ABSTRACT

RITSCHER, STEPHAN. Degree Bounds for Zero-dimensional Gröbner Bases. (Under the direction of Dr. Hoon Hong).

The theory of Gröbner bases plays a fundamental role in solving and reasoning with polynomial equations (ideals). This thesis will review and prove matching upper and lower degree bounds of Gröbner bases for zero-dimensional ideals and prove that this degree is also obtained in the generic case. With n being the number of variables and d the degree of the generators, for the lexicographic monomial ordering this degree is d^n, for graded monomial orderings it is $n(d-1)+1$.

Degree Bounds for Zero-dimensional Gröbner Bases

by
Stephan Ritscher

A thesis submitted to the Graduate Faculty of
North Carolina State University
in partial fullfillment of the
requirements for the Degree of
Master of Science

Mathematics

Raleigh, North Carolina

2009

APPROVED BY:

Dr. M. F. Singer

Dr. A. Szanto

Dr. H. Hong
Chair of Advisory Committee

BIOGRAPHY

After graduating from Gymnasium Friedericianum Erlangen with intense courses in Mathematics and Physics, I enrolled for Mathematics with minor Computer Science at Friedrich Alexander University Erlangen-Nürnberg where I finished my Vordiplom in two years. Being accepted for the study program TopMath at Technische Universität München I finished my Bachelor of Science in Mathematics one year later. After another year I came to North Carolina State University in order to finish my Master studies.

ACKNOWLEDGMENTS

It is a pleasure for me to thank the many people and organizations that made this thesis possible.

First of all, I am deeply indebted to my thesis supervisor at North Carolina State University, Dr. Hoon Hong. He spent many valuable hours teaching me, from basic approaches to research to complex tools in the field of polynomial algebra and methods of presentation. His simple and intuitive explanations along with clarifying exercises helped me as much as his enthusiasm about research motivated me. Whenever I had a question, he was the one to help me with advice.

I also want to thank my thesis committee, Prof. Singer and Prof. Szanto from North Carolina State University, for their advice for my research and the comfortable atmosphere during the examination.

Many thanks go to my supervisor at Technische Univerität München (Germany), Dr. Ernst W. Mayr. He encouraged me to join the TopMath study program in Munich and did a great job supervising me henceforth. Also the choice of my special topic is due to him - a choice I continue to be pleased with. Furthermore, he recommended Dr. Hong as a supervisor for research and a Master thesis to me.

I want to thank all my teachers in mathematics, the professors at the Friedrich Alexander Universität Erlangen-Nürnberg, Technische Universität München, and North Carolina State University as well as my high school teachers, especially Mr. Stark and Mrs. Schmidt-Nessler for encouraging me to participate in high school math contests respectively preparing me well for university in my last two years at high school.

I am grateful to all the organizations that supported me financially - especially for my studies abroad -, but also provided me with beneficially opportunities to continue learning beyond the horizon of mathematics, even during my studies at universities. These are the Max-Weber-Programm (a Bavarian scholarship program), the Studienstiftung des deutschen Volkes (a German scholarship program) and TopMath.

Lastly, but most importantly, I want to thank my parents, Christine and Matthias Ritscher. They raised and taught me, always encouraged me to gather knowledge, helped me in school, and always stood by me.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF SYMBOLS

$R, \mathbb{K}, \mathbb{N}, \mathbb{Z}, \mathbb{C}$	ring, field, natural numbers $(1, 2, 3, \ldots)$, integers, complex numbers
$\mathcal{R}, \mathcal{S}$	ring of coefficients of polynomials/homogeneous polynomials
f, g, h	polynomials
$\deg(f)$	total degree of f
$\mathrm{LM}(f), \mathrm{LT}(f)$	leading monomial / leading term of polynomial f
p, q	points with coordinates p_i, q_i
$x_1, \ldots, x_n$	ring variables ($x_0, \ldots, x_n$ for homogeneous ideals)
$F = \{f_1, \ldots, f_s\}$	ideal generators
d_i	degree of f_i ($d_1 \leq \ldots \leq d_s$ is assumed)
$G = \{g_1, \ldots, g_t\}$	Gröbner basis
I, J	ideals (J homogeneous)
$\mathcal{I}, \mathcal{J}$	ideal of polynomials with indeterminate coeff. ($\mathcal{J}$ homogeneous)
$\dim(I), \dim_{\mathbb{P}}(J)$	ideal dimension of I, projective ideal dimension of J
$\dim_{\mathbb{K}}(V)$	vector space dimension of V over $\mathbb{K}$
$\mathfrak{m}, \mathfrak{p}$	prime ideals
$f_{=d}$	homogeneous part of polynomial f of degree d
$S_{=d}$	$\{f \in S : f \text{ homogeneous}, \deg(f) = d \text{ or } f = 0\}$
$\mathbf{I}(S)$	ideal generated by point set S
$\mathbf{V}(F), \mathbf{V}_{\mathbb{P}}(F)$	variety/projective variety generated by polynomials in set F
$\mathrm{Res}(F_0, \ldots, F_n)$	resultant polynomial of the homogeneous polynomials
m_y	multiplication with y as a map
$[f]$	factor class containing f
$\Lambda = (\Lambda_r)$	Koszul complex
δ_r	maps of the Koszul complex
$e_{i_1} \wedge \ldots \wedge e_{i_r}$	basis vector of Λ_r
H_r	homology of the Koszul complex $(\ker(\delta_r)/\mathrm{im}(\delta_{r+1}))$
$\det(\varphi)$	determinant of the linear map φ
ψ	a specialization of $\mathcal{R}[x_1, \ldots, x_n]$ or $\mathcal{S}[x_0, \ldots, x_n]$ to $\mathbb{K}[x_1, \ldots, x_n]$ respectively $\mathbb{K}[x_0, \ldots, x_n]$
$\mathrm{span}_R(S)$	R-linear subspace spanned by S

Chapter 1

Introduction

In many contexts mathematical questions can be naturally formulated using polynomial systems. Their solution often can be given by standard algorithms of polynomial algebra and algebraic geometry, for example ideal membership tests and consistency and finiteness tests for the set of common roots.

Many of these algorithms use Gröbner bases, which are nice representations of polynomial ideals. They were introduced by Bruno Buchberger ([1], translated in [2]), who named them in honor of his supervisor Wolfgang Gröbner. For an overview consult [3] or [4]. In general, Gröbner bases are very hard to compute. Ernst Mayr and Albert Meyer were able to show in [5], that the membership problem for ideals is exponential space hard. On the other hand Klaus Kühnle and Ernst Mayr developed in [6] an exponential space algorithm for the computation of Gröbner bases. The complexity of this algorithm heavily depends on a good upper degree bound for Gröbner bases. This entails the question, whether better upper degree bounds for certain classes of ideals exist.

In this thesis the class of zero-dimensional ideals will be considered. For these ideals much better bounds are known, depending on the monomial ordering. The upper bounds by Daniel Lazard ([7] and [8], translated in [9]) and matching lower bounds for graded monomial orderings will be stated and proved. Additionally the generic case will be analyzed, which, to the knowledge of the author, wasn't explicitely mentioned before, although the result is an immediate application of Marc Chardin's multivariate subresultant introduced in [10]. Also the well-known bounds for the lexicographic monomial ordering will be treated.

Following several applications, basic notations together with common problem statements will be introduced and motivated in the first chapter. The examples will raise questions that cannot be answered in this chapter. Therefore the examples will be continued throughout a large part of the thesis. Claims regarding ideal theory and Gröbner bases that are stated in this chapter, will be stated rigorously with proof or citation in chapter 2.

The second chapter will give an introduction to Gröbner bases, their computation and some of their properties. The state of the art of degree bounds for Gröbner bases will be summarized, but only proofs for the zero-dimensional case will be given. This also includes the earlier mentioned generic case.

1.1 Motivating Example: Optimization

A well known and very useful method in optimization theory is linear programming. The aim is to optimize a linear cost function with respect to a set of constraints which are formulated as linear equations or inequalities. This problem is solved by the simplex algorithm by George Dantzig, which is efficient for most inputs, but needs exponential time in degenerate cases. Newer algorithms known as the ellipsoid method by Leonid Khachiyan and the inner point method by Nardendra Karmarkar always run in polynomial time and the latter is also more efficient in practice.

But sometimes linear equations don't suffice in order to model a problem. A standard approach would be to use gradient and Newton methods to optimize continous functions without constraints or penalty, barrier methods and sequential linear programming in order to optimize funtions with constraints. These numerical methods are fast, but they only find local optima in general, not the overall best solution.

Using Gröbner bases, however, one can compute the global optimum of a polynomial function with respect to polynomial constraints. Concerning the focus of this thesis only a very simple example will be discussed. For a better treatment see [11].

Example 1. Find the point (x, y) inside the unit cirle around $(1, 0)$ which maximizes

$$f(x, y) := x - 3y.$$

Solution: The constraint can be written as

$$h(x, y) := x^2 + y^2 - 1 \leq 0.$$

Optimization theory provides necessary optimality conditions, known as Karush-Kuhn-Tucker conditions:

$$\begin{aligned}
0 &= \partial_x f(x,y) + \lambda \partial_x h(x,y) = 1 + 2\lambda x \\
0 &= \partial_y f(x,y) + \lambda \partial_y h(x,y) = -3 + 2\lambda y \\
0 &= \lambda h(x,y) = \lambda x^2 + \lambda y^2 - \lambda
\end{aligned} \tag{1.1}$$

Ignoring the additional condition $\lambda > 0$ leaves the problem of solving a system of polynomials in several variables. This easily can be done using Gröbner bases as will be demonstrated later. The solutions then will be evaluated in order to find the global maximum.

1.2 Motivating Example: Automatic Theorem Proving

Another broad application field for Gröbner bases is automatic theorem proving. Basically one formulates the premises and the claim as polynomial equations. Then an algebraical method is desirable which checks whether the claim follows from the premises. Especially suited for this approach are geometric problems. Here one can easily describe points by coordinates and the geometric construction by polynomials. This will be demonstrated following a small example. But be aware that not all examples will work as nicely as the one described here. For more on the possible problems and how to overcome them consult [12], Chapter 6, §3-4.

Example 2. In figure 1.1 an equilateral triangle ABC with the center M of its circumcirle and the line from A to the median D of BC is depicted. This example shall prove the well-known fact that M lies on the median line AD.

Therefore the configuration has to be modeled by polynomial equations. In order to reduce the number of variables, the coordinate system was chosen with origin A and x-axis through B (without loss of generality). Note that the only free variable is called u. All other variables $x_1, \ldots x_6$ will depend on u. Since there are six dependend variables, one would expect six equations to determine them.

The point C is the third point of the equilateral triangle. So its distances to A and B must equal the distance between A and B. This gives

$$\begin{aligned}
f_1 &:= x_1^2 + x_2^2 - u^2 = 0 \\
f_2 &:= (x_1 - u)^2 + x_2^2 - u^2 = 0.
\end{aligned}$$

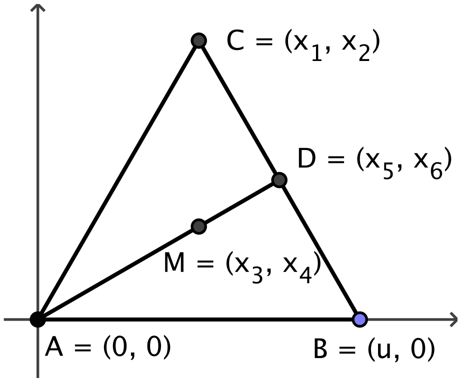


Figure 1.1: Equilateral triangle ABC with cirumcirle center M and one median line.

M is the center of the circumcircle, so its distances to A, B and C must match, which is described by

$$f_3 := x_3^2 + x_4^2 - (x_3 - u)^2 - x_4^2 = 0$$
$$f_4 := x_3^2 + x_4^2 - (x_3 - x_1)^2 - (x_4 - x_2)^2 = 0.$$

Finally D is the median of BC, so

$$f_5 := x_5 - \frac{1}{2}(x_1 + u) = 0$$
$$f_6 := x_6 - \frac{1}{2}x_2 = 0.$$

These six polynomials fully describe the geometric construction. This means every assignment of $u, x_1, \ldots, x_6$ such that $f_i(u, x_1, \ldots, x_6) = 0$ is a valid configuration. The claim is now that for all these configurations M lies on the line AD, which is captured by

$$h := x_3x_6 - x_4x_5 = 0.$$

So the proof boils down to showing that $f_1 = \ldots = f_6 = 0$ implies $h = 0$. The next chapter will reveal how to do this.

Chapter 2

Gröbner Bases

In the first chapter, the use of polynomial ideals was motivated by examples. Several important non-trivial questions arose naturally during their treatment.

This chapter will first give an overview of the theory of Gröbner bases which can be used to answer the questions from chapter 1. Also definition and characterizations of the ideal dimension will be given. This is motivated by the focus on zero-dimensional ideals in chapter 3.

2.1 Ideals

In this section the foundations of ideal theory will be given. This establishes a language to speak about the problems of chapter 1. Therefore the examples will be continued until finally resolved.

A *ring* (with one) is a set R with two distinguished elements 0 and 1 and two operators acting on it called addition

$$+ : R \times R \longrightarrow R$$

and multiplication

$$\cdot : R \times R \longrightarrow R.$$

$(R, +, 0)$ has to be an abelian group, i.e. $\forall a, b, c \in R$

$$(a+b)+c = a+(b+c) \qquad \text{(associativity)}$$
$$a+b = b+a \qquad \text{(commutativity)}$$
$$a+0 = a \qquad \text{(identity)}$$
$$a+(-a) = 0 \text{ for some } -a \in R \qquad \text{(existence of inverse).}$$

Furthermore $(R, \cdot, 1)$ has to be a monoid, i.e. $\forall a, b, c \in R$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \qquad \text{(associativity)}$$
$$a \cdot 1 = a = 1 \cdot a \qquad \text{(identity).}$$

Finally, addition and multiplication have to interact nicely:

$$a \cdot (b+c) = (a \cdot b) + (a \cdot c) \qquad \text{(distributivity)}$$
$$(a+b) \cdot c = (a \cdot c) + (b \cdot c) \qquad \text{(distributivity)}$$

A ring is called *commutative*, if $\forall a, b \in R$

$$a \cdot b = b \cdot a.$$

As usually ab denotes $a \cdot b$ and parenthesis may be omitted if not neccessary (following the PEMDAS order of evaluation). Well known rings are the integers $(\mathbb{Z}, +, \cdot, 0, 1)$ and the polynomials over a field $(\mathbb{K}[x_1, \ldots, x_n], +, \cdot, 0, 1)$. Furthermore every field constitutes a ring.

The ring of polynomials over $\mathbb{K}$ in the indeterminates $x_1, \ldots, x_n$ is denoted by $\mathbb{K}[x_0, \ldots, x_n]$. The following grading of polynomials will be used. The *(total) degree* of a monomial is defined as the sum of the exponents of the variables that occur in the monomial. The degree of a polynomial is the maximum of the degrees of the monomials of its terms. A polynomial is called *homogeneous* if all terms have the same degree.

One can *homogenize* a polynomial $f \in \mathbb{K}[x_1, \ldots, x_n]$ by introducing a new variable x_0 and defining

$$^hf := x_0^{\deg(f)} f\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right).$$

Then ^hf is a homogeneous polynomial in $\mathbb{K}[x_0, \ldots, x_n]$ with

$$f(x_1, \ldots, x_n) = {}^hf(1, x_1, \ldots, x_n).$$

Of special interest are the subsets which are closed under polynomial combinations, called ideals. In formulas, $I \subset R$ is an *ideal* if $\forall a, b \in I, r \in R$

$$a + b \in R$$
$$r \cdot a \in R.$$

For given polynomials $f_1, \ldots, f_s$,

$$\langle f_1, \ldots, f_s \rangle := \left\{ \sum_{i=1}^{s} a_i f_i : a_i \in \mathbb{K}[x_1, \ldots, x_n] \right\}$$

represents the smallest ideal containing these polynomials. Furthermore $\{f_1, \ldots, f_s\}$ is called an *(ideal) basis* of the ideal $I = \langle f_1, \ldots, f_s \rangle$.

As already seen in the introduction, the set of common roots of polynomials $f_1, \ldots, f_s$ is of natural interest. This set is called *(algebraic) variety* (generated by $f_1, \ldots, f_s$) and will be written as

$$\mathbf{V}(f_1, \ldots, f_s) := \{x \in \mathbb{K}^n : f_i(x) = 0 \text{ for } i = 1, \ldots, s\}$$

An immediate observation is that polynomial combinations of $f_1, \ldots, f_s$ also vanish on this variety, i.e.

$$\forall p \in \mathbf{V}(f_1, \ldots, f_s), f \in \langle f_1, \ldots, f_s \rangle : f(p) = 0.$$

Example 3. Consider again the system of polynomials (1.1). Let

$$f_1 := 1 + 2\lambda x$$
$$f_2 := -3 + 2\lambda y$$
$$f_3 := \lambda x^2 + \lambda y^2 - \lambda.$$

The ideal $I = \langle f_1, f_2, f_3 \rangle$ contains e.g. the polynomial

$$h = 3x + y.$$

You can see this from the equation

$$h = y f_1 - x f_2.$$

But you might guess that it is not always easy to see whether a polynomial is contained in a given ideal. So an algorithm to test ideal membership would be of great help. That will be one of the topics in the next sections.

Consider the points $(x, y, \lambda) = (0, 0, 0)$ respectively $\left(\frac{-1}{\sqrt{10}}, \frac{3}{\sqrt{10}}, \frac{5}{\sqrt{10}}\right)$. For the first point one obtains

$$f_1(0, 0, 0) = 1,$$

so $(0, 0, 0) \notin \mathbf{V}(f_1, f_2, f_3)$. The second point gives

$$f_1\left(\frac{-1}{\sqrt{10}}, \frac{3}{\sqrt{10}}, \frac{5}{\sqrt{10}}\right) = f_2\left(\frac{-1}{\sqrt{10}}, \frac{3}{\sqrt{10}}, \frac{5}{\sqrt{10}}\right) = f_3\left(\frac{-1}{\sqrt{10}}, \frac{3}{\sqrt{10}}, \frac{5}{\sqrt{10}}\right) = 0.$$

Thus $\left(\frac{-1}{\sqrt{10}}, \frac{3}{\sqrt{10}}, \frac{5}{\sqrt{10}}\right) \in \mathbf{V}(f_1, f_2, f_3)$. Sometimes one can guess a few solutions, but in general it is hard - especially to find all of them. This encourages to analyze ideals in more detail in the next chapter.

For computations it is really hard to deal with infinite sets. A finite description is always necessary. Therefore Hilbert's Basis Theorem is of great importance for all ideal algorithms.

Theorem 4 (Hilbert's Basis Theorem)**.** *If R is noetherian, i.e. every ideal in R has a finite basis, so is $R[x_1, \ldots, x_n]$. Especially, $\mathbb{K}[x_1, \ldots, x_n]$ is noetherian.*

Proof. See [13] (Theorem 1.2) and note that any field is noetherian since it only has trivial ideals. □

Another way to construct an ideal is the set of polynomials that vanish on a (not neccessarily finite) given set $V \subset \mathbb{K}^n$

$$\mathbf{I}(V) := \{f \in \mathbb{K}[x_1, \ldots, x_n] : f(x_1, \ldots, x_n) = 0 \ \forall (x_1, \ldots, x_n) \in V\}.$$

Conversely define a subset of $\mathbb{K}^n$, called *(algebraic) variety*, as the set of common root of a (not neccessarily finite) given set of polynomials F

$$\mathbf{V}(F) := \{x \in \mathbb{K}^n : f(x) = 0 \ \forall f \in F\}.$$

From an abstract point of view, $\mathbf{I}$ maps from the subsets of $\mathbb{K}^n$ to the ideals of $\mathbb{K}[x_1, \ldots, x_n]$ (actually to the radical ideals, see Hilbert's Nullstellensatz, theorem 5) and $\mathbf{V}$ maps from the subsets of $\mathbb{K}[x_1, \ldots, x_n]$ to the set of varieties in $\mathbb{K}^n$.

It is easily verified that $\mathbf{I}$ and $\mathbf{V}$ are inclusion reversing, i.e. $\forall V, W \subset \mathbb{K}^n, F, G \subset \mathbb{K}[x_1, \ldots, x_n]$

$$\begin{aligned} V \subset W &\Rightarrow \mathbf{I}(V) &\supset \mathbf{I}(W) \\ F \subset G &\Rightarrow \mathbf{V}(F) &\supset \mathbf{V}(G) \end{aligned}$$

Finally, Hilbert's Nullstellensatz connects the ideals I and $\mathbf{I}(\mathbf{V}(I))$. But two more concepts are necessary for this theorem.

Given an ideal I of a ring R, the set

$$\sqrt{I} := \{f \in R : \exists d \in \mathbb{N} \text{ such that } f^d \in I\}$$

is an ideal called the *radical* of I. Obviously, $\sqrt{I}$ contains I and $\sqrt{\sqrt{I}} = \sqrt{I}$. An ideal $I = \sqrt{I}$ is called *radical.*

A field $\mathbb{K}$ is called *algebraically closed* if every polynomial over $\mathbb{K}$ can be written as product of linear terms. The most important example of an algebraically closed field are the complex numbers $\mathbb{C}$.

Theorem 5 (Hilbert's Nullstellensatz)**.** *If $\mathbb{K}$ is algebraically closed and $I \subset \mathbb{K}[x_1, \ldots, x_n]$ an ideal, then*

$$\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$$

Proof. See [12] (Chapter 4, Theorem 1.2). □

The same theory can be established in the projective space

$$\mathbb{P}^n := \{(x_0 : \ldots : x_n) \subset \mathbb{C}^{n+1} \setminus \{0\} : x_i \neq 0 \text{ for some } i\}.$$

Here the notation $(x_0 : \ldots : x_n)$ stands for the equivalence class of all points $(\alpha x_0, \ldots, \alpha x_n)$ for $\alpha \in \mathbb{C} \setminus \{0\}$, which can be interpreted as line through the origin in $\mathbb{C}^{n+1}$. There are only very little well defined functions on $\mathbb{P}^n$, e.g. polynomials and homogeneous polynomials are not well defined - even for degree 1. But the roots of homogeneous polynomials f_i can be expressed in terms of these equivalence classes since

$$f_i(x_0, \ldots, x_n) = 0 \Rightarrow f_i(\alpha x_0, \ldots, \alpha x_n) = \alpha^{\deg(f_i)} f_i(x_0, \ldots, x_n) = 0.$$

Every polynomial f can be decomposited into homogeneous components

$$f = \sum_{i=0}^{\deg(f)} f_{=i}$$

where $f_{=i}$ is homogeneous of degree i. A set I is called *homogeneous*, if $f \in F$ implies $f_{=i} \in F$ for all i.

So one can consider the projective variety in $\mathbb{P}^n$ of an homogeneous set F

$$\mathbf{V}_{\mathbb{P}}(F) := \{x \in \mathbb{P}^n : f(x) = 0 \ \forall f \in F\}.$$

There is an equivalent version of of Nullstellensatz in the projective setting, but only a (slightly) weaker version will be needed.

Theorem 6 (Projective Weak Nullstellensatz)**.** *Let $\mathbb{K}$ be an algebraically closed field and J a homogeneous ideal in $\mathbb{K}[x_0, \ldots, x_n]$. Then $\mathbf{V}_{\mathbb{P}}(J) = \emptyset$ if and only if $\langle x_0, \ldots, x_n \rangle \subset \sqrt{J}$.*

Proof. See [12] (Chapter 8, Theorem 3.8). □

2.2 Gröbner Bases

Building upon the foundations of the last section, it is possible to provide solutions for the examples 3 and 2. The key is the concept of Gröbner bases. They will provide algorithms for ideal membership tests and variable elimination.

The first part of the chapter is dedicated to example 2. Missing for the solution is a decision procedure for the radical ideal membership problem, i.e. given a polynomial f one has to determine whether $f \in \sqrt{I}$. But before that the simple ideal membership will be treated.

The ring of polynomials in one variable is a *principal ring*, i.e. all ideals can be generated by only one ring element, namely, given $f_1, \ldots, f_s \in \mathbb{K}[x]$,

$$\langle f_1, \ldots, f_s \rangle = \langle \gcd(f_1, \ldots, f_s) \rangle .$$

Then ideal membership for a polynomial $f \in \mathbb{K}[x]$ can be tested by dividing f by the greatest common divisor $\gcd(f_1, \ldots, f_s)$. f is contained in the ideal if and only if the remainder is 0.

For several variables, this approach doesn't work quite the same, but it can be adopted. The first module is a division algorithm that is able to handle several polynomials. This is necessary since most ideals in $\mathbb{K}[x_1, \ldots, x_n]$ are not principal. To accomplish this, one has to decide on an order of the monomials (for one variable there is only one "good" ordering).

A (total) monomial ordering $\prec$ will be called *admissible* if for all monomials m, n, p

$$m \prec n \;\Rightarrow\; pm \prec pn$$

$$1 \prec m$$

The first premise ensures that the ordering is compatible with multiplication, the second renders it a well-ordering, i.e. every non-empty set of monomials has a smallest element. Both are crucial for the Buchberger algorithm that will be presented soon. If the monomial also fulfills

$$\deg(m) < \deg(n) \Rightarrow m \prec n$$

it is called *degree compatible*. Here, as in the rest of the thesis, the *degree* $\deg(m)$ is the total degree, i.e. the sum of the exponents of all variables that occur in m.

Mainly the following monomial orderings will be treated. As notation, *multiindices* $\alpha = (\alpha_1, \ldots, \alpha_n) \subset \mathbb{N}_0^n$ will be used for writing monomials

$$x^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$$

The *lexicographic ordering* $\prec_{\text{lex}}$ is given by

$$x^\alpha \prec_{\text{lex}} x^\beta \;:\Longleftrightarrow\; \beta_i = \alpha_i \text{ and } \alpha_k < \beta \text{ for some } k \text{ and each } 1 \le i < k.$$

The *reverse lexicographic ordering* is

$$x^\alpha \prec_{\text{revlex}} x^\beta \;:\Longleftrightarrow\; \beta_i = \alpha_i \text{ and } \alpha_k > \beta \text{ for some } k \text{ and each } k < i \le n.$$

Finally, the *graded reverse lexicographic ordering* is defined as

$$x^\alpha \prec_{\text{grevlex}} x^\beta \;:\Longleftrightarrow\; \deg(x^\alpha) < \deg(x^\beta) \text{ or } \Big(\deg(x^\alpha) = \deg(x^\beta) \text{ and } x^\alpha \prec_{\text{revlex}} x^\beta\Big).$$

Example 7. For the better understanding of the above definitions, an excerpt of each ordering (with $x_1 > x_2 > x_3$) in the ring $\mathbb{K}[x_1, x_2, x_3]$ is given.

$$\prec = \prec_{\text{lex}}\colon 1 \prec x_3 \prec x_3^2 \prec \ldots \prec x_2 \prec x_2x_3 \prec x_2x_3^2 \prec \ldots \prec x_1 \prec x_1x_3 \prec x_1x_3^2 \prec \ldots$$

$$\prec = \prec_{\text{revlex}}\colon \ldots \prec x_1^2x_3 \prec x_1x_3 \prec x_3 \prec \ldots \prec x_1^2x_2 \prec x_1x_2 \prec x_2 \prec \ldots \prec x_1^2 \prec x_1 \prec 1$$

$$\prec = \prec_{\text{grevlex}}\colon 1 \prec x_3 \prec x_2 \prec x_1 \prec x_3^2 \prec x_2x_3 \prec x_1x_3 \prec x_2^2 \prec x_1x_2 \prec x_1^2 \prec x_1^3 \prec \ldots$$

Obviously $\prec_{\text{revlex}}$ is *not* admissible. $\prec_{\text{lex}}$ and $\prec_{\text{grevlex}}$, however, are admissible monomial orderings. Both will be used recurrently in this thesis. Furthermore the graded reverse lexicographic ordering is degree compatible while the lexicographic ordering is not.

Now all that is missing for the division algorithm is some notation. Given a polynomial f, the largest monomial of f with respect to some monomial ordering $\prec$ with nonzero coefficient is called the *leading monomial* of f and denoted by $\mathrm{LM}_\prec(f)$. Its coefficient, the *leading coefficient*, is written as $\mathrm{LC}_\prec(f)$ and the *leading term* of f is simply $\mathrm{LT}_\prec(f) := \mathrm{LC}_\prec(f)\cdot\mathrm{LM}_\prec(f)$. Usually the monomial ordering will be fixed and the subscripts will be omitted.

In order to divide a polynomial f by a polynomial g, the leading monomial of f must be divisible by the leading monomial of g. The basic idea for the division algorithm is to just try this with all given divisor polynomials. If nothing works, the leading term is declared as remainder and one continues with the next biggest term.

However, the result of the algorithm is not as expressive as one might expect or wish.

Example 8. This shall be illustrated with example 3 and the lexicographic monomial ordering with $x \succ y \succ \lambda$. The ideal I was generated by

$$\begin{aligned} f_1 &:= 2x\lambda + 1 \\ f_2 &:= 2y\lambda - 3 \\ f_3 &:= x^2\lambda + y^2\lambda - \lambda. \end{aligned}$$

Obviously f_3 is contained in the ideal I. So one could expect to get a zero remainder of division. Consider the following two calls of DIVIDE:

Algorithm 1 DIVIDE

```
Procedure DIVIDE($h, (f_1, \dots, f_s)$)
Input: Polynomials $h, f_1, \dots, f_s$
Output: Representation $h = \sum_{i=1}^{s} a_i f_i + r$
$\widehat{h} \leftarrow h, r \leftarrow 0,\ a_i \leftarrow 0\ \forall i = 1, \dots, s$
while $\widehat{h} \neq 0$ do
    Let $i \in \{1, \dots, s\}$ be minimal such that $\mathrm{LM}(f_i) \mid \mathrm{LM}(\widehat{h})$.
    if such $i$ exists then
        $a_i \leftarrow a_i + \frac{\mathrm{LT}(\widehat{h})}{\mathrm{LT}(f_i)}$
        $\widehat{h} \leftarrow \widehat{h} - \frac{\mathrm{LT}(\widehat{h})}{\mathrm{LT}(f_i)} f_i$
    else
        $r \leftarrow \mathrm{LT}(\widehat{h})$
        $\widehat{h} \leftarrow \widehat{h} - \mathrm{LT}(\widehat{h})$
    end if
end while
return $h = \sum_{i=1}^{s} a_i f_i + r$
EndProcedure
```

Division algorithm for multiple variables and polynomials

DIVIDE($f_3, (f_3, f_2, f_1)$): This call returns after the first pass with the representation

$$f_3 = 1 \cdot f_3 + 0 \cdot f_2 + 0 \cdot f_1 + 0$$

DIVIDE($f_3, (f_1, f_2, f_3)$): According to the algorithm $\widehat{h} := f_3$ is first divided by f_1, yielding

$$\begin{aligned} a_1 &\leftarrow \frac{x^2\lambda}{2x\lambda} = \frac{x}{2} \\ \widehat{h} &\leftarrow \widehat{h} - \frac{x}{2} f_1 = -\frac{x}{2} + y^2\lambda - \lambda \end{aligned}$$

Since the leading monomial $\mathrm{LM}(\widehat{h}) = x$ is not divisible by any leading monomial of f_1, f_2, f_3, the next step is

$$\begin{aligned} r &\leftarrow -\frac{x}{2} \\ \widehat{h} &\leftarrow \widehat{h} + \frac{x}{2} = y^2\lambda - \lambda \end{aligned}$$

Now $\widehat{h}$'s leading monomial is divisible by f_2's, which results in

$$\begin{aligned} a_2 &\leftarrow \frac{y^2\lambda}{2y\lambda} = \frac{y}{2} \\ \widehat{h} &\leftarrow \widehat{h} - \frac{y}{2} f_2 = \frac{3}{2} y - \lambda \end{aligned}$$

Finally the remaining terms of $\widehat{h}$ cannot be divided further such that they will be added to r. This gives the representation

$$f_3 = \frac{x}{2} f_1 + \frac{y}{2} f_2 + (-\frac{x}{2} + \frac{3}{2} y - \lambda).$$

From the example it is clear that the remainder of the division depends on the order of the divisors $f_1, \ldots, f_s$, whereas the ideal $\langle f_1, \ldots, f_s \rangle$ is independent of the order of the generators. From a remainder $r = \mathrm{DIVIDE}(h, (f_1, \ldots, f_s)) = 0$, one can deduce that the polynomial h is in the ideal $I = \langle f_1, \ldots, f_s \rangle$. But in the current form the contrary is not true, as was exposed by the second call of DIVIDE: a nonzero remainder does not necessarily imply that $h \notin I$.

This flaw will be overcome by choosing a special ideal basis. It should be required that the leading monomial of every polynomial that is contained in the ideal is divisible by at least one of the leading monomials of the basis polynomials. This alone already fixes the algorithm. To see this, consider $h \in I$ and note that

$$\widehat{h} = h - \sum_{i=1}^{s} a_i f_i - r$$

Since $r = 0$ in the beginning, $\widehat{h}$ will be in the ideal and therefore its leading monomial is divisible by one of the monomials in the basis. Therefore $r = 0$ will remain true throughout the algorithm as $\widehat{h}$ will always be in the ideal.

A basis $G = \{g_1, \ldots, g_t\}$ of an ideal I fulfilling this property is called *Gröbner basis*. In other words,

$$\forall h \in I : \mathrm{LM}(g_i) \mid \mathrm{LM}(h) \text{ for some } i \in \{1, \ldots, t\}$$

Theorem 9. *If G is a Gröbner basis, the remainder of the division algorithm*

$$\mathrm{nf}(f) := \mathrm{DIVIDE}(f, G)$$

is unique (i.e. does not depend on the order of the emelents of G). It is called normal form *of f (with respect to G/with respect to $\prec$) and no term of* $\mathrm{nf}(f)$ *is divisible by an element of* $\mathrm{LM}(G)$. *Furthermore* $\mathrm{nf} : \mathbb{K}[x_1, \ldots, x_n] \longrightarrow \mathbb{K}[x_1, \ldots, x_n]$ *is linear and for all* $f_1, f_2 \in \mathbb{K}[x_1, \ldots, x_n]$

$$\mathrm{nf}(f_1) = \mathrm{nf}(f_2) \Longleftrightarrow f_1 - f_2 \in \langle G \rangle .$$

Finally, $A := \{\mathrm{nf}(f) : f \in \mathbb{K}[x_1, \ldots, x_n]\}$ *with*

$$+ : A \times A \longrightarrow A, (f_1, f_2) \mapsto f_1 + f_2$$

$$\cdot : A \times A \longrightarrow A, (f_1, f_2) \mapsto \mathrm{nf}(f_1 f_2)$$

is a ring generated by the monomials not contained in $\langle \mathrm{LM}(I) \rangle$ *and is isomorphic to* $\mathbb{K}[x_1, \ldots, x_n]/I$.

Proof. For the first part see [12] (Chapter 2, Proposition 6.1, Corollary 6.2 and Exercise 6.12).

For $A \cong \mathbb{K}[x_1, \ldots, x_n]/I$ note that, by the first part of the theorem, every equivalence class of $\mathbb{K}[x_1, \ldots, x_n]/I$ contains exactly one normal form. The addition and multiplication on A are defined to mimic the behaviour on $\mathbb{K}[x_1, \ldots, x_n]/I$. □

In some places the notation $\text{nf}_G(f)$ will be used to emphasize the dependence on G. Usually this will be clear from the context.

For the computation of a Gröbner basis the *Buchberger algorithm* can be used. It takes as input an arbitrary basis and outputs a Gröbner basis. It works iteratively and improves the basis in every round in the sense that strictly more leading monomials of the ideal will be divisible by one of the basis monomials. The new polynomials are obtained by eliminating the leading terms of two polynomials in the basis, the so-called *S-polynomials*:

$$S(f,g) := \frac{\text{LT}(g)}{\gcd(\text{LM}(f), \text{LM}(g))} f - \frac{\text{LT}(f)}{\gcd(\text{LM}(f), \text{LM}(g))} g$$

Algorithm 2 BUCHBERGER

```
Procedure BUCHBERGER($f_1, \dots, f_s$)
Input: Polynomials $F = \{f_1, \dots, f_s\}$
Output: Gröbner basis $G = \{g_1, \dots, g_t\}$ of $I = \langle f_1, \dots, f_s \rangle$.
  $G \leftarrow F$
  while $\exists f, g \in G : \text{nf}_G(S(f,g) \neq 0$ do
      $G \leftarrow G \cup \{\text{nf}_G(S(f,g))\}$
  end while
EndProcedure
```

Buchberger algorithm for the computation of a Gröbner basis

Theorem 10. *The Buchberger algorithm (algorithm 2) always terminates and outputs a Gröbner basis $G = \{g_1, \dots, g_t\}$ of the ideal $I = \langle f_1, \dots, f_s \rangle$.*

Proof. See [12] (Chapter 2, Theorem 7.2). Note that neither the choice of the pair $f, g \in G$ nor the order of the polynomials in G for the division affect finiteness and correctness of the algorithm (but its efficiency might vary). □

Example 11. Returning to example 3 with the lexicographic ordering, one would need a Gröbner basis of the ideal I generated by

$$f_1 = 2x\lambda + 1$$

$$f_2 = 2y\lambda - 3$$

$$f_3 = x^2\lambda + y^2\lambda - \lambda.$$

in order to properly use the division algorithm. First consider the S-polynomial of f_1 and f_3:

$$S(f_1, f_2) = \frac{2y\lambda}{\lambda} f_1 - \frac{2x\lambda}{\lambda} f_2 = 6x + 2y$$

Division of $S(f_1, f_3)$ by $G = (f_1, f_2, f_3)$ doesn't change the polynomial, so

$$f_4 := \mathrm{nf}_G(S(f_1, f_2)) = 6x + 2y.$$

Now f_4 is added to G. Continue with

$$S(f_1, f_3) = x - 2y^2\lambda + 2\lambda.$$

This time the polynomial can be divided which results in

$$f_5 := \mathrm{nf}_G(S(f_1, f_3)) = -\frac{10}{3}y + 2\lambda$$

After inserting f_5 in G, the leading term of f_5 can be eliminated again, this time combining it with f_2:

$$f_6 := \mathrm{nf}_G(S(f_2, f_5)) = -4\lambda^2 + 10$$

A final check yields that $G = \{f_1, \ldots, f_6\}$ is a Gröbner basis of I with respect to the lexicographic ordering.

A closer look at these polynomials yield a nice surprise. f_6 depends only on λ, such that its solutions can be computed with an ordinary solver for one-variable polynomials. Then one obtains the values of y and x by substituting into f_5 and f_4 and crosschecking whether the other polynomials also vanish. The generalization of this phenomenon is known as the elimination theorem.

Theorem 12 (Elimination Theorem). *Let I be an ideal in $\mathbb{K}[x_1, \ldots, x_n]$ and G be its Gröbner basis with respect to the lexicographic monomial ordering with $x_1 \succ \ldots \succ x_n$. Then*

$$G \cap \mathbb{K}[x_k, \ldots, x_n]$$

is the Gröbner basis of the ideal $I \cap \mathbb{K}[x_k, \ldots, x_n]$ (with respect to the to $\mathbb{K}[x_k, \ldots, x_n]$ restricted monomial ordering).

Proof. See [12] (Chapter 3, Theorem 1.2). □

Even better suited for the calculation of the variety is given by the rational univariate representation [14] or the geometric resolution [15], although technical limitations apply in both cases.

Gröbner bases are by no means unique, even for a fixed monomial ordering. Given a Gröbner basis G, you can add polynomials which belong to the ideal I and again obtain a Gröbner basis. You may even replace a polynomial $g \in G$ by $f + g$ for some $f \in I$ as long as $f + g$ and g have the same leading monomial. These two properties can be used to calculate a normal form of Gröbner bases.

Theorem 13. *Every ideal I in $\mathbb{K}[x_1, \ldots, x_n]$ has a unique* reduced *Gröbner basis G, which is characterized by*

1. *$I = \langle G \rangle$.*

2. *$\mathrm{LC}(g) = 1$ for all $g \in G$.*

3. *For all $g \in G$, no term of g lies in $\langle \mathrm{LM}(G \setminus \{g\}) \rangle$.*

Proof. See [12] (Chapter 2, Theorem 7.6). □

Luckily, the Buchberger algorithm or more advanced algorithms are implemented in many computer algebra packages, for example in Singular and Maple. For the computations in this thesis, Singular [16] was used.

Example 14. As second example for the usefulness of Gröbner bases consider example 2 again. Here the graded reverse lexicographic monomial ordering with $u \succ x_5 \succ x_6 \succ x_3 \succ x_2 \succ x_1 \succ x_4$ will be used. Usually, this yields to much smaller Gröbner bases (especially lower degree) than the lexicographic ordering. Rigorous differerences regarding the degree of occurring polynomials will be established in the end of the chapter.

A Gröbner basis of $I = \langle f_1, \dots, f_6 \rangle$ is $G = \{g_1, \dots, g_8\}$ with

$$\begin{aligned}
g_1 &:= 2x_6 - x_2 \\
g_2 &:= u - 2x_5 + x_1 \\
g_3 &:= 2x_5x_1 - x_3x_1 - x_1^2 - x_2x_4 \\
g_4 &:= x_2^2 - 2x_3x_1 + x_1^2 - 2x_2x_4 \\
g_5 &:= 2x_5x_3 - 2x_3x_1 - x_2x_4 \\
g_6 &:= 4x_5^2 - 4x_3x_1 - x_1^2 - 4x_2x_4 \\
g_7 &:= x_3x_1^2 - 2x_5x_2x_4 + 2x_2x_1x4 \\
g_8 &:= x_3^2x_1 - 2x_5x_2x_4 + x_3x_2x_4 + x_2x_1x_4
\end{aligned}$$

The hypothesis to prove was formulated as

$$h = x_3x_6 - x_4x_5.$$

So one first can check whether $h \in I$. This would imply that $h = 0$ for all configurations that fulfill the conditions $f_1 = 0, \dots, f_6 = 0$. But

$$\mathrm{nf}(h) = \frac{1}{2}x_3x_2 - x_5x_4.$$

Theorem 9 implies that $h \notin I$. However it turns out that

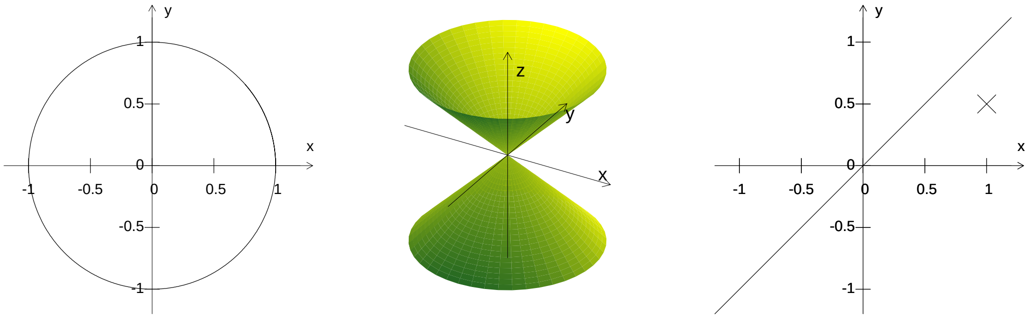
$$\mathrm{nf}(h^3) = 0.$$

This means $h^3 = 0$ and therefore also $h = 0$ for all configurations in $\mathbf{V}(f_1, \dots, f_6)$. This proves the claim that the cirumcirle center M lies on the median line AD.

In general the radical ideal membership (i.e. is $h \in \sqrt{I}$?) can be solved by the so-called Rabinovic trick (consult [12], Chapter 4, Proposition 2.8).

2.3 Ideal Dimension

Example 15. In figure 2.1a you see a circle which is the set $V_1 := \mathbf{V}(x^2 + y^2 - 1)$. This would clearly be called one-dimensional, whether as a subset of $\mathbb{R}^2$ as it is drawed in the figure or as subset of a higher space. One would also expect, that translations, isometric mappings and many other functions preserve the dimension of a variety.



(a) Circle (b) Cone (c) Union of line and point

Figure 2.1: Examples intuitively clear variety dimensions.

Figure 2.1b is the cone defined by $V_2 := \mathbf{V}(x^2 + y^2 - z^2)$ and intuitively two-dimensional. As in the first example, the dimension equals the number of variables minus the number of equations. But that's not necessarily true for varieties generated by several equations.

This is illustrated by figure 2.1c, which is $V_3 := \mathbf{V}((x-y)(x-1), (x-y)(y-0.5))$. This variety is the union of the line $y = x$ and the point $(1, 0.5)$. The line has clearly dimension 1, the point dimension 0. Therefore one would define the dimension of V_3 as the maximum of both, namely 1.

For many varieties one can define a dimension quite intuitively when looking at them. But it's hard to draw higher dimensional varieties and furthermore a rigorous definition is desirable when one wishes to analyze related properties and maybe even compute it automatically. Mathematicians have found many equivalent ways to do so. The most intuitive notion is probably this.

For a variety V, let its *dimension* $\dim(V)$ be the largest dimension of a subspace $H \subset \mathbb{K}^n$ such that the projection of V onto H is contained in no proper subvariety of H.

Now turning to ideals, one defines the dimension $\dim(I)$ of an ideal I to be the dimension of the corresponding variety $\dim(\mathbf{V}(I))$.

But this definition is not very useful for proofs and algorithms. Therefore algebraic equivalences were studied. The following notation will be used: Let F be a set of polynomials. Then

$$F_{\leq s} := \{f \in F : \deg(f) \leq s\}.$$

Theorem 16. *Let $\mathbb{K}$ be algebraically closed and I be an ideal in $\mathbb{K}[x_1, \ldots, x_n]$. Then $\dim(I)$ can be calculated as follows.*

1. $\dim(I) = \deg(HP_I)$ *where HP_I is the Hilbert polynomial of I, defined as*

$$HP_I(s) = \dim_{\mathbb{K}}(\mathbb{K}[x_1, \ldots, x_n]_{\leq s}/I_{\leq s}) \text{ for sufficiently large } s.$$

2. $\dim(I)$ *equals the cardinality of the biggest set $S \subset \{x_1, \ldots, x_n\}$ such that*

$$I \cap \mathbb{K}[S] = \{0\}.$$

Proof. See [12] (Chapter 9, Proposition 3.6, Definition 3.7, Theorem 3.8, Corollary 5.4 and Proposition 5.5). □

Theorem 17. *Let $\mathbb{K}$ be algebraically closed and I be an ideal in $\mathbb{K}[x_1, \ldots, x_n]$. If $\prec$ is a graded monomial ordering, then additionally*

3. $\dim(I) = \deg(HP_{\langle \mathrm{LM}(I)\rangle})$.

4. $\dim(I)$ *is the maximum dimension of a subspace H of $\mathbf{V}(\langle \mathrm{LM}(I)\rangle)$ of the form*

$$H = \{(a_1, \ldots, a_n) \in \mathbb{K}^n : a_i = 0 \; \forall i \in S\} \text{ for some } S \subset \{1, \ldots, n\}.$$

Proof. See [12] (Chapter 9, Theorem 3.8 and Proposition 5.5). □

These definitions of the dimension of a variety shall be illustrated in the following example. There will be no rigorous proof but explanations of the diverse notions of the dimension.

Example 18. This example studies the variety of figure 2.1c. This variety is corresponding to the ideal $I = \langle (x-y)(x-1), (x-y)(y-0.5)\rangle$. In order to check the various formulas of the dimension, a lexicographic monomial ordering (for 2.) and a graded monomial ordering (for 3. and 4.) will be needed. The Gröbner basis with respect to $\prec_{\text{lex}}$ respectively $\prec_{\text{grevlex}}$ (with $x \succ y$ for both) are

$$G_{\text{lex}} := \{2xy - x - 2y^2 + y, x^2 - xy - x + y\}$$

$$G_{\text{grevlex}} := \{2xy - 2y^2 - x + y, x^2 - 3xy + 2y^2\}$$

Please note, that the example must be considered over the algebraically closure of $\mathbb{R}$, which is $\mathbb{C}$. Thus the variety under consideration is

$$\mathbf{V}(I) = \{(a, a) : a \in \mathbb{C}\} \cup \{(1, 0.5)\}.$$

The only subspace of $\mathbb{C}^2$ of dimension 2 is $\mathbb{C}^2$. But since $\mathbf{V}(I)$ itself is a proper subvariety of $\mathbb{C}^2$, the dimension of the variety is not 2. However the projection of $V(I)$ into the one-dimensional subspace $H = \{(a, 0) : a \in \mathbb{C}\}$ is the whole subspace H and therefore no proper subset. Thus the dimension of I is 1. This will be checked with the various formulas given in theorem 16 and 17.

1. In order to find the Hilbert polynomial, one has to determine the dimensions of $\dim_{\mathbb{C}}(\mathbb{C}[x, y]_{\leq s}/I_{\leq s})$. One basis for $\mathbb{C}[x, y]_{\leq s}$ is given by the monomials of degree at most s. Thus the dimension of this linear space is $\binom{s+2}{2}$. The basis for $I_{\leq s}$ is slightly more complicated. According to the division algorithm, the two monomials of G_{grevlex} form a basis of $I_{\leq 2}$. For $s > 2$, the dimension of $I_{\leq s}$ is the dimension of $I_{\leq s-1}$ plus the dimension of the space generated by the parts of the generators with degree 2 ($2xy - 2y^2$ and $x^2 - 3xy + 2y^2$) multiplied with monomials of degree $s - 2$. A basis for this linear space is given by

$$\begin{aligned} &m(x^2 - xy) \text{ for } m \text{ monomial}, \deg(m) = s - 2 \\ &n(xy - y^2) \text{ for } n \text{ monomial}, \deg(n) = 2, x \nmid n. \end{aligned}$$

The condition $x \nmid n$ is necessary since only so the system is linearly independent. Otherwise one would obtain the same polynomial for $m = \frac{y}{x}n$. So the dimension of $I_{\leq s}$ for $s \geq 2$ is

$$\dim_{\mathbb{C}}(I_{\leq s}) = 2 + \sum_{i=3}^{s} ((s - 1) + 1) = 2 + \frac{1}{2}s(s + 1) - 3 = \frac{1}{2}(s^2 + s - 2).$$

This yields the Hilbert polynomial

$$HP_I(s) = \dim_{\mathbb{C}}(\mathbb{C}[x, y]_{\leq s}) - \dim_{\mathbb{C}}(I_{\leq s}) = \binom{s+2}{2} - \frac{1}{2}(s^2 + s - 2) = s + 2,$$

which has degree 1. So the ideal dimension $\dim(I) = 1$.

2. Obviously, $I \cap \mathbb{C}[x, y] \neq \{0\}$. So the dimension cannot be 2. On the other hand, by the elimination theorem 12, $I \cap \mathbb{C}[y] = \{0\}$ since $G_{\text{lex}} \cap \mathbb{C}[y] = \emptyset$. Thus the dimension of I must be 1.

3. The leading monomials of I with respect to $\prec_{\text{grevlex}}$ are the multiples of xy and x^2. Thus $\text{LM}(I)_{\leq 1}$ is empty. There are $\binom{s+2}{2}$ monomials in 2 variables of degree at most s. So, for $s \geq 2$, there are $\binom{s}{2}$ multiples of x^2 of degree at most s. Additionally there are all monomials of the form xy^α with $\alpha = 1, \dots, s-1$. So for $s \geq 2$

$$\dim_{\mathbb{C}}(\text{LM}(I)_{\leq s}) = \binom{s}{2} + s - 1 = \frac{1}{2}(s^2 + s - 2)$$

$$HP_{\langle \text{LM}(I) \rangle}(s) = \dim_{\mathbb{C}}(\mathbb{C}[x, y]_{\leq s}) - \dim_{\mathbb{C}}(\text{LM}(I)_{\leq s}) = \binom{s+2}{2} - \frac{1}{2}(s^2 + s - 2) = s + 2$$

Finally, $\dim(I) = \deg(HP_{\langle \text{LM}(I) \rangle}(s)) = 1$.

4. $\mathbf{V}(\text{LM}(I)) = \mathbf{V}(xy, x^2) = \{(0, a) : a \in \mathbb{C}\}$. In this case, $\mathbf{V}(I)$ is a subspace of $\mathbb{C}^2$ with dimension 1. Therefore also $\dim(I) = 1$.

The special focus of this thesis is on zero-dimensional ideals. Hence it is suggesting to study in which cases an ideal has dimension 0. Of course one could use the definitions of theorems 16 and 17 directly. But it turns out, that one can this special case allows even more characterizations.

Theorem 19. *Let $\mathbb{K}$ be algebraically closed, I an ideal in $\mathbb{K}[x_1, \dots, x_n]$ and $\prec$ an admissible monomial ordering. Then* $\dim(I) = 0$ *if and only if one of the following equivalent conditions holds:*

1. $\mathbf{V}(I)$ *is a finite set.*

2. $x_i^{m_i} \in \text{LM}(I)$ *for all* $i = 1, \dots, n$ *and some* $m_i \geq 0$*. Thus, if G is a Gröbner basis for I, it contains elements g_i with* $\text{LM}(I) = x_i^{m_i}$*.*

3. $\mathbb{K}[x_1, \dots, x_n]/I$ *is finite-dimensional.*

Proof. See [12] (Chapter 5, Theorem 3.6). Note that the Hilbert polynomial has degree 0 if and only if $\mathbb{K}[x_1, \dots, x_n]/I$ is finite-dimensional. □

Example 20. The ideal I considered in example 3 is zero-dimensional. This shall be checked using the conditions provided in 19. For the sake of simplicity, the following, smaller Gröbner basis (but also with respect to the lexicographic monomial ordering for $x \succ y \succ \lambda$)

$$G := \{2\lambda^2 - 5, 5y - 3\lambda, 3x + y\}$$

will be used instead of the Gröbner basis calculated in example 11.

1. The first polynomial in G has the roots $\lambda_1 = \sqrt{\frac{5}{2}}$ and $\lambda_2 = -\sqrt{\frac{5}{2}}$. Plugging these into the other polynomials immediately gives
$$\mathbf{V}(I) = \left\{ \left(-\frac{1}{\sqrt{10}}, \frac{3}{\sqrt{10}}, \sqrt{\frac{5}{2}} \right), \left(\frac{1}{\sqrt{10}}, -\frac{3}{\sqrt{10}}, -\sqrt{\frac{5}{2}} \right) \right\},$$
which is obviously finite.

2. The leading monomials of the Gröbner basis G are
$$\begin{aligned} \mathrm{LM}(2\lambda^2 - 5) &= \lambda^2 \\ \mathrm{LM}(5y - 3\lambda) &= y \\ \mathrm{LM}(3x + y) &= x \end{aligned}$$

3. A basis of $\mathbb{K}[x_1, \ldots, x_n]/I$ is given by the factor classes of the monomials that are not reducible, i.e. the monomials not divisible by the leading monomials of a Gröbner basis. In this case these are $\{1, \lambda\}$ such that $\dim_{\mathbb{C}}(\mathbb{K}[x_1, \ldots, x_n]/I) = 2 < \infty$.

Finally, one can give similar definitions for homogeneous ideals and projective varieties and connect them to the affine case. In the following $F_{=d}$ denotes all homogeneous elements of degree d contained in the set F and the zero element, i.e.

$$S_{=d} := \{f \in S : \deg(f) = d \text{ or } f = 0\}$$

Then the *(projective) dimension* $\dim_{\mathbb{P}}(J)$ can be defined as

$$\dim_{\mathbb{P}}(J) = \deg(HP_J^{\mathbb{P}})$$

where $HP_J^{\mathbb{P}}$ is the projective Hilbert polynomial of J

$$HP_J^{\mathbb{P}}(s) = \dim_{\mathbb{K}}(\mathbb{K}[x_0, \ldots, x_n]_{=s}/J_{=s}) \text{ for sufficiently large s.}$$

Theorem 21. *Let* $\mathbb{K}$ *be algebraically closed,* J *a homogeneous ideal in* $\mathbb{K}[x_0, \ldots, x_n]$*. If* J *is the homogenization of* I*, i.e.* $J = \left\langle {}^h f : f \in I \right\rangle$*, then* $\dim(I) = \dim_{\mathbb{P}}(J)$*.*

Proof. See [12] (Chapter 9, Definition 3.10, Theorem 3.12, Corollary 5.4 and Proposition 5.5). □

Note that speaking of homogeneous ideals, usually the projective dimension will be meant unless something else is stated explicitely.

Chapter 3

Degree Bounds

3.1 General

As powerful as Gröbner bases are, their computation is usually very expensive. In [5], Ernst Mayr and Albert Meyer were able to show that all algorithms which solve the ideal membership problem for arbitrary bases require space exponential in the size of the input in the worst case. Once a Gröbner basis is computed, the division algorithm easily solves the ideal membership problem. Therefore the Gröbner basis computation must be the hard part.

But why is it sufficient to worry about the degrees of the polynomials? Of course these contribute to the size, but so do the coefficients and the number of Gröbner basis polynomials. Klaus Kühnle and Ernst Mayr presented in [6] an algorithm that computes Gröbner bases using only exponential space. Their argument heavily relies on the upper degree bound by Thomas Dubé:

Theorem 22 (Dubé, 1990)**.** *Let $I = \langle f_1, \ldots, f_s \rangle$ in $\mathbb{K}[x_1, \ldots, x_n]$ with maximal degree of the generators $d = \max\{\deg(f_1), \ldots, \deg(f_s)\}$. Then for any admissible monomial ordering, there is a Gröbner basis with polynomials that have degrees bounded by*

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

Proof. See [17] (Corollary 8.3). □

With the same reasoning as in [6] one could derive a more efficient algorithm if one could prove a better upper degree bound. However, in general it is not possible to improve the degree bound qualitatively. This was shown by Michael Möller and Fernando Mora:

Theorem 23 (Möller, Mora, 1984, Mayr, Meyer, 1982)**.** *There is a family of ideals K_n of polynomials in $14(n+1)$ variables with degrees bounded by $d+2$ such that, with respect to any degree compatible monomial ordering, every Gröbner basis of J_n contains a polynomial of degree at least*

$$\frac{d^{2^n}}{2}+4.$$

Proof. See [18] (Proposition 3.4) and note that for degree compatible orderings every Gröbner basis is also a H-basis. The construction relies on an example given by Ernst Mayr and Albert Meyer in [5]. □

Therefore the best one can do is to search for certain classes of ideals that allow better upper degree bounds. It will be shown that Gröbner bases for zero-dimensional ideals behave much better. Herefore different monomial orderings will be considered and matching upper and lower degree bounds will be given.

3.2 Zero-dimensional Ideals, Lexicographic Ordering

Usually one desires to have good upper degree bounds. Those limit the complexity of the studied object, in this case Gröbner bases. As mentioned in section 3.1, these can determine the effort needed to compute Gröbner bases even explicitely.

Additionally, lower bounds can be very useful as well. They can tell, whether it is possible to further improve existing upper bounds. As soon as the upper and lower bounds match, these are optimal for this class of ideals. Then, if even better upper bounds are necessary, the only remaining possibility is to restrict the class of ideals further.

As in section 3.1, bounds of the following type will be of interest: Given arbitrary polynomials $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$ of degrees $d_1, \ldots, d_s$, how can the degrees of the polynomials in a Gröbner basis for the ideal $I = \langle f_1, \ldots, f_s \rangle$ be bounded, in terms of the number of variables n and the degrees of the generators $d_1, \ldots, d_s$? From now on throughout the rest of the thesis, $d_1 \leq \ldots \leq d_s$ will be assumed.

Usually bounds are already considered to be matching if their growth is similar, e.g. exponential or polynomial of the same degree. For zero-dimensional ideals, however, the situation is especially beautiful because exactly matching upper and lower bounds are known.

This section will provide and prove lower and upper bounds for the lexicographic monomial ordering. Additionally the usual behaviour of randomly chosen polynomials will be studied, a notion that will have to be formalized first. The graded reverse lexicographic ordering will be treated in the next section.

3.2.1 Lower Bound

First consider an example for which the degrees in the Gröbner basis are large compared to the generators.

Example 24. This example is well-known. In a slightly different form it was stated in [18] (Proposition 2.2). For an arbitrary $n \geq 1$, let $K_n \subset \mathbb{K}[x_1, \ldots, x_n]$ be the ideal generated by

$$\begin{aligned} f_1 &:= x_1 + x_2^{d_1} \\ f_2 &:= x_2 + x_3^{d_2} \\ &\vdots \\ f_{n-1} &:= x_{n-1} + x_n^{d_{n-1}} \\ f_n &:= x_1^{d_n} \end{aligned}$$

So $\deg(f_k) = d_k$. Consider the lexicographic monomial ordering with $x_1 \succ \ldots \succ x_n$. Now one can form the S-polynomial of f_1 and f_n

$$S(f_1, f_n) = x_1^{d_n-1} x_2^{d_1}$$

This polynomial is reducible with respect to f_1:

$$S(f_1, f_n) - \left(x_1^{d_n-2} x_2^{d_1} - x_1^{d_n-3} x_2^{2d_1} + \ldots \pm x_2^{(d_n-1)d_1}\right) f_1 = \pm x_2^{d_1 d_n}$$

Similarily, reducing the result with respect to f_2 gives $\pm x_3^{d_1 d_2 d_n}$. Inductively, one obtains a new polynomial (the sign can be chosen arbitrarily)

$$g := x_n^{d_1 \cdots d_n} \in K_n.$$

The system of polynomials

$$\begin{aligned} f_1 &= x_1 + x_2^{d_1} \\ f_2 &= x_2 + x_3^{d_2} \\ &\vdots \\ f_{n-1} &= x_{n-1} + x_n^{d_{n-1}} \\ g &= x_n^{d_1 \cdots d_n} \end{aligned}$$

still generates the same ideal and is a Gröbner basis. This can be easily checked with the following criterion.

Proposition 25. *Let I be an ideal in $\mathbb{K}[x_1, \ldots, x_n]$ and G a basis for I. If*

$$\gcd(\mathrm{LM}(g), \mathrm{LM}(h)) = 1 \text{ for all } g, h \in G, g \neq h$$

then G is a Gröbner basis for I.

Proof. See [12] (Chapter 2, Theorem 9.3 and Proposition 9.4). □

On the other hand, by the elimination theorem 12, $G \cap \mathbb{K}[x_n]$ is a Gröbner basis of $I \cap \mathbb{K}[x_n]$. Since this is also true for every other Gröbner basis of I, every Gröbner basis of I must either contain the polynomial g or several multiples of g whose greatest common divisor is g.

Finally, it's easy to see that the conditions of theorem 19 are satisfied (look at the condition for Gröbner bases in 2.) such that $\dim(K_n) = 0$.

The example can be summarized as follows.

Theorem 26 (Folklore). *There is a family of ideals $K_n \subset \mathbb{K}[x_1, \ldots, x_n]$ generated by polynomials $f_1, \ldots, f_n$ of degrees $d_1, \ldots, d_n$ such that every lexicographic Gröbner basis for K_n contains a polynomial of degree $d_1 \cdots d_n$.*

If all polynomials $f_1, \ldots, f_n$ have the same degree d, the maximal degree in the Gröbner basis of K_n will be d^n and therefore exponential in the number of variables. Here the question arises, whether this is exceptional or the "usual case" and whether even worse growth can occur. The rest of the section shall answer both questions.

3.2.2 Upper Bound

Intuitively the lexicographic monomial ordering allows really large degrees in the Gröbner basis since there are monomials with high degree that are very small in this ordering. In fact, the upper bound that will be provided holds not only for the lexicographic monomial ordering but for any admissible monomial ordering. Since it matches the lower bound given by theorem 26, one can say that the lexicographic monomial ordering constitutes the worst case. For the proof the well-known Bézout theorem is needed.

Theorem 27 (Bézout's Theorem)**.** *Let $f_1, \ldots, f_s$ be polynomials of degrees $d_1 < \ldots < d_s$ in $\mathbb{K}[x_1, \ldots, x_n]$ and $I = \langle f_1, \ldots, f_s \rangle$. If I is zero-dimensional then*

$$\dim_{\mathbb{K}}(\mathbb{K}[x_1, \ldots, x_n]/I) \leq d_1 \cdots d_n.$$

The bound is exact for $s = n$ if and only if the system

$$\begin{aligned} \mathrm{in}(f_1) &= 0 \\ &\vdots \\ \mathrm{in}(f_n) &= 0 \end{aligned}$$

has no solutions. Here $\mathrm{in}(f_i)$ *is the sum of all terms of f_i of degree d_i, which is sometimes called* initial *of f_i.*

Proof. A well-known version of Bézout's theorem states that for $n = s$ the number of projective solutions (counting multiplicities) of a system of homogeneous polynomials over an algebraically closed field is exactly the product of the degrees of the polynomials if it is finite (see [19], Chapter IV, §2, Example 1).

Note that for $s < n$ either $\dim(I) > 0$ or $\mathbf{V}(I) = \emptyset$, so there is nothing to prove. For $s > n$ and $\dim(I) = 0$, one can pick n polynomials in I of degrees $d_1 \geq \ldots \geq d_n$ that induce a zero-dimensional variety (analogous to [20], Proof of Lemma to Proposition 5.4.1). The number of solutions of $f_1, \ldots, f_s$ is, of course, at most the number of solutions of these n polynomials.

By dehomogenizing, i.e. setting one of the variables to 1 (usually x_0), the solutions at infinity disappear. Those solutions have a zero in the coordinate that is dehomogenized.

In other words they are the common solutions of the initials

$$\begin{aligned} \operatorname{in}(f_1) &= 0 \\ &\vdots \\ \operatorname{in}(f_s) &= 0 \end{aligned}$$

So the number of affine solutions may be less but not more than the number of projective solutions. Finally, the number of solutions counting multiplicity equals the dimension of the factor ring $\mathbb{K}[x_1, \ldots, x_n]/I$ (see [21], Chapter 4, Corollary 2.5). □

Example 28. Consider the affine system

$$\begin{aligned} f_1 &= x^2 + y \\ f_2 &= y^2 + x^3 \end{aligned}$$

The system of initials is

$$\begin{aligned} \operatorname{in}(f_1) &= x^2 = 0 \\ \operatorname{in}(f_2) &= x^3 = 0. \end{aligned}$$

This has the projective solution $(x : y) = (0 : 1)$ with multiplicity 2.

The affine solutions of $f_1 = f_2 = 0$ are $(x, y) = (0, 0)$ with multiplicity 3 and $(-1, -1)$ with multiplicity 1. Here the multiplicities can be explained by solving f_1 for y and substituting in f_2.

So the number of affine solutions counting multiplicities is 4, which is smaller than $\deg(f_1)\deg(f_2) = 6$. However there are 2 solutions at infinity. Counting those, the number of solutions equals the product of the degrees.

A strategy used to prove an upper degree bound for Gröbner bases is to prove an upper degree bound for normal forms. Then all polynomials in the reduced Gröbner basis have degrees bounded by the degrees of the normal forms. This approach was used by Daniel Lazard in [7] (Theorem 2). It will be verified in the following proposition and reused in the next section.

Proposition 29. *Let I be an ideal in $\mathbb{K}[x_1, \ldots, x_n]$. For a fixed monomial ordering, assume that all normal forms have degrees bounded by d. Then the reduced Gröbner basis G for I contains only polynomials of degrees bounded by $d + 1$.*

Proof. By assumption, all monomials x^α of degree at least $d+1$ have normal forms of lower degree. Since $x^\alpha \succeq \mathrm{LM}(\mathrm{nf}(x^\alpha))$ by the division algorithm, one has $x^\alpha \in \mathrm{LM}(I)$.

Let G be the reduced Gröbner basis for I. By theorem 13, all monomials of polynomials in G except the leading monomials are not contained in $\mathrm{LM}(I)$ and therefore their degrees are bounded by d.

Furthermore no leading monomial of a polynomial in G is divisible by another monomial in $\mathrm{LM}(G)$ (which generates $\mathrm{LM}(I)$) such that the degrees of the leading monomials are bounded by $d+1$. □

Theorem 30 (Folklore)**.** *Let $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be an zero-dimensional ideal generated by polynomials $f_1, \ldots, f_s$ of degree $d_1, \ldots, d_s$. Then there is a lexicographic Gröbner basis for I which contains only polynomials of degrees bounded by $d_1 \cdots d_n$.*

Proof. Consider the ring of normal forms $A := \{\mathrm{nf}(f) : f \in \mathbb{K}[x_1, \ldots, x_n]\}$ as defined in theorem 9. By Bézout's theorem (27),

$$\dim_{\mathbb{K}}(A) = \dim_{\mathbb{K}}(\mathbb{K}[x_1, \ldots, x_n]/I) \leq d_1 \cdots d_n.$$

Let x^α be any monomial in A. Then neither x^α nor any of its divisors $x^\beta \mid x^\alpha$ are contained in $\langle \mathrm{LM}(I) \rangle$ and thus $x^\beta \in A$. Since every monomial of degree $d_1 \cdots d_n$ has at least $d_1 \cdots d_n + 1$ divisors (counting x^α) and all monomials are linearly independent, $\deg(x^\alpha) < d_1 \cdots d_n$. Finally proposition 29 yields the desired upper degree bound. □

3.2.3 Generic Degree

For the further studies of the lexicographic monomial ordering, a rigorous definition of the "usual case" is needed. This notion is supposed to capture what happens almost surely for randomly chosen polynomials. One of the problems is the definition of random. Since the degrees of polynomials are fixed, only the coefficients have to be chosen randomly, preferedly uniformly distributed. But the field $\mathbb{K}$ is usually infinite. This challenges the quality of all kinds of sample methods and disallows using this approach for a formal definition.

Since the objects of studies are polynomial equations, it turned out to be natural to use themselves for this definition. Consider polynomials $f_1, \ldots, f_s$ whose coefficients are coefficients, i.e.

$$f_i := \sum_{\substack{\alpha \in \mathbb{Z}^n_{\geq 0} \\ |\alpha| \leq d_i}} u_{i,\alpha} x^\alpha \in \mathcal{R}[x_1, \ldots, x_n]$$

where

$$\mathcal{R} := \mathbb{Z}[u_{i,\alpha} : i = 1, \ldots, s, \alpha \in \mathbb{Z}^n_{\geq 0}, |\alpha| \leq d_i]$$

is the ring of the coefficients. The ideal generated by those polynomials will be called $\mathcal{I} = \langle f_1, \ldots, f_s \rangle$. Choosing specific polynomials of degrees $d_1, \ldots, d_s$ with coefficients in $\mathbb{K}$ is equivalent to choosing a homomorphism from $\mathcal{R}[x_1, \ldots, x_n]$ to $\mathbb{K}[x_1, \ldots, x_n]$ that preserves $x_1, \ldots, x_n$. These homomorphisms are called *specializations.*

A property is said to hold *generically* respectively to be *generic* if for any tuple of degrees $d_1, \ldots, d_s$ there is a polynomial $0 \neq h \in \mathcal{R}$ that fulfills:

For all specializations $\psi : \mathcal{R}[x_1, \ldots, x_n] \longrightarrow \mathbb{K}[x_1, \ldots, x_n]$, the property holds for $\psi(f_1), \ldots, \psi(f_s)$ whenever $\psi(h) \neq 0$.

This means, that only the solutions h are allowed to be exceptions. Since h is not the zero-polynomial, h most likely won't vanish on a randomly chosen point.

Example 31 ([21] Chapter 3, Exercise 5.1)**.** A polynomial in one variable of degree 2 has generically two distinct solutions. To see this let

$$f := ax^2 + bx + c$$

such a polynomial and ψ be a specialization. It is well-known, that $\psi(f)$ has two solutions over $\mathbb{C}$ if $a \neq 0$. They are distinct if the discriminant $b^2 - 4ac$ does not vanish. Together, $\psi(f)$ has two distinct solutions if

$$h := a(b^2 - 4ac) \neq 0.$$

Instead of only giving degree bounds for the generic case, it is possible to describe the form of the lexicographic Gröbner basis in much greater detail (as usually, $x_1 \succ \ldots \succ x_n$). This is accomplished by the so-called shape lemma. For the proof multivariate resultants are needed. This only applies to the situation $s = n$.

Theorem 32. *Let $\mathbb{K}$ be an algebraically closed field. For fixed degrees $d_1, \ldots, d_n$ consider homogeneous polynomials*

$$F_i = \sum_{\substack{\alpha \in \mathbb{Z}^n_{\geq 0} \\ |\alpha| = d_i}} u_{i,\alpha} x^\alpha \in \mathcal{S}[x_0, \ldots, x_n]$$

for $i = 0, \ldots, n$ and

$$\mathcal{S} := \mathbb{Z}[u_{i,\alpha} : i = 0, \ldots, n, \alpha \in \mathbb{Z}^n_{\geq 0}, |\alpha| = d_i].$$

Then there is a polynomial $\mathrm{Res}(F_0, \ldots, F_n) \in \mathcal{S}$*, called resultant, such that for all specializations $\psi : \mathcal{S}[x_0, \ldots, x_n] \to \mathbb{K}[x_0, \ldots, x_n]$ the following holds:*

$$\psi(\mathrm{Res}(F_0, \ldots, F_n)) = 0 \iff \psi(F_0)(p) = \ldots = \psi(F_n)(p) = 0 \textit{ for some } 0 \neq p \in \mathbb{C}^n$$

Proof. See [22] (Chapter 3.1). □

For linear homogeneous polynomials, i.e. $d_0 = \ldots = d_n = 1$, this polynomial is the determinant of the coefficient matrix of the linear system. In the case of two homogeneous polynomials in two variables this resultant equals the well-known Sylverster resultant.

Theorem 33 (Shape Lemma)**.** *Let $\mathbb{K}$ be an algebraically closed field and for $i = 1, \ldots, n$ define*

$$f_i := \sum_{\substack{\alpha \in \mathbb{Z}^n_{\geq 0} \\ |\alpha| \leq d_i}} u_{i,\alpha} x^\alpha \in \mathcal{R}[x_1, \ldots, x_n]$$

where

$$\mathcal{R} := \mathbb{Z}[u_{i,\alpha} : i = 1, \ldots, n, \alpha \in \mathbb{Z}^n_{\geq 0}, |\alpha| \leq d_i].$$

Let $\psi : \mathcal{R}[x_1, \ldots, x_n] \longrightarrow \mathbb{K}[x_1, \ldots, x_n]$ denote a specialization and assume that $I = \langle \psi(f_1), \ldots, \psi(f_n) \rangle$ is an zero-dimensional ideal in $\mathbb{K}[x_1, \ldots, x_n]$. Then the reduced Gröbner basis of I generically consists of n polynomials of the form

$$\begin{aligned} g_1 &= x_1 + \widetilde{g}_1(x_n) \\ &\vdots \\ g_{n-1} &= x_{n-1} + \widetilde{g}_{n-1}(x_n) \\ g_n &= x_n^{d_1 \cdots d_n} + \widetilde{g}_n(x_n) \end{aligned}$$

where $\widetilde{g}_1, \ldots, \widetilde{g}_n$ are polynomials in x_n of degree less than $d_1 \cdots d_n$.

Proof. It is to show that there is a polynomial $h \in \mathcal{R}$ such that whenever $\psi(h) \neq 0$, the Gröbner basis of I has the stated form.

Bézout's Theorem 27 and theorem 32 imply that

$$m := \dim(\mathbb{K}[x_1, \dots, x_n]/I) = d_1 \cdots d_n$$

whenever

$$\psi(\mathrm{Res}(\mathrm{in}(f_1), \dots, \mathrm{in}(f_n))) \neq 0.$$

Following the hints of [21], Chapter 3, Exercise 5.6, the following fact from multiplicity theory will be used. Since the projective extension theorem shall be used, all notions have to be formulated for homogeneous polynomials.

If the affine tangent space to an affine variety V in a point p is of the same dimension as the variety, then p is a nonsingular point, i.e. the multiplicity of p is 1 ([19], Chapter 1.4, Theorem 3). This will be needed in the following context. The variety $V \subset \mathbb{K}[x_0, \dots, x_n]$ is generated by homogeneous polynomials $F_1, \dots, F_n \in \mathbb{K}[x_0, \dots, x_n]$ with only finitely many common roots in $\mathbb{P}^n$, i.e. $\dim_{\mathbb{P}}(V) = 0$ and the affine dimension $\dim(V) = 1$. So in order to show that some $p \in V$ has multiplicity 1, one has to show that the affine tangent space in p has dimension 1. The tangent space T_p at p is defined as the set of lines through p that are tangent to V. This can be written as (see [19], beginning of Chapter 1.3)

$$T_p = \left\{ q \in \mathbb{K}^{n+1} : \sum_{k=0}^{n} \frac{\partial F_i}{\partial x_k}(p)(q_k - p_k) = 0 \text{ for } i = 1, \dots, n \right\}.$$

Obviously, this vector space has dimension 1 if and only if

$$\nabla F_i(p) = \left(\frac{\partial F_i}{\partial x_0}(p), \dots, \frac{\partial F_i}{\partial x_n}(p) \right), \; i = 1, \dots, n$$

are linearly independent.

This will be applied to the homogenizations ${}^h f_1, \dots, {}^h f_n \in \mathcal{R}[x_1, \dots, x_n]$. Let M be the number of coefficients $u_{i,\alpha}$ of $f_1, \dots, f_n$ and define the variety

$$\begin{aligned} W := \{(c_{i,\alpha}, p, a_1, \dots, a_n) \in \mathbb{K}^M \times \mathbb{P}^n \times \mathbb{P}^{n-1} : & \psi_c({}^h f_1)(p) = \ldots = \psi_c({}^h f_n)(p) = 0 \text{ and} \\ & a_1 \nabla \psi_c({}^h f_1)(p) + \ldots + a_n \nabla \psi_c({}^h f_n)(p) = 0\}. \end{aligned}$$

Here ψ_c stands for the specialization homomorphism defined by $\psi(u_{i,\alpha}) = c_{i,\alpha}$ for $i = 1, \ldots, n$ and $\alpha \in \mathbb{Z}^n_{\geq 0}, |\alpha| \leq d_i$. W can be viewed as projective in p and $(a_1 : \ldots : a_n)$ since all defining equations are homogeneous in p and homogeneous in $(a_1 : \ldots : a_n)$.

Consider the projection $\pi : \mathbb{K}^M \times \mathbb{P}^n \times \mathbb{P}^{n-1} \longrightarrow \mathbb{K}^M$ applied to the variety W. The element $c \in \pi(W)$ represents all polynomial systems $\psi_c({}^hf_1), \ldots, \psi_c({}^hf_n)$ that have at least one common root $p \in \mathbb{P}^n$ with multiplicity more than one. To see this, note that $a_1, \ldots, a_n$ are chosen from $\mathbb{P}^{n-1}$ and therefore form a nontrivial relation of $\nabla\psi_c({}^hf_1)(p), \ldots, \nabla\psi_c({}^hf_n)(p)$. The Extension Theorem (see [12], Chapter 8, Theorem 5.6) says that the a projection from $V_1 \times V_2$ to V_1 of a variety is a variety, if the ground field is algebraically closed and V_2 is projective. One can view π as two projections

$$\mathbb{K}^M \times \mathbb{P}^n \times \mathbb{P}^{n-1} \longrightarrow \mathbb{K}^M \times \mathbb{P}^n \longrightarrow \mathbb{K}^M.$$

Thus W is a variety. So it remains to show that $W \neq \mathbb{K}^M$. It is easy to see that

$$F_i := \prod_{k=1}^{d_i} (x_i - kx_0)$$

for $i = 1, \ldots, n-1$ and

$$F_n := \prod_{k=1}^{d_n} \left(x_n - kx_0 - \sum_{l=1}^{n-1} \left((d_n + 1) \prod_{j=1}^{l} (d_j + 1) \right) x_l \right)$$

has exactly $d_1 \cdots d_n$ distinct solutions, namely

$$(1 : a_1 : \ldots : a_n) \text{ for } a_i \in \{1, \ldots, d_i\} \ (i = 1, \ldots, n-1)$$

and $a_n = \widetilde{a}_n + \sum_{l=1}^{n-1} a_i(d_n + 1) \prod_{j=1}^{l} (d_j + 1)$, $\widetilde{a}_n \in \{1, \ldots, d_n\}$. By Bézout's theorem 27 all these solutions must have multiplicity 1. This proves that $\pi(W) \neq \mathbb{K}^M$.

Similarily one can define

$$\begin{aligned} W' := \{(c_{i,\alpha}, p, q_0, \ldots, q_{n-1}) \in \mathbb{K}^M \times \mathbb{P}^n \times \mathbb{P}^{n-1} :& \psi_c({}^hf_1)(p) = \ldots = \psi_c({}^hf_n)(p) = 0 \text{ and} \\ & \psi_c({}^hf_1)(p+q) = \ldots = \psi_c({}^hf_n)(p+q) = 0\} \end{aligned}$$

for $q := (q_0 : \ldots : q_{n-1} : 0)$. Note that $\psi_c({}^hf_i)(p+q)$ is homogeneous in q since each polynomial $\psi_c({}^hf_i)(q_0, \ldots, q_{n-1}, 0)$ only contains terms without x_n coordinate of degree $\deg(\psi_c({}^hf_i))$. Then $\pi(W')$ just represents the systems which have at least two different roots with the same x_n coordinate. The same example $F_1, \ldots, F_n$ given above also shows that $\pi(W') \neq \mathbb{K}^M$ since the x_n coordinates of all $d_1 \cdots d_n$ solutions are different.

Since $\pi(W)$ and $\pi(W')$ are proper subvarieties, one can choose nonzero polynomials $h_1 \in \mathbf{I}(\pi(W))$ and $h_2 \in \mathbf{I}(\pi(W'))$. Then $h_1, h_2 \in R$. Let

$$h := \operatorname{Res}(\operatorname{in}(f_1), \ldots, \operatorname{in}(f_n)) \cdot h_1 \cdot h_2 \in \mathcal{R}.$$

Then $\psi(h) \neq 0$ implies, that $\psi(f_1), \ldots, \psi(f_n)$ have no common roots at infinity, all their roots have multiplicity 1, and the roots have different x_n coordinates. Again by Bézout's theorem, there must be exactly $d_1 \cdots d_n$ different common roots. Thus this is a generic situation.

Assume now that $\psi(h) \neq 0$ and consider the ideal $I = \langle \psi(f_1), \ldots, \psi(f_n) \rangle$ and the factor ring $\mathbb{K}[x_1, \ldots, x_n]/I$. For $d := \dim(\mathbb{K}[x_1, \ldots, x_n]/I) = d_1 \cdots d_n$, the equivalence classes $[1], [x_n], \ldots, [x_n^{d-1}]$ must be linearly independent. Otherwise there would be a polynomial

$$f := c_{d-1} x_n^{d-1} + \ldots + c_1 x_n + c_0 \in I$$

Let $p_{1,n} \ldots p_{d,n}$ be the d distinct x_n-coordinates of the points in $\mathbf{V}(I)$. Then $f(p_{i,n}) = 0$ for $i = 1, \ldots, d$. Viewed as equations for the d coefficients c_i, these d linear equations constitute a homogeneous system whose coefficient matrix is a Vandermonde matrix in the $p_{i,n}$ which are pairwisely distinct. Since this matrix is non-singular, there is only the trivial solution $f = 0$. Because $\dim(\mathbb{K}[x_1, \ldots, x_n]/I) = d$, the classes $[1], [x_n], \ldots, [x_n^{d-1}]$ form a basis of $\mathbb{K}[x_1, \ldots, x_n]/I$.

So one can express $[x_1], \ldots, [x_{n-1}], [x_n^d]$ in this basis yielding

$$\begin{aligned} &[x_1] - \widetilde{g}_1([x_n]) = 0 \\ &\vdots \\ &[x_{n-1}] - \widetilde{g}_{n-1}([x_n]) = 0 \\ &[x_n]^m - \widetilde{g}_n([x_n]) = 0. \end{aligned}$$

Replacing the equivalence classes $[x_i]$ by the variables x_i one obtains polynomials $g_1, \ldots, g_n$ of the claimed form. Since they vanish on the equivalence classes, they are contained in I. Thus $\mathbf{V}(I) \subset \mathbf{V}(g_1, \ldots, g_n)$. But g_n has exactly d roots since $\mathbb{K}$ is algebraically closed and $g_1, \ldots, g_{n-1}$ give exactly one solution $p \in \mathbf{V}(g_1, \ldots, g_n)$ for every root of g_n. Thus

$$|\mathbf{V}(g_1, \ldots, g_n)| = d = |\mathbf{V}(I)|$$

and therefore $\mathbf{V}(I) = \mathbf{V}(g_1, \ldots, g_n)$. By Hilbert's Nullstellensatz (theorem 5)

$$\sqrt{I} = \sqrt{\langle g_1, \ldots, g_n \rangle}.$$

Since both I and $\langle g_1, \ldots, g_n \rangle$ have no multiple roots, they are radical (see [21], Chapter 4, Corollary 2.6) and thus

$$I = \langle g_1, \ldots, g_n \rangle$$

Proposition 25 finally shows that $\{g_1, \ldots, g_n\}$ is a Gröbner basis of I. □

So one can summarize the results for the lexicographic ordering of zero-dimensional ideals as follows: for an ideal generated by $f_1, \ldots, f_s$ of degree $d_1, \ldots, d_s$, only polynomials of degree at most $d_1 \cdots d_n$ are necessary for the lexicographic Gröbner basis. On the other hand, generically (i.e. usually) for $n = s$ at least one polynomial of the same degree is necessary. If all generators have the same degree d, the degree bound can be written as d^n.

Note that $n = s$ is no real restriction for the statement in the generic case since the dimension of $\langle f_1, \ldots, f_s \rangle$ is generically $\max(n - s, 0)$, which is only zero if $n = s$.

3.3 Zero-dimensional Ideals, Graded Orderings

Graded monomial orderings and especially the graded reverse lexicographic monomial ordering are known to be computationally more efficient. This highly correlates to the results presented in this section. The last section showed that the degrees in lexicographic Gröbner bases grow exponentially in the number of variables, even for zero-dimensional ideals. In the same setting, this exponential growth can be avoided by using a graded monomial ordering.

3.3.1 Lower Bound

But the first look will be into a lower degree bound, again. As in the last chapter, this will match the upper bound provided later.

Example 34. In order to establish a lower degree bound, consider the ideal L_n generated by

$$\begin{aligned} f_1 &:= x_1 x_2^{d_1-1} + x_2^{d_1} \\ f_2 &:= x_2 x_3^{d_2-1} + x_3^{d_2} \\ &\vdots \\ f_{n-1} &:= x_{n-1} x_n^{d_{n-1}-1} + x_n^{d_{n-1}} \\ f_n &:= x_1^{d_n} \end{aligned}$$

For an arbitrary graded monomial ordering $\prec$ with $x_1 \prec \ldots \prec x_n$, a Gröbner basis of L_n is given by

$$\begin{aligned} g_1 &:= f_1 = x_1 x_2^{d_1-1} + x_2^{d_1} \\ g_2 &:= f_2 = x_2 x_3^{d_2-1} + x_3^{d_2} \\ &\vdots \\ g_{n-1} &:= f_{n-1} = x_{n-1} x_n^{d_{n-1}-1} + x_n^{d_{n-1}} \\ g_n &:= f_n = x_1^{d_n} \\ g_{n+1} &:= \mathrm{nf}(S(g_n, g_1)) = \mathrm{nf}(x_1^{d_n-1} x_2^{d_1}) = x_2^{d_1+d_n-1} \\ g_{n+2} &:= \mathrm{nf}(S(g_{n+1}, g_2)) = \mathrm{nf}(x_2^{d_1+d_n-2} x_3^{d_2}) = x_3^{d_1+d_2+d_n-2} \\ &\vdots \\ g_{2n-1} &:= \mathrm{nf}(S(g_{2n-2}, g_{n-1})) = \mathrm{nf}(x_{n-1}^{d_1+\ldots+d_{n-2}+d_n-(n-1)} x_n^{d_{n-1}}) = x_n^{d_1+\ldots+d_n-(n-1)} \end{aligned}$$

The key that leads to this observation is that all occurring polynomials only depend on two variables. Thus the relative order of their terms is the same for all considered monomial orderings. $\{g_1, \ldots, g_{2n-1}\}$ obviously generates the ideal L_n since it contains the generators $f_1, \ldots, f_n$ and since $g_1, \ldots, g_{2n-1} \in L_n$. Furthermore one can verify that the Buchberger algorithm 2 would not add any more polynomials to this set. By the correctness of the algorithm (theorem 10) it must therefore be a Gröbner basis. Thus the monomial $x_n^{d_1+\ldots+d_n-(n-2)} \notin \mathrm{LM}(L_n)$ whereas some polynomial of at least degree $d_1 + \ldots + d_n - (n-1)$ must be element of every Gröbner basis of L_n.

Finally, $\dim(L_n) = 0$ due to the leading monomials of $g_n, \ldots g_{2n-1}$ and theorem 19.

This example proves the following theorem.

Theorem 35 (Folklore)**.** *There is a family of ideals $L_n \subset \mathbb{K}[x_1, \ldots, x_n]$ generated by polynomials $f_1, \ldots, f_n$ of degrees $d_1, \ldots, d_n$ such that every Gröbner basis for L_n with respect to any fixed graded monomial ordering contains a polynomial of degree $\sum_{i=1}^{n}(d_i - 1) + 1$.*

3.3.2 Upper Bound

This section closely follows the expositions of Daniel Lazard in [7] and [8]. The citation won't be included at each single lemma, although also proofs of lemmas are taken from these sources.

The proof of the matching upper degree bound is much more involved. First a short outline shall be given. The proof is of algebraic nature as it works with properties of the factor ring $\mathbb{K}[x_0, \ldots, x_n]/J$ of a homogeneous ideal J. In a first step it will be proved that for any zero-dimensional homogeneous ideal J there is a $z_0 \in \mathbb{K}[x_0, \ldots, x_n]/J$ such that every element of the factor ring with sufficiently large degree d is a multiple of z_0.

An equivalence class y of $\mathbb{K}[x_0, \ldots, x_n]/J$ is said to be homogeneous of degree d or $y \in (\mathbb{K}[x_0, \ldots, x_n]/J)_{=d}$ if y contains a polynomial that is homogeneous of the same degree. Since all $y \in \mathbb{K}[x_0, \ldots, x_n]/J$ can be decomposed to

$$y = \sum_{i=1}^{d} y_{=i}$$

whereby $y_{=i} \in (\mathbb{K}[x_0, \ldots, x_n]/J)_{=i}$ for $i = 1, \ldots, n$, one can call the minimal such d the degree of y. $[f]$ will denote the equivalence class that contains f.

In a second step, the smallest degree d is determined for which this statement holds. Then one can dehomogenize the ideal and obtain a degree bound on the normal forms. Finally, proposition 29 can be applied to establish the degree bound for the reduced Gröbner basis.

The first step requires a structure theorem for radical ideals. It proves that every radical ideal is the intersection of prime ideals. An ideal I in a ring R is called *prime* if $\{0\} \subsetneq I \subsetneq R$ and

$$fg \in I \Rightarrow f \in I \text{ or } g \in I.$$

Example 36. The ideal $I := \langle x_1 x_2 \rangle \subset \mathbb{C}[x_1, x_2]$ is not prime since $x_1 x_2 \in I$ but neither $x_1 \in I$ not $x_2 \in I$. On the other hand it is radical since $f \in \sqrt{I}$ implies $f^d = x_1 x_2 g$ for some $d \in \mathbb{N}$ and $g \in \mathbb{C}[x_1, x_2]$. But $x_1x_2 \mid f^d$ implies $x_1x_2 \mid f$ and thus $f \in I$. Now I can be written as

$$I = \langle x_1 \rangle \cap \langle x_2 \rangle .$$

$\langle x_1 \rangle$ is a prime ideal since $fg \in \langle x_1 \rangle$ implies $x_1 \mid fg$ and therefore $x_1 \mid f$ (i.e. $f \in \langle x_1 \rangle$) or $x_1 \mid g$ (i.e. $g \in \langle x_1 \rangle$) because x_1 is not the product of two polynomials. The same reasoning yields that $\langle x_2 \rangle$ is prime.

Of course this example was quite trivial. The generalization of this situation, however, is not. It is summarized in the following theorem.

Theorem 37 (Prime Decomposition)**.** *Let $\mathbb{K}$ be algebraically closed and J be a radical ideal in $\mathbb{K}[x_0, \dots, x_n]$. Then*

$$J = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_r$$

for some $r \geq 0$ and prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ with $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$ for $1 \leq i \neq j \leq r$.

Proof. See [12] (Chapter 4, Theorem 6.5). □

Now it will be proved that for some z_0 every element of $\mathbb{K}[x_0, \dots, x_n]/J$ of sufficiently large degree is a multiple of z_0. The precise statement is given by the following lemma.

Lemma 38. *Let $\mathbb{K}$ be algebraically closed and $J \subset \mathbb{K}[x_0, \dots, x_n]$ be a homogeneous zero-dimensional ideal. Then there is an element z_0 of $\mathbb{K}[x_0, \dots, x_n]/J$ such that the multiplication map*

$$m_{z_0} : (\mathbb{K}[x_0, \dots, x_n]/J)_{=d-1} \longrightarrow (\mathbb{K}[x_0, \dots, x_n]/J)_{=d}, y \mapsto y \cdot z_0$$

is a bijection for sufficiently large degrees d.

Proof. The strategy is to choose z_0 such that it is contained in only one prime ideal, namely

$$\mathfrak{m} := \langle [x_0], \dots, [x_n] \rangle \subset \mathbb{K}[x_0, \dots, x_n]/J.$$

Let $\mathfrak{p} \neq \mathfrak{m}$ be a prime ideal of $\mathbb{K}[x_0, \dots, x_n]/J$. Then $J \subsetneq \mathfrak{p} + J \subsetneq \mathbb{K}[x_0, \dots, x_n]$. Since $\mathfrak{m}$ is a maximal ideal, $\mathfrak{m} \not\subseteq \mathfrak{p} = \sqrt{\mathfrak{p}}$. Therefore $\mathbf{V}_{\mathbb{P}}(\mathfrak{p} + J) \neq \emptyset$ by the projective Nullstellensatz (theorem 6). So one can choose $p \in \mathbf{V}_{\mathbb{P}}(\mathfrak{p} + J)$. Then $\mathfrak{p}$ is contained in the ideal

$$L(p) := \langle p_i[x_j] - p_j[x_i] : 0 \leq i \leq j \leq n \rangle \subset \mathbb{K}[x_0, \dots, x_n]/J$$

since $V_{\mathbb{P}}(\mathfrak{p}+J) \supset V_{\mathbb{P}}(L(p)+J) = \{p\}$ and $L(p)$ is prime. The latter is a consequence of $\mathbb{K}[x_0,\ldots,x_n]/L(p)$ being isomorphic to $\mathbb{K}[x]$ and the theorem that J is prime if and only if $\mathbb{K}[x_0,\ldots,x_n]/J$ is integral. The isomorphism can be constructed from the representation

$$L(p) = \left\langle \frac{p_i}{p_k}[x_k] - [x_i] : 0 \leq i \leq n \right\rangle \tag{3.1}$$

for $p_k \neq 0$ (since $p \in \mathbb{P}^n$, at least one coordinate is nonzero).

Now it is time to choose $z_0 \in (\mathbb{K}[x_0,\ldots,x_n]/J)_{=1}$. By the above consideration, $z_0 \notin \mathfrak{p}$ for any prime ideal $\mathfrak{p} \neq \mathfrak{m}$ can be achieved by choosing $z_0 \notin L(p) \cap (\mathbb{K}[x_0,\ldots,x_n]/J)_{=1}$ for all $p \in \mathbf{V}_{\mathbb{P}}(J)$. For every p, at least one coordinate p_k must be non-zero. But (3.1) implies

$$L(p)_{=1} = \left\{ \alpha_0[x_0] + \ldots + \alpha_n[x_n] : \alpha_i \in \mathbb{K}, \alpha_k = \sum_{\substack{i=0 \\ i \neq k}}^{n} \alpha_i \frac{p_i}{p_k} \right\}.$$

Because $J \subsetneq \mathfrak{p}+J \subset L(p)+J \subsetneq \mathfrak{m}+J$, $L(p)_{=1}$ is a proper subspace of $(\mathbb{K}[x_0,\ldots,x_n]/J)_{=1} = \mathfrak{m}_{=1}$ for every $p \in \mathbf{V}_{\mathbb{P}}(J)$. Now J being zero-dimensional implies that $\mathbf{V}_{\mathbb{P}}(J)$ is finite by theorem 19 such that

$$\bigcup_{p \in \mathbf{V}_{\mathbb{P}}(J)} L(p)_{=1} \subsetneq (\mathbb{K}[x_0,\ldots,x_n]/J)_{=1}.$$

Here the fact that $\mathbb{K}$ is infinite (since algebraically closed) is used.

Thus it is possible to choose $z_0 \in (\mathbb{K}[x_0,\ldots,x_n]/J)_{=1}$ such that $z_0 \notin L(p)$ for all $p \in \mathbf{V}_{\mathbb{P}}(J)$. By the prime decomposition theorem 37

$$\sqrt{\langle z_0 \rangle + J} = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r$$

for some prime ideals $\mathfrak{p}_i$ of $\mathbb{K}[x_0,\ldots,x_n]$. So $\mathfrak{p}_i/J$ are prime ideals of $\mathbb{K}[x_0,\ldots,x_n]/J$. Since

$$z_0 \in \sqrt{\langle z_0 \rangle + J}/J \subset \mathfrak{p}_i/J$$

was chosen such that $\mathfrak{m}$ is the only prime ideal that contains z,

$$\mathfrak{p}_i/J = \mathfrak{m}$$

for all i and thus

$$\sqrt{\langle z_0 \rangle + J}/J = \mathfrak{m}$$

respectively

$$\mathfrak{m}^d = \underbrace{\mathfrak{m} \cdots \mathfrak{m}}_{d \text{ times}} \subset \langle z_0 \rangle \text{ for some } d > 0.$$

Since $\mathfrak{m}^d$ contains all homogeneous elements of $\mathbb{K}[x_0, \dots, x_n]/J$ of degree at least d, m_z is surjective for this sufficiently large d. Furthermore, by theorem 21,

$$\deg(HP_J) = \dim(J) = 0$$

and therefore $\dim_{\mathbb{K}}(\mathbb{K}[x_0, \dots, x_n]/J)_{=d-1} = \dim_{\mathbb{K}}(\mathbb{K}[x_0, \dots, x_n]/J)_{=d}$ is constant for sufficiently large d. This means m_{z_0} is bijective. □

Example 39. To reproduce this strategy in an example, consider the ring $\mathbb{C}[x_0, x_1, x_2]$ with the homogeneous ideal J generated by

$$\begin{aligned} f_1 :=& x_0^2 \\ f_2 :=& x_0x_1 - x_1x_2 \\ f_3 :=& x_1^2 - x_1x_2. \end{aligned}$$

Its graded reverse lexicographic Gröbner basis is given by

$$\begin{aligned} g_1 :=& x_0^2 \\ g_2 :=& x_0x_1 - x_1x_2 \\ g_3 :=& x_1^2 - x_1x_2 \\ g_4 :=& x_1x_2^2. \end{aligned}$$

It is easy to see that the only point in the projective variety $\mathbf{V}_{\mathbb{P}}(J)$ is $p = (0 : 0 : 1)$. According to the lemma one has to choose

$$z_0 \notin L(p) = \langle [x_0], [x_1] \rangle$$

of degree 1, e.g. $z_0 := [x_2] \neq 0$ in $\mathbb{C}[x_0, x_1, x_2]/J$. Since $x_0^2, x_0x_1, x_1^2 \in \mathrm{LM}(G)$, each monomial of degree at least 2 is equivalent to a multiple of x_2 modulo J. For $d \geq 3$, $\dim(\mathbb{C}[x_0, x_1, x_2]/J)_{=d} = 2$ and thus the map m_{x_2} is bijective for $d \geq 4$.

The next step is to conclude that m_{z_0} is bijective for all degrees

$$d \geq \sum_{i=1}^{n+1} (d_i - 1) + 1$$

if the ideal J is generated by homogeneous polynomials $f_1, \ldots, f_s$ of degrees $d_1 \leq \ldots \leq d_s$ (if $s < n+1$, let $d_i = 1$ for $s < i \leq n+1$). This part of the proof will be presented using the Koszul complex.

The Koszul complex is a formalization of ideas going back to Cayley. It is a way to describe and analyze dependencies among polynomials. As any complex, it is a sequence of linear maps (or their representation matrices) such that the composition of two adjacent matrices is the zero-map.

Start with generators $f_1, \ldots, f_s$ of an ideal in $R[x_0, \ldots, x_n]$ for a *noetherian* integral domain R, i.e. a notherian ring without zerodivisors and with $0 \neq 1$ being distinct additively and multiplicatively neutral elements. Remember that any field is noetherian since it has only trivial ideals and, by Hilberts Basis Theorem 4, any polynomial ring over a field is noetherian, too. The first map expresses that these polynomials generate an ideal. It is defined as

$$\delta_1 : R[x_0, \ldots, x_n]^s \longrightarrow R[x_0, \ldots, x_n], (a_1, \ldots, a_s) \mapsto \sum_{i=1}^{s} a_i f_i.$$

So the image of δ_1 is exactly the ideal $\langle f_1, \ldots, f_s \rangle$. But δ_1 is (for $s > 1$) not surjective. In other words, there are relations

$$\sum_{i=1}^{s} a_i f_i = 0, \text{ not all } a_i = 0.$$

Which are these relations, also called *syzygies*? Assume you do not know the polynomials $f_1, \ldots, f_s$. Then it is still possible to come up with some syzygies, e.g. $f_2 f_1 - f_1 f_2 = 0$. This corresponds to the choice

$$(a_1, \ldots, a_s) = (f_2, -f_1, 0, \ldots, 0).$$

Obviously, there are more relations of the same kind. For $i < j$, let $a_i = f_j$, $a_j = -f_i$ and $a_k = 0$ for all $k \neq i, j$. Note, that for $i > j$ you would get the same relations, just multiplied with -1. It turns out, that these $\binom{s}{2}$ syzygies are basically all. Of course, polynomial combinations of these syzygies are syzygies again. And for special choices of $f_1, \ldots, f_s$ there might be more, as well. But beyond that, there are no more syzygies of $f_1, \ldots, f_s$. Therefore one can describe them by a linear map

$$\delta_2 : R[x_0, \ldots, x_n]^{\binom{s}{2}} \longrightarrow R[x_0, \ldots, x_n]^s.$$

Here it is convenient to introduce bases of $\Lambda_2 = R[x_0, \ldots, x_n]^{\binom{s}{2}}$ and $\Lambda_1 = R[x_0, \ldots, x_n]^s$ and define δ_2 on the bases. The basis of Λ_1 will simply be $e_1, \ldots, e_s$ where e_i is the vector of zeros with a 1 in the i-th row. So, letting $\Lambda_0 = R[x_0, \ldots, x_n]$, δ_1 can be described as the linear map defined by

$$\delta_1 : \Lambda_1 \longrightarrow \Lambda_0, e_i \mapsto f_i.$$

The basis of Λ_2 will be denoted by $e_i \wedge e_j$ for $i < j$. Then the dependencies of $f_1, \ldots, f_s$ are described by

$$\delta_2 : \Lambda_2 \longrightarrow \Lambda_1, e_i \wedge e_j \mapsto f_i e_j - f_j e_i \text{ for } i < j.$$

To further simplify the notation, it is common to define $e_i \wedge e_i := 0$ and, for $i < j$, $e_j \wedge e_i := -e_i \wedge e_j$. This is consistent with the definition of δ_2 (without the restriction $i < j$), since

$$\delta_2(e_j \wedge e_i) = f_j e_i - f_i e_j = -(f_i e_j - f_j e_i) = -\delta_2(e_i \wedge e_j) = \delta_2(-e_i \wedge e_j)$$

and

$$\delta_2(e_i \wedge e_i) = f_i e_i - f_i e_i = 0 = \delta_2(0).$$

If $s > 2$, one would face the same problem again: the map δ_2 is never injective, since there are relations between the syzygies, e.g.

$$\delta_2(f_3 e_1 \wedge e_2 - f_2 e_1 \wedge e_3 + f_1 e_2 \wedge e_3) = 0.$$

So one can define another map that captures these relations. Since this process can go on over s levels, a general definition of the maps shall be given now. In level r, each basis relation involves r of the s polynomials where the order is unimportant. So there are $\binom{s}{r}$ basis elements which will be denoted by $e_{i_1} \wedge \ldots \wedge e_{i_r}$ with $i_1 \leq \ldots \leq i_r$. Again, for an easier notation, one consideres vectors $e_{i_1} \wedge \ldots \wedge e_{i_r}$ as basis vectors of

$$R[x_0, \ldots, x_n] \cdot (R[x_0, \ldots, x_n]^s)^r.$$

This vector space is considered modulo the relations

$$c \cdot (v_1 \wedge \ldots \wedge v_r) = (c \cdot v_1) \wedge v_2 \wedge \ldots \wedge v_r = \ldots = v_1 \wedge \ldots \wedge v_{r-1} \wedge (c \cdot v_r)$$

$$v_1 \wedge \ldots \wedge (v_i' + v_i'') \wedge \ldots \wedge v_r = (v_1 \wedge \ldots \wedge v_i' \wedge \ldots \wedge v_r) + (v_1 \wedge \ldots \wedge v_i'' \wedge \ldots \wedge v_r)$$

for all $v_1, \ldots, v_r, v_i', v_i'' \in R[x_0, \ldots, x_n]^s$, $c \in R$ and

$$v_1 \wedge \ldots \wedge v_r = 0 \text{ for all } v_1, \ldots, v_r \in R[x_0, \ldots, x_n]^s \text{ linearly dependent.}$$

A structure with the first two relations is called *tensor product*, together with the third one it is called *wedge product* and denoted by

$$(R[x_0, \ldots, x_n]^s)^{\wedge r} = \underbrace{R[x_0, \ldots, x_n]^s \wedge \ldots \wedge R[x_0, \ldots, x_n]^s}_{r \text{ times}}.$$

So let now $\Lambda_r := (R[x_0, \ldots, x_n]^s)^{\wedge r}$, $r = 1, \ldots, s$, and $\Lambda_0 := R[x_0, \ldots, x_n]$. Then the maps of the Koszul complex are defined as the linear extensions of

$$\delta_r : \Lambda_r \longrightarrow \Lambda_{r-1}, e_{i_1} \wedge \ldots \wedge e_{i_r} \mapsto \sum_{k=1}^{r} (-1)^{k+1} f_{i_k} e_{i_1} \wedge \ldots \wedge e_{i_{k-1}} \wedge e_{i_{k+1}} \wedge \ldots \wedge e_{i_r}.$$

It is easily checked that $\delta_r \circ \delta_{r+1} = 0$. Such a complex Λ is typically written as

$$\Lambda : \Lambda_s \xrightarrow{\delta_s} \Lambda_{s-1} \xrightarrow{\delta_{s-1}} \ldots \xrightarrow{\delta_2} \Lambda_1 \xrightarrow{\delta_1} \Lambda_0. \tag{3.2}$$

If the degree of $h \cdot e_{i_1} \wedge e_{i_r}$ is assigned to $\deg(h) + d_{i_1} + \ldots + d_{i_r}$, δ_r is degree-preserving in the sense that

$$\deg(\delta_r(y)) \leq \deg(y) \text{ for all } y \in \Lambda_r.$$

If all polynomials $f_1, \ldots, f_s$ are homogeneous, one even gets

$$\deg(\delta_r(y)) = \deg(y) \text{ or } \delta_r(y) = 0 \text{ for all } y \in \Lambda_r.$$

In this case, one can consider the restriction of the complex to degree d. Remember that $(\Lambda_r)_{=d}$ is the subspace of the homogeneous elements of degree d. Then the *Koszul complex in degree d* is

$$\Lambda_{=d} : (\Lambda_s)_{=d} \xrightarrow{\delta_s} (\Lambda_{s-1})_{=d} \xrightarrow{\delta_{s-1}} \ldots \xrightarrow{\delta_2} (\Lambda_1)_{=d} \xrightarrow{\delta_1} (\Lambda_0)_{=d}.$$

As mentioned before, the maps δ_{r+1} only capture the syzygies of the basis vectors of Λ_r that are common to all polynomials $f_1, \ldots, f_s$. So what about specific syzygies? These are the syzygies of the basis vectors of Λ_r that are not in the image of δ_{r+1}. Since many of them only differ by syzygies in the image of δ_{r+1}, good representations are

$$H_r := \ker(\delta_r)/\mathrm{im}(\delta_{r+1}),$$

the so-called *homologies* of the complex. Here $\delta_0 : \Lambda_0 \longrightarrow 0$ and $\delta_{s+1} : 0 \longrightarrow \Lambda_s$ are assumed to allow the definition for $r = 0, \dots, s$. Finally, a complex is called *exact*, if all its homologies are zero.

Example 40. Let's pick up example 39 and consider the Koszul complex of the generating polynomials. Since there are three polynomials, $\Lambda_0 = \mathbb{C}[x_0, x_1, x_2]$ and $\mathbb{C}[x_0, x_1, x_2]$-bases of Λ_1, Λ_2 and Λ_3 are $\{e_1, e_2, e_3\}$, $\{e_1 \wedge e_2, e_1 \wedge e_3, e_2 \wedge e_3\}$ respectively $\{e_1 \wedge e_2 \wedge e_3\}$. As mentioned above, $\delta_1(\Lambda_1) = \langle f_1, f_2, f_3\rangle$. Therefore the homology H_0 is the factor ring $\mathbb{C}[x_0, x_1, x_2]/\langle f_1, f_2, f_3\rangle$ for which $\{[x_1], [x_1x_2], [x_2^k], [x_0x_2^k] : k \geq 0\}$ is a basis.

H_1 is defined as $\ker(\delta_1)/\operatorname{im}(\delta_2)$. Here

$$\begin{aligned}\operatorname{im}(\delta_2) = \langle & x_0^2e_2 - (x_0x_1 - x_1x_2)e_1,\\ & x_0^2e_3 - (x_1^2 - x_1x_2)e_1,\\ & (x_0x_1 - x_1x_2)e_3 - (x_1^2 - x_1x_2)e_2\rangle \subset \Lambda_1\end{aligned}$$

which does not contain any elements with terms whose coefficients have degree 0 or 1. However

$$(x_1 - x_2)e_2 + (-x_0 + x_2)e_3 \in \ker(\delta_1) \subset \Lambda_1$$

So clearly $H_1 \neq \{0\}$, although no explicit representation shall be given here. Similarly H_2 turns out to be nonzero. Only $H_3 = 0$ since δ_3, defined by

$$e_1 \wedge e_2 \wedge e_3 \longrightarrow f_1e_2 \wedge e_3 - f_2e_1 \wedge e_3 + f_3e_1 \wedge e_2$$

is injective.

A very important property in connection with the spaces Λ_r is a generalization of the Hilbert basis theorem.

Lemma 41. *Every submodule M of Λ_r is finitely generated if the ground ring R is noetherian.*

Proof. A module M is the analogon of vector spaces over a ring R. Formally, there is an addition $+ : M \times M \longrightarrow M$ and a scalar multiplication $\cdot : R \times M \longrightarrow M$ such that $(M, +, 0)$

is an abelian group and

$$\begin{aligned} a\cdot(f+g) =& a\cdot f + c\cdot g && \text{for all } a\in R, f,g\in M\\ (a+b)\cdot f =& a\cdot f + b\cdot f && \text{for all } a,b\in R, f\in M\\ (ab)\cdot f =& a\cdot(b\cdot f) && \text{for all } a,b\in R, f\in M\\ 1\cdot f =& f && \text{for all } f\in M \end{aligned}$$

By Hilbert's basis theorem 4 and the assumption that R is notherian, ideals in $R[x_0,\ldots,x_n]$ are finitely generated. Then, by [21], Chapter 5, Exercise 1.32, modules in $(R[x_0,\ldots,x_n]^s)^r$ are finitely generated. Finally, Exercise 1.11 of [13] implies that modules in $\Lambda_r = (R[x_0,\ldots,x_n]^s)^{\wedge r}$ are finitely generated. □

For the proof of the upper degree bound, the Koszul complex in degree d of homogeneous polynomials $f_1,\ldots,f_s$ will be considered. The proof will be by induction on the number of variables. This will be achieved by considerations modulo some homogeneous $z\in R[x_0,\ldots,x_n]$ of degree 1 and comparing these to the situation in $R[x_0,\ldots,x_n]$. Therefore the complex

$$0\longrightarrow R[x_0,\ldots,x_n]_{=d-1}\overset{m_z}{\longrightarrow} R[x_0,\ldots,x_n]_{=d}\longrightarrow (R[x_0,\ldots,x_n]/\langle z\rangle)_{=d}\longrightarrow 0 \qquad (3.3)$$

is introduced. m_z denotes the multiplication with z which obviously increases the degree by one, and $R[x_0,\ldots,x_n]_{=d}\longrightarrow (R[x_0,\ldots,x_n]/\langle z\rangle)_{=d}$ is the canonical homomorphism that takes each element to its factor class. It is easily seen that this complex is always exact. Here adding $0\longrightarrow$ in front of the exact complex means that m_z is injective since R is an integral domain, the arrow $\longrightarrow 0$ in the end that the canonical homomorphism is surjective.

So this complex provides a mechanism to compare the rings $R[x_0,\ldots,x_n]$ and $R[x_0,\ldots,x_n]/\langle z\rangle$. But how to apply this to the Koszul complex? The key to this question is to form the tensor product of each term of the sequence (3.3) with the Koszul complex Λ:

$$\begin{aligned} 0\longrightarrow (R[x_0,\ldots,x_n]\otimes\Lambda)_{=d-1}\overset{m_z\otimes\mathrm{id}}{\longrightarrow} (R[x_0,\ldots,x_n]\otimes\Lambda)_{=d}\longrightarrow&\\ \longrightarrow (R[x_0,\ldots,x_n]/\langle z\rangle\otimes\Lambda)_{=d}\longrightarrow 0& \quad (3.4)\end{aligned}$$

Note that each $f\otimes y\in R[x_0,\ldots,x_n]\otimes\Lambda_r$ can be written as

$$f\otimes y = 1\otimes(f\cdot y)$$

and for $f \otimes y, \widetilde{f} \otimes \widetilde{y} \in R[x_0, \dots, x_n] \otimes \Lambda_r$,

$$f \otimes y = \widetilde{f} \otimes \widetilde{y} \iff f \cdot y = \widetilde{f} \cdot \widetilde{y} \text{ in } \Lambda_r$$

such that $R[x_0, \dots, x_n] \otimes \Lambda \equiv \Lambda$. Therefore

$$m_z \otimes \mathrm{id} : (R[x_0, \dots, x_n] \otimes \Lambda)_{=d-1} \longrightarrow (R[x_0, \dots, x_n] \otimes \Lambda)_{=d}$$

is injective. Now the following lemma implies that the sequence of complexes (3.4) is exact.

Lemma 42. *Consider an exact complex of modules over a ring*

$$A : A_3 \longrightarrow A_2 \longrightarrow A_1 \longrightarrow 0$$

and a module T over the same ring. Then

$$A \otimes T : A_3 \otimes T \longrightarrow A_2 \otimes T \longrightarrow A_1 \otimes T \longrightarrow 0$$

is also exact.

Proof. See [13] (Proposition A2.1). □

Since (3.4) is an exact sequence of complexes, one can relate the homologies of these complexes in an interesting way. As noted above, $R[x_0, \dots, x_n] \otimes \Lambda \equiv \Lambda$ such that the first two complexes in the sequence are isomorphic to the Koszul complex in degree $d-1$ respectively d. Their homologies shall be denoted by $(H_t)_{=d-1}$ respectively $(H_t)_{=d}$. The third complex $(R[x_0, \dots, x_n]/\langle z \rangle \otimes \Lambda)_{=d}$, however, is the Koszul complex in degree d over the factor ring $R[x_0, \dots, x_n]/\langle z \rangle$ of the factor classes $[f_1], \dots, [f_t]$. Its homologies will be denoted by $(\widetilde{H}_t)_{=d}$.

It is easy to see that (3.4) induces maps from $(H_t)_{=d-1}$ to $(H_t)_{=d}$ and from $(H_t)_{=d}$ to $(\widetilde{H}_t)_{=d}$. Surprisingly there is also an induced map from $(\widetilde{H}_t)_{=d}$ to $(H_{t-1})_{=d-1}$, whose construction is given by the so-called *Snake lemma* (see [13], Appendix A3.7). This yields a sequence

$$\dots \longrightarrow (\widetilde{H}_{t+1})_{=d} \longrightarrow (H_t)_{=d-1} \longrightarrow (H_t)_{=d} \longrightarrow (\widetilde{H}_t)_{=d} \longrightarrow (H_{t-1})_{=d-1} \longrightarrow \dots \qquad (3.5)$$

which is exact by [13], Proposition A3.15.

Remember, that z is a homogeneous polynomial of degree 1. Therefore the factor ring $R[x_0, \dots, x_n]/\langle z \rangle$ is isomorphic to a polynomial ring in n variables which is easiest seen for the choice $z := x_n$. The general case follows from a coordinate transformation. This will be the key to the induction on the number of variables. Also note, that Koszul complexes in different degrees are involved. So once $(\widetilde{H}_{t+1})_{=d} = 0$ and $(H_t)_{=d} = 0$ are known, one can conclude $(H_t)_{=d-1} = 0$.

The proof strategy from here is as follows. The first step is to conclude from lemma 38, that modulo z_0 (as in that lemma) the Koszul complex is exact in large degrees, i.e. $(\widetilde{H}_t)_{=d} = 0$ for $z := z_0$ and sufficiently large d. Then one uses the complex (3.5) and induction on the number of variables to show that $(\widetilde{H}_t)_{=d} = 0$ for all d larger than a constant (which will depend on the number of variables and the number of polynomials. After dehomogenization, proposition 29 can be applied to establish the degree bound.

For this conclusion the context is an algebraically closed field $R = \mathbb{K}$ as in lemma 38. First remember that in the Koszul complex $\operatorname{im}(\delta_1) = \langle f_1, \ldots, f_s \rangle =: J$. Therefore the last homology of the complex is

$$H_0 = \ker(\Lambda_0 \longrightarrow 0)/\operatorname{im}(\delta_1) = \Lambda_0/J = \mathbb{K}[x_0, \ldots, x_n]/J$$

which is the factor ring. z_0 was chosen such that the multiplication m_{z_0} in $\mathbb{K}[x_0, \ldots, x_n]/J$ is bijective in large degrees. So for large d, all elements of $(\mathbb{K}[x_0, \ldots, x_n]/J)_{=d}$ are multiples of z_0. Hence

$$(\mathbb{K}[x_0, \ldots, x_n]/\langle J, z_0 \rangle)_{=d} = 0$$

which is just the homology $(\widetilde{H}_0)_{=d}$ of the Koszul complex in $\mathbb{K}[x_0, \ldots, x_n]/\langle z_0 \rangle$ (so here $z := z_0$ in the above notation).

Since $\mathbb{K}[x_0, \ldots, x_n]/\langle z_0 \rangle$ is isomorphic to a polynomial ring in n variables, the following lemma shows that $(\widetilde{H}_r)_{=d}$, the homologies of the Koszul complex of $f_1, \ldots, f_s$ in $\mathbb{K}[x_0, \ldots, x_n]/\langle z_0 \rangle$, are zero for all $r > 0$:

Lemma 43. *Let Λ be the Koszul complex of homogeneous polynomials $f_1, \ldots, f_s$ in the ring $R[x_0, \ldots, x_n]$ and $H_r = \ker(\delta_r)/\operatorname{im}(\delta_{r+1})$ its homologies for $r = 0, \ldots, s$. Then $(H_0)_{=d} = 0$ for sufficiently large d implies that $(H_r)_{=d} = 0$ for sufficiently large d.*

Proof. The strategy for this proof is to localize the ring at a prime ideal and find local inverses for the mappings δ_r. From the fact that the localized homologies are zero, one can conclude the same for large degrees for $(H_r)_{=d}$.

The assumption $(H_0)_{=d} = R[x_0, \ldots, x_n]/J = 0$ for sufficiently large d implies $\sqrt{J} = \langle x_0, \ldots, x_n \rangle$. For convenience define $\mathfrak{m} := \langle x_0, \ldots, x_n \rangle$ (note that this is the same ideal as in lemma 38, but in another ring). Now $\mathfrak{m}$ is maximal, such that it is the only prime ideal containing J.

Consider the localization $R_\mathfrak{p}$ of $R[x_0, \ldots, x_n]$ with respect to a prime ideal $\mathfrak{p} \neq \mathfrak{m}$, i.e.

$$R_\mathfrak{p} := \left\{ \frac{f}{g} : f \in R[x_0, \ldots, x_n], g \in R[x_0, \ldots, x_n] \setminus \mathfrak{p} \right\}.$$

Since R and therefore $R[x_0, \ldots, x_n]$ are integral domains, also $R_\mathfrak{p}$ is a ring. In this extension all elements except those contained in $\mathfrak{p}$ are units. This means $\mathfrak{p}$ is the only maximal ideal.

Then $\Lambda \otimes R_\mathfrak{p}$ is the Koszul complex of the polynomials $f_1, \ldots, f_s$ in the ring $R_\mathfrak{p}$. Since $\sqrt{J} = \mathfrak{m}$, J is not completely contained in $\mathfrak{p}$, i.e. there is a unit of $R_\mathfrak{p}$ contained in $J \otimes R_\mathfrak{p}$. This implies $J \otimes R_\mathfrak{p} = R_\mathfrak{p}$. Furthermore

$$\Lambda_0 \otimes R_\mathfrak{p} = R[x_0, \ldots, x_n] \otimes R_\mathfrak{p} = R_\mathfrak{p}.$$

It follows that the map

$$\delta_1 \otimes \mathrm{id} : \Lambda_1 \otimes R_\mathfrak{p} \longrightarrow \Lambda_0 \otimes R_\mathfrak{p}$$

is surjective since $\mathrm{im}(\delta_1 \otimes \mathrm{id}) = J \otimes R_\mathfrak{p}$. Therefore one can choose $\varepsilon \in \Lambda_1 \otimes R_\mathfrak{p}$ such that

$$(\delta_1 \otimes \mathrm{id})(\varepsilon) = 1.$$

The homomorphisms defined by

$$\varepsilon_r : \Lambda_r \longrightarrow \Lambda_{r+1}, e_{i_1} \wedge \ldots \wedge e_{i_r} \mapsto \varepsilon \wedge e_{i_1} \wedge \ldots \wedge e_{i_r}$$

will provide an inverse of $\delta_{r+1} \otimes \mathrm{id}$, restricted to the kernel of $\delta_r \otimes \mathrm{id}$. This will clearly imply that $\ker(\delta_r \otimes \mathrm{id})/\mathrm{im}(\delta_{r+1} \otimes \mathrm{id})$, the homologies of $\Lambda \otimes R_\mathfrak{p}$, are zero.

To see that $\delta_{r+1} \otimes \mathrm{id}$ can be inverted, the following will be proved:

$$\varepsilon_{r-1} \circ (\delta_r \otimes \mathrm{id}) + (\delta_{r+1} \otimes \mathrm{id}) \circ \varepsilon_r = \mathrm{id} \tag{3.6}$$

Then $x \in \ker(\delta_r \otimes \mathrm{id})$ yields $(\delta_{r+1} \otimes \mathrm{id}) \circ \varepsilon_r(x) = x$ and thus $x \in \mathrm{im}(\delta_{r+1})$ as wished. So it remains to verify (3.6). Since only homomorphisms are involved, a check on the basis elements suffices. Have a look at the first term first.

$$\begin{aligned}\varepsilon_{r-1} \circ (\delta_r \otimes \mathrm{id})(e_{i_1} \wedge \ldots \wedge e_{i_r}) &= \varepsilon_{r-1}\left(\sum_{k=1}^{r} (-1)^{k+1} f_{i_k} e_{i_1} \wedge \ldots \wedge e_{i_{k-1}} \wedge e_{i_{k+1}} \wedge \ldots \wedge e_{i_r}\right) \\ &= \sum_{k=1}^{r} (-1)^{k+1} f_{i_k} \varepsilon \wedge e_{i_1} \wedge \ldots \wedge e_{i_{k-1}} \wedge e_{i_{k+1}} \wedge \ldots \wedge e_{i_r}\end{aligned}$$

Now compare with the second term.

$$\begin{aligned}(\delta_{r+1} \otimes \mathrm{id}) \circ \varepsilon_r(e_{i_1} \wedge \ldots \wedge e_{i_r}) &= (\delta_{r+1} \otimes \mathrm{id})(\varepsilon \wedge e_{i_1} \wedge \ldots \wedge e_{i_r}) \\ &= e_{i_1} \wedge \ldots \wedge e_{i_r} + \sum_{k=1}^{r} (-1)^{k+2} f_{i_k} \varepsilon \wedge e_{i_1} \wedge \ldots \wedge e_{i_{k-1}} \wedge e_{i_{k+1}} \wedge \ldots \wedge e_{i_r}\end{aligned}$$

So all terms on the left hand side of equation (3.6) except for $e_{i_1} \wedge \ldots \wedge e_{i_r}$ cancel out, which yields exactly the identity map.

It was proved that for all prime ideals $\mathfrak{p} \neq \mathfrak{m}$, the homologies H_r of Λ fulfill

$$H_r \otimes R_{\mathfrak{p}} = \ker(\delta_r \otimes \mathrm{id})/\mathrm{im}(\delta_{r+1} \otimes \mathrm{id}) = 0.$$

Hence one can conclude that

$$\forall y \in \ker(\delta_r) \exists f \in R[x_0, \ldots, x_n] \setminus \mathfrak{p} : fy \in \mathrm{im}(\delta_{r+1}).$$

Choose now the prime ideal $\mathfrak{p} = \langle x_0, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n \rangle$. Consider a finite basis F of the ideal $\ker(\delta_r)$ which exists by lemma 41. Then for each $y \in F$ there is an integer $c \geq 0$ such that $yx_k^c \in \mathrm{im}(\delta_{r+1})$. With C being the maximum of the values of c for all basis elements $y \in F$ and for all $k = 0, \ldots, n$, one obtains

$$\mathfrak{m}^C \ker(\delta_r) = \underbrace{\mathfrak{m} \cdots \mathfrak{m}}_{C \text{ times}} \cdot \ker(\delta_r) \subset \mathrm{im}(\delta_{r+1})$$

and therefore

$$(H_r)_{=d} = \ker(\delta_r)_{=d} = \mathrm{im}(\delta_r)_{=d}$$

for all $d \geq C + \max\{\deg(y) : y \in F\}$. □

Applying this lemma one obtains $(\widetilde{H}_r)_{=d} = 0$ whereby $\widetilde{H}_r$ are the homologies of the Koszul complex of $f_1, \ldots, f_s$ in $\mathbb{K}[x_0, \ldots, x_n]/\langle z_0 \rangle$.

Example 44. To verify this in example 39, one has to calculate the homologies $\widetilde{H}_r$ modulo $z_0 = x_2$ (z_0 as in 40). For this exercise, $\mathbb{C}[x_0, x_1, x_2]/\langle x_2\rangle$ will be identified with $\mathbb{C}[x_0, x_1]$. Then the polynomials have the form

$$\begin{aligned}\widetilde{f}_1 :=& x_0^2\\ \widetilde{f}_2 :=& x_0x_1\\ \widetilde{f}_3 :=& x_1^2\end{aligned}$$

Clearly $\widetilde{J} = \left\langle \widetilde{f}_1, \widetilde{f}_2, \widetilde{f}_3 \right\rangle \subset \mathbb{C}[x_0, x_1]$ contains all monomials of degree ≥ 2. Therefore

$$\widetilde{H}_0 = \mathbb{C}[x_0, x_1]/\widetilde{J} = \{[1], [x_0], [x_1]\}$$

and $(\widetilde{H}_0)_{=d} = 0$ for $d \geq 2$. Now consider $\widetilde{H}_1$ which is the factor module of

$$\ker(\delta_1) = \langle x_0e_2 - x_1e_1, x_0e_3 - x_1e_2\rangle$$

and

$$\operatorname{im}(\delta_2) = \left\langle x_0^2e_2 - x_0x_1e_1, x_0^2e_3 - x_1^2e_1, x_0x_1e_3 - x_1^2e_2\right\rangle.$$

Then a homogeneous element y of $\ker(\delta_1)$, i.e.

$$y = h_1(x_0e_2 - x_1e_1) + h_2(x_0e_3 - x_1e_2) \text{ for homogeneous } h_1, h_2 \in \mathbb{C}[x_0, x_1].$$

If $\deg(y) \geq 5$, h_1 and h_2 have degree at least 2 (e_1, e_2, e_3 have degree 2). Since h_1, h_2 are homogeneous, it suffices to check $m(x_0e_2 - x_1e_1), m(x_0e_3 - x_1e_2) \in \operatorname{im}(\delta_2)$ for all monomials $m \in \mathbb{C}[x_0, x_1]$ of degree 2. E.g.

$$x_1^2(x_0e_2 - x_1e_1) = x_1(x_0^2e_3 - x_1^2e_1) - x_0(x_0x_1e_3 - x_1^2e_2).$$

All other checks are trivial or analogous. Therefore $(\widetilde{H}_1)_{=d} = 0$ for $d \geq 5$. Similar results can be obtained for $\widetilde{H}_2$ and $\widetilde{H}_3$.

Since the homologies $\widetilde{H}_r$ of the Koszul complex of $f_1, \ldots, f_s$ in $\mathbb{K}[x_0, \ldots, x_n]/\langle z_0\rangle$ are zero in high degrees, this Koszul complex fulfills the precondition for the following lemma.

Lemma 45. *If the homologies of the Koszul complex Λ in a ring $R[x_0, \ldots, x_n]$ with $n+1$ variables fulfill $(H_r)_{=d} = 0$ for sufficiently large d, then* *(a)* $(H_r)_{=d} = 0$ *for all* d *if* $r \geq s-n$

(b) $(H_r)_{=d} = 0$ *for all* $d \geq D(r,n) := d_1 + \ldots + d_{r+n+1} - n + 1$ *if* $r < s-n$.

Proof. This proof is by induction on the number of variables. First assume $n = 0$. For part (a) one only has to show that $(H_s)_{=d} = 0$ for all d. But $H_s = \ker(\delta_s) = 0$ since Λ_s has only one basis element, namely $e_1 \wedge \ldots \wedge e_s$ and its image is not zero. To prove part (b) take $y \in \ker(\delta_r)$. Then $x_0^c y \in \ker(\delta_r)$ for all $c \geq 0$ and, by assumtion, $x_0^c y \in \operatorname{im}(\delta_{r+1})$ for some $c \geq 0$, i.e.

$$x_0^c y = \delta_{r+1}(z) \text{ for some } z \in \Lambda_{r+1}.$$

The basis elements of Λ_{r+1} have the form $e_{i_1} \wedge \ldots \wedge e_{i_{r+1}}$ and have degree at most $d_1 + \ldots + d_{r+1}$. Remember that $d_1 \geq \ldots \geq d_s$ was assumed. So if $\deg(y) \geq d_1 + \ldots + d_{r+1}$,

$$\deg(z) = \deg(\delta_{r+1}(z)) = \deg(x_0^c y) = c + \deg(y) \geq c + d_1 + \ldots + d_{r+1}$$

implies that the coefficients of z are of degree at least c. Since $n = 0$ and the coefficients are homogeneous, they are powers of x_0 and therefore divisible by x_0^c. Thus $y \in \operatorname{im}(\delta_{r+1})$.

Now consider the case $n > 0$. By assumption the homologies $(H_r)_{=d}$ of Λ in $R[x_0, \ldots, x_n]$ are zero for large degrees d. Choose an arbitrary homogeneous $0 \neq z \in R[x_0, \ldots, x_n]$ of degree 1 and let $\widetilde{\Lambda}$ denote the Koszul complex of the same polynomials in $R[x_0, \ldots, x_n]/\langle z \rangle$. Then its homologies $(\widetilde{H}_r)_{=d} = 0$ for large degrees d, too. Since $R[x_0, \ldots, x_n]/\langle z \rangle \cong R[x_0, \ldots, x_{n-1}]$, one can apply the induction hypothesis and conclude that

$$(\widetilde{H}_{r+1})_{=d} = 0 \text{ for } \begin{cases} \text{all } d \text{ if } r+1 \geq s-(n-1) \Longleftrightarrow r \geq s-n \\ d \geq D(r+1, n-1) = d_1 + \ldots + d_{r+n+1} - n + 2 \text{ if } r < s-n \end{cases} \tag{3.7}$$

The following part of the exact sequence (3.5) is the key.

$$(\widetilde{H}_{r+1})_{=d} \longrightarrow (H_r)_{=d-1} \longrightarrow (H_r)_{=d}$$

Whenever

$$(\widetilde{H}_{r+1})_{=d} = (H_r)_{=d} = 0,$$

also $(H_r)_{=d-1} = 0$. Since $(H_r)_{=d} = 0$ for large d by assumption, equation (3.7) implies the claim. □

The rest of the proof is very easy. It remains to dehomogenize, which will be done in this theorem. As convenience, the whole strategy will be recapitulated.

Theorem 46 (Lazard, 1983)**.** *Let $\mathbb{K}$ be an algebraically closed field and $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be a zero-dimensional ideal generated by polynomials $f_1, \ldots, f_s$ of degrees $d_1 < \ldots < d_s$. Then for every graded monomial ordering there is a Gröbner basis for I which contains only polynomials of degrees bounded by*

$$D := (d_1 - 1) + \ldots + (d_{n+1} - 1) + 1$$

(with $d_i := 1$ for $s < i \leq n+1$ if necessary).

Proof. Consider the homogenizations ${}^hf_1, \ldots, {}^hf_s \in \mathbb{K}[x_0, \ldots, x_n]$ of $f_1, \ldots, f_s$ (which have the same degrees) and their ideal $J := \left\langle {}^hf_1, \ldots, {}^hf_s \right\rangle$. Since $\dim(J) = \dim(I) = 0$, lemma 38 provides $z_0 \in \mathbb{K}[x_0, \ldots, x_n]/J$ homogeneous of degree 1 such that the multiplication m_{z_0} is a bijection in large degrees. Therefore the homology $\widetilde{H}_0$ of the Koszul complex of $[{}^hf_1], \ldots, [{}^hf_s] \in \mathbb{K}[x_0, \ldots, x_n]/\langle z_0 \rangle$ is zero in large degrees. Then lemma 43 implies the same for all $\widetilde{H}_r$ $(0 \leq r \leq s)$ and lemma 45 gives an explicit degree from which the homologies are zero.

Especially $(\mathbb{K}[x_0, \ldots, x_n]/J)_{=d} = (\widetilde{H}_0)_{=d} = 0$ for $d \geq d_1 + \ldots + d_{n+1} - n + 1 = D$. Since the sequence (part of (3.5))

$$(H_0)_{=d-1} \longrightarrow (H_0)_{=d} \longrightarrow (\widetilde{H}_0)_{=d}$$

is exact, the map $(H_0)_{=d-1} \longrightarrow (H_0)_{=d}$, which is the multiplication m_{z_0}, is surjective for all $d \geq D$. It is time to dehomogenize. This can be done before or after the multiplication with z_0. Since the order doesn't matter, the diagramm

$$\begin{tikzcd}
(\mathbb{K}[x_0, \ldots, x_n]/J)_{=D-1} \arrow[r, "m_{z_0}"] \arrow[d] & (\mathbb{K}[x_0, \ldots, x_n]/J)_{=D} \arrow[d] \\
(\mathbb{K}[x_1, \ldots, x_n]/I)_{\leq D-1} \arrow[r, "m_{\widetilde{z}_0}"] & (\mathbb{K}[x_1, \ldots, x_n]/I)_{\leq D}
\end{tikzcd}$$

is commutative (with ${}^h\widetilde{z}_0 = z_0$). Thus also $m_{\widetilde{z}_0}$ is surjective for degrees D and larger. Since

$$(\mathbb{K}[x_1, \ldots, x_n]/I)_{\leq D-1} \subset (\mathbb{K}[x_1, \ldots, x_n]/I)_{\leq d} \text{ for } d \geq D$$

and there is a surjection from the first to the second space,

$$(\mathbb{K}[x_1, \ldots, x_n]/I)_{\leq D-1} = (\mathbb{K}[x_1, \ldots, x_n]/I)_{\leq d} \text{ for } d \geq D.$$

So all normal forms have degree at most $D-1$. Finally the claims follows by proposition 29. □

3.3.3 Generic Degree

The rest of this chapter will be dedicated to the generic degree of Gröbner bases with respect to a graded monomial ordering. It relies heavily on the multivariate subresultant as introduced by Marc Chardin in [10]. Therefore this result will be explained first, though not in its full generality.

To introduce subresultants, Chardin consideres the Koszul complex as introduced in (3.2), but applied to n homogeneous polynomials with indeterminate coefficients in $n+1$ coordinate intederminates

$$F_i = \sum_{\substack{\alpha \in \mathbb{Z}_{\geq 0}^{n+1} \\ |\alpha| = d_i}} u_{i,\alpha} x^\alpha \in \mathcal{S}[x_0, \ldots, x_n]$$

for $i = 1, \ldots, n$ and

$$\mathcal{S} := \mathbb{Z}[u_{i,\alpha} : i = 1, \ldots, n, \alpha \in \mathbb{Z}_{\geq 0}^{n+1}, |\alpha| = d_i].$$

Note that $\mathcal{S}$ is an noetherian integral domain. Since in some places it is convenient to talk about dimensions, one has to consider the field of fractions

$$\mathcal{K} := \left\{ \frac{f}{g} : f, g \in \mathcal{S}, g \neq 0 \right\}.$$

First two basic facts about specializations are needed.

Lemma 47. *Let $\mathcal{V} \subset \mathcal{S}[x_0, \ldots, x_n]$ be an $\mathcal{S}$-vector space, $\psi : \mathcal{S}[x_0, \ldots, x_n] \longrightarrow \mathbb{K}[x_0, \ldots, x_n]$ a specialization and $\varphi : \mathcal{V} \longrightarrow \mathcal{V}$ a linear map. Then*

$$\dim_{\mathcal{K}}(\operatorname{im}(\varphi) \otimes \mathcal{K}) \geq \dim_{\mathbb{K}}(\psi(\operatorname{im}(\varphi)))$$

and, if $\dim_{\mathcal{K}}(\mathcal{V}) = \dim_{\mathbb{K}}(V)$*,*

$$\dim_{\mathcal{K}}(\ker(\varphi) \otimes \mathcal{K}) \leq \dim_{\mathbb{K}}(\psi(\ker(\varphi))).$$

Proof. Consider a basis $\{\psi(\varphi(b_1)), \ldots, \psi(\varphi(b_r))\}$ of $\psi(\mathrm{im}(\varphi))_{=d}$ for any fixed d. Of course $\varphi(b_1), \ldots, \varphi(b_r) \in \mathrm{im}(\varphi) \otimes \mathcal{K}$. So all one has to prove is that these vectors are linearly independent over $\mathcal{K}$. Assume $\{\varphi(b_1), \ldots, \varphi(b_r)\}$ dependent over $\mathcal{K}$. Then there are $a_1, \ldots, a_r \in \mathcal{K}$, not all of them zero, such that

$$a_1\varphi(b_1) + \ldots + a_r\varphi(b_r) = 0.$$

By multiplying with the common denominator of $a_1, \ldots, a_r$, one can assume $a_1, \ldots, a_r \in \mathcal{S}$. Assume the coefficients $a_1, \ldots, a_r$ have no common factor in $\mathcal{S}$. Now specialize one variable after the other. If, on specialization of a variable $u_{i,\alpha}$ to $c_{i,\alpha}$, all coefficients $a_1, \ldots, a_r$ vanish, they must be divisible by $u_{i,\alpha} - c_{i,\alpha}$. Divide all coefficients by the highest common power of $u_{i,\alpha} - c_{i,\alpha}$ and call the new coefficients $a'_1, \ldots, a'_r$. Then

$$a'_1\varphi(b_1) + \ldots + a'_r\varphi(b_r) = 0$$

and on specialization of $u_{i,\alpha}$ not all coefficients $a'_1, \ldots, a'_r$ vanish. Inductively one obtains a relation

$$\widetilde{a}_1\varphi(b_1) + \ldots + \widetilde{a}_r\varphi(b_r) = 0 \text{ for some } \widetilde{a}_1, \ldots \widetilde{a}_r \in \mathbb{K}, \text{ not all zero.}$$

This contradicts the assumption that $\{\varphi(b_1), \ldots, \varphi(b_r)\}$ is a basis. Therefore

$$\dim_{\mathcal{K}}(\mathrm{im}(\varphi) \otimes \mathcal{K})_{=d} \geq \dim_{\mathbb{K}}(\psi(\mathrm{im}(\varphi))_{=d}) \tag{3.8}$$

Then the second inequality simply follow from

$$\dim_{\mathcal{K}}(\ker(\varphi) \otimes \mathcal{K}) + \dim_{\mathcal{K}}(\mathrm{im}(\varphi) \otimes \mathcal{K}) = \dim_{\mathcal{K}}(\mathcal{V})$$

and

$$\dim_{\mathbb{K}}(\psi(\ker(\varphi))) + \dim_{\mathbb{K}}(\psi(\mathrm{im}(\varphi))) = \dim_{\mathcal{K}}(V)$$

□

Actually the theory works as long as the number of polynomials is not larger than the number of variables, but only the case of n polynomials in $n+1$ variables will be needed in this thesis. The ideal of these polynomials will be denoted by $\mathcal{J} := \langle F_1, \ldots, F_n \rangle$. This ideal is well-studied. The following property will be needed:

Lemma 48. *With definitions as above, $\mathcal{J}$ is a prime ideal.*

Proof. See [10], Proposition 3 and [23]. □

The goal is to derive an exact sequence from the Koszul complex and then decompose it in order to define the subresultant using an alternating product of determinants. First note that the homologies H_r of the Koszul complex of $F_1, \dots, F_n$ are zero for $r > 0$, where the complex looks like

$$\Lambda : \Lambda_n \xrightarrow{\delta_n} \Lambda_{n-1} \xrightarrow{\delta_{n-1}} \dots \xrightarrow{\delta_2} \Lambda_1 \xrightarrow{\delta_1} \Lambda_0,$$

Lemma 49. *Let $\Lambda = (\Lambda_r)$ be the Koszul complex of $F_1, \dots, F_n$ in $\mathcal{S}$ (as defined above) and $H_0, \dots, H_n$ its homologies. Then $H_r = 0$ for all $0 < r \leq n$.*

Proof. See [10], Proposition 2 and [23]. □

So only $H_0 = \mathcal{S}[x_0, \dots, x_n]/\mathcal{J}$ is nonzero. Choose now a set S of monomials of degree d that is a vector space basis of $(H_0 \otimes \mathcal{K})_{=d}$. This is an important step. For every degree d and set S (and of course for every tuple of degrees $d_1, \dots, d_n$ of $F_1, \dots, F_n$) one will obtain a different subresultant. The dependence on the degrees will be implicit since they are considered to be constant. So the subresultant polynomial will be denoted by $\Delta_S \in \mathcal{S}$.

Note that the dimension of $(H_0 \otimes \mathcal{K})_{=d}$ can only increase on specialization. To see this, remember $H_0 = \mathcal{S}[x_0, \dots, x_n]/\mathrm{im}(\delta_1)$. On the one hand

$$\dim_{\mathcal{K}}(\mathcal{K}[x_0, \dots, x_n]_{=d}) = \dim_{\mathbb{K}}(\mathbb{K}[x_0, \dots, x_n]_{=d}).$$

On the other hand

$$\dim_{\mathcal{K}}(\mathrm{im}(\delta_1) \otimes \mathcal{K})_{=d} \geq \dim_{\mathbb{K}}(\mathrm{im}(\delta_1)_{=d})$$

by lemma 47.

In order to obtain an exact complex, replace $\delta_1 : (\Lambda_1)_{=d} \longrightarrow (\Lambda_0)_{=d}$ in the Koszul complex by the induced

$$\delta_1^* : (\Lambda_1)_{=d} \longrightarrow (\Lambda_0/\mathrm{span}_{\mathcal{S}}(S))_{=d}, y \mapsto [\delta_1(y)].$$

Here

$$\mathrm{span}_R(S) := \{a_1 s_1 + \dots a_k s_k : k \in \mathbb{N}, a_i \in R, s_i \in S \text{ for } i = 1, \dots, k\}.$$

Writing the matrix of δ_1 in the monomials basis of $(\Lambda_0/\mathrm{span}_{\mathcal{S}}(S))_{=d}$, one column being the coefficients of the image of one basis vector, δ_1^* is represented by the submatrix corresponding to the rows of the monomials not contained in S. Since S is by definition a basis of the homology $H_0 \otimes \mathcal{K} = (\Lambda_0 \otimes \mathcal{K})/(\mathrm{im}(\delta_1) \otimes \mathcal{K})$ in degree d, $\delta_1^* \otimes \mathrm{id}$ is surjective. It was already noted before that δ_n is injective, so the complex

$$0 \longrightarrow (\Lambda_n \otimes \mathcal{K})_{=d} \xrightarrow{\delta_n} (\Lambda_{n-1} \otimes \mathcal{K})_{=d} \xrightarrow{\delta_{n-1}} \ldots \xrightarrow{\delta_2} (\Lambda_1)_{=d} \xrightarrow{\delta_1^*} (\Lambda_0 \otimes \mathcal{K})_{=d}/S_{=d} \longrightarrow 0$$

is exact.

In order to define the subresultant, this complex will be decomposed. Fix bases B_i for $(\Lambda_i)_{=d}$ for $i = 1, \ldots, n$ and B_0 for $(\Lambda_0 \otimes \mathcal{K})_{=d}/\mathrm{span}_{\mathcal{K}}(S)$. Consider first $\delta_1^* \otimes \mathrm{id}$ which is surjective. So B_1 can be decomposed into B_1' and B_1'' (i.e. $B_1 = B_1' \cup B_1''$ and $B_1' \cap B_1'' = \emptyset$) such that $(\delta_1^* \otimes \mathrm{id})(B_1')$ is a basis for $(\Lambda_0 \otimes \mathcal{K})_{=d}/\mathrm{span}_{\mathcal{K}}(S)$. Therefore $\#B_1' = \#B_0$. This decomposition is usually not unique. Define $B_0' = \emptyset$ and $B_0'' = B_0$ for the recursion following.

The same can be done recursively for $\delta_r \otimes \mathrm{id}$ $(r = 2, \ldots, n)$. To obtain a surjective mapping that agrees with $\delta_{r-1}^* \otimes \mathrm{id}$, define

$$\delta_r^* : (\Lambda_r)_{=d} \longrightarrow (\Lambda_{r-1})_{=d}/\mathrm{span}(B_1'), y \mapsto [\delta_r(y)].$$

Again there is a decomposition of B_r into B_r' and B_r'' such that $\delta_r^*(B_r')$ is a basis of the linear space in $(\Lambda_{r-1} \otimes \mathcal{K})_{=d}/\mathrm{span}_{\mathcal{K}}(B_1')$ generated by the factor classes of B_{r-1}''. This implies $\#B_r' = \#B_{r-1}''$. Since $\delta_n \otimes \mathrm{id}$ is injective, $B_n' = B_n$ and $B_n'' = \emptyset$.

The restricitons $\varphi_r := \delta_r^*|_{\mathrm{span}_{\mathcal{S}}(B_r')}$ are injective linear maps since they are also restrictions of the bijective maps

$$\delta_r^* \otimes \mathrm{id}|_{\mathrm{span}_{\mathcal{K}}(B_r')} : \mathrm{span}_{\mathcal{K}}(B_r') \longrightarrow \mathrm{span}_{\mathcal{K}}(B_{r-1}'')$$

to $\mathrm{span}_{\mathcal{S}}(B_r') \subset \mathrm{span}_{\mathcal{K}}(B_r')$. So their determinants $\det(\varphi_r)$ are well-defined and non-zero. If the dependence on S has to be underlined, $\varphi_1^S := \varphi_1$ will be written. So one can define

$$\Delta_S := \prod_{i=1}^{n} \det(\varphi_i)^{(-1)^{i+1}}.$$

If S does not generate $(H_0 \otimes \mathcal{K})_{=d}$, one defines $\Delta_S := 0$. This is the multivariate subresultant as defined by Chardin up to the sign which is not important for this proof. Its first important property is

Lemma 50. *With all definitions as above,*

$$\Delta_k := \prod_{i=k}^{n} \det(\varphi_i)^{(-1)^{i+k}} \in \mathcal{S}$$

for $k = 1, \ldots, n$ and $\Delta_S = \Delta_1$ is independent of the chosen decomposition.

Proof. See [24], Proposition 2 and Remark 2 following the theorem. □

So the subresultant is a polynomial in the coefficients of the polynomials $F_1, \ldots, F_n$ and therefore can be used as criterion for a generic situation as introduced in section 3.2.3. As already pointed out, it depends on the degrees of the polynomials $F_1, \ldots, F_n$, the degree d to which the Koszul complex is restricted and the set S which has to be a basis of $(H_0 \otimes \mathcal{K})_{=d}$.

There are two important properties of the subresultant. First it is possible to explicitely state polynomials of arbitrary degrees that are contained in the ideal $\mathcal{J}$ generated by $F_1, \ldots, F_n$ and therefore also in any specialization $\psi(\mathcal{J})$ (although they might specialize to the zero-polynomial). Second will be an equivalence of the non-vanishing of the subresultant and $\psi(\mathcal{J}) + S$ generating all polynomials of degree d for any specialization ψ. Both together will be used for the analysis of the generic Gröbner basis degree for graded monomial orderings.

Theorem 51 (Chardin, 1995)**.** *Let $F_1, \ldots, F_n$, $\mathcal{S}$, $\mathcal{K}$ and $\mathcal{J}$ be as defined above and $d_i = \deg(F_i)$. If T is a set of*

$$\dim_{\mathcal{K}}((\mathcal{S}[x_0, \ldots, x_n]/\mathcal{J})_{=d} \otimes \mathcal{K}) + 1$$

monomials of degree d then

$$\sum_{x^\alpha \in T} \varepsilon_{\alpha,T} \Delta_{T \setminus \{x^\alpha\}} x^\alpha \in \mathcal{J}$$

for some $\varepsilon_{\alpha,T} \in \{-1, 1\}$.

Proof. If T doesn't contain a basis of $(H_0 \otimes \mathcal{K})_{=d}$, the claim is trivial since all subresultants are zero-polynomials.

For this lemma the determinant of $\varphi_1^{T \setminus \{x^\alpha\}}$ will be developed using the Laplace expansion. Let

$$\mathcal{N}_{=d} := \left\{ x^\alpha e_i : \alpha \in \mathbb{Z}_{\geq 0}^{n+1}, 1 \leq i \leq n, \deg(x^\alpha e_i) = d, \alpha_j < d_j \forall j < i \right\}$$

and $W_{=d} := \operatorname{span}_{\mathcal{S}}(\mathcal{N}_{=d}) \subset (\Lambda_1)_{=d}$. Consider the matrix M of the linear map

$$\varphi_1^{T \setminus \{x^\alpha\}} : W_{=d} \longrightarrow (\Lambda_0 / \operatorname{span}_{\mathcal{S}}(T \setminus \{x^\alpha\}))_{=d}, y \mapsto [\delta_1(y)]$$

with respect to the bases $\mathcal{N}_{=d}$ of $W_{=d}$ and

$$B_0 := \left\{[x^\alpha] \notin T : \alpha \in \mathbb{Z}_{\geq 0}^{n+1}, \deg(x^\alpha) = d\right\}$$

of $(\Lambda_0/\operatorname{span}_{\mathcal{S}}(T))_{=d}$. To see that $\varphi_1^{T\setminus x^\alpha} \otimes \mathrm{id}$ is bijective, it suffices to consider a specialization, namely $\psi(F_i) := x_i^{d_i}$. For $d > \max\{d_i : i = 1, \ldots, n\}$ this is obvious from the construction of $\mathcal{N}_{=d}$. Therefore $\mathcal{N}_{=d}$ is a possible choice for B_1' in the decomposition of the complex.

Since $\varphi_1^{T\setminus\{x^\alpha\}} \otimes \mathrm{id}$ is bijective, its matrix is square and one can develop its determinant along the row corresponding to $[x^\alpha]$ using the Laplace expansion. This yields

$$\det\left(\phi_1^{T\setminus\{x^\alpha\}}\right) = \sum_{x^\beta e_i \in \mathcal{N}_{=d}} \sigma_{i,\beta,\alpha} c_{(i,\beta),\alpha} \det(M_{i,\beta})$$

for appropriate signs $\sigma_{i,\beta,\alpha} \in \{-1,+1\}$ and submatrices $M_{i,\beta}$ of M, in which the row corresponding to $[x^\alpha]$ and the column corresponding to $x^\beta e_i$ are deleted. $c_{(i,\beta),\alpha}$ is the coefficient of $[x^\alpha]$ in $\phi_1^{T\setminus\{x^\alpha\}}(x_\beta e_i)$. Note that, for fixed T, $M_{i,\beta}$ does not depend on the choice of $x^\alpha \in T$, since $M_{i,\beta}$ can also be viewed as the submatrix of the matrix of $\delta_1 : W_{=d} \longrightarrow (\Lambda_0)_{=d}$ in which all rows corresponding to monomials not contained in T and the column corresponding to $x^\beta e_i$ are deleted. Furthermore, the signs $\sigma_{i,\beta,\alpha}$ and $\sigma_{i,\beta,\alpha_0}$ in the developments of $\phi_1^{T\setminus\{x^\alpha\}}$ and $\phi_1^{T\setminus\{x^{\alpha_0}\}}$ only differ by a constant sign depending on T, α and α_0 (depending on whether the difference of their row indices is odd or even), which shall be called $\varepsilon_{\alpha,T} \in \{-1,1\}$. Then

$$\begin{aligned}\sum_{x^\alpha \in T} \varepsilon_{\alpha,T} \det\left(\phi_1^{T\setminus\{x^\alpha\}}\right) x^\alpha &= \sum_{x^\alpha \in T} \sum_{x^\beta e_i \in \mathcal{N}_{=d}} \varepsilon_{\alpha,T} \sigma_{i,\beta,\alpha} c_{(i,\beta),\alpha} \det(M_{i,\beta}) x^\alpha \\ &= \sum_{x^\alpha \in T} \sum_{x^\beta e_i \in \mathcal{N}_{=d}} \sigma_{i,\beta,\alpha_0} c_{(i,\beta),\alpha} \det(M_{i,\beta}) x^\alpha\end{aligned}$$

Now one can extend the sum over α to all monomials of degree d. The additional terms vanish since they correspond to expansions of determinants of matrices that contain one row twice.

$$\begin{aligned}
&= \sum_{\substack{\alpha\in\mathbb{Z}_{\geq 0}^{n+1}\\ |\alpha|=d}} \sum_{x^\beta e_i\in\mathcal{N}_{=d}} \sigma_{i,\beta,\alpha_0} c_{(i,\beta),\alpha} \det(M_{i,\beta}) x^\alpha \\
&= \sum_{x^\beta e_i\in\mathcal{N}_{=d}} \sigma_{i,\beta,\alpha_0} \det(M_{i,\beta}) \sum_{\substack{\alpha\in\mathbb{Z}_{\geq 0}^{n+1}\\ |\alpha|=d}} c_{(i,\beta),\alpha} x^\alpha \\
&= \sum_{x^\beta e_i\in\mathcal{N}_{=d}} \sigma_{i,\beta,\alpha_0} \det(M_{i,\beta}) \sum_{\substack{\alpha\in\mathbb{Z}_{\geq 0}^{n+1}\\ |\alpha|=d_i}} u_{\alpha,i} x^{\alpha+\beta} \\
&= \sum_{x^\beta e_i\in\mathcal{N}_{=d}} \sigma_{i,\beta,\alpha_0} \det(M_{i,\beta}) x^\beta F_i \in \mathcal{J}
\end{aligned}$$

On the other hand, one can rewrite

$$\mathcal{J} \ni \sum_{x^\alpha\in T} \varepsilon_{\alpha,T} \det\left(\phi_1^{T\setminus\{x^\alpha\}}\right) x^\alpha = \Delta_1 \sum_{x^\alpha\in T} \varepsilon_{\alpha,T} \Delta_{T\setminus\{x^\alpha\}} x^\alpha$$

By lemma 50, Δ_1 and $\Delta_{T\setminus\{x^\alpha\}}$ are polynomials. But since their degree in the variables $x_0, \ldots, x_n$ is zero and the ideal $\mathcal{J}$ is homogeneous, $\Delta_1 \notin \mathcal{J}$. According to lemma 48, $\mathcal{J}$ is prime. Thus

$$\sum_{x^\alpha\in T} \varepsilon_{\alpha,T} \Delta_{T\setminus\{x^\alpha\}} x^\alpha \in \mathcal{J}.$$

□

Corollary 52. *Let $F_1, \ldots, F_n$, $\mathcal{S}$, $\mathcal{K}$ and $\mathcal{J}$ be as defined above. If S is a set of*

$$\dim_{\mathcal{K}}((\mathcal{S}[x_0, \ldots, x_n]_{=d}/\mathcal{J}_{=d}) \otimes \mathcal{K})$$

monomials of degree d then for all monomials x^β of degree d that are not contained in S

$$g_\beta := \Delta_S x^\beta + \sum_{x^\alpha\in S} \varepsilon_{\alpha,S\cup\{x^\beta\}} \Delta_{S\cup\{x^\beta\}\setminus\{x^\alpha\}} x^\alpha \in \mathcal{J}$$

for some $\varepsilon_{\alpha,T} \in \{-1, 1\}$.

The second important property provides a tool to check whether $\psi(\mathcal{J}) + \operatorname{span}_{\mathbb{K}}(S)$ contains all polynomials of degree d.

Theorem 53 (Chardin, 1995)**.** *Let $F_1, \ldots, F_n$, $\mathcal{S}$, $\mathcal{K}$ and $\mathcal{J}$ be as defined above. If S is a set of*

$$\dim_{\mathcal{K}}((\mathcal{S}[x_0, \ldots, x_n]/\mathcal{J})_{=d} \otimes \mathcal{K})$$

monomials of degree d, then the following holds for any specialization $\psi : \mathcal{S}[x_0, \ldots, x_n] \longrightarrow \mathbb{K}[x_0, \ldots, x_n]$.

$$\psi(\Delta_S) \neq 0 \Longleftrightarrow \psi(\mathcal{J})_{=d} + \operatorname{span}_{\mathbb{K}}(S) = \mathbb{K}[x_0, \ldots, x_n]_{=d}$$

Proof. First assume $\psi(\Delta_S) \neq 0$. Then for all monomials $x^\beta \notin S$ of degree d the polynomial g_β defined in corollary 52 specializes to a monomial $\psi(g_\beta)$ that has a non-zero x^β coefficient. Therefore all such x^β are equivalent to polynomials that only contain the monomials in S modulo $\psi(\mathcal{J})$. So S generates $(\mathbb{K}[x_1, \ldots, x_n]/\psi(\mathcal{J}))_{=d}$ which implies $\psi(\mathcal{J})_{=d} + \operatorname{span}_{\mathbb{K}}(S) = \mathbb{K}[x_0, \ldots, x_n]_{=d}$.

On the other hand assume $\psi(\Delta_S) = 0$. Recall that Δ_S is independent of the decomposition by lemma 50. Now consider the linear map

$$\delta_1 : (\Lambda_1)_{=d} \longrightarrow (\Lambda_0)_{=d}.$$

Choosing a minor M, i.e. the determinant of a submatrix of the matrix representation of δ_1, is equivalent to choosing an set S' of monomials of degree d and considering the induced map $(\Lambda_1)_{=d} \longrightarrow (\Lambda_0)_{=d}/\operatorname{span}_{\mathcal{S}}(S')$. If the minor is non-zero and of size $\dim_{\mathcal{K}}(\mathcal{J} \otimes \mathcal{K})_{=d}$, S' generates $(H_0 \otimes \mathcal{K})_{=d}$. Thus one can extend this minor to a decomposition of the complex as seen before. This decomposition can be used to define $\Delta_{S'}$. Therefore $\Delta_{S'} = M \cdot \Delta_2$ with $\Delta_2 \in \mathcal{J}$ (lemma 50) and $\Delta_{S'}$ divides the minor M.

Now $\psi(\Delta_S) = 0$ implies that all minors M of δ_1 that induce the same set S specialize to zero. Thus $\psi(\delta_1^*)$ is not surjective, i.e.

$$\psi(\operatorname{im}(\delta_1^*)_{=d}) \neq (\mathbb{K}[x_0, \ldots, x_n]/S)_{=d}$$

$$\Rightarrow \psi(\mathcal{J})_{=d} + \operatorname{span}_{\mathbb{K}}(S) \neq \mathbb{K}[x_0, \ldots, x_n]_{=d}.$$

□

This finishes the summary of Chardin's paper. Now the multivariate subresultant Δ_S will be used to study the generic degree of Gröbner bases for graded monomial orderings.

Theorem 54. *Let $\mathbb{K}$ be an algebraically closed field and for $i = 1, \ldots, n$ define*

$$f_i := \sum_{\substack{\alpha \in \mathbb{Z}^n_{\geq 0} \\ |\alpha| \leq d_i}} u_{i,\alpha} x^\alpha \in \mathcal{R}[x_1, \ldots, x_n]$$

where

$$\mathcal{R} := \mathbb{Z}[u_{i,\alpha} : i = 1, \ldots, n, \alpha \in \mathbb{Z}^n_{\geq 0}, |\alpha| \leq d_i].$$

Let $\psi : \mathcal{R}[x_1, \ldots, x_n] \longrightarrow \mathbb{K}[x_1, \ldots, x_n]$ denote a specialization and assume that the ideal $I = \langle \psi(f_1), \ldots, \psi(f_n) \rangle$ is zero-dimensional in $\mathbb{K}[x_1, \ldots, x_n]$. Then the reduced Gröbner basis G of I generically fulfills

$$\max\{\deg(g) : g \in G\} = (d_1 - 1) + \ldots + (d_n - 1) + 1.$$

Proof. To apply the multivariate subresultant theory, it is necessary to consider the homogenizations $F_i = {}^h f_i$ for $i = 1, \ldots, n$. This homogenization shows that the rings $\mathcal{R}$ an $\mathcal{S}$ are essentially the same, so one can view F_i as elements of $\mathcal{S}[x_0, \ldots, x_n]$ and ψ as specialization $\mathcal{S}[x_0, \ldots, x_n] \longrightarrow \mathbb{K}[x_0, \ldots, x_n]$.

First consider the specialization defined by

$$\begin{aligned}
\psi(F_1) &:= x_1 x_2^{d_1 - 1} + x_2^{d_1} \\
\psi(F_2) &:= x_2 x_3^{d_2 - 1} + x_3^{d_2} \\
&\vdots \\
\psi(F_{n-1}) &:= x_{n-1} x_n^{d_{n-1} - 1} + x_n^{d_{n-1}} \\
\psi(F_n) &:= x_1^{d_n}
\end{aligned}$$

Remember that this is the ideal from example 34, but over the ring $\mathbb{K}[x_0, \ldots, x_n]$. These polynomials $\psi(F_1), \ldots, \psi(F_n)$ generate an homogeneous zero-dimensional ideal $\psi(\mathcal{J})$. Let $D := (d_1 - 1) + \ldots + (d_n - 1)$ and S be the set of all with respect to $\psi(\mathcal{J})$ irreducible monomials of degree D. First the cardinality of S has to be checked. Since S is a basis of $(\mathbb{K}[x_0, \ldots, x_n]/\psi(\mathcal{J}))_{=D}$, it suffices to show

$$\dim_{\mathcal{K}}((\mathcal{S} \otimes \mathcal{K})/(\mathcal{J} \otimes \mathcal{K}))_{=D} = \dim_{\mathbb{K}}(\mathbb{K}[x_0, \ldots, x_n]/\psi(\mathcal{J}))_{=D}$$

or equivalently

$$\dim_{\mathcal{K}}(\mathcal{J} \otimes \mathcal{K})_{=D} = \dim_{\mathbb{K}}(\psi(\mathcal{J})_{=D}).$$

Lemma 47 implies

$$\dim_{\mathcal{K}}(\mathcal{J} \otimes \mathcal{K})_{=d} \geq \dim_{\mathbb{K}}(\psi(\mathcal{J})_{=d}) \tag{3.9}$$

for any specialization since $\mathcal{J}$ is the image of δ_1. For the opposite inequality, let $\mathcal{J}_1 := \langle F_n \rangle$ and, for $k = 2, \dots, n$, $\mathcal{J}_k := \langle F_n, F_1, \dots, F_{k-1} \rangle$. The idea is to prove by induction on k that

$$\dim_{\mathcal{K}}(\mathcal{J}_k \otimes \mathcal{K})_{=d} = \dim_{\mathbb{K}}(\psi(\mathcal{J}_k)_{=d}).$$

The claim is obvious for $k = 1$. So assume $k > 1$ and use $\mathcal{J}_k = \mathcal{J}_{k-1} + \langle F_{k-1} \rangle$ and $\psi(\mathcal{J}_k) = \psi(\mathcal{J}_{k-1}) + \psi(\langle F_{k-1} \rangle)$. The dimensions of these vector spaces can be calculated using

$$\begin{aligned} \dim_{\mathcal{K}}(\mathcal{J}_k \otimes \mathcal{K})_{=d} &= \dim_{\mathcal{K}}((\mathcal{J}_{k-1} \otimes \mathcal{K})_{=d} + (\langle F_{k-1} \rangle \otimes \mathcal{K})_{=d}) \\ &= \dim_{\mathcal{K}}(\mathcal{J}_{k-1} \otimes \mathcal{K})_{=d} + \dim_{\mathcal{K}}(\langle F_{k-1} \rangle \otimes \mathcal{K})_{=d} \\ &\quad - \dim_{\mathcal{K}}(\mathcal{J}_{k-1} \otimes \mathcal{K})_{=d} \cap (\langle F_{k-1} \rangle \otimes \mathcal{K})_{=d} \end{aligned} \tag{3.10}$$

respectively

$$\begin{aligned} \dim_{\mathbb{K}}(\psi(\mathcal{J}_k)_{=d}) &= \dim_{\mathbb{K}}(\psi(\mathcal{J}_{k-1})_{=d} + \psi(\langle F_{k-1} \rangle)_{=d}) \\ &= \dim_{\mathbb{K}}(\psi(\mathcal{J}_{k-1})_{=d}) + \dim_{\mathbb{K}}(\psi(\langle F_{k-1} \rangle)_{=d}) \\ &\quad - \dim_{\mathbb{K}}(\psi(\mathcal{J}_{k-1})_{=d} \cap \psi(\langle F_{k-1} \rangle)_{=d}). \end{aligned} \tag{3.11}$$

All terms on the right-hand sides of (3.10) and (3.11) but the dimensions of the ideal intersections are equal by induction hypothesis. For all ideals I, J, $I \cdot J \subset I \cap J$ is true. Now

$$\psi(F_{k-1}) \cdot \psi(\mathcal{J}_{k-1}) = \psi(\mathcal{J}_{k-1}) \cap \langle \psi(F_{k-1}) \rangle$$

is clear since F_{k-1} contains the variable x_k which is not contained in $F_n, F_1, \dots, F_{k-2}$. Thus

$$\dim_{\mathbb{K}}(\psi(F_{k-1}) \cdot \psi(\mathcal{J}_{k-1}))_{=d} = \dim_{\mathbb{K}}(\psi(\mathcal{J}_{k-1})_{=d} \cap \langle \psi(F_{k-1}) \rangle_{=d}).$$

On the other hand,

$$\dim_{\mathbb{K}}(\psi(F_{k-1}) \cdot \psi(\mathcal{J}_{k-1}))_{=d} = \dim_{\mathcal{K}}(F_{k-1} \cdot \mathcal{J}_{k-1} \otimes \mathcal{K})_{=d}$$

and

$$\dim_{\mathcal{K}}(F_{k-1} \cdot \mathcal{J}_{k-1} \otimes \mathcal{K})_{=d} \leq \dim_{\mathcal{K}}(\mathcal{J}_{k-1} \otimes \mathcal{K})_{=d} \cap (\langle F_{k-1} \rangle \otimes \mathcal{K})_{=d}$$

which imply, together with the former proved inequality (3.9),

$$\dim_{\mathcal{K}}(\mathcal{J}_k \otimes \mathcal{K})_{=d} = \dim_{\mathbb{K}}(\psi(\mathcal{J}_k)_{=d}).$$

So S has by definition the right cardinality and theorem 53 can be applied. According to example 34, where an explicit Gröbner basis was given, the only monomial in S that is not divisible by x_0, is x_n^D. Furthermore S contains all monomials $x_0^k x_n^{D-k}$ $(k = 0, \ldots, D)$. Now thoerem 53 implies that the specialization of the corresponding subresultant $\psi(\Delta_S) \neq 0$. Thus Δ_S is not the zero-polynomial.

Assume $\psi(\Delta_S) \neq 0$. This is obviously a generic situation. The polynomials $\psi(g_\beta)$ defined in corollary 52 are contained in $\psi(\mathcal{J})$. Consider their dehomogenizations by $x_0 = 1$ and denote them by g'_β. Then $g'_\beta \in I$ and $\mathrm{LM}(g'_\beta) = x^\beta$ since this is the only monomial in S whose degree doesn't decrease on dehomogenization. Since specialization of $\mathcal{J}_{=D}$ to $\psi(\mathcal{J})$ only could decrease the dimension as seen before,

$$\dim_{\mathcal{K}}(\mathcal{S}[x_0, \ldots, x_n]/\mathcal{J}) \otimes \mathcal{K} \geq \dim_{\mathbb{K}}(\mathbb{K}[x_0, \ldots, x_n]/\psi(\mathcal{J})).$$

Now theorem 53 implies that S generates $\mathbb{K}[x_0, \ldots, x_n]/\psi(\mathcal{J})$ which implies the opposite inequality and therefore

$$\#S = \dim_{\mathcal{K}}(\mathcal{S}[x_0, \ldots, x_n]/\mathcal{J}) \otimes \mathcal{K} = \dim_{\mathbb{K}}(\mathbb{K}[x_0, \ldots, x_n]/\psi(\mathcal{J})).$$

So the monomials in S are independent modulo $\psi(\mathcal{J})$, i.e. $\langle S \rangle \cup \psi(\mathcal{J}) = \{0\}$. If x_n^k was reducible with respect to $\psi(\mathcal{J})$ for some $k \in \{0, \ldots, D\}$, there would be a polynomial

$$x_n^k - \sum_{x_n^k \neq x^\alpha \in S} c_\alpha x^\alpha \in \psi(\mathcal{J}) \text{ for some } c_\alpha \in \mathbb{K}$$

since all not in this polynomial appearing monomials can be expressed in terms of monomials in S modulo $\psi(\mathcal{J})$. But the existence of this monomial contradicts the independence of the monomials in S. Thus x_n^D, the smallest monomial of degree D, is irreducible with respect to I. But I is zero-dimensional, so by theorem 19 any Gröbner basis contains a polynomial with leading term x_n^d for some $d > D$. Together with theorem 46, one obtains $d = D + 1$ and the claim

$$\max\{\deg(g) : g \in G\} = D + 1 = (d_1 - 1) + \ldots + (d_n - 1) + 1.$$

□

Example 55. Lastly an explicit example will be given, where S can easily be computed. Consider the case of three polynomials in the degrees $d_1 = 3, d_2 = 2, d_3 = 2$. Then the specialization given in the theorem is

$$\begin{aligned} \psi(F_1) &:= x_1x_2^2 + x_2^3 \\ \psi(F_2) &:= x_2x_3 + x_3^2 \\ \psi(F_3) &:= x_1^2 \end{aligned}$$

and a Gröbner basis is

$$\begin{aligned} g_1 &:= x_1x_2^2 + x_2^3 \\ g_2 &:= x_2x_3 + x_3^2 \\ g_3 &:= x_1^2 \\ g_4 &:= x_1x_3^3 - x_3^4 \\ g_5 &:= x_2^4 \\ g_6 &:= x_3^5. \end{aligned}$$

So the irreducible monomials in degree $D = 4$ are

$$S := \{x_0^4, x_0^3x_1, x_0^3x_2, x_0^3x_3, x_0^2x_1x_2, x_0^2x_2^2, x_0^2x_1x_3, x_0^2x_3^2, x_0x_2^3, x_0x_1x_3^2, x_0x_3^3, x_3^4\}.$$

Those monomials generate $(\mathbb{K}[x_0, \ldots, x_n]/\psi(\mathcal{J}))_{=4}$ and thus, as seen in the last theorem, $(\mathcal{K}[x_0, \ldots, x_n]/(\mathcal{J} \otimes \mathcal{K}))_{=4}$.

3.4 Summary

First general upper and lower degree bounds due to Dubé and Möller, Mora (building on an example by Mayr, Meyer) were presented. Both upper and lower bounds were essentially doubly exponentially with the degree of the generators in the base and the number of variables in the second exponent. This growth is immense and perhibits explicit computations in the worst cases already for quite low numbers of variables even with fast computers.

Henceforth a special case arising from applications was studied, namely if the polynomial systems have only finitely many solutions, i.e. the generated ideals are of dimension zero. Here two groups of monomial orderings were studied.

For the lexicographic ordering upper and lower bound were proved to be singly exponentially, again with the generator degree in the base and the number of variables in the exponent. Moreover, upper and lower bound exactly match and are obtained in the generic case. These results are folklore, the last one is commonly known as Shape Lemma.

Finally, graded monomial orderings were studies. Again matching upper and lower bounds were proved, this time polynomially (roughly the product of number of variables and the degree of the generators). As for the lexicographic ordering, the generic degree of the Gröbner basis coincides with the upper bound. The upper bound was due to Lazard, the lower bound folklore and the generic degree was not known to the author before.

So Gröbner bases for zero-dimensional ideals are much more well behaved than for arbitrary dimensions. Since the ideals considered by Möller and Mora for the lower bound are of very high dimension, the author ask whether there is an gradual transition. This demands upper and lower degree bounds that depend on the ideal dimension as parameter.

Bibliography

[1] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* PhD thesis, Universität Innsbruck, 1965.

[2] B. Buchberger. An algorithm for finding the basis elements in the residue class ring modulo a zero dimensional polynomial ideal. *Journal of Symbolic Computation*, 41(3-4):475–511, 2006.

[3] B. Buchberger. *Gröbner-Bases: An Algorithmic Method in Polynomial Ideal Theory.* Reidel Publishing Company, Dodrecht - Boston - Lancaster, 1985.

[4] B. Buchberger. Gröbner bases and systems theory. *Multidimensional systems and Signal processing*, 12(3):223–251, 2001.

[5] E.W. Mayr and A.R. Meyer. The complexity of the word problems for commutative semigroups and polynomial ideals. *Advances in Mathematics*, 46(3):305–329, 1982.

[6] K. Kühnle and E.W. Mayr. Exponential space computation of Gröbner bases. In *Proceedings of the 1996 international symposium on Symbolic and algebraic computation*, pages 63–71. ACM New York, NY, USA, 1996.

[7] D. Lazard. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In *Proc. EUROCAL*, volume 83, pages 146–156. Springer, 1983.

[8] D. Lazard. Resolution des systemes d'equations algebriques. Theor. Comp. *Sciences*, 15:77–110, 1981.

[9] D. Lazard. Solving systems of algebraic equations. *ACM SIGSAM Bulletin*, 35(3):11–37, 2001.

[10] M. Chardin. Multivariate subresultants. *Journal of Pure and Applied Algebra*, 101(2):129–138, 1995.

[11] K. Hägglöf, PO Lindberg, and L. Svensson. Computing global minima to polynomial optimization problems using Gröbner bases. *Journal of Global Optimization*, 7(2):115–125, 1995.

[12] D.A. Cox, J.B. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms.* Springer New York, 1992.

[13] D. Eisenbud. *Commutative algebra with a view toward algebraic geometry.* Springer, 1995.

[14] F. Rouillier. Solving Zero-Dimensional Systems Through the Rational Univariate Representation. *Applicable Algebra in Engineering, Communication and Computing*, 9(5):433–461, 1999.

[15] M. Giusti and J. Heintz. Algorithmes-disons rapides-pour la decomposition d'une variete algebrique en composantes irreductibles et equidimensionnelles.

[16] G.-M. Greuel, G. Pfister, and H. Schönemann. SINGULAR 3.1.0 — A computer algebra system for polynomial computations. 2009. http://www.singular.uni-kl.de.

[17] T.W. Dubé. The Structure of Polynomial Ideals and Gröbner Bases. *SIAM Journal on Computing*, 19:750, 1990.

[18] H.M. Möller and F. Mora. *Upper and Lower Bounds for the Degree of Groebner Bases.* Springer-Verlag London, UK, 1984.

[19] I.R. Shafarevich. *Basic Algebraic Geometry.* Springer-Verlag, 1994.

[20] M. Giusti. Combinatorial dimension theory of algebraic varieties. *Journal of symbolic computation*, 6(2-3):249–265, 1988.

[21] D.A. Cox, J.B. Little, and D. O'Shea. *Using Algebraic Geometry.* Springer Verlag, 2005.

[22] J. Canny. *The Complexity of Robot Motion Planning.* MIT Press, 1988.

[23] JP Jouanolou. ldeaux Resultants. *Advances in Mathematics*, 37:212–238, 1965.

[24] M. Chardin. The resultant via a Koszul complex. *Computational Algebraic Geometry*, 109:29–39, 1993.