JOHANNES KEPLER
UNIVERSITÄT LINZ
JKU

TNF
Technisch-Naturwissenschaftliche
Fakultät

Dual Space Algorithms for Computing Multiplicity Structure of Isolated Points

DISSERTATION

zur Erlangung des akademischen Grades

Doktor der Technischen Wissenschaften

im Doktoratsstudium der

Technischen Wissenschaften

Eingereicht von:
Hamid Rahkooy

Angefertigt am:
Research Institute for Symbolic Computation

Beurteilung:
Prof. Bruno Buchberger
Dr. Nikolay Vasilyev

Linz, July 2015

I hereby declare under oath that the submitted doctoral dissertation has been written solely by me without any outside assistance, information other than provided sources or aids have not been used and those used have been fully documented. The dissertation here present is identical to the electronically transmitted text document.

Ich erkläre an Eides statt, dass ich die vorliegende Dissertation selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt bzw. die wörtlich oder sinngemäß entnommenen Stellen als solche kenntlich gemacht habe. Die vorliegende Dissertation ist mit dem elektronisch übermittelten Textdokument identisch.

Contents

Abstract

Dual space of a primary ideal associated to an isolated point is a major topic of study in computational algebraic geometry with applications in many fields, for example in tensor decomposition and arrangements of planar curves. We study the basis computation for these dual spaces. Such a basis indicates the multiplicity structure of the point under study.

Macaulay's algorithm is the classic algorithm for computing such a basis which is still in use. However it is not the most efficient algorithm due to large matrix constructions and repetition of computation. There are several improvements on Macaulay's algorithm. Mourrain's integration method serves as the most advanced algorithm which constructs much smaller matrices. These algorithms are incremental. They compute a basis for the dual space degree by degree, via computing the kernel of a certain matrix at each step. An improvement on the integration method has been provided by Mourrain and Mantzaflaris which avoids repeated computations.

In this thesis, we give another improvement for the integration method by reducing the size of the matrices. Similar to the Mourrain-Mantzaflaris' improvement, our improvement avoids repeating many computations.

Mourrain-Mantzaflaris' method, while avoiding repetition of computations, goes by adding new rows to the matrix at each step of the algorithm. Our method on the other hand makes advancements, by removing some columns, hence reducing the size of the matrix and consequently the size of the computations. We show that a similar improvement can be applied to Macaulay's algorithm as well, reducing the size of the matrices as much as possible. We also introduce the notion of *directional multiplicity*, which has applications in studying degeneracy in elimination in many problems, in particular in arrangements of planar curves.

Acknowledgment

My deepest thanks to Bruno Buchberger for advising me through my PhD studies.

Here is a small but valuable group of friends that made life bearable for me in the castle: Jakob, Manuela, Max, Zapf, Angelos and Ilse.

Official Acknowledgment. The research was funded by the Austrian Science Fund (FWF): W1214-N15, project DK1 and it was supported by the strategic program "Innovatives OÖ 2010 plus" by the Upper Austrian Government. The author has been supported by the Austrian Marshall Plan Foundation for his stay in UC Berkeley and by the DeVMath scholarship of the Centre Recerca de Matemàtica in Bellaterra, Barcelona.

Chapter 1

Introduction

1.1 Problem, Previous Work and Contribution

The Problem

Consider an isolated point in the variety of a given ideal and its associated primary component. The quotient of the polynomial ring modulo this associated primary ideal is a vector space, whose dimension is the multiplicity of the point. A basis for the quotient and therefore the multiplicity can be computed via Gröbner basis.

It is classically known that the dual space of the polynomial ring is isomorphic to the space of differential operators. This space is in general infinite dimensional. However, the dual space of a primary ideal is a finite dimensional subspace and can be computed. In fact, the dimension of this subspace is the multiplicity of the point. Having the dual space of this subspace, a Gröbner basis of the primary component can be obtained from it. Computing a basis for this dual space is the main problem of this thesis.

Considering the differential operators as polynomials, there is a bound on the degree of the monomials of such polynomials, the so called Nil-index. The existence of this bound allows us to search for a basis incrementally, i.e., degree by degree, among the monomials with degree at most Nil-index. In fact a basis can be found among the linear combination of such monomials. Assigning symbolic coefficients for those monomials and applying some necessary and sufficient conditions that the differential operators must satisfy, we obtain a matrix whose kernel gives us the values of the coefficients.

This argument reduces the problem into the kernel computation problem in some specific matrices. Because of the structure of the matrices that are constructed at each step of the procedure, they can be very large and also there are repeated and redundant computations. The problem of making improvements via constructing smaller matrices and efficient computations is at the heart of this thesis.

It turns out that a basis for the dual space captures more information than a Gröbner basis for the primary component. The dual space shows us the local multiplicity structure, which provides us with information on the geometry of isolated points. The multiplicity structure plays an essential role in several problems related to multiplicity and elimination, which can be treated via directional multiplicities that will be introduced in this work. The motivation for this work stems from our earlier investigation on using resultants in Gröbner basis computation. The idea was to project a given ideal by resultants and then use it as an element in the elimination ideal in order to facilitate computing a Gröbner basis. This problem lead us to the multiplicity problem in the elimination ideal of two affine algebraic planar curves. Directional multiplicity can be used to study the geometric properties of a point and our motivational problem.

Previous Work

Multiplicity structure of isolated points has been well studied in literature [27, 46, 63, 58, 47] and it is an active research field and there are recent articles on the topic, e.g. [41]. There are efficient linear algebra algorithms to compute the multiplicity structure via dual space. A historical work conducted by Macaulay [46] shows how to construct the simplest matrices in order to compute a basis for the dual space. This algorithm is still used widely and several improvements have been made that make Macaulay's algorithm faster. Wu and Zhi worked on a symbolic-numeric method for computing the primary components and the differential operators [62], which is based on an algorithm for determining the dual space that is mentioned in the book [58] by Stetter. In [63] Zeng used the ideas in Stetter's algorithm and introduced his closedness property in order to make Macaulay's matrices smaller. Mourrain gave a new algorithm based on integration in [53], which is more efficient than the algorithm of Macaulay in terms of the size of the matrices. This algorithm was improved by Mantzaflaris and Mourrain in [47] adding a new criterion. A detailed review of the integration method and how it works in relation with deflation methods is given in [48]

Marinari, Mora and Möller's work on dual spaces in [49, 50], includes studying the behaviour of the dual space under the projection, which is the base of our result on using dual elements to study the elimination ideal. A survey on dual spaces, including Marinari, Mora and Möller's main results, is given in the book by Elkadi and Mourrain [27]. Also Bates, Peterson and Sommese have worked on the multiplicity of the primary components [5]. Li and Zhi's have investigated computing the Nil-index [45]. Examining the multiplicity structure via deflation is exhibited in the work of Dayton and Zeng [24] and Leykin and Verschelde [44].

Out motivational ideas for using resultants in Gröbner basis computation is described in [24], which considers Elimination problem, independent of the dual computation. Polynomials elimination theory is an old and central topic. Gröbner has an article on this topic [35]. Two main tools in elimination theory are Gröbner Bases and resultants. Buchberger introduced and expanded the Gröbner basis concept and gave an algorithm for Gröbner bases computation in his PhD thesis [10, 11]. Gröbner bases initiated a field of study in computational commutative algebra and algebraic geometry. The applications of Gröbner bases are countless both in theoretical as well as practical problems, when dealing with algebraic systems. Apart from the application of Gröbner bases in computing the multiplicity, we will extensively use its elimination property [11] that allows computing the elimination ideals.

Buchberger's algorithm is a critical pair comparison algorithm. There are other techniques to improve Gröbner basis computation. Among them are those that use linear algebra techniques to speed up the procedure, e.g. Faugère's F4 [29], MXL3 [52] and their comparison with each other [4]. Following Buchberger's idea in [12] on using Guassian elimination on a generalized Sylvester matrix, Gaussian triangularization and taking the so called "contour" in the diagonal elements in order to compute a Gröbner basis, Wiesinger-Widi in [61] found an upper bound for such a matirx. This has been presented in [14] and is a recent work connecting Gröbner basis to resultants. Signature Based techniques avoid major (or all in some cases) of the zero reductions, e.g. [30], [33], [34] and [25]. Computing Gröbner Bases can be very expensive. It has been shown by Mayr and Meyer that the complexity of computing Gröbner basis is doubly exponential [51]. However, there are faster methods for special cases that are of high interest. One such case is zero dimensional ideals, for which the complexity is single exponential [42]. Also as the complexity changes by change of the order, Faugere, Gianni, Lazard and Mora gave an algorithm to change a Gröbner basis computed with respect to an arbitrary order into a Gröbner basis with respect to a different order in the zero dimensional case [31]. This algorithm has been inspired by a work of Buchberger and Möller [16] which computes a Gröbner basis for a zero dimensional ideal with given zeros.

Resultants is a classic tool in elimination theory. It has been extensively studied by Sylvester, Bezout, Dixon, Macaulay and van der Waerden [59, 60]. A smooth introduction to resultants, including Sylvester and Macaulay resultants is given in [20] and [21]. A survey on computational methods is given in [28], and a modern view towards the topic is [38].

Our Contribution

The main contributions of this work are improvements to the integration method and Macaulay's algorithm. As the size of the matrices constructed in each step of the algorithms is the main obstacle in computations, we propose criteria that allow deleting some columns from the matrices in order to reduce the size of the matrices.

For the integration method, the state of art algorithm, in Proposition 9 we give an explicit generalization of Mourrain-Mantzaflaris' improvement in [47], as we detect and use a polynomial basis for the quotient rather than the monomial basis in the Mourrain-Mantzaflaris' improvement. It give s a generalization of Proposition 3.7 in [53] too. Corollary 76 shows our criterion for deleting some columns such that the kernel of the new matrix only detects new members of a basis of the dual space, which avoids recomputing the lower degree basis elements that are obtained in the previous steps. Although Mourrain and Mantzaflaris' improvement in [47] gives the same output, however it adds new rows to the matrix and in this sense our improvement is stronger.

For Macaulay's algorithm, we propose two criteria, each reducing the size of the matrices at each step drastically. First we show Criterion 79 similar to the one for the integration method that deletes some columns at each step so that we do not recompute the previously computed basis elements. Also using the properties of the dual space, we show Criterion 12 that predicts that some columns will not appear in the basis. These criteria will reduce the size of the Macaulay matrices so that it becomes the closest possible to the matrices of the integration method, meaning that for a matrix constructed in a fixed step of Macaulay's algorithm, each column of the matrix is used to be added to other columns in order to form the matrix in the integration method.

Apart from those criteria that can be used for computing the whole dual basis, we introduce directional multiplicity in Definition 60, which can give us more information than the Nil-index, a classic invariant which has been the topic of various studies in the multiplicity structure field. Our modified algorithms can be used to compute the directional multiplicity often faster than the whole dual space.

An interesting interplay between the directional multiplicity and the degree of the elimination ideal is presented. As an application, in studying arrangements and topology of curves one can use directional multiplicities in order to project the extreme point of a curve.

Structure of the Thesis

In the first chapter, after introducing the problem and literature work, we will present the preliminaries from Gröbner Bases, resultants, algebraic geometry and elimination theory.

In Chapter 2 we explain our motivation to study the multiplicity structure. It contains our initial problem on studying and comparing the elimination ideal and the resultant for two $n-$dimensional curves. After a short discussion on the dimension of the varieties, we focus on the case of two algebraic curves in dimension two. We investigate the difference between the resultant and the generator of the elimination ideal and see that the problem is reduced to the multiplicity problem . We show several examples and discuss the multiplicity problem and degeneracy in elimination.

Chapter 3 includes our main results. In this chapter , we first give a short introduction to dual spaces of polynomial rings. Then we focus on the multiplicity structure of an isolated point. In this way, we introduce directional multiplicity and the extended Buchberger diagram. We show bounds on the directional multiplicities with respect to Nil-index and the intersection multiplicity. In Section 3.3, after demonstrating the existing algorithms for computing the dual space, we show our improvements on those algorithms and discuss the advantages.

Chapter 4 contains two sections. In Section 4.1 we briefly show some applications of directional multiplicities in computational problems. Section 4.2 includes the main problems that we are considering as the future directions of research.

For the rest of the current chapter, we provide the necessary definitions, fix notation and present some theorems from the literature that we will use in what follows. The notation introduced in this chapter will be consistently used for the whole of the thesis, unless otherwise is clearly stated.

1.2 Preliminaries

1.2.1 Gröbner Bases

We introduce the basis definitions in Gröbner basis theory here. The fundamental notions and results are invented and given by Buchberger in his PhD thesis and later article as the primary, original literature in [10, 11]. We use the terminology and formulations of some later papers, e.g. text books by Becker, Kredel and Weispfenning [7] and Cox, Little and O'Shea [20].
We work on the ring of polynomials with n variables over an algebraically closed field $\mathbb{K}$, which will be denoted by $R = \mathbb{K}[x_1, \ldots, x_n]$. This ring is known to be *Noetherian* and therefore its ideals are finitely generated. Each polynomial in this ring is a some of *terms*, which are the multiplication of coefficients with *monomials*. One can put orders on the monomials in R.

Definition 1 (Term Order, [7]). *A total order $\prec$ on the monomials of R is called an admissible order or a term order if $\prec$ satisfies the following conditions.*

- $1 \prec m$ *for every nonzero monomial* m
- *If* $m_1 \prec m_2$*, then for every nonzero monomials* m*,* $mm_1 \prec mm_2$*.*

An example of such a term order is the *lexicographic order*, in which $x_n \prec x_{n-1} \prec \ldots \prec x_1$ and $x_1^{\alpha_1} \ldots x_n^{\alpha_n} \prec x_1^{\beta_1} \ldots x_n^{\beta_n}$ if and only if the first nonzero coordinate of $(\beta_1 - \alpha_1, \cdots, \beta_n - \alpha_n)$ is positive.
Bayer and Stillman in [6] considered a special sort of term orders which is very useful in studying elimination. We will show this below.

Definition 2 (Elimination Order, [20]). *A term order is called an elimination order if one can partition the variables into two sets A_1 and A_2 such that if a monomial m_1 contains variables only in A_1 and a monomial m_2 contains variables only in A_2, then $m_1 \prec m_2$.*

Lexicographic ordering is an elimination ordering. Another interesting term order is the degree lexicographic ordering, in which $x_1^{\alpha_1} \ldots x_n^{\alpha_n} \prec x_1^{\beta_1} \ldots x_n^{\beta_n}$ if and only if either $\sum_{i=1}^{n} \alpha_i < \sum_{j=1}^{n} \beta_j$ or $\sum_{i=1}^{n} \alpha_i = \sum_{j=1}^{n} \beta_j$ and the first nonzero coordinate of $(\beta_1 - \alpha_1, \cdots, \beta_n - \alpha_n)$ is positive. There are infinitely many term orders. having a term order on monomials, one can impose the same order on terms, ignoring their coefficients. Having a term order for the monomials in R, one can write a polynomial in such a way that the first term is bigger than the second one, the second term is bigger than the third one and so on. For a polynomial $f \in R$, $lt(f)$, the leading term of f is defined to be the biggest term in f. leading monomial of f, $lm(f)$ is defined similarly for monomials.

Definition 3 (Gröbner Bases, [20]). *A Gröbner basis G for an ideal I with respect to a term order $\prec$ is a basis for I,such that $\mathrm{lm}_\prec(G) = \mathrm{lm}_\prec(I)$, where $\mathrm{lm}_\prec(G)$ and $\mathrm{lm}_\prec(I)$ are the ideals generated by the leading monomials of g and I, respectively.*

Definition 4 (S-polynomial, [20]). *Given $f_1, f_2 \in \mathbb{K}[x_1, \ldots, x_n]$, we define S_{12}, the S-polynomial of f_1 and f_2, as:*

$$S_{12} = \frac{\operatorname{lcm}(\operatorname{lt}(f_1), \operatorname{lt}(f_2))}{\operatorname{lt}(f_1)} f_1 - \frac{\operatorname{lcm}(\operatorname{lt}(f_1), \operatorname{lt}(f_2))}{\operatorname{lt}(f_2)} f_2,$$

where lcm *stand for the least common multiple.*

Definition 5 (Reduction, [7]). *Let $\prec$ be a term order. For two polynomials $f_1, f_2 \in R$, f_1 is called reducible with respect to f_2 if $lt(f_2)|lt(f_2)$. If f_1 is reducible with respect to f_2, then reducing f_1 with respect to f_2 is the subtraction $f_1 - \frac{lc(f_2)}{lc(f_1)} lt(f_2)$, where $lc(f_i)$ is the leading coefficient, i.e., the coefficient of $lt(f_i)$, $1 \leqslant i \leqslant 2$.*

The above definition of Gröbner basis is not constructive. However there's a well-known algorithm by Buchberger which computes a Gröbner basis of an ideal. The Buchberger algorithm works as follows. Let $I = \langle G \rangle$, where $G = \{f_1, \ldots, f_m\}$, i.e., G is a basis for I. For every pair $1 \leqslant i < j \leqslant m$, compute S_{ij}, the S-polynomial of f_i and f_j. If S_{ij} is neither zero nor reducible with respect to any member of G, then add it to G. Otherwise, reduce it with respect to the other members of G until it is not reducible anymore. If it is not zero then add it to G. Buchberger proved in his PhD thesis that the above algorithm terminates and produces a Gröbner basis for I [10] .

Gröbner basis of an ideal with respect to a fixed term order is not unique, however reduced Gröbner basis is unique.

Definition 6 (Reduced Gröbner basis, [7]). *For a given ideal I, a Gröbner basis G with respect to an order $\prec$ is called reduced, if every element of G is monic and for every $f_1, f_2 \in G$, f_1 is not reducible with respect to f_2.*

Theorem 7 ([7]). *For every given ideal I in a polynomial ring and for every given term order $\prec$, there exits a uniqe reduced Gröbner basis for I with respect to $\prec$.*

Buchberger introduced the diagram shown in Figure 1.1, called the staircase or the Buchberger diagram, which gives a good intuition about a Gröbner basis and also the Buchberger algorithm. Having a Gröbner basis G computed for an ideal I with respect to a term order, consider the exponents of the leading monomials of G and attach a point in $\mathbb{R}^n$ for each exponent. In Figure 1.1, the blue points correspond to the leading terms and the green diagram is the staircase of the Buchberger diagram.

Gröbner basis has a lot of properties and applications. We mention a few of them that are used in this thesis. The first application that is at the heart of this thesis is the following.

Theorem 8 (Basis for ${}^{R}/_{I}$, [20]). *Let G be a Gröbner basis for the ideal I. Then the monomials under the staircase obtained via G form a basis for ${}^{R}/_{I}$ as a $\mathbb{K}-$vector space.*

Another property of Gröbner bases that will be used very often in this thesis is the *Elimination Property*. In order to explain the elimination property, we need to introduce elimination ideal and some notation.

The following definition is taken from [20], however we have changed the notation for simplifying future statements.

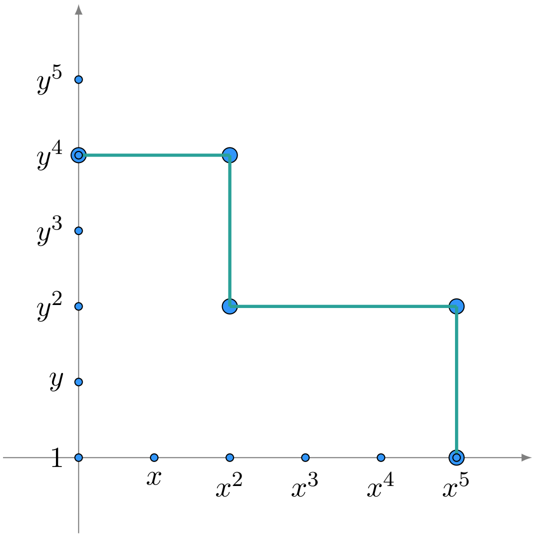


Figure 1.1: Buchberger Diagram or Staircase

Definition 9 (Elimination ideal, [20])**.** *For every ideal $I \trianglelefteq \mathbb{K}[x_1, \ldots, x_n]$, for $J \subseteq \{1, \ldots, n\}$, the elimination ideal of I with respect to J is defined as $I_J := I \cap \mathbb{K}[x_1, \ldots, \widehat{x_J}, \ldots, x_n]$, i.e. I_J consists of those polynomials in I that contain only the variables indexed by J. Also the i-th elimination ideal of I is defined to be $I_{i+1,\ldots,n} := I \cap \mathbb{K}[x_{i+1}, \ldots, x_n]$.*

Theorem 10 (Elimination property, [7])**.** *let G be a Gröbner basis for an ideal I with respect to an elimination term order in which $x_n, \ldots, x_{i+1} \prec x_i, \ldots, x_1$. Then $G \cap \mathbb{K}[x_{i+1}, \ldots, x_n]$ is a Gröbner basis for $I_{i+1\ldots n}$ with respect to that elimination order.*

1.2.2 Resultants

We introduce Resultants introductory material mostly from two books by Cox, Little and O'Shea [20, 21].

Definition 11 (Sylvester Matrix, [20])**.** *Let R be a commutative ring and $f_1, f_2 \in R[x]$ be of degree d_1, d_2 respectively. The Sylvester matrix $\mathrm{Syl}(f_1, f_2)$ is defined to be the matrix of size $(d_1 + d_2) \times (d_1 + d_2)$ with the following entries: if $1 \leqslant i \leqslant d_2$ and $1 \leqslant j \leqslant d_1 + d_2$, the entry in the i-th row and j-th column is the $(d_1 + d_2 - j)$-th coefficient of $x^{d_2 - i} f_1$. If $d_2 + 1 \leqslant i \leqslant d_1 + d_2$ and $1 \leqslant j \leqslant d_1 + d_2$, the entry in the i-th row and j-th column is the $(d_1 + d_2 - j)$-th coefficient of $x^{d_1 - (i - d_2)} f_2$.*

$$\left(\begin{array}{cccccc} f_{1,d_1} & \cdots & \cdots & f_{1,0} & & \\ & \ddots & & & \ddots & \\ & & f_{1,d_1} & \cdots & \cdots & f_{1,0} \\ f_{2,d_2} & \cdots & f_{2,0} & & & \\ & \ddots & & \ddots & & \\ & & \ddots & & \ddots & \\ & & & f_{2,d_2} & \cdots & f_{2,0} \end{array}\right) \begin{array}{l} \left.\vphantom{\begin{array}{c}1\\1\\1\end{array}}\right\} d_2 \\ \left.\vphantom{\begin{array}{c}1\\1\\1\\1\end{array}}\right\} d_1 \end{array}$$

Definition 12 (Resultant, [20])**.** *For $f_1, f_2 \in \mathbb{K}[x]$, we define the resultant of f_1, f_2 to be*

$$\operatorname{res}_x(f_1, f_2) = \det(\operatorname{Syl}(f_1, f_2)).$$

The following are among the properties of resultants that are of interest in this thesis.

Theorem 13 ([20])**.** *Let $f_1, f_2 \in \mathbb{K}[x]$ have positive degrees. Then $\operatorname{res}_x(f_1, f_2)$ is an integer polynomial in the coefficients of f_1 and f_2. Also f_1 and f_2 have a common factor in $\mathbb{K}[x]$ if and only if $\operatorname{res}_x(f_1, f_2) = 0$.*

Theorem 14 ([20])**.** *Let $f_1, f_2 \in \mathbb{K}[x_2, \dots, x_n][x_1]$ have positive degree in x_1. Then*

- $\operatorname{res}_{x_1}(f_1, f_2) \in I_1$.
- $\operatorname{res}_{x_1}(f_1, f_2) = 0$ *if and only if f_1 and f_2 have a common factor, which has positive degree in x_1, in $\mathbb{K}[x_1, \dots, x_n]$.*

When the resultant is not zero we will use the following lemma in order to identify roots of the resultant. This will show us how and when resultants project roots of the system and how this can give us information about the roots of the elimination ideal, roots of the system and multiplicities of the roots of the system.

Lemma 15 ([20])**.** *Let $f_1, f_2 \in \mathbb{K}[x_1, \dots, x_n]$ have (total) degree N_1 and N_2 respectively, and let $c = (c_2, \dots, c_n) \in \mathbb{K}^{n-1}$ satisfy the following conditions:*

- $f_1(x_1, c) \in \mathbb{K}[x_1]$ *has degree N_1,*
- $f_2(x_1, c) \in \mathbb{K}[x_1]$ *has degree $p \leqslant N_2$.*

Then the polynomial $\operatorname{res}_{x_1}(f_1, f_2) \in \mathbb{K}[x_2, x_3, \dots, x_n]$ satisfies

$$\operatorname{res}_{x_1}(f_1, f_2)(c) = h_1(c)^{N_2 - p} \operatorname{res}_{x_1}(f_1(x_1, c), f_2(x_1, c))$$

For n homogeneous polynomials $f_1, \dots, f_n \in \mathbb{K}[x_1, \dots, x_n]$ resultant is defined and gives a condition on the coefficients of $f_1, \dots, f_n$ such that $f_1, \dots, f_n$ have a common root if and only if the resultant is zero. Discussing resultants in general case is beyond the scope of this thesis and we refer the reader to several existing books and surveys in the literature, e.g. [21, 38, 28].

1.2.3 Algebraic Geometry

Here we introduce the algebraic geometry basics from Shafarevich [57] and Hartshorne [36].
In this thesis we work on *affine spaces.* $n-$dimensional affine space over a field $\mathbb{K}$ will be denoted by $\mathbb{A}^n_{\mathbb{K}}$. If $\mathbb{K}$ is clear from the context, then we write $\mathbb{A}^n$ instead of $\mathbb{A}^n_{\mathbb{K}}$.

Definition 16 (Zariski Topology, [36])**.** *Zariski topology on $\mathbb{A}^n$ is defined by taking the closed sets to be the set of zeros of a set of polynomials in $\mathbb{K}[x_1, \ldots, x_n]$.*

$\varnothing$ and $\mathbb{A}^n$ are closed and open.

Definition 17 (Variety, [36])**.** *An affine algebraic variety (or simply a variety) is a closed subset of $\mathbb{A}^n$. $\mathcal{V}(f_1, \ldots, f_m)$ denotes the variety defined by the set of zero of $f_1, \ldots, f_m$. An open subset of an affine variety is called a quasi affine variety.*

Curves and surfaces are examples of varieties.
By *Hilbert's Nullstellansatz* there is a one to one correspondence between the (radical) ideals of $\mathbb{K}[x_1, \ldots, x_n]$ and the varieties in $\mathbb{A}^n$. For a variety $\mathcal{V} \subseteq \mathbb{A}$ we denote its corresponding ideal by $I(\mathcal{V})$ and for an ideal $I \trianglelefteq \mathbb{K}[x_1, \ldots, x_n]$ we denotes its corresponding variety by $\mathcal{V}(I)$.
Primary ideals play an essential role in studying varieties.

Definition 18 (Primary Ideal, [20])**.** *An ideal $I \in \mathbb{K}[x_1, \ldots, x_n]$ is primary if $fg \in I$ implies either $f \in I$ or some power $g^m \in I$ (for some $m > 0$).*

Prime ideals are primary.

Lemma 19 ([20])**.** *If I is a primary ideal, then $\sqrt{I}$ is prime and is the smallest prime ideal containing I.*

Definition 20 (Primary Decomposition of an Ideal, [20])**.** *A primary decomposition of an ideal I is an expression of I as an intersection of primary ideals: $I = \bigcap_{i=1}^{r} Q_i$. Such a decomposition is called irreducible if $\sqrt{Q_i}$ are all distinct and $\bigcap_{j \neq i} Q_j \not\subset Q_i$. Each Q_i is called a primary component of I.*

Theorem 21 ([20])**.** *Every ideal $I \trianglelefteq \mathbb{K}[x_1, \ldots, x_n]$ has a(n) (irreducible) primary decomposition.*

In this thesis by a primary decomposition we refer to an irreducible primary decomposition.
Equivalently every variety has a decomposition into *irreducible* varieties: $\mathcal{V} = \bigcup_i \mathcal{V}_i$ and each $\mathcal{V}_i$ is called an irreducible component of $\mathcal{V}$. Every irreducible variety is the variety of a prime ideal and vice versa. A closed point $\zeta = (\zeta_1, \ldots, \zeta_n) \in \mathbb{A}^n$ is an irreducible variety corresponding to the *maximal* ideal $\mathfrak{m}_\zeta = \langle x_1 - \zeta_1, \ldots, x_n - \zeta_n \rangle$.

Definition 22. *Let Q_ζ be a primary ideal such that $\sqrt{Q_\zeta} = \mathfrak{m}_\zeta$. Then we say that ζ is an isolated point of $\mathcal{V}(I)$.*

Let $\mathbb{K}[x_1, \ldots, x_n]_{(x_1-\zeta_1,\ldots,x_n-\zeta_n)}$ denote the set of all rational function $\frac{f}{g}$ with $g(\zeta) \neq 0$. This is a local ring, i.e., it has only one maximal ideal $\mathfrak{m}_\zeta := \langle x_1 - \zeta_1, \ldots, x_n - \zeta_n \rangle$ and the above is called *localization* of $\mathbb{K}[x_1, \ldots, x_n]$ with respect to ζ or at the maximal ideal $\mathfrak{m}_\zeta$. Having the concept of localization, we are ready to define the *multiplicity* of ζ.

Definition 23 ([21]). *Let I be an ideal and $\zeta \in \mathcal{V}(I)$ be an isolated point in $\mathcal{V}(I)$. The multiplicity of ζ, $\mu(\zeta)$ is defined as follows*

$$\mu(\zeta) := dim_{\mathbb{K}} \mathbb{K}[x_1, \ldots, x_n]_{\mathfrak{m}_\zeta} \Big/ I\mathbb{K}[x_1, \ldots, x_n]_{\mathfrak{m}_\zeta}.$$

Theorem 24 ([21]). *Let I be and ideal such that its variety contains m isolated points, i.e., $\mathcal{V}(I) = \{\zeta_1, \ldots, \zeta_m\}$ and therefore $I = \bigcap_{i=1}^{k} Q_{\zeta_i}$, where $Q_{\zeta_i} = I(\zeta_i)$. Then $dim_{\mathbb{K}}\mathbb{K}[x_1, \ldots, x_n]/I = \sum_{i=1}^{m} \mu(\zeta_i)$ and $dim_{\mathbb{K}}\mathbb{K}[x_1, \ldots, x_n] \Big/ Q_{\zeta_i} = \mu(\zeta_i)$.*

If it is clear from the context, we will use μ instead of $\mu(\zeta)$. From Theorem 8, we can see that having a Gröbner basis for I, we can find the multiplicity of its isolated points.

Definition 25 (Dimension of a Variety, [36]). *If X is a variety, then dimension of X, denoted $dimX$, is defined to be the supremum of all integers m such that there exists a chain $Z_0 \subset Z_1 \subset \ldots \subset Z_m$ of distinct irreducible closed subsets of X. The dimension of a quasi affine variety is defined to be the dimension of its closure.*

We take the dimension of an ideal I to be equal to the dimension of its variety. Therefore a zero dimensional ideal is an ideal whose variety consists of finitely many points.
We mention two theorems about the dimension of varieties.

Theorem 26 ([57]). *If $Y \subseteq X$, then $dimY \leqslant dimX$. If X is irreducible, Y is closed in X and $dimX = dimY$, then $X = Y$.*

Theorem 27 ([57]). *If $f : X \to Y$ is a regular mapping of irreducible varieties and $f(X) = Y$ then $dimX \geqslant dimY$ and*

1. *for every point $y \in Y$, $dimf^{-1}(y) \geqslant dimX - dimY$.*
2. *in Y there exists a non-empty open set U such that $dimf^{-1}(y) = dimX - ximY$ for $y \in U$.*

1.2.4 Elimination Theory

We saw that Gröbner bases and resultants give us information about the elimination ideals. Variety of the elimination ideal and its relation to the projection of the variety of the ideal are considered in the literature. In this section we mention the required theorems for us in this thesis on elimination theory in polynomials. First we mention the following theorem that says which zeros of the elimination ideal can be extended to a root of the ideal.

Theorem 28 (Extension Theorem [20, 59]). *Let $I = \langle f_1, \dots, f_m \rangle \trianglelefteq \mathbb{K}[x_1, \dots, x_n]$. For every $1 \leqslant i \leqslant m$, write f_i in the form*

$$f_i = h_i(x_2, \dots, x_n)x_1^{N_i} + \text{ terms of } x_1\text{-degree less than } N_i.$$

Assume that $(c_2, \dots, c_n) \in \mathcal{V}(I_{2\dots n})$. Then

$$(c_2, \dots, c_n) \notin \mathcal{V}(h_1, \dots, h_m) \Rightarrow \text{ there exists } c_1 \text{ such that } (c_1, \dots, c_n) \in \mathcal{V}(I).$$

Consider the projection operator $\pi : \mathbb{K}^n \to \mathbb{K}^{n-1}$ that acts as follows.

$$\pi((c_1, c_2, \dots, c_n)) = (c_2, c_3, \dots, c_n).$$

For $S \subseteq \mathbb{K}^n$ we denote the set $\{\pi(c) : c \in S\}$ by $\pi(S)$. The following theorem shows the relation between the variety of the elimination ideal and the projection of the variety.

Theorem 29 (Elimination Theorem, [20, 59]). *Let $I_{2\dots n}$ be the first elimination ideal of an ideal $I \in polringn$. Then*

$$\mathcal{V}(I_{2\dots n}) = \pi(\mathcal{V}(I)) \cup (\mathcal{V}(h_1, \dots, h_m) \cap \mathcal{V}(I_{2\dots n})).$$

although the projection of the variety of an ideal and variety of the elimination ideal are not the same, but the latter is the Zariski closure of the projection.

Theorem 30 (The Closure Property, [20]). *Let I, $I_{2\dots n}$ and π be as above. Then*

- *$\mathcal{V}(I_{2\dots n})$ is the smallest affine variety containing $\pi(\mathcal{V}(I))$, i.e., it is the Zariski closure of $\pi(\mathcal{V}(I))$.*
- *If $\mathcal{V}(I) \neq \emptyset$, then there is an affine variety $W \subsetneq \mathcal{V}(I_{2\dots n})$ such that $\mathcal{V}(I_{2\dots n}) \backslash W \subset \pi(\mathcal{V}(I))$.*

Chapter 2

Motivational Problem: Multiplicity in Elimination Ideal

This chapter is about our initial problem on studying elimination ideals via resultants. This chapter can be considered as a detailed description of our initial and motivational problems, which lead us to study the multiplicity structure of isolated points, the core of this thesis. Studying the difference between the projection via resultant and Gröbner basis and comparing their variety with the projection of the initial variety is out of the scope of this thesis.

More precisely, the initial problem was to study the difference between the projection of a variety and the variety of the elimination, whether the elimination is done via Gröbner bases or resultants. In this chapter, we review and clarify some results, which are mostly known for the case of two curves. In this case, degeneracy that often happen in elimination is related to the multiplicity problem. This case is non-trivial, is of interest and has applications in some other areas, e.g. studying arrangements, topology and isotopic graphs of curves.

In this chapter-the same as the rest of the thesis-we work on affine spaces and do not have any root at infinity, unless otherwise is clearly stated. Therefore, some statements are not correct in the projective space, e.g. Corollary 37. Section 2.1 includes examples and propositions that show that the degeneracy problem is non-trivial, even for simple cases. In Section 2.2, we indicate how the factors of the resultant and the generator of the elimination ideal can differ for the case of two curves in $\mathbb{R}$ (or $\mathbb{C}$). This is important specially when considering the degeneracy issue in the topology of a curve. This section continues with comparing the differences of the multiplicities. Finally we quote on using pairwise resultants for several polynomials in several variables.

The major part of this chapter is a joint work with Zafeirakis Zafeirakopoulos and appeared in a preliminary form in [55]. The figures are drawn using `Sage`.

2.1 Variety of Elimination Ideals v.s. Variety of Resultants

In this section we first review the difference between the projection of a variety and the the variety itself, in terms o their dimension. Then considering Gröbner basis and resultants as two standard tools for projection, we will look at the difference between the projection via Gröbner basis and resultants for two $n-$dimensional curves. Knowing this difference will help us to search for the difference between the factors of the corresponding polynomials, when the projection is a hyperplane, which is what we will review in the next section.

Let us recall the following from the two main results on the connection between the elimination ideal and the projection of the variety of that ideal, i.e., Theorems 29 and 30.

$$\mathcal{V}\left(I_{2\ldots n}\right) = \pi\left(\mathcal{V}\left(I\right)\right) \cup \left(\mathcal{V}\left(h_1, \ldots, h_m\right) \cap \mathcal{V}\left(I_{2\ldots n}\right)\right). \tag{2.1}$$

$$\mathcal{V}\left(I_{2\ldots n}\right) \text{ is the Zariski closure of } \pi\left(\mathcal{V}\left(I\right)\right). \tag{2.2}$$

We want to know how big $\mathcal{V}\left(h_1, \ldots, h_m\right) \cap \mathcal{V}\left(I_{2\ldots n}\right)$ can be. In another words, how close $\pi\left(\mathcal{V}\left(I\right)\right)$ and $\mathcal{V}\left(I_{2\ldots n}\right)$ are. One way to phrase these into mathematical terms is to look at the ideals and their generators, and study their differences and intersections. This is what we will investigate in the next section. Here we take a look at the dimension of the varieties in the Elimination Theorem which was suggested to the author by D'Andrea [22] and Ahmadinezhad [1]. We will see that these varieties can be far from each other. This makes computations in the next section/chapter non-trivial.

Note that $\pi\left(\mathcal{V}\left(I\right)\right)$ is not necessarily closed and hence Theorem 30 implies that

$$dim(\pi\left(\mathcal{V}\left(I\right)\right)) = dim(\mathcal{V}\left(I_{2\ldots n}\right)).$$

In fact, this projection is a quasi-affine variety. In general, $dim(\mathcal{V}\left(h_1, \ldots, h_m\right))$ can be as big as $dim(\mathcal{V}\left(I\right))$ and as small as 0. Below we give examples for such cases.

Example 31 (Top Dimensional Case)**.** For the case in which the dimension of $\mathcal{V}\left(h_1, \ldots, h_m\right)$ is the biggest possible, take $I = \langle f_1 = x_1 h, f_2 = h\rangle \in \mathbb{K}[x_1, \ldots, x_n]$, where $h \in \mathbb{K}[x_2, \ldots, x_n]$ with $\mathcal{V}\left(h\right) = \mathbb{A}^2$. Then $I_{2\ldots n} = \langle f_2\rangle$ and $\mathcal{V}\left(I_{2\ldots n}\right) = \pi\left(\mathcal{V}\left(I\right)\right) = \mathcal{V}\left(h\right) = \mathbb{A}^2$, which means that $dim(\mathcal{V}\left(h_1, h_2\right)) = 2$.

Example 32 (Zero Dimensional Case)**.** If we take $I = \langle f_1 = x_1 x_3, f_2 = x_2\rangle \trianglelefteq \mathbb{K}[x_1, x_2, x_3]$, then $\mathcal{V}\left(I\right)$ consists of two lines, x_1-axis and x_3-axis. projection of these axis along the x_1-axis gives us the x_3-axis which is a line, which is of dimension 1. However $\mathcal{V}\left(h_1 = x_3, h_2 = y\right) = \{(0, 0)\}$ is a point, which means that it is of dimension 0.

Also in the following example we see that we can have $\mathcal{V}\left(I_{2\ldots n}\right) = \pi\left(\mathcal{V}\left(I\right)\right)$, independent of how big or how small $\mathcal{V}\left(h_1, \ldots, h_m\right)$ is.

Example 33. Consider $I = \langle f_1 = x_1 h_1, f_2 = x_1 h_2\rangle \trianglelefteq \mathbb{K}[x_1, \ldots, x_n]$, where $h_i \in \mathbb{K}[x_2, \ldots, x_n]$. Then independent of what h_1 and h_2 are, we will have that $I_{2\ldots n} = \{0\}$, which means that $\mathcal{V}\left(I_{2\ldots n}\right) = \pi\left(\mathcal{V}\left(I\right)\right) = \mathbb{A}^2$. We will give a description of an instance this case in Lemma 36.

Also not necessarily $\mathcal{V}(h_1, \ldots, h_m) \subseteq \mathcal{V}(I_1)$ is true. In the next section, we will give more examples for complicated and degenerate situations that may occur. Also we will have Remark 45 in this direction .

Note that $\mathcal{V}(h_1, \ldots, h_m)$ is not the complement of the quasi-affine variety $\pi(\mathcal{V}(I))$, but contains the complement. Also the dimensions of $\mathcal{V}(h_1, \ldots, h_m)$ and the complement are independent of each other. This point makes $\mathcal{V}(h_1, \ldots, h_m)$ more complex and yet more interesting.

In the Elimination and Closure Theorems, $I_{2\ldots n}$ can be computed using Gröbner basis. If we have $I = \langle f_1, f_2 \rangle \trianglelefteq \mathbb{K}[x_1, \ldots, x_n]$, one can think of f_1 and f_2 as two $n-$dimensional curves. Then eliminating the variable x_1 can be done using the Sylvester resultant of f_1 and f_2 with respect to x_1, i.e. $\operatorname{res}_{x_1}(f_1, f_2)$. In the following, we show the connection between the variety of the resultant and the projection of the variety of the ideal I. In this sense this is similar to the elimination theorem. We provide the reader with the proof in the affine case. In fact this theorem is an *affine* description of the roots of the resultant. The theorem and its proof in the affine sense have been derived from the proof that is shown for Lemma 15 in [20], Section 6 of Chapter 3, which itself is used in a proof of the *Extension Theorem* (Theorem 28). In the projective space, we know that the variety of the resultant describes *roots at infinity* and affine roots of the polynomial system we started with (see [20] and [26]), which is the homogeneous case of the theorem. We did not find the proof for the affine case in the literature.

Theorem 34. *Let $I = \langle f_1, f_2 \rangle \in \mathbb{K}[x_1, \ldots, x_n]$ and $\mathcal{R} = \operatorname{res}_{x_1}(f_1, f_2)$. Then*

$$\mathcal{V}(\mathcal{R}) = \mathcal{V}(h_1, h_2) \cup \pi(\mathcal{V}(I))$$

Proof. We prove the following three statements. The theorem follows immediately from these statements.

1. $\mathcal{V}(h_1, h_2) \subseteq \mathcal{V}(\mathcal{R})$.
   It is easy to see from the Laplace expansion of the Sylvester matrix, that the greatest common divisor of h_1 and h_2 divides $\mathcal{R}$. Thus $\mathcal{V}(h_1, h_2) \subseteq \mathcal{V}(\mathcal{R})$.

2. $\pi(\mathcal{V}(I)) \subseteq \mathcal{V}(\mathcal{R})$.
   If $f_1, f_2 \in \mathbb{K}[x_2, \ldots, x_n][x_1]$ have positive degree in x_1, then by Theorem 14, $\operatorname{res}_{x_1}(f_1, f_2) \in I_{2\ldots n}$. Thus $\mathcal{V}(I_{2\ldots n}) \subseteq \mathcal{V}(\mathcal{R})$. From Theorem 29 we have that

$$\mathcal{V}(I_{2\ldots n}) = \pi(\mathcal{V}(I)) \cup (\mathcal{V}(h_1, h_2) \cap \mathcal{V}(I_{2\ldots n})),$$

   which proves that $\pi(\mathcal{V}(I)) \subseteq \mathcal{V}(I_{2\ldots n})$.

3. $\mathcal{V}(\mathcal{R}) \backslash \mathcal{V}(h_1, h_2) \subseteq \pi(\mathcal{V}(I))$.
   Let $c \notin \mathcal{V}(h_1, h_2)$. Then we have two cases:

Case 1: $h_1(c) \neq 0$ and $h_2(c) \neq 0$.
By Lemma 15, w have that $\mathcal{R}(c) = \operatorname{res}_{x_1}(f_1(x_1, c), f_2(x_1, c))$. Thus,

$$\forall c \in \mathbb{K}^n \ \ \mathcal{R}(c) = 0 \Rightarrow \operatorname{res}_{x_1}(f_1(x_1, c), f_2(x_1, c)) = 0.$$

Case 2: Either $h_1(c) \neq 0, h_2(c) = 0$ or $h_1(c) = 0, h_2(c) \neq 0$.

Without loss of generality, assume that $h_1(c) \neq 0, h_2(c) = 0$. Also assume that d_2 is the degree of f_2 and $m < d_2$ is the degree of $f_2(x_1, c)$. From Lemma 15, we have that

$$\forall c \in \mathbb{K}^n \quad \operatorname{res}_{x_1}(f_1, f_2)(c) = h_1(c)^{d_2-m} \operatorname{res}_{x_1}(f_1(x_1, c), f_2(x_1, c)).$$

Thus,

$$\forall c \in \mathbb{K}^n \quad \mathcal{R}(c) = h_1(c)^{d_2-m} \operatorname{res}_x(f_1(x, c), f_2(x, c)),$$

and, since $h_1(c) \neq 0$, we have that

$$\forall c \in \mathbb{K}^n \quad \mathcal{R}(c) = 0 \Rightarrow \operatorname{res}_x(f_1(x, c), f_2(x, c)) = 0.$$

So in both cases we have that $\mathcal{R}(c) = 0 \Rightarrow \operatorname{res}_x(f_1(x, c), f_2(x, c)) = 0$. On the other hand, we have that

$$c \in \pi(\mathcal{V}(f_1, f_2)) \Leftrightarrow \exists c_1 \in \mathbb{K} \text{ such that } (c_1, c) \in \mathcal{V}(f_1, f_2).$$

Therefore

$$\exists c_1 \in \mathbb{K} \text{ such that } (c_1, c) \in \mathcal{V}(f_1, f_2) \Leftrightarrow \exists c_1 \in \mathcal{V}(f_1(x, c), f_2(x, c)).$$

Therefore,

$$\exists c_1 \in \mathcal{V}(f_1(x, c), f_2(x, c)) \Leftrightarrow \operatorname{res}_x(f_1(x, c), f_2(x, c)) = 0.$$

The last equivalence implies that $c \in \pi(\mathcal{V}(I))$ and $\mathcal{V}(\mathcal{R}) \backslash \mathcal{V}(h_1, h_2) \subseteq \pi(\mathcal{V}(I))$.

The theorem follows immediately from the three statements. □

Combining Theorem 34 with the elimination theorem, one can see that $\mathcal{V}(I_{2\ldots n}) \subseteq \mathcal{V}(\mathcal{R})$, which is also clear from the fact that $\mathcal{R} \in I_{2\ldots n}$.

Similar to $I_{2\ldots n}$, one can think of the dimension of $\mathcal{V}(\mathcal{R})$ and compare it with $\pi(\mathcal{V}(I_{2\ldots n}))$. The examples that we mentioned for $\mathcal{V}(I_{2\ldots n})$ can be considered for this purpose and will show non-triviality for these varieties as well.

Having the varieties of $\mathcal{R}$ and $I_{2\ldots n}$, we want to use the polynomial $\mathcal{R}$ in order to extract information about $I_{2\ldots n}$. In the following, we will see that in the special case that the resultant is zero the elimination ideal is also zero. In order to prove thism we need the following lemma. The following lemma about S-polynomials can be viewed as a criterion in Buchberger's algorithm for computing Gröbner basis. In order to use the lemma, one could compute the gcd of each pair of the generator at each step. If each gcd does not contain x_1, then one can factor the gcd out from the two polynomials and compute their S-polynomial and reduce it with respect to the other polynomials in the basis and then multiply the result of the reduction by the gcd. The advantage of this criterion is doing the computation with smaller polynomials.

The lemma also helps us proving the next proposition, which states that in case that the resultant of the generators is zero then the elimination ideal is zero and vice versa.

Lemma 35. *Let $f_1, f_2 \in \mathbb{K}[x_1, \dots, x_n]$ and suppose that $h \in \mathbb{K}[x_1, \dots, x_n]$ with $\deg_{x_1}(h) > 0$ is a common factor of them. Write $f_1 = h{f_1}'$ and $f_2 = h{f_2}'$ for some f_1', f_2' in $\mathbb{K}[x_1, \dots, x_n]$. Let $\ell_1 = lm(f_1)$, $\ell_2 = lm(f_2)$, $\ell_1' = lm(f_1')$, $\ell_2' = lm(f_2')$ and $\ell_h = lm(h)$, denote by S_{12} the S-polynomial of f_1 and f_2 and by S_{12}' the S-polynomial of f_1' and f_2'. Then*

$$S_{12} = hS_{12}'.$$

Proof. Let $\ell = \mathrm{lcm}(\ell_1, \ell_2)$ and $\ell' = \mathrm{lcm}(\ell_1', \ell_2')$. Then

$$\begin{aligned} S_{12} &= \frac{\ell}{\ell_1}f_1 - \frac{\ell}{\ell_2}f_2 \\ &= \frac{\ell}{\ell_1}hf_1' - \frac{\ell}{\ell_2}hf_2' \\ &= h(\frac{\ell}{\ell_1}f_1' - \frac{\ell}{\ell_2}f_2') \end{aligned}$$

Since $\mathrm{lcm}(\ell_1, \ell_2) = \ell_h \, \mathrm{lcm}(\ell_1', \ell_2')$, we have that $\ell = \ell'\ell_h$. Therefore $\frac{\ell}{\ell_1} = \frac{\ell'}{{\ell_1}'}$ and

$$\begin{aligned} h(\frac{\ell}{\ell_1}f_1' - \frac{\ell}{\ell_2}f_2') &= h\left(\frac{\ell'}{{\ell_1}'}f_1' - \frac{\ell'}{{\ell_2}'}f_2'\right) \\ &= hS_{12}'. \end{aligned}$$

□

Theorem 36. *Let $I = \langle f_1, f_2 \rangle \in \mathbb{K}[x_1, \dots, x_n]$ and $\mathcal{R} = \mathrm{res}_{x_1}(f_1, f_2)$. Then*

$$\mathcal{R} \equiv 0 \Leftrightarrow I_{2\dots n} = \langle 0 \rangle .$$

Proof. ($\Leftarrow$) Assume that $I_{2\dots n} = \langle 0 \rangle$. Since $\mathcal{R} \in I_{2\dots n}$ we have $\mathcal{R} \equiv 0$.
($\Rightarrow$) Assume that $\mathcal{R} \equiv 0$. Then either one of f_i is zero (for which the theorem is trivial) or f_1 and f_2 have a common factor h with $\deg_{x_1}(h) > 0$. Let S be the normal form of S_{12}, i.e., S is the result of reducing S_{12} with respect to f_1 and f_2 as many times as possible. If $S = 0$, then $\{f_1, f_2\}$ is a Gröbner basis for the ideal I. Since $f_1, f_2 \in \mathbb{K}[x_1, \dots, x_n] \backslash \mathbb{K}[x_2, \dots, x_n]$ which means that none of them is in $I_{2\dots n}$, then by the Elimination Property of Gröbner bases we have $I_{2\dots n} = \langle 0 \rangle$. Now assume $S \neq 0$. Let S_{12}',f_1',f_2' and h be as in Lemma 35, and S' be the reduced form of S_{12}' with respect to f_1' and f_2'. From Lemma 35 and the fact that reducing S_{12} by f_1 and f_2 is equivalent to reducing S_{12}' by f_1' and f_2', we have that $S = hS'$. Therefore in the process of the Gröbner basis computation by Buchberger's algorithm, all of the new polynomials will have h as a factor, and since $h \in \mathbb{K}[x_1, \dots, x_n] \backslash \mathbb{K}[x_2, \dots, x_n]$, all the polynomials in the Gröbner basis will belong to $\mathbb{K}[x_1, \dots, x_n] \backslash \mathbb{K}[x_2, \dots, x_n]$. By the Elimination Property of Gröbner bases we have $I_{2\dots n} = \langle 0 \rangle$. □

2.2 Multiplicity of Intersection points of Two Curves

Since we know the elimination ideal when the resultant is zero, we are interested in understanding the situation when the resultant is nonzero. From now on, we restrict ourselves to the bivariate case, i.e., two algebraic planar curves in $\mathbb{A}^2$. Studying this case is of interest in some areas, e.g. in computing arrangements and topology of real algebraic curves in $\mathbb{R}^2$, which we will treat in Section 4.1 as an application. In this case we have the following corollary for Theorem 34, which is true only for the *affine case*, i.e., when there is no root at infinity.

Corollary 37. *If $f_1, f_2 \in \mathbb{K}[x, y]$ and $\mathcal{R}$ is not identically zero and the system has no root at infinity, then*

$$\mathcal{V}(I_2) = \pi(\mathcal{V}(I))$$

Proof. Assume that $\mathcal{R}$ is not identically 0. Then $\mathcal{R}$ is a non-zero univariate polynomial. Therefore it has finitely many roots, that are the projection of the roots of the system that are not roots at infinity. So since $\mathcal{R}$ vanishes at $\pi(\mathcal{V}(I))$, we have that $\pi(\mathcal{V}(I))$ is finite. By the Closure Property (Theorem 30), we have that $\mathcal{V}(I_2)$ is the Zariski closure of $\pi(\mathcal{V}(I))$. However, finite sets are Zariski closed, therefore $\mathcal{V}(I_2) = \pi(\mathcal{V}(I))$. □

Even if we have more than two curves in the bivariate case, i.e. $f_1, f_2, \ldots, f_m \in \mathbb{K}[x, y]$, we can consider $R_{ij} = \operatorname{res}_{x_1}(f_i, f_j)$ and let $\mathcal{R} = gcd(R_{ij})$. If g is the unique monic generator of I_1, then

$$g|\mathcal{R}. \tag{2.3}$$

Let us fix the following notation for the rest of this section. $I = \langle f_1, f_2 \rangle \trianglelefteq \mathbb{K}[x, y]$ and it elimination ideal is $I_2 = \langle g \rangle \trianglelefteq \mathbb{K}[y]$. From the above discussion we have that although $\mathcal{R}$ does not necessarily generate the elimination ideal, the product of some of its factors does. In [43] Lazard gave a structure theorem for the minimal lexicographic Gröbner basis of a bivariate ideal which reveals some of the factors of g, but not all of them, neither does it say anything about their powers. Also he has shown that the product of some of those factors divides the resultant, however without Gröbner basis computation it does not tell us about the extra factors that we are looking for.

We make a couple of observations about the factors of the resultant which come from the construction of the Sylverster matrix. Write f_1 and f_2 in the following form

$$f_i = t_i + h_i x^{d_i} + \sum_{j=1}^{d_i - 1} h_{i_j} x^j,$$

where d_i is the degree of f_i with respect to x, $t_i \in \mathbb{K}[y]$ is the trailing coefficient, $h_i \in \mathbb{K}[y]$ is the leading coefficient of f_i and $h_{i_j} \in \mathbb{K}[y]$ are the other coefficients , for $i = 1, 2$. If we expand the Sylvester matrix along its columns/rows we have

$$\gcd(\text{entries in each column/row})\,|\mathcal{R}.$$

But for columns it suffices to consider only first and last columns, because entries of at least one of these two columns appear in all other columns. Also for the rows it suffices to consider only first and last rows, as all other rows are shifts of these two rows. Thus we have the following divisibility relations:

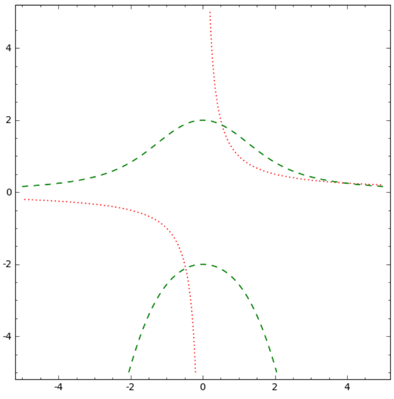
$$\gcd(h_1, h_2)\,|\mathcal{R}, \gcd(t_1, t_2)\,|\mathcal{R},\ \gcd\left(h_i, t_i, h_{i_1}, \ldots, h_{i_{(d_k - 1)}}\right)|\mathcal{R}, \tag{2.4}$$

for $i = 1, 2$.
Note that Theorem 34 does not imply the above divisibility relations, because it doesn't say anything about the multiplicities of the factors of the gcd of the leading coefficients. Also the above is true for two curves in any number of variables.
The above comments reduce the problem into the multiplicity problem for two curves $f_1, f_2 \in \mathbb{K}[x, y]$. We know that the factors of g are factors of $\mathcal{R}$. The converse is true if the projection of the variety is Zariski-closed, e.g. if we are in the zero-dimensional case which is what we study for the rest of this thesis. We again emphasize that there is no root at infinity during our investigations in this thesis. However the multiplicities of the factors of $\mathcal{R}$ and g can be different. The next natural question is to identify their multiplicities.
Since $g|\mathcal{R}$, if $c \in \mathbb{C}$ is a root of g with multiplicity μ then c is a root of $\mathcal{R}$ with multiplicity ν and $\mu \leqslant \nu$. In the following we investigate the problems that were faced while trying to establish a lower bound. We will use the notation μ and ν for multiplicities of factors of g and $\mathcal{R}$ respectively.
case $\nu = 1$
Let $f \in \mathbb{K}[y]$ be an irreducible factor of $\mathcal{R}$ with multiplicity $\nu = 1$. Then the roots of the resultant are either roots of h_1 and h_2 or roots of I_1. Moreover, from Theorem 34 and, since roots of $\gcd(h_1, h_2)$ correspond to roots at infinity if we homogenize, we know that if f corresponds to both a root of I_1 and of $\gcd(h_1, h_2)$ then the degree of f in $\mathcal{R}$ would be greater than 1. Thus

$$f \nmid \gcd(h_1, h_2) \Rightarrow f|g$$

and therefore if $\mathcal{R}$ is square free, then $g = \frac{\mathcal{R}}{\gcd(h_1,h_2)}$. The following is an example that one of the factors of $\mathcal{R}$ appears in g, while the other one does not.

Example 38. Let $f_1 = xy - 1, f_2 = x^2y + y^2 - 4 \in \mathbb{C}[x, y]$. Then $\mathcal{R} = y(y^3 - 4y + 1)$ and $I_1 = \langle y^3 - 4y + 1 \rangle$. $c = 0$ is a root of $\mathcal{R}$ with multiplicity 1, but it is not a root of g. y is the common factor of h_1 and h_2 and that $g = \frac{\mathcal{R}}{\gcd(h_1,h_2)}$.



f_1	$xy - 1$
f_2	$x^2y + y^2 - 4$
h_1	y
h_2	y
g	$y^3 - 4y + 1$
$\mathcal{R}$	$y(y^3 - 4y + 1)$

The above ideal is radical, however $g = \frac{\mathcal{R}}{\gcd(h_1,h_2)}$ does not hold for all radical ideals. Neither is the case under the stronger assumption that g is square-free, nor this is the

case if I is radical and $\mathcal{R}$ and g are square-free. An example of this case will be show below.
The following is a more general question that arises naturally.

Question 39. Given $\mathcal{R}, g$ (and maybe h) in $\mathbb{K}[y]$, find $f_1, f_2 \in \mathbb{K}[x,y]$ such that $\mathcal{R} = \text{res}_{x_1}(f_1, f_2)$ and g is the unique generator of the elimination ideal of the ideal generated by f_1 and f_2.

One way to attack this problem is explained in the following special case. Let $\mathcal{R} = (y-1)(y-2)(y-3), h = gcd(h_1, h_2) = (y-2)(y-3)$.
Ansatz. Let $f_1 = (y-2)(y-3)x^2 + cx + d$ and $f_2 = (y-2)(y-3)x + a$, where $c \in \mathbb{K}[y], a, d \in \mathbb{K}$. Then

$$\begin{aligned}\mathcal{R} &= det \begin{pmatrix} (y-2)(y-3) & c & d \\ (y-2)(y-3) & a & 0 \\ 0 & (y-2)(y-3) & a \end{pmatrix} \\ &= (y-2)(y-3)a^2 - (y-2)(y-3)(ac - d(y-2)(y-3)) \\ &= (y-2)(y-3)(a^2 - ac - d(y-2)(y-3))\end{aligned}$$

However we know that $\mathcal{R} = (y-1)(y-2)(y-3)$. By coefficient comparison we have that

$$\begin{aligned} y-1 &= a^2 - ac - d(y-2)(y-3) \\ &= -dy^2 + 5dy - ac + a^2 - 6d \end{aligned}$$

Setting $d = 0$, the following answer can be achieved:

$$\begin{aligned} f_1 &= (y-2)(y-3)x^2 - ixy \\ f_2 &= (y-2)(y-3)x + i. \end{aligned}$$

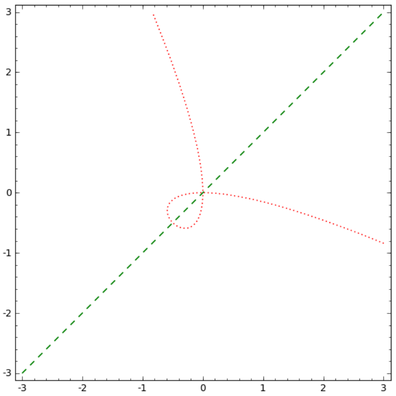
Plugging other values into d we can achieve other answers. The ideal generated by f_1 and f_2 is radical. $\mathcal{R}$ and g are square free and $g = \frac{\mathcal{R}}{h}$.
The following is a slightly different ideal which is radical, $\mathcal{R}$ and g are square free and it does satisfy $g = \frac{\mathcal{R}}{h}$.

Example 40. Let $f_1 = (y-2)(y-3)x^2 - 2xy, f_2 = (y-2)(y-3)x + 2$. Then $\mathcal{R} = 4(y-2)(y-3)(y+1), G = \{x-1, y+1\}$, where G is the reduced Gröbner basis.

case $\nu > 1$

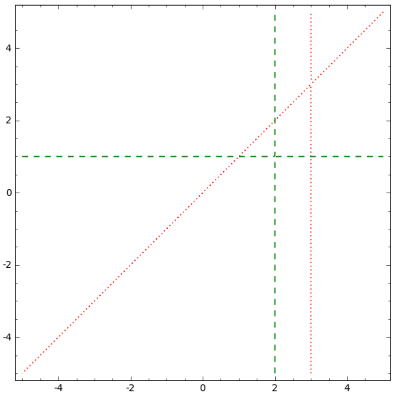
Let us now assume that $\mathcal{R}$ contains factors with multiplicity greater than 1. We propose some examples for this case. Via these examples, on one side, we consider the intersection multiplicity at a point P of the two curves in the affine plane defined by f_1 and f_2, namely the multiplicity ν of the factor corresponding to P in $\mathcal{R}$ and on the other side, we consider the multiplicity μ of the factor corresponding to the projection of P along the x-axis in g. There are situations in which μ can be strictly smaller than ν. We will propose a sufficient condition for this phenomenon to happen.

$\mu = \nu$



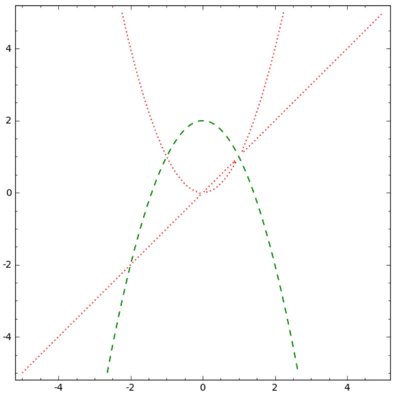
f_1	$x^3 + 3x^2y + 3xy^2 + 4xy + y^3$
f_2	$x - y$
h_1	1
h_2	1
g	$\frac{1}{2} \cdot (2y+1) \cdot y^2$
$\mathcal{R}$	$(-4) \cdot (2y+1) \cdot y^2$

$\mu < \nu$



f_1	$(x-y)(x-3)$
f_2	$(y-1)(x-2)$
h_1	1
h_2	$y-1$
g	$(y-2)(y-1)$
$\mathcal{R}$	$(y-2)(y-1)^2$

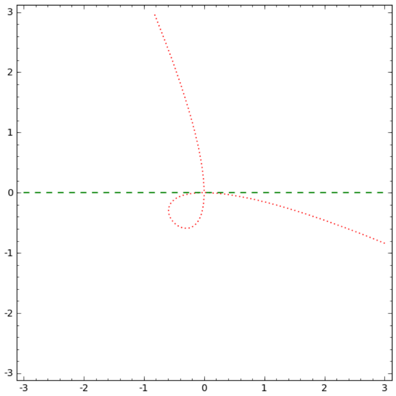
One might be tempted to think that the multiplicity drop is related to the fact that $h_2 = y - 1$. The following example shows that the situation is more complicated.



f_1	$-(x^2+y-2)$
f_2	$(x-y)(y-x^2)$
h_1	1
h_2	1
g	$(y+2)(y-1)^2$
$\mathcal{R}$	$-4(y+2)(y-1)^3$

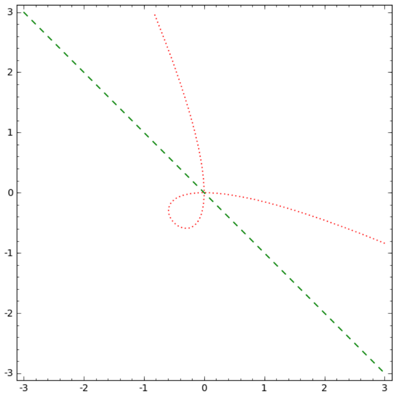
Looking back at the first example above, the curve $x^3+3x^2y+3xy^2+4xy+y^3$ and a line, all the factors of $\mathcal{R}$ and g were of multiplicity one. Fixing the curve and rotating the line by 90 degrees give an interesting intuition which leads us to the Remark 45.

Example 41.



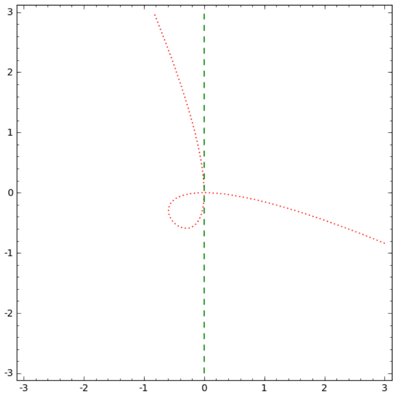
f_1	$x^3 + 3x^2y + 3xy^2 + 4xy + y^3$
f_2	y
h_1	1
h_2	y
g	y
$\mathcal{R}$	y^3

Example 42.



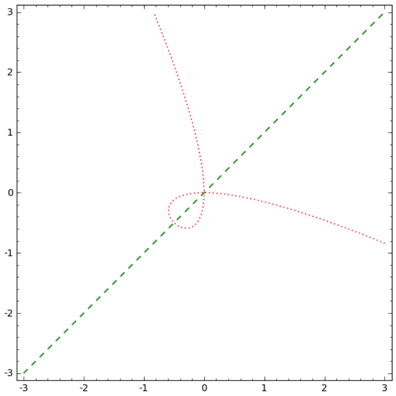
f_1	$x^3 + 3x^2y + 3xy^2 + 4xy + y^3$
f_2	$x + y$
h_1	1
h_2	1
g	y^2
$\mathcal{R}$	$4y^2$

Example 43.



f_1	$x^3 + 3x^2y + 3xy^2 + 4xy + y^3$
f_2	x
h_1	1
h_2	1
g	y^3
$\mathcal{R}$	$-y^3$

Example 44.



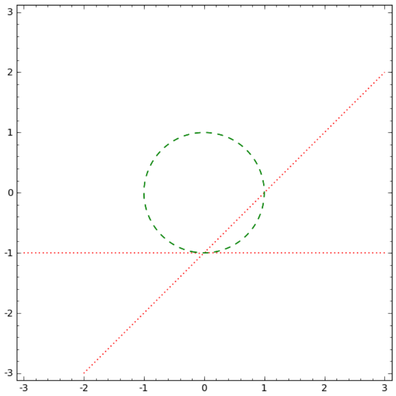
f_1	$x^3 + 3x^2y + 3xy^2 + 4xy + y^3$
f_2	$x - y$
h_1	1
h_2	1
g	$\frac{1}{2}(2y + 1)y^2$
$\mathcal{R}$	$-4(2y + 1)y^2$

In Examples 42 and 44, the intersection point has multiplicity 2, while in Examples 41 and 43, the intersection point has multiplicity 3. Observe that, in the case $f_2 = x$, the multiplicity is preserved in the corresponding factor of g, while in the case $f_2 = y$ it is reduced to 1. These examples support evidence for the following remark.

Remark 45. Assume that no two affine roots of the system given by f_1 and f_2 have the same y-coordinate. If the two curves defined by f_1 and f_2 admit a common tangent at an intersection point P which is parallel to the x-axis, then the multiplicity of the factor corresponding to (the projection of) P in g is strictly smaller than the multiplicity of the factor corresponding to P in R.

The following is another example satisfying the above remark in which the factor y in g is preserved with the same multiplicity as in $\mathcal{R}$, but the factor $(y + 1)$ drops by one. One can notice that we are in the situation covered by the remark, since $(y + 1)$ and the circle have a common tangent parallel to the x-axis at their intersection.

Example 46.



f_1	$-1(y + 1)(x - y - 1)$
f_2	$x^2 + y^2 - 1$
h_1	$-(y + 1)$
h_2	1
g	$y(y + 1)^2$
$\mathcal{R}$	$2y(y + 1)^3$

Remark 47. If I *is radical or zero-dimensional it does not imply that* $\mathcal{V}(\mathcal{R}) = \mathcal{V}(g)$. To see this consider the following. Let $f_1 = (y^2 - y)x^2 + x$ and $f_2 = (y^2 - y)x + y$. Then $G = \{x, y\}$ and therefore the ideal is both radical and zero dimensional. However

$$g = y \neq y^2(y-1)^2 = \mathcal{R}.$$

and thus $\mathcal{V}(\mathcal{R}) \neq \mathcal{V}(g)$.

Remark 48. *Not necessarily* $R = g^{k_1} \gcd(h_1, h_2)^{k_2} \gcd(t_1, t_2)^{k_3}$ *for some* $k_1, k_2, k_3 \in \mathbb{N}$. Let h denote $\gcd(h_1, h_2)$ and t denote $\gcd(t_1, t_2)$. From Theorem 34 and its corollary we can conclude that every factor of $\mathcal{R}$ is either a factor of g or a factor of h. Or equivalently $\mathcal{V}(\mathcal{R}) = \mathcal{V}(hg)$. From Equation 2.4 we have even the stronger result that $h|\mathcal{R}$ and $t|\mathcal{R}$. However we cannot conclude that there exist natural numbers k_1, k_2 and k_3 such that $\mathcal{R}^{k_1} = g^{k_1}h^{k_2}t^{k_3}$. The following example shows this.

Example 49. Let $f_1 = y(\frac{-1}{666}x^2 + \frac{29}{4}x + y^2)$ and $f_2 = x(y+1)$. Then

$$\mathcal{R} = y^3(y+1)^2 \neq g = y^3(y+1),$$

$h_1 = -\frac{1}{666}y$, $h_2 = (y+1)$, $h = 1$ and $t = 1$. Here the extra factor is $e = (y+1)$. It is obvious that there do not exist $k_1, k_2 \in \mathbb{N}$ such that $e = \gcd(h_1, h_2)^{k_1} \gcd(t_1, t_2)^{k_2}$.

The fact that the resultant of f_1 and f_2 with respect to x does not vanish identically (and the system has no roots at infinity) means that there are finitely many projections of roots of the system $\{f_1, f_2\}$ in the y axis. This is enough for our argument in the proof of Corollary 37. Assuming that also the projection of the roots on the x-axis are finitely many does not give us more freedom. Being zero dimensional implies that for each variable, the resultant with respect to that variable does not vanish identically. But since we eliminate variables in a particular order (given by a fixed term order) it is not necessarily a natural condition.
In the next chapter we will introduce a method to recognize the *extra* factors, i.e. the factors of $\mathcal{R}$ that are not factors of g.

Notes on using pairwise Sylvester resultants To finalize the discussion about the difference between $\mathcal{R}$ and g, we try to see if a set of Sylvester resultants can be used in order to obtain I_1 or some generators of it. Let $I = \langle f_1, \ldots, f_m \rangle \trianglelefteq \mathbb{K}[x_1, \ldots, x_n]$, where $m \geqslant 2$. Consider the ideal generated by the pairwise Sylvester resultants of the m polynomials with respect to x_1 and let

$$R := \langle \{r_{ij} := \operatorname{res}_{x_1}(f_i, f_j) \,|1 \leqslant i < j \leqslant m\} \rangle,$$

The variety of R can be described in terms of the varieties of r_{ij}, i.e., $\mathcal{V}(R) = \bigcap \mathcal{V}(r_{ij})$. By Theorem 34 we have that $\mathcal{V}(r_{ij}) = \pi(\mathcal{V}(f_i, f_j)) \cup \mathcal{V}(h_i, h_j)$. Then $\mathcal{V}(R) = \bigcap (\pi(\mathcal{V}(f_i, f_j)) \cup \mathcal{V}(h_i, h_j)) =$

$\bigcup_{c\in C}\bigcap_{i=1}^{\binom{m}{2}} c_i$. Now Let $\mathcal{V}_{ij} = \{\pi\left(\mathcal{V}\left(f_i, f_j\right)\right), \mathcal{V}\left(h_i, h_j\right)\}$, for $1 \leqslant i < j \leqslant m$ and C be the Cartesian product $C = \times_{1\leqslant i<j\leqslant m}\mathcal{V}_{ij}$. Then

$$\mathcal{V}\left(R\right) = \bigcup_{c\in C}\bigcap_{i=1}^{\binom{m}{2}} c_i.$$

Also we have that $\mathcal{V}\left(h_1, \ldots, h_m\right) \subseteq \mathcal{V}\left(R\right)$ and $\pi\left(\mathcal{V}\left(I\right)\right) \subseteq \mathcal{V}\left(R\right)$, however, not necessarily $\bigcap \pi\left(\mathcal{V}\left(f_i, f_j\right)\right) \subseteq \pi\left(\mathcal{V}\left(I\right)\right)$.

Note that $R \subseteq \mathbb{K}[x_2, \ldots, x_n]$, and therefore R is not necessarily principal. Now let $\mathcal{R} := \gcd\left(r_{ij}\right)$. Then not necessarily the ideal generated by $\mathcal{R}$ is equal to R, however, setting $\mathcal{R} := \gcd\left(r_{ij}\right)$ makes sense, as gcd has a meaning, although Euclidean algorithm for computing gcd will not work in the case of $n \geqslant 3$, i.e. when $\mathbb{K}[x_2, \ldots, x_n]$ is not a Euclidean domain. For details on the gcd in the multivariate case, refer to Definition 11 in Chapter 4 of in [20] and the discussion afterwards. From the above discussion one can see that all the factors of $\gcd\left(h_1, \ldots, h_m\right)$ are factors of $\mathcal{R}$ as well, however, we cannot deduce anything about their multiplicity although we have the following divisibility condition.

$$\gcd\left(h_1, \ldots, h_m\right)|\mathcal{R}.$$

This is because , for $1 \leqslant i < j \leqslant m$ we have that $\gcd\left(h_i, h_j\right) | \operatorname{res}_x\left(f_i, f_j\right)$, and thus $\gcd\left(\gcd\left(h_i, h_j\right)\right) | \gcd\left(r_{ij}\right)$, which means that $\gcd\left(h_1, \ldots, h_m\right)|\mathcal{R}$.

If we set $f_i = f_1$ in R and consider the ideal $R' := \langle\{res_x(f_1, f_j)|2 \leqslant j \leqslant m\}\rangle$ then all the theorems and corollaries of this section about R will be correct for R'. The question however is the possible computational advantages and disadvantages of working with R or R'. Since $R' \subseteq R$ then $\mathcal{V}\left(R\right) \subseteq \mathcal{V}\left(R'\right)$, which means that $\mathcal{V}\left(R\right)$ can be *closer* to $\mathcal{V}\left(I_1\right)$ than $\mathcal{V}\left(R'\right)$. On the other hand for R' we have a basis with much less generators than for R (m vs. $\binom{m}{2}$) and therefore working with R' may lead us to less computations.

We end this section with some words about the multiplicity issue in the general case. If we have a principal elimination ideal, then the problem reduces to the difference between the multiplicity of the factors of $\mathcal{R}$ vs those of g. In the special case that the number of variables is the same as the number of polynomials, one can consider the *u-Resultant* of the generators of the ideal, instead of $\mathcal{R}$. This is more efficient as it gives us exactly the roots and their multiplicities. The factors of the u-Resultant are the same as the factors of g, but not necessarily the multiplicities are the same. There are techniques to obtain the projection of the roots and their exact multiplicity via u-resultants [18, 17]. In spite of all those modifications, there are restrictions on using u-Resultants, as they only work under certain conditions and the author is not aware of any work that is related to the multiplicities obtained via u-Resultants and the multiplicity of the factors of g.

Chapter 3

Main Results: Dual Spaces and Directional Multiplicities, Improved Algorithms

The major part of this Chapter is a joint ongoing work with A. Mantzaflaris and Z. Zafeirakopoulos and a preprint will appear soon. M. Gallet [32] had contributed to the early version of the work.

This chapter contains the main contributions of our work to the multiplicity structure problem. It is a self-contained chapter. We start with the preliminaries of dual spaces of polynomial rings. Then, looking at the monomials in a basis of the dual space rather than a base of $R/_{Q}$, we introduce directional multiplicity, which gives us a lot of information about the multiplicity structure at an isolated point. We show that directional multiplicities can be bounded and can bound some other invariants of an ideal, namely Nil-index and the intersection multiplicity.

Then, we shortly demonstrate the two existing algorithms for computing a basis for the dual space which gives us the multiplicity. The major part of this chapter is our improvements on those algorithms. These include criteria that allow us to reduce the size of the matrices that are constructed at each step of both of the algorithms. We will show that our improvements give the smallest known matrices for computing the multiplicity structure. A prototype implementation of Macaulay's algorithms and the integration method has been done in `Sage`. Also a prototype implementation of our improvements to the integration method has been done in `Maple`, as an extension to the package of Mantzaflaris in [47].

3.1 Preliminaries on Dual Spaces

We start with a brief review of the dual space of a vector space which can be found in any linear algebra book, e.g. [37]. Then we present definitions and results on the dual space of polynomial rings from [53].

Let V be a vector space over a field K. The dual of V- which will be denoted by $\hat{V}$- is the set of linear functionals from V to K, i.e.

$$\hat{V} = \{\lambda : V \to K | \lambda \text{ is linear}\}.$$

For the vector space of the continuous real-valued functions over an interval, integration over that interval is in the dual space. Another well-known example is the evaluation. Consider $R = \mathbb{K}[x_1, \ldots, x_n]$ as a $\mathbb{K}$-vector space. Then evaluation at a point ζ is in the dual of R:

$$\begin{aligned} ev_\zeta : R &\to \mathbb{K} \\ p &\mapsto p(\zeta). \end{aligned}$$

For a $\mathbb{K}$-vector space V, $\hat{V}$ is also a $\mathbb{K}$-vector space. Also if V is finite dimensional with a basis $\{v_1, \ldots, v_b\}$, then $\{f_1, \ldots, f_B\}$ defined by $f_i(v_j) = \delta_{ij}$ is a basis for $\hat{V}$, which is called the *dual basis*. The construction above does not work for vector spaces of infinite dimension. Hilbert spaces do not generally have nice bases. Neither does the ring of formal power series over a field, nor can we construct a nice basis for $\hat{R}$.
However, some particular members of $\hat{R}$ describe the whole $\hat{R}$. Below we make this more precise.

Definition 50. *Let $\zeta = (\zeta_1, \ldots, \zeta_n) \in \mathbb{K}^n$ and $\boldsymbol{a} = (a_1, \ldots, a_n) \in \mathbb{N}^n$. Then define*

$$\begin{array}{rccc} \partial_\zeta^{\boldsymbol{a}}: & R & \longrightarrow & \mathbb{K} \\ & p & \mapsto & (d_{x_1})^{a_1} \ldots (d_{x_n})^{a_n}(p)(\zeta), \end{array}$$

Namely $\partial_\zeta^{\boldsymbol{a}}$ acts on p first by differentiation and then by evaluation at the point ζ.

Notation. *For the rest of this chapter, by a translation, we can assume that $\zeta = 0$, unless otherwise stated. When it is clear from the context, we will use $\partial^{\boldsymbol{a}}$ instead of $\partial_\zeta^{\boldsymbol{a}}$. Also $\mathbb{K}[[\partial_\zeta]]$ denotes the $\mathbb{K}$-vector space of power series in the variables $d_{x_1}, \ldots, d_{x_n}$, which are linear forms that act on R as described in Definition 50. If it is clear from the context, we will use $\mathbb{K}[[\partial]]$ instead of $\mathbb{K}[[\partial_\zeta]]$.*

One can prove ([53], Proposition 2.2) that every element of the dual of R can be written as a formal power series of linear functions defined above:

Theorem 51. *With the above notation, there is an isomorphism of $\mathbb{K}$-vector spaces between $\hat{R}$ and $\mathbb{K}[[\partial_\zeta]]$ given by the following correspondence:*

$$\hat{R} \ni \lambda \quad \longleftrightarrow \quad \Lambda = \sum_{\boldsymbol{a} \in \mathbb{N}^n} \lambda(\prod (x_i - \zeta_i)^{a_i}) \frac{1}{\prod a_i!} \partial_\zeta^{\boldsymbol{a}} \in \mathbb{K}[[\partial_\zeta]].$$

The above isomorphism can be seen as a topological isomorphism if we consider $\hat{R}$ equipped with the simple convergence and $\mathbb{K}[[\partial]]$ equipped with ∂-adic topology.

Remark 52. To verify the above isomorphism note that

$$\frac{1}{\prod a_i!}\partial_\zeta^{\mathbf{a}}\left(\prod(x_i-\zeta_i)^{a_i}\right)=\delta_{ij},$$

where δ_{ij} is the Kronecker function. Actually this shows that the action of $\mathbb{K}[[\partial_\zeta]]$ on R given by the action of its projection on R is the same as the differentiation and evaluation action.

From now on, we identify $\hat{R}$ with $\mathbb{K}[[\partial_\zeta]]$. Also we may use $\partial_\zeta^{\mathbf{a}}$ instead of $\frac{1}{\prod a_i!}\partial_\zeta^{\mathbf{a}}$ in order to make computations easier.
One can consider $\hat{R}$ as an R-module via

$$\begin{aligned} p.\lambda : R &\to \mathbb{K} \\ q &\mapsto \lambda(pq) \end{aligned}$$

for any $p \in R$ and $\lambda \in \hat{R}$. The following is a useful property that will pave the way to study the orthogonal of an ideal, which can be easily obtained from Lemma 2.3 and Remark 2.4 in [53].

Lemma 53. *The multiplication by $x_i - \zeta_i$ in $\hat{R}$ corresponds to the derivation with respect to ∂_ζ at i-th coordinate in $\mathbb{K}[[\partial_\zeta]]$. Similarly, the multiplication by ∂_ζ at i-th coordinate in $\mathbb{K}[[\partial_\zeta]]$ acts as a derivation on polynomials.*

Definition 54. *(Definition 2.5, [53]) The orthogonal of an ideal I of R is defined as*

$$I^\perp \;=\; \left\{\lambda \in \hat{R}\;:\;\lambda(f)=0 \quad \forall f \in I\right\}.$$

Macaulay has called the above, the *inverse system.*
From the Lemma 53, since I is closed under multiplication, $I^\perp$ is closed under derivation. From its definition, the orthogonal of I is a linear subspace of $\hat{R}$. Under the isomorphism given previously, for every $\zeta \in \mathbb{K}^n$ we can think of $I^\perp$ as a linear subspace of $\mathbb{K}[[\partial_\zeta]]$. More precisely,

Proposition 1. *(Proposition 2.6, [53]) The ideals of R are in one-to-one correspondence with the vector spaces of* $\mathbb{K}[[\partial_\zeta]]$.

Primary ideals, i.e., correspond to isolated points, can be identified by looking at those elements in the orthogonal of I which, in the description as formal power series, admit only finitely many non zero coefficients, namely the polynomials in ∂_ζ. In fact, not many ideals are primary ideals corresponding to isolated points. However, if the given ideal has a primary ideal in its primary decomposition, corresponding to an isolated point, then we can forget about the other components and work on this ideal and we will deal with the local properties at that point only. Therefore, in this work we let ζ be an isolated point of the variety of I. Then the primary decomposition of I contains a primary ideal Q_ζ whose radical is of the form $\mathfrak{m}_\zeta = \langle x_1-\zeta_1,\ldots,x_n-\zeta_n\rangle$. If $\sqrt{I}=\mathfrak{m}_\zeta$, then we call I an $\mathfrak{m}_\zeta$-primary ideal and usually we denote it by Q_ζ.
Marinari, Mora and Möller in [49] have shown that the $\mathfrak{m}_\zeta$-primary ideals are in one-to-one correspondence with the non-null vector spaces of finite dimension of $\mathbb{K}[\partial]$, which are stable by derivation. This is apparently work attributed to Gröbner.

Theorem 55. *([49]) The $\mathfrak{m}_\zeta$-primary ideals are in one-to-one correspondence with the non-null vector spaces of finite dimension of $\mathbb{K}[\partial]$, which are stable by derivation.*

The following theorem and its corollary are essential for the algorithms that will be presented later.

Theorem 56. *(Theorem 3.2, [53]) Let I be an ideal of R with an $\mathfrak{m}_\zeta$-primary component Q_ζ. Then*

$$\left(I^\perp \cap \mathbb{K}[\partial_\zeta]\right)^\perp = Q_\zeta \text{ and } Q^\perp = I^\perp \cap \mathbb{K}[\partial_\zeta],$$

where $\left(I^\perp \cap \mathbb{K}[\partial_\zeta]\right)^\perp = \Big\{ f \in R \,:\, \lambda(f) = 0 \quad \forall \lambda \in \langle D \rangle \Big\}$.

From now on, given an $\mathfrak{m}_\zeta$-primary ideal Q_ζ, D will stand for a basis for $Q_\zeta^\perp$. Therefore $\langle D \rangle = Q_\zeta^\perp = I^\perp \cap \mathbb{K}[\partial_\zeta]$.

Corollary 57. *([53]) If $I = Q_\zeta$ is an $\mathfrak{m}_\zeta$-primary ideal, then we can identify $I^\perp$ with a linear subspace of the polynomial ring $\mathbb{K}[\partial_\zeta]$.*

Therefore, we are after computing a basis for a finite-dimensional linear subspace of $\mathbb{K}[\partial_\zeta]$.

3.2 Directional Multiplicity

In this section, we take a look at the dual space structure of an ideal. This leads us to introduce the notion of *Directional Multiplicity*. Directional multiplicities give us a lot of information about the multiplicity structure at an isolated point. We show that directional multiplicities can be bounded and can bound some other invariants of an ideal, namely the Nil-index and the intersection multiplicity. Lemma 58 provides us with the information that leads to the soundness of the definition of directional multiplicity.

Studying dual spaces, we define the directional multiplicity and show some properties of it. We also show how it gives information about elimination. We first prove that the set of monomials that appear in elements of $Q^\perp$ is exactly the set of monomials $\partial^{\mathbf{a}}$ such that $x^{\mathbf{a}} \notin Q$, where $x^{\mathbf{a}} = x_1^{a_1} \cdots x_n^{a_n}$. Let us observe that

$$\partial^{\mathbf{a}}(x^{\mathbf{b}}) = \prod \delta_{a_i,b_j} \tag{3.1}$$

where $\delta_{i,j}$ is the Kronecker delta.

Proposition 2 (Characterization of Monomials in $Q^\perp$, in [47] without proof). *Let $Q = Q_\zeta$ be an $\mathfrak{m}_\zeta$-primary ideal. Consider $Q^\perp$ as a sub-vector space of $\mathbb{K}[\partial_\zeta]$ as above. Then*

$$\bigcup_{\Lambda \in Q^\perp} \operatorname{supp}(\Lambda) \;=\; \Big\{ \partial^{\boldsymbol{a}} \mid x^{\boldsymbol{a}} \notin Q \Big\},$$

where $\operatorname{supp}(\Lambda)$ *is the set of monomials with nonzero coefficient in* Λ.

Proof. By Theorem 56, for all f

$$f \in Q \Leftrightarrow \left(\lambda(f) = 0 \text{ for all } \lambda \in Q^{\perp}\right).$$

Now choose a basis $D \subset \mathbb{K}[\partial]$ of $Q^{\perp}$, the above implies that for all f

$$f \in Q \Leftrightarrow (\lambda(f) = 0 \text{ for all } \lambda \in D).$$

We are ready to prove the thesis:

"$\subseteq$" If $\partial^{\mathbf{a}}$ is in $\operatorname{supp}(\Lambda)$ then the monomial $x^{\mathbf{a}}$ is not annihilated by Λ (see Equation 3.1), which implies $x^{\mathbf{a}} \notin Q$.

"$\supseteq$" If $x^{\mathbf{a}} \notin Q$, then there exists $\lambda \in D$ such that $\lambda(x^{\mathbf{a}}) \neq 0$. Let $\Lambda \in \mathbb{K}[\partial]$ be the differential operator corresponding to λ, so $\Lambda(x^{\mathbf{a}}) \neq 0$. By Equation 3.1, we know that $m(x^{\mathbf{a}}) = 0$ for all monomials m in $\operatorname{supp}(\Lambda)$ which are different from $\partial^{\mathbf{a}}$. Hence $\partial^{\mathbf{a}}$ has to be in $\operatorname{supp}(\Lambda)$.

□

Now that we have a picture of the monomials in $Q^{\perp}$, we want to know how they look like under projection. The following result shows that the objects introduced so far, behave well in the framework of elimination theory.

Proposition 3 ([27], Proposition 7.19)**.** *Let π be the linear map*

$$\begin{array}{rccc} \pi: & \mathbb{K}[[dx_1,\ldots,dx_n]] & \longrightarrow & \mathbb{K}[[dx_2,\ldots,dx_n]] \\ & \Lambda & \mapsto & \Lambda(0, dx_2, \ldots, dx_n). \end{array}$$

Also suppose that I is an ideal in R and $I_{2,\ldots,n} = I \cap \mathbb{K}[x_2,\ldots,x_n]$ is its first elimination ideal. Then we have

$$(I_{2,\ldots,n})^{\perp} = \pi\left(I^{\perp}\right).$$

We use the above proposition in order to prove the Dual Projection Lemma which shows how to get a basis of the dual space of the elimination ideal, having a basis for the dual space. Note that I in Proposition 3 can be any ideal, however the following lemma is only for the local case, i.e., when we are working on an $\mathfrak{m}_{\zeta}$-primary ideal $Q = Q_{\zeta}$.

Lemma 58 (Dual Projection Lemma)**.** *With the hypotheses of Proposition 2, suppose that $D = \{\Lambda_0, \Lambda_1, \ldots, \Lambda_{l-1}\} \subset \mathbb{K}[\partial]$ is a basis of $Q^{\perp}$. Let $Q_{2,\ldots,n} = Q \cap \mathbb{K}[x_2,\ldots,x_n]$. Then*

$$Q^{\perp}_{2,\ldots,n} = \langle \Lambda_0|_{dx_1=0}, \Lambda_1|_{dx_1=0}, \ldots, \Lambda_{l-1}|_{dx_1=0} \rangle.$$

Proof. We prove the lemma by proving two inclusions.

($\supseteq$) For all i, $(1 \leqslant i \leqslant l-1)$, since $\Lambda_i \in Q^{\perp}$, therefore we have that $\Lambda_i|_{dx_1=0} \in Q^{\perp}|_{dx_1=0}$. But since by proposition 3, $Q^{\perp}|_{dx_1=0} \in Q^{\perp}_{2,\ldots,n}$, then $\Lambda_i|_{dx_1=0} \in Q^{\perp}_{2,\ldots,n}$. This means that $\langle \Lambda_0|_{dx_1=0}, \Lambda_1|_{dx_1=0} \rangle \subseteq Q^{\perp}_{2,\ldots,n}$.

($\subseteq$) Suppose that $\Lambda' \in Q^{\perp}_{2,\ldots,n}$. Since by Proposition 3, $Q^{\perp}|_{dx_1=0} \in Q^{\perp}_{2,\ldots,n}$, then $\Lambda' \in Q^{\perp}|_{dx_1=0}$. Therefore, there exists a $\Lambda \in Q^{\perp}$, such that $\Lambda' = \Lambda|_{dx_1=0}$. We know that $Q^{\perp} = \langle \Lambda_0, \Lambda_1, \ldots, \Lambda_{l-1} \rangle$. So, there exist $c_i \in \mathbb{K}$, $(1 \leqslant i \leqslant l-1)$, such that $\Lambda = \sum_{i=0}^{l-1} c_i \Lambda_i$, and therefore $\Lambda|_{dx_1=0} = \sum_{i=0}^{l-1} c_i \Lambda_i|_{dx_1=0}$, which means that $\Lambda' = \sum_{i=0}^{l-1} c_i \Lambda_i|_{dx_1=0}$. Therefore

$$\Lambda' \in \langle \Lambda_0|_{dx_1=0}, \Lambda_1|_{dx_1=0}, \ldots, \Lambda_{l-1}|_{dx_1=0} \rangle .$$

Thus, $\quad Q^{\perp}_{2,\ldots,n} \subseteq \langle \Lambda_0|_{dx_1=0}, \Lambda_1|_{dx_1=0}, \ldots, \Lambda_{l-1}|_{dx_1=0} \rangle$.

□

Corollary 59. *Let $D = \{\Lambda_0, \Lambda_1, \ldots, \Lambda_{l-1}\} \subset \mathbb{K}[\partial]$ be a basis of $Q^{\perp}$, and $Q_i = Q \cap \mathbb{K}[x_i]$, for $1 \leqslant i \leqslant n$. Denote by $\Lambda|_{dx_i \neq 0}$ the polynomial obtained by substituting $dx_j = 0$ for $1 \leqslant i \neq j \leqslant n$ in Λ. Then*

$$Q_i^{\perp} = \langle \Lambda_0|_{dx_i \neq 0}, \Lambda_1|_{dx_i \neq 0}, \ldots, \Lambda_{l-1}|_{dx_i \neq 0} \rangle .$$

Moreover, there exists $\mu_i \in \mathbb{N}$ such that

$$Q_i^{\perp} = \left\langle 1, dx_i, \ldots, dx_i^{\mu_i - 1} \right\rangle .$$

Now we have the necessary tools to define the notion of directional multiplicity.

Definition 60 (Directional Multiplicity). *Let ζ be an isolated point in the variety of an ideal I and Q_ζ be the corresponding $\mathfrak{m}_\zeta$-primary component. Using the notation of Corollary 59, for $1 \leqslant i \leqslant n$, we define the $i-$th directional multiplicity of ζ to be μ_i.*

In order to give an intuition of directional multiplicity, let's have a look at the quotient R/Q_ζ, which we will denote by B_ζ. If we consider this quotient as a vector space, finding a basis for such a quotient was the task given to Buchberger for his PhD thesis by Gröbner, which led to the invention of Gröbner bases [10]. Let us recall that the multiplicity of ζ is defined as $dim_{\mathbb{K}}\ R/Q_\zeta$. We will denote the multiplicity by $\mu(\zeta)$ or simply by μ if ζ is clear from the context. Another notion that is highly studied in the literature that describes an intrinsic parameter of an $\mathfrak{m}_\zeta$-primary ideal is the *Nil-index*, e.g. see work in [45].

Definition 61. *The Nil-index of an $\mathfrak{m}_\zeta$-primary ideal Q_ζ is the maximum integer $\mathcal{N} \in \mathbb{N}$ such that $\mathfrak{m}_\zeta^{\mathcal{N}} \nsubseteq Q_\zeta$.*

There is a tight connection between the dual space of $\mathfrak{m}_\zeta$-primary ideals and their Nil-index.

Lemma 62. *(Lemma 3.3, [53]) The maximum degree of the elements of $I^{\perp} \cap \mathbb{K}[\partial_\zeta]$ is equal to the Nil-index of Q_ζ.*

Theorem 56 and Lemma 62 show that we can find the monomials of D by searching among those monomials of $I^{\perp}$ that have degree at most the Nil-index, i.e., there exists a degree bound over the monomials of D. These monomials are actually the monomials under the *Extended Buchberger Diagram* which is defined below.

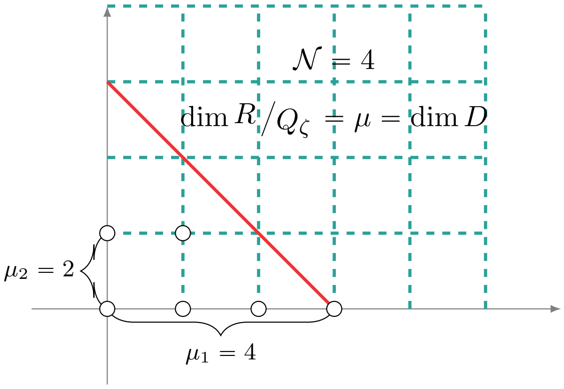


Figure 3.1: Extended Buchberger Diagram for Example 67

Definition 63 (Extended Buchberger Diagram)**.** *The Extended Buchberger Diagram of an $\mathfrak{m}_\zeta$-primary ideal Q_ζ is obtained by considering all the monomials that appear in a basis of dual space of Q_ζ .*

We can think of the Nil-index of Q_ζ as the largest degree of the monomials under the extended Buchberger diagram. Figure 3.1 shows the extended Buchberger diagram and all of its monomials for Example 67.

Note that the monomials under the Buchberger diagram with respect to an ordering form a vector space basis for R/Q. They include some monomials in a basis of $Q^\perp$, but they do not necessarily include all the monomials in D. In particular, they may not include the highest powers of dx_i, i.e., the monomials corresponding to the directional multiplicities. However in the extended Buchberger diagram, one can see all the possible monomials in D, which are all the monomials that do now appear in Q, which include all the monomials in the Buchberger diagram of Q.

The above comments have been illustrated in Figure 3.2. The black dots show a basis for R/Q, while the white dots are the rest of the monomials in the basis of $Q^\perp$. In [48], Mourrain and Mantzaflaris show the new monomials in a basis of $Q^\perp$ that are discovered at each step of their algorithm, comparing two different primal dual bases that they obtain for R/Q during their computations. Also Figures 3.3 and 3.4 show the quotient of the elimination ideal with respect to x and the quotient of the elimination ideal with respect to y, respectively. In Figure 3.3 , black dots are the basis for $Q_2^\perp$ and the white dots are the rest of the monomials in the dual basis. In Figure 3.4 , black dots are the basis for $Q_1^\perp$ and the white dots are the rest of the monomials in the dual basis.

Considering the above figures, one can see that the extended Buchberger diagram includes the Buchberger diagram with respect to every order. $\mathcal{N}$ is a bound for the degree of the members of a Gröbner basis with respect to every order. Directional multiplicity with respect to an axis is the largest intersection point of the extended Buchberger diagram with that axis. The Buchberger diagram does not necessarily have an intersection with the hyperplane $x_1 + \cdots + x_n = \mathcal{N}$, but the extended Buchberger diagram does have at least a point in common with that hyperplane.

Example 64. Let $I = \langle f_1 = x^8 + y^5, f_2 = x^7y^4 \rangle$. Origin is the root of the system with multiplicity $\mu = 67$. We have that $\mathcal{N} = 18$, while $\mu_1 = 15, \mu_2 = 9$. The reduced Gröbner basis for

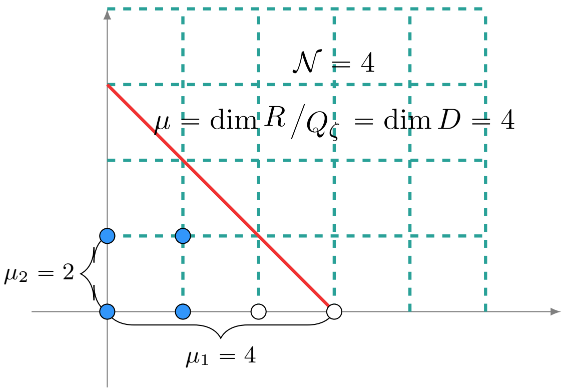


Figure 3.2: Extended Buchberger Diagram vs a Basis for B_ζ wrt a Degree Ordering for Example 67

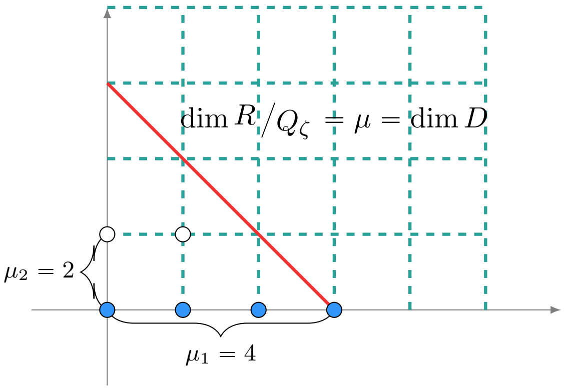


Figure 3.3: Extended Buchberger Diagram vs Directional Multiplicity wrt x for Example 67

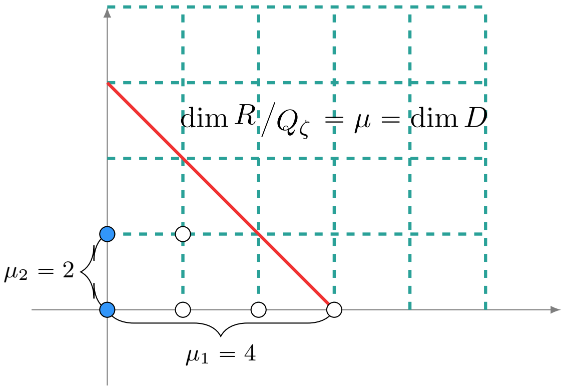


Figure 3.4: Extended Buchberger Diagram vs Directional Multiplicity wrt y for Example 67

I with respect to the lexicographic order ($x > y$) is $\{f_1 = x^8 + y^5, f_2 = x^7y^4, g_y = y^9\}$, and with respect to lexicographic order ($y > x$) is $\{f_1 = y^5 + x^8, f_2 = y^4x^7, g_x = x^{15}\}$, where g_y and g_x are the generators of the elimination ideal with respect to the lexicographic orders $x > y$ and $y > x$ respectively.

These observations give us the intuition that the directional multiplicities are at most as large as the Nil-index. Also their product gives us the volume of a cuboid which contains the Buchberger diagram. The following statements make the comments above more precise.

Remark 65. One can easily see that the Nil-index is as large as the multiplicity and also the multiplicity is bounded by the number of lattice points in the n-simplex. The simple conclusion of the definition of $\mathcal{N}$ and μ is that

$$\mathcal{N} \leqslant \mu \leqslant \text{Number of Lattice point in the n-simplex} = \binom{\mathcal{N}+n}{n}.$$

Proposition 4. *Let μ be the multiplicity of an isolated point ζ. Then*

- $\mu_i \leqslant \mu$ *for every* $1 \leqslant i \leqslant n$.
- $\mu \leqslant \prod_{1 \leqslant i \leqslant n} \mu_i$.
- $\sum_{i=1}^{n} \mu_i - n + 1 \leqslant \mu$.

Proof. For the first part, recall that $dim_{\mathbb{K}} Q_{\zeta}^{\perp} = \mu$ and that μ_i is the dimension of a vector subspace of $Q_{\zeta}^{\perp}$. Thus $\mu_i \leqslant \mu$.
For the second part, first remember that for every $1 \leqslant i \leqslant n$, μ_i is the largest degree of the elements in $Q_{\zeta}^{\perp} \cap \mathbb{K}[d_i]$. This means that $\mu_i + 1$ is the largest possible degree of x_i in R/Q. Since $\mu = dim_{\mathbb{K}} R/Q$, we conclude that $\mu \leqslant \prod_{1 \leqslant i \leqslant n} \mu_i$.
For the third statement, note that as argued above, $dx_i^{a_i} \in Q_{\zeta}^{\perp}$ if and only if $a_i < \mu_i$. This means that $x_i^{a_i} \notin Q_{\zeta}$ if and only if $a_i < \mu_i$. Now, for all $1 \leqslant i \leqslant n$, let $A_i := \{1, x_i, \cdots, x_i^{\mu_i - 1}\}$. Then, $\langle \bigcup A_i \rangle \subseteq R/Q_{\zeta}$ as vector spaces. Note that the elements of $\bigcup A_i$ are linearly independent. Then $dim\langle \bigcup A_i \rangle = \sum \mu_i - n + 1 \leqslant dim R/Q_{\zeta} = \mu$ and the result follows. □

Proposition 5. *Let $\mathcal{N}$ be the Nil-index of Q_{ζ}. Then*

- $\mathcal{N} \geqslant \mu_i$ *for all* $1 \leqslant i \leqslant n$,
- $\mathcal{N} \leqslant \sum_{1 \leqslant i \leqslant n} \mu_i - n$

Proof. According to the definition of the Nil-index we have $\mathfrak{m}_{\zeta}^{\mathcal{N}} \nsubseteq Q_{\zeta}$ and $\mathfrak{m}_{\zeta}^{\mathcal{N}+1} \subseteq Q_{\zeta}$. Since $\mathfrak{m}_{\zeta}^{\mathcal{N}} = \langle x_1 - \zeta_1, \ldots, x_n - \zeta_n \rangle^{\mathcal{N}}$, therefore $(x_i - \zeta_i)^{\mathcal{N}} \notin Q_{\zeta}$ and $(x_i - \zeta_i)^{\mathcal{N}+1} \in Q_{\zeta}$. By the definition of μ_i and the Proposition 2, $dx_i^{\mu_i}(x_i - \zeta_i)^{\mathcal{N}} = 0$ and $dx_i^{\mu_i}(x_i - \zeta_i)^{\mathcal{N}-1} \neq 0$. Therefore $\mu_i \leqslant \mathcal{N}$.

For the second part, note that for all x_i, $d_{x_i}^{\mu_i - 1} \in supp(Q_\zeta^\perp)$ and $d_{x_i}^{\mu_i} \notin supp(Q_\zeta^\perp)$. Therefore by Proposition 2, $x_i^{\mu_i - 1} \notin Q_\zeta$ and $x_i^{\mu_i} \in Q_\zeta$. Consider $A = \{\mathbf{a} \in \mathbb{N}^n | \ |\mathbf{a}| = \sum(\mu_i - 1) + 1\}$. By the Pigeonhole principle, there exists an i, $1 \leqslant i \leqslant n$, such that $x_i^{\mu_i} | x^{\mathbf{a}}$. Therefore $x^{\mathbf{a}} \in Q_\zeta$ for all $\mathbf{a} \in A$, which implies that $\mathfrak{m}_\zeta^{|\mathbf{a}|} \subseteq Q_\zeta$ and $\mathcal{N} < |\mathbf{a}| = 1 + \sum(\mu_i - 1)$. The result follows by minimality of $\mathcal{N}$. □

Remark 66. The inequalities in the Propositions 4 and 5 are sharp. An example that shows this, is the univariate case, where $I = Q_\zeta \in \mathbb{K}[x]$. In this case the Nil-index of $I_1 = \mu_1$ is equal to its i-th directional multiplicity, which is equal to the degree of $(x - \zeta)$ in g, the monic generator of the elimination ideal. The latter doesn't happen by accident. We will discuss more about this in Section 4.2.

A geometric interpretation of the i-th directional multiplicity at an intersection point could be the number of copies of the intersection point that can be seen when we look at the intersection point in the direction parallel to the x_i axis.

We note that despite the simplicity of the inequalities presented, they show the importance of the directional multiplicity. Namely, knowing the directional multiplicities we can deduce information about the multiplicity or the Nil-index. The other way though is not possible. Thus, the notion of directional multiplicity is, in this sense, a refinement of multiplicity and Nil-index. Moreover, in some applications, this refined information is crucial as we will see in Section 4.1. As it has been mentioned in Chapter 1, there are several recent papers on computing Nil-index, which mostly use the dual spaces, e.g., work of Wu and Zhi [62] and Li and Zhi in [45]. Complexity of computing Nil-index using dual space has also been discussed in those articles.

3.3 Algorithms for Dual Basis and Directional Multiplicity

In this section we present modifications of Macaulay's algorithm and the integration method for computing a basis for the dual space efficiently. Also the algorithms give us the directional multiplicities as well. Before presenting our modifications, we review two approaches for computing the dual space of an $\mathfrak{m}_\zeta$-primary component of a given ideal $I = \langle f_1, \ldots, f_e \rangle \subseteq \mathbb{K}[x_1, \ldots, x_n]$. We refer the reader to [48] for a recent overview.

These algorithms compute a basis D for $Q^\perp$ degree by degree. Let D_t be the subset of $\mathbb{K}[\partial_\zeta]$ that contains degree t elements of D. Then $D_0 = \langle 1 \rangle$. The algorithms extends D_t into D_{t+1}, a basis for the degree $t + 1$ part of $Q^\perp$, until $D_t = D_{t+1}$. Then we can conclude that $D = D_t$ and we have the basis D. We set $d_i := dx_i$ for presentation reasons in what follows.

3.3.1 Macaulay's Algorithm

Macaulay's algorithm [46] is the first algorithm for computing a basis for the dual space $Q^\perp$. It is based on a simple condition that the coefficients of the elements of the dual space must fulfill. Let $\Lambda = \sum\limits_{|\alpha| \leqslant \mathcal{N}} \lambda_\alpha d^\alpha$, where we use the multi-index notation with $d = d_1 d_2 \cdots d_n$. Then $\Lambda(f) = 0, \ \forall f \in I$ if and only if $\Lambda(x^\beta f_i) = 0, \ \forall \beta \in \mathbb{N}^n$ and $1 \leqslant i \leqslant e$. This observation, for $1 \leqslant |\beta| \leqslant \mathcal{N}$, reduces checking that $\Lambda(f) = 0$ for an infinite number of polynomials f into

checking the finitely many conditions that are given in the right hand side. Namely, it suffices to impose conditions on λ_α's, the coefficients of Λ. For $1 \leqslant |\beta| \leqslant \mathcal{N}$, we obtain a system of linear homogeneous equations and construct the corresponding matrix. The rows of this matrix are labeled by $x^\beta f_i$ and the columns are labeled by d^α. Every element in the kernel of this matrix is a coefficient vector, corresponding to an element of D.
Macaulay's algorithm starts with $D_0 = \{d^0 = 1\}$. At step t, the algorithm computes the polynomials $\Lambda(x^\alpha f_i)$ for $\deg(\Lambda) \leqslant t$ and constructs the coefficient matrix. The kernel of this matrix contains coefficient vectors of elements of a basis D_t. If $D_t = D_{t-1}$, then the algorithm terminates, otherwise continues with computing D_{t+1}.

```
Algorithm 1: Macaulay's Algorithm
  Input  : A basis for an $\mathfrak{m}_\zeta$-primary ideal $Q_\zeta$
  Output A basis for $D$, the dual of $Q_\zeta$
  :
  def ComputeBasis:
      $D_{\text{old}} = \varnothing$
      $D_{\text{new}} = \{\Lambda = d^0 = 1\}$
      while $D_{\text{old}} \neq D_{\text{new}}$:
          $D_{\text{old}} = D_{\text{new}}$
          Construct matrix $M_{\text{new}}$, the coefficient matrix of $D_{\text{new}}$
          $D_{\text{new}} = \text{kernel}(M_{\text{new}})$
      return $D_{\text{new}}$
```

We illustarte the algorithm by two examples.

Example 67. Let

$$\begin{aligned} f_1 &= x^2 + (y-1)^2 - 1 \\ f_2 &= y^2. \end{aligned}$$

Then for the root $(0,0)$, we have that

$$M_1 = \begin{array}{c} \\ f_1 \\ f_2 \end{array} \begin{array}{c} \begin{array}{ccc} 1 & d_1 & d_2 \end{array} \\ \begin{pmatrix} 0 & 0 & -2 \\ 0 & 0 & 0 \end{pmatrix} \end{array}. \tag{3.2}$$

The kernel of this matrix is $D_1 = \{1, d_1\}$. In the second step, we have

$$M_2 = \begin{array}{c|cccccc} & 1 & d_1 & d_2 & d_1^2 & d_1 d_2 & d_2^2 \\ \hline f_1 & 0 & 0 & -2 & 1 & 0 & 1 \\ f_2 & 0 & 0 & 0 & 0 & 0 & 1 \\ x_1 f_1 & 0 & 0 & 0 & 0 & -2 & 0 \\ x_1 f_2 & 0 & 0 & 0 & 0 & 0 & 0 \\ x_2 f_1 & 0 & 0 & 0 & 0 & 0 & -2 \\ x_2 f_1 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}, \tag{3.3}$$

from which we have $D_2 = \{1, d_1, 2d_1^2 + d_2\}$. The algorithm runs until step 4, during which we have a matrix of size 20×15, and

$$D_3 = D_4 = \{1, d_1, 2d_1^2 + d_2, 2d_1^3 + d_1 d_2\}.$$

Thus, $\mu = 4, \mu_1 = 4$ and $\mu_2 = 2$.

Example 68. Let

$$\begin{aligned} f_1 &= y^3 \\ f_2 &= x^2 y^2 \\ f_3 &= x^4 - x^3 y. \end{aligned}$$

The matrices in the first, second and third steps of the algorithm are zero matrices. So we have $D_1 = \{1, d_1, d_2\}, D_2 = \{1, d_1, d_2, d_1^2, d_1 d_2, d_2^2\}$ and

$$D_3 = \{1, d_1, d_2, d_1^2, d_1 d_2, d_2^2, d_1^3, d_1 d_2^2, d_1^2 d_2\}.$$

The computation goes on till step 5, during which we have a matrix of size 45×21 whose kernel gives the dual basis

$$D_4 = D_5 = \{1, d_1, d_2, d_1^2, d_1 d_2, d_2^2, d_1^3, d_1 d_2^2, d_1^2 d_2, d_1^4 + d_1^3 d_2\}.$$

Thus, $\mu = 10, \mu_1 = 5$ and $\mu_2 = 3$.

3.3.2 Integration method

Macaulay's algorithm is not efficient. In every step it builds new matrices which include previously constructed matrices, thus some computations are repeated.

In [53], Mourrain suggested another algorithm, which builds smaller matrices. Later, Mourrain and Mantzaflaris improved Mourrain's algorithm in [47]. We will demonstrate the improved version in this section. We first present the necessary background.

Given a basis for the vector space $B_\zeta = \mathbb{K}[x_1, \ldots, x_n] / Q_\zeta$, one can construct a basis D for $Q^\perp$ and vice versa. This can be deduced from the constructions in the work of Macaulay in [46]. The work of Mourrain in [53], shows the construction explicitly. Moreover, Mourrain has shown how to construct a Gröbner basis for Q_ζ having a basis for $Q^\perp$. Below we will explain the construction of D from a basis of B_ζ as in [47] in brief.

For every $\Lambda \in Q^\perp$, let $Supp(\Lambda)$ be the set of monomials that have a non-zero coefficient in Λ. Proposition 2 says that $\partial^{\mathbf{a}} \in Supp(\Lambda)$ if and only if $x^{\mathbf{a}} \notin Q_\zeta$ for $\mathbf{a} \in \mathbb{N}^n$. Let us denote by $Supp(Q^\perp)$ the union of supports of all elements of $Q^\perp$ and by s its cardinality. Then

$$Supp(Q^\perp) = \bigcup_{\Lambda \in Q^\perp} \{Supp(\Lambda)\} = \{\partial^{\mathbf{a}} | x^{\mathbf{a}} \notin Q_\zeta\}.$$

Since the degree of the monomials in $Supp(Q^{\perp})$ is bounded by the Nil-index of Q_{ζ}, the above sets are finite. One can find a basis $B = \{x^{\beta_1}, \ldots, x^{\beta_\mu}\}$ for B_{ζ} among the monomials in the above set. Then for every monomial $x^{\gamma_j} \in Supp(Q^{\perp})$ such that $x^{\gamma_j} \notin B$ we can write

$$x^{\gamma_j} = \sum_{i=1}^{\mu} \lambda_{ij} x^{\beta_i} \mod Q_{\zeta}.$$

Now let

$$\Lambda_i = d^{\beta_i} + \sum_{j=1}^{s-\mu} \lambda_{ij} d^{\gamma_j}. \tag{3.4}$$

Then we have the following theorems that explain the relationship between a monomial basis for the quotient and a basis for the dual as well as a Gröbner basis for the ideal.

Theorem 69 (Lemma 2.4 in [47]). *With the above notation, $\{\Lambda_1, \ldots, \Lambda_\mu\}$ is a basis for $Q^{\perp}$ and the normal form of any $g \in \mathbb{K}[x_1, \ldots, x_n]$ with respect to B is*

$$NF(g) = \sum_{i=1}^{\mu} \Lambda_i(g) x^{\beta_i}.$$

Theorem 70 (Proposition 3.7 in [53]). *Let $\prec$ be a term order and $1 \prec x^{\beta_1} \prec \cdots \prec x^{\beta_\mu}$. Using the above notation, let $G := \{g_{\gamma_j} := x^{\gamma_j} + \sum_{i+1}^{\mu} x^{\beta_i} | 1 \leqslant j \leqslant s\}$ and $C := \{x^{\mathbf{c}} | \quad |c| = \mathcal{N} + 1\}$. Then $G \cup C$ is a Gröbner basis for Q with respect to $\prec$.*

Given a basis D for $Q^{\perp}$, consider the matrix $M \in \mathbb{K}^{\mu \times s}$ of the coefficients of the elements of this basis. Every set of μ independent columns of M give a basis for B_{ζ}. Let G be the matrix whose columns are the columns of M indexed by d^{β_i}. Then

$$G^{-1}M = \begin{array}{c} \\ \Lambda'_1 \\ \vdots \\ \Lambda'_\mu \end{array} \begin{array}{c} \begin{array}{cccccc} \beta_1 & \cdots & \beta_\mu & \gamma_1 & \cdots & \gamma_{s-\mu} \end{array} \\ \begin{pmatrix} 1 & & 0 & \lambda_{1,1} & \cdots & \lambda_{1,s-\mu} \\ & \ddots & & \vdots & & \vdots \\ 0 & & 1 & \lambda_{\mu,1} & \cdots & \lambda_{\mu,s-\mu} \end{pmatrix} \end{array}, \tag{3.5}$$

which gives a basis of the form 3.4.
Having the above matrix construction, we are ready to explain Mourrain's algorithm. The algorithm is based on *integrating* elements of $Q_{t-1}^{\perp}$ in order to generate the elements of $Q_t^{\perp}$ with symbolic coefficients, and then applying necessary and sufficient conditions on the generated elements, gives a system of equations for the coefficients. Similar to Macaulay's algorithm, each vector in the kernel of the matrix determines the coefficients of an element in $Q_t^{\perp}$. The following definition is useful in what follows.

Definition 71. *For every $\Lambda \in \mathbb{K}[\partial]$ and $1 \leqslant i \leqslant n$, denote by $\int_i \Lambda$ the i-th integral of Λ, which is defined as follows.*

$$\int_i \Lambda = \Phi \in \mathbb{K}[\partial] \textit{ such that } d_i(\Phi) = \Lambda \textit{ and } \Phi(d_1, \ldots, d_{i-1}, d_i = 0, d_{i+1}, \ldots, d_n) = 0.$$

The next theorem is the combination of Mourrain's algorithm in [53] and the improvement presented by Mantzaflaris and Mourrain in [47].

Theorem 72 ([53, 47])**.** *Let $\{\Lambda_1, \dots, \Lambda_m\}$ be the basis D_{t-1} with the coefficient matrix of the form 3.5, yielding the standard basis $B_t = \{x^{\beta_i} | 1 \leqslant i \leqslant m\}$, i.e., the elements of the basis B that are of degree up to t. An element $\Lambda \in \mathbb{K}[\partial]$ with no constant term is in D_t if and only if it is of the form*

$$\Lambda = \sum_{i=1}^{m} \sum_{k=1}^{n} \lambda_{ik} \int_k \Lambda_i(d_1, \dots, d_k, 0, \dots, 0), \tag{3.6}$$

where $\lambda_{ij} \in \mathbb{K}$, and the following conditions hold

1. *for all $1 \leqslant k < l \leqslant n$,*
$$\sum_{i=1}^{1} \lambda_{ik} d_l(\Lambda_i) - \sum_{i=1}^{1} \lambda_{il} d_k(\Lambda_i) = 0. \tag{3.7}$$

2. *for all $1 \leqslant k \leqslant e$,*
$$\Lambda(f_k) = 0 \tag{3.8}$$

3. *for all $1 \leqslant i \leqslant m$,*
$$\Lambda(x^{\beta_i}) = 0. \tag{3.9}$$

The first condition implies that the new elements Λ that have been introduced are stable by derivation. The second condition comes from the fact that Λ must be inside $Q_\zeta^\perp$. Based on Theorem 72, having $D_{t-1} = \{\Lambda_1, \dots, \Lambda_m\}$, we have an algorithmic way to compute D_t. Consider Λ from the theorem with symbolic coefficients λ_{ik}. Plug Λ into the conditions of the theorem and obtain a system of equations. In step t the corresponding matrix will look like below.

$$M_t = \begin{array}{l|ccccccc|} & \lambda_{11}p_{11} & \dots & \lambda_{1n}p_{1n} & \dots & \lambda_{e1}p_{e1} & \dots & \lambda_{en}p_{en} \\ \Lambda(f_1) & & & & & & & \\ \vdots & & & & & & & \\ \Lambda(f_e) & & & & & & & \\ \text{Condition 3.7} & & & & & & & \\ \text{Condition 3.9} & & & & & & & \end{array}. \tag{3.10}$$

By abuse of notation and for simplifying the presentation, we use the symbolic coefficients λ_{ij} instead of the product of λ_{ij} by the polynomials $p_{ij} = \int_j \Lambda_i(d_1, \dots, d_j, 0, \dots, 0)$ in order to label the columns of M_t. The kernel of M_t will give us the possible values for λ_{ij}.

The first two conditions already guarantee that $\Lambda \in D_t$ [53]. However, we might have that $\Lambda \in D_{t-1}$ as well. This means that we reproduce the elements of the previous step. The third condition which has been introduced in [47], gives us a sufficient condition for having $\Lambda \in D_t \backslash D_{t-1}$. This helps with avoiding repetition of the computations that have been done in the previous steps by adding new rows to the matrix, which in some cases may lead to removing some column. It also provides a method to compute a basis D at the same time as a dual basis for B_ζ.

Algorithm 2: Integration method

```
Input  : A basis for an $\mathfrak{m}_\zeta$-primary ideal $Q_\zeta$
Output  A basis for $R/Q_\zeta$ and a basis $D$ for $Q_\zeta^\perp$
:
def ComputeBasis:
    $D_{\text{old}} = \varnothing$
    $D_{\text{new}} = \{\Lambda = d^0 = 1\}$
    while $D_{\text{old}} \neq D_{\text{new}}$:
        $D_{\text{old}} = D_{\text{new}}$
        $\Lambda := \sum_{i=1}^{m} \sum_{k=1}^{n} \lambda_{ik} \int_k \Lambda_i(d_1, \ldots, d_k, 0, \ldots, 0)$
        for all $1 \leqslant k \leqslant l \leqslant n$, $\sum_{i=1}^{m} \lambda_{ik} d_l(\Lambda_i) - \sum_{i=1}^{m} \lambda_{il} d_k(\Lambda_i) = 0$
        for all $1 \leqslant k \leqslant e$, $\Lambda(f_k) = 0$
        for all $1 \leqslant k \leqslant m$, $\Lambda(x^{\beta_i}) = 0$
        Construct matrix $M_{\text{new}}$, the coefficient matrix of $\Lambda$
        Compute a basis $K_{\text{new}}$ for kernel($M_{\text{new}}$)
        $D_{\text{new}} = D_{\text{old}} \bigcup K_{\text{new}}$
    return new
```

Below, we do the computations for Examples 67 and 68, first without and then with considering Condition 3.9.

Example 73 (Computations without Condition 3.9 for Example 67)**.**

$$M_1 = \begin{array}{c} \\ \Lambda(f_1) \\ \Lambda(f_2) \end{array} \begin{array}{c} \begin{array}{cc} d_1 & d_2 \end{array} \\ \begin{pmatrix} 0 & -2 \\ 0 & 0 \end{pmatrix} \end{array}. \tag{3.11}$$

which is the same as the matrix in Macaulay's algorithm, and $D_1 = \{1, d_1\}$. Continuing into the second step ($\Lambda \in D_2$), we apply the first two conditions on $\Lambda = \lambda_1 d_1 + \lambda_2 d_2 + \lambda_3 d_1^2 + \lambda_4 (d_1 d_2)$, which gives us the matrix

$$M_2 = \begin{array}{c} \\ \mathrm{C}ondition3.7 \\ \Lambda(f_1) \\ \Lambda(f_2) \end{array} \begin{array}{c} \begin{array}{cccc} d_1 & d_2 & d_1^2 & d_1 d_2 \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & -2 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \end{array}, \tag{3.12}$$

which has two columns less that the second matrix of Macaulay's algorithm. We have $D_2 = \{1, 2d_1^2 + d_2, d_1\}$. The third and fourth step matrices are also smaller than the ones in Macaulay's algorithm.

Example 74 (Computations for Example 67 with Condition 3.9)**.** I this case the matrix of D_1 is the same, while the matrices for D_2 and D_3 are different.

$$M_1 = \begin{array}{c} \\ \Lambda(f_1) \\ \Lambda(f_2) \end{array} \begin{array}{c} \begin{array}{cc} d_1 & d_2 \end{array} \\ \begin{pmatrix} 0 & -2 \\ 0 & 0 \end{pmatrix} \end{array}, \tag{3.13}$$

which is the same as the matrix in Macaulay's algorithm, and $D_1 = \{1, d_1\}$.
In step 2 we have

$$M_2 = \begin{array}{l} \\ \mathrm{C}ondition 3.9 \\ \mathrm{C}ondition 3.7 \\ \Lambda(f_1) \\ \Lambda(f_2) \end{array} \begin{array}{c} \begin{array}{cccc} d_1 & d_2 & d_1^2 & d_1d_2 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & -2 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \end{array}. \tag{3.14}$$

Condition 3.9 implies that $\lambda_1 = 0$. Therefore we can remove column one from M_2.

Example 75 (Computations with and without Condition 3.9 for Example 68)**.** $D_0 = \{1\}$. If we do the computations without considering Condition 3.9, then in step 2 of the integration method, we will reach to a 3×2 zero matrix, which has one column less than the matrix in Macaulay's algorithm. The matrix in step 3 is a 3×5 zero matrix, which is much smaller than the matrix in Macaulay's method.
Re-doing the computations considering Condition 3.9, we get M_0 and M_1 same as above. In step 2, M_2 is a matrix of size 5×5. The two extra rows in this case comes from Condition 3.9. However each of the two last rows simply will have one nonzero coordinate, which implies that two of the coefficients λ_{ij} are zero. Having the value of a coefficient equal to zero means that we can remove the corresponding column from the matrix and therefore the size of the matrix will finally be 3×3, smaller than the previous one. In step 3, applying Condition 3.9, we will get a matrix with 4 columns instead of 9 columns in the previous case.

In the next subsection we will show modifications on the above algorithms in order to make them more efficient for computing the directional multiplicities.

3.3.3 Modified Algorithms for Dual Basis

In this subsection we present modifications to the integration method and Macaulay's algorithms, which make computations more efficient. In particular, we give a more efficient criterion than Condition 3.9 in the integration method.
We will use the following notation throughout subsection 3.3.3. We denote the Nil-index by $\mathcal{N}$. Let t be a fixed number between 1 and $\mathcal{N}$. We refer to the current step of the algorithm as step t. Same as previous sections, D is a basis for $Q^\perp$ and therefore $\langle D \rangle = Q^\perp$. D_t stands for the degree t part of a basis of $Q^\perp$. Obviously $\langle D_t \rangle$ is a sub-vector space of $\langle D \rangle$. If we assume that D_t is equipped with a total degree term order, e.g. degree lexicographic ordering, then the leading term of an element Λ of D_t is denoted by $\mathrm{lt}(\Lambda)$. If v is a column of a matrix M, then $M - v$ denotes the matrix obtained by deleting the column v from M.

Modifications on Integration Method

Let M_t denote the matrix in step t of the integration method and $\widetilde{M_t}$ denote the matrix that is constructed in step t without considering Condition 3.9. We assume that $D_{t-1} = \{\Lambda_1, \ldots, \Lambda_m\}$ is already computed in step $t-1$.

In the integration method, columns of M_t (similarly for $\widetilde{M_t}$) are labeled by the λ_{ij}'s appearing in Λ (see Equation 3.10). Fix one of the λ_{ij}'s and call it λ. We denote by v_λ the column of M_t (similarly for $\widetilde{M_t}$) that is indexed by λ. Then p_λ denotes the corresponding polynomial.

A basis D of $Q^\perp$ is in one to one correspondence with a basis K for $Ker(\widetilde{M_\mathcal{N}})$ (similarly for $Ker(\widetilde{M_t})$). In step t, this correspondence is reduced to a correspondence between D_t and K_t, a basis of $Ker(\widetilde{M_t})$). If there exists a vector $q \in K_t$, for which the coordinate corresponding to λ in this vector is nonzero, then we say that v_λ is active in D_t. In case we explicitly know such a vector q, i.e., a particular element of the kernel corresponding to an element E of D_t, then we say that v_λ is active in E. Since, M_{t-1} is a submatrix of M_t and $\widetilde{M_{t-1}}$ is a submatrix of $\widetilde{M_t}$, if it is clear from the context, by *a column of* M_{t-1}(respectively $\widetilde{M_{t-1}}$) we will refer to the corresponding column in M_t(respectively $\widetilde{M_t}$) as well. We work on $\widetilde{M_t}$ rather than M_t in this section, although many of our arguments are correct for M_t as well.

We start with a proposition that provides us with an improvement on the integration method, related to Condition 3.9.

Proposition 6. *Let $\widetilde{M_t}, \widetilde{M_{t-1}}, D_t, \Lambda_i$ $(1 \leqslant i \leqslant m), \lambda, p_\lambda$ and v_λ be as above. Then the following hold.*

1. *If v_λ is a column of $\widetilde{M_t}$, then v_λ is active in D_t if and only if v_λ can be reduced to zero by some other columns of $\widetilde{M_t}$.*

2. *For all $1 \leqslant i \leqslant m$, if v_{λ_i} is active in Λ_i, K'_{t_i} is a basis for $Ker(\widetilde{M_t} - v_{\lambda_i})$ and D'_{t_i} is the set of its correspondent dual elements, then $\{\Lambda_i\} \cup D'_{t_i}$ is a basis for the degree t part of $Q^\perp$. Moreover, if v_{λ_i} is active in Λ_i, but is not active in Λ_j, $1 \leqslant j \neq i \leqslant m$, then there exists a basis D'_{t_i} such that $\Lambda_j \in D'_{t_i}, j \neq i$.*

3. *Let $K_{t_{1\ldots m}}$ be a basis for $Ker(\widetilde{M_t} - v_{\lambda_1} - \cdots - v_{\lambda_m})$ and $D_{t_{1\ldots m}}$ be the set of its correspondent dual elements. For all $1 \leqslant i \leqslant m$, if v_{λ_i} is active in Λ_i, but is not active in $1, \ldots, \Lambda_{i-1}$, then $D_{t-1} \cup D_{t_{1\ldots m}}$ is a basis for the degree t part of $Q^\perp$.*

Proof.

1. Let $v_\lambda, v_1, \ldots, v_k$ denote the columns of $\widetilde{M_t}$ and $p_\lambda, p_1, \ldots, p_k$ be the polynomials labeling the columns of $\widetilde{M_t}$. Then v_λ can be reduced to zero by $v_1, \ldots, v_k$ if and only if there exist $c_1, \ldots, c_k \in \mathbb{K}$, such that $v_\lambda = c_1 v_1 + \cdots + c_k v_k$, or equivalently $v_\lambda - c_1 v_1 - \cdots - c_k v_k = 0$. This holds if and only if $q := (1, c_1, \cdots, c_k) \in K_t$, which holds if and only if $\Lambda' := p_\lambda - c_1 p_1 - \cdots - c_k p_k \in D_t$ (Note that this is exactly the fact that Λ' in D_t corresponds to $q \in K_t$). The latter is the case if and only if v_λ is active in Λ', or equivalently v_λ is active in D_t.

2. Fix $1 \leqslant i \neq j \leqslant m$ and let q_i and q_j be the elements of K_t corresponding to Λ_i and Λ_j in D_t, respectively.

First we prove that for all $\Lambda' \in D_t$ if $\Lambda' \neq \Lambda_i$, then $\Lambda' \in \left\langle D'_{t_i} \cup \{\Lambda_i\} \right\rangle$. Let q' be the corresponding elements of Λ' in K_t. If v_{λ_i} is not active in Λ', then by part 1 it cannot be reduced to zero by the active columns in Λ'. So the column v_{λ_i} is not involved in computing Λ' via column reducing in $\widetilde{M}_t$. So Λ' can be computed via column reducing in $\widetilde{M}_t - v_\lambda$. Let q' be the corresponding element to Λ' in $Ker(\widetilde{M}_t)$. Then $q' \in Ker(\widetilde{M}_t - v_\lambda)$. This means that $\Lambda' \in \left\langle D'_{t_i} \right\rangle$.

If v_{λ_i} is active in Λ', then we prove that there exists a Λ'' in D'_{t_i} such that $\Lambda' = \Lambda_i + \Lambda''$. This is because of the following. Let $q' \in K_t$ be the element corresponding to $\Lambda' \in D_t$, such that that the first coordinate of q' corresponds to v_{λ_i}. Take $q' = (1, b_1, \ldots, b_k)$. Then we have that $v_{\lambda_i} + b_1 v1 + b_2 v_2 + \cdots b_k v_k = 0$, where the columns $v_1, \ldots, v_k$ are as in the proof of part 1. Also again as in the proof of the part 1, $v_{\lambda_i} = c_1 v_1 + \cdots + c_k v_k$. Therefore $(b_1 - c_1) v_1 + \cdots + (b_k - c_k) v_k = 0$, which means that $(0, b_1 - c_1, \ldots, b_k - c_k) \in Ker(\widetilde{M}_t)$, and therefore $q'' := (b_1 - c_1, \ldots, b_k - c_k) \in Ker(\widetilde{M}_t - v_\lambda)$. So one can construct a basis K'_{t_i} in such a way that $q'' \in K'_{t_i}$. Let Λ'' be the member of D'_{t_i} corresponding to q''. Then $\Lambda' = \Lambda_i + \Lambda''$.

Secondly we note that if v_{λ_i} is not active in Λ_j, for $1 \leqslant j \neq i \leqslant m$, then by the above argument, one can compute a basis K'_{t_i} (and respectively, D'_{t_i}) in such a way that $\Lambda_j \in D'_{t_i}$.

So every element of D_t can be obtained from Λ_i and an element of K'_{t_i} and therefore $\langle D_t \rangle \subseteq \left\langle \{\Lambda_i\} \cup D'_{t_i} \right\rangle$. Linear independence of the elements of $\{\Lambda_i\} \cup D'_{t_i}$ is clear, and therefore $\langle D_t \rangle = \left\langle \{\Lambda_i\} \cup D'_{t_i} \right\rangle = Q^\perp$.

3. $K_{t_{1\ldots l}}$ be a basis for $Ker(\widetilde{M}_t - v_{\lambda_1} - \cdots - v_{\lambda_l})$ and $D_{t_{1\ldots l}}$ the correspondent dual elements. Also as in the proof of the previous parts, let K_t be a basis for $Ker(\widetilde{M}_t)$ and also let $q_1, \ldots, q_m \in K_t$ correspond to $\Lambda_1, \ldots, \Lambda_m$ respectively. Then from the proof of part 2 we have that $\{q_1\} \cup K_{t_1}$ is a basis for $Ker(\widetilde{M}_t)$. Also by part 2 of the proposition, $q_2, \ldots, q_m \in \langle K_t \rangle$ and correspondingly $\Lambda_2, \ldots, \Lambda_m \in \langle D_{t_1} \rangle$. Now consider the matrix $\widetilde{M}_t - v_{\lambda_1}$ and the basis D_{t_1} obtained from it. Since v_{λ_2} is active in Λ_2 (which corresponds to q_2 in K_t), and it is not active in Λ_1, then we can apply part 2 of the proposition to the matrix $\widetilde{M}_t - v_{\lambda_1}$ and the basis D_{t_1} obtained by it. Then we will have that $\{q_2\} \cup K_{t_{12}}$ is a basis for $Ker(\widetilde{M}_t - v_{\lambda_1})$ and $q_3, \ldots, q_m \in \langle K_{t_{12}} \rangle$. Correspondingly, $\Lambda_3, \ldots, \Lambda_m \in \langle D_{12} \rangle$. This implies that $\{q_1, q_2\} \cup K_{t_{12}}$ is a basis for $Ker(\widetilde{M}_t)$. Continuing with $v_{\lambda_i},\ i \geqslant 3$, and considering the assumption that v_{λ_i} is not active in $\Lambda_1, \ldots, \Lambda_{i-1}$, $j \neq i$, we finally get $\{q_1, \ldots, q_m\} \cup K_{t_{1\ldots m}}$ as a basis for $Ker(\widetilde{M}_t)$ and correspondingly $\{\Lambda_1, \ldots, \Lambda_m\} \cup D_{1\ldots m}$ as a basis for the degree t part of $Q^\perp$

□

The above proposition shows us that deleting some columns from $\widetilde{M}_t$ helps us to avoid re-computing the basis elements of degree at most $t-1$, which were already computed in the previous steps. Not every set of m active columns will give us degree t elements of a basis. In fact if we delete two columns that both are active in two different basis members of D_{t-1}, then

we may not obtain some members of D_t, For instance Let $D_2 = \{\Lambda_1 = d_1 + d_2 + d_1^2 + d_2^2, \Lambda_2 = d_1 + d_2 + 2d_1^2 + d_1d_2\}$ and $\Lambda' = d_1 + d_2^3 \in Ker(\widetilde{M_3})$. Then $\Lambda' \notin Ker(\widetilde{M_3} - v_{d_1} - v_{d_2})$.
Choosing the appropriate columns can be seen as a combinatorial problem. For each element of D_{t-1}, if we consider sets corresponding to the active columns in that element, then a set of columns that satisfy the assumptions of part 3 of Proposition 6 form a *System of Distinct Representatives*. However, not every set of distinct representatives gives us the appropriate columns. The above example shows this. There are combinatorial and graph theoretical equivalences for the above conditions.
In the following we show how to detect columns $v_{\lambda_1}, \ldots, v_{\lambda_m}$ that satisfy the assumption of part 3 of Proposition 6. This is basically done via changing the basis $\{\Lambda_1, \ldots, \Lambda_m\}$ into a new *reduced* basis $\{\Lambda'_1, \ldots, \Lambda'_m\}$, in which their leading terms satisfy the assumptions of part 3 of Proposition 6.
Let $D_{t-1} = \{\Lambda_1, \ldots, \Lambda_m\}$ as above. Remember that having D_{t-1}, one can construct Matrix 3.5 in order to obtain a basis for the degree t part of $R/_Q$, so that Condition 3.9 can be applied. Below we show constructing a similar, but smaller matrix which gives us the desired set of active columns. Same as $\widetilde{M_t}$, the columns of this matrix are labeled by the coefficients/polynomials that appear in Λ in Equation 3.6. Same as Matrix 3.5, the rows of this matrix come from $\Lambda_1, \ldots, \Lambda_m$. Let $v_{\lambda_1}, \ldots, v_{\lambda_u}$ be the columns of $\widetilde{M_t}$ such that they are active in D_{t-1}. Construct the following matrix containing the columns $v_{\lambda_1}, \ldots, v_{\lambda_u}$.

$$M' = \begin{array}{c} \\ \Lambda_1 \\ \vdots \\ \Lambda_m \end{array} \begin{array}{c} \text{Columns' labeled same as } \widetilde{M_t} \\ \left(\begin{array}{ccc} & & \\ v_{\lambda_1} & \cdots & v_{\lambda_s} \\ & & \end{array} \right) \end{array}, \tag{3.15}$$

Changing M' into a row echelon form matrix, after moving the pivot columns to the left hand, we will reach to a matrix of the following form.

$$G'^{-1}M' = \begin{array}{c} \Lambda'_1 \\ \Lambda'_2 \\ \vdots \\ \Lambda'_m \end{array} \left(\begin{array}{cccccccc} * & & * & & & & & \\ 0 & \ddots & & & * & & & \\ \vdots & \ddots & * & & & & & \\ 0 & \cdots & 0 & * & * & \cdots & * & \end{array} \right), \tag{3.16}$$

where diagonal entries are nonzero and G' is the matrix that takes care of the operations done for the column swapping and the row echelon form. Note that we will not have any zero row. This is because otherwise, if we obtain a zero row in $G'^{-1}M'$, then it means that that row is linearly dependent to the other rows. But this is in contradiction with $\Lambda_1, \ldots, \Lambda_m$ (and therefore $\Lambda'_1, \ldots, \Lambda'_m$ as their linear combination) being linearly independent. Then our basis will satisfy the conditions of part 3 of Proposition 6.
Another quite similar method for choosing appropriate active columns to delete is the following. Instead of M', consider the submatrix of M_{t-1} that contains only the active columns and

triangulate it. Then as above. first columns are the appropriate active columns that we can delete from M_t. This matrix has the same number of columns as M', while it might have more rows. Now we are ready to prove the following, which provides us with an algorithmic improvement of the integration method, more efficient than Condition 3.9.

Corollary 76. ***(Criterion for Deleting Active Columns)*** *Let $D_{t-1} = \{\Lambda_1, \cdots, \Lambda_m\}$, $\widetilde{M_t}$, $D_t, v_{\lambda_1}, \ldots, v_{\lambda_u}$ and $G'^{-1}M'$ be as in Equation 3.16, and (by abuse of notation) let $v_{\lambda_1}, \ldots, v_{\lambda_m}$ be the columns of $\widetilde{M_t}$ corresponding to the first m columns in $G'^{-1}M'$. Also let $K_{t_{1\ldots m}}$ be a basis for $Ker(\widetilde{M_t} - v_{\lambda_1} - \cdots - v_{\lambda_m})$ and $D_{t_{1\ldots m}}$ be the set of its corresponding dual elements. Then $D_{t-1} \cup D_{t_{1\ldots m}}$ is a basis for the degree t part of $Q^{\perp}$.*

Proof. We only need to prove that the columns $v_{\lambda_1}, \ldots, v_{\lambda_m}$ in $G'^{-1}M'$ satisfy the conditions of part 3 of Proposition 6. This is the case because for all $1 \leqslant i \leqslant m$, v_{λ_i} has zero in coordinates $i+1, \ldots, m$ and has non-zero coordinate i, which is the row corresponding to Λ_i. This means that for all $1 \leqslant i \leqslant m$, v_{λ_i} is not active in $\Lambda_1, \ldots, \Lambda_{i-1}$. Having the above argument, the result comes directly from Proposition 6. □

Comparison Between Condition 3.9 and Corollary 76 Corollary 76 provides us with an optimization in the integration method. In general this optimization is not the same as the improvement done via Condition 3.9. The difference is that our optimization allows us to delete m columns from $\widetilde{M_t}$ at step t, which brings computational efficiency reducing the size of the matrix, which is the main computational obstacle in dual basis computations, while Condition 3.9 of Theorem 72 adds one more equation to the system, i.e., one more row to the matrix at large.

The two improvements are the same only in a special case that we explain below. In all other cases, our improvement is more efficient. In Example 77 we will show these aspects of the two improvements.

Assume that the monomials $x^{\mathbf{a}_1}, \ldots, x^{\mathbf{a}_m}$ form a basis for the degree $t-1$ part of $R/_Q$. If the monomial $dx^{\mathbf{a}_i}$ only appear once in Λ in Equation 3.6, then applying Condition 3.9, we have that

$$\Lambda(x^{\mathbf{a}_i}) = \lambda dx^{\mathbf{a}_i}(x^{\mathbf{a}_i}) = \lambda_i = 0.$$

This gives us an equation which adds a row to $\widetilde{M_t}$. However, instead of adding the corresponding row to $\widetilde{M_t}$, one can just plug in $\lambda_i = 0$ in the other equations obtained from Conditions 3.7, 3.8. This will remove λ_i from the other equations, or equivalently will remove the column v_{λ_i} from $\widetilde{M_t}$. At the other hand, if we let v_{λ_i} be the only column of M_t such that its label contains $dx^{\mathbf{a}_i}$, then v_{λ_i} is active in Λ_i and therefore according to Corollary 76, one can delete it from $\widetilde{M_t}$ in order to avoid re-computing D_{t-1}. This is the only case where the two improvements on the integration method, i.e., Condition 3.9 and Corollary 76 intersect, and it is quite rare.

Having the above comments, we prove the following proposition which explicitly shows that our method is a generalization of of Mourrain-Mantzaflaris improvement, i.e., Condition 3.9.

Proposition 7. *Let $v_{\lambda_1}, \ldots, v_{\lambda_m}$ be the columns in the criterion for deleting active columns, i.e., Corollary 76. Also assume that $p_1, \ldots, p_m$ are the corresponding polynomials to the coefficients $\lambda_1, \ldots, \lambda_m$ in Λ in Equation 3.6 and let $p_i' \in \mathbb{K}[x_1, \ldots, x_n]$ be the polynomial with the same* *monomials as $p_i \in \mathbb{K}[\partial]$ for $1 \leqslant i \leqslant m$. Then $\{p_1, \ldots, p_m\}$ is a basis for the degree $t-1$ part of R/Q.*

Proof. Let $l_1, \ldots, l_m$ be the leading terms of $p_1, \ldots, p_m$. Then from the discussion in the integration method, we know that $\{l_1, \ldots, l_m\}$ is a basis for the degree $t-1$ part of R/Q. Since $p_1, \ldots, p_m \in R/Q$ and also the cardinality of $\{l_1, \ldots, l_m\}$ and $\{p_1, \ldots, p_m\}$ are the same, then in order to prove that $\{p_1, \ldots, p_m\}$ is a basis for R/Q, we just need to prove that $p_1, \ldots, p_m$ are linearly independent. Without loss of generality, we can assume that l_i appears only in p_i, $1 \leqslant i \leqslant m$. Because otherwise, we can reduce $p_1, \ldots, p_m$ with respect to each other so that we obtain polynomials $p'_1, \ldots, p'_m$ such that $l_1, \ldots, l_m$ are the leading terms of $p'_1, \ldots, p'_m$ and l_i appears only in p_i, for $1 \leqslant i \leqslant m$ and also $\langle p'_1, \ldots, p'_m \rangle = \langle p_1, \ldots, p_m \rangle$. Now this shows that $p_1, \ldots, p_m$ are linearly independent, because each leading term only appears in one single polynomial and therefore no p_i can be in the span of the other p_j, $1 \leqslant j \neq i \leqslant m$. □

Let $p'_i \in \mathbb{K}[x_1, \ldots, x_n]$ be the polynomial with the same monomials as $p_i \in \mathbb{K}[\partial]$ for $1 \leqslant i \leqslant m$. Then Proposition 7 implies that the criterion for deleting active basis can be viewed as adding the equation $\Lambda(p'_i) = 0$, for $1 \leqslant i \leqslant m$. Exactly the same as Condition 3.9, this equation leads to adding rows to $\widetilde{M_t}$, however those rows are in the form $(0, \ldots, 0, c, 0, \ldots, 0)$, where c is a nonzero element in coordinate $i, 1 \leqslant i \leqslant m$ and therefore they result in deleting the corresponding columns.
We can say even more.

Proposition 8. *Let $\{p'_1, \ldots, p'_m\} \subseteq \mathbb{K}[x_1, \ldots, x_n]$ be a (not necessarily monomial) basis for the degree t part of R/Q such that no monomial of p'_i is in Q and let $p_1, \ldots, p_m \in \mathbb{K}[\partial]$ be the polynomials with the same monomials as p'_i. For monomials $m_1, \ldots, m_k \notin Q$ such that $m_1, \ldots, m_k \notin Supp(p_1) \cup \ldots \cup Supp(p_m)$, write $m_j = \sum_{i=1}^{m} \lambda_{ij} p'_i$. Then $\Lambda_i = p_i + \sum_{j=1}^{k} \lambda_{ij} m_j$, $1 \leqslant j \leqslant m$, is a basis for the degree t part of $Q^{\perp}$ and the normal form of any $g \in \mathbb{K}[x_1, \ldots, x_n]$ with respect to the basis $\{p'_1, \ldots, p'_m\}$ is*

$$NF(g) = \sum_{i=1}^{m} \Lambda_i(g) p'_i.$$

Proof. First of all we note that $\Lambda_1, \ldots, \Lambda_m$ are linearly independent because $p_1, \ldots, p_m$ are linearly independent in R/Q, which comes from the linear independence of $p'_1, \ldots, p'_m$. The latter is the case by Proposition 7. The rest of the proof is exactly the same as the proof of Theorem 69 as it has been give in [47]. □

If $\{p'_1, \ldots, p'_m\} \subseteq \mathbb{K}[x_1, \ldots, x_n]$ is an arbitrary basis of R/Q and $\{p_1, \ldots, p_m\} \subseteq \mathbb{K}[\partial]$ are the corresponding differential polynomials, then removing the monomials in each p'_i that are in Q, we will obtain a new basis for R/Q. So this assumption in the proposition holds without loss of generality. So we have the following generalization of Lemma 3.4 in [47].

Proposition 9. *Let $\{p'_1, \ldots, p'_m\} \subseteq \mathbb{K}[x_1, \ldots, x_n]$ be a basis for the degree t part of R/Q such that no monomial of p'_i is in Q. An element $\Lambda \in \mathbb{K}[\partial]$ is not zero in $Q_t^\perp \backslash Q_{t-1}^\perp$ if and only if in addition to Equations 3.8 and 3.7 it satisfies*

$$\Lambda(p_i) = 0, \;\; 1 \leqslant i \leqslant m.$$

constructing matrices M' and $G'^{-1}M'$ in order to choose particular active columns and deleting them is special case of the above proposition. We have the following generalization of Proposition 3.7 in [53] too.

Proposition 10. *Let $\prec$ be a term order and $m_j, p_i, p'_i, \Lambda_i,\ 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant k$ be as in Proposition 9. Also let $l_i = lt(p'_i)$ and $w_1, \ldots, w_s$ be the monomials different from l_i in $p'_1, \ldots, p'_m$. Write $w_i = \sum\limits_{j=1}^{m} \gamma_{ij} p'_j$. Consider $W = \{g_{w_i} := w_i + \sum\limits_{j=1}^{m} \gamma_{ij} p'_j | 1 \leqslant i \leqslant s\}$, $G := \{m_j + \sum\limits_{i=1}^{m} \lambda_{ij} p'_i | 1 \leqslant j \leqslant m\}$ and $C := \{\boldsymbol{x^c} | c \in \mathbb{N}^n,\ |c| = \mathcal{N} + 1\}$. Then $G \cup W \cup C$ is a Gröbner basis for Q with respect to $\prec$.*

Proof. Proof of Theorem 70 (given in Proposition 3.7 in [53]) works here as well. We just need to note that for every $f \in Q$, $lt(f) \in \langle lt(G) \cup lt(W) \cup C \rangle$. □

Note that unlike Proposition 3.7 in [53] $G \cup C$ is not a Gröbner basis in this case as we don't necessarily have $\langle lt(Q) \rangle = \langle lt(G) \cup lt(W) \cup C \rangle$..
We explain the computations in step 3 of Example 3.3 in [47] using the above result. We also compare our proposition with Condition 3.9. This is done below in Example 77.

Example 77. Let $I = \langle f_1, f_2 \rangle \trianglelefteq \mathbb{K}[x, y]$, where

$$\begin{aligned} f_1 &= x - y + x^2 \\ f2 &= x - y + y^2. \end{aligned}$$

In step 2 we have that

$$\widetilde{M_2} = \begin{array}{c} \\ \text{Condition 3.7} \\ \Lambda(f_1) = 0 \\ \Lambda(f_2) = 0 \end{array} \begin{array}{c} \begin{array}{cccc} d_1 & d_2 & d_1^2 & d_1 d_2 + d_2^2 \end{array} \\ \begin{pmatrix} 0 & 0 & 1 & -1 \\ 1 & -1 & 1 & 0 \\ 1 & -1 & 0 & 1 \end{pmatrix} \end{array},$$

from which we have $D_2 = \{\Lambda_1 = 1, \Lambda_2 = d_1 + d_2, \Lambda_3 = d_2 + d_1^2 + d_1 d_2 + d_2^2\}$. The active columns in D_2 are v_1, v_2, v_3, v_4, where v_i refers to column i and therefore Matrix M' defined in 3.15 (ignoring $\Lambda_1 = 1$) is

$$M' = \begin{array}{c} \\ \Lambda_2 \\ \Lambda_3 \end{array} \begin{array}{c} \begin{array}{cccc} d_1 & d_2 & d_1^2 & d_1 d_2 + d_2^2 \end{array} \\ \begin{pmatrix} 1 & -1 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \end{array}.$$

Substituting some columns of M' and then changing it into a (reduced) echelon form, for example we have the following matrices.

$$G_1'^{-1}M' = \begin{array}{c} \\ \Lambda_2' \\ \Lambda_3' \end{array}\begin{array}{c} \begin{array}{cccc} d_2 & d_1^2 & d_1 & d_1d_2 + d_2^2 \end{array} \\ \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \end{array},$$

which gives columns v_2 and v_3.

$$G_2'^{-1}M' = \begin{array}{c} \\ \Lambda_2' \\ \Lambda_3' \end{array}\begin{array}{c} \begin{array}{cccc} d_2 & d_1d_2 + d_2^2 & d_1 & d_1^2 \end{array} \\ \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \end{array}.$$

which gives columns v_2 and v_4.
For instance if we consider $G_2'^{-1}M'$, then $\Lambda_2' = d_2 + d_1 + d_1^2$ and $\Lambda_3' = d_1d_2 + d_2^2 + d_1 + d_1^2$. d_2 only appears in λ_2' and $d_1d_2 + d_2^2$ only appears in Λ_3', and therefore deleting columns v_2 and v_4 from $\widetilde{M_3}$ we will have the following in step 3.

$$\widetilde{M_3} - v_2 - v_4 = \begin{array}{r} \\ \text{Condition 3.7} \\ \text{Condition 3.7} \\ \Lambda(f_1) = 0 \\ \Lambda(f_2) = 0 \end{array}\begin{array}{c} \begin{array}{cccc} d_1 & d_1^2 & d_1^3 - d_1^2 & d_2^3 + d_1d_2^2 + d_1^3d_2 - d_1d_2 \end{array} \\ \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & -1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \end{array}.$$

$Ker(\widetilde{M_3} - v_2 - v_4) = 0$ and we are done. Using any of the pairs of columns obtained via other possible matrices we would have gotten the same result.

Other observations We present observations concerning the algorithm. On one hand we show how pivoting could help and on the other hand we compare the sizes of the matrices produced by the theory presented above.
Let us put an order on the monomials of D_{t-1}, e.g., degree lexicographic. Then $lt(\Lambda')$, the leading term of Λ', would be well-defined for every $\Lambda' \in D_t$. Now one can consider reducing the members of a basis of D_t with respect to each other so that $lt(\Lambda') \notin Supp(\Lambda'')$ for all $\Lambda' \neq \Lambda'' \in D_t$. We call such a basis a *reduced basis*. Then the leading term will be a monomial that uniquely appears in the reduced basis. If $\Lambda_1, \ldots, \Lambda_m$ is a basis for D_{t-1}, then removing the columns corresponding to $lt(\Lambda_1), \ldots, lt(\lambda_m)$ from $\widetilde{M_t}$ is equivalent to part 3 of Proposition 6. Using part 1 of Proposition 6, one may check whether v_λ is active in D efficiently. This must be done with precise pivoting. For that, one must start with reducing v_λ with the *appropriate* columns, without doing the column reductions for the other columns, unless it is required. In the worst case, we will need to compute the whole kernel, i.e., the whole D_t, but this is not necessarily the case all the time and therefore this can be viewed as a first potential optimization step. As a side remark, using row echelon form is also taking advantage of pivoting.

Change of the Integration Order at Each Step We conclude by another possible optimization strategy. One can change the order of the variables at each step of the integration method in order to gain some computational advantage. Suppose that we have computed $D_{t-1} = \{\Lambda_1, \ldots, \Lambda_m\}$. Consider $n_i := \#\{dx_i^{\alpha_i} \in \bigcup_i Supp(\Lambda_i) | \alpha_i \in \mathbb{N}\}$. re-order the variables in the following way: if $n_i \leqslant n_j$, then put $x_i < x_j$ (note that if the equality happens, we don't care whether x_i appears before x_j or vice versa). We call such an order a *good integrable* order. Assume that $x_{b_1} < x_{b_2} < \ldots < x_{b_n}$ is a good integrable ordering, where $b_i \in \{1, \ldots, n\}$. Now we consider $\Lambda_1, \ldots, \Lambda_m$ as polynomials in $\mathbb{K}[dx_{b_1}, \ldots, dx_{b_n}]$ and continue with the integration in the following order:

$$\Lambda = \sum_i \lambda_{i1} \int_{b_1} \Lambda_i|_{dx_{b_2}=\cdots=dx_{b_n}=0} + \cdots + \sum_i \lambda_{in-1} \int_{b_{n-1}} \Lambda_i|_{dx_{b_2}=\cdots=dx_{b_n}=0} + \sum_i \lambda_{in} \int_{b_n} \Lambda_i.$$

This way, we will do the least possible number of integrations. Note that the number of integrands and the number of basis elements of D_{t-1} are fixed and therefore we won't gain any advantage in terms of the size of M_t. The following example illustrates the optimization.

Example 78. Consider Example 73. In step two we have that

$$D_2 = \left\langle \Lambda_1 = 1, \Lambda_2 = d_1 + d_2, \Lambda_3 = -d_1 + d_1^2 + d_1 d_2 + d_2^2 \right\rangle.$$

Then $n_1 = 3, n_2 = 2$. Therefore we change the order into $y < x$ and work on $\mathbb{K}[dy, dx]$. Then

$$\Lambda = \lambda_1 dy + \lambda_2 dx + \lambda_3 dy^2 + \lambda_4(dydx + dx^2) + \lambda_5(dy^3) + \lambda_6(dx^3 - dx^2 + dx^2 dy + dxdy^2).$$

We have have only one monomial in the 5-th column of M_3, while in the original ordering, we had two:

$$\Lambda = \lambda_1 dx + \lambda_2 dy + \lambda_3 dx^2 + \lambda_4(dxdy + dy^2) + \lambda_5(dx^3 - dx^2) + \lambda_6(dy^3 + dxdy^2 + dx^2 dy + dxdy).$$

Algorithm 3: Modified Integration Method

```
Input  : A basis for an $\mathfrak{m}_\zeta$-primary ideal $Q_\zeta$
Output  A basis for $Q_\zeta^\perp$ and directional multiplicities
:
def ComputeBasis:
    $D_{\text{old}} = \varnothing$
    $D_{\text{new}} = \{\Lambda = d^0 = 1\}$
    $\mu_i = 0, i = 1, \ldots, n$
    while $D_{\text{old}} \neq D_{\text{new}}$:
        $D_{\text{old}} = D_{\text{new}}$
        Change the order of the variables into a good integrable order
        $\Lambda := \sum_{i=1}^{s} \sum_{k=1}^{n} \lambda_{ik} \int_k \Lambda_i(d_1, \ldots, d_k, 0, \ldots, 0)$
        $\forall 1 \leqslant k < l \leqslant n, \sum_{i=1}^{s} \lambda_{ik} d_l(\Lambda_i) - \sum_{i=1}^{1} \lambda_{il} d_k(\Lambda_i) = 0$
        $\forall 1 \leqslant i \leqslant s, \ \Lambda(f_i) = 0$
        Construct matrix $M_{\text{new}}$, the coefficient matrix of $\Lambda$
        Apply Criterion 76 and choose good columns $v_{\lambda_1}, \ldots, v_{\lambda_m}$
        $M_{\text{new}} : M_{\text{new}} - v_{\lambda_1} - \cdots - v_{\lambda_m}$
        $D_{\text{new}} = D_{\text{old}} \bigcup Ker(M_{\text{new}})$
        If $dx_i^{\mu_i+1} \in Supp(D_{\text{new}})$, then $\mu_i$ = highest power of $dx_i$ in $D_{\text{new}}|_{x_i \neq 0}$
    return $D_{\text{new}}$ and $\mu_i$
```

Modifications of Macaulay's Algorithm

For Macaulay's algorithm we use the following notation. M_t stands for the matrix in step t. Columns of M_t in Macaulay's algorithm are labeled by monomials $dx^{\mathbf{a}} \in \mathbb{K}[dx_1, \ldots, dx_n]$. Then $v_{dx^{\mathbf{a}}}$ denotes the column corresponding to $dx^{\mathbf{a}}$ in M_t. Note that $v_{dx^{\mathbf{a}}}$ is well-defined because in M_t obtained via Macaulay's algorithm, for every monomial of degree at most t, there exists a column labeled by it and vice versa. Also note that since the columns are labeled by the monomials, a column $v_{dx^{\mathbf{a}}}$ is active in a basis D of $Q^\perp$ if and only if $v_{dx^{\mathbf{a}}} \in Supp(D)$.
Below we show a modification of Proposition 6 and its corollary for Macaulay's algorithm. This enables us to make Macaulay's algorithm more efficient.

Proposition 11. *Let $M_t, M_{t-1}, D_t, \Lambda_i$ $(1 \leqslant i \leqslant m), \lambda, dx^{\boldsymbol{a}}$ and $v_{dx^{\boldsymbol{a}}}$ be as above.*
Then the following hold.

1. *If $v_{dx^{\boldsymbol{a}}}$ is a column of M_t, then $v_{dx^{\boldsymbol{a}}} \in Supp(D_t)$ if and only if $v_{dx^{\boldsymbol{a}}}$ can be reduced to zero by some other columns of M_t.*

2. *For all $1 \leqslant i \leqslant m$, if $v_{dx_i^{\boldsymbol{a}}} \in Supp(\Lambda_i)$, K'_{t_i} is a basis for $Ker(\widetilde{M_t} - v_{\lambda_i})$ and D'_{t_i} is the set of its correspondent dual elements, then $\{\Lambda_i\} \cup D'_{t_i}$ is a basis for the degree t part of $Q^\perp$. Moreover, if $v_{dx^{\boldsymbol{a}_i}} \in Supp(\Lambda_i)$, but $v_{dx^{\boldsymbol{a}_i}} \notin Supp(\Lambda_j)$, $1 \leqslant j \neq i \leqslant m$, then there exists a basis D'_{t_i} such that $\Lambda_j \in D'_{t_i}, j \neq i$.*

3. *For all* $1 \leqslant i \leqslant m$, *if* $v_{dx^{\boldsymbol{a}_i}} \in Supp(\Lambda_i)$, *but* $v_{dx^{\boldsymbol{a}_i}} \notin Supp(\Lambda_j),\ 1 \leqslant j \leqslant i-1$, *then* $D_{t-1} \cup D_{t_{1\ldots m}}$ *is a basis for the degree t part of* $Q^{\perp}$.

Proof. Similar to the proof of Proposition 6. □

In order to detect columns $v_{dx^{\mathbf{a}_i}}$ that satisfy the assumptions of Proposition 11, one can simply adapt the methods mentioned for the modified integration method and equivalently form the matrices $M'', G''^{-1}M''$. Then we have the following corollary, which is the equivalent of Corollary 76 for Macaulay's algorithm.

Corollary 79. ***(Criterion for Deleting Suitable Columns in Macaulay's Matrices)*** *Let* $D_{t-1} = \{\Lambda_1, \cdots, \Lambda_m\}, M_t$ *and* $D_t, v_{\lambda_1}, \ldots, v_{\lambda_u}$ *be as in 3.16 and* $G''^{-1}M''$ *be as above and (by abuse of notation) let* $v_{\lambda_1}, \ldots, v_{\lambda_m}$ *be the columns of* M_t *corresponding to the first* m *columns in* $G''^{-1}M''$ *. Also let* $K_{t_{1\ldots m}}$ *be a basis for* $Ker(M_t - v_{\lambda_1} - \cdots - v_{\lambda_m})$ *and* $D_{t_{1\ldots m}}$ *be the set of its corresponding dual elements. Then* $D_{t-1} \cup D_{t_{1\ldots m}}$ *is a basis for* $Q^{\perp}$.

Proof. Similar to the proof of Corollary 76. □

The following provides us with more modifications on Macaulay's algorithm.

Lemma 80. *For all* $1 \leqslant i \leqslant n$, $1 \leqslant m, t \leqslant N$ *and* $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{N}^n$ *the following holds.*

1. *Let* $dx^{\boldsymbol{a}} \in Supp(D_t)$ *and* $dx^{\boldsymbol{b}}|dx^{\boldsymbol{a}}$ *then* $dx^{\boldsymbol{b}} \in Supp(D)$. *In particular, if* $dx^{\boldsymbol{a}} \in Supp(D_t)$ *and* $dx_i^m|dx^{\boldsymbol{a}}$ *then* $dx_i^m, \cdots, dx_i, 1 \in Supp(D)$.

2. *Let* $dx^{\boldsymbol{b}} \notin Supp(D)$, $dx^{\boldsymbol{b}}|dx^{\boldsymbol{a}}$ *and* $|\boldsymbol{a}| \leqslant t$. *Then* $dx^{\boldsymbol{a}} \notin Supp(D_t)$. *In particular, if* $dx_i^m \notin Supp(D)$ *then* $dx_i^{m+1}, \ldots dx_i^t \notin Supp(D_t)$. *Also if* $dx_i^m \notin Supp(D_{t-1})$ *then* $dx_i^{m+1}, dx_i^{m+2}, \ldots \notin Supp(D_t)$.

Proof. 1. For all $1 \leqslant i \leqslant n$:

$$\begin{aligned} dx^{\mathbf{a}} \in Supp(D_t) &\Leftrightarrow x^{\mathbf{a}} \notin Q_\zeta \\ x^{\mathbf{a}} \notin Q_\zeta &\Rightarrow x^{\mathbf{b}} \notin Q_\zeta \\ x^{\mathbf{b}} \notin Q_\zeta &\Leftrightarrow dx^{\mathbf{b}} \in Supp(D). \end{aligned}$$

The rest can be proved by putting $x^{\mathbf{b}} = x_i^m$.

2. Although this part can be proved directly, however, we use a simple logic argument to prove it. Consider the following notations for the three logic statements that appear in the proposition:

$$\mathtt{p} = dx^{\mathbf{a}} \in Supp(D_t),\ \mathtt{q} = dx^{\mathbf{b}}|dx^{\mathbf{a}},\ \mathtt{r} = dx^{\mathbf{b}} \in Supp(D).$$

Then the previous part says that

$$\mathtt{p} \wedge \mathtt{q} \Rightarrow \mathtt{r}.$$

Therefore, we have the following (Note that the condition $|\mathbf{a}| \leqslant t$ is a consequence of $\mathtt{p}$):

$$\begin{aligned}(\mathtt{p} \wedge \mathtt{q} \Rightarrow \mathtt{r}) &\Leftrightarrow (\neg\mathtt{r} \Rightarrow \neg(\mathtt{p} \wedge \mathtt{q}))\\ &\Leftrightarrow (\neg\mathtt{r} \Rightarrow \neg\mathtt{p} \vee \neg\mathtt{q})\\ &\Leftrightarrow (\neg\mathtt{r} \wedge \mathtt{q} \Rightarrow \neg\mathtt{p}),\end{aligned}$$

which means that if $dx^{\mathbf{b}} \notin Supp(D)$ and $dx^{\mathbf{b}}|dx^{\mathbf{a}}$ then $dx^{\mathbf{a}} \notin Supp(D_t)$.

□

By Lemma 80, one may find some monomials in $Supp(D)$ that are of degree at most t, but not necessarily belong to $Supp(D_t)$ and therefore not necessarily they appear as monomials in the generators of D_t. Also if dx_i^m is the largest power of dx_i that appears in $Supp(D_{t-1})$ then by Lemma 80 dx_i^{m+1} is the largest possible power of dx_i that can appear in $Supp(D_t)$. Another point that we can deduce from the above proposition is that if dx_i^m is the largest power of dx_i that appears in $Supp(D_{t-1})$ and $dx_i^{m+1} \notin D_t$, then not necessarily $\mu_i = m$, because dx_i^{m+1} may appear in some other step of the algorithm and therefore, for computing μ_i, this doesn't give us a termination criterion. However, in that case there won't be anymore a leading term of the form dx_i^k, $k \in \mathbb{N}$ when we work with respect to a degree term order. Also obviously, we have that $dx_i^{\mu_i}, \ldots, dx_i \in Supp(D)$. All these monomials appear in $Supp(D_t)$ at some step of the integration method, as they only will be obtained via integrating the lower power and therefore they will appear at some step of the integration algorithm. But this doesn't imply that they necessarily appear during Macaulay's algorithm. The same applies not only for the powers of a variable x_i, but also to every monomial $dx^{\mathbf{a}} \in Supp(D_{t-1})$, i.e., $\int_i dx^{\mathbf{a}}, 1 \leqslant i \leqslant n$ is the only multiple of $dx^{\mathbf{a}}$ that can appear in $Supp(D_t)$.
Based on the above remarks, we can make the following improvement to Macaulay's algorithm.

Proposition 12 (Improvement on Macaulay's Algorithm)**.** *Let M_t be the matrix obtained via Macaulay's algorithm. Consider the set*

$$A = \{\int_i dx^{\boldsymbol{a}}, 1 \leqslant i \leqslant n \ : \ dx^{\boldsymbol{a}} \in Supp(D_{t-1}) \wedge (\nexists dx^{\boldsymbol{b}} \in Supp(D_{t-1}),\ dx^{\boldsymbol{a}}|dx^{\boldsymbol{b}})\}. \quad (3.17)$$

Then $Ker(M_t - v_A) = Ker(M_t)$, where $M - v_A$ is the matrix obtained by deleting the columns corresponding to the members of A.

Proof. The proof is immediate from part 2 of Lemma 80. □

We explain the improvement by redoing the calculations for Example 67, step 3 using the above result and comparing the computations.

Example 81. Let

$$\begin{aligned}f_1 &= x^2 + (y-1)^2 - 1\\ f_2 &= y^2.\end{aligned}$$

After doing the computations in step 2, we have $D_2 = \{1, d_1, 2d_1^2 + d_2\}$. $d_2 \in Supp(D_2)$, but $d_2^2 \notin Supp(D_2)$. So, in step 3, by the above improvement, we can remove $v_{d_1 d_2^2}$ and $v_{d_2^3}$ from M_3. Also we can remove the columns $v_1, v_{d_1}, v_{d_1^2}$ using proposition 11. So the new matrix has 5 columns, while the original matrix in Macaulay's method has 10 columns.

```
Algorithm 4: Modified Macaulay's Algorithm
  Input  : A basis for an $\mathfrak{m}_\zeta$-primary ideal $Q_\zeta$
  Output  A basis for $Q_\zeta^\perp$ and the directional multiplicities
  :
  def ComputeBasis:
      $D_{\text{old}} = \varnothing$
      $D_{\text{new}} = \{\Lambda = d^0 = 1\}$
      $t = 0$
      $\mu_i = 0, i = 1, \ldots, m$
      while $D_{\text{old}} \neq D_{\text{new}}$:
          $D_t = D_{\text{old}}$
          $D_{\text{old}} = D_{\text{new}}$
          Construct matrix $M_{\text{new}}$, the coefficient matrix of $D_{\text{new}}$
          $\forall \Lambda \in D_t$ , delete a good active column in $\Lambda$ from $M_{\text{new}}$
          Compute $A$ as in Equation 3.17
          $M_{new} = M_{new} - v_A$
          If $v_{dx_i^{\mu_i+1}} \in Ker(M_{\text{new}})$, then $\mu_i = \mu_i + 1$
          $D_{\text{new}} = \text{kernel}(M_{\text{new}})$
          $D_{\text{new}} = D_{\text{old}} \bigcup Ker(M_{\text{new}})$
          $t = t + 1$
      return $D_{\text{new}}$ and $\mu_i$
```

Example 82. Let $I = \langle f_1, f_2, f_3 \rangle \subseteq \mathbb{K}[x, y, z]$, where

$$\begin{aligned} f_1 &= 2x + 2x^2 + 2y + 2y^2 + z^2 - 1, \\ f_2 &= (x + y - z - 1)^3 - x^3, \\ f_3 &= (2x^3 + 2y^2 + 10z + 5z^2 + 5)^3 - 1000x^5. \end{aligned}$$

$(0, 0, -1)$ is a root of multiplicity 18, $\mu_x = 5, \mu_y = 8, \mu_z = 8$ and $N = 9$. From step 3 to 5, the highest power of dx is 2. In steps 6, the monomial dx^3 appears and in steps 7 and 8, we see the monomial dx^4. For dy and dz all the powers appear in all steps. This is a very dense system for computing μ_x and μ_y, in the sense that all the powers of dy and dz appear in all the steps. However for dx we see that we have done many redundant computations.

At the end of this section, we comment on the comparison between the size of the matrices obtained at step t of the above algorithms and their modifications, as size is a big obstacle in computations. The matrix obtained via Macaulay's algorithm has $\binom{t+n}{n}$ columns and at least same number of rows. In the integration method, $\widetilde{M_t}$ has nm columns and $\binom{n}{2} + e$ rows. Applying Condition 3.9 in the integration method, one gets m extra rows, which in special cases can result in deleting at most those m rows and also at most m columns. So the size of the matrix is at least $\binom{n}{2} + e + m \times (n-1)m$. However, this is exactly the size of the matrix obtained using our modification to the integration method. Also if we let $\widehat{M_t}$ be the matrix obtained from Macaulay's algorithm applying our modifications, for every column $v_{dx^{\mathbf{a}}}$ of $\widehat{M_t}$, there exists a p_λ such that $dx^{\mathbf{a}} \in Supp(p_\lambda)$. In other words, all the monomials appearing as the columns of $\widehat{M_t}$, will appear in the columns of $\widetilde{M_t}$, but the difference is that they might be a monomial in a polynomial. This means that the number of columns of $\widetilde{M_t}$ and $\widehat{M_T}$ will be the same if every p_λ is a monomial. This means that $\widetilde{M_t}$ is basically $\widehat{M_t}$ in which some columns are added to each other. Note that many of the rows in both methods can (and in practice are) zero and can be simply deleted.

Concluding this section we provide a list of computational observations:

- Computing the directional multiplicity is basically equivalent to computing the projection of the kernel of $M_{\mathcal{N}}$. There are several classic kernel computation algorithm, e.g, *Singular Value Decomposition*. However, we are not aware of any algorithm for projection, without computing the whole kernel. Proposition 6 can be considered as a proposal for an incremental algorithm for computing kernel projection.

- Having a bound for the directional multiplicities, one can construct a single matrix and compute the dual basis using that matrix rather than running several steps. This is guaranteed by Proposition 4, part 4. The idea for constructing such a matrix is to use the resultant in order to get a bound U for directional multiplicities. Having M_U, Macaulay matrix of size U, the kernel of M_U will give us the whole dual. Note that the main obstacles for this method are the size of M_U and also computing the resultant. The bound U could be the Bezout bound in worst case.

Chapter 4

Applications and Future Work

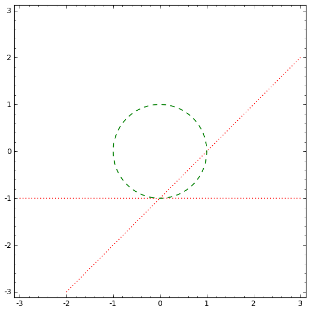
4.1 Applications

We explore some applications of dual space and directional multiplicity. The exploration does not go into details, as the main purpose is to show the usefulness of the concept rather than presenting the applications themselves.

Arrangement and Topology of Planar Algebraic Curves There are several methods in the literature for computing the arrangement and topology of a planar algebraic curve, e.g [3, 2, 19, 23, 8]. In principle, all methods use some elimination tool, e.g Gröbner basis or resultants, in order to project algebraic curves on one axis and identify the critical points (points where derivatives vanish). This is done by finding the real roots of the elimination ideal and using this information to reconstruct/identify the arrangement and topology of the curve. These approaches typically assume that no two critical points have the same projection on the axis. Our work explains what happens in that situation. In Section 4.1, we show how directional multiplicity can handle degenerate situations. Particularly, our algorithms for computing directional multiplicity with respect to an axis could be useful for computing the *multiplicity of a point in its fiber*. Devising a full algorithm for determining the topology of the algebraic curve is beyond the scope of this paper.

Geometry of the Elimination Ideal Let $I \subseteq \mathbb{C}[x, y]$ be a zero dimensional ideal with no roots at infinity generated by two polynomials corresponding to two planar curves and $I_1 = I \cap \mathbb{C}[y] = \langle g \rangle$ be its elimination ideal. We illustrate the case of geometric degeneracy and how directional multiplicity can be used, in a concrete example. Let $f_1 = (y + 1)(y - x + 1)$ and $f_2 = x^2 + y^2 - 1$ as shown in the figure. The two curves intersect at two points, namely $(1, 0)$ and $(0, -1)$. Their Sylvester resultant is $2y(y+1)^3$, which implies that the projection on the y-axis of the roots $(1, 0)$ and $(0, -1)$ have multiplicity 1 and 3 respectively. On the other hand, computing the Gröbner basis of the elimination ideal in $\mathbb{C}[y]$, we obtain the unique monic generator $g =$

$y(y+1)^2$.



f_1	$(y+1)(y-x+1)$
f_2	x^2+y^2-1
g	$y(y+1)^2$
resultant	$2y(y+1)^3$

Observing the difference in the multiplicities of the resultant and g, the questions "when does the multiplicity drop?" and "what does the multiplicity of a factor in g mean?" arise. Using the concept of directional multiplicity, we are able to address these question in the degenerate case, as the one in the example.

The exponent of the factor of g corresponding to an intersection point is the directional multiplicity at that point. The exponent of the corresponding factor of the resultant give us the multiplicity of the intersection points. However Gröbner basis did not say much about the geometry of the intersection. Now having the concept of directional multiplicity, we can explain the generator of the elimination ideal geometrically. In general given dense polynomials $f_1, \dots, f_n \in \mathbb{K}[x_1, \dots, x_n]$, let $I_1 = \langle g \rangle$ and $R_1 \dots R_k$ be the square-free factorization of the Macaulay resultant. Then $g = R_1^{\mu_1} \dots R_k^{\mu_k}$.

Comparison Between Border bases and Dual Bases In the case of $\mathfrak{m}_\zeta$-primary ideals, *Border Basis* is closely related to the dual bases. We briefly explain this relation below. For the definitions and properties of border basis we mainly follow [40].

Assume that we have fixed a term order on the monomials $\partial^{\mathbf{a}}$ and write all the polynomials in $\mathbb{K}[\partial]$ with respect to that order. Following the discussion in Section 3.3.2, one can consider $B = \{x^{\beta_1}, \dots, x^{\beta_\mu}\}$ as an order ideal. We know that the derivation of every element in the dual basis obtained via the integration method is in the dual. Therefore B is a a term order of the form $\mathcal{O}_\prec(Q)$ and the set G in Theorem 70 is a subset of the border basis for B. The rest of the elements of the the borer basis have some elements of the set C in Theorem 70 as their leading terms.

The above discussion gives the idea of computing the border basis of an $\mathfrak{m}_\zeta$-primary ideal degree by degree by constructing the matrices either in Macaulay's algorithm or in the integration method. In order to do so, one can compute D_t, a basis for the dual space of degree t, and read off G from it. Also other elements of the border basis can be checked considering the ansatz that they have the leading term x^c, $|c| = t+1$. note that this does not necessarily work for an arbitrary zero dimensional ideal, as the dual space might not be a polynomial ring. However, obviously the other way round works i.e., having a dual basis for an $\mathfrak{m}_\zeta$-primary ideal Q, one can read off the elements of the dual.

The concept of border bases clarifies the distinction between the Buchberger diagram and the extended Buchberger diagram. The monomials under the Buchberger diagram form an order ideal of the form $\mathcal{O}_\prec(Q)$ for which a unique border basis exists. However, this is not necessarily the case for the monomials under the extended Buchberger diagram of Q. The latter as an order ideal can have a border basis, which gives us a dual basis. This shows that the border basis is somehow stronger that the dual basis. Border bases algorithms proposed in [39] and [9] can be used in accordance to the above discussion.

Computing Hilbert Series of Zero Dimensional Ideals For an isolated point ζ and its corresponding $\mathfrak{m}_\zeta$-primary ideal Q_ζ, Mourrain has shown in [53] that having a base for $Q_\zeta^\perp$, one can obtain a basis for R/Q_ζ. Also the improvement of the integration method using Equation 3.9 is based on computing a dual basis along with a basis for R/Q_ζ. The function mapping t to the dimension of the space generated by the degree t part of this quotient is actually the Hilbert Function. Hilbert function and Hilbert series can be computed via Gröbner bases. Having the dual basis, one can compute the Hilbert function and Hilbert series. For instance, for a 0-dimensional ideal, given the set of points in the variety of the ideal, Chapter 7 of [56] shows such a method to compute the Hilbert function and series as well as the regularity. These are based on using Gröbner basis for the computations. Alternatively, one can use dual bases in order to compute these objects. In particular, directional multiplicities can be used to compute the degree of the elements of the ideal, which can be useful in computing the regularity. Finally, directional multiplicities can be used in computing the Hilbert series of the last elimination ideal.

4.2 Future Work

Dimension of the Elimination Ideal Below we explain a problem that was proposed by Carlos D'Andrea [22].
We know that $dim(\mathcal{V}(I)) \leqslant n$, so $dim(\pi(\mathcal{V}(I))) = dim(I_1) \leqslant n-1$. Also as $\mathcal{V}(h_1, \dots, h_m) \subseteq \mathbb{A}^{n-1}$, from Theorem 26 we have $dim(V(h_1, \dots, h_m)) \leqslant n-1$. Also from Theorem 27, as projection is an onto map, we have $dim(\pi(V)) \leqslant dim(V)$. An interesting question is when $dim(V) = dim(\pi(V))$. This is the case if and only if for almost all $x \in \pi(V)$, $\pi^{-1}(x)$ is of dimension 0, i.e. every fiber is of dimension 0. There are many simple examples that this can happen, e.g. if $\mathcal{V}(I)$ is a plane parallel to x_1-axis. However, up to now we are not able to classify all the cases that this happens by a condition on the generating polynomials. Neither we know when such x cannot be in $\mathcal{V}(h_1, \dots, h_m)$ as this will tell us when $\mathcal{V}(h_1, \dots, h_m) \cap \pi(\mathcal{V}(I)) = \varnothing$.

Directional Multiplicity with respect to arbitrary $v \in \mathbb{R}^n$ In the definition of directional multiplicity, we have considered the n axes as the directions. One could think of defining the multiplicities in the direction of an arbitrary vector $v \in \mathbb{R}^n$. The directional multiplicities along these vectors might be useful in studying singularities of curves.

Benchmarks It is essential that the algorithms presented and their implementations are tested for their practical efficiency. In particular we plan to benchmark the following:

- Experiments with directional multiplicity algorithms:
  - Comparison of Macaulay's algorithm and the integration method for directional multiplicity in their original form, using the improvement in [47] and using the improvements of Corollary 76, Corollary 79 and Proposition 12.

- Matrix size comparison for Macaulay algorithm's and the integration method's improvements.
- Behavior on the sparse case.

- Explore the behavior with respect to sparsity, degree, complexity of multiplicity structure
- Compare with standard tests in the literature, e.g., Cyclic 9.

Directional Multiplicity for Sparse Systems Let us consider the following example.

Example 83. Let $I = \langle f_1 = x^9 - x^6y^2, f_2 = y \rangle \subseteq \mathbb{K}[x, y]$. Then the origin is a root of degree 9, $\mu_1 = 9, \mu_2 = 1$. Both the integration method and Macaulay's algorithm need to run until step 10 in order to find the dual space.

In the above example many columns (corresponding to monomials) are considered, which are equal to the zero vector. This is because the system is *sparse*. If we knew a priori that $dx^9 \in D$, then we could have avoided the previous steps. One idea to deal with such cases is to start with the matrix M_k, where k is an upper bound for $\mathcal{N}$ and do the binary search top-down. However the only such bound that we are aware of is the Bezout bound for μ, which can be too big and hence this method is impractical. For computing μ_i, when we have a sparse system with respect to x_i, one could follow a down-top algorithm which works by a-priori adding extra columns $v_{dx_i}, \dots, v_{dx_i^{2t}}$ to the *modified* matrix M_t, where modified M_t refers to the matrix that has been obtained at step t of either modified integration method or Macauley's algorithm.

Expansion Problem Our motivation to study the elimination problem was originally to give an incremental algorithm for lexicographic Gröbner basis computation, based on induction on the number of variables. The algorithm that was first suggested in [54] is as follows.
Let I be the ideal in $\mathbb{K}[x_1, \dots, x_n]$ generated by $F_0 = \{f_1, \dots, f_m\}$, I_i the i-th elimination ideal of I and G_i its reduced Gröbner basis. Given F_0, assume that we can compute F_i iteratively using resultants. Then, having F_{n-1} compute G_n by a GCD algorithm for the case we arrive to univariate non zero resultants. Now, having F_{n-1} and G_n we are interested in finding an algorithm that computes G_{n-1}. We can iterate such an algorithm until we have G_0.
So we are concerned with the following problem, which was formulated by Buchberger [13]:
The Expansion Problem. Given F_{i-1}, a generating set for I_{i-1} and G_i, the reduced Gröbner basis of I_i, find G_{i-1}, the reduced Gröbner basis of I_{i-1}.
First, based on the Elimination Property of Gröbner basis and also the uniqueness of the reduced Gröbner basis, we have the following observation:

> If G_0 and G_1 are the reduced Gröbner bases of I and I_1 with respect to the lexicographic order ($x_1 > \dots > x_n$), then $G_1 \subseteq G_0$.

We suggest the following modification of Buchberger's algorithm for the expansion problem:

- Reduce F_{i-1} by G_i:

    1. consider $F_{i-1} \subset K[x_{i+1}, \cdots, x_n][x_i]$.

2. reduce coefficients of polynomials in F_{i-1} by G_i.

- Compute G_{i-1} in the following way:
  1. Compute $\{NF(Spol(f,g)) | f,g \in F_{i-1} \backslash (F_{i-1} \cap K[x_i,\ldots,x_n])\}$
  2. Compute $\{NF(Spol(f,g)) | f \in F_{i-1} \backslash (F_{i-1} \cap K[x_i,\ldots,x_n]), g \in G_i\}$
  3. Run Buchberger's algorithm on the union of the sets above and autoreduce

Removing the condition for the Gröbner basis to be reduced, the following more general question arises naturally:

> Given G_1, a Gröbner basis which is not necessarily reduced, how to *construct* G_0, a Gröbner basis of I such that $G_1 \subseteq G_0$? Note that the existence of such G_0 is obvious.

In the following there are some problems related to the elimination and expansion problems.

1. Investigate possibilities of generating I_1 by random combinations of the resultants with coefficients from the polynomial ring.
2. Investigate the degenerate cases: Suppose that all the resultants are zero but there's no common factor for all of the polynomials. Can we describe this by conditions on the (degree of) polynomials?
3. Let $f_1,\ldots,f_m \in \mathbb{K}[x_1,\ldots,x_n]$ be generic polynomials and r_{ij} as above. Does there exist $e_{ij} \in \mathbb{K}[x_2,\ldots,x_n]$ such that $I_1 = \left\langle \frac{r_{ij}}{e_{ij}} | 1 \leqslant i < j \leqslant m \right\rangle$?

Resultants of Gröbner basis members Can we find a (necessary) condition for a set G to be a (reduced) Gröbner basis by looking at the properties/forms of the resultants of the members of G?

We try to approach this problem by computing the resultant of S_{12} and f_2. In the following we set the notation and do the computations in several steps. Let $f_1 = \sum_{i=0}^{d_1} a_i x^i$, $f_2 = \sum_{i=0}^{d_2} b_i x^i$, in which $a_i, b_j \in \mathbb{K}[y]$. Then $S_{12} = m_1 f_1 - m_2 f_2$, where $m_1 = c_1 y^{k_1}, m_2 = c_2 y^{k_2} x^{d_1-d_2}$ such that $c_i \in \mathbb{K}$. During the following computations we use several properties of the resultants which can be found in [15].

Step 1. $\operatorname{res}(f_2, S_{12})$.

Let , $d_{12} := deg(S_{12})$ and $\operatorname{res}(f_1,f_2) := \operatorname{res}_x(f_1,f_2)$. Then

$$\begin{aligned}
\operatorname{res}(f_2, S_{12}) &= \operatorname{res}(f_2, m_1 f_1 - m_2 f_2) \\
&= b_{d_2}^{(d_1-d_2)-d_1} \operatorname{res}(f_2, m_1 f_1) \\
&= b_{d_2}^{-d_2} \operatorname{res}(f_2, m_1) \operatorname{res}(f_2, f_1) \\
&= b_{d_2}^{-d_2} m_1^{d_2} \operatorname{res}(f_2, f_1) \\
&= b_{d_2}^{-d_2} c_1^{d_2} y^{kd_2} \operatorname{res}(f_2, f_1) .
\end{aligned}$$

Step 2. $\operatorname{res}(f_2, S_{12} - hf_2)$.
Let $S_{12} - hf_2$ be a step in reducing the S-polynomial and $l := deg(h)$, then

$$\begin{aligned}
\operatorname{res}(f_2, S_{12} - hf_2) &= \operatorname{res}(f_2, -hf_2 + S_{12}) \\
&= b_{d_2}^{l-d_{12}} \operatorname{res}(f_2, S_{12}) \\
&= b_{d_2}^{l-d_2} b_{d_2}^{-d_2} c_1^{d_2} y^{kd_2} \operatorname{res}(f_2, f_1) \\
&= b_{d_2}^{l-2d_2} c_1^{d_2} y^{kd_2} \operatorname{res}(f_2, f_1).
\end{aligned}$$

Step 3. $\operatorname{res}(f_2, S_{12} - kf_1)$ Let $S_{12} - kf_1$ be a step in reducing the S-polynomial. Then

$$\begin{aligned}
\operatorname{res}(f_2, S_{12} - kf_1) &= \operatorname{res}(f_2, m_1 f_1 - m_2 f_2 - kf_1) \\
&= \operatorname{res}(f_2, -m_2 f_2 + (m_1 - k) f_1) \\
&= b_{d_2}^{(d_1-d_2)-d_2} \operatorname{res}(f_2, (m_1 - k) f_1) \\
&= b_{d_2}^{d_1-2d_2} \operatorname{res}(f_2, m_1 - k) \operatorname{res}(f_2, f_1).
\end{aligned}$$

Let $k := c_k y^u x^v$. Performing Gaussian elimination on the rows of $Syl(f_2, m_1 - k)$ that contain coefficients of $m_1 - k$ using the rows corresponding to the coefficients of f_2, we obtain a triangularized matrix and the resultant will be equal to:

$$\operatorname{res}(f_2, m_1 - k) = b_{d_2}^{*} \prod (c_1 y^{k_1} - p(b_i)),$$

where p is a univariate polynomial and $b_{d_2}^{*}$ is a power of b_{d_2}. Therefore we have:

$$\operatorname{res}(f_2, S_{12} - kf_1) = b_{d_2}^{l-d_2} b_{d_2}^{*} \prod (c_1 y^{k_1} - p^{(s)}(b_i)) \operatorname{res}(f_2, f_1).$$

Step 4. $\operatorname{res}(f_2, S_{12} - hf_2 - kf_1)$

$$\begin{aligned}
\operatorname{res}(f_2, S_{12} - hf_2 - kf_1) &= \operatorname{res}(f_2, m_1 f_1 - m_2 f_2 - hf_2 - kf_1) \\
&= \operatorname{res}(f_2, (-m_2 - h) f_2 + (m_1 - k) f_1) \\
&= b_{d_2}^{t-s-d_1} \operatorname{res}(f_2, (m_1 - k) f_1) \\
&= b_{d_2}^{t-s-d_1} \operatorname{res}_b (f_2, m_1 - k)_{d_2}^{t-s-d_1}, \\
&= b_{d_2}^{*} \prod (c_1 y^{k_1} - p(b_i)) b_{d_2}^{t-s-d_1},
\end{aligned}$$

where $t = deg(-m_2 - h) = deg(m_2 + h) \leqslant max\{deg(m_2), deg(h)\}$ and $s = deg(m_1 - k)$ and therefore $deg\,((m_1 - k) f_1) = s + d_1$ and b^* and p are as above.
Finally, we know that the normal form of S_{12} can be written as $S_{12} - \sum_{i=1} h_i f_i$, where h_i are the cofactors. Then the above computations can be adapted for computing $\operatorname{res}(f_2, S_{12} - \sum_{i=1} h_i f_i)$ in terms of degrees of h_i and f_i and also coefficients of f_i.
Note that if $\{f_1, f_2\}$ is a Gröbner basis, then S_{12} can be reduced to zero with respect to $\{f_1, f_2\}$. From the above steps in the special case that all of the reduction steps were done only by f_2, $\operatorname{res}(S_1 2, f_2)$ can be written in terms of $\operatorname{res}(f_2, f_1)$ and some coefficients in $\mathbb{K}$ and some monomials in y. But since reductions are only done using f_2 we can conclude that there exists a polynomial h such that $S_1 2 = hf_2$. Therefore $f_2 | S_1 2$ and then $\operatorname{res}(S_1 2, f_2) = 0$. So $\{f_1, f_2\}$ being a Gröbner basis means that $\operatorname{res}(f_2, f_1) = 0$, which means that f_1 and f_2 have a common factor that contains x with positive degree.

Bibliography

[1] H. Ahmadinezhad. Personal communications, 2014.

[2] L. Alberti, B. Mourrain, and J. Wintz. Topology and arrangement computation of semi-algebraic planar curves. Computer Aided Geometric Design, 25(8):631–651, 2008.

[3] D. S. Arnon and S. McCallum. A polynomial-time algorithm for the topological type of a real algebraic curve. Journal of Symbolic Computation, 5(1):213–236, 1988.

[4] G. Ars, J.-C. Faugere, H. Imai, M. Kawazoe, and M. Sugita. Comparison between xl and gröbner basis algorithms. In Advances in Cryptology-ASIACRYPT 2004, pages 338–353. Springer, 2004.

[5] D. Bates, C. Peterson, and A. J. Sommese. A numerical-symbolic algorithm for computing the multiplicity of a component of an algebraic set. Journal of Complexity, 22(4):475–489, 2006.

[6] D. Bayer and M. Stillman. A theorem on refinding division orders by the reverse lexicographic order. Duke Mathematical Journal (C), 1987.

[7] T. Becker, H. Kredel, and V. Weispfenning. Gröbner Bases: A Computational Approach to Commutative Algebra. Springer-Verlag, 1993.

[8] E. Berberich, P. Emeliyanenko, A. Kobel, and M. Sagraloff. Arrangement computation for planar algebraic curves. In Proceedings of the 2011 International Workshop on Symbolic-Numeric Computation, pages 88–98. ACM, 2012.

[9] G. Braun and S. Pokutta. A polyhedral approach to computing border bases. arXiv preprint arXiv:0911.0859, 2009.

[10] B. Buchberger. Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem Nulldimensionalen Polynomiideal (An Algorithm for Finding the Basis Elements in the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal). PhD thesis, Mathematical Institute, University of Innsbruck, Austria, 1965. (English translation in Journal of Symbolic Computation, Special Issue on Logic, Mathematics, and Computer Science: Interactions. Vol. 41, Number 3-4, Pages 475-511, 2006).

[11] B. Buchberger. Ein Algorithmisches Kriterium für die Lösbarkeit eines Algebraischen Gleichungssystems (An Algorithmic Criterion for the Solvability of Algebraic Systems of Equations) . Aequationes Mathematicae, 3:374–383, 1970. (English translation in B. Buchberger, F. Winkler (eds.): Gröbner Bases and Applications, London Math. Society Lecture Note Series 251, Cambridge Univ. Press, 1998, Pages 535 -545).

[12] B. Buchberger. Miscellaneous results on groebner bases for polynomial ideals ii. Technical Report 83/1, University of Delaware, Department of Computer and Information Sciences,, 1983.

[13] B. Buchberger. Personal communications, 2013.

[14] B. Buchberger. A new algorithm for computing gröbner bases using generalized sylvester matrices. In International Conference "Polynomial Computer Algebra", Saint-Petersburg, Euler International Mathematical Institute, 2015.

[15] B. Buchberger, G. E. Collins, and R. Loos, editors. Computer Algebra - Symbolic and Algebraic Computation, volume Supplement Nr. 4 (1st ed.). Springer Verlag Wien, 1982.

[16] B. Buchberger and H. M. Möller. The construction of multivariate polynomials with preassigned zeros. In EUROCAM, pages 24–31, 1982.

[17] J. Canny. Generalised characteristic polynomials. Journal of Symbolic Computation, 9(3):241–250, 1990.

[18] J. F. Canny and D. Manocha. Multipolynomial resultant algorithms. Journal of Symbolic Computation, 15(2):99–122, 1993.

[19] J. Cheng, S. Lazard, L. Peñaranda, M. Pouget, F. Rouillier, and E. Tsigaridas. On the topology of planar algebraic curves. In Proceedings of the twenty-fifth annual symposium on Computational geometry, pages 361–370. ACM, 2009.

[20] D. Cox, J. Little, and D. O'Shea. Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra. Springer, 7 2005.

[21] D. Cox, J. Little, and D. O'Shea. Using Algebraic Geometry. Springer, 2nd edition, 2005.

[22] C. D'Andrea. Personal communications, 2013.

[23] D. N. Daouda, B. Mourrain, and O. Ruatta. On the computation of the topology of a non-reduced implicit space curve. In Proceedings of the Twenty-first International Symposium on Symbolic and Algebraic Computation, ISSAC '08, pages 47–54, New York, NY, USA, 2008. ACM.

[24] B. H. Dayton and Z. Zeng. Computing the multiplicity structure in solving polynomial systems. In Proceedings of the 2005 International Symposium on Symbolic and Algebraic Computation, ISSAC '05, pages 116–123, New York, NY, USA, 2005. ACM.

[25] C. Eder. Improving incremental signature-based gröbner basis algorithms. ACM Communications in Computer Algebra, 47(1/2):1–13, 2013.

[26] D. Eisenbud. Commutative Algebra with a View Toward Algebraic Geometry, volume 150 of Graduate Texts in Mathematics. Springer-Verlag, 1995.

[27] M. Elkadi and B. Mourrain. Introduction à la Résolution des Systèmes Polynomiaux, volume 59. Springer, 2007.

[28] I. Emiris and B. Mourrain. Matrices in elimination theory. Journal of Symbolic Computation, 28(1-2):3–44, 1999.

[29] J. C. Faugère. A new efficient algorithm for computing Gröbner basis (f4). Journal of Pure and Applied Algebra, 139(1-3):61–88, 1999.

[30] J. C. Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (f5). In Proceedings of the 2002 international symposium on Symbolic and algebraic computation, ISSAC '02, pages 75–83, New York, NY, USA, 2002. ACM.

[31] J. C. Faugère, P. Gianni, D. Lazard, and T. Mora. Efficient computation of zero-dimensional gröbner bases by change of ordering. Journal of Symbolic Computation, 16(4):329–344, 1993.

[32] M. Gallet. Personal communications, 2013.

[33] S. Gao, Y. Guan, and F. Volny IV. A new incremental algorithm for computing gröbner bases. In Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation, pages 13–19. ACM, 2010.

[34] S. Gao, F. Volny IV, and M. Wang. A new algorithm for computing Göbner bases, 2011.

[35] W. Gröbner. Über die eliminationtheorie. Monatschafte für Mathematik, 5:71–78, 1950.

[36] R. Hartshorne. Algebraic Geometry, volume 52. Springer Science & Business Media, 1977.

[37] K. Hoffman and R. A. Kunze. Linear Algebra. Prentice-Hall mathematics series. Prentice-Hall, 1971.

[38] M. M. Kapranov I. M. Gelfand and A. V. Zelevinski. Discriminants, Resultants, and Multidimensional Determinants. Birkhäuser, 1994.

[39] A. Kehrein and M. Kreuzer. Computing border bases. Journal of Pure and Applied Algebra, 205(2):279–295, 2006.

[40] A. Kehrein, M. Kreuzer, and L. Robbiano. An algebraist's view on border bases. In Solving polynomial equations, pages 169–202. Springer, 2005.

[41] R. Krone and A. Leykin. Eliminating dual spaces. arXiv preprint arXiv:1503.02038, 2015.

[42] Y. N. Lakshman. A single exponential bound on the complexity of computing gröbner bases of zero dimensional ideals. In Effective Methods in Algebraic Geometry, pages 227–234. Springer, 1991.

[43] D. Lazard. Ideal bases and primary decomposition: Case of two variables. Journal of Symbolic Computation, 1(3):261 – 270, 1985.

[44] A. Leykin, J. Verschelde, and A. Zhao. Higher-order deflation for polynomial systems with isolated singular solutions. In Algorithms in algebraic geometry, pages 79–97. Springer, 2008.

[45] N. Li and L. Zhi. Computing isolated singular solutions of polynomial systems: case of breadth one. SIAM Journal on Numerical Analysis, 50(1):354–372, 2012.

[46] F. S. Macaulay. The Algebraic Theory of Modular Systems. Cambridge mathematical library. Cambridge University Press, Cambridge, New York, Melbourne, 1994.

[47] A. Mantzaflaris and B. Mourrain. Deflation and certified isolation of singular zeros of polynomial systems. In Proceedings of the 36th international symposium on Symbolic and algebraic computation, pages 249–256. ACM, 2011.

[48] A. Mantzaflaris and B. Mourrain. Singular zeros of polynomial systems. In Tor Dokken and Georg Muntingh, editors, SAGA – Advances in ShApes, Geometry, and Algebra, volume 10 of Geometry and Computing, pages 77–103. Springer International Publishing, 2014.

[49] M Marinari, H Möller, and T. Mora. Gröbner duality and multiplicities in polynomial system solving. In Proceedings of the 1995 international symposium on Symbolic and algebraic computation, pages 167–179. ACM, 1995.

[50] M Marinari, H Möller, and T. Mora. On multiplicities in polynomial system solving. Transactions of the American Mathematical Society, 348(8):3283–3321, 1996.

[51] E. W. Mayr and A. R. Meyer. The complexity of the finite containment problem for petri nets. Journal of ACM, 28(3):561–576, July 1981.

[52] M. S. E. Mohamed, D. Cabarcas, J. Ding, J. Buchmann, and S. Bulygin. Mxl3: An efficient algorithm for computing gröbner bases of zero-dimensional ideals. In Information, Security and Cryptology–ICISC 2009, pages 87–100. Springer, 2010.

[53] B. Mourrain. Isolated points, duality and residues. Journal of Pure and Applied Algebra, 117:469–493, 1997.

[54] H. Rahkooy and Z. Zafeirakopoulos. Using resultants for inductive gröbner bases computation. ACM Communications in Computer Algebra, 45(1), 2011.

[55] H. Rahkooy and Z. Zafeirakopoulos. On computing elimination ideals using resultants with applications to groebner bases. Technical report, Research Institute for Symbolic Computations, Doctoral College Computational Mathematics, 2013.

[56] H. Schenck. Computational Algebraic Geometry, volume 58. Cambridge University Press, 2003.

[57] I. R. Shafarevich. Basic Algebraic Geometry, volume 197. Springer, New York, 1977.

[58] H. J. Stetter. Numerical Polynomial Algebra. SIAM, 2004.

[59] B. L. van der Waerden. Algebra, volume 1. Springer, New York, 7th edition, 1991. Based in part on lectures by E. Artin and E. Noether.

[60] B. L. van der Waerden. Algebra, volume 2. Springer, New York, 5th edition, 1991. Based in part on lectures by E. Artin and E. Noether.

[61] M. Wiesinger-Widi. Gröbner Bases and Generalized Sylvester Matrices. PhD thesis, Johannes Kepler University, Research Institute for Symbolic Computation, 2014.

[62] X. Wu and L. Zhi. Computing the multiplicity structure from geometric involutive form. In Proceedings of the twenty-first international symposium on Symbolic and algebraic computation, pages 325–332. ACM, 2008.

[63] Z. Zeng. The closedness subspace method for computing the multiplicity structure of a polynomial system. Contemporary Mathematics, 496:347, 2009.