \mathrm{lm}(v)$, hence p is covered. Thus, (iii) is proved.

The proof that (iii) implies (i) is done by contradiction. Suppose there is a nonzero pair $p = (\mathbf{u}, v) \in M$ not top-reducible by any pair in G. Choose p with minimal signature $T = \mathrm{lm}(\mathbf{u})$.

Since p is nonzero, $T \neq 0$. By the assumption on G, there is a pair $p_1 = (\mathbf{u}_1, v_1) \in G$ and a monomial $t \in R$ such that $T = t\,\mathrm{lm}(\mathbf{u_1})$. Choose p_1 so that $t\,\mathrm{lm}(v_1)$ is minimal.

We want to see that tp_1 is not regular top-reducible by G. Suppose tp_1 is regular top-reducible by some pair $p_2 = (\mathbf{u}_2, v_2) \in G$. Then the J-pair of p_1 and p_2 is $t_1 p_1$, where

$$t_1 = \frac{\mathrm{lcm}(\mathrm{lm}(v_1), \mathrm{lm}(v_2))}{\mathrm{lm}(v_1)} = \frac{\mathrm{lm}(v_2)}{\gcd(\mathrm{lm}(v_1), \mathrm{lm}(v_2))}, \qquad t = t_1 w$$

for some monomial w, and $t_1 p_1$ is regular top-reducible by p_2 (see [26, Lemma 2.3]). Now, by hypothesis, the J-pair $t_1 p_1$ is covered by G, so there is a pair $p_3 = (\mathbf{u}_3, v_3) \in G$ such that $t_3\,\mathrm{lm}(v_3) < t_1\,\mathrm{lm}(v_1)$, with $t_3 = \frac{t_1\,\mathrm{lm}(\mathbf{u}_1)}{\mathrm{lm}(\mathbf{u}_3)}$ is a monomial. It follows that

$$T = t\,\mathrm{lm}(\mathbf{u}_1) = wt_1\,\mathrm{lm}(\mathbf{u}_1) = wt_3\,\mathrm{lm}(\mathbf{u}_3)$$

and

$$wt_3\,\mathrm{lm}(v_3) < wt_1\,\mathrm{lm}(v_1) = t\,\mathrm{lm}(v_1)$$

contradicting the minimality of p_1.

Now let

$$(\mathbf{u}', v') = (\mathbf{u}, v) - ct(\mathbf{u}_1, v_1)$$

where $c = \frac{\mathrm{lc}(\mathbf{u})}{\mathbf{u}_1}$. Then $\mathrm{lm}(\mathbf{u}') < \mathrm{lm}(\mathbf{u}) = T$, and since $(\mathbf{u}', v') \in M$, this implies that $(\mathbf{u}', v')$ is top-reducible by some pair $p_2 = (\mathbf{u}_2, v_2) \in G$. If $v_2 = 0$, then we can reduce $(\mathbf{u}', v')$ by such pairs until we get a pair $\mathbf{u}'', v'$ that is not top-reducible by pairs in G with v-part zero. Since $(\mathbf{u}'', v') \in M$ and $\mathrm{lm}(\mathbf{u}'') < T$, $(\mathbf{u}'', v')$ must be top-reducible by some pair $p_2 = (\mathbf{u}_2, v_2) \in G$ with $v_2 \neq 0$.

Since p is not top-reducible by p_1, it follows that $\mathrm{lm}(v) \neq t\,\mathrm{lm}(v_1)$. If $\mathrm{lm}(v) < t\,\mathrm{lm}(v_1)$, then $\mathrm{lm}(v') = t\,\mathrm{lm}(v_1)$, and since $\mathrm{lm}(\mathbf{u}') < t\,\mathrm{lm}(\mathbf{u}_1)$, it follows that tp_1 is regular top-reducible by p_2, which is impossible. If $\mathrm{lm}(v) > t\,\mathrm{lm}(v_1)$, then $\mathrm{lm}(v') = \mathrm{lm}(v)$, and so p is regular top-reducible by p_2, which is a contradiction.

We conclude that every pair in M is top-reducible by G, and (i) is proved. □

Theorem 2.4.2 gives the foundation for the algorithm. The basic idea is to start with the set

$$(\mathbf{e}_1, f_1), (\mathbf{e}_2, f_2), \ldots, (\mathbf{e}_m, f_m)$$

and form all J-pairs. We need only to keep one J-pair for each J-signature, the one with smallest v-part.

Algorithm 2.4.1 GVW Algorithm

Input: $F = \{f_1, \ldots, f_m\} \subset R$ and term orders for R and R^m.
Output: A Gröbner basis for $I = \langle F \rangle$ and a Gröbner basis for the syzygy module of $f_1, \ldots, f_m$.
$U = \{\mathbf{e}_1, \ldots, \mathbf{e}_m\}$
$G_1 = \{f_1, \ldots, f_m\}$
Compute all the J-pairs of $(\mathbf{e}_1, f_1), (\mathbf{e}_2, f_2), \ldots, (\mathbf{e}_m, f_m)$ storing into JP only one J-pair for each distinct signature.
while JP is not empty **do**
  Take any pair $(\mathbf{u}, v) = x^\alpha(\mathbf{u}_i, v_i)$ from JP.
  if $(\mathbf{u}, v)$ is not covered by $G = [U, G_1]$ **then**
    Reduce the pair $(\mathbf{u}, v)$ repeatedly by G using only regular top-reductions until it is not regular top-reducible, say to get $(\tilde{\mathbf{u}}, \tilde{v})$
    if $\tilde{v} = 0$ **then**
      $G_0 = G_0 \cup \{\tilde{\mathbf{u}}\}$
      Delete every J-pair in JP whose signature is divisible by $\mathrm{lm}(\mathbf{u}) = \mathrm{lm}(\tilde{\mathbf{u}})$
    else
      Form the new J-pairs between $(\tilde{\mathbf{u}}, \tilde{v})$ and $(\mathbf{u}_i, v_i)$, $1 \leq i \leq \|U\|$ and insert into JP only one J-pair for each distinct signature, the one with v-part minimal
      Append $(\tilde{\mathbf{u}}, \tilde{v})$ to G (i.e. $\tilde{\mathbf{u}}$ to U and v to G_1).
    end if
  end if
end while
return G_0 and G_1

Theorem 2.4.3. *If the term order in R is compatible with the term order in R^m, then Algorithm 2.4.1 terminates in finitely many steps with a strong Gröbner basis for M.*

Proof. The correctness follows from Theorem 2.4.2. To see that the algorithm terminates in finitely many steps, list the pairs in G in the order they were obtained:

$$(\mathbf{e}_1, f_1), \ldots, (\mathbf{e}_m, f_m), (T_1, v_1), \ldots, (T_i, v_i), \ldots$$

For all $i \geq 1$, there exists $\mathbf{u}_i \in R^m$ such that $\mathrm{lm}(\mathbf{u}_i) = T_i$. Let $p_i = (\mathbf{u}_i, v_i)$. Let $i < j$, and suppose that $\mathrm{lm}(\mathbf{u}_i)$ divides $\mathrm{lm}(\mathbf{u}_j)$ and $\mathrm{lm}(v_i)$ divides $\mathrm{lm}(v_j)$. Then there are monomials $t_1, t_2 \in R$ such that

$$\mathrm{lm}(v_j) = t_1 \,\mathrm{lm}(v_i), \qquad \mathrm{lm}(\mathbf{u}_j) = t_2 \,\mathrm{lm}(\mathbf{u}_i).$$

If $t_1 < t_2$, then, since the term orders are compatible, $t_1 \,\mathrm{lm}(\mathbf{u}_i) < t_2 \,\mathrm{lm}(\mathbf{u}_i) = \mathrm{lm}(\mathbf{u}_j)$. But this implies that p_j is regular top-reducible by p_i, which is impossible as only the pairs that are not

regular top-reducible are added to G. Thus, we must have $t_2 \leq t_1$, which implies $t_2 \operatorname{lm}(v_i) \leq t_1 \operatorname{lm}(v_i) = \operatorname{lm}(v_j)$. Let $p = (\mathbf{u}, v)$ be the J-pair that was reduced to p_2 by the algorithm. Then $\operatorname{lm}(\mathbf{u}) = \operatorname{lm}(\mathbf{u}_j) = T_j$ and $\operatorname{lm}(v_j) < \operatorname{lm}(v)$, because J-pairs are always regular top-reducible. But then the J-pair p is covered by p_i, and would have been discarded by the algorithm.

It follows that given any pairs $p_i, p_j \in G$ with $i < j$, $\operatorname{lm}(\mathbf{u}_j)$ is not divisible by $\operatorname{lm}(\mathbf{u}_i)$, or $\operatorname{lm}(v_j)$ is not divisible by $\operatorname{lm}(v_i)$. We introduce new variables

$$y_i = (y_{i1}, y_{i2}, \ldots, y_{in}), \quad 1 \leq i \leq m$$

so that a pair $(x^\alpha \mathbf{e}_i, x^\beta)$ corresponds to the monomial $y_i^\alpha x^\beta$. It follows that

$$(T_1, \operatorname{lm}(v_1)), (T_2, \operatorname{lm}(v_2)) \ldots, (T_i, \operatorname{lm}(v_i)), \ldots$$

gives a list of monomials in the variables x_i's and Y_{ij}'s such that no monomial is divisible by the previous ones. Thus this list of monomials must be finite. Therefore, G is finite. □

2.5 Hilbert Functions

A polynomial $f \in R$ is called *homogeneous* provided that the degree of every term in f is the same. Any nonzero polynomial $f \in R$ may be decomposed, in a unique way, as a sum of homogeneous polynomials of different degrees, which are called the *homogeneous components* of f.

Example 2.5.1. The polynomial $f = x_1^5 + 2x_1^3x_2^2 + x_1x_2^4$ is homogeneous of degree 5. The polynomial $g = x_1^3 + 3x_1^2x_2 + 5x_3^7$ is not homogeneous, because $\deg(x_1^3) = \deg(3x_1^2x_2) \neq \deg(5x_3^7)$. Simply collecting terms of the same degree, we can see that $g = (x_1^3 + 3x_1^2x_2) + (x_3^7)$ is the sum of a homogenous polynomial of degree 3 and a homogeneous polynomial of degree 7, which are its homogenous components. ♢

We denote by R_s the set of all homogeneous polynomials of degree s in R together with 0. There is a direct sum decomposition of R into the additive subgroups, or K-vector spaces, R_s

$$R = \bigoplus_{s \geq 0} R_s.$$

A *graded module* over R is a module M with a family of subgroups $\{M_t : t \in \mathbb{Z}\}$ of the additive group M such that

$$M = \bigoplus_{t \in \mathbb{Z}} M_t$$

and $R_s M_t \subseteq M_{t+s}$ for all $s \geq 0$ and all $t \in \mathbb{Z}$. The elements of M_t are called the homogeneous elements of degree t in the grading.

If M is a finitely generated graded R-module, then for each t, the degree t homogeneous part M_t is a finite dimensional K-vector space.

Definition 2.5.2. Let M be a finitely generated graded R-module. The *Hilbert function* $H_M : \mathbb{Z} \longrightarrow \mathbb{Z}$ of M is defined by

$$H_M(t) = \dim_K(M_t),$$

where $\dim_K$ denotes the dimension as a K-vector space. The *Hilbert series* S_M of M is defined by

$$S_M(z) = \sum_{t \in \mathbb{Z}} H_M(t) z^t.$$

The first example of a graded R-module is R itself. In this case, R_t is generated as a K-vector space by all monomials of degree t, and so for $t \geq 0$ we have

$$H_R(t) = \binom{t+n-1}{n-1}, \tag{2.4}$$

and

$$S_R(z) = \frac{1}{(1-z)^n}.$$

For a proof of these identities, see [31, Proposition 5.1.13 and Lemma 5.2.9].

An ideal $I \subset R$ is called *homogeneous* if for each $f \in I$, the homogeneous components of f are all in I as well, or, equivalently, if there exist homogeneous polynomials $f_1, \ldots, f_r \in R$ such that $I = \langle f_1, \ldots f_r \rangle$. Suppose I is a homogeneous ideal in R. Then both I and the quotient R/I are graded R-modules, where

$$I_t = I \cap R_t \quad \text{and} \quad (R/I)_t = R_t/I_t.$$

From the exact sequence

$$0 \longrightarrow I \longrightarrow R \longrightarrow R/I \longrightarrow 0,$$

we get an exact sequence of K-vector spaces by taking the degree t part of each module

$$0 \longrightarrow I_t \longrightarrow R_t \longrightarrow (R/I)_t \longrightarrow 0$$

which gives

$$H_R(t) = H_I(t) + H_{R/I}(t). \tag{2.5}$$

Since the Hilbert function of R is given by (2.4), given the Hilbert function of I, one can easily determine the Hilbert function of R/I using Equation (2.5), and vice-versa. By Proposition 2.1.14, the residue classes of monomials in $B = \mathrm{B}(I)$ form a K-basis of R/I. Thus, for every $t \geq 0$, the residue classes of monomials of degree t form a K-basis of $(R/I)_t$. Denoting by B_t the set of monomials of degree t in B, we have that

$$H_{R/I}(t) = \dim_K (R/I)_t = |B_t|.$$

Chapter 3

Bounds in Polynomial Ideal Theory

Many computational problems involving polynomial ideals can be reduced to a few basic constructions, such as Gröbner bases. The complexity of such constructions is not yet fully understood. One measure usually used to estimate the complexity is the maximum degree of the polynomials generated during the computations. For this reason, a great effort has been made to find upper bounds on the degrees. In Sections 3.1 and 3.2, we survey degree bounds for some of these basic problems, namely the ideal membership, the effective Nullstellensatz, and the computation of Gröbner bases, all of which are closely related. In Section 3.3, we present a detailed proof of a bound given by Lazard in [36]. His bound is related to the regularity of an ideal, which is an important concept in algebraic geometry, and is considered a better measure of complexity than the degree of Gröbner bases.

3.1 Ideal membership and effective Nullstellensatz

Let $f_1, \ldots, f_r, g$ be polynomials in $R = K[x_1, \ldots, x_n]$. The *ideal membership problem* consists of deciding whether g is in the ideal $I = \langle f_1, \ldots, f_r \rangle$. If $g \in I$, computing an explicit representation

$$g = g_1 f_1 + \cdots + g_r f_r, \tag{3.1}$$

with $g_1, \ldots, g_r \in R$, is sometimes called *representation problem*. In this case, if the degrees of the generators $f_1, \ldots, f_r$ and g are at most d, we want to find a bound for the degrees of $g_1, \ldots, g_r$ of

minimal degree satisfying (3.1).

In 1926, Hermann [29] proved that the degrees of $g_1, \ldots, g_r$ are bounded by $\beta = \beta(n, d)$ that does not depend on the field K or the polynomials f_i. Her proof, however, was incorrect. In 1974, Seidenberg [48] gave a correct proof of this result, with an explicit but incorrect bound β. In [47], 1980, it was shown that one may take $\beta(n, d) = (2d)^{2^n}$.

Mayr and Meyer [39] showed that this double exponential bound for the ideal membership problem cannot be avoided. We give a modified construction of the Mayr-Meyer ideals from [6].

Example 3.1.1. Let $n \geq 0$ and $d \geq 2$ be integers. For $0 \leq r \leq n$, let $e_r = d^{2^r}$, and let

$$V_r = \{s_r, f_r, b_{r1}, b_{r2}, b_{r3}, b_{r4}, c_{r1}, c_{r2}, c_{r3}, c_{r4}\}$$

be a set of variables, said to be "of level r". We write monomials in $K[V_0, \ldots, V_n]$ in the form $T^\alpha = s_0^{\alpha_1} f_0^{\alpha_2} b_{01}^{\alpha_3} b_{02}^{\alpha_4} \cdots$, for $\alpha \in \mathbb{N}^{10(r+1)}$. A monomial T^α is said to be of level j if

(i) T^α involves only variables of levels $\geq j$

(ii) T^α is linear in $s_j, f_j, c_{j1}, c_{j2}, c_{j3}$ and c_{j4}

(iii) T^α is not divisible by $s_{j+1}, \ldots, s_n$ or $f_{j+1}, \ldots, f_n$.

Define $I_0 = \langle s_0 c_{0i} - f_0 c_{0i} b_{0i}^d \mid i = 1, 2, 3, 4 \rangle$. For $1 \leq r \leq n$, to avoid the subscripts we use upper-case letters to denote variables of level r, and lower-case letters to denote variables of level $r - 1$. We define

$$\begin{aligned} I_r \;=\; \langle \;& I_{r-1}, \\ & S - sc_1, && sc_4 - F && fc_1 - sc_2, \\ & sc_3 - fc_4 && fc_2 b_1 - fc_3 b_4, && sc_3 - sc_2, \\ & fc_2 C_i b_2 - fc_2 C_i B_i b_3 && \text{for } i = 1, 2, 3, 4 && \rangle. \end{aligned}$$

First, we see that $SC_i - FC_i B_i^{e_r} \in I_r$, for $1 \leq i \leq 4$. We use induction on r. For $r = 0$ the statement is true by the definition of I_0. Now, let $r > 0$, and assume the statement holds for level $r - 1$, that is, $sc_i - fc_i b_i^{e_{r-1}} \in I_{r-1} \subset I_r$. Then

$$SC_i \;\equiv\; sc_1 C_i$$

$$
\begin{aligned}
&\equiv fc_1C_ib_1^{e_{r-1}}\\
&\equiv sc_2C_ib_1^{e_{r-1}}\\
&\equiv fc_2C_ib_1^{e_{r-1}}b_2^{e_{r-1}}\\
&\vdots\\
&\equiv fc_2C_iB_i^{e_{r-1}}b_1^{e_{r-1}}b_3^{e_{r-1}}\\
&\equiv fc_3C_iB_i^{e_{r-1}}b_1^{e_{r-1}-1}b_3^{e_{r-1}}b_4\\
&\equiv sc_3C_iB_i^{e_{r-1}}b_1^{e_{r-1}-1}b_4\\
&\equiv sc_2C_iB_i^{e_{r-1}}b_1^{e_{r-1}-1}b_4\\
&\equiv fc_2C_iB_i^{2e_{r-1}}b_1^{e_{r-1}-1}b_2^{e_{r-1}}b_4\\
&\vdots\\
&\equiv fc_2C_iB_i^{2e_{r-1}}b_1^{e_{r-1}-1}b_3^{e_{r-1}}b_4\\
&\equiv fc_3C_iB_i^{2e_{r-1}}b_1^{e_{r-1}-2}b_3^{e_{r-1}}b_4^2\\
&\equiv sc_3C_iB_i^{2e_{r-1}}b_1^{e_{r-1}-2}b_4^2\\
&\vdots\\
&\equiv sc_3C_iB_i^{e_{r-1}^2}b_4^{e_{r-1}}\\
&\equiv fc_4C_iB_i^{e_{r-1}^2}b_4^{e_{r-1}}\\
&\equiv fc_4C_iB_i^{e_{r-1}^2}\\
&\equiv FC_iB_i^{e_r} \pmod{I_r}.
\end{aligned}
$$

Now let J_r be the ideal obtained from I_r by setting $B_1 = \cdots = B_4 = C_1 = \cdots = C_4 = 1$. It follows that $S - F \in J_r$.

Suppose $I_r = \langle h_1, \ldots, h_s \rangle$, where the h_i's denote the generators given above. Each h_i is a difference of monomials, say $h_i = T^{\alpha_i} - T^{\beta_i}$. Define a directed graph G with vertex set the monomials of $K[V_0, \ldots, V_n]$. The edge set consists of pairs (α, β) corresponding to a directed edge from T^α to T^β, such that $\alpha - \beta = \alpha_i - \beta_i$ for some $1 \leq i \leq s$. A *chain* in G is a formal combination of edges $\sum c_{\alpha,\beta}(\alpha, \beta)$ with coefficients $c_{\alpha,\beta} \in K$. The set of all chains in G is denoted by $C(G)$. The monomials of a chain $C = \sum c_{\alpha,\beta}(\alpha, \beta)$ are the monomials x^α such that $c_{\alpha,\beta} \neq 0$ or $c_{\beta,\alpha} \neq 0$ for some x^β. We define $|C| = \sum(c_{\alpha,\beta}T^\alpha - c_{\alpha,\beta}T^\beta)$.

Similarly, we can define a directed graph G' associated to the generators of J_r. The graphs G and G' have the following properties:

(i) Let T^α be a monomial of level r in G. The monomials in the connected component of G containing T^α are all of level $\leq r$. This connected component contains no cycles.

(ii) The monomials in the connected component of G' containing S and F are S, F or monomials of level $< r$. This component contains no cycles.

(iii) In G' there is a unique chain C whose monomials are the ones in the connected component containing S with $|C| = S - F$.

(iv) In G, if T^α and T^β are distinct monomials of level $\geq r$ such that $T^\alpha - T^\beta \in I_r$, then there is a unique chain C whose monomials are the ones in the component of G containing T^α with $|C| = T^\alpha - T^\beta$. Moreover, $T^\alpha - T^\beta$ is a multiple of one of the polynomials $SC_i - FC_iB_i^{e_r} \in I_r$, for $1 \leq i \leq 4$.

The monomial

$$m = f_0 c_{03} b_{03}^{e_0} b_{03}^{e_0} \cdots c_{r-1,3} b_{r-1,3}^{e_{r-1}} b_{r-1,4}^{e_{r-1}}$$

is one of the monomials that appear in the unique chain C in (iii). One of the two edges of C incident on m is a multiple of the generator $s_0 c_{03} - f_0 c_{04}$ with degree $r - 1 + 2e_0 + \cdots + 2e_{r-1}$. Any expression

$$S - F = \sum_{i=1}^{s} g_i h_i$$

corresponds to a chain in G' that may differ from C only by the addition of cycles containing monomials in other components of G', so some g_i has at least the degree $r - 1 + 2e_0 + \cdots + 2e_{r-1}$. $\diamondsuit$

Under suitable geometric assumptions, however, single-exponential bounds were obtained for zero-dimensional ideals and complete intersections in [17, 9]. In [17], it is also shown that ideal membership can be decided in single-exponential time for unmixed ideals. In the particular case when $f_1, \ldots, f_r$ have no common zeroes in $\bar{K}^n$, Hilbert's Nullstellensatz guarantees the existence of polynomials $g_1, \ldots, g_r \in K[x_1, \ldots, x_n]$ such that

$$1 = g_1 f_1 + \cdots + g_s f_s. \tag{3.2}$$

The effective Nullstellensatz includes an estimate for the degrees of the polynomials in (3.2).

Suppose the maximum degree of the polynomials $f_1, \ldots, f_r$ is d. Masser and Wüstholz [38] used Hermann's techniques from [29] to show that

$$\deg(g_i) \leq 2(2d)^{2^{n-1}}.$$

In 1987, Brownawell [10] greatly improved this bound, showing that the degrees of the g_i's are single-exponentially bounded:

$$\deg(g_i) \leq n^2 d^n$$

when $K = \mathbb{C}$. The best bound known in terms of d and n is

$$\deg g_i \leq \max\{3, d\}^n$$

for $1 \leq i \leq r$, due to Kollár [30], which is optimal for $d \geq 3$. Fitchas and Galligo [22] showed that this bound holds for polynomials with coefficients in any algebraically closed field. For $d = 2$, Sombra [50] showed that $\deg g_i f_i \leq 2^{n+1}$.

3.2 Gröbner bases

In this section, we show how the problem of bounding the degree of Gröbner bases can be restricted to homogeneous ideals. This allows the use of techniques suited to these ideals, such as Hilbert functions.

Let $S = K[x_0, x_1, \ldots, x_n]$ and $R = K[x_1, \ldots, x_n] \subset S$. For $f \in R$, let f^h denote the homogenization of f with respect to x_0, that is,

$$f^h = x_0^d f\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right),$$

where $d = \deg(f)$. For $f \in S$, let $f^a = f(1, x_1, \ldots, x_n)$ be the dehomogenized form of f.

Let $<$ be any monomial order on the monomials in R. Define an order $<^h$ on the monomials in S by

$$u <^h v \text{ iff } \deg(u) < \deg(v), \text{ or } \deg(u) = \deg(v) \text{ and } u^a < v^a.$$

One can check that $<^h$ is a monomial order in S.

Proposition 3.2.1. *Let $I = \langle f_1, \ldots, f_k \rangle \subset R$ and $J = \langle f_1^h, \ldots, f_k^h \rangle \subset S$. If $G = \{g_1, \ldots, g_m\}$ is a Gröbner basis for J with respect to $<^h$, then $G^a = \{g_1^a, \ldots, g_m^a\}$ is a Gröbner basis for I with respect to $<$.*

Lemma 3.2.2. *Let $f \in R$, and let $g \in S$ be homogeneous. Then*

(i) $(f^h)^a = f$

(ii) *There exists $p \in S \backslash \langle x_0 \rangle$ and an integer t such that $g = x_0^t p$, $g^a = p^a$ and $(g^a)^h = p$.*

Proof. To prove (i), suppose $\deg(f) = d$. By definition, $f^h = x_0^d f\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right)$, so, clearly,

$$(f^h)^a = f^h(1, x_1, \ldots, x_n) = f(x_1, \ldots, x_n).$$

To see (ii), let t be the largest power of x_0 dividing g. Then $g = x_0^t p$, with $p \notin \langle x_0 \rangle$. It follows that

$$g^a = g(1, x_1, \ldots, x_n) = p(1, x_1, \ldots, x_n) = p^a$$

and

$$(g^a)^h = (p^a)^h = p.$$

□

Lemma 3.2.3. *Let $I = \langle f_1, \ldots, f_k \rangle \subset R$ and $J = \langle f_1^h, \ldots, f_k^h \rangle \subset S$. If $f \in I$, then there exists an integer t such that $x_0^t f^h \in J$.*

Proof. Let $f \in I$. Write $f = g_1 f_1 + \cdots + g_k f_k$. Consider the following polynomial:

$$F = g_1^h f_1^h + \cdots + g_k^h f_k^h.$$

Then, each product $g_i^h f_i^h$ is homogeneous, but F might not be. Multiplying each product by an appropriate power of x_0, we get a homogeneous polynomial $H \in J$

$$H = x_0^{t_1} g_1^h f_1^h + \cdots + x_0^{t_k} g_k^h f_k^h$$

such that

$$H^a = F^a = (g_1^h)^a(f_1^h)^a + \cdots + (g_k^h)^a(f_k^h)^a = g_1f_1 + \cdots + g_kf_k = f$$

and so by Lemma 3.2.2, $H = x_0^t f^h$, for some integer t. □

Proof of Proposition 3.2.1. Let $f \in I$, and suppose $\operatorname{lm}(f) = x^\alpha$. Then, when we homogenize f, $x_0^s x^\alpha$ appears in f^h, for some $s \geq 0$. By Lemma 3.2.3, there exists $t \geq 0$ such that $F = x_0^t f^h \in J$. Then

$$\operatorname{lm}(F) = x_0^t \operatorname{lm}(f^h) = x_0^{t+s} \operatorname{lm}(f).$$

Since G is a Gröbner basis for J, $\operatorname{lm}(F) = m \operatorname{lm}(g_i)$ for some i, which implies

$$m \operatorname{lm}(g_i) = x_0^{t+s} \operatorname{lm}(f),$$

and, dehomogenizing, we have

$$\operatorname{lm}(f) = m^a \operatorname{lm}(g_i^a) = m^a \operatorname{lm}(g_i)^a.$$

Hence, G^a is a Gröbner basis for I. □

Proposition 3.2.4. *Let $I = \langle f_1, \ldots, f_k \rangle \subset R$ and $J = \langle f_1^h, \ldots, f_k^h \rangle \subset S$. If $G = \{g_1, \ldots, g_m\}$ is a Gröbner basis for I with respect to $<$, and $<$ is graded, then $G^h = \{g_1^h, \ldots, g_m^h\}$ is a Gröbner basis for J.*

Proof. Let $f \in J$. Then

$$f = \sum_{i=1}^{k} p_i f_i^h$$

with $p_i \in S$, so

$$f^a = \sum_{i=1}^{k} p_i(1, x_1, \ldots, x_n) f_i \in I.$$

By Lemma 3.2.2, $f = x_0^t (f^a)^h$ for some $t \geq 0$.

Since the monomial order in R is graded, $\operatorname{lm}(f^a)$ is one of the monomials x^α appearing in the homogenous component of maximal degree. When we homogenize f^a, this term is unchanged. If $x_0^s x^\beta$ is any of the other monomials appearing in $(f^a)^h$, then $\deg(x_0^s x^\beta) = \deg(x^\alpha)$ and $x^\alpha > x^\beta$.

By the definition of $<^h$, $x^\alpha >^h x_0^s x^\beta$, and thus $\mathrm{lm}((f^a)^h) = x^\alpha$. Hence

$$\mathrm{lm}(f) = x_0^t \,\mathrm{lm}((f^a)^h) = x_0^t \,\mathrm{lm}(f^a).$$

Now, as G is a Gröbner basis for I, $\mathrm{lm}(f^a)$ is divisible by $\mathrm{lm}(g_i)$ for some i. By the same reasoning above, $\mathrm{lm}(g_i) = \mathrm{lm}(g_i^h)$, and it follows that $\mathrm{lm}(f)$ is divisible by $\mathrm{lm}(g_i^h)$. Therefore, G^h is a Gröbner basis for J. □

To assess the complexity of computing Gröbner bases, a bound on the degree of the elements of such bases is not enough. A bound on the degree of the polynomials that appear during the computations is also necessary. The following example, by Masser and Philippon, illustrates this necessity.

Example 3.2.5. For $n, d > 0$, consider the ideal $I = \langle f_1, \ldots, f_n \rangle \subset K[x_1, \ldots, x_n]$, where

$$\begin{aligned} f_1 &= x_1^d \\ f_2 &= x_1 - x_2^d \\ &\vdots \\ f_{n-1} &= x_{n-2} - x_{n-1}^d \\ f_n &= 1 - x_{n-1} x_n^{d-1} \end{aligned}$$

It is easy to see that the system $f_1 = \cdots = f_n = 0$ has no solution, thus $I = K[x_1, \ldots, x_n]$, and $G = \{1\}$ is a Gröbner basis of I. Now, there exist $g_1, \ldots, g_n$ such that

$$1 = g_1 f_1 + \cdots + g_n f_n.$$

Specializing at

$$x_1 = t^{(d-1)d^{n-2}}, x_2 = t^{(d-1)d^{n-3}}, \ldots, x_{n-1} = t^{d-1}, x_n = \frac{1}{t}$$

for $t \neq 0$ we obtain

$$1 = g_1(t^{(d-1)d^{n-2}}, \ldots, t^{d-1}, 1/t) t^{(d-1)d^{n-1}},$$

which implies that $\deg_{x_n} g_1 \geq (d-1)d^{n-1}$. ♢

However, when working with homogenized generators this problem is avoided. Assume we use Buchberger's Algorithm with the normal selection strategy and restricted to what Buchberger called essential pairs to find a Gröbner basis of the ideal generated by the homogenizations with respect to the monomial order defined above. By setting $x_0 = 1$, we obtain not only a Gröbner basis of the original ideal, but also the sequence of computations that lead to the basis. Thus, the degrees of all intermediate polynomials are also bounded by the same bound of the basis.

The results from Bayer's thesis [7], Giusti [28], and Möller and Mora [41] show that the degree of the elements in a Gröbner basis is bounded by

$$(2d)^{(2n+2)^{n+1}}.$$

In [18], Dubé obtained a somewhat stronger result, showing that the degree is bounded by

$$2\left(\frac{d^2}{2}+d\right)^{2^{n-1}}.$$

If one has a Gröbner basis of the ideal $I = \langle f_1, \ldots, f_r \rangle$, a representation $g = g_1 f_1 + \cdots + g_r f_r$ can be easily found for any $g \in I$. Thus, the complexity of the membership problem gives a lower bound for the complexity of computing Gröbner bases. In [41], Möller and Mora used the Mayr-Meyer ideal to show the double exponential bounds cannot be improved. They showed that any Gröbner basis for the Mayr-Meyer ideal contains an element with degree at least $\frac{d^{2^n}}{2} + 4$.

If an ideal $I = \langle f_1, \ldots, f_r \rangle$ is zero-dimensional and the degree of generators is at most d, then Bezout's Theorem implies a singly exponential bound. This suggests that better bounds for the degree are possible for ideals with small dimension. Mayr and Ritscher [40] proved the bound

$$2\left(\frac{d^{n-r}}{2}+d\right)^{2^r},$$

where r is the dimension of the ideal I.

The complexity of computing Gröbner bases is not determined only by the maximum degree of polynomials, but by the total number of arithmetic operations in the field K that are required. This complexity has not been examined in general, but some results in this direction can be found in [33, 34, 25], where it is shown that for zero-dimensional ideals the complexity of computing Gröbner bases is bounded by a polynomial in d^n, and [32], that gives a singly exponential bound for the

complexity for one-dimensional ideals.

3.3 Lazard's bound on Gröbner bases degree

In this section, we study a bound on Gröbner bases degree given by Lazard in [36]. Lazard's result concerns Gröbner bases of homogeneous ideals after a generic change of variables, with respect to the graded reverse lexicographical order. The maximum degree of an element in such a Gröbner basis is related to the *regularity* of the ideal, an important concept in algebraic geometry. In [36], Lazard proved the bound for some cases and conjectured that the result holds in general; however, examples of ideals with high regularity, where Lazard's bound does not hold, are now known. Furthermore, in general, the linear change of variables cannot be avoided, not even in the zero-dimensional case.

3.3.1 Zero-dimensional ideals

In what follows, we present a collection of results from [37], which are the foundation to the bounds on Gröbner bases degree in [36]. Throughout this chapter, we let $R = K[x_0, \ldots, x_n]$. We denote the algebraic closure of K by $\overline{K}$.

Definition 3.3.1. Let L be an extension field of K, and let $f_1, \ldots, f_r \in R$ be homogeneous polynomials. The *projective variety* defined by $f_1, \ldots, f_r$ is

$$\mathbf{V}_L(f_1, \ldots, f_r) = \{(a_0, \ldots, a_n) \in \mathbb{P}^n(L) : f_i(a_0, \ldots, a_n) = 0 \text{ for all } 1 \leq i \leq r\}.$$

We note that if I is a homogeneous ideal in R, then $I = \langle f_1, \ldots, f_r \rangle$ for some homogeneous polynomials $f_1, \ldots, f_r$, and

$$\mathbf{V}_L(I) = \{p \in \mathbb{P}^n(L) : f(p) = 0 \text{ for all } f \in I\} = \mathbf{V}_L(f_1, \ldots, f_r).$$

Theorem 3.3.2 (Projective Weak Nullstellensatz)**.** *Suppose K is algebraically closed, and let I be a homogeneous ideal in R. Then the following are equivalent:*

(i) $\mathbf{V}_K(I) \subset \mathbb{P}^n(K)$ *is empty.*

(ii) *If G is a Gröbner basis for I, then, for each $0 \leq i \leq n$, there is a $g \in G$ such that $\mathrm{lm}(g)$ is a power of x_i.*

(iii) *For each $0 \leq i \leq n$, there is an integer $m_i \geq 0$ such that $x_i^{m_i} \in I$.*

(iv) *There is an integer $r \geq 1$ such that $\langle x_0, \ldots, x_n \rangle^r \subseteq I$.*

For a proof of this well known result, see [16, Chapter 8, Section 3, Theorem 8].

In what follows, X^d denotes the set of all homogeneous elements of degree d in a graded ring or module X. If L is an extension field of K, I an ideal in $K[x_0, \ldots, x_n]$ and $A = R/I$, then A_L denotes the ring

$$A_L = L \otimes_K A = L[x_0, \ldots, x_n]/I.$$

We will also need this other form of the Nullstellensatz.

Proposition 3.3.3. *Let I be a homogeneous ideal in R, and let $A = R/I$. If L is an extension field of K, then the function that associates $(a_0, \ldots, a_n)$ with the ideal generated by $a_i x_j - a_j x_i$, for $0 \leq i < j \leq n$, is an injection from the projective variety $\mathbf{V}_L(I)$ into the set of graded prime ideals of A_L maximal among those not containing A_L^1. If L is algebraically closed, then this function is a bijection.*

Theorem 3.3.4. *Let I be a homogeneous ideal in R, and let $A = R/I$. The following conditions are equivalent.*

(i) *$\mathbf{V}_{\overline{K}}(I)$ is a finite set.*

(ii) *For all extensions L of K, $\mathbf{V}_L(I)$ is a finite set.*

(iii) *There exists an integer D such that*

$$\dim_K(A^d) = \dim_K(A^D)$$

for all $d \geq D$.

(iv) *For all infinite extensions L of K, there exists an integer D' and an element $y \in A_L^1$ such that multiplication by y is a surjection from $A_L^{D'-1}$ onto $A_L^{D'}$.*

Proof. We start by showing that (iv) implies (iii). Assertion (iv) actually implies that multiplication by y is surjective for all $d \geq D'$. It follows that $\dim_L(A_L^d)$ is non-increasing for $d \geq D'$. Since the dimensions are nonnegative, there exists an integer D such that $\dim_L(A_L^d) = \dim_L(A_L^D)$ for all $d \geq D$. Now (iii) holds because $\dim_K(A^d) = \dim_L(A_L^d)$ for all d.

To see that (iii) implies (ii), note that if (iii) holds, than $\dim_L A_L^d = \dim_K A^d$ for all extensions L of K, and all $d \geq D$. Moreover, (iii) implies that all homogeneous prime ideals other than $\mathfrak{m}$ are minimal [49, III.B, Theorem 1]. Let $(a_0, \ldots, a_n) \in \mathbf{V}_L(I)$; then the prime ideal $\langle a_i x_j - a_j x_i : 0 \leq i < j \leq n \rangle$ is minimal. These prime ideals correspond to the prime ideals minimal among those containing I, which are finite in number [20, Theorem 3.1]. By Proposition 3.3.3, $\mathbf{V}_L(I)$ is a finite set.

That (ii) implies (i) is obvious.

To prove that (i) implies (iv), we first assume that $L \subseteq \overline{K}$. To each solution $(a_0, \ldots, a_n)$ in $\overline{K}$ we associate a vector space S generated by $a_i x_j - a_j x_i$, for $0 \leq i < j \leq n$. At least one of the coordinates of $(a_0, \ldots, a_n)$ is nonzero, say $a_0 \neq 0$. Then

$$S = \sum_{0 \leq i < j \leq n} (a_i x_j - a_j x_i)\overline{K} = \sum_{j=1}^{n} \left(x_j - \frac{a_j}{a_0} x_0 \right) \overline{K}$$

because

$$a_i x_j - a_j x_i = a_i \left(x_j - \frac{a_j}{a_0} x_0 \right) - a_j \left(x_i - \frac{a_i}{a_0} x_0 \right).$$

Let $y = y_0 x_0 + \cdots + y_n x_n \in A_{\overline{K}}^1$. Then $y \in S$ if and only if there exist $u_1, \ldots, u_n$ such that

$$\begin{aligned} y_0 x_0 + \cdots + y_n x_n &= u_1 \left(x_1 - \frac{a_1}{a_0} x_0 \right) + \cdots + u_n \left(x_n - \frac{a_n}{a_0} x_0 \right) \\ &= -\left(\frac{a_1}{a_0} u_1 + \cdots + \frac{a_n}{a_0} u_n \right) x_0 + u_1 x_1 + \cdots + u_n x_n \end{aligned}$$

that is,

$$y_0 = -\left(\frac{a_1}{a_0} u_1 + \cdots + \frac{a_n}{a_0} u_n \right), \; y_1 = u_1, \; \cdots, \; y_n = u_n.$$

Thus, $y \in S$ if and only if $a_0 y_0 + a_1 y_1 + \cdots + a_n y_n = 0$.

Hence, S is a proper subspace of $A_{\overline{K}}^1$, and since L is an infinite field, $S \cap A_L^1$ is also a proper subspace of A_L^1. Since there are only finitely many such subspaces S, there exists $y = y_0 x_0 + \cdots + y_n x_n \in A_L^1$ that does not belong to any of them.

Since $\mathbf{V}_{\overline{K}}(\langle I, y\rangle) = \emptyset$, by Theorem 3.3.2, there exists an integer d such that $\mathfrak{m}^d A_{\overline{K}} \subseteq A_{\overline{K}} y$. Suppose the annihilator of y in $A_{\overline{K}}$ is generated by $z_1, \ldots, z_s$, and let d' be the largest degree of the z_i.

Now, consider the ideal $J = \langle I, y-1\rangle \subseteq L[x_0, \ldots, x_n]$. There is a bijection between the projective variety $\mathbf{V}_{\overline{K}}(I)$ and the affine variety defined by J. Thus, $B = A_L/(y-1)A_L$ is a finitely generated L-vector space [16, Chapter 5, Section 3, Theorem 6]. It follows that there exists an integer d'' such that every element of B is the image of an element of degree at most d'' in A_L.

Set $D' = \max(d'', d+d') + 1$. We claim that multiplication by y is a surjection from $A_L^{D'-1}$ onto $A_L^{D'}$. Let $t \in A_L^{D'}$. Since every element in B is the image of an element of degree at most d'', there exist u and v in A_L such that

$$t = (y-1)u + v$$

with $\deg v \leq d'' < \deg t$. Let u' denote the homogeneous part of highest degree of u. Then $\deg u' \geq D' - 1 \geq d + d'$. Suppose $yu' = 0$. Then $u' \in Ann(y)$, which is generated by $z_1, \ldots, z_s$ with degrees at most d'. So we would have

$$u' \in \sum_{i=1}^{s} \mathfrak{m}^d A_{\overline{K}} z_i \subseteq \sum_{i=1}^{s} A_{\overline{K}} y z_i = 0,$$

which is a contradiction. It follows that $yu' \neq 0$, and hence $t = yu'$. This proves (iv) when $L \subseteq \overline{K}$. Note that this also shows that (i) implies (iii).

Now suppose that L is an infinite extension of K not contained in $\overline{K}$. Since (iii) holds and $\dim_L(A_L^d) = \dim_K(A)$ for all d, we have that $\dim_L(A_L^d) = \dim_L(A_L^D)$ for all $d \geq D$. We already proved that this implies $\mathbf{V}_{\overline{L}}(I)$ is finite, and applying the reasoning from the previous paragraph, we have that for all extensions $L' \subseteq \overline{L}$, there exist an integer D' and an element $y \in A_{L'}^1$ such that multiplication by y is a surjection from $A_{L'}^{D'-1}$ onto $A_{L'}^{D'}$. In particular, this holds for $L' = L$, proving (iv). □

Corollary 3.3.5. *If the conditions of Theorem 3.3.4 are satisfied, then multiplication by y is a bijection from A_L^d onto A_L^{d+1}, for all $d \geq \max\{D, D'\}$.*

Proof. This is a consequence of (iii) and (iv). □

Proposition 3.3.6. *If the conditions of Theorem 3.3.4 are satisfied, the number of points in $\mathbf{V}_{\overline{K}}(I)$ is at most $\dim_K(A^D)$.*

Proof. There is a bijection between the projective variety $\mathbf{V}_{\overline{K}}(I)$ and the affine variety defined by the ideal $\langle I, y-1\rangle$. Thus, the number of points in $\mathbf{V}_{\overline{K}}(I)$ is at most $\dim_L B$, where $B = A_L/(y-1)A_L$ [16, Chapter 5, Section 3, Theorem 6].

We will prove that $\dim_L B = \dim_K A^D$, by showing that the surjection from A_L onto B induces a bijection from A_L^d onto B, for $d > D'$, where D' is as in the proof of Theorem 3.3.4. Let $z \in A_L^d$ and assume z maps to zero, that is, $z = (y-1)t$, for some $t \in A_L$. Let t' denote the homogeneous part of highest degree in t. Then $\deg t' \geq D'$, and t' annihilates y, because z is homogeneous. By the same reasoning used in the proof of part (iv) of Theorem 3.3.4, this implies that $t' = 0$, and hence $t = 0$. It follows that the map $A_L^d \longrightarrow B$ is injective. □

Proposition 3.3.7. *Let $I \subseteq R$ be a homogeneous ideal and $A = R/I$. Then $\mathbf{V}_{\overline{K}}(I) = \emptyset$ if and only if there exists an integer D such that $A^d = 0$ for all $d \geq D$.*

Proof. Follows from Theorem 3.3.2 and from the fact that $\dim_K A^d = \dim_{\overline{K}} A_{\overline{K}}^d$ for all d. □

The main result of this section is the following theorem, which gives explicit bounds on the integers that appear in Theorem 3.3.4.

Theorem 3.3.8 (Lazard [37])**.** *Let $I = \langle f_1, \ldots, f_k\rangle$, with f_i homogeneous of degree d_i, and suppose $d_1 \geq d_2 \geq \cdots \geq d_k$. Then we may take $D = D' = d_1 + \cdots + d_{n+1} - n$ in the statement of Theorem 3.3.4, where $d_i = 1$ for $i \geq k$ if $k \leq n$.*

The results that follow are standard in commutative algebra and will be used in the proof of Theorem 3.3.8.

Proposition 3.3.9. *Let R be a commutative ring and P a prime ideal of R. Let M be a finitely generated R-module and A its annihilator. Then $M_P \neq 0$ if and only if $P \supseteq A$.*

Given a complex

$$A : \cdots \xrightarrow{\delta_{n+1}} A_n \xrightarrow{\delta_n} A_{n-1} \xrightarrow{\delta_{n-1}} \cdots \xrightarrow{\delta_2} A_1 \xrightarrow{\delta_1} A_0 \longrightarrow 0$$

denote its j-th homology module by $H_j(A)$, that is, $H_j(A) = \ker(\delta_j)/\operatorname{im}(\delta_{j+1})$.

Theorem 3.3.10 (Long exact sequence in homology)**.** *Let* $0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$ *be an exact sequence of complexes. Then there is a long exact sequence of homology modules*

$$\cdots \longrightarrow H_{j+1}(A) \longrightarrow H_{j+1}(B) \longrightarrow H_{j+1}(C) \xrightarrow{\delta} H_j(A) \longrightarrow H_j(B) \longrightarrow H_j(C) \longrightarrow \cdots$$

For a proof of Proposition 3.3.9, see [49], and for a proof of Theorem 3.3.10, see [35].

Given polynomials $f_1, \ldots, f_k$, let $I = \langle f_1, \ldots f_k \rangle$ and $A = R/I$. Consider the Koszul complex

$$\Lambda : 0 \longrightarrow \Lambda_k \xrightarrow{\delta_k} \Lambda_{k-1} \xrightarrow{\delta_{k-1}} \cdots \xrightarrow{\delta_2} \Lambda_1 \xrightarrow{\delta_1} \Lambda_0 \longrightarrow 0$$

where $\Lambda_0 = R$ and Λ_j is a free R-module of rank $\binom{k}{j}$, with basis $\{e_{i_1} \wedge \cdots \wedge e_{i_j} : 1 \leq i_1 < i_2 < \cdots < i_j \leq k\}$. The boundary maps δ_j are given by

$$\delta_1(e_i) = f_i$$

and

$$\delta_j(e_{i_1} \wedge \cdots \wedge e_{i_j}) = \sum_{\ell=1}^{j} (-1)^{\ell-1} f_{i_\ell} e_{i_1} \wedge \cdots \widehat{e_{i_\ell}} \wedge \cdots \wedge e_{i_j}$$

Let $H_j = \ker(\delta_j)/\operatorname{im}(\delta_{j+1})$ denote the homology modules. Note that $H_0 = A$, and since $\delta_k : \Lambda_k \cong Re_1 \wedge \cdots \wedge e_k \longrightarrow \Lambda_{k-1}$ is injective, $H_k = 0$. Suppose f_i has degree d_i, for $1 \leq i \leq k$, and assign degree $d_{i_1} + \cdots + d_{i_j}$ to the basis element $e_{i_1} \wedge \cdots \wedge e_{i_j}$. Then the modules Λ_j are graded, and the functions δ_j are homogeneous, and thus, for each degree d, we have a complex Λ^d of finitely generated K-vector spaces, with homology $H_j^d = \ker(\delta_j^d)/\operatorname{im}(\delta_{j+1}^d)$, where δ_j^d denotes the restriction of δ_j to the degree d homogeneous component Λ_j^d.

Assume the equivalent conditions of Theorem 3.3.4 are satisfied, and let $y \in A^1$ be such that multiplication by y from A^d into A^{d+1} is bijective for d sufficiently large. Then y comes from an element $Y \in R^1$, and we have the exact sequence

$$0 \longrightarrow R^{d-1} \xrightarrow{Y} R^d \longrightarrow (R/YR)^d \longrightarrow 0.$$

Consider the complex $\overline{\Lambda}$ obtained from the tensor product $\Lambda \otimes R/YR$. $\overline{\Lambda}$ is the Koszul

complex of the image of $f_1, \ldots, f_k$ in R/YR. Then we have the exact sequence of complexes

$$0 \longrightarrow \Lambda^{d-1} \longrightarrow \Lambda^d \longrightarrow \overline{\Lambda}^d \longrightarrow 0$$

and hence the exact homology sequence

$$\cdots \longrightarrow \overline{H}^d_{j+1} \longrightarrow H^{d-1}_j \longrightarrow H^d_j \longrightarrow \overline{H}^d_j \longrightarrow \cdots \tag{3.3}$$

where $\overline{H}_j$ denotes the homology of the complex $\overline{\Lambda}$.

For now, let us assume that the system $f_1 = \cdots = f_k = 0$ has no nontrivial solution. Then, by Theorem 3.3.4, $A^d = 0$ for d sufficiently large.

Lemma 3.3.11. *If $A^d = 0$ for sufficiently large d, then $H^d_j = 0$ for sufficiently large d, for all j.*

Proof. The hypothesis implies that the ideal $M = \langle x_0, \ldots, x_n \rangle$ is the only prime ideal containing I. Let P be another prime ideal, and consider the Koszul complex $\Lambda \otimes R_P$ of the ideal $I \otimes R_P \cong I_P$ of the localization R_P. Since P does not contain I, $I_P = R_P$, and it follows that the map $\delta_1 \otimes R_P : R^k \otimes R_P \longrightarrow R_P$ is surjective. Thus, there exists $\varepsilon \in \Lambda_1 \otimes R_P$ such that $(\delta_1 \otimes R_P)(\varepsilon) = 1$. For each $1 \leq j \leq k$, define the mapping $\varepsilon_j : \Lambda_j \otimes R_P \longrightarrow \Lambda_{j+1} \otimes$ by $\varepsilon_j(e_{i_1} \wedge \cdots \wedge e_{i_j}) = \varepsilon \wedge e_{i_1} \wedge \cdots \wedge e_{i_j}$.

$$\Lambda_{j+1} \otimes R_P \underset{\varepsilon_j}{\overset{\delta_{j+1}}{\rightleftarrows}} \Lambda_j \otimes R_P \underset{\varepsilon_{j-1}}{\overset{\delta_j}{\rightleftarrows}} \Lambda_{j-1} \otimes R_P$$

We claim $\varepsilon_{j-1} \circ (\delta_j \otimes R_P) + (\delta_{j+1} \otimes R_P) \circ \varepsilon_j$ is the identity map on $\Lambda_j \otimes R_P$. Suppose $\varepsilon = \frac{h_1}{g_1} e_1 + \cdots + \frac{h_k}{g_k} e_k$. Then $\delta_1(\varepsilon) = \frac{h_1}{g_1} f_1 + \cdots + \frac{h_k}{g_k} f_k = 1$. Let $e_{i_1} \wedge \cdots \wedge e_{i_j}$ be a basis element of $\Lambda_j \otimes R_P$. Then,

$$\begin{aligned}
\varepsilon_{j-1}(\delta_j \otimes R_P(e_{i_1} \wedge \cdots \wedge e_{i_j})) &= \\
\varepsilon_{j-1}\left(\sum_{\ell=1}^{j} (-1)^{\ell+1} f_{i_\ell} e_{i_1} \wedge \cdots \wedge \widehat{e_{i_\ell}} \wedge \cdots \wedge e_{i_j}\right) &= \\
\sum_{\ell=1}^{j} (-1)^{\ell+1} f_{i_\ell} \varepsilon_{j-1}(e_{i_1} \wedge \cdots \wedge \widehat{e_{i_\ell}} \wedge \cdots \wedge e_{i_j}) &= \\
\sum_{\ell=1}^{j} (-1)^{\ell+1} f_{i_\ell} \varepsilon \wedge e_{i_1} \wedge \cdots \wedge \widehat{e_{i_\ell}} \wedge \cdots \wedge e_{i_j} &=
\end{aligned}$$

$$\begin{aligned}
\sum_{\ell=1}^{j}(-1)^{\ell+1}f_{i_\ell}\left(\frac{h_1}{g_1}e_1+\cdots+\frac{h_k}{g_k}e_k\right)\wedge e_{i_1}\wedge\cdots\wedge\widehat{e_{i_\ell}}\wedge\cdots\wedge e_{i_j} &= \\
\sum_{\ell=1}^{j}\sum_{m=1}^{k}(-1)^{\ell+1}f_{i_\ell}\frac{h_m}{g_m}e_m\wedge e_{i_1}\wedge\cdots\wedge\widehat{e_{i_\ell}}\wedge\cdots\wedge e_{i_j} &= \\
\left(\sum_{\ell=1}^{j}f_{i_\ell}\frac{h_{i_\ell}}{g_{i_\ell}}\right)e_{i_1}\wedge\cdots\wedge e_{i_j}+ & \\
\sum_{\ell=1}^{j}\sum_{m\notin\{i_1,\ldots,i_j\}}(-1)^{\ell+1}f_{i_\ell}\frac{h_m}{g_m}e_m\wedge e_{i_1}\wedge\cdots\wedge\widehat{e_{i_\ell}}\wedge\cdots\wedge e_{i_j}. & \qquad (3.4)
\end{aligned}$$

For each $m\notin\{i_1,\ldots,i_j\}$, let M be such that $e_m\wedge e_{i_1}\wedge\cdots\wedge e_{i_j}=(-1)^M e_{i_1}\wedge\cdots\wedge e_m\wedge\cdots\wedge e_{i_j}$, with $i_1<\cdots<m<\cdots<i_j$. Then

$$\begin{aligned}
\sum_{\ell=1}^{j}(-1)^{\ell+1}f_{i_\ell}\frac{h_m}{g_m}e_m\wedge e_{i_1}\wedge\cdots\wedge\widehat{e_{i_\ell}}\wedge\cdots\wedge e_{i_j} &= \\
(-1)^{M-1}\frac{h_m}{g_m}\sum_{\ell=1}^{M}(-1)^{\ell+1}f_{i_\ell}e_{i_1}\wedge\cdots\wedge\widehat{e_{i_\ell}}\wedge\cdots\wedge e_m\wedge\cdots\wedge e_{i_j}+ & \\
(-1)^{M}\frac{h_m}{g_m}\sum_{\ell=M+1}^{j}(-1)^{\ell+1}f_{i_\ell}e_{i_1}\wedge\cdots\wedge e_m\wedge\cdots\wedge\widehat{e_{i_\ell}}\wedge\cdots\wedge e_{i_j}. & \qquad (3.5)
\end{aligned}$$

On the other hand

$$\begin{aligned}
\delta_{j+1}\otimes R_P(\varepsilon_j(e_{i_1}\wedge\cdots\wedge e_{i_j})) &= \\
\delta_{j+1}\otimes R_P(\varepsilon\wedge e_{i_1}\wedge\cdots\wedge e_{i_j}) &= \\
\delta_{j+1}\otimes R_P\left(\sum_{m=1}^{k}\frac{h_m}{g_m}e_m\wedge e_{i_1}\wedge\cdots\wedge e_{i_j}\right) &= \\
\sum_{m=1}^{k}\frac{h_m}{g_m}\delta_{j+1}\otimes R_P(e_m\wedge e_{i_1}\wedge\cdots\wedge e_{i_j}) &= \\
\sum_{m\notin\{i_1,\ldots,i_j\}}\frac{h_m}{g_m}\delta_{j+1}\otimes R_P(e_m\wedge e_{i_1}\wedge\cdots\wedge e_{i_j}). &
\end{aligned}$$

Now, for each $m\notin\{i_1,\ldots,i_j\}$, let M be such that $e_m\wedge e_{i_1}\wedge\cdots\wedge e_{i_j}=(-1)^M e_{i_1}\wedge\cdots\wedge e_m\wedge\cdots\wedge e_{i_j}$, with $i_1<\cdots<m<\cdots<i_j$. Then

$$\begin{aligned}
\delta_{j+1}\otimes R_P(e_m\wedge e_{i_1}\wedge\cdots\wedge e_{i_j}) &= \\
(-1)^M\delta_{j+1}\otimes R_P(e_{i_1}\wedge\cdots\wedge e_m\wedge\cdots\wedge e_{i_j}) &=
\end{aligned}$$

$$(-1)^M \sum_{\ell=1}^{M-1} (-1)^{\ell+1} f_{i_\ell} e_{i_1} \wedge \cdots \wedge \widehat{e_{i_\ell}} \wedge \cdots \wedge e_m \wedge \cdots \wedge e_{i_j} + f_m e_{i_1} \wedge \cdots \wedge e_{i_j} +$$
$$(-1)^M \sum_{\ell=M+1}^{j} (-1)^{\ell+2} f_{i_\ell} e_{i_1} \wedge \cdots \wedge e_m \wedge \cdots \wedge \widehat{e_{i_\ell}} \wedge \cdots \wedge e_{i_j}. \tag{3.6}$$

From equations (3.4), (3.5) and (3.6), we conclude that

$$\begin{aligned} \varepsilon_{j-1} \circ (\delta_j \otimes R_P)(e_{i_1} \wedge \cdots \wedge e_{i_j}) + (\delta_{j+1} \otimes R_P) \circ \varepsilon_j(e_{i_1} \wedge \cdots \wedge e_{i_j}) &= \\ \left(\frac{h_1}{g_1} f_1 + \cdots + \frac{h_k}{g_k} f_k \right) e_{i_1} \wedge \cdots \wedge e_{i_j} &= \\ e_{i_1} \wedge \cdots \wedge e_{i_j} \end{aligned}$$

and our claim is proved. Thus, if $\xi \in \ker(\delta_j \otimes R_P)$, then

$$\xi = (\delta_{j+1} \otimes R_P)(\varepsilon_j(\xi)) + \varepsilon_{j-1}((\delta_j \otimes R_P)(\xi)) = (\delta_{j+1} \otimes R_P)(\varepsilon_j(\xi))$$

and hence $\xi \in \operatorname{im}(\delta_{j+1} \otimes R_P)$, which implies $H_j \otimes R_P = 0$. Since $H_j \otimes R_P \cong (H_j)_P = 0$ for all $P \neq M$, it follows from Proposition 3.3.9 that M is the only prime ideal that contains the annihilator of H_j, and thus, H_j is annihilated by a power of M. Therefore, $H_j^d = 0$ for sufficiently large d. $\square$

Theorem 3.3.12. *Suppose $d_1 \geq d_2 \geq \cdots \geq d_k$. If $A^d = 0$ for sufficiently large d, then $H_j^d = 0$*

(i) *for all d if $j \geq k - n$,*

(ii) *for all $d \geq d_1 + \cdots + d_{j+n+1} - n$ if $j < k - n$.*

Proof. We proceed by induction on n. For $n = 0$, we need to show that $H_j^d = 0$ for all $d \geq d_1 + \cdots + d_{j+1}$ and $0 \leq j \leq k-1$. From the proof of Lemma 3.3.11 above we have that $H_j = \ker(\delta_j)/\operatorname{im}(\delta_{j+1})$ is annihilated by a power of $M = \langle x_0 \rangle$. Let $\xi \in \ker(\delta_j)$ be homogeneous of degree d. Then, there exists an integer h such that $x_0^h \xi \in \operatorname{im}(\delta_{j+1})$, that is, $x_0^h \xi = \delta_{j+1}(z)$ for some homogeneous $z \in \Lambda_{j+1}$. Write z as a combination of basis elements

$$z = \sum_{1 \leq i_1 < \cdots < i_{j+1} \leq k} c_{i_1,\ldots,i_{j+1}} x_0^{\alpha_{i_1,\ldots,i_{j+1}}} e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_{j+1}}$$

The degree of the basis elements of Λ_{j+1} is at most $d_1 + \cdots + d_{j+1}$. Suppose $d \geq d_1 + \cdots + d_{j+1}$.

Then

$$h + d_1 + \cdots + d_{j+1} \leq \deg(x_0^h \xi) = \deg(\delta_{j+1}(z)) = \deg(z)$$

hence

$$\deg(x_0^{\alpha_{i_1,\ldots,i_{j+1}}} e_{i_1} \wedge \cdots \wedge e_{i_{j+1}}) \geq h + d_1 + \cdots + d_{j+1}$$

Since

$$\deg(e_{i_1} \wedge \cdots \wedge e_{i_{j+1}}) \leq d_1 + \cdots + d_{j+1}$$

we conclude that $\alpha_{i_1,\ldots,i_{j+1}} \geq h$ for each $1 \leq i_1 < i_2 < \cdots < i_{j+1} \leq k$. Thus, we can divide by x_0^h and get

$$\xi = \delta_{j+1}\left(\sum_{1 \leq i_1 < i_2 < \cdots < i_{j+1} \leq k} c_{i_1,\ldots,i_{j+1}} x_0^{\alpha_{i_1,\ldots,i_{j+1}} - h} e_{i_1} \wedge \cdots \wedge e_{i_{j+1}}\right)$$

that is, $\xi \in \mathrm{im}(\delta_{j+1})$. Therefore, $H_j^d = 0$ for $d \geq d_1 + \cdots + d_{j+1}$.

Assume the result is true for $n-1$. Consider the complex $\overline{\Lambda}$. Since $R/YR \cong K[x_0, \ldots, x_{n-1}]$, the induction hypothesis implies that $\overline{H}_j^d = 0$ for (i) all d if $j \geq k - n + 1$ and (ii) $d \geq d_1 + \cdots + d_{j+n} - n + 1$ if $j < k - n + 1$.

We now use induction on d. By Lemma 3.3.11, $H_j^d = 0$ for sufficiently large d. Suppose $H_j^d = 0$, and either $j \geq k - n$, or $j < k - n$ and $d > d_1 + \cdots + d_{j+n+1} - n$. From the last paragraph, we have that $\overline{H}_{j+1}^d = 0$, and the exact sequence

$$\overline{H}_{j+1}^d \longrightarrow H_j^{d-1} \longrightarrow H_j^d$$

implies that $H_j^{d-1} = 0$. The result is then proved. □

Proof of Theorem 3.3.8. From the homology sequence in Equation (3.3), in particular we have that the following sequence is exact

$$\overline{H}_1^d \longrightarrow H_0^{d-1} \xrightarrow{y} H_0^d \longrightarrow \overline{H}_0^d,$$

where $H_0^{d-1} = A^{d-1}$ and $H_0^d = A^d$. Thus, to show that multiplication by y is bijective is equivalent to showing that $\overline{H}_1^d = \overline{H}_0^d = 0$.

Now note that Y was chosen so that the system $f_1 = \cdots = f_k = Y = 0$ has no nontrivial solution, and, thus, by Theorem 3.3.4, $\overline{A}^d = (R/\langle I, Y \rangle)^d = 0$ for sufficiently large d. Applying

Theorem 3.3.12, we have that $\overline{H}_0^d = 0$ for $d \geq d_1 + \cdots + d_n - n + 1$, and $\overline{H}_1^d = 0$ for $k = n$ or $k > n$ and $d \geq d_1 + \cdots + d_{n+1} - n + 1$.

Thus, multiplication by y is surjective for $d \geq d_1 + \cdots + d_n - n + 1$ and injective for $k = n$ or $d \geq d_1 + \cdots + d_{n+1} - n + 1$. Therefore, in the notation of Theorem 3.3.4, we may take $D' = d_1 + \cdots + d_n + 1 - n$, and $D = D'$ if $k = n$ and $D = d_1 + \cdots + d_{n+1} - n$ if $k > n$. With the convention that $d_{n+1} = 1$ if $k = n$, we have $\max\{D, D'\} = d_1 + \cdots + d_{n+1} - n$, which concludes the proof. □

We give a direct proof of Theorem 3.3.12 for the case $n = 0$, and, as a consequence, obtain a slightly different bound. Let us assume, for now, that $R = K[x]$, and that $f_i = x^{d_i}$, for $1 \leq i \leq k$, with $d_1 \geq d_2 \geq \cdots \geq d_k$. Since $H_0 = A = R/I$, it follows that $H_0^d = 0$ for $d \geq d_k$.

We now work the cases of H_1 and H_2, hoping they will help us understand the general case. Consider $H_1 = \ker(\delta_1)/\operatorname{im}(\delta_2)$. Let z be homogeneous of degree d in $\Lambda_1 \cong R^k$. Suppose $d \geq d_1$. Then,

$$z = c_1 x^{d-d_1} e_1 + \cdots + c_k x^{d-d_k} e_k,$$

with $c_i \in K$ for $1 \leq i \leq k$. Then,

$$\delta_1(z) = (c_1 + \cdots + c_k) x^d,$$

so that $z \in \ker(\delta_1)$ if and only if $c_1 + \cdots + c_k = 0$.

Claim 3.3.13. *If $d \geq d_1$, then the set $V = \{x^{d-d_i} e_i - x^{d-d_k} e_k, 1 \leq i \leq k-1\}$ forms a K-linear basis of $\ker(\delta_1)^d$.*

Proof. To see that V spans $\ker(\delta_1)^d$, note that if $z = c_1 x^{d-d_1} e_1 + \cdots + c_k x^{d-d_k} e_k \in \ker(\delta_1)^d$, then

$$\begin{aligned} z &= z - (c_1 + \cdots + c_k) x^{d-d_k} e_k \\ &= c_1(x^{d-d_1} e_1 - x^{d-d_k} e_k) + \cdots + c_{k-1}(x^{d-d_{k-1}} e_{k-1} - x^{d-d_k} e_k). \end{aligned}$$

That the elements of V are linearly independent follows from the fact that $e_1, \ldots, e_k$ are a basis of the R-module Λ_1, as

$$c_1(x^{d-d_1} e_1 - x^{d-d_k} e_k) + \cdots + c_{k-1}(x^{d-d_{k-1}} e_{k-1} - x^{d-d_k} e_k) =$$

$$c_1 x^{d-d_1} e_1 + \cdots + c_{k-1} x^{d-d_{k-1} e_{k-1}} - (c_1 + \cdots + c_{k-1}) x^{d-d_k} e_k.$$

□

Now, we show that each one of the basis elements are in the image of δ_2 for $d \geq d_1 + d_k$. In fact, for each $1 \leq i \leq k-1$,

$$x^{d-d_i} e_i - x^{d-d_k} e_k = \delta_2(-x^{d-d_i-d_k} e_i \wedge e_k).$$

Thus, $H_1^d = 0$ for $d \geq d_1 + d_k$.

Next, we consider $H_2 = \ker(\delta_2)/\operatorname{im}(\delta_3)$. For $d \geq d_1 + d_2$, a homogeneous element of degree d in Λ_2 has the form

$$z = \sum_{1 \leq i < j \leq k} c_{i,j} x^{d-d_i-d_j} e_i \wedge e_j,$$

and by applying δ_2, we have

$$\begin{aligned}
\delta_2(z) &= \sum_{1 \leq i < j \leq k} c_{i,j}(x^{d-d_j} e_j - x^{d-d_i} e_i) \\
&= -(c_{1,2} + c_{1,3} + \cdots + c_{1,k}) x^{d-d_1} e_1 + (c_{1,2} - c_{2,3} - \cdots - c_{2,k}) x^{d-d_2} e_2 \\
&\quad + (c_{1,3} + c_{2,3} - c_{3,4} - \cdots - c_{3,k}) x^{d-d_3} e_3 + \cdots \\
&\quad + (c_{1,k-1} + \cdots + c_{k-2,k-1} - c_{k-1,k}) x^{d-d_{k-1}} e_{k-1} \\
&\quad + (c_{1,k} + \cdots + c_{k-1,k}) x^{d-d_k} e_k.
\end{aligned}$$

So z is in the kernel of δ_2 if and only if the coefficients $c_{i,j}$ satisfy

$$\begin{aligned}
-(c_{1,2} + c_{1,3} + \cdots + c_{1,k}) &= 0 \\
c_{1,2} - c_{2,3} - \cdots - c_{2,k} &= 0 \\
&\vdots \\
c_{1,k} + \cdots + c_{k-1,k} &= 0.
\end{aligned}$$

Claim 3.3.14. *If $d \geq d_1 + d_2$, then the set $V = \{x^{d-d_i-d_j} e_i \wedge e_j - x^{d-d_i-d_k} e_i \wedge e_k + x^{d-d_j-d_k} e_j \wedge e_k, 1 \leq i < j < k\}$ forms a K-linear basis of $\ker(\delta_2)^d$.*

Proof. Suppose $z = \sum_{1\leq i<j\leq k} c_{i,j}x^{d-d_i-d_j}e_i \wedge e_j$ is in $\ker(\delta_2)$. Then,

$$\begin{aligned}
\sum_{1\leq i<j<k} c_{i,j}(x^{d-d_i-d_j}e_i \wedge e_j - x^{d-d_i-d_k}e_i \wedge e_k + x^{d-d_j-d_k}e_j) &= \\
\sum_{1\leq i<j\leq k} c_{i,j}(x^{d-d_i-d_j}e_i \wedge e_j - x^{d-d_i-d_k}e_i \wedge e_k + x^{d-d_j-d_k}e_j \wedge e_k) &= \\
z - (c_{1,2} + \cdots + c_{1,k})x^{d-d_1-d_k}e_1 \wedge e_k + & \\
(c_{1,2} - c_{2,3} - \cdots - c_{2,k})x^{d-d_2-d_k}e_2 \wedge e_k + \cdots + & \\
(c_{1,k} + \cdots + c_{k-1,k})x^{d-d_{k-1}-d_k}e_{k-1} \wedge e_k &= \quad z.
\end{aligned}$$

This shows that V spans $\ker(\delta_2)$. To see that the elements of V are linearly independent follows from the equations above and the fact that $\{e_i \wedge e_j, 1 \leq i < j \leq k\}$ is a basis of the free R-module Λ_2. □

Each one of the elements of the basis V above are in the image of δ_3 for $d \geq d_1 + d_2 + d_k$, as we can write

$$x^{d-d_i-d_j}e_i \wedge e_j - x^{d-d_i-d_k}e_i \wedge e_k + x^{d-d_j-d_k}e_j \wedge e_k = \delta_3(x^{d-d_i-d_j-d_k}e_i \wedge e_j \wedge e_k).$$

Hence $H_2^d = 0$ for $d \geq d_1 + d_2 + d_k$.

Now, we attack the general case. Let $1 \leq j \leq k$. Based on the cases $j = 1$ and $j = 2$ above, we "guess" a K-linear basis for $\ker(\delta_j)^d$, for $d \geq d_1 + \cdots + d_j + d_k$:

$$V = \{(-1)^j\delta_{j+1}(x^{d-d_{i_1}-\cdots-d_{i_j}-d_k}e_{i_1} \wedge \cdots \wedge e_{i_j} \wedge e_k), 1 \leq i_1 < \cdots < i_j < k\}.$$

Proposition 3.3.15. *The set V above is a K-linear basis of $\ker(\delta_j)^d$, for $d \geq d_1 + \cdots + d_j + d_k$.*

Proof. Let $d \geq d_1 + \cdots + d_j + d_k$ and $z \in \Lambda_j^d$. Write z as a combination of the basis elements

$$z = \sum_{1\leq i_1<\cdots<i_j\leq k} c_{i_1,\ldots,i_j}x^{d-d_{i_1}-\cdots-d_{i_j}}e_{i_1} \wedge \cdots \wedge e_{i_j}.$$

Applying δ_j we have

$$\delta_j(z) = \sum_{1\leq i_1<\cdots<i_j\leq k} \left[c_{i_1,\ldots,i_j}x^{d-d_{i_1}-\cdots-d_{i_j}}\left(\sum_{\ell=1}^{j}(-1)^{\ell+1}x^{d_{i_\ell}}e_{i_1} \wedge \cdots \wedge \widehat{e_{i_\ell}} \cdots \wedge e_{i_j}\right)\right]$$

and then we collect terms to write $\delta_j(z)$ as combination of basis elements of Λ^d_{j-1}

$$\delta_j(z) = \sum_{1\leq i_1<\cdots<i_{j-1}\leq k} b_{i_1,\ldots,i_{j-1}} x^{d-d_{i_1}-\cdots-d_{i_{j-1}}} e_{i_1}\wedge\cdots\wedge e_{i_{j-1}},$$

where

$$b_{i_1,\ldots,i_{j-1}} = \sum_{m=0}^{j-1} \sum_{i_m<\ell<i_{m+1}} (-1)^{m+2} c_{i_1,\ldots,i_m,\ell,i_{m+1},\ldots,i_{j-1}},$$

where $i_0 = 0$ and $i_j = k+1$.

On the other hand,

$$\begin{aligned}
\sum_{1\leq i_1<\cdots<i_j<k} c_{i_1,\ldots,i_j}(-1)^j \delta_{j+1}(x^{d-d_{i_1}-\cdots-d_{i_j}-d_k} e_{i_1}\wedge\cdots\wedge e_{i_j}\wedge e_k) &= \\
\sum_{1\leq i_1<\cdots<i_j\leq k} c_{i_1,\ldots,i_j}(-1)^j \delta_{j+1}(x^{d-d_{i_1}-\cdots-d_{i_j}-d_k} e_{i_1}\wedge\cdots\wedge e_{i_j}\wedge e_k) &= \\
(-1)^j \sum_{1\leq i_1<\cdots<i_j\leq k} \left[c_{i_1,\ldots,i_j} x^{d-d_{i_1}-\cdots-d_{i_j}-d_k} \sum_{\ell=1}^{j+1} (-1)^{\ell+1} x^{d_{i_\ell}} e_{i_1}\wedge\cdots\wedge \widehat{e_{i_\ell}}\wedge\cdots\wedge e_{i_j}\wedge e_k \right] &= \\
z + (-1)^j \sum_{1\leq i_1<\cdots<i_j\leq k} \left[c_{i_1,\ldots,i_j} x^{d-d_{i_1}-\cdots-d_{i_j}-d_k} \sum_{\ell=1}^{j} (-1)^{\ell+1} x^{d_{i_\ell}} e_{i_1}\wedge\cdots\wedge \widehat{e_{i_\ell}}\wedge\cdots\wedge e_{i_j}\wedge e_k \right] &= \\
z + (-1)^j \sum_{1\leq i_1<\cdots<i_{j-1}\leq k} b_{i_1,\ldots,i_{j-1}} x^{d-d_{i_1}-\cdots-d_{i_{j-1}}-d_k} e_{i_1}\wedge\cdots\wedge e_{i_{j-1}}\wedge e_k.
\end{aligned}$$

Thus, if $z\in\ker(\delta_j)$, then $b_{i_1,\ldots,i_{j-1}} = 0$ for all $1\leq i_1<\cdots<i_{j-1}\leq k$, and

$$z = \sum_{1\leq i_1<\cdots<i_j<k} c_{i_1,\ldots,i_j}(-1)^j \delta_{j+1}(x^{d-d_{i_1}-\cdots-d_{i_j}-d_k} e_{i_1}\wedge\cdots\wedge e_{i_j}\wedge e_k).$$

Hence V spans $\ker(\delta_j)^d$. That V is linearly independent follows from the equations above, where it is shown that the coefficients used to write z as a combination of elements of V are the same as the ones used to write z as a combination of the free basis of Λ_j. □

Corollary 3.3.16. *$H^d_j = 0$ for $d\geq d_1+\cdots+d_j+d_k$.*

Note that we instead of fixing e_k to form the basis elements

$$(-1)^j \delta_{j+1}(x^{d-d_{i_1}-\cdots-d_{i_j}-d_k} e_{i_1}\wedge\cdots\wedge e_{i_j}\wedge e_k),$$

we could have fixed any other index. In particular, fixing e_{j+1} would give the same result as Theorem

3.3.12 for $n = 0$. In fact, the same proof by induction extends the result for more variables, and we obtain the following theorems, analog to Theorem 3.3.12 and Theorem 3.3.8.

Theorem 3.3.17. *Suppose $d_1 \geq d_2 \geq \cdots \geq d_k$. If $A^d = 0$ for sufficiently large d, then $H_j^d = 0$*

(i) *for all d if $j \geq k - n$,*

(ii) *for all $d \geq d_1 + \cdots + d_{j+n} + d_k - n$ if $j < k - n$.*

Theorem 3.3.18. *Suppose the polynomials $f_1, \ldots, f_k$ are sorted in decreasing order of degrees, that is, $d_1 \geq d_2 \geq \cdots \geq d_k$. Then we may take $D = D' = d_1 + \cdots + d_n + d_k - n$ in the statement of Theorem 3.3.4.*

3.3.2 Degree bound

Definition 3.3.19. Let A be a graded ring. Define $\operatorname{depth}(A)$ to be 0 if there is no $x \in A^1$ such that $Ann(x) = 0$, or $1 + \operatorname{depth}(A/xA)$ if $x \in A^1$ and $Ann(x) = 0$.

In what follows, when we say *most changes of variables*, or *generic change of variables*, we mean changes of variable in a Zariski open set.

Let $f_1, \ldots, f_k$ be homogeneous polynomials in $K[x_0, \ldots, x_n]$ with degrees $d_1 \geq \cdots \geq d_k$. Let $I = \langle f_1, \ldots, f_k \rangle$ and $A = K[x_0, \ldots, x_n]/I$.

Theorem 3.3.20 (Lazard [36])**.** *Suppose one of the following conditions holds:*

(i) $\operatorname{depth}(A) \geq \dim(I)$*;*

(ii) $\operatorname{depth}(A) \geq n - 2$*;*

(iii) $\dim(I) \leq 0$*;*

(iv) $n \leq 2$.

Then, after most linear changes of variable, the elements of any minimal reduced Gröbner basis of I with respect to the graded reverse lexicographical order have degree at most $d_1 + \cdots + d_{r+1} - r$, where $r = n - \operatorname{depth}(A)$.

Lemma 3.3.21. *With the same hypothesis of Theorem 3.3.20, after most linear changes of variables, if $s = \dim(I)$, then*

(i) *every monomial of degree* $D = d_1 + \cdots + d_{r+1} - r$ *is congruent to an element of* $x_{n-s}A + x_{n-s+1}A + \cdots + x_nA$ *modulo* I*;*

(ii) *if* z *is a homogeneous polynomial of degree* $d > D$ *such that* $z \in I \cap (x_{n-s}A + \cdots + x_nA)$*, then* $z \in x_{n-s}I + \cdots + x_nI$*.*

Proof. First, we prove the result in the case $\dim(I) = 0$. We claim that, in this case, $\operatorname{depth}(A)$ is zero or one. In fact, if $\mathfrak{m}$ is an associated prime of I, then A contains no non-zero divisor, which implies $\operatorname{depth} A = 0$. If $\mathfrak{m}$ is not an associated prime of I, let $y \in A^1$ be such that $y(P) \neq 0$ for all $P \in \mathbf{V}_{\overline{K}}(I)$ (such y exists if K is infinite – or large enough). Then $Ann(y) = 0$, and since $(A/yA)^d = 0$ for d large, it follows that $\operatorname{depth}(A/yA) = 0$, which implies $\operatorname{depth}(A) = 1$.

After most linear changes of variable, x_n has the properties of y given in Theorem 3.3.4. To prove part (i), let m be a monomial of degree D. By Theorem 3.3.8, multiplication by x_n from $A^{D-1} \longrightarrow A^D$ is surjective. Thus, there exists $g \in A^{D-1}$ such that $gx_n = m$ in A^D.

To prove part (ii), let $z \in I \cap x_nA$. Suppose $z = x_ng$, with $g \in A$. Since $z \in I$, we have that $x_ng = z = 0$ in A. By Theorem 3.3.8, multiplication by x_n from $A^{d-1} \longrightarrow A^d$ is injective for $d > D$, so $g = 0$ in A, that is, $z \in x_nI$. This concludes the proof of the Lemma for zero-dimensional ideals.

Now suppose $\operatorname{depth} A \geq \dim I > 0$. Then, after a generic change of variables, x_n is such that $Ann(x_n) = 0$. Consider $\overline{A} = A/x_nA$; then $\operatorname{depth} \overline{A} = \operatorname{depth} A - 1$. Let $\overline{I} = \langle I, x_n \rangle$; then $\dim \overline{I} = \dim I - 1 = s - 1$. Assume the result is true for $\overline{A}$. To prove (i), let m be a monomial of degree D in $K[x_0, \ldots, x_n]$, and suppose $m \equiv g + x_nh \pmod{I}$, where $x_n \nmid g$. Then g is a K-linear combinations of monomials of degree D not divisible by x_n, say $g = \sum_i a_i m_i$.

If x_n does not divide m_i, then m_i can be seen as a monomial in $\overline{A}$, and thus m_i is congruent modulo $\overline{I}$ to an element of $x_{n-s}\overline{A} + \cdots + x_{n-1}\overline{A}$. It follows that m_i is congruent modulo I to an element of $x_{n-s}A + \cdots + x_nA$. So we can write $m_i \equiv \sum_{j=n-s}^{n} x_j g_{ij}$. Then

$$\begin{aligned} m &\equiv \sum_i a_i \sum_{j=n-s}^{n} x_j g_{ij} + x_nh \\ &\equiv \left(\sum_i a_i g_{in-s}\right) x_{n-s} + \cdots + \left(\sum_i a_i g_{in-1}\right) x_{n-1} + \left(\sum_i a_i g_i n + h\right) x_n \pmod{I}. \end{aligned}$$

For the proof of part (ii), suppose $z \in I \cap (x_{n-s}A + \cdots + x_nA)$. It immediately follows that $z \in \overline{I} \cap (x_{n-s}\overline{A} + \cdots + x_{n-1}\overline{A})$. The induction hypothesis implies that z is in $x_{n-s}\overline{I} + \cdots + x_{n-1}\overline{I}$,

so we can write z as

$$z = x_{n-s}h_{n-s} + \cdots + x_{n-1}h_{n-1} + h$$

where each $h_i \in \overline{I}$ and $h \in \overline{I}$. Then $h_i = h'_i + h''_i x_n$, with $h'_i \in I$, and $h = h' + h''x_n$, with $h' \in I$. Hence,

$$z = x_{n-s}h'_{n-s} + \cdots + x_{n-1}h'_{n-1} + (h''_{n-s} + \cdots + h''_{n-1} + h'')x_n + h'.$$

Since z, h'_{n-s}, ..., h'_{n-1} and h' are all in I, it follows that $(h''_{n-s} + \cdots + h''_{n-1} + h'')x_n \in I$. As $Ann(x_n) = 0$, it follows that $h''_{n-s} + \cdots + h''_{n-1} + h'' \in I$. Therefore $z \in x_{n-s}I + \cdots + x_nI$. □

Proof of Theorem 3.3.20. Let G be a Gröbner basis of I and $D = d_1 + \cdots + d_{r+1} - r$. Let $G' = \{g \in G : \deg(g) \leq D\}$. Let $g \in I$, and suppose $\deg(g) = d > D$. We want to show that $\mathrm{lm}(g)$ is a multiple of the leading monomial of some element of G'. Since we are using a graded order, the leading monomial of g equals the leading monomial of its homogeneous part of degree d, so we can assume g is homogeneous.

If $\mathrm{lm}(g)$ does not depend on $x_{n-s}, \ldots, x_n$, then it is a multiple of some monomial m of degree D not depending on $x_{n-s}, \ldots, x_n$. By Lemma 3.3.21, there exist $g_{n-s}, g_{n-s+1}, \ldots, g_n$ such that m is congruent to $x_{n-s}g_{n-s} + \cdots + x_ng_n$ modulo I. It follows that $G_m = m - x_{n-s}g_{n-s} - \cdots - x_ng_n \in I$, and, because we are using the reverse lexicographical order, $\mathrm{lm}(G_m) = m$. It follows that m is a multiple of the leading monomial of some element in G', and thus so is $\mathrm{lm}(g)$.

If $\mathrm{lm}(g)$ depends on $x_{n-s}, \ldots, x_n$, then all terms in g depend on $x_{n-s}, \ldots, x_n$, hence $g \in x_{n-s}A + \cdots + x_nA$. By Lemma 3.3.21, $g \in x_{n-s}I + \cdots + x_nI$, and so $\mathrm{lm}(g)$ is a multiple of the leading monomial of some element of I of degree $d-1$. Induction on the degree shows that the leading monomial of all elements in I are multiples of the leading terms of elements in G', hence G' is a Gröbner basis. □

The following example shows that the linear change of variables cannot be avoided.

Example 3.3.22. Consider again the Masser and Philippon ideal in Example 3.2.5. Homogenize the polynomials $f_1, \ldots, f_n$ to get

$$\begin{aligned} F_1 &= x_1^d \\ F_2 &= x_1x_{n+1}^{d-1} - x_2^d \\ &\vdots \end{aligned}$$

$$\begin{aligned} F_{n-1} &= x_{n-2}x_{n+1}^{d-1} - x_{n-1}^d \\ F_n &= x_{n+1}^d - x_{n-1}x_n^{d-1} \end{aligned}$$

and then let $J = \langle F_1, \ldots, F_n \rangle \subset K[x_1, \ldots, x_{n+1}]$. Note that the solutions to the system $F_1 = \cdots = F_n = 0$ have the form $(0, \ldots, 0, x_n, 0)$, so that there are finitely many (projective) solutions, and Lazard's result holds. Let H be the reduced Gröbner basis of J with respect to the graded reverse lexicographic order. Since $1 \in I$, by Lemma 3.2.3, there is an integer s such that $x_{n+1}^s \in J$. Since H is a Gröbner basis, $\mathrm{lm}(h)$ divides x_{n+1}^s, for some $h \in H$, which implies that $\mathrm{lm}(h) = x_{n+1}^t$, for some $t \geq 0$. Because we are using the grevlex order, it follows that $h = x_{n+1}^t$. We can write

$$x_{n+1}^t = G_1F_1 + \cdots + G_nF_n$$

with $G_i \in K[x_1, \ldots, x_{n+1}]$ homogeneous, as $F_1, \ldots, F_n$ are all homogeneous of degree d. Dehomogenizing we get

$$1 = G_1(x_1, \ldots, x_n, 1)f_1 + \cdots + G_n(x_1, \ldots, x_n, 1)f_n$$

which implies that

$$\deg G_1 \geq \deg_{x_n} G_1(x_1, \ldots, x_n, 1) \geq (d-1)d^{n-1}.$$

So $\deg h = t \geq d + (d-1)d^{n-1}$. ♢

In [36], there is, in fact, a result that does not require any change of variables. However, it applies only in the affine zero-dimensional case.

Theorem 3.3.23 (Lazard [36])**.** *Let $I = \langle f_1, \ldots, f_k \rangle$ be an ideal in $K[x_1, \ldots, x_n]$, with $\deg(f_i) = d_i$ for $1 \leq i \leq k$ and $d_1 \geq d_2 \geq \cdots \geq d_k$. Let $\tilde{I} = \langle \tilde{f}_1, \ldots, \tilde{f}_k \rangle \subset K[x_0, \ldots, x_n]$, where $\tilde{f}_i$ is the homogenization of f_i. If $\dim(\tilde{I}) \leq 0$, then the polynomials of every minimal reduced Gröbner basis of I have degree at most $d_1 + \cdots + d_n - n + 1$.*

Proof. Let $\tilde{A} = K[x_0, \ldots, x_n]/\tilde{I}$, and let $\tilde{A}^d$ denote its homogeneous part of degree d. By Theorems 3.3.4 and 3.3.8, there exists $\tilde{y} \in \tilde{A}^1$ such that multiplication by $\tilde{y}$ is a surjection from $\tilde{A}^{d-1}$ to $\tilde{A}^d$, for $d \geq D = d_1 + \cdots + d_n - n + 1$.

Now let $A = K[x_1, \ldots, x_n]/I$, and let A_d denote the image in A of the set of polynomials of degree at most d. Then $A_d \subset A_{d+1}$ for every d. The function that takes $f \in \tilde{A}^d$ to $f(1, x_1, \ldots, x_n) \in$

A_d is a surjection, and if $y = \tilde{y}(1, x_1, \ldots, x_n)$, then the following diagram commutes

$$\begin{array}{ccc} \tilde{A}^{d-1} & \xrightarrow{\tilde{y}} & \tilde{A}^d \\ \downarrow & & \downarrow \\ A_{d-1} & \xrightarrow{y} & A_d \end{array}$$

which shows that multiplication by y is a surjection from A_{d-1} to A_d, for $d \geq D$. Thus, $\dim_K A_d \leq \dim_k A_{d-1}$, and since $A_{d-1} \subset A_d$, we have $A_{d-1} = A_d$. This implies that every monomial of degree greater than D is congruent modulo I to a polynomial of degree at most D. By the same argument used in the proof of Theorem 3.3.20, if G is any reduced Gröbner basis for I, then $G' = \{g \in G : \deg(g) \leq D\}$ is also a Gröbner basis for I. □

3.3.3 Generic initial ideals and regularity

By allowing a generic change of variables, we obtain initial ideals that depend only on the monomial order, but not on the coordinates. The *generic initial ideal* is a combinatorial invariant that contains a lot of information.

Throughout this section we assume the field K is infinite. Let $GL_n(K)$ denote the general linear group, that is, the group of invertible $n \times n$ matrices with coefficients in the field K. For an invertible matrix $g = (g_{ij}) \in GL_n(K)$ and a polynomial $f \in K[x_1, \ldots, x_n] \in R$, let g act on f by

$$g \cdot f = f(gx_1, \ldots, gx_n),$$

where

$$gx_j = \sum_{i=1}^{n} g_{ij} x_i.$$

Given an ideal $I \subset R$, let

$$g \cdot I = \{g \cdot f | f \in I\}.$$

Theorem 3.3.24. *Let I be a homogeneous ideal in R. Then there is a Zariski open set $U \subset GL_n(K)$ and a monomial ideal $J \subset R$ such that, for all $g \in U$, $\text{in}(g \cdot I) = J$.*

Proof. See [19, Theorem 15.18]. □

Definition 3.3.25. Let I and J be as in Theorem 3.3.24. Then, J is called the *generic initial ideal* of I, and denoted $\text{gin}(I)$.

Thus, Theorem 3.3.20 actually gives a bound on the degree of generators of the generic initial ideal. If the field K has characteristic zero, then this degree equals the *regularity* of the ideal I, which is another important invariant.

To define the regularity, let $\mathfrak{m} = \langle x_1, \ldots, x_n \rangle$. Given a graded R-module M, we let $H^i_{\mathfrak{m}}(M)_d$ denote the degree d part of the i-th local cohomology group of M.

Definition 3.3.26. A homogeneous ideal $I \subset K[x_1, \ldots, x_n]$ is said to be m-regular if equivalently

(i) There exists a free resolution

$$0 \longrightarrow \bigoplus_j S(-e_{rj}) \longrightarrow \cdots \longrightarrow \bigoplus_j S(-e_{1j}) \longrightarrow \bigoplus_j S(-e_{0j}) \longrightarrow I \longrightarrow 0$$

of I, with $e_{ij} - i \leq m$, for all i, j.

(ii) $H^i_{\mathfrak{m}}(I)_d = 0$ for all i and $d \geq m - i + 1$.

The *Castelnuovo-Mumford regularity*, or simply *regularity*, of I is defined to be the least m for which I is m-regular, and is denoted by $\text{reg}(I)$.

The following theorem due to Bayer and Stillman makes the connection between the regularity and the generic initial ideal.

Theorem 3.3.27 (Bayer and Stillman [5])**.** *Let I be a homogeneous ideal in R, with* $\text{reg}(I) = m$. *If the characteristic of K is zero, then* $\text{gin}(I)$ *has a minimal generator of degree m.*

Examples of ideals with high regularity show that Lazard's conjecture is not true in general. The following example, from [6], is based on Mayr and Meyer ideal.

Example 3.3.28. Consider the ideal J_n from Example 3.1.1. We introduce a homogenizing variable z, and consider the ideal K_n generated by the homogenized generators of J_n and $S - F$. K_n is an ideal with $10n+1$ generators in the polynomial ring in $10n+1$ variables. It is proved in [6] that K_n has a minimal syzygy of degree $n + 2e_0 + \cdots + 2e_{n-1} + 1$. $\diamondsuit$

This example shows that any bound for the regularity must grow double exponentially in the number of variables and the number of generators.

Chapter 4

Gröbner Bases of Generic Ideals

A K-algebra A is of type $(n, d_1, \ldots, d_r)$ if A is isomorphic $K[x_1, \ldots, x_n]/\langle f_1, \ldots, f_r \rangle$, for homogeneous polynomials f_i, with $\deg(f_i) = d_i$. We consider the Hilbert series of A

$$S_A(z) = \sum_{i=0}^{\infty} \dim_K(A_i) z^i.$$

Let B be another graded K-algebra. We say $S_A(z) \leq S_B(z)$ if $\dim_K(A_i) \leq \dim_K(B_i)$ for all $i \geq 0$. We ask, among all the K-algebras of type $(n, d_1, \ldots, d_r)$, what are the minimal Hilbert series? As shown in Section 4.1, the smallest Hilbert series coefficientwise is given by a generic algebra, that is, $K[x_1, \ldots, x_n]/\langle g_1, \ldots, g_r \rangle$, where $g_1, \ldots, g_r$ are generic polynomials of degree $d_1, \ldots, d_r$.

In Section 4.1, we present conjectures concerning generic ideals. Section 4.2 contains properties of the standard basis $\mathrm{B}(I)$ for $I = \langle f_1, \ldots, f_n \rangle \subset K[x_1, \ldots, x_n]$ a generic ideal. In Section 4.3, we describe an incremental method to construct Gröbner bases from [25]. In Section 4.4, we apply this incremental method for generic ideals. We give a description of the initial ideal of such ideals when the degrees of generators satisfy a certain condition. As a result, we are able to give a partial answer to Moreno-Socías conjecture.

4.1 Generic Ideals and Moreno-Socías Conjecture

Let $R = K[x_1, \ldots, x_n]$ be the polynomial ring in n variables over an infinite field K, which is an extension of a base field F.

Definition 4.1.1. (i) A polynomial $f \in R$ of degree d is called *generic* over F if

$$f = \sum_{\alpha} c_\alpha x^\alpha,$$

where the sum runs over all monomials of degree d in R, and the coefficients c_α are algebraically independent over F.

(ii) An ideal $I \subset R$ is generic if it is generated by generic polynomials $f_1, \ldots, f_r$ with all the coefficients algebraically independent over F.

We are interested in Gröbner bases, or initial ideals, of generic ideals with respect to the graded reverse lexicographic (grevlex) order. In what follows, this is the only monomial order used. We are particularly interested in a conjecture by Moreno-Socías [44], related to the weak reverse lexicographic property.

Definition 4.1.2. Let $J = \langle x^{\alpha_1}, \ldots, x^{\alpha_r} \rangle$ be a monomial ideal, and suppose $x^{\alpha_1}, \ldots, x^{\alpha_r}$ are minimal generators, that is, these monomials are not divisible by one another. J is said to be *almost reverse lexicographic*, or *weakly reverse lexicographic*, if, for every i, J contains every monomial x^α such that $\deg x^\alpha = \deg x^{\alpha_i}$ and $x^\alpha > x^{\alpha_i}$.

Example 4.1.3. (i) Let $J = \langle x_1^2, x_1x_2, x_2^2 \rangle \subset R = \mathbb{C}[x_1, x_2]$. Then J is almost reverse lexicographic, since its generators are all the monomials of degree 2 in R.

(ii) Let $J = \langle x_1^2, x_1x_2^3, x_1^2x_2x_3 \rangle \subset \mathbb{C}[x_1, x_2, x_3]$. We verify the condition for each generator. For x_1^2, since there is no greater monomial of degree 2, the condition is satisfied. For $x_1x_2^3$, the monomials of same degree and greater than $x_1x_2^3$ are $x_1^2x_2^2, x_1^3x_2, x_1^4$, which are all in J, thus the condition is satisfied. Now, note that the third generator $x_1^2x_2x_3$ is not minimal, as it is divisible by x_1^2. So we do not need to check the condition for this monomial. It follows that J is almost reverse lexicographic.

(iii) Let $J = \langle x_2 \rangle \subset \mathbb{C}[x_1, x_2]$. Then J is not almost reverse lexicographic, because x_1 is a monomial of the same degree as x_2 such that $x_1 > x_2$, but $x_1 \notin J$.

$\diamondsuit$

Conjecture 4.1.4 (Moreno-Socías [44])**.** *If I is a generic homogeneous ideal in R, then the initial ideal of I is almost reverse lexicographic.*

The following is a weaker version of the Moreno-Socías conjecture, restricted to generic ideals generated by n polynomials.

Conjecture 4.1.5. *Let $I = \langle f_1, \ldots, f_n \rangle$ be a generic ideal in R. Then $\operatorname{lm}(I)$ is almost reverse lexicographic.*

It turns out that Conjecture 4.1.5 implies the case where the number r of polynomials is different from the number of variables. We now state a few results that will be useful here. For proofs, see Section 15.7 in [19].

Lemma 4.1.6. *Let $I \subset R$ be a homogeneous ideal, and $G = \{g_1, \ldots, g_r\}$ a Gröbner basis for I. Then*

(i) $\operatorname{lm}(I + \langle x_n \rangle) = \operatorname{lm}(I) + \langle x_n \rangle$. *Thus $G \cup \{x_n\}$ is a Gröbner basis for $I + \langle x_n \rangle$*

(ii) $(\operatorname{lm}(I) : x_n) = \operatorname{lm}(I : x_n)$. *Furthermore, setting*

$$\widetilde{g}_i = \frac{g_i}{\gcd(x_n, g_i))},$$

we have that $\widetilde{G} = \{\widetilde{g}_1, \ldots, \widetilde{g}_r\}$ is a Gröbner basis for $(I : x_n)$

Lemma 4.1.7. *Let $I \subset R$ be a homogeneous ideal. Then $x_n, x_{n-1}, \ldots, x_r$ form a regular sequence on R/I if and only if $x_n, x_{n-1}, \ldots, x_r$ form a regular sequence on $R/\operatorname{lm}(I)$.*

Lemma 4.1.8. *Let $N \subset R$ be a monomial ideal minimally generated by $\{n_1, \ldots, n_t\}$. A sequence of monomials $m_1, \ldots, m_u \in R$ is a regular sequence modulo N if and only if each m_i is relatively prime to each n_ℓ and to each m_j for $j \neq i$.*

Proposition 4.1.9. *Conjecture 4.1.5 implies Conjecture 4.1.4.*

Proof. Let $I = \langle f_1, \ldots, f_r \rangle$ be a generic ideal in R. First, assume that $n < r$. We consider generic polynomials $F_1, \ldots, F_r \in S = K[x_1, \ldots, x_r]$ such that the image of F_i in $S/\langle x_{n+1}, \ldots, x_r \rangle = R$ is f_i, for $1 \leq i \leq r$. Let $J = \langle F_1, \ldots, F_r \rangle$. Assuming Conjecture 4.1.5 holds, $\operatorname{lm}(J)$ is almost reverse lexicographic. The image of an almost reverse lexicographic ideal in the quotient $R/\langle x_r \rangle$ is also almost reverse lexicographic, so the initial ideal

$$\operatorname{lm}(J)/\langle x_r \rangle = \operatorname{lm}(J/\langle x_r \rangle)$$

is almost reverse lexicographic. Repeating this argument for variables x_{r-1}, x_{r-2}, ..., x_{n+1}, we conclude that $\operatorname{lm}(I)$ is almost reverse lexicographic.

Now suppose $r < n$, and let $I = \langle f_1, \ldots, f_r \rangle$ be a generic ideal in $R = K[x_1, \ldots, x_n]$. Then $f_1, \ldots, f_r, x_n, \ldots, x_{r+1}$ is a regular sequence. By Lemma 4.1.7, $x_n, \ldots, x_{r+1}$ is a regular sequence in $R/\operatorname{lm}(I)$, and by Lemma 4.1.8, $\operatorname{lm}(I)$ is generated by monomials not divisible by $x_n, \ldots, x_{r+1}$. Thus, the generators of $\operatorname{lm}(I)$ are the same as the generators of the initial ideal of the image of I in $K[x_1, \ldots, x_n]$. Since this initial ideal is almost reverse lexicographic, it follows that so is $\operatorname{lm}(I)$. □

Partial answers to Moreno-Socías Conjecture have been given in the case $n = 2$ by Aguirre *et al.* [2] and Moreno-Socías [44], $n = 3$ by Cimpoeaş [15], and the case for $d_1, \ldots, d_n$ satisfying $d_i > \sum_{j=1}^{i} d_j - i + 1$ by Cho and Park [14]. In this chapter, we give a new proof for the result in [14] and also show a stronger result.

Another longstanding conjecture on generic ideals is Fröberg conjecture.

Conjecture 4.1.10 (Fröberg [23]). *If I is a generic ideal generated by generic polynomials $f_1, \ldots, f_r \in R$ of degrees $d_1, \ldots, d_r$, respectively, then the Hilbert series of R/I, $S_{R/I}(z)$, is given by*

$$S_{R/I}(z) = \left| \frac{\prod_{i=1}^{r}(1 - z^{d_i})}{(1-z)^n} \right|.$$

The notation above means the following: if $\sum_{d=0}^{\infty} a_d z^d$ is a power series with integer coefficients, then

$$\left| \sum_{d=0}^{\infty} a_d z^d \right| = \sum_{d=0}^{\infty} b_d z^d$$

where $b_d = a_d$ if $a_i > 0$ for $0 \leq i \leq d$, and $b_d = 0$ otherwise.

In [45] Pardue shows that the Moreno-Socías conjecture implies a series of other conjectures. In particular, it implies the Fröberg conjecture. This was also proven by Cho and Park [14].

Proposition 4.1.11 (Pardue [45], Cho and Park [14]). *The Moreno-Socías Conjecture implies the Fröberg Conjecture, that is, if the Moreno-Socías Conjecture is true for any number r of generic polynomials in a polynomial ring $K[x_1, \ldots, x_n]$, then the Fröberg Conjecture is also true for any r.*

Conjecture 4.1.10 has been proven in some cases. The proofs in general were done not by dealing with generic ideals directly. They make use of the following results.

Given two power series $\sum_{d=0}^{\infty} a_d z^d$ and $\sum_{d=0}^{\infty} b_d z^d$, we say that $\sum_{d=0}^{\infty} a_d z^d \leq \sum_{d=0}^{\infty} b_d z^d$ if and only if $a_d \leq b_d$ for all d.

Lemma 4.1.12. *Let $I = \langle f_1, \ldots, f_r \rangle$ be any homogeneous ideal in R, and let $G = \langle g_1, \ldots, g_r \rangle$ be a generic ideal in R, such that $\deg(f_i) = \deg(g_i) = d_i$ for $1 \leq i \leq r$. Then*

$$S_{R/I}(z) \geq S_{R/G}(z).$$

In particular, $S_{R/G}(z)$ depends only on $n, d_1, \ldots, d_r$.

Proof. Let I and G be as in the statement. Suppose $g_i = \sum_{|\alpha|=d_i} C_{i\alpha} x^\alpha$, with the $C_{i\alpha}$'s in K algebraically independent over F. We have the following exact sequence

$$R^r \xrightarrow{\varphi} R \longrightarrow R/G \longrightarrow 0$$

where $\varphi(\mathbf{e}_i) = g_i$, which induces the exact sequence of K-vector spaces

$$(R^r)_d \xrightarrow{\varphi} R_d \longrightarrow (R/G)_d \longrightarrow 0,$$

where we define $\deg(\mathbf{e}_i) = d_i$, for $1 \leq i \leq r$. It follows that

$$\begin{aligned} H_{R/G}(d) = \dim_K (R/G)_d &= \dim_K R_d - \dim_K G_d \\ &= \dim_K R_d - \dim_K \operatorname{im}(\varphi)_d \\ &= \dim_K R_d - \operatorname{rank} M \end{aligned}$$

where M is the matrix of the restriction of φ to R_d^r, whose columns are the coefficients of mg_i in the basis of monomials of degree d, where m is a monomial of degree $d - d_i$.

Now, suppose $f_i = \sum_{|\alpha|=d_i} c_{i\alpha} x^\alpha$. Since the coefficients of the g_i's are algebraically independent over F, there is a ring homomorphism $\psi : K \longrightarrow K$ such that ψ fixes every element in F, and $\psi(C_{i\alpha}) = c_{i\alpha}$. We extend ψ to $R \longrightarrow R$ by setting $\psi(x_i) = x_i$. Then, we have the exact sequence

$$(R^r)_d \xrightarrow{\widetilde{\varphi}} R_d \longrightarrow (R/I)_d \longrightarrow 0,$$

where $\widetilde{\varphi} = \psi \circ \varphi$, that is, $\widetilde{\varphi}(\mathbf{e}_i) = f_i$. Thus,

$$H_{R/I}(d) = \dim_K (R/I)_d = \dim_K R_d - \operatorname{rank} \widetilde{M},$$

where $\widetilde{M}$ is the matrix of the restriction of $\widetilde{\varphi}$ to R_d^r. Since $\operatorname{rank} M \geq \operatorname{rank} \widetilde{M}$, we conclude that $H_{R/I} \leq H_{R/G}$. □

We denote the generic Hilbert series from Lemma 4.1.12 by $\mathfrak{S}_{n,\mathbf{d}}(z)$, where $\mathbf{d} = (d_1, \ldots, d_r)$. We can also use a lexicographic order to compare series, where $\sum_{d=0}^{\infty} a_d z^d \prec \sum_{d=0}^{\infty} b_d z^d$ if and only if there is $i \in \mathbb{N}$ such that $a_d = b_d$ for $d < i$, and $a_i < b_i$. The following result was proven in [23].

Theorem 4.1.13 (Fröberg [23])**.** *If* $\mathbf{d} = (d_1, \ldots, d_r)$*, then*

$$\mathfrak{S}_{n,\mathbf{d}}(z) \succeq \left| \frac{\prod_{i=1}^{r}(1 - z^{d_i})}{(1-z)^n} \right|.$$

Combining Lemma 4.1.12 and Theorem 4.1.13, we have the following.

Proposition 4.1.14. *If there exists an ideal* $I = \langle f_1, \ldots, f_r \rangle \in R$*, with* $\deg(f_i) = d_i$*, such that* $S_{R/I}(z) = \left| \frac{\prod_{i=1}^{r}(1-z^{d_i})}{(1-z)^n} \right|$*, then*

$$\mathfrak{S}_{n,\mathbf{d}}(z) = \left| \frac{\prod_{i=1}^{r}(1 - z^{d_i})}{(1-z)^n} \right|.$$

Proof. We have

$$S_{R/I}(z) = \left| \frac{\prod_{i=1}^{r}(1 - z^{d_i})}{(1-z)^n} \right| \geq \mathfrak{S}_{n,\mathbf{d}}(z) \succeq \left| \frac{\prod_{i=1}^{r}(1 - z^{d_i})}{(1-z)^n} \right|,$$

which implies that the inequalities are actually equalities. □

Thus, one can prove the Fröberg Conjecture by presenting an ideal satisfying the condition of Proposition 4.1.14. For $r \leq n$, for instance, the ideal $\langle x_1^{d_1}, \ldots, x_r^{d_r} \rangle$ works. Other cases where Fröberg Conjecture is known to be true include

(i) $n = 2$ [23],

(ii) $n = 3$ [3],

(iii) $r = n + 1$ [23],

(iv) $d_1 = \cdots = d_r = 2$ and $n \leq 11$, $d_1 = \cdots = d_r = 3$ and $n \leq 8$ [24].

4.2 Structure of standard bases of generic ideals

Let $f_1, \ldots, f_n$ be generic polynomials in R, with $\deg(f_i) = d_i$ for $1 \leq i \leq n$. Let $I = \langle f_1, \ldots, f_n \rangle$ and $A = R/I$. Define

$$\begin{aligned} \delta &= d_1 + \cdots + d_n - n, \\ \delta^* &= d_1 + \cdots + d_{n-1} - (n-1), \\ \sigma &= \min\{\delta^*, \lfloor \delta/2 \rfloor\}, \\ \mu &= \delta - 2\sigma. \end{aligned}$$

The Hilbert series of A is known to be a symmetrical polynomial of degree δ, given by

$$S(z) = \frac{\prod_{j=1}^{n}(1 - z^{d_j})}{(1-z)^n} = \sum_{\nu=0}^{\delta} a_\nu z^\nu$$

with $0 < a_0 < \cdots < a_\sigma = \cdots = a_{\sigma+\mu} > \cdots > a_\delta > 0$ (see [44, Proposition 2.2]). Let $B = \mathrm{B}(I)$, so that $a_\nu = |B_\nu|$.

To prove the properties of $\mathrm{B}(I)$ we need in our proofs, we use a result from [44]. For $e \geq 0$, we define

$$\begin{aligned} B^e &= \{x_1^{\alpha_1} \cdots x_{n-1}^{\alpha_{n-1}} x_n^{\alpha_n} \in B | \alpha_n = e\} \subset K[x_1, \ldots, x_n], \\ \widetilde{B}^e &= \{x_1^{\alpha_1} \cdots x_{n-1}^{\alpha_{n-1}} | x_1^{\alpha_1} \cdots x_{n-1}^{\alpha_{n-1}} x_n^e \in B\} \subset K[x_1, \ldots, x_{n-1}]. \end{aligned}$$

Proposition 4.2.1 (Moreno-Socías [44])**.** *With the notation above,*

$$\widetilde{B}^0 = \widetilde{B}^1 = \cdots = \widetilde{B}^\mu,$$

$$\widetilde{B}^{\mu+1} = \widetilde{B}^{\mu+2}, \ldots, \widetilde{B}^{\delta-1} = \widetilde{B}^\delta,$$

and

$$\widetilde{B}^{\delta-2\lambda} = \{m \in \widetilde{B}^0 | \deg(m) \leq \lambda\},$$

for $0 \leq \lambda < \sigma$.

Lemma 4.2.2. *Let* $0 \leq i \leq \frac{\delta}{2}$. *Then* $B_{\delta-i} = x_n^{\delta-2i} B_i$.

Proof. Note that $B_{\delta-i} = x_n^{\delta-2i} B_i$ if and only if $\widetilde{B}_i^e = \widetilde{B}_{\delta-i}^{e+\delta-2i}$, for all $e \geq 0$. We then apply Proposition 4.2.1 to see the sections are equal.

For $e > i$, $\widetilde{B}_i^e = \emptyset$, and $e + \delta - 2i > \delta - i$, so $\widetilde{B}_{\delta-i}^{e+\delta-2i} = \emptyset = \widetilde{B}_i^e$.

If $e + \delta - 2i \leq \mu$, then $\widetilde{B}_i^e = \widetilde{B}_{\delta-i}^{e+\delta-2i} = \widetilde{B}_{i-e}^0$.

If $e \leq \mu$ and $e + \delta - 2i > \mu$, then $\widetilde{B}_i^e = \widetilde{B}_{i-e}^0$, and $\widetilde{B}_{\delta-i}^{e+\delta-2i} = \{m \in \widetilde{B}_{i-e}^0 | \deg(m) \leq \lambda\}$, where $e + \delta - 2i = \delta - 2\lambda$ or $e + \delta - 2i = \delta - 2\lambda - 1$. We need to see that $i - e \leq \lambda$. In the first case we have $\lambda = \frac{2i-e}{2} \geq \frac{2i-2e}{2} = i - e$, and in the second case, $\lambda = \frac{2i-e-1}{2} \geq \frac{2i-e-e}{2} = i - e$, as $e \geq 1$.

Now, if $e > \mu$, then

$$\widetilde{B}^e = \{m \in \widetilde{B}^0 | \deg(m) \leq \lambda\},$$

where $e = \delta - 2\lambda$ or $e = \delta - 2\lambda - 1$, and

$$\widetilde{B}^{e+\delta-2i} = \{m \in \widetilde{B}^0 | \deg(m) \leq \lambda'\},$$

where $e + \delta - 2i = \delta - 2\lambda'$ or $e + \delta - 2i = \delta - 2\lambda' - 1$. We want to see that $i - e \leq \lambda$ if and only if $i - e \leq \lambda'$.

Suppose $e = \delta - 2\lambda$ and $e + \delta - 2i = \delta - 2\lambda'$. This happens when δ is even, giving $\lambda' = \lambda + i - \frac{\delta}{2}$. Then,

$$i - e \leq \lambda \Longrightarrow \lambda' = \lambda + i - \frac{\delta}{2} = i - \frac{e}{2} \geq i - e,$$

and

$$i - e \leq \lambda' \Longrightarrow \lambda \geq \lambda + i - \frac{\delta}{2} = \lambda' \geq i - e,$$

as $i - \frac{\delta}{2} \leq 0$.

If $e = \delta - 2\lambda$ and $e + \delta - 2i = \delta - 2\lambda' - 1$, with δ odd and $\lambda' = \lambda + i - \frac{\delta-1}{2}$, then

$$i - e \leq \lambda \Longrightarrow \lambda' = \lambda + i - \frac{\delta - 1}{2} = i - \frac{e}{2} \geq i - e$$

and

$$i - e \leq \lambda' \Longrightarrow \lambda \geq \lambda + i - \frac{\delta - 1}{2} = \lambda' \geq i - e$$

as $i - \frac{\delta-1}{2} \leq 0$.

Suppose $e = \delta - 2\lambda - 1$ and $e + \delta - 2i = \delta - 2\lambda'$, with δ odd and $\lambda' = \lambda + i - \frac{\delta+1}{2}$. Then,

$$i - e \leq \lambda \Longrightarrow \lambda' = \lambda + i - \frac{\delta+1}{2} = i - \left(\frac{e}{2} + 1\right) \geq i - e,$$

as $e > \mu \geq 1$ ($\mu = 0$ would contradict the fact that δ is odd), and

$$i - e \leq \lambda' \Longrightarrow \lambda = \lambda + i - \frac{\delta+1}{2} = i - \left(\frac{e}{2} + 1\right) \geq i - e.$$

Finally, if $e = \delta - 2\lambda - 1$ and $e + \delta - 2i = \delta - 2\lambda' - 1$, with δ an even integer and $\lambda' = \lambda + i - \frac{\delta}{2}$, then

$$i - e \leq \lambda \Longrightarrow \lambda' = \lambda + i - \frac{\delta}{2} = i - \frac{e+1}{2} \geq i - e,$$

as $e > \mu \geq 0$, and

$$i - e \leq \lambda' \Longrightarrow \lambda \geq \lambda + i - \frac{\delta}{2} = i - \frac{e+1}{2} \geq i - e.$$

□

Lemma 4.2.3. *Let $0 \leq j \leq \delta$ and $r \geq 0$. Then multiplication by x_n^r from A_j to A_{j+r} is either injective or surjective. More precisely:*

(i) *Suppose $|B_j| \leq |B_{j+r}|$. Let S denote the subset of B_{j+r} consisting of $|B_j|$ smallest monomials in B_{j+r}. Then*

$$S = x_n^r B_j.$$

(ii) *Suppose $|B_j| \geq |B_{j+r}|$. Let S denote the subset of B_j consisting of $|B_{j+r}|$ smallest monomials in B_j. Then*

$$B_{j+r} = x_n^r S.$$

Proof. First, suppose $0 \leq j \leq \delta/2$ and $j + r \leq \delta - j$. Then $|B_j| \leq |B_{j+r}|$. By Lemma 4.2.2, $B_{\delta-j} = x_n^{\delta-2j} B_j$, so multiplication by $x_n^{\delta-2j}$ from A_j to $A_{\delta-j}$ is bijective. This multiplication can be seen as the composition

$$A_j \xrightarrow{x_n^r} A_{j+r} \xrightarrow{x_n^{\delta-2j-r}} A_{\delta-j}$$

so that multiplication by x_n^r from A_j to A_{j+r} must be injective. Moreover, if m is a monomial in B_j, $x_n^{\delta-2j} m$ is in $B_{\delta-j}$, which implies $x_n^r m \in B_{j+r}$. So, $x_n^r B_j \subseteq B_{j+r}$. Suppose $B_j = \{x^{\alpha_1}, \ldots, x^{\alpha_N}\}$,

with $x^{\alpha_1} < \cdots < x^{\alpha_N}$, and suppose m is a monomial in B_{j+r} such that $m < x^{\alpha_i} x_n^r$. Then x_n^r divides m, and $m' = m/x_n^r \in B_j$, with $m' < x^{\alpha_i}$. This proves (i).

Now suppose $0 \leq j \leq \delta/2$ and $j + r \geq \delta - i$. Then $|B_j| \geq |B_{j+r}|$. Let m be a monomial in B_{j+r}. Since $B_{j+r} = x_n^{2(j+r)-\delta} B_{\delta-j-r}$, we can write $m = x_n^{2(j+r)-\delta} m'$, for some monomial $m' \in B_{\delta-j-r}$. By the previous paragraph, $m'' = x_n^{2j+r-\delta} m' \in B_j$, so $m = x_n^r m''$. So multiplication by x_n^r is surjective. Moreover, the monomials $m'' \in B_j$ that are taken to $m \in B_{j+r}$ are in the image of $B_{\delta-j-r}$ under multiplication by $x_n^{2j+r-\delta}$, and, by part (i), correspond to the smallest monomials in B_j.

If $\delta/2 \geq j \geq \delta$, then $|B_j| \geq |B_{j+r}|$, and the same argument from the previous paragraph works. □

4.3 Incremental Gröbner bases

Let I be any ideal in R and suppose G is a Gröbner basis for I with respect to some monomial order. Let g be any polynomial in R. We now describe the method given in [25] to obtain a Gröbner basis of the ideal $\langle I, g \rangle$. This method is useful in attacking the Moreno-Socías Conjecture.

Let $B = \mathrm{B}(I) = \{x^{\alpha_1}, x^{\alpha_2}, \ldots, x^{\alpha_N}\}$. Note that when I is not zero-dimensional, we have $N = \infty$.

Suppose $x^{\alpha_i} g \equiv h_i \pmod{G}$, where $h_i \in R$ is a K-linear combination of monomials in B, for $1 \leq i \leq N$. We can write this as

$$\begin{pmatrix} x^{\alpha_1} \\ x^{\alpha_2} \\ \vdots \\ x^{\alpha_N} \end{pmatrix} \cdot g \equiv \begin{pmatrix} h_1 \\ h_2 \\ \vdots \\ h_N \end{pmatrix} \pmod{G}. \tag{4.1}$$

We apply row operations to both sides of Equation (4.1) as follows: for $1 \leq i < j \leq N$ and $a \in K$, subtract from the j-th row the i-th row multiplied by a. Our goal is to eliminate equal leading terms. So if $\mathrm{lm}(h_i) = \mathrm{lm}(h_j)$, with $i < j$, we use a row operation to eliminate the leading term of h_j. This means we only perform row operations downward. We start with h_1, using the first row to eliminate the leading term of all h_j bellow that have the same leading monomial as h_1. Then we pass to the leading monomial of the new second row, and eliminate the leading terms of

all h_j's with the same leading monomial. Then we go to the new third row, and so on. Since the monomial order is a well ordering, any decreasing sequence of monomials must be finite. Hence we perform only a finite number of row operations on row j, using rows above it. By induction, we may assume that Equation (4.1) can be transformed into the form

$$\begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_N \end{pmatrix} \cdot g \equiv \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_N \end{pmatrix} \pmod{G} \tag{4.2}$$

where $u_i, v_i \in R$ are K-linear combinations of monomials in B, and for $1 \leq i < j \leq N$ with $v_i, v_j \neq 0$, we have $\mathrm{lm}(v_i) \neq \mathrm{lm}(v_j)$, that is, the nonzero rows in the right-hand side of (4.2) have distinct leading monomials. We illustrate this procedure with an example.

Example 4.3.1. Let $G = \{f_1, f_2, f_3\}$, where

$$\begin{aligned} f_1 &= x_1x_2^2 - x_1 + x_2, \\ f_2 &= -x_1^2 + x_1x_2 + x_2^2, \\ f_3 &= x_2^3 + x_1 - 2x_2. \end{aligned}$$

It is easy to see that G is a Gröbner basis for the ideal $I = \langle G \rangle$ with respect to the grevlex order. The standard basis is given by

$$\mathrm{B}(I) = \{1, x_2, x_1, x_2^2, x_1x_2\}.$$

Now, let $g = x_1x_2 - x_2^2 + x_2$. Then

$$\begin{pmatrix} 1 \\ x_2 \\ x_1 \\ x_2^2 \\ x_1x_2 \end{pmatrix} \cdot g \equiv \begin{pmatrix} x_1x_2 - x_2^2 + x_2 \\ x_2^2 + 2x_1 - 3x_2 \\ x_1x_2 - x_1 + 2x_2 \\ 2x_1x_2 - 3x_2^2 - x_1 + 2x_2 \\ -x_1x_2 + 2x_2^2 + x_1 - x_2 \end{pmatrix} \pmod{G}.$$

The leading monomial of the right-hand side of the first row is x_1x_2, which is also the leading

monomial in rows 3, 4 and 5. So we perform the following row operations to cancel leading terms:

$$\begin{aligned} \text{row } 3 &:= \text{row } 3 - \text{row } 1 , \\ \text{row } 4 &:= \text{row } 4 - 2\,\text{row } 1 , \\ \text{row } 5 &:= \text{row } 5 + \text{row } 1 . \end{aligned}$$

This gives

$$\begin{pmatrix} 1 \\ x_2 \\ x_1 - 1 \\ x_2^2 - 2 \\ x_1x_2 + 1 \end{pmatrix} \cdot g \equiv \begin{pmatrix} x_1x_2 - x_2^2 + x_2 \\ x_2^2 + 2x_1 - 3x_2 \\ x_2^2 - x_1 + x_2 \\ -x_2^2 - x_1 \\ x_2^2 + x_1 \end{pmatrix} \pmod{G}. \tag{4.3}$$

The leading monomial of the right-hand side of the second row is still x_2^2, as the second row was not changed. New rows 3, 4 and 5 have the same leading monomial. The row operations

$$\begin{aligned} \text{row } 3 &:= \text{row } 3 - \text{row } 2 , \\ \text{row } 4 &:= \text{row } 4 + \text{row } 2 , \\ \text{row } 5 &:= \text{row } 5 - \text{row } 2 \end{aligned}$$

transform Equation (4.3) into

$$\begin{pmatrix} 1 \\ x_2 \\ x_1 - x_2 - 1 \\ x_2^2 + x_2 - 2 \\ x_1x_2 - x_2 + 1 \end{pmatrix} \cdot g \equiv \begin{pmatrix} x_1x_2 - x_2^2 + x_2 \\ x_2^2 + 2x_1 - 3x_2 \\ -3x_1 + 4x_2 \\ x_1 - 3x_2 \\ -x_1 + 3x_2 \end{pmatrix} \pmod{G}.$$

The leading monomial of the new third, fourth and fifth rows is x_1, so we use the third row to cancel the leading terms in rows bellow it. The operations

$$\text{row } 4 := \text{row } 4 + \frac{1}{3}\,\text{row } 3 ,$$

$$\text{row } 5 \quad := \quad \text{row } 5 \; - \frac{1}{3} \text{ row } 3 \; ,$$

give

$$\begin{pmatrix} 1 \\ x_2 \\ x_1 - x_2 - 1 \\ x_2^2 + \frac{1}{3}x_1 + \frac{2}{3}x_2 - \frac{7}{3} \\ x_1x_2 - \frac{1}{3}x_1 - \frac{2}{3}x_2 + \frac{4}{3} \end{pmatrix} \cdot g \equiv \begin{pmatrix} x_1x_2 - x_2^2 + x_2 \\ x_2^2 + 2x_1 - 3x_2 \\ -3x_1 + 4x_2 \\ -\frac{5}{3}x_2 \\ \frac{5}{3}x_2 \end{pmatrix} \pmod{G}.$$

Finally, the row operation

$$\text{row } 5 \; := \; \text{row } 5 \; + \; \text{row } 4$$

transforms the equation above into

$$\begin{pmatrix} 1 \\ x_2 \\ x_1 - x_2 - 1 \\ x_2^2 + \frac{1}{3}x_1 + \frac{2}{3}x_2 - \frac{7}{3} \\ x_1x_2 + x_2^2 - 1 \end{pmatrix} \cdot g \equiv \begin{pmatrix} x_1x_2 - x_2^2 + x_2 \\ x_2^2 + 2x_1 - 3x_2 \\ -3x_1 + 4x_2 \\ -\frac{5}{3}x_2 \\ 0 \end{pmatrix} \pmod{G}.$$

After the row operations, we obtain polynomials on the right-hand side with distinct leading monomials. As the next theorem shows, adding these polynomials to G we have a Gröbner basis for $\langle I, g \rangle$. ♢

Theorem 4.3.2 (Gao, Guan and Volny [25])**.** *Let $\widetilde{G} = G \cup \{v_i | 1 \leq i \leq N\}$. Then $\widetilde{G}$ is a Gröbner basis of $\langle I, g \rangle$.*

Proof. Let $f \in \langle I, g \rangle$. Then

$$f \equiv wg \pmod{G}$$

for some $w \in R$ of the form

$$w = \sum_{i=1}^{N} w_i x^{\alpha_i}$$

where $w_i \in K$, and there are only a finite number of nonzero coefficients w_i.

Since Equation (4.2) was obtained from (4.1) by a sequence of row operations, there is an

$N \times N$ nonsingular lower triangular matrix U, with entries in K, such that

$$\begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_N \end{pmatrix} = U \begin{pmatrix} x^{\alpha_1} \\ x^{\alpha_2} \\ \vdots \\ x^{\alpha_N} \end{pmatrix} \text{ and } \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_N \end{pmatrix} = U \begin{pmatrix} h_1 \\ h_2 \\ \vdots \\ h_N \end{pmatrix},$$

where each row of U contains only finitely many nonzero entries. Let

$$(c_1, \ldots, c_N) = (w_1, \ldots, w_N)U^{-1} \in K^N.$$

Since U is lower triangular and $(w_1, \ldots, w_N)$ has only finitely many nonzero entries, $(c_1, \ldots, c_N)$ also has only finitely many nonzero entries and

$$\begin{aligned} wg &\equiv (w_1, \ldots, w_N)U^{-1}U \begin{pmatrix} h_1 \\ h_2 \\ \vdots \\ h_N \end{pmatrix} \pmod{G} \\ &= (c_1, \ldots, c_N) \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_N \end{pmatrix} \\ &= \sum_{i=1}^{N} c_i v_i. \end{aligned}$$

Thus, f can be reduced to 0 by $\widetilde{G}$. Since f is an arbitrary polynomial in $\langle I, g \rangle$, this implies that $\widetilde{G}$ is a Gröbner basis for $\langle I, g \rangle$. □

4.4 Gröbner bases of generic ideals

Now, let us return to the generic setting. We want to apply the method above to generic ideals. Let $f_1, \ldots, f_n$ and g denote generic polynomials in the polynomial ring in $n+1$ variables $K[x_1, \ldots, x_n, z]$, with $\deg(f_i) = d_i$ for $1 \leq i \leq n$ and $\deg(g) = d$. Let $f_i^* = f_i(x_1, \ldots, x_n, 0) \in$

$K[x_1,\ldots,x_n]$, for $1 \leq i \leq n$. Then $f_1^*,\ldots,f_n^*$ are generic polynomials in $K[x_1,\ldots,x_n]$. Suppose G^* is a reduced Gröbner basis of the ideal I^* generated by $f_1^*,\ldots,f_n^*$ in $K[x_1,\ldots,x_n]$, and let $B = \mathrm{B}(I^*) \subset K[x_1,\ldots,x_n]$. Let $a_i = |B_i|$ and $\delta = d_1 + \cdots + d_n - n$. Suppose G is a reduced Gröbner basis of $I = \langle f_1,\ldots,f_n\rangle \subset K[x_1,\ldots,x_n,z]$, and let $E = \mathrm{B}(I)$. Since the generators of $\mathrm{lm}(I)$ are the same as the generators of $\mathrm{lm}(I^*)$, we have that $\mathrm{lm}(G) = \mathrm{lm}(G^*)$, and

$$\begin{aligned} E &= \{mz^\ell | m \in B,\ \ell \geq 0\} \\ &= B \cup zB \cup z^2B \cup z^3B \cup \cdots . \end{aligned}$$

For each $0 \leq i \leq \delta$,

$$E_i = B_i \cup zB_{i-1} \cup z^2B_{i-1} \cup \cdots \cup z^{i-1}B_1 \cup z^iB_0,$$

and for $i \geq \delta$,

$$E_i = z^{i-\delta}B_\delta \cup z^{i-\delta+1}B_{\delta-1} \cup \cdots \cup z^{i-1}B_1 \cup z^iB_0.$$

Suppose $g = c_1m_1 + c_2m_2 + \cdots + c_Nm_N$, where $m_1 > m_2 > \cdots > m_N$ are all the monomials of degree d in $K[x_1,\ldots,x_n,z]$ and $N = \binom{n+d}{d}$. Let $G = \{g_1,\ldots,g_r\}$. Since the coefficients of $f_1,\ldots,f_n$ and g are algebraically independent, it follows that the coefficients of g are algebraically independent of the coefficients of the elements of G. Reducing g modulo G we get

$$N_G(g) = g - t_1g_{i_1} - t_2g_{i_2} - \cdots - t_sg_{i_s}$$

where $t_1,\ldots,t_s$ are terms. We obtain $N_G(g)$ which is a linear combination of monomials in E of degree d with coefficients of the form

$$c_j - a_1c_{j_1} - \cdots - a_\ell c_{j_\ell}$$

with $j_1 < \cdots < j_\ell < j$. Thus, the coefficients of $N_G(g)$ are still algebraically independent over F, and are algebraically independent over the extension of F generated by the coefficients of elements of G.

From now on we assume that g is reduced modulo G, that is, we take g to be a linear combination of monomials in E_d with coefficients algebraically independent over the extension of F generated by coefficients of elements of G.

Let $\mathbf{B}$ and $\mathbf{E}$ denote the column vectors whose entries are the monomials in B and E, respectively, listed in decreasing order, according to the reverse lexicographic order. Let M be the matrix satisfying

$$\mathbf{E}g \equiv M\mathbf{E} \pmod{G}. \tag{4.4}$$

Note that all polynomials involved are homogeneous. So, for a monomial $m \in E_i$, the product mg is homogeneous and its reduced form is a homogenous polynomial of degree $i + d$, that is, a K-linear combination of monomials in E_{i+d} only. Also, the row operations can only be performed using two rows containing polynomials of the same degree. Thus, we consider rows of different degrees separately. Let M_i denote the matrix such that

$$\mathbf{E}_i g \equiv M_i \mathbf{E}_{i+d} \pmod{G}. \tag{4.5}$$

Furthermore, note that for $i > \delta$, $\mathbf{E}_i = z^{i-\delta}\mathbf{E}_\delta$ and

$$\mathbf{E}_i g \equiv z^{i-\delta} M_\delta \mathbf{E}_{\delta+d} \pmod{G}.$$

Thus, the Gröbner basis elements obtained at this point are redundant, and we only need to consider $\mathbf{E}_i g$ for $0 \leq i \leq \delta$.

Lemma 4.4.1. *The rows of M_i are linearly independent, for $1 \leq i \leq \delta$.*

Proof. Denote the rows of M_i by $\mathbf{v}_1, \ldots, \mathbf{v}_\ell$, and suppose $\mathbf{E}_i = (m_1, \ldots, m_\ell)^{\mathrm{T}}$. Assume $c_1\mathbf{v}_1 + \cdots + c_\ell\mathbf{v}_\ell = 0$, with $c_1, \ldots, c_\ell \in K$. Then

$$(c_1 m_1 + \cdots + c_\ell m_\ell)g \equiv c_1\mathbf{v}_1 + \cdots + c_\ell\mathbf{v}_\ell \equiv 0 \pmod{G}.$$

Since g is regular, g is not a zero divisor in R/I, and it follows that $c_1 m_1 + \cdots + c_\ell m_\ell = 0$ in R/I. Since the monomials in E_i are K-linear independent, it follows that $c_j = 0$ for all $1 \leq j \leq \ell$. Hence, $\mathbf{v}_1, \ldots, \mathbf{v}_\ell$ are linearly independent. □

Thus, each matrix M_i has rank $|E_i|$. To be able to describe $\mathrm{lm}(I, g)$, we need to see which columns are linearly independent.

4.4.1 Case I: $d \geq \delta$

First, we assume $d \geq \delta$. Since the degree of monomials in B is at most δ, in this case g can be written as

$$g = \mathbf{v}_\delta \cdot \mathbf{B}_\delta z^{d-\delta} + \mathbf{v}_{\delta-1} \cdot \mathbf{B}_{\delta-1} z^{d-\delta+1} + \cdots + \mathbf{v}_1 \cdot \mathbf{B}_1 z^{d-1} + \mathbf{v}_0 \cdot \mathbf{B}_0 z^d,$$

where $\mathbf{B}_i$ denotes the column vector whose entries are the monomials in B_i listed in decreasing order, according to the reverse lexicographic order, and $\mathbf{v}_i$ is a row vector of coefficients.

Let A_i denote the matrix such that

$$\mathbf{B}_i g \equiv A_i \mathbf{E}_{i+d} \pmod{G}.$$

Since $d > \delta$, $E_{i+d} = z^{i+d-\delta} E_\delta$ for all $0 \leq i \leq \delta$. So (4.4) can be written in the form

$$\mathbf{E}_i g = \begin{pmatrix} \mathbf{B}_i \\ z\mathbf{B}_{i-1} \\ \vdots \\ z^i \mathbf{B}_0 \end{pmatrix} g \equiv \begin{pmatrix} A_i \\ A_{i-1} \\ \vdots \\ A_0 \end{pmatrix} \mathbf{E}_{i+d} \pmod{G},$$

that is,

$$M_i = \begin{pmatrix} A_i \\ A_{i-1} \\ \vdots \\ A_0 \end{pmatrix}.$$

Thus, all matrices M_i are submatrices of M_δ. The rows and columns can be indexed by elements of B. For $0 \leq i \leq \delta/2$, we denote by Γ_i the submatrix, or block, formed by entries on rows corresponding to B_i, and columns corresponding to $B_{\delta-i}$. For $0 \leq i \leq \delta$, we denote by Θ_i the submatrix formed by entries on rows and columns corresponding to B_i. Let $m = \lfloor \delta/2 \rfloor$. If δ is odd, then the blocks Γ_i and Θ_i appear in M_δ as follows:

$$M_\delta = \begin{array}{c} \begin{array}{cccccccc} \mathbf{B}_\delta & \mathbf{B}_{\delta-1} & \cdots & \mathbf{B}_{m+1} & \mathbf{B}_m & \cdots & \mathbf{B}_1 & \mathbf{B}_0 \end{array} \\ \begin{pmatrix} \Theta_\delta & & & & & & & \\ & \Theta_{\delta-1} & & & & & & \\ & & \ddots & & & & & \\ & & & \Theta_{m+1} & & & & \\ & & & \Gamma_m & \Theta_m & & & \\ & & \iddots & & & \ddots & & \\ & \Gamma_1 & & & & & \Theta_1 & \\ \Gamma_0 & & & & & & & \Theta_0 \end{pmatrix} \end{array} \begin{array}{c} \mathbf{B}_\delta \\ \mathbf{B}_{\delta-1} \\ \vdots \\ \mathbf{B}_{m+1} \\ \mathbf{B}_m \\ \vdots \\ \mathbf{B}_1 \\ \mathbf{B}_0 \end{array}.$$

If δ is even, then $\Gamma_m = \Theta_m$, and M_δ is given by

$$M_\delta = \begin{array}{c} \begin{array}{ccccccccc} \mathbf{B}_\delta & \mathbf{B}_{\delta-1} & \cdots & \mathbf{B}_{m+1} & \mathbf{B}_m & \mathbf{B}_{m-1} & \cdots & \mathbf{B}_1 & \mathbf{B}_0 \end{array} \\ \begin{pmatrix} \Theta_\delta & & & & & & & & \\ & \Theta_{\delta-1} & & & & & & & \\ & & \ddots & & & & & & \\ & & & \Theta_{m+1} & & & & & \\ & & & & \Gamma_m & & & & \\ & & & \Gamma_{m-1} & & \Theta_{m-1} & & & \\ & & \iddots & & & \ddots & & \vdots & \\ & \Gamma_1 & & & & & & \Theta_1 & \\ \Gamma_0 & & & & & & & & \Theta_0 \end{pmatrix} \end{array} \begin{array}{c} \mathbf{B}_\delta \\ \mathbf{B}_{\delta-1} \\ \vdots \\ \mathbf{B}_{m+1} \\ \mathbf{B}_m \\ \mathbf{B}_{m-1} \\ \\ \mathbf{B}_1 \\ \mathbf{B}_0 \end{array}.$$

In what follows, we give properties of the blocks Γ_i and Θ_i.

Lemma 4.4.2. *Let $0 \le i \le \delta/2$, and let $c_{\delta-2i}$ denote the last component of $\mathbf{v}_{\delta-2i}$. Then the square submatrix Γ_i of A_i formed by the columns corresponding to monomials in $\mathbf{B}_{\delta-i}z^{d+2i-\delta}$ has diagonal entries of the form*

$$c_{\delta-2i} + L, \tag{4.6}$$

where L is a linear function of coefficients in $\mathbf{v}_\delta, \ldots, \mathbf{v}_{\delta-2i}$, except $c_{\delta-2i}$. The coefficient $c_{\delta-2i}$ does not appear in any other entry of the matrix A_i.

Proof. Since g is given by

$$g = \mathbf{v}_\delta \cdot \mathbf{B}_\delta z^{d-\delta} + \mathbf{v}_{\delta-1} \cdot \mathbf{B}_{\delta-1} z^{d-\delta+1} + \cdots + \mathbf{v}_1 \cdot \mathbf{B}_1 z^{d-1} + \mathbf{v}_0 \cdot \mathbf{B}_0 z^d,$$

we have

$$\begin{aligned} \mathbf{B}_i g &= \mathbf{B}_i(\mathbf{v}_\delta \cdot \mathbf{B}_\delta z^{d-\delta} + \mathbf{v}_{\delta-1} \cdot \mathbf{B}_{\delta-1} z^{d-\delta+1} + \cdots + \mathbf{v}_0 \cdot \mathbf{B}_0 z^d) \\ &= \sum_{j=0}^{\delta} \mathbf{B}_i(\mathbf{v}_j \cdot \mathbf{B}_j) z^{d-j}. \end{aligned}$$

For $j = \delta - 2i$, the last component of $\mathbf{B}_j$ is $x_n^{\delta-2i}$. Suppose

$$\mathbf{B}_i = (x^{\alpha_1}, \ldots, x^{\alpha_{a_i}})^{\mathrm{T}}.$$

By Lemma 4.2.2, the product $x^{\alpha_i} x_n^{\delta-2i}$ is in $B_{\delta-i}$, thus the term

$$c_{\delta-2i} x^{\alpha_j} x_n^{\delta-2i}$$

is reduced modulo G. Larger terms might need to be reduced, which would produce a coefficient of the form in (4.6). However, since the term $c_{\delta-2i} x^{\alpha_j} x_n^{\delta-2i}$ is reduced, the coefficient $c_{\delta-2i}$ will not appear in other entries in the row corresponding to x^{α_j}.

By Lemma 4.2.2, when we multiply $\mathbf{B}_i$ by $c_{\delta-2i} x_n^{\delta-2i}$ we obtain the vector $\mathbf{B}_{\delta-i}$, thus the coefficient $c_{\delta-2i}$ will appear on the diagonal, and only on the diagonal, as claimed. □

Lemma 4.4.3. *Let $0 \leq i \leq \delta$ and $\mathbf{v}_0 = c$. Then the square submatrix Θ_i of A_i formed by columns corresponding to monomials in $\mathbf{B}_i z^d$ has diagonal entries of the form*

$$c + L, \tag{4.7}$$

where L is a linear function of coefficients in $\mathbf{v}_1, \ldots, \mathbf{v}_\delta$. The coefficient c does not appear in any other entry of A_i.

Proof. Multiplying a monomial $x^\alpha \in \mathbf{B}_i$ by the smallest term in g, which is cz^d, we obtain the irreducible term $cx^\alpha z^d$. Larger terms in $x^\alpha g$ might be reducible modulo G, and the reduction would

result in coefficients of the form (4.7). This coefficient would not appear in any other term of the reduced form of $x^\alpha g$. □

Lemma 4.4.4. *For $0 \leq i \leq \delta$, the square submatrix Λ_i of M_i formed by the columns corresponding to monomials in $B_\delta z^{d+i-\delta}, \ldots, B_{\delta-i} z^{d+2i-\delta}$ is nonsingular.*

Proof. We will proceed by induction on i. For $i = 0$, $|E_0| = 1$ and Λ_0 has a single entry given by the coefficient $\mathbf{v}_\delta$.

Suppose that $0 < i \leq \lfloor \delta/2 \rfloor$. In this case, M_i has the form

$$M_i = \left(\begin{array}{c} A_i \\ \hline M_{i-1} \end{array} \right),$$

and Λ_i is given by

$$\Lambda_i = \left(\begin{array}{c|c} \Omega & \Gamma_i \\ \hline \Lambda_{i-1} & \Phi \end{array} \right).$$

So, the determinant of Λ_i is given by

$$\det(\Lambda_i) = \det(\Lambda_{i-1}) \cdot \det(\Gamma_i - \Omega \Lambda_{i-1}^{-1} \Phi).$$

By the induction hypothesis, Λ_{i-1} is nonsingular. By Lemma 4.4.2, the diagonal entries of Γ_i have the form (4.6). Note that the coefficient $c_{\delta-2i}$ appears on the diagonal of Γ_i, but not in the other submatrices, as it would appear only with smaller monomials (columns of M_{i-1} not included in Λ_{i-1}). So the entries on the diagonal of $\Gamma_i - \Omega \Lambda_{i-1}^{-1} \Phi$ still have the form $c_{\delta-2i}$ + other terms, with $c_{\delta-2i}$ not appearing in any other entry. It follows that $\det(\Gamma_i - \Omega \Lambda_{i-1}^{-1} \Phi) \neq 0$, as this determinant is a nonzero polynomial in the coefficients of g, $c_{\delta-2i}^{a_i}$ being one of the terms in the determinant. Hence Λ_i is nonsingular.

Now suppose $i > \lfloor \delta/2 \rfloor$. Then Λ_i has the form

$$\Lambda_i = \left(\begin{array}{c|cccc} & \Theta_i & * & \cdots & * \\ & * & \Theta_{i-1} & \cdots & * \\ \Omega & & & \ddots & \\ & * & * & \cdots & \Theta_{\delta-i} \\ \hline \Lambda_{\delta-i-1} & \multicolumn{4}{c}{\Phi} \end{array}\right),$$

where the stars represent other entries, that, by Lemma 4.4.3, do not involve the coefficient c. Let Θ denote the submatrix in the upper right corner. Then Θ is nonsingular, as its diagonal entries are all of the form (4.7), but c does not appear out of the diagonal. By induction, $\Lambda_{\delta-i-1}$ is nonsingular. We have that

$$\det(\Lambda_i) = \det(\Lambda_{i-1}) \cdot \det(\Theta - \Omega\Lambda_{i-1}^{-1}\Phi).$$

Since c is also not present in the entries of Λ_{i-1}, Ω and Φ, the entries on the diagonal of $\Theta - \Omega\Lambda_{i-1}^{-1}\Phi$ still have the form $c +$ other terms, with c not appearing in any other entry out of the diagonal. It follows that $\det(\Theta - \Omega\Lambda_{i-1}^{-1}\Phi) \neq 0$, and hence Λ_i is nonsingular. □

Proposition 4.4.5. *If $d \geq \delta$, then*

$$\mathrm{lm}(I, g) = \langle \mathrm{lm}(I), z^{d-\delta}B_\delta, z^{d-\delta+2}B_{\delta-1}, \ldots, z^{\delta+d-3}B_1, z^{\delta+d-1}B_0 \rangle.$$

Proof. Fix $1 \leq i \leq \delta$. Since the submatrix of M_i formed by columns corresponding to monomials in $B_\delta z^{d+i-\delta}, \ldots, B_{\delta-i}z^{d+2i-\delta}$ is nonsingular, we can perform row operations on M_i and change Equation (4.5) into

$$\begin{pmatrix} \mathbf{u}_i \\ \mathbf{u}_{i-1} \\ \vdots \\ \mathbf{u}_0 \end{pmatrix} \cdot g \equiv \begin{pmatrix} \mathbf{w}_i \\ \mathbf{w}_{i-1} \\ \vdots \\ \mathbf{w}_0 \end{pmatrix} \pmod{G},$$

where the entries of each $\mathbf{w}_j$ are polynomials with distinct initial terms, so that each monomial in $B_\delta z^{d+i-\delta}, \ldots, B_{\delta-i}z^{d+2i-\delta}$ occurs as leading monomial of some polynomial in $\mathbf{w}_0, \ldots, \mathbf{w}_i$. But the monomials in $B_\delta z^{d+i-\delta}$, …, $B_{\delta-i+1}z^{d+2(i-1)-\delta}$ are redundant as they are multiples of monomials that occur as leading terms when we perform row operations on $\mathbf{E}_{i-1}g \equiv M_{i-1}\mathbf{E}_{i+d-1} \pmod{G}$.

Thus, only the monomials in $B_{\delta-i}z^{d+2i-\delta}$ are minimal generators of $\mathrm{lm}(I,g)$. $\square$

Corollary 4.4.6. *Let* $\widetilde{B} = \mathrm{B}(I,g) \subset K[x_1,\ldots,x_n,z]$. *Then*

$$\begin{aligned}
\widetilde{B}_0 &= B_0 \\
\widetilde{B}_1 &= B_1 \cup zB_0 \\
\widetilde{B}_2 &= B_2 \cup zB_1 \cup z^2B_0 \\
&\vdots \\
\widetilde{B}_\delta &= B_\delta \cup zB_{\delta-1} \cup \cdots \cup z^\delta B_0 \\
\widetilde{B}_{\delta+1} &= z\widetilde{B}_\delta \\
&\vdots \\
\widetilde{B}_{d-1} &= z^{d-\delta-1}\widetilde{B}_\delta \\
\widetilde{B}_d &= z^{d-\delta+1}\widetilde{B}_{\delta-1} \\
\widetilde{B}_{d+1} &= z^{d-\delta+3}\widetilde{B}_{\delta-2} \\
&\vdots \\
\widetilde{B}_{d+\delta-1} &= z^{d+\delta-1}B_0.
\end{aligned}$$

Example 4.4.7. Let f_1, f_2 be generic polynomials in $R = K[x_1,x_2,z]$ of degree $d_1 = 2$ and $d_2 = 3$. The initial ideal of I is given by

$$\mathrm{lm}(I) = \langle x_1^2, x_1x_2^2, x_2^4\rangle,$$

and $B = \mathrm{B}(I^*)$ is formed by

$$\begin{aligned}
B_0 &= \{1\}, \\
B_1 &= \{x_1, x_2\}, \\
B_2 &= \{x_1x_2, x_2^2\}, \\
B_3 &= \{x_2^3\}.
\end{aligned}$$

Let $d = 5 > \delta = 3$. Suppose g is a linear combination of monomials in E_5,

$$g = b_1x_2^3z^2 + b_2x_1x_2z^3 + b_3x_2^2z^3 + b_4x_1z^4 + b_5x_2z^4 + b_6z^5.$$

In the notation above, we have

$$\begin{aligned} \mathbf{v}_3 &= (b_1), & c_3 &= b_1, \\ \mathbf{v}_2 &= (b_2, b_3), & c_2 &= b_3, \\ \mathbf{v}_1 &= (b_4, b_5), & c_1 &= b_5, \\ \mathbf{v}_0 &= (b_6), & c_0 &= b_6. \end{aligned}$$

First, we consider the equivalence

$$1 \cdot g \equiv M_0 \mathbf{E}_5 \pmod{G},$$

where $M_0 = \begin{pmatrix} b_1 & b_2 & b_3 & b_4 & b_5 & b_6 \end{pmatrix}$. Then $\Lambda_0 = (b_1)$ is the 1×1 submatrix corresponding to the first column, which is nonsingular. Thus, we add g to the Gröbner basis of $\langle I, g \rangle$, and the monomial $x_2^3 z^2$ enters the basis of $\operatorname{lm}(I, g)$.

When writing the next matrix, we use L to denote linear functions, and write entries in terms of coefficients of g. Then

$$\begin{pmatrix} x_1 \\ x_2 \\ z \end{pmatrix} g \equiv M_1 \mathbf{E}_6 \pmod{G},$$

where M_1 is given by

$$\begin{pmatrix} L(b_1,b_2,b_3) & b_5 + L(b_1,b_2,b_3,b_4) & L(b_1,b_2,b_3,b_4) & b_6 + L(b_1,b_2,b_3,b_4) & L(b_1,b_2,b_3,b_4) & L(b_1,b_2,b_3,b_4) \\ b_3 + L(b_1,b_2) & b_4 + L(b_1,b_2) & b_5 + L(b_1,b_2) & L(b_1,b_2) & b_6 + L(b_1,b_2) & L(b_1,b_2) \\ b_1 & b_2 & b_3 & b_4 & b_5 & b_6 \end{pmatrix}.$$

Writing the columns corresponding to the three largest monomials in E_6, which are $x_2^3 z^3, x_1 x_2 z^4, x_2^2 z^4$, we have

$$\Lambda_1 = \begin{pmatrix} L(b_1,b_2,b_3) & b_5 + L(b_1,b_2,b_3,b_4) & L(b_1,b_2,b_3,b_4) \\ b_3 + L(b_1,b_2) & b_4 + L(b_1,b_2) & b_5 + L(b_1,b_2) \\ b_1 & b_2 & b_3 \end{pmatrix} = \left(\begin{array}{cc|c} & & c_1 \\ & & \\ \hline & & c_1 \\ c_3 & & \end{array}\right).$$

Now, $\det \Lambda_1 = \det \Lambda_0 \cdot \det(\Gamma_1 - \Omega \Lambda_0^{-1} \Phi)$, where

$$\Gamma_1 = \begin{pmatrix} b_5 + L(b_1,b_2,b_3,b_4) & L(b_1,b_2,b_3,b_4) \\ b_4 + L(b_1,b_2) & b_5 + L(b_1,b_2) \end{pmatrix} = \begin{pmatrix} c_1 & \\ & c_1 \end{pmatrix}.$$

So, $\det \Lambda_1 = c_1^2 + \text{other terms} \neq 0$. The monomials $x_2^3z^3, x_1x_2z^4, x_2^2z^4 \in E_6$ enter the basis of $\text{lm}(I, g)$. Note that the monomial $x_2^3z^3$ can be discarded, as it is a multiple of the generator added to the basis in the previous step.

Similarly, we write Λ_2 and Λ_3 showing the coefficients of interest

$$\Lambda_2 = \left(\begin{array}{c|cccc} & c_0 & & & \\ & & c_0 & & \\ & c_1 & & c_0 & \\ & & c_1 & & c_0 \\ \hline c_3 & & & & \end{array}\right),$$

$$\Lambda_3 = \begin{pmatrix} c_0 & & & & & \\ & c_0 & & & & \\ & & c_0 & & & \\ & c_1 & & c_0 & & \\ & & c_1 & & c_0 & \\ c_3 & & & & & c_0 \end{pmatrix}.$$

Thus, the five greatest monomials in E_7, and the six greatest monomials in E_8 are added to the basis of $\text{lm}(I, g)$. Removing redundant generators, we have

$$\text{lm}(I, g) = \langle x_1^2, x_1x_2^2, x_2^4, x_2^3z^2, x_1x_2z^4, x_2^2z^4, x_1z^6, x_2z^6, z^8 \rangle.$$

At each step, we added the greatest monomials of each degree to the basis of $\text{lm}(I, g)$, so this ideal is almost reverse lexicographic. ♢

Corollary 4.4.8. *If* $\text{lm}(I)$ *is almost reverse lexicographic, then* $\text{lm}(I, g)$ *is also almost reverse lexicographic.*

Proof. For all $t \geq d$, the minimal generators of degree t introduced to the basis of $\text{lm}(I, g)$ are the largest monomials in E_t. □

Theorem 4.4.9. *Let* $I = \langle f_1, \ldots, f_n \rangle \subset K[x_1, \ldots, x_n]$ *be a generic ideal, with* $\deg(f_i) = d_i$ *and* $d_i > \sum_{j=1}^{i-1} d_j - i$. *Then* $\text{lm}(I)$ *is almost reverse lexicographic.*

Proof. The result clearly holds for $n = 1$. Assuming it holds for $n-1$, the initial ideal of $\langle f_1, \ldots, f_{n-1}\rangle \subset K[x_1, \ldots, x_{n-1}]$ is almost reverse lexicographic. By Corollary 4.4.8, $\mathrm{lm}(I)$ is almost reverse lexicographic. □

4.4.2 Case II: $d < \delta$

In this case g can be written as

$$g = \mathbf{v}_d \cdot \mathbf{B}_d + \mathbf{v}_{d-1} \cdot \mathbf{B}_{d-1} z + \cdots + \mathbf{v}_1 \cdot \mathbf{B}_1 z^{d-1} + \mathbf{v}_0 \cdot \mathbf{B}_0 z^d,$$

where again $\mathbf{B}_i$ denotes the column vector whose entries are the monomials in B_i listed in decreasing order, according to the reverse lexicographic order, and $\mathbf{v}_i$ is a row vector of coefficients. We denote the last entry of $\mathbf{v}_i$ by c_i.

Again, we would like to show that the submatrix of M_i formed by columns corresponding to the largest monomials in E_{i+d} is nonsingular. The matrix M_i is formed by blocks $\Gamma_{j,k}$, for $0 \le j \le i$ and $0 \le k \le \delta$, where the entries of $\Gamma_{j,k}$ are the coefficients of monomials in $B_k z^{d+i-k}$ in the reduced form of polynomials in $B_j z^{i-j} g$. So Equation (4.5) takes the form

$$\begin{pmatrix} \mathbf{B}_i \\ z\mathbf{B}_{i-1} \\ \vdots \\ z^i\mathbf{B}_0 \end{pmatrix} g \equiv \begin{pmatrix} \Gamma_{i,d+i} & \Gamma_{i,d+i-1} & \cdots & \Gamma_{i,0} \\ \Gamma_{i-1,d+i} & \Gamma_{i-1,d+i-1} & \cdots & \Gamma_{i-1,0} \\ & & \ddots & \\ \Gamma_{0,d+i} & \Gamma_{0,d+i-1} & \cdots & \Gamma_{0,0} \end{pmatrix} \begin{pmatrix} \mathbf{B}_{d+i} \\ z\mathbf{B}_{d+i-1} \\ \vdots \\ z^{d+i}\mathbf{B}_0 \end{pmatrix} \pmod{G}$$

The following lemma gives some of the structure of the blocks $\Gamma_{j,k}$.

Lemma 4.4.10. *Let $0 \le i \le \delta$, $0 \le j \le i$ and $j \le k \le \delta$.*

(i) *Suppose $|B_j| \le |B_k|$. Then the entries on the diagonal of the square submatrix of $\Gamma_{j,k}$ formed by the last $|B_j|$ columns have the form $c_{k-j} + L$, where L is linear on other coefficients in $\mathbf{v}_{k-j}, \mathbf{v}_{k-j+1}, \ldots, \mathbf{v}_\delta$ and does not involve c_{k-j}. Also, c_{k-j} does not appear in the other entries*

of $\Gamma_{j,k}$.

$$\Gamma_{j,k} = \begin{pmatrix} * & \cdots & * & c_{k-j}+L & * & \cdots & * \\ * & \cdots & * & * & c_{k-j}+L & \cdots & * \\ & & & & & \ddots & \\ * & \cdots & * & * & * & \ldots & c_{k-j}+L \end{pmatrix} \tag{4.8}$$

(ii) *Suppose* $|B_j| \geq |B_k|$. *Then the entries on the diagonal of the square submatrix of* $\Gamma_{j,k}$ *formed by the last (bottom)* $|B_k|$ *rows have the form* $c_{k-j}+L$, *where* L *is linear on other coefficients in* $\mathbf{v}_{k-j}, \mathbf{v}_{k-j+1}, \ldots, \mathbf{v}_\delta$ *and does not involve* c_{k-j}.

$$\Gamma_{j,k} = \begin{pmatrix} * & * & \cdots & * \\ & & \vdots & \\ * & * & \cdots & * \\ c_{k-j}+L & * & \cdots & * \\ * & c_{k-j}+L & \cdots & * \\ & & \ddots & \\ * & * & \cdots & c_{k-j}+L \end{pmatrix} \tag{4.9}$$

Proof. (i) Let $x^\alpha \in B_j$, and consider the term $c_{k-j}x_n^{k-j}z^{d+j-k}$ of g. By Lemma 4.2.3, the monomial $x^\alpha x_n^{k-j}$ is in B_k, that is, it is reduced modulo G. So in the reduced form of the product $x^\alpha z^{i-j} \cdot g$, c_{k-j} will certainly appear in the coefficient of the monomial $x^\alpha x_n^{k-j} z^{d+i-k}$. Larger monomials that appear in the product might not be reduced, and the reduction would result in a coefficient of the form $c_{k-j}+L$, as claimed. Since the coefficient c_{k-j} comes from a unique term in g, it cannot appear in any other entries.

(ii) Again, we let x^α be a monomial in B_j. Suppose that x^α is among the $|B_k|$ smallest monomials in B_j. By Lemma 4.2.3, the monomial $x^\alpha x_n^{k-j}$ is in B_k, so c_{k-j} appears in the coefficient of the monomial $x^\alpha x_n^{k-j} z^{d+i-k}$ in the reduced form of $x^\alpha z^{i-j} \cdot g$. In the reduction process, possibly larger terms will be reduced resulting in a coefficient of the form $c_{k-j}+L$. Note that c_{k-j} might appear in the top rows of $\Gamma_{k,j}$, that is, c_{k-j} appears only once in each of $|B_k|$ the bottom rows, but we cannot guarantee it does not appear in other entries in the top rows. □

Let Θ_i denote the square submatrix of M_i formed by columns corresponding to the $|E_i|$

largest monomials in E_{i+d}. We want to show that Θ_i is nonsingular, for all $0 \leq i \leq \delta$. The determinant of Θ_i is a polynomial in the coefficients of g. We need to see that this polynomial is nonzero. Our goal is to show there is a term that can be obtained as a product of entries in a unique way, and hence cannot be cancelled.

In the next lemmas we handle the case with $\delta - d \leq i \leq \delta$. In this case the $|E_i|$ largest monomials in E_{d+i} are the monomials in $z^{i+d-\delta}B_\delta, z^{i+d-\delta+1}B_{\delta-1}, \ldots, z^{2i+d-\delta}B_{\delta-i}$, and Θ_i is formed by the following blocks

$$\Theta_i = \begin{pmatrix} \mathbf{B}_\delta & \mathbf{B}_{\delta-1} & \cdots & \mathbf{B}_{\delta-i+1} & \mathbf{B}_{\delta-i} \\ \Gamma_{i,\delta} & \Gamma_{i,\delta-1} & \cdots & \Gamma_{i,\delta-i+1} & \Gamma_{i,\delta-i} & \mathbf{B}_i \\ \Gamma_{i-1,\delta} & \Gamma_{i-1,\delta-1} & \cdots & \Gamma_{i-1,\delta-i+1} & \Gamma_{i-1,\delta-i} & \mathbf{B}_{i-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ \Gamma_{1,\delta} & \Gamma_{1,\delta-1} & \cdots & \Gamma_{\delta-i+1} & \Gamma_{1,\delta-i} & \mathbf{B}_1 \\ \Gamma_{0,\delta} & \Gamma_{0,\delta-1} & \cdots & \Gamma_{0,\delta-i+1} & \Gamma_{0,\delta-i} & \mathbf{B}_0 \end{pmatrix}.$$

Lemma 4.4.11. *Suppose $\delta - d \leq i \leq \delta$, and $i \geq \delta/2$. Then the term*

$$c_{\delta-i}^{(i+1)a_0} c_{\delta-i-1}^{i(a_1-a_0)} c_{\delta-i-2}^{(i-1)(a_2-a_1)} \cdots c_0^{(2i-\delta+1)(a_{\delta-i}-a_{\delta-i-1})} \tag{4.10}$$

can be obtained from the product of entries of Θ_i, with one entry from each column and row.

Proof. We will show how to select entries from Θ_i in steps. In each step, we pick entries from a certain set of blocks $\Gamma_{j,k}$. We start at step 0, selecting entries from the blocks on the diagonal of Θ_i, and then blocks above the diagonal in the next step, and so on.

Let $0 \leq \ell \leq \delta - i$. At step ℓ we select $a_\ell - a_{\ell-1}$ entries from blocks

$$\Gamma_{i,\delta-\ell}, \Gamma_{i-1,\delta-\ell+1}, \ldots, \Gamma_{\ell,\delta-i}. \tag{4.11}$$

The entries selected are the ones in the bottom a_ℓ rows, skipping the bottom $a_{\ell-1}$, and a_ℓ right-most

columns, skipping the last $a_{\ell-1}$ columns. These entries have the form $c_{\delta-\ell-i}+L$.

$$\left(\begin{array}{cccccc}
\ddots & & & & & \\
c_{\delta-\ell-i+L} & * & * & * & * & * \\
* & \underline{c_{\delta-\ell-i+L}} & * & * & * & * \\
* & * & \underline{c_{\delta-\ell-i+L}} & * & * & * \\
* & * & * & \underline{c_{\delta-\ell-i+L}} & * & * \\
* & * & * & * & c_{\delta-\ell-i+L} & * \\
* & * & * & * & * & c_{\delta-\ell-i+L}
\end{array}\right)
\begin{array}{l}
\left.\begin{array}{c}\\ \\ \\ \\ \\ \\ \end{array}\right\} a_\ell - a_{\ell-1} \\
\left.\begin{array}{c}\\ \\ \\ \\ \\ \\ \end{array}\right\} a_{\ell-1}
\end{array}$$

$$\underbrace{\qquad\qquad\qquad\qquad}_{a_\ell - a_{\ell-1}} \quad \underbrace{\qquad\qquad}_{a_{\ell-1}}$$

Note that for any of the blocks $\Gamma_{j,k}$ in (4.11), since $\ell \le \delta - i \le i$, and $\ell \le j \le i$, it follows that $a_\ell \le a_j$. Also, since $\delta - i \le k \le \delta - \ell$, we have $a_\ell = a_{\delta-\ell} \le a_k$. Thus, we indeed have enough entries to pick in all blocks.

Furthermore, for a group of rows corresponding to B_j, we picked entries from the bottom a_0 rows of the block $\Gamma_{j,\delta+j-i}$, then entries from the next $a_1 - a_0$ rows from the block $\Gamma_{j,\delta+j-i-1}$, and so on, so that we never select entries from the same rows. The same reasoning applies to columns. Fixing a group of columns corresponding to B_k, we pick a_0 entries from right column of $\Gamma_{k+i-\delta,k}$, then $a_1 - a_0$ entries from the next columns, and so on, never repeating columns. So we select a single entry from each row and each column.

At each step ℓ, for $0 \le \ell \le \delta - i$, we picked $a_\ell - a_{\ell-1}$ entries of the form $c_{\delta-\ell-i}$ from $i-\ell+1$ blocks. Taking the product of all entries selected, we have a polynomial in the coefficients of g of the form

$$c_{\delta-i}^{(i+1)a_0} c_{\delta-i-1}^{i(a_1-a_0)} c_{\delta-i-2}^{(i-1)(a_2-a_1)} \cdots c_0^{(2i-\delta+1)(a_{\delta-i}-a_{\delta-i-1})} + \text{ other terms.}$$

□

Lemma 4.4.12. *There is only one way of selecting entries from Θ_i and obtaining the term in Equation (4.10).*

Proof. We use induction to show that for $\ell = \delta - i, \delta - i - 1, \ldots, 0$, there is only one way of obtaining the power of c_ℓ in Equation (4.10) from the product of entries of Θ_i.

We first consider $c_{\delta-i}$. We now use induction to show that for all $0 \le j \le i$, the only entry

available to select in the last row of the set of rows corresponding to B_j is the one on the last column of the block $\Gamma_{j,\delta+j-i}$, of the form $c_{\delta-i}+L$. Note that the only coefficient in Equation (4.10) that appears in the bottom row of Θ_i, corresponding to B_0, is $c_{\delta-i}$, which is in the last column of the block $\Gamma_{0,\delta-i}$. So we pick this entry. Suppose now that the only way of selecting an entry containing a coefficient in Equation (4.10) from the last row of the block corresponding to B_j is picking the one containing $c_{\delta-i}$, from the last column of the block $\Gamma_{j,\delta+j-i}$. This means that the other entries in this row involving coefficients in Equation (4.10) cannot be selected at this point, and so entries in the last columns of the blocks $\Gamma_{j,\delta+j-i-1}, \Gamma_{j,\delta+j-i-2}, \cdots$ have been selected in previous steps, from blocks below. Passing to the set of rows corresponding to B_{j+1}, it follows that entries have been selected on the last columns of blocks $\Gamma_{j+1,\delta+j-i}, \Gamma_{j+1,\delta+j-i-1,\ldots}$, and hence we are left with no choice other than selecting the entry from the last column of the block $\Gamma_{j+1,\delta+j-i+1}$, which has the form $c_{\delta-i}$. This proves our claim.

Let $1 \leq \ell \leq \delta - i$, and suppose we have selected entries involving $c_{\delta-i}, c_{\delta-i-1}, \ldots, c_{\delta-i-\ell+1}$ as in Lemma 4.4.11, and that this selection was the only possible choice. This means that we have already picked entries from the bottom $a_{\ell-1}$ rows of all blocks $B_0, \ldots, B_i$. So let us consider the next $a_\ell - a_{\ell-1}$ rows. Starting with the block B_ℓ, note that the coefficients from Equation (4.10) that appear in this block are $c_{\delta-i}, c_{\delta-i-1}, \ldots, c_{\delta-i-\ell}$. But with the selections we have already made, the exponents of $c_{\delta-i}, c_{\delta-i-1}, \ldots, c_{\delta-i-\ell+1}$ in Equation (4.10) were reached, so that at this point we cannot select the entries involving these coefficients. Hence, the only choice left is selecting the entries of the form $c_{\delta-i-\ell}+L$ from $\Gamma_{\ell,\delta-i}$.

Let $\ell+1 \leq j \leq i$. Suppose we already picked entries of the form $c_{\delta-i-\ell}+L$ as in Lemma 4.4.11 from blocks $B_\ell, B_{\ell+1}, \ldots, B_{j-1}$. Consider block B_j. Still assuming that entries have been selected from the bottom $a_{\ell-1}$ rows, we pass to the next $a_\ell - a_{\ell-1}$. The selections made in blocks bellow prevent us from picking the entries involving $c_{\delta-i-\ell-1}, \ldots, c_0$. Also, we cannot select entries where coefficients $c_{\delta-i}, \ldots, c_{\delta-i-\ell+1}$ appear. Thus, we are left with entries containing $c_{\delta-i-\ell}$. □

Lemma 4.4.13. *Suppose $\delta - d \leq i \leq \delta$, and $i \leq \delta/2$. Then the term*

$$c_{\delta-i}^{(i+1)a_0} c_{\delta-i-1}^{i(a_1-a_0)} c_{\delta-i-2}^{(i-1)(a_2-a_1)} \cdots c_i^{(a_i-a_{i-1})} \tag{4.12}$$

can be obtained from the product of entries of Θ_i, with one entry from each column and row.

Proof. The proof is the same as Lemma 4.4.11, except that in this case we select entries in steps ℓ, for $0 \leq \ell \leq \delta - 2i$. □

The same proof of Lemma 4.4.12 works to show the following.

Lemma 4.4.14. *There is only one way of selecting entries from Θ_i and obtaining the term in Equation (4.12).*

Corollary 4.4.15. $\det \Theta_i \neq 0$ *for* $\delta - d \leq i \leq \delta$.

For $0 \leq i < \delta - d$, the same idea does not work. It is clear from examples that the monomials of degree $d + i$ that enter the basis of $\mathrm{lm}(I, g)$ are not necessarily the largest monomials in E_{i+d}, and hence the square submatrix of M_i formed by columns corresponding to those monomials is not necessarily nonsingular.

Let $i^\star = \lfloor \frac{\delta - d}{2} \rfloor$. We conjecture the following.

Conjecture 4.4.16. *Suppose $d_1 \leq d_2 \leq \cdots \leq d_n \leq d$, and $0 \leq i \leq i^\star$. Let Θ_i denote the square submatrix of M_i formed by the columns corresponding to the a_i largest monomials of B_{i+d}, the a_{i-1} largest monomials of zB_{i+d-1}, and so on, up to the a_0 largest monomials of $z^{i+d}B_d$. Then Θ_i is nonsingular.*

Conjecture 4.4.17. *Suppose $d_1 \leq d_2 \leq \cdots \leq d_n \leq d$, and $i^\star < i < \delta - d$. Let Θ_i denote the square submatrix of M_i formed by columns corresponding to*

(i) *all monomials in B_{d+j}, for $\delta - d - i \leq j \leq i$, and*

(ii) *the a_j largest monomials in B_{d+j}, for $0 \leq j < \delta - d - i$.*

Then Θ_i is nonsingular.

In fact, matrices Θ_j for $0 \leq j \leq i^\star$ are submatrices of Θ_i for $i^\star < i < \delta - d$, and if we can prove the smaller matrices are nonsingular, we are actually able to prove all Θ_i are nonsingular.

Proposition 4.4.18. *Conjecture 4.4.16 implies Conjecture 4.4.17.*

Proof. Let $i^\star < i < \delta - d$. Let Λ_i denote the submatrix of Θ_i formed by the following blocks

$$\Lambda_i = \begin{pmatrix} \Gamma_{i,d+i} & \Gamma_{i,d+i-1} & \cdots & \Gamma_{i,\delta-i} \\ \Gamma_{i-1,d+i} & \Gamma_{i-1,d+i-1} & \cdots & \Gamma_{i-1,\delta-i} \\ \vdots & \vdots & \ddots & \vdots \\ \Gamma_{\delta-d-i,d+i} & \Gamma_{\delta-d-i,d+i-1} & \cdots & \Gamma_{\delta-d-i,\delta-i} \end{pmatrix}$$

Then, Θ_i can be written as

$$\Theta_i = \left(\begin{array}{c|c} \Lambda_i & \Omega \\ \hline 0 & \Theta_{\delta-d-i-1} \end{array}\right)$$

that is, the columns formed by $\binom{\Lambda_i}{0}$ are the ones in Conjecture 4.4.17(i), and the columns formed by $\binom{\Omega}{\Theta_{\delta-d-i-1}}$ are the columns in (ii).

Now, $\det \Theta_i = \det(\Lambda_i) \cdot \det(\Theta_{\delta-d-i-1})$. If Conjecture 4.4.16 is true, then $\det \Theta_{\delta-d-i-1} \neq 0$. So we need to see that $\det \Lambda_i \neq 0$. In fact, an argument similar to that applied in Lemmas 4.4.11-4.4.14 can be used. We claim the term

$$c_d^{(2i+d-\delta+1)a_{d+i}} c_{d-1}^{(2i+d-\delta)(a_{d+i-1}-a_{d+i})} \cdots c_{\delta-2i}^{(a_{\delta-i}-a_{\delta-i+1})} \tag{4.13}$$

appears in the determinant of Λ_i. Again we start by selecting entries from the blocks on the diagonal at step 0, and then from the blocks above the diagonal at step 1, and so on.

In general, at step ℓ, for $0 \leq \ell \leq 2i + d - \delta$, we select entries from the blocks

$$\Gamma_{i,d_i-\ell}, \Gamma_{i-1,d+i-\ell-1}, \ldots, \Gamma_{\delta-d-i+\ell,\delta-i}.$$

We select the entries in the diagonal of the bottom $a_{d+i-\ell}$ rows and right-most $a_{d+i-\ell}$ columns, skipping the bottom $a_{d+i-\ell+1}$. The proof that these selections can be made, and that this is the only way of obtaining the term (4.13) is identical to Lemma 4.4.11 and Lemma 4.4.12. □

We will use the following notation: for a set $S = \{s_1, \ldots, s_\ell\}$ and $1 \leq a \leq b \leq \ell$, let

$$\begin{aligned} S^{[a,b]} &= \{s_a, \ldots, s_b\}, \\ S^{(a,b]} &= \{s_{a+1}, \ldots, s_b\}. \end{aligned}$$

If $\delta - d \equiv 0 \pmod 2$, the initial ideal of $\langle I, g \rangle$ can be described as

$$\begin{aligned}\mathrm{lm}(I,g) \quad = \langle \quad & \mathrm{lm}(I), B_d^{[1,a_0]}, B_{d+1}^{[1,a_1]}, \ldots, B_{d+i^\star-1}^{[1,a_{i^\star-1}]}, B_{d+i^\star}, \\ & z^2 B_{d+i^\star-1}^{(a_{i^\star-1},a_{d+i^\star-1}]}, z^4 B_{d+i^\star-2}^{(a_{i^\star-2},a_{d+i^\star-2}]}, \ldots, z^{\delta-d} B_d^{(a_0,a_d]}, \\ & z^{\delta-d+2} B_{d-1}, \ldots, z^{\delta+d-2} B_1, z^{\delta+d} B_0 \quad \rangle.\end{aligned}$$

The corresponding set $\widetilde{B} = \mathrm{B}(I,g)$ is

$$\begin{aligned}\widetilde{B}_0 &= B_0 \\ \widetilde{B}_1 &= B_1 \cup zB_0 \\ \widetilde{B}_2 &= B_2 \cup zB_1 \cup z^2 B_0 \\ &\vdots \\ \widetilde{B}_{d-1} &= B_{d-1} \cup z\widetilde{B}_{d-2} \\ \widetilde{B}_d &= B_d^{(a_0,a_d]} \cup z\widetilde{B}_{d-1} \\ \widetilde{B}_{d+1} &= B_{d+1}^{(a_1,a_{d+1}]} \cup z\widetilde{B}_{d-2} \\ &\vdots \\ \widetilde{B}_{d+i^\star} &= z\widetilde{B}_{d+i^\star-1} \\ \widetilde{B}_{d+i^\star+1} &= z^3\widetilde{B}_{d+i^\star-2} \\ &\vdots \\ \widetilde{B}_\delta &= z^{\delta-d+1}\widetilde{B}_{d-1} \\ \widetilde{B}_{\delta+1} &= z^{\delta-d+3}\widetilde{B}_{d-2} \\ &\vdots \\ \widetilde{B}_{\delta+d-1} &= z^{\delta+d-1}\widetilde{B}_0.\end{aligned}$$

If $\delta - d \equiv 1 \pmod 2$, the initial ideal of $\langle I, g \rangle$ can be described as

$$\begin{aligned}\mathrm{lm}(I,g) \quad = \langle \quad & \mathrm{lm}(I), B_d^{[1,a_0]}, B_{d+1}^{[1,a_1]}, \ldots, B_{d+i^\star}^{[1,a_{i^\star}]}, \\ & zB_{d+i^\star}^{(a_{i^\star},a_{d+i^\star}]}, z^3 B_{d+i^\star-1}^{(a_{i^\star-1},a_{d+i^\star-1}]}, \ldots, z^{\delta-d} B_d^{(a_0,a_d]}, \\ & z^{\delta-d+2} B_{d-1}, \ldots, z^{\delta+d-2} B_1, z^{\delta+d} B_0 \quad \rangle.\end{aligned}$$

The corresponding set $\widetilde{B} = \mathrm{B}(I, g)$ is

$$\begin{aligned}
\widetilde{B}_0 &= B_0 \\
\widetilde{B}_1 &= B_1 \cup zB_0 \\
\widetilde{B}_2 &= B_2 \cup zB_1 \cup z^2 B_0 \\
&\vdots \\
\widetilde{B}_{d-1} &= B_{d-1} \cup z\widetilde{B}_{d-2} \\
\widetilde{B}_d &= B_d^{(a_0,a_d]} \cup z\widetilde{B}_{d-1} \\
\widetilde{B}_{d+1} &= B_{d+1}^{(a_1,a_{d+1}]} \cup z\widetilde{B}_{d-2} \\
&\vdots \\
\widetilde{B}_{d+i^\star} &= B_{d+i^\star} \cup z\widetilde{B}_{d+i^\star-1} \\
\widetilde{B}_{d+i^\star+1} &= z^2\widetilde{B}_{d+i^\star-1} \\
\widetilde{B}_{d+i^\star+2} &= z^4\widetilde{B}_{d+i^\star-2} \\
&\vdots \\
\widetilde{B}_\delta &= z^{\delta-d+1}\widetilde{B}_{d-1} \\
\widetilde{B}_{\delta+1} &= z^{\delta-d+3}\widetilde{B}_{d-2} \\
&\vdots \\
\widetilde{B}_{\delta+d-1} &= z^{\delta+d-1}\widetilde{B}_0.
\end{aligned}$$

From the description above, we have that Conjecture 4.4.16 implies that $\mathrm{lm}(I, g)$ is almost reverse lexicographic, and hence also implies the Moreno-Socías conjecture. When $d = \delta - 1$, the only matrix treated in Conjecture 4.4.16 is Θ_0, which is a one by one matrix whose single entry is the leading coefficient of g, and thus is nonzero. For $d = \delta - 2$, Θ_0 is once again a one by one matrix

whose entry is $\mathrm{lc}(g)$, and Θ_1 is given by

$$\Theta_1 = \left(\begin{array}{c|c} \Gamma_{1,\delta-1} & \Omega \\ \hline 0 & \mathrm{lc}(g) \end{array}\right) = \left(\begin{array}{cccc|c} c_{\delta-2}+L & * & \cdots & * & * \\ * & c_{\delta-2}+L & \cdots & * & * \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ * & * & \cdots & c_{\delta-2}+L & * \\ \hline 0 & 0 & \cdots & 0 & \mathrm{lc}(g) \end{array}\right)$$

so $\det \Theta_1 = \mathrm{lc}(g) \cdot \det \Gamma_{1,\delta-1}$, and the determinant of $\Gamma_{1,\delta-1}$ is nonzero because the term $c_{\delta-2}^{a_1}$ appears in it. This, together with the results from the previous section, proves the following.

Proposition 4.4.19. *Suppose $d \geq \delta - 2$. If $\mathrm{lm}(I)$ is almost reverse lexicographic, then $\mathrm{lm}(I, g)$ is almost reverse lexicographic.*

Example 4.4.20. Let f_1, f_2 be generic polynomials of degrees $d_1 = d_2 = 4$, and let $I = \langle f_1, f_2 \rangle$. The initial ideal of I is given by

$$\mathrm{lm}(I) = \langle x_1^4, x_1^3 x_2, x_1^2 x_2^3, x_1 x_2^5, x_2^7 \rangle.$$

Then $\delta = 6$, and we consider g of degree $d = 4 = \delta - 2$.

$$\begin{aligned} g \;=\; & b_1 x_1^2 x_2^2 + b_2 x_1 x_2^3 + b_3 x_2^4 + b_4 x_1^3 z + b_5 x_1^2 x_2 z + b_6 x_1 x_2^2 z + b_7 x_2^3 z + b_8 x_1^2 z^2 + b_9 x_1 x_2 z^2 \\ & + b_{10} x_2^2 z^2 + b_{11} x_1 z^3 + b_{12} x_2 z^3 + b_{13} z^4. \end{aligned}$$

We give the matrices Θ_i below. We write entries as functions of the coefficients b_i's. All entries have the form $b_i + L(b_1, \ldots, b_{i-1})$ or $L(b_1, \ldots, b_i)$. We show only the entries of the first form, ignoring the L portion. The entries selected to form the terms in Lemma 4.4.11 and Lemma 4.4.13

are shown in boldface. We start with $\Theta_6 = M_6$:

$$
\begin{array}{c}
\\
x_2^6 \\
x_1x_2^4 \\
x_2^5 \\
x_1^2x_2^2 \\
x_1x_2^3 \\
x_2^4 \\
x_1^3 \\
x_1^2x_2 \\
x_1x_2^2 \\
x_2^3 \\
x_1^2 \\
x_1x_2 \\
x_2^2 \\
x_1 \\
x_2 \\
1
\end{array}
\begin{array}{c}
\begin{array}{cccccccccccccccc}
x_2^6 & x_1x_2^4 & x_2^5 & x_1^2x_2^2 & x_1x_2^3 & x_2^4 & x_1^3 & x_1^2x_2 & x_1x_2^2 & x_2^3 & x_1^2 & x_1x_2 & x_2^2 & x_1 & x_2 & 1
\end{array} \\
\left(\begin{array}{cccccccccccccccc}
\mathbf{b_{13}} & & & & & & & & & & & & & & & \\
 & \mathbf{b_{13}} & & & & & & & & & & & & & & \\
b_{12} & & \mathbf{b_{13}} & & & & & & & & & & & & & \\
 & & & \mathbf{b_{13}} & & & & & & & & & & & & \\
 & b_{12} & & & \mathbf{b_{13}} & & & & & & & & & & & \\
b_{10} & b_{11} & b_{12} & & & \mathbf{b_{13}} & & & & & & & & & & \\
 & & & & & & \mathbf{b_{13}} & & & & & & & & & \\
 & & & b_{12} & & & & \mathbf{b_{13}} & & & & & & & & \\
 & b_{10} & & b_{11} & b_{12} & & & & \mathbf{b_{13}} & & & & & & & \\
b_7 & b_9 & b_{10} & & b_{11} & b_{12} & & & & \mathbf{b_{13}} & & & & & & \\
 & & & b_{10} & & & b_{11} & b_{12} & & & \mathbf{b_{13}} & & & & & \\
 & b_7 & & b_9 & b_{10} & & & b_{11} & b_{12} & & & \mathbf{b_{13}} & & & & \\
b_3 & b_6 & b_7 & b_8 & b_9 & b_{10} & & & b_{11} & b_{12} & & & \mathbf{b_{13}} & & & \\
 & b_3 & & b_6 & b_7 & & & b_9 & b_{10} & & b_{11} & b_{12} & & \mathbf{b_{13}} & & \\
 & b_2 & b_3 & b_5 & b_6 & b_7 & & b_8 & b_9 & b_{10} & & b_{11} & b_{12} & & \mathbf{b_{13}} & \\
 & & & b_1 & b_2 & b_3 & b_4 & b_5 & b_6 & b_7 & b_8 & b_9 & b_{10} & b_{11} & b_{12} & \mathbf{b_{13}}
\end{array}\right)
\end{array}.
$$

The entries in boldface give a nonzero term in $\det \Theta_6$. Since the determinant is nonzero, performing row operations on

$$\mathbf{E}_6 \cdot g \equiv M_6 \mathbf{E}_{10} \pmod{G},$$

all monomials in E_{10} will appear as leading monomials on the right-hand side. Thus, the monomials

$$x_2^6z^4, x_1x_2^4z^5, x_2^5z^5, x_1^2x_2^2z^6, x_1x_2^3z^6, x_2^4z^6, x_1^3z^7, x_1^2x_2z^7, x_1x_2^2z^7, x_2^3z^7, x_1^2z^8, x_1x_2z^8, x_2^2z^8, x_1z^9, x_2z^9, z^{10}$$

are in the basis of $\operatorname{lm}(I, g)$. The matrix Θ_5 is obtained from Θ_6 by removing the top row and rightmost column. Again we show in boldface the entries that are used to guarantee that the determinant

of this matrix is nonzero. This is the form of Θ_5

$$
\begin{array}{c}
 \\
x_1x_2^4 \\
x_2^5 \\
x_1^2x_2^2 \\
x_1x_2^3 \\
x_2^4 \\
x_1^3 \\
x_1^2x_2 \\
x_1x_2^2 \\
x_2^3 \\
x_1^2 \\
x_1x_2 \\
x_2^2 \\
x_1 \\
x_2 \\
1
\end{array}
\begin{array}{c}
\begin{array}{cccccccccccccc}
x_2^6 & x_1x_2^4 & x_2^5 & x_1^2x_2^2 & x_1x_2^3 & x_2^4 & x_1^3 & x_1^2x_2 & x_1x_2^2 & x_2^3 & x_1^2 & x_1x_2 & x_2^2 & x_1 & x_2
\end{array} \\
\left(\begin{array}{cccccccccccccc}
 & \mathbf{b_{13}} & & & & & & & & & & & & & \\
\mathbf{b_{12}} & & b_{13} & & & & & & & & & & & & \\
 & & & \mathbf{b_{13}} & & & & & & & & & & & \\
 & b_{12} & & & \mathbf{b_{13}} & & & & & & & & & & \\
b_{10} & b_{11} & \mathbf{b_{12}} & & & b_{13} & & & & & & & & & \\
 & & & & & & \mathbf{b_{13}} & & & & & & & & \\
 & & & b_{12} & & & & \mathbf{b_{13}} & & & & & & & \\
 & b_{10} & & b_{11} & b_{12} & & & & \mathbf{b_{13}} & & & & & & \\
b_7 & b_9 & b_{10} & & b_{11} & \mathbf{b_{12}} & & & & b_{13} & & & & & \\
 & & & b_{10} & & & b_{11} & b_{12} & & & \mathbf{b_{13}} & & & & \\
 & b_7 & & b_9 & b_{10} & & & b_{11} & b_{12} & & & \mathbf{b_{13}} & & & \\
b_3 & b_6 & b_7 & b_8 & b_9 & b_{10} & & & b_{11} & \mathbf{b_{12}} & & & b_{13} & & \\
 & b_3 & & b_6 & b_7 & & & b_9 & b_{10} & & b_{11} & b_{12} & & \mathbf{b_{13}} & \\
 & b_2 & b_3 & b_5 & b_6 & b_7 & & b_8 & b_9 & b_{10} & & b_{11} & \mathbf{b_{12}} & & b_{13} \\
 & & & b_1 & b_2 & b_3 & b_4 & b_5 & b_6 & b_7 & b_8 & b_9 & b_{10} & b_{11} & \mathbf{b_{12}}
\end{array}\right)
\end{array}.
$$

So, performing row operations on

$$\mathbf{E}_5 \cdot g \equiv M_5 \mathbf{E}_9 \pmod{G}$$

leads to the 15 greatest monomials in E_9 being leading monomials on the right-hand side, which means that

$$x_2^6z^3, x_1x_2^4z^4, x_2^5z^4, x_1^2x_2^2z^5, x_1x_2^3z^5, x_2^4z^5, x_1^3z^6, x_1^2x_2z^6, x_1x_2^2z^6, x_2^3z^6, x_1^2z^7, x_1x_2z^7, x_2^2z^7, x_1z^8, x_2z^8$$

are in $\mathrm{lm}(I, g)$. Next, we consider

$$\mathbf{E}_4 \cdot g \equiv M_4 \mathbf{E}_8 \pmod{G}.$$

The matrix M_4 is 13×16, and Θ_4 is the 13×13 submatrix given by

$$\begin{array}{c} \\ x_1^2x_2^2 \\ x_1x_2^3 \\ x_2^4 \\ x_1^3 \\ x_1^2x_2 \\ x_1x_2^2 \\ x_2^3 \\ x_1^2 \\ x_1x_2 \\ x_2^2 \\ x_1 \\ x_2 \\ 1 \end{array} \begin{array}{c} \begin{array}{cccccccccccccc} x_2^6 & x_1x_2^4 & x_2^5 & x_1^2x_2^2 & x_1x_2^3 & x_2^4 & x_1^3 & x_1^2x_2 & x_1x_2^2 & x_2^3 & x_1^2 & x_1x_2 & x_2^2 \end{array} \\ \begin{pmatrix} & & & \mathbf{b_{13}} & & & & & & & & & \\ & \mathbf{b_{12}} & & & b_{13} & & & & & & & & \\ \mathbf{b_{10}} & b_{11} & b_{12} & & & b_{13} & & & & & & & \\ & & & & & & \mathbf{b_{13}} & & & & & & \\ & & & b_{12} & & & & \mathbf{b_{13}} & & & & & \\ & b_{10} & & b_{11} & \mathbf{b_{12}} & & & & b_{13} & & & & \\ b_7 & b_9 & \mathbf{b_{10}} & & b_{11} & b_{12} & & & & b_{13} & & & \\ & & & b_{10} & & & b_{11} & b_{12} & & & \mathbf{b_{13}} & & \\ & b_7 & & b_9 & b_{10} & & & b_{11} & \mathbf{b_{12}} & & & b_{13} & \\ b_3 & b_6 & b_7 & b_8 & b_9 & \mathbf{b_{10}} & & & b_{11} & b_{12} & & & b_{13} \\ & b_3 & & b_6 & b_7 & & & b_9 & b_{10} & & b_{11} & \mathbf{b_{12}} & \\ & b_2 & b_3 & b_5 & b_6 & b_7 & & b_8 & b_9 & \mathbf{b_{10}} & & b_{11} & b_{12} \\ & & & b_1 & b_2 & b_3 & b_4 & b_5 & b_6 & b_7 & b_8 & b_9 & \mathbf{b_{10}} \end{pmatrix} \end{array},$$

which is also a submatrix of Θ_5, obtained by removing the rows corresponding to B_5 and the columns corresponding to B_1. After row operations,

$$x_2^6z^2, x_1x_2^4z^3, x_2^5z^3, x_1^2x_2^2z^4, x_1x_2^3z^4, x_2^4z^4, x_1^3z^5, x_1^2x_2z^5, x_1x_2^2z^5, x_2^3z^5, x_1^2z^6, x_1x_2z^6, x_2^2z^6$$

are leading monomials. Similarly, removing from Θ_4 the rows corresponding to B_4 and the columns corresponding to B_2, we get Θ_3 given by

$$\begin{array}{c} \\ x_1^3 \\ x_1^2x_2 \\ x_1x_2^2 \\ x_2^3 \\ x_1^2 \\ x_1x_2 \\ x_2^2 \\ x_1 \\ x_2 \\ 1 \end{array} \begin{array}{c} \begin{array}{ccccccccccc} x_2^6 & x_1x_2^4 & x_2^5 & x_1^2x_2^2 & x_1x_2^3 & x_2^4 & x_1^3 & x_1^2x_2 & x_1x_2^2 & x_2^3 \end{array} \\ \begin{pmatrix} & & & & & & \mathbf{b_{13}} & & & \\ & & & \mathbf{b_{12}} & & & & b_{13} & & \\ & \mathbf{b_{10}} & & b_{11} & b_{12} & & & & b_{13} & \\ \mathbf{b_7} & b_9 & b_{10} & & b_{11} & b_{12} & & & & b_{13} \\ & & & b_{10} & & & b_{11} & \mathbf{b_{12}} & & \\ & b_7 & & b_9 & \mathbf{b_{10}} & & & b_{11} & b_{12} & \\ b_3 & b_6 & \mathbf{b_7} & b_8 & b_9 & b_{10} & & & b_{11} & b_{12} \\ & b_3 & & b_6 & b_7 & & & b_9 & \mathbf{b_{10}} & \\ & b_2 & b_3 & b_5 & b_6 & \mathbf{b_7} & & b_8 & b_9 & b_{10} \\ & & & b_1 & b_2 & b_3 & b_4 & b_5 & b_6 & \mathbf{b_7} \end{pmatrix} \end{array}.$$

The leading monomials obtained are

$$x_2^6 z, x_1 x_2^4 z^2, x_2^5 z^2, x_1^2 x_2^2 z^3, x_1 x_2^3 z^3, x_2^4 z^3, x_1^3 z^4, x_1^2 x_2 z^4, x_1 x_2^2 z^4, x_2^3 z^4.$$

Next, Θ_2 is given by

$$\begin{array}{c} \\ x_1^2 \\ x_1x_2 \\ x_2^2 \\ x_1 \\ x_2 \\ 1 \end{array} \begin{array}{c} \begin{array}{cccccc} x_2^6 & x_1x_2^4 & x_2^5 & x_1^2x_2^2 & x_1x_2^3 & x_2^4 \end{array} \\ \begin{pmatrix} & & & \mathbf{b_{10}} & & \\ & \mathbf{b_7} & & b_9 & b_{10} & \\ \mathbf{b_3} & b_6 & b_7 & b_8 & b_9 & b_{10} \\ & b_3 & & b_6 & \mathbf{b_7} & \\ & b_2 & \mathbf{b_3} & b_5 & b_6 & b_7 \\ & & & b_1 & b_2 & \mathbf{b_3} \end{pmatrix} \end{array},$$

and the elements in E_6 that are leading monomials are

$$x_2^6, x_1 x_2^4 z, x_2^5 z, x_1^2 x_2^2 z^2, x_1 x_2^3 z^2, x_2^4 z^2.$$

The matrix Θ_1 is given by

$$\begin{array}{c} \\ x_1 \\ x_2 \\ 1 \end{array} \begin{array}{c} \begin{array}{ccc} x_1x_2^4 & x_2^5 & x_1^2x_2^2 \end{array} \\ \begin{pmatrix} \mathbf{b_3} & & b_6 \\ b_2 & \mathbf{b_3} & b_5 \\ & & \mathbf{b_1} \end{pmatrix} \end{array},$$

and the monomials of degree 5 that enter the basis of $\mathrm{lm}(I, g)$ are

$$x_1 x_2^4, x_2^5, x_1^2 x_2^2 z.$$

Finally, Θ_0 is the 1×1 matrix

$$\begin{array}{c} \\ 1 \end{array} \begin{array}{c} \begin{array}{c} x_1^2x_2^2 \end{array} \\ \begin{pmatrix} \mathbf{b_1} \end{pmatrix} \end{array},$$

and the monomial $x_1^2 x_2^2$ is in $\mathrm{lm}(I, g)$. Putting all the leading monomials we found together, and discarding the redundant ones, we have

$$\begin{aligned} \mathrm{lm}(I, g) &= \langle x_1^4, x_1^3 x_2, x_1^2 x_2^2, x_1 x_2^4, x_2^5, x_1 x_2^3 z^2, x_2^4 z^2, x_1^3 z^4, x_1^2 x_2 z^4, \\ &\quad x_1 x_2^2 z^4, x_2^3 z^4, x_1^2 z^6, x_1 x_2 z^6, x_2^2 z^6, x_1 z^8, x_2 z^8, z^{10} \rangle, \end{aligned}$$

which is an almost reverse lexicographical monomial ideal. $\diamondsuit$

Using induction we have a partial answer to Moreno-Socías Conjecture.

Theorem 4.4.21. *Let* $I = \langle f_1, \ldots, f_n \rangle \subset K[x_1, \ldots, x_n]$ *be a generic ideal, with* $\deg(f_i) = d_i$ *and* $d_i \geq \left(\sum_{j=1}^{i-1} d_j\right) - i - 2$. *Then* $\operatorname{lm}(I)$ *is almost reverse lexicographic.*

The theorem above is somewhat more general than the result given in [14], where Cho and Park proved the case $d_i > \left(\sum_{j=1}^{i-1} d_j\right) - i + 1$. We believe that our approach is promising, and that by investigating further the properties of $\mathrm{B}(I)$ and the structure of the matrices from Conjecture 4.4.16, we could be able to give an answer to Moreno-Socías Conjecture.

Bibliography

[1] William W. Adams and Philippe Loustaunau. *An Introduction to Gröbner Bases*, volume 3 of *Graduate Studies in Mathematics*. American Mathematical Society, 1994.

[2] Edith Aguirre, Abdul Salam Jarrah, and Reinhard Laubenbacher. Generic ideals and Moreno-Socías conjecture. In *Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation*, pages 21–23, New York, 2001. ACM.

[3] David J. Anick. Thin algebras of embedding dimension three. *J. Algebra*, 100(1):235–259, 1986.

[4] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[5] David Bayer and Michael Stillman. A criterion for detecting m-regularity. *Invent. Math.*, 87(1):1–11, 1987.

[6] David Bayer and Michael Stillman. On the complexity of computing syzygies. *J. Symbolic Comput.*, 6(2-3):135–147, 1988. Computational aspects of commutative algebra.

[7] David Allen Bayer. *The Division Algorithm and the Hilbert Scheme*. ProQuest LLC, Ann Arbor, MI, 1982. Thesis (Ph.D.)–Harvard University.

[8] T. Becker, V. Weispfenning, and H. Kredel. *Gröbner Bases: A Computational Approach to Commutative Algebra*. Springer-Verlag, New York, 1993.

[9] Carlos A. Berenstein and Alain Yger. Bounds for the degrees in the division problem. *Michigan Math. J.*, 37(1):25–43, 1990.

[10] W. Dale Brownawell. Bounds for the degrees in the Nullstellensatz. *Ann. of Math. (2)*, 126(3):577–591, 1987.

[11] B. Buchberger. *Gröbner-Bases: An Algorithmic Method in Polynomial Ideal Theory*. Reidel Publishing Company, Dodrecht - Boston - Lancaster, 1985.

[12] Bruno Buchberger. *An algorithm for finding the basis elements in the residue class ring modulo a zero dimensional polynomial ideal*. PhD thesis, Mathematical Institute, University of Innsbruck, Austria, 1965. English translation published in the Journal of Symbolic Computation 41 (2006) 475–511.

[13] Bruno Buchberger. A criterion for detecting unnecessary reductions in the construction of Gröbner bases. In *EUROSAM '79: Proceedings of the International Symposiumon on Symbolic and Algebraic Computation*, pages 3–21, London, UK, 1979. Springer-Verlag.

[14] Young Hyun Cho and Jung Pil Park. Conditions for generic initial ideals to be almost reverse lexicographic. *J. Algebra*, 319(7):2761–2771, 2008.

[15] Mircea Cimpoeaş. Generic initial ideal for complete intersections of embedding dimension three with strong Lefschetz property. *Bull. Math. Soc. Sci. Math. Roumanie (N.S.)*, 50(98)(1):33–66, 2007.

[16] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms*. Springer-Verlag, New York, 2nd edition, 1997.

[17] Alicia Dickenstein, Noaï Fitchas, Marc Giusti, and Carmen Sessa. The membership problem for unmixed polynomial ideals is solvable in single exponential time. *Discrete Appl. Math.*, 33(1-3):73–94, 1991. Applied algebra, algebraic algorithms, and error-correcting codes (Toulouse, 1989).

[18] Thomas W. Dubé. The structure of polynomial ideals and Gröbner bases. *SIAM J. Comput.*, 19(4):750–775, 1990.

[19] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[20] David Eisenbud, Craig Huneke, and Wolmer Vasconcelos. Direct methods for primary decomposition. *Invent. Math.*, 110(2):207–235, 1992.

[21] Jean Charles Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In *ISSAC '02: Proceedings of the 2002 international symposium on Symbolic and algebraic computation*, pages 75–83, New York, NY, USA, 2002. ACM.

[22] Noaï Fitchas and André Galligo. Nullstellensatz effectif et conjecture de Serre (théorème de Quillen-Suslin) pour le calcul formel. *Math. Nachr.*, 149:231–253, 1990.

[23] Ralf Fröberg. An inequality for Hilbert series of graded algebras. *Math. Scand.*, 56(2):117–144, 1985.

[24] Ralf Fröberg and Joachim Hollman. Hilbert series for ideals generated by generic forms. *J. Symbolic Comput.*, 17(2):149–157, 1994.

[25] Shuhong Gao, Yinhua Guan, and Frank Volny IV. A new incremental algorithm for computing Gröbner bases. In *ISSAC'10: Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation*, pages 13–19, Munich, Germany, 2010. ACM.

[26] Shuhong Gao, Frank Volny IV, and Mingsheng Wang. A new algorithm for computing Gröbner bases. July 2013.

[27] Alessandro Giovini, Teo Mora, Gianfranco Niesi, Lorenzo Robbiano, and Carlo Traverso. “one sugar cube, please” or selection strategies in the buchberger algorithm. In *Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation*, ISSAC '91, pages 49–54, New York, NY, USA, 1991. ACM.

[28] M. Giusti. Some effectivity problems in polynomial ideal theory. In *EUROSAM 84 (Cambridge, 1984)*, volume 174 of *Lecture Notes in Comput. Sci.*, pages 159–171. Springer, Berlin, 1984.

[29] Grete Hermann. Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. *Math. Ann.*, 95(1):736–788, 1926.

[30] János Kollár. Sharp effective Nullstellensatz. *J. Amer. Math. Soc.*, 1(4):963–975, 1988.

[31] Martin Kreuzer and Lorenzo Robbiano. *Computational Commutative Algebra 2*. Springer-Verlag, Heidelberg, 2005.

[32] Teresa Krick and Alessandro Logar. Membership problem, representation problem and the computation of the radical for one-dimensional ideals. In *Effective methods in algebraic geometry (Castiglioncello, 1990)*, volume 94 of *Progr. Math.*, pages 203–216. Birkhäuser Boston, Boston, MA, 1991.

[33] Y. N. Lakshman. A single exponential bound on the complexity of computing Gröbner bases of zero-dimensional ideals. In *Effective methods in algebraic geometry (Castiglioncello, 1990)*, volume 94 of *Progr. Math.*, pages 227–234. Birkhäuser Boston, Boston, MA, 1991.

[34] Y. N. Lakshman and Daniel Lazard. On the complexity of zero-dimensional algebraic systems. In *Effective methods in algebraic geometry (Castiglioncello, 1990)*, volume 94 of *Progr. Math.*, pages 217–225. Birkhäuser Boston, Boston, MA, 1991.

[35] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[36] D. Lazard. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In *Computer algebra (London, 1983)*, volume 162 of *Lecture Notes in Comput. Sci.*, pages 146–156. Springer, Berlin, 1983.

[37] Daniel Lazard. Résolution des systèmes d'équations algébriques. *Theoret. Comput. Sci.*, 15(1):77–110, 1981.

[38] D. W. Masser and G. Wüstholz. Fields of large transcendence degree generated by values of elliptic functions. *Invent. Math.*, 72(3):407–464, 1983.

[39] Ernst W. Mayr and Albert R. Meyer. The complexity of the word problems for commutative semigroups and polynomial ideals. *Adv. in Math.*, 46(3):305–329, 1982.

[40] Ernst W. Mayr and Stephan Ritscher. Degree bounds for gröbner bases of low-dimensional polynomial ideals. In *Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation*, ISSAC '10, pages 21–27, New York, NY, USA, 2010. ACM.

[41] H. Michael Möller and Ferdinando Mora. Upper and lower bounds for the degree of groebner bases. In *Proceedings of the International Symposium on Symbolic and Algebraic Computation*, EUROSAM '84, pages 172–183, London, UK, UK, 1984. Springer-Verlag.

[42] H. Michael Möller, Teo Mora, and Carlo Traverso. Gröbner bases computation using syzygies. In *ISSAC '92: Papers from the international symposium on Symbolic and algebraic computation*, pages 320–328, New York, NY, USA, 1992. ACM.

[43] Guillermo Moreno-Socías. Autour de la fonction de hilbert-samuel (escaliers d'idéaux polynomiaux).

[44] Guillermo Moreno-Socías. Degrevlex Gröbner bases of generic complete intersections. *J. Pure Appl. Algebra*, 180(3):263–283, 2003.

[45] Keith Pardue. Generic sequences of polynomials. *J. Algebra*, 324(4):579–590, 2010.

[46] R˙On an installation of buchberger's algorithm. *Journal of Symbolic Computation*, 6(2-3):275–286, 1988.

[47] Bodo Renschuch. Beiträge zur konstruktiven Theorie der Polynomideale. XVII/1. Zur Hentzelt/Noether/Hermannschen Theorie der endlich vielen Schritte. *Wiss. Z. Pädagog. Hochsch. "Karl Liebknecht" Potsdam*, 24(1):87–99, 1980.

[48] A. Seidenberg. Constructions in algebra. *Trans. Amer. Math. Soc.*, 197:273–313, 1974.

[49] Jean-Pierre Serre. *Local algebra*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2000. Translated from the French by CheeWhye Chin and revised by the author.

[50] Martín Sombra. A sparse effective Nullstellensatz. *Adv. in Appl. Math.*, 22(2):271–295, 1999.

Index