Journal of Algebra 523 (2019) 342–364

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Complexity of triangular representations of algebraic sets ☆

Eli Amzallag [a,b], Mengxiao Sun [b], Gleb Pogudin [c,1], Thieu N. Vo [d,*]

[a] *The City College of New York, Department of Mathematics, NY 10031, USA*
[b] *CUNY Graduate Center, Department of Mathematics, NY 10016, USA*
[c] *Institute for Algebra, Johannes Kepler University, 4040 Linz, Austria*
[d] *Fractional Calculus, Optimization and Algebra Research Group, Faculty of Mathematics and Statistics, Ton Duc Thang University, Ho Chi Minh City, Vietnam*

ARTICLE INFO

Article history:
Received 14 June 2017
Available online 18 January 2019
Communicated by Seth Sullivant

MSC:
14Q20
68W30
13P99

MSC:
Triangular set
Unmixed algebraic set
Regular chain
Radical polynomial ideal
Gröbner basis
Complexity

ABSTRACT

Triangular decomposition is one of the standard ways to represent the radical of a polynomial ideal. A general algorithm for computing such a decomposition was proposed by A. Szántó. In this paper, we give the first complete bounds for the degrees of the polynomials and the number of components in the output of the algorithm, providing explicit formulas for these bounds.

☆ Work was supported by the strategic program "Innovatives OÖ 2020" by the Upper Austrian Government, by Austrian Science Fund FWF grant Y464-N18, by the NSF grants CCF-095259, CCF-1564132, CCF-1563942, DMS-1606334, DMS-1760448, by the NSA grant #H98230-15-1-0245, by CUNY CIRG #2248, and by PSC-CUNY grants #69827-00 47 and #60098-00 48.

* Corresponding author.
E-mail addresses: eamzallag@ccny.cuny.edu (E. Amzallag), msun@gradcenter.cuny.edu (M. Sun), pogudin.gleb@gmail.com (G. Pogudin), vongocthieu@tdtu.edu.vn (T.N. Vo).
[1] Current address: Courant Institute of Mathematical Sciences, New York University, USA.

https://doi.org/10.1016/j.jalgebra.2019.01.007
0021-8693/

1. Introduction

The general problem considered in the paper is: given polynomials $f_0, \ldots, f_r \in k[x_1, \ldots, x_n]$, where k is a computable subfield of $\mathbb{C}$, represent the set of all polynomials vanishing on the set of solutions of the system $f_0 = \ldots = f_r = 0$. This set of polynomials is called *the radical* of the ideal generated by $f_0, \ldots, f_r$. The problem is important for computer algebra and symbolic computations, as well as for their applications (for example, [14,2]). Several techniques can be used to solve the problem; for example, Gröbner bases, geometric resolution, and triangular decomposition. Representing the radical of an ideal is an intermediate step in many other algorithms. Thus, it is crucial to understand the size of such a representation, as the size affects the complexity of the further steps. The size of the representation can be expressed in terms of a degree bound for the polynomials appearing in the representation and their number. The main result of the paper is the first complete bound on the degrees (Theorem 4.4) and the number of components (Theorem 5.1) for the algorithm designed by A. Szántó in [17] for computing a triangular decomposition.

For Gröbner bases, a bound which is doubly-exponential in the number of variables is given in [11]. Moreover, an example constructed in [3] shows that there are ideals such that every set of generators of the radical (even those sets that are not Gröbner bases) contains a polynomial of doubly-exponential degree. Geometric resolution and triangular decomposition do not represent the radical via its generators, so it was hoped that these representations might have better degree bounds. For geometric resolution, singly-exponential degree bounds were obtained in [7,12,13] (for prior results in this direction, see references in [13]).

Algorithms for triangular decomposition were an active area of research during the last two decades. Some results of this research were tight degree upper bounds for a triangular decomposition of an algebraic variety given that the decomposition is irredundant [15, 5], an efficient algorithm for zero-dimensional varieties [4], and implementations [18,1]. However, to the best of our knowledge, there are only a few algorithms [6,17,15] for computing triangular decomposition with proven degree upper bounds for the output. The algorithms in [15] and [6] have restrictions on the input polynomial system. The algorithm in [15] requires the system to define an irreducible variety. The algorithm in [6, Theorem 4.14] produces a characteristic set of an ideal, which represents the radical of the ideal only if the ideal is characterizable [9, Definition 5.10] (for example, an ideal defined by x_1x_2 is not characterizable). Together with [9, Proposition 5.17] this means that the algorithm from [6] represents the radical of an ideal if the radical can be defined by a single regular chain.

The algorithm designed by [16,17] does not have any restrictions on the input system. However, it turns out that the argument in [17] does not imply the degree bound $d^{O(m^2)}$ (m is the maximum codimension of the components of the ideal, d is a bound for degrees of the input polynomials) stated there. The reason is that the argument in [17] did not take into account possible redundancy of the output (see Remark 4.6). Moreover,

in Example 3.1 we show that the sum of degrees of extra components produced by the algorithm can be significantly larger than the degree of the original variety. In this paper, we take these extra components into account and prove an explicit degree bound of the form $d^{\mathrm{O}(m^3)}$ for the algorithm. More precisely, we prove that:

Main Result *(Theorem 4.4). Let $f_0, \ldots, f_r \in k[x_1, \ldots, x_n]$ be polynomials with $\deg f_i \leq d$ for all $0 \leq i \leq r$ $(d > 1)$. Assume that the maximum codimension of prime components of the ideal $(f_0, \ldots, f_r)$ is $m \geq 2$, and $r \leq d^m$. Then the degree of any polynomial p appearing in the output of Szántó's algorithm or during the computation does not exceed*

$$\deg(p) \leq nd^{(\frac{1}{2}+\epsilon)m^3}$$

where ϵ is some decreasing function of m, d and ϵ is bounded by 5 (for a more general statement, we refer to Section 4).

Main Result *(Theorem 5.1). Let $F \subset k[x_1, \ldots, x_n]$ be a finite set of polynomials of degree at most d. Let m be the maximum of codimension of prime components of $\sqrt{(F)} \subseteq k[x_1, \ldots, x_n]$. Then the number of squarefree regular chains in the output of Szántó's algorithm applied to F is at most*

$$\binom{n}{m} \left((m+1)d^m + 1\right)^m.$$

2. Preliminaries

Throughout the paper, all fields are of characteristic zero and all logarithms are binary.

Throughout this section, let $R = k[x_1, x_2, \ldots, x_n]$, where k is a field. We fix an ordering on the variables $x_1 < x_2 < \cdots < x_n$. Consider a polynomial $p \in R$. We set $\mathrm{height}(p) := \max_i \deg_{x_i}(p)$. The highest indeterminate appearing in p is called its leader and will be defined by $\mathrm{lead}(p)$. By $\mathrm{lc}(p)$ we denote the leading coefficient of p when p is written as a univariate polynomial in $\mathrm{lead}(p)$.

Definition 2.1. Given a sequence $\Delta = (g_1, g_2, \ldots, g_m)$ in R, we say that Δ is a *triangular set* if $\mathrm{lead}(g_i) < \mathrm{lead}(g_j)$ for all $i < j$.

Remark 2.2. Note that any subsequence of a triangular set is a triangular set. In what follows, the subsequences of Δ of particular interest are the ones of the form $\Delta_j := (g_1, g_2, \ldots, g_j)$, $1 \leq j \leq m$ and $\Delta_0 := \varnothing$.

Triangular sets give rise to ideals via the following notion.

Definition 2.3. Let $f, g \in R$ with $\mathrm{lead}(g) = x_j$. We consider f and g as univariate polynomials in x_j with the coefficients from the field $k(x_1, x_2, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n)$ and

let $f = \tilde{q}g + \tilde{r}$ be the result of univariate polynomial division of f by g with coefficients in this field. Let α be the smallest nonnegative integer such that $g := \mathrm{lc}\,(g)^{\alpha}\tilde{g}$ and $r := \mathrm{lc}\,(g)^{\alpha}\tilde{r}$ are polynomials, so we obtain an equation

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

with $q, r \in R, \deg_{x_j}(r) < \deg_{x_j}(g), \alpha \in \mathbb{N}$. One can show that $\alpha \leq \deg_{x_j}(f) - \deg_{x_j}(g) + 1$. We say that r is *pseudoreminder of f by g* and denote it by $\mathrm{sprem}(f, g)$.

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 with respect to Δ* is the polynomial f_0 in the sequence $f_m = f, f_{s-1} = \mathrm{sprem}(f_s, g_s), 1 \leq s \leq m$. We denote f_0 by $\mathrm{sprem}(f, \Delta)$.

We say that f is *reduced with respect to* Δ if $f = \mathrm{sprem}(f, \Delta)$.

Remark 2.5. The computation of the pseudoremainder of f with respect to Δ gives rise to the equation

$$\mathrm{lc}\,(g_m)^{\alpha_m} \ldots \mathrm{lc}\,(g_1)^{\alpha_1} f = \sum_{s=1}^{m} q_s g_s + f_0$$

where each $\alpha_s \leq \deg_{\mathrm{lead}\,(g_s)}(f_s) - \deg_{\mathrm{lead}(g_s)}(g_s) + 1$.

Definition 2.6. Given a triangular set Δ in R, we define the ideal

$$\mathrm{Rep}(\Delta) := \{p \in R \,|\, \exists N \,:\, H^N p \in \langle \Delta \rangle\}, \text{ where } H := \mathrm{lc}(g_1) \ldots \mathrm{lc}(g_m).$$

We say that a triangular set $\Delta \subset R$ *represents* an ideal I if $I = \mathrm{Rep}(\Delta)$.

Definition 2.7. For an ideal $I \subset R$, we consider the irredundant prime decomposition $\sqrt{I} = I_1 \cap \ldots \cap I_r$ of its radical. We call the $I_1, \ldots, I_r$ *the associated primes* of I and denote the set of associated primes of I by $\mathrm{Ass}(I)$. When $I = \mathrm{Rep}(\Delta)$, we will write $\mathrm{Ass}(\Delta)$ instead of $\mathrm{Ass}(I)$.

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

Definition 2.8. Let $\Delta = (g_1, g_2, \ldots, g_m)$ be a triangular set of R with $I = \mathrm{Rep}(\Delta)$ and, for each $1 \leq i \leq m-1$, let $\{P_{i,j}\}_{j=1}^{r_i}$ be the prime ideals in the irredundant prime decomposition of the radical of $\mathrm{Rep}(\Delta_i)$.

(a) if $\mathrm{lc}(g_{i+1}) \notin P_{i,j}$ for every $1 \leq i \leq m-1$ and $1 \leq j \leq r_i$, then Δ is called *a regular chain*, see [9, Definition 5.7].
(b) if g_{i+1} is square-free over $K(P_{i,j}) := \mathrm{Quot}(R/P_{i,j})$ for every $1 \leq j \leq r_i$ and $1 \leq j \leq r_i$, then Δ is called *a squarefree regular chain*, see [9, Definition 7.2]
(Here, $\mathrm{Quot}(R/P_{i,j})$ is the field of fractions of $R/P_{i,j}$.)

Theorem 2.9 *(See [2, Proposition 2.7]). If* Δ *is a regular chain, then* $\mathrm{Rep}(\Delta) = \{h \in R \mid \mathrm{sprem}(h, \Delta) = 0\}$ *and all of the prime ideals in the irredundant prime decomposition of* $\mathrm{Rep}(\Delta)$ *have the same dimension.*

Theorem 2.10 *(See [9, Corollary 7.3]). If* Δ *is a squarefree regular chain, then* $\mathrm{Rep}(\Delta)$ *is a radical ideal.*

Remark 2.11. We use terminology different from the one used in [17, Section 2.4.3]. The correspondence between these two terminologies is the following: a regular chain is called a weakly unmixed triangular set in [17] and a squarefree regular chain is called an unmixed triangular set in [17].

Now we are ready to define the main object we will compute.

Definition 2.12. The *triangular decomposition* of an ideal $I \subset R$ is a set $\{\Delta_1, \ldots, \Delta_s\}$ of squarefree regular chains such that

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

In the rest of the section, we introduce notions and recall results about computing modulo a triangular set.

Definition 2.13. Let $\Delta = (g_1, \ldots, g_m)$ be a triangular set in R with $\mathrm{lead}\,(g_s) = x_{l+s}$ and $d_s := \deg_{x_{l+s}}(g_s)$ for every $1 \leq s \leq m$, where $l := n - m$. We define

- $A(\Delta) := k(x_1, x_2, \ldots, x_l)[x_{l+1}, \ldots, x_n]/(\Delta)_{k(x_1, x_2, \ldots, x_l)}$, 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

$$B(\Delta) := \{x_{l+1}^{\alpha_1} \ldots x_n^{\alpha_m} \mid 0 \leq \alpha_s < d_s, 1 \leq s \leq m\}.$$

- 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 Γ when the triangular set under consideration is clear from context. We will also use the notation Γ_j for $\Gamma(\Delta_j)$.
- An element of $A(\Delta)$ is called *integral* if its coordinates in the standard basis $B(\Delta)$ belong to $k[x_1, \ldots, x_l]$.

Proposition 2.14 *(see [17, Proposition 3.3.1, p.76]). Let Δ 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 $\prod_{s=1}^{m} \mathrm{lc}(g_s)^{\beta_s}$ and also assume that $\sum_{s=1}^{m} \beta_s \cdot \mathrm{height}(\mathrm{lc}(g_s)) \leq d'$. Then*

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

In Proposition 2.14, if $a_1, \ldots, a_k$ are integral elements, then $\beta_1 = \ldots = \beta_s = 0$. In this case, one can choose $d' = 0$. We will also use denominator bounds in reducing an element modulo Δ.

Lemma 2.15. *Let $\Delta := (g_1, \ldots, g_m) \subset k[x_1, \ldots, x_n]$ be a squarefree regular chain such that $\mathrm{height}(g_s) \leq d$ 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:*

- $\mathrm{lc}(g_1)^{\alpha_1} \cdot \cdots \cdot \mathrm{lc}(g_m)^{\alpha_m} \cdot f = q_1 g_1 + \cdots + q_m g_m + f_0$,
- *f_0 is reduced modulo Δ, and*
- *$\alpha_s \leq t(d+1)^{m-s}$, $s = 1, 2, \ldots, m$.*

Proof. Similar to [2, Lemma 3.7]. □

Remark 2.16. Gallo and Mishra gave a bound in [6, Lemma 5.2] for the degree of the pseudoremainder f_0. We compare that bound with the corresponding bound on f_0 that can be derived from Lemma 2.15. In the table below, OB stands for "Our Bound" and GM stands for "Gallo–Mishra."

	$\mathrm{height}(g_s) \leq d$ & $\mathrm{height}(f) \leq t$	$\deg(g_s) \leq d$ & $\deg(f) \leq t$
$\deg(f_0)$	OB: $nt(d+1)^m$	OB: $nt(d+1)^m$
	GM: $(nt+1)(nd+1)^m$	GM: $(t+1)(d+1)^m$
$\mathrm{height}(f_0)$	OB: $t(d+1)^m$	OB: $t(d+1)^m$
	GM: $(nt+1)(nd+1)^m$	GM: $(t+1)(d+1)^m$

We see that the only case in which the bound from [6, Lemma 5.2] is smaller than the corresponding one derived from Lemma 2.15 is represented by the upper-right cell, in which solely degrees are considered. In fact, [6] analyzes the complexity of the Ritt–Wu Characteristic Set Algorithm in terms of degrees. So our pseudoremainder bound cannot be used to improve their complexity analysis and vice versa, as can be seen by examining the lower-left cell in which heights are the focus.

3. Outline of Szántó's algorithm

In this section, we recall main steps of the algorithm in [17] for computing a triangular decomposition for a given algebraic set. The main algorithm is described in [17, Theorem 4.1.7, p. 118] and its proof.

Algorithm 1 Triangular decomposition algorithm.

In A set of polynomials $F = \{f_0, f_1, \ldots, f_r\} \subset k[x_1, \ldots, x_n]$.
Out A set $\Theta(F)$ of squarefree regular chains such that

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

(a) For every $\mathbf{i} \subsetneq \{1, \ldots, n\}$, compute a regular chain $\Delta_{\mathbf{i}}$ with leaders $\{x_j | j \notin \mathbf{i}\}$ such that for every prime component P of $\sqrt{\langle F \rangle}$

$$\left(\dim(P) = |\mathbf{i}| \text{ and } P \cap k[x_i \mid i \in \mathbf{i}] = \{0\}\right) \Rightarrow \mathrm{Rep}(\Delta_{\mathbf{i}}) \subseteq P.$$

For details, see [17, Corollary 4.1.5, p. 115].
(b) For every $\mathbf{i} \subsetneq \{1, \ldots, n\}$, compute the multiplication table $M(\Delta_{\mathbf{i}})$ of the algebra $A(\Delta_{\mathbf{i}})$ (see Definition 2.13).
(c) For every $\mathbf{i} \subsetneq \{1, \ldots, n\}$, compute a set $\mathcal{U}(\Delta_{\mathbf{i}})$ of squarefree regular chains

$$\mathbf{unmixed}^{|\mathbf{i}|}_{|\Delta_{\mathbf{i}}|}(\Delta_{\mathbf{i}}, M(\Delta_{\mathbf{i}}), f, 1), \text{ where } f := \sum_{j=0}^{r} f_i x_{n+1}^j$$

using Algorithm 2 below.
(d) **Return** $\Theta(F) := \bigcup_{\mathbf{i} \subsetneq \{1, \ldots, n\}} \mathcal{U}(\Delta_{\mathbf{i}})$.

Step (c) of Algorithm 1 uses the function **unmixed** with the following full specification. Parts concerning multiplication tables are technical and important only for efficiency.

Specification of $\mathbf{unmixed}^l_m$.

In 1. Nonnegative integers m and l. We set $n := m + l$.
2. A regular chain $\Delta = \{g_1, \ldots, g_m\} \subset k[x_1, \ldots, x_n]$ such that for all $1 \leq s \leq m$
- $\mathrm{lead}(g_s) = x_{l+s}$;
- $\mathrm{lc}(g_s) \in k[x_1, \ldots, x_l]$;
- g_s is reduced modulo $\{g_1, \ldots, g_{s-1}\}$.

(a) The multiplication table $M(\Delta)$ of the algebra $A(\Delta)$, see Definition 2.13.
3. Polynomials f, h in $k[x_1, \ldots, x_{n+c}]$ for some $c > 0$ reduced with respect to Δ.

Out A set $\{(\Delta_1, M(\Delta_1)), \ldots, (\Delta_r, M(\Delta_r))\}$ such that
- Δ_i is a squarefree regular chain in $k[x_1, \ldots, x_n]$ for every $1 \leq i \leq r$;
- $M(\Delta_i)$ is the multiplication table of the algebra $A(\Delta_i)$ for every $1 \leq i \leq r$;
- $\bigcup_{i=1}^{r} \mathrm{Ass}(\Delta_i) = \{P \in \mathrm{Ass}(\Delta) \mid f \equiv 0, h \not\equiv 0 \mod P\}$ (see Definition 2.7);

- $\mathrm{Ass}(\Delta_i) \cap \mathrm{Ass}(\Delta_j) = \varnothing \ \forall\, i \neq j$.

Before describing the algorithm itself, we will give some intuition behind it.

Informally speaking, the main goal of **unmixed** is to transform a single regular chain Δ into a set of regular chains $\Delta_1, \ldots, \Delta_r$ such that

(a) $\Delta_1, \ldots, \Delta_r$ are squarefree regular chains;
(b) prime components of $\bigcap_{i=1}^{r} \mathrm{Rep}(\Delta_i)$ are exactly the prime components of $\mathrm{Rep}(\Delta)$, on which f vanishes and h does not vanish.

It is instructive first to understand how this transformation is performed in the univariate case, i.e. in the case when all regular chains consist of a single polynomial only. This case is also discussed in [17, p. 124-125]. Let Δ consist $g(x) \in k[x]$. A polynomial satisfying only property (b) can be computed using gcd's as follows

$$\frac{\gcd_x(g, f)}{\gcd_x(g, f, h)}. \tag{1}$$

A set of polynomials satisfying only property (a) can be obtained by separating the roots of $g(x)$ according to their multiplicity again using gcd's

$$\frac{g \gcd_x(g, g', g'')}{\gcd_x^2(g, g')}, \frac{\gcd_x(g, g') \gcd_x(g, g', g'', g^{(3)})}{\gcd_x^2(g, g', g'')}, \ldots \tag{2}$$

Formulas (1) and (2) can be combined to yield to a set of polynomials satisfying both properties (a) and (b):

$$q_i := \frac{\gcd_x(g, \ldots, g^{(i-1)}, f) \gcd_x(g, \ldots, g^{(i+1)}, f) \gcd_x^2(g, \ldots, g^{(i)}, f, h)}{\gcd_x^2(g, \ldots, g^{(i)}, f) \gcd_x(g, \ldots, g^{(i-1)}, f, h) \gcd_x(g, \ldots, g^{(i+1)}, f, h)}, \quad i = 1, 2, \ldots, \deg g. \tag{3}$$

The generalization of this approach to the multivariate case is based on two ideas

(a) Perform the same manipulations with g_m considered as univariate polynomials in x_n.
(b) Replace the standard univariate gcd with the *generalized gcd* (denoted by ggcd), that is a gcd modulo a regular chain $\Lambda := \{g_1, \ldots, g_{m-1}\}$. Generalized gcds are described in [17, Lemma 3.1.3]. Formula (3) is replaced then by

$$q_i := \frac{\mathrm{ggcd}_{x_n}(\Lambda, g_m, \ldots, g_m^{(i-1)}, f) \, \mathrm{ggcd}_{x_n}(\Lambda, g_m, \ldots, g_m^{(i+1)}, f) \, \mathrm{ggcd}_{x_n}^2(\Lambda, g_m, \ldots, g_m^{(i)}, f, h)}{\mathrm{ggcd}_{x_n}^2(\Lambda, g_m, \ldots, g_m^{(i)}, f) \, \mathrm{ggcd}_{x_n}(\Lambda, g_m, \ldots, g_m^{(i-1)}, f, h) \, \mathrm{ggcd}_{x_n}(\Lambda, g_m, \ldots, g_m^{(i+1)}, f, h)} \tag{4}$$

for $i = 1, 2, \ldots, \deg_{x_n} g_m$.

Generalized gcd is always well-defined modulo a regular chain representing a prime ideal. If the ideal represented by the regular chain is not prime, then generalized gcds modulo different prime components might have different degree, so it might be impossible to "glue" them together. In order to address this issue, the **unmixed** function splits $\mathrm{Rep}(\Lambda)$ into a union of varieties represented by regular chains, over which all the generalized gcds in (4) will be well defined. Interestingly, this can be done by calling **unmixed** recursively, because the fact that some generalized gcd is well-defined and has degree d can be expressed using equations and inequations. These equations and inequations can be further combined with f and h.

Algorithm 2 Function $\mathbf{unmixed}_m^l(\Delta, M(\Delta), f, h)$.

Input and output are described in the specification above.

(a) If $m = 0$ (so $\Delta = \varnothing$), **return** $\varnothing$ if $f \neq 0$ or $h = 0$, and **return** $\{(\varnothing, \varnothing)\}$ otherwise
(b) Set $\Lambda := \Delta_{m-1} = \{g_1, \ldots, g_{m-1}\}$ and compute $M(\Lambda)$.
(c) For every $1 \leq i \leq \deg_{x_n} g_m$ and every tuple $\mathbf{v} \in \mathbb{Z}^6_{\geqslant 0}$ with entries not exceeding $\deg_{x_n} g_m$, compute a pair of polynomials $\phi_{i,\mathbf{v}}, \psi_{i,\mathbf{v}}$ as described in [17, p. 128] such that a system $\phi_{i,\mathbf{v}} = 0,\ \psi_{i,\mathbf{v}} \neq 0$ is equivalent to
  - $f = 0$ and $h \neq 0$,
  - all six generalized gcds in (4) are well-defined and their degrees are the entries of $\mathbf{v}$.

  Formulas for $\phi_{i,\mathbf{v}}$ and $\psi_{i,\mathbf{v}}$ are given in the proof of Lemma 4.3 and in [17, p. 128].
(d) For every pair $(\phi_{i,\mathbf{v}}, \psi_{i,\mathbf{v}})$ computed in the previous step
  (i) Compute

$$\mathcal{L}_{i,\mathbf{v}} := \mathbf{unmixed}^l_{m-1}(\Lambda, M(\Lambda), \phi_{i,\mathbf{v}}, \psi_{i,\mathbf{v}}).$$

  (ii) For every $(\Lambda_{i,\mathbf{v}}, M(\Lambda_{i,\mathbf{v}})) \in \mathcal{L}_{i,\mathbf{v}}$ compute $q_{i,\mathbf{v}}$ using (4) (more details in the proof of Theorem 4.2 and in [17, pp. 129–130])
  (iii) For every $q_{i,\mathbf{v}}$ computed in the previous step, add $(\Lambda_{i,\mathbf{v}} \cup \{q_{i,\mathbf{v}}\}, M(\Lambda_{i,\mathbf{v}} \cup \{q_{i,\mathbf{v}}\}))$ to the **output**
(e) **Return** the set of all pairs $(\Lambda_{i,\mathbf{v}} \cup \{q_{i,\mathbf{v}}\}, M(\Lambda_{i,\mathbf{v}} \cup \{q_{i,\mathbf{v}}\}))$ computed in the previous step

Example 3.1. In this example, we will show that the output of Algorithm 1 can be redundant confirming [2, Remark 2.9]. We fix a positive integer D and consider

$$F := \{(x_1 - 1)(x_1 - 2)\ldots(x_1 - D)(x_2 - 1)(x_2 - 2)\ldots(x_2 - D)\}. \tag{5}$$

Step (a) of Algorithm 1 will output the following regular chains (see [17, Corollary 4.1.5] for details)

$$\Delta_{\{1\}} = \Delta_{\{2\}} = \{(x_1 - 1)(x_1 - 2)\ldots(x_1 - D)(x_2 - 1)(x_2 - 2)\ldots(x_2 - D)\},$$
$$\Delta_{\varnothing} = \{(x_1 - 1)(x_1 - 2)\ldots(x_1 - D)p_1(x_1), (x_2 - 1)(x_2 - 2)\ldots(x_2 - D)p_2(x_2)\},$$

where $p_1(x_1)$ and $p_2(x_2)$ are additional factors, which can appear during the computation with Canny's generalized resultants (see [17, Proposition 4.1.2]).

At Step (c) of Algorithm 1, $\mathbf{unmixed}_2^0(\Delta_\varnothing, M(\Delta_\varnothing), f, 1)$ will be computed. According to the specification of **unmixed**, the result of this computation will be a triangular decomposition of the set of common zeros of $\mathrm{Rep}(\Delta_\varnothing)$ and F. Since the zero set of $\mathrm{Rep}(\Delta_\varnothing)$ is finite, all these components are not components of the zero set of F. Points $\{(a_1, a_2) | a_1, a_2 \in \{1, 2, \ldots, D\}\}$ are common zeros of $\mathrm{Rep}(\Delta_\varnothing)$ and F, so the sum of the degrees of these extra components is at least D^2, and the degree of the zero set of F is just $2D$.

Moreover, this example can be generalized to higher dimensions by replacing (5) by

$$F := \{(x_1 - 1)(x_1 - 2)\ldots(x_1 - D)\ldots(x_n - 1)(x_n - 2)\ldots(x_n - D)\}.$$

The degree of the zero set of F is nD, but the sum of the degrees of extra components will be at least D^n.

4. Bounds for degrees

The following lemma is a refinement of [17, Proposition 3.3.4, p. 75].

Lemma 4.1. *Let $\Delta = (g_1, \ldots, g_m)$ be a squarefree regular chain such that* $\mathrm{height}(g_s) \leq d$ *for all s. Suppose that for all $1 \leq s \leq m$ that*

1. $\mathrm{lead}(g_s) = x_{l+s}$;
2. $lc(g_s) \in k[x_1, \ldots, x_l]$;
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 $M(\Delta)$ of structure constants of $A(\Delta)$ (see Definition 2.13) does not exceed

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

Proof. We first apply the matrix description of the pseudoremainder (see Appendix) to products of the form $x_{l+1}^{e_1} x_{l+2}^{e_2} \ldots x_{l+m}^{e_m}$, 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 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 Δ. We have two cases to consider: $e_m < d_m$ and $e_m \geq d_m$.

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 Δ by taking the maximum of $\Gamma_{m-1} := \Gamma(\Delta_{m-1})$ and d_m.

In the second case, what we denote by $\mathbf{f}^{\mathrm{low}}$ in the Appendix is here a column vector with every entry 0 and what we denote by $\mathbf{f}^{\mathrm{up}}$ 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 $G_0 \cdot \mathrm{adj}(G_d)$ 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 sum 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 Δ_{m-1}.)

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

So by Proposition 2.14 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

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

Combining these inequalities, we have

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

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

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

So we obtain $\Gamma_m \leq (d+2)^{m+1} (\log(d+2))^{m-1}$. □

Theorem 4.2. *Let $\Delta = (g_1, \dots, g_m) \subset k[x_1, \dots, x_n]$ be a regular chain of height at most d ($d > 1$). Let $l := n - m$, and assume that the following conditions are satisfied for every $s = 1, \dots, m$:*

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

Let $M(\Delta)$ be the multiplication table for the algebra $A(\Delta)$. For $f, h \in A(\Delta)[x_{n+1}, \dots, x_{n+c}]$, denote $d_f := \mathrm{height}(f)$ and $d_h := \mathrm{height}(h)$. Then for each polynomial p occurring in the computation of $\mathbf{unmixed}_m^l(\Delta, M(\Delta), f, h)$ *(see Algorithm 2), we have:*

$$\begin{aligned}\text{height}(p) \leq\ & 5.2 \cdot 242^m (d^2+2d)^m d^{\frac{1}{2}m(m+1)} \\ & \times \left(max\{d, d_f, d_h\} + 7(d+2)^m [\log(d+2)]^{m-1}\right) \log d.\end{aligned}$$

Proof. Since for the case $m = 1$ unmixed representation can be obtained simply by taking square-free part of the corresponding polynomial (see [17, p. 124]), in what follows we assume that $m > 1$. Let

$$\{(\Delta_1, M(\Delta_1)), \ldots, (\Delta_r, M(\Delta_r))\} := \mathbf{unmixed}^l_m(\Delta, M(\Delta), f, h)$$

be the output of the algorithm $\mathbf{unmixed}^l_m$ 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

$$\tilde{d}_s := \max\left\{\deg_{x_{l+s}}(g_{s,j}) \mid j = 1, \ldots, r\right\}. \tag{6}$$

The computation of $\mathbf{unmixed}^l_m$ has a tree structure. Consider a path of the computation tree with successive recursive calls:

$$\mathbf{unmixed}^l_m(\Delta_m, M(\Delta_m), f_m, h_m), \ldots, \mathbf{unmixed}^l_0(\Delta_0, M(\Delta_0), f_0, h_0)$$

where $f_m = f$, $h_m = h$ and f_s and h_s are computed from $(\Delta_{s+1}, M(\Delta_{s+1}), f_{s+1}, h_{s+1})$ for each $s = 0, \ldots, m-1$ as described in Step (c) of Algorithm 2 and [17, p. 128]. First we estimate the height of the input at each level.

Lemma 4.3. *Let* $\boldsymbol{Input}(s) := \max\{d, \text{height}(f_s), \text{height}(h_s)\}$ *for every* $s = 0, \ldots, m$. *Then*

$$\boldsymbol{Input}(s) \leq (6d)^{m-s}\left(\boldsymbol{Input}(m) + 7(d+2)^m(\log(d+2))^{m-1}\right).$$

Proof. We give an inductive analysis to obtain a bound on $\mathbf{Input}(s)$. For $s = m$, there is nothing to do. So we start with $s = m-1$ and consider the heights of f_{m-1}, h_{m-1}. Computation of these polynomials from the data of level m in Step (c) of Algorithm 2 can be summarized as follows (see also [17, pp. 127–128]):

1. Compute the j-th sub-resultants

$$\varphi^{(j)}_k(y,z) := \text{Res}^{(j)}_{x_n}\left(g_m, f_m + \sum_{l=1}^{k} g^{(l)}_m y^{l-1} + z h_m\right),$$

   for $1 \leq k \leq d$ and $0 \leq j \leq d$. Here y, z are new variables (i.e. different from the ones which g_m, f_m, h_m are polynomials in).
2. For each $1 \leq i \leq d$ and $\mathbf{v} = (v_1, \ldots, v_6) \in \mathbb{Z}^6_{\geqslant 0}$, where $0 \leq v_t \leq d$ for $1 \leq t \leq 6$,
   (a) define the polynomial $\phi_{i,\mathbf{v}}(y,z,w)$ to be a linear combination of polynomials

$$\varphi^{(u_1)}_{i-1}(y,0),\ \ \varphi^{(u_2)}_i(y,0),\ \ \varphi^{(u_3)}_{i+1}(y,0),\ \ \varphi^{(u_4)}_{i-1}(y,z),\ \ \varphi^{(u_5)}_i(y,z),\ \ \varphi^{(u_6)}_{i+1}(y,z)$$

for all $u_1, \ldots, u_6$ such that $u_i < v_i$ for $1 \leq i \leq 6$ by using the powers of a new variable w.

(b) define

$$\psi_{i,\mathbf{v}}(y,z) := \varphi_{i-1}^{(v_1)}(y,0) \cdot \varphi_i^{(v_2)}(y,0) \cdot \varphi_{i+1}^{(v_3)}(y,0) \cdot \varphi_{i-1}^{(v_4)}(y,z) \cdot \varphi_i^{(v_5)}(y,z) \cdot \varphi_{i+1}^{(v_6)}(y,z).$$

(c) reduce $\phi_{i,\mathbf{v}}$ and $\psi_{i,\mathbf{v}}$ with respect to Λ.

(d) Set $f_{m-1} := \phi_{i,\mathbf{v}}$ and $h_{m-1} := \psi_{i,\mathbf{v}}$ for this choice of $i, \mathbf{v}$.

Note that new variables y, z and w were introduced. In Algorithm 2, all new introduced variables are denoted by $x_{n+1}, \ldots, x_{n+c}$. Here we use names y, z, and w for notational simplicity.

In order to bound the heights of f_{m-1} and h_{m-1}, we bound the heights of the subresultants $\varphi_k^{(j)}(y,z)$. In the computation of a bound for the heights of the subresultants, the largest bound will be a bound for the 0-th subresultant, because higher ones are obtained by deleting rows and columns of the Sylvester matrix, whose determinant produces the 0-th subresultant.

Since we are taking subresultants with respect to x_n, all the entries of the Sylvester matrix are polynomials in $x_1, x_2, \ldots, x_{n-1}$. In particular, this means that their degrees in x_{l+i} are less than d_i for all $1 \leq i < m$. Size of this matrix is at most $d_m + d_m = 2d_m$. The first d_m is because $\deg_{x_n} g_m = d_m$. The second d_m is because f, h are reduced with respect to Δ.

Since f_{m-1}, h_{m-1} must be reduced modulo Δ_{m-1}, we will be carrying out all operations in $A(\Delta_{m-1})$. One can see 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 $\mathbf{Input}(m-1)$. In fact, our technique will give us a bound for $\mathbf{Input}(s)$ in terms of $\mathbf{Input}(s+1)$.

Since the computation of h_{m-1} involves a multiplication of six evaluated subresultants, we apply Proposition 2.14 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 0-th 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.

Assume that the heights of denominators of C and D are bounded by d'. Our two-step analysis of the height of CD using Proposition 2.14 yields:

$$\begin{aligned}\text{height}(CD) &\leq \text{height}(C) + \text{height}(D) + 2\log(2)\cdot(\Gamma(\Delta_{m-1}) + d') \\ &\leq 6d_m \cdot d + 6d_m \cdot \mathbf{Input}(m) + 12d_m \log(6d_m)\cdot\Gamma(\Delta_{m-1}) \\ &\quad + 2\cdot(\Gamma(\Delta_{m-1}) + d') \\ &\leq 6d^2 + 6d\cdot\mathbf{Input}(m) + 12d\log(6d)\cdot\Gamma(\Delta_{m-1}) + 2\cdot(\Gamma(\Delta_{m-1}) + d').\end{aligned}$$

We may bound d' by considering the sequence of exponents we obtain on $\text{lc}(g_i)$ when reducing C, D modulo Δ_{m-1}. Applying Lemma 2.15 with $\text{height}(C) \leq 6d^2 =: t$, we have

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

Therefore

$$\begin{aligned}\text{height}(h_{m-1}) \leq 6d^2 + 6d\cdot\mathbf{Input}(m) + 12d\log(6d)\cdot\Gamma(\Delta_{m-1}) + \\ + 2\cdot\left(\Gamma(\Delta_{m-1}) + 6d^2(d+1)^{m-1} - 6d^2\right).\end{aligned}$$

As a result, we have

$$\mathbf{Input}(m-1) \leq \Gamma(\Delta_{m-1})\cdot(12d\log(6d)+2) + 6d\cdot\mathbf{Input}(m) + 12d^2(d+1)^{m-1}.$$

Moreover, we can obtain a bound for $\mathbf{Input}(s)$ in term of $\mathbf{Input}(s+1)$ in a similar way. In particular, we have

$$\mathbf{Input}(s) \leq \Gamma(\Delta_s)\cdot(12d\log(6d)+2) + 6d\cdot\mathbf{Input}(s+1) + 12d^2(d+1)^s$$

for every $s = 0, \ldots, m-1$. Due to Lemma 4.1

$$\Gamma(\Delta_s) \leq (d+2)^{s+1}(\log(d+2))^{s-1}.$$

Using $d \geq 2$, it can be shown that

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

We therefore modify our recursive bound and obtain

$$\mathbf{Input}(s) \leq 17\cdot(d+2)^{s+2}(\log(d+2))^s + 6d\cdot\mathbf{Input}(s+1) + 12(d+1)^{s+2}$$

for $s = 0, 1, \ldots, m-1$. Thus, $\mathbf{Input}(s)$ does not exceed

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

Using the formula for geometric series and $d \geq 2$, we can deduce that

$$\mathbf{Input}(s) \leq (6d)^{m-s} \left(\mathbf{Input}(m) + 6(d+2)^m (\log(d+2))^{m-1} + 3.1(d+1)^m \right).$$

Using $d, m \geq 2$ we can further show that $3.1(d+1)^m \leq (d+2)^m (\log(d+2))^{m-1}$, so the above expression is bounded by

$$(6d)^{m-s} \left(\mathbf{Input}(m) + 7(d+2)^m (\log(d+2))^{m-1} \right). \quad \square$$

We return to the proof of Theorem 4.2. Using the same notation as in [17, p. 141], we denote by $\mathbf{Output}(s)$ the maximum height of polynomials computed up to level s. For example, if $s = 0$, we have $\mathbf{Output}(0) = \mathbf{Input}(0)$.

We are going to derive an upper bound for $\mathbf{Output}(m)$ recursively. Assume that we have determined $\mathbf{Output}(m-1)$ which is an upper bound for all polynomials computed up to level $m-1$. Let $i \leq d$ and $\mathbf{v} \in \mathbb{Z}^6_{\geq 0}$ such that $0 \leq v_t \leq d$ for every $t = 1, 2, \ldots, 6$. Let $(\Lambda_{i,\mathbf{v}}, M(\Lambda_{i,\mathbf{v}}))$ be an arbitrary output after the recursive call at level $m-1$ for these i and $\mathbf{v}$ (see Steps (c) and (d) of Algorithm 2). The construction of the corresponding output $(\Lambda_{i,\mathbf{v}} \cup \{q_{i,\mathbf{v}}\}, M(\Lambda_{i,\mathbf{v}} \cup \{q_{i,\mathbf{v}}\}))$ from Step (d) of Algorithm 2 (see also [17, p. 129]) is the following

1. Compute d_{t,i,v_t}, $1 \leq t \leq 6$, defined by (see [17, p. 127])

$$d_{1,i,v_1} := \mathrm{ggcd}_{x_n} \left(\Lambda_{i,\mathbf{v}} \cup \{g_m\}, g'_m, \ldots, g_m^{(i-1)}, f_m \right)$$
$$d_{2,i,v_2} := \mathrm{ggcd}_{x_n} \left(\Lambda_{i,\mathbf{v}} \cup \{g_m\}, g'_m, \ldots, g_m^{(i)}, f_m \right)$$
$$d_{3,i,v_3} := \mathrm{ggcd}_{x_n} \left(\Lambda_{i,\mathbf{v}} \cup \{g_m\}, g'_m, \ldots, g_m^{(i+1)}, f_m \right)$$
$$d_{4,i,v_4} := \mathrm{ggcd}_{x_n} \left(\Lambda_{i,\mathbf{v}} \cup \{g_m\}, g'_m, \ldots, g_m^{(i-1)}, f_m, h_m \right)$$
$$d_{5,i,v_5} := \mathrm{ggcd}_{x_n} \left(\Lambda_{i,\mathbf{v}} \cup \{g_m\}, g'_m, \ldots, g_m^{(i)}, f_m, h_m \right)$$
$$d_{6,i,v_6} := \mathrm{ggcd}_{x_n} \left(\Lambda_{i,\mathbf{v}} \cup \{g_m\}, g'_m, \ldots, g_m^{(i+1)}, f_m, h_m \right)$$

   Generalized gcd (ggcd) is described in [17, Lemma 3.1.3].
2. Compute

$$\overline{\mathrm{lc}(d_{t,i,v_t})} := \mathbf{pinvert}^l_{m-} \left(\Lambda_{i,\mathbf{v}}, M(\Lambda_{i,\mathbf{v}}), \mathrm{lc}(d_{t,i,v_t}) \right) \text{ for } 1 \leq t \leq 6,$$

where the function $\mathbf{pinvert}_m^l(\Delta, M(\Delta), f)$ for computing the pseudo-inverse of f has the following specification (see also [17, Section 3.4])

In Δ: a squarefree regular chain in $k[x_1, \ldots, x_{l+m}]$, where $x_{l+1}, \ldots, x_{l+m}$ are the leaders of Δ;
$M(\Delta)$: the multiplication table of $A(\Delta)$ (see Definition 2.13);
f: a polynomial in $k[x_1, \ldots, x_{l+m}]$ such that $f \notin P$ for every $P \in \mathrm{Ass}(\Delta)$;
Out $\bar{f} \in k[x_1, \ldots, x_{m+l}]$ such that $\bar{f} \cdot \bar{f} \equiv r \pmod{\mathrm{Rep}(\Delta)}$, where $r \in k[x_1, \ldots, x_l] \setminus \{0\}$.

3. Compute $\overline{d}_{t,i,v_t} := \overline{\mathrm{lc}(d_{t,i,v_t})} \cdot d_{t,i,v_t}$ for $1 \leq t \leq 6$.
4. Compute

$$p_{i,\mathbf{v}}^{(1)} := \overline{d}_{1,i,v_1} \cdot \overline{d}_{3,i,v_3} \cdot \overline{d}_{5,i,v_5}^2 \quad \text{and} \quad p_{i,\mathbf{v}}^{(2)} := \overline{d}_{2,i,v_2}^2 \cdot \overline{d}_{4,i,v_4} \cdot \overline{d}_{6,i,v_6},$$

and then $q_{i,\mathbf{v}}$, the result of the pseudo-division $p_{i,\mathbf{v}}^{(1)}$ by $p_{i,\mathbf{v}}^{(2)}$.
5. Compute the multiplication table $M(\Lambda_{i,\mathbf{v}} \cup \{q_{i,\mathbf{v}}\})$.

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

Step 1. The construction of ggcd in [17, Lemma 3.1.3] implies that $\mathrm{height}(d_{t,i,v_t}) \leq \mathbf{Input}(m-1)$ for every $t = 1, \ldots, 6$.

Step 2. We denote by D_{m-1} the dimension of the algebra $A(\Delta)$ over k. Then $D_{m-1} = \prod_{i=1}^{m-1} \tilde{d}_i$ (see (6)). The coefficients of $\overline{\mathrm{lc}(d_{t,i,v_t})}$ are defined as the determinants of matrices of size $D_{m-1} \times D_{m-1}$ (see [17, p. 84]). Every such matrix has a column of the form $[0, \ldots, 0, 1]^t$, and the entries of the matrix have the height at most

$$\mathrm{height}(d_{t,i,v_t}) + \Gamma(\Lambda_{i,\mathbf{v}}) \leq \mathbf{Input}(m-1) + \mathbf{Output}(m-1).$$

Therefore

$$\mathrm{height}(\overline{\mathrm{lc}(d_{t,i,v_t})}) \leq (D_{m-1} - 1)(\mathbf{Input}(m-1) + \mathbf{Output}(m-1)).$$

Step 3. Now we compute $\overline{d}_{t,i,v_t} := \overline{\mathrm{lc}(d_{t,i,v_t})} \cdot d_{t,i,v_t}$. Applying [17, Proposition 3.3.1, p. 66], we have

$$\begin{aligned} \mathrm{height}(\overline{d}_{t,i,v_t}) &\leq \mathrm{height}(\overline{\mathrm{lc}(d_{t,i,v_t})}) + \mathrm{height}(d_{t,i,v_t}) + 2\log 2 \cdot \Gamma(\Lambda_{i,\mathbf{v}}) \\ &= D_{m-1}\,\mathbf{Input}(m-1) + (D_{m-1}+1)\,\mathbf{Output}(m-1). \end{aligned}$$

Step 4. Note that, for each $t = 1, \ldots, 6$, we have $\deg_{x_n} \overline{d}_{t,i,v_t} = \deg_{x_n}(d_{t,i,v_t}) \leq d$. Therefore $p_{i,\mathbf{v}}^{(1)}$ and $p_{i,\mathbf{v}}^{(2)}$ 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 $p_{i,\mathbf{v}}^{(1)}$ or $p_{i,\mathbf{v}}^{(2)}$. Each coefficient of $p_{i,\mathbf{v}}^{(1)}$ and $p_{i,\mathbf{v}}^{(2)}$ is a sum of products of 4 coefficients of $\overline{d}_{t,i,v_t}$, $t = 1, \ldots, 6$. Thus, coefficients

of $q_{i,\mathbf{v}}$ are sums of products of at most $16d$ coefficients of $\overline{d}_{t,i,v_t}$, $t = 1, \ldots, 6$. Note that $\overline{d}_{t,i,v_t}$ are polynomials and are reduced by $\Lambda_{i,\mathbf{v}}$. Applying [17, Proposition 3.3.1, p. 66], we obtain

$$\begin{aligned}\operatorname{height}(q_{i,\mathbf{v}}) &\leq 16d \cdot \max_{t=1,\ldots,6}\{\operatorname{height}(\overline{d}_{t,i,v_t})\} + 16d\log(16d)\cdot\Gamma(\Lambda_{i,\mathbf{v}})\\ &\leq (16dD_{m-1} + 16d + 16d\log(16d))\,\mathbf{Output}(m-1)\\ &\quad + 16dD_{m-1}\,\mathbf{Input}(m-1).\end{aligned}$$

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

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

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

$$\begin{aligned}\mathbf{Output}(m) \leq (\tilde{d}_m + 2)\left(16dD_{m-1} + 16d + 16d\log(16d) + \log(\tilde{d}_m + 2)\right)\mathbf{Output}(m-1)\\ + 16dD_{m-1}(\tilde{d}_m + 2)\,\mathbf{Input}(m-1).\end{aligned}$$

We note that the computations are in the algebra $A(\Delta)$. Therefore we always have

$$\tilde{d}_i \leq d \text{ for every } i = 1, \ldots, m. \tag{7}$$

Thus $\mathbf{Output}(m)$ does not exceed

$$(d+2)(16d^m + 16d\log(32d) + \log(d+2))\,\mathbf{Output}(m-1) + 16(d+2)d^m\,\mathbf{Input}(m-1).$$

A similar argument shows that $\mathbf{Output}(s)$ does not exceed

$$\begin{aligned}\mathbf{Output}(s) \leq (d+2)(16d^s + 16d\log(32d) + \log(d+2))\,\mathbf{Output}(s-1)\\ + 16(d+2)d^s\,\mathbf{Input}(s-1)\end{aligned} \tag{8}$$

for every $s = 1, \ldots, m$. Lemma 4.3 implies that

$$\mathbf{Input}(0) \leq I_0 := (6d)^m \left(\max\{d, d_f, d_h\} + 11(d+2)^m(\log(d+2))^{m-1}\right)$$

and

$$\mathbf{Input}(s-1) \leq (6d)^{-s+1} I_0.$$

Using this notation in (8), we see that

$$(6^s\,\mathbf{Output}(s)) \leq C(s)(6^{s-1}\,\mathbf{Output}(s-1)) + 96d(d+2)I_0 \tag{9}$$

where

$$C(s) := 6(d+2)(16d^s + 16d\log(32d) + \log(d+2)). \tag{10}$$

Now we unfold this recursion and rewrite $6^m\,\mathbf{Output}(m)$ using $6^{m-1}\,\mathbf{Output}(m-1)$ and so on, we see that

$$\begin{aligned} 6^m\,\mathbf{Output}(m) &\leq \left(\prod_{s=1}^{m} C(s)\right) \cdot \mathbf{Output}(0) + 96d(d+2)I_0 \sum_{s=2}^{m}\prod_{i=s}^{m} C(i) \\ &= \left(\prod_{s=1}^{m} C(s) + 96d(d+2)\sum_{s=2}^{m}\prod_{i=s}^{m} C(i)\right) \cdot I_0. \end{aligned} \tag{11}$$

We simplify (11) by applying Lemma 4.7. In particular, we have:

$$6^m\,\mathbf{Output}(m) < 5.2 \cdot (242(d+2))^m \cdot d^{\frac{1}{2}m(m+1)} \cdot \log d \cdot I_0.$$

The inequality obtained after canceling the factor 6^m from both sides is exactly the inequality we need to prove. □

Theorem 4.4. *Let $F := \{f_0, f_1, \ldots, f_r\} \subset k[x_1, \ldots, x_n]$ be a set of polynomials of degree at most d. Let m be the maximum codimension of prime components of $\sqrt{(F)}$. Then the degree of any polynomial p appearing in the output of Algorithm 1 applied to F or during the computation does not exceed*

$$\begin{aligned} B(m,d) := {} & 5.2n \cdot 242^m (d^{2m} + 2d^m)^m d^{\frac{1}{2}m^2(m+1)} \\ & \times \left(\max\{d^m, r\} + 7(d^m+2)^m(\log(d^m+2))^{m-1}\right)\log d^m. \end{aligned} \tag{12}$$

In particular, in case r is not too large, for instance if $r \leq d^m$, we have

$$\deg p \leq n d^{(\frac{1}{2}+\epsilon)m^3}$$

where $\epsilon = \epsilon(m,d)$ is a decreasing function such that $\epsilon(m,d) < 5$ for every $d \geq 2$, $m \geq 2$, and $\lim_{m\to\infty} \epsilon(m,d) = 0$ for all d.

Remark 4.5. Ref. [10, Lemma 3] implies that $f_0, \ldots, f_r$ can be replaced by their $n+1$ generic linear combinations, so one can achieve $r \leq n$.

Proof. By [17, Corollary 4.1.5, p. 115], for every $\Delta \in \Sigma(F)$ computed in Step (a) of Algorithm 1, the height of polynomials in Δ is at most $d^{|\Delta|} \leq d^m$.

At Step (b) of Algorithm 1, for each $\Delta \in \Sigma(F)$, we compute the multiplication table $M(\Delta)$. Step (c) of Algorithm 1 is a computation of

$$\mathcal{U}(\Delta) := \mathbf{unmixed}_{|\Delta|}^{n-|\Delta|}(\Delta, M(\Delta), f, 1) \text{ for every } \Delta \in \Sigma(F)$$

where $f = f_0 + yf_1 + \ldots + y^r f_r \in k[x_1, \ldots, x_n, y]$. Note, that for each $\Delta \in \Sigma(F)$, we have $|\Delta| \leq m$.

By Theorem 4.2, for every polynomial p occurring in the computation of $\mathcal{U}(\Delta)$, we have

$$\text{height}(p) \leq \frac{1}{n} B(|\Delta|, d).$$

Since $B(m, d)$ is monotonic in m and $|\Delta| \leq m$, this implies (12).

In case $r \leq d^m$, we have $\max\{r, d^m\} = d^m$. Direct computation shows that the right hand side of (12) can be bounded by $\deg p \leq n d^{(\frac{1}{2}+\epsilon)m^3}$, where

$$\epsilon = \epsilon(m, d) := \frac{\log_d\left(\frac{1}{n} B(m, d)\right)}{m^3} - \frac{1}{2}$$

which is a decreasing function with $\epsilon(m, d) < 5$ for every $d \geq 2$, $m \geq 2$. Moreover, $\lim_{m \to \infty} \epsilon(m, d) = 0$ for all d. □

Remark 4.6. Unlike [17, Theorem 4.1.7, p. 118], the height of polynomials occurring in the computations is bounded by $d^{O(m^3)}$. In general, Algorithm 1 might produce a redundant unmixed decomposition for a given algebraic set. Moreover, it can output varieties defined by regular chains whose irreducible components are not the irreducible components of the initial algebraic set (see Example 3.1). Therefore the inequality (4.13) in [17, p. 121] is not necessarily true in general. Instead of it we use (7) in order to bound $\tilde{d}_i$. The right-hand side of (7) is d^m in terms of the input data of Algorithm 1, and this makes our bound $d^{O(m^3)}$.

Lemma 4.7. *Consider $C(s)$ defined as (see also (10))*

$$C(s) := 6(d+2)(16d^s + 16d\log(32d) + \log(d+2)).$$

Then we have:

$$\prod_{s=1}^{m} C(s) \leq \frac{678 \cdot 387}{242^2} \cdot (242(d+2))^m \cdot d^{\frac{1}{2}m(m+1)} \log d, \quad \textit{and}$$

$$\sum_{s=2}^{m}\prod_{i=s}^{m} C(i) \leq \frac{387\cdot 4}{967}\cdot (242(d+2))^{m-1}\cdot d^{\frac{1}{2}m(m+1)-1}.$$

Proof. Using $d \geq 2$, we can verify the following inequalities by direct computation

$$C(s) \leq \begin{cases} 242(d+2)d^s \text{ if } s > 2, \\ 387(d+2)d^s \text{ if } s = 2, \\ 678(d+2)d^s \log d \text{ if } s = 1. \end{cases}$$

This immediately implies the first inequality in the lemma. For the second one:

$$\begin{aligned}
\sum_{s=2}^{m}\prod_{i=s}^{m} C(i) &\leq \frac{387}{242}\sum_{s=2}^{m}(242(d+2))^{m-s+1}\cdot d^{s+(s+1)+\ldots+m} \\
&\leq \frac{387}{242}d^{\frac{1}{2}m(m+1)-1}\sum_{s=1}^{m-1}(242(d+2))^{s} \\
&\leq \frac{387}{242}d^{\frac{1}{2}m(m+1)-1}\cdot (242(d+2)^{m-1}\cdot \frac{(242(d+2))}{(242(d+2))-1} \\
&\leq \frac{387\cdot 4}{967}\cdot d^{\frac{1}{2}m(m+1)-1}\cdot (242(d+2))^{m-1}. \quad \square
\end{aligned}$$

5. Bound for the number of components

In this section, we study the number of components in the output of Szántó's algorithm.

Theorem 5.1. *Let $F \subset k[x_1,\ldots,x_n]$ be a finite set of polynomials of degree at most d. Let m be the maximum codimension of prime components of $\sqrt{(F)} \subseteq k[x_1,\ldots,x_n]$. Then the number of unmixed components in the output of Algorithm 1 applied to F is at most*

$$\binom{n}{m}\left((m+1)d^m+1\right)^m.$$

Proof. Since the degree of the given polynomials is at most d, so is their height. Step (a) of Algorithm 1 produces a set $\Sigma(F) := \{\Delta_{\mathbf{i}} \mid \mathbf{i} \subsetneq [n]\}$ of regular chains such that for every prime component P of $\sqrt{(F)}$, we have

$$(\dim P = |\mathbf{i}| \text{ and } P \cap k[x_i \mid i \in \mathbf{i}] = 0) \Rightarrow \mathrm{Rep}(\Delta) \subseteq P.$$

Due to [9, Theorem 4.4], the number of elements in a regular chain Δ is equal to the codimension of the ideal $\mathrm{Rep}(\Delta)$. Therefore the number of regular chains in $\Sigma(F)$ is not larger than the number of proper subsets of $[n]$ which has cardinality at most m.

In Step (c), we use the function **unmixed** to transform each regular chain $\Delta \in \Sigma(F)$ to the set

$$\mathcal{U}(\Delta) := \mathbf{unmixed}_{|\Delta|}^{n-|\Delta|}(\Delta, M(\Delta), f, 1)$$

of squarefree regular chains (see Algorithm 2). Thus the number of squarefree regular chains in the output is

$$M(n,m,d) := \left| \bigcup_{\Delta \in \Sigma(F)} \mathcal{U}(\Delta) \right| \leq \sum_{\Delta \in \Sigma(F)} |\mathcal{U}(\Delta)| \,.$$

We fix a regular chain $\Delta = (g_1, \ldots, g_s)$ of codimension s. The collection of squarefree regular chains in the output of $\mathbf{unmixed}_{|\Delta|}^{s}$ is simple, meaning that any two distinct unmixed components have no common irreducible components (see [17, page 124]). Since all the components of $\mathrm{Rep}(\Delta)$ are of codimension s, $|\mathcal{U}(\Delta)|$ is bounded from above by the degree of $\mathrm{Rep}(\Delta)$. Due to the definition of $\mathrm{Rep}(\Delta)$, we have $\mathrm{Rep}(\Delta) \supset (\Delta)$. Moreover, since $V(\Delta)$ and $V(\mathrm{Rep}(\Delta))$ coincide outside the zero set of the product of the initials of Δ, every irreducible component of $V(\mathrm{Rep}(\Delta))$ is an irreducible component of $V(\Delta)$. Hence, the degree of $\mathrm{Rep}(\Delta)$ does not exceed the sum of degrees of irreducible components of $V(\Delta)$. The latter can be bounded by $\deg g_1 \cdot \ldots \cdot \deg g_s$ due to [8, Theorem 1]. The proof of [17, Corollary 4.1.5] implies that every g_i depends on at most $s+1$ variables, so

$$\deg g_i \leq (s+1) \operatorname{height} g_i \leq (s+1)d^s.$$

Therefore

$$|\mathcal{U}(\Delta)| \leq (s+1)^s d^{s^2} \leq ((m+1)d^m)^s \,.$$

Since for each $s = 1, \ldots, m$, there are $\binom{n}{s}$ squarefree regular chains in $\Sigma(F)$ of cardinality s,

$$M(n,m,d) \leq \sum_{s=1}^{m} \binom{n}{s} ((m+1)d^m)^s \,.$$

Since $\binom{n}{s} \leq \binom{n}{m} \cdot \binom{m}{s}$, we have that $M(n,m,d) \leq \binom{n}{m} ((m+1)d^m + 1)^m$. □

Acknowledgments

We are grateful to Agnes Szántó and Alexey Ovchinnikov for discussions related to this work and to the anonymous referees for comments and suggestions, which helped us improve the paper significantly.

Appendix

The following results on matrix representations of pseudoremainders are used in Section 4. They are mentioned and used in [17, Section 3.3]. We include here a shortened and refined version of them.

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 $A(\Delta)$, see Definition 2.13). We will allow the degree of f to go up to $2d-1$ in fact. We first write f and g as univariate polynomials in x_n with coefficients $k[x_1, \ldots, x_{n-1}, x_{n+1}, \ldots, x_l]$:

$$f = f_0 + f_1 x_n + \cdots + f_{2d-1} x_n^{2d-1}, \quad g = g_0 + g_1 x_n + \cdots + g_d x_n^d.$$

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. Writing q and r as we wrote f, g above and substituting these expressions into the pseudoremainder equation, we obtain:

$$g_d^d(f_0 + \ldots + f_{2d-1} x_n^{2d-1}) = (g_0 + \ldots + g_d x_n^d)(q_0 + \ldots + q_{d-1} x_n^{d-1}) + r_0 + \ldots + r_{d-1} x_n^{d-1}.$$

Comparing coefficients of the powers of x_n from d to $2d-1$, we obtain the following linear system

$$\begin{pmatrix} g_d & 0 & 0 & \ldots & 0 \\ g_{d-1} & g_d & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ g_1 & g_2 & \ldots & \ldots & g_d \end{pmatrix} \begin{pmatrix} q_{d-1} \\ q_{d-2} \\ \ldots \\ q_0 \end{pmatrix} = \begin{pmatrix} f_{2d-1} \\ f_{2d-2} \\ \ldots \\ f_d \end{pmatrix} g_d^d.$$

We write the system above as $G_d \mathbf{q} = \mathbf{f}^{\text{up}} g_d^d$. 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.

Since $r = g_d^d f - qg$, after substituting we obtain one more linear system

$$\begin{pmatrix} r_{d-1} \\ r_{d-2} \\ \ldots \\ r_0 \end{pmatrix} = g_d^d \begin{pmatrix} f_{d-1} \\ f_{d-2} \\ \ldots \\ f_0 \end{pmatrix} - \begin{pmatrix} g_0 & g_1 & \ldots & \ldots & g_{d-1} \\ 0 & g_0 & g_1 & \ldots & g_{d-2} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \ldots & g_0 \end{pmatrix} \begin{pmatrix} q_{d-1} \\ q_{d-2} \\ \ldots \\ q_0 \end{pmatrix}.$$

We write this system as $\mathbf{r} = g_d^d \mathbf{f}^{\text{low}} - G_0 \mathbf{q}$. Combining with the equation for $\mathbf{q}$, we obtain

$$\mathbf{r} = g_d^d \mathbf{f}^{\text{low}} - g_d^d G_0 G_d^{-1} \mathbf{f}^{\text{up}}.$$

To count multiplications in the formula for the pseudoremainder, we re-express G_d^{-1} using Cramer's Rule: $G_d^{-1} = g_d^{-d} \cdot \text{adj}(G_d)$ where $\text{adj}(G_d)$ denotes the adjugate of G_d, (i.e. its matrix of cofactors transposed). So we have $\mathbf{r} = g_d^d \mathbf{f}^{\text{low}} - G_0 \cdot \text{adj}(G_d) \mathbf{f}^{\text{up}}$.

Observe that the entries of $\text{adj}(G_d)$ are sums of products of $d-1$ entries of G_d.

References

[1] P. Alvandi, C. Chen, S. Marcus, M.M. Maza, É. Schost, P. Vrbik, Doing algebraic geometry with the RegularChains library, in: H. Hong, C. Yap (Eds.), Mathematical Software, ICMS 2014, Springer, Berlin–Heidelberg, 2014, pp. 472–479.

[2] P. Bürgisser, P. Scheiblechner, On the complexity of counting components of algebraic varieties, J. Symbolic Comput. 44 (9) (2009) 1114–1136, https://doi.org/10.1016/j.jsc.2008.02.009.

[3] A. Chistov, Double-exponential lower bound for the degree of any system of generators of a polynomial prime ideal, St. Petersburg Math. J. 20 (6) (2009) 983–1001, https://doi.org/10.1090/S1061-0022-09-01081-4.

[4] X. Dahan, M. Moreno Maza, E. Schost, W. Wu, Y. Xie, Lifting techniques for triangular decompositions, in: ISSAC'05, ACM, New York, 2005, pp. 108–115.

[5] X. Dahan, E. Schost, Sharp estimates for triangular sets, in: Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation, ISSAC '04, ACM, New York, NY, USA, 2004, pp. 103–110.

[6] G. Gallo, B. Mishra, Efficient algorithms and bounds for Wu–Ritt characteristic sets, in: Effective Methods in Algebraic Geometry, Springer, 1991, pp. 119–142.

[7] M. Giusti, G. Lecerf, B. Salvy, A Gröbner free alternative for polynomial system solving, J. Complexity 17 (1) (2001) 154–211, https://doi.org/10.1006/jcom.2000.0571.

[8] J. Heintz, Definability and fast quantifier elimination in algebraically closed fields, Theoret. Comput. Sci. 24 (3) (1983) 239–277, https://doi.org/10.1016/0304-3975(83)90002-6.

[9] E. Hubert, Notes on triangular sets and triangulation-decomposition algorithms I: Polynomial systems, in: Proceedings of the 2nd International Conference on Symbolic and Numerical Scientific Computation, SNSC'01, Springer-Verlag, Berlin, Heidelberg, 2003, pp. 1–39.

[10] G. Jeronimo, J. Sabia, Effective equidimensional decomposition of affine varieties, J. Pure Appl. Algebra 169 (2) (2002) 229–248, https://doi.org/10.1016/S0022-4049(01)00083-4.

[11] S. Laplagne, An algorithm for the computation of the radical of an ideal, in: Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computation, ISSAC '06, ACM, New York, NY, USA, 2006, pp. 191–195.

[12] G. Lecerf, Computing an equidimensional decomposition of an algebraic variety by means of geometric resolutions, in: Proceedings of the 2000 International Symposium on Symbolic and Algebraic Computation, 2000, pp. 209–216.

[13] G. Lecerf, Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers, J. Complexity 19 (4) (2003) 564–596, https://doi.org/10.1016/S0885-064X(03)00031-1.

[14] A. Ovchinnikov, G. Pogudin, T.N. Vo, Bounds for elimination of unknowns in systems of differential-algebraic equations, Preprint, arXiv:1610.04022, 2018.

[15] E. Schost, Complexity results for triangular sets, in: ISSAC 2002, J. Symbolic Comput. 36 (3–4) (2003) 555–594, https://doi.org/10.1016/S0747-7171(03)00095-6.

[16] A. Szántó, Complexity of the Wu–Ritt decomposition, in: Second International Symposium on Parallel Symbolic Computation, PASCO '97, Maui, HI, USA, July 20–22, ACM Press, ew York, NY, 1997, pp. 139–149.

[17] A. Szántó, Computation with Polynomial Systems, Ph.D. thesis, Cornell University, 1999, http://www4.ncsu.edu/~aszanto/szanto.pdf.

[18] D. Wang, Epsilon: a library of software tools for polynomial elimination, in: Mathematical Software, World Scientific, 2002, pp. 379–389.