Irredundant Triangular Decomposition

Gleb Pogudin

Courant Institute of Mathematical Sciences
New York, NY
pogudin@cims.nyu.edu

Agnes Szanto

North Carolina State University
Raleigh, NC
aszanto@ncsu.edu

ABSTRACT

Triangular decomposition is a classic, widely used and well-developed way to represent algebraic varieties with many applications. In particular, there exist

- sharp degree bounds for a single triangular set in terms of intrinsic data of the variety it represents,
- powerful randomized algorithms for computing triangular decompositions using Hensel lifting in the zero-dimensional case and for irreducible varieties.

However, in the general case, most of the algorithms computing triangular decompositions produce embedded components, which makes it impossible to directly apply the intrinsic degree bounds. This, in turn, is an obstacle for efficiently applying Hensel lifting due to the higher degrees of the output polynomials and the lower probability of success.

In this paper, we give an algorithm to compute an irredundant triangular decomposition of an arbitrary algebraic set W defined by a set of polynomials in $\mathbb{C}[x_1, x_2, \dots, x_n]$. Using this irredundant triangular decomposition, we are able to give intrinsic degree bounds for the polynomials appearing in the triangular sets and apply Hensel lifting techniques. Our decomposition algorithm is randomized, and we analyze the probability of success.

ACM Reference Format:

Gleb Pogudin and Agnes Szanto. 2018. Irredundant Triangular Decomposition. In *ISSAC '18: 2018 ACM International Symposium on Symbolic and Algebraic Computation, July 16–19, 2018, New York, NY, USA*. ACM, New York, NY, USA, 8 pages. <https://doi.org/10.1145/3208976.3208996>

1 INTRODUCTION

Given a set of polynomials $f_1, \dots, f_s \in \mathbb{C}[x_1, x_2, \dots, x_n]$, consider the algebraic set

$$W = \{z \in \mathbb{C}^n : f_1(z) = \dots = f_s(z) = 0\}.$$

There are several common representations of algebraic sets that allow one to answer different questions about algebraic sets or perform operations with them efficiently, for example representations via Gröbner bases, geometric resolution, and triangular decomposition. This paper is focused on the latter.

Triangular decomposition is an important tool with many applications, its origins going back to the works of Ritt [20], who

introduced the concept of characteristic sets. Several authors, including Wu [27], Lazard [17], Kalkbrener [14], Wang [26], Moreno Maza [19], Schost [22], Chen [4, 5], Dahan et al. [8], have worked on triangular decompositions of algebraic sets, and some of these algorithms are implemented in MAPLE in the package RegularChains. There exist sharp degree and height bounds for a single triangular set in terms of intrinsic data of the variety it represents, see for example the sequence of papers [21, 22, 7, 9], these bounds are polynomial in the degree and the height of the variety. There are also powerful randomized algorithms for computing triangular decompositions using Hensel lifting in the zero-dimensional case [8] and for irreducible varieties [21].

On the other hand, most of the algorithms computing triangular decompositions in the general case produce embedded components. We are not aware of any easy way to delete all the embedded components afterward. Moreover, the problem of checking inclusion between two algebraic sets defined by triangular sets is known as the algebraic version of the *Ritt problem* (see [16, p. 190] and [1, p. 44] for the algebraic version) and appears to be hard. Embedded components make it impossible to directly apply the intrinsic degree bounds. The best known degree bounds for the polynomials in a triangular decomposition are essentially $D^{O(n^2)}$ [10, 24, 2] (D is a bound on the total degrees of $f_1, \dots, f_s$), which is not polynomial in the degree of the algebraic set represented by the triangular decomposition. As we show in the present paper, an irredundant triangular decomposition was needed to apply the intrinsic degree bounds of [7] that are polynomial in the degree of the variety. We note that one could achieve irredundant triangular decompositions by computing the irreducible components of the variety and their Gröbner basis, which would allow one to factor out repeated and embedded components [25, 15]. However, this method is too expensive, for example, they require polynomial factorization and Gröbner basis computation with much higher worst-case degree bounds than we aim in this paper.

We also mention that using random linear changes of the variables one can avoid embedded components and compute an irredundant equidimensional decomposition, as demonstrated in [13, 18]. However, changing the coordinate system destroys the triangular structure in the original variables, and, in particular, does not allow to perform elimination of some of the original variables. We use [13] in the present paper as one of the subroutines, but in a way that our final output does not use coordinate transformations.

As far as we know, irredundant decomposition using triangular sets, without random changes of variables, was not known previously. There are two difficulties:

- (1) The first difficulty is to detect common irreducible components among triangular sets of the same dimension but with different sets of *free variables* (see Definition 1), because even in the equidimensional case we may need to compute triangular sets using

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

ISSAC '18, July 16–19, 2018, New York, NY, USA

© 2018 Association for Computing Machinery.

ACM ISBN 978-1-4503-5550-6/18/07...\$15.00

<https://doi.org/10.1145/3208976.3208996>

different sets of free variables. As far as we know, there were no previous methods to detect if two such representations have a common irreducible component or not. One of the main results of this paper is a new technique that ensures that triangular sets representing equidimensional components with different sets of free variables have no common irreducible components (see Step 2d of Algorithm 3 and Lemma 5).

- (2) The second difficulty is to factor out components that are embedded in higher dimensional irreducible components, similarly as it is stated in the Ritt problem, mentioned above. This problem has only been solved for triangular sets in one and two dimensions [6, 1]. The second result of this paper is that we show how to use the results in [13] and turn their irredundant equidimensional decomposition into an irredundant triangular decomposition. To do that, we use the zero-dimensional *equiprojectable* decomposition of [8] and the lifting techniques of [21].

2 MAIN RESULT

For $T \subset \mathbb{C}[\mathbf{x}]$, $Z(T) \subset \mathbb{C}^n$ denotes the set of common roots of T . For $V \subset \mathbb{C}^n$, $I(V)$ denotes the set of polynomials in $\mathbb{C}[\mathbf{x}]$ vanishing on V . We recall some definitions from [12].

Definition 1. A set of polynomials Δ of the form

$$\Delta = \{g_1(\mathbf{y}, z_1), g_2(\mathbf{y}, z_1, z_2), \dots, g_m(\mathbf{y}, z_1, \dots, z_m)\} \subset \mathbb{C}[\mathbf{x}], \quad (1)$$

where $\mathbf{y} = y_1, \dots, y_d$, $\{x_1, \dots, x_n\} = \{\mathbf{y}, z_1, \dots, z_m\}$, $d + m = n$, and g_i involves z_i for every $1 \leq i \leq m$ is said to be a *triangular set*.

The variables $\mathbf{y}$ are called *free variables*. For every $1 \leq i \leq m$, z_i is said to be the *leader* of g_i , and we denote the leading coefficient of g_i , viewed as a univariate polynomial in z_i , by $\text{lc}(g_i)$. Let $I_\Delta := \{\text{lc}(g_k) : k = 1, \dots, m\}$. The ideal generated by Δ in $\mathbb{C}[\mathbf{x}]$ is denoted by (Δ) , and the ideal “pseudo-generated” by Δ is the saturated ideal

$$\mathcal{I}(\Delta) := (\Delta) : I_\Delta^\infty.$$

$\text{Rep}(\Delta)$ denotes the affine variety represented by a triangular set Δ , defined as

$$\text{Rep}(\Delta) := Z(\mathcal{I}(\Delta)) = \overline{Z(\Delta) \setminus Z(\prod_k \text{lc}(g_k))} \subset \mathbb{C}^n.$$

Definition 2. The triangular set (1) is called a *regular chain* if

- $\deg_{z_i}(g_j) < \deg_{z_i}(g_i)$ for every $1 \leq i < j \leq m$;
- $\text{lc}(g_k)$ is not a zero divisor in $\mathbb{C}[\mathbf{y}, z_1, \dots, z_{k-1}]/\mathcal{I}(g_1, \dots, g_{k-1})$ for every $1 \leq k \leq m$.

The regular chain Δ is called a *square-free regular chain* if it is a regular chain and g_k is a square-free polynomial in z_k over $\mathbb{C}[\mathbf{y}, z_1, \dots, z_{k-1}]/\mathcal{I}(g_1, \dots, g_{k-1})$ for every $1 \leq k \leq m$.

The main result of the paper is the following.

THEOREM 3. Let $W = Z(f_1, \dots, f_s)$ for $f_i \in \mathbb{C}[x_1, x_2, \dots, x_n]$ for $i = 1, \dots, s$. Assume that the total degree of f_i does not exceed $D \geq 2$ for every $1 \leq i \leq s$. We give a randomized algorithm (Algorithm 3) that computes

$$\mathbf{T} = \{\Delta_i : 1 \leq i \leq N\}$$

such that

- (1) Δ_i is a square-free regular chain for every $1 \leq i \leq N$;
- (2) None of the irreducible components of $\text{Rep}(\Delta_i)$ is contained in $\text{Rep}(\Delta_j)$ for $i \neq j$;

$$(3) W = \bigcup_{i=1}^N \text{Rep}(\Delta_i);$$

- (4) For every $1 \leq i \leq N$ and every $g \in \Delta_i$, the total degree of g with respect to the free variables does not exceed $(\deg W)^2$ and the degree with respect to every other variable does not exceed $\deg W$;

- (5) All polynomials appearing in Algorithm 3 have total degrees bounded by

$$\max\left((n+1)D^{n+1}, D^{2n} + D^n\right);$$

- (6) Assuming that in Algorithm 3 we make random choices independently and uniformly from a finite subset $\Gamma \subset \mathbb{C}$, the probability that the output of Algorithm 3 is correct is at least

$$1 - \frac{cD^{n^2+n} + (n+1)^4 D^{c'(n+1)}}{|\Gamma|}$$

for some constants c and c' .

Remark 3. One can check that our algorithm uses only gcd computation and linear algebra, so if the input polynomials are over a subfield $k \subset \mathbb{C}$ (for example, $k = \mathbb{Q}$), then the output polynomials will be also over this subfield.

4 THE TOOLBOX

4.1 Notation

Let $\mathbf{x} = (x_1, \dots, x_n)$, and for a subset $S = \{i_1, \dots, i_m\} \subset \{1, \dots, n\}$, denote $\mathbf{x}_S := (x_{i_1}, \dots, x_{i_m})$ with $i_1 < i_2 < \dots < i_m$.

4.2 Equidimensional decomposition

We use the method in [13] to eliminate embedded components in our Main Algorithm. The main idea of [13] to avoid embedded components is to represent each equidimensional part as the intersections of $n+1$ hypersurfaces, each a Chow form with respect to a random coordinate system. Then they use the equations of the higher dimensional parts to factor out lower dimensional embedded components. Algorithm 1 below is the input and output specification of the algorithm in [13].

Algorithm 1 EquiDim($f_1, \dots, f_s$)

Input $f_1, \dots, f_s \in \mathbb{C}[x_1, \dots, x_n]$, defining an algebraic variety $W = Z(f_1, \dots, f_s)$ and a real number $0 < p < 1$.

Output The sets

$$\mathbf{p}_0 = \{p_{0,0}, \dots, p_{0,n}\}, \dots, \mathbf{p}_{n-1} = \{p_{n-1,0}, \dots, p_{n-1,n}\}$$

of polynomials in $\mathbb{C}[x_1, \dots, x_n]$ represented by straight-line programs such that with probability at least p the following holds

- the set $Z(p_{\ell,0}, \dots, p_{\ell,n}) \subset \mathbb{C}^n$ is exactly W_ℓ , that is the union of all irreducible components of W of dimension ℓ , for all $0 \leq \ell \leq n-1$;
 - $\deg p_{\ell,i} \leq \deg W_\ell$ for all $0 \leq \ell \leq n-1$ and $0 \leq i \leq n$.
-

4.3 Canny's generalized resultant

Consider polynomials $f_1, \dots, f_{n+1} \in \mathbb{C}[\mathbf{x}, \mathbf{y}]$, where $\mathbf{x} = (x_1, \dots, x_n)$ and $\mathbf{y} = (y_1, \dots, y_m)$. Let $\deg f_i \leq D$ for every $1 \leq i \leq n+1$. By $\pi: \mathbb{C}^{m+n} \rightarrow \mathbb{C}^m$ we denote the projection of the $(\mathbf{x}, \mathbf{y})$ -space onto

the y-coordinates. Then the construction of the generalized perturbed resultant proposed in [3] provides a non zero polynomial $\text{PRes}_x(f_1, \dots, f_{n+1}) \in \mathbb{C}[y]$ such that

- $\text{PRes}_x(f_1, \dots, f_{n+1})$ vanishes on $\pi(C)$ for every irreducible component $C \subset Z(f_1, \dots, f_{n+1})$ with $\pi(C) \neq \mathbb{C}^m$;
- $\deg \text{PRes}_x(f_1, \dots, f_{n+1}) \leq (n+1)D^{n+1}$ (this follows from the degree bound for multivariate resultants [11, Proposition 1.1]);
- $\text{PRes}_x(f_1, \dots, f_{n+1})$ can be computed using one multivariate resultant computation for $n+1$ polynomials of degree at most D .

4.4 Triangular Decomposition over Fraction Fields

A randomized algorithm `TriangularZeroDim` with the following specifications will be used as a subroutine in Algorithm 3. One possible way to design such an algorithm is based on the equiprojectable triangular decomposition algorithm of [8] and is described in Section 6. There are also other possibilities such as the unmixed procedure from [24].

Algorithm 2 `TriangularZeroDim`($S, \{h_1, \dots, h_\ell\}$)

Input • a proper subset $S := \{i_1, \dots, i_m\} \subset \{1, \dots, n\}$ with $i_1 < \dots < i_m$

- polynomials $h_1, \dots, h_\ell \in \mathbb{C}[x]$ with $\ell \geq m$ such that
 - (1) the ideal I generated by $h_1, \dots, h_\ell$ in $\mathbb{C}(\overline{x_S})[x_S]$ is zero dimensional
 - (2) the Jacobian of $h_1, \dots, h_m$ with respect to x_S is invertible at every solution of I in the algebraic closure $\overline{\mathbb{C}(\overline{x_S})}$

Output Square-free regular chains $\Delta_1, \dots, \Delta_q \subset \mathbb{C}[x]$ such that

- (1) leaders of Δ_j are $x_{i_1}, \dots, x_{i_m}$ for every $1 \leq j \leq q$
- (2) $\text{Rep}(\Delta_i)$ and $\text{Rep}(\Delta_j)$ do not have common irreducible components for every $1 \leq i < j \leq q$
- (3) $\bigcap_{i=1}^q I(\Delta_i) \cdot \mathbb{C}(\overline{x_S}) = \sqrt{I}$
- (4) for every $g \in \Delta_1 \cup \dots \cup \Delta_q$, the coefficients of g considered as a polynomial in x_S are coprime.

Note that the algorithm in Section 6 returns triangular sets such that the leading coefficients of their elements belong to $\mathbb{C}[\overline{x_S}]$. This property is not needed in the proof of correctness of Algorithm 3, but we use it to prove our degree bounds.

5 THE MAIN ALGORITHM

See our Main Algorithm, Algorithm 3, below.

Proof of Theorem 3 (1)-(5). Denote by $\{\Delta_1, \dots, \Delta_N\}$ the output of Algorithm 3. We make the following assumptions on random choices made in Algorithm 3 (the probabilities will be estimated in the proof of (6) in Section 6):

- A1 The choice of $\lambda_{i,j}$ in Step 2a satisfies the following property:
for every $-1 \leq d \leq n-1$, $Z(\tilde{f}_1, \dots, \tilde{f}_{n-d})$ and W have the same irreducible components of dimensions larger than d .
- A2 The point α in Step 2d is chosen such that $\hat{g}_S(\alpha) \neq 0$ for all $S \subset \{1, \dots, n\}$.

Proof of (1). The fact that Δ_i is a squarefree regular chain would follow from the specification of `TriangularZeroDim` if we show that

Algorithm 3 Main Algorithm

Input $f_1, \dots, f_s \in \mathbb{C}[x_1, x_2, \dots, x_n]$ defining the affine variety $W = Z(f_1, \dots, f_s)$.

Output Representation of W as a union of varieties defined by square-free regular chains, as described in Theorem 3.

- (1) *Compute the equidimensional decomposition.* For every $0 \leq d < n$, we call the subroutine `EquiDim`($f_1, \dots, f_s$) described in Section 4.2 to compute a set of polynomials

$$\mathbf{p}_d := \{p_{d,0}, \dots, p_{d,n}\}$$

such that

$$Z(\mathbf{p}_d) = W_d,$$

where W_d is the union of irreducible components of dimension d in W . Let d_0 and d_1 be the minimal and maximal dimensions, respectively.

- (2) *Compute a cover by “univariate” triangular sets.*

- (a) *Square the system.* Let

$$\tilde{f}_i := \lambda_{i,1}f_1 + \dots + \lambda_{i,s}f_s \text{ for } 1 \leq i \leq n - d_0 + 1,$$

where $\lambda_{i,j}$ is chosen uniformly random from a finite set $\Gamma \subset \mathbb{C}$.

- (b) *Compute projections.* For each $S \subset \{1, \dots, n\}$ such that $n - d_1 - 1 \leq |S| \leq n - d_0 - 1$, compute Canny’s generalized resultants

$$\hat{g}_S := \text{PRes}_{x_S}(\tilde{f}_1, \dots, \tilde{f}_m) \in \mathbb{C}[\overline{x_S}] \subset \mathbb{C}[x],$$

defined in Section 4.3, where $|S| = m - 1$.

- (c) *Define the cover.* For each $S \subset \{1, \dots, n\}$ such that $n - d_1 \leq |S| \leq n - d_0$ define

$$\widehat{\nabla}_S := \{\hat{g}_{S_1}, \dots, \hat{g}_{S_m}\},$$

where $S = \{i_1, \dots, i_m\} \subset \{1, \dots, n\}$ with $i_1 < \dots < i_m$, and $S_j := S \setminus \{i_j\}$

- (d) *Avoid repetitions.* Choose a random point $\alpha := (\alpha_1, \dots, \alpha_n) \in \Gamma^n$ such that $\hat{g}_S(\alpha) \neq 0$ for all $S \subset \{1, \dots, n\}$. For every $n - d_1 \leq m \leq n - d_0$, for every subset $S = \{i_1, \dots, i_m\} \subset \{1, \dots, n\}$ with $i_1 < \dots < i_m$, let

$$\nabla_S := \{g_{S,1}, \dots, g_{S,m}\},$$

where $g_{S,j}$ is the squarefree part of

$$\hat{g}_{S_j}(\alpha_1, \dots, \alpha_{i_{j-1}}, x_{i_j}, \dots, x_n)$$

for $1 \leq j \leq m$, considered as a univariate polynomial in x_{i_j} .

- (3) *Compute the result.* Return

$$\bigcup_{d=d_0}^{d_1} \bigcup_{\substack{S \subset \{1, \dots, n\}, \\ |S|=n-d}} \text{TriangularZeroDim}(S, \nabla_S \cup \mathbf{p}_d)$$

The subroutine `TriangularZeroDim` is described in Section 4.4.

the input specification of `TriangularZeroDim` is satisfied. We fix $S \subset \{1, \dots, n\}$ of cardinality $n - d$. Then the first $n - d$ polynomials in the input of

$$\text{TriangularZeroDim}(S, \nabla_S \cup \mathbf{p}_d)$$

in Step 3 are ∇_S . These polynomials already generate a zero-dimensional ideal in $\mathbb{C}(\overline{x_S})[x_S]$, so $\nabla_S \cup \mathbf{p}_d$ also do. Since $g_{S,j}$ belongs to $\mathbb{C}[x_{i_j}, \overline{x_S}]$, the Jacobian of ∇_S with respect to x_S is a diagonal matrix. Moreover, since every $g_{S,j}$ is squarefree, the matrix is invertible at every solution of (∇_S) in $\overline{\mathbb{C}(\overline{x_S})}$.

Proof of (2). Let C be an irreducible component of $\text{Rep}(\Delta_i)$. Below, Lemma 4 implies that C is an irreducible component of W .

Using A1 and Lemma 5, we conclude that C is contained in $\text{Rep}(\Delta_j)$ only for $j = i$. This proves the statement.

Proof of (3). Lemma 4 implies that $\bigcup_{i=1}^N \text{Rep}(\Delta_i) \subset W$. Lemma 5 together with A1 imply that $W \subset \bigcup_{i=1}^N \text{Rep}(\Delta_i)$.

Proof of (4). Fix $S = \{i_1, \dots, i_m\}$ with $i_1 < \dots < i_m$, and consider the coordinate system $\mathbf{x}_S = (x_{i_1}, \dots, x_{i_m}) =: (z_1, \dots, z_m)$ and $\mathbf{y} := \mathbf{x}_{\bar{S}}$. First we prove that if V is represented by a square-free regular chain in the fixed coordinate system, then this square-free regular chain representing V is unique, as long as the leading coefficients are in $\mathbb{C}[\mathbf{y}]$ and the coefficients in $\mathbb{C}[\mathbf{y}]$ of each polynomial are relatively prime. This is because for any such square-free regular chain, after dividing by the leading coefficients, we get a reduced Gröbner basis with respect to the lexicographic monomial ordering with $z_1 < \dots < z_m$ of the ideal generated by $I(V)$ in the ring $\mathbb{C}(\mathbf{y})[\mathbf{z}]$. Since the reduced Gröbner basis of an ideal with a fixed monomial ordering is unique, using the assumption that the coefficients of each polynomial in the regular chain are relatively prime, we get that the square-free regular chain representing V that satisfy the above conditions is unique.

Statement (4) of Theorem 3 follows from the fact that, as described in Section 6, $\text{TriangularZeroDim}(S, \nabla_S \cup \mathbf{p}_d)$ returns a set $\{\Delta_a, \dots, \Delta_b\}$ of square-free regular chains such that the leading terms are in $\mathbb{C}[\mathbf{x}_{\bar{S}}]$ and the coefficients of the polynomials in the triangular sets are relatively prime. Moreover, the output of $\{\Delta_a, \dots, \Delta_b\}$ is an irredundant triangular decomposition of W_S , where W_S is the union of all irreducible components C of W of co-dimension m such that $\mathbf{x}_{\bar{S}}$ is the maximal subset of $\{x_1, \dots, x_n\}$ among the subsets of free variables for C , with respect to the lexicographic ordering of the variables $x_1, \dots, x_n$. So for each $i = a, \dots, b$, $V := \text{Rep}(\Delta_i)$ is a disjoint union of irreducible components of W_S . Finally we note that $\Delta_i = \{g_1, \dots, g_m\}$ is the unique square-free regular chain representing V with leading coefficients in $\mathbb{C}[\mathbf{y}]$, so we can apply the degree bounds proved in [7, Theorem 2] to get for $k = 1, \dots, m$

$$\deg_{\mathbf{y}}(g_k) \leq \left(1 + 2 \sum_{i=k-1}^m (d_i - 1)\right) \deg(V_k) \leq \deg(W_{S,k})^2 \quad (2)$$

where $d_i := \deg_{z_i}(g_i)$, and $V_k(W_{S,k})$ is the projection of V (W_S) to the coordinates $(\mathbf{y}, z_1, \dots, z_k)$. Since $\deg(W_{S,k}) \leq \deg(W)$, we get the desired bound for the free variable.

For the non-free variables, we use inequalities

$$\prod_{i=1}^m \deg_{z_i} g_i \leq \deg W \text{ and } \deg_{z_k} g_k \leq \sum_{i=1}^m \deg_{z_i} g_i - m + 1$$

to deduce $\deg_{z_k} g_k \leq \deg W$ for $k = 1, \dots, m$.

Proof of (5). Due to Section 4.2, the degrees of the polynomials appearing in Step 1 of the algorithms do not exceed $\deg W \leq D^n$.

The bounds on the degrees of the polynomials in Step 2 of the algorithm are bounded by $(n+1)D^{n+1}$, the bound on the degree of Canny's generalized resultant (see Section 4.3).

As we show in Section 6, we can use Hensel lifting in the $\mathbf{x}_{\bar{S}}$ variables to compute the output of $\text{TriangularZeroDim}(S, \nabla_S \cup \mathbf{p}_d)$, thus the $\mathbf{x}_{\bar{S}}$ -degrees and $\mathbf{x}_S$ -degrees of the polynomials computed in this subroutine do not exceed the bounds D^{2n} and D^n , respectively, stated in (4). $\square$

LEMMA 4. Let C be an irreducible component of $\text{Rep}(\Delta_i)$ for some $1 \leq i \leq N$. Then C is an irreducible component of W .

PROOF. Since Δ_i belongs to the output of Algorithm 3, Δ_i belongs to

$$\text{TriangularZeroDim}(S, \{g_{S,1}, \dots, g_{S,m}\} \cup \mathbf{p}_{n-m})$$

for some $S := \{i_1, \dots, i_m\} \subset \{1, \dots, n\}$. The specification of TriangularZeroDim implies that

- (1) $|\Delta_i| = |S| = m$, so $\dim C = n - m$ by [12, Theorem 4.4];
- (2) leaders of Δ_i are $x_{i_1}, \dots, x_{i_m}$, so $I(C) \cap \mathbb{C}[\mathbf{x}_{\bar{S}}] = 0$ by [12, Proposition 5.8];
- (3) the ideal generated by $I(\Delta_i)$ in $\mathbb{C}(\mathbf{x}_{\bar{S}})[\mathbf{x}_S]$ contains $\mathbf{p}_{n-m}$.

Due to (3), there exists $q_j \in \mathbb{C}[\mathbf{x}_{\bar{S}}]$ such that $q_j p_{n-m,j} \in I(\Delta_i) \subset I(C)$ for every $0 \leq j \leq n$. Since $I(C)$ is prime and $I(C) \cap \mathbb{C}[\mathbf{x}_{\bar{S}}] = 0$ due to (2), $p_{n-m,j} \in I(C)$ for every $0 \leq j \leq n$. Since $W_{n-m} = Z(\mathbf{p}_{n-m})$, we have $C \subset W_{n-m}$. Moreover, C is an irreducible component of W_{n-m} since $\dim C = n - m$ due to (1). This proves the lemma. $\square$

LEMMA 5. Assume that Assumptions A1 and A2 are satisfied. Then for every irreducible component $C \subset W$, there exists a unique $1 \leq i \leq N$ such that $C \subset \text{Rep}(\Delta_i)$. Moreover, C is an irreducible component of $\text{Rep}(\Delta_i)$.

PROOF. **Existence.** Let C be an irreducible component of W , $m := \text{codim } C$ and $d := n - m$. Consider all subsets $\{j_1, \dots, j_d\} \subset \{1, \dots, n\}$ such that the image of $x_{j_1}, \dots, x_{j_d}$ constitute a transcendence basis of $\mathbb{C}[\mathbf{x}]$ modulo $I(C)$. Among all these sets we find one for which the tuple $(j_1, \dots, j_d)$ (assuming that $j_1 < j_2 < \dots < j_d$) is maximal with respect to the lexicographic ordering. By $S := \{i_1, \dots, i_m\}$ we denote the complement to this subset in $\{1, \dots, n\}$.

Since $\dim C = d$ and $W \subset Z(\tilde{f}_1, \dots, \tilde{f}_{n-d})$, our assumption that $Z(\tilde{f}_1, \dots, \tilde{f}_{n-d})$ and W have the same irreducible components of dimension larger than d implies that C is a (non-embedded) irreducible component of $Z(\tilde{f}_1, \dots, \tilde{f}_{n-d})$. Since $\dim C = d$, C does not project dominantly on the $\mathbf{x}_{S \cup \{i_k\}}$ -coordinates for $1 \leq k \leq m$. Then the property 4.3 of the Canny's resultant implies that $\hat{g}_{S_k}$ (defined in Step 2b with $S_k := S \setminus \{i_k\}$) vanishes on C for every $1 \leq k \leq m$. Consider $1 \leq k \leq m$. We will prove that $g_{S,k}$ (defined in Step 2d) vanishes on C . Let

$$B := \{\ell \mid x_\ell \text{ appears in } \hat{g}_{S_k}, \ell < i_k\}.$$

If $B = \emptyset$, then $g_{S,k} = \hat{g}_{S_k}$ and vanishes on C . Otherwise, we write $\hat{g}_{S_k}$ as $\sum_{i=1}^M c_i m_i$, where $m_0, \dots, m_M$ are distinct monomials in $\mathbf{x}_B$ with $m_0 = 1$ and $c_0, \dots, c_M$ are polynomials in $\mathbb{C}[\mathbf{x}_{\bar{B}}]$. If all $c_0, \dots, c_M$ vanish on C , then $g_{S,k}$ vanishes on C . Otherwise, there exists $1 \leq t \leq M$ such that c_t does not vanish on C . Let x_{j_ℓ} be any variable in m_t , then $\hat{g}_{S_k} = 0$ is a nontrivial algebraic equation for x_{j_ℓ} over $\mathbf{x}_{\bar{S}} \setminus \{x_{j_\ell}\} \cup \{x_{i_k}\}$ modulo $I(C)$. Then, replacing x_{j_ℓ} with x_{i_k} , we obtain a lexicographically larger transcendence basis of $\mathbb{C}[\mathbf{x}]$ modulo $I(C)$. Thus $g_{S,k}$ vanishes on C .

Let $\{\Delta_a, \dots, \Delta_b\} = \text{TriangularZeroDim}(S, \nabla_S \cup \mathbf{p}_d)$ for some $1 \leq a \leq b \leq N$ with $\nabla_S = \{g_{S,1}, \dots, g_{S,m}\}$. The specification of TriangularZeroDim together with the fact that $\{g_{S,1}, \dots, g_{S,m}\} \cup$

$\mathfrak{p}_d \subset I(C)$ imply

$$\bigcap_{i=a}^b \mathbb{C}(\mathbf{x}_{\bar{S}})I(\Delta_i) = \sqrt{I} \subset \mathbb{C}(\mathbf{x}_{\bar{S}})I(C).$$

Since the latter ideal is prime, there exists $a \leq c \leq b$ such that

$$\mathbb{C}(\mathbf{x}_{\bar{S}})I(\Delta_c) \subset \mathbb{C}(\mathbf{x}_{\bar{S}})I(C).$$

Since $I(C) \cap \mathbb{C}[\mathbf{x}_{\bar{S}}] = 0$, we have $I(\Delta_c) \subset I(C)$. Hence $C \subset \text{Rep}(\Delta_c)$. Since $\dim C = \dim \text{Rep}(\Delta_c)$, C is an irreducible component of $\text{Rep}(\Delta_c)$. The existence is proved.

Uniqueness. Assume that $C \subset \text{Rep}(\Delta_{c'})$ for some $c' \neq c$. Consider the following cases

Case 1. $\dim \text{Rep}(\Delta_{c'}) = D > d = \dim C$ Since $\text{Rep}(\Delta_{c'}) \subset W_D$ and C is an irreducible component of W_d by Lemma 4, C cannot be contained in $\text{Rep}(\Delta_{c'})$.

Case 2. $\dim \text{Rep}(\Delta_{c'}) = d = \dim C$ Let

$$\Delta_{c'} \subset \text{TriangularZeroDim}(S', \{g_{S',1}, \dots, g_{S',m}\} \cup \mathfrak{p}_d)$$

for some $S' = \{i'_1, \dots, i'_m\} \subset \{1, \dots, n\}$. Consider an arbitrary $1 \leq k \leq n$, and define $\bar{S}'_k := \bar{S} \cap \{k, \dots, n\}$. Since $I(C)$ contains $g_{S,1}, \dots, g_{S,m}$, $\mathbf{x}_{\bar{S}'_k}$ is a transcendence basis of $\mathbb{C}[x_k, \dots, x_n]$ modulo $I(C) \cap \mathbb{C}[x_k, \dots, x_n]$, since $\mathbf{x}_{\bar{S}'_k}$ is clearly algebraically independent modulo $I(C) \cap \mathbb{C}[x_k, \dots, x_n]$, and for all $j \geq k$ such that $j \in S$ there exists $t \in \{1, \dots, m\}$ such that $j = i_t$ and by the construction in Step 2d we have $g_{S,t} \in I(C) \cap \mathbb{C}[x_k, \dots, x_n]$. Analogously, for $\bar{S}'_k := \bar{S}' \cap \{k, \dots, n\}$, $\mathbf{x}_{\bar{S}'_k}$ is a transcendence basis of $\mathbb{C}[x_k, \dots, x_n]$ modulo $I(C) \cap \mathbb{C}[x_k, \dots, x_n]$. Hence

$$|\bar{S} \cap \{k, \dots, n\}| = |\bar{S}' \cap \{k, \dots, n\}|$$

for every $1 \leq k \leq n$. Thus, $S = S'$. Then varieties $\text{Rep}(\Delta_c)$ and $\text{Rep}(\Delta_{c'})$ do not have common irreducible components due to the specification of `TriangularZeroDim`. $\square$

6 ZERO-DIMENSIONAL TRIANGULAR DECOMPOSITION OVER RATIONAL FUNCTIONS

In this section we describe a slight modification of the zero dimensional equiprojectable triangular decomposition algorithm of [8] that was given over the field $K = \mathbb{Q}$, while here we work over the field $K = \mathbb{C}(\mathbf{y})$ for $\mathbf{y} = y_1, \dots, y_d$.

6.1 Equiprojectable decomposition

Definition 6 ([8], p. 109). Given $h_1, \dots, h_\ell \in K[z_1, \dots, z_m]$ where K is a field (here we use both $K = \mathbb{C}(\mathbf{y})$ and $K = \mathbb{C}$), assume that

$$V = Z(h_1, \dots, h_\ell) \subset \bar{K}^m$$

is zero-dimensional, where $\bar{K}$ is the algebraic closure of K . Consider $\pi: \bar{K}^n \rightarrow \bar{K}^{n-1}$ the projection onto the first $n-1$ coordinates, and for each $x \in V$ let $N(x) := \#\pi^{-1}(\pi(x))$, the number of points in V in the π -fiber of x . Then decompose $V = V_1 \cup \dots \cup V_d$ such that $V_i := \{x \in V : N(x) = i\}$ for $i = 1, \dots, d$. Apply this splitting process recursively to each $V_1, \dots, V_d$, using the fibers of the successive projections $\bar{K}^n \rightarrow \bar{K}^i$ onto the first i coordinates, for $i = n-2, \dots, 1$. Thus we obtain a decomposition of V into

pairwise disjoint varieties that are each *equiprojectable*, which form the *equiprojectable decomposition* of V .

The reason we consider the equiprojectable decomposition is because each equiprojectable component of V is representable by a single triangular set with coefficients in K (c.f. [8, Section 2]). We use this fact to ensure that when lifting the equiprojectable components from $\mathbb{C}$ to $\mathbb{C}[[\mathbf{y}]]$ (see below), the resulting triangular sets are reconstructable over $K = \mathbb{C}(\mathbf{y})$.

The main idea for computing an equiprojectable decomposition, encoded by triangular sets, of a zero-dimensional affine variety defined by polynomials $\mathbf{H} = \{h_1, \dots, h_\ell\} \subset \mathbb{C}(\mathbf{y})[\mathbf{z}]$, is first to specify the variables $\mathbf{y}$ in a random point $\mathbf{y}^* \in \bar{\mathbb{C}}^d$ such that the equiprojectable decomposition of $Z(\mathbf{H}) \subset \bar{\mathbb{C}}(\mathbf{y})^m$, described by triangular sets in $\mathbb{C}(\mathbf{y})[\mathbf{z}]$, specializes to the equiprojectable decomposition of $Z(\mathbf{H}_{\mathbf{y}=\mathbf{y}^*}) \subset \mathbb{C}^m$. Then we can lift each triangular set in the equiprojectable decomposition of $Z(\mathbf{H}_{\mathbf{y}=\mathbf{y}^*}) \subset \mathbb{C}^m$ to a triangular set in $\mathbb{C}(\mathbf{y})[\mathbf{z}]$ in the equiprojectable decomposition of $Z(\mathbf{H}) \subset \bar{\mathbb{C}}(\mathbf{y})^m$.

To compute the equiprojectable decomposition, encoded by triangular sets, of a zero-dimensional affine variety $Z(\mathbf{H}_{\mathbf{y}=\mathbf{y}^*}) \subset \mathbb{C}^m$, we cite the algorithm outlined in [8, Section 4.]. Namely, they first call the zero-dimensional triangularization algorithm of [19], followed by the Split-and-Merge algorithm of [8, Section 2.].

6.2 Lifting and reconstructing

The lifting algorithm is a (slight extension) of the lifting procedure from [22, Section 4.2]. We will work in the ring $\mathbb{C}[\mathbf{y}, \mathbf{z}]$ with $\mathbf{y} = (y_1, \dots, y_d)$ and $\mathbf{z} = (z_1, \dots, z_m)$ with $d + m = n$.

For a single lifting step we restate the specification of [22, Algorithm LIFT] as follows:

Algorithm 4 Lift($\mathbf{H}, \mathbf{y}^*, s, \tilde{\Delta}$)

Input

- (1) set of polynomials $\mathbf{H} = \{h_1(\mathbf{y}, \mathbf{z}), \dots, h_m(\mathbf{y}, \mathbf{z})\} \subset \mathbb{C}[\mathbf{y}, \mathbf{z}]$;
- (2) a point $\mathbf{y}^* \in \bar{\mathbb{C}}^d$;
- (3) a nonnegative integer s ;
- (4) a regular chain $\tilde{\Delta} = \{\tilde{g}_1(\mathbf{y}, z_1), \tilde{g}_2(\mathbf{y}, z_1, z_2), \dots, \tilde{g}_m(\mathbf{y}, \mathbf{z})\} \subset \mathbb{C}[\mathbf{y} - \mathbf{y}^*, \mathbf{z}]$ such that
 - $\text{lc}(\tilde{g}_k) = 1$ for $k = 1, \dots, m$
 - $\tilde{g}_k$ is reduced modulo $\{\tilde{g}_1, \dots, \tilde{g}_{k-1}\}$
 - there exists $\Delta = \{g_1(\mathbf{y}, z_1), g_2(\mathbf{y}, z_1, z_2), \dots, g_m(\mathbf{y}, \mathbf{z})\} \subset \mathbb{C}(\mathbf{y})[\mathbf{z}]$ such that
 - every element of $\mathbf{H}$ can be reduced to zero using Δ
 - $\tilde{\Delta} \equiv \Delta \pmod{(\mathbf{y} - \mathbf{y}^*)^{2^s}}$
 - $\text{jac}_{\mathbf{z}}(\mathbf{H}|_{\mathbf{y}=\mathbf{y}^*})$ is invertible modulo $\tilde{\Delta}|_{\mathbf{y}=\mathbf{y}^*}$;

Output Regular chain $\hat{\Delta} = \{\hat{g}_1(\mathbf{y}, z_1), \dots, \hat{g}_m(\mathbf{y}, \mathbf{z})\} \subset \mathbb{C}[\mathbf{y} - \mathbf{y}^*, \mathbf{z}]$ satisfying

- $\text{lc}(\hat{g}_k) = 1$ for $k = 1, \dots, m$;
 - $\hat{\Delta} \equiv \Delta \pmod{(\mathbf{y} - \mathbf{y}^*)^{2^{s+1}}}$;
-

Then one can adapt the general strategy of the main algorithm from [8, p. 113] to generalize the algorithm from [21, p. 584] as shown in Algorithm 5.

In Algorithm 5, we use the subroutine `RationalReconstruction` described in [22, Section 4.3.1].

The following lemma is an adaptation of the arguments presented in [8, Section 3] for the rational function field case. Since the

Algorithm 5 TriangularZeroDim via Hensel lifting

Input Set of polynomials $\mathbf{H} = \{h_1(\mathbf{y}, \mathbf{z}), \dots, h_\ell(\mathbf{y}, \mathbf{z})\} \subset \mathbb{C}[\mathbf{y}, \mathbf{z}]$ such that $\text{jac}_{\mathbf{z}}(\mathbf{H}_0)$ is invertible at every solution of $\mathbf{H}$ in $\overline{\mathbb{C}(\mathbf{y})}$, where $\mathbf{H}_0 = \{h_1(\mathbf{y}, \mathbf{z}), \dots, h_m(\mathbf{y}, \mathbf{z})\}$.

Output Equiprojectable triangular decomposition of $\mathbf{H}$

- (1) Pick coordinates of $\mathbf{y}_1, \mathbf{y}_2 \in \mathbb{C}^d$ randomly from a finite $\Gamma \subset \mathbb{C}$
- (2) Compute the equiprojectable decompositions $\tilde{\Delta}_1, \dots, \tilde{\Delta}_N$ and $\bar{\Delta}_1, \dots, \bar{\Delta}_N$ of $\mathbf{H}|_{\mathbf{y}=\mathbf{y}_1}$ and $\mathbf{H}|_{\mathbf{y}=\mathbf{y}_2}$, respectively
- (3) $s = 0$
- (4) While not Stop
 - (a) $\tilde{\Delta}_i := \text{Lift}(\mathbf{H}_0, \mathbf{y}_1, s, \tilde{\Delta}_i)$ for every $1 \leq i \leq N$
 - (b) $s := s + 1$
 - (c) $\Delta_i := \text{RationalReconstruction}(\tilde{\Delta}_i)$ for every $1 \leq i \leq N$
 - (d) if $\{\bar{\Delta}_1, \dots, \bar{\Delta}_N\} = \{\Delta_1|_{\mathbf{y}=\mathbf{y}_2}, \dots, \Delta_N|_{\mathbf{y}=\mathbf{y}_2}\}$, then Stop := true
- (5) Return $\{\Delta_1, \dots, \Delta_N\}$

bounds in [8, Section 3] were given in terms of heights of rational numbers, we cannot straightforwardly cite those results, so we present the analogous bounds for $\mathbb{C}(\mathbf{y})$.

LEMMA 7. Assume that $\mathbf{H} = \{h_1(\mathbf{y}, \mathbf{z}), \dots, h_\ell(\mathbf{y}, \mathbf{z})\} \subset \mathbb{C}[\mathbf{y}, \mathbf{z}]$ satisfies the input specifications of Algorithm 5, and assume that $\deg_{(\mathbf{z}, \mathbf{y})}(h_i) \leq \mathcal{H}$ for $i = 1, \dots, \ell$. Denote by P the (finite) number of solutions of $\mathbf{H}$ in the algebraic closure $\overline{\mathbb{C}(\mathbf{y})}$ and by Q the degree of the affine variety $Z(\mathbf{H})$ in $\mathbb{C}^{m+d} = \mathbb{C}^n$. Then there exists a polynomial $F \in \mathbb{C}[\mathbf{y}]$ with

$$\deg_{\mathbf{y}}(F) \leq 4m^2 P Q \mathcal{H}^2$$

with the property that if $F(\mathbf{y}^*) \neq 0$ for $\mathbf{y}^* \in \mathbb{C}^d$ then the equiprojectable triangular decomposition of $\mathbf{H}$ specializes to the equiprojectable triangular decomposition of $\mathbf{H}|_{\mathbf{y}=\mathbf{y}^*}$, and the Jacobian of $\mathbf{H}_0|_{\mathbf{y}=\mathbf{y}^*}$ does not vanish at any of the solutions of $\mathbf{H}|_{\mathbf{y}=\mathbf{y}^*}$ in $\mathbb{C}^m$.

PROOF. Using the notation of [8, Section 3], for $k = 1, \dots, m$, denote by $u_k = u_{k,1}z_1 + \dots + u_{k,k}z_k$ ($u_{k,j} \in \mathbb{C}$) a primitive element for the projection of the finite number of solutions of $\mathbf{H}$ in the algebraic closure $\overline{\mathbb{C}(\mathbf{y})}$, where the projection is to the $(z_1, \dots, z_k)$ coordinates. Let $\mu_k \in \mathbb{C}[\mathbf{y}][T]$ be the minimal polynomial of u_k . Furthermore, let $w_1, \dots, w_m \in \mathbb{C}(\mathbf{y})[T]$ be the parametrization of the solutions of $\mathbf{H}$ in $\overline{\mathbb{C}(\mathbf{y})}$ with respect to u_m . Analogously to [8, Lemmas 4-7], we can prove that the 3 hypotheses

- H_1 : None of the coefficients of $\mu_m, w_1, \dots, w_m$ vanish at $\mathbf{y} = \mathbf{y}^*$;
- H_2 : $\mu_k|_{\mathbf{y}=\mathbf{y}^*} \in \mathbb{C}[T]$ is squarefree for $k = 1, \dots, m$;
- H_3 : The Jacobian of $\mathbf{H}_0|_{\mathbf{y}=\mathbf{y}^*}$ is not zero at the solutions of $\mathbf{H}|_{\mathbf{y}=\mathbf{y}^*}$;

imply that the equiprojectable triangular decomposition of $\mathbf{H}$ specializes to the equiprojectable triangular decomposition of $\mathbf{H}|_{\mathbf{y}=\mathbf{y}^*}$, and the set of solutions of $\mathbf{H}$ in $\overline{\mathbb{C}(\mathbf{y})}$ specializes at $\mathbf{y} = \mathbf{y}^*$ to the set of solutions of $\mathbf{H}|_{\mathbf{y}=\mathbf{y}^*}$ in $\mathbb{C}^m$. In [8, Lemma 8] they prove that H_1 and H_2 is satisfied if for $a_k := \text{Res}_T(\mu_k, \mu'_k) \in \mathbb{C}[\mathbf{y}]$ we have $a_k(\mathbf{y}^*) \neq 0$ for $k = 1, \dots, m$. Let $a = a_1 \cdots a_m$. Using that $\deg_T(\mu_k) \leq P$ and $\deg_{\mathbf{y}}(\mu_k) \leq Q$ by [22, Theorem 1], we can see that

$$\deg_{\mathbf{y}}(a) \leq m(2P - 1)Q.$$

Furthermore, let J^h be the homogenization of the Jacobian of $\mathbf{H}_0$ by adding a homogenizing variable z_0 to $z_1, \dots, z_m$, and consider $J^h(\mu'_m, v_1, \dots, v_m)$ where $v_k := w_k \mu'_m \bmod \mu_m \in \mathbb{C}[\mathbf{y}][T]$ (note that this homogenization step turns the polynomials w_i from having coefficients in $\mathbb{C}(\mathbf{y})$ with higher degree numerators and denominators into polynomials $v_i \in \mathbb{C}[\mathbf{y}][T]$ with $\mathbf{y}$ -degrees at most Q , see [22] for more details). In [8, Lemma 9] they prove that H_3 is satisfied if for the Sylvester resultant $b := \text{Res}_T(J^h(\mu'_m, v_1, \dots, v_m), \mu_m) \in \mathbb{C}[\mathbf{y}]$ we have $b(\mathbf{y}^*) \neq 0$. To bound the degree of b first note that

$$\deg_T J^h(\mu'_m, v_1, \dots, v_m) \leq mP\mathcal{H}$$

and

$$\deg_{\mathbf{y}} J^h(\mu'_m, v_1, \dots, v_m) \leq mQ\mathcal{H}$$

again by [22, Theorem 1], so

$$\deg_{\mathbf{y}}(b) \leq 2m^2 Q P \mathcal{H}^2.$$

Putting it all together, for $F = ab$ we get the claimed degree bound. $\square$

Now we are able to prove the last remaining part of our main theorem:

Proof of Theorem 3, (6). Assume that $\deg_{\mathbf{x}}(f_i) \leq D$ for $i = 1, \dots, s$. In Algorithm 3, we have the following independent random uniform choices from a finite subset Γ of the coefficient field $\mathbb{C}$, and we bound the probability of success using the Schwartz-Zippel lemma [28, 23].

- In Step 1 we call the equidimensional decomposition algorithm of [13] with input $f_1, \dots, f_s$. In [13, Remark 10] they prove that the probability of success for their algorithm is at least

$$1 - \frac{c_1 D^{n^2+n} + D^{c_2(n+1)}}{|\Gamma|}$$

where c_1 and c_2 are constants. They use randomization to obtain linear combinations of the input polynomials, changes of variables and the linear forms for the primitive elements used in each step.

- In Step 2a, we choose at most $n + 1$ random linear combinations $f_1, \dots, f_{n+1}$ of the input polynomials $f_1, \dots, f_s$. The correctness of the algorithm requires the assumption A1 to hold. In [13, Remark 4] they prove that this can be done with a probability of success

$$\prod_{h=1}^{n+1} \left(1 - \frac{D^{h-1}}{|\Gamma|}\right).$$

- In Step 2d we choose $\alpha \in \Gamma^n$ randomly, and we require Assumption A2 to hold. Since $\deg_{\mathbf{x}}(\hat{g}_s) \leq (n + 1)D^{n+1}$ (due to the degree bound for a Canny's resultant, see Section 4.3), we have that the probability of success is at least

$$1 - \frac{2^n(n + 1)D^{n+1}}{|\Gamma|}$$

- In Step 3 we assume that we use the randomized algorithm described in Algorithm 5 with input $\mathbf{H} = \{h_1, \dots, h_\ell\}$. We use Lemma 7 to bound the probability of success. We have

$\deg_x(h_i) \leq \mathcal{H} = (n+1)D^{n+1}$, $P, Q \leq \deg W \leq D^n$, $m \leq n$, so we get that the probability of success is at least

$$1 - \frac{(n+1)^4 D^{4(n+1)}}{|\Gamma|}.$$

Since these random choices are independent, the probability of the success is the product of the individual probabilities, thus we get that the probability of the overall success of Algorithm 3 is at least the product of the above four probabilities, which, as long as $D \geq 2$, can be bounded from below by

$$1 - \frac{cD^{n^2+n} + (n+1)^4 D^{c'(n+1)}}{|\Gamma|},$$

for some constants c and c' , proving the claim. $\square$

7 EXAMPLES

To keep the presentation simple, in the following examples instead of random choices of numbers we use some choices which satisfy the requirements of the algorithm.

Example 8. This simple example demonstrates how our algorithm avoids repetition of irreducible components when they need different sets of free variables. Let $n = 2$, $s = 1$, and $f_1 = x_1 x_2 (x_1 + x_2)$. Then

- (1) All irreducible components are of dimension one, so $\mathbf{p}_1 = \{f_1\}$ and $d_0 = d_1 = 1$. Note that for a hypersurface, EquiDim from [13] always returns its defining equation.
- (2)(a) Since $s = 1$, $\tilde{f}_1 = f_1$.
- (b) $n - d_1 - 1 \leq |S| \leq n - d_0 - 1$ implies $S = \emptyset$. We set

$$\hat{g}_\emptyset = \text{PRes}_\emptyset(f_1) = f_1.$$

- (c) We define $\widehat{\nabla}_{S_1} = \widehat{\nabla}_{S_2} = \{\hat{g}_\emptyset\} = \{f_1\}$.
- (d) We choose $\alpha = (1, 1)$. Then

$$\nabla_{S_1} := \{f_1\}, \quad \nabla_{S_2} := \{f_1|_{x_1=1}\} = \{x_2(x_2 + 1)\}.$$

- (3) The output is a union of
 - $\text{TriangularZeroDim}(\{1\}, \{f_1\} \cup \{f_1\})$. Since f_1 alone is already a triangular set over $\mathbb{C}(\overline{\mathbf{x}}_{\{1\}}) = \mathbb{C}(x_2)$, we only have to make its coefficient coprime by division by x_2 . Thus, the output is $\{x_1(x_1 + x_2)\}$.
 - $\text{TriangularZeroDim}(\{2\}, \{x_2(x_2 + 1)\} \cup \{f_1\})$. This is equal to the gcd of $x_2(x_2 + 1)$ and f_1 as univariate polynomials in x_2 , that is x_2 .
 So, the output is $\{x_1(x_1 + x_2)\}, \{x_2\}$.

Example 9. Here, the algebraic set is the projective twisted cubic space curve (interpreted as the cone over it in $\mathbb{C}^4$). Since this curve is not a complete intersection, leading coefficients of its triangular set vanish on an extraneous projective curve, independently of the coordinate system. The intersection of this extraneous curve with the original twisted cubic will create embedded components that Triangularize in MAPLE does not factor out. Here we show how our algorithm handles this example. Let $n = 4$, $s = 3$, and

$$(f_1, f_2, f_3) = (x_1 x_3 - x_2^2, x_2^2 + x_2 x_4 - x_3^2, x_1(x_2 + x_4) - x_2 x_3).$$

Then

- (1) The system $f_1 = f_2 = f_3 = 0$ defines an irreducible two-dimensional variety, so $d_0 = d_1 = 2$. The output of [13] is a set of at most 5 polynomials defining this irreducible variety, so we can assume that $\mathbf{p}_2 = \{f_1, f_2, f_3\}$.
- (2)(a) One can check that the choice $\tilde{f}_1 = f_1$ and $\tilde{f}_2 = f_2$ satisfies A1.
- (b) Since $n - d_0 - 1 = n - d_1 - 1 = 3$, we compute four Canny's resultants, which turn out to be usual resultants in this case

$$\begin{aligned} \hat{g}_{\{1\}} &= x_2^2 + x_2 x_4 - x_3^2, \\ \hat{g}_{\{2\}} &= x_3(x_1 x_4^2 - x_1^2 x_3 + 2x_1 x_3^2 - x_3^3), \\ \hat{g}_{\{3\}} &= x_2(x_1^2 x_4 + x_1^2 x_2 - x_2^3), \\ \hat{g}_{\{4\}} &= x_1 x_3 - x_2^2. \end{aligned}$$

- (c) Using $\hat{g}_{\{1\}}, \dots, \hat{g}_{\{4\}}$, we can define $\widehat{\nabla}_S$ for every two-element subset $S \subset \{1, 2, 3, 4\}$. In what follows, we will discuss only $S_1 = \{1, 2\}$ and $S_2 = \{1, 4\}$. Other subsets will yield to the results similar to S_2 .
- (d) We can set $\alpha = (1, 1, 1, 1)$. Then $g_{S_1,1} = \hat{g}_{\{2\}}$, $g_{S_1,2} = \hat{g}_{\{1\}}$, so $\nabla_{S_1} = \{\hat{g}_{\{2\}}, \hat{g}_{\{1\}}\}$. For S_2 we have $g_{S_2,1} = \hat{g}_{\{4\}}$ and

$$g_{S_2,2} = (x_2^2 + x_2 x_4 - x_3^2)|_{x_2=1, x_3=1} = x_4.$$

- (3) $\text{TriangularizeZeroDim}(S_1, \nabla_{S_1} \cup \{f_1, f_2, f_3\})$ will return a single triangular set

$$\{x_3 x_1^2 + x_2 x_4 - x_3^2, x_2^2 + x_2 x_4 - x_3^2\}.$$

One can see that $\text{TriangularizeZeroDim}(S_2, \nabla_{S_2} \cup \{f_1, f_2, f_3\})$ is empty, because

$$f_2 - x_2 g_{S_2,2} = x_2^2 - x_3^2 \in \mathbb{C}[\mathbf{x}_{S_2}^-].$$

Analogously, all other calls of $\text{TriangularizeZeroDim}$ will return empty sets.

Although the ideal generated by f_1, f_2, f_3 in this example is prime, Triangularize function for REGULARCHAINS library (MAPLE 2016) returns two additional triangular sets, namely $\{x_1, x_2, x_3\}$ and $\{x_2, x_3, x_4\}$.

Example 10. Our last example demonstrates how Algorithm 3 handles mixed dimensional algebraic sets with embedded components. Let $n = 2$, $s = 2$, and

$$(f_1, f_2) = (x_2(x_1 + x_2)(x_1^2 - 2), x_2(x_1 + x_2)(x_2^2 - 2)).$$

Then

- (1) The system $f_1 = f_2 = 0$ defines a union of two lines and two points, so $d_0 = 0$, $d_1 = 1$, and we assume that [13] returns

$$\mathbf{p}_0 = \{(x_1 - 2x_2)^2 - 2, (x_1 + x_2)^2 - 8, (x_1 + 2x_2)^2 - 18\},$$

$$\mathbf{p}_1 = \{x_2(x_1 + x_2)\}.$$

- (2)(a) The choice $\tilde{f}_1 = f_1$ and $\tilde{f}_2 = f_2$ satisfies A1.

- (b) We compute

$$\begin{aligned} \hat{g}_\emptyset &= \text{PRes}_\emptyset(f_1) = f_1, \\ \hat{g}_{\{1\}} &= \text{PRes}_{x_1}(f_1, f_2) = x_2^2(x_2 - 1)(x_2^2 - 2)^3, \\ \hat{g}_{\{2\}} &= \text{PRes}_{x_2}(f_1, f_2) = 2(x_1 - 1)(x_1^2 + 2x_1 - 2)(x_1^2 - 2)^3, \end{aligned}$$

where $\hat{g}_{\{1\}}$ and $\hat{g}_{\{2\}}$ are actually perturbed resultants, because f_1 and f_2 are not coprime.

- (c) We set $\widehat{\nabla}_{\{1,2\}} = \{\hat{g}_{\{2\}}, \hat{g}_{\{1\}}\}$, $\widehat{\nabla}_{\{1\}} = \widehat{\nabla}_{\{2\}} = \{\hat{g}_\emptyset\}$.

(d) We chose $\alpha = (1, 1)$. Then $\nabla_{\{1\}} = \widehat{\nabla}_{\{1\}}$,

$$\nabla_{\{2\}} = \{f_1|_{x_1=1}\} = \{-x_2(x_2 + 1)\},$$

and $\nabla_{\{1,2\}}$ is obtained from $\widehat{\nabla}_{\{1,2\}}$ by taking squarefree parts

$$\nabla_{\{1,2\}} = \{2(x_1 - 1)(x_1^2 + 2x_1 - 2)(x_1^2 - 2), x_2(x_2 - 1)(x_2^2 - 2)\}.$$

(3) The output is a union of

- $\text{TriangularZeroDim}(\{1, 2\}, \nabla_{\{1,2\}} \cup \mathbf{p}_0)$. The output is $\{x_1 - x_2, x_2^2 - 2\}$.
- $\text{TriangularZeroDim}(\{1\}, \nabla_{\{1\}} \cup \mathbf{p}_1)$. Since $\nabla_{\{1\}} \cup \mathbf{p}_1$ consists of $x_2(x_1 + x_2)(x_1^2 - 2)$ and $x_2(x_1 + x_2)$, the ideal is defined by a single polynomial $x_2(x_1 + x_2)$, which is already a triangular set itself. Dividing it by x_2 , we make all its coefficients coprime as elements of $\mathbb{C}[x_2]$, so the output will be $\{x_1 + x_2\}$.
- $\text{TriangularZeroDim}(\{2\}, \nabla_{\{2\}} \cup \mathbf{p}_1)$. Since $\nabla_{\{2\}} \cup \mathbf{p}_1$ consists of $-x_2(x_2 + 1)$ and $x_2(x_1 + x_2)$, the result will consist of the gcd of these two polynomials as polynomials in x_2 , that is x_2 itself. Hence, the output is $\{x_2\}$.

Thus, we obtain three triangular sets

$$\{x_1 - x_2, x_2^2 - 2\}, \{x_1 + x_2\}, \{x_2\}.$$

The output of `Triangularize` function from `REGULARCHAINS` library (MAPLE 2016) consists of $\{x_1^2 - 2, x_2^2 - 2\}, \{x_1 + x_2\}, \{x_2\}$, so it contains embedded components.

8 CONCLUDING REMARKS

In a longer version of this paper we plan to further extend the results of this paper as follows:

- Consider a modification of our algorithms that outputs squarefree regular chains that have degrees essentially bounded by $\deg W$. These triangular sets were studied for example in [7], they are multiples of the ones our algorithm outputs, and have leading coefficients that depend on non-parametric variables.
- Modify the algorithm so that all intermediate degrees are also bounded by intrinsic geometric data of the input.
- Consider algebraic sets defined by polynomials over $\mathbb{Q}$ and bound the height of the coefficients of the polynomials in the triangular sets. Such bit-size estimates were given for a single triangular set in the positive dimensional case in [9].
- Generalize Algorithm 3 to the case when the input system contains inequations.

ACKNOWLEDGEMENTS

Gleb Pogudin was supported by NSF grants CCF-0952591, CCF-1563942, DMS-1413859, by PSC-CUNY grant #60098-00 48, by Queens College Research Enhancement, and by the Austrian Science Fund FWF grant Y464-N18. The authors would like to thank the Department of Mathematics at North Carolina State University and the Symbolic Computation Group for their hospitality during the visit of Gleb Pogudin in 2017, allowing to make progress on this research. The authors are grateful to the referees for the comments which helped to improve the paper.

REFERENCES

- [1] P. Alvandi. *Computing Limit Points of Quasi-components of Regular Chains and its Applications*. PhD thesis, The University of Western Ontario, 2017. Electronic Thesis and Dissertation Repository. 4565.
- [2] E. Amzallag, G. Pogudin, M. Sun, and N. Thieu Vo. Complexity of triangular representations of algebraic sets. arxiv.org/abs/1609.09824, 2016.
- [3] J. Canny. Generalised characteristic polynomials. *Journal of Symbolic Computation*, 9(3):241–250, 1990. URL [https://doi.org/10.1016/S0747-7171\(08\)80012-0](https://doi.org/10.1016/S0747-7171(08)80012-0).
- [4] C. Chen. *Solving Polynomial Systems via Triangular Decomposition*. PhD thesis, The University of Western Ontario, 2011.
- [5] C. Chen and M. Moreno Maza. Algorithms for computing triangular decomposition of polynomial systems. *J. Symbolic Comput.*, 47(6):610–642, 2012. ISSN 0747-7171. URL <https://doi.org/10.1016/j.jsc.2011.12.023>.
- [6] C. Chen, P. Alvandi, and M. Moreno Maza. Computing the limit points of the quasi-component of a regular chain in dimension one. In *Proceedings of Computer Algebra in Scientific Computing - 15th International Workshop, CASC 2013*, Lecture Notes in Computer Science, volume 8136, pages 30–45. Springer-Verlag, 2013.
- [7] X. Dahan and E. Schost. Sharp estimates for triangular sets. In *ISSAC 2004*, pages 103–110. 2004. URL <http://dx.doi.org/10.1145/1005285.1005302>.
- [8] X. Dahan, M. Moreno Maza, E. Schost, W. Wu, and Y. Xie. Lifting techniques for triangular decompositions. In *ISSAC'05*, pages 108–115. ACM, New York, 2005.
- [9] X. Dahan, A. Kadri, and E. Schost. Bit-size estimates for triangular sets in positive dimension. *J. Complexity*, 28(1):109–135, 2012. ISSN 0885-064X.
- [10] G. Gallo and B. Mishra. Wu-Ritt characteristic sets and their complexity. In *Discrete and computational geometry (New Brunswick, NJ, 1989/1990)*, volume 6 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, pages 111–136. Amer. Math. Soc., Providence, RI, 1991.
- [11] I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky. *Discriminants, Resultants and Multidimensional Determinants*. Birkhäuser Boston, 1994.
- [12] 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*, pages 1–39, Berlin, Heidelberg, 2003. Springer-Verlag.
- [13] G. Jeronimo and J. Sabia. Effective equidimensional decomposition of affine varieties. *Journal of Pure and Applied Algebra*, 169(2):229–248, 2002. URL [https://doi.org/10.1016/S0022-4049\(01\)00083-4](https://doi.org/10.1016/S0022-4049(01)00083-4).
- [14] M. Kalkbrener. A generalized Euclidean algorithm for computing triangular representations of algebraic varieties. *J. Symbolic Comput.*, 15(2):143–167, 1993. ISSN 0747-7171. URL <https://doi.org/10.1006/jsc.1993.1011>.
- [15] M. Kalkbrener. Prime decompositions of radicals in polynomial rings. *J. Symbolic Comput.*, 18(4):365–372, 1994. ISSN 0747-7171. URL <https://doi.org/10.1006/jsc.1994.1052>.
- [16] E. R. Kolchin. *Differential algebra and algebraic groups*. Academic Press, New York-London, 1973. Pure and Applied Mathematics, Vol. 54.
- [17] D. Lazard. A new method for solving algebraic systems of positive dimension. *Discrete Appl. Math.*, 33(1-3):147–160, 1991. ISSN 0166-218X. URL [https://doi.org/10.1016/0166-218X\(91\)90113-B](https://doi.org/10.1016/0166-218X(91)90113-B). Applied algebra, algebraic algorithms, and error-correcting codes (Toulouse, 1989).
- [18] G. Lecerf. Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers. *J. Complexity*, 19(4):564–596, 2003. ISSN 0885-064X.
- [19] M. Moreno Maza. On triangular decompositions of algebraic varieties. Presented at the MEGA-2000 conference, Bath, UK, June 2000. URL www.csd.uwo.ca/~moreno/Publications/M3-MEGA-2005.pdf.
- [20] J. F. Ritt. *Differential algebra*. Dover Publications, Inc., New York, 1966.
- [21] É. Schost. Complexity results for triangular sets. *Journal of Symbolic Computation*, 36(3):555–594, 2003. URL [https://doi.org/10.1016/S0747-7171\(03\)00095-6](https://doi.org/10.1016/S0747-7171(03)00095-6).
- [22] É. Schost. Computing parametric geometric resolutions. *Applicable Algebra in Engineering, Communication and Computing*, 13(5):349–393, 2003. URL <https://doi.org/10.1007/s00200-002-0109-x>.
- [23] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. ACM*, 27(4):701–717, Oct. 1980. ISSN 0004-5411. URL <http://doi.acm.org/10.1145/322217.322225>.
- [24] A. Szanto. *Computation with polynomial systems*. PhD thesis, Cornell University, 1999.
- [25] D. M. Wang. Irreducible decomposition of algebraic varieties via characteristic sets and Gröbner bases. *Comput. Aided Geom. Design*, 9(6):471–484, 1992. ISSN 0167-8396. URL [https://doi.org/10.1016/0167-8396\(92\)90045-Q](https://doi.org/10.1016/0167-8396(92)90045-Q).
- [26] D. M. Wang. An elimination method for polynomial systems. *J. Symbolic Comput.*, 16(2):83–114, 1993. ISSN 0747-7171. URL <https://doi.org/10.1006/jsc.1993.1035>.
- [27] W. J. Wu. Basic principles of mechanical theorem proving in elementary geometries. *J. Systems Sci. Math. Sci.*, 4(3):207–235, 1984. ISSN 1000-0577.
- [28] R. Zippel. Probabilistic algorithms for sparse polynomials. In *Proceedings of the International Symposium on Symbolic and Algebraic Computation, EUROSAM '79*, pages 216–226, London, UK, UK, 1979. Springer-Verlag. ISBN 3-540-09519-5. URL <http://dl.acm.org/citation.cfm?id=646670.698972>.