COMPUTATION WITH POLYNOMIAL SYSTEMS

A Dissertation

Presented to the Faculty of the Graduate School

of Cornell University

in Partial Fulfillment of the Requirements for the Degree of

Doctor of Philosophy

by

Ágnes Szántó

January 1999

BIOGRAPHICAL SKETCH

Ágnes Szántó was born in Budapest on June 16, 1966. She graduated in Mathematics from Eötvös Lóránd University, Budapest, in May 1991.

She joined the Computer and Automation Institute of the Hungarian Academy of Sciences in 1991. She took part in a computer algebra project at the Informatics Laboratory with Lajos Rónyai and Gábor Ivanyos.

Continuing her education she enrolled in the Ph.D. program at the Center for Applied Mathematics, Cornell University, in Fall 1993. She was awarded a M.S. in 1996 and a Ph.D in 1998 in Applied Mathematics.

Currently she holds a postdoctoral fellowship at the Mathematical Sciences Research Institute, Berkeley, where she spends the 1998-99 academic year.

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my advisor, Dexter Kozen, for the time he spent with me and for his constant support and encouragement. Without his help this thesis would not exist. I am also grateful for the generous financial support provided by Dexter Kozen through the following grants: CCR-9123730, CCR-9317320, CCR-9708915C.

I am deeply grateful to Lajos Rónyai, my advisor at SZTAKI, for his unlimited availability and patience. Lajos made it possible for me to come to Cornell and without his encouragement and guidance I would have never achieved this. I also want to thank Gábor Ivanyos and Ferenc Bródy for the many friendly conversations that we had and for all the good advice.

Thanks goes to Ronitt Rubinfeld for her friendship, her support and for the many things that I have learned from her. She set high standards as a professional model for my future career in academia.

There are others I would like to acknowledge as well: Moss Sweedler for introducing me to characteristic sets, for always willing to answer questions and for serving on my committee; Mike Stillman for his comments on parts of this thesis and for

serving as a member of my committee; Mark Gross for teaching excellent algebra courses in my first years at Cornell;

I would also like to thank John Guggenheimer, Dolores Pendel, Kaila Patel and all the students for making the Center for Applied Mathematics such a wonderful place. Dolores, thank you very much for all the help you provided during my years at Cornell. Also, I want to thank Karla Conroe for her help in administrative issues.

Special thanks to Raphael Hauser for reading and correcting parts of the manuscript, and for helping to run administrative errunds connected to the submission of this thesis.

I would have never achieved this without the support of my parents and my sister: I will be always indebted to them. Köszönöm.

And, of course, many thanks for all my great friends, without whom none of this would have been so enjoyable.

Table of Contents

Chapter 1

Introduction

1.1 Overview of the main results

The dissertation addresses the classic problem in algebraic and symbolic computation of finding the complex solutions of systems of polynomial equations. Originating from the second half of the last century, J.J. Sylvester, A. Cayley, F.S. Macauley, L. Kronecker, A. Hurwitz and others addressed the problem of deciding solvability of polynomial systems. Their approach to the problem evolved into the theory of resultants - the foundation of elimination theory. In recent years, the search for efficient algorithms for these problems has received extensive attention because of their demonstrated importance to a variety of problems of both practical and theoretical interest.

The motivation to our research stems from the fact that the need to find solutions to polynomial systems over a variety of fields has arisen in a wide range of

practical efforts, including robotics, automated theorem proving, and computational geometry. A concrete example is the problem of resolving singularities of algebraic varieties. For the case of plane curves, the works in [DD84, Koz94, Tei90] approach the problem from the point of view of computational complexity. They handle arithmetic operations in successive field extensions, which arise in the resolution procedure, by using resultant based methods and avoiding polynomial factorization. In the thesis we generalize these "passive factorization" techniques to handle general algebraic varieties over field extensions of the coefficient field $\mathbb{k}$, giving a sufficient computational tool for an explicit desingularization algorithm for surfaces and higher dimensional varieties, which is the subject of future research.

In the thesis we investigate a representation for algebraic sets originally proposed by Kalkbrener, which is computationally convenient for many applications and is suitable for deriving improved time and space complexity bounds. This representation extends the Ritt-Wu characteristic sets as described below. We express the radical of an ideal as the intersection of unmixed ideals represented by characteristic sets, where unmixed means that all irreducible components have the same dimension. Similar techniques have been extensively studied and are widely used in computer algebra systems [BCK88, Wu84, Kal94, Wan92], but it required extra efforts to overcome the problem of computing superfluous components. Kalkbrener states this as a "challenging problem for future research" [Kal94]. In [Sza97] we gave complexity bound for this Ritt-Wu type decomposition algorithm in the dense representation, which compares to the best known bounds for computing the Ritt-Wu characteristic sets [GM91].

More formally, we consider the following problem: Given a set of multivariate polynomials $\{f_1, \ldots, f_k\} \subset \mathbb{k}[x_1, \ldots, x_n]$, compute a representation of the algebraic set $V = \{x \in \mathbf{K}^n \mid f_1(x) = \ldots = f_k(x) = 0\}$, where $\mathbf{K}$ is the algebraic closure of the coefficient field $\mathbb{k}$, which satisfies the following properties:

- membership in the radical ideal $I(V)$ is efficiently decidable;
- set operations such as the union or the difference of algebraic sets are efficiently computable;
- the representation of the empty set is unique;
- the size of the representation is reasonably small relative to the input size in both the dense and sparse representation of polynomials;
- the computation is reasonably fast and is parallelizable.

Various algorithmic tools are used in the literature for the representation and computation of algebraic sets. Gröbner bases [Buc85, Buc84] give a suitable representation of the ideal generated by the input polynomials, solving the general ideal membership problem. Although algorithms using Gröbner bases work efficiently in practice for many applications, they are unlikely to give sub-exponential complexity bounds, since the ideal membership problem over $\mathbb{Q}$ is exponential space complete [May89]. Another procedure is to find a decomposition of the algebraic set and represent each component by a birational projection and a single defining polynomial as a hyper-surface. This approach is used in most prime and unmixed decomposition algorithms [Chi84, Gri84, GH91]. Finally, the representation by Ritt-Wu character-

istic sets serves as a starting point for the representation we propose in the thesis. In the next paragraph we summarize some of the properties of characteristic sets.

The notion of a *characteristic set* of an ideal was first introduced by J.F. Ritt in 1950 [Rit50] in the context of differential geometry. In 1984 Wu Wen-Tsün [Wu84] realized the power of characteristic sets in commutative algebra and in automated geometric theorem proving. The "triangular" structure of characteristic sets, in which each variable is introduced by one polynomial, is convenient when conducting symbolic computation on the common roots of a system of polynomials without explicitly computing them. Although we might lose information about the original ideal when we consider only characteristic sets, the roots of the polynomials in the characteristic set and the roots of the polynomials in the ideal are related: only degenerate cases, in which leading coefficients of the characteristic set vanish, give superfluous roots.

In the dissertation we present a Ritt-Wu type decomposition algorithm. As we mentioned earlier, we express the radical of an ideal given by a generating set as the intersection of unmixed ideals represented by characteristic sets, similarly as in the work of Kalkbrener [Kal96]. To overcome the problem of doubly exponential degree growth of the polynomials occurring in the algorithm and to give a complexity analysis for the algorithm, we need to modify Kalkbrener's algorithm using an approach with multivariate resultant methods and add extra work. In Theorem 4.1.7 we give a randomized algorithm to compute the unmixed decomposition which is efficiently parallelizable, whose sequential [parallel] complexity is $d^{O(n^2(l+1))}$ $[(n\log(d))^{O(1)}]$, where n is the number of variables, d is the maximal degree of the polynomials in

the generating set and l is the dimension of the algebraic set. These are the same bounds as the bounds of Gallo and Mishra [GM91] to compute the characteristic set of a given ideal. Note that for zero dimensional ideals the above bound is optimal in the sense that there are ideals in n variables such that the generating sets of the ideals have maximal degree d but the maximal degree in the characteristic sets is d^n, thus the size of the output is d^{n^2} in the dense representation (see the example in [GM91]). In the case when the algebraic set is not zero dimensional the sequential complexity of our algorithm has $n^2(l+1)$ in the exponent, while the algorithms in [GH91, Chi84, Gri84] give sequential complexity bounds which has n^2 in the exponent. This is due to the fact that our algorithm does not use coordinate transformations. On the other hand, the methods presented here can be modified so as to preserve sparseness.

The subroutines we use in our constructions are of independent interest. Given a set of unmixed varieties represented by characteristic sets, our method gives a "lazy decomposition" procedure (see [DD84, DD85]), which is an efficient algorithm for conducting symbolic arithmetic on algebraic numbers without explicitly computing them. In the zero-dimensional case, both of these algorithms are in the complexity class NC (using arithmetic circuits over $\mathbb{k}$). These results have applications for instance in mechanical geometric theorem proving [Wan95] and in resolving singularities of plane curves ([Koz94. Tei90]) and of higher dimensional varieties.

1.2 Outline of the dissertation

As we noted in the overview, the problem addressed in this thesis is the question of how to represent algebraic sets efficiently such that no information is lost about them. Kalkbrener in [Kal96] proposes such representation, which we call Kalkbrener's unmixed representation. He proves in [Kal96] that the unmixed representation faithfully describes the algebraic sets, and gives heuristics for an algorithm which computes it. Similar constructions for the representation of algebraic sets are widely used in practical implementations [MWW95]. We develop a fast parallel algorithm which finds Kalkbrener's unmixed representation. The algorithms in this thesis represent a significant theoretical improvement over the known algorithms computing the unmixed representation [Kal94, Kal93, Wan95, PW95], since for the first time we prove sequential and parallel complexity bounds which are the same as the best known complexity bounds for computing characteristic sets [GM91]. The main part of the dissertation comprises the description of the algorithm and its complexity analysis.

Before the description of the algorithms we give an overview of the algorithmic tools that are used in the literature for the representation of algebraic sets. In Section 2.2 we give a brief review of the concept of Gröbner bases. Since we will not use Gröbner bases in the rest of the dissertation, we only give the definitions and the computational methods without proofs, following the approach in [BuCoKu].

In Section 2.3 we define the notion of Ritt-Wu characteristic sets. First we define *triangular sets* (usually denoted by Δ), sets of multivariate polynomials in

$\Bbbk[x_1, \ldots, x_n]$ such that each polynomial introduces a new variable. We view each polynomial in a triangular set as a univariate polynomial in its variable of maximal index, with coefficients in the ring of polynomials depending on variables with smaller indices. Unfortunately, the leading coefficients are usually not invertible in the ring, which raises difficulties when conducting division with remainder by the elements of a triangular set. We define the notion of *pseudo-division* of multivariate polynomials, which is a relaxed generalization of the univariate division with remainder, in a way that avoids division by the leading coefficients of the divisors. The generalization of the pseudo-division to triangular sets gives a notion of reduced form of multivariate polynomials modulo triangular sets. This reduced form is denoted by $\mathrm{prem}(f, \Delta)$ and called the pseudo-remainder of f modulo the triangular set Δ. Using pseudo-division has the advantage that finding the reduced form of a polynomial modulo a triangular set is as efficient as if the elements of the triangular sets were monic. Pseudo-division plays an important role in the theory of characteristic sets and also in the notion of unmixed sets defined in Section 2.4.3.

Given an ideal $\mathcal{I} \in \Bbbk[x_1, \ldots, x_n]$, we call a triangular set Δ a *characteristic set of* $\mathcal{I}$, if Δ "pseudo-generates" $\mathcal{I}$, i.e. if all the polynomials in $\mathcal{I}$ have 0 pseudo-remainders modulo Δ. Unfortunately, since the pseudo-division ignores the leading coefficients of Δ, we lose information when we consider only characteristic sets. We can interpret this phenomenon geometrically in two ways:

1. "consider all the roots of the polynomials in Δ", in which case we might introduce components which are not in the algebraic set corresponding to $\mathcal{I}$. These superfluous components are roots of leading coefficients of the polynomials in

Δ.

2. "ignore the roots of the leading coefficients of Δ", in which case we might lose components of the algebraic set corresponding to $\mathcal{I}$.

We present results in Section 2.3 relating the roots of the polynomials in $\mathcal{I}$ and its characteristic set. Furthermore, we describe the results of Gallo and Mishra [GM91] in which they give upper bounds for the degree of the polynomials in a characteristic set of a given ideal $\mathcal{I}$, and where they give complexity bounds for the computation of characteristic sets.

In Section 2.4.3 we describe an extension of the notion of characteristic sets, originally introduced by Kalkbrener [Kal96]. The main idea is to decompose the algebraic set into components which are faithfully represented by triangular sets in a way that we do not lose components of the algebraic set when we ignore the roots of the leading coefficients in the triangular set. More precisely, a triangular set $\Delta \subset \Bbbk[x_1, \ldots, x_n]$ represents an ideal $\mathcal{I}$ if $\mathcal{I} = \{h \in \Bbbk[x_1, \ldots, x_n] \mid \mathrm{prem}(h, \Delta) = 0\}$. We denote the ideal represented by Δ by $\mathrm{Rep}(\Delta)$. We call a triangular set Δ an *unmixed triangular set*, or simply unmixed set, if the leading coefficients of any of the polynomials in Δ do not have common components with the other polynomials in Δ. We prove in Theorem 2.4.6 that if Δ is an unmixed triangular set then $\mathrm{Rep}(\Delta)$ is a radical ideal, $\mathrm{Rep}(\Delta) \neq \Bbbk[x_1, \ldots, x_n]$ and all the components in the algebraic set corresponding to $\mathrm{Rep}(\Delta)$ have the same dimension. Moreover, we also prove that every radical ideal $\sqrt{\mathcal{I}}$ is the intersection of ideals represented by unmixed

triangular sets, i.e. there exist unmixed sets $\Delta_1, ..., \Delta_r$ such that

$$\sqrt{\mathcal{I}} = \bigcap_{i=1}^{r} \mathrm{Rep}(\Delta_i).$$

We call such an expression *Kalkbrener's unmixed representation* of $\sqrt{\mathcal{I}}$. By Hilbert's Nullstellensatz the unmixed representation of a radical is equivalent to finding an unmixed decomposition to the algebraic set $V(\mathcal{I}) = \{x \in \mathbf{K}^n \mid f_0(x) = \cdots = f_k(x) = 0\}$ where $\mathbf{K}$ is the algebraic closure of the coefficient field $\Bbbk$.

In the last section of Chapter 2 we describe a representation method which is used in both the prime and unmixed decomposition algorithms and complexity results of [Chi84, Gri84, GH91]. The main idea is to represent each component by a birational projection and a single defining polynomial as a hyper-surface. We follow an approach similar to the one of Giusti and Heintz [GH91], but instead of the worst case analysis of [GH91] we stress the possibility of randomization. We also point out the connection of this representation to the concept of *u-resultants*.

In Chapter 3 we present the computational tools and algorithms which are the main building blocks of the algorithms in the dissertation. In Section 3.3, after describing the basic computational model using arithmetic circuits over the coefficient field $\Bbbk$, we develop the foundations of a computation model in which we can compute modulo an unmixed triangular set. More precisely, assume that the unmixed triangular set $\Delta = \{\mathrm{g}_1, \ldots, \mathrm{g}_m\} \subset \Bbbk[x_1, \ldots, x_n]$ satisfies that for all $1 \leq s \leq m$

1. the variable with maximal index in g_s is x_{l+s};

2. the leading coefficient of g_s considered as a univariate polynomial in the variable x_{l+s} is in $\Bbbk[x_1, \ldots, x_l]$;

3. g_s is reduced modulo $\{\mathrm{g}_1, \ldots, \mathrm{g}_{s-1}\}$, i.e. $\deg_{x_{l+t}}(\mathrm{g}_s) < \deg_{x_{l+t}}(\mathrm{g}_t) \ \forall\, t < s$.

We develop an arithmetic computation model in the quotient ring

$$\mathcal{A}(\Delta) := \Bbbk(x_1, \ldots, x_l)[x_{l+1}, \ldots, x_n]/\langle\Delta\rangle_{\Bbbk(x_1,\ldots,x_l)} \tag{1.1}$$

where $\langle\Delta\rangle_{\Bbbk(x_1,\ldots,x_l)} \subset \Bbbk(x_1, \ldots, x_l)[x_{l+1}, \ldots, x_n]$ denotes the ideal generated by Δ. We also describe how to obtain the elementary arithmetic operations in the ring

$$\mathcal{R}(\Delta) := \Bbbk[x_1, \ldots, x_n]/\mathrm{Rep}(\Delta)$$

and we express the complexity of the ring operations in $\mathcal{R}(\Delta)$ with respect to arithmetic circuits over $\Bbbk$. We use an approach in which we precompute the multiplication table of $\mathcal{A}(\Delta)$. We also outline alternative precomputational methods.

In Section 3.5 we describe a generalized version of the well-known sub-resultant method to compute the GCD of several univariate polynomials over an arbitrary (function) field, described for example in the work [IK93]. Our method also works for certain coefficient rings with zero-divisors. We give sufficient conditions on the coefficient ring for the GCD method to work. Moreover, we use only ring arithmetics and our method returns a GCD with "integral" coefficients, i.e. the coefficients of the GCD are polynomials without denominator. The leading coefficient of the GCD satisfies some non-vanishing conditions. This method is one of the main building blocks of the decomposition algorithms described in Chapter 4. There we decompose the coefficient rings in order to satisfy the conditions for the existence of the GCD. We describe both a deterministic and a randomized version of the algorithm.

In Section 3.6 we compute a polynomial h in *general position* with respect to the triangular set Δ of codimension m and the set of polynomials F, i.e. a linear

combination of the polynomials in F which intersects each irreducible component of $V(\Delta)$ in codimension $m+1$. This subroutine is applied in the decomposition algorithm. Also, this algorithm is used in deciding whether a given polynomial does not vanish over any component of $V(\Delta)$.

In Chapter 4 we start the description of the algorithm computing the unmixed representation of Kalkbrener. We will construct a modified version of the decomposition algorithm of Kalkbrener. In the work [Kal96], the method **decompose** has a finite set of polynomials F as input and it computes the unmixed representation of the corresponding radical $\sqrt{\langle F \rangle}$ by creating branches of the computation and recursively calling **decompose**. Unfortunately, it often computes superfluous components embedded in other components which are computed in different branches, and Kalkbrener only proved termination of the algorithm. Also, experiments shows that the degrees of the polynomials occurring in the algorithm can grow double-exponentially.

To get a reasonable complexity bound for the above algorithm, we have to overcome some obstacles and add more work. In the next paragraphs we give a brief overview about what factors cause **decompose** to be inefficient.

Let $\Delta = \{\mathrm{g}_1, \ldots \mathrm{g}_m\} \subset \Bbbk[x_1, \ldots, x_n]$ be an unmixed set in the unmixed representation of $V(F)$, i.e. an unmixed set in the output of the algorithm **decompose**. Denote $l = n - m$. Assume also that variable with highest index in g_s is x_{l+s} for $1 \leq s \leq m$. Then the degree in the variable of highest index of the polynomials occurring in Δ has an a priori upper bound: $\deg_{x_{l+s}}(\mathrm{g}_s) \leq \deg V(F)$ where $\deg V(F)$ is the degree of the algebraic set $V(F)$, and bounded by d^n by Bezout's theorem,

where d is the maximal degree of the polynomials in F.

Unfortunately, an a priori bound of the same order of magnitude could not be stated for the "free" variables, i.e. for the variables $x_1, \ldots, x_l$. This has two consequences. First, for every higher dimensional component, the degree in the free variables is bounded only by the number of arithmetic operation of the algorithm. This implies that inefficiency in the number of arithmetic operations during the algorithm also effects the degree of the output in the free variables.

The second consequence is the following: even if a variable x_{l+s} is a class variable for g_s in a given output instance, the polynomials computed before the computation of g_s can have as high degree in x_{l+s} as in any other free variable. We can only conduct reduction by g_s after g_s is found. To find g_s, Kalkbrener computes the gcd of previously computed polynomials in the variable x_{l+s}. The most costly operation is the computation of sub-resultants with matrices of size equal to the degree of the operands in x_{l+s}. Unless we have a polynomial at the beginning of the computation with maximal variable x_{l+s} and with small degree, such that we can reduce the degrees in x_{l+s} of all occurring polynomials at each step, the size of the sub-resultant matrix has no a priori bound. In other words, before starting Kalkbrener's decomposition algorithm, we need to find a polynomial in the ideal with sufficiently small degree, such that the variables $x_{l+s+1}, \ldots, x_n$ are eliminated. As we shall see below, our improved algorithm uses multivariate resultant methods to eliminate the variables $x_{l+s+1}, \ldots, x_n$ simultaneously and to construct polynomials in the ideal with maximal variable x_{l+s} and with small degree.

In Chapter 4 we present an improved version of Kalkbrener's algorithm and we

give sub-exponential complexity bounds. First we discuss multivariate resultant methods to eliminate variables simultaneously. Macaulay in [Mac16] proved that for a system of $n+1$ homogeneous polynomials in $n+1$ variables of degree d with generic coefficients $(c_{i,j})$, there exists a polynomial $\Re_{n,d}(c_{i,j}) \in \mathbb{Z}[c_{i,j}]$, called the *resultant* of the system, depending only on n and d, such that $\Re_{n,d}(\bar{c}_{i,j}) = 0$ if and only if the polynomial system with coefficients $(\bar{c}_{i,j})$ has common solution in the projective space $\mathbb{P}^n$. Moreover, he also proved that $\Re_{m,d}(c_{i,j})$ is the quotient of two determinants, each of them corresponding to a matrix of size at most d^n and with entries either 0 or the coefficients $c_{i,j}$. To compute Macauley's multivariate resultant we refer to the method in [IK93][Theorem 15.3].

Multivariate resultants generalize the notion of Sylvester resultants. Similarly as the Sylvester resultant is applied to eliminate a variable from a system of two equations, multivariate resultants are used to eliminate more variables simultaneously from a system of polynomials, assuming that the components of the algebraic set corresponding to the polynomial system are "proper", i.e. their codimension equals the number of polynomials in the system. In Section 4.1 we present a method to eliminate the assumption of $V(F)$ consisting only of proper components. We use a certain version of techniques widely used in numeric computations for approximating roots of polynomial systems, known collectively as homotopy methods. Canny in [Can90] developed a construction based on a generalization of the characteristic polynomial of linear systems to polynomial systems. Ierardi in [Ier89] derived the same construction by adapting the homotopy method for symbolic computations. Using Canny's generalized characteristic polynomial method allows the multivariate

resultant method described above to succeed even in the presence of a non-proper component. We obtain the projection of all the isolated proper components in the solution set. Finally, in Section 4.1 we show how to find the isolated components of arbitrary codimension even in the case when the number of polynomials in the system is greater than the codimension of the component.

We note here that we can interchange the methods of Ierardi and Canny by sparse elimination techniques as follows. I.M. Gelfand, M.M. Kapranov and A.V. Zelevinsky developed the notion of sparse resultants and sparse elimination theory in a sequence of papers between 1990 and 1994 [GKZ94]. Sparse elimination exploits the structure of multivariate polynomials by considering the Newton polygon of the polynomials instead of the total degree. The degree of the sparse resultant is measured in the mixed volume of the Minkowski sum of the Newton polygons of the input polynomials, which is usually smaller than d^n, the degree of Macauley's resultant. Also, the number of isolated points in the algebraic set is measured in the mixed volume as a consequence of Berstein's theorem [Ful93]. Generalizing the Sylvester matrix, Canny, Emiris and others [Stu93, CP93, EC95, EP97] have developed efficient methods to compute the so called Newton matrix, and they express the sparse resultant as the gcd of sub-determinants of the Newton matrix. This gives a method to find the zero dimensional algebraic set when the ideal is generated by a regular sequence. In order to generalize the zero dimensional algorithm for higher dimensions, we must use a framework where coefficients are parameters. Moreover, Rojas and Wang in [RW96] gave a modified version of the homotopy method mentioned above that preserves the sparse structure of the polynomial system.

By the methods described above we are able to compute a triangular representation of an algebraic set which contains our original algebraic set. We can eliminate the superfluous and multiple roots using a subroutine called **unmixed** described in Section 4.2. The input of the procedure **unmixed** is a triangular set $\Delta = \{\mathbf{g}_1, \ldots, \mathbf{g}_m\} \subset \Bbbk[x_1, \ldots, x_n]$ such that the leading coefficients of the polynomials in Δ are non-zero elements of $\Bbbk[x_1, \ldots, x_{n-m}]$, together with two polynomials $\mathbf{f}, \mathbf{h} \in \Bbbk[x_1, \ldots, x_{n+c}]$. The output is a set of triangular sets $\{\Delta_1, \ldots, \Delta_r\}$ such that $\mathrm{Rep}(\Delta_i)$ is radical of codimension m for $1 \leq i \leq r$. Moreover, the union of the algebraic sets corresponding to the unmixed sets Δ_i consists of exactly those components of $V(\Delta)$ where $\mathbf{f}$ vanish identically but $\mathbf{h}$ is not identically zero. The algorithm is a generalization of the sub-resultant method for finding the gcd of several univariate polynomials described in [IK93, chapter 15.2], and the univariate square-free factorization method described in [BKR85]. The subroutine **unmixed** is of independent interest, since it can be applied to conduct symbolic computation on algebraic numbers which are given as roots of polynomials in unmixed triangular sets.

Theorem 4.1.7 combines the results of Section 4.1 and 4.2. Given a set of polynomials $F \subset \Bbbk[x_1, \ldots, x_n]$. We present an algorithm which computes a set of triangular sets $\Xi(F)$ such that for each $\Delta \in \Xi(F)$ there exists a partition $\imath \cup \jmath = [n]$ of the set $[n] = \{1, \ldots, n\}$ such that Δ is an unmixed triangular set with respect to the variable ordering of $\{x_1, \ldots, x_n\}$ corresponding to the partition $\imath \cup \jmath$. Moreover,

$$\sqrt{F} = \bigcup_{\Delta \in \Xi(F)} \mathrm{Rep}(\Delta).$$

We call a representation satisfying the above conditions an "unordered" unmixed representation of $V(F)$. The statement of Theorem 4.1.7 is the following:

Theorem 4.1.7 Let $F = \{\mathbf{f}_0, \ldots, \mathbf{f}_k\} \subset \Bbbk[x_1, \ldots, x_n]$ be a set of polynomials and assume that

$$\deg_{x_j}(\mathbf{f}_i) \leq d \quad \forall j \in [n], \quad 0 \leq i \leq k.$$

Then there is an algorithm computing the set $\Xi(F)$, an unordered unmixed representation of $V(F)$.

Moreover, if $\Delta = \{\mathbf{g}_1, \ldots, \mathbf{g}_m\} \in \Xi(F)$ and $\imath \cup \jmath = [n]$ is the corresponding partition of $[n]$, i.e. $\text{class}(\mathbf{g}_s) = x_{j_s}$ where $\jmath = \{j_1, \ldots, j_m\}$ and $\imath = [n] - \jmath = \{i_1, \ldots, i_l\}$ then

$$\deg_{x_{j_s}}(\Delta) \leq d^m \quad \forall j_s \in \jmath \quad \text{and}$$

$$\deg_{x_{i_r}}(\Delta) \leq d^{O(m^2)} \quad \forall i_r \in \imath.$$

For any polynomial h occurring in the computation of Δ we have the following degree upper bounds:

$$\deg_{x_{j_s}}(h) \leq d^{2m} \quad \forall j_s \in \jmath \quad \text{and}$$

$$\deg_{x_{i_r}}(h) \leq d^{O(m^2)} \quad \forall i_r \in \imath.$$

Furthermore, if l is the dimension of $V(F)$, the arithmetic circuit computing the unordered unmixed representation $\Xi(F)$ has depth

$$(n \log(d))^{O(1)}$$

and size

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

Chapter 2

Representation of Algebraic Sets

In the following we describe the various algorithmic tools that are used in the literature for the representation and computation of algebraic sets. We propose representations which are computationally convenient for many applications and are suitable for deriving improved time and space complexity bounds. Before the description of the different representation methods let us state the general objectives of representing algebraic sets.

Given a set of polynomials $f_1, ..., f_k \subset \mathbb{k}[x_1, ..., x_n]$ compute a representation of the algebraic set $V = \{x \in \mathbb{C}^n \mid f_1(x) = \ldots = f_k(x) = 0\}$ such that membership in the radical ideal $I(V)$ is decidable, the representation of the empty set is unique, set operations on algebraic sets are efficiently computable, the size of the representation is small relative to the dense size of the input, and the computation is reasonably fast and is parallelizable.

2.1 Notation

Throughout the dissertation we use the following notation:

Let R denote a Noetherian ring with identity and let F be a subset of R. The ideal generated by F is denoted by $\langle F \rangle$, the radical of $\langle F \rangle$ by $\sqrt{F}$. For an ideal $\mathcal{I} \subset R$ and for $f \in R[x]$, $f^{\mathcal{I}}$ denotes the image of f in $(R/\mathcal{I})[x]$.

If $\mathcal{I} = \mathcal{Q}_1 \cap \ldots \cap \mathcal{Q}_r$ is the irredundant primary decomposition of $\mathcal{I}$, then $\mathcal{P}_1 = \sqrt{\mathcal{Q}_1}, \ldots, \mathcal{P}_r = \sqrt{\mathcal{Q}_r}$ are the associated primes of $\mathcal{I}$, and we denote the set $\{\mathcal{P}_1, \ldots, \mathcal{P}_r\}$ by $\mathrm{Ap}(I)$. For a prime ideal $\mathcal{P} \subset R$ the quotient field of the integral domain $R/\mathcal{P}$ is denoted by $\mathbf{K}(\mathcal{P})$.

The *codimension* or *height* of a prime ideal $\mathcal{P} \neq R$ is said to be m if there exists at least one chain $\mathcal{P}_0 \subset \mathcal{P}_1 \subset \ldots \subset \mathcal{P}_m = \mathcal{P}$, where $\mathcal{P}_i$ are prime ideals, and there is no chain with more than $m+1$ elements. The codimension of an arbitrary ideal $\mathcal{I} \neq R$ is the minimum of the codimension of the prime ideals containing $\mathcal{I}$.

We consider polynomials in the polynomial ring $R := \Bbbk[x_1, \ldots, x_n]$ where $\Bbbk$ is an arbitrary field. Assume that the variables are linearly ordered by their subscript: $x_1 < x_2 < \cdots < x_n$. Then class(p) denotes the highest indeterminate appearing in a polynomial p, and lc(p) denote the leading coefficient of p regarded as a univariate polynomial in class(p).

A set of polynomials $\Delta = \{g_1, \ldots, g_k\} \subset R$ is called a *triangular set* if class(g_i) $<$

class(g_j) for all $i < j$. See Section 2.3 for the definition of *pseudo-division* of a polynomial $f \in R$ by a triangular set $\Delta \subset R$. We denote the *pseudo-remainder* by $\text{prem}(f, \Delta)$.

We give a description of the algorithms using geometric notation instead of algebraic. As before, let the coefficient field $\Bbbk$ be an arbitrary field, and $\mathbf{K}$ be the algebraic closure of $\Bbbk$. Since we apply randomization in the algorithms below, we need to restrict $\Bbbk$ to have cardinality sufficiently large to obtain good probabilities. Denote by $\mathbb{A}^n$ and $\mathbb{P}^n$ respectively the affine and projective space over $\mathbf{K}$. Let $F = \{f_0, \ldots, f_k\} \subset \Bbbk[x_1, \ldots, x_n]$ be a set of polynomials, $\mathcal{I} = \langle f_0, \ldots, f_k \rangle$ the ideal generated by F in $\Bbbk[x_1, \ldots, x_n]$. The algebraic set $V = V(F) \subset \mathbb{A}^n$ is the set of common roots of the polynomials in F with coordinates from $\mathbf{K}$, which is the same as the common roots of the polynomials in $\mathcal{I}$:

$$V(\mathcal{I}) = \{x \in \mathbf{K}^n \mid f_0(x) = \cdots = f_k(x) = 0\} \subseteq \mathbb{A}^n.$$

For an *unmixed triangular set* $\Delta \subset \Bbbk[x_1, \ldots, x_n]$ (for definition see Theorem 2.4.6) the ideal reprepresented by Δ is

$$\text{Rep}(\Delta) = \{h \in \Bbbk[x_1, \ldots, x_n] \mid \text{prem}(h, \Delta) = 0\}.$$

In Theorem 2.4.6 we proved that if Δ is an unmixed triangular set, then $\text{Rep}(\Delta)$ is a proper unmixed radical ideal. Denote by $\text{codim}(\Delta)$ the codimension $\text{Rep}(\Delta)$, which equals to the number of polynomials in Δ if Δ is an unmixed set.

We call a triangular set Δ a *weakly unmixed set* if part (b) of Theorem 2.4.6 is not satisfied, i.e. the polynomials in Δ are not necessary square-free.

For a triangular set Δ the sets $V_{\mathrm{Rep}}(\Delta)$ and $\mathrm{Ap}(\Delta)$ denotes respectively the algebraic set and the associated primes corresponding to the radical $\mathrm{Rep}(\Delta)$ and not to $\langle\Delta\rangle$.

We call a set of triangular sets Σ *simple* if for all $\Delta \neq \Delta' \in \Sigma$ we have

$$\mathrm{Ap}(\Delta) \cap \mathrm{Ap}(\Delta') = \emptyset.$$

2.2 Gröbner bases

Gröbner bases and their computations were introduced by Buchberger in 1965, and are the most widespread methods for computing with multivariate polynomials, due to their wide range of applications. The core of the method is to compute a standard form G (Gröbner basis) for a given set of multivariate polynomials F such that F and G generate the same ideal I and ideal membership in I is decidable using a systematic series of multivariate divisions with remainders by the elements of G. Applications of Gröbner bases include solving the ideal and radical-ideal membership problem, the computation of elimination ideals or the intersection of ideals, and the determination of the solvability of polynomial systems.

Although algorithms using Gröbner bases work efficiently in practice for many applications, they are unlikely to give sub-exponential complexity bounds, since the

ideal membership problem over $\mathbb{Q}$ is exponential space complete [May89]. In the setting of this thesis we are interested in recovering the geometric properties of the algebraic set corresponding to given polynomials and not the ideal generated by the polynomials. Hilbert's Nullstellensatz gives a one-to-one correspondence between the algebraic sets corresponding to an ideal and the radical of the ideal. Solving the radical-ideal membership problem is a sub-case of the general ideal membership problem, and as we shall see later, there are single exponential and sub-exponential complexity bounds solving the former problem. It would be interesting to see if a modified version of the Gröbner basis method could give similar bounds for the special case of radical ideals. Another unsolved issue concerning Gröbner bases is whether the running time of the algorithms can be considerably reduced by parallelizing the computations.

Since we will not use the concept of Gröbner bases in the rest of this dissertation, we only give a brief overview of the definitions and the computational methods, following the approach in [BCK88].

Let $\Bbbk$ be an arbitrary coefficient field and $R = \Bbbk[x_1, \ldots, x_n]$ be the set of polynomials in n variables with coefficients from $\Bbbk$. A *monomial* in R is a polynomial in the product form $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ where $(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$. We shall abbreviate $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ by x^α. First we need a notion of reduction of polynomials which is an appropriate generalization of the univariate division with remainder for the multivariate case. For this end we need a total ordering T on the monomials in R satisfying the following properties:

1. $1 <_T m$ for all $m \neq 1$,

2. if $m_1 <_T m_2$ then $m_1 \cdot u <_T m_2 \cdot u$ for all u

where m, m_1, m_2, u are monomials in R. Total orders satisfying these conditions are called *term orders*. The following representation of term orders are due to Ostrowski (see [GS93]):

Proposition 2.2.1 *Let $M \subset R$ be a finite set of monomials, denote the corresponding exponents by $\mathcal{A} = \{\alpha \in \mathbb{N}^n \mid x^\alpha \in M\}$, and let T be a term order on the monomials of R. Then there exists a positive weight vector $w \in \mathbb{R}_+$ such that for all $x^\alpha, x^\beta \in M$ $x^\alpha <_T x^\beta$ if and only if $\alpha \cdot w < \beta \cdot w$.* ■

Let $\prec$ be a fixed term order on the monomials of R. The *initial monomial* $\text{init}_\prec(p)$ of a polynomial $p \in R$ is the largest monomial with nonzero coefficient that appears in p. A polynomial f *reduces to* g *modulo* $P := \{p_1, \ldots, p_k\} \subset R$ with respect to $\prec$ if there exists $p_i \in P$ and a monomial m such that $g = f - mp_i$ and $\text{init}_\prec(g) \prec \text{init}_\prec(f)$. Denote by $f \to_P g$ the relation "f reduced to g modulo P", and $f \to_P^* g$ the transitive closure of $f \to_P g$. We say that a polynomial f is in reduced form (sometimes called normal form) modulo P if $f \to_P^* g$ implies that $f = g$. Finally, we define the *S-polynomial* of two polynomials $f, g \in R$ to be

$$\text{Spoly}(f, g) := m_1 f - m_2 g$$

where $m_1 \cdot \text{init}_\prec(f) = m_2 \cdot \text{init}_\prec(g) = \text{lcm}(\text{init}_\prec(f), \text{init}_\prec(g))$.

The following proposition gives equivalent definitions for the Gröbner bases of an ideal [GM91]:

Proposition 2.2.2 *Given an ideal $\mathcal{I} \subset R$ and a finite subset $G = \{g_1, \ldots, g_m\}$ of I. The following statements are equivalent:*

1. *The ideal* $\text{init}_\prec(\mathcal{I}) := \langle \text{init}_\prec(p) \mid p \in \mathcal{I} \rangle$ *is generated by monomials* $\{\text{init}_\prec(g_1), \ldots \text{init}_\prec(g_m)\}$.

2. *G generates $\mathcal{I}$ and every polynomial $p \in R$ has a unique reduced form modulo G.*

3. *G generates $\mathcal{I}$ and the S-polynomial of any two elements in G reduces to 0 modulo G.*

If G satisfies either of the above conditions we call G a Gröbner basis for $\mathcal{I}$. ■

The first statement is the usual way to define Gröbner bases. As a consequence of the first statement, Gröbner bases can be used for many applications, e.g. computing the Hilbert polynomial of an ideal, or computing elimination ideals, etc. As a consequence of the second statement Gröbner bases enable us to solve the ideal membership problem. The third statement gives the following algorithm which transforms any generating set F of $\mathcal{I}$ into a Gröbner basis:

Algorithm 2.2.3 (Buchberger)

$i := 0$

$\Delta_0 := F$

do $\Delta_{i+1} := \Delta_i \cup (\{\text{reduced}_{\Delta_i, \prec}(\text{Spoly}(g, g')) \mid g, g' \in \Delta_i\} - \{0\})$

while$(\Delta_i \neq \Delta_{i+1})$.

We call a Gröbner basis $G = \{g_1, \ldots, g_m\} \subset \mathcal{I}$ to be *reduced* if no monomial in g_i is a multiple of an initial monomial $\text{init}_{\prec}(g_j)$ for $i \neq j$. If the polynomials in F have total degree $\leq D$ and G is a reduced Gröbner basis then all polynomials in G have degree $\leq D^{2^n}$, and all the polynomials occurring in the above computation have at most that degree. This double exponential bound is attained in the general case, but for some important special cases (e.g. zero-dimensional ideal) singly exponential bounds are known.

2.3 Ritt-Wu Characteristic sets

Before defining the Ritt-Wu characteristic sets, first we give some definitions following the approach in [BCK88].

We consider polynomials in the polynomial ring $R := \Bbbk[x_1, \ldots, x_n]$ where k is an arbitrary field. Assume that the variables are linearly ordered by their subscript: $x_1 < x_2 < \cdots < x_n$. Then class(p) denotes the highest indeterminate appearing in a polynomial p, and lc(p) denote the leading coefficient of p regarded as a univariate polynomial in class(p). So, if class(p) $= x_k$ then lc(p) $\in \Bbbk[x_1, \ldots, x_{k-1}]$.

We call a set of polynomials $\Delta = \{g_1, \ldots, g_k\}$ a *triangular set* if class(g_i) $<$ class(g_j) for all $i < j$. E.g. $\Delta = \{x_1x_2,\ x_1^3x_3^2 - x_1x_2^4,\ x_4^2,\ x_1x_2 + x_5\}$ is a triangular set because class(x_1x_2) $= x_2 <$ class($x_1^3x_3^2 - x_1x_2^4$) $= x_3 <$ class(x_4^2) $= x_4 <$ class($x_1x_2 + x_5$) $= x_5$.

The *type* of a triangular set $\Delta = \{g_1, \ldots, g_k\}$ is a vector in $(\mathbb{N} \cup \{\infty\})^n$ such that the jth entry of type(Δ) is ∞ if there exists no $g_s \in \Delta$ with class(g_s) $= x_j$ and it is

equal to $\deg_{x_j} g_s$ if $\text{class}(g_s) = x_j$.

The procedure *pseudo division* generalizes the method of division with remainder for univariate polynomials to multivariate polynomials. Let $f, g \in \mathbb{k}[x_1, \ldots, x_n]$ be polynomials with $\text{class}(g) = x_j$. Then there exist polynomials q and r and a number $\alpha \in \mathbb{N}$ such that

$$\text{lc}(g)^\alpha f = qg + r$$

where $\deg_{x_j}(r) < \deg_{x_j}(g)$ and $\alpha \leq \deg_{x_j}(f) - \deg_{x_j}(g) + 1$. We denote by $r = \text{prem}(f, g)$ the *pseudo remainder* of f by g, and by $q = \text{pquo}(f, g)$ the *pseudo quotient* of f by g. If α is minimal, then q and r are uniquely determined.

In order to generalize the pseudo remainder concept for triangular sets, consider a triangular set $\Delta = \{g_1, \ldots, g_k\} \subset \mathbb{k}[x_1, \ldots, x_n]$ and a polynomial $f \in \mathbb{k}[x_1, \ldots, x_n]$. There exists a sequence of polynomials $f_k = f, \ldots, f_0$ such that for each $k \geq s \geq 1$, f_{s-1} is the pseudo remainder obtained when dividing f_s by g_s. Combining these pseudo divisions for $k \geq s \geq 1$ we get that

$$\text{lc}(g_k)^{\alpha_k} \cdots \text{lc}(g_1)^{\alpha_1} f = \sum_{s=1}^{k} q_s g_s + f_0$$

and we denote by $f_0 = \text{prem}(f, \Delta)$ the *pseudo remainder* of f by Δ. Note that $\deg_{x_{i_s}}(f_0) < \deg_{x_{i_s}}(g_s)$ if $\text{class}(g_s) = x_{i_s}$ $(s = 1, \ldots, k)$. We say that f is *reduced* modulo the triangular set Δ if $f = \text{prem}(f, \Delta)$.

We give two equivalent definitions (and characterizations) of Ritt-Wu character-

istic sets [BCK88, GM91]:

Proposition 2.3.1 : *Let* $\mathcal{I} \subseteq R = \Bbbk[x_1, \ldots, x_n]$ *be an ideal and* $\Delta = \{g_1, \ldots, g_k\} \subset \mathcal{I}$ *be a triangular set. The following statements are equivalent:*

1. Δ *is a minimal element among all the triangular sets in* $\mathcal{I}$ *with respect to the following ordering* $\prec$*:* $F \prec \Delta$ *if and only if* $\text{type}(F) <_{\text{lex}} \text{type}(\Delta)$.

2. *For every element* $f \in \mathcal{I}$, $\text{prem}(f, \Delta) = 0$.

If a triangular set $\Delta \subset \mathcal{I}$ *satisfies either of the above conditions we call* Δ *a characteristic set for* $\mathcal{I}$.

Remark: By the second statement, if Δ is a characteristic set of the ideal $\mathcal{I}$, then

$$\langle \Delta \rangle \subseteq \mathcal{I} \subseteq \{h \in \Bbbk[x_1, \ldots, x_n] \mid \text{prem}(h, \Delta) = 0\}.$$

The above inclusions are usually proper.

Example: If $\mathcal{I} = \langle x^2y^2 - x^2 - y^2 + 1,\ xy \rangle$ and $x < y$, then $\Delta = \{x^3 - x, xy\}$ is a characteristic set, but $\langle x^3 - x, xy \rangle \neq \langle x^2y^2 - x^2 - y^2 + 1,\ xy \rangle$ because the dimensions of the corresponding varieties are not equal. Also, $\langle x^2y^2 - x^2 - y^2 + 1,\ xy \rangle \neq \mathcal{J} = \{h \mid \text{prem}(h, \Delta) = 0\}$; for example y is in $\mathcal{J}$ but not in $\mathcal{I}$.

Proof: (1) $\Longrightarrow$ (2): Suppose $\Delta = \{g_1, \ldots, g_k\}$ is minimal w.r.t. $\prec$ and there is a polynomial $p \in I$ s.t. $p' := \text{prem}(p, \Delta) \neq 0$. If for an index $0 \leq j \leq n$ we have

$$0 < \text{class}(g_1) < \cdots < \text{class}(g_j) < \text{class}(p') \leq \text{class}(g_{j+1})$$

then it is easy to show that $\Delta' := \{g_1, \ldots g_j, p'\}$ is a triangular set smaller than Δ w.r.t. $\prec$.

(2) $\Longrightarrow$ (1): If there is a triangular set $\Delta' \prec \Delta$ and $g_i' \in \Delta'$ is the first element which differs from the elements in Δ, then $g_i' \in I$ and $\mathrm{prem}(g_i', \Delta) \neq 0$ which contradicts (2). ■

In the following we summarize the main geometric properties of characteristic sets [BCK88]: Informally, if F is a finite set of polynomials, then Δ is a characteristic set of the ideal $\langle F \rangle$ if Δ is triangular and F and Δ have "almost" the same zeros. More formally:

Proposition 2.3.2 *Let F be a finite set of polynomials in $\mathbb{k}[x_1, \ldots, x_n]$. If Δ is a characteristic set of the ideal $\langle F \rangle$ then*

$$V(\Delta) - \left(\bigcup_{i=1}^{k} V(\mathrm{lc}(g_i)) \right) \subseteq V(F) \subseteq V(\Delta),$$

where $V(P) = \{x \in \mathbf{K}^n \mid \forall p \in P\ p(x) = 0\}$ and $\mathbf{K}$ is the algebraic closure of $\mathbb{k}$.

Proof: To prove the first inequality, let $x \in V(\Delta) - \left(\bigcup_{i=1}^{k} V(\mathrm{lc}(g_i)) \right)$ and $f \in I$. Since $\mathrm{prem}(f, \Delta) = 0$ by Proposition 2.3.1.(2), we have $\mathrm{lc}(g_r)^{\alpha_r} \cdots \mathrm{lc}(g_1)^{\alpha_1} f = \sum_{s=1}^{k} q_s g_s$. Now $\sum_{s=1}^{k} q_s g_s(x) = 0$ and $\mathrm{lc}(g_r)^{\alpha_r} \cdots \mathrm{lc}(g_1)^{\alpha_1}(x) \neq 0$, therefore $f(x) = 0$. The second inequality is true since $\Delta \subset I$. ■

In the original work of Ritt and later by Wu they propose an algorithm to compute an "extended" characteristic set by repeated application of pseudo division.

Without defining the notion of extended characteristic sets we just mention that they satisfy Proposition 2.3.2. Since the algorithms developed in this thesis are extensions of the original Ritt-Wu process, we state a version of it without proof of correctness. For more details see [GM91].

Algorithm 2.3.3 (Ritt-Wu process)

Input: $F = \{f_1, \ldots, f_r\}$

Output: Δ *an extended characteristic set of* F

$\Delta := \emptyset$; $R := \emptyset$;

do $F := F \cup R$; $F' := F$; $R := \emptyset$;

  while$(F' \neq \emptyset)$ **do**

    Let $f \in F'$ *minimal* class *and* deg;

    $F' := F' - \{g \mid \text{class}(g) = \text{class}(f),\ \text{prem}(g, f) \neq g\}$

    $\Delta := \Delta \cup \{f\}$ **od**

  for all $f \in F - \Delta$ **do**

    if $r := \text{prem}(f, \Delta) \neq 0$ **then** $R := R \cup \{r\}$ **od**

od while $(R \neq \emptyset)$

return Δ

It is not hard to see that the algorithm terminates, but its worst case running time has been shown to be a non-elementary function in the input-size. [GM91].

On the other hand, Gallo and Mishra prove upper bounds for the degree of the polynomials in a characteristic set. Moreover, they also show that their degree bounds are sharp. Thus, they obtain a complexity bound in the dense representation

of polynomials for the computation of characteristic sets by simply solving a linear equation system for the coefficients of the polynomials in the characteristic set. Below we describe these results of Gallo and Mishra together with the proofs. First we discuss the zero-dimensional case and then the general case.

Lemma 2.3.4 (Gallo-Mishra) *Let $\mathcal{I} = \langle f_1, ..., f_s \rangle$ be a zero-dimensional ideal in $R := \Bbbk[x_1, \ldots, x_n]$ where k is an arbitrary field and $\deg(f_i) \leq d$ for all $1 \leq i \leq s$. Then for every $1 \leq j \leq n$ there exists a monic univariate polynomial $h_j \in I \cap \Bbbk[x_j]$ and $b_{j,1}, \ldots, b_{j,s} \in R$ such that*

$$h_j = \sum_{i=1}^{s} b_{j,i} f_i,$$

where $\deg(h_j) \leq 2(d+1)^{2n}$, and $\deg(b_{j,i} f_i) \leq 4(d+1)^{2n}$, $1 \leq i \leq s$.

Proof Let K be the algebraic closure of k and assume that $\mathcal{I}$ has T zeroes $V(\mathcal{I}) = \{(p_{i,1}, \ldots, p_{i,n}) \in K^n \mid 1 \leq i \leq T\}$. By Bezout's theorem we have $T \leq (d+1)^n$. Define $h'_j(x_j) \in \Bbbk[x_j]$ by

$$h'_j(x_j) = \prod_{i=1}^{T} (x_j - p_{i,j})$$

a monic degree T univariate polynomial in x_j for $1 \leq j \leq n$. Since h'_j vanishes on $V(I)$, by Hilbert's Nullstellensatz we have

$$h'_j \in \sqrt{I}$$

i.e. there is an $M \in \mathbb{N}$ such that $h_j := (h'_j)^M \in \mathcal{I}$. By the effective Nullstellensatz results of Brownawell [Bro87] or Kollar [Kol88] we have that $M \leq 2(d+1)^n$. Therefore

$$\deg(h_j) \leq 2(d+1)^{2n} \quad 1 \leq j \leq n.$$

Also as a consequence of the effective Nullstellensatz we have that

$$\deg(b_{j,i}f_i) \leq 2(T+1)(d+1)^n \leq 4(d+1)^{2n}.$$

■

Corollary 2.3.5 *Let R and $\mathcal{I} = \langle f_1, ..., f_s \rangle$ as above, and let $g \in \mathcal{I}$ a polynomial of degree D. Then there are polynomials $a_1, \ldots, a_s$ such that*

$$g = \sum_{i=1}^{s} a_i f_i$$

and $\deg(a_i f_i) \leq \max(d, D) + 6n(d+1)^{2n}$, $1 \leq i \leq s$.

Proof: Using univariate division with remainder by the polynomials $h_1, \ldots, h_n$ from lemma 2.3.4, g may be expressed as

$$g = h + \sum_{i=1}^{s} a_i' f_i$$

where $h \in \mathcal{J} := \langle h_1, \ldots, h_n \rangle$ and $\deg_{x_j}(a_i') \leq \deg_{x_j}(h_j)$ for all $1 \leq i \leq s$ and $1 \leq j \leq n$. Therefore $\deg(a_i' f_i) \leq \max_{1 \leq i \leq s}\{\deg(f_i)\} + \sum_{j=1}^{n} \deg_{x_j}(h_j) \leq d + 2n(d+1)^{2n}$.

From $h = g - \sum_{i=1}^{s} a_i' f_i$ we have $\deg(h) \leq \max(D, d + 2n(d+1)^{2n})$. Since all the polynomials in $\mathcal{H} = \{h_1, \ldots, h_n\}$ are monic, $\mathcal{H}$ forms a characteristic set for $\mathcal{J}$ and we can express

$$h = \sum_{i=1}^{n} q_i h_i = \sum_{j=1}^{s} (\sum_{i=1}^{n} q_i b_{i,j}) f_j = \sum_{j=1}^{s} a_j'' f_j$$

where $\deg(a_j'' f_j) \leq \deg(h) + 4(d+1)^{2n} \leq \max(D, d) + 6n(d+1)^{2n}$, using Lemma 2.3.4. We have

$$g = \sum_{i=1}^{s} (a_i' + a_i'') f_i$$

and the claim of the corollary is proved. ■

Theorem 2.3.6 (Zero-dimensional degree upper bound) *Let R and $\mathcal{I}$ be as above. Then $\mathcal{I}$ has a characteristic set $\Delta = \{g_1, \ldots, g_n\}$ where for each $1 \leq j \leq r$*

1. $\text{class}(g_j) = x_j$,
2. $\deg(g_j) \leq 2n(d+1)^{2n}$ *and*
3. $\exists a_{j,1}, \ldots a_{j,s} \in R$ *such that* $g_j = \sum_{i+1}^{s} a_{j,i} f_i$ *with* $\deg(a_{j,i} f_i) \leq 8n(d+1)^{2n}$ *for all* $1 \leq i \leq s$.

Proof: The first statement is trivial. Using the univariate polynomials

$$h_1, \ldots, h_n \in \mathcal{I}$$

from Lemma 2.3.4 we can obtain that $\deg_{x_j}(g_i) \leq \deg_{x_j}(h_j) \leq 2(d+1)^{2n}$ for all $1 \leq i, j \leq n$, which gives the second statement. Corollary 2.3.5 gives the third statement. ■

Theorem 2.3.7 (General degree upper bound) *Let R be as above and let $\mathcal{I} = \langle f_1, ..., f_s \rangle$ be an ideal in R. Suppose that $r = n - \dim(\mathcal{I}) = n - l$, and $\deg(f_i) \leq d$, for $1 \leq i \leq s$. Assume that $x_1, \ldots x_l$ are independent variables with respect to $\mathcal{I}$. Then $\mathcal{I}$ has a characteristic set $\Delta = \{g_1, \ldots, g_r\}$, where for each $1 \leq j \leq r$:*

1. $\text{class}(g_j) = j + l$
2. $\deg(g_j) \leq 4(s+1)(9r)^{2r} d(d+1)^{4r^2}$
3. $\exists a_{j,1}, \ldots a_{j,s} \in R$ *such that* $g_j = \sum_{i+1}^{s} a_{j,i} f_i$ *and* $\deg(a_{j,i} f_i) \leq 11(s+1)(9r)^{2r} d(d+1)^{4r^2}$ *for all* $1 \leq i \leq s$.

Proof: Assuming that the variables $x_1, \ldots x_l$ are independent with respect to $\mathcal{I}$, we can apply Theorem 2.3.6 over the function field $K = \Bbbk(x_1, \ldots, x_l)$ and the ring $R' = \mathbf{K}[x_{l+1}, \ldots, x_{l+r}]$, since $\mathcal{I}$ is zero-dimensional over K by the assumption on the dimension of $\mathcal{I}$. Thus there exists a characteristic set $\Delta' = \{g'_1, \ldots, g'_r\} \subset R'$ for $\mathcal{I}$ with degree upper bounds $2r(d+1)^{2r}$ for the variables $\{x_{l+1}, \ldots, x_{l+r}\}$. To compute Δ' one can set up a linear equation system for the unknown coefficients of $a_{j,i}$ in the equation $g_j = \sum_{i+1}^{s} a_{j,i} f_i$ such that the size of this system is bounded by

$$\Gamma := \binom{8r(d+1)^{2r} + r}{r}.$$

The entries of this equation system are from $K = \Bbbk(x_1, \ldots, x_l)$. Hence the degree in the variables $x_1, \ldots, x_l$ of the numerators and the denominators of the solution are bounded by determinants of polynomial matrices of size $\leq \Gamma$. To get the characteristic set of $\mathcal{I}$ in R we just have to multiply g'_j by the least common multiple of its denominators. The claim of the theorem follows after some calculations.

2.4 Kalkbrener's unmixed representation

As we mentioned earlier, our objective is to find a generalization of the notion of Ritt-Wu characteristic sets, where the computational convenience of triangular sets is preserved, but no information is lost about the roots of the polynomials in the ideal. Below we define the unmixed triangular sets, which are triangular sets representing algebraic varieties such that all the irreducible components have the same dimension. Based on the work of Michael Kalkbrener [Kal96] we show that every algebraic variety can be expressed as the union of varieties represented by

unmixed triangular sets. We also prove in this section and in the next chapter that the unmixed representation of radical ideals satisfies the following properties mentioned in the introduction:

- membership in the radical ideal $I(V)$ is efficiently decidable;
- set operations such as the union or the difference of algebraic sets are efficiently computable;
- the representation of the empty set is unique;
- the size of the representation is reasonably small relative to the input size in the dense representation of polynomials;
- the computation is reasonably fast and is parallelizable.

In the following subsections we discuss the connection between characteristic sets and decomposition of algebraic varieties. This will lead us to our main subject, the unmixed representation of radical ideals, which we define in Theorem 2.4.6. In the next chapter we give an algorithm which finds this unmixed representation, together with its complexity analysis.

2.4.1 Decomposition of algebraic varieties

We start this section with an example:

Example 2.4.1 In the example of the previous section, $V(x^2y^2-x^2-y^2+1,\ xy) \subset \mathbb{A}^2$ consist of the four points $\{(1,0),(-1,0),(0,1),(0,-1)\}$, while $V(x^3-x, xy)$

contains the points $\{(1,0),(-1,0)\}$ together with the whole y axis. We saw in the previous section that all the superfluous zeros of the characteristic set come from "degenerate" cases, when leading coefficients vanish. A possible solution to avoid superfluous roots would be to find the sub-varieties of $V(x^3-x) \subset \mathbb{A}^1$, at which leading coefficients of the polynomials in $\{x^2y^2-x^2-y^2+1,\ xy\}$ vanish. These leading coefficients are x and x^2-1, thus we can factor $V(x^3-x) = V(x) \cup V(x^2-1)$. After reducing the polynomials modulo x^2-1 and x, we get that

$$V(x^2y^2-x^2-y^2+1,\ xy) = V(x^2-1,\ y) \cup V(x, y^2-1).$$

Note that $\{x^2-1,\ y\}$ and $\{x, y^2-1\}$ are triangular sets and all the leading coefficients are 1. In the above example, we were able to express $\mathcal{I}$ as an intersection of two ideals which were generated by triangular sets, even though we could not find a generating characteristic set for $\mathcal{I}$.

More generally, suppose we are given an ideal $\mathcal{I} \subset \Bbbk[x_1, \ldots, x_n]$ where k is an arbitrary field with algebraic closure K. The example above suggests that if we could express the radical $\sqrt{\mathcal{I}}$ as

$$\sqrt{\mathcal{I}} = \mathcal{I}_1 \cap \ldots \cap \mathcal{I}_r$$

such that each $\mathcal{I}_i$ is generated by a triangular set, then this decomposition would preserve the computational convenience of triangular sets and give all the information about the roots of the polynomials in $\mathcal{I}$.

2.4.2 Zero-dimensional ideals

In the case when the ideal $\mathcal{I}$ is zero-dimensional, i.e. the polynomials in the ideal have only finitely many common zeros in K^n, the prime decomposition of the radical will give the desired representation of the radical as intersection of ideals generated by triangular sets, as asserted by the following:

Proposition 2.4.2 *Let $\mathcal{P} \subset \Bbbk[x_1, \ldots, x_n]$ be a zero-dimensional prime ideal. Then there exists a triangular set $\Delta = \{g_1, \ldots, g_n\}$ such that Δ generates $\mathcal{P}$,* $\mathrm{class}(g_i) = x_i$, $\mathrm{lc}(g_i) = 1$, *and the image of g_i in $\mathbf{K}(\mathcal{P} \cap \Bbbk[x_1, \ldots, x_{i-1}])[x_i]$ is irreducible.*

Proof: Before we start the proof we need the following observations:

1. Every zero-dimensional (Artinian) integral domain is a field. Hence, if $\mathcal{Q} \subset \Bbbk[x_1, \ldots, x_k]$ is a zero-dimensional prime ideal then $\Bbbk[x_1, \ldots, x_k]/\mathcal{Q}$ is a field.

2. If $\mathcal{I} \subset \Bbbk[x_1, \ldots, x_k]$ is zero-dimensional then $\mathcal{I} \cap \Bbbk[x_1] \neq \{0\}$.

We prove the proposition by induction on $i = 1, \ldots, n$. For $i = 1$ consider $\mathcal{P}_1 := \mathcal{P} \cap \Bbbk[x_1] \neq \{0\}$. Since $\mathcal{P}_1$ is a principal ideal, there exists $g_1 \in \Bbbk[x_1]$ such that $\langle g_1 \rangle_{\Bbbk[x_1]} = \mathcal{P}_1$. g_1 is monic irreducible over k which follows from $\mathcal{P}_1$ being a prime ideal.

Assume inductively that we have constructed $g_1, \ldots, g_{i-1} \in \mathcal{P}$ monic polynomials, such that $\mathrm{class}(g_j) = x_j$ and that $\langle g_1, \ldots, g_j \rangle = \mathcal{P} \cap \Bbbk[x_1 \ldots x_j]$ for all $1 \leq j \leq i-1$. Denote by $\mathcal{P}_{i-1} := \mathcal{P} \cap \Bbbk[x_1 \ldots x_{i-1}]$, and by $\mathcal{P}^{(i-1)}$ the image of $\mathcal{P}$ modulo $\mathcal{P}_{i-1}$. It is easy to prove that $\mathcal{P}_{i-1}$, and $\mathcal{P}^{(i-1)}$ are prime ideals in the rings $\Bbbk[x_1, \ldots, x_{i-1}]$ and $(\Bbbk[x_1, \ldots, x_{i-1}]/\mathcal{P}_{i-1})[x_i, \ldots, x_n]$ respectively.

Denote the field $\Bbbk[x_1, \ldots, x_{i-1}]/\mathcal{P}_{i-1} = \mathbf{K}(\mathcal{P}_{i-1})$ by k_{i-1}. Since $\mathcal{P}^{(i-1)} \cap k_{i-1}[x_i]$ is a principal prime ideal in $k_{i-1}[x_i]$, there exists a monic irreducible polynomial $g_i' \in k_{i-1}[x_i]$ such that $\langle g_i' \rangle = \mathcal{P}^{(i-1)} \cap k_{i-1}[x_i]$. It is easy to prove that for any inverse image $g_i(x_1, \ldots, x_i) \in \Bbbk[x_1, \ldots, x_i]$ of $g'(x_i)$ we have $\langle g_1, \ldots, g_i \rangle = \mathcal{P} \cap \Bbbk[x_1, \ldots x_i]$, which proves the proposition. ■

As a consequence, for a zero-dimensional prime ideal $\mathcal{P}$ we can find a characteristic set Δ such that

$$\langle \Delta \rangle = \mathcal{P} = \{h \mid \text{prem}(h, \Delta) = 0\}.$$

Thus, for zero-dimensional ideals, it is enough to find the prime decomposition of the radical and then to find a triangular generating set for each prime ideal. The primary decomposition of zero-dimensional ideals has been studied and analyzed by D. Lazard in [Laz81]. Also, D. Ierardi [Ier89] gives a method for solving algebraic systems using generalized resultant methods. In fact, in both approaches, the prime decomposition of radicals is reduced to the problem of factoring multivariate polynomials. Unfortunately, there is no efficient parallel algorithm known for factoring univariate polynomials over $\mathbb{Q}$.

As the example at the beginning of this subsection suggests, we do not necessarily need to find the complete prime decomposition of the ideal. The ideals $\langle x^2 - 1, y \rangle$ and $\langle x, y^2 - 1 \rangle$ are not prime ideals, but they are generated by triangular sets of monic polynomials. To compute this decomposition, we did not need to factor poly-

nomials completely, but only split a polynomial when there was a leading coefficient such that they have nontrivial gcd. Teitelbaum [Tei90] proposes an algorithm for such "lazy factorization" of zero-dimensional ideals. He reduces the problem to the univariate case by applying rational coordinate transformations and by finding primitive elements.

Applied to zero-dimensional ideals $\mathcal{I} = \langle F \rangle$, the algorithms in the present paper will *decompose* the radical of a zero-dimensional ideal $\mathcal{I}$ into

$$\sqrt{\mathcal{I}} = \langle \Delta_1 \rangle \cap \cdots \cap \langle \Delta_r \rangle$$

where Δ_i are triangular sets of monic polynomials. The sequential complexity of the algorithm is $(d^{n^2})^{O(1)}$, and the parallel arithmetic complexity is $(n \log(d))^{O(1)}$, where d is the maximal degree of the polynomials in F and n is the number of variables in F.

Moreover, given a triangular set Δ of monic polynomials which generates a zero-dimensional radical, and also given a polynomial f, we give an algorithm which splits $\langle \Delta \rangle$ into

$$\langle \Delta \rangle = (\bigcap_{i=1}^{r} \langle \Delta_i' \rangle) \cap (\bigcap_{j=1}^{s} \langle \Delta_j'' \rangle)$$

where Δ_i' and Δ_j'' are triangular sets of monic polynomials and

1. f is zero modulo $\langle \Delta_i' \rangle$.
2. f has an inverse modulo $\langle \Delta_j'' \rangle$.

for each $1 \leq i \leq r$ and $1 \leq j \leq s$. This algorithm will enable us to conduct symbolic computation on the complex roots of the polynomials in a zero-dimensional ideal

generated by a triangular set without computing the roots explicitly. Also, we give an algorithm which computes the union, the intersection and the quotient of zero-dimensional ideals generated by triangular sets of monic polynomials. These two algorithms are in the complexity class NC, i.e. they can be computed by an arithmetic circuit of polynomial size and depth polylogarithmic in the input size, which is in this case d^n, where d is the maximal degree of the input and n is the number of variables in the input. We use the dense representation of polynomials.

2.4.3 Higher dimensional ideals

In higher dimensions it is not true that every prime ideal is generated by a triangular set. Consider the following example:

Example 2.4.3 Consider the affine curve $\mathcal{C} = \{(x, y, z) \in \mathbb{A}^3 \mid x = t^3, y = t^4, z = t^5, t \in \mathbb{C}\}$. The corresponding ideal $\mathcal{I} \subset \mathbb{Q}[x, y, z]$ is generated by the polynomials $\{y^3 - x^4, z^2 - yx^2, xz - y^2\}$. It can be proved that $\mathcal{I}$ is a prime ideal in $\mathbb{Q}[x, y, z]$ (also in $\mathbb{C}[x, y, z]$), the codimension of $\mathcal{I}$ is 2 in $\mathbb{A}^3$, and $\mathcal{I}$ cannot be generated by fewer than 3 polynomials.

Ideals which are generated by a set of polynomials with cardinality equal to the codimension are called *complete intersections*. A more detailed treatment of the subject can be found e.g. in [Har77].

The above example suggests that if $\mathcal{P}$ is a prime ideal and Δ is any triangular set from $\mathcal{P}$, then in

$$\langle \Delta \rangle \subseteq \mathcal{P} \subseteq \{h \mid \mathrm{prem}(h, \Delta) = 0\}$$

the first inclusion must be proper if $\mathcal{P}$ is not a complete intersection. Our objective is to find a triangular set for which the second inclusion holds at equality. It turns out that such a triangular set always exists [Kal94].

Kalkbrener [Kal94] gives a representation (described below) of a prime ideal $\mathcal{P}$ by a triangular set Δ such that the second inclusion above is an equality, i.e.

$$\mathcal{P} = \{h \mid \text{prem}(h, \Delta) = 0\}.$$

Therefore, ideal membership can be algorithmically decided, given this triangular set. Furthermore, certain non-prime ideals are also representable by triangular sets in the same manner. This will lead to the notion of unmixed sets and unmixed representations and will enable us to avoid prime factorization. Kalkbrener's approach is based on the following result:

Proposition 2.4.4 (Kalkbrener) *Let R be a Noetherian commutative ring and $\mathcal{I}$ be an ideal in $R[x]$. Denote by $\mathbf{K}(\mathcal{P})$ the quotient field of the integral domain $R/\mathcal{P}$ where $\mathcal{P}$ is a prime ideal in R. Then the following are equivalent:*

(a) $\mathcal{I}$ is a prime ideal in $R[x]$

(b) $\mathcal{I} \cap R$ is prime in R, $\mathcal{J}$ is prime in $\mathbf{K}(\mathcal{I} \cap R)[x]$ and $\mathcal{I}(R/\mathcal{I} \cap R)[x] = \mathcal{J} \cap (R/\mathcal{I} \cap R)[x]$, where $\mathcal{J}$ is the ideal $\mathcal{I}\mathbf{K}(\mathcal{I} \cap R)[x]$.

(c) $\mathcal{I} \cap R$ is prime in R and there exists a polynomial $q \in R[x]$ such that the image of q in $\mathbf{K}(\mathcal{I} \cap R)[x]$ is either irreducible over $\mathbf{K}(\mathcal{I} \cap R)$ or zero and

$$\text{for every } f \in R[x]: \quad f \in \mathcal{I} \iff f^{\mathcal{I} \cap R} \in \langle q \rangle_{\mathbf{K}}$$

where $\langle q \rangle_{\mathbf{K}}$ *denotes the ideal in* $\mathbf{K}(\mathcal{I} \cap R)[x]$ *generated by* q *and* $f^{\mathcal{I} \cap R}$ *denotes the image of* f *in* $(R/\mathcal{I} \cap R)[x]$. ■

Proof:

(a)$\Longrightarrow$(b): If $\mathcal{I}$ is a prime ideal then clearly $\mathcal{I} \cap R \neq R$ and $\mathcal{I} \cdot (R/\mathcal{I} \cap R)[x] \neq (R/\mathcal{I} \cap R)[x]$ are also prime ideals. Since $\mathcal{I} \cdot (R/\mathcal{I} \cap R)[x] \cap (R/\mathcal{I} \cap R) = \{0\}$ we have that $\mathcal{J} = \mathcal{I} \cdot \mathbf{K}(\mathcal{I} \cap R)[x] \neq \mathbf{K}(\mathcal{I} \cap R)[x]$ which implies that $\mathcal{J}$ is also a prime ideal. The equation $\mathcal{I} \cdot \mathbf{K}(\mathcal{I} \cap R)[x] \cap (R/R \cap \mathcal{I})[x] = \mathcal{I} \cdot (R/R \cap \mathcal{I})[x]$ is also easy to verify.

(b)$\Longrightarrow$(a): Denote $\mathcal{I} \cap R$ by $\mathcal{P}$. Note that since $\mathcal{J}$ is a prime ideal in $\mathbf{K}(\mathcal{P})[x]$, $\mathcal{J} \cap (R/\mathcal{P})[x]$ is also a prime ideal in $(R/\mathcal{P})[x]$. Let $a, b \in R$ such that $ab \in \mathcal{I}$. Using the natural map $\varphi : R[x] \to (R/\mathcal{P})[x]$, we have that $\varphi(a), \varphi(b) \in (R/\mathcal{P})[x]$ and $\varphi(a)\varphi(b) = \varphi(ab) \in \mathcal{I} \cdot (R/\mathcal{P})[x]$. Since $\mathcal{I} \cdot (R/\mathcal{P})[x] = \mathcal{J} \cap (R/\mathcal{P})[x]$ is a prime ideal, we have that either $\varphi(a)$ or $\varphi(b)$ is in $\mathcal{I} \cdot (R/\mathcal{P})[x]$, which implies that a or b is in $\mathcal{I}$, therefore $\mathcal{I}$ is prime.

(b)$\Longrightarrow$(c): Let $\mathcal{P} = \mathcal{I} \cap R$. Since $\mathbf{K}(\mathcal{P})[x]$ is a principal ideal domain, there exists $\bar{q} \in \mathbf{K}(\mathcal{P})[x]$ such that $\mathcal{J} = \langle \bar{q} \rangle_{\mathbf{K}}$. Also, since $\mathcal{J}$ is prime, $\bar{q} = 0$ or $\bar{q}$ is irreducible over $\mathbf{K}(\mathcal{P})$. After multiplying by the denominators of the coefficients of $\bar{q}$ and taking any inverse image with respect to the map $R[x] \to (R/\mathcal{P})[x]$ we get $q \in R[x]$, such that $\langle q \rangle_{\mathbf{K}} = \mathcal{J}$. Let $f \in R[x]$. Then

$$f \in \mathcal{I} \implies f^{\mathcal{P}} \in \mathcal{I} \cdot (R/\mathcal{P})[x] \subseteq \mathcal{J} = \langle q \rangle_{\mathbf{K}}.$$

On the other hand,

$$f^{\mathcal{P}} \in \mathcal{J} \implies f^{\mathcal{P}} \in \mathcal{J} \cap (R/\mathcal{P}[x]) = \mathcal{I} \cdot (R/\mathcal{P})[x] \implies f \in \mathcal{I}.$$

(c)$\Longrightarrow$(b): $\mathcal{J} = \langle q \rangle_{\mathbf{K}}$ is prime because q is irreducible or zero. Let $f \in R[x]$ such that $f^{\mathcal{P}} \in \mathcal{J}$. Then $f \in \mathcal{I}$ and hence $f^{\mathcal{P}} \in \mathcal{I} \cdot (R/\mathcal{P})[x]$. On the other hand if $f \in \mathcal{I}$ then $f^{\mathcal{P}} \in \langle q \rangle_{\mathbf{K}} \cap (R/\mathcal{P})[x]$. ■

We use the above proposition inductively for $R = \Bbbk[x_1, \ldots, x_{n-1}]$ with the trivial base case where $R = \Bbbk$. If $\mathcal{P}$ is a prime ideal, then there exist polynomials $q_1, \ldots, q_n$ such that each q_i is in $\Bbbk[x_1, \ldots, x_i]$ and q_i is either zero or irreducible over $\mathbf{K}(\mathcal{I} \cap \Bbbk[x_1, \ldots, x_{i-1}])$. Moreover, for every $f \in \Bbbk[x_1, \ldots, x_n]$,

$$f \in \mathcal{P} \iff f = \sum_{i=1}^{n} p_i q_i$$

for some $p_i \in \mathbf{K}(I \cap \Bbbk[x_1, \ldots, x_{i-1}])[x_i]$, $1 \leq i \leq n$. It is easy to see that the latter condition is equivalent to the following: if $\Delta = \{q_i \mid q_i \neq 0,\ 1 \leq i \leq n\}$ then Δ is a triangular set and

$$\mathcal{P} = \{h \in \Bbbk[x_1, \ldots, x_n] \mid \mathrm{prem}(h, \Delta) = 0\}.$$

Example 2.4.5 As in the previous example, let $\mathcal{I} = \langle y^3 - x^4,\ z^2 - yx^2,\ xz - y^2 \rangle \subset \mathbb{Q}[x, y, z]$ be the prime ideal defining the curve $\mathcal{C} \in A^3$. For each $1 \leq i \leq 3$ we compute the polynomials q_i as follows:

1. For $i = 1$, $\mathcal{I} \cap \mathbb{Q}[x] = \{0\}$. Let $q_1 = 0$ and $\mathcal{P}_1 = \{0\}$. Then $\mathbf{K}(\mathcal{P}_1) = \mathbb{Q}(x)$.

2. For $i = 2$, $\mathcal{I} \cap \mathbb{Q}[x, y] = \langle y^3 - x^4 \rangle$. Let $q_2 = y^3 - x^4$. Then $\langle q_2 \rangle_{\mathbf{K}} \subset \mathbf{K}(\mathcal{P}_1)[y]$ obviously generates $\mathcal{I} \cap \mathbb{Q}[x, y]$. It is also clear that $\langle q_2 \rangle_{\mathbf{K}} \cap \mathbb{Q}[x, y] = \langle y^3 - x^4 \rangle$. Let $\mathcal{P}_2 = \langle y^3 - x^4 \rangle$. Then $\mathbf{K}(\mathcal{P}_2) = \mathbb{Q}(x)[y]/\langle y^3 - x^4 \rangle$.

3. Since $\mathbf{K}(\mathcal{P}_2)[z]$ is a principal ideal domain, $\mathcal{I}\mathbf{K}(\mathcal{P}_2)[z] = \langle z^2 - yx^2,\ xz - y^2\rangle_{\mathbf{K}}$ is generated by the gcd of the images of the polynomials $(z^2 - yx^2)$ and $(xz - y^2)$ in $\mathbf{K}(\mathcal{P}_2)[z]$. Since

$$\begin{aligned}(z^2 - yx^2) &= (xz - y^2)(\frac{z}{x} + \frac{y^2}{x^2}) + (\frac{y^4}{x^2} - yx^2)\\ \frac{y^4}{x^2} - yx^2 &= \frac{y}{x^2}(y^3 - x^4)\end{aligned}$$

we have that $\gcd(z^2 - yx^2, xz - y^2) = xz - y^2$ over $\mathbf{K}(\mathcal{P}_2)$. Note that after multiplying by the denominators in the above calculation we get the pseudo division of $(z^2 - yx^2)$ by the triangular set $\{y^3 - x^4,\ xz - y^2\}$. Let $q_3 = xz - y^2$.

Claim: $\langle q_3\rangle_{\mathbf{K}} \cap \mathbb{Q}[x, y, z] = \mathcal{I}$.

Proof: First observe that

$$\langle q_3\rangle_{\mathbf{K}} \cap \mathbb{Q}[x, y, z] = \{h \in \mathbb{Q}[x, y, z] \mid \mathrm{prem}(h, \Delta) = 0\}$$

where $\Delta = \{q_2, q_3\}$ is a triangular set. We saw in section 2.3 that $\mathrm{prem}(h, \Delta) = 0$ iff there are numbers α, β such that $\mathrm{lc}(q_2)^\alpha \mathrm{lc}(q_3)^\beta h \in \mathcal{I}$. Here $\mathrm{lc}(q_2) = 1$ and $\mathrm{lc}(q_3) = x$. Thus $\mathrm{prem}(h, \Delta) = 0$ iff $x^\beta h \in \mathcal{I}$ iff $h \in \mathcal{I}$ using that $x \notin \mathcal{I}$ and $\mathcal{I}$ is prime ideal. ■

To summarize the above results, let $\mathcal{P} \subset \Bbbk[x_1, \ldots, x_n]$ be a prime ideal. Then there exists a triangular set $\Delta = \{g_1, \ldots, g_m\}$ such that

$$\mathcal{P} = \{h \in \mathbb{Q}[x_1, \ldots, x_n] \mid \mathrm{prem}(h, \Delta) = 0\},$$

and if $\mathrm{class}(g_i) = x_j$ then g_i is irreducible in $\mathbf{K}(\mathcal{P} \cap \Bbbk[x_1, \ldots, x_{j-1}])[x_j]$. A triangular set satisfying the latter condition is called an *irreducible triangular set.*

We say that Δ *represents* the ideal $\mathcal{I}$ if

$$\mathcal{I} = \{h \in \Bbbk[x_1, \ldots, x_n] \mid \mathrm{prem}(h, \Delta) = 0\}. \tag{2.1}$$

Also, we will denote the right hand side of (2.1) by $\mathrm{Rep}_{\Bbbk[x_1,\ldots,x_n]}(\Delta)$ or simply $\mathcal{I} = \mathrm{Rep}(\Delta)$ if it is unambiguous. Thus using the prime decomposition of the radical of an ideal $\mathcal{I}$, we can express

$$\sqrt{\mathcal{I}} = \mathcal{I}_1 \cap \ldots \cap \mathcal{I}_r$$

where each $\mathcal{I}_i$ is represented by an irreducible triangular set.

Similarly to the zero-dimensional case, a "lazy" approach – using only gcd computations on polynomials – is sufficient to express radicals as

$$\sqrt{\mathcal{I}} = \mathcal{I}_1 \cap \ldots \cap \mathcal{I}_r$$

where $\mathcal{I}_i$ is represented by a triangular set Δ_i for each $1 \leq i \leq r$. In the case of a prime decomposition, we require the triangular set to be an irreducible triangular set in order to represent a prime ideal. In the "lazy" version we weaken this condition, and we only require the ideal represented by the triangular set to be a radical and a proper subset of $\Bbbk[x_1, \ldots, x_n]$. Theorem 2.4.6 below gives a sufficient condition for this.

A radical ideal and the corresponding variety are called *unmixed* if all the associated prime ideals have the same codimension. We will call a triangular set an *unmixed triangular set*, or simply unmixed set, if conditions (a) and (b) of Theorem 2.4.6 are satisfied. We shall see that the codimension of an ideal represented

by an unmixed triangular set C is equal to the number of polynomials in C. The *unmixed representation* of an ideal is a set of unmixed triangular sets such that the intersection of the radicals represented by these unmixed sets is the radical of the ideal.

Theorem 2.4.6 (Kalkbrener) *Let $R = \Bbbk[x_1, \ldots, x_{n-1}]$, let $\Delta \subset R[x_n]$ be a triangular set and $\mathcal{I} = \mathrm{Rep}_{R[x_n]}(\Delta)$. Suppose that $\mathcal{J} := \mathrm{Rep}_R(\Delta \cap R)$ is a radical ideal in R. Let $\mathcal{J} = \bigcap_{j=1}^{r} \mathcal{P}_j$ be the irredundant prime decomposition of $\mathcal{J}$. Furthermore, if $g \in \Delta - R$, then assume that g satisfies the following two conditions:*

(a) $\mathrm{lc}(g) \notin \mathcal{P}_j$ for each $1 \leq j \leq r$.

(b) g is square-free over $\mathbf{K}(\mathcal{P}_j)$ for each $1 \leq j \leq r$.

Then $\mathcal{I}$ is a radical ideal and $\mathcal{I} \neq \Bbbk[x_1, \ldots, x_n]$. Furthermore, all the prime ideals in the irredundant prime decomposition of $\mathcal{I}$ have the same codimension, assuming that the same is true for $\mathcal{J}$.

Proof: We prove the theorem modulo Lemma 2.4.8 which we state below. If $\Delta \cap R = \Delta$ then $\mathcal{I} = \mathcal{J} \cdot R[x_n]$, therefore $\mathcal{I}$ is also radical and $\mathcal{I} \neq R[x_n]$. Also, for $1 \leq j \leq r$, $\mathcal{P}'_j := \mathcal{P}_j \cdot R[x_n]$ are the associated primes of $\mathcal{I}$, thus, by Lemma 2.4.8 below, we have $\mathrm{height}(\mathcal{P}'_j) = \mathrm{height}(\mathcal{P}_j)$, so the second claim is also true.

Now assume that $g \in \Delta - R$ and for every $1 \leq j \leq r$ denote by $g^{(j)}$ the image of g in $\mathbf{K}(P_j)[x_n]$. By condition (a) we have $\deg_{x_n}(g_j) = \deg_{x_n}(g^{(j)}) > 0$. Let

$$g^{(j)} = \mathrm{lc}(g^{(j)}) \prod_{i=1}^{s_j} q_{i,j}$$

be the irreducible factorization of $g^{(j)}$ in $\mathbf{K}(P_j)[x_n]$. By condition (b) we have $q_{s,j} \neq q_{t,j}$ if $s \neq t$. By Proposition 2.4.4

$$\mathcal{Q}_{i,j} := \{f \in R[x_n] \mid f^{\mathcal{P}_j} \in \langle q_{i,j} \rangle_{\mathbf{K}(P_j)[x_n]}\}$$

is a prime ideal and clearly $\mathrm{Rep}_{R[x_n]}(\Delta) = \bigcap_{i,j} \mathcal{Q}_{i,j}$ is a prime decomposition for $\mathcal{I}$. Therefore $\mathcal{I}$ is radical. Since $\mathcal{Q}_{i,j} \neq \mathcal{P}_j \cdot R[x_n]$ and $\mathcal{Q}_{i,j} \cap R = \mathcal{P}_j$ for all $1 \leq i \leq s_j$, we have $\mathrm{height}(\mathcal{Q}_{i,j}) = \mathrm{height}(\mathcal{P}_j) + 1$ by Lemma 2.4.8, thus the second claim is also true. ■

The following corollary translates the previous result into a geometric characterization of the unmixed representation. As before, for a set of polynomials $P \in k[x_1, \ldots, x_n]$, the algebraic set $V(P)$ denotes $\{x \in \mathbf{K}^n \mid \forall p \in P;\ \ p(x) = 0\}$, where $\mathbf{K}$ is the algebraic closure of $\Bbbk$.

Corollary 2.4.7 *Let $\Delta = \{g_1, \ldots, g_m\} \subset \Bbbk[x_1, \ldots, x_n]$ be an unmixed triangular set. Then*

$$V(\mathrm{Rep}(\Delta)) = V(\Delta) - \bigcup_{i=1}^{m} V(\mathrm{lc}(g_i)),$$

where the right hand side of the equation is the Zariski closure of the difference, i.e. the smallest algebraic set containing the difference.

Proof: "$\supseteq$" is proved in Proposition 2.3.2.

"$\subseteq$": We prove the claim by induction on n, and use the notations of Theorem 2.4.6. For $n = 1$ the claim is trivial.

Assume that

$$V_{n-1}(\mathrm{Rep}(\Delta \cap R)) = V_{n-1}(\Delta \cap R) - \bigcup_{g \in \Delta \cap R} V_{n-1}(\mathrm{lc}(g)),$$

where $V_{n-1}(P) = \{x \in \mathbf{K}^{n-1} \mid \forall p \in P;\ p(x) = 0\}$ for $P \subset R$.

If $\Delta \subset R$, then the claim follows since $V(P)$ is a cylinder over $V_{n-1}(P)$ for all $P \subset R$.

Assume that $g_m \in \Delta - R$. We have to prove that for each irreducible component X in $V(\mathrm{Rep}(\Delta))$, X is not a subset of $V(\mathrm{lc}(g_m))$. By Hilbert's Nullstellenzats this is equivalent to showing that $\mathrm{lc}(g_m) \notin \mathcal{P}$ if $\mathcal{P}$ is an associated prime ideal of Δ. We saw in the previous proof that every associated prime of Δ is in the form

$$\mathcal{Q}_{i,j} := \{f \in R[x_n] \mid f^{\mathcal{P}_j} \in \langle q_{i,j} \rangle_{\mathbf{K}(\mathcal{P}_j)[x_n]}\}$$

where $\mathcal{P}_j$ is an associated prime of $\Delta \cap R$, and $g_m^{\mathcal{P}_j} = \mathrm{lc}(g_m^{\mathcal{P}_j}) \prod_{i=1}^{s_j} q_{i,j}$ is the irreducible factorization of $g_m^{\mathcal{P}_j}$ in $\mathbf{K}(P_j)[x_n]$. But $\mathrm{lc}(g_m)^{\mathcal{P}_j} \in \mathbf{K}(P_j)$, and is non-zero by assumption (a) of Theorem 2.4.6, hence it is a unit in $\mathbf{K}(P_j)[x_n]$. Therefore, $\mathrm{lc}(g_m) \in \mathcal{Q}_{i,j}$ would imply that $\langle q_{i,j} \rangle_{\mathbf{K}(P_j)[x_n]} = \mathbf{K}(P_j)[x_n]$, hence $q_{i,j} = 1$, a contradiction. ■

The following lemmas are used in the proof of Theorem 2.4.6.

Lemma 2.4.8 *Let R be a Noetherian ring, $\mathcal{P} \subset R$ prime ideal,* $\mathrm{height}(\mathcal{P}) = m$. *Let $\mathcal{Q} \subset R[x]$ be a prime ideal, $\mathcal{Q} \cap R = \mathcal{P}$ and $\mathcal{Q} \neq \mathcal{P} \cdot R[x]$. Then*

(a) $\mathrm{height}(\mathcal{P} \cdot R[x]) = m$

(b) $\mathrm{height}(\mathcal{Q}) = m + 1$

In order to prove Lemma 2.4.8 we need some commutative algebra and dimension theory, following the approach of Atiyah-Macdonald [AM69].

Fact 2.4.9 (Dimension theorem for local rings) *[AM69]*

Let R be a Noetherian local ring with maximal ideal $\mathcal{M}$. The following two integers are equal:

(a) the maximum length of chains of prime ideals in R;

(b) the least number of generators of an $\mathcal{M}$-primary ideal of R. ■

Corollary 2.4.10 *Let R be a Noetherian ring, $x_1, \ldots, x_r \in R$. Then every minimal associated prime ideal $\mathcal{P}$ of $\langle x_1, \ldots, x_r \rangle$ has height $\leq r$.*

Proof: In the local ring $R_{\mathcal{P}}$ the ideal $\langle x_1, \ldots, x_r \rangle_{A_{\mathcal{P}}}$ is $\mathcal{P}_{\mathcal{P}}$-primary, therefore $r \geq \dim(R_{\mathcal{P}}) = \text{height}(\mathcal{P})$. ■

Proof of Lemma 2.4.8

(a): Since $\text{height}(\mathcal{P}) = m$, there are elements $r_1, \ldots r_m \in R$ such that $\mathcal{P}$ is a minimal associated prime of $\mathcal{I} := \langle r_1, \ldots, r_m \rangle \subset R$. Then $\mathcal{P} \cdot R[x]$ is a minimal associated prime of $\mathcal{I} \cdot R[x]$ and hence $\text{height}(\mathcal{P}) \leq m$ by Corollary 2.4.10. On the other hand, if $\mathcal{P}_0 \subset \cdots \subset \mathcal{P}_m = \mathcal{P}$ is a maximal chain for $\mathcal{P}$, then $\mathcal{P}_0 \cdot R[x] \subset \cdots \subset \mathcal{P}_m \cdot R[x] = \mathcal{P} \cdot R[x]$ is a chain for $\mathcal{P} \cdot R[x]$, thus $\text{height}(\mathcal{P}) \geq m$.

(b): Since $\mathcal{P} \cdot R[x] \subset \mathcal{Q}$ we have $\text{height}(\mathcal{Q}) \geq \text{height}(\mathcal{P} \cdot R[x]) + 1 = m + 1$. Assume indirectly that $r := \text{height}(\mathcal{Q}) > m + 1$. Then it is easy to see (using the quotient ring $R[x]/\mathcal{P} \cdot R[x]$) that there is a chain $\mathcal{Q}_0 \subset \cdots \subset \mathcal{Q}_r = \mathcal{Q}$ such that $\mathcal{Q}_m = \mathcal{P} \cdot R[x]$. Let $S := R - \mathcal{P}$ a multiplicative set and $R'[x] = S^{-1}R[x]$. Consider the factor ring $R'[x]/\mathcal{P} \cdot \mathbb{R}'[x] \cong \mathbf{K}(\mathcal{P})[x]$ which has dimension 1. Since the images of

$\mathcal{Q}_m \subset \cdots \subset \mathcal{Q}_r$ form a proper chain of prime ideals for the image of $\mathcal{Q}$ in $\mathbf{K}(\mathcal{P})[x]$, we get that $r - m \leq 1$. ■

2.5 The u-representation

The last representation method we describe here is used in both the prime and unmixed decomposition algorithms and complexity results of [Chi84, Gri84, GH91]. The main idea is to represent each component by a birational projection and a single defining polynomial as a hyper-surface. We follow an approach similar to that of Giusti and Heintz [GH91], but instead of the worst case analysis of [GH91] we stress the possibility of randomization. We will also point out the connection of this representation to the concept of *u-resultants* together with its application in order to preserve and exploit the sparseness of the input polynomials. There are some basic algebraic facts we need for the proofs, which we will include below.

Definition 2.5.1 *The coordinate system* $\{x_1, \ldots, x_n\}$ *is normal with respect to* $V(f_1, \ldots, f_s) \subset \mathbb{A}^n$ *if there exists* $r \leq n$ *such that for the projection*

$$\pi_0 : (x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_r),$$

the restriction $\pi_0|_V$ *is surjective and finite. We note that a sufficient condition for* $\{x_1, ..., x_n\}$ *being normal is that the homomorphism*

$$\Bbbk[x_1, \ldots, x_r] \hookrightarrow \mathcal{A} := \Bbbk[x_1, \ldots, x_n]/(f_1, \ldots, f_s)$$

is injective and $\mathcal{A}$ *is integral over* $\Bbbk[x_1, \ldots, x_r]$.

Lemma 2.5.2 (Noether's normalization lemma) *Let k be an infinite field and $\mathcal{A} \neq 0$ be a finitely generated k-algebra. Then there exist elements*

$$y_1, \ldots, y_r \in \mathcal{A}$$

which are algebraically independent over k and $\mathcal{A}$ is integral over $\Bbbk[y_1, \ldots, y_r]$, i.e every elements of $\mathcal{A}$ has a monic minimal polynomial over $\Bbbk[y_1, \ldots, y_r]$.

Proof: Let $\{x_1, \ldots, x_n\}$ be a set of generators for A as a k-algebra. After permuting the indices we can assume that $x_1, \ldots, x_r$ are algebraically independent and $x_{r+1}, \ldots x_n$ are algebraic over $\Bbbk[x_1, \ldots, x_r]$. Assume that $n > r$ and assume by induction on n that x_i is integral over $\Bbbk[x_1, \ldots, x_{i-1}]$ for $1 \leq i \leq n-1$. Since x_n is algebraic over $\Bbbk[x_1, \ldots, x_r]$ it has a minimal polynomial $f(x_1, \ldots x_n) \in \Bbbk[x_1, \ldots, x_r, x_n]$, possibly not monic. Let F be the highest degree homogeneous part of f and assume that F has degree d. Choose $\lambda_1, \ldots \lambda_r \in k$ such that $F(\lambda_1, \ldots \lambda_r, 1) \neq 0$ and define $x_i' := x_i - \lambda_i x_n$ for $1 \leq i \leq r$. Then

$$\begin{aligned} f(x_1, \ldots x_n) &= f(x_1' + \lambda_1 x_n, \ldots, x_r' + \lambda_r x_n, , x_n) \\ &= f'(x_1', \ldots, x_r', \ldots, x_n) \\ &= F(\lambda_1, \ldots \lambda_r, 1) x_n^d + \ldots \quad . \end{aligned}$$

therefore $f'/F(\lambda_1, \ldots \lambda_r, 1) \in \Bbbk[x_1', \ldots, x_r', x_n]$ is a monic polynomial vanishing on x_n. ■

Note: we can see from the proof that a generic choice of linear combination of the coordinates will suffice to get a normal system of coordinates.

Definition 2.5.3 *The coordinate system* $\{x_1, \ldots, x_n\}$ *is generic with respect to* $V(f_1, \ldots, f_s) \subset \mathbb{A}^n$ *if it is normal and the projection*

$$\pi : (x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_{r+1})$$

separates the irreducible components of V*, i.e. if* $V_1 \not\subset V_2$ *are irreducible components of* V *then* $\pi(V_1) \not\subset \pi(V_2)$.

The following proposition is a generalization of the primitive element theorem for separable field extensions.

Proposition 2.5.4 *Let* $\Bbbk$ *be a perfect field and* $\mathcal{A}$ *be a finite dimensional semi-simple algebra over the function field* $\Bbbk(y_1, \ldots, y_r)$*. Then there exists an element* $y_{r+1} \in \mathcal{A}$ *such that* y_{r+1} *generates* $\mathcal{A}$ *as an algebra over* $\Bbbk(y_1, \ldots, y_r)$.

Proof: Since $\mathcal{A}$ is a finite dimensional semi-simple algebra over $\Bbbk(y_1, \ldots y_r)$, by Weddernburn's theorem we have an isomorphism

$$\varphi : \mathcal{A} \to \bigoplus_{i=1}^{m} K_i$$

where each K_i is a separable field extension of $\Bbbk(y_1, \ldots, y_r)$ for $1 \leq i \leq m$. By the primitive element theorem for separable fields, there exist primitive elements $z_i \in K_i$ for K_i over $\Bbbk(y_1, \ldots, y_r)$, i.e. $K_i = \Bbbk(y_1, \ldots, y_r, z_i)$ for $1 \leq i \leq m$. Then $y_{r+1} := \varphi^{-1}((z_1, \ldots, z_m))$ will generate $\mathcal{A}$ as an algebra over $\Bbbk(y_1, \ldots, y_r)$. ■

The following corollary combines the previous propositions.

Corollary 2.5.5 *Let $\Bbbk$ be an infinite field and assume that the polynomials*

$$f_1, \ldots f_k \in \Bbbk[x_1, \ldots, x_n]$$

define a radical ideal and an unmixed algebraic set V of dimension d. Then there exist linear forms $l_j = u_j - \sum_{i=1}^{n} c_{i,j} x_i$, $0 \leq j \leq d$ and polynomials $P \in \Bbbk[u_0, \ldots u_d]$ and $L_i \in \Bbbk[u_0, \ldots u_d, x_i]$, $(1 \leq i \leq n)$, such that the map

$$\Bbbk[\mathbf{x}, \mathbf{u}]/(f_1, \ldots f_k, l_1, \ldots, l_d) \longrightarrow \Bbbk[\mathbf{x}, \mathbf{u}]/(P, L_1, \ldots, L_n)$$

is an isomorphism. Moreover, the polynomials $L_i(\mathbf{u}, x_i) = g_i(\mathbf{u})x_i - h_i(\mathbf{u})$ are linear in the variable x_i, and the leading coefficients g_i are relatively prime to P.

Chapter 3

Building Blocks

3.1 Technical lemmas

Lemma 3.1.1 *Denote* $R = \Bbbk[x_1, \ldots, x_{n-1}]$. *Let* $\Delta = \{g_1, \ldots, g_m\}$ *be an unmixed set in* $R[x_n]$, *and assume that* $\deg_{x_n}(g_m) > 0$. *Then*

$$\mathrm{Rep}_{R[x_n]}(\Delta) = \{f \in R[x_n] \mid \forall\, \mathcal{P} \in \mathrm{Ap}(\Delta \cap R) : \quad f \in \langle g_m \rangle_{\mathbf{K}(\mathcal{P})[x_n]}\}.$$

Proof: "$\subseteq$" is trivial.

"$\supseteq$": Assume that $\forall\ \mathcal{P} \in \mathrm{Ap}(\Delta \cap R) : \quad f \in \langle g_m \rangle_{\mathbf{K}(\mathcal{P})[x_n]}$. Since $\langle g_m \rangle_{\mathbf{K}(\mathcal{P})[x_n]}$ is radical, this implies that $\mathrm{prem}(f, g_m) \in \mathcal{P}$ for all $\mathcal{P} \in \mathrm{Ap}(\Delta \cap R)$. Therefore

$$\mathrm{prem}(f, g_m) \in \bigcap_{\mathcal{P} \in \mathrm{Ap}(\Delta \cap R)} \mathcal{P} = \mathrm{Rep}(\Delta \cap R)$$

which implies that

$$f \in \langle \mathrm{Rep}(\Delta \cap R) \cup \{g_m\} \rangle \ : \ \mathrm{lc}(g_m)^\infty = \mathrm{Rep}(\Delta),$$

where $\mathrm{lc}(g_m)^\infty := \{\mathrm{lc}(g_m)^\alpha \mid \alpha > 0\}$. ■

Lemma 3.1.2 *Let $\mathcal{P}' \subset \Bbbk[x_1, \ldots x_s]$ be a prime ideal and $g, f_0, \ldots, f_k$ be polynomials in $\Bbbk[x_1, \ldots x_n]$. Assume that the maximal variable in g is x_t, $t > s$, and denote $R = \Bbbk[x_1, \ldots, x_{t-1}]$. Let $\mathcal{P} = \mathcal{P}' \cdot R$. Suppose that the leading coefficient* $\mathrm{lc}(g) \notin \mathcal{P}$. *Also, assume that* $\deg_{x_t}(g) \leq \deg_{x_t}(\sum_{i=0}^{k} y^i f_i)$ *where y is a new variable. Then*

1. $\gcd_{\mathbf{K}(\mathcal{P})}(g, f_0, \ldots f_k) = \gcd_{\mathbf{K}(\mathcal{P})(y)}(g, \sum_{i=0}^{k} y^i f_i)$, *and*

2. $\gcd_{\mathbf{K}(\mathcal{P})}(g, f_0, \ldots, f_k) = d$, $\deg_{x_t}(d) = D$ *if and only if*
   $\mathrm{RES}_{x_t}^{(D)}(g, \sum_{i=0}^{k} y^i f_i) \not\equiv 0$ *and* $\mathrm{RES}_{x_t}^{(D')}(g, \sum_{i=0}^{k} y^i f_i) \equiv 0 \mod (\mathcal{P})$ *for all* $0 \leq D' < D$.

The sub-resultants (see definition in Section 3.5) on the left hand side of (2) are taken over the function field $\mathbf{K}(\mathcal{P})(y)$ and g and $f := \sum_{i=0}^{k} y^i f_i$ are considered as univariate polynomials in x_t over $\mathbf{K}(\mathcal{P})(y)$.

Proof: 1. We follow the proof in [IK93, Lemma 15.2]. There they assume that the polynomials $f_0, \ldots, f_k$ are univariate over the coefficient field, but as we shall see, the proof is valid without this assumption. Let $d = \gcd_{\mathbf{K}(\mathcal{P})}(g, f_0, \ldots f_k)$ and $h = \gcd_{\mathbf{K}(\mathcal{P})(y)}(g, \sum_{i=0}^{k} y^i f_i)$. Then obviously d divides h. We need to show that h divides $f_0, \ldots, f_k$. Since h divides g, we have $h \in \mathbf{K}(\mathcal{P})[x_t]$, and we can assume that h is monic. There exist $q_i, p_i \in \mathbf{K}(\mathcal{P})[x_t, \ldots x_n]$ such that

$$f_i = q_i h + p_i$$

and the degree in the variable x_t of the polynomials p_i is strictly less that $\deg_{x_t} h$ for $0 \leq i \leq k$. Then $f = qh + p$, where

$$q = \sum_{i=0}^{k} q_i y^i, \quad p = \sum_{i=0}^{k} p_i y^i,$$

and the degree in the variable x_t of the polynomial p is strictly less than $\deg_{x_t} h$. Since h divides f, h divides $p = f - qh$. Consider p as a multivariate polynomial in the variables $x_{t+1}, \ldots, x_n, y$ with coefficients in $\mathbf{K}(\mathcal{P})[x_t]$. Then h divides all the coefficients of p, but these coefficients must also have smaller degree in x_t than h, therefore p must be identically zero. Since y is transcendental, this implies that $p_i = 0$ for all $0 \leq i \leq k$, which proves the first statement.

2. $\mathrm{RES}_{x_t}^{(D)}(g, f) \equiv 0 \mod (\mathcal{P})$ if and only if the matrix of the D-th sub-resultant of f and g is singular over $\mathbf{K}(\mathcal{P})(x_{t+1}, \ldots, x_n, y)$. Then by the definition of the D-th sub-resultant matrix (see the proof of the next theorem), there exist polynomials $p_1, p_2 \in \mathbf{K}(\mathcal{P})(x_{t+1}, \ldots, x_n, y)[x_t]$ not both zero, such that

$$\deg_{x_t}(fp_1 - gp_2) < D$$

and $\deg_{x_t}(p_1) < \deg_{x_t}(g) - D$, $\deg_{x_t}(p_2) < \deg_{x_t}(f) - D$. If $\gcd_{\mathbf{K}(\mathcal{P})}(f, g) = d$ and $\deg_{x_t}(d) = D$ then d divides $fp_1 - gp_2$, therefore $fp_1 - gp_2 \equiv 0$, i.e.

$$fp_1 = gp_2.$$

If $p_2 \equiv 0$ then $fp_1 \equiv 0$ and $p_1 \not\equiv 0$. Since $\mathbf{K}(\mathcal{P})(x_{t+1}, \ldots, x_n, y)[x_t]$ is an integral domain, we get that $f \equiv 0$. Therefore $d = g$, $D = \deg_{x_t}(g)$, and $\mathrm{RES}_{x_t}^{(D)}(g, f) = \mathrm{lc}(g) \notin \mathcal{P}$, contradiction. If $p_1 \equiv 0$ then $gp_2 \equiv 0$ and $p_2 \not\equiv 0$, therefore $g \equiv 0$ which is a contradiction, since $\mathrm{lc}(g) \notin \mathcal{P}$. So assume that both p_1 and p_2 are not identically zero. Then g divides fp_1 over $\mathbf{K}(\mathcal{P})(x_{t+1}, \ldots, x_n, y)$. This implies that g/d must divide p_1, but $\deg_{x_t}(p_1) < \deg_{x_t}(g) - D$, so $p_1 \equiv 0$, a contradiction.

To prove the other direction, if $\gcd_{\mathbf{K}(\mathcal{P})}(f, g) = d$ has positive degree in x_t then the equation $p_1 f + p_2 g = d'$ is infeasible for $D' = deg_{x_t}(d') \leq \deg_{x_t}(d)$, so again by

definition, the matrix of D'-th sub-resultant is singular over $\mathbf{K}(\mathcal{P})(x_{t+1}, \ldots, x_n, y)$, therefore its determinant is identically zero modulo $\mathcal{P}$. ■

Lemma 3.1.3 *Let $\Delta = \{g_1, \ldots, g_m\}$ be an unmixed set in $\Bbbk[x_1, \ldots x_t]$, $f_0, \ldots, f_k \in k[x_1, \ldots x_n]$, $n \geq t$, and assume that $\deg_{x_t}(g_m) > 0$. Assume that the following conditions are satisfied:*

$$\begin{aligned} \mathrm{RES}_{x_t}^{(D)}(g_m, \textstyle\sum_{i=0}^{k} y^i f_i) &\not\equiv 0 \mod (\mathcal{P}) \text{ and} \\ \mathrm{RES}_{x_t}^{(D')}(g_m, \textstyle\sum_{i=0}^{k} y^i f_i) &\equiv 0 \mod (\mathcal{P}),\ 0 \leq D' < D \end{aligned} \tag{3.1}$$

for all $\mathcal{P} \in \mathrm{Ap}(\Delta_{m-1})$, where $\Delta_{m-1} = \{g_1, \ldots, g_{m-1}\}$. Then there exists a polynomial

$$\mathbf{d} = \mathbf{ggcd_t}(\Delta, f_0, \ldots, f_k)$$

such that

1. $\mathbf{d} \in \Bbbk[x_1, \ldots x_t]$;
2. $\mathbf{d} \in \langle \mathrm{Rep}(\Delta_{m-1}) \cup \{g_m\} \cup \mathrm{coeff}_{t+1}^{n}(f_0, \ldots, f_k) \rangle$, *where* $\mathrm{coeff}_{t+1}^{n} \subset k[x_1, \ldots, x_t]$ *is the set of coefficients of $f_1, \ldots f_k$ as multivariate polynomials in the variables $\{x_{t+1}, \ldots, x_n\}$.*
3. $\mathrm{lc}(\mathbf{d}) \notin \mathcal{P}$ *for all* $\mathcal{P} \in \mathrm{Ap}(\Delta_{m-1})$;
4. *the monic image of* $\mathbf{d}$ *in* $\mathbf{K}_{R_m}(\mathcal{P})[x_t]$ *is* $d = \gcd_{\mathbf{K}_{R_m}(\mathcal{P})}(g_m, f_0, \ldots, f_k)$ *for all* $\mathcal{P} \in \mathrm{Ap}(\Delta_{m-1})$.

Proof:

We will prove the proposition by constructing the polynomial

$$\mathbf{ggcd_t}(\Delta, f_0, \ldots, f_k)$$

as follows. Let

$$f = \sum_{i=0}^{k} y^i f_i,$$

and consider the unique solution of the non-singular linear system over $\mathbf{K}_{R_{m-1}}(\mathcal{P})(y)$ for some $\mathcal{P} \in \mathrm{Ap}(\Delta_{m-1})$

$$\Phi_D \cdot \begin{pmatrix} p_{d_2'} \\ \vdots \\ p_0 \\ q_{d_1'} \\ \vdots \\ q_0 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \tag{3.2}$$

where Φ_D is the D-th sub-resultant of f and g_m, $d_1' = \deg_{x_t}(g_m) - D - 1$ and $d_2' = \max_i\{\deg_{x_t}(f_i)\} - D - 1$. Define

$$p = \sum_{i=0}^{d_2'} p_i x_t^i \text{ and } q = \sum_{j=0}^{d_1'} q_j x_t^j.$$

From Lemma 3.1.2 and from the fact that d is monic we have that

$$d = fp + gq.$$

Now let $\Phi_D^{(j)}$ be the matrix obtained by interchanging the j-th column with the right hand side of the system (3.2) for all $1 \leq j \leq d_1' + d_2' + 2$, i.e.

$$\Phi_D^{(j)} = \left[\begin{array}{c|c|c} & \overset{j}{\underline{}} & \\ & 0 & \\ & 0 & \\ \Phi_D & \vdots & \\ & 0 & \\ & 1 & \end{array}\right]$$

Define

$$\begin{aligned} \bar{p}_i &:= \det(\Phi_D^{(i+1)}), \quad 0 \leq i \leq d_2' \\ \bar{q}_j &:= \det(\Phi_D^{(d_2'+j+1)}), \quad 0 \leq j \leq d_1' \end{aligned} \tag{3.3}$$

polynomials in $\Bbbk[x_1, \ldots, x_{t-1}, x_{t+1}, \ldots, x_n, y]$. By Cramer's rule, the vector

$$\begin{pmatrix} p_{d_2'} \\ \vdots \\ p_0 \\ q_{d_1'} \\ \vdots \\ q_0 \end{pmatrix} = \frac{1}{\det(\Phi_d)} \cdot \begin{pmatrix} \bar{p}_{d_2'} \\ \vdots \\ \bar{p}_0 \\ \bar{q}_{d_1'} \\ \vdots \\ \bar{q}_0 \end{pmatrix}$$

is the solution of the linear system (3.2), which also shows that d does not depend on the choice of $\mathcal{P} \in \mathrm{Ap}(\Delta_{m-1})$. Therefore

$$\bar{p} := \sum_{i=0}^{d_2'} \bar{p}_i x^i = \det(\Phi_D) \cdot p, \quad \bar{q} := \sum_{j=0}^{d_1'} \bar{q}_j x^j = \det(\Phi_D) \cdot q$$

are polynomials in $\Bbbk[x_1, \ldots, x_n, y]$ and $\bar{d} := f\bar{p} + g\bar{q} = \det(\Phi_D) \cdot d$.

If $\det(\Phi_D) \in \Bbbk[x_1, \ldots, x_{t-1}]$ then $\bar{d} = f\bar{p} + g\bar{q}$ satisfies the specifications of $\mathbf{ggcd_t}(\Delta, f_0, \ldots, f_k)$.

Otherwise, since $\det(\Phi_D) \not\equiv 0 \mod \mathcal{P}$ for all $\mathcal{P} \in \mathrm{Ap}(\Delta_{m-1})$, assuming that the cardinality of $\Bbbk$ is sufficiently large, there exists $\sigma := (\alpha_{t+1}, \ldots \alpha_n, \beta) \in \Bbbk^{n-t+1}$ such that $\det(\Phi_D^\sigma) \notin \mathcal{P}$ for all $\mathcal{P} \in \mathrm{Ap}(\Delta_{m-1})$, where Φ_D^σ denotes the matrix obtained by substituting σ in $(x_{t+1}, \ldots, x_n, y)$. ■

Lemma 3.1.4 *Let $\Delta = \{g_1, \ldots g_m\} \subset \Bbbk[x_1, \ldots x_t]$ be an unmixed set, denote $R_m = \Bbbk[x_1, \ldots x_{t-1}]$, and assume that g_m has positive degree in x_t over R_m. Let $f \in \Bbbk[x_1, \ldots, x_n]$ be any polynomial for some $n \geq t$. Then*

$$\forall \mathcal{P} \in \mathrm{Ap}(\Delta): \quad f \not\equiv 0 \mod (\mathcal{P})$$

if and only if

$$\forall \mathcal{P}' \in \mathrm{Ap}(\Delta_{m-1}): \quad \gcd_{\mathbf{K}_{R_m}(\mathcal{P}')}(g_m, f) = 1,$$

where $\Delta_{m-1} = \{g_1, \ldots g_{m-1}\}$.

Proof: $\Rightarrow$: Suppose that the maximal variable in g_{m-1} is x_s, where $s < t$. Assume indirectly that there exists $\mathcal{P}' \in \mathrm{Ap}(\Delta_{m-1})$ such that

$$d := \gcd_{\mathbf{K}_{R_m}(\mathcal{P}')}(g_m, f)$$

is a polynomial in $\mathbf{K}(\mathcal{P}')[x_{s+1}, \ldots, x_t]$, and has positive degree in x_t. Proposition 3.1.3 implies that there exists $\mathbf{d} \in \Bbbk[x_1, \ldots, x_t]$ such that $\mathrm{lc}(\mathbf{d}) \notin \mathcal{P}'$ and the monic image of $\mathbf{d}$ in $\mathbf{K}_{R_m}(\mathcal{P}')[x_t]$ is d. Then $\mathrm{Rep}(\mathcal{P}' \cup \{\mathbf{d}\})$ is an unmixed ideal of codimension m. Then for any $\mathcal{P} \in \mathrm{Ap}(\mathcal{P}' \cup \{\mathbf{d}\})$, $\mathcal{P}$ is also a minimal prime in the prime decomposition of $\mathrm{Rep}(\Delta)$, since $\mathrm{Rep}(\Delta) \subseteq \mathrm{Rep}(\mathcal{P}' \cup \{\mathbf{d}\})$ and both have codimension m. Also, since f is divisible by d over $\mathbf{K}_{R_m}(\mathcal{P}')$, f is pseudo-divisible by $\mathbf{d}$ modulo $\mathcal{P}'$, therefore $f \equiv 0 \mod (\mathrm{Rep}(\mathcal{P}' \cup \{\mathbf{d}\}))$, and thus $f \equiv 0 \mod (\mathcal{P})$ for all $\mathcal{P} \in \mathrm{Ap}(\mathcal{P}' \cup \{\mathbf{d}\})$, which is a contradiction.

$\Leftarrow$: Suppose indirectly that $\exists \mathcal{P} \in \mathrm{Ap}(\Delta)$ such that $f \equiv 0 \mod (\mathcal{P})$. This implies that the coefficients of f as a multivariate polynomial in $\{x_{t+1}, \ldots, x_n\}$ are in $\mathcal{P}$, i.e. $\mathrm{coeff}^n_{t+1}(f) \subset \mathcal{P}$, using the notation of Proposition 3.1.3. Let $\mathcal{P}' = \mathcal{P} \cap R_m$. Since $\gcd_{\mathbf{K}_{R_m}(\mathcal{P}')}(g_m, f) = 1$, Proposition 3.1.3 implies that there exists

$$\mathbf{d} \in \langle \mathrm{Rep}(\Delta) \cup \mathrm{coeff}^n_{t+1}(f) \rangle \tag{3.4}$$

such that $\mathrm{lc}(\mathbf{d}) \notin \mathcal{P}'$ and the monic image of $\mathbf{d}$ in $\mathbf{K}_{R_m}(\mathcal{P}')[x_t]$ is 1. Therefore $\mathbf{d} \in \Bbbk[x_1, \ldots, x_{t-1}]$, and $\mathrm{lc}(\mathbf{d}) = \mathbf{d} \notin \mathcal{P}'$. But the ideal in the the right hand side of (3.4) is included in $\mathcal{P}$, therefore $\mathbf{d} \in \mathcal{P} \cap R_m = \mathcal{P}'$, a contradiction. ■

Lemma 3.1.5 *Let $\Delta = \{g_1, \ldots, g_m\}$ be an unmixed set in $\Bbbk[x_1, \ldots, x_n]$ and assume that $\mathrm{class}(g_s) = x_{l+s}$ for $l = n - m$ and $1 \leq s \leq m$. Moreover let $f \in \Bbbk[x_1, \ldots, x_n]$ and assume that $f \notin \mathcal{P}$ for all $\mathcal{P} \in \mathrm{Ap}(\Delta)$. Then there exists $\bar{f} \in \Bbbk[x_1, \ldots, x_n]$ such that $\bar{f} \notin \mathcal{P}$ for all $\mathcal{P} \in \mathrm{Ap}(\Delta)$, and*

$$f \cdot \bar{f} \equiv r \mod \langle \Delta \rangle \text{ and } r \in \Bbbk[x_1, \ldots, x_l].$$

Proof: We prove the claim by induction on m. For $m = 0$ we have

$$\Bbbk[x_1, \ldots, x_n] = \Bbbk[x_1, \ldots, x_l],$$

therefore the claim is trivial.

Assume that $m > 0$. Denote $R = \Bbbk[x_1, \ldots, x_{n-1}]$. Since $f \notin \mathcal{P}$ for all $\mathcal{P} \in \mathrm{Ap}(\Delta)$, by Lemma 3.1.4 we have that

$$\forall \mathcal{P}' \in \mathrm{Ap}(\Delta_{m-1}): \quad \gcd_{\mathbf{K}(\mathcal{P}')}(g_m, f) = 1$$

where $\Delta_{m-1} = \{g_1, \ldots, g_{m-1}\}$. By Proposition 3.1.3 there exist a polynomial $d \in R[x_n]$ such that

$$d = p \cdot f + q \cdot g_m$$

for some $p, q \in R[x_n]$, $d \notin \mathcal{P}'$ for all $\mathcal{P}' \in \mathrm{Ap}(\Delta_{m-1})$, and the monic image of d modulo $\mathcal{P}'$ is $\gcd_{\mathbf{K}(\mathcal{P}')}(g_m, f) = 1$. Also, since we can interchange the role of f and p, using again Lemma 3.1.4, we have that $p \notin \mathcal{P}$ for all $\mathcal{P} \in \mathrm{Ap}(\Delta)$. This implies that $d \in R$. Then, by the inductive hypothesis there exists $\bar{d} \in R$ such that $\bar{d} \notin \mathcal{P}'$ for all $\mathcal{P}' \in \mathrm{Ap}(\Delta_{m-1})$ and

$$d \cdot \bar{d} \equiv r \mod (\langle \Delta_{m-1} \rangle) \text{ and } r \in \Bbbk[x_1, \ldots, x_l].$$

In other words, there exists $q_1, \ldots, q_{m-1}$ such that

$$r = d \cdot \bar{d} + \sum_{i=1}^{m-1} q_i \cdot g_i = \bar{d} \cdot p \cdot f + \bar{d} \cdot q \cdot g_m + \sum_{i=1}^{m-1} q_i \cdot g_i$$

hence

$$\bar{f} := \bar{d} \cdot p$$

is a sufficient choice to prove the claim. Observing that $\bar{d} \notin \mathcal{P}'$ for all $\mathcal{P}' \in \mathrm{Ap}(\Delta_{m-1})$ implies that $\bar{d} \notin \mathcal{P}$ for all $\mathcal{P} \in \mathrm{Ap}(\Delta)$ — otherwise $d \in \mathcal{P} \cap R \in \mathrm{Ap}(\Delta_{m-1})$, a contradiction — we also have that $\bar{f} = \bar{d} \cdot p \notin \mathcal{P}$ for all $\mathcal{P} \in \mathrm{Ap}(\Delta)$. ■

Lemma 3.1.6 *Let* $\Delta = \{g_1, \ldots, g_m\}$ *be an unmixed set in* $\Bbbk[x_1, \ldots, x_n]$ *and assume that* $\mathrm{class}(g_s) = x_{l+s}$ *for* $l = n - m$ *and* $1 \leq s \leq m$. *Then there exist* $\Delta' = \{g'_1, \ldots, g'_m\}$ *such that* $\mathrm{Rep}(\Delta') = \mathrm{Rep}(\Delta)$ *and*

$$\mathrm{lc}(g'_s) \in \Bbbk[x_1, \ldots, x_l]$$

for $1 \leq s \leq m$.

Proof: We prove the claim by induction on m. For $m = 0$ and $m = 1$ the claim is trivial.

Assume that $m > 0$. By the inductive hypothesis we can assume that $\mathrm{lc}(g_s) \in k[x_1, \ldots, x_l]$ for $1 \leq s \leq m-1$.

Since $\{g_1, \ldots, g_m\}$ is unmixed, $\mathrm{lc}(g_m) \notin \mathcal{P}$ for all $\mathcal{P} \in \mathrm{Ap}(\Delta_{m-1})$. By Lemma 3.1.5 there exists $\overline{\mathrm{lc}(g_m)} \in \Bbbk[x_1, \ldots, x_{n-1}]$ such that $\overline{\mathrm{lc}(g_m)} \notin \mathcal{P}$ for all $\mathcal{P} \in \mathrm{Ap}(\Delta_{m-1})$ and

$$\mathrm{lc}(g_m) \cdot \overline{\mathrm{lc}(g_m)} \equiv r \mod (\langle \Delta \rangle_{m-1}) \text{ and } r \in \Bbbk[x_1, \ldots, x_l],$$

i.e. there exist $q_1, \ldots q_{m-1}$ such that

$$\mathrm{lc}(g_m) \cdot \overline{\mathrm{lc}(g_m)} - r = \sum_{i=1}^{m-1} q_i g_i.$$

Define

$$g'_m := \overline{\mathrm{lc}(g_m)} g_m - x_n^{d_m} \sum_{i=1}^{m-1} q_i g_i$$

where $d_m := \deg_{x_n}(g_m) > 0$. Clearly $\mathrm{lc}(g'_m) = r \in \Bbbk[x_1, \ldots, x_l]$. Moreover,

$$\langle g_m \rangle_{\mathbf{K}(\mathcal{P})} = \langle g'_m \rangle_{\mathbf{K}(\mathcal{P})}$$

for all $\mathcal{P} \in \mathrm{Ap}(\Delta_{m-1})$, therefore, by Lemma 3.1.1 we have that

$$\mathrm{Rep}(\Delta_{m-1} \cup \{g_m\}) = \mathrm{Rep}(\Delta_{m-1} \cup \{g'_m\})$$

which proves the claim. ■

3.2 The computational model

In this section we describe the computational model and collect some elementary facts about the computational ingredients of our methods. In the description and in the notation we follow the approach of [IRS94].

As the model of parallel computation we use arithmetic circuits, described in [vzG84]. The algorithms presented below are defined for some class of fields. For a field $\Bbbk$ and for a fixed size of the problem instances there is a circuit – a directed acyclic graph – which performs the computations. Each node performs a basic operation, which can be a field operation in $\Bbbk$ or a Boolean operation. Each of these operations is assumed to have unit cost. We measure the complexity of the computation by the depth and the size of the circuit.

The *height* of a polynomial $0 \not\equiv f \in \Bbbk[X_1, \ldots, X_l]$ is the maximum of the degrees of f in the variables $X_1, \ldots, X_l$. Polynomials are considered in the *dense representation*, i.e. if f is of height d then f is viewed as a vector of d^l elements of the ground field, corresponding to the coefficients of the monomials of height at most

d. Therefore the size of a polynomial $f \in \mathbb{k}[X_1, \ldots, X_l]$ of height d has size $O(d^l)$ in our arithmetic computational model over $\mathbb{k}$.

A rational function $f \in \mathbb{k}(X_1, \ldots, X_l)$ is represented as a quotient of two (not necessarily relative prime) polynomials. The height of f is the maximum height of the numerator and denominator of its reduced form. The size of a rational function of height d is at most $O(d^l)$.

The height of a D-dimensional vector over the field $\mathbb{k}(X_1, \ldots, X_l)$ is the maximum height of its components. The size of a D-dimensional vector of height d is at most $O(Dd^l)$.

The product and sum of k elements of $\mathbb{k}(X_1, \ldots, X_l)$ of heights $d_1, \ldots, d_k \leq d$ has height at most $d_1 + \cdots + d_k$, and the arithmetic circuit computing them has depth $O(l \log(kd))$ and size $O((dk)^{2l})$. An important case is the addition of *integral* operands, i.e. if the operands are all in $\mathbb{k}[X_1, \ldots, X_l]$. In this case the height of a sum is bounded by the largest of the height of the operands. Thus integrality simplifies the computations.

Computing a linear combination of k vectors over $\mathbb{k}(X_1, \ldots, X_l)$ has depth $O(l \log(kd))$ and size $O((2dk)^{2l} D)$ where d is a bound on the height of the operands and D is the dimension of the vector space.

We use the term *algebra* for a finite dimensional associative algebra over some field. Given an a priori basis $b_1, \ldots b_D$ of an algebra $\mathcal{B}$ over a field $\mathbb{k}(X_1, \ldots, X_l)$, we represent the elements of $\mathcal{B}$ by their coordinates with respect to the a priori basis as D dimensional vectors over the field $\mathbb{k}(X_1, \ldots, X_l)$. The height of an element b of an algebra $\mathcal{B}$ is the maximum height of the coordinates of b with respect to the

a priori basis.

3.3 Arithmetics modulo unmixed triangular sets

Let $\Delta = \{\mathrm{g}_1, \ldots \mathrm{g}_m\} \subset \Bbbk[x_1, \ldots, x_n]$ be an unmixed set such that $n = m + l$ and for all $1 \leq s \leq m$

1. $\mathrm{class}(\mathrm{g}_s) = x_{l+s}$ and $d_s := \deg_{x_{l+s}}(\mathrm{g}_s)$;

2. $\mathrm{lc}(\mathrm{g}_s) \in \Bbbk[x_1, \ldots, x_l]$;

3. g_s is reduced modulo $\Delta_{s-1} := \{\mathrm{g}_1, \ldots, \mathrm{g}_{s-1}\}$, i.e.

$$\forall t < s \quad \deg_{x_{l+t}}(\mathrm{g}_s) < \deg_{x_{l+t}}(\mathrm{g}_t).$$

In the following paragraphs we describe how to conduct arithmetic operations in the quotient ring

$$\mathcal{A}(\Delta) := \Bbbk(x_1, \ldots, x_l)[x_{l+1}, \ldots, x_n]/\langle\Delta\rangle_{\Bbbk(x_1,\ldots,x_l)}.$$

Since the leading coefficients $\mathrm{lc}(\mathrm{g}_s)$ are in $\Bbbk[x_1, \ldots, x_l]$, every polynomial $\mathrm{p} \in \Bbbk[x_1, \ldots, x_n]$ has a unique reduced form $\mathrm{p}_0 \in \Bbbk(x_1, \ldots, x_l)[x_{l+1}, \ldots, x_n]$ such that

$$\mathrm{p} = \sum_{s=1}^{m} \mathrm{q}_s \mathrm{g}_{s,i,\vec{v}} + \mathrm{p}_0, \quad \deg_{x_{l+s}}(\mathrm{p}_0) < \deg_{x_{l+s}}(\mathrm{g}_{s,i,\vec{v}}), \quad 1 \leq s \leq m \tag{3.5}$$

where $\mathrm{q}_s \in \Bbbk(x_1, \ldots, x_l)[x_{l+1}, \ldots, x_n]$. This implies that $\mathcal{A}(\Delta)$ is a finite dimensional vector space over $\Bbbk(x_1, \ldots, x_l)$ with basis

$$\mathbf{B}(\Delta) := \left\{ x_{l+1}^{\alpha_1} \cdots x_n^{\alpha_m} \mid 0 \leq \alpha_s < \deg_{x_{l+s}}(\mathrm{g}_s),\ 1 \leq s \leq m \right\}$$

of dimension $D := \prod_{s=1}^{m} d_s$. We will identify $\mathrm{p}_0 \in \Bbbk(x_1, \ldots, x_l)[x_{l+1}, \ldots, x_n]$ in reduced form with the corresponding vector, i.e. we consider p_0 as an element of the vector space $\Bbbk(x_1 \ldots, x_l)^D$. Clearly, if $\mathrm{p}, \mathrm{p}' \in \Bbbk(x_1, \ldots, x_l)[x_{l+1}, \ldots, x_n]$ then the congruence class corresponding to $\mathrm{p} + \mathrm{p}'$ is represented by the (coordinate-wise) sum of the vectors p_0 and p'_0.

Next we relate the algebra $\mathcal{A}(\Delta)$ to the quotient ring

$$\mathcal{R}(\Delta) := \Bbbk[x_1, \ldots, x_n]/\mathrm{Rep}(\Delta).$$

The reduced form of a polynomial $\mathrm{p} \in \Bbbk[x_1, \ldots, x_n]$ modulo $\mathrm{Rep}(\Delta)$ is the pseudo-remainder of p modulo Δ defined in section 2.3, i.e. $\bar{\mathrm{p}}_0 \in \Bbbk[x_1, \ldots, x_n]$ if it satisfies

$$\mathrm{lc}(\mathrm{g}_m)^{\alpha_m} \cdots \mathrm{lc}(\mathrm{g}_1)^{\alpha_1} \cdot \mathrm{p} = \sum_{s=1}^{m} \mathrm{q}_s \mathrm{g}_s + \bar{\mathrm{p}}_0 \tag{3.6}$$

and $\deg_{x_{l+s}}(\bar{\mathrm{p}}_0) < \deg_{x_{l+s}}(\mathrm{g}_s)$ for $1 \leq s \leq m$. By the uniqueness of the expression in (3.5) we have

$$\mathrm{p}_0 = \frac{1}{\mathrm{lc}(\mathrm{g}_m)^{\alpha_m} \cdots \mathrm{lc}(\mathrm{g}_1)^{\alpha_1}} \cdot \bar{\mathrm{p}}_0. \tag{3.7}$$

Therefore, if we represent each element $\mathrm{p} \in \Bbbk[x_1, \ldots, x_n]$ by the (integral) coordinates of $\bar{\mathrm{p}}_0 = \mathrm{prem}(\mathrm{p}, \Delta) \in \Bbbk[x_1, \ldots, x_n]$ and the vector of exponents $\vec{\alpha} := (\alpha_1, \ldots, \alpha_m)$ in the expression (3.6), then we can recover p_0, the unique representation of p in $\mathcal{A}(\Delta)$, using (3.7). We will use the following notation:

$$\mathrm{Rep}(\mathrm{p}) := (\bar{\mathrm{p}}_0, \vec{\alpha}) \in \Bbbk[x_1, \ldots, x_l]^D \times \mathbb{N}^m \tag{3.8}$$

$$\mathrm{lc}(\Delta)^{\vec{\alpha}} := \mathrm{lc}(\mathrm{g}_m)^{\alpha_m} \cdots \mathrm{lc}(\mathrm{g}_1)^{\alpha_1} \in k[x_1, \ldots, x_l], \tag{3.9}$$

$$\max\{\vec{\alpha}, \vec{\alpha}'\} := (\max\{\alpha_1, \alpha'_1\}, \ldots, \max\{\alpha_m, \alpha'_m\}) \in \mathbb{N}^m. \tag{3.10}$$

We can define the arithmetic operations in $\mathcal{R}(\Delta)$ using the above notation as follows. Let $\mathbf{p}$ and $\mathbf{p}'$ be polynomials in $\Bbbk[x_1, \ldots, x_n]$ and let

$$\mathrm{Rep}(\mathbf{p}) := (\mathbf{p}_0, \vec{\alpha}), \quad \mathrm{Rep}(\mathbf{p}') := (\mathbf{p}'_0, \vec{\alpha}') \in \Bbbk[x_1, \ldots, x_l]^D \times \mathbb{N}^m$$

be the representation of the congruence class of $\mathbf{p}$ and $\mathbf{p}'$ in $\mathcal{R}(\Delta)$ respectively. Then

$$\mathrm{Rep}(\mathbf{p} + \mathbf{p}') = (\mathrm{lc}(\Delta)^{\max\{\vec{\alpha}, \vec{\alpha}'\} - \vec{\alpha}} \cdot \mathbf{p}_0 + \mathrm{lc}(\Delta)^{\max\{\vec{\alpha}, \vec{\alpha}'\} - \vec{\alpha}} \cdot \mathbf{p}'_0,\ \max\{\vec{\alpha}, \vec{\alpha}'\}).$$

In the next section we show how to compute a multiplication table for $\mathcal{A}(\Delta)$, i.e. for each pairs $\mathbf{a}, \mathbf{a}' \in \mathbf{B}(\Delta)$ the coordinates of the product $\mathbf{a} \cdot \mathbf{a}'$ with respect to the basis $\mathbf{B}(\Delta)$. We call these coordinates the *structure constants* of $\mathcal{A}(\Delta)$. We will see in the next section that the denominators of the structure constants are all in the form $\mathrm{lc}(\Delta)^{\vec{\alpha}}$, therefore, using the multiplication table of $\mathcal{A}(\Delta)$, we can conduct multiplication also in $\mathcal{R}(\Delta)$. The size of the multiplication table is D^3 times the size of the structure constants. Since the algebra $\mathcal{A}(\Delta)$ is given by the minimal polynomials of the multiplicative generators, the size of the structure constants depends on the size of the minimal polynomials. Let Υ be an upper bound on the height of the structure constants, and assume also that Υ is an upper bound on the height of the lcm of the denominators of the structure constants. In the next section we give an upper bound Υ in terms of the size of the polynomials in Δ.

Proposition 3.3.1 *Assume that the $\Bbbk(x_1, \ldots, x_n)$-algebra $\mathcal{A}(\Delta)$ has dimension D and is given by structure constants of heights at most Υ. Let $\mathbf{a}_1, \ldots, \mathbf{a}_k$ be elements of $\mathcal{A}(\Delta)$ with heights at most d. Moreover, assume that the denominators of the*

coordinates of $\mathbf{a}_1, \ldots, \mathbf{a}_k$ *divide*

$$\prod_{s=1}^{m} \mathrm{lc}(\mathbf{g}_s)^{\beta_s}, \quad \textit{and} \quad \sum_{s=1}^{m} \beta_s \cdot \mathrm{height}(\mathrm{lc}(\mathbf{g}_s)) \leq d'. \tag{3.11}$$

Also, assume that the denominators of the structure constants of $\mathcal{A}(\Delta)$ *divide*

$$\prod_{s=1}^{m} \mathrm{lc}(\mathbf{g}_s)^{\alpha_s}, \quad \textit{and} \quad \sum_{s=1}^{m} \alpha_s \cdot \mathrm{height}(\mathrm{lc}(\mathbf{g}_s)) \leq \Upsilon. \tag{3.12}$$

Then we have

$$\mathrm{height}(\mathbf{a}_1 \cdots \mathbf{a}_k) \leq k \cdot d + k \log(k)(d' + \Upsilon).$$

The denominators of the coordinates of the product $\mathbf{a}_1 \cdots \mathbf{a}_k$ *divide*

$$\prod_{s=1}^{m} \mathrm{lc}(\mathbf{g}_s)^{k(\beta_s+\alpha_s)},$$

and $k(d' + \Upsilon)$ *gives an upper bound on the height of the* lcm *of the denominators of the coordinates of the product.*

The arithmetic circuit over $\mathbb{k}$ *computing the product of* k *elements of* $\mathcal{A}(\Delta)$ *has depth at most*

$$O(l \log(D) \log^2(k) \log(d + d' + \Upsilon))$$

and size

$$O\left(D^3 k \left[k \log(k)(d + d' + \Upsilon)\right]^{2l}\right),$$

where $l = n - m$.

Proof: We prove the proposition using induction on k. Let $\Delta = \{\mathbf{g}_1, \ldots, \mathbf{g}_m\}$ and $\mathbf{B}(\Delta) = \{\mathbf{e}_1, \ldots, \mathbf{e}_D\}$ be the a priori basis for $\mathcal{A}(\Delta)$, and

$$\mathbf{a}_1 = \sum_{i=1}^{D} a_{1,i}\mathbf{e}_i, \ \ldots, \ \mathbf{a}_k = \sum_{i=1}^{D} a_{k,i}\mathbf{e}_i \in \mathcal{A}(\Delta)$$

be the operands, where $a_{i,j} \in \mathbb{k}(x_1, \ldots, x_l)$ of height at most d. Also, the denominators of $\{a_{i,j} \mid 1 \leq i \leq D,\ 1 \leq j \leq k\}$ divide $\prod_{s=1}^{m} \mathrm{lc}(\mathrm{g}_s)^{\beta^*}$ as in (3.11).

We use the following notation for the structure constants:

$$\mathrm{e}_i \cdot \mathrm{e}_j = \sum_{l=1}^{D} c_{i,j,l}\mathrm{e}_l;\ \ c_{i,j,l} \in k(x_1, \ldots, x_l),$$

for $1 \leq i, j \leq D$. Assume also that the denominators of the structure constants $\{c_{i,j,l}\}$ divide $\prod_{s=1}^{m} \mathrm{lc}(\mathrm{g}_s)^{\alpha_s}$ as in (3.12).

If $k = 2$ then

$$\begin{aligned} \mathrm{a}_1 \cdot \mathrm{a}_2 &= (\sum_{i=1}^{D} a_{1,i}\mathrm{e}_i)(\sum_{j=1}^{D} a_{2,j}\mathrm{e}_j) = \sum_{i,j} a_{1,i}a_{2,j}(\mathrm{e}_i \cdot \mathrm{e}_j) \\ &= \sum_{l=1}^{D} \left(\sum_{i,j} a_{1,i}a_{2,j}c_{i,j,l} \right) \mathrm{e}_l. \end{aligned}$$

Since $2d' + \Upsilon$ is an upper bound for the height of the lcm of the denominators of the products $\{a_{1,i}a_{2,j}c_{i,j,l} \mid 1 \leq i, j, l \leq D\}$, we get that

$$\mathrm{height}(\mathrm{a}_1 \cdot \mathrm{a}_2) \leq \mathrm{height}(\mathrm{a}_1) + \mathrm{height}(\mathrm{a}_2) + \Upsilon + (2d' + \Upsilon) \leq 2(d + d' + \Upsilon), \quad (3.13)$$

and the denominators of the coordinates of $\mathrm{a}_1 \cdot \mathrm{a}_2$ divide

$$\prod_{s=1}^{m} \mathrm{lc}(\mathrm{g}_s)^{2\beta_s + \alpha_s}.$$

Furthermore, $\mathrm{a}_1 \cdot \mathrm{a}_2$ can be computed with an arithmetic circuit of depth at most

$$\mathrm{Depth}(2) := O(\log(D^3) l \log(d + d' + \Upsilon))$$

and size at most

$$\mathrm{Size}(2) := D^3(2(d + d' + \Upsilon))^{2l}.$$

For $k = 2^r$ assume that $\mathbf{a}'_1 := \prod_{i=1}^{2^{r-1}} \mathbf{a}_i$ and $\mathbf{a}'_2 := \prod_{j=2^{r-1}+1}^{2^r} \mathbf{a}_j$ are already computed. Assume also that the lcm of the denominators of the coordinates of both $\mathbf{a}'_1$ and $\mathbf{a}'_2$ divides

$$\prod_{s=1}^{m} \mathrm{lc}(\mathbf{g}_s)^{2^{r-1}\beta_s+(2^{r-1}-1)\alpha_s},$$

which implies that $2^{r-1}d' + (2^{r-1}-1)\Upsilon$ is an upper bound for the height of the lcm. Then, by (3.13), the denominators of the coordinates of $\mathbf{a}'_1 \cdot \mathbf{a}'_2$ divide

$$\prod_{s=1}^{m} \mathrm{lc}(\mathbf{g}_s)^{2^r\beta_s+(2^r-1)\alpha_s} = \prod_{s=1}^{m} \mathrm{lc}(\mathbf{g}_s)^{k\beta_s+(k-1)\alpha_s},$$

therefore the height of the lcm of the denominators of the coordinates of $\mathbf{a}'_1 \cdot \mathbf{a}'_2$ is at most $kd' + (k-1)\Upsilon$. Formula (3.13) also implies that

$$\begin{aligned}
\mathrm{height}(k) &\leq kd' + (k-1)\Upsilon + 2 \cdot \mathrm{height}(k/2) + \Upsilon \\
&\leq k(d'+\Upsilon) + 2 \cdot \frac{k}{2}(d'+\Upsilon) + \cdots + 2^{r-1}\frac{k}{2^{r-1}}(d'+\Upsilon) + k \cdot d \\
&\leq k \cdot d + k\log(k)(d'+\Upsilon).
\end{aligned}$$

The depth of the arithmetic circuit computing $a'_1 \cdot a'_2$ is at most

$$c_1 \log(D^3) l(\log(k) + \log(d+\Upsilon)) + \mathrm{Depth}(k/2) \leq O(l\log(D)\log^2(k)\log(d+\Upsilon)),$$

and the size of the arithmetic circuit is at most

$$c_2 D^3 (k\log(k)(d+d'+\Upsilon))^{2l} + 2 \cdot \mathrm{Size}(k/2) \leq O(D^3 \cdot k(k\log(k)(d+d'+\Upsilon))^{2l})$$

where c_1 (c_2) denotes the constant in the depth (size) of the arithmetic circuit computing the product of 2 elements of $\mathbb{k}(x_1, \ldots, x_l)$. ■

Corollary 3.3.2 *Let* $\Delta = \{\mathbf{g}_1, \ldots \mathbf{g}_m\}$ *be an unmixed set such that* $n = m + l$ *and for all* $1 \leq s \leq m$

1. $\mathrm{class}(\mathbf{g}_s) = x_{l+s}$ *and* $d_s := \deg_{x_{l+s}}(\mathbf{g}_s)$;

2. $\mathrm{lc}(\mathbf{g}_s) \in \Bbbk[x_1, \ldots, x_l]$;

3. $\mathbf{g}_s$ *is reduced modulo* $\Delta_{s-1} := \{\mathbf{g}_1, \ldots, \mathbf{g}_{s-1}\}$.

Assume that the structure constants of $\mathcal{A}(\Delta)$ *are in the form*

$$\frac{c_{i,j,k}}{\mathrm{lc}(\Delta)^{\vec{\alpha}}} \quad 1 \leq i, j, k \leq D$$

where $c_{i,j,k} \in \Bbbk[x_1, \ldots, x_l]$, $\alpha \in \mathbb{N}^m$ *and* $\mathrm{lc}(\Delta)^{\vec{\alpha}}$ *denotes* $\prod_{s=1}^{m} \mathrm{lc}(\mathbf{g}_s)^{\alpha_s}$. *Let* $\mathbf{p}, \mathbf{p}' \in \Bbbk[x_1, \ldots, x_n]$ *such that*

$$\mathrm{Rep}(\mathbf{p}) = (\mathbf{p}_0, \vec{\beta}), \quad \mathrm{Rep}(\mathbf{p}') = (\mathbf{p}'_0, \vec{\beta}') \quad \in \mathcal{R}(\Delta)$$

where $\mathbf{p}_0 = (p_i)_{i=1}^{D}$, $\mathbf{p}'_0 = (p'_i)_{i=1}^{D}$ *are in* $\Bbbk[x_1, \ldots, x_l]^D$, $\vec{\beta}, \vec{\beta}' \in \mathbb{N}^m$ *and* $\mathrm{Rep}(\cdot)$ *is defined in (3.8). Then*

$$\begin{aligned} \mathrm{Rep}(\mathbf{p} + \mathbf{p}') &= \left(\mathrm{lc}(\Delta)^{\max\{\vec{\beta},\vec{\beta}'\}-\vec{\beta}'} \cdot \mathbf{p}_0 + \mathrm{lc}(\Delta)^{\max\{\vec{\beta},\vec{\beta}'\}-\vec{\beta}} \cdot \mathbf{p}'_0,\ \max\{\vec{\beta}, \vec{\beta}'\}\right) \\ \mathrm{Rep}(\mathbf{p} \cdot \mathbf{p}') &= \left(\left(\sum_{i,j=1}^{D} p_i p'_j c_{i,j,k}\right)_{k=1}^{D},\ \vec{\beta} + \vec{\beta}' + \vec{\alpha}\right) \end{aligned}$$

defines the ring operations in $\mathcal{R}(\Delta)$. *Moreover, the arithmetic circuit over* $\Bbbk$ *computing* $\mathrm{Rep}(\mathbf{p} + \mathbf{p}')$ *or* $\mathrm{Rep}(\mathbf{p} \cdot \mathbf{p}')$ *has depth at most*

$$O\left(\log(D^3) l \log(d + d' + \Upsilon)\right)$$

and size at most

$$O\left(D^3(2(d+d'+\Upsilon))^{2l}\right)$$

where

$$\text{height}(\mathbf{p}_0),\ \text{height}(\mathbf{p}'_0) < d,$$

$$\text{height}(\text{lc}(\Delta)^{\vec{\beta}}),\ \text{height}(\text{lc}(\Delta)^{\vec{\beta}'}) < d',$$

$$\text{height}(c_{i,j,k}),\ \text{height}(\text{lc}(\Delta)^{\vec{\alpha}}) < \Upsilon, \qquad 1 \leq i,j,k \leq D. \quad \blacksquare$$

Remark: As we noted above, the algebra $\mathcal{A}(\Delta)$ is given by the minimal polynomials of its multiplicative generators, i.e. by the polynomials in Δ. In the rest of the thesis we assume that the multiplication table of $\mathcal{A}(\Delta)$ with respect to the basis $\mathbf{B}(\Delta)$ is also part of the input, or it is assumed to be precomputed. Without this assumption we could only prove a parallel complexity bound $\Omega(\log(D)^l)$ for conducting arithmetic operations in $\mathcal{A}(\Delta)$.

We also note that there are other alternatives for precomputation besides computing the whole multiplication table in order to conduct ring arithmetics in $\mathcal{A}(\Delta)$ with the same parallel complexity bounds as in Proposition 3.3.1. For example, using either of the following precomputed data, we can efficiently conduct ring arithmetics in $\mathcal{A}(\Delta)$:

1. The set of polynomials

$$\mathcal{S}(\Delta) := \{x_{l+s}^{\alpha_s} \mod (\Delta_s) \mid d_s \leq \alpha_s \leq 2d_s - 1,\ 1 \leq s \leq m\} \qquad (3.14)$$

where $\Delta_s = \{\mathbf{g}_1, \ldots, \mathbf{g}_s\}$. Here $\mathcal{S}(\Delta)$ contains only $\sum_{s=1}^{m} d_s$ reduced polynomials.

2. A primitive element of $\mathcal{A}(\Delta)$ i.e. an element $\mathbf{u} \in \mathcal{A}(\Delta)$ with its minimal polynomial $P(\mathbf{u}) \in \Bbbk(x_1, \ldots, x_l)[\mathbf{u}]$ of degree $\prod_{s=1}^{m} d_s$ and the polynomials $u_s(\mathbf{u})$ of degree $< \deg_{\mathbf{u}}(P)$ for $0 \leq s \leq m$ such that

$$\begin{aligned} \mathcal{A}(\Delta) &\rightarrow \Bbbk(x_1, \ldots, x_l)[\mathbf{u}]/P(\mathbf{u}) \\ x_{l+s} &\mapsto u_s(\mathbf{u}) \quad 1 \leq s \leq m \end{aligned}$$

is an isomorphism.

3.3.1 Pseudo-division

The reduced form of a polynomial modulo an unmixed set is obtained by successive application of pseudo-division. For the pseudo-division we use similar method as in [vzG84], solving linear equation systems. More precisely, let $f \in \Bbbk[x_1, \ldots, x_l]$ and $g \in \Bbbk[x_1, \ldots, x_n]$ and assume that $\text{class}(g_m) = x_n$ and $l \geq n$. Write

$$f = \sum_{i=0}^{d'} f_i x_n^i \quad \text{and} \quad g = \sum_{i=0}^{d} g_i x_n^i$$

as univariate polynomials in x_n with coefficients $f_i \in \Bbbk[x_1, \ldots, x_{n-1}, x_{n+1}, \ldots x_l]$ and $g_i \in \Bbbk[x_1, \ldots, x_{n-1}]$. Consider the equation

$$f = gq + r \quad \deg_{x_n}(r) < \deg_{x_n}(g)$$

over the field $\Bbbk(x_1, \ldots, x_{n-1}, x_{n+1}, \ldots x_l)$, which is linear in the coefficients of q. Therefore the coefficients of q are the solutions of the $(k+1) \times (k+1)$ linear system

$$\begin{pmatrix} g_d & 0 & 0 & \ldots & \ldots & 0 \\ g_{d-1} & g_d & 0 & \ldots & \ldots & 0 \\ \vdots & \vdots & \ddots & & & \vdots \\ g_0 & g_1 & \ldots & g_d & 0 & 0 \\ 0 & \ddots & & & \ddots & 0 \\ 0 & 0 & g_0 & \ldots & & g_d \end{pmatrix} \cdot \begin{pmatrix} q_k \\ q_{k-1} \\ \vdots \\ \\ \vdots \\ q_0 \end{pmatrix} = \begin{pmatrix} f_{d'} \\ f_{d'-1} \\ \vdots \\ \\ \vdots \\ f_d \end{pmatrix}, \tag{3.15}$$

where $k = d' - d$. Denote the lower triangular matrix on the left hand side by $L(g)$ and note that $\det(L(g)) = \mathrm{lc}(g)^{k+1}$. Using Cramer's rule, we can compute

$$L'(g) := \det(L(g)) \cdot L^{-1}(g),$$

which is a matrix with elements from $\Bbbk[x_1, \ldots, x_{n-1}]$. Multiplying the right hand side of (3.15) with $L'(g)$, we can find the polynomial $q' \in \Bbbk[x_1, \ldots, x_l]$ satisfying

$$\mathrm{lc}(g)^{k+1} f = gq' + r' \quad \deg_{x_n}(r') < \deg_{x_n}(g).$$

The pseudo remainder r' is simply the difference $\mathrm{lc}(g)^{k+1} f - q'g$.

We will use the following simpler expression of the pseudo-remainder in the computation of the structure constants of an algebra in the next section. Let f and g be as above and assume that $\deg_{x_n}(f) < 2\deg_{x_n}(g)$. We can write

$$f = \sum_{i=0}^{2d-1} f_i x_n^i, \quad g_m = \sum_{i=0}^{d} g_i x_n^i.$$

Then the pseudo remainder of f by g can be written as

$$\mathrm{lc}(g)^d \begin{pmatrix} f_{d-1} \\ f_{d-2} \\ \vdots \\ f_0 \end{pmatrix} - \begin{pmatrix} g_0 & g_1 & \cdots & g_{d-1} \\ 0 & g_0 & \cdots & g_{d-2} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & g_0 \end{pmatrix} \begin{pmatrix} g_d & 0 & \cdots & 0 \\ g_{d-1} & g_d & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ g_0 & g_1 & \cdots & g_d \end{pmatrix}^* \begin{pmatrix} f_{2d-1} \\ f_{2d-2} \\ \vdots \\ f_d \end{pmatrix} \quad (3.16)$$

where M^* denotes $\det(M) \cdot M^{-1}$ for a square matrix M. Note that if M is a $d \times d$ triangular matrix, then M^* can be computed using only ring operations on the entries of M, and the entries of M^* are degree d polynomials of the entries of M.

Lemma 3.3.3 *Let f, g as above. Suppose that we computed*

$$r' \in \Bbbk[x_1, \ldots, x_l]$$

such that there exists $q' \in \Bbbk[x_1, \ldots, x_l]$ satisfying

$$\mathrm{lc}(g)^{k+1} f = gq' + r' \quad \deg_{x_n}(r) < \deg_{x_n}(g),$$

where $k = \deg_{x_n}(f) - \deg_{x_n}(g)$. Then for $j < n$

$$\deg_{x_j}(q') \leq (k+1)\deg_{x_j}(g) + \deg_{x_j}(f), \quad (3.17)$$

$$\deg_{x_j}(r') \leq (k+2)\deg_{x_j}(g) + \deg_{x_j}(f). \quad (3.18)$$

For $j > n$

$$\deg_{x_j}(q'),\ \deg_{x_j}(r') \leq \deg_{x_j}(f). \quad (3.19)$$

Proof: Inequality (3.19) follows since for $j > n$ the variable x_j only appears on the right hand side of the linear system (3.15).

To prove (3.17), we observe that the entries of $L'(g) = \det(L(g)) \cdot L^{-1}(g)$ are determinants of the matrix $L(g)$ with one of the columns interchanged with a unit vector. Therefore, the degree in x_j of the entries of $L'(g)$ is at most $(k+1)\deg_{x_j}(g)$. To obtain q', we multiply the right hand side of the system (3.15) with $L'(g)$, therefore

$$\deg_{x_j}(q') \leq \deg_{x_j}(g) \cdot (k+1) + \deg_{x_j}(f).$$

The claim for $\deg_{x_j}(r')$ follows from $r' = \mathrm{lc}(g)^{k+1} f - q'g$. ■

3.3.2 Computation of the structure constants for $\mathcal{A}(\Delta)$

Proposition 3.3.4 *Let* $\Delta = \{\mathrm{g}_1, \ldots, \mathrm{g}_m\}$ *be an unmixed set such that for all* $1 \leq s \leq m$

1. $\mathrm{class}(\mathrm{g}_s) = x_{l+s}$ *and* $d_s := \deg_{x_{l+s}}(\mathrm{g}_s)$;
2. $\mathrm{lc}(\mathrm{g}_s) \in \Bbbk[x_1, \ldots, x_l]$;
3. g_s *is reduced modulo* $\Delta_{s-1} := \{\mathrm{g}_1, \ldots, \mathrm{g}_{s-1}\}$, *i.e.*

$$\forall\, t < s \quad \deg_{x_{l+t}}(\mathrm{g}_s) < \deg_{x_{l+t}}(\mathrm{g}_t).$$

Then the height Υ *of the structure constants of* $\mathcal{A}(\Delta)$ *is bounded by*

$$\Upsilon \leq \sum_{s=1}^{m} \mathrm{height}(\mathrm{g}_s) \cdot \prod_{t=s}^{m} (d_t + 4)\log(d_t + 4). \tag{3.20}$$

Moreover, the lcm *of the denominators of the structure constants divides*

$$\prod_{s=1}^{m} \mathrm{lc}(\mathrm{g}_s)^{\alpha_s}, \tag{3.21}$$

where

$$\alpha_s \leq (d_m + 4) \cdots (d_s + 4)$$

for all $1 \leq s \leq m$.

Proof:

Denote $\Delta_s := \{g_1, \ldots, g_s\}$ for $1 \leq s \leq m$.

For $m = 1$ the multiplication table consist of the reduced polynomials

$$\mathcal{M}_1 = \{\text{prem}(x_{l+1}^e, g_1) \mid 0 \leq e \leq 2d_1 - 1\} \subset k[x_1, \ldots x_{l+1}].$$

The structure constants of $\mathcal{A}(\Delta_1)$ are the coefficients of $\text{prem}(x_{l+1}^e, g_1)$ in the basis $1, x_{l+1}, \ldots, x_{l+1}^{d_1-1}$, divided by an exponent of the leading coefficient $\text{lc}(g_1)$. Using lemma 3.3.3 for $k \leq d_1$, we get that the height Υ_1 of the structure constants of $\mathcal{A}(\Delta_1)$ satisfies

$$\Upsilon_1 \leq (d_1 + 3) \cdot \text{height}(g_1).$$

Also, the denominators of the structure constants is a divisor of $\text{lc}(g_1)^{d_1+1}$, therefore $\alpha_1 \leq d_1 + 4$, where α_1 is the exponent of $\text{lc}(g_1)$ in (3.21).

Let $m > 1$ and assume inductively that we have computed the multiplication table $\mathcal{M}_{m-1}$, and we have proved that the structure constants for the algebra $\mathcal{A}(\Delta_{m-1})$ have heights at most

$$\Upsilon_{m-1} \leq \sum_{s=1}^{m-1} \text{height}(g_s) \cdot \prod_{t=s}^{m-1} (d_t + 4) \log(d_t + 4).$$

Also, assume that the denominators of the structure constants of $\mathcal{A}(\Delta_{m-1})$ divide

$$\prod_{s=1}^{m-1} \text{lc}(g_s)^{\alpha'_s}, \quad \text{where} \quad \alpha'_s \leq \prod_{t=s}^{m-1} (d_t + 4). \tag{3.22}$$

Consider a monomial $\mathbf{m} := x_{l+1}^{e_1} \cdots x_{l+m}^{e_m}$ for some $0 \leq e_s \leq 2d_s - 1$ if $s \leq m$. If $e_m < d_m$ then

$$\mathbf{m} \mod \mathrm{Rep}(\Delta_m) = (\mathbf{m}_{m-1} \mod \mathrm{Rep}(\Delta_{m-1})) \cdot x_{l+m}^{e_m}$$

where $\mathbf{m}_{m-1} = x_{l+1}^{e_1} \cdots x_{l+m-1}^{e_{m-1}}$, therefore the corresponding structure constants are computed in $\mathcal{M}_{m-1}$. Assume that $e_m \geq d_m$. Using expression (3.16), we get that the pseudo-remainder of $\mathbf{m}$ by $\mathbf{g}_m$ is given by

$$-\begin{pmatrix} g_0^{(s)} & g_1^{(m)} & \cdots & g_{d_m-1}^{(m)} \\ 0 & g_0^{(m)} & \cdots & g_{d_m-2}^{(m)} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & g_0^{(m)} \end{pmatrix} \cdot \begin{pmatrix} g_{d_m}^{(m)} & 0 & \cdots & 0 \\ g_{d_m-1}^{(m)} & g_{d_m}^{(m)} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ g_0^{(m)} & g_1^{(m)} & \cdots & g_{d_m}^{(m)} \end{pmatrix}^* \cdot \begin{pmatrix} 0 \\ \mathbf{m}_{m-1} \\ \vdots \\ 0 \end{pmatrix}, \quad (3.23)$$

where $\mathbf{g}_m = \sum_{j=0}^{d_m} g_j^{(m)} x_{l+m}^j$, and $g_j^{(m)} \in \Bbbk[x_1, \ldots, x_{n-1}]$. Using the fact that the polynomial $\mathbf{g}_m$ is reduced modulo Δ_{m-1} with integral coefficients and that the exponents of $\mathbf{m}_{m-1}$ satisfy $e_s < 2d_s$ $(s \leq m-1)$, we get that the entries of the product of the matrices in (3.23) are combinations of products of at most $(d_m + 4)$ reduced integral elements of $\mathcal{A}(\Delta_{m-1})$. Using Proposition 3.3.1 and Lemma 3.3.3, we have that the height of the entries of the products of the matrices in (3.23) are at most

$$\begin{aligned} \Upsilon_m &\leq (d_m + 4)\log(d_m + 4)(\mathrm{height}(\mathbf{g}_m) + \Upsilon_{m-1}) \\ &\leq (d_m + 4)\log(d_m + 4) \\ &\quad \cdot \left(\mathrm{height}(\mathbf{g}_m) + \sum_{s=1}^{m-1} \mathrm{height}(\mathbf{g}_s) \cdot \prod_{t=s}^{m-1} (d_t + 4)\log(d_t + 4) \right) \\ &\leq \sum_{s=1}^{m} \mathrm{height}(\mathbf{g}_s) \cdot \prod_{t=s}^{m} (d_t + 4)\log(d_t + 4). \end{aligned}$$

To analyze the denominators of the structure constants, we use the fact that $\mathrm{prem}(\mathbf{m}, \mathbf{g}_m)$ is the combination of the product of at most $d_m + 4$ integral elements of $\mathcal{A}(\Delta_{m-1})$, and the denominators of the structure constants of $\mathcal{A}(\Delta_{m-1})$ divide $\prod_{s=1}^{m-1} \mathrm{lc}(\mathbf{g}_s)^{\alpha'_s}$ by (3.22). Using Proposition 3.3.1, we have that the denominators of the coordinates of the reduced form of $\mathrm{prem}(\mathbf{m}, \mathbf{g}_m)$ divide

$$\prod_{s=1}^{m-1} \mathrm{lc}(\mathbf{g}_s)^{\alpha_s}$$

where

$$\alpha_s \leq (d_m + 4) \cdot \alpha'_s \leq \prod_{t=s}^{m} (d_t + 4)$$

for $1 \leq s \leq m-1$. By Lemma 3.3.3, we have

$$\mathbf{m} = \mathbf{g}_m \cdot \mathbf{q} + \frac{\mathrm{prem}(\mathbf{m}, \mathbf{g}_m)}{\mathrm{lc}(\mathbf{g}_m)^{d_m+1}},$$

therefore the denominators of the coordinates of the reduced form of $\mathbf{m}$ divide

$$\prod_{s=1}^{m} \mathrm{lc}(\mathbf{g}_s)^{\alpha_s}$$

where $\alpha_s \leq \prod_{t=s}^{m}(d_t + 4)$ for $1 \leq s \leq m$, which proves the claim. ■

Using the method in the proof of the previous proposition, we give an algorithm

reduce(Δ)

which reduces an unmixed set Δ and finds the structure constants of the algebra $\mathcal{A}(\Delta)$, as the following corollary asserts it.

Corollary 3.3.5 *Let* $\Delta = \{g_1, \ldots, g_m\} \subset \Bbbk[x_1, \ldots, x_n]$ *be an unmixed set, and let* $\mathrm{class}(g_s) = x_{l+s}$ *and* $d_s = \deg_{x_{l+s}}(g_s)$. *Assume that* $\deg_{x_{l+s}}(g_{s'}) \leq d$ *if* $s' \neq s$ *for some* $d \geq 0$. *The the algorithm* **reduce**(Δ) *returns the reduced unmixed set*

$$\Delta' := \{g'_1, \ldots, g'_m\}$$

such that

$$\mathrm{Rep}(g_1, \ldots, g_m) = \mathrm{Rep}(g'_1, \ldots, g'_m),$$

together with the structure constants of the algebra $\mathcal{A}(\Delta')$. *The height of the polynomials in* Δ' *is bounded by*

$$\mathrm{height}(g'_s) \leq \sum_{s=1}^{m} \mathrm{height}(g_s)(d \log(d))^{s-r+1} \cdot \prod_{t=s}^{m} (d_t + 4) \log(d_t + 4).$$

The heights Υ *of the structure constants of* $\mathcal{A}(\Delta')$ *are bounded by*

$$\Upsilon \leq \sum_{s=1}^{m} \mathrm{height}(g_s)(d \log(d))^{s-r+1} \cdot \prod_{t=s}^{m} (d_t + 4) \log(d_t + 4),$$

and the lcm *of the denominators of the structure constants divides*

$$\prod_{s=1}^{m} \mathrm{lc}(g_s)^{\alpha_s}, \quad \textit{where} \quad \alpha_s \leq (d+1)(d_m + 4) \cdots (d_s + 4) \tag{3.24}$$

for all $1 \leq s \leq m$.

Moreover the arithmetic circuit over $\Bbbk$ *computing* Δ' *and the structure constants of* $\mathcal{A}(\Delta')$ *have depth*

$$\begin{aligned} \mathrm{Depth}(\textbf{reduce}) &\leq c \cdot \sum_{s=1}^{m} (n-m) \log^2(d \cdot d_s) \log(\mathrm{height}(g_s) + \Upsilon) \log(\prod_{t-1}^{s-1} d_t) \\ &\leq O(m^3 (n-m) \log^3(d' \cdot d) \log(h)), \end{aligned}$$

and the size

$$\begin{aligned}\text{Size}(\textbf{reduce}) &\leq C \cdot D^3 \sum_{s=1}^{m} d \cdot d_s(d \cdot d_s(\text{height}(\mathrm{g}_s) + \Upsilon))^{2(n-m)} \\ &\leq O((d')^{4m}(d\log(d))^m(h(d'\log(d')d\log(d))^m)^{2(n-m)})\end{aligned}$$

for some constants c and C, where d' is an upper bound for $\{d_1, \ldots, d_s\}$, and h is an upper bound for the height of the input.

Proof:

Denote $\Delta_s := \{\mathrm{g}_1, \ldots, \mathrm{g}_s\}$ for $1 \leq s \leq m$.

For $m = 1$ let $\Delta_1' := \Delta_1$. The computation of the structure constants of $\mathcal{A}(\Delta_1)$ is the same as in the proof of Proposition 3.3.4, therefore we get that the height Υ_1 of the structure constants of $\mathcal{A}(\Delta_1)$ satisfies

$$\Upsilon_1 \leq (d_1 + 3) \cdot \text{height}(\mathrm{g}_1).$$

Also, the denominators of the structure constants is a divisor of $\text{lc}(\mathrm{g}_1)^{d_1+1}$.

Let $m > 1$ and assume inductively that we have computed the reduced unmixed set $\Delta_{s-1}' = \{g_1', \ldots, g_{m-1}'\}$ and the multiplication tables $\mathcal{M}_1, \ldots, \mathcal{M}_{m-1}$, and we haveproved that the structure constants for the algebra $\mathcal{A}(\Delta_{m-1}')$ have heights at most

$$\Upsilon_{m-1} \leq \sum_{s=1}^{m-1}(d\log(d))^{m-s}\text{height}(\mathrm{g}_s) \cdot \prod_{t=s}^{m-1}(d_t + 4)\log(d_t + 4).$$

To compute g_m', we have to reduce each coefficient $\mathrm{g}_j^{(m)}$ of $\mathrm{g}_s = \sum_{j=0}^{d_m} \mathrm{g}_j^{(m)} x_n^j$ by

Δ'_{m-1}. Using Proposition 3.3.1 we get

$$\begin{aligned}
\text{height}(\mathrm{g}'_m) &\leq d\log(d)\cdot(\text{height}(\mathrm{g}_m)+\Upsilon_{m-1}) \\
&\leq d\log(d)\cdot\text{height}(\mathrm{g}_m)+d\log(d)\sum_{s=1}^{m-1}(d\log(d))^{m-s}\text{height}(\mathrm{g}_s) \\
&\quad\cdot\prod_{t=s}^{m-1}(d_t+4)\log(d_t+4) \\
&\leq \sum_{s=1}^{m}(d\log(d))^{m-s+1}\text{height}(\mathrm{g}_s)\cdot\prod_{t=s}^{m-1}(d_t+4)\log(d_t+4).
\end{aligned}$$

Let $\Delta'_m=\{\mathrm{g}'_1,\ldots,\mathrm{g}'_m\}$. Since Δ'_m is reduced we can compute the structure constants of $\mathcal{A}(\Delta'_m)$ using the method described in the proof of Proposition 3.3.4. Using Proposition 3.3.1 and Lemma 3.3.3, we have that the height of the entries of the products of the matrices in (3.16) are at most

$$\begin{aligned}
\Upsilon_m &\leq (d_m+4)\log(d_m+4)(\text{height}(g'_m)+\Upsilon_{m-1}) \\
&\leq (d_m+4)\log(d_m+4)(d\log(d)\cdot(\text{height}(\mathrm{g}_m)+\Upsilon_{m-1})+\Upsilon_{m-1}) \\
&\leq \sum_{s=1}^{m}(d\log(d))^{m-s+1}\text{height}(\mathrm{g}_s)\cdot\prod_{t=s}^{m}(d_t+4)\log(d_t+4)
\end{aligned}$$

which proves the claim for the degree bounds.

To give bounds for the arithmetic circuit over $\Bbbk$ computing $\mathbf{reduce}(\Delta)$ we use the results in Proposition 3.3.1. For the depth we get

$$\begin{aligned}
\text{Depth}(\mathbf{reduce}) &\leq \sum_{s=1}^{m}c\cdot(n-m)\log(\prod_{t-1}^{s-1}d_t)\log^2(d\cdot d_s)\log(\text{height}(\mathrm{g}_s)+\Upsilon_{s-1}) \\
&\leq O(m^3(n-m)\log^3(d'\cdot d)\log(h)),
\end{aligned}$$

and for the size

$$\begin{aligned}
\text{Size}(\mathbf{reduce}) &\leq C\cdot D^3\sum_{s=1}^{m}d\cdot d_s(d\cdot d_s(\text{height}(\mathrm{g}_s)+\Upsilon_{s-1}))^{2(n-m)} \\
&\leq O((d')^{4m}(d\log(d))^m(h(d'\log(d')d\log(d))^m)^{2(n-m)})
\end{aligned}$$

for some constants c and C. ■

3.4 The pseudo-inverse

Let $\Delta = \{\mathbf{g}_1, \dots \mathbf{g}_m\} \subset \Bbbk[x_1, \dots, x_n]$ be an unmixed set such that $n = m + l$ and for all $1 \leq s \leq m$

1. $\text{class}(\mathbf{g}_s) = x_{l+s}$;
2. $\text{lc}(\mathbf{g}_s) \in \Bbbk[x_1, \dots, x_l]$;
3. $\mathbf{g}_s$ is reduced modulo $\Delta_{s-1} := \{\mathbf{g}_1, \dots, \mathbf{g}_{s-1}\}$.

Denote the a priori basis of $\mathcal{A}(\Delta)$ by $\mathbf{B}(\Delta) = \{\mathbf{e}_1, \dots, \mathbf{e}_D\}$, and assume that the multiplication table $\mathcal{M}(\Delta)$ of the algebra $\mathcal{A}(\Delta)$ is also given, i.e. we have

$$\mathbf{e}_i \cdot \mathbf{e}_j = \frac{1}{\text{lc}(\Delta)^{\vec{\alpha}}} \sum_{k=1}^{D} c_{i,j,k} \mathbf{e}_k;$$

where $c_{i,j,k} \in k[x_1, \dots, x_l]$ for $1 \leq i, j \leq D$ and $\vec{\alpha} \in \mathbb{N}^m$ and $\text{lc}(\Delta)^{\vec{\alpha}} = \prod_{s=1}^{m} \text{lc}(\mathbf{g}_s)^{\alpha_s}$.

Also, let $\mathbf{f} \in \Bbbk[x_1, \dots, x_n]$ and assume that $\mathbf{f} \notin \mathcal{P}$ for all $\mathcal{P} \in \text{Ap}(\Delta)$. We assume that $\mathbf{f}$ is reduced modulo Δ, i.e. it is an element of the algebra $\mathcal{A}(\Delta)$, and

$$\mathbf{f} = \frac{1}{\text{lc}(\Delta)^{\vec{\beta}}} \sum_{i=1}^{D} f_i \mathbf{e}_i \in \mathcal{A}(\Delta),$$

where $f_i, \in \Bbbk[x_1, \dots, x_l]$, $\vec{\beta} \in \mathbb{N}^m$.In Lemma 3.1.5 we proved that there exists $\bar{\mathbf{f}} \in \Bbbk[x_1, \dots, x_n]$ such that $\bar{\mathbf{f}} \notin \mathcal{P}$ for all $\mathcal{P} \in \text{Ap}(\Delta)$, and

$$\mathbf{f} \cdot \bar{\mathbf{f}} \equiv \mathbf{r} \mod \langle \Delta \rangle \text{ and } \mathbf{r} \in \Bbbk[x_1, \dots, x_l]. \tag{3.25}$$

We call $\bar{\mathbf{f}}$ the *pseudo-inverse* of $\mathbf{f}$ in $\mathcal{A}(\Delta)$. In this section we describe the subroutine

$$\mathbf{pinverse}_m^l(\Delta, \mathcal{M}(\Delta), \mathbf{f})$$

which computes the pseudo-inverse of $\mathbf{f}$ in $\mathcal{A}(\Delta)$.

The main idea to compute $\bar{\mathbf{f}}$ is to express the coefficients of $\bar{\mathbf{f}}$ in the a priori basis of $\mathcal{A}(\Delta)$ as the solution of a linear equation system. Denote the unknown coefficients of $\bar{\mathbf{f}}$ by

$$\bar{\mathbf{f}} = \sum_{i=1}^{D} \bar{f}_i \mathbf{e}_i$$

where $\bar{f}_i$ are variables over $k(x_1, \ldots, x_l)$. Then

$$\mathbf{f} \cdot \bar{\mathbf{f}} = \frac{1}{\mathrm{lc}(\Delta)^{\bar{\alpha}+\bar{\beta}}} \sum_{k=1}^{d} \left(\sum_{i,j=1}^{D} f_i \bar{f}_j c_{i,j,k} \right) \mathbf{e}_k = \mathbf{e}_1 \tag{3.26}$$

where we can assume that $\mathbf{e}_1 = 1 \in \mathcal{A}(\Delta)$. Notice that (3.26) gives a linear equation system over the field $\mathbb{k}(x_1, \ldots, x_l)$ with unknowns $(\bar{f}_j)_{j=1}^{D}$.

Define the matrix

$$\mathbf{M}_{\mathbf{f}} := \left(\sum_{i=1}^{D} f_i c_{i,j,k} \right)_{j,k=1}^{D}.$$

Note that $\frac{1}{\mathrm{lc}(\Delta)^{\bar{\alpha}+\bar{j}}} \cdot \mathbf{M}_{\mathbf{f}}$ is the matrix of the linear transformation

$$\varphi_{\mathbf{f}} : \mathcal{A}(\Delta) \to \mathcal{A}(\Delta), \quad \varphi_{\mathbf{f}}(\mathbf{a}) := \mathbf{f} \cdot \mathbf{a}.$$

Therefore, if $\mathbf{f} \notin \mathcal{P}$ for all $\mathcal{P} \in \mathrm{Ap}(\Delta)$, then $\mathbf{f}$ is invertible in $\mathcal{A}(\Delta)$ by Lemma 3.1.5, hence $\varphi_{\mathbf{f}}$ is nonsingular. This implies that $\det(\mathbf{M}_{\mathbf{f}}) \neq 0$, and we can apply Cramer's

rule to solve (3.26). Let

$$\mathbf{M}_{\mathbf{f}}^{(j)} = \begin{array}{|c|c|c|} \hline & \underline{j} & \\ \hline & 0 & \\ & 0 & \\ \mathbf{M}_{\mathbf{f}} & \vdots & \\ & 0 & \\ & 1 & \\ \hline \end{array}$$

for all $1 \leq j \leq D$. If we define

$$\bar{f}_j := \det(\mathbf{M}_{\mathbf{f}}^{(j)}) \in \Bbbk[x_1, \ldots, x_n]$$

then, by Cramer's rule, we get that

$$\sum_{k=1}^{d} \left(\sum_{i,j=1}^{D} f_i \bar{f}_j c_{i,j,k} \right) \mathbf{e}_k = \det(\mathbf{M}_{\mathbf{f}}) \cdot \mathbf{e}_1.$$

Define $\bar{\mathbf{f}} = \sum_{j=1}^{D} \bar{f}_j \mathbf{e}_j$. Then

$$\mathbf{f} \cdot \bar{\mathbf{f}} = \frac{1}{\mathrm{lc}(\Delta)^{\vec{\alpha}+\vec{\beta}}} \sum_{k=1}^{d} \left(\sum_{i,j=1}^{D} f_i \bar{f}_j c_{i,j,k} \right) \mathbf{e}_k = \frac{1}{\mathrm{lc}(\Delta)^{\vec{\alpha}+\vec{\beta}}} \det(\mathbf{M}_{\mathbf{f}}) \cdot \mathbf{e}_1.$$

Theorem 3.4.1 *Let* $\Delta = \{\mathbf{g}_1, \ldots \mathbf{g}_m\} \subset \Bbbk[x_1, \ldots, x_n]$ *be as above and*

$$\mathbf{f} \in \Bbbk[x_1, \ldots, x_n] \text{ where } \mathbf{f} \notin \mathcal{P} \ \forall \mathcal{P} \in \mathrm{Ap}(\Delta).$$

Assume also that the multiplication table $\mathcal{M}(\Delta)$ *of the algebra* $\mathcal{A}(\Delta)$ *is also given and the height of the structure constants are bounded by* Υ. *Let* D *be the dimension of* $\mathcal{A}(\Delta)$ *over* $\Bbbk(x_1, \ldots, x_l)$. *Then any polynomial* h *occurring in the computation of*

$$\mathbf{pinverse}_m^l(\Delta, \mathcal{M}(\Delta), \mathbf{f})$$

described above has

$$\text{height}(h) \leq D(\text{height}(\mathbf{f}) + \Upsilon).$$

Moreover, the arithmetic circuit computing $\bar{\mathbf{f}} = \mathbf{pinverse}_m^l(\Delta, \mathbf{f})$ *over* $\Bbbk$ *has depth*

$$O(l \cdot \log^2(D(\text{height}(\mathbf{f}) + \Upsilon)))$$

and size

$$O(D^{4.5}(D(\text{height}(\mathbf{f}) + \Upsilon))^{2l})$$

Proof:

The computation of $\bar{\mathbf{f}}$ consists of computing the determinants $\det(\mathbf{M}_{\mathbf{f}}^{(j)})$ of size $D \times D$ for $1 \leq j \leq D$. The entries of the matrix $\mathbf{M}_{\mathbf{f}}^{(j)}$ have height at most $\text{height}(\mathbf{f}) + \Upsilon$. Since the entries of $\mathbf{M}_{\mathbf{f}}^{(j)}$ are integral, we have that the height of its determinant is at most $D(\text{height}(\mathbf{f}) + \Upsilon)$.

By [Ber84] a $D \times D$ determinant over an arbitrary commutative ring can be computed by a uniform circuit with size $O(D^{3.5})$ and depth $O(\log^2(D))$. Since the product and sum of k elements of $\Bbbk(x_1, \ldots, x_l)$ of height d can be computed in depth $O(l \log(kd))$ and size $O((dk)^{2l})$, the complexity bounds of the claim follow. ■

3.5 Sub-resultant and GCD over rings with zero-divisors.

In this section we describe some well-known methods to compute the GCD of several univariate polynomials over certain coefficient rings with zero-divisors. We give

sufficient conditions on the coefficient ring for the GCD to be well defined. Moreover, we use only ring arithmetics and our method returns a GCD with integral coefficients. This method is one of the main building blocks of the decomposition algorithms described in Chapter 4. There we decompose the coefficient rings in order to satisfy the conditions for the existence of the GCD. We describe both a deterministic and a randomized version of the algorithm. We follow an approach similar to [IK93]. In the subsequent sections we assume that the polynomials in the algorithm have coefficients from an infinite field $\mathbb{k}$, although the algorithm below can be modified to work also for polynomial rings over finite fields.

We use the following notation throughout this section. As before, we denote by $\mathbf{K}(\mathcal{P})$ the function field of the integral domain $R/\mathcal{P}$, where R is any ring and $\mathcal{P} \subset R$ is a prime ideal. For a ring extension $R \subseteq R'$ we denote the function field of $R'/(\mathcal{P} \cdot R')$ by $\mathbf{K}_{R'}(\mathcal{P})$. For $\Delta = \{\mathrm{g}_1, \ldots \mathrm{g}_m\}$ an unmixed set in $\mathbb{k}[x_1, \ldots x_n]$, denote $\{\mathrm{g}_1, \ldots \mathrm{g}_s\}$ by Δ_s, the maximal variable of g_s by x_{i_s} and the ring $\mathbb{k}[x_1, \ldots, x_{i_s-1}]$ by R_s. Note that g_s is univariate over the ring R_s.

Let $\mathbf{K}$ be an arbitrary field and $\mathbf{K}[x]_d$ denotes the vector space over $\mathbf{K}$ consisting of the univariate polynomials in $\mathbf{K}[x]$ of degree at most d. Then the polynomials $1, x, \ldots, x^d$ form a basis for $\mathbf{K}[x]_d$, which is called the *standard basis*. Let $f = \sum_{i=0}^{d_1} f_i x^i$ and $g = \sum_{i=0}^{d_2} g_i x^i$ be two polynomials in $\mathbf{K}[x]$ with f_{d_1} and g_{d_2} non-zero. Consider the linear map

$$\begin{aligned} \varphi_0 \;:\; & \mathbf{K}[x]_{d_2-1} \times \mathbf{K}[x]_{d_1-1} \longrightarrow \mathbf{K}[x]_{d_1+d_2-1} \\ & (p, q) \mapsto fp + gq. \end{aligned}$$

The $(d_2 + d_1) \times (d_2 + d_1)$ matrix Φ_0 of the map φ_0 in the standard basis is of the form

$$\Phi_0 = \begin{pmatrix} f_{d_1} & 0 & 0 & 0 & g_{d_2} & 0 & 0 & 0 & 0 & 0 \\ f_{d_1-1} & f_{d_1} & 0 & 0 & g_{d_2-1} & g_{d_2} & 0 & 0 & 0 & 0 \\ \vdots & \ddots & & \vdots & \vdots & & \ddots & & & \vdots \\ f_0 & f_1 & \dots & f_{d_1-d_2-1} & 0 & \dots & g_0 & g_1 & \dots & g_{d_1-d_2} \\ 0 & f_0 & \dots & f_{d_1-d_2-1} & 0 & \dots & 0 & g_0 & \dots & g_{d_1-d_2-1} \\ \vdots & & \ddots & \vdots & \vdots & & & & \ddots & \vdots \\ 0 & 0 & \dots & f_0 & 0 & 0 & \dots & 0 & & g_0 \end{pmatrix}.$$

We call Φ_0 the Sylvester matrix of f and g. The determinant of Φ_0 is the resultant of f and g, denoted by $\mathrm{RES}_x^{(0)}(f, g)$.

We also define the sub-resultants of f and g as follows. For any $0 < D < \min(d_1, d_2)$, consider the linear map

$$\begin{aligned} \varphi_D \quad : \quad & \mathbf{K}[x]_{d_2-D-1} \times \mathbf{K}[x]_{d_1-D-1} \longrightarrow \mathbf{K}[x]_{d_1+d_2-2D-1} \\ & (p, q) \mapsto \frac{1}{x^D}(fp + gq)_{\geq D}, \end{aligned}$$

where $(fp + gq)_{\geq D}$ is the degree $\geq D$ part of $fp + gq$, i.e.

$$(fp + gq)_{\geq D} = (fp + gq) - [fp + gq \mod (x^D)].$$

We obtain the matrix Φ_D of φ_D in the standard basis by deleting the last D columns of the coefficients of f, the last D columns of the coefficients of g and the last $2D$ rows in the matrix Φ_0. The determinant of Φ_D is the D-th sub-resultant of f and g and denoted by $\mathrm{RES}_x^{(D)}(f, g)$.

Let $\Delta = \{\mathbf{g}_1, \ldots, \mathbf{g}_m\}$ be an unmixed set in $\Bbbk[x_1, \ldots x_t]$, $f_0, \ldots, f_k \in \Bbbk[x_1, \ldots x_n]$, $n \geq t$, and assume that $\deg_{x_t}(\mathbf{g}_m) > 0$. Suppose that

$$\begin{aligned} \mathrm{RES}^{(D)}_{x_t}(\mathbf{g}_m, \textstyle\sum_{i=0}^{k} y^i f_i) &\not\equiv 0 \mod (\mathcal{P}) \text{ and} \\ \mathrm{RES}^{(D')}_{x_t}(\mathbf{g}_m, \textstyle\sum_{i=0}^{k} y^i f_i) &\equiv 0 \mod (\mathcal{P}),\ 0 \leq D' < D \end{aligned} \tag{3.27}$$

for all $\mathcal{P} \in \mathrm{Ap}(\Delta_{m-1})$. Then by Lemma 3.1.2, for any $\mathcal{P} \in \mathrm{Ap}(\Delta_{m-1})$

$$\gcd_{\mathbf{K}_{R_m}(\mathcal{P})}(\mathbf{g}_m, f_0, \ldots, f_k) = d, \quad \deg_{x_t}(d) = D$$

and we can assume that d is monic over $\mathbf{K}_{R_m}(\mathcal{P})$.

We proved in Lemma 3.1.3 that assuming that the conditions in (3.27) are satisfied, there exists a polynomial

$$\mathbf{d} = \mathbf{ggcd_t}(\Delta, f_0, \ldots, f_k)$$

such that

1. $\mathbf{d} \in \Bbbk[x_1, \ldots x_t]$;
2. $\mathbf{d} \in \langle \mathrm{Rep}(\Delta_{m-1}) \cup \{\mathbf{g}_m\} \cup \mathbf{coeff^n_{t+1}}(f_0, \ldots, f_k) \rangle$, where $\Delta_{m-1} = \{\mathbf{g}_1, \ldots, \mathbf{g}_{m-1}\}$, and $\mathbf{coeff^n_{t+1}} \subset k[x_1, \ldots, x_t]$ is the set of coefficients of $f_1, \ldots f_k$ as multivariate polynomials in the variables $\{x_{t+1}, \ldots, x_n\}$.
3. $\mathrm{lc}(\mathbf{d}) \notin \mathcal{P}$ for all $\mathcal{P} \in \mathrm{Ap}(\Delta_{m-1})$;
4. the monic image of $\mathbf{d}$ in $\mathbf{K}_{R_m}(\mathcal{P})[x_t]$ is $d = \gcd_{\mathbf{K}_{R_m}(\mathcal{P})}(\mathbf{g}_m, f_0, \ldots, f_k)$ for all $\mathcal{P} \in \mathrm{Ap}(\Delta_{m-1})$.

We proved Lemma 3.1.3 by constructing the polynomial $\mathbf{d}$. To obtain $\mathbf{d}$ we solved the linear equation system corresponding to the D-th sub-resultant

$$\Phi_D := \mathrm{RES}_{x_n}^{(D)}(\mathbf{g}_m, \sum_{i=0}^{k} f_i y_i)$$

over the field $\Bbbk(x_1, \ldots, x_{t-1}, x_{t+1}, \ldots, x_n, y)$ using Cramer's rule without the division by $\det(\Phi_D)$. By this we obtained a polynomial $\bar{d} \in \Bbbk[x_1, \ldots, x_n, y]$ such that

$$\bar{d} = \det(\Phi_D) \cdot \mathrm{gcd}_{\mathbf{K}_{R_m}(\mathcal{P})}(\mathbf{g}_m, f_0, \ldots, f_k).$$

If $\det(\Phi_D) \in \Bbbk[x_1, \ldots, x_{t-1}]$ then $\bar{d} = f\bar{p} + g\bar{q}$ satisfies the specifications of

$$\mathbf{ggcd_t}(\Delta, f_0, \ldots, f_k).$$

To find a polynomial $\mathbf{d} \in \Bbbk[x_1, \ldots x_t]$ satisfying the specification of Lemma 3.1.3, we can either use a randomized approach or a deterministic approach. The advantage of the randomized approach is that it significantly improves the efficiency of the algorithm. Choose random elements $\sigma := (\alpha_{t+1}, \ldots \alpha_n, \beta) \in S^{n-t+1}$ uniformly from a large finite set $S \subset \Bbbk$, and obtain the matrix Φ_D^σ by substituting σ in $(x_{t+1}, \ldots, x_n, y)$. Below we prove that with high probability $\det(\Phi_D^\sigma) \notin \mathcal{P}$ for all $\mathcal{P} \in \mathrm{Ap}(\Delta_{m-1})$. To get a Las Vegas algorithm we use the algorithm **general**, described in the next section, which returns a random combination of the input polynomials which do not vanish modulo any $\mathcal{P} \in \mathrm{Ap}(\Delta_{m-1})$, or returns an error sign if this is not possible. In other words, the subroutine

$$\mathbf{general_{t-1}^{m-1}}(\Delta_{m-1}, \det(\Phi_D^\sigma))$$

described in section 3.6 either returns that the polynomial $\det(\Phi_D^\sigma)$ itself is in general position, or an error signal if it vanishes modulo some $\mathcal{P} \in \mathrm{Ap}(\Delta_{m-1})$. In the second case we choose a new substitution σ. In the first case the polynomial $d^\sigma = f^\sigma p^\sigma + g q^\sigma$ will satisfy the specifications of the proposition, where p^σ and q^σ are obtained using Cramer's rule for the matrix Φ_D^σ as in (3.3).

The following lemma asserts that $\det(\Phi_D^\sigma) \notin \mathcal{P}$ for all $\mathcal{P} \in \mathrm{Ap}(\Delta_{m-1})$ with high probability.

Lemma 3.5.1 *Let $\mathcal{I} \subset \Bbbk[x_1, \ldots, x_t]$ be a proper radical ideal, $\mathcal{I} = \bigcap_{i=1}^k \mathcal{P}_i$ its irredundant prime decomposition, and $f \in \Bbbk[x_1, \ldots x_n]$ for $n > t$. Denote by $f^\mathcal{P}$ the image of f in the quotient field $K(\mathcal{P})$ for $\mathcal{P} \in \mathrm{Ap}(\mathcal{I})$, i.e. $f^\mathcal{P} \in K(\mathcal{P})[x_{t+1}, \ldots, x_n]$. Assume that $f^\mathcal{P} \not\equiv 0$ and the total degree of $f^\mathcal{P}$ is at most D for all $\mathcal{P} \in \mathrm{Ap}(\mathcal{I})$. Let S be a finite subset of $\Bbbk$, and $(s_{t+1}, \ldots, s_n) \in S^{n-t}$ random elements uniformly chosen from S. Then $f^\mathcal{P}(s_{t+1}, \ldots, s_n) = 0$ for some $\mathcal{P} \in \mathrm{Ap}(\mathcal{I})$ with probability at most $\frac{kD}{|S|}$.*

Proof of lemma: Denote $\Bbbk[x_1, \ldots x_t]$ by R. The lemma easily follows from Schwartz's lemma [Sch80] and from the fact that the composition of the ring homomorphisms

$$\varphi : \Bbbk \hookrightarrow R \longrightarrow R/\mathcal{P} \hookrightarrow \mathbf{K}(\mathcal{P})$$

is injective for every $\mathcal{P} \in \mathrm{Ap}(\mathcal{I})$. ■

For a deterministic algorithm, we can call the deterministic version of the sub-

routine

$$\mathbf{general}_{\mathbf{t-1}}^{\mathbf{m-1}}(\Delta_{m-1}, \mathrm{coeff}_{x_{t+1},\ldots,y}(\det(\Phi_D))$$

described in section 3.6, where $\mathrm{coeff}_{x_{t+1},\ldots,y}(f)$ denotes the set of coefficients of f as a multivariate polynomial in the variables $\{x_{t+1}, \ldots x_n, y\}$. Also, note that we can assume that $t = n$, since the gcd of $\mathbf{g}_m$ and $f_0, \ldots, f_k$ is the same as the gcd of $\mathbf{g}_m$ and $\mathrm{coeff}_{x_{t+1},\ldots,x_n}(f_0, \ldots, f_k)$. Therefore the polynomial $h \in \Bbbk[x_1, \ldots, x_{t-1}]$ returned by $\mathbf{general}_{\mathbf{t-1}}^{\mathbf{m-1}}(\Delta_{m-1}, \mathrm{coeff}_y(\det(\Phi_D))$ is a specialization of $\det(\Phi_D)$, which does not vanish over any prime $\mathcal{P} \in \mathrm{Ap}(\Delta_{m-1})$.

Theorem 3.5.2 *Let $\Delta = \{\mathbf{g}_1, \ldots, \mathbf{g}_m\} \subset \Bbbk[x_1, \ldots x_t]$ be an unmixed set, let $f_0, \ldots, f_k$ be polynomials in $k[x_1, \ldots x_n]$, $n \geq t$, and assume that $\deg_{x_t}(g_m) = d_m > 0$. Assume that $\Delta = \Delta_{m-1} \cup \{\mathbf{g}_m\}$ and $f_0, \ldots, f_k$ satisfy the conditions of Lemma 3.1.3. Also, assume that the polynomials $f_0, \ldots, f_k$ are reduced modulo Δ. Then there exists a randomized Monte Carlo algorithm using an arithmetic circuit over $\Bbbk$ which computes*

$$\mathbf{d} := \mathbf{ggcd}_{\mathbf{t}}(\Delta, f_0, \ldots, f_k)$$

and has depth at most

$$O((t-m)\log(D)\log^2(d_m)\log(\mathrm{height}(f) + \Upsilon))$$

and size at most

$$O(D^3 d_m^{3.5}(d_m^{3.5} d_m(\mathrm{height}(f) + \Upsilon))^{2(t-m)}),$$

where D is the dimension of the algebra $\mathcal{A}(\Delta)$ and Υ is a bound on the height of the structure constants of $\mathcal{A}(\Delta)$.

To achieve a Las Vegas algorithm we call the subroutine $\mathbf{general}_{\mathbf{n-1}}^{\mathbf{m-1}}$, *therefore we obtain an arithmetic circuit of depth*

$$O(m(t-m)\log^4(D)\log(k)\log(\text{height}(\Delta, f)))$$

and size

$$O(mkD^4(D^3\text{height}(\Delta, f))^{2(t-m)}).$$

The deterministic version has depth at most

$$O(m(t-m)\log^4(D)\log(k\mathbf{H}(f)^{n-t})\log(\text{height}(\Delta, f)))$$

and size at most

$$O(mk\mathbf{H}(f)^{n-t}D^4(D^3\text{height}(\Delta, f))^{2(t-m)}),$$

where $\mathbf{H}(f)$ *is the maximal degree of the polynomial* $f = \sum f_i y^i$ *in the variables* $x_{t+1}, \ldots, x_n, y$.

Moreover, the height of the polynomial d' *is at most*

$$\text{height}(\mathbf{d}) \leq d_m \log(d_m)(\text{height}(f) + \text{height}(\mathbf{g}_m) + 2\Upsilon) \tag{3.28}$$

where $\text{height}(f) = \max\{\text{height}(f_i)\}_{i=0}^{k}$. *Furthermore, for every polynomial* h *occurring in the deterministic version of the algorithm*

$$\deg_{x_j}(h) \leq 2d_m(\max_{i=0}^{k}\deg_{x_j}(f_i)), \quad t < j \leq n \tag{3.29}$$

$$\deg_y(h) \leq 2d_m k. \tag{3.30}$$

Proof: We assume that the polynomials occurring in the computation are all reduced modulo Δ_{m-1}.

The computation of d' consist of computing the $2d_m - D + 1$ determinants $\det(\Phi_D^{(j)})$ of size $(2d_m - D) \times (2d_m - D)$ (see (3.3)), and then combining the result with the coefficients of f and g_m. By [Ber84] an $N \times N$ determinant over an arbitrary commutative ring can be computed by a uniform circuit with size $O(N^{3.5})$ and depth $O(\log^2(N))$.

In the randomized Monte Carlo version we use a substitution σ of elements from $\mathbb{k}$ into $x_{t+1}, \ldots, x_n, y$, therefore the coefficients of the equation system (3.2) are elements of $\mathcal{A}(\Delta_{m-1})$. Therefore, by [Ber84], d' can be computed using an arithmetic circuit over $\mathbb{k}$ with depth $c_1 \log^2(d_m)$ times the depth, and size $c_2 d_m^{4.5}$ the size of arithmetics in $\mathcal{A}(\Delta_{m-1})$ with elements of heights $\leq d_m \mathrm{height}(\Delta, f)$, given in Proposition 3.3.1.

In the Las Vegas version in addition to the above, we call the subroutine

$$\mathbf{general}_{t-1}^{m-1}(\Delta_{m-1}, \{\det(\Phi_D^{\sigma})\}).$$

Note that the polynomial Ψ_m defined in Proposition 3.6.1 is a special case of $\det(\Phi_D^{\sigma})$ for $D = 0$. Therefore, to get the complexity of the Las Vegas algorithm, we can apply the complexity results of Theorem 3.6.3 with input Δ and $\{f_0, \ldots, f_k\}$.

In the deterministic version the coefficients of the linear system (3.3) are elements of $\mathcal{A}(\Delta_{m-1})[x_{t+1}, \ldots, x_n, y]$. Note that the gcd of g_m and $F = \{f_0, \ldots, f_k\} \subset \mathbb{k}[x_1, \ldots, x_n]$ is the same as the gcd of g_m and the coefficients of the polynomials in F as multivariate polynomials in the variables $\{x_{t+1}, \ldots, x_n\}$. Therefore, we can assume that the input is $F' := \mathrm{coeff}_{x_{t+1} \cdots x_n}(F) \subset \mathbb{k}[x_1, \ldots, x_t]$, and $k' = |F'| = k\mathbf{H}(F)^{n-t}$, where $\mathbf{H}(F)$ is the maximal degree of the polynomials in F in the

variables $\{x_{t+1}, \ldots, x_n\}$. By the same argument as above, we get the complexity of the deterministic algorithm by applying the complexity results of Theorem 3.6.3 for the subroutine $\mathbf{general_t^m}$ with input Δ and F'.

Claim (3.28) about the height of $\mathbf{d}$ follows simply from Proposition 3.3.1 and the computation of $\mathbf{d}$ described in the beginning of the proof. ■

3.6 Finding a polynomial in general position

Let $\Delta = \{\mathbf{g}_1, \ldots, \mathbf{g}_m\} \subset \mathbb{k}[x_1, \ldots, x_n]$ be an unmixed set of codimension m and $F = \{f_0, \ldots, f_k\} \subset \mathbb{k}[x_1, \ldots, x_n]$ be a finite set of polynomials. Again, we assume that the coefficient field $\mathbb{k}$ is infinite. We use the notation of the previous section.

Suppose that $V(\Delta) \cap V(F)$ has codimension $\geq m + 1$. Then there exists a polynomial $h \in \mathbb{k}[x_1, \ldots, x_n]$ such that

$$h = \sum_{j=0}^{k} a^j f_j$$

for some $a \in \mathbb{k}$ and h is in *general position*, i.e. $V(\mathcal{P}) \cap V(h)$ has codimension $m+1$ for all $\mathcal{P} \in \mathrm{Ap}(\Delta)$ associated prime ideals of $\mathrm{Rep}(\Delta)$.

We compute the polynomial h using the algorithm $\mathbf{general_n^{m+1}}(\Delta, F)$ as follows:

If $m = 0$, then $h = f_0 \in F$ will satisfy the desired properties. If $m > 0$ we define

$$\Psi_{m+1}(\vec{x}, y) := f_k y^k + f_{k-1} y^{k-1} + \ldots + f_0 \in \mathbb{k}[x_1, \ldots, x_n, y]$$

where y is a new variable. The algorithm is based on the equivalence of the statements in the following proposition:

Proposition 3.6.1 *Let Δ, F and Ψ_{m+1} be as above. Then the following statements are equivalent:*

(a) $V(\mathcal{P}) \cap V(F)$ has codimension $\geq m+1$ for all $\mathcal{P} \in \mathrm{Ap}(\Delta)$.

(b) The gcd of the polynomials $\{\mathbf{g}_m, f_0, \ldots f_k\}$ is 1 over $\mathbf{K}_{R_m}(\mathcal{P})$ for all $\mathcal{P} \in \mathrm{Ap}(\Delta_{m-1})$ where $\Delta_{m-1} = \{\mathbf{g}_1, \ldots, \mathbf{g}_{m-1}\}$.

(c) Define $\Psi_s := \mathrm{RES}_{x_{i_s}}(\Psi_{s+1}, \mathbf{g}_s)$ the Sylvester resultant in the variable $x_{i_s} = \mathrm{class}(\mathbf{g}_s)$ inductively for $s = m, \ldots, 1$. (We assume that Ψ_{s+1} is in reduced form modulo Δ_s.) Then $\Psi_1 \in \Bbbk[\bar{x}, y]$, where $\bar{x} = \{x_i \mid i \neq i_s,\ 1 < s \leq m\}$ and Ψ_1 is not identically zero.

(d) Let Ψ_1 be as above. There exists $a \in \Bbbk$ such that $\Psi_1(\bar{x}, a)$ is not identically zero.

(e) Let a be as above. Then $h := \Psi_{m+1}(\vec{x}, a)$ is in general position.

Proof:

$(a) \Rightarrow (b)$: Suppose that for some $\mathcal{P} \in \mathrm{Ap}(\Delta_{m-1})$

$$d := \mathrm{gcd}_{\mathbf{K}_{R_m}(\mathcal{P})}(\mathbf{g}_m, f_0, \ldots f_k)$$

is a polynomial in $\mathbf{K}_{R_m}(\mathcal{P})[x_{i_m}]$, and has positive degree in x_{i_m}. Lemma 3.1.3 implies that there exists $d' \in \Bbbk[x_1, \ldots, x_{i_m}]$ such that $\mathrm{lc}(d') \notin \mathcal{P}$ and the monic image of d' in $\mathbf{K}_{R_m}(\mathcal{P})[x_{i_m}]$ is d. Then the ideal $\mathrm{Rep}(\mathcal{P} \cup \{d'\})$ is unmixed of codimension

m, since $\operatorname{codim}(\mathcal{P}) = m - 1$. This is a contradiction, since $\operatorname{Rep}(\Delta) \cup \{f_0, \ldots f_k\} \subset \operatorname{Rep}(\mathcal{P} \cup \{d'\})$, therefore $V(\operatorname{Rep}(\mathcal{P} \cup \{d'\})) \subset V(\Delta) \cap V(F)$ which has codimension $m + 1$ by (a).

$(b) \Rightarrow (c)$: By (b) and Lemma 3.1.2 we have

$$1 = \gcd_{\mathbf{K}_{R_m}(\mathcal{P}_{m-1})}(\mathrm{g}_m, f_0, \ldots f_k) = \gcd_{\mathbf{K}_{R_m}(\mathcal{P}_{m-1})(y)}(\mathrm{g}_m, \Psi_{m+1})$$

for all $\mathcal{P}_{m-1} \in \operatorname{Ap}(\Delta_{m-1})$. We can assume that Ψ_{m+1} is reduced modulo Δ, since the pseudo-reduction by Δ does not change the gcd over $\mathbf{K}(\mathcal{P})$. (Note that we need the polynomials to be reduced in order to get a better degree bound and complexity.) Therefore, the Sylvester resultant of g_m and Ψ_{m+1} is not 0 modulo $\mathcal{P}_{m-1}$ for any $\mathcal{P}_{m-1} \in \operatorname{Ap}(\Delta_{m-1})$, also by Lemma 3.1.2. Thus $1 = \gcd_{\mathbf{K}_{R_{m-1}}(\mathcal{P}_{m-2})}(\mathrm{g}_{m-1}, \Psi_m)$ for all $\mathcal{P}_{m-2} \in \operatorname{Ap}(\Delta_{m-2})$. By induction on m we can show that $\gcd_{\mathbf{k}(x_1, \ldots x_{i_1-1})}(\mathrm{g}_1, \Psi_2) = 1$, therefore $\Psi_1 = \operatorname{RES}_{x_{i_1}}(\mathrm{g}_1, \Psi_2) \not\equiv 0$, which proves the first part of the claim. The variables occurring in Ψ_1 are as in the claim, which follows directly from the definition of Ψ_i, $1 \leq i \leq m + 1$.

$(c) \Leftrightarrow (d)$ True, since $|\Bbbk| = \infty$. The next proposition will give an upper bound for the cardinality of a set which contains such an a.

$(d) \Rightarrow (e)$: Since $\Psi_1(\bar{x}, a) = \operatorname{RES}_{x_{i_1}}(\mathrm{g}_1, \Psi_2|_{y=a}) \not\equiv 0$, we have by Lemma 3.1.2 that $\gcd_{\mathbf{k}(x_1, \ldots x_{i_1-1})}(\mathrm{g}_1, \Psi_2|_{y=a}) = 1$, therefore $\Psi_2|_{y=a} \notin \mathcal{P}_1$ for all $\mathcal{P}_1 \in \operatorname{Ap}(\{\mathrm{g}_1\})$ by Lemma 3.1.4. By induction on m we get that $\Psi_m|_{y=a} = \operatorname{RES}_{x_{i_m}}(\mathrm{g}_m, \Psi_{m+1}(\vec{x}, a)) \notin \mathcal{P}_{m-1}$ for any $\mathcal{P}_{m-1} \in \operatorname{Ap}(\Delta_{m-1})$. Therefore

$$\gcd_{\mathbf{K}_{R_m}(\mathcal{P}_{m-1})}(\mathrm{g}_m, h) = \gcd_{\mathbf{K}_{R_m}(\mathcal{P}_{m-1})(y)}(\mathrm{g}_m, \Psi_{m+1}|_{y=a}) = 1$$

for all $\mathcal{P}_{m-1} \in \operatorname{Ap}(\Delta_{m-1})$, which implies that $h \notin \mathcal{P}$ for any $\mathcal{P} \in \operatorname{Ap}(\Delta)$, so

h properly intersects every irreducible component of Δ, therefore h is in general position.

$(e) \Rightarrow (a)$: True, since $V(\Delta) \cap V(\mathcal{P}) \subseteq V(\Delta) \cap V(h)$. ■

Proposition 3.6.2 *Let* $F = \{f_1, \ldots, f_k\}$ *and* $\Delta = \{\mathrm{g}_1, \ldots, \mathrm{g}_m\}$ *as above. Assume that* $\mathrm{class}(\mathrm{g}_s) = x_{i_s}$ *for* $1 \leq s \leq m$. *Then for any* $S \subset \Bbbk$ *and*

$$|S| \geq k(\prod_{s=1}^{m} \deg_{x_{i_s}}(\mathrm{g}_s)) + 1$$

there must be $a \in S$ *such that*

$$h = f_k a^k + f_{k-1} a^{k-1} + \ldots + f_0$$

is in general position with respect to Δ.

Proof: Consider $\Psi_{m+1}, \ldots, \Psi_1$ defined above. Then by Proposition 3.6.1, h is in general position if and only if $\Psi_1(\bar{x}, a)$ is not identically zero. Since Ψ_s is the determinant of the Sylvester matrix in the variable x_{i_s} of the polynomials g_s and Ψ_{s+1} and $\deg_{x_{i_s}}(\Psi_{s+1}) < \deg_{x_{i_s}}(\mathrm{g}_s)$ because we assumed that Ψ_{s+1} is reduced modulo Δ_s, we have that

$$\begin{aligned} \deg_y(\Psi_1) &= \deg_y(\Psi_2) \cdot \deg_{x_{i_1}}(\mathrm{g}_1) \\ &= \deg_y(\Psi_{m+1}) \prod_{s=1}^{m} \deg_{x_{i_s}}(\mathrm{g}_s) \\ &= k(\prod_{s=1}^{m} \deg_{x_{i_s}}(\mathrm{g}_s)). \end{aligned}$$

Thus, if $S \subset \Bbbk$ and $|S| \geq k(\prod_{s=1}^{m} \deg_{x_{i_s}}(\mathrm{g}_s)) + 1$, then there must be $a \in S$ such that $\Psi_1(\bar{x}, a)$ is not identically zero. ■

To compute a polynomial h in general position with respect to Δ, we can use either a randomized Las Vegas approach or a deterministic approach. In the randomized approach we choose a random integer $0 \leq a \leq k(\prod_{s=1}^{m} \deg_{x_{i_s}}(\mathbf{g}_s))$ and compute

$$h = f_k a^k + f_{k-1} a^{k-1} + \ldots + f_0.$$

By computing the polynomial $\Psi_1(\bar{x}, a)$ defined in Proposition 3.6.1 part (c), we can check if a satisfies $\Psi_1(\bar{x}, a) \not\equiv 0$. We can derandomize this method by trying all the numbers in $S = \{a \in \mathbb{N} \mid 0 \leq a \leq k(\prod_{s=1}^{m} \deg_{x_{i_s}}(\mathbf{g}_s))\}$ in the worst case.

Theorem 3.6.3 *Let $\Delta = \{\mathbf{g}_1, \ldots, \mathbf{g}_m\} \subset \Bbbk[x_1, \ldots, x_n]$ be an unmixed set of codimension m and $F = \{f_0, \ldots, f_k\} \subset \Bbbk[x_1, \ldots, x_n]$ be a finite set of polynomials. Let $\Psi_1 \in \Bbbk[\bar{x}, y]$ be the polynomial defined in Proposition 3.6.1 part (c). Then*

$$\text{height}(\Psi_1) \leq (\prod_{s=1}^{m} d_s \log(d_s))(\text{height}(\Delta, f) + \Upsilon) \tag{3.31}$$

where Υ is an upper bound of the structure constants of the algebras $\mathcal{A}(\Delta)$ and $\text{height}(\Delta, f)$ is the maximum of the heights of the polynomials in the set $\Delta \cup \{f_0, \ldots, f_k\}$. Moreover, the arithmetic circuit over $\Bbbk$ computing $\Psi_1 \in \Bbbk[\bar{x}, a]$ for any given $a \in \Bbbk$ has depth at most

$$\leq \quad m(n-m) \log^4(D) \log(k) \log(\text{height}(\Delta, f)) \tag{3.32}$$

and size at most

$$\leq \quad mkD^4(D^3 \text{height}(\Delta, f))^{2(n-m)} \tag{3.33}$$

where D is the dimension of the algebra $\mathcal{A}(\Delta)$.

Remark: The randomized version of the algorithm $\mathbf{general}_{\mathbf{n}}^{\mathbf{m}}(\Delta, F)$ has the same complexity as in (3.32) and (3.33). On the other hand, the deterministic circuit computing $\mathbf{general}_{\mathbf{n}}^{\mathbf{m}}(\Delta, F)$ has depth (3.32) and size kD times (3.33).

Proof: Denote $\deg_{x_{i,s}}(\mathbf{g}_s)$ by d_s and the height of the structure constants of $\mathcal{A}(\Delta_s)$ by Υ_s for $1 \leq s \leq m$. For each $s = m+1, \ldots, 1$ we compute Ψ_s defined in Proposition 3.6.1 part (c), using arithmetic circuits over the ring $\mathcal{A}(\Delta_{s-1})$. Using Proposition 3.3.1 we get the following upper bound for the heights of the polynomials occurring in the computation of $\Psi_1(\bar{x}, a)$:

$$\begin{aligned}
\text{height}(\Psi_1) &\leq d_1 \log(d_1)(\text{height}(\Psi_2) + \text{height}(\mathbf{g}_1)) \\
&\leq d_1 \log(d_1) d_2 \log(d_2)(\text{height}(\Psi_3) + \text{height}(\mathbf{g}_2) + \Upsilon_1) \\
&\quad + d_1 \log(d_1)\text{height}(\mathbf{g}_1) \\
&\vdots \\
&\leq (\prod_{s=1}^{m} d_s \log(d_s))\text{height}(\Psi_{m+1}) \\
&\quad + \sum_{s=1}^{m}(\text{height}(\mathbf{g}_s) + \Upsilon_{s-1}) \prod_{t=1}^{s-1} d_t \log(d_t) \\
&\leq (\prod_{s=1}^{m} d_s \log(d_s))(\text{height}(\Delta, f) + \Upsilon)
\end{aligned}$$

which proves (3.31).

The depth of the arithmetic circuit over k computing Ψ_1 is at most

$$\begin{aligned}
& \sum_{s=m+1}^{1} \text{Depth(computation of } \Psi_s) + \text{Depth(reduction of } \Psi_s) \\
\leq\ & (n-m)\log(D)\log(k)\log(\text{height}(f) \\
& + \sum_{s=m}^{1} c_1(n-m)\log(D)\log^2(d_s)\log(D^2\text{height}(\Delta, f)) \\
\leq\ & O(m(n-m)\log^4(D)\log(k)\log(\text{height}(\Delta, f)))
\end{aligned}$$

using the result in [Ber84] for the complexity of computing the determinant over arbitrary rings. The size of the arithmetic circuit computing Ψ_1 is at most

$$\begin{aligned}
& \sum_{s=m+1}^{1} \text{Size(computation of } \Psi_s) + \text{Size(reduction of } \Psi_s) \\
\leq\ & kD^3(\text{height}(f))^{2(n-m)} + \sum_{s=m}^{1} c_2 D^3 d_s (d_s \text{height}(\Psi_{s+1}))^{2(n-m)} \\
\leq\ & kD^3(\text{height}(f))^{2(n-m)} + \sum_{s=m}^{1} c_2 D^3 d_s (d_s D^2 \text{height}(\Delta, f)))^{2(n-m)} \\
\leq\ & O(mkD^4(D^3\text{height}(\Delta, f))^{2(n-m)}).
\end{aligned}$$

■

Chapter 4

Computing the unmixed representation

In this chapter we present an improved version of Kalkbrener's decomposition algorithm for finding an unmixed representation of a radical ideal, and we give subexponential complexity bounds. First we discuss multivariate resultant methods which we apply to compute polynomials in the radical with as few variables as possible. We eliminate multiple variables simultaneously from a system of polynomials using multivariate resultants, assuming that the components of the algebraic set corresponding to the polynomial system are "proper", i.e. their codimension equals the number of polynomials in the system. Moreover, we present a method which also works without assuming that the algebraic set contains only proper components.

Using the multivariate resultant methods described in Section 4.1 we are able to compute a triangular representation of an algebraic set which contains our orig-

inal algebraic set. We can eliminate the superfluous and multiple roots using a decomposition technique called **unmixed** described in Section 4.2. The algorithm is a generalization of the sub-resultant method for finding the gcd of several univariate polynomials described in [IK93, chapter 15.2] and the univariate square-free factorization method described in [BKR85].

4.1 Multivariate resultant method

Let $F = \{f_0, \ldots, f_k\} \subset \Bbbk[x_1, \ldots, x_n]$ be a set of polynomials. In the next sections we propose an algorithm which computes unmixed sets $\Delta_1, \ldots, \Delta_r \subset \Bbbk[x_1, \ldots, x_n]$ such that

$$V(F) = \bigcup_{i=1}^{r} V_{\mathrm{Rep}}(\Delta_i) \subset \mathbb{A}^n$$

or equivalently

$$\sqrt{\langle F \rangle} = \bigcap_{i=1}^{r} \mathrm{Rep}(\Delta_i)$$

based on multivariate resultant and decomposition techniques.

First we present a brief description of the theory of multivariate resultants, together with the application to our problem.

For given numbers $m, d > 0$ consider the over-constrained system of generic

homogeneous equations

$$p_0 := \sum_{\alpha \in \Omega_{m,d}} c_{0,\alpha} \mathbf{x}^\alpha$$

$$\vdots$$

$$p_m := \sum_{\alpha \in \Omega_{m,d}} c_{m,\alpha} \mathbf{x}^\alpha$$

where $\Omega_{m,d} := \{(\alpha_0, \ldots, \alpha_m) \in \mathbb{N}^{m+1} \mid \sum_{j=0}^{m} \alpha_j = d\}$. We denote $\mathbf{x}^\alpha = x_0^{\alpha_0} \cdots x_m^{\alpha_m}$. The $c_{i,\alpha}$-s are symbols for generic coefficients. Note that $|\Omega_{m,d}| = \binom{m+d}{d}$.

Then there exists a polynomial

$$\mathfrak{R}_{m,d}(c_{i,\alpha}) \in \mathbb{Z}[c_{i,\alpha} \,:\, 0 \leq i \leq m,\ \alpha \in \Omega_{m,d}]$$

such that for all $(\bar{c}_{i,\alpha}) \in \mathbf{K}^{(m+1)\binom{m+d}{d}}$

$$\mathfrak{R}_{m,d}(\bar{c}_{i,\alpha}) = 0 \quad \Leftrightarrow \quad V(\bar{p}_0, \ldots, \bar{p}_m) \neq \emptyset \subset \mathbb{P}^m$$

where $\bar{p}_i := \sum_{\alpha \in \Omega_{m,d}} \bar{c}_{0,\alpha} \mathbf{x}^\alpha$ for $0 \leq i \leq m$. For a particular system $\bar{P} = \{\bar{p}_0, \ldots \bar{p}_m\}$ with coefficients $(\bar{c}_{i,\alpha})$, the polynomial $\mathfrak{R}_{m,d}(\bar{c}_{i,\alpha})$ is called the *resultant* of the system $\bar{P}$. These facts were originally proved by Macaulay [Mac16].

To compute the multivariate resultant $\mathfrak{R}_{m,d}(\bar{c}_{i,\alpha})$ corresponding to a given system, we refer to the method in [IK93][Theorem 15.3]. They express $\mathfrak{R}_{m,d}(\bar{c}_{i,\alpha})$ as the quotient of two determinants, each of them corresponding to a matrix of size at most d^m and with entries either 0 or the coefficients $\bar{c}_{i,\alpha}$. Assume that the coefficients $\bar{c}_{i,\alpha}$ are elements of a ring R. They show that $\mathfrak{R}_{m,d}(\bar{c}_{i,\alpha})$ can be computed using only ring operations in R, and the arithmetic circuit over R computing $\mathfrak{R}_{m,d}$ has depth $O(m^2 \log^2(d))$ and size $O(d^{3.5m})$. Moreover, since the computation uses only ring

operations on the coefficients, the calculation commutes with substitution. Also, the resultant $\Re_{m,d}(\bar{c}_{i,\alpha})$ is homogeneous of degree d^m in the coefficients of each $\bar{p}_i$ for $0 \leq i \leq m$ [vdW49][II. Chapter 82].

Multivariate resultants generalize the notion of Sylvester resultants. Similarly as the Sylvester resultant is applied to eliminate a variable from a system of two equations, we will use multivariate resultants to eliminate more variables simultaneously from a system of equations as follows.

Consider the set $F = \{\mathbf{f}_0, \ldots, \mathbf{f}_m\} \subset \Bbbk[x_1, \ldots, x_{m+1}]$ containing $m+1$ polynomials in $m+1$ variables, and assume that $V(F)$ is a finite set in the affine space $\mathbb{A}^{m+1}$. We will show how to eliminate the first m variables using multivariate resultants, i.e. we compute a polynomial $\Re(x_{m+1})$ such that for all $z_{m+1} \in \bar{\mathbf{K}}$

$$\Re(z_{m+1}) = 0 \iff \exists z_1 \ldots z_m \in \bar{\mathbf{K}} : \ (z_1, \ldots, z_{m+1}) \in V(F) \subset \mathbb{A}^{m+1}.$$

To achieve this goal we need a stronger assumption then the finiteness of $V(F) \subset \mathbb{A}^m$. Later we will show how to eliminate this stronger assumption. Informally, the stronger assumption is that the polynomials in F have finitely many common roots also at infinity.

More formally, consider each $\mathbf{f}_i \in F$ as a polynomial in m variables with coefficients from $\Bbbk[x_{m+1}]$, i.e.

$$\mathbf{f}_i = \sum_{\beta \in \mathbf{N}^m} f_{i,\beta}(x_{m+1}) \bar{\mathbf{x}}^\beta, \ \ 0 \leq i \leq m$$

where $\bar{\mathbf{x}}^\beta$ denotes the monomial $x_1^{\beta_1} \cdots x_m^{\beta_m}$ for $\beta = (\beta_1, \ldots, \beta_m) \in \mathbb{N}^m$. Let x_0 be a new variable, and let d be the maximum of the total degrees of the polynomials

$\mathbf{f}_i$ in the variables $x_1, \ldots, x_m$. Denote by $\mathbf{f}_i^h$ the polynomial we get from $\mathbf{f}_i$ by homogenizing each term with x_0, i.e.

$$\mathbf{f}_i^h := \sum_{\beta \in \mathbb{N}^m} f_{i,\beta}(x_{m+1}) \tilde{\mathbf{x}}^\beta x_0^{\beta_0} = \sum_{\alpha \in \Omega_{m,d}} f_{i,\alpha}(x_{m+1}) \mathbf{x}^\alpha,$$

where $\beta_0 = d - \sum_{j=1}^m \beta_j$ and $\alpha = (\beta_0, \ldots, \beta_m)$. The stronger assumption is that the ideal $\langle \mathbf{f}_0^h, \ldots \mathbf{f}_m^h \rangle \subset \Bbbk[x_0, \ldots, x_{m+1}]$ is also zero dimensional.

Since the polynomials $\mathbf{f}_0^h, \ldots \mathbf{f}_m^h$ are homogeneous of degree d in $m+1$ variables over $\Bbbk(x_{m+1})$, we can compute the value of the resultant $\mathfrak{R}_{m,d}(f_{i,\alpha}(z_{m+1})) \in \mathbf{K}$ for every fixed $z_{m+1} \in \mathbf{K}$. We saw above that

$$\begin{aligned} & \mathfrak{R}_{m,d}(f_{i,\alpha}(z_{m+1})) = 0 \iff V(\mathbf{f}_0^h(z_{m+1}), \ldots \mathbf{f}_m^h(z_{m+1})) \neq \emptyset \subset \mathbb{P}^m \\ \iff & \exists (z_0, \ldots z_m) \in \mathbb{P}^m : \quad (z_0, \ldots, z_{m+1}) \in V(\mathbf{f}_0^h, \ldots \mathbf{f}_m^h) \subset \mathbb{P}^m \times \mathbb{A}^1. \end{aligned}$$

Now consider the polynomial

$$\mathfrak{R}(x_{m+1}) := \mathfrak{R}_{m,d}(f_{i,\alpha}(x_{m+1})) \in \Bbbk[x_{m+1}].$$

We get the following implications:

$$\begin{aligned} (z_1, \ldots z_{m+1}) \in V(F) \iff & \exists z_0 \neq 0 : \quad (z_0, z_1, \ldots z_{m+1}) \in V(\mathbf{f}_0^h, \ldots \mathbf{f}_m^h) \in \mathbb{P}^m \times \mathbb{A}^1 \\ \implies & V(\mathbf{f}_0^h(z_{m+1}), \ldots \mathbf{f}_m^h(z_{m+1})) \neq \emptyset \subset \mathbb{P}^m \\ \implies & \mathfrak{R}(z_{m+1}) = \mathfrak{R}_{m,d}(f_{m,\alpha}(z_{m+1})) = 0. \end{aligned}$$

Also, since $V(\mathbf{f}_0^h, \ldots \mathbf{f}_m^h) \in \mathbb{P}^m \times \mathbb{A}^1$ is a finite set, there exists $\bar{z}_{m+1}$ such that $\forall (z_0, z_1, \ldots z_m)$ the points $(z_0, \ldots, z_m, \bar{z}_{m+1}) \notin V(\mathbf{f}_0^h, \ldots \mathbf{f}_m^h)$, therefore, $\mathfrak{R}(\bar{z}_{m+1}) \neq 0$ which implies that $\mathfrak{R}(x_{m+1})$ is not identically zero. Unfortunately, the presence of a

higher dimensional component of the solution set in $\mathbb{P}^n \times \mathbb{A}^1$ causes the polynomial $\Re$ to vanish identically, thus causes the above method to fail.

Next we describe the above method in a slightly more general setting than above. Instead of computing the 0-dimensional components over the field $\Bbbk$, we extend the computation to the function field $\Bbbk(y_1, \ldots, y_l)$ and by this we are able to compute the $l-1$ dimensional components over $\Bbbk$.

Assume that we are given the system F^h consisting of

$$\begin{aligned} \mathbf{f}_0^h &= \sum_{\alpha \in \Omega_{m,d}} f_{0,\alpha}(\mathbf{y})\mathbf{x}^\alpha, \\ &\vdots \\ \mathbf{f}_m^h &= \sum_{\alpha \in \Omega_{m,d}} f_{m,\alpha}(\mathbf{y})\mathbf{x}^\alpha, \end{aligned}$$

homogeneous polynomials in the variables $\mathbf{x} = (x_0, \ldots, x_m)$, where $f_{s,\alpha}(\mathbf{y})$ are polynomials in the variables $\mathbf{y} = (y_1, \ldots, y_l)$. Then every component in the algebraic set $V(\mathbf{f}_0^h, \ldots, \mathbf{f}_m^h) \subset \mathbb{P}^m \times \mathbb{A}^l$ has dimension at least $(m+l)-(m+1) = l-1$. The components of dimension $l-1$ are called *proper*. The higher dimensional components are called *excess* components. By the same argument as above, in the case of no excess components, we can compute the polynomial

$$\Re(\mathbf{y}) := \Re_{m,d}(f_{i,\alpha}(\mathbf{y})) \tag{4.1}$$

not identically zero such that for all $(\bar{y}_1, \ldots, \bar{y}_l) \in \mathbb{A}^l$

$$V(\mathbf{f}_0^h(\bar{\mathbf{y}}), \ldots, \mathbf{f}_m^h(\bar{\mathbf{y}})) \neq \emptyset \subset \mathbb{P}^m \iff \Re(\bar{\mathbf{y}}) = 0.$$

To see that $\Re(\mathbf{y})$ is not identically zero if all the components of $V(F^h) \subset \mathbb{P}^m \times \mathbb{A}^l$ have dimension $l-1$, observe that defining the projection

$$\pi : (\mathbf{x}, \mathbf{y}) \mapsto (\mathbf{y}),$$

$\pi(V(F^h)) \subset \mathbb{A}^l$ has dimension at most $l-1$. Hence,

$$\exists \bar{\mathbf{y}} \in \mathbb{A}^l - \pi(V(F^h))$$

which implies that $\Re(\bar{\mathbf{y}}) \neq 0$.

Corollary 4.1.1 *Let*

$$F = \{\mathbf{f}_0, \ldots, \mathbf{f}_m\} \subset \Bbbk[x_1, \ldots, x_m, y_1, \ldots, y_l]$$

and define $F^h = \{\mathbf{f}_0^h, \ldots, \mathbf{f}_m^h\} \subset \Bbbk[\mathbf{x}, \mathbf{y}]$ *homogeneous polynomials in the variables* $\mathbf{x}$ *deriving from* F *after homogenization by* x_0. *Assume that* $V(F^h) \subset \mathbb{P}^m \times \mathbb{A}^l$ *contains only proper components. If* $\Re \in \Bbbk[\mathbf{y}]$ *is the resultant of the system* F^h *defined in (4.1) then for any* $(\bar{x}_1, \ldots, \bar{x}_m, \bar{y}_1, \ldots, \bar{y}_l) \in \mathbb{A}^{m+l}$

$$(\bar{x}_1, \ldots, \bar{x}_m, \bar{y}_1, \ldots, \bar{y}_l) \in V(F) \Longrightarrow V(\mathbf{f}_0^h(\bar{\mathbf{y}}), \ldots, \mathbf{f}_m^h(\bar{\mathbf{y}})) \neq \emptyset \Longleftrightarrow \Re(\bar{\mathbf{y}}) = 0;$$

in other words, $V(F) \subseteq V(\Re) \subsetneq \mathbb{A}^{m+l}$.

Moreover, assume that the degrees of the polynomials in F *are less than* d *for all variables* $\mathbf{x}, \mathbf{y}$. *Then*

$$\deg_{y_i}(\Re) \leq d^m \deg_{y_i}(F) \leq d^{(m+1)}. \tag{4.2}$$

Proof: It only remains to prove the degree bounds. The degree bound (4.2) follows from the fact that the resultant $\mathfrak{R}_{m,d}$ of a system of polynomials is homogeneous of degree d^m in the (indeterminate) coefficients of the polynomials in the system, as noted above. ■

Next we show how to eliminate the stronger assumption of $V(F^h)$ consisting only of proper components. We use a certain version of techniques widely used in numeric computations for approximating roots of polynomial systems, known collectively as homotopy methods. Canny in [Can90] developed a construction based on a generalization of the characteristic polynomial of linear systems to polynomial systems. Ierardi in [Ier89] derived the same construction by adapting the homotopy method for symbolic computations.

Using Canny's *generalized characteristic polynomial* method allows the resultant method described above to succeed even in the presence of an excess component, and it does not matter whether the excess components are at infinity or elsewhere. We obtain the projection of all isolated proper components in the solution set.

The underlying idea of the generalized characteristic polynomial method is the following. Instead of the polynomial system $F^h = \{\mathbf{f}_0^h, \ldots \mathbf{f}_m^h\}$, consider the per-

turbed system $\hat{F}(t)$ consisting of the polynomials

$$\begin{aligned}\hat{\mathbf{f}}_0(t,\mathbf{x},\mathbf{y}) :=&\ (1-t)\mathbf{f}_0^h(\mathbf{x},\mathbf{y}) + tx_0^d = \sum_{\alpha\in\Omega_{d,m}} \hat{f}_{0,\alpha}(t,\mathbf{y})\mathbf{x}^\alpha \\ &\vdots \\ \hat{\mathbf{f}}_m(t,\mathbf{x},\mathbf{y}) :=&(1-t)\mathbf{f}_0^h(\mathbf{x},\mathbf{y}) + tx_m^d = \sum_{\alpha\in\Omega_{d,m}} \hat{f}_{m,\alpha}(t,\mathbf{y})\mathbf{x}^\alpha,\end{aligned} \tag{4.3}$$

where $\mathbf{x} = (x_0,\ldots,x_m)$, $\mathbf{y} = (y_1,\ldots,y_l)$ as before, and t is a complex variable. Now consider the resultant corresponding to $\hat{F}(t)$, i.e. define

$$\hat{\mathfrak{R}}(t,\mathbf{y}) := \mathfrak{R}_{m,d}(\hat{f}_{m,\alpha}(t,\mathbf{y})).$$

Write

$$\hat{\mathfrak{R}}(t,\mathbf{y}) = \sum_{i=0}^{D} \hat{\mathfrak{R}}_i(\mathbf{y})t^i$$

as a polynomial in t, and define

$$\hat{\mathfrak{R}}(\mathbf{y}) := \hat{\mathfrak{R}}_k(\mathbf{y}) = \lim_{t\to 0} \hat{\mathfrak{R}}(t,\mathbf{y}) \tag{4.4}$$

where k is the first non-zero coefficient of $\hat{\mathfrak{R}}(t,\mathbf{y})$ in the variable t.

Proposition 4.1.2 (Canny) *Let F, $\hat{F}(t)$, $\hat{\mathfrak{R}}(t,\mathbf{y})$ and $\hat{\mathfrak{R}}(\mathbf{y})$ as above. Then*

1. *$\hat{\mathfrak{R}}(t,\mathbf{y})$ is not identically zero.*
2. *Let $X \subset V(F) \subset \mathbb{A}^{m+l}$ be a proper irreducible component of $V(F)$, i.e. the dimension of X is $l-1$. Then $X \subset V(\hat{\mathfrak{R}}(\mathbf{y})) \subset \mathbb{A}^{m+l}$.*

Proof:

1. To prove that $\hat{\mathfrak{R}}(t, \mathbf{y})$ is not identically zero, simply observe that for $t = 1$ we have $\hat{F}(1) = \{x_0^d, \ldots, x_m^d\}$, therefore $V(\hat{F}(1)) \subset \mathbb{P}^m \times \mathbb{A}^l$ is the empty set, thus $\hat{\mathfrak{R}}(1, \mathbf{y}) \neq 0$.

2. With the addition of the complex variable t, the algebraic set $Z := V(\hat{F}(t))$ lies in $\mathbb{P}^m \times \mathbb{A}^l \times \mathbb{C}$. Since $V(F) = V(\hat{F}(0))$, the intersection of Z with the $t = 0$ hyperplane is $V(F) \times \{0\} \subset Z$. Since $\hat{F}(t)$ consist of $m+1$ polynomials, all the components of Z have dimension at least $(m + l + 1) - (m + 1) = l$.

   Let $X \subset V(F)$ be a component such that the dimension of X is $l - 1$. Since $X \times \{0\} \subset Z$, there exists an irreducible component $\hat{X}$ of Z such that $X \times \{0\} \subset \hat{X}$. But

$$\dim(\hat{X}) \geq l > l - 1 = \dim(X \times \{0\}),$$

   therefore for every point $p_0 \in X \times \{0\}$ there is a sequence of points $(p_i)_{i>0} \subset Z - V(F)$ such that $\lim_{i\to\infty} p_i = p_0$. Also, $p_i \in Z - \{0\}$, since $Z \cap \{0\} = V(F)$. Denote the coordinates of the points p_i by $(\mathbf{x}_i, \mathbf{y}_i, t_i)$ for $i \geq 0$. Since $p_i \in Z$ we have that

$$0 = \hat{\mathfrak{R}}(t_i, \mathbf{y}_i) = \sum_{j=k}^{D} \hat{\mathfrak{R}}_j(\mathbf{y}_i) t_i^j$$

   for $i \geq 0$. Since $t_i \neq 0$ for $i > 0$, we can divide by t_i^k, and get that

$$0 = \hat{\mathfrak{R}}_k(\mathbf{y}_i) + \sum_{j=k+1}^{D} \hat{\mathfrak{R}}_j(\mathbf{y}_i) t_i^{j-k}$$

   for $i > 0$. Since $\lim_{i\to\infty}(\mathbf{y}_i, t_i) = (\mathbf{y}_0, t_0)$, $t_0 = 0$, and both sides of the above equation are continuous in the variables $\mathbf{y}$ and t, by taking the limits $i \to \infty$ we get that

$$0 = \hat{\mathfrak{R}}_k(\mathbf{y}_0) + 0 = \hat{\mathfrak{R}}(\mathbf{y}_0).$$

Hence for all $p_0 \in X$, $p_0 \in V(\Re)$, which proves the claim. ■

Next we show how to proceed if the number of polynomials in the system F is larger than the codimension of its components. Let $F = \{\mathbf{f}_0, \ldots, \mathbf{f}_k\} \subset \Bbbk[x_1, \ldots, x_n]$, $l \geq 0$, and $m := n - l$. We aim to find a projection of all the $l-1$ dimensional components of $V(F)$. To apply the homotopy method described above, we have to find a sequence F' of $n-(l-1) = m+1$ elements in $\langle F \rangle$ such that all the $l-1$ dimensional components of $V(F)$ are also (not embedded) components of $V(F')$. We will use a randomized approach applying the following lemma.

Lemma 4.1.3 *Let $F = \{\mathbf{f}_0, \ldots, \mathbf{f}_k\}$, $l \geq 0$ and m be as above. Denote by $V_{l-1}(F)$ the union of the dimension $l-1$ irreducible components of $V(F) \subset \mathbb{A}^n$. Let $S \subset \Bbbk$ be a finite set, and let $\{a_i \mid 0 \leq i \leq m\} \subset S$ be random values uniformly chosen from S. Then for the system F' of polynomials*

$$\mathbf{f}'_0 := \sum_{j=0}^{k} a_0^j \mathbf{f}_i, \quad \ldots, \quad \mathbf{f}'_m := \sum_{j=0}^{k} a_m^j \mathbf{f}_i \tag{4.5}$$

we have that

$$V_{l-1}(F) \subseteq V_{l-1}(F')$$

with probability at least

$$1 - \frac{k \cdot d^{m+1}}{|S|},$$

where d is the maximum degree of the polynomials in F.

Proof: We use the idea of the proof of [Ier89, Lemma 5.5]. Assume that we

have constructed the set of polynomials

$$F'_s := \{\mathbf{f}'_0 = \sum_{j=0}^{k} a_0^j \mathbf{f}_i, \ \ldots, \ \mathbf{f}'_s := \sum_{j=0}^{k} a_m^j \mathbf{f}_i\} \tag{4.6}$$

for some $0 \leq s < m$ such that every irreducible component of $V(F'_s)$ of codimension less than s is a component of $V(F)$. Therefore, all the components of $V(F'_s)$ which are not components of $V(F)$ have codimension s. Note that $V(F'_s)$ has at most d^s irreducible components (see e.g. [Ier89, Lemma 2.20]). This implies that there exists a set of points

$$P_s \subset \mathbb{A}^n \qquad |P_s| \leq d^s$$

such that if $X \subseteq V(F'_s)$ is not a component of $V(F)$ then there exists $p \in P_s$ such that $p \in X$ but $p \notin V(F)$.

To construct $\mathbf{f}'_{s+1}$ consider the polynomials in the variable y:

$$\sum_{j=0}^{k} y^j \mathbf{f}_j(p) \in \mathbf{K}[y] \quad p \in P_s.$$

By the definition of P_s none of the polynomials above are identically zero. Therefore, if $a_{s+1} \in S$ is a random element uniformly chosen from S then $\sum_{j=0}^{k} a_{s+1}^j \mathbf{f}_j(p) = 0$ for some $p \in P_s$ with probability at most $\frac{d^s \cdot k}{|S|}$, using Schwartz's lemma [Sch80]. Hence, defining

$$\mathbf{f}'_{s+1} := \sum_{j=0}^{k} a_{s+1}^j \mathbf{f}_j \in \mathbb{k}[x_1, \ldots, x_n]$$

we have that $\mathbf{f}'_{s+1}(p) \neq 0$ for all $p \in P_s$ with probability at least $1 - \frac{d^s \cdot k}{|S|}$. This implies that if $F'_{s+1} := F'_s \cup \{\mathbf{f}'_{s+1}\}$ then every irreducible component of $V(F'_{s+1})$ of codimension less than $s+1$ is a component of $V(F)$. The claim of the lemma follows

by induction on s. ■

Now we are able to summarize the results of this section.

Theorem 4.1.4 *Let $F = \{\mathbf{f}_0, \ldots, \mathbf{f}_k\} \subset \Bbbk[x_1, \ldots, x_n]$. Then for any $0 < l \leq n$ and for any set of indices*

$$\Im := \{i_1 < \cdots < i_l\} \subseteq \{1, \ldots, n\},$$

we can compute a polynomial

$$\Re_\Im \in \Bbbk[x_{i_1}, \ldots, x_{i_l}]$$

not identically zero, such that if $X \subset V(F) \subset \mathbb{A}^n$ is an irreducible component of dimension $l-1$ with prime ideal $\mathcal{P} \subset \Bbbk[x_1, \ldots, x_n]$ then

$$X \subset V(\Re_\Im) \subsetneq \mathbb{A}^n, \quad \textit{i.e. } \Re_\Im \in \mathcal{P} \cap \Bbbk[x_{i_1}, \ldots, x_{i_l}].$$

Moreover, assume that the degrees of the polynomials in F are bounded by d for all variables $x_1, \ldots, x_n$. Then for all $i_j \in \Im$ we have

$$\deg_{x_{i_j}}(\Re_\Im) \leq d^{(n-l)} \cdot \deg_{x_{i_j}}(F) \leq d^{(n-l+1)}.$$

For any polynomial h occurring in the computation,

$$\deg_{x_{i_j}}(h) \leq d^{2(n-l)} \deg_{x_{i_j}}(F) \leq d^{2(n-l)+1}. \tag{4.7}$$

Furthermore $\Re_\Im$ can be computed with an arithmetic circuit over $\Bbbk$ in depth

$$O((n-l)^2 l \log^3(d))$$

and size

$$O(d^{6(n-l)(l+1)}).$$

Remark: For isolated zero-dimensional components of an algebraic set we obtain univariate polynomials $\Re(x_i) \in \Bbbk[x_i]$ of degree at most d^n for each $1 \leq i \leq n$ such that $\Re$ vanishes on each isolated point in the algebraic set.

Proof: Fix a value $0 < l \leq n$ and a set of indices $\Im = \{i_1 < \cdots < i_l\} \subset [n]$, where $[n] = \{1, \ldots, n\}$. To simplify the notation, denote

$$\begin{aligned} \mathbf{y}_\Im &:= \{x_{i_1}, \ldots, x_{i_l}\}, \\ \tilde{\mathbf{x}}_\Im &:= \{x_j \mid j \in [n] - \Im\}, \\ \mathbf{x}_\Im &:= \{x_0\} \cup \tilde{\mathbf{x}}_\Im, \end{aligned} \tag{4.8}$$

where x_0 is a new variable. Also, let $m = n - l$.

Let $S \subset \Bbbk$ be a finite set, and let $\{a_{ij} \mid 0 \leq i \leq m,\ 0 \leq j \leq k\} \subset S$ be random values uniformly chosen from S. Compute $F' := \{\mathbf{f}'_0, \ldots, \mathbf{f}'_m\} \subset \Bbbk[\tilde{\mathbf{x}}_\Im, \mathbf{y}_\Im]$ defined in (4.5). Also, let $(F')^h := \{(\mathbf{f}'_0)^h, \ldots, (\mathbf{f}'_m)^h\} \subset \Bbbk[\mathbf{x}_\Im, \mathbf{y}_\Im]$ be homogeneous polynomials in the variables $\mathbf{x}$ deriving from F' after homogenization with the variable x_0. Finally compute the system $\hat{F}(t)$ consisting of the perturbed polynomials

$$\hat{\mathbf{f}}_i := (1-t)(\mathbf{f}'_i)^h + t x_i^d \in \Bbbk[t, \mathbf{x}_\Im, \mathbf{y}_\Im] \quad 0 \leq i \leq m.$$

The resultant $\Re_\Im$ in the claim is $\hat{\Re}(\mathbf{y}_\Im)$ defined in (4.4), the lowest non-zero coefficient of $\hat{\Re}(t, \mathbf{y}_\Im)$, the resultant of the system $\hat{F}(t)$.

Let X be an irreducible component of $V(F) \subset \mathbb{A}^n$ of dimension $l-1$ with prime ideal $\mathcal{P}$. Then by Lemma 4.1.3 and Proposition 4.1.2 we have

$$X \subset V_{l-1}(F') \implies X \subset V(\hat{\Re}) \iff \hat{\Re} \in \mathcal{P} \cap \Bbbk[\mathbf{y}_\Im].$$

Note that the degrees of the polynomials in $\hat{F}(t)$ are also less than d in the variables $\mathbf{x}_\mathfrak{I}$ and $\mathbf{y}_\mathfrak{I}$, and they are linear in the variable t. Therefore, the bound for the degree of $\mathfrak{R}_\mathfrak{I}$ follows from Corollary 4.1.1.

The bound for the degree of the polynomials h occurring in the computation follows from the fact that the resultant $\hat{\mathfrak{R}}(t, \mathbf{y}_\mathfrak{I})$ of $\hat{F}(t)$ is the quotient of two determinants, which are polynomials in the variables $\mathbf{y}_\mathfrak{I}$ and t of degree at most $d^m \deg_{\mathbf{y}_\mathfrak{I}}(F)$ and d_m respectively. Using the pseudo-division algorithm for the variable t (see section 3.3), we obtain the desired quotient, since these determinants are monic in t. Also the degree bound (4.7) follows from Lemma 3.3.3.

Finally, as we mentioned earlier, by [IK93][Theorem 15.3] the resultant $\hat{\mathfrak{R}}(t, \mathbf{y}_\mathfrak{I})$ of $\hat{F}(t)$ can be computed using only ring operations in $\Bbbk[t, \mathbf{y}_\mathfrak{I}]$, and the arithmetic circuit over $\Bbbk[t, \mathbf{y}_\mathfrak{I}]$ computing $\hat{\mathfrak{R}}(t, \mathbf{y}_\mathfrak{I})$ has depth $O(m^2 \log^2(d))$ and size $O(d^{3.5m})$. Since the operands are polynomials in $\Bbbk[t, \mathbf{y}_\mathfrak{I}]$ of degree at most d^{2m+1} in $l+1$ variables, we get that the arithmetic circuit over $\Bbbk$ computing $\hat{\mathfrak{R}}(t, \mathbf{y}_\mathfrak{I})$ has depth $O(lm^2 \log^3(d))$ and size $O(d^{3.5m} \cdot d^{(2m+1)(l+1)})$. ■

Recall that we call a triangular set Δ a *weakly unmixed set* if the polynomials in Δ are not necessary square-free.

Corollary 4.1.5 *Let $F \subset \Bbbk[x_1, \ldots, x_n]$ be a set of polynomials and assume that the degrees of the polynomials in F are bounded by d. Let $0 \leq l < n$ and let*

$$\imath \cup \jmath = [n]$$

be a partition of $[n] = \{1, \ldots, n\}$ *with* $|\imath| = l$ *and denote*

$$\imath := \{i_1 < \cdots < i_l\} \quad \jmath := \{j_1 < \cdots < j_{n-l}\}.$$

Also, define

$$\mathbf{x}_\imath \prec \mathbf{x}_\jmath := x_{i_1} \prec \cdots \prec x_{i_l} \prec x_{j_1} \prec \cdots \prec x_{j_{n-l}},$$

the ordering of the variables $\{x_1, \ldots, x_n\}$ *corresponding to the partition* $\imath \cup \jmath = [n]$. *Then we can compute the weakly unmixed sets with respect to the variable ordering* $\mathbf{x}_\imath \prec \mathbf{x}_\jmath$

$$\Delta_\imath := \{\mathbf{g}_s(\mathbf{x}_\imath, x_{j_s}) \mid 1 \leq s \leq n-l\} \subset k[\mathbf{x}_\imath, \mathbf{x}_\jmath]$$

with the property

$$\begin{aligned}(\mathcal{P} \in \mathrm{Ap}(F)) \wedge (\dim_{\mathrm{Krull}}(\mathcal{P}) = n-l) \wedge (\mathcal{P} \cap \Bbbk[\mathbf{x}_\imath] = \{0\}) \\ \Longrightarrow \mathrm{Rep}(\Delta_\imath) \subseteq \mathcal{P}.\end{aligned} \tag{4.9}$$

Moreover,

$$\max\{\deg_{x_i}(\mathbf{g}) \mid \mathbf{g} \in \Delta_\imath,\ i \in [n],\ \imath \subsetneq [n]\} \leq d^{(n-l)}, \tag{4.10}$$

and for any polynomial h *occurring in the computation*

$$\deg_{x_i}(h) \leq d^{2(n-l)} \ \forall\, i \in [n]. \tag{4.11}$$

Furthermore, the set $\Sigma := \{\Delta_\imath \mid \imath \subsetneq [n]\}$ *can be computed with an arithmetic circuit over* $\Bbbk$ *of depth* $O(n^3 \log^3(d))$ *and size* $O(d^{7n^2})$.

Proof: For a fixed $\imath \subsetneq [n]$ and $j_s \in \jmath$, let $\Im = \imath \cup \{j_s\}$, and define

$$\mathbf{g}_s := \Re_\Im \in \Bbbk[x_{i_1}, \ldots, x_{i_l}, x_{j_s}]$$

defined in Theorem 4.1.4. Define

$$\Delta_\imath := \{\mathbf{g}_s \mid 1 \leq s \leq n-l\}.$$

Then clearly $\Delta_\imath$ is triangular with respect to $\mathbf{x}_i \prec \mathbf{x}_j$, and it is also a weakly unmixed set, since the coefficients of $\mathbf{g}_s$ are elements of $\Bbbk[\mathbf{x}_\imath]$ for all $1 \leq s \leq n-l$. Note that in Theorem 4.1.4, the number $l-1$ denoted the codimension of the components, whereas here it is denoted by l. This implies that the expression in (4.9), (4.10) and (4.11) are valid by Theorem 4.1.4.

For the complexity of computation of the sets $\Delta_\imath$ for all possible partition $\imath \cup \jmath = [n]$, we first observe that we can compute them in parallel. Therefore, using Theorem 4.1.4, the depth of the arithmetic circuit computing Σ is at most

$$\max_{1 \leq l \leq n} (c \cdot (n-l)^2 l \log^3(d)) \leq O(n^3 \log^3(d))$$

where c is a constant.

The size of the arithmetic circuit computing Σ is at most

$$\sum_{l=1}^{n} C \cdot n^l (n-l) d^{6(n-l)l} \leq C \cdot 2^{n^2} d^{6n^2} \leq O(d^{7n^2}),$$

using the bounds in Theorem 4.1.4, where C is a constant. ■

Corollary 4.1.5 gives a method to compute the weakly unmixed sets $\Delta_\imath$, for $\imath = \{x_{i_1}, \ldots x_{i_l}\} \subsetneqq [n]$ such that if X is an irreducible component of $V(F)$ such that $\dim(X) = l$ and $\pi_\imath(X) = \mathbb{A}^l$, where $\pi_\imath$ is the projection $(x_1, \ldots, x_n) \mapsto (x_{i_1}, \ldots x_{i_l})$, then X is also an irreducible component of $V_{\text{Rep}}(\Delta_\imath)$. Using the results of the next section we are able to convert the set $\Sigma = \{\Delta_\imath \mid \imath \subsetneqq [n]\}$ into an "unordered" unmixed representation of $V(F)$. First we need the following definition:

Definition 4.1.6 *Let* $\Xi = \{\Delta_1, \ldots, \Delta_r\}$ *be a set of polynomial sets such that for each* $\Delta \in \Sigma$ *there exists a partition* $\imath \cup \jmath = [n]$ *such that* $|\jmath| = \#(\Delta)$ *and* Δ *is an unmixed set with respect to the variable ordering* $\mathbf{x}_\imath \prec \mathbf{x}_\jmath$. *Let* $\mathrm{Rep}_\imath(\Delta)$ *be the ideal represented by* Δ *w.r.t the variable ordering* $\mathbf{x}_\imath \prec \mathbf{x}_\jmath$. *We call* Ξ *an* " unordered unmixed representation" *of the algebraic set* $V(F)$ *if*

$$\sqrt{\langle F \rangle} = \bigcap_{\Delta \in \Xi} \mathrm{Rep}_\imath(\Delta).$$

The next theorem gives the main result of the thesis. Using the results of the next section it gives an algorithm together with its complexity analysis of computing an unordered unmixed representation of $V(F)$.

Theorem 4.1.7 *Let* $F = \{\mathbf{f}_0, \ldots, \mathbf{f}_k\} \subset \Bbbk[x_1, \ldots, x_n]$ *be a set of polynomials and assume that*

$$\forall j \in [n] \quad \deg_{x_j}(\mathbf{f}_i) \leq d, \;\; 0 \leq i \leq k.$$

Then there is an algorithm computing the set $\Xi(F)$, *an unordered unmixed representation of* $V(F)$.

Moreover, if $\Delta = \{\mathbf{g}_1, \ldots, \mathbf{g}_m\} \in \Xi(F)$ *and* $\imath \cup \jmath = [n]$ *is the corresponding partition of* $[n]$, *i.e.* $\mathrm{class}(\mathbf{g}_s) = x_{j_s}$ *where* $\jmath = \{j_1, \ldots, j_m\}$ *and* $\imath = [n] - \jmath = \{i_1, \ldots, i_l\}$, *then*

$$\forall j_s \in \jmath \;\; \deg_{x_{j_s}}(\Delta) \leq d^m \quad \textit{and}$$

$$\forall i_r \in \imath \;\; \deg_{x_{i_r}}(\Delta) \leq d^{O(m^2)}.$$

For any polynomial h *occurring in the computation of* Δ *we have the following degree*

upper bounds:

$$\deg_{x_{j_s}}(h) \leq d^{2m}, \quad j_s \in \jmath \quad \textit{and}$$

$$\deg_{x_{i_r}}(h) \leq d^{O(m^2)}, \quad i_r \in \imath.$$

Furthermore the arithmetic circuit computing the unordered unmixed representation of $V(F)$ *has depth*

$$(n \log(d))^{O(1)}$$

and size

$$k^{O(1)}(d^{O(n^2)})^{2l+1}$$

where l *is the dimension of* $V(F)$.

Proof: In Corollary 4.1.5 we computed the set Σ such that if $\Delta \subset \Sigma$ then there exist $0 \leq l < n-1$ and a partition

$$\imath \cup \jmath = [n]$$

of $[n] = \{1, \ldots, n\}$ with $|\imath| = l$ and $m := n - l$ such that

$$\Delta = \{\mathbf{g}_s(\mathbf{x}_{i_s}, x_{j_s}) \mid 1 \leq s \leq m\} \subset k[\mathbf{x}_\imath, \mathbf{x}_\jmath]$$

forms a weakly unmixed set with respect to the variable ordering $\mathbf{x}_\imath \prec \mathbf{x}_\jmath$ and has the property (4.9).

Also, by Corollary 4.1.5, for all $\Delta \in \Sigma$ with $|\Delta| = m$, we have

$$\max\{\deg_{x_i}(\mathbf{g}) \mid i \in [n], \mathbf{g} \in \Delta\} \leq d^m$$

and for any polynomial h occurring in the computation of Δ

$$\deg_{x_i}(h) \leq d^{2m}, \quad i \in [n].$$

Fix $\Delta = \{\mathbf{g}_s(\mathbf{x}_i, x_{j_s}) \mid 1 \leq s \leq m\} \in \Sigma$ a weakly unmixed set with respect to the variable ordering $\mathbf{x}_i \prec \mathbf{x}_j$. Next we compute the multiplication table $\mathcal{M}(\Delta)$ for Δ. Since the coefficients of Δ are polynomials in $\mathbb{k}[\mathbf{x}_i]$, we can apply Proposition 3.3.4 to compute the structure constants of the algebra $\mathcal{A}(\Delta)$. Then the height $\Upsilon(\Delta)$ of the structure constants of $\mathcal{A}(\Delta)$ is bounded by

$$\Upsilon(\Delta) \leq \sum_{s=1}^{m} \text{height}(\mathbf{g}_s) \prod_{t=s}^{m} d^m \log(d^m) \leq d^{2(m)^2}. \tag{4.12}$$

We can transform each weakly unmixed set $\Delta \in \Sigma$ into a set of unmixed sets containing only components of $V(F)$ using the subroutine

$$\mathbf{unmixed}_m^l(\Delta, \mathcal{M}(\Delta), \mathbf{f}, 1)$$

described in Section 4.2, where

$$\mathbf{f} := \sum_{i=0}^{k} \mathbf{f}_i y^i,$$

with a new variable y. Assume that $\tilde{\Delta} = \{\tilde{\mathbf{g}}_1, \ldots, \tilde{\mathbf{g}}_m\}$ is an unmixed set in the output of $\mathbf{unmixed}(\Delta, \mathcal{M}(\Delta), \mathbf{f}, 1)$. Then $\tilde{\Delta}$ is unmixed with respect to the variable ordering $\mathbf{x}_i \prec \mathbf{x}_j$. By Theorem 4.2.2, for every polynomial $\mathbf{p}$ occurring in the computation of $\mathbf{unmixed}(\Delta, \mathcal{M}(\Delta), \mathbf{f}, 1)$ we have that

$$\text{height}(\mathbf{p}) \leq C^m d^{2(m)^2} \prod_{s=1}^{m} \tilde{d}_s^{n-s+1}(\text{height}(\mathbf{f}) + \Upsilon(\Delta))$$

where $\tilde{d}_s = \deg_{x_{j_s}}(\tilde{\mathbf{g}}_s)$ for $1 \leq s \leq m$. Since $\tilde{\Delta}$ is an unmixed component of $V(F)$ of dimension $l = n - m$, we have that

$$\prod_{s=1}^{m} \tilde{d}_s = \deg(V_{\mathrm{Rep}}(\tilde{\Delta})) \leq \deg(V_l(F)) \leq (d+1)^{n-l}, \tag{4.13}$$

where $\deg(V_l(F))$ denotes the sum of the degrees of the irreducible components of $V(F)$ of dimension l. The first equality follows from the triangular structure of $\tilde{\Delta}$ and the definition of $V_{\mathrm{Rep}}(\tilde{\Delta})$. The last inequality is proved for example in [Ier89, Lemma 2.20]. Therefore

$$\mathrm{height}(\mathbf{p}) \leq C^m d^{4(m)^2} d^{m^2} = d^{O(m^2)}.$$

Denote by $\mathcal{U}(\Delta)$ the set of unmixed sets in the output of $\mathbf{unmixed}_m^l(\Delta, \mathcal{M}(\Delta), \mathbf{f}, 1)$. Then clearly

$$\Xi(F) := \bigcup_{\Delta \in \Sigma} \mathcal{U}(\Delta)$$

gives the desired unordered unmixed representation of $V(F)$. The complexity bounds in the claim follow from Corollary 4.1.5, Theorem 4.2.2, (4.13) and (4.12). ■

4.2 Combined splitting and square-free factorization

The following algorithm, denoted by

$$\mathbf{unmixed}^{l}_{m},$$

combines the square-free factorization algorithm and the splitting algorithm for weakly unmixed sets mentioned in the proof of Theorem 4.1.7. For a weakly unmixed set Δ, i.e. where the polynomials in Δ are not necessary square-free, the algorithm **unmixed** computes a (strongly) unmixed representation corresponding to the union of the irreducible components X of $V_{\mathrm{Rep}}(\Delta)$ such that

$$X \subseteq V(F) \quad \text{and} \quad X \nsubseteq V(H)$$

for given polynomial sets F and H.

The input of $\mathbf{unmixed}^{l}_{m}$ consists of

$$(\Delta,\ \mathcal{M},\ \mathbf{f},\ \mathbf{h})$$

specified as follows.

1. $\Delta = \{\mathrm{g}_1, \ldots, \mathrm{g}_m\} \subset \Bbbk[x_1, \ldots, x_n]$ a weakly unmixed set such that $n = m + l$ and for all $1 \leq s \leq m$

   (a) $\mathrm{class}(\mathrm{g}_s) = x_{l+s}$ and $d_s := \deg_{x_{l+s}}(\mathrm{g}_s)$;

   (b) $\mathrm{lc}(\mathrm{g}_s) \in \Bbbk[x_1, \ldots, x_l]$;

(c) $\mathbf{g}_s$ is reduced modulo $\Delta_{s-1} := \{\mathbf{g}_1, \ldots, \mathbf{g}_{s-1}\}$, i.e.

$$\forall\, t < s \quad \deg_{x_{l+t}}(\mathbf{g}_s) < \deg_{x_{l+t}}(\mathbf{g}_t).$$

2. $\mathcal{M}$ is the multiplication table of the algebra

$$\mathcal{A}(\Delta) = \Bbbk(x_1, \ldots, x_l)[x_{l+1}, \ldots, x_n]/\langle\Delta\rangle_{\Bbbk(x_1,\ldots,x_l)}$$

with respect to the a priori basis

$$\mathrm{B}(\Delta) := \left\{ x_{l+1}^{\alpha_1} \cdots x_n^{\alpha_m} \mid 0 \leq \alpha_s < \deg_{x_{l+s}}(\mathbf{g}_s),\ 1 \leq s \leq m \right\}$$

over the field $\Bbbk(x_1, \ldots, x_l)$.

3. $\mathbf{f} \in \Bbbk[x_1, \ldots, x_{n+c}]$ reduced modulo Δ, where $c \geq 0$.

4. $\mathbf{h} \in \Bbbk[x_1, \ldots, x_{n+c}]$, reduced modulo Δ.

The output of $\mathbf{unmixed}_m^l$ consists of the following set of pairs:

$$\{\, (\Delta_1,\ \mathcal{M}_1), \ldots, (\Delta_r,\ \mathcal{M}_r)\}$$

satisfying the following specification.

1.
$$\bigcup_{i=1}^{r} \mathrm{Ap}(\Delta_i) = \{\mathcal{P} \in \mathrm{Ap}(\Delta) \mid \mathbf{f} \equiv 0;\ \mathbf{h} \not\equiv 0 \mod (\mathcal{P})\}\,;$$

2. For each $1 \leq i \leq r$, the set $\Delta_i = \{\mathbf{g}_1^{(i)}, \ldots, \mathbf{g}_m^{(i)}\}$ is a (strongly) unmixed set, and for each $1 \leq s \leq m$,

(a) $\mathrm{class}(\mathbf{g}_s^{(i)}) = x_{l+s}$;

(b) $\mathrm{lc}(\mathrm{g}_s^{(i)}) \in \Bbbk[x_1, \ldots, x_l]$;

(c) $\mathrm{g}_s^{(i)}$ is reduced modulo $\{\mathrm{g}_1^{(i)}, \ldots, \mathrm{g}_{s-1}^{(i)}\}$.

3. The set $\{\Delta_1, \ldots, \Delta_r\}$ is simple, i.e. $\mathrm{Ap}(\Delta_i) \cap \mathrm{Ap}(\Delta_j) = \emptyset$ if $i \neq j$.

4. $\mathcal{M}_i$ is the multiplication table of the algebra

$$\mathcal{A}(\Delta_i) = \Bbbk(x_1, \ldots, x_l)[x_{l+1}, \ldots, x_n]/\langle \Delta_i \rangle_{\Bbbk(x_1, \ldots, x_l)}$$

with respect to the a priori basis

$$\mathbf{B}(\Delta_i) := \left\{ x_{l+1}^{\alpha_1} \cdots x_n^{\alpha_m} \mid 0 \leq \alpha_s < \deg_{x_{l+s}}(\mathrm{g}_s^{(i)}),\ 1 \leq s \leq m \right\}$$

over the field $\Bbbk(x_1, \ldots, x_l)$.

First we describe the method for $m = 1$, $l = 0$ and $c = 0$, which is based on the univariate square-free factorization and the multi-polynomial gcd algorithms. For $m > 1$ the algorithm $\mathbf{unmixed}_m^l$ generalizes the $m = 1$ case.

We use the following univariate square-free factorization method (see [BKR85]): Assume that $\mathrm{g} \in \Bbbk[x]$ has degree d. Define for each $1 \leq j \leq d$

$$q_j := \prod_{\alpha} (x - \alpha),$$

where the product is taken for all $\alpha \in \mathbf{K}$ such that α is a root of g with multiplicity j. Then

$$\mathrm{g} = q_1 \cdot q_2^2 \cdots q_d^d$$

and

$$q_i = \frac{\gcd(\mathrm{g}, \mathrm{g}', \ldots, \mathrm{g}^{(i-1)}) \cdot \gcd(\mathrm{g}, \mathrm{g}', \ldots, \mathrm{g}^{(i+1)})}{\gcd(\mathrm{g}, \mathrm{g}', \ldots, \mathrm{g}^{(i)})^2},$$

where $\mathbf{g}^{(i)}$ denotes the i-th formal derivative of $\mathbf{g}$.

Assume further that we are given polynomials $\mathbf{f} \in \mathbb{k}[x]$ and $\mathbf{h} \in \mathbb{k}[x]$ such that we only want those factors of the polynomials q_i which divide $\mathbf{f}$ and relative prime to $\mathbf{h}$. Then we have to compute

$$\begin{aligned}\mathbf{q}_i &:= \frac{\gcd(q_i, \mathbf{f})}{\gcd(q_i, \mathbf{f}, \mathbf{h})} \\ &= \frac{\gcd(\mathbf{g}, \ldots, \mathbf{g}^{(i-1)}, \mathbf{f}) \cdot \gcd(\mathbf{g}, \ldots, \mathbf{g}^{(i+1)}, \mathbf{f}) \cdot \gcd(\mathbf{g}, \ldots, \mathbf{g}^{(i)}, \mathbf{f}, \mathbf{h})^2}{\gcd(\mathbf{g}, \ldots, \mathbf{g}^{(i)}, \mathbf{f})^2 \cdot \gcd(\mathbf{g}, \ldots, \mathbf{g}^{(i-1)}, \mathbf{f}, \mathbf{h}) \cdot \gcd(\mathbf{g}, \ldots, \mathbf{g}^{(i+1)}, \mathbf{f}, \mathbf{h})}.\end{aligned} \tag{4.14}$$

The correctness of (4.14) follows from

$$\gcd(q_i, p) = \frac{\gcd(\mathbf{g}, \mathbf{g}', \ldots, \mathbf{g}^{(i-1)}, p) \cdot \gcd(\mathbf{g}, \mathbf{g}', \ldots, \mathbf{g}^{(i+1)}, p)}{\gcd(\mathbf{g}, \mathbf{g}', \ldots, \mathbf{g}^{(i)}, p)^2},$$

for any polynomial $p \in \mathbb{k}[x]$.

Notice that the set $\{\mathbf{q}_1 \ldots \mathbf{q}_d\}$ is simple, since $\gcd(q_i, q_j) = 1$ if $i \neq j$. Also, in the $m = 1, l = 0$ case $\mathrm{lc}(\mathbf{q}_i) \in \mathbb{k}$, therefore the leading coefficients satisfy the output specifications. Moreover, since all the coefficients are in $\mathbb{k}$, they are reduced.

We can compute $\mathbf{q}_i$ for $1 \leq i \leq d$ by computing the six univariate multi-polynomial gcds in (4.14) parallel, using sub-resultant techniques, (see [vzG84]).

Assume that we have computed $\mathbf{q}_1, \ldots, \mathbf{q}_d$, and fix $1 \leq i \leq d$ such that $\mathbf{q}_i \neq 1$. To simplify the notation, denote $\mathbf{q}_i$ by $\mathbf{q}$.

Next we compute the multiplication table $\mathcal{M}$ of the algebra $\mathcal{A}(\{\mathbf{q}\}) := \mathbb{k}[x]/\langle \mathbf{q} \rangle$. Let $\deg_x(\mathbf{q}) = \bar{d}$. For each $0 \leq i, j < \bar{d}$ we compute the coordinates of $x^i \cdot x^j$ in the basis $\{1, x, \ldots, x^{\bar{d}-1}\}$ of the algebra $\mathcal{A}(\{\mathbf{q}\})$. We compute the remainder of x^{i+j} divided by $\mathbf{q}$, solving a linear system with a coefficient matrix which is triangular and has size $\bar{d} \times \bar{d}$ (see [vzG84]).

Now consider the general case. If $m = 0$ then

$$\mathbf{unmixed}_0^l(\emptyset,\ \mathbf{f},\ \mathbf{h}) := \begin{cases} \emptyset & \text{if } \mathbf{f} \not\equiv 0 \text{ or } \mathbf{h} \equiv 0 \\ \{(\emptyset,\ \emptyset)\} & \text{if } \mathbf{f} \equiv 0 \text{ and } \mathbf{h} \not\equiv 0. \end{cases}$$

If $m > 0$ then denote

$$\mathbf{g} := \mathbf{g}_m,\ \ d := d_m = \deg_{x_n}(\mathbf{g}_m),\ \ \Lambda := \{\mathbf{g}_1, \ldots, \mathbf{g}_{m-1}\}.$$

We compute the sets $\Sigma_1, \ldots \Sigma_d$ of unmixed sets of codimension $m-1$ and for each $\Lambda_i \in \Sigma_i$ the polynomial $\mathbf{q}_i \in \Bbbk[x_1, \ldots, x_n]$ such that

1. The set Σ_i is simple and $\mathrm{Ap}(\Lambda) = \bigcup_{\Lambda_i \in \Sigma_i} \mathrm{Ap}(\Lambda_i)$ for each $1 \leq i \leq d$.

2. For all $\mathcal{P} \in \mathrm{Ap}(\Lambda)$ and for each $1 \leq i \leq d$ there exists a unique $\Lambda_i \in \Sigma_i$ such that $\mathcal{P} \in \mathrm{Ap}(\Lambda_i)$. Then the corresponding polynomial $\mathbf{q}_i$ satisfies

$$\mathbf{q}_i = \frac{\gcd_{\mathbf{K}(\mathcal{P})}(q_i, \mathbf{f})}{\gcd_{\mathbf{K}(\mathcal{P})}(q_i, \mathbf{f}, \mathbf{h})}$$

   where $\{q_i \mid 1 \leq i \leq d\}$ are the polynomials in the square-free decomposition of $\mathbf{g}$, i.e. over the quotient field $\mathbf{K}(\mathcal{P})$ the following is satisfied:

$$\mathbf{g} = r \cdot q_1 \cdot q_2^2 \cdots q_d^d, \quad \gcd_{\mathbf{K}(\mathcal{P})}(q_i, q_j) = 1, \quad q_i \text{ is square-free}$$

   for some $r \in \mathbf{K}(\mathcal{P})$.

3. For each $1 \leq i \leq d$ and for each $\Lambda_i \in \Sigma_i$ such that $\deg_{x_n}(\mathbf{q}_i) > 0$, the sets

$$\Delta_i := \Lambda_i \cup \{\mathbf{q}_i\}$$

   form an unmixed set of codimension m;

4. $\mathrm{lc}(\mathbf{q}_i) \in \Bbbk[x_1, \ldots, x_l]$;

5. The set

$$\Sigma := \bigcup_{i=1}^{d} \{\Delta_i \mid \Lambda_i \in \Sigma_i, \ \deg_{x_n}(\mathbf{q}_i) > 0\} \tag{4.15}$$

is simple.

To obtain the above decomposition, fix a value $1 \leq i \leq d$. We split $\mathrm{Ap}(\Lambda)$ into

$$\mathrm{Ap}(\Lambda) = \bigcup_{\vec{v}} \mathrm{Ap}(\Lambda_{i,\vec{v}})$$

such that the union is taken for all vectors $\vec{v} = (v_1, \ldots, v_6)$ where $0 \leq v_t \leq d$ for $1 \leq t \leq 6$, and

$$\begin{aligned}
\mathbf{d}_{1,i,v_1} &:= \mathbf{ggcd_n}(\Lambda_{i,\vec{v}} \cup \{\mathbf{g}\}, \mathbf{g}', \ldots, \mathbf{g}^{(i-1)}, \mathbf{f}) \quad \deg_{x_n}(\mathbf{d}_{1,i,v_1}) = v_1 \\
\mathbf{d}_{2,i,v_2} &:= \mathbf{ggcd_n}(\Lambda_{i,\vec{v}} \cup \{\mathbf{g}\}, \mathbf{g}', \ldots, \mathbf{g}^{(i)}, \mathbf{f}) \quad \deg_{x_n}(\mathbf{d}_{2,i,v_2}) = v_2 \\
\mathbf{d}_{3,i,v_3} &:= \mathbf{ggcd_n}(\Lambda_{i,\vec{v}} \cup \{\mathbf{g}\}, \mathbf{g}', \ldots, \mathbf{g}^{(i+1)}, \mathbf{f}) \quad \deg_{x_n}(\mathbf{d}_{3,i,v_3}) = v_3 \\
\mathbf{d}_{4,i,v_4} &:= \mathbf{ggcd_n}(\Lambda_{i,\vec{v}} \cup \{\mathbf{g}\}, \mathbf{g}', \ldots, \mathbf{g}^{(i-1)}, \mathbf{f}, \mathbf{h}) \quad \deg_{x_n}(\mathbf{d}_{4,i,v_4}) = v_4 \\
\mathbf{d}_{5,i,v_5} &:= \mathbf{ggcd_n}(\Lambda_{i,\vec{v}} \cup \{\mathbf{g}\}, \mathbf{g}', \ldots, \mathbf{g}^{(i)}, \mathbf{f}, \mathbf{h}) \quad \deg_{x_n}(\mathbf{d}_{5,i,v_5}) = v_5 \\
\mathbf{d}_{6,i,v_6} &:= \mathbf{ggcd_n}(\Lambda_{i,\vec{v}} \cup \{\mathbf{g}\}, \mathbf{g}', \ldots, \mathbf{g}^{(i+1)}, \mathbf{f}, \mathbf{h}) \quad \deg_{x_n}(\mathbf{d}_{6,i,v_6}) = v_6
\end{aligned} \tag{4.16}$$

are well defined, i.e. the assumptions of Lemma 3.1.3 are satisfied.

To satisfy the assumption of Lemma 3.1.3, first we need to compute the j-th sub-resultants

$$\varphi_k^{(j)}(y, z) := \mathrm{RES}_{x_n}^{(j)}(\mathbf{g}, \ \mathbf{f} + \sum_{l=1}^{k} \mathbf{g}^{(l)} \cdot y^{l-1} + z \cdot \mathbf{h}), \quad 1 \leq k \leq d,$$

for $0 \leq j \leq d$, where y and z are new variables.

Fix a vector $\vec{v} = (v_1, \ldots, v_6)$, where $0 \leq v_t \leq d$ for $1 \leq t \leq 6$. Lemma 3.1.3 states that if the congruences

$$\left.\begin{array}{c} \varphi_{i-1}^{(u_1)}(y,0),\ \ \varphi_i^{(u_2)}(y,0),\ \ \varphi_{i+1}^{(u_3)}(y,0), \\ \varphi_{i-1}^{(u_4)}(y,z),\ \ \varphi_i^{(u_5)}(y,z),\ \ \varphi_{i+1}^{(u_5)}(y,z) \end{array}\right\} \equiv 0 \mod (\mathcal{P})\ \ \forall\, \vec{u} < \vec{v} \quad (4.17)$$

$$\left.\begin{array}{c} \varphi_1 := \varphi_{i-1}^{(v_1)}(y,0),\ \ \varphi_2 := \varphi_i^{(v_2)}(y,0),\ \ \varphi_3 := \varphi_{i+1}^{(v_3)}(y,0), \\ \varphi_4 := \varphi_{i-1}^{(v_4)}(y,z),\ \ \varphi_5 := \varphi_i^{(v_5)}(y,z),\ \ \varphi_6 := \varphi_{i+1}^{(v_6)}(y,z) \end{array}\right\} \not\equiv 0 \mod (\mathcal{P}) \quad (4.18)$$

are satisfied for each $\mathcal{P} \in \mathrm{Ap}(\Lambda_{i.\vec{v}})$, then the six polynomials in (4.16) are well defined and have the prescribed degrees. Therefore, $\mathrm{Ap}(\Lambda_{i.\vec{v}})$ consists of exactly those components of $\mathrm{Ap}(\Lambda)$, where the congruences (4.17) and (4.18) are satisfied. We will compute $\mathrm{Ap}(\Lambda_{i.\vec{v}})$ by calling recursively $\mathbf{unmixed}^l_{m-1}$.

Define the polynomial $\Phi_{i.\vec{v}}(y,z,w)$ by combining the polynomials in (4.17) using the powers of a new variable w. Also, define the polynomial

$$\Psi_{i.\vec{v}}(y,z) = \prod_{t=1}^{6} \varphi_t$$

the product of the six polynomials in (4.18). To satisfy the input specification of $\mathbf{unmixed}^l_{m-1}$, reduce the polynomials $\Phi_{i.\vec{v}}$ and $\Psi_{i.\vec{v}}$ modulo Λ. Notice also that the multiplication table $\mathcal{M}(\Lambda)$ of Λ is contained in the multiplication table $\mathcal{M}$ of Δ. Hence $(\Lambda,\ \mathcal{M}(\Lambda),\ \Phi_{i.\vec{v}},\ \Psi_{i.\vec{v}})$ satisfies the input specification of $\mathbf{unmixed}^l_{m-1}$.

Compute recursively

$$\mathcal{L}_{i.\vec{v}} := \mathbf{unmixed}^l_{m-1}(\ \Lambda, \mathcal{M}(\Lambda),\ \Phi_{i.\vec{v}},\ \Psi_{i.\vec{v}}) \quad (4.19)$$

consisting of pairs of the form

$$(\ \Lambda_{i.\vec{v}},\ \mathcal{M}(\Lambda_{i.\vec{v}})) \in \mathcal{L}_{i.\vec{v}}. \quad (4.20)$$

We will prove that the sets

$$\Sigma_i := \{\Lambda_{i.\vec{v}} \in \mathcal{L}_{i.\vec{v}} \mid 0 \leq v_t \leq d,\ 1 \leq t \leq 6\}$$

are simple and satisfy

$$\mathrm{Ap}(\Lambda) = \bigcup_{\Lambda_{i.\vec{v}} \in \Sigma_i} \mathrm{Ap}(\Lambda_{i.\vec{v}})$$

for each $1 \leq i \leq d$.

We continue the computation only with those i and $\vec{v}$ such that the set $\mathcal{L}_{i.\vec{v}} \neq \emptyset$. Fix i, $\vec{v}$ and a pair

$$(\ \Lambda_{i.\vec{v}},\ \mathcal{M}(\Lambda_{i.\vec{v}})) \in \mathcal{L}_{i.\vec{v}}.$$

The rest of the computation is assumed to be conducted using arithmetics in the algebra $\mathcal{A}(\Lambda_{i.\vec{v}})$, using the multiplication table $\mathcal{M}(\Lambda_{i.\vec{v}})$.

By the definition of $\Lambda_{i.\vec{v}}$, the polynomials $\mathbf{d}_{t.i.v_t} \in \Bbbk[x_1, \ldots, x_n]$ defined in (4.16) are well defined and have degree v_t in x_n for each $1 \leq t \leq 6$. Also,

$$\mathrm{lc}(\mathbf{d}_{t.i.v_t}) = \varphi_t(x_1, \ldots, x_n, a_{n+1}, \ldots a_{n+c'}) \in \Bbbk[x_1, \ldots, x_{n-1}]$$

where $\varphi_t \in \Bbbk[x_1, \ldots, x_{n+c}, y, z]$ is defined in (4.18), and $a_{n+1}, \ldots, a_{n+c'} \in \Bbbk$ is chosen such that

$$\forall \mathcal{P} \in \mathrm{Ap}(\Lambda_{i.\vec{v}}) \quad \varphi_t(x_1, \ldots, x_n, a_{n+1}, \ldots a_{n+c'}) \notin \mathcal{P}.$$

For each $1 \leq t \leq 6$ compute

$$\overline{\mathrm{lc}(\mathbf{d}_{t.i.v_t})} := \mathbf{pinverse}^{l}_{m-1}(\Lambda_{i.\vec{v}},\ \mathcal{M}(\Lambda_{i.\vec{v}}),\ \mathrm{lc}(\mathbf{d}_{t.i.v_t}))$$

defined in Section 3.4. Define

$$\bar{\mathbf{d}}_{t.i.v_t} :=\ \overline{\mathrm{lc}(\mathbf{d}_{t.i.v_t})} \cdot \mathbf{d}_{t.i.v_t} \in \mathcal{A}(\Lambda_{i.\vec{v}}). \tag{4.21}$$

Since

$$\overline{\mathrm{lc}(\mathbf{d}_{t,i,v_t})} \cdot \mathrm{lc}(\mathbf{d}_{t,i,v_t}) \equiv \mathbf{r}_{i,\vec{v},t} \mod \langle \Lambda_{i,\vec{v}} \rangle, \quad \mathbf{r}_{i,\vec{v},t} \in \Bbbk[x_1, \ldots, x_l],$$

by the output specification of $\mathbf{pinverse}^l_{m-1}$ we have that

$$\mathrm{lc}(\bar{\mathbf{d}}_{t,i,v_t}) \in \Bbbk[x_1, \ldots, x_l]. \tag{4.22}$$

Analogously to the $m = 1$, $l = 0$ case, we compute

$$\mathbf{q}_{i,\vec{v}} := \frac{\bar{\mathbf{d}}_{1,i,v_1} \cdot \bar{\mathbf{d}}_{3,i,v_3} \cdot \bar{\mathbf{d}}^2_{5,i,v_5}}{\bar{\mathbf{d}}^2_{2,i,v_2} \cdot \bar{\mathbf{d}}_{4,i,v_4} \cdot \bar{\mathbf{d}}_{6,i,v_6}}, \tag{4.23}$$

where the division above is pseudo-division, computed as in section 3.3.1, using ring arithmetics in $\mathcal{A}(\Lambda_{i\vec{v}})$. More precisely, $\mathbf{q}_{i,\vec{v}}$ is defined by

$$\prod_{t=2.4.6} \mathrm{lc}(\bar{\mathbf{d}}_{t,i,v_t})^{\alpha_t} \cdot \left(\bar{\mathbf{d}}_{1,i,v_1} \cdot \bar{\mathbf{d}}_{3,i,v_3} \cdot \bar{\mathbf{d}}^2_{5,i,v_5}\right) = \left(\bar{\mathbf{d}}^2_{2,i,v_2} \cdot \bar{\mathbf{d}}_{4,i,v_4} \cdot \bar{\mathbf{d}}_{6,i,v_6} \cdot\right) \mathbf{q}_{i,\vec{v}} + \mathbf{r}_{i,\vec{v}}$$

where $\mathbf{r}_{i,\vec{v}} \in \mathrm{Rep}(\Lambda_{i,\vec{v}})$. Note that $\deg_{x_n}(\mathbf{q}_{i,\vec{v}}) = v_1 + v_3 - 2v_2 - v_4 - v_6 + 2v_5$ and

$$\mathrm{lc}(\mathbf{q}_{i,\vec{v}}) = \prod_{t=1}^{6} \mathrm{lc}(\bar{\mathbf{d}}_{t,i,v_t})^{\beta_t} \in \Bbbk[x_1, \ldots, x_l] \tag{4.24}$$

where $\beta_t = \alpha_t - 1$ if $t = 2, 4, 6$ and $\beta_t = 1$ otherwise.

For vectors $\vec{v}$ such that $\deg_{x_n}(\mathbf{q}_{i,\vec{v}}) > 0$, define

$$\Delta_{i,\vec{v}} := \Lambda_{i,\vec{v}} \cup \{\mathbf{q}_{i,\vec{v}}\}. \tag{4.25}$$

We will prove that each $\Delta_{i,\vec{v}}$ forms a reduced unmixed set of codimension m.

Finally, to compute the multiplication table $\mathcal{M}_{i,\vec{v}}$ corresponding to the algebra $\mathcal{A}(\Delta_{i,\vec{v}})$ for a given $\Delta_{i,\vec{v}}$, we use the method described in section 3.3.2. Denote

$$\Lambda_{i,\vec{v}} =: \{\mathbf{g}_{1,i,\vec{v}}, \ldots, \mathbf{g}_{m-1,i,\vec{v}}\} \text{ and } \mathbf{q}_{i,\vec{v}} =: \mathbf{g}_{m,i,\vec{v}},$$

and denote $\tilde{d}_s := \deg_{x_{l+s}}(\mathbf{g}_{s,i,\bar{v}})$ for $1 \leq s \leq m$. As in section 3.3.2, we consider all monomials $\mathbf{m}$ of the form $\mathbf{m} := x_{l+1}^{\alpha_1} \cdots x_n^{\alpha_m}$ for $0 \leq \alpha_s \leq 2\tilde{d}_s - 1, \ \ 1 \leq s \leq m$. If $\alpha_m < \tilde{d}_m$ then

$$\mathbf{m} \mod \mathrm{Rep}(\Delta_{i,\bar{v}}) = (\mathbf{m}_{n-1} \mod \mathrm{Rep}(\Lambda_{i,\bar{v}})) \cdot x_n^{\alpha_n}$$

where $\mathbf{m}_{n-1} = x_{l+1}^{\alpha_1} \cdots x_{n-1}^{\alpha_{m-1}}$. Therefore the corresponding structure constants are computed in the multiplication table $\mathcal{M}(\Lambda_{i,\bar{v}})$ defined in (4.20).

Assume that $\alpha_m \geq \tilde{d}_m$. To find the coordinates of $\mathbf{m}$ in the basis

$$\{x_{l+1}^{\alpha_1} \cdots x_n^{\alpha_m} \mid 0 \leq \alpha_s \leq \tilde{d}_s - 1, \ \ 1 \leq s \leq m\}$$

over $\Bbbk(x_1, \ldots, x_l)$, in section 3.3.2 we find the pseudo-remainder of $\mathbf{m}$ by $\mathbf{g}_{m,i,\bar{v}}$ by solving a linear system with a triangular matrix of size $\tilde{d}_m \times \tilde{d}_m$, using ring arithmetics over the algebra $\mathcal{A}(\Lambda_{i,\bar{v}})$.

Now we are ready to define the output of

$$\mathbf{unmixed}_m^l(\Delta, \mathcal{M}, \mathbf{f}, \mathbf{h})$$

as the following proposition asserts it.

Proposition 4.2.1 *Let $\Delta = \{\mathbf{g}_1, \ldots, \mathbf{g}_m\} \subset \Bbbk[x_1, \ldots, x_n]$ be a weakly unmixed set, let $l = n - m$, and assume that for all $1 \leq s \leq m$ the following conditions are satisfied:*

1. $\mathrm{class}(\mathbf{g}_s) = x_{l+s}$ *and* $d_s := \deg_{x_{l+s}}(\mathbf{g}_s)$;

2. $\mathrm{lc}(\mathbf{g}_s) \in \Bbbk[x_1, \ldots, x_l]$;

3. $\mathbf{g}_s$ *is reduced modulo* $\Delta_{s-1} := \{\mathbf{g}_1, \ldots, \mathbf{g}_{s-1}\}$.

Let $\mathcal{M}$ *be the multiplication table of the algebra*

$$\mathcal{A}(\Delta) = \Bbbk(x_1, \ldots, x_l)[x_{l+1}, \ldots, x_n]/\langle\Delta\rangle_{\Bbbk(x_1,\ldots,x_l)}$$

with respect to the a priori basis

$$\mathbf{B}(\Delta) := \left\{ x_{l+1}^{\alpha_1} \cdots x_n^{\alpha_m} \mid 0 \leq \alpha_s < \deg_{x_{l+s}}(\mathbf{g}_s),\ 1 \leq s \leq m \right\}$$

over the field $\Bbbk(x_1, \ldots, x_l)$. *Furthermore, for some* $c \geq 0$, *let* $\mathbf{f}, \mathbf{h} \in \Bbbk[x_1, \ldots, x_{n+c}]$ *be polynomials reduced modulo* Δ. *Consider the set of pairs*

$$\mathcal{L} := \{(\ \Delta_{i,\vec{v}},\ \mathcal{M}_{i,\vec{v}})\ \mid \forall\ i, \vec{v}\},$$

defined in (4.25), where $1 \leq i \leq d_m$ *and* $\vec{v} = (v_1, \ldots, v_6)$, $0 \leq v_t \leq d_m$, *such that* $\Delta_{i,\vec{v}}$ *forms an unmixed set of codimension* m. *Then* $\mathcal{L}$ *satisfies the output specification of the algorithm*

$$\mathbf{unmixed}_m^l(\Delta,\ \mathcal{M},\ \mathbf{f},\ \mathbf{h}).$$

Proof:

Denote $d := d_m$. Using the notation in (4.19) and (4.20), define

$$\Sigma_i := \{\Lambda_{i,\vec{v}} \in \mathcal{L}_{i,\vec{v}} \mid 0 \leq v_t \leq d,\ 1 \leq t \leq 6\}$$

for each $1 \leq i \leq d$. Then

1. **Claim:** If $\Lambda = \{\mathbf{g}_1, \ldots, \mathbf{g}_{m-1}\}$ and $1 \leq i \leq d$ is fixed then

$$\mathrm{Ap}(\Lambda) = \bigcup_{\Lambda_{i,\vec{v}} \in \Sigma_i} \mathrm{Ap}(\Lambda_{i,\vec{v}}).$$

Proof: First notice that if $\mathcal{P}$ is an element of the right hand side then it is an element of $\mathrm{Ap}(\Lambda)$ by induction. On the other hand, if $\mathcal{P} \in \mathrm{Ap}(\Lambda)$ then for each $1 \leq i \leq d$ there exist $0 \leq v_1, \ldots, v_6 \leq d$ such that (4.17) and (4.18) are satisfied. Since $\Phi_{i,\vec{v}}$ is the combination of the polynomials in (4.17) using the powers of a new variable, the vanishing of $\Phi_{i,\vec{v}}$ implies the vanishing of the polynomials in (4.17) modulo $\mathcal{P}$. Also, since $\Psi_{i,\vec{v}}$ is the product of the polynomials in (4.18), if $\Psi_{i,\vec{v}}$ does not vanish then none of the polynomials in (4.18) vanish modulo $\mathcal{P}$. Therefore, by induction and by the definition of $\mathcal{L}_{i,\vec{v}}$ in (4.19) we have that $\mathcal{P} \in \mathrm{Ap}(\Lambda_{i,\vec{v}})$ for some $\Lambda_{i,\vec{v}} \in \Sigma_i$.

2. **Claim:** The set Σ_i is simple.

   Proof: First observe that for a fixed $\vec{v}$ the set

   $$\Sigma_{i,\vec{v}} := \{\Lambda_{i,\vec{v}} \in \mathcal{L}_{i,\vec{v}}\},$$

   defined in (4.19), is simple by induction. Let $\vec{v} \neq \vec{v}'$ and suppose that $v_1' < v_1$. Indirectly, if

   $$\mathcal{P} \in \bigcup_{\Lambda_{i,\vec{v}} \in \Sigma_{i,\vec{v}}} \mathrm{Ap}(\Lambda_{i,\vec{v}}) \cap \bigcup_{\Lambda_{i,\vec{v}'} \in \Sigma_{i,\vec{v}'}} \mathrm{Ap}(\Lambda_{i,\vec{v}'})$$

   then, by the definition of $\mathcal{L}_{i,\vec{v}'}$ we have $\varphi_{i-1}^{(v_1')}(y,0) \not\equiv 0 \mod (\mathcal{P})$, but by the definition of $\mathcal{L}_{i,\vec{v}}$ we have $\varphi_{i-1}^{(v_1')}(y,0) \equiv 0 \mod (\mathcal{P})$, a contradiction. The cases $v_t' < v_t$, $2 \leq t \leq 6$ follow similarly.

3. **Claim:** For all $\mathcal{P} \in \mathrm{Ap}(\Lambda)$ and for each $1 \leq i \leq d$ there exists a unique $\Lambda_{i,\vec{v}} \in \Sigma_i$ such that $\mathcal{P} \in \mathrm{Ap}(\Lambda_{i,\vec{v}})$. Then the corresponding polynomial $\mathbf{q}_{i,\vec{v}}$

satisfies

$$\mathbf{q}_{i,\vec{v}} = \frac{\gcd_{\mathbf{K}(\mathcal{P})}(q_i, \mathbf{f})}{\gcd_{\mathbf{K}(\mathcal{P})}(q_i, \mathbf{f}, \mathbf{h})} \tag{4.26}$$

where $\{q_i \mid 1 \leq i \leq d\}$ are the polynomials in the square-free decomposition of $\mathbf{g}$; i.e. over the quotient field $\mathbf{K}(\mathcal{P})$ the following is satisfied:

$$\mathbf{g} = r \cdot q_1 \cdot q_2^2 \cdots q_d^d, \quad \gcd_{\mathbf{K}(\mathcal{P})}(q_i, q_j) = 1, \quad q_i \text{ square-free} \tag{4.27}$$

for some $r \in \mathbf{K}(\mathcal{P})$.

Proof: The previous statements about Σ_i imply the existence of a unique $\Lambda_{i,\vec{v}} \in \Sigma_i$ such that $\mathcal{P} \in \mathrm{Ap}(\Lambda_{i,\vec{v}})$. The second part of the claim follows from the definition of the polynomials $\mathbf{d}_{t,i,v_t}$ in (4.16), the definition of $\mathbf{q}_{i,\vec{v}}$ in (4.23), and the correctness of the algorithm for univariate polynomials over the field $\mathbf{K}(\mathcal{P})$.

4. **Claim:** For each $1 \leq i \leq d$ and for each $\Lambda_{i,\vec{v}} \in \Sigma_i$ such that $\deg_{x_n}(\mathbf{q}_{i,\vec{v}}) > 0$ the sets

$$\Delta_{i,\vec{v}} := \Lambda_{i,\vec{v}} \cup \{\mathbf{q}_{i,\vec{v}}\}$$

form (strongly) unmixed sets of codimension m. Moreover, if we denote

$$\Delta_{i,\vec{v}} := \{\mathbf{g}_{1,i,\vec{v}}, \ldots, \mathbf{g}_{m,i,\vec{v}}\},$$

then for each $1 \leq s \leq m$

(a) $\mathrm{class}(\mathbf{g}_{s,i,\vec{v}}) = x_{l+s}$;

(b) $\mathrm{lc}(\mathbf{g}_{s,i,\vec{v}}) \in \Bbbk[x_1, \ldots, x_l]$;

(c) $\deg_{x_{l+t}}(\mathbf{g}_{s,i,\vec{v}}) < \deg_{x_{l+t}}(\mathbf{g}_{t,i,\vec{v}})$ for all $t < s$.

Proof: By induction, $\Lambda_{i,\vec{v}}$ is a strongly unmixed set of codimension $m-1$. and the claims are true for $\mathbf{g}_{s,i,\vec{v}}$ if $1 \leq s \leq m-1$. By (4.27) and (4.26) the polynomial $\mathbf{q}_{i,\vec{v}}$ is square-free over $\mathbf{K}(\mathcal{P})$ for all $\mathcal{P} \in \Lambda_{i,\vec{v}}$. The second part of the claim follows from the definition of $\bar{\mathbf{d}}_{t,i,v_t}$ in (4.21), from (4.22), from the definition of $\mathbf{q}_{i,\vec{v}}$ in (4.23), and from (4.24).

5. **Claim:** The set

$$\Sigma := \bigcup_{i=1}^{d} \left\{ \Delta_{i,\vec{v}} \mid \Lambda_{i,\vec{v}} \in \Sigma_i,\ \deg_{x_n}(\bar{\mathbf{q}}_{i,\vec{v}}) > 0 \right\} \tag{4.28}$$

is simple.

Proof: First we observe that for a fixed $1 \leq i \leq d$, if $\vec{v} \neq \vec{v}'$ then

$$\mathrm{Ap}\left(\Lambda_{i,\vec{v}} \cup \{\mathbf{q}_{i,\vec{v}}\}\right) \cap \mathrm{Ap}\left(\Lambda_{i,\vec{v}'} \cup \{\mathbf{q}_{i,\vec{v}'}\}\right) = \emptyset,$$

which follows from the fact that Σ_i is simple.

Suppose that $i \neq i'$ and assume indirectly that

$$\mathcal{P} \in \bigcup_{\Lambda_{i,\vec{v}} \in \Sigma_i} \mathrm{Ap}(\Lambda_{i,\vec{v}} \cup \{\mathbf{q}_{i,\vec{v}}\}) \ \cap \bigcup_{\Lambda_{i',\vec{v}'} \in \Sigma_{i'}} \mathrm{Ap}(\Lambda_{i',\vec{v}'} \cup \{\mathbf{q}_{i',\vec{v}'}\}).$$

This implies that there exist unique sets $\Lambda_{i,\vec{v}} \in \Sigma_i$ and $\Lambda_{i',\vec{v}'} \in \Sigma_{i'}$ such that for $\mathcal{P}' := \mathcal{P} \cap \Bbbk[x_1, \ldots x_{n-1}]$

$$\mathcal{P}' \in \mathrm{Ap}(\Lambda_{i,\vec{v}}) \cap \mathrm{Ap}(\Lambda_{i',\vec{v}'}).$$

Then

$$\mathbf{q}_{i,\vec{v}} = \frac{\gcd_{\mathbf{K}(\mathcal{P}')}(q_i, \mathbf{f})}{\gcd_{\mathbf{K}(\mathcal{P}')}(q_i, \mathbf{f}, \mathbf{h})} \quad \text{and} \quad \mathbf{q}_{i',\vec{v}'} = \frac{\gcd_{\mathbf{K}(\mathcal{P}')}(q_{i'}, \mathbf{f})}{\gcd_{\mathbf{K}(\mathcal{P}')}(q_{i'}, \mathbf{f}, \mathbf{h})}$$

and q_i and $q_{i'}$ are polynomials in the square-free factorization of $\mathbf{g}$ over $\mathbf{K}(\mathcal{P}')$. Therefore q_i and $q_{i'}$ are relatively prime over $\mathbf{K}(\mathcal{P}')$, which implies that $\mathbf{q}_{i,\bar{v}}$ and $\mathbf{q}_{i',\bar{v}'}$ are also relative prime over $\mathbf{K}(\mathcal{P}')$. Hence

$$\mathcal{P} \in \mathrm{Ap}(\mathrm{Rep}(\mathcal{P}' \cup \{\mathbf{q}_{i,\bar{v}}\})) \cap \mathrm{Ap}(\mathrm{Rep}(\mathcal{P}' \cup \{\mathbf{q}_{i',\bar{v}'}\})) = \emptyset,$$

a contradiction.

6. **Claim:**

$$\bigcup_{\Delta_{i,\bar{v}} \in \Sigma} \mathrm{Ap}(\Delta_{i,\bar{v}}) = \{\mathcal{P} \in \mathrm{Ap}(\Delta) \mid \mathbf{f} \equiv 0;\ \mathbf{h} \not\equiv 0 \mod (\mathcal{P})\}.$$

Proof:

"$\subseteq$": Let $\Delta_{i,\bar{v}} = \Lambda_{i,\bar{v}} \cup \{\mathbf{q}_{i,\bar{v}}\} \in \Sigma$. We proved above that $\mathrm{Ap}(\Lambda_{i,\bar{v}}) \subseteq \mathrm{Ap}(\Lambda)$. Since $\mathbf{q}_{i,\bar{v}}$ divides $\mathbf{g}_m$ over the field $\mathbf{K}(\mathcal{P})$ for all $\mathcal{P} \in \mathrm{Ap}(\Lambda_{i,\bar{v}})$, we have that

$$\mathrm{Rep}(\Lambda \cup \{\mathbf{g}_m\}) \subseteq \mathrm{Rep}(\Delta_{i,\bar{v}}).$$

Since $\mathrm{Rep}(\Lambda \cup \{\mathbf{g}_m\})$ and $\mathrm{Rep}(\Delta_{i,\bar{v}})$ are both unmixed and have the same codimension, this implies that

$$\mathrm{Ap}(\Delta_{i,\bar{v}}) \subseteq \mathrm{Ap}(\Delta).$$

"$\supseteq$": Let $\mathcal{P} \in \mathrm{Ap}(\Delta)$ and $\mathcal{P}' := \mathcal{P} \cap \Bbbk[x_1, \ldots, x_{n-1}]$. Fix a value $1 \leq i \leq d$. Consider the polynomials

$$d_{i,1} := \gcd_{\mathbf{K}(\mathcal{P}')}(\mathbf{g}, \mathbf{g}', \ldots, \mathbf{g}^{(i-1)}, \mathbf{f}), \quad d_{i,4} := \gcd_{\mathbf{K}(\mathcal{P}')}(\mathbf{g}, \mathbf{g}', \ldots, \mathbf{g}^{(i-1)}, \mathbf{f}, \mathbf{h}),$$

$$d_{i,2} := \gcd_{\mathbf{K}(\mathcal{P}')}(\mathbf{g}, \mathbf{g}', \ldots, \mathbf{g}^{(i)}, \mathbf{f}), \quad d_{i,5} := \gcd_{\mathbf{K}(\mathcal{P}')}(\mathbf{g}, \mathbf{g}', \ldots, \mathbf{g}^{(i)}, \mathbf{f}, \mathbf{h}),$$

$$d_{i,3} := \gcd_{\mathbf{K}(\mathcal{P}')}(\mathbf{g}, \mathbf{g}', \ldots, \mathbf{g}^{(i+1)}, \mathbf{f}), \quad d_{i,6} := \gcd_{\mathbf{K}(\mathcal{P}')}(\mathbf{g}, \mathbf{g}', \ldots, \mathbf{g}^{(i+1)}, \mathbf{f}, \mathbf{h}).$$

Then there exists $\vec{v}_i = (v_{i.1}, \ldots, v_{i.6})$, such that $0 \leq v_{i.t} \leq \deg_{x_n}(\mathbf{g}_m)$ for $1 \leq t \leq 6$, and

$$\deg_{x_n}(d_{t.i}) = v_{i.t} \qquad 1 \leq t \leq 6.$$

By Lemma 3.1.2 this implies that the congruences in (4.17) and in (4.18) are satisfied modulo $\mathcal{P}'$. Hence, using induction, we get that $\mathcal{P}' \in \Lambda_{i.\vec{v}_i}$ for some $\Lambda_{i.\vec{v}_i} \in \mathcal{L}_{i.\vec{v}_i}$ defined in (4.19). Since this is true for every $1 \leq i \leq d$, we have

$$\mathcal{P}' \in \bigcap_{i=1}^{d} \mathrm{Ap}(\Lambda_{i.\vec{v}_i}).$$

Further assume that $\mathbf{f} \equiv 0 \mod (\mathcal{P})$ and $\mathbf{h} \not\equiv 0 \mod (\mathcal{P})$. Then it is easy to see that

$$\sqrt{\langle \mathbf{g}_m, \mathbf{f} \rangle}_{\mathbf{K}(\mathcal{P}')} : \{\mathbf{h}\} \subseteq \mathcal{P} \cdot \mathbf{K}(\mathcal{P}')[x_n].$$

On the other hand, using the facts that

$$\mathbf{q}_{i.\vec{v}_i} = \frac{\gcd_{\mathbf{K}(\mathcal{P}')}(q_i, \mathbf{f})}{\gcd_{\mathbf{K}(\mathcal{P}')}(q_i, \mathbf{f}, \mathbf{h})} \quad \text{and} \quad \sqrt{\langle \mathbf{g}_m \rangle}_{\mathbf{K}(\mathcal{P}')} = \bigcap_{i=1}^{d} \langle q_i \rangle_{\mathbf{K}(\mathcal{P}')}$$

we have that

$$\bigcap_{i=1}^{d} \langle \mathbf{q}_{i.\vec{v}_i} \rangle_{\mathbf{K}(\mathcal{P}')} = \sqrt{\langle \mathbf{g}_m, \mathbf{f} \rangle}_{\mathbf{K}(\mathcal{P}')} : \{\mathbf{h}\}.$$

Therefore

$$\bigcap_{i=1}^{d} \langle \mathbf{q}_{i.\vec{v}_i} \rangle_{\mathbf{K}(\mathcal{P}')} \subseteq \mathcal{P} \cdot \mathbf{K}(\mathcal{P}')[x_n],$$

which, together with $\mathcal{P}' \in \bigcap_{i=1}^{d} \mathrm{Ap}(\Lambda_{i.\vec{v}_i})$, proves that

$$\mathcal{P} \in \bigcup_{i=1}^{d} \mathrm{Ap}(\mathcal{P}' \cup \{\mathbf{q}_{i.\vec{v}_i}\}) \subseteq \bigcup_{i=1}^{d} \mathrm{Ap}(\Delta_{i.\vec{v}_i}).$$

7. **Claim:** Let $\Delta_{i,\bar{v}} \in \Sigma$ and denote

$$\Delta_{i,\bar{v}} = \{g_{1,i,\bar{v}}, \ldots, g_{m,i,\bar{v}}\}.$$

Then $\mathcal{M}_{i,\bar{v}}$ is the multiplication table of the algebra $\mathcal{A}(\Delta_{i,\bar{v}})$ with respect to the a priori basis

$$\mathbf{B}(\Delta_{i,\bar{v}}) = \left\{ x_{l+1}^{\alpha_1} \cdots x_n^{\alpha_m} \mid 0 \leq \alpha_s < \deg_{x_{l+s}}(g_{s,i,\bar{v}}),\ 1 \leq s \leq m \right\}$$

over the field $\Bbbk(x_1, \ldots, x_l)$.

Proof: Since the leading coefficients $\mathrm{lc}(g_{s,i,\bar{v}})$ are in $\Bbbk[x_1, \ldots, x_l]$, and $g_{s,i,\bar{v}}$ is reduced modulo $\{g_{1,i,\bar{v}}, \ldots, g_{s-1,i,\bar{v}}\}$ for $1 \leq s \leq m$, the assumptions of Proposition 3.3.4 are satisfied, thus the method described in the proof of Proposition 3.3.4 gives the multiplication table for $\mathcal{A}(\Delta_{i,\bar{v}})$. ■

In the next theorem we give a complexity analysis for the algorithm **unmixed**. We use the following notation: For $p \in \Bbbk[x_1, \ldots, x_{n+c}]$ denote

$$\mathrm{height}(p) := \max\{\deg_{x_i}(p) \mid 1 \leq i \leq l\}, \quad H(p) := \prod_{j=n+1}^{n+c} (\deg_{x_j}(p) + 1).$$

Theorem 4.2.2 *Let $\Delta = \{g_1, \ldots, g_m\} \subset \Bbbk[x_1, \ldots, x_n]$ be a weakly unmixed set, let $l = n - m$, and assume that for all $1 \leq s \leq m$ the following conditions are satisfied:*

1. $\mathrm{class}(g_s) = x_{l+s}$ *and* $d_s := \deg_{x_{l+s}}(g_s)$;
2. $\mathrm{lc}(g_s) \in \Bbbk[x_1, \ldots, x_l]$;
3. g_s *is reduced modulo* $\Delta_{s-1} := \{g_1, \ldots, g_{s-1}\}$.

Let $\mathcal{M}(\Delta)$ *be the multiplication table of the algebra* $\mathcal{A}(\Delta)$*, and assume that the height of the structure constants are bounded by* $\Upsilon(\Delta)$*. Also, let*

$$d_s := \deg_{x_{l+s}}(\mathbf{g}_s), \quad 1 \leq s \leq m.$$

For $\mathbf{f}, \mathbf{h} \in \mathcal{A}(\Delta)[x_{n+1}, \ldots, x_{n+c}]$ *let*

$$\{(\Delta_1, \mathcal{M}(\Delta_1)) \ldots, (\Delta_r, \mathcal{M}(\Delta_r))\} = \mathbf{unmixed}_m^l(\Delta, \mathcal{M}(\Delta), \mathbf{f}, \mathbf{h})$$

where $\Delta_j = \{\mathbf{g}_1^{(j)}, \ldots, \mathbf{g}_m^{(j)}\}$ *for* $1 \leq j \leq r$*. Assume that for all* $1 \leq s \leq m$

$$\deg_{x_{l+s}}(\mathbf{g}_s^{(j)}) \leq \tilde{d}_s, \quad 1 \leq j \leq r.$$

Then for each polynomial $\mathbf{p}$ *occurring in the computation we have*

$$\text{height}(\mathbf{p}) \leq C^m \prod_{s=1}^{m} d_s^2 \cdot \tilde{d}_s^{m-s+1} \cdot (\text{height}(\mathbf{f}, \mathbf{h}) + \Upsilon(\Delta))$$

for some constant C *and*

$$\mathbf{H}(\mathbf{p}) \leq 6^m \cdot \prod_{s=1}^{m} (d_s + 1)^9 \cdot \mathbf{H}(\mathbf{f}, \mathbf{h}).$$

Moreover, the arithmetic circuit over $\Bbbk$ *computing* $\mathbf{unmixed}_m^l(\Delta, \mathcal{M}(\Delta), \mathbf{f}, \mathbf{h})$ *has depth*

$$\left(lm \log(\mathbf{H}(\mathbf{f}, \mathbf{h})) \log(\text{height}(\mathbf{f}, \mathbf{h}) + \Upsilon(\Delta)) \sum_{s=1}^{m} \log(d_s \tilde{d}_s) \right)^{O(1)}$$

and size

$$\left(m\mathbf{H}(\mathbf{f}, \mathbf{h}) \prod_{s=1}^{m} d_s \cdot \prod_{s=1}^{m} \tilde{d}_s \right)^{O(1)} \left((\text{height}(\mathbf{f}, \mathbf{h}) + \Upsilon(\Delta)) \prod_{s=1}^{m} d_s^4 \cdot \prod_{s=1}^{m} (c \cdot \tilde{d}_s)^{m+3} \right)^{2l}$$

for some constant c*.*

Proof: The computation of **unmixed** has a tree structure. The computation tree has levels $m \geq l \geq 0$. At each level we create branches corresponding to the degrees of the polynomials in (4.16), then we call **unmixed** recursively in (4.19), and finally we compute the output of that level using the output of the recursive call. Consider a path of the computation tree with the successive recursive calls

$$\mathbf{unmixed}_m^l(\Delta_m, \mathcal{M}(\Delta_m), \mathbf{f}_m, \mathbf{h}_m), \ldots, \mathbf{unmixed}_1^l(\Delta_1, \mathcal{M}(\Delta_1), \mathbf{f}_1, \mathbf{h}_1)$$

where $\Delta_s := \{\mathbf{g}_1, \ldots, \mathbf{g}_s\}$ $(1 \leq s \leq m)$, $\Delta_0 := \emptyset$, $\mathbf{f}_m = \mathbf{f}$, $\mathbf{h}_m = \mathbf{h}$ and for $m - 1 \geq s \geq 0$ the polynomials $\mathbf{f}_s, \mathbf{h}_s$ are the input of the recursive calls defined in (4.19).

First we give upper bounds for height$(\mathbf{p})$ and $\mathbf{H}(\mathbf{p})$ where $\mathbf{p} = \mathbf{f}_s$ or $\mathbf{p} = \mathbf{h}_s$ for some $0 \leq s \leq m$. For $0 \leq s \leq m$ denote

$$\text{Input}(s) := \max\{\text{height}(\mathbf{f}_s), \text{height}(\mathbf{h}_s)\}, \quad \mathbf{H}(s) := \max\{\mathbf{H}(\mathbf{f}_s), \mathbf{H}(\mathbf{h}_s)\}.$$

We use induction on $m - s$. Let $s = m - 1$. To compute $\mathbf{f}_{m-1}$ and $\mathbf{h}_{m-1}$ we assume that all the computations are conducted using arithmetics in $\mathcal{A}(\Delta_{m-1})$. Note that the height of the structure constants of $\mathcal{A}(\Delta_{m-1})$ are also bounded by $\Upsilon(\Delta)$.

First we computed the j-th sub-resultants

$$\varphi_k^{(j)}(y, z) := \text{RES}_{x_n}^{(j)}(\mathbf{g}_m, \ \mathbf{f} + \sum_{l=1}^{k} \mathbf{g}_m^{(l)} \cdot y^{l-1} + z \cdot \mathbf{h}), \quad 1 \leq k \leq d,$$

for $0 \leq j \leq d$, where y and z are new variables. Using Proposition 3.3.1, we have

$$\begin{aligned} \text{height}(\varphi_k^{(j)}(y, z)) &\leq 2d_m \cdot \log(d_m)(\text{Input}(m) + \Upsilon(\Delta)), \\ \mathbf{H}(\varphi_k^{(j)}(y, z)) &\leq (d_m + 1)^3 \cdot \mathbf{H}(m). \end{aligned}$$

Since $\mathbf{f}_{m-1} = \Phi_{i,\bar{v}}$ is the combination of at most d_m^6 polynomials of the form $\varphi_k^{(u)}(y,z)$ using the powers of a new variable w, we have

$$\begin{aligned} \text{height}(\mathbf{f}_{m-1}) &\leq 2d_m \cdot \log(d_m)(\text{Input}(m) + \Upsilon(\Delta)), \\ \mathbf{H}(\mathbf{f}_{m-1}) &\leq (d_m+1)^9 \cdot \mathbf{H}(m). \end{aligned}$$

The polynomial $\mathbf{h}_{m-1} = \Psi_{i,\bar{v}}$ is the product of six polynomials of the form $\varphi_k^{(u)}(y,z)$, therefore

$$\begin{aligned} \text{Input}(\mathbf{h}_{m-1}) &\leq 12d_m \cdot \log(d_m)(\text{Input}(m) + \Upsilon(\Delta)), \\ \mathbf{H}(\mathbf{h}_{m-1}) &\leq 6(d_m+1)^3 \cdot \mathbf{H}(m). \end{aligned}$$

Therefore

$$\begin{aligned} \text{Input}(m-1) &\leq 12 \cdot d_m \cdot \log(d_m)(\text{Input}(m) + \Upsilon(\Delta)), \\ \mathbf{H}(m-1) &\leq 6(d_m+1)^9 \mathbf{H}(m). \end{aligned}$$

We can prove by induction that

$$\begin{aligned} \text{Input}(0) &\leq m \cdot 12^m \cdot \prod_{s=1}^{m} d_s \cdot \log(d_s) \cdot (\text{Input}(m) + \Upsilon(\Delta)) \\ \mathbf{H}(0) &\leq 6^m \prod_{s=1}^{m} (d_s+1)^9 \mathbf{H}(m). \end{aligned}$$

Next we give upper bounds for the heights of the polynomials computed after the recursive calls at each level. Note that all the polynomials $\mathbf{p}$ occurring in this part of the algorithm are in $\mathbb{k}[x_1, \ldots, x_{l+s}]$, therefore $\mathbf{H}(\mathbf{p}) = 1$.

Denote by $\text{Output}(s)$ the maximum height of the polynomials computed in level s. If $s = 0$ then $\text{Output}(0) = \text{Input}(0)$. Without loss of generality we can assume that $\text{Input}(s) \leq \text{Input}(0) \leq \text{Output}(s)$ for $1 \leq s \leq m$.

Assume that we already computed Output$(m-1)$, an upper bound for the polynomials computed at level $m-1$. Hence Output$(m-1)$ is an upper bound for the height of all $(\Lambda_{i.\bar{v}}, \mathcal{M}(\Lambda_{i.\bar{v}})) \in \mathcal{L}_{i.\bar{v}}$ defined in (4.20).

After the recursive call in (4.19) we computed the polynomials

$$\mathbf{d}_{t.i.v_t} := \mathbf{ggcd_n}(\mathbf{g}_m,\, \mathbf{g}'_m, \ldots, \mathbf{g}_m^{(k)},\, \mathbf{f}_m,\, \epsilon \cdot \mathbf{h}_m) \in \Bbbk[x_1, \ldots, x_{l+1}]$$

where $1 \leq t \leq 6$, $k \in \{i-1,\, i,\, i+1\}$ and $\epsilon \in \{0, 1\}$ depending on the value of t, as defined in (4.16). Note that $\deg_{x_n}(\mathbf{d}_{t.i.v_t}) \leq d_m$, since $\mathbf{d}_{t.i.v_t}$ divides $\mathbf{g}_m$ over $\mathbf{K}(\mathcal{P})$ for all $\mathcal{P} \in \mathrm{Ap}(\Lambda_{i.\bar{v}})$.

The coefficients of the polynomial $\mathbf{d}_{t.i.v_t}$ are the solutions of the linear system corresponding to the Sylvester matrix of $\mathbf{g}_m$ and $\mathbf{f}_m + \sum_{j=1}^{k} \mathbf{g}_m^{(j)} \cdot y^{j-1} + z \cdot \mathbf{h}_m$ such that variables with index $> n$ are substituted by elements from $\Bbbk$. Therefore, the degree in these variables do not contribute to the height of $\mathbf{d}_{t.i.v_t}$. Since the determinant of the linear system is

$$\varphi_k^{(d)} = \mathrm{RES}_{x_{l+1}}^{(v_t)}(\mathbf{g}_m,\, \mathbf{f}_m + \sum_{j=1}^{k} \mathbf{g}_m^{(j)} \cdot y^{j-1} + z \cdot \mathbf{h}_m)$$

for some d, using Cramer's rule, we have that $\mathbf{d}_{t.i.v_t}$ does not depend on the output of the recursive call, and

$$\mathrm{height}(\mathbf{d}_{t.i.v_t}) \leq \mathrm{Input}(m-1).$$

Next we computed

$$\overline{\mathrm{lc}(\mathbf{d}_{t.i.v_t})} := \mathbf{pinverse}_0^l(\, \Lambda_{i.\bar{v}},\, \mathrm{lc}(\mathbf{d}_{t.i.v_t})).$$

Applying Theorem 3.4.1 we have that

$$\begin{aligned} \text{height}(\overline{\text{lc}(\mathbf{d}_{t.i.v_t})}) &\leq D \cdot (\text{height}(\text{lc}(\mathbf{d}_{t.i.v_t})) + \Upsilon(\Lambda_{i.v_t})) \\ &\leq (\prod_{s=1}^{m-1} \tilde{d}_s)(\text{Input}(m-1) + \text{Output}(m-1)) \end{aligned}$$

where D is the dimension of the algebra $\mathcal{A}(\Lambda_{i.\vec{v}})$ over $\Bbbk(x_1, \ldots, x_l)$. This also gives an upper bound for the height of $\bar{\mathbf{d}}_{t.i.v_t} = \overline{\text{lc}(\mathbf{d}_{t.i.v_t})} \cdot \mathbf{d}_{t.i.v_t}$, where the multiplication is in the algebra $\mathcal{A}(\Lambda_{i.\vec{v}})$.

Next we computed

$$\mathbf{p}_{i.\vec{v}}^{(1)} := \bar{\mathbf{d}}_{1.i.v_1}\bar{\mathbf{d}}_{3.i.v_3}\bar{\mathbf{d}}_{5.i.v_5}^2, \quad \mathbf{p}_{i.\vec{v}}^{(2)} := \bar{\mathbf{d}}_{2.i.v_2}^2\bar{\mathbf{d}}_{4.i.v_4}\bar{\mathbf{d}}_{6.i.v_6}$$

and found $\mathbf{q}_{i.\vec{v}} \in \Bbbk[x_1, \ldots, x_n]$ such that

$$\text{lc}(\mathbf{p}_{i.\vec{v}}^{(2)})^{\alpha}\mathbf{p}_{i.\vec{v}}^{(1)} = \mathbf{p}_{i.\vec{v}}^{(2)}\mathbf{q}_{i.\vec{v}} + \mathbf{r}_{i.\vec{v}}, \quad \text{where} \quad \mathbf{r}_{i.\vec{v}} \in \text{Rep}(\Lambda_{i.\vec{v}}).$$

Since $\deg_{x_n}(\mathbf{p}_{i.\vec{v}}^{(2)}) \leq 4 \cdot d_m$, the coefficients in the variable x_n of the polynomial $\mathbf{q}_i$ are solutions of a linear system of size $(4d_m) \times (4d_m)$. This implies that

$$\begin{aligned} \text{height}(\mathbf{q}_{i.\vec{v}}) &\leq 4d_m \cdot \log(d_m) \cdot (4 \cdot \text{height}(\mathbf{p}_{i.\vec{v}}^{(2)}) + \Upsilon(\Lambda_{i.\vec{v}})) \\ &\leq 20 \cdot d_m \cdot \log(d_m) \cdot (\prod_{s=1}^{m-1} \tilde{d}_s) \cdot \text{Output}(m-1). \end{aligned}$$

We defined the unmixed set $\Delta_{i.\vec{v}} := \Lambda_{i.\vec{v}} \cup \{\mathbf{q}_{i.\vec{v}}\}$. Note that

$$\deg_{x_n}(\mathbf{q}_{i.\vec{v}}) \leq \tilde{d}_m.$$

by definition.

To compute the multiplication table $\mathcal{M}(\Delta_{i.\vec{v}})$ of $\mathcal{A}(\Delta_{i.\vec{v}})$ we solved a linear system of size $\leq \tilde{d}_m$ whose entries were the coefficients of $\mathbf{q}_i$ for each monomial

$x_{l+1}^{\alpha_1} \cdots x_n^{\alpha_m}$, where $0 \leq \alpha_s < 2\tilde{d}_s$. Therefore, the structure constants of $\mathcal{A}(\Delta_{i,\bar{v}})$ have height at most

$$\begin{aligned}\Upsilon(\Delta_{i,\bar{v}}) &\leq \tilde{d}_m \cdot \log(\tilde{d}_m)(\text{height}(\mathbf{q}_{i,\bar{v}}) + \Upsilon(\Lambda_{i,\bar{v}})) \\ &\leq 21 \cdot d_m \cdot \log(d_m)(\prod_{s=1}^{m} \tilde{d}_s) \cdot \log(\tilde{d}_m) \cdot \text{Output}(m-1).\end{aligned}$$

This also gives an upper bound for the heights of the polynomials computed at level m, i.e.

$$\text{Output}(m) \leq 21 \cdot d_m \cdot \log(d_m)(\prod_{s=1}^{m} \tilde{d}_s) \cdot \log(\tilde{d}_m) \cdot \text{Output}(m-1).$$

Then, using induction, we get

$$\begin{aligned}\text{Output}(m) &\leq 21 \cdot d_m(\prod_{s=1}^{m} \tilde{d}_s) \cdot \log(d_m) \cdot \log(\tilde{d}_m) \cdot \text{Output}(m-1) \\ &\leq 21 d_m(\prod_{s=1}^{m} \tilde{d}_s) \log(d_m) \log(\tilde{d}_m) \cdot 21 d_{m-1}(\prod_{s=1}^{m-1} \tilde{d}_s) \log(d_{m-1}) \log(\tilde{d}_{m-1}) \\ &\quad \cdots 21 d_1 \tilde{d}_1 \log(d_1) \log(\tilde{d}_1) \cdot \text{Output}(0) \\ &\leq m \cdot 21^m \cdot 12^m \prod_{s=1}^{m} d_s^2 \log^2(d_s) \log(\tilde{d}_s) \cdot \tilde{d}_s^{m-s+1} \cdot (\text{Input}(m) + \Upsilon(\Delta)) \\ &\leq C^m \cdot (\text{height}(\mathbf{f}, \mathbf{h}) + \Upsilon(\Delta)) \prod_{s=1}^{m} d_s^3 \cdot \tilde{d}_s^{m-s+2}.\end{aligned}$$

To give an upper bound for the depth and the size of the arithmetic circuit over $\mathbb{k}$ computing $\mathbf{unmixed}_m^l(\Delta, \mathcal{M}, \mathbf{f}, \mathbf{h})$, first we consider the depth of the computation of the polynomials $\mathbf{f}_s, \mathbf{h}_s$, the input of the recursive calls defined in (4.19) for $m-1 \geq s \geq 0$.

For $s = m-1$ first we computed

$$\varphi_k^{(j)}(y,z) = \text{RES}_{x_n}^{(j)}(\mathbf{g}_m,\ \mathbf{f}_m + \sum_{l=1}^{k} \mathbf{g}_m^{(l)} \cdot y^{l-1} + z \cdot \mathbf{h}_m), \quad 1 \leq k \leq d,$$

which is the determinant of a matrix of size at most $(2d_m) \times (2d_m)$ with entries from $\mathcal{A}(\Lambda)[x_{n+1}, \ldots, x_{n+c+3}]$. As we noted before, we can replace each polynomial $\mathrm{p} \in \mathcal{A}(\Lambda)[x_{n+1}, \ldots, x_{n+c+3}]$ by a polynomial $\bar{\mathrm{p}} \in \mathcal{A}(\Lambda)[x_{n+1}]$ with

$$\deg_{x_{n+1}}(\bar{\mathrm{p}}) = \mathbf{H}(\mathrm{p}).$$

An $N \times N$ determinant over an arbitrary commutative ring can be computed by a uniform circuit with size $O(N^{3.5})$ and depth $O(\log^2(N))$, by [Ber84]. We can compute the product and sum of two polynomials $\mathrm{p}, \mathrm{p}' \in R[x]$ over an arbitrary commutative ring in depth $O(\log(\deg_x(\mathrm{p})) + \log(\deg_x(\mathrm{p}')))$ and size $O(\deg_x(\mathrm{p})^2 \cdot \deg_x(\mathrm{p}')^2)$. By proposition 3.3.1 the arithmetic circuit computing the product of k elements of $\mathcal{A}(\Delta)$ of height at most d has depth at most

$$O(l \log(D) \log^2(k) \log(d + \Upsilon(\Delta)))$$

and size at most

$$O(D^3 k \log(k)(k \log(k)(d + \Upsilon))^{2l}).$$

Therefore

$$\begin{aligned}
\mathrm{Depth}(\varphi_k^{(j)}(y, z)) &\leq c_1 \log(\mathbf{H}(\mathbf{f}_m)\mathbf{H}(\mathbf{h}_m)d_m) \\
&\quad \cdot l \log(D) \log^2(d_m) \log(\mathrm{height}(\mathbf{f}_m, \mathbf{h}_m) + \Upsilon(\Delta)) \\
\mathrm{Size}(\varphi_k^{(j)}(y, z)) &\leq c_2 \mathbf{H}(\mathbf{f}_m)^2 \mathbf{H}(\mathbf{h}_m)^2 d_m^6 D^3 d_m^4 (d_m^4 (\mathrm{height}(\mathbf{f}_m, \mathbf{h}_m) + \Upsilon(\Delta)))^{2l}
\end{aligned}$$

where D denotes the dimension of $\mathcal{A}(\Delta)$, i.e. $D = \prod_{s=1}^{m} d_s$. This also gives an upper bound for the height of the circuit computing $\mathbf{f}_{m-1} = \Phi_{i,\vec{v}}$ and $\mathbf{h}_{m-1} = \Psi_{i,\vec{v}}$. By

induction we get that

$$\begin{aligned}
\text{Depth}(0) &\leq \sum_{s=0}^{m-1} \text{Depth}(\mathbf{f}_s, \mathbf{h}_s) \\
&\leq \sum_{s=0}^{m-1} c_1 \log(\mathbf{H}(s)) l \log(D) \log^3(d_s) \log(\text{Input}(s) + \Upsilon(\Delta_s)) \\
&\leq c_1 l \log(D) \log(\mathbf{H}(0)) \log(\text{Input}(0) + \Upsilon(\Delta)) \sum_{s=0}^{m-1} \log^3(d_s) \\
&\leq c_1' l m \log^6(D) \log(\mathbf{H}(m)) \log(\text{Input}(m) + \Upsilon(\Delta)). \qquad (4.29)
\end{aligned}$$

Since at each level of the computation tree we create at most d_s^7 branches, we get for the size of the circuit computing all the recursive calls that

$$\begin{aligned}
\text{Size}(0) &\leq \sum_{s=0}^{m-1} \left(\prod_{t=s}^{m-1} d_t^7 \right) \text{Size}(\mathbf{f}_s, \mathbf{h}_s) \\
&\leq \sum_{s=0}^{m-1} \left(\prod_{t=s}^{m-1} d_t^7 \right) c_2 \mathbf{H}(s)^2 d_s^{10} D^3 (d_s^4 (\text{Input}(s) + \Upsilon(\Delta_s)))^{2l} \\
&\leq c_2 D^3 \mathbf{H}(0)^2 (\text{Input}(0) + \Upsilon(\Delta))^{2l} \left(\prod_{t=0}^{m-1} d_t^7 \right) \sum_{s=0}^{m-1} d_s^{8l+10} \\
&\leq C^m m D^{30} \cdot \left(\sum_{s=0}^{m-1} d_s^{8l+10} \right) \cdot (D(\text{Input}(m) + \Upsilon(\Delta)))^{2l} \mathbf{H}(m)^2. \qquad (4.30)
\end{aligned}$$

Next we give upper bounds for the size and depth of the arithmetic circuit computing the output at each level of the computation tree. For level $s = m$ we first computed the polynomials $\mathbf{d}_{t,i,v_t}$ defined in (4.16), which involved the computation of at most d_m determinants each of size $(2d_m) \times (2d_m)$ with entries from $\mathcal{A}(\Lambda)$ of height at most $\text{Input}(m-1)$. By Theorem 3.5.2 we have that the arithmetic circuit computing $\mathbf{d}_{t,i,v_t}$ has depth

$$\begin{aligned}
&\leq O(l \log(D) \log^2(d_m^{3.5}) \log(d_m(\text{height}(\mathbf{f}_m, \mathbf{h}_m) + \Upsilon))) \\
&\leq O(l \log(D) \log^2(d_m) \log(\text{height}(\mathbf{f}_m, \mathbf{h}_m) + \Upsilon(\Delta))) \qquad (4.31)
\end{aligned}$$

and size

$$\begin{aligned} &\leq O(D^3 d_m^{3.5}(d_m^{3.5} d_m(\text{height}(\mathbf{f}_m, \mathbf{h}_m) + \Upsilon))^{2l}) \\ &\leq O(D^3 d_m^{3.5}(d_m^{4.5}(\text{height}(\mathbf{f}_m, \mathbf{h}_m) + \Upsilon(\Delta)))^{2l}). \end{aligned} \tag{4.32}$$

Then we computed $\overline{\text{lc}(\mathbf{d}_{t.i.v_t})} = \mathbf{pinverse}_{m-1}^{l}(\Lambda_{i.\vec{v}}, \text{lc}(\mathbf{d}_{t.i.v_t}))$. By Theorem 3.4.1 the arithmetic circuit computing $\overline{\text{lc}(\mathbf{d}_{t.i.v_t})}$ has depth

$$\begin{aligned} &\leq C \cdot l \cdot \log^2\left(\tilde{D}(\text{height}(\text{lc}(\mathbf{d}_{t.i.v_t}) + \Upsilon(\Lambda_{i.\vec{v}})))\right) \\ &\leq C' \cdot l \cdot \log^2(\tilde{D}\text{Output}(m)) \\ &\leq O(l \cdot m^2 \left(\sum_{s=1}^{m} \log(d_s \tilde{d}_s)\right)^2 \log^2(\text{height}(\mathbf{f}_m, \mathbf{h}_m) + \Upsilon(\Delta))) \end{aligned} \tag{4.33}$$

for some constants C, C', and size

$$\begin{aligned} &\leq C_1 \tilde{D}^{4.5}(\tilde{D} \cdot \text{Output}(m))^{2l} \\ &\leq \prod_{s=1}^{m} \tilde{d}_s^{4.5} \cdot \left(C_2^m(\text{height}(\mathbf{f}_m, \mathbf{h}_m) + \Upsilon(\Delta)) \prod_{s=1}^{m} d_s^3 \tilde{d}_s^{m-s+3}\right)^{2l}, \end{aligned} \tag{4.34}$$

where $\tilde{D}$ is the dimension of the algebra $\mathcal{A}(\Lambda_{i.\vec{v}})$, hence $\tilde{D} \leq \prod_{s=1}^{m} \tilde{d}_s$, and C_1, C_2 are constants.

Next we computed $\Delta_{i.\vec{v}} = \Lambda_{i.\vec{v}} \cup \{\mathbf{q}_{i.\vec{v}}\}$ and the multiplication table $\mathcal{M}(\Delta_{i.\vec{v}})$. By Corollary 3.3.5 the arithmetic circuit computing $\mathcal{M}(\Delta_{i.\vec{v}})$ has depth

$$\begin{aligned} &\leq c \cdot l \cdot \log^3(\prod_{s=1}^{m} \tilde{d}_s)\text{Output}(m) \\ &\leq O\left(lm^2 \left(\sum_{s=1}^{m} \log(d_s \tilde{d}_s)\right)^3 \log^3(\text{height}(\mathbf{f}_m, \mathbf{h}_m) + \Upsilon(\Delta))\right) \end{aligned} \tag{4.35}$$

and size

$$\begin{aligned}
&\leq c' \cdot \tilde{D}^3 \sum_{s=1}^{m} \tilde{d}_s(\tilde{d}_s(\text{height}(\tilde{\mathbf{g}}_s) + \Upsilon(\Delta_{i,\vec{v}}))^{2l} \\
&\leq c' \cdot \text{Output}(m)^{2l} \cdot \left(\sum_{s=1}^{m} \tilde{d}_s\right)^{2l} \cdot \prod_{s=1}^{m} \tilde{d}_s^4 \\
&\leq \left(\prod_{s=1}^{m} \tilde{d}_s^4\right)\left((c'')^m \cdot (\text{height}(\mathbf{f}_m, \mathbf{h}_m) + \Upsilon(\Delta)) \prod_{s=1}^{m} d_s^3 \cdot \prod_{s=1}^{m} \tilde{d}_s^{m+3}\right)^{2l} \qquad (4.36)
\end{aligned}$$

for some constants c, c', c''.

Using the upper bounds in (4.29), (4.31), (4.33) and (4.35), we get that the arithmetic circuit computing $\mathbf{unmixed}_m^l(\Delta, \mathcal{M}(\Delta), \mathbf{f}, \mathbf{h})$ has depth

$$\begin{aligned}
&\leq c_1' lm \log^6(D) \log(\mathbf{H}(m)) \log(\text{Input}(m) + \Upsilon(\Delta)) \\
&\quad + c_2'' l \left(m \log(\text{height}(\mathbf{f}_m, \mathbf{h}_m) + \Upsilon(\Delta)) \sum_{s=1}^{m} \log(d_s \tilde{d}_s)\right)^3 \\
&\leq \left(lm \log(\mathbf{H}(\mathbf{f}, \mathbf{h})) \log(\text{height}(\mathbf{f}, \mathbf{h}) + \Upsilon(\Delta)) \sum_{s=1}^{m} \log(d_s \tilde{d}_s)\right)^{O(1)}.
\end{aligned}$$

Using the upper bounds in (4.30), (4.32), (4.34) and (4.36) and the fact that the number of branches that give non-trivial components do not exceed $\deg(V_{\text{Rep}}(\Delta)) \leq \prod_{s=1}^{m} d_s$, we get that the arithmetic circuit computing

$$\mathbf{unmixed}_m^l(\Delta, \mathcal{M}(\Delta), \mathbf{f}, \mathbf{h})$$

has size

$$\begin{aligned}
&\leq C^m m D^{30} \cdot \left(\sum_{s=0}^{m-1} d_s^{8l+10}\right) \cdot (D(\text{Input}(m) + \Upsilon(\Delta)))^{2l} \cdot \mathbf{H}(m)^2. \\
&+ m \cdot \left(\prod_{s=1}^{m} d_s\right)\left(\prod_{s=1}^{m} \tilde{d}_s^4\right)\left((c'')^m \cdot (\text{height}(\mathbf{f}, \mathbf{h}) + \Upsilon(\Delta)) \prod_{s=1}^{m} d_s^3 \cdot \prod_{s=1}^{m} \tilde{d}_s^{m+3}\right)^{2l} \\
&\leq \left(m\mathbf{H}(\mathbf{f}, \mathbf{h}) D \cdot \prod_{s=1}^{m} \tilde{d}_s\right)^{O(1)} \left((\text{height}(\mathbf{f}, \mathbf{h}) + \Upsilon(\Delta)) D^4 \cdot \prod_{s=1}^{m} (c'' \cdot \tilde{d}_s)^{m+3}\right)^{2l}
\end{aligned}$$

where C is the constant from (4.30), and c'' is the constant from (4.36). This concludes the proof of the theorem. ■

Bibliography

[AM69] M. F. Atiyah and I.G. MacDonald. *Introduction to commutative algebra.* Addison-Wesley Publishing CO., 1969.

[BCK88] B. Buchberger, G. E. Collins, and B. Kutzler. Algebraic methods for geometric reasoning. *Ann. Rev. Comput. Sci.*, 3:85–119, 1988.

[Ber84] Stuart J. Berkowitz. On computing the determinant in small parallel time using a small number of processors. *Information Processing Letters*, (18):147–150, 1984.

[BKR85] Michael Ben-Or, Dexter Kozen, and John Reif. The complexity of elementary algebra and geometry. *J. Comput. Syst. Sci.*, 32:251–264, 1985.

[Bro87] W. Dale Brownawell. Bounds for the degrees in the Nullstellensatz. *Annals of Mathematics*, 126:577–591, 1987.

[Buc84] B Buchberger. *Gröbner bases: An algorithmic method in polynomial ideal theory*, volume 174 of *Lecture Notes in Computer Science*, pages 100–107. Springer, 1984.

[Buc85] B Buchberger. Gröbner bases: An algorithmic method in polynomial ideal theory. In Bose, editor, *Multidimensional System Theory*, pages 184–229. D.Riedel Publishing Co., 1985.

[Can90] John Canny. Generalized characteristic polynomials. *J. Symbolic Computation*, 9:241–250, 1990.

[Chi84] A. L. Chistov. An algorithm of polynomial complexity for factoring polynomials, and determination of the components of a variety in a subexponential time. *Zap. Nauchn. Se,. Leningrad. Otdel. Inst. Steklov (LOMI)*, 137:124–188, 1984. Russian, English summary.

[CP93] John Canny and Paul Pedersen. An algorithm for the newton resultant. Technical report, Cornell University, Computer Science Department, 1993.

[DD84] Claire Dicrescenzo and Dominique Duval. *Computations on curves*, volume 174 of *Lecture Notes in Computer Science*, pages 100–107. Springer, 1984.

[DD85] Claire Dicrescenzo and Dominique Duval. Algebraic computations on algebraic numbers. In *Informatique et Calcul*, pages 54–61. Wiley-Masson, 1985.

[EC95] Ioannis Z. Emiris and John F. Canny. Efficient incremental algorithms for the sparse resultant and the mixed volume. *J. Symbolic Computation*, 20:117–149, 1995.

[EP97] Ioannis Z. Emiris and Victor Y. Pan. The structure of sparse elimination matrices. In *Proceedings of ISSAC'97*, pages 189–196, 1997.

[Ful93] William Fulton. *Introduction to Toric Varieties.* Princeton University Press, 1993.

[GH91] Marc Giusti and Joos Heintz. Algorithmes - disons rapides - pour la décomposition d'une variété algébrique en composantes irréductibles et équidimensionnelles. In Teo Mora and Carlo Traverso, editors, *Effective Methods in Algebraic Geometry*, pages 169–194. Birkhäuser, 1991.

[GKZ94] I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky. *Discriminants, Resultants and Multidimensional Determinants.* Birkhäuser, 1994.

[GM91] G. Gallo and B. Mishra. Wu-Ritt characteristic sets and their complexity. *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, 6:111–136, 1991.

[Gri84] D. Yu. Grigorév. Factoring polynomials over a finite field and solving systems of algebraic equations. *Zap. Nauchn. Se,. Leningrad. Otdel. Inst. Steklov (LOMI)*, 137:20–79, 1984. Russian, English summary.

[GS93] Peter Gritzmann and Bernd Sturmfels. Minkowski addition of polytopes, computational complexity and application to grobbner bases. *SIAM Journal of Discrete Mathematics*, 6:246–269, 1993.

[Har77] Robin Hartshorne. *Algebraic Geometry.* Springer-Verlag, 1977.

[Ier89] Douglas John Ierardi. *The complexity of quantifier elimination in the theory of an algebraically closed field.* PhD thesis, Cornell University, 1989.

[IK93] Doug Ierardi and Dexter Kozen. Parallel resultant computation. In John Reif, editor, *Synthesis of Parallel Algorithms*, pages 679–720. Morgan Kauffman, 1993.

[IRS94] Gabor Ivanyos, Lajos Ronyai, and Agnes Szanto. Decomposition of algebras over $f_q(x_1, \ldots, x_m)$. *Applicable Algebra in Engineering, Communication and Computing*, 5(2):71–90, 1994.

[Kal93] Michael Kalkbrener. A generalized euclidean algorithm for computing triangular representations of algebraic varieties. *J. Symb. Comp.*, 15:143–167, 1993.

[Kal94] Michael Kalkbrener. Prime decomposition of radicals in polynomial rings. *J. Symbolic Computation*, 18:365–372, 1994.

[Kal96] Michael Kalkbrener. Algorithmic properties of polynomial rings. Habilitationsschrift, 1996.

[Kol88] János Kollár. Sharp effective Nullstellensatz. *Journal of the American Mathematical Society*, 1(4), 1988.

[Koz94] Dexter Kozen. Efficient resolution of singularities of plane curves. Technical report, Cornell University, Mathematical Science Institute, 1994.

[Laz81] Daniel Lazard. Resolution des systemes d'equations algebriques. *Theoret. Comp. Sci.*, 15(1), 1981. French, English summary.

[Mac16] F. S. Macauley. *The algebraic theory of modular systems.* Cambridge University Press, 1916. Revised reprint of the 1916 original.

[May89] Ernst Mayr. Membership in polynomial ideals over $\mathbb{Q}$ is exponential space comlete. In *STACS 89*, Lecture Notes in Computer Science, pages 400–406. Springer, 1989.

[MWW95] Michal Mnuk, Bernhard Wall, and Franz Winkler. CASA reference manual. Technical Report 5, RISC-Linz, 1995.

[PW95] J. Pfalzgraf and D. Wang, editors. *Automated Practical Reasoning.* Texts and Monographs in Symbolic Computation. Springer-Verlag, 1995.

[Rit50] Joseph Fels Ritt. *Differential algebra.* American Mathematical Society, 1950.

[RW96] J. Maurice Rojas and Xiaoshen Wang. Counting affine roots of polynomial systems via pointed newton polytopes. *Journal of Complexity*, 12(2), 1996.

[Sch80] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. ACM*, 27(4):707–717, 1980.

[Stu93] Bernd Sturmfels. Sparse elimination theory. In David Eisenbud and Lorenzo Robbiano, editors, *Computational algebraic geometry and commutative algebra (Cortona, 1991)*, volume XXXIV of *Sympos. Math.*, pages 264–298. Cambridge, 1993.

[Sza97] Agnes Szanto. Complexity of the Wu-Ritt decomposition. In *Proceedings of PASCO'97*, pages 139–149. ACM Press, 1997.

[Tei90] Jeremy Teitelbaum. The computational complexity of the resolution of plane curve singularities. *Math. Comp.*, 54:797–837, 1990.

[vdW49] B.L. van der Wearden. *Modern algebra.* Frederick Ungar Publishing Co., 1949.

[vzG84] Joachim von zur Gathen. Parallel algorithms for algebraic problems. *SIAM J. Comput.*, 13(4):802–824, 1984.

[Wan92] Dongming Wang. Irreducible decomposition of algebraic varieties via characteristic sets and Gröbner bases. *Computer Aided Geometric Design*, 9:471–484, 1992.

[Wan95] Dongming Wang. Elimination method for mechanical theorem proving in geometries. *Annals of Math. and Artificial Intelligence*, 13:1–24, 1995.

[Wu84] Wen-Tsün Wu. Basic principles of mechanical theorem proving in elementary geometries. *J. Syst. Sci. Math. Sci.*, 4:207–235, 1984.