Complexity of Triangular Representations of Algebraic Sets

Eli Amzallag  Gleb Pogudin  Mengxiao Sun  N. Thieu Vo

October 4, 2016

Abstract

Szanto presented an algorithm to determine an unmixed representation of the radical of a given polynomial ideal. Szanto provided an asymptotic upper bound for the degrees of the polynomials occurring in the computation. The degrees of these polynomials in their leading variables were bounded effectively, but for the non-leading variables, only a big $O$ bound was given. In this paper, by performing a detailed analysis of the Szanto’s algorithm, we present an explicit bound. In addition, we also bound the number of components in the output. Finally, we compare our degree bounds to ones of Gröbner basis computation.

1 Introduction

A long-standing problem in polynomial computation has been how to most efficiently represent a given algebraic set without sacrificing important information about it. Similarly, how might we most efficiently represent its corresponding ideal? Over an algebraically closed field, Hilbert’s Nullstellensatz informs us that both of these issues can be addressed by studying radical ideals.

Gröbner bases have afforded one solution to this problem ([1, 2]). These representations allow ideal membership tests, determining consistency of the corresponding system, and preserve the zero set of the ideal. However, they are also often quite costly to compute in the following sense: given a generating set for an ideal where each element in the generating set has degree at most $d$, the degree of an element in a Gröbner basis can be as large as doubly exponential (with a base of $d$) in the number of variables ([8, 22, 23]). And similar bounds are given for computing a Gröbner basis for the radical of an ideal in [6, 18]. In fact, Chistov’s results in [6] imply double-exponential lower bounds for computing any basis of the radical from a given set of generators of the original ideal in [6].

Thus, efforts to find alternative representations have persisted, with the hope that some of these will be computationally cheaper. One alternative representation that arose independently of Gröbner bases is the notion of a characteristic set, introduced by Ritt in the late 1940s ([24]) and used to solve multivariate polynomial equations by Wu in the late 1970s ([31]). Generalizations of such sets grew out of the work of Lazard and Kalkbrener in [14, 20, 21].
There is much potential for such sets to lower the complexity of existing algorithms or to be used alternately with Gröbner bases, depending on which is expected to be more efficient for an algorithm for given values of parameters. Two examples of this potential can be seen in differential algebra, in the context of effectivizing Differential Nullstellensatz and in Differential Galois Theory. For the former, one may see a forthcoming paper, where a theoretical bound is established using representation of the radical of a polynomial ideal by triangular sets. The proof may be turned into a working algorithm which makes use of Szanto’s algorithm, so our bound will help an analysis of the complexity of its possible implementation. For the latter, it is expected that the complexity of Hrushovski’s algorithm to compute the differential Galois group of a linear differential equation (as described by Feng in [9]) can be reduced by replacing the uses of Gröbner bases by characteristic sets. In fact, any algorithm relying on the use of Gröbner bases can perhaps be made more efficient by applying our results.

Although Lazard noted that triangular sets could pave the way to new methods for solving systems of algebraic equations and gave an algorithm for obtaining a triangular representation from a Gröbner basis, it took some time for an algorithm emerged that allowed computation of a triangular representation from an arbitrary set of generators. Szanto gave an algorithm in [25, 29] for representing the radical of an ideal by triangular sets with some additional special properties and showed that the complexity of this algorithm has better asymptotics than one has for computing a Gröbner basis. To compare this type of representation to one via Gröbner bases, we need numerical upper bounds for the objects in the output of this algorithm. This is what we compute in Sections 3 and 4, after setting up some terminology and notation and recording some auxiliary results we will need in Section 2. Our main results on the degree bounds and the number of components in the output of the algorithm be may found in Theorem 3.8 and Theorem 4.4 respectively.

**Main Result 1** (Theorem 3.8). If the number of given polynomials (each in the variables $x_1, \ldots, x_n$) is not too large, the codimension of the ideal they generate is $m$, and the degree of each of the given polynomials is bounded by $d$, then the degree of any polynomial $p$ in the output satisfies

$$\deg(p) \leq nd^{(4+\rho)m^2}$$

where $\rho$ is some decaying function of $m,n$.

**Main Result 2** (Theorem 4.4). Moreover, for $d,m \geq 2$ the number of components in the output of Szanto’s algorithm is bounded by

$$n\sqrt{2d} + \left( \frac{\pi^6}{272160} \right)^{m-2} \left( \frac{n}{m} \right)^{d^m^2 - 10.5m + 3}$$

We remark that there are also interesting papers solving another important complexity problems about triangular sets, for example, the reader may see [7, 10, 25].
2 Preliminaries

This section is to introduce notation for the paper and to sketch the unmixed representation algorithm by Szanto. Throughout this section, let \( R = k[x_1, x_2, \ldots, x_n] \), where \( k \) is a field of characteristic zero. We fix an ordering on the variables \( x_1 < x_2 < \cdots < x_n \). For a given polynomial \( p \in R \), we let \( \text{height}(p) : = \max \deg_{x_i}(p) \). We also let \( \text{class}(p) \) denote the highest indeterminate appearing in \( p \) and \( \text{lc}(p) \) denote the leading coefficient of \( p \) when \( p \) is written as a univariate polynomial in \( \text{class}(p) \).

**Definition 2.1.** Let \( \Delta = \{g_1, g_2, \ldots, g_m\} \subset R \). We say that \( \Delta \) is a triangular set if \( \text{class}(g_i) < \text{class}(g_j) \) for all \( i < j \).

**Remark 2.2.** Note that any subset of a triangular set is triangular. In what follows, the subsets of \( \Delta \) of particular interest are the ones of the form \( \Delta_j : = \{g_1, g_2, \ldots, g_j\} \), \( 1 \leq j \leq m \) and \( \Delta_0 : = \emptyset \).

Triangular sets give rise to ideals via the following notion.

**Definition 2.3.** Let \( f, g \in R \) with \( \text{class}(g) = x_j \). We first write \( f, g \) as univariate polynomials in \( x_j \). The pseudoremainder of \( f \) by \( g \) is the remainder obtained from considering the coefficients of \( f, g \) as coming from the field \( k(x_1, x_2, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n) \), performing univariate polynomial division of \( f \) by \( g \) with coefficients in this field, and then clearing denominators to obtain some equation of the form:

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

with \( \deg_{x_j}(r) < \deg_{x_j}(g), \alpha \in \mathbb{N} \). We require that \( \alpha \leq \deg_{x_j}(f) - \deg_{x_j}(g) + 1 \). (For uniqueness of \( q, r \), one takes \( \alpha \) minimal.) We sometimes denote \( r \) by \( \text{prem}(f, g) \).

We will not be so much interested in a pseudoremainder of one polynomial by another. Instead, we will be considering pseudoremainders by a triangular set \( \Delta = \{g_1, g_2, \ldots, g_m\} \).

**Definition 2.4.** Let \( \Delta = \{g_1, g_2, \ldots, g_m\} \) be a triangular set and let \( f \in R \). The pseudoremainder of \( f \) by \( \Delta \) is the polynomial \( f_0 \) in the sequence \( f_m = f, f_{s-1} = \text{prem}(f_s, g_s), 1 \leq s \leq m \). We denote \( f_0 \) by \( \text{prem}(f, \Delta) \) and we say that \( f \) is reduced with respect to \( \Delta \) if \( f = \text{prem}(f, \Delta) \).

**Remark 2.5.** The computation of the pseudoremainder of \( f \) by \( \Delta \) gives rise to the equation

\[
\text{lc}(g_m)^{\alpha_m} \cdots \text{lc}(g_1)^{\alpha_1} f = \sum_{s=1}^{m} q_s g_s + f_0
\]

where each \( \alpha_s \leq \deg_{\text{class}(g_s)}(f_s) - \deg_{\text{class}(g_s)}(g_s) + 1 \)

**Definition 2.6.** Given \( \Delta \) a triangular set, we define

\[
\text{Rep}_R(\Delta) : = \{ h \in R \mid \text{prem}(h, \Delta) = 0 \}
\]
Remark 2.7. If it is evident which polynomial ring ∆ is considered as a subset of, we simply write $\text{Rep}(\Delta)$.

Definition 2.8. Suppose $\Delta \subset R$ is a triangular set and that $I \subset R$ is an ideal. We say that $\Delta$ represents $I$ if

$$I = \text{Rep}_R(\Delta)$$

Given an ideal $I \subset R$, we can compute the prime decomposition of its radical, say

$$\sqrt{I} = I_1 \cap \ldots \cap I_r,$$

where each $I_i, 1 \leq i \leq r$ is a prime ideal of $R$ and the decomposition is assumed irredundant. We call the $I_i$ the associated primes of $I$ and denote this collection by $\text{Ap}(I)$. When we write $\text{Ap}(\Delta)$, we shall mean $\text{Ap}(I)$ for $I = \text{Rep}(\Delta)$.

Definition 2.9. We say that $\sqrt{I}$ and the corresponding variety $V(I)$ are unmixed if all the associated prime ideals have the same codimension.

Given an ideal $I$ represented by a triangular set $\Delta$, Kalkbrener found criteria to check if $I$ is unmixed. This is given in the following theorem.

Theorem 2.10. (see [17, Lemma 4.2, p.13]) Let $R' := k[x_1, x_2, \ldots, x_{n-1}]$ and let $\Delta \subset R$ be a triangular set with $I = \text{Rep}_R(\Delta)$. Suppose that $J := \text{Rep}_{R'}(\Delta \cap R')$ is a radical ideal in $R'$ with $\cap_{j=1}^r P_j$ its irredundant prime decomposition and assume that for all $g \in \Delta - R'$ and for all $1 \leq j \leq r$ both of the following conditions hold:

(a) $\text{lc}(g) \notin P_j$

(b) $g$ is square-free over $K(P_j) := \text{Quot}(R'/P_j)$ (the field of fractions of $R'/P_j$)

Then $I$ is a proper, radical ideal. Furthermore, if $J$ is unmixed then so is $I$.

In light of the above theorem, we have the following definition.

Definition 2.11. Let $\Delta \subset R$ be a triangular set. We say that $\Delta$ is unmixed if conditions (a) and (b) in the above theorem hold. If only (a) holds, we call $\Delta$ weakly unmixed.

Remark 2.12. The notions of regular chain, triangular set, and unmixed set have some variations in the literature. However, we follow Kalkbrener and Szanto in their uses of this terminology.

Remark 2.13. If $\Delta$ is an unmixed set, then $\text{Rep}(\Delta)$ is a radical ideal. Moreover, all the prime ideals in the irredundant prime decomposition of $\text{Rep}(\Delta)$ have the same codimension and this common codimension will match the number of elements of $\Delta$. An important fact to note is that the ideal membership problem for $\text{Rep}(\Delta)$ is easily solved by using the pseudo remainder algorithm.

Now we are ready to define the main object we would like to compute.
Definition 2.14. The *unmixed representation* of an ideal $I \subset R$ is a set of unmixed triangular sets such that the intersection of the radicals represented by these unmixed sets is the radical of $I$.

In order to describe Szanto’s algorithm to compute such a representation we need to define some additional objects.

Definition 2.15. Let $\Delta = \{g_1, \ldots, g_m\}$ be a triangular set in $R$ with class $(g_s) = x_{l+s}, d_s := \deg_{x_{l+s}}(g_s)$ and $l + m = n$. We define

- $A(\Delta) := k[x_1, x_2, \ldots, x_l][x_{l+1}, \ldots, x_n]/\langle \Delta \rangle_{k(x_1, x_2, \ldots, x_l)}$, where the subscript reminds us that we treat elements of the field $k(x_1, x_2, \ldots, x_l)$ as scalars and consider the quotient $A(\Delta)$ as an algebra over this field.

- The standard basis of $A(\Delta)$, which we will denote by $B(\Delta)$, is the set $\{x_{l+1}^{\alpha_1} \cdots x_n^{\alpha_m} \mid 0 \leq \alpha_s < d_s, 1 \leq s \leq m\}$

- The set of structure constants of $A(\Delta)$ is the collection of the coordinates of all products of pairs of elements of $B(\Delta)$ in the basis $B(\Delta)$. These structure constants may be organized into a table, which we will refer to as the multiplication table for $A(\Delta)$ and which we will denote by $M(\Delta)$.

- The height of the structure constants of $A(\Delta)$ is the maximum of the heights of the entries of $M(\Delta)$. We denote this quantity by $\Gamma(\Delta)$ or $\Gamma$ when the triangular set under consideration is clear from context. We will also use the notation $\Gamma_j$ for $\Gamma(\Delta_j)$.

We have now defined the objects necessary to describe the algorithm to compute the unmixed representation of the ideal generated by a given set of polynomials.
Algorithm 1 Unordered unmixed representation algorithm

Require: $F = \{f_0, f_1, \ldots, f_k\} \subset k[x_1, \ldots, x_n]$

Ensure: The set $\Theta(F)$ of unmixed sets such that 

$$\sqrt{\langle F \rangle} = \bigcap_{\Delta \in \Theta} \text{Rep}(\Delta)$$

1. Compute the set $\Sigma(F) = \{\Delta | i \subseteq [n]\}$ of weakly unmixed sets such that for every prime ideal $P$ in the irredundant prime decomposition of the ideal $\sqrt{\langle F \rangle}$, if $\dim_{\text{Krull}}(P) = n - |i|$ and $P \cap k[X_i] = \{0\}$ then $\text{Rep}(\Delta) \subseteq P$ (see [29, Thm. 4.1.5, p. 115]). Here, $k[X_i]$ is the ring of polynomials with coefficients in $k$ that only contain variables with index in $i$.

2. For each $\Delta \in \Sigma(F)$, compute the multiplication table $M(\Delta)$ for the algebra $A(\Delta) := k(X_1)[X_{[n]\setminus i}] / \langle \Delta \rangle$.

3. For each pair $(\Delta, M(\Delta))$, compute a set $U(\Delta)$ of unmixed sets containing only components of $V(F)$ by using the subroutine $\text{unmixed}_{[\Delta]}(\Delta, M(\Delta), f, 1)$, where $f = \sum_{j=0}^{k} f_i y^j \in k[x_1, \ldots, x_n, y]$, and the algorithm $\text{unmixed}$ is described in [29, Sec. 4.2].

4. Return $\Theta(F) := \bigcup_{\Delta \in \Sigma(F)} U(\Delta)$. For a more detailed description of this algorithm, we refer the reader to [29].

In computing structure constants for $A(\Delta)$, we will need to reduce products with respect to $\Delta$. In this reduction, degrees of auxiliary variables can go up. The next theorem tells us by how much. (Since we will also find it useful to have a more specific statement regarding a product of two elements of $A(\Delta)$, we record that here as well.)

Proposition 2.16. (see [29 Prop. 3.3.1, p. 76]) Let $\Delta$ be a triangular set and let $a_1, a_2, \ldots, a_k$ be elements of $A(\Delta)$ with heights at most $d$. Moreover, assume that the denominators of the coordinates of $a_1, a_2, \ldots, a_k$ in the basis $B(\Delta)$ divide

$$\prod_{s=1}^{m} \text{lc}(g_s)^{\beta_s} \quad \text{and} \quad \sum_{s=1}^{m} \beta_s \cdot \text{height}(\text{lc}(g_s)) \leq d'$$

Then

- $\text{height}(a_1 a_2) \leq \text{height}(a_1) + \text{height}(a_2) + 2(d' + \Gamma)$ and
- $\text{height}(a_1 a_2 \ldots a_k) \leq kd + k \log k(d' + \Gamma)$

For a proof of the above result, please see the source.

We will also need denominator bounds in reducing an element modulo $\Delta$. That is, we will need bounds on $\alpha_1, \alpha_2, \ldots, \alpha_m$ after performing reduction modulo $\Delta$ to obtain the equation $\prod_{s=1}^{m} \text{lc}(g_s)^{\alpha_s} \cdot f = \sum_{s=1}^{m} q_s g_s + r$. To this end, we will write another mentioned in [29].


but omit the restriction on degrees. The following lemma can be proven by making slight modifications of the matrix description of pseudoremainders offered in the appendix.

**Lemma 2.17.** Let \( f \in k[x_1, x_2, \ldots, x_l], g \in k[x_1, x_2, \ldots, x_n], l \geq n \). For \( \alpha = \deg_{x_n}(f) - \deg_{x_n}(g) + 1 \) there exist \( q, r \in k[x_1, x_2, \ldots, x_l] \) such that

\[
\text{lc}(g)^\alpha f = gq + r, \quad \deg_{x_n}(r) < \deg_{x_n}(g).
\]

We have the following bounds for the degrees of \( q, r \) in the other variables.

- For \( j < n \), we have
  \[
  \deg_{x_j}(q) \leq \alpha \cdot \deg_{x_j}(g) + \deg_{x_j}(f) \quad \text{and} \quad \deg_{x_j}(r) \leq (\alpha + 1) \cdot \deg_{x_j}(g) + \deg_{x_j}(f)
  \]

- For \( j > n \), we have
  \[
  \deg_{x_j}(q), \deg_{x_j}(r) \leq \deg_{x_j}(f).
  \]

For a proof of the above, we again refer the reader to the source.

**Lemma 2.18.** Let \( \Delta := \{g_1, \ldots, g_m\} \subset k[x_1, \ldots, x_n] \) be an unmixed set such that \( \text{height}(g_s) \leq \deg_{x_n}(g) \leq d \) for all \( s = 1, \ldots, m \). Let \( f \in k[x_1, \ldots, x_n] \) be a polynomial of height at most \( t \). Then there exist \( \alpha_1, \ldots, \alpha_m \in \mathbb{N} \) and \( q_1, \ldots, q_m, r \in k[x_1, \ldots, x_n] \) such that:

- \( \text{lc}(g_1)^{\alpha_1} \cdots \text{lc}(g_m)^{\alpha_m} \cdot f = q_1g_1 + \cdots + q_mg_m + f_0 \)
- \( f_0 \) is reduced modulo \( \Delta \), and
- \( \alpha_k \leq (t + 1) \cdot (d + 1)^{m-s} - 1, \quad s = 1, 2, \ldots, m \)

**Proof.** The first step of the reduction involves reducing \( f \) modulo \( g_m \). We have

\[
\text{lc}(g_m)^{\alpha_m} f = g_m q_m + f_{m-1}
\]

where Lemma 2.17 gives

\[
\alpha_m = \deg_{x_n}(f) - \deg_{x_n}(g_m) + 1 \leq \deg_{x_n}(f) \leq t
\]

We now wish to bound \( \alpha_{m-1} \). In order to do so, we need to compute \( \deg_{x_{n-1}}(r_m) \) because this is what we reduce in the next stage of the pseudodivision by \( g_{m-1} \). That is, the next equation that we obtain will have the form

\[
\text{lc}(g_{m-1})^{\alpha_{m-1}} f_{m-1} = g_{m-1} q_{m-1} + f_{m-2}
\]

In fact, another use of Lemma 2.17 gives that

\[
\deg_{x_{n-1}}(f_{m-1}) \leq (\alpha_{m-1} + 1) \cdot \deg_{x_{n-1}}(g_{m-1}) + \deg_{x_{n-1}}(f) \leq (t + 1) \cdot d + t
\]
(In fact, this is a bound on the degree of $f_{m-1}$ in all of the leading variables.)

Using Lemma 2.17 yet again, we get that

$$\alpha_{m-1} = \deg_{x_{n-1}}(f_{m-1}) - \deg_{x_{n-1}}(g_{m-1}) + 1$$

$$\leq \deg_{x_{n-1}}(f_{m-1}) \leq (t + 1) \cdot d + t$$

For $\alpha_{m-2}$, we will need to compute $\deg_{x_{n-2}}(f_{m-2})$. We have

$$\deg_{x_{n-2}}(f_{m-2}) \leq (\alpha_{m-1} + 1) \cdot \deg_{x_{n-2}}(g_{m-1}) + \deg_{x_{n-2}}(f_{m-1})$$

$$\leq (((t + 1) \cdot d + t) + 1) \cdot d + ((t + 1) \cdot d + t)$$

Examining what we did to bound $\alpha_{m-1}$, we see that this also gives a bound for $\alpha_{m-2}$. Calling the bound for each $\alpha_s$ by $\beta_s$, we see that for $s = 1, \ldots, m - 1$,

$$\beta_s + 1 = (\beta_{s+1} + 1) \cdot (d + 1)$$

(1)

and $\beta_m = t$. So we have

$$\beta_s + 1 = (\beta_m + 1) \cdot (d + 1)^{m-s}, s = 1, 2, \ldots, m$$

$\square$

3 Bounds for degrees

Lemma 3.1. (see [23, Prop. 3.3.4, p. 75]) Let $\Delta = \Delta_m = \{g_1, \ldots, g_m\}$ be an unmixed set such that $\text{height}(g_s) \leq d$ for all $s$. Suppose that for all $1 \leq s \leq m$ that

1. $\text{class}(g_s) = x_{l+s}$;
2. $\text{lc}(g_s) \in k[x_1, \ldots, x_l]$;
3. $g_s$ is reduced modulo $\Delta_{s-1} = \{g_1, \ldots, g_{s-1}\}$, i.e.

$$\forall t < s \deg_{x_{l+t}}(g_s) < \deg_{x_{l+t}}(g_t)$$

Then the height $\Gamma(\Delta)$ of the matrix of structure constants $A(\Delta)$ does not exceed

$$(d + 2)^{m+1}(\log(d + 2))^{m-1}$$

Proof. We first apply the matrix description of the pseudoremainder (see the Appendix) to products of the form $x_{l+1}^{e_1}x_{l+2}^{e_2} \cdots x_{l+m}^{e_m}$, where $e_s \leq 2d_s - 2$. Note that these products are the ones considered in computing the structure constants for $A(\Delta)$ and that such a product will play the role of what we call $f$ in the appendix. Also, what we called $g$ in the appendix will be $g_m$ in our application, as that is the first element we pseudo-divide by in reducing by $\Delta$. We have two cases to consider
1. $e_m < d_m$

2. $e_m \geq d_m$

In the first case, the product of interest is already reduced modulo $g_m$ and so can itself be selected as the pseudoremainder by $g_m$. So we can bound the height of its pseudoremainder by $\Delta$ by taking the maximum of $\Gamma_{m-1} := \Gamma(\Delta_{m-1})$ and $d_m$. In this case, we do not need the matrix representation. It should be noted that the bound we obtain in this case is smaller than the one we get in the second case.

In the second case, what we denote by $f_{\text{lower}}$ in the appendix is here a column vector with every entry 0 and what we denote by $f_{\text{upper}}$ has exactly one nonzero entry, namely $x_{l+1}^{e_1}x_{l+2}^{e_2} \ldots x_{l+m-1}^{e_{m-1}}$.

We first inspect the $G_0 \cdot \text{adj}(G_d)$ part of the pseudoremainder expression. In computing this product, one will obtain a $d_m \times d_m$ matrix and each of its entries will be sums of products of at most $1 + (d_m - 1) = d_m$ reduced integral elements of $A(\Delta_{m-1})$. (Note that we have products of reduced integral elements of $A(\Delta_{m-1})$ because $g_m$ is assumed to be reduced modulo $\Delta_{m-1}$.)

Completing the analysis of the number of multiplications needed to compute the pseudoremainder by $g_m$, we note that the product $x_{l+1}^{e_1}x_{l+2}^{e_2} \ldots x_{l+m-1}^{e_{m-1}}$ can be split into two factors where the exponent on each $x_s$ is less than $d_s$ (because $e_s \leq 2d_s - 2$). So multiplying $G_0 \cdot \text{adj}(G_d)$ by the column vector corresponding to this product results in sums of products of at most $d_m + 2$ reduced integral elements of $A(\Delta_{m-1})$.

So by Proposition 2.16 we have

$$\Gamma_m \leq (d_m + 2) \cdot d + (d_m + 2) \log(d_m + 2) \cdot \Gamma_{m-1}$$

We first replace $d_m$ by $d$ and estimate the first term as $(d + 2)^2$ to obtain

$$\Gamma_s < (d + 2)^2 + (d + 2) \log(d + 2) \cdot \Gamma_{s-1}, s = 2, \ldots, m$$

Combining these inequalities, we have

$$\Gamma_m \leq (d + 2)^2 \cdot \sum_{k=0}^{m-2} ((d + 2) \log(d + 2))^k + ((d + 2) \log(d + 2))^{m-1} \Gamma_1$$

Noting that the sum in brackets is a finite geometric series of $m - 1$ terms and that $\Gamma_1 \leq d^2$, we have

$$\Gamma_m \leq (d + 2)^2 \left[ \frac{(d + 2) \log(d + 2))^{m-1} - 1}{(d + 2) \log(d + 2) - 1} \right] + ((d + 2) \log(d + 2))^{m-1} \cdot d^2$$

So we have

$$\Gamma_m \leq (d + 2)^{m+1} \log(d + 2))^{m-1}$$
Theorem 3.2. (see [29, Thm. 4.2.2, p. 138]) Let $\Delta = \Delta_m = \{g_1, \ldots, g_m\} \subset k[x_1, \ldots, x_n]$ be a weakly unmixed set of height at most $d$. Let $l := n - m$, and assume that the following conditions are satisfied for all $s = 1, \ldots, m$:

1. $\text{class}(g_s) = x_{l+s}$
2. $\text{lc}(g_s) \in k[x_1, \ldots, x_l]$
3. $g_s$ is reduced modulo $\Delta_{s-1} = \{g_1, \ldots, g_{s-1}\}$.

Let $M(\Delta)$ be the multiplication table for the algebra $A(\Delta)$. For $f, h \in A(\Delta)[x_{n+1}, \ldots, x_{n+c}]$, denote $d_f := \text{height}(f)$ and $d_h := \text{height}(h)$, and

$$\{(\Delta_1, M(\Delta_1), \ldots, (\Delta_r, M(\Delta_r)))\} := \text{unmixed}_m^l(\Delta, M(\Delta), f, h)$$

the output of the algorithm $\text{unmixed}_m^l$ applied to $(\Delta, M(\Delta), f, h)$. Assume that $\Delta_j = \{g_{1,j}, \ldots, g_{m,j}\}$ for $j = 1, \ldots, r$. For each $s = 1, \ldots, m$, we denote

$$d_s := \max \left\{ \deg_{x_{l+s}}(g_{s,j}) \mid j = 1, \ldots, r \right\}$$

Then for each polynomial $p$ occurring in the computation, we have:

$$\text{height}(p) \leq (20d)^m \left( \prod_{s=1}^{m} (d_s + 2) \prod_{i=1}^{s-1} d_i \right) \prod_{s=1}^{m} \log \left( 56d \frac{\sqrt{d_s} + 2}{d_s} \right) \text{Input}(0)$$

where $\text{Input}(0) := \max\{d, \text{height}(f_0), \text{height}(h_0)\}$ and

$$\text{Input}(0) \leq (6d)^m \left( \max\{d, d_f, d_h\} + 11(d + 2)^m \log(d + 2)^{m-1} \right)$$

Proof. The computation of $\text{unmixed}_m^l$ has a tree structure. Consider a path of the computation tree with successive recursive calls:

$$\text{unmixed}_m^l(\Delta_m, M(\Delta_m), f_m, h_m), \ldots, \text{unmixed}_0^l(\Delta_0, M(\Delta_0), f_0, h_0)$$

where $f_m = f$, $h_m = h$ and for each $s = 0, \ldots, m - 1$, $f_s$ and $h_s$ are determined from $(\Delta_{s+1}, M(\Delta_{s+1}), f_{s+1}, h_{s+1})$ (see [29, p. 128]). First we estimate the height of the input at each level.

Lemma 3.3. For each $s = 0, \ldots, m$, we denote $\text{Input}(s) := \max\{d, \text{height}(f_s), \text{height}(h_s)\}$. Then

$$\text{Input}(s) \leq (6d)^{m-s} \left( \text{Input}(m) + 11(d + 2)^m \log(d + 2)^{m-1} \right)$$

Proof. We give an inductive analysis to obtain a bound on $\text{Input}(s)$. For $s = m$, obviously there is nothing to do. So we start with $s = m - 1$ and we consider the heights of $f_{m-1}, h_{m-1}$.
Szanto’s construction of these polynomials from the data of level \( m \) involves evaluations of the \( j \)th subresultants

\[
\psi_k^{(j)}(y, z) := \text{RES}_{x_n}^{(j)}(g_m, f + \sum_{l=1}^{k} g_m(l)y^{l-1} + zh), 1 \leq k \leq d
\]

at specific pairs for \( 0 \leq j \leq d \) and with \( y, z \) new variables (i.e. different from the ones which \( g_m, f, h \) are polynomials in). In order to bound the heights of \( f_{m-1}, h_{m-1} \) (which are constructed from these subresultants), we bound the height of these subresultants. The subresultant with the largest possible height will be the 0th subresultant, as higher ones are obtained by deleting rows and columns of the matrix whose determinant produces the 0th subresultant.

Since we are taking subresultants with respect to \( x_n \), all of the entries in the matrix we must take the determinant of are polynomials in \( x_1, x_2, \ldots, x_{n-1} \). Note also that the size of this matrix is at most \( d_m + d_m = 2d_m \). The first \( d_m \) is because the degree of \( g_m \) in \( x_n \) is \( d_m \). The second \( d_m \) is because \( f, h \) are reduced modulo \( \Delta \). In particular, this means that their degrees in \( x_{l+i} \) are less than \( d_i \) for all \( 1 \leq i \leq m \).

Since \( f_{m-1}, h_{m-1} \) must be reduced modulo \( \Delta_{m-1} \), we must remember that we are carrying out operations in \( A(\Delta_{m-1}) \) and therefore cannot simply estimate the heights of these polynomials as if we were doing regular polynomial multiplication to obtain them. Instead we must make use of Proposition \( \ref{prop:heights} \). Nonetheless, it can be easily checked that the bound for the height of \( h_{m-1} \) that we will obtain is larger than a similar computation would produce for \( f_{m-1} \). So we focus on getting a bound for the height of \( h_{m-1} \), thereby obtaining a bound for \( \text{Input}(m - 1) \). In fact, our technique will give us a bound for \( \text{Input}(s) \) in terms of \( \text{Input}(s + 1) \).

Because the computation of \( h_{m-1} \) involves a multiplication of six evaluated subresultants, we apply the proposition to the sixth power of the 0th subresultant (as described above) in two stages:

1. For the first stage, note that each term of the sixth power of the 0th subresultant is a product of \( 12d_m \) factors. We split these up into two groups: the \( 6d_m \) factors of any term coming from the coefficients of \( g_m \) (call the product of these \( C \)) and the rest from the coefficients of \( f + \sum_{l=1}^{k} g_m(l)y^{l-1} + zh \) (call the product of these \( D \)). In this first stage, we need not worry about denominator bounds because all of the factors of \( C \) and \( D \) are integral elements of \( A(\Delta) \).

2. We then take these two groups of \( 6d_m \) factors, reduce them, and multiply them. In the reduction step, we obtain some denominators in general and so we will need to compute bounds on these.

Our two-step analysis of the height of \( CD \) yields:

\[
\text{height}(CD) \leq \text{height}(C) + \text{height}(D) + 2 \log(2) \cdot \left( \gamma(\Delta_{m-1}) + d' \right)
\]
\[
\leq 6d_m \cdot d + 6d_m \cdot \text{Input}(m) + 12d_m \log(6d_m) \cdot \gamma(\Delta_{m-1}) + 2 \cdot \left( \gamma(\Delta_{m-1}) + d' \right)
\]
\[
\leq 6d^2 + 6d \cdot \text{Input}(m) + 12d \log(6d) \cdot \gamma(\Delta_{m-1}) + 2 \cdot \left( \gamma(\Delta_{m-1}) + d' \right)
\]
We need to determine a possible value for $d'$ by considering the sequence of exponents we obtain on $\text{lc}(g_i)$ when reducing $C, D$ modulo $\Delta_{m-1}$. By applying Lemma 2.18 with $\text{height}(C) \leq 6d^2 =: t$, we can set $d'$ equal to

$$\sum_{i=1}^{m-1} \left( (6d^2 + 1)(d + 1)^{m-i-1} - 1 \right) \cdot d = (6d^2 + 1)(d + 1)^{m-1} - 6d^2 - 1 - (m - 1)d.$$ 

Therefore

$$\text{height}(h_{m-1}) \leq 6d^2 + 6d \cdot \text{Input}(m) + 12d \log(6d) \cdot \gamma(\Delta_{m-1}) + 2 \cdot (\gamma(\Delta_{m-1}) + (6d^2 + 1)(d + 1)^{m-1} - 6d^2 - 1 - (m - 1) \cdot d)$$

As a result, we have

$$\text{Input}(m - 1) \leq \gamma(\Delta_{m-1}) \cdot [12d \log(6d) + 2] + 6d \cdot \text{Input}(m) + 2(6d^2 + 1)(d + 1)^{m-1}$$

Note that we dropped some terms being subtracted because these ultimately turn out to not drastically improve the bound on $\text{Input}(s)$. In fact, what we now have is

$$\text{Input}(s) \leq \gamma(\Delta_s) \cdot [12d \log(6d) + 2] + 6d \cdot \text{Input}(s + 1) + 2(6d^2 + 1)(d + 1)^s$$

Recall that $\gamma(\Delta_s) \leq (d + 2)^{s+1}[\log(d + 2)]^{s-1}$. Assuming $d \geq 1$ and using calculus, it can be shown that

$$\frac{12d \log(6d) + 2}{(d + 2) \log(d + 2)} \leq 17 \quad \text{and} \quad \frac{6d^2 + 1}{(d + 1)^2} \leq 6$$

We therefore modify our recursive bound and obtain

$$\text{Input}(s) \leq (6d)^{m-s} \cdot \text{Input}(m) + 17 \cdot \sum_{k=0}^{m-s-1} (6d)^k (d + 2)^{s+k+2} (\log(d + 2))^{s+k+1} + 12 \cdot \sum_{k=0}^{m-s-1} (6d)^k (d + 1)^{s+k+2}$$

Using calculus, we can replace the above bound to obtain

$$\text{Input}(s) \leq (6d)^{m-s} \cdot \text{Input}(m) + 9(d + 2)^m (\log(d + 2))^{m-1} + 5(d + 1)^m$$

Note that it is possible to condense this bound further because the sum of the last two terms in the square brackets is bounded by $11(d + 2)^m (\log(d + 2))^{m-1}$, which can be verified using yet more calculus.
Let us go back to the proof of Theorem 3.2. We propose an upper bound for the heights of polynomials computed at each level. Using the same notation as in Szanto’s thesis, we denote by Output(s) the maximum height of polynomials computed up to level s. For example, in case s = 0, we have Output(0) = Input(0).

We are going to determine an upper bound for Output(m) recursively. Assume that we have determined Output(m−1) which is an upper bound for all polynomials computed up to level m − 1. Let (Λ_{i,v}, M(Λ_{i,v})) be an arbitrary output after the recursive call at level m − 1. The construction of the corresponding output (∆_{i,v}, M(∆_{i,v})), which is described in [29, p. 129], can be summarized into 5 steps:

1. Computing \( d_{t,i,v} := \gcd_n \left( g_{m}, g'_{m}, \ldots, g^{(k)}_{m}, f_m, \epsilon h_m \right) \), where \( 1 \leq t \leq 6 \) and \( k \in \{i-1, i, i+1\}, \epsilon \in \{0, 1\} \) depending on the value of t (see [29, p. 127]).

2. Determining \( \text{lc}(d_{t,i,v}) := \text{pinvert}(A_{i,v}, \text{lc}(d_{t,i,v})) \), where the algorithm \( \text{pinvert} \) is described in [29, Sec. 3.4, p. 82].

3. Computing \( d_{t,i,v} := \text{lc}(d_{t,i,v}) \cdot d_{t,i,v} \).

4. Computing \( p_{i,v}^{(1)} := \overline{d_{1,i,v}} \cdot \overline{d_{3,i,v}} \cdot \overline{d_{5,i,v}} \) and \( p_{i,v}^{(2)} := \overline{d_{2,i,v}} \cdot \overline{d_{4,i,v}} \cdot \overline{d_{6,i,v}} \), and then \( q_{i,v} \), the quotient of the pseudo-division \( p_{i,v}^{(1)} \) by \( p_{i,v}^{(2)} \).

5. Denote \( \Delta_{i,v} := \Lambda_{i,v} \cup \{q_{i,v}\} \), and determine the multiplication table \( M(\Delta_{i,v}) \).

We are going to bound the heights of the polynomials appearing in each step.

**Step 1:** The construction of \( \gcd \) in [29, Lem. 3.1.3, p. 56] implies that height \( (d_{t,i,v}) \leq \text{Input}(m-1) \) for every \( t = 1, \ldots, 6 \).

**Step 2:** We denote by \( D_{m-1} \) the dimension of the algebra \( A(\Delta) \) over \( k \). Then \( D_{m-1} = \prod_{i=1}^{m-1} d_i \). The coefficients of \( \text{lc}(d_{t,i,v}) \) is defined as the determinant of a matrix of size \( D_{m-1} \times D_{m-1} \). The matrix has a column of the form \([0, \ldots, 0, 1]^t\). And the entries of the matrix have height at most

\[
\text{height}(d_{t,i,v}) + \Gamma(\Lambda_{i,v}) \leq \text{Input}(m-1) + \text{Output}(m-1).
\]

Therefore

\[
\text{height}(\text{lc}(d_{t,i,v})) \leq (D_{m-1} - 1)(\text{Input}(m-1) + \text{Output}(m-1)).
\]

**Step 3:** Now we compute \( \overline{d_{t,i,v}} := \text{lc}(d_{t,i,v}) \cdot d_{t,i,v} \). By applying [29, Prop. 3.3.1, p. 66], we have

\[
\text{height}(\overline{d_{t,i,v}}) \leq \text{height}(\text{lc}(d_{t,i,v})) + \text{height}(d_{t,i,v}) + 2 \log 2 \cdot \Gamma(\Lambda_{i,v}) \leq (D_{m-1} - 1)[\text{Input}(m-1) + \text{Output}(m-1)] + \text{Input}(m-1) + 2 \text{Output}(m-1) = D_{m-1} \text{Input}(m-1) + (D_{m-1} + 1) \text{Output}(m-1).
\]
Step 4: Note that, for each $t = 1, \ldots, 6$, we have $\deg_{x_n}(d_{t,i,v_t}) \leq d$. Therefore $p_{i,v}^{(1)}$ and $p_{i,v}^{(2)}$ are polynomials of degree at most $4d$ in $x_n$. By using the matrix representation for the quotient of the pseudo-division algorithm, the coefficients of $q_{i,v}$ are equal to a sum of products of at most $4d$ coefficients of $p_{i,v}^{(1)}$ or $p_{i,v}^{(2)}$. Each coefficient of $p_{i,v}^{(1)}$ and $p_{i,v}^{(2)}$ is a sum of products of 4 coefficients of $d_{t,i,v_t}$, $t = 1, \ldots, 6$. Thus, coefficients of $q_{i,v}$ are sums of products of at most $16d$ coefficients of $d_{t,i,v_t}$, $t = 1, \ldots, 6$. Note that $d_{t,i,v_t}$ are polynomials and are reduced by $\Lambda_{i,v}$. By applying [29, Prop. 3.3.1, p. 66], we obtain

$$\text{height}(q_{i,v}) \leq 16d \cdot \max_{t=1,\ldots,6} \{\text{height}(d_{t,i,v_t})\} + 16d \log(16d) \cdot \Gamma(\Lambda_{i,v})$$

$$\leq (16dD_{m-1} + 16d + 16d \log(16d)) \text{Output}(m-1) + 16dD_{m-1} \text{Input}(m-1).$$

Step 5: As the last step of the computation at level $m$, we must determine the multiplication table $M(\Delta_{i,v})$ for the algebra $A(\Delta_{i,v})$. We already know that the height of any entry in the multiplication table $M(\Lambda_{i,v})$ is at most $\text{Output}(m-1)$. In order to obtain an upper bound for the heights of coefficients in $M(\Delta_{i,v})$, we need to estimate the height of the remainder in the pseudo-division of $x_1^{\alpha_1} \cdots x_n^{\alpha_m}$ by $q_{i,v}$, where $0 \leq \alpha_s \leq 2 \deg_{x_{l+1}}(g_s) - 2$, $1 \leq s \leq m$. Note that $q_{i,v}$ is reduced modulo $\Lambda_{i,v}$, and that $\deg_{x_n} q_{i,v} \leq \tilde{d}_m$. By using the matrix representation of the remainder in the pseudo remainder algorithm, the remainder obtained when we divide $x_1^{\alpha_1} \cdots x_n^{\alpha_m}$ by $q_{i,v}$ is equal to a sum of products of at most $\tilde{d}_m + 2$ integral elements in $A(\Lambda_{i,v})$. Therefore,

$$\Gamma(\Delta_{i,v}) \leq (\tilde{d}_m + 2) \text{height}(q_{i,v}) + (\tilde{d}_m + 2) \log(\tilde{d}_m + 2) \Gamma(\Lambda_{i,v}).$$

This is also an upper bound for all polynomials computed up to level $m$. In other words, we have

$$\text{Output}(m) \leq (\tilde{d}_m + 2) \left[16dD_{m-1} + 16d + 16d \log(16d) + \log(\tilde{d}_m + 2)\right] \text{Output}(m-1) +$$

$$+ 16dD_{m-1}(\tilde{d}_m + 2) \text{Input}(m-1)$$

$$\leq 16d(\tilde{d}_m + 2) \left[D_{m-1} + \frac{1}{16} \log \left((32d)^{16}(\tilde{d}_m + 2)\right)\right] \text{Output}(m-1) +$$

$$16dD_{m-1}(\tilde{d}_m + 2) \text{Input}(m-1)$$

One can prove by using only elementary calculus that

$$16d(\tilde{d}_m + 2) \left[D_{m-1} + \frac{1}{16} \log \left((32d)^{16}(\tilde{d}_m + 2)\right)\right] \leq 1.2d(\tilde{d}_m + 2)D_{m-1} \log \left((32d)^{16}(\tilde{d}_m + 2)\right)$$

14
Since $\text{Input}(m - 1) \leq \text{Output}(m - 1)$, we can proceed to bound $\text{Output}(m)$ in terms of initial data as follows:

\[
\text{Output}(m) \leq 20 \cdot d(\tilde{d}_m + 2)D_{m-1} \log \left( \frac{32d}{\sqrt{(\tilde{d}_m + 2)}} \right) \text{Output}(m - 1) + 16dD_{m-1}(\tilde{d}_m + 2) \text{Output}(m - 1)
\]

\[
\leq 20 \cdot d(\tilde{d}_m + 2)D_{m-1} \log \left( \frac{56d}{\sqrt{(\tilde{d}_m + 2)}} \right) \text{Output}(m - 1).
\]

Similar computations show that for every $s = 1, \ldots, m - 1$, we also have

\[
\text{Output}(s) \leq 20 \cdot d(\tilde{d}_s + 2)D_{s-1} \log \left( \frac{56d}{\sqrt{(\tilde{d}_s + 2)}} \right) \text{Output}(s - 1).
\]

Hence

\[
\text{Output}(m) \leq \prod_{s=1}^{m} 20 \cdot d(\tilde{d}_s + 2)D_{s-1} \log \left( \frac{56d}{\sqrt{(\tilde{d}_s + 2)}} \right) \text{Output}(s - 1)
\]

\[
= 20^m d^n \left( \prod_{s=1}^{m} (\tilde{d}_s + 2) \prod_{s=1}^{m} d_s \right) \prod_{s=1}^{m} \log \left( \frac{56d}{\sqrt{(\tilde{d}_s + 2)}} \right) \text{Input}(0).
\]

\[\square\]

**Lemma 3.4.** Let $F = \{f_0, f_1, \ldots, f_k\} \subset k[x_1, \ldots, x_n]$ be a set of polynomials, such that $\deg f_i \leq D$ for all $i$. Assume that $\Delta = \{g_1, \ldots, g_m\}$ is an unmixed triangular set such that every component of $V(\text{Rep}(\Delta))$ is a component of $V(F)$. By $d_i$ denote the degree of $g_i$ with respect to its leading variable. Then,

\[
\prod_{i=1}^{m} d_i \leq D^{m+1}
\]

**Proof.** We claim that the product $\prod_{i=1}^{m} d_i$ does not exceed the sum of the degrees of the irreducible components of $V(\text{Rep}(\Delta))$.

**Lemma 3.5.** Let $\Delta = \{g_1, \ldots, g_m\}$ be an unmixed triangular set in $k[x_1, \ldots, x_{l+m}]$, and $\text{class}(g_i) = x_{l+i}$ and $\text{deg}_{x_{l+i}} g_i = d_i$ for all $i \leq m$. Then, there exists a nonzero $q \in k[x_1, \ldots, x_l]$ such that for every $(a_1, \ldots, a_l) \in k^l(k) \setminus V(q)$ the system

\[
\begin{cases}
g_1 = g_2 = \ldots = g_m = 0, \\
\text{lc}(g_1) \neq 0, \ldots, \text{lc}(g_m) \neq 0 \\
x_1 = a_1, \ldots, x_l = a_l
\end{cases}
\]

has exactly $\prod_{i=1}^{m} d_i$ distinct solutions.
Proof. The proof is by induction on $m$. If $m = 1$, then we set
\[ q = \text{Res}_{x_{l+1}} \left( g_1, \frac{\partial}{\partial x_{l+1}} g_1 \right) \]
This polynomial is nonzero and, because $\{g_1\}$ is unmixed, $g_1$ is squarefree with respect to $x_{l+1}$. Then, for every $(a_1, \ldots, a_{l+1}) \in \mathbb{A}^l(k) \setminus V(q)$ the polynomial $g_1(a_1, \ldots, a_l, x_{l+1})$ is squarefree of degree $d_1$.

Let $m > 1$. Applying the induction hypothesis to the triangular set $\{g_1, \ldots, g_{m-1}\} \subset k[x_1, \ldots, x_{l+m-1}]$, we obtain a polynomial $q_0 \in k[x_1, \ldots, x_l] \setminus \{0\}$. We define polynomials $h_m, \ldots, h_1$ by the formulas
\[ h_m = \text{Res}_{x_{l+m}} \left( g_m, \frac{\partial}{\partial x_{l+m}} g_m \right), \quad \text{and} \quad h_i = \text{Res}_{x_{l+1}}(h_{i+1}, g_i) \quad \text{for} \quad i < m \]
Again, since $\Delta$ is unmixed, all of these polynomials are nonzero. Note also that $h_1 \in k[x_1, \ldots, x_l]$. We now set $q = q_0 h_1$. The induction hypothesis implies that for every $(a_1, \ldots, a_{l+1}) \in \mathbb{A}^l(k) \setminus V(q)$ the corresponding system for $\{g_1, \ldots, g_{m-1}\}$ has at least $\prod_{i=1}^{m-1} d_i$ solutions. For any solution, say $(a_1, \ldots, a_{l+m-1})$, the inequality $h_1 \neq 0$ and the equalities $g_1 = \ldots = g_{m-1} = 0$ imply that $h_i \neq 0$ for all $i \leq m$. Hence, $g_m(a_1, \ldots, a_{l+m-1}, x_{l+m})$ is squarefree of degree $d_m$. Thus, the whole system has $d_m \cdot \prod_{i=1}^{m-1} d_i = \prod_{i=1}^m d_i$ solutions. \hfill \Box

Let us return to the proof of Lemma 3.4. Assume that $x_1, \ldots, x_{n-m}$ are the nonleading variables of $\Delta$. The lemma above implies that there exist $a_1, \ldots, a_{n-m} \in k$ such that the affine subspace $L$ defined by the equations $x_1 = a_1, \ldots, x_{n-m} = a_{n-m}$ intersects $V(\text{Rep}(\Delta))$ in $\prod_{i=1}^m d_i$ distinct points. Since the degree of a variety is its maximal possible number of intersection points with a complementary subspace (see [27, p. 234]), the sum of the degrees of the irreducible components of $V(\text{Rep}(\Delta))$ is at least $\prod_{i=1}^m d_i$.

Due to [11, Lemma 5.5] there exist polynomials $\tilde{f}_1, \ldots, \tilde{f}_{m+1}$ such that $\deg \tilde{f}_i \leq D$ for all $i$, $V(F) \subset V(\tilde{f}_1, \ldots, \tilde{f}_{m+1})$, and every component of $V(F)$ of codimension $\leq m$ is a component of $V(\tilde{f}_1, \ldots, \tilde{f}_{m+1})$. Hence, all components of $V_{\text{rep}}(\Delta)$ are components of $V(\tilde{f}_1, \ldots, \tilde{f}_{m+1})$. From [3, 8.28] it follows that the sum of the degrees of the components of $V(\tilde{f}_1, \ldots, \tilde{f}_{m+1})$ does not exceed $D^{m+1}$. This proves the lemma. \hfill \Box

Remark 3.6. If it is known that $\text{height}(f_i) \leq d$ for all $i$, the right-hand side of the inequality in Lemma 3.4 can be replaced by $(nd)^{m+1}$.

Theorem 3.7. (see [27, Thm. 4.1.7, p. 118]) Let $F := \{f_0, f_1, \ldots, f_k\} \subset k[x_1, \ldots, x_n]$ be a set of polynomials of height at most $d$. Let $m$ be the codimension of the radical ideal $\sqrt{(F)}$. Then for any polynomial $p$ occurring in the computation of an unmixed representation for the ideal $\sqrt{(F)}$ by using Algorithm 1, we have

16
height(p) ≤ 360^m m^m n^{m^2 + m} d^{3m^2 + m} \left( \log \left( \sqrt{60n^{1.125}} \cdot d^{1.125} \right) \right)^m.

\cdot \left( \max\{d^m, k\} + 11(d^m + 2)^m \log(d^m + 2)^{m-1} \right)

In particular, in case \( k \) is not too large, for instance if \( k \leq d^m \), we have

height(p) ≤ (d^m)^{(1+\epsilon)m^2}

where \( \epsilon = \epsilon(n, m, d) \) is a decreasing function such that \( \epsilon(n, m, d) < 4 \) for every \( d \geq 2, m \geq 1, n \geq 2 \) and

\[ \lim_{n,m,d \to \infty} \epsilon(n, m, d) = 0. \]

Proof. According to Algorithm [1] we first compute the set \( \Sigma(F) := \{ \Delta_i \mid i \subseteq [n] \} \) of weakly unmixed sets such that: for every prime component \( P \) of \( \sqrt{\langle F \rangle} \), if \( \dim_{\text{Krull}} P = n - |i| \), and \( P \cap k[X_i] = \{0\} \), then \( \text{Rep}(\Delta) \subseteq P \). By [29, Cor. 4.1.5, p. 115], for every \( \Delta \in \Sigma(F) \), the height of polynomials in \( \Delta \) is at most \( d_{|\Delta|} \).

Next, for each \( \Delta \in \Sigma(F) \), we compute the multiplication table \( M(\Delta) \), and then determine

\( U(\Delta) := \text{unmixed}_{|\Delta|}(\Delta, M(\Delta), f, 1) \)

where \( f = f_0 + yf_1 + \ldots + y^kf_k \in k[x_1, \ldots, x_n, y] \). Without loss of generality, we may assume that \( |\Delta| = m \). Let \( \Delta := \{\tilde{g}_1, \ldots, \tilde{g}_m\} \) be an arbitrary element in \( U(\Delta) \). For each \( s = 1, \ldots, m \), we denote by \( \tilde{d}_s \) the degree of \( \tilde{g}_s \) in its leading variable. By Theorem 3.2, for every polynomial \( p \) occurring in the computation of \( U(\Delta) \), we have

\[
\text{height}(p) \leq (20d^m)^m \cdot \left( \prod_{s=1}^{m} \left( \tilde{d}_s + 2 \right) \prod_{i=1}^{s-1} \tilde{d}_i \right) \prod_{s=1}^{m} \log \left( 56d^m 16 \tilde{d}_s + 2 \right) \cdot \left( 6d^m \right)^m \left( \max\{d^m, k\} + 11(d^m + 2)^m \log(d^m + 2)^{m-1} \right)
\]

By Lemma 3.3 we know that

\[
\prod_{i=1}^{m} \tilde{d}_i \leq (nd)^{m+1}. \tag{2}
\]

Thus,

\[
\left( \prod_{s=1}^{m} \left( \tilde{d}_s + 2 \right) \prod_{i=1}^{s-1} \tilde{d}_i \right) \leq 3^m \left( \prod_{s=1}^{m} \tilde{d}_s \right)^m \leq 3^m n^{m^2 + m} d^{m^2 + m}
\]

17
and
\[
\prod_{s=1}^{m} \log \left( 56d^m \frac{16}{\sqrt{d_s + 2}} \right) \leq \prod_{s=1}^{m} \log \left( 56d^m \frac{16}{\sqrt{3d_s}} \right)
\]
\[
\leq \left( \frac{1}{m} \sum_{s=1}^{m} \log \left( 56d^m \frac{16}{\sqrt{3d_s}} \right) \right)^m
\]
\[
= \left( \frac{1}{m} \log \left( (56 \frac{16}{\sqrt{3}})^m d^m \left( \prod_{s=1}^{m} d_s \right) \frac{1}{m} \right) \right)^m
\]
\[
\leq \left( \frac{1}{m} \log \left( 60^m d^m (nd) \frac{m+1}{16} \right) \right)^m
\]
\[
\leq m^m \left( \log \left( \sqrt{60n^{0.125}} \cdot d^{1.125} \right) \right)^m
\]

Now we substitute the last two inequalities into the upper bound for height\((p)\) above to obtain

\[
\text{height}(p) \leq B(n, m, d) := 360^m m^m n^{m^2 + m} d^{3m^2 + m} \left( \log \left( \sqrt{60n^{0.125}} \cdot d^{1.125} \right) \right)^m \cdot (\max\{d^m, k\} + 11(d^m + 2)^m [\log(d^m + 2)]^{m-1})
\]

In case \(k \leq d^m\), we have \(\max\{k, d^m\} = d^m\). By using elementary calculus, we can estimate the above product by

\[
\text{height}(p) \leq (d^3n)^{(1+\epsilon)m^2}
\]

where

\[
\epsilon = \epsilon(n, m, d) := \frac{\log_{d^m} B(n, m, d)}{m^2} - 1
\]

which is a decreasing function with \(\epsilon(n, m, d) < 4\) for every \(d \geq 2, m \geq 1, n \geq 2\) and

\[
\lim_{n,m,d \to \infty} \epsilon(n, m, d) = 0.
\]

We now consider what can be said when height is replaced by total degree in the statement above. Such information will be useful for making our comparisons later. The reader will note that the details of the proof below are mostly the same as for Theorem 3.7 except for one crucial step.

**Theorem 3.8.** Let \(F := \{f_0, f_1, \ldots, f_k\} \subset k[x_1, \ldots, x_n] \) be a set of polynomials of total degree at most \(d\). Let \(m\) be the codimension of the radical ideal \(\sqrt{F}\). Then for any polynomial \(p\) occurring in the computation of an unmixed representation for the ideal \(\sqrt{F}\) by using Algorithm 7, we have

\[
\text{height}(p) \leq B(n, m, d)
\]

where

\[
B(n, m, d) := 360^m m^m n^{m^2 + m} d^{3m^2 + m} \left( \log \left( \sqrt{60n^{0.125}} \cdot d^{1.125} \right) \right)^m \cdot (\max\{d^m, m\} + 11(d^m + 2)^m [\log(d^m + 2)]^{m-1})
\]

In case \(m \leq d^m\), we have \(\max\{m, d^m\} = d^m\). By using elementary calculus, we can estimate the above product by

\[
\text{height}(p) \leq (d^3n)^{(1+\epsilon)m^2}
\]

where

\[
\epsilon = \epsilon(n, m, d) := \frac{\log_{d^m} B(n, m, d)}{m^2} - 1
\]

which is a decreasing function with \(\epsilon(n, m, d) < 4\) for every \(d \geq 2, m \geq 1, n \geq 2\) and

\[
\lim_{n,m,d \to \infty} \epsilon(n, m, d) = 0.
\]
\[
\deg(p) \leq S(n, m, d) := n360^m m^m d^{3m^2 + m} \left( \log \left( \sqrt[60]{d^{1.125}} \right) \right)^m \cdot \left( \max\{d^m, k\} + 11(d^m + 2)^m \log(d^m + 2) \right)^{m-1}.
\]

In particular, in case \(k\) is not too large, for instance if \(k \leq d^m\), we have

\[
\deg(p) \leq nd^{(4 + \rho)m^2}
\]

where \(\rho = \rho(m, d)\) is a decreasing function such that \(\rho(m, d) < 17\) for every \(m \geq 1, d \geq 2\) and

\[
\lim_{m,d \to \infty} \rho(m,d) = 0.
\]

**Proof.** Since the given polynomials are of degree at most \(d\), their heights are also at most \(d\). Now we can estimate the height for \(p\) in the same way as we did in the proof of Theorem 3.7. The only change here is that there is no \(n\) in the right hand side of the inequality (2). Therefore, we have

\[
\text{height}(p) \leq 360^m m^m d^{3m^2 + m} \left( \log \left( \sqrt[60]{d^{1.125}} \right) \right)^m \cdot \left( \max\{d^m, k\} + 11(d^m + 2)^m \log(d^m + 2) \right)^{m-1}
\]

Note that the degree of \(p\) is at most \(n\) times its height. Hence, the degree of \(p\) is at most \(S(n, m, d)\). In the case that \(k \leq d^m, d \geq 2\), we can estimate this as follows. Observe that the highest power on \(d\) in \(S(n, m, d)\) is \(4m^2\). Write \(S(n,m,d)\) with a base of \(d\) and an exponent of \((4 + \rho)m^2\), where \(\rho\) is some function of \(d, m\). Using elementary calculus, it can be verified that \(\rho(m,d) < 17\) for \(m \geq 1, d \geq 2\) and that \(\rho\) goes to zero as \(m, d\) grow. \(\square\)

### 4 Bounds for the number of components

**Lemma 4.1.** The number of vectors \((v_1, \ldots, v_6) \in \mathbb{Z}_{\geq 0}^6\) such that

- \(v_i \leq d\) for all \(i\);
- \(v_1 \geq v_2 \geq v_3, v_4 \geq v_5 \geq v_6, v_1 \geq v_4, v_2 \geq v_5,\) and \(v_3 \geq v_6\);
- \(v_1 + v_3 + 2v_5 - v_4 - v_6 - 2v_2 > 0\)

does not exceed \(\frac{5}{2} \binom{d+6}{6}\).

**Proof.** First of all we count number of distinct multisets of \(\{0, \ldots, d\}\) of cardinality 6. The number of such multisets is \(\binom{d+6}{6}\). Using a case-by-case analysis, it is easy to verify that there are only five possible orderings for \(v_i\) compatible with the second condition:

\[
v_1 \geq v_2 \geq v_3 \geq v_5 \geq v_6, \ v_1 \geq v_2 \geq v_4 \geq v_5 \geq v_3 \geq v_6, \ v_1 \geq v_2 \geq v_3 \geq v_4 \geq v_5 \geq v_6,
\]
\[ v_1 \geq v_4 \geq v_2 \geq v_3 \geq v_5 \geq v_6, \quad v_1 \geq v_4 \geq v_2 \geq v_5 \geq v_3 \geq v_6 \]

Thus, every multiset gives us at most five different vectors, satisfying the first two conditions. So, we have at most \( 5 \binom{d+6}{6} \) such vectors.

Let us observe that the transformation

\[(v_1, \ldots, v_6) \to (d - v_6, d - v_5, d - v_4, d - v_3, d - v_2, d - v_1)\]

maps a vector satisfying the first two conditions to a vector satisfying the first two conditions and changes the sign of the expression \( v_1 + v_3 + 2v_5 - v_4 - v_6 - 2v_2 \). This transformation is inverse to itself, so the set of all vectors satisfying first two conditions is split into pairs with different signs of \( v_1 + v_3 + 2v_5 - v_4 - v_6 - 2v_2 \) and fixed points of the transformation, which satisfy \( v_1 + v_3 + 2v_5 - v_4 - v_6 - 2v_2 = 0 \). Due to the third condition, we can discard at least half of the \( 5 \binom{d+6}{6} \) vectors and obtain the desired upper bound.

**Lemma 4.2.** Let \( \Delta = \{g_1, \ldots, g_m\} \subset k[x_1, \ldots, x_{l+m}] \) be a weakly unmixed set such that height \((g_i) \leq d^m \) and \( \text{class}(g_i) = x_i+1 \) for all \( i \), and suppose \( f \in k[x_1, \ldots, x_{l+m+1}] \) with \( \deg_{x_i} f \leq d \) for all \( 1 \leq i \leq l + m \). If \( m > 1 \) the number of unmixed sets in the output of \( \text{unmixed}_m(\Delta, M(\Delta), f, 1) \) does not exceed

\[
\sqrt{2}d^{m/2} \cdot \frac{d^m(d+1)(d+3)(2d+1)}{24} \cdot \left( \frac{5}{2} \sum_{i=1}^{d^m} \left( \frac{d^{m}/i + 6}{6} \right) \right)^{m-2}.
\]

If \( m = 1 \), then \( \text{unmixed}^{m-1}_1(\Delta, M(\Delta), f, 1) \leq \sqrt{2d} \).

**Proof.** The \( \text{unmixed} \) routine is recursive, so the computation has a tree structure. Each leaf gives us at most one component. Note that each recursive call is of the form (see [29, Eq. 4.19])

\[\text{unmixed}_s(\Lambda, M(\Lambda), \tilde{f}, \tilde{h}), \text{ where } \Lambda = \{g_1, \ldots, g_s\}\]

for some \( 0 \leq s \leq m \) and some polynomials \( \tilde{f} \) and \( \tilde{h} \). We are going to estimate the number of branches created by this recursive call. All these branches are parametrized by the set of pairs \((i, \vec{v})\), where \( 1 \leq i \leq \deg_{x_{l+i}} g_s \leq d^m \) and \( \vec{v} = (v_1, \ldots, v_6) \in \mathbb{Z}_{\geq 0}^6 \). The meaning of these parameters is described in [29, Eq. 4.16]. Since \( v_i \)'s are defined as degrees of certain generalized gcd's, we will use the following properties of \( \text{ggcd} \) (see [29, Sec. 3.5] for more details about \( \text{ggcd} \)):

**Lemma 4.3.** Given an unmixed triangular set \( \Delta = \Lambda \cup \{g\} \) and polynomials \( f_0, \ldots, f_{k+c} \):

1. if \( a = \text{ggcd}_t(\Delta, f_0, \ldots, f_k) \) and \( b = \text{ggcd}_t(\Delta, f_0, \ldots, f_{k+c}) \), then, \( \deg_{x_{l+i}} a \geq \deg_{x_{l+i}} b \).

2. if \( p = \text{ggcd}_t(\Delta, g', \ldots, g^{(i)}, f_0, \ldots, f_k) \), then \( \deg_{x_{l+i}} p \leq \frac{\deg_{x_{l+i}} g}{i+1} \).

**Proof.** First of all, let us recall the relevant properties of \( \text{ggcd} \) (see [29, p. 88]). By \( R_t \) we denote the polynomial ring generated by all variables except \( x_t \). If \( q = \text{ggcd}_t(\Delta, f_0, \ldots, f_k) \), then
Now we return to the proof.

Lemma 4.3 implies that the first part of Lemma 4.3 yields inequalities $\Delta v_1 + v_3 - 2v_2 > 0$, and we should make recursive calls only for vectors $v$ such that $v_1 + v_3 - 2v_2 > 0$. Hence, we can apply Lemma A.1 and conclude that the number of branches produced by the call $\text{unmixed}_d(I, M(I), f, h)$ does not exceed

$$\frac{5}{2} \sum_{i=1}^{d} \binom{d + m / i + 6}{6}$$

(3)

For the first and the last calls in the recursion tree we will estimate the number of recursive calls more carefully.

For the first call $\text{unmixed}_d(I, M(I), f, 1)$ we have $\deg_z f \leq d$ and $\deg h = 0$, so $d \geq v_1 \geq v_2 \geq v_3 \geq 0$, $v_4 = v_5 = v_6 = 0$, and $v_1 + v_3 > 2v_2$. We can find the number of such vectors using arguments similar to those given for Lemma A.1. The number of multisets in $\{0, \ldots, d\}$ of cardinality 3 is equal to $\binom{d + 3}{3}$. For each vector $(v_1, v_2, v_3)$ such that $v_1 + v_3 - 2v_2 > 0$ we can assign a vector $(d - v_3, d - v_2, d - v_1)$ with $(d - v_1) + (d - v_3) - 2(d - v_2) < 0$. In order to find all vectors $(v_1, v_2, v_3)$ with $v_1 + v_3 - 2v_2 = 0$, we should pick a pair of (not necessarily distinct) numbers in $\{0, \ldots, d\}$ of the same parity and set $v_2 = (v_1 + v_3)/2$. This can be done in

$$\left\lfloor \frac{(d + 1)/2}{2} \right\rfloor + \left\lfloor \frac{(d + 1)/2}{2} \right\rfloor + 1 = \frac{1}{2} \left( \left(\frac{(d + 1)/2}{2} + \left(\frac{(d + 1)/2}{2} + 1 \right) \right) = \frac{1}{2} \left( \left( (d + 1)/2 \right)^2 + \left( (d + 1)/2 \right)^2 + d + 1 \right) \leq \frac{(d + 1)(d + 3)}{4}$$
ways for every single $i$. Thus, we will make at most
\[
\frac{d^m}{2} \left( \binom{d+3}{3} - \frac{(d+1)(d+3)}{4} \right) = \frac{d^m(d+1)(d+3)(2d+1)}{24} \tag{4}
\]
recursive calls.

Now we consider a call of the form $\text{unmixed}_1(\{g_1\}, M(\{g_1\}), f, h)$. All recursive calls will be of the form $\text{unmixed}_0(\emptyset, \tilde{f}, \tilde{h})$ for some $\tilde{f}$ and $\tilde{h}$. By the definition (see [29, p. 126]), the output of such a call is empty unless $\tilde{f} = 0$ and $\tilde{h} \neq 0$. Note that, since $\Lambda = \emptyset$ in this case, generalized gcd’s in [29, Eq. 4.16] are ordinary gcd’s over the ring $k[x_1, \ldots, x_l]$.

Putting any further restrictions on the degree of these polynomials leads us to a nonzero polynomial $\tilde{f}$. Thus, for every fixed $i$ there is only one possible vector $\overline{v}$, which is a vector of degrees of these gcd’s. Moreover, if $g_1$ has no irreducible factors over $k[x_1, \ldots, x_l]$ of multiplicity exactly $i$, then $v_1 - 2v_2 + v_3 = 0$ and $v_4 - 2v_5 + v_6 = 0$. Let $\{i_1, \ldots, i_k\}$ be distinct multiplicities of irreducible factors of $g_1$. Then, the number of recursive calls is at most $k$. On the other hand,
\[
d^m \geq i_1 + i_2 + \ldots + i_k \geq 1 + 2 + \ldots + k > \frac{k^2}{2}, \tag{5}
\]
so $k \leq \sqrt{2d^{m/2}}$.

Putting things together (see equations (4), (5), (5)), we obtain that the number of components in the output of $\text{unmixed}_m(\Delta, M(\Delta), f, 1)$ does not exceed
\[
\sqrt{2d^{m/2}} \cdot \frac{d^m(d+1)(d+3)(2d+1)}{24} \cdot \left( \frac{5}{2} \sum_{i=1}^{d^m} \binom{d^m / i + 6}{6} \right)^{m-2}.
\]
if $m \geq 2$.

In the case $m = 1$ we can apply the bound for the last level of recursion
\[
\text{unmixed}_1^{n-1}(\Delta, M(\Delta), f, 1) \leq \sqrt{2d}
\]

\[\square\]

**Theorem 4.4.** Let $F \subset k[x_1, \ldots, x_n]$ be a finite set of polynomials of degree at most $d \geq 2$. Let $m$ be the codimension of the radical ideal $\sqrt{\langle F \rangle} \subseteq k[x_1, \ldots, x_n]$. Then the number of unmixed components in the output of Algorithm applied to $F$ is at most
\[
\begin{cases}
  n\sqrt{2d} & \text{if } m = 1 \\
  n\sqrt{2d} + \left( \frac{\pi^6}{272160} \right)^{m-2} \left( \frac{n}{m} \right)^{d^m - 10.5m + 3} & \text{if } m \geq 2
\end{cases}
\]

22
Proof. Since the degree of the given polynomials is at most \( d \), so is their height. The first step in the computation of an unmixed representation for the radical ideal \( \sqrt{\langle F \rangle} \) using Algorithm 1 is determining the set \( \Sigma(F) := \{ \Delta_i | i \subseteq [n] \} \) of weakly unmixed sets such that for every prime component \( P \) of \( \sqrt{\langle F \rangle} \), we have
\[
\text{dim}_{\text{Krull}} P = n - |i| \quad \text{and} \quad P \cap k[X_i] = 0 \Rightarrow \text{Rep}(\Delta) \subseteq P.
\]

It is well-known that the number of elements in a weakly unmixed set \( \Delta \) is equal to the codimension of the ideal \( \text{Rep}(\Delta) \). Therefore the number of weakly unmixed sets in \( \Sigma(F) \) is not larger than the number of proper subsets of \([n]\) which has cardinality at most \( m \).

In step 2, we determine the multiplication table \( M(\Delta) \) for each \( \Delta \in \Sigma(F) \). And then, in step 3, we use the subroutine \texttt{unmixed} to transform each weakly unmixed set \( \Delta \in \Sigma(F) \) to the set
\[
\mathcal{U}(\Delta) := \text{unmixed}_{\delta - |\Delta|}(\Delta, M(\Delta), f, 1)
\]
of unmixed sets (see Algorithm 1). Thus the number of unmixed sets in the output is
\[
M(n, m, d) := \left| \bigcup_{\Delta \in \Sigma(F)} \mathcal{U}(\Delta) \right| \leq \sum_{\Delta \in \Sigma(F)} |\mathcal{U}(\Delta)| \quad (6)
\]

Note that for each \( s = 1, \ldots, m \), there are \( \binom{n}{s} \) unmixed set in \( \Sigma(F) \) of cardinality \( s \). And for each \( \Delta \in \Sigma(F) \) of cardinality \( s \), Lemma 4.2 yields
\[
|\mathcal{U}(\Delta)| \leq \begin{cases} \sqrt{2d} & \text{if } s = 1 \\ \frac{1}{12\sqrt{2}}(d + 1)(d + 3)(2d + 1)d^{3s/2} \left[ \sum_{i=1}^{d^s} \frac{5}{2} \left( \binom{d^s}{i} + 6 \right) \right]^{s-2} & \text{if } s \geq 2 \end{cases} \quad (7)
\]

In case the codimension of the given ideal is equal to 1, the number of unmixed components is
\[
M(n, m, d) \leq \binom{n}{1} \sqrt{2d} = n \sqrt{2d}.
\]

Let us assume that \( m \geq 2 \). In this case, we first consider the summation in (7). We have:
\[
\frac{5}{2} \sum_{i=1}^{d^s} \left( \binom{d^s}{i} + 6 \right) = \frac{5}{2 \cdot 6!} \sum_{i=1}^{d^s} \left( \frac{1}{i^6} d^{6s} + \frac{21}{i^5} d^{5s} + \frac{175}{i^4} d^{4s} + \frac{735}{i^3} d^{3s} + \frac{1624}{i^2} d^{2s} + \frac{1764}{i} d^s + 720 \right)
\leq \frac{5}{2 \cdot 6!} (\zeta(6)d^{6s} + 21\zeta(5)d^{5s} + 175\zeta(4)d^{4s} + 735\zeta(3)d^{3s} + 1624\zeta(2)d^{2s} + 1764d^s \ln(d^s) + 1) + 720d^s
\]

23
which will be denoted by $U(s, d)$. By substituting the above inequality and (7) into (6), we see that

$$M(n, m, d) \leq n\sqrt{2d} + \sum_{s=2}^{m} \binom{n}{s} \frac{1}{12\sqrt{2}}(d+1)(d+3)(2d+1)d^{3s/2}U(s, d)^{s-2}$$

$$\leq n\sqrt{2d} + \frac{1}{12\sqrt{2}}(d+1)(d+3)(2d+1)\sum_{s=2}^{m} \binom{n}{s} d^{3s/2}U(s, d)^{s-2}$$

By direct computation, one may check that $\binom{n}{s} \leq \binom{m}{s} \binom{m}{s}$. Therefore

$$M(n, m, d) \leq n\sqrt{2d} + \frac{1}{12\sqrt{2}}(d+1)(d+3)(2d+1)\binom{n}{m} \sum_{s=2}^{m} \binom{m}{s} d^{3s/2}U(s, d)^{s-2} \tag{8}$$

We denote the summation in the above inequality by $S$. We can estimate $S$ as follows:

$$S := \sum_{s=2}^{m} \binom{m}{s} d^{3s/2}U(m, d)^{s-2}$$

$$\leq \left( d^{3/2}U(m, d) + 1 \right)^m \frac{1}{U(m, d)^2}$$

$$= d^{3m/2} \left( U(m, d) + d^{-3/2} \right)^{m-2} \left( 1 + \frac{1}{d^{3/2}U(m, d)} \right)^2$$

By using elementary calculus, we can prove that

$$U(m, d) + d^{-3/2} \leq \left( \frac{5\pi^6}{2 \cdot 6!} \right) (d^m + 4)^6$$

and that

$$\left( 1 + \frac{1}{d^{3/2}U(m, d)} \right)^2 \leq 1.1.$$  

By substituting these bounds into the bound above for the summation $S$, and using the result to replace $S$ in (8), we finally have

$$M(n, m, d) \leq n\sqrt{2d} + 0.07(d+1)(d+3)(2d+1)\binom{n}{m} \left( \frac{5\pi^6}{2 \cdot 6! \cdot 945} \right)^{m-2} d^{3m/2}(d^m + 4)^6(m-2)$$

$$\leq n\sqrt{2d} + \left( \frac{\pi^6}{272160} \right)^{m-2} \binom{n}{m} d^{6m^2-10.5m+3}$$

**Remark 4.5.** The proof of Lemma 3.4 implies that the sum of the degrees of all components of the variety from Theorem 4.4 does not exceed $d^{m+1}$. So it is sufficient to leave only this number of components in the final output.
5 Comparison to degree bounds for Gröbner basis methods

As alluded to in the introduction, classical methods for solving the ideal membership problem make use of Gröbner bases. We wish to compare degree bounds for such methods applied to computing a radical with degree bounds for Szanto’s algorithm. In [18], Laplagne proposed an algorithm to compute the radical of an ideal using Gröbner bases. We first estimate the degrees of polynomials in the output of his algorithm. Then we will carry out our comparison.

5.1 Degree Bounds for Laplagne’s Algorithm

In [23], Mayr and Ritscher gave an upper bound for the degree of a polynomial that may occur in the reduced Gröbner basis for a given polynomial ideal. The following bound given by Mayr and Ritscher improves upon the one proposed by Dubé in [8]. (For further details, we refer the reader to [23].)

**Theorem 5.1.** (see [23, Thm. 36, p. 92]) Let $F \subset \mathbb{k}[x_1, \ldots, x_n]$ be a finite set of polynomials of degree at most $d$, and $m$ the codimension of the ideal generated by $F$. Then for any admissible ordering $<$, the degree of a polynomial in a reduced Gröbner basis for the ideal generated by $F$ with respect to $<$ is at most

$$MR(n, m, d) := 2 \left( \frac{d^2m}{2} + d \right)^{2n-m}$$

**Remark 5.2.** Unlike Szanto’s algorithm, the output of the algorithm studied by Mayr and Ritscher in [23] gives a representation of the original ideal, not the radical. Thus it is more appropriate to compare the complexity of Szanto’s algorithm to that of one that computes a radical.

We will apply the bound above in our analysis of Laplagne’s algorithm. The steps of this algorithm and a result quoted within the algorithm have been reproduced below for the convenience of the reader. We will refer to each of the steps by its number in explaining why the algorithm involves at least four Gröbner basis computations.

**Proposition 5.3.** (Seidenberg Lemma, see [26]) Let $I \subset \mathbb{k}[x_1, x_2, \ldots, x_n] := \mathbb{k}[x]$ (with $k$ a perfect field) be a zero-dimensional ideal and $I \cap \mathbb{k}[x_i] = \langle f_i \rangle$ for $i = 1, 2, \ldots, n$. Let $g_i := \sqrt{f_i} = f_i / \gcd(f_i, f_i')$, the square free part of $f_i$. Then

$$\sqrt{I} = \langle I, g_1, \ldots, g_n \rangle$$
Algorithm 2 Laplagne’s algorithm for the computation of a radical, RADICAL2(I)

Require: \( I \subset k[x_1, \ldots, x_n] =: k[x] \).
Ensure: \( \sqrt{I} = P \), the radical of \( I \).

1. Make a suitable linear coordinate change of variables such that the ideal \( Ik(u)[x \setminus u] \) is zero-dimensional, where \( u := \{x_1, x_2, \ldots, x_e\} \) and \( e = \dim(I) \).
2. Compute the radical of the zero-dimensional ideal \( Ik(u)[x \setminus u] \) using Proposition 5.3.
3. Contract \( \sqrt{Ik(u)[x \setminus u]} \) to \( k[x] \) and set \( J \) equal to \( \sqrt{Ik(u)[x \setminus u]} \cap k[x] \).
4. output = \( J \cap \text{RADICAL2}(I : J^\infty) \)

We analyze the degrees of the polynomials computed in each step. (For more details on each step, please see Laplagne’s paper.)

1. The degrees of the input polynomials are unaffected as the coordinate change is linear.

2. In this step, one must compute elimination ideals to obtain the \( f_i \)'s mentioned in Proposition 5.3. (Note that the \( g_i \)'s computed from these will generally have lower degree than the \( f_i \)'s. But their degrees are bounded by the degrees of the \( f_i \)'s.) Laplagne suggests computing these elimination ideals using Gröbner bases in the polynomial ring \( k[x] \). So one may compute up to \( n \) Gröbner bases in this step, each with degree bounded by \( MR(n, m, d) \).

3. Here one computes a Gröbner basis for the radical computed in the second step. This is where the second application of the Mayr-Ritscher bound comes in. This step also involves taking the least common multiple of the polynomials in the Gröbner basis. So the degree bound may be even greater than \( MR(n, m, MR(n, m, d)) \). We obtain a lower bound for the degrees of polynomials generated by assuming that there is only one element in the Gröbner basis obtained, so that the degree bound for the lcm \( h \) is the same as the degree bound produced from a second application of \( MR \). We also remark that the reason the second application of \( MR \) has \( m \) as input in the second component is that the dimension of the radical (after clearing denominators for a generating set) is the same as the dimension of the original ideal.

   The contraction then involves computing an ideal saturation by introducing a new indeterminate \( t \) and computing a Gröbner basis for the ideal generated by the Gröbner basis of the radical and \( th - 1 \). So we are now up to three applications of \( MR \), with this third application taking \( n + 1 \) as the number of variables. We again remark that the codimension remains the same in this step. This is because we first consider the ideal we are contracting as an ideal in \( k[x, t] \), so its dimension goes up by 1. But then we enlarge this ideal by adding a generator in with the new variable \( t \) in it. So the dimension returns to what it was. Note that we end this step back in \( k[x] \), so that our number of variables returns to \( n \). So the bound up to this point is \( MR(n + 1, m, MR(n, m, MR(n, m, d))) \).

4. In this last step of a loop, we compute another saturation, namely \( I : J^\infty \). This involves introducing two new indeterminates and then performing a Gröbner basis
computation. This gives us a fourth application of MR, now with \( n + 2 \) variables. In this step, the dimension does change because the Gröbner basis computation is applied to the ideal generated by \( I \) and a single carefully chosen polynomial that involves the two new variables. So, loosely speaking, the number of “free” variables in the corresponding system may go up by at most 1, which implies the codimension would drop to nothing lower than \( m - 1 \).

So we see that, at best, we expect the degrees of polynomials in the output of Laplagne’s algorithm to be bounded by

\[
L(n, m, d) := MR(n + 2, m - 1, MR(n + 1, m, MR(n, m, MR(n, m, d)))).
\]

**Remark 5.4.** Note that this bound is just for one loop of Laplagne’s algorithm and that, in general, the full algorithm might take up to \( \dim(I) \) loops. This is what is meant above by the words “at best.”

### 5.2 The Comparison

Next we compare the two bounds \( S(n, m, d) \) and \( L(n, m, d) \) for a given set \( F \) of polynomials in a small number of variables. Note that the bound \( S(n, m, d) \) depends on the number of polynomials in \( F \). For practical applications, it is safe to assume that the number of polynomials in \( F \) is not very large, in the sense that \( k \leq d^m \). So we will assume that \( \max\{d^m, k\} \) is \( d^m \) and give a comparison for this typical situation.

The following table is for the case when the given polynomials come from a polynomial ring in two, three or four variables (\( n = 2, 3, 4 \)).

| \( n \) | \( m \) | \( d \) | \( S(n, m, d) \) | \( L(n, m, d) \) |
|---|---|---|---|---|
| 2 | 2 | 2 | \(< 3 \cdot 10^{14}\) | \(< 2 \cdot 10^{9}\) |
| | | 3 | \(< 6 \cdot 10^{17}\) | \(< 2 \cdot 10^{986}\) |
| | | 4 | \(< 2 \cdot 10^{20}\) | \(< 10^{1232}\) |
| 3 | 2 | 2 | \(< 5 \cdot 10^{14}\) | \(< 2 \cdot 10^{9237}\) |
| | | 3 | \(< 8 \cdot 10^{17}\) | \(< 2 \cdot 10^{14467}\) |
| | | 4 | \(< 2 \cdot 10^{20}\) | \(< 5 \cdot 10^{18417}\) |
| 3 | 3 | 2 | \(< 2 \cdot 10^{23}\) | \(< 7 \cdot 10^{42420}\) |
| | | 3 | \(< 3 \cdot 10^{32}\) | \(< 2 \cdot 10^{6592}\) |
| | | 4 | \(< 4 \cdot 10^{37}\) | \(< 3 \cdot 10^{8313}\) |
| 4 | 2 | 2 | \(< 6 \cdot 10^{14}\) | \(< 3 \cdot 10^{138942}\) |
| | | 3 | \(< 2 \cdot 10^{18}\) | \(< 4 \cdot 10^{222630}\) |
| | | 4 | \(< 3 \cdot 10^{20}\) | \(< 10^{285818}\) |
| 3 | 2 | 2 | \(< 2 \cdot 10^{25}\) | \(< 6 \cdot 10^{61480}\) |
| | | 3 | \(< 4 \cdot 10^{32}\) | \(< 3 \cdot 10^{99589}\) |
| | | 4 | \(< 6 \cdot 10^{37}\) | \(< 7 \cdot 10^{127123}\) |
| 3 | 3 | 2 | \(< 3 \cdot 10^{38}\) | \(< 3 \cdot 10^{14821}\) |
| | | 3 | \(< 4 \cdot 10^{51}\) | \(< 4 \cdot 10^{23437}\) |
| | | 4 | \(< 2 \cdot 10^{60}\) | \(< 2 \cdot 10^{29576}\) |

We see from these tables that the bound on the degrees of polynomials in the output of Szanto’s algorithm (given by Proposition 3.8) is much smaller than the lower bound we established for Laplagne’s algorithm.

Our bound on the degrees of polynomials in the output of Szanto’s algorithm (when \( k \leq d^m \)) is asymptotic to \( nd^{k_m^2} \), as explained in Theorem 3.8. Clearly, the complexity of Szanto’s algorithm is lower. So, if it is a representation of the radical that one seeks, we see that an unmixed representation is less costly than a reduced Gröbner basis.
6 Conclusion

We have presented an effective bound for polynomials occurring in the output of Szanto’s algorithm for computing an unmixed representation of a radical ideal. We have also compared this with the bound for the degrees of polynomials produced in the algorithm Laplagne gave in [18]. In addition, a bound for the number of unmixed components in an unmixed representation for a radical ideal has also been produced.

We are grateful to Agnes Szanto and Alexey I. Ovchinnikov for discussions related to this work.

7 Appendix

The following results on matrix representations of pseudoremainders are used in Section 3. They are mentioned and used in [29, Section 3.3]. We include them here for the convenience of the reader.

Let \( f \in k[x_1, x_2, \ldots, x_l] \), \( g \in k[x_1, x_2, \ldots, x_n] \) with \( k \) a field and \( l \geq n \). We wish to describe the pseudoremainder of \( f \) by \( g \) with respect to \( x_n \) in matrix form. More specifically, we wish to describe this pseudoremainder when \( \deg_{x_n}(g) = d \) and \( \deg_{x_n}(f) \leq 2d - 2 \), (the application in mind being computing the structure constants for \( A(\Delta) \), as defined in Algorithm 1). We will allow the degree of \( f \) to go up to \( 2d - 1 \) in fact, as writing the matrix equation will require an additional coefficient anyway, (which will be 0 in our application). We first write \( f \) and \( g \) as univariate polynomials in \( x_n \) with coefficients \( k[x_1, \ldots, x_{n-1}, x_{n+1}, \ldots, x_l] \):

\[
\begin{align*}
    f &= f_0 + f_1 x_n + \cdots + f_{2d-1} x_n^{2d-1} \\
    g &= g_0 + g_1 x_n + \cdots + g_d x_n^d
\end{align*}
\]

Note that the difference between the degrees in \( x_n \) of \( f \) and \( g \) is \( d - 1 \). Thus, the pseudoremainder equation we consider (in scalar form) is

\[
g_d^d f = gq + r
\]  

where the degrees in \( x_n \) of \( r, q \) are less than \( d \). (For \( r \), this is because of the usual features we ask for in a remainder from polynomial division. For \( q \), this is because \( f \) appears on the left-hand side and so the sum of the degrees in \( x_n \) of \( q \) and \( g \) must not exceed \( 2d - 1 \).)

Writing \( q \) and \( r \) as we wrote \( f, g \) above (having now noted their maximal degrees in \( x_n \)) and substituting these expressions into [9] we obtain:

\[
g_d^d (f_0 + f_1 x_n + \cdots + f_{2d-1} x_n^{2d-1}) = (g_0 + g_1 x_n + \cdots + g_d x_n^d)(g_0 + g_1 x_n + \cdots + g_{d-1} x_n^{d-1}) + r_0 + r_1 x_n + \cdots + r_{d-1} x_n^{d-1}
\]
Comparing coefficients of the powers of \(x_n\) from \(d\) to \(2d - 1\), we see that
\[
\begin{align*}
f_{2d-1}g_d^d &= g_dq_{d-1} \\
f_{2d-2}g_d^d &= g_{d-1}q_{d-1} + g_dq_{d-2} \\
&\vdots \\
f_dg_d^d &= g_1q_{d-1} + g_2q_{d-2} + \cdots + g dq_0
\end{align*}
\]
we can write these equations as the following matrix equation:
\[
\begin{bmatrix}
g_d & 0 & 0 & \cdots & 0 \\
g_{d-1} & g_d & 0 & \cdots & 0 \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
g_1 & g_2 & \cdots & \cdots & g_d
\end{bmatrix}
\begin{bmatrix}
g_{d-1} \\
g_{d-2} \\
\vdots \\
g_0
\end{bmatrix}
= 
\begin{bmatrix}
f_{2d-1} \\
f_{2d-2} \\
\vdots \\
f_d
\end{bmatrix}
\]
We can write the matrix equation above as \(G_dq = f^\text{upper}g_d^d\). Since \(g_d \neq 0\) (as \(g\) is assumed to have degree \(d\) in \(x_n\)), we can find the coefficients of the desired quotient by inverting \(G_d\).

Now, since \(r = g_d^df - qg\), after substituting we see that
\[
\begin{align*}
r_{d-1} &= f_{d-1}g_d^d - (q_{d-1}g_0 + q_{d-2}g_1 + \cdots + q_0g_{d-1}) \\
r_{d-2} &= f_{d-2}g_d^d - (q_{d-2}g_0 + q_{d-3}g_1 + \cdots + q_0g_{d-2}) \\
&\vdots \\
r_0 &= f_0g_d^d - q_0g_0
\end{align*}
\]
In matrix form, we can summarize these equations as:
\[
\begin{bmatrix}
r_{d-1} \\
r_{d-2} \\
\vdots \\
r_0
\end{bmatrix}
= 
\begin{bmatrix}
g_{d-1} \\
g_{d-2} \\
\vdots \\
g_0
\end{bmatrix}
\begin{bmatrix}
f_{d-1} \\
f_{d-2} \\
\vdots \\
f_0
\end{bmatrix}
- 
\begin{bmatrix}
g_0 & g_1 & \cdots & g_{d-1} \\
0 & g_0 & g_1 & \cdots & g_{d-2} \\
0 & 0 & \cdots & g_0
\end{bmatrix}
\begin{bmatrix}
g_{d-1} \\
g_{d-2} \\
\vdots \\
g_0
\end{bmatrix}
\]
Writing this equation as \(r = g_d^d\text{lower} - G_0q\). Using our description of \(q\) from the previous linear system, we have \(r = g_d^d\text{lower} - g_d^dG_0G_d^{-1}f^\text{upper}\).

To count multiplications in the formula for the pseudoremainder, we re-express \(G_d^{-1}\) using Cramer’s Rule:
\[
G_d^{-1} = \frac{1}{g_d^d} \cdot \text{adj}(G_d)
\]
where \(\text{adj}(G_d)\) denotes the adjugate of \(G_d\), (i.e. its matrix of cofactors transposed). So we have
\[
r = g_d^d\text{lower} - G_0 \cdot \text{adj}(G_d)f^\text{upper}
\]
Observe that the entries of \(\text{adj}(G_d)\) are sums of products of \(d - 1\) entries of \(G_d\).

Remark 7.1. A matrix representation of the pseudoremainder can also be constructed without restricting the degree in \(x_n\) of \(f\). We leave it as an exercise for the reader to determine the necessary adjustments to the above.
References

[1] B. Buchberger. *Gröbner bases: An algorithmic method in polynomial ideal theory*, volume 174 of *Lecture Notes in Computer Science*, pages 100-107. Springer, 1984.

[2] B. Buchberger. *Gröbner bases: An algorithmic method in polynomial ideal theory*

[3] P. Bürgisser, P. Clausen, A. Shokrollahi. *Algebraic Complexity Theory*. Springer, 1997.

[4] P. Bürgisser, P. Scheiblechner. *On the complexity of counting components of algebraic varieties*. J. Symbolic Computation, vol. 44, 1114-1136, 2009.

[5] 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.

[6] A. L. Chistov. *Double-exponential lower bound for the degree of any system of generators of a polynomial prime ideal*. St. Petersburg Math. J. 20, 983-1001, 2009.

[7] X. Dahan, E. Schost. *Sharp Estimates for Triangular Sets*. ISSAC ’04 Proceedings, Pages 103-110, 2004.

[8] T. Dube. *Combinatorial Proof of the Effective Nullstellensatz*. J. Symbolic Computation, vol. 15, 277-296, 1993.

[9] R. Feng. *Hrushovski’s algorithm for computing the Galois group of a linear differential equation*. Advances in Applied Mathematics (Elsevier), vol. 65, pp. 1-37, 2016.

[10] G. Gallo, B. Mishra. *Efficient algorithms and bounds for WuRitt characteristic sets*. Proceedings of MEGA90, Progress in Mathematics, vol. 94, Birkhuser (1990), pp. 119142.

[11] D.J. Ierardi. *The complexity of quantifier elimination in the theory of an algebraically closed field*. PhD thesis, Cornell University, 1989.

[12] M. Kalkbrener. *Applications of Gröbner bases: solution of algebraic equations and decomposition of radicals*. PhD thesis, RISC at Johannes Kepler University, 1987.

[13] M. Kalkbrener. *Solving systems of algebraic equations by using Gröbner bases*. European Conference on Computer Algebra, 282-292, 1987.

[14] M. Kalkbrener. *A generalized Euclidean algorithm for computing triangular representations of algebraic varieties*. Mathematical Sciences Institute, Cornell University 92 (13), 1992.

[15] M. Kalkbrener. *Prime decompositions of radicals in polynomial rings*. Journal of Symbolic Computation 18 (4), 365-372, 1994.
[16] M. Kalkbrener and D., Wang. Polynomial Elimination: Algorithms and Applications. SIGSAM Bulletin 31, 31-31, 1997.

[17] M. Kalkbrener. Algorithmic Properties of Polynomial Rings. Journal of Symbolic Computation 26 (5), 525-581, 1998.

[18] S. Laplagne. An algorithm for the computation of the radical of an ideal. ISSAC 2006: 191-195.

[19] D. Lazard. Gr"{o}bner Bases, Gaussian elimination and resolution of systems of algebraic equations. In Proc. EUROCAL 83, pages 146-157, 1983.

[20] D. Lazard. A new method for solving algebraic systems of positive dimension. Discrete Applied Mathematics 33, pp. 147-160, 1991.

[21] D. Lazard. Solving zero-dimensional algebraic systems. Journal of Symbolic Computation 13 (2), pp. 117-131, 1992.

[22] E.W. Mayr and S. Ritscher. Degree bounds for Gr"{o}bner bases of low-dimensional polynomial ideals. In: Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation ACM, pp.2127.

[23] E.W. Mayr and S. Ritscher. Dimension-dependent bounds for Gr"{o}bner bases of polynomial ideals. Journal of Symbolic Computation, 49:7894, 2013.

[24] J.F., Ritt. Differential algebra. American Mathematical Society, 1950.

[25] E. Schost. Complexity results for triangular sets. Journal of Symbolic Computation, 36:555594, 2003.

[26] A. Seidenberg. Construction in Algebra. Trans. Amer. Math. Soc., (197):273-313, 1974.

[27] I.R. Shafarevich. Basic Algebraic Geometry 1. Springer, 1994.

[28] A. Szanto. Complexity of the Wu-Ritt Decomposition. In Proceedings of PASCO ’97, pages 139-149. ACM Press, 1997.

[29] A. Szanto. Computation with polynomial systems. PhD thesis, Cornell University, 1999.

[30] D. Wang. Irreducible decomposition of algebraic varieties via characteristic sets and Gr"{o}bner bases. Computer Aided Geometric Design, 9:471-484, 1992.

[31] W.-T. Wu. Basic principles of mechanical theorem proving in elementary geometries. J. Syst. Sci. Math. Sci, 4:207-235, 1984.