A Modified Van der Waerden Algorithm to Decompose Algebraic Varieties and Zero-dimensional Radical Ideals¹

Jia Li², and Xiao-Shan Gao

Key Laboratory of Mathematics Mechanization

Institute of Systems Science, AMSS, Academia Sinica, Beijing, 100080, China

Abstract. In this paper, we introduce a modified Van der Waerden algorithm to decompose a variety into the union of irreducible varieties. We give an effective representation for irreducible varieties obtained by the algorithm, which allows us to obtain an irredundant decomposition easily. We show that in the zero dimensional case, the polynomial systems for the irreducible varieties obtained in the Van der Waerden algorithm are prime ideals. As a consequence, we have an algorithm to decompose the radical ideal generated by a finite set of polynomials as the intersection of prime ideals and the degree of the polynomials in the computation is bounded by $O(d^n)$ where d is the degree of the input polynomials and n is the number of variables.

Keywords. Algebraic variety, zero dimensional variety, resultant, irredundant decomposition.

1. Introduction

A fundamental construction in commutative algebra is to decompose a radical ideal into the intersection of prime ideals. From a geometric viewpoint, this is equivalent to decomposing an algebraic variety into irreducible varieties. The geometric version is slightly weaker than the algebraic version, since an irreducible variety is not necessarily represented by a prime ideal.

In recent years, there appeared a lot of work on this kind of decomposition algorithms. Algorithms for computing the prime decomposition of radical ideals have been proposed in [9, 10, 12, 13]. All of these algorithms are based on the Gröbner basis and have no complexity analysis. Corresponding to the prime decomposition of radical ideals, algorithms for irreducible decomposition of varieties are developed in [2, 3, 5, 6, 17, 18, 19]. The method in [6] uses Bezontian matrices. It only gives the general point of each irreducible variety, but can not give the generating polynomial

¹)Partially supported by a National Key Basic Research Project of China (2004CB318000).

²)Corresponding author.

systems of these varieties. This method also needs combinatorial selection of parameters. The algorithms developed in [2, 3] use multivariate resultants. They introduce ϵ as a perturbed parameter to obtain a regular system F_ϵ and recover the information about the isolated roots from the trailing coefficient in ϵ of the determinant of the Macaulay matrix associated to the system F_ϵ . Another approach is the characteristic set method [4, 5, 7, 13, 14, 17, 19], which can decompose a variety into the union of irreducible varieties represented by irreducible ascending chains. Generating polynomial systems for the irreducible varieties can also be found via Chow form or Gröbner bases [4, 7, 17, 18]. This approach has a very high worst case complexity. A characteristic set method with single exponential complexity is given in [14]. This method only decomposes the variety as unmixed ones represented by their characteristic sets.

In this paper, we give an algorithm to compute the irredundant irreducible variety decomposition of a given variety defined by the following polynomial equations

$$f_1(x_1, \dots, x_n) = 0, \dots, f_m(x_1, \dots, x_n) = 0. \quad (1)$$

We give a complexity analysis of this algorithm. We prove that our algorithm also gives an irredundant prime ideal decomposition of the radical ideal generated by $f_1, \dots, f_n$ when this ideal is zero-dimensional.

We use an algorithm developed by B. L. Van der Waerden in [15] (abbr, VDW algorithm) to decompose the variety generated by (1) into irreducible varieties. This algorithm computes $2n$ resultants at most, and the degree of the polynomials which occur in the computation in any variable is bounded by d^{4^n} where $d = \max_{i \in \{1, \dots, n\}} \{\deg_{x_i}(f_1), \dots, \deg_{x_i}(f_m)\}$. As a consequence, we obtain an irreducible decomposition for a variety by computing at most $2n$ resultants of polynomials with degrees bounded by d^{4^n} .

We present two major improvements of this algorithm. First, we give an effective representation for the irreducible varieties obtained by the algorithm. Using this representation, we can easily decide the inclusion relationship of two varieties. As a consequence, we may give an irredundant decomposition. Note that the generating polynomial systems given in the VDW algorithm are not prime ideals in the general case and deciding the inclusion relationship of two varieties need compute Gröbner bases without our method. Second, we show that in the zero dimensional case, the VDW algorithm gives prime ideals. Combining the ideas from [2] and the result in this paper, we give an algorithm to decompose the zero-dimensional radical ideal generated by (1) as intersection of prime ideals and the degree of the polynomials in the computation is bounded by $O(d^n)$.

Comparing to the Gröbner basis method, the computation step of the VDW algorithm is very “large” in the sense that each step eliminates one variable in all the polynomials. In the Gröbner basis computation, each step is very “small”, which only eliminates one monomial. The characteristic set method is in between: each step decreases the degree of a polynomial. Also note that to obtain a prime decomposition requires to compute the Gröbner bases for many times. The VDW algorithm is quite similar to the one in [2]. The difference is that the VDW algorithm uses a top-to-down

approach in the sense that it computes the components with higher dimensions first, while the algorithm in [2] computes components with lower dimension first.

2. Preliminaries

Notations and results needed in this paper are summarized in this section.

In what follows the reader is assumed to be familiar with the basic notions about characteristic sets for which we refer to [8, 19].

Let K be a computable field of characteristic zero, e.g., $\mathbf{Q}$. We use $K[x_1, \dots, x_n]$ or $K[x]$ to denote the ring of polynomials in the indeterminates $x_1, \dots, x_n$. Unless explicitly mentioned otherwise, all polynomials in this paper are in $K[x]$. Let E be a *universal extension field* of K , i.e., an algebraic closed extension of K which contains sufficiently many independent indeterminates over K . We will consider zeros of polynomials in the field E .

Let P be a polynomial. The *class* of P , denoted by $\text{cls}(P)$, is the largest p such that some x_p actually occurs in P . If $P \in K$, $\text{cls}(P) = 0$. A sequence of polynomials $\mathcal{A} = A_1, \dots, A_p$ is said to be an *ascending chain* (asc chain), or simply, a *chain*, if either $r = 1$ and $A_1 \neq 0$ or $0 < \text{cls}(A_i) < \text{cls}(A_j)$ for $1 \leq i < j$ and A_k is of higher degree than A_m for $m > k$ in x_{n_k} where $n_k = \text{cls}(A_k)$.

Definition 2.1 *The dimension of an irreducible chain $\mathcal{A} = A_1, \dots, A_p$ is defined to be $\dim(\mathcal{A}) = n - p$ which is the number of parameters of $\mathcal{A}$.*

Definition 2.2 *A characteristic set (abbr. char set) of an ideal I is a chain $\mathcal{A}$ in I such that for all $P \in I$, $\text{prem}(P, \mathcal{A}) = 0$.*

Theorem 2.3 [13, 19] *If $\mathcal{A}$ is an irreducible chain then $\text{sat}(\mathcal{A})$ is a prime ideal with dimension $\dim(\mathcal{A})$, and $\mathcal{A}$ is a char set of $\text{sat}(\mathcal{A})$. Conversely, each char set of a prime ideal is an irreducible chain.*

Lemma 2.4 [19] *Let $\mathcal{A}$ be an irreducible ascending chain with parameters $u_1, \dots, u_q$. If Q is a polynomial not in $\text{sat}(\mathcal{A})$, then we can find a $P \in K[u]$ such that $P \in \text{ideal}(\mathcal{A} \cup \{Q\})$.*

An ideal distinct from (1) and (0) is called nontrivial.

Lemma 2.5 *Let $\mathcal{A}$ be an irreducible chain with parameters $u_1, \dots, u_q$, we can find an irreducible chain $\mathcal{A}'$ such that $\text{sat}(\mathcal{A}) = \text{sat}(\mathcal{A}')$ and the initials of the polynomials in $\mathcal{A}'$ are in $K[u]$.*

Definition 2.6 *Let I be a nontrivial prime ideal in $K[x]$. We can divide the x into two groups, $u_1, \dots, u_q$ and $y_1, \dots, y_p$, $p + q = n$, such that $I \cap K[u_1, \dots, u_q] = \emptyset$, while, for $i = 1, \dots, p$, I contains a nonzero polynomial in y_i and the u alone. We call the u a parameter set of I .*

Lemma 2.7 [8] *Use the notations as above. Let I be a nontrivial prime ideal in $K[x]$. A char set of I under the variable order $u_1 < \dots < u_q < y_1 < \dots < y_p$ is of the form*

$$\mathcal{A} = A_1(u, y_1), A_2(u, y_1, y_2), \dots, A_p(u, y_1, \dots, y_p) \quad (2)$$

where A_i is a polynomial involving y_i effectively. Conversely, for an irreducible chain like (2), the u consists of a parameter set of the prime ideal $\text{sat}(\mathcal{A})$.

Let $f_1, f_2, \dots, f_r$ be r polynomials in a single variable x of given degrees with indeterminate coefficients. The resultant system of the polynomials $f_1, f_2, \dots, f_r$ can be computed in the following way[16].

First, we transform the polynomials $f_1, f_2, \dots, f_r$ into polynomials of the same degree by multiplying every polynomial f_i by x^{n-n_i} and $(x-1)^{n-n_i}$ respectively where n_i is the degree of f_i in x , and n is the greatest of n_i . We designate these new polynomials by $g_1, g_2, \dots, g_s$.

Next, from $g_1, g_2, \dots, g_s$, we form the linear combinations

$$g_u = u_1g_1 + u_2g_2 + \dots + u_sg_s; g_v = v_1g_1 + v_2g_2 + \dots + v_sg_s,$$

where u, v are indeterminates which are adjoined to the field K .

Finally, let $R = \text{resl}(g_u, g_v, x)$ be the resultant of g_u and g_v wrt x . If we arrange R according to the power products of the u and v , and denote the coefficients by $D_1, D_2, \dots, D_h$. Then $D_1, D_2, \dots, D_h$ are the resultant system of $f_1, \dots, f_r$.

Remark 2.8 *If it is known beforehand that the leading coefficient of one of the polynomials f_v , say f_1 , does not vanish, we may omit the entire preliminary operation whereby the polynomials f_v are transformed into polynomials of the same degree. Moreover the calculations may then be simplified by forming the resultant of f_1 and $v_2f_2 + v_3f_3 + \dots + v_rf_r$ rather than that of g_u and g_v .*

3. Outline of the VDW Decomposition Algorithm

In this section, we will introduce the algorithm developed by B.L. van der Waerden [15] without prove. Suppose that we want to decompose the zero set of the following polynomial equations

$$f_1(x_1, x_2, \dots, x_n) = 0, f_2(x_1, x_2, \dots, x_n) = 0, \dots, f_m(x_1, x_2, \dots, x_n) = 0 \quad (3)$$

into irreducible varieties. Denote this variety by $M = \text{Zero}(f_1, f_2, \dots, f_m)$. The polynomial set $\{f_1, f_2, \dots, f_m\}$ is called the *definition system* of M .

To construct this algorithm, we introduce a new variable z as follows

$$z - u_1x_1 - \dots - u_nx_n = 0 \quad (4)$$

where $u_1, \dots, u_n$ are indeterminates.

Now, let us explain the algorithm described in [15] that computes the zero decomposition of (3) by eliminating the variables successively from x_n to x_1 in n steps. In the first step, we rename x_j and u_j in (3),(4) as $x_j^{(0)}$ and $u_j^{(0)}$ respectively, where $i=1, \dots, n$. We give a sketch to describe this algorithm:

VDW Algorithm

$$\begin{array}{ccccccc}
 \mathbb{P}^{(1)} & \longrightarrow & \mathbb{P}^{(2)} & \longrightarrow \dots \longrightarrow & \mathbb{P}^{(i)} & \longrightarrow \dots \longrightarrow & \mathbb{P}^{(n)} \\
 \downarrow & & \downarrow & & \downarrow & & \downarrow \\
 \bar{\mathbb{P}}^{(1)} & & \bar{\mathbb{P}}^{(2)} & & \bar{\mathbb{P}}^{(i)} & & \bar{\mathbb{P}}^{(n)} \\
 \downarrow & & \downarrow & & \downarrow & & \downarrow \\
 g_j^{(1)} & & g_j^{(2)} & & g_j^{(i)} & & g_j^{(n)} \\
 \downarrow & & \downarrow & & \downarrow & & \downarrow \\
 h^{(1)}, l_j^{(1)} & & h^{(2)}, l_j^{(2)} & & h^{(i)}, l_j^{(i)} & & h^{(n)}, l_j^{(n)} \\
 \downarrow \quad \downarrow & & \downarrow \quad \downarrow & & \downarrow \quad \downarrow & & \downarrow \\
 h_{\mu k}^{(1)} \quad e_j^{(1)} & & h_{\mu k}^{(2)} \quad e_j^{(2)} & & h_{\mu k}^{(i)} \quad e_j^{(i)} & & h_{\mu k}^{(n)}
 \end{array}$$

In the above sketch, $\mathbb{P}^{(1)} = \{(3), (4)\}$, and $\mathbb{P}^{(i)} = \{l_j^{(i-1)}, e_j^{(i-1)}\}$, $i = 2, \dots, n$.

Now, let us explain the **i -th step** of above algorithm. To discuss conveniently, we denote $\mathbb{P}^{(i)} = \{f_1^{(i)}, \dots, f_s^{(i)}\}$, where $f_k^{(i)} \in K[u^{(i-1)}, x_1^{(i-1)}, \dots, x_{n-i+1}^{(i-1)}, z]$ and at least one $f_k^{(i)}$ said $f_1^{(i)}$ is in $K[x_1^{(i-1)}, \dots, x_{n-i+1}^{(i-1)}]$.

STEP i.1: To avoid the resultant system vanishing identically, we do a linear transformation:

$$\mathbf{x}^{(i-1)} = M_{i-1} \mathbf{x}^{(i)}, \quad \mathbf{u}^{(i-1)} = N_{i-1} \mathbf{u}^{(i)}$$

where $\mathbf{x}^{(i)} = (x_1^{(i)}, \dots, x_n^{(i)})'$, $\mathbf{u}^{(i)} = (u_1^{(i)}, \dots, u_n^{(i)})'$, and

$$M_{i-1} = \begin{pmatrix} 1 & \cdots & 0 & v_1^{(i-1)} & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 1 & v_{n-i}^{(i-1)} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 1 \end{pmatrix}, \quad N_{i-1} = \begin{pmatrix} 1 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 1 & 0 & 0 & \cdots & 0 \\ -v_1^{(i-1)} & \cdots & -v_{n-i}^{(i-1)} & 1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 1 \end{pmatrix}, \quad (5)$$

and $v_k^{(i-1)}$, $k = 1, \dots, n-i$ are constants in K such that the leading coefficient of $f_1^{(i)}(x_1^{(i)} + v_1^{(i-1)}x_{n-i+1}^{(i)}, \dots, x_{n-i}^{(i)} + v_{n-i}^{(i-1)}x_{n-i+1}^{(i)})$ in $x_{n-i+1}^{(i)}$ is a nonzero constant in K .

After this transformation, z is still a linear form in $x^{(i)}$ and $u^{(i)}$:

$$z = u_1^{(i)}x_1^{(i)} + \dots + u_n^{(i)}x_n^{(i)}.$$

Let $\bar{\mathbb{P}}^{(i)}$ to be the set of new polynomials obtained from $\mathbb{P}^{(i)}$ by doing the above transformation.

STEP i.2: Compute $\{g_j^{(i)}\}$, the resultant system of the polynomials in $\bar{\mathbb{P}}^{(i)}$ wrt $x_{n-i+1}^{(i)}$.

STEP i.3: Compute $h^{(i)}$, the greatest common factor of all $g_j^{(i)}$, which is called the *i-th partial resultant* of (3) and $l_j^{(i)} = g_j^{(i)}/h^{(i)}$. So $l_j^{(i)}$ are co-prime.

STEP i.4: To obtain equations in $x^{(i)}$ only, compute the resultant system of $\{l_j^{(i)}\}$ wrt z , and arrange them according to the power products of the $u^{(i)}$, and denote $\{e_j^{(i)}\}$ to be these coefficients. Since $l_j^{(i)}$ are co-prime, $e_j^{(i)}$ do not vanish identically.

STEP i.5: Factorizing $h^{(i)}$ into irreducible factors in $K[u^{(i)}, x_1^{(i)}, \dots, x_{n-i}^{(i)}, z]$:

$$h^{(i)}(u^{(i)}, x_1^{(i)}, \dots, x_{n-i}^{(i)}, z) = \Theta(u^{(i)}, x_1^{(i)}, \dots, x_{n-i}^{(i)}) \prod_{\mu} h_{\mu}^{(i)}(u^{(i)}, x_1^{(i)}, \dots, x_{n-i}^{(i)}, z)^{\sigma_{\mu}}. \quad (6)$$

Replacing z by $u_1^{(i)}x_1^{(i)} + \dots + u_n^{(i)}x_n^{(i)}$ in $h_{\mu}^{(i)}$, and arranging it according to the power products of the $u^{(i)}$. Denote $\{h_{\mu k}^{(i)}\}$ to be these coefficients.

Definition 3.1 $u_1, \dots, u_s$ are different indeterminates. η is said to be independent with $u_1, \dots, u_s$ if $\eta \in K$ or η and $u_1, \dots, u_s$ are algebraic independent over K . $(\eta_1, \dots, \eta_t)$ is said to be independent with $u_1, \dots, u_s$ if η_i is independent with $u_1, \dots, u_s$ for all i .

After all the x are eliminated. We obtain a sequence of partial resultants

$$h^{(1)}(u^{(1)}, x_1^{(1)}, \dots, x_{n-1}^{(1)}, z) = 0, \dots, h^{(n-1)}(u^{(n-1)}, x_1^{(n-1)}, z) = 0, h^{(n)}(u^{(n)}, z) = 0. \quad (7)$$

Theorem 3.2 [15] Assume (η, ζ) to be a solution of $(3) \cup (4)$. When the η are independent with the u , (η, ζ) is a solution of one of the $h^{(i)} = 0$ in (7).

Theorem 3.3 [15] Assume $\xi_1, \dots, \xi_{n-r}$ to be given (constants or variables). Then every solution of the r -th equation of (7) is of the form

$$\zeta = u_1^{(r)}\xi_1 + \dots + u_n^{(r)}\xi_n \quad (8)$$

where ξ_k are independent with $u_i^{(r)}$ and $\{\xi_k\}$ is a set of solutions of (3).

Now we consider an irreducible factor $h_{\mu}^{(i)}$ of $h^{(i)}$. According to Theorem 3.3, if we set $x_1^{(i)} = \xi_1, \dots, x_{n-i}^{(i)} = \xi_{n-i}$ where $\xi_1, \dots, \xi_{n-i}$ are indeterminates independent with the u , then the zeros of $h^{(i)}(u^{(i)}, x_1^{(i)}, \dots, x_{n-i}^{(i)}, z)$ are of the form referred in (8). So factorizing $h_{\mu}^{(i)}$ into linear factors in certain extensional field of $K(u^{(i)}, \xi)$, we have

$$h_{\mu}^{(i)}(u^{(i)}, x_1^{(i)}, \dots, x_{n-i}^{(i)}, z) = \gamma_{\mu} \prod_{\nu} (z - u_1^{(i)}\xi_1 - \dots - u_n^{(i)}\xi_n^{(\nu)}) \quad (9)$$

where different $\xi^{(\nu)} = \{\xi_1, \dots, \xi_{n-i}, \xi_{n-i+1}^{(\nu)}, \dots, \xi_{n-1}^{(\nu)}, \xi_n^{(\nu)}\}$ are conjugate to each other. Let $\xi_{\mu}^{(i)} = \xi^{(1)}$. Then ξ is a $(n-i)$ -dimensional point in variety M because $\xi_1, \dots, \xi_{n-i}$ are indeterminates and $\xi_{n-i+1}, \dots, \xi_n$ are their algebraic functions.

The set of equations

$$h_{\mu 1}^{(i)}(x^{(i)}) = 0, \dots, h_{\mu m_\mu}^{(i)}(x^{(i)}) = 0. \quad (10)$$

defines a variety $M_\mu^{(i)}$ with the following property.

Theorem 3.4 [15] *Let $M_\mu^{(i)}$ be the variety defined by the irreducible factors of the (i) -th partial resultant of M according to (10). Then $M_\mu^{(i)}$ is an irreducible variety of dimension $n - i$ with $\xi_\mu^{(i)}$ as a generic point. Furthermore, we have*

$$M = \bigcup_{i=1, \dots, n; \mu} M_\mu^i.$$

We give following example to explain this algorithm.

Example 3.5 *Let $M = \text{Zero}(f_1, f_2, f_3)$ where $f_1 = x_1 x_2 x_3 - x_1 x_2^2 - x_3 - x_1 - x_2$, $f_2 = x_1 x_3 - x_1^2 - x_2 - x_3 + x_1$, and $f_3 = x_3^2 - x_1^2 - x_2^2$.*

Let $\mathbb{P}^{(1)} = \{f_1, f_2, f_3, f_4 = z - u_1 x_1 - u_2 x_2 - u_3 x_3\}$. Since the leading coefficient of f_3 in x_2 is not zero, we will eliminate x_2 first. The resultant system of $\mathbb{P}^{(1)}$ wrt x_2 is

$$\begin{aligned} g_1^{(1)} &= -5x_1^3 x_3 + 2x_1^4 x_3 - 2x_1 + x_1^2 + 3x_1^2 x_3 - x_1^5 - x_1^3 + 3x_1^2 x_3^2 - x_1^3 x_3^2 - x_1 x_3 - 2x_1 x_3^2 + 2x_1^4, \\ g_2^{(1)} &= x_1 x_3 u_2 - z + x_1 u_2 + u_1 x_1 - x_1^2 u_2 - x_3 u_2 + u_3 x_3, \\ g_3^{(1)} &= -4x_1^2 x_3 + 2x_1^3 x_3 - 2x_1^2 + 2x_1 x_3 - x_1^4 + 2x_1 x_3^2 + 2x_1^3 - x_1^2 x_3^2; \end{aligned}$$

The GCD of $g_1^{(1)}, g_2^{(1)}, g_3^{(1)}$ is $h^{(1)} = 1$. So $l_1^{(1)} = g_1, l_2^{(1)} = g_2, l_3^{(1)} = g_3$. The resultant system of $l^{(1)}$ w.r.t z is

$$e_1^{(1)} = -4x_1^2 x_3 + 2x_1^3 x_3 - 2x_1^2 + 2x_1 x_3 - x_1^4 + 2x_1 x_3^2 + 2x_1^3 - x_1^2 x_3^2.$$

We obtain $\mathbb{P}^{(2)} = \{l_1^{(1)}, l_2^{(1)}, l_3^{(1)}, e_1^{(1)}\}$. We compute the resultant system $\mathbb{P}^{(2)}$ wrt x_1 and obtain the second partial resultant:

$$h^{(2)} = x_3 u_2 - u_3 x_3 + z.$$

Substituting $z = u_1 x_1 + u_2 x_2 + u_3 x_3$ into $h^{(2)}$, we obtain the coefficients of the power products of the u :

$$h_{21}^{(2)} = x_1, h_{12}^{(2)} = x_3 + x_2.$$

Now we obtain an 1-dimensional irreducible variety $M_1^{(2)} = \text{Zero}(h_{11}^{(2)}, h_{12}^{(2)})$.

Continuing our computation, we obtain the third partial resultant

$$h^{(3)} = 68719476736z(-z + u_2 - u_3)^2(u_1 - z - u_3)^2(3u_1 + 4u_2 - z + 5u_3)$$

which has four irreducible factors:

$$h_1^{(3)} = z, h_2^{(3)} = -z + u_2 - u_3, h_3^{(3)} = u_1 - z - u_3, h_4^{(3)} = 3u_1 + 4u_2 - z + 5u_3.$$

Substituting $z = u_1x_1 + u_2x_2 + u_3x_3$ into the above polynomials, we obtain the coefficients of the power products of the u :

$$\begin{aligned} h_{11}^{(3)} &= x_1, & h_{12}^{(3)} &= x_2, & h_{13}^{(3)} &= x_3; \\ h_{21}^{(3)} &= -x_1, & h_{22}^{(3)} &= -x_2 + 1, & h_{23}^{(3)} &= -x_3 - 1; \\ h_{31}^{(3)} &= 1 - x_1, & h_{32}^{(3)} &= -x_2, & h_{33}^{(3)} &= -x_3 - 1; \\ h_{41}^{(3)} &= 3 - x_1, & h_{42}^{(3)} &= 4 - x_2, & h_{43}^{(3)} &= -x_3 + 5. \end{aligned}$$

We obtain four zero-dimensional irreducible varieties: $M_1^{(3)} = \text{Zero}(h_{11}^{(3)}, h_{12}^{(3)}, h_{13}^{(3)})$, $M_2^{(3)} = \text{Zero}(h_{21}^{(3)}, h_{22}^{(3)}, h_{23}^{(3)})$, $M_3^{(3)} = \text{Zero}(h_{31}^{(3)}, h_{32}^{(3)}, h_{33}^{(3)})$, and $M_4^{(3)} = \text{Zero}(h_{41}^{(3)}, h_{42}^{(3)}, h_{43}^{(3)})$. The final decomposition is:

$$M = M_1^{(2)} \cup M_1^{(3)} \cup M_2^{(3)} \cup M_3^{(3)} \cup M_4^{(3)}.$$

In the following result, we give an estimation for the degrees of the polynomials in the computation procedure.

Theorem 3.6 *Let (3) define a variety M , and $d = \max_{i \in \{1, \dots, n\}} \{\deg_{x_i}(f_1), \dots, \deg_{x_i}(f_m)\}$. Then, in the VDW Algorithm, the maximal degree in any x_i of any polynomial occurring in the computation is bounded by d^{4^n} .*

Proof: The only computation in the algorithm increasing the degree is the computation of the resultant. After computing a resultant wrt x_n , the maximal degree of $g_j^{(1)}$ in any variable is bounded by d^2 . So the degree bound of h and l_j is also d^2 . Similarly, the maximal degree of $e_i^{(1)}$ is d^4 . Then the degree bound for $\mathbb{P}^{(1)}$ is d^4 . Repeat the operation, the degree bound for $\mathbb{P}^{(2)}$ is $(d^4)^2 = d^8$. Finally, the degree bound of $\mathbb{P}^{(n-1)}$ is d^{4^n} . $\square$

As a consequence, we may obtain an irreducible decomposition for a variety by computing $2n$ resultants of polynomials with degrees bounded by d^{4^n} .

In the following sections, we will discuss the applications and improvements of this algorithm.

4. Irredundant Decomposition

In Sect. 3, we know that the VDW algorithm can be used to decompose a variety into the union of irreducible varieties. In general, this decomposition is redundant. In this section, we will show how to obtain an irredundant decomposition. In order to do that, we need to remove those varieties $M_\mu^{(i)}$ which are contained in varieties $M_\eta^{(k)}$ with higher dimensions. As suggested in [15], since we know the basis of $M_\mu^{(i)}$, the irredundant decomposition can be reached in principle with the methods such as the characteristic set method [19] or the Groebner basis method [1]. But to use these general methods needs extra work. We will give a direct method to find an irredundant decomposition.

Let $h_\mu^{(i)}(u^{(i)}, x_1^{(i)}, \dots, x_{n-i}^{(i)}, z) \in K[u^{(i)}, x_1^{(i)}, \dots, x_{n-i}^{(i)}, z]$ be an irreducible factor of the i -th partial resultant from (6). Introduce the following notations.

$$\begin{aligned}\mathbb{H}_\mu^{(i)} &= \{h_{\mu 1}^{(i)}, \dots, h_{\mu m_\mu}^{(i)}\} \\ \mathbb{D}_\mu^{(i)} &= (h_{\mu 1}^{(i)}, \dots, h_{\mu m_\mu}^{(i)}) \\ M_\mu^{(i)} &= V(h_{\mu 1}^{(i)}, \dots, h_{\mu m_\mu}^{(i)}) \\ \mathbb{K}_\mu^{(i)} &= (h_{\mu 1}^{(i)}, \dots, h_{\mu m_\mu}^{(i)}, z - (u_1^{(i)}x_1^{(i)} + \dots + u_n^{(i)}x_n^{(i)})) \\ \mathbb{J}_\mu^{(i)} &= \sqrt{\mathbb{D}_\mu^{(i)}} \\ \mathbb{I}_\mu^{(i)} &= (\mathbb{J}_\mu^{(i)}, z - (u_1^{(i)}x_1^{(i)} + \dots + u_n^{(i)}x_n^{(i)}))\end{aligned}\tag{11}$$

where the $h_{\mu j}^{(i)}$ are from (10). By Theorem 3.4, we know that $\mathbb{J}_\mu^{(i)}$ and hence $\mathbb{I}_\mu^{(i)}$ are prime ideals.

In the following discussion, to simplify the expressions, we still use x, u to denote $x^{(i)}, u^{(i)}$ when we do not need to distinguish $x^{(i)}, u^{(i)}$ and $x^{(j)}, u^{(j)}$.

Lemma 4.1 *Use the notations in (11). Under the variable order $u < x_1 < \dots < x_{n-i} < z < x_{n-i+1} < \dots < x_n$, the ideal $\mathbb{I}_\mu^{(i)}$ has a char set of the form*

$$\begin{aligned}R_{\mu 0}^{(i)} &= h_\mu^{(i)}(u, x_1, \dots, x_{n-i}, z) \\ R_{\mu 1}^{(i)} &= I_{\mu 1}^{(i)}(u, x_1, \dots, x_{n-i}, z)x_{n-i+1} + U_{\mu 1}^{(i)}(u, x_1, \dots, x_{n-i}, z) \\ &\dots \\ R_{\mu i}^{(i)} &= I_{\mu i}^{(i)}(u, x_1, \dots, x_{n-i}, z)x_n + U_{\mu i}^{(i)}(u, x_1, \dots, x_{n-i}, z)\end{aligned}\tag{12}$$

Proof: We know that $\mathbb{J}_\mu^{(i)}$ is a prime ideal whose parameter set is $u, x_1, \dots, x_{n-i}, z - (u_1x_1 + \dots + u_nx_n)$ is a polynomial linear in z , so $\mathbb{I}_\mu^{(i)}$ is also a prime ideal whose parameter set is $u, x_1, \dots, x_{n-i}$. According to Lemma 2.7, $\mathbb{I}_\mu^{(i)}$ has a char set $\mathcal{A}$ of the form

$$\begin{aligned}R_{\mu 0}^{(i)}(u, x_1, \dots, x_{n-i}, z), \\ R_{\mu 1}^{(i)}(u, x_1, \dots, x_{n-i}, z, x_{n-i+1}), \\ \dots, \\ R_{\mu i}^{(i)}(u, x_1, \dots, x_{n-i}, z, x_{n-i+1}, \dots, x_n).\end{aligned}$$

where $R_{\mu 0}^{(i)}$ contains z and $R_{\mu j}^{(i)}$ contains x_{n-i+j} effectively. Furthermore, $\mathbb{I}_\mu^{(i)} = \text{sat}(\mathcal{A})$. Note that $R_{\mu 0}^{(i)}$ is an irreducible polynomial in $u, x_1, \dots, x_{n-i}, z$ and $h_\mu^{(i)} \in \mathbb{I}_\mu^{(i)}$, so we can assume $R_{\mu 0}^{(i)} = h_\mu^{(i)}(u, x_1, \dots, x_{n-i}, z)$.

Let $\alpha_1, \dots, \alpha_n, \tau_1, \dots, \tau_{n-i}, \beta, \tau_{n-i+1}, \dots, \tau_n$ be a generic zero of $\mathbb{I}_\mu^{(i)}$. So $h_\mu^{(i)}(u, x_1, \dots, x_{n-i}, z)$ vanishes at this generic zero, and hence $\beta = \alpha_1\tau_1 + \dots + \alpha_n\tau_n$. Furthermore,

$$\begin{aligned}\frac{dh_\mu^{(i)}}{d\alpha_j}(\alpha, \tau_1, \dots, \tau_{n-j}, \beta) &= \frac{\partial h_\mu^{(i)}}{\partial u_j}(u, x_1, \dots, x_{n-i}, z) \\ + x_j \frac{\partial h_\mu^{(i)}}{\partial z}(u, x_1, \dots, x_{n-i}, z)|_{(u, x, z)(\alpha, \tau, \beta)} &= 0, j = n - i + 1, \dots, n.\end{aligned}$$

That is $B_{j-n+i} = \frac{\partial h_\mu^{(i)}}{\partial u_j}(u, x_1, \dots, x_{n-i}, z) + x_j \frac{\partial h_\mu^{(i)}}{\partial z}(u, x_1, \dots, x_{n-i}, z)$ vanishes at the generic zero of $I_\mu^{(i)}$, $j = n - i + 1, \dots, n$. So $B_k, k = 1, \dots, i$ are in $I_\mu^{(i)}$ and they are linear in x_{n-i+k} . Also note that $\frac{\partial h_\mu^{(i)}}{\partial z}(u, x_1, \dots, x_{n-i}, z)|_{(u,x,z)=(\alpha,\tau,\beta)} \neq 0$. From the definition of irreducible chain, we can choose $R_{\mu k}^{(i)} = \text{prem}(B_k, h_\mu^{(i)})$ as $R_{\mu k}^{(i)}$. $\square$

From the above lemma, we know that $\alpha_1, \dots, \alpha_n, \tau_1, \dots, \tau_{n-i}, \beta, \tau_{n-i+1}, \dots, \tau_n$ given above is a generic zero of ideal $I_\mu^{(i)}$. So $\tau_1, \dots, \tau_n$ is a generic zero of prime ideal $\mathbb{J}_\mu^{(i)}$ and a generic point of the corresponding irreducible variety $M_\mu^{(i)}$ of $\mathbb{J}_\mu^{(i)}$.

From Lemma 4.1, we obtain the following *effective representation* for the prime ideal $\mathbb{J}_\mu^{(i)}$:

$$\mathbb{H}_\mu^{(i)} = \{h_{\mu 1}^{(i)}, \dots, h_{\mu m_\mu}^{(i)}\} \text{ and } \mathcal{A}_\mu^{(i)} = R_{\mu 0}^{(i)}, R_{\mu 1}^{(i)}, \dots, R_{\mu i}^{(i)} \quad (13)$$

where $R_{\mu j}^{(i)}$ is from (12). This representation is called effective due to the following reasons.

Lemma 4.2 *A polynomial $g \in K[x]$ is in $\mathbb{J}_\mu^{(i)}$ if and only if $\text{prem}(g, \mathcal{A}_\mu^{(i)}) = 0$.*

Proof: We need only to prove $\mathbb{J}_\mu^{(i)} = I_\mu^{(i)} \cap K[x]$. Obviously, $\mathbb{J}_\mu^{(i)} \subseteq I_\mu^{(i)} \cap K[x]$. On the other hand, assume $P \in I_\mu^{(i)} \cap K[x]$. So $P(x^{(i)}) \in \sqrt{(\mathbb{D}_\mu^{(i)}, z - \sum_{i=1}^n u_i^{(i)} x_i^{(i)})}$. Then there exists an integer $r > 0$ and polynomials $A_j \in K[u^{(i)}, x^{(i)}, z], j = 0, \dots, n$ such that $P(x^{(i)})^r = \sum_{j=1}^n A_j h_{\mu j}^{(i)} + A_0(z - \sum_{i=1}^n u_i^{(i)} x_i^{(i)})$. Substituting $z = \sum_{i=1}^n u_i^{(i)} x_i^{(i)}$ into this equation, we obtain $P(x)^r = \sum_{j=1}^n \hat{A}_j h_{\mu j}^{(i)}$. That is, $P \in \sqrt{\mathbb{D}_\mu^{(i)}} = \mathbb{J}_\mu^{(i)}$. So $I_\mu^{(i)} \cap K[x] \subseteq \mathbb{J}_\mu^{(i)}$. We prove the lemma. $\square$

As a consequence, we have the following result.

Theorem 4.3 *For $i > k$, $M_\mu^{(i)} \subset M_\eta^{(k)}$ if and only if $\text{prem}(\tilde{h}_{\eta j}^{(k)}(x_1^{(i)}, \dots, x_n^{(i)}), \mathcal{A}_\mu^{(i)}) = 0$ for $j = 1, \dots, m_\eta$, where $\mathcal{A}_\mu^{(i)}$ is defined in (13) and $\tilde{h}_{\eta j}^{(k)}(x_1^{(i)}, \dots, x_n^{(i)})$ is obtained by substituting $\mathbf{x}^{(k)} = M_k \cdots M_{i-1} \mathbf{x}^{(i)}$ into $h_{\eta j}^{(k)}$. As a consequence, we give an irredundant decomposition of variety M with the VDW algorithm.*

Proof: When we consider the including relationship between two varieties, we need to present them in the same coordinate. Note that

$$\mathbf{x}^{(k)} = M_k \cdots M_{i-1} \mathbf{x}^{(i)}$$

is the linear transformation between $x^{(i)}$ and $x^{(k)}$.

If $\text{prem}(\tilde{h}_{\eta j}^{(k)}(x_1^{(i)}, \dots, x_n^{(i)}), \mathcal{A}_\mu^{(i)}) = 0$ for $j = 1, \dots, m_\eta$. According to Lemma 4.2, $\tilde{h}_{\eta j}^{(k)} \in \mathbb{J}_\mu^{(i)}$. So $\mathbb{D}_\eta^{(k)} \subset \mathbb{J}_\mu^{(i)}$. According to the Nullstellensatz Theorem, $M_\mu^{(i)} \subset M_\eta^{(k)}$.

On the other hand, if $M_\mu^{(i)} \subset M_\eta^{(k)}$, then $\mathbb{J}_\eta^{(k)} \subset \mathbb{J}_\mu^{(i)}$. So $\mathbb{D}_\eta^{(k)} \subset \mathbb{J}_\eta^{(k)} \subset \mathbb{J}_\mu^{(i)}$. According to Lemma 4.2, $\text{prem}(\tilde{h}_{\eta j}^{(k)}(x_1^{(i)}, \dots, x_n^{(i)}), \mathcal{A}_\mu^{(i)}) = 0$. $\square$

From the above theorem, we have a new and more efficient method to decide the including relationship of irreducible components.

Example 4.4 *Continue Example 1. Compute the irredundant irreducible decomposition of variety $M = \text{Zero}(f_1, f_2, f_3)$.*

We have computed the irreducible decomposition of the variety in Example 3.5. We need only remove those irreducible varieties which are included in some higher dimensional varieties.

For $M_1^{(3)}$, the ascending chain corresponding to it is $\mathcal{A}_1^{(3)} = \{z, x_3, x_1, x_2\}$. $\text{prem}(h_{11}^{(2)}, \mathcal{A}_1^{(3)}) = 0$ and $\text{prem}(h_{12}^{(2)}, \mathcal{A}_1^{(3)}) = 0$. So according to Lemma 4.2 and Theorem 4.3, we know $M_1^{(3)} \subset M_1^{(2)}$.

Similarly, we can decide $M_2^{(3)} \subset M_1^{(2)}$, $M_3^{(3)} \not\subset M_1^{(2)}$ and $M_4^{(3)} \not\subset M_1^{(2)}$.

We obtain the following irredundant irreducible decomposition of M :

$$M = M_1^{(2)} \cup M_3^{(3)} \cup M_4^{(3)}.$$

5. Decomposing Zero-dimensional Radical Ideals

In this section, we will show that if the given polynomial system is zero-dimensional, then we can decompose the radical ideal generated by them as the intersection of prime ideals with the VDW Algorithm. We also give a modified algorithm using Macaulay resultant to decompose the zero-dimensional radical ideals.

5.1. Decomposing Zero-Dimensional Radical Ideals Using VDW Algorithm

Lemma 5.1 *Use the notations defined in (11) and (13). Then $\mathcal{A}_\mu^{(i)}$ is a char set of $\mathbb{K}_\mu^{(i)}$.*

Proof: Let $p = z - (u_1x_1 + \dots + u_nx_n)$. Then $h_\mu^{(i)}(u, x_1, \dots, x_{n-i}, z) = h_\mu^{(i)}(u, x_1, \dots, x_{n-i}, p + u_1x_1 + \dots + u_nx_n) = \bar{h}_\mu^{(i)}(u, x, p)p + h_\mu^{(i)}(u, x_1, \dots, x_{n-i}, u_1x_1 + \dots + u_nx_n)$, where $\bar{h}_\mu^{(i)}(u, x, p)$ is a polynomial in u, x, p . Since $p, h_\mu^{(i)}(u, x_1, \dots, x_{n-i}, u_1x_1 + \dots + u_nx_n) \in \mathbb{K}_\mu^{(i)}$, $h_\mu^{(i)}(u, x_1, \dots, x_{n-i}, z)$ is in $\mathbb{K}_\mu^{(i)}$. Use the same method, we have

$$\begin{aligned} & B_k(u, x_1, \dots, x_{n-i}, z, x_{k+n-i}) \\ &= \frac{dh_\mu^{(i)}}{du_{n-i+k}}(u, x_1, \dots, x_{n-i}, z) \\ &= \frac{dh_\mu^{(i)}}{du_{n-i+k}}(u, x_1, \dots, x_{n-i}, p + u_1x_1 + \dots + u_nx_n) \\ &= B'_k p + \frac{dh_\mu^{(i)}}{du_{n-i+k}}(u, x_1, \dots, x_{n-i}, u_1x_1 + \dots + u_nx_n). \end{aligned}$$

Let $h_\mu^{(i)}(u, x_1, \dots, x_{n-i}, u_1x_1 + \dots + u_nx_n) = \sum_{j=1}^s h_{\mu_j}^{(i)} u_1^{r_{j,1}} \dots u_n^{r_{j,n}}$. Then

$$\begin{aligned} & \frac{dh_\mu^{(i)}}{du_{n-i+k}}(u, x_1, \dots, x_{n-i}, u_1x_1 + \dots + u_nx_n) \\ &= \sum_{j=1}^s r_{j,n-i+k} h_{\mu_j}^{(i)} u_1^{r_{j,1}} \dots u_{n-i+k}^{r_{j,n-i+k}-1} \dots u_n^{r_{j,n}} \in \mathbb{K}_\mu^{(i)}. \end{aligned}$$

So $R_{\mu k}^{(i)} = \text{prem}(B_k, h_{\mu}^{(i)}) \in \mathbb{K}_{\mu}^{(i)}$. Hence $\mathcal{A}_{\mu}^{(i)} \subset \mathbb{K}_{\mu}^{(i)}$. $\mathbb{K}_{\mu}^{(i)} \subset \mathbb{I}_{\mu}^{(i)}$, so $\forall g \in \mathbb{K}_{\mu}^{(i)}$, we have $\text{prem}(g, \mathcal{A}_{\mu}^{(i)}) = 0$. According to the definition of char sets, $\mathcal{A}_{\mu}^{(i)}$ is a char set of $\mathbb{K}_{\mu}^{(i)}$. $\square$

Theorem 5.2 *Use the notations introduced above. If the ideal $\mathbb{D}_{\mu}^{(i)}$ is zero-dimensional, that is, $i = n$, then $\mathbb{D}_{\mu}^{(n)}$ is prime.*

Proof: We need only to prove $\mathbb{D}_{\mu}^{(n)} = \mathbb{J}_{\mu}^{(n)} = \sqrt{\mathbb{D}_{\mu}^{(n)}}$. It is clear that $\mathbb{D}_{\mu}^{(n)} \subset \mathbb{J}_{\mu}^{(n)}$. On the other hand, we need to prove $\mathbb{J}_{\mu}^{(n)} \subset \mathbb{D}_{\mu}^{(n)}$. $\mathcal{A}_{\mu}^{(n)}$ is a char set of $\mathbb{J}_{\mu}^{(n)}$ by Lemma 5.1. According to the proof of Lemma 2.5, we can get a new char set $\tilde{\mathcal{A}}_{\mu}^{(n)} = \{\tilde{R}_{\mu 0}^{(n)}, \tilde{R}_{\mu 1}^{(n)}, \dots, \tilde{R}_{\mu n}^{(n)}\}$ of $\mathbb{J}_{\mu}^{(n)}$ where

$$\tilde{R}_{\mu 0}^{(n)} = R_{\mu 0}^{(n)}, \tilde{R}_{\mu i}^{(n)} = Q_i R_{\mu i}^{(n)} + \left(\sum_{k=0}^{i-1} Q_k R_{\mu k}^{(n)} x_i \right) (k = 1, \dots, n) \quad (14)$$

and the initials of $\tilde{R}_{\mu i}^{(n)}$ are in $K[u]$.

If $g(x) \in \mathbb{J}_{\mu}^{(n)} \subset \mathbb{I}_{\mu}^{(n)}$, by Lemma 5.1, there exist Q , a product of the powers of the initials of polynomials in $\tilde{\mathcal{A}}_{\mu}^{(n)}$, and a chain $C_0, C_1, \dots, C_n \in K[u, x, z]$ such that

$$Q(u)g(x) = \sum_{j=0}^n C_j \tilde{R}_{\mu j}^{(n)}.$$

Substituting (14) into the above equation and arranging the right hand polynomial according to $R_{\mu i}^{(n)}$, we get

$$Q(u)g(x) = C'_0 R_{\mu 0}^{(n)} + \sum_{j=1}^n C'_j R_{\mu j}^{(n)},$$

where $C'_i \in K[u, x, z]$. We have $R_{\mu j}^{(n)} = \text{prem}(B_j, R_{\mu 0}^{(n)})$, where B_j are defined in the proof of Lemma 4.1. So there exist $Q_j(u) \in K[u]$, a power of the initial of $R_{\mu 0}^{(n)}$ and $P_j \in K[u, x, z]$ such that

$$R_{\mu j}^{(n)} = Q_j B_j - P_j R_{\mu 0}^{(n)} (j = 1, \dots, n).$$

So the above equation becomes

$$Q(u)g(x) = C''_0 R_{\mu 0}^{(n)} + \sum_{j=1}^n C''_j B_j$$

where $C''_i \in K[u, x, z]$. Replacing z with $u_1 x_1 + \dots + u_n x_n$ in the above equation, we have

$$\begin{aligned} Q(u)g(x) &= C''_0(u, x) \sum_{j=1}^s h_{\mu j}^{(n)} u_1^{r_{j,1}} \dots u_n^{r_{j,n}} \\ &+ \sum_{i=1}^n (C''_i(u, x) \sum_{j=1}^s r_{j,n-i+k} h_{\mu j}^{(n)} u_1^{r_{j,1}} \dots u_{n-i+k}^{r_{j,n-i+k}-1} \dots u_n^{r_{j,n}}). \end{aligned}$$

Substitute $u = u_0 \in K$, we have

$$g(x) = \sum_{j=1}^s h_{\mu j}^{(n)}(x) T_j(x) \in \mathbb{D}_{\mu}^{(n)}.$$

□

As a consequence of Theorem 5.2, we have that if the ideal I generated by (3) is zero-dimensional, the VDW Algorithm gives a prime decomposition of the radical ideal $\sqrt{I}$. We write this result as a corollary.

Corollary 5.3 *Let (3) define a zero-dimensional ideal I and $\mathbb{D}_{\mu}^{(n)} = (h_{\mu 1}^{(n)}(x), \dots, h_{\mu m_{\mu}}^{(n)}(x))$ where $h_{\mu 1}^{(n)}$ are from (10). Then, $\sqrt{I} = \cap_{\mu} \mathbb{D}_{\mu}^{(n)}$ decomposes the radical ideal $\sqrt{I}$ as an intersection of prime ideals.*

Corollary 5.4 *Let $\mathbb{H}_{\mu}^{(i)}$ be defined in (11). Then the ideal generated by $\mathbb{H}_{\mu}^{(i)}$ in the ring $K(x_1, \dots, x_{n-i})[x_{n-i+1}, \dots, x_n]$ is prime.*

Proof: Let $\tilde{\mathbb{D}}_{\mu}^{(i)}$ be the ideal generated by $\mathbb{H}_{\mu}^{(i)}$ in the ring $K(x_1, \dots, x_{n-i})[x_{n-i+1}, \dots, x_n]$. Obviously $\tilde{\mathbb{D}}_{\mu}^{(i)}$ is a zero-dimensional ideal in $K(x_1, \dots, x_{n-i})[x_{n-i+1}, \dots, x_n]$. Then the result is a consequence of Theorem 5.2 □

Unfortunately, Theorem 5.2 is false when ideal $\mathbb{D}_{\mu}^{(i)}$ is not zero-dimensional as shown by the following example.

Example 5.5 $f_1 = x_1 + x_2 + x_3, f_2 = x_1^2 + x_2^2 + x_1 x_2$.

Using the algorithm given in Sect. 3, we obtain the following polynomials:

$$\mathbb{P}^{(1)} = \{f_1, f_2, f_3 = z - u_1 x_1 - u_2 x_2\},$$

$$g_1^{(1)} = -x_2 x_1 - x_1^2 - x_2^2, g_2^{(1)} = -z + u_1 x_1 + u_2 x_2 - u_3 x_1 - u_3 x_2,$$

$$h^{(1)} = 1,$$

$$l_1^{(1)} = -x_2 x_1 - x_1^2 - x_2^2, l_2^{(1)} = -z + u_1 x_1 + u_2 x_2 - u_3 x_1 - u_3 x_2,$$

$$e_1^{(1)} = -x_2 x_1 - x_1^2 - x_2^2;$$

$$\mathbb{P}^{(2)} = \{l_1, l_2, e_1\},$$

$$g_1^{(2)} = -z^2 + 2z u_1 x_1 - z u_3 x_1 - u_1^2 x_1^2 + u_1 x_1^2 u_3 - x_1 u_2 z + x_1^2 u_2 u_1 + x_1^2 u_2 u_3 - x_1^2 u_2^2 - x_1^2 u_3^2,$$

$$h^{(2)} = -z^2 + 2z u_1 x_1 - z u_3 x_1 - u_1^2 x_1^2 + u_1 x_1^2 u_3 - x_1 u_2 z + x_1^2 u_2 u_1 + x_1^2 u_2 u_3 - x_1^2 u_2^2 - x_1^2 u_3^2,$$

$$h_{11}^{(2)} = -x_2 x_1 - x_1^2 - x_2^2, h_{12}^{(2)} = -x_1 x_3 - x_2 x_1 - 2x_2 x_3 + x_1^2, h_{13}^{(2)} = -x_3^2 - x_1 x_3 - x_1^2.$$

Let $\mathbb{D}_1^{(2)} = (h_{11}^{(2)}, h_{12}^{(2)}, h_{13}^{(2)})$. Although $\sqrt{\mathbb{D}_1^{(2)}} = \sqrt{(h_{11}^{(2)}, h_{12}^{(2)}, h_{13}^{(2)})}$ is prime, $\mathbb{D}_1^{(2)}$ itself is not a prime ideal. Compute the primary decomposition of $\mathbb{D}_1^{(2)}$, we have

$$\mathbb{D}_1^{(2)} = (x_1 + x_2 + x_3, x_1^2 + x_2^2 + x_1 x_2) \cap (2x_2 x_3 + x_1 x_3 + x_2 x_1, x_1^2, x_2^2 + x_2 x_1, x_3^2 + x_1 x_3).$$

5.2. Decomposing Zero-Dimensional Radical Ideals Using Macaulay Resultant

Denote

$$F = \{f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)\}. \quad (15)$$

In this subsection we always assume that the ideal generated by the polynomials in F is zero-dimensional. We have $m \geq n$. We first consider the case $m = n$.

Denote

$$F^h = \{f_1^h(x_0, x_1, \dots, x_n), \dots, f_n^h(x_0, x_1, \dots, x_n), f_{n+1}^h(x_0, x_1, \dots, x_n, z)\},$$

where f_i^h are the polynomials obtained from f_i (denote $f_{n+1} = z - \sum_{i=1}^n u_i x_i$) by homogenizing them with x_0 .

Lemma 5.6 *Using the notations given above. Assume $V(F^h)$ is still a zero-dimensional variety in the projective space, that is the polynomial system F^h has a finite number of solutions in which $x_0 = 0$. Then we can compute a nonzero polynomial $R(z) \in K[u, z]$ such that all the solutions of F^h vanish this polynomial and any z_0 such that $R(z_0) = 0$ can be extended to a solution of F^h . Proof:* Using the method in [11], we can compute the Macaulay resultant of the polynomial system F w.r.t $x_1, \dots, x_n$. Denote it to be $R(z)$. According to the assumption that both $V(F)$ and $V(F^h)$ are zero-dimensional varieties, we know that $R(z)$ does not vanish identically. From the properties of resultant, we get the conclusions of this lemma. $\square$

If $\langle F \rangle$ is a zero-dimensional radical ideal then $R(z)$ has the same properties as the n -th partial resultant of (3). So we can compute the prime decomposition of $\langle F \rangle$ from $R(z)$ according to method in Sect. 3.

When $m > n$, denote

$$f'_i = \sum_{j=1}^m c_{ij} f_j, \quad i = 1, \dots, n,$$

where c_{ij} are random chosen integers. Denote $F' = \{f'_1(x_1, \dots, x_n), \dots, f'_n(x_1, \dots, x_n)\}$.

Lemma 5.7 *Using the notations given above, we have*

$$\langle f_1, \dots, f_m \rangle = \langle f'_1, \dots, f'_n \rangle$$

with probability almost 1. As a consequence, $V(F) = V(F')$.

Proof: $\langle f'_1, \dots, f'_n \rangle \subseteq \langle f_1, \dots, f_m \rangle$ is obviously valid. Conversely, we prove that $\langle f_1, \dots, f_m \rangle \subseteq \langle f'_1, \dots, f'_n \rangle$ is correct unless c_{ij} are selected to be zeros of a nonzero linear system. $\langle f_1, \dots, f_m \rangle$ is a zero-dimensional ideal, so it has a Gröbner basis containing n elements. We denote this Gröbner basis to be $G = \{g_1, \dots, g_n\}$. There exists a unique set of integers $\{b_{jk}\}$ such that

$$f_j = \sum_{k=1}^n b_{jk} g_k, \quad j = 1, \dots, n.$$

Then

$$f'_i = \sum_{j=1}^m \sum_{k=1}^n c_{ij} b_{jk} g_k.$$

Denote B to be an $m \times n$ matrix whose element in i -th row and j -th column is b_{ij} and C to be an $n \times m$ matrix whose element in j -th row and k -th column are c_{jk} . According to the theory of linear equation systems, if $\det(CB) \neq 0$ then all g_k can be uniquely represented by the linear combinations of $f'_1, \dots, f'_n$. That is unless $\{c_{ij}\}$ is zeros of $\det(CB) = 0$, $\langle g_1, \dots, g_n \rangle \subseteq \langle f'_1, \dots, f'_n \rangle$. Now we prove this lemma. $\square$

If $m > n$, we can use F' to compute the Macaulay resultant $R(z)$ and to decompose ideal into the intersection of prime ideas.

Lemma 5.8 *Using notations given above, let $f_1(x_1, x_2, \dots, x_n), f_2(x_1, x_2, \dots, x_n), \dots, f_m(x_1, x_2, \dots, x_n)$ define a zero-dimensional variety in the affine space and $f'_1(x_0, x_1, x_2, \dots, x_n), f'_2(x_0, x_1, x_2, \dots, x_n), \dots, f'_m(x_0, x_1, x_2, \dots, x_n)$ define a zero-dimensional variety in the projective space, and $d = \max\{\deg(f_1), \dots, \deg(f_m)\}$ where $\deg(f_i)$ is the total degree of f_i in variables $x_1, \dots, x_n$. Then, using Macaulay resultant, the maximal total degree in $x_1, \dots, x_n$ of polynomials occurring in the computation is bounded by d , and the degree of resultant $R(z)$ is bounded by d^n .*

Proof: These conclusions are consequences of properties of the Macaulay resultant [11]. $\square$

Obviously, when the ideal is a zero-dimensional radical ideal, it is more efficient to use Macaulay resultant than using the VDW algorithm.

We summarize the results in this section as the following result.

Theorem 5.9 *For a zero dimensional polynomial equation system like (15), we can decompose $\langle F \rangle$ as the irredundant intersection of prime ideals with probability one. Also the polynomials occurring in the computation is bounded in degree by $O(d^n)$.*

Example 5.10 $f_1 = x_1^2 + x_2^2 + x_3^2 - 4, f_2 = x_1^2 + x_2^2 - x_3^2 - 2, f_3 = (x_1 + x_2 + x_3 - 1)(x_1 + x_2 - x_3 + 2)$.

The ideal I defined by f_1, f_2, f_3 is a zero-dimensional radical ideal. So we can compute the prime decomposition of this ideal using Macaulay resultant.

First introducing the new polynomial:

$$f_0 = z - u_1x_1 - u_2x_2 - u_3x_3.$$

Then homogenizing f_0, f_1, f_2, f_3 with x_0 and computing the Macaulay resultant of the new polynomial system with respect to the variables x_0, x_1, x_2, x_3 :

$$\begin{aligned} h = & 16384(3u_1^2 + 3u_1z + z^2 + 3u_1u_2 + 3u_2^2 + 3u_2z + 3u_3u_1 + 2u_3z + 3u_2u_3 + u_3^2) \\ & (-3u_1^2 + 2z^2 + 6u_1u_2 - 3u_2^2 - 4u_3z + 2u_3^2) \\ & (-u_1^2 + u_1z + z^2 + 3u_1u_2 + u_2z - u_2^2 - u_3u_1 - 2u_3z - u_2u_3 + u_3^2) \\ & (u_1^2 - 4u_1z + 2z^2 + 6u_1u_2 - 4u_2z + u_2^2 - 4u_3u_1 + 4u_3z - 4u_2u_3 + 2u_3^2). \end{aligned}$$

The resultant h has four irreducible factors containing z , we know that I has four prime components and they can be computed from

$$\begin{aligned} h_1 &= 3u_1^2 + 3u_1z + z^2 + 3u_1u_2 + 3u_2^2 + 3u_2z + 3u_3u_1 + 2u_3z + 3u_2u_3 + u_3^2, \\ h_2 &= -3u_1^2 + 2z^2 + 6u_1u_2 - 3u_2^2 - 4u_3z + 2u_3^2, \\ h_3 &= -u_1^2 + u_1z + z^2 + 3u_1u_2 + u_2z - u_2^2 - u_3u_1 - 2u_3z - u_2u_3 + u_3^2, \\ h_4 &= u_1^2 - 4u_1z + 2z^2 + 6u_1u_2 - 4u_2z + u_2^2 - 4u_3u_1 + 4u_3z - 4u_2u_3 + 2u_3^2. \end{aligned}$$

Substituting $z = u_1x_1 + u_2x_2 + u_3x_3$ into above polynomials and arranging them according to the power products of the u , we get four zero-dimensional prime ideals:

$$\begin{aligned} I_1 &= \langle h_{11}, h_{12}, h_{13}, h_{14}, h_{15}, h_{16} \rangle, & I_2 &= \langle h_{21}, h_{22}, h_{23}, h_{24}, h_{25}, h_{26} \rangle, \\ I_3 &= \langle h_{31}, h_{32}, h_{33}, h_{34}, h_{35}, h_{36} \rangle, & I_4 &= \langle h_{41}, h_{42}, h_{43}, h_{44}, h_{45}, h_{46} \rangle. \end{aligned}$$

where

$$\begin{aligned} h_{11} &= 2x_1 + 3 + 3x_3 + 2x_1x_3, & h_{12} &= 2x_1x_2 + 3x_1 + 3x_2 + 3, & h_{13} &= 3x_1 + 3 + x_1^2, \\ h_{14} &= 2x_2 + 3 + 3x_3 + 2x_2x_3, & h_{15} &= 3x_2 + x_2^2 + 3, & h_{16} &= x_3^2 + 2x_3 + 1; \\ h_{21} &= -4x_1 + 4x_1x_3, & h_{22} &= 4x_1x_2 + 6, & h_{23} &= -3 + 2x_1^2, \\ h_{24} &= -4x_2 + 4x_2x_3, & h_{25} &= 2x_2^2 - 3, & h_{26} &= 2x_3^2 - 4x_3 + 2; \\ h_{31} &= -2x_1 - 1 + x_3 + 2x_1x_3, & h_{32} &= 2x_1x_2 + x_1 + 3 + x_2, & h_{33} &= -1 + x_1 + x_1^2, \\ h_{34} &= x_3 + 2x_2x_3 - 2x_2 - 1, & h_{35} &= -1 + x_2 + x_2^2, & h_{36} &= x_3^2 - 2x_3 + 1; \\ h_{41} &= 4x_1 - 4 - 4x_3 + 4x_1x_3, & h_{42} &= 4x_1x_2 - 4x_1 + 6 - 4x_2, & h_{43} &= 1 - 4x_1 + 2x_1^2, \\ h_{44} &= -4x_3 + 4x_2x_3 + 4x_2 - 4, & h_{45} &= 1 - 4x_2 + 2x_2^2, & h_{46} &= 2x_3^2 + 4x_3 + 2. \end{aligned}$$

Then we get the prime decomposition of given ideal:

$$I = I_1 \cup I_2 \cup I_3 \cup I_4.$$

6. Conclusions

In this article, we introduce the WDW algorithm, and use this algorithm to solve two problems:

1. The irredundant irreducible decomposition of varieties.
2. The prime decomposition of zero-dimensional radical ideals.

We also give the complexity of this algorithm.

References

- [1] B. Buchberger, *Gröbner bases: an algorithmic method in polynomial ideal theory*, in *Recent Trends in Multidimensional Systems theory* (ed. N.K. Bose), D.Reidel Publ. Comp., 1985.
- [2] J. Canny, *Generalised characteristics polynomials*, Journal of Symbolic Computation, **9**, 241-250, 1990.
- [3] A. Chistov, *Algorithm of polynomial complexity for factoring polynomials and finding the components of varieties in subexponential time*, J. Sov. Math **34**, **4**, 1838-1882, 1986.

- [4] S.C. Chou, *Mechanical geometry theorem proving*, D.Reidel Publishing Company, Dordrecht, Netherlands, 1988.
- [5] S.C. Chou and X.S. Gao, *Ritt-Wu's decomposition algorithm and geometry theorem proving*, CADE'10, 207-220, LNCS, No. 449, Springer-Verlag, 1990.
- [6] M. Elkadi and B. Mourrain, *A new algorithm for the geometric decomposition of a variety*, Proc. of ISSAC-99, ACM Press, 9-16.
- [7] X.S. Gao and S.C. Chou, *On the dimension for arbitrary ascending chains*, Chinese Bull. of Scis., **38**, 396-399, 1993.
- [8] X.S. Gao and S.C. Chou, *On the theory of resolvents and its applications*, Systems Science and Mathematical Sciences, **12**, 17-30, 1999.
- [9] P. Gianni, B. Trager, and G. Zacharias, *Gröbner bases and primary decomposition of polynomial ideals*, Journal of Symbolic Computation, **6**, 149-167, 1988.
- [10] S. Laplagne, *An algorithm for the computation of the radical of an ideal*, Proc. of ISSAC-06, ACM Press, 191-195.
- [11] F.S. Macaulay, *The algebraic theory of modular systems*, Cambridge University Press, 1916.
- [12] A. Sausse, *A new approach to primary decomposition*, Journal of Symbolic Computation, **31**, 243-257, 2001.
- [13] J.F. Ritt, *Differential algebra*, American Mathematical Society, 1950.
- [14] Á. Szántó, *Computation with polynomial systems*, PhD thesis, Cornell University, 1999.
- [15] B.L. Van der Waerden, *Einführung in die algebraischen geometrie*, SpringerVerlag, Berlin, 1973.
- [16] B.L. Van der Waerden, *Modern algebra II*, Frederick Ungar Pub., New York, 1953.
- [17] D.M. Wang, *Irreducible decomposition of algebraic varieties via characteristic sets and Gröbner bases*, Computer Aided Geometric Design, **9**, 471-484, 1992.
- [18] D.M. Wang, *Decomposing algebraic varieties, Automated Deduction in Geometry, LNAI 1669*, 180-206, Springer-Verlag, Berlin Heidelberg, 1999.
- [19] W.T. Wu, *Basic principles of mechanical theorem-proving in elementary geometries*, Journal of System Science and Mathematical Sciences, **4**, 207-235, 1984. Re-published in Journal of Automated Reasoning, **2**, 221-252, 1986.