J Syst Sci Complex (2014) 27: 1320–1344

MULTIPLICITY-PRESERVING TRIANGULAR SET DECOMPOSITION OF TWO POLYNOMIALS*

CHENG Jin-San · GAO Xiao-Shan

DOI: 10.1007/s11424-014-2017-0
Received: 17 February 2012 / Revised: 26 May 2013

Abstract In this paper, a multiplicity-preserving triangular set decomposition algorithm is proposed for a system of two polynomials, which involves only computing the primitive polynomial remainder sequence of two polynomials once and certain GCD computations. The algorithm decomposes the unmixed variety defined by two polynomials into square free and disjoint (for non-vertical components, see Definition 4) algebraic cycles represented by triangular sets, which may have negative multiplicities. Thus, the authors can count the multiplicities of the non-vertical components. In the bivariate case, the authors give a complete algorithm to decompose the system into zeros represented by triangular sets with multiplicities. The authors also analyze the complexity of the algorithm in the bivariate case. The authors implement the algorithm and show the effectiveness of the method with extensive experiments.

Keywords Algebraic cycle, multiplicity-preserving, primitive polynomial remainder sequence, triangular set decomposition.

1 Introduction

Decomposing a polynomial system into triangular sets is a classical method to solve polynomial systems. The method was first introduced in [1] and revised by Wu in his work of elementary geometry theorem proving[2, 3]. There exists extensive work about this topic[4–21]. The main tool to decompose a polynomial system is pseudo-division. In most existing triangular decomposition methods based on pseudo-division, one needs to deal with the initial of certain polynomial(s), say h, which will bring extraneous zeros. Usually, one decomposes a given system into two systems corresponding to the cases $h = 0$ and $h \neq 0$, respectively. In

CHENG Jin-San (Corresponding author) · GAO Xiao-Shan
Key Laboratory of Mathematics Mechanization, Institute of Systems Science, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190*, China.*
Email: jcheng@amss.ac.cn; xgao@mmrc.iss.ac.cn.
*The work is partially supported by NKBRPC under Grant No. 2011CB302400, the National Natural Science Foundation of China under Grant Nos. 11001258, 60821002, 91118001, SRF for ROCS, SEM, and China-France cooperation project EXACTA under Grant No. 60911130369.
◇ *This paper was recommended for publication by Editor LI Ziming.*

doing so, the number of the components increases quickly, leading to an un-elementary worst case complexity bound[10].

It is well known that the multiplicity of a component or a zero of a polynomial system contains important information which helps us to obtain a deeper understanding of the structure of the variety defined by the polynomial system. While, most triangular set decomposition algorithms do not preserve the multiplicities of the zeros or the components. One approach remedying this drawback is to decompose the polynomial system into triangular sets first and then recover the multiplicities. Li proposed a method to compute the multiplicities of zeros of a zero-dimensional polynomial system after obtaining a triangular decomposition of the system[22]. Recently, Li, et al. proved that the main component in the decomposition in Wu's sense for a zero-dimensional polynomial system is actually multiplicity-preserving[23]. They also gave a multiplicity-preserving decomposition, but some of the components are not in triangular form.

In [24], Bates, et al. proposed a numerical-symbolic algorithm to compute the multiplicity of a component (may not be zero-dimensional) of an algebraic set. Given a general point on the component, they constructed a zero-dimensional system which had the same multiplicity at the point as the component in the algebraic set. Computing the multiplicity of the zero-dimensional system at the point numerically, they derived the multiplicity of the component in the algebraic set. And there are some other methods to compute multiplicities of zeros of polynomial systems, which are not by triangular set theories, for example, [25]. In [26], the author took a primary decomposition for a system with two variables by Gröbner basis method, then derived triangular forms of the output.

In this paper, we give an algorithm to decompose the variety defined by two polynomials into algebraic cycles represented by triangular sets, that is, the components and their multiplicities in the original polynomial system. During the decomposition, the initials bring some extraneous algebraic cycles in each pseudo-division step during the computation of primitive polynomial remainder sequences. We record them during the computation and remove them later, which helps us to recover the algebraic cycles in triangular forms of the original system. This avoids some redundant computation during the decomposition. Currently, the theory is complete for polynomial systems consisting of two polynomials, which are decomposed into square free and disjoint algebraic cycles in triangular forms. Thus the multiplicities of the non-vertical components are obtained directly. In particular, we provide an algorithm to compute the zeros of a zero-dimensional bivariate system consisting of two polynomials as well as their multiplicities. We also analyze the complexity of the algorithm under certain conditions.

The proposed algorithm has two nice properties. First, the algorithm can find all the components by computing the primitive polynomial remainder sequence of the two polynomials. Second, the multiplicities of the components in the system can be found directly.

Kalkbrener[16] also used primitive polynomial remainder sequences to decompose zero-dimensional bivariate polynomial systems. But his method ignores multiplicities. Our method preserves multiplicities and removes the extraneous zeros.

The paper is organized as follows. In Section 2, we provide some properties of primitive

polynomial remainder sequences. In Section 3, we give the definition of algebraic cycles of an unmixed ideal. In Section 4, we provide the theories to decompose a polynomial system with two polynomials into square free and disjoint triangular sets which preserve the multiplicities of the components of the original system. We provide a multiplicity-preserving algorithm to decompose a zero-dimensional bivariate polynomial system into multiplicative-zeros in triangular forms in Section 5. The complexity of the algorithm under some conditions is analyzed. Algorithms and examples are used to illustrate the effectiveness and efficiency of our method. We also compare our method with other related methods. We draw a conclusion in the last section.

2 Primitive Polynomial Remainder Sequence

In this section, we introduce some basic properties for primitive polynomial remainder sequences. There are many references to this topic, in particular, [15, 16, 27]. We modify the procedure for our own purpose.

Let K be a computable field with characteristic zero, such as the field of rational numbers and $K[y_1, y_2, \cdots, y_n]$ the polynomial ring in the indeterminates $y_1, y_2, \cdots, y_n$. For $p, q \in K[y_1, y_2, \cdots, y_n]$, we set $\gcd(p, q) = 1$ if $\gcd(p, q) \in K \setminus \{0\}$.

Let $p \in K[x_1, x_2, \cdots, x_n, x]$. We define

$$\begin{aligned}&\mathrm{Cont}(p, x) = \gcd(\mathrm{coeff}(p, x^i), i = 0, 1, \cdots, \deg(p, x)),\\ &\mathrm{Prim}(p, x) = p/\mathrm{Cont}(p, x),\end{aligned}$$

where $\mathrm{coeff}(p, x^i)$ means the coefficient of x^i in p and $\deg(p, x)$ means the degree of p in x. p is called primitive w.r.t. x if $\mathrm{Cont}(p, x) = 1$.

The pseudo-division procedure can be extended to the following form.

Lemma 1 *Let $f, g \in K[x_1, x_2, \cdots, x_n, x]$, $\deg(f, x) = d_1$, $\deg(g, x) = d_2$, $d_1 \geq d_2 > 0$, and $\gcd(f, g) = 1$. There exist $q, r \in K[x_1, x_2, \cdots, x_n, x]$ such that*

$$l^{\delta+1} f + q\, g = r, \tag{1}$$

where l is the leading coefficient of g in x, $\delta = d_1 - d_2$, $\deg(g, x) > \deg(r, x)$. Denote $r = \mathrm{Prem}(f, g, x)$. Furthermore, q has the form:

$$q = l\, t\, x + s, \tag{2}$$

where $t \in K[x_1, x_2, \cdots, x_n, x], s \in K[x_1, x_2, \cdots, x_n]$. Moreover, if $r_1 = \mathrm{Cont}(f, x), r_2 = \mathrm{Cont}(g, x)$, then

$$r_1 | q,\ r_2^{d_1 - d_2} | q, r_1 | r, r_2^{d_1 - d_2 + 1} | r. \tag{3}$$

Proof Write f, g as univariate polynomials in x,

$$\begin{aligned}f &= a_1\, x^{d_1} + a_2\, x^{d_1 - 1} + \cdots + a_{d_1 + 1},\\ g &= b_1\, x^{d_2} + b_2\, x^{d_2 - 1} + \cdots + b_{d_2 + 1}.\end{aligned}$$

Note that $l = b_1$. We prove the lemma by induction on $\delta = d_1 - d_2$. To eliminate the terms of f with degree d_1 in x, we have

$$T_0(x) = b_1\, f + q_0\, g = h_0\, x^{d_1-1} + \text{ lower powers in } x,$$

where $q_0 = -a_1\, x^{d_1-d_2}, h_0 = b_1\, a_2 - a_1 b_2$. It is clear that $r_1|q_0$. Since $r_1|a_1$, $r_2^0(=1)|q_0$ and $r_1|T_0, r_2|T_0$. Set $r = T_0$ when $\delta = 0$. We can find that the lemma holds when $\delta = 0$. Now, we need to eliminate $h_0 * x^{d_1-1}$ from $T_0(x)$. If $h_0 \neq 0$,

$$\begin{aligned} T_1(x) &= b_1\, T_0(x) - h_0\, x^{d_1-d_2-1} g \\ &= b_1^2\, f + (b_1\, q_0 - (b_1\, a_2 - a_1 b_2)\, x^{d_1-d_2-1}) g \\ &= b_1^2\, f + q_1\, g \\ &= h_1\, x^{d_1-2} + \text{ lower powers in } x, \end{aligned}$$

where $h_1 \in K[x_1, x_2, \cdots, x_n]$ and $q_1 = -b_1\, a_1\, x^{d_1-d_2} - (b_1\, a_2 - a_1 b_2)\, x^{d_1-d_2-1}$. Each term of q_1 contains a factor of the form $a_i\, b_j$. So $r_1|q_1$, $r_2|q_1$ and $r_1|T_1, r_2^2|T_1$. If $h_0 = 0$, $T_1(x) = b_1\, T_0(x)$, and the result is still true. So the lemma holds when $\delta = 1$. Assuming that the lemma holds for the cases $\delta \leq i (i > 1)$, then we have

$$T_\delta(x) = b_1^{\delta+1}\, f + q_\delta\, g,$$

where $q_\delta = l\, t_\delta\, x + s_\delta, r_1|q_\delta, r_2^\delta|q_\delta, r_1|T_\delta, r_2^{\delta+1}|T_\delta$. Then when $\delta = i + 1$, that is, $\deg(f, x) - \deg(g, x) = i + 1$, we set $g' = x * g$. Thus $\delta = i$ for f and g'. So we have

$$S(x) = b_1^{i+1}\, f - q_i\, g',$$

and $r_1|q_i, r_2^i|q_i, r_1|S, r_2^{i+1}|S$ by the assumption.

If $\deg(S, x) < d_2 = \deg(g, x)$, then

$$r = b_1\, S(x) = b_1\, b_1^{i+1}\, f - b_1\, q_i\, g' = b_1^{i+2}\, f - b_1\, q_i\, x\, g = b_1^{i+2}\, f - q_{i+1}\, g.$$

It is easy to find that $r_1|q_{i+1}, r_2^i|q_{i+1}, r_1|q_{i+1}, r_2^{i+2}|q_{i+1}$.

Otherwise, $\deg(S, x) = d_2 = \deg(g, x)$. Let p be the leading coefficient of S w.r.t. x. It is clear that $r_1|p, r_2^{i+1}|p$. We have

$$r = b_1\, S(x) - p\, g = b_1^{i+2}\, f - (b_1\, q_i\, x - p)\, g = b_1^{i+2}\, f - q_{i+1}\, g.$$

We can find that $r_1|q_{i+1}, r_2^i|q_{i+1}, r_1|q_{i+1}, r_2^{i+2}|q_{i+1}$. Thus the lemma is proved. ∎

The following corollary is obvious.

Corollary 2 *Let $f, g \in K[x_1, x_2, \cdots, x_n, x]$ be primitive, $d_1 = \deg(f, x) \geq d_2 = \deg(g, x) > 0$, and $\gcd(f, g) = 1$. Regard f, g as univariate polynomials in x. Then there exists an $m \in K[x_1, x_2, \cdots, x_n]$ such that*

$$m\, f = q\, g + r,$$

and $\gcd(m, q) = \gcd(m, r) = 1$. Furthermore,

$$(m\, f, g) = (g, r),$$

where (P) represents the ideal generated by a polynomial system P.

The result below is a necessary condition to check whether g has factors in $K[x_1, x_2, \cdots, x_n]$.

Corollary 3 $\mathrm{Cont}(g, x) = 1$ *if* $\gcd(l, s) = 1$ *and* $d_1 > d_2$, *where* l *and* s *are from* (1) *and* (2).

Proof Regard f, g as univariate polynomials in x, and q a polynomial in x and a_i, b_j, where $i = 1, 2, \cdots, d_1 + 1, j = 1, 2, \cdots, d_2 + 1$. Let $r_2 | g$ and $r_2 \in K[x_1, x_2, \cdots, x_n]$. From Lemma 1, $r_2 | q$ if $d_1 > d_2$. So $r_2 | s$. Since $r_2 | l$, $r_2 | \gcd(l, s)$. We have $r_2 = 1$ if $\gcd(l, s) = 1$. The corollary is proved. ∎

Lemma 4 *Let* $f_1, f_2 \in K[x_1, x_2, \cdots, x_n, x]$, $d_1 = \deg(f_1, x) \geq d_2 = \deg(f_2, x) > 0$. *Assume that* $\mathrm{Cont}(f_i, x) = 1, i = 1, 2$. *Regarding* f_1, f_2 *as polynomials in* x, *we can obtain a polynomial sequence* $\{f_1, f_2, \cdots, f_{k+2}\}$ *such that*

$$m_i f_i + q_i f_{i+1} = m_{i-1} p_i f_{i+2}, \quad i = 1, 2, \cdots, k, \tag{4}$$

where $m_0 = 1, p_k = 1, m_i, p_i, f_{k+2} \in K[x_1, x_2, \cdots, x_n], q_i \in K[x_1, x_2, \cdots, x_n, x], i = 1, 2, \cdots, k$, *and* $\mathrm{Cont}(f_i, x) = 1 (1 \leq i \leq k + 1)$, $\gcd(m_i, p_i) = 1$.

Proof When $i = 1$, from Lemma 1, there exist $q \in K[x_1, x_2, \cdots, x_n, x], r \in K[x_1, x_2, \cdots, x_n, x]$ such that $l_2^{\delta+1} f_1 + q f_2 = r$, where l_i is the leading coefficient of f_i in x, $\delta = d_1 - d_2$. Let $t = \gcd(l_2^{\delta+1}, q)$, $m_1 = \frac{l_2^{\delta+1}}{t}, q_1 = \frac{q}{t}$. If $\deg(r, x) = 0$, set $f_3 = \frac{r}{t}, m_0 = p_1 = 1$ and $k = 1$. We have obtained the sequence and the lemma is proved. Else, let $p_1 = \frac{\mathrm{Cont}(r,x)}{t}$ and $f_3 = \mathrm{Prim}(r, x)$. It is clear that $\gcd(m_1, p_1) = 1$. Denote $d_i = \deg(f_i, x)$. For f_i, f_{i+1}, we have $l_{i+1}^{\theta+1} f_i + q_t f_{i+1} = r_{i+2}$ by Lemma 1, where $\theta = d_i - d_{i+1}, d_{i+1} > 0$. If m_{i-1} is a factor of r_{i+2}, set p_i' as the product of all the factors of $\frac{r_{i+2}}{m_{i-1}}$ in $K[x_1, x_2, \cdots, x_n]$. Let $h = \gcd(l_{i+1}^{\theta+1}, p_i')$. Then $m_i = \frac{l_{i+1}^{\theta+1}}{h}, q_i = \frac{q_t}{h}, p_i = \frac{p_i'}{h}$, $\gcd(m_i, p_i) = 1$. Let $f_{i+2} = \frac{r_{i+2}}{m_{i-1} p_i'}$. If $\deg(f_{i+2}, x) = 0$, set $f_{i+2} = p_i$ and $p_i = 1$. Thus $k = i$. If m_{i-1} is not a factor of r_{i+2}, we can multiply $g = \frac{m_{i-1}}{\gcd(m_{i-1}, r_{i+2})}$ to the two sides of the equation. Then doing the same operation as before, we can derive $m_i f_i + q_i f_{i+1} = m_{i-1} p_i f_{i+2}$ which satisfies all the conditions. Doing the same computation recursively, the operation will end for some k such that $\deg(f_{k+2}, x) = 0$. This proves the lemma. ∎

In most cases, we have $\gcd(m_i, q_i) = 1$ and $p_i = 1$ which help us to design efficient algorithms. We call the algorithm to compute the sequence $f_1, f_2, \cdots, f_{k+1}, f_{k+2}$ the extended Euclidean algorithm.

Corollary 5 *Let* $f_1, f_2 \in K[x_1, x_2, \cdots, x_n, x], \gcd(f_1, f_2) = 1$, $\mathrm{Cont}(f_i, x) = 1, i = 1, 2$, *and* $\deg(f_1, x) \geq \deg(f_2, x) > 0$. *From the extended Euclidean algorithm, we can obtain*

$$m_i f_i + q_i f_{i+1} = g_i f_{i+2}, \quad i = 1, 2, \cdots, k, \tag{5}$$

$$(m_i f_i, f_{i+1}) = (f_{i+1}, g_i f_{i+2}), \tag{6}$$

where $m_i, g_i \in K[x_1, x_2, \cdots, x_n]$, $\gcd(m_i, g_i) = 1$, $g_k = 1$, $\gcd(m_k, g_k f_{k+2}) = 1$, *and* $f_{i+2} (1 \leq i \leq k - 1)$ *are primitive.*

Proof From Lemma 4, we have (4). Note that $\gcd(m_i, p_i) = 1$. Let $h = \gcd(m_i, m_{i-1})$, denote $m_i = \frac{m_i}{h}, q_i = \frac{q_i}{h}, g_i = \frac{m_{i-1} p_i}{h}$. Then we have $\gcd(m_i, g_i) = 1$. Since $f_{k+2} \in$

$K[x_1, x_2, \cdots, x_n]$, we can set $g_k = 1$. We can delete $\gcd(m_k, g_k f_{k+2})$ if it exists. Thus we obtain (5). (6) is obvious. So the corollary holds. ∎

The following corollary is clear and useful.

Corollary 6 *We can rewrite* (5) *and* (6) *as below.*

$$m_i f_i + q_i f_{i+1} = \frac{m_{i-1}}{w_i} p_i f_{i+2}, \quad i = 1, 2, \cdots, k, \tag{7}$$

$$(m_i\, f_i, f_{i+1}) = \left(f_{i+1}, \frac{m_{i-1}}{w_i} p_i\, f_{i+2}\right), \tag{8}$$

where w_i *is a factor of* m_{i-1}, $g_i = \frac{m_{i-1}}{w_i} p_i$, *and* $p_k = 1$.

3 Algebraic Cycles of Unmixed Ideals

A d-dimensional algebraic cycle is generally defined to be a formal linear combination $\sum_i m_i V_i$ of d-dimensional irreducible algebraic varieties V_i with non-negative integer coefficients m_i[28, 29]. This definition does not suit for our computational approach of algebraic cycles. In this section, we will define the algebraic cycle associated with an unmixed ideal, which will be served as the basis for our decomposition algorithm to be presented in this paper.

3.1 Algebraic Cycle in Projective Space

We will define the multiplicities of the irreducible components of an unmixed homogenous polynomial system in this subsection, which will be used to define multiplicative varieties in affine case in the next subsection.

We first recall the concept of multiplicity of a point of a zero-dimensional polynomial system in affine case.

Let I be a zero-dimensional ideal in $K[x_1, x_2, \cdots, x_n]$ such that the affine variety $V(I)$ defined by I consists of finitely many points in $\overline{K}^n$, where $\overline{K}$ is the algebraic closure of K, and assume $p = (a_1, a_2, \cdots, a_n) \in V(I)$. Then the multiplicity of p[30] as a zero of I, denoted by $m(p)$, is the dimension of the vector field obtained by localizing $\overline{K}[x_1, x_2, \cdots, x_n]$ at the maximal ideal $M = I(p) = (x_1 - a_1, x_2 - a_2, \cdots, x_n - a_n)$ corresponding to p, that is,

$$m(p) = \dim_{\overline{K}} \overline{K}[x_1, x_2, \cdots, x_n]_M / I\overline{K}[x_1, x_2, \cdots, x_n]_M.$$

We can easily extend the above definition to projective space, since for any zero $\eta = (\eta_0, \eta_1, \cdots, \eta_n)$ of a zero-dimensional polynomial system Σ in projective space, there is one coordinate, say η_0, which is not equal to zero. Then $(1, \frac{\eta_1}{\eta_0}, \frac{\eta_2}{\eta_0}, \cdots, \frac{\eta_n}{\eta_0})$ is still a zero of Σ. Let Σ' be the corresponding system of Σ in affine space such that $\Gamma = (\frac{\eta_1}{\eta_0}, \frac{\eta_2}{\eta_0}, \cdots, \frac{\eta_n}{\eta_0})$ is a zero of Σ'. The multiplicity of η in Σ is defined to be the multiplicity of Γ in Σ'.

Let $\mathcal{P} \subset K[x_0, x_1, \cdots, x_n]$ be a zero-dimensional homogenous polynomial system, which has a finite number of solutions in projective space:

$$(\xi_0^{(j)}, \xi_1^{(j)}, \cdots, \xi_n^{(j)}), \quad j = 1, 2, \cdots, s \tag{9}$$

with multiplicity m_j in some extension $\overline{K}$ of K. Let

$$L = u_0\, x_0 + u_1\, x_1 + \cdots + u_n\, x_n = 0,$$

where $u = (u_0, u_1, \cdots, u_n)$ are indeterminates. Then the u-resultant of $\mathcal{P}$ (see p.172 of [31] and p.144 of [30]) is a homogenous polynomial $D(u)$ in $K[u]$, which can be factored as

$$D(u) = \Pi_{j=1}^{s}(u_0\, \xi_0^{(j)} + u_1\, \xi_1^{(j)} + \cdots + u_n\, \xi_n^{(j)})^{m_j}. \tag{10}$$

The u-resultant has the property that for a specialization $u \to \overline{u}$, $\mathcal{P} = 0$ and $\overline{L} = \overline{u}_0\, x_0 + \overline{u}_1\, x_1 + \cdots + \overline{u}_n\, x_n = 0$ have common solutions if and only if $D(\overline{u}) = 0$.

In order to extend the concept of multiplicity to the case of an irreducible component of an unmixed homogenous polynomial ideal, we need the following result. A polynomial ideal I is called unmixed if it has no embedded associated primes. Equivalently, all associated primes of an unmixed I have the same dimension. It is clear that if I is an unmixed ideal of dimension d, then all irredundant irreducible varieties of I are of dimension d.

Lemma 7 (Theorem IV of [28]) *Let $I_d^H \subset K[x_0, x_1, \cdots, x_n]$ be a prime homogeneous ideal of dimension d and*

$$L_i = v_{i0}x_0 + v_{i1}x_1 + \cdots + v_{in}x_n, \quad i = 1, 2, \cdots, d, \tag{11}$$

d generic hyperplanes. Then $\overline{I} = (I_d^H, L_1, L_2, \cdots, L_d)$ is a prime zero-dimensional ideal in $K^*[x_0, x_1, \cdots, x_n]$, where $K^* = K(v_1, v_2, \cdots, v_d)$ and $v_i = (v_{i0}, v_{i1}, \cdots, v_{in})$. Furthermore, each zero of $\overline{I}$ is a generic point of I.

Let $I_d^H \subset K[x_0, x_1, \cdots, x_n]$ be an unmixed homogenous ideal of dimension d and

$$V(I_d^H) = \sum_{i=1}^{t} V_i \tag{12}$$

be an irredundant decomposition of $V(I_d^H)$. Then each V_i is an irreducible variety of dimension d. Let $L_1, L_2, \cdots, L_d$ be the generic hyperplanes in (11) and

$$\overline{I}_d^H = (I_d^H, L_1, L_2, \cdots, L_d).$$

Then it is easy to show that

$$\mathbb{V}(\overline{I}_d^H) = \sum_{i=1}^{t} V_i \cap \mathbb{V}(L_1, L_2, \cdots, L_d).$$

By Lemma 7, each $\overline{V}_i = V_i \cap \mathbb{V}(L_1, L_2, \cdots, L_d)$ is an irreducible variety of dimensional zero over K^*. As a consequence, $\overline{I}_d^H$ is also zero-dimensional over K^*. We have

Lemma 8 *Using the notations introduced above. Let $\overline{V}_i = V_i \cap \mathbb{V}(L_1, L_2, \cdots, L_d) = \{\eta_{ij}, j = 1, 2, \cdots, s_i\}$ where $\eta_{ij} = (\eta_{ij0}, \eta_{ij1}, \cdots, \eta_{ijn})$. Then the multiplicities of $\eta_{ij}, j = 1, 2, \cdots, s_i$ as zeros of $\overline{I}_d^H$ are all the same.*

Proof According to the definition of multiplicities, we need only to show that the lemma is valid in affine case, which will be proved below. Let M_j be the maximal ideal associated with η_{ij}. It suffices to show that the localization rings R_{M_j} for different j are the same, where $R = K[x_1, x_2, \cdots, x_n]$. R_{M_j} can be written as $\{P/Q \,|\, P, Q \in R \& Q(\eta_{ij}) \neq 0\}$. Since $\eta_{ij}, j = 1, 2, \cdots, s_i$ are the zeros of an irreducible variety $\overline{V}_i$, R_{M_j} are the same for all j, which proves the lemma. ∎

Let $D(u)$ be the u-resultant of $\overline{I}_d^H$. Then by Lemma 8 and (10), we have

$$D(u) = \Pi_{i=1}^{t} \Pi_{j=1}^{s_i} (u_0\, \eta_{ij0} + u_1\, \eta_{ij1} + \cdots + u_n\, \eta_{ijn})^{m_i}, \tag{13}$$

where m_i is the multiplicity of η_{ij} as a zero of $\overline{I}_d^H$, t is from (12), s_i is from Lemma 8. Now, we can define the algebraic cycle of I_d^H.

Definition 1 Let $I_d^H \subset K[x_0, x_1, \cdots, x_n]$ be an unmixed homogenous ideal of dimension d, V_i the irreducible components of $\mathbb{V}(I_d^H)$ defined in (12), and $D(u)$ the u-resultant of $\overline{I}_d^H$ given in (13). Then the multiplicity of V_i in I_d^H is defined to be m_i and the algebraic cycle of I_d^H is defined to be

$$\mathbb{M}(I_d^H) = \sum_{i=1}^{h} m_i\, \mathbb{M}_i, \tag{14}$$

where $\mathbb{M}_i$ corresponds to V_i and has multiplicity m_i in $\mathbb{M}(I_d^H)$.

Consider two algebraic cycles with the forms $\mathbb{M}_d = \sum_{i=1}^{h} a_i \mathbb{M}_d^{(i)}$ and $\mathbb{N}_d = \sum_{i=1}^{h} b_i \mathbb{M}_d^{(i)}$, where $\mathbb{M}_d^{(i)}$ are irreducible algebraic cycles. Without loss of generality, we assume that some of the a_i or b_i maybe zero, meaning that the corresponding $\mathbb{M}_d^{(i)}$ is not in $\mathbb{M}_d$ or $\mathbb{N}_d$. It is clear that we can define "+" between algebraic cycles:

$$\mathbb{M}_d + \mathbb{N}_d = \sum_{i=1}^{h} (a_i + b_i) \mathbb{M}_d^{(i)}.$$

Let F_m and F_n be the u-resultant of $\mathbb{M}_d$ and $\mathbb{N}_d$, respectively. Then, the u-resultant of $\mathbb{M}_d + \mathbb{N}_d$ is $F_m\, F_n$.

$\mathbb{N}_d$ is called a subvariety of $\mathbb{M}_d$ if $a_i \geq b_i (i = 1, 2, \cdots, h)$. If $\mathbb{N}_d$ is a subvariety of $\mathbb{M}_d$, then we can define "−" as follows

$$\mathbb{M}_d - \mathbb{N}_d = \sum_{i=1}^{h} (a_i - b_i) \mathbb{M}_d^{(i)},$$

where $a_i - b_i \geq 0$. Then, the u-resultant of $\mathbb{M}_d - \mathbb{N}_d$ is F_m / F_n. Note that F_n is a factor of F_m.

3.2 A Product Formula of Affine Algebraic Cycles

We will define the multiplicities of the irreducible components of an unmixed polynomial system in the affine case and prove a property of algebraic cycles which is the basis for the decomposition algorithm to be proposed in this paper.

We first define the algebraic cycle of an unmixed ideal in the affine case under certain conditions.

Definition 2 Let $I_d \subset K[x_1, x_2, \cdots, x_n]$ be an unmixed polynomial ideal of dimension d in affine space and $I_d^H \subset K[x_0, x_1, \cdots, x_n]$ the homogenization of I_d by introducing a new variable x_0. If I_d^H is unmixed and $\dim(I_d) = \dim(I_d^H) = d$, the algebraic cycle of I_d is defined to be a representation similar as (14) but removing the components at infinity.

We need to mention that an ideal corresponds to an algebraic cycle uniquely, but an algebraic cycle may corresponds to many different ideals. For example, $I_1 = (x^2, y) \neq I_2 = (x, y^2)$, but $\mathbb{M}(I_1) = \mathbb{M}(I_2) = 2\mathbb{M}(I)$, where $I = (x, y)$.

In the rest of this section, we will concentrate on the algebraic cycles of two polynomials.

Let $f, g \in K[x_1, x_2, \cdots, x_n]$ such that $\gcd(f, g) = 1$ and f^H, g^H be the homogenization of f and g respectively. As a consequence of Macaulay's unmixed theorem[32], we have

Lemma 9 *If f and g are not conflict and $\gcd(f, g) = 1$, then (f, g) is an unmixed ideal of dimension $n - 2$.*

As a consequence, (f^H, g^H) is an unmixed homogenous ideal of dimension $n - 2$. Thus, we can always define $\mathbb{M}(f, g) = \mathbb{M}((f, g))$. The following is a key result of this paper.

Theorem 10 *Let $f, g, h \in K[x_1, x_2, \cdots, x_n]$. If $\gcd(f\,g, h) = 1$, then*

$$\mathbb{M}(f\,g, h) = \mathbb{M}(f, h) + \mathbb{M}(g, h). \tag{15}$$

Proof It is not difficult to find that $V(f\,g, h) = V(f, h) \cup V(g, h)$. Thus the components of $\mathbb{M}(f\,g, h)$ and $\mathbb{M}(f, h)+\mathbb{M}(g, h)$ are the same. We need only to prove that the multiplicity of each component on the two sides is the same. Since $\gcd(f\,g, h) = 1$, $\dim(V(f\,g, h)) = \dim(V(f, h)) = \dim(V(g, h)) = n - 2$. Let $I = (f\,g, h)$ and $I^H = (f^H\,g^H, h^H)$ be the homogenization of I (in $x_0, x_1, x_2, \cdots, x_n$) by introducing the new variable x_0. We can find that $\dim(V(I)) = \dim(V(I^H))$. Denote $L_i = u_{i,0}\,x_0 + u_{i,1}\,x_1 + \cdots + u_{j,n}\,x_n (i = 0, 1, \cdots, n - 2)$, and $u_i = (u_{i,0}, u_{i,1}, \cdots, u_{i,n})$. Then

$$\Sigma = (f^H\,g^H, h^H, L_1, L_2, \cdots, L_{n-2})$$

is a zero-dimensional system in the field extension $K^* = K(u_1, u_2, \cdots, u_{n-2})$. Then by the property of multi-polynomial resultants[30], we have

$$\begin{aligned} &\operatorname{Res}(L_0, f^H\,g^H, h^H, L_1, L_2, \cdots, L_{n-2}) \\ &= \operatorname{Res}(L_0, f^H, h^H, L_1, L_2, \cdots, L_{n-2}) \operatorname{Res}(L_0, g^H, h^H, L_1, L_2, \cdots, L_{n-2}), \end{aligned} \tag{16}$$

where $\operatorname{Res}(L_0, f^H\,g^H, h^H, L_1, L_2, \cdots, L_{n-2})$, $\operatorname{Res}(L_0, f^H, h^H, L_1, L_2, \cdots, L_{n-2})$, $\operatorname{Res}(L_0, g^H, h^H, L_1, L_2, \cdots, L_{n-2})$ are u-resultants of $(f^H\,g^H, h^H)$, (f^H, h^H), and (g^H, h^H) in K^*, respectively. Thus the multiplicities of the components in $\mathbb{M}(f^H\,g^H, h^H)$ and $\mathbb{M}(f^H, h^H) + \mathbb{M}(g^H, h^H)$ are the same, which means that the lemma is true when f, g, h are homogeneous.

We can rewrite the zero $\xi_j = (\xi_0^{(j)}, \xi_1^{(j)}, \cdots, \xi_n^{(j)})$ of $\Sigma = 0$ into two forms by deciding whether $\xi_0^{(j)} = 0$ or not. If $\xi_0^{(j)} = 0$, then

$$\xi_j = (0, \xi_1^{(j)}, \xi_2^{(j)}, \cdots, \xi_n^{(j)}).$$

These are the solutions of $\{f\,g, h, L_1, L_2, \cdots, L_{n-2}\} = 0$ at infinity. If $\xi_0^{(j)} \neq 0$, then

$$\xi_j = \left(1, \frac{\xi_1^{(j)}}{\xi_0^{(j)}}, \frac{\xi_2^{(j)}}{\xi_0^{(j)}}, \cdots, \frac{\xi_n^{(j)}}{\xi_0^{(j)}}\right) = (1, \xi_1'^{(j)}, \xi_2'^{(j)}, \cdots, \xi_n'^{(j)}).$$

These correspond to the solutions of $\{f\,g, h, L_1, L_2, \cdots, L_{n-2}\} = 0$ in the affine space. Thus, the u-resultant of $(f^H\,g^H, h^H, L_1, L_2, \cdots, L_{n-2})$ can be written as the following form for some $C \in K^*$ and $1 \leq t \leq s$:

$$\begin{aligned} D(u_0) = C\,\Pi_{j=1}^{t}(u_{0,0} + u_{0,1}\,\xi_1'^{(j)} + u_{0,2}\,\xi_2'^{(j)} + \cdots + u_{0,n}\,\xi_n'^{(j)})^{m_j} \\ \Pi_{j=t+1}^{s}(u_{0,1}\,\xi_1^{(j)} + u_{0,2}\,\xi_2^{(j)} + \cdots + u_{0,n}\,\xi_n^{(j)})^{m_j}. \end{aligned} \tag{17}$$

We can get a similar representation for $(f^H, h^H, L_1, L_2, \cdots, L_{n-2})$ and $(g^H, h^H, L_1, L_2, \cdots, L_{n-2})$. From (16) and (17), we can see that the multiplicity for an irreducible component V of $\{f\,g, h\}$ is the sum of the multiplicities of V in $\{f, g\}$ and $\{g, h\}$. This proves the theorem. ∎

In the case of two variables, the above theorem is a direct consequence of Theorem 3 of [33].

There do exist general results similar to Theorem 10, for instance in [28]. But due to the different definition of algebraic cycles in [28] and in our paper, such results cannot be used directly to deduce Theorem 10.

4 Multiplicity-Preserving Triangular Set Decomposition of Two Polynomials

In this section, we will give a method to decompose a system consisting of two polynomials into square free and disjoint triangular sets, which preserves the multiplicities of the components in the system.

4.1 Triangular Decomposition of Two Polynomials

Let $x_1 \prec x_2 \prec \cdots \prec x_n$ be ordered variables and $K[x_1, x_2, \cdots, x_n]$ the ring of polynomials in x_i. A variable x_c is said to be the main variable of $t \in K[x_1, x_2, \cdots, x_n]$ if x_c is the largest variable occurring in t. Let x_c be the main variable of t. Then t can be written uniquely as a univariate polynomial in x_c:

$$t = a_d x_c^d + a_{d-1} x_c^{d-1} + \cdots + a_0,$$

where $a_i \in K[x_1, x_2, \cdots, x_{c-1}]$. Then, a_d is called the initial of t and $a_d x_c^d$ is called the leading term of t.

A polynomial system $T = \{t_1, t_2, \cdots, t_s\} \subset K[x_1, x_2, \cdots, x_n]$ is said to be a triangular set if $t_i \in T (1 \leq i \leq s)$ are non-constant and have distinct main variables.

A triangular set $T = \{t_1, t_2, \cdots, t_s\} \subset K[x_1, x_2, \cdots, x_n]$ such that $t_i (i = 1, 2, \cdots, s)$ are listed in order of their main variables, say x_{m_i}, from low to high, is said to be regular[15, 20] if

$$\mathrm{Res}(I, T) = \mathrm{Res}_{x_{m_1}}(\cdots(\mathrm{Res}_{x_{m_s}}(I, t_s), \cdots), t_{m_1}) \neq 0,$$

where I is the product of all the initials of t_i. Regular triangular sets have the following properties.

Lemma 11 *If $T = \{f, g\} \subset K[x_1, x_2, \cdots, x_n]$ is a regular triangular set, then $\mathbb{M}(T)$ is a nonempty algebraic cycle of dimension $n-2$.*

Proof Let I be the initial of g. Then $\gcd(h, I) = 1$. As a consequence, $\gcd(g, h) = 1$. Then it suffices to show that $\mathbb{V}(T)$ is not empty. It is well known that $\mathbb{V}(T/I)$ is not empty[15]. Since $\mathbb{V}(T/I) \subset \mathbb{V}(T)$, the lemma is proved. ∎

From the definition, we can easily decompose a triangular set $\{h, f\}$ ($h \in K[x_1, x_2, \cdots, x_n]$, $f \in K[x_1, x_2, \cdots, x_n, x]$) into regular ones. Let the initial of f be $p \in K[x_1, x_2, \cdots, x_n]$, t the leading term of f in x, and $q = \gcd(p, h) \in K[x_1, x_2, \cdots, x_n]$. If q is a constant in K, $\{h, f\}$ is regular. Otherwise, by Theorem 10

$$\mathbb{M}(h, f) = \mathbb{M}(h/q, f) + \mathbb{M}(q, f - t).$$

And we can continue to decompose $\mathbb{M}(q, f - t)$ until it is regular. Therefore, in the rest of the paper, a triangular set consisting of two polynomials is always assumed to be regular.

Definition 3 A multiplicity-preserving triangular set decomposition of an unmixed polynomial system Σ of dimension d is a decomposition like

$$\mathbb{M}(\Sigma) = \sum_{i=1}^{m^+} \mathbb{M}(T_i^+) - \sum_{j=1}^{m^-} \mathbb{M}(T_i^-), \tag{18}$$

where $\{T_i^+, T_j^-, i = 1, 2, \cdots, m^+, j = 1, 2, \cdots, m^-\}$ are regular triangular sets such that $\mathbb{M}(T_i^+)$ and $\mathbb{M}(T_i^-)$ are algebraic cycles of dimension d.

We will show that a multiplicity-preserving triangular sets decomposition exists for systems with two polynomials in the rest of this section. Note that for a zero-dimensional polynomial system, the existence of (18) is obvious. The existence of (18) in the general case (dimension mixed, more polynomials) is our future work.

We can strengthen the decomposition in Definition 3 in the two polynomials case.

Definition 4 Let $T = \{h, f\}$ be a triangular set such that $h \in K[x_1, x_2, \cdots, x_n], f \in K[x_1, x_2, \cdots, x_n, x]$. Denote all the zeros of the coefficients of f in x as $V_{\text{coef}}(f, x) \subset \overline{K}^n$, where $\overline{K}$ is the algebraic closure of K and $V(P)$ is the zeros of $P \in K[x_1, x_2, \cdots, x_n]$ in $\overline{K}^n$. We call the corresponding algebraic cycles of $V_{\text{coef}}(f, x) \cap V(h)$ the vertical components of $\mathbb{M}(T)$. The components of $\mathbb{M}(T)$ removing the vertical components are called non-vertical components. Let $T_1, T_2 \subset K[x_1, x_2, \cdots, x_n, x]$ be two triangular sets of dimension $n-1$, each has two polynomial elements. And let V_i be the zero set of the vertical components of T_i, $i = 1, 2$. We say T_1, T_2 or $\mathbb{M}(T_1), \mathbb{M}(T_2)$ are disjoint if $\dim((V(T_1) \setminus V_1) \cap (V(T_2) \setminus V_2)) < n-2$. We call $\{h, f\}$ or $\mathbb{M}(h, f)$ square free if h is square free, and $\{h, f\}, \{h, \frac{\partial f}{\partial x}\}$ or $\mathbb{M}(h, f), \mathbb{M}(h, \frac{\partial f}{\partial x})$ are disjoint.

For example, $T_1 = \{x_2 - x_1^2, x_2\, x - x_1\}$ and $T_2 = \{x_2 - x_1^2, x_1\, x + x_2 - x_1\}$ are disjoint. Note that $x_1 = x_2 = 0$ is their common vertical component of dimension 1 and $\dim(T_1) = \dim(T_2) = 1$ in $\mathbb{C}^3$.

The following theorem and its corollary are key results of the paper.

Theorem 12 *Let* $f_1, f_2 \in K[x_1, x_2, \cdots, x_n, x]$ *such that* gcd $(f_1, f_2) = 1$, $\mathrm{Cont}(f_i, x) = 1, i = 1, 2$, *and* $\deg(f_1, x) \geq \deg(f_2, x) > 0$. *Then, we have the following multiplicity-preserving triangular decomposition*

$$\mathbb{M}(f_1, f_2) = \mathbb{M}(f_{k+1}, f_{k+2}) + \sum_{i=1}^{k} \mathbb{M}(g_i, f_{i+1}) - \sum_{i=1}^{k} \mathbb{M}(m_i, f_{i+1}), \tag{19}$$

where f_i, g_i, m_i *are defined in Corollary* 5.

Proof From (6), we have

$$\mathbb{M}(m_i f_i, f_{i+1}) = \mathbb{M}(f_{i+1}, g_i\, f_{i+2}),$$

and $\gcd(m_i f_i, f_{i+1}) = \gcd(f_{i+1}, g_i\, f_{i+2}) = 1$. Then by Theorem 10, for $1 \leq i \leq k$, we have

$$\mathbb{M}(m_i, f_{i+1}) + \mathbb{M}(f_i, f_{i+1}) = \mathbb{M}(g_i, f_{i+1}) + \mathbb{M}(f_{i+1}, f_{i+2}), \tag{20}$$

$$\mathbb{M}(f_i, f_{i+1}) = \mathbb{M}(f_{i+1}, f_{i+2}) + \mathbb{M}(g_i, f_{i+1}) - \mathbb{M}(m_i, f_{i+1}). \tag{21}$$

From (20), $\mathbb{M}(m_i, f_{i+1})$ is a subvariety of $\mathbb{M}(g_i, f_{i+1}) + \mathbb{M}(f_{i+1}, f_{i+2})$. Then we can do subtraction in (21). So we have

$$\begin{aligned}
\mathbb{M}(f_1, f_2) &= \mathbb{M}(f_2, f_3) + \mathbb{M}(g_1, f_2) - \mathbb{M}(m_1, f_2) \\
&= \mathbb{M}(f_3, f_4) + \mathbb{M}(g_1, f_2) + \mathbb{M}(g_2, f_3) - \mathbb{M}(m_1, f_2) - \mathbb{M}(m_2, f_3) \\
&\ \ \vdots \\
&= \mathbb{M}(f_{k+1}, f_{k+2}) + \sum_{i=1}^{k} \mathbb{M}(g_i, f_{i+1}) - \sum_{i=1}^{k} \mathbb{M}(m_i, f_{i+1}).
\end{aligned}$$

The proof is completed. ∎

By the definition of algebraic cycle, the decomposition in (19) is about the $(n-1)$-dimensional component of $\mathbb{M}(f_1, f_2)$. The following corollary is very useful in practice.

Corollary 13 *Use the notations in Corollary* 6, *we have*

$$\begin{aligned}
\mathbb{M}(f_1, f_2) = \mathbb{M}(f_{k+1}, f_{k+2}) &+ \sum_{i=1}^{k} (\mathbb{M}(p_i, f_{i+1}) - \mathbb{M}(w_i, f_{i+1})) \\
&- \sum_{i=1}^{k-1} \left(\mathbb{M}\Big(m_i, \frac{m_{i-1}}{w_i}\Big) + \mathbb{M}(m_i, p_i) - \mathbb{M}(m_i, q_i) \right) - \mathbb{M}(m_k, f_{k+1}).
\end{aligned} \tag{22}$$

Proof From Corollary 6, we have $w_i\, g_i = m_{i-1} p_i$. So by Theorem 10, we have

$$\mathbb{M}(g_i, f_{i+1}) = \mathbb{M}(p_i, f_{i+1}) + \mathbb{M}(m_{i-1}, f_{i+1}) - \mathbb{M}(w_i, f_{i+1}). \tag{23}$$

This helps us simplifying the computation. By (20), we have

$$\begin{aligned}\mathbb{M}(f_1,f_2) &= \mathbb{M}(f_{k+1},f_{k+2}) + \sum_{i=1}^{k}(\mathbb{M}(p_i,f_{i+1}) + \mathbb{M}(m_{i-1},f_{i+1}) \\ &\quad -\mathbb{M}(w_i,f_{i+1})) - \sum_{i=1}^{k}\mathbb{M}(m_i,f_{i+1}) \\ &= \mathbb{M}(f_{k+1},f_{k+2}) + \sum_{i=1}^{k}\mathbb{M}(p_i,f_{i+1}) - \sum_{i=1}^{k}\mathbb{M}(w_i,f_{i+1}) + \mathbb{M}(m_0,f_2) \\ &\quad + \sum_{i=1}^{k-1}\mathbb{M}(m_i,f_{i+2}) - \sum_{i=1}^{k-1}\mathbb{M}(m_i,f_{i+1}) - \mathbb{M}(m_k,f_{k+1}). \end{aligned} \tag{24}$$

From

$$m_i f_i + q_i f_{i+1} = \frac{m_{i-1}}{w_i} p_i f_{i+2},$$

we have

$$\mathbb{M}(m_i, q_i f_{i+1}) = \mathbb{M}\Big(m_i, \frac{m_{i-1}}{w_i} p_i f_{i+2}\Big).$$

By Theorem 10, we have

$$\mathbb{M}(m_i,f_{i+1}) = \mathbb{M}(m_i,f_{i+2}) + \mathbb{M}\Big(m_i,\frac{m_{i-1}}{w_i}\Big) + \mathbb{M}(m_i,p_i) - \mathbb{M}(m_i,q_i).$$

And $m_0 = 1$, so $\mathbb{M}(m_0,f_2) = \emptyset$. Then we have (22). ∎

Remark 1 The components $\mathbb{M}(m_i,\frac{m_{i-1}}{w_i})$, $\mathbb{M}(m_i,p_i)$, and $\mathbb{M}(m_i,q_i)$ only involve polynomials in $K[x_1,x_2,\cdots,x_n]$. Note that by Lemma 1, the coefficient of q_i in x^t for $t>0$ is zero when $m_i = 0$. These components can also be decomposed into triangular sets recursively. This corollary is very important since it provides a method to eliminate the main variable x in f_i's, which simplifies the decomposition.

4.2 Disjoint and Square Free Decomposition

In this subsection, we will discuss how to decompose algebraic cycles in triangular forms into disjoint and square free ones.

In the following lemma, we will show how to decompose algebraic cycles in triangular forms into disjoint ones.

Lemma 14 *Let $f_1,f_2 \in K[x_1,x_2,\cdots,x_n,x]$ be primitive, $\deg(f_1,x) \geq \deg(f_2,x) > 0$, $\gcd(f_1,f_2) = 1$. And $h \in K[x_1,x_2,\cdots,x_n]$ be square free and primitive. There exists an algorithm to decompose $\mathbb{M}(h,f_1)$, $\mathbb{M}(h,f_2)$ into disjoint algebraic cycles in triangular forms.*

Proof From f_1,f_2, we can derive a sequence like (5) such that $\mathrm{Cont}(f_i,x) = 1$, $\gcd(m_i,g_i) = 1$, for $i = 1,2,\cdots,k$, $\gcd(h,g_i) = 1$ for $i = 1,2,\cdots,k-1$. Assume that $\gcd(h,m_i) = 1$ for $i = 1,2,\cdots,k$. Otherwise, we can split h such that the condition holds. Let $r = \gcd(h,g_k)$. If $r \in K$ and $\deg(f_{k+1},x) = 0$, it is obvious that $\mathbb{M}(h,f_1)$ and $\mathbb{M}(h,f_2)$ are disjoint. If $r \notin K$ and $h \nmid g_k$, we can split h into $r, r' = h/r$. Thus $r|g_k$. And we can continue to decompose $\mathbb{M}(r',f_1)$,

$\mathbb{M}(r', f_2)$. The last case is $h|g_k$. So we consider the case that there exists a k such that $h|g_k$. Denote $m_i\, f_i + q_i\, f_{i+1} = g_i\, f_{i+2}$ as formula F_i. Simplifying $m_k\, F_{k-1} - q_{k-1}\, F_k$, we have

$$m_k\, m_{k-1}\, f_{k-1} - (q_{k-1}\, q_k + m_k\, g_{k-1})\, f_{k+1} = -q_{k+1}\, g_k\, f_{k+2}.$$

Recursively, we have

$$m_k\, m_{k-1} \cdots m_2 f_2 - Q_2\, f_{k+1} = g_k\, R_2.$$

Since $h|g_k$, we have

$$(h, m_k\, m_{k-1} \cdots m_2 f_2) = (h, Q_2\, f_{k+1}).$$

Thus we have a decomposition for $\mathbb{M}(h, f_2)$ by Theorem 10:

$$\mathbb{M}(h, f_2) = \mathbb{M}(h, Q_2) + \mathbb{M}(h, f_{k+1}) - \sum_{i=2}^{k} \mathbb{M}(h, m_i). \tag{25}$$

Similarly, we have the following equation:

$$m_k\, m_{k-1} \cdots m_1 f_1 - Q_1\, f_{k+1} = g_k\, R_1$$

and decomposition:

$$\mathbb{M}(h, f_1) = \mathbb{M}(h, Q_1) + \mathbb{M}(h, f_{k+1}) - \sum_{i=1}^{k} \mathbb{M}(h, m_i). \tag{26}$$

From the property of Euclidean algorithm over algebraic extension (see [34, 35] and related work), $\mathbb{M}(h, Q_1)$ and $\mathbb{M}(h, Q_2)$ are disjoint. Recursively, we can ensure that $\mathbb{M}(h, f_{k+1})$ and $\mathbb{M}(h, Q_1)$, $\mathbb{M}(h, f_{k+1})$ and $\mathbb{M}(h, Q_2)$ are disjoint. We can decompose $\mathbb{M}(h, m_i)$ into disjoint algebraic cycles in triangular forms recursively. Since the degrees of f_1, f_2 are finite, the algorithm will terminate in the end. Thus we prove the lemma. ∎

Based on the lemma, we have an algorithm to find out the common components with dimension $n-1$ in $\mathbb{M}(h, f_1)$ and $\mathbb{M}(h, f_2)$.

Theorem 15 *Let $f, g \in K[x_1, x_2, \cdots, x_n]$ and $\gcd(f, g) = 1$. There exists an algorithm to decompose $\mathbb{M}(f, g)$ into square free and disjoint algebraic cycles in triangular forms as* (18).

Proof For the resulting algebraic cycles in Corollary 13, we can check whether any two of them, say $\mathbb{M}(p_1, q_1), \mathbb{M}(p_2, q_2)$, $r = \gcd(p_1, p_2)$ is a constant or not. If so, $\mathbb{M}(p_i, q_i), i = 1, 2$ are disjoint. If not, decompose them as below: $\mathbb{M}(p_i, q_i) = \mathbb{M}(r, q_i) + \mathbb{M}(p_i/r, q_i), i = 1, 2$. From Lemma 14, we can decompose $\mathbb{M}(r, q_1)$ and $\mathbb{M}(r, q_2)$ into disjoint algebraic cycles in triangular forms. Thus in the end we can decompose $\mathbb{M}(f, g)$ into disjoint algebraic cycles in triangular forms. Now we are going to show that each algebraic cycle $\mathbb{M}(p, q)$ can be made square free. Let $p \in K[x_1, x_2, \cdots, x_{n-1}], q \in K[x_1, x_2, \cdots, x_n]$. Still with the result in Lemma 14, we can decompose $\mathbb{M}(p, q)$ into lower degree algebraic cycles such that the non-vertical components of $\mathbb{M}(p, q)$ and $\mathbb{M}(p, \frac{\partial q}{\partial x_n})$ are disjoint as (26). And continuously decompose the non-vertical components of $\mathbb{M}(h, f_{k+1})$ in (26) into square free algebraic cycles. In a similar way, we can

decompose the algebraic cycles in triangular forms without the variable x_n into disjoint and square free ones. And the method mentioned below Lemma 11 can help us to decompose a triangular set into regular ones. So we can obtain a decomposition as (18) in the end. The decomposition will terminate since the number of the variables are finite. Thus we prove the theorem. ∎

We can also make the algebraic cycles square free at first and then make them disjoint in practice. The theorem allows us to count the multiplicities of the non-vertical components of $\mathbb{M}(f, g)$.

We do not write an algorithm for decomposing two polynomials system. The algorithm is similar to that of two bivariate polynomial system, which will be given in the next section. Here we will give an illustrative example.

Example 1 Consider the system $[f_1, f_2] = [x^3 + {x_1}^2 + {x_2}^2 - 1, x_1\, x^2 - x_2\, x + 1]$ using the result in Corollary 13, we have

$$\begin{aligned} f_3 &= \left(-x_1 + {x_2}^2\right) x + {x_1}^4 + {x_1}^2{x_2}^2 - {x_1}^2 - x_2, \\ f_4 &= 1 - 3\,{x_1}^3x_2 - 3\,x_1\,{x_2}^3 + 3\,x_1\,x_2 + {x_2}^3{x_1}^2 + {x_2}^5 - {x_2}^3 + {x_1}^7 + 2\,{x_1}^5{x_2}^2 \\ &\quad -2\,{x_1}^5 + {x_1}^3{x_2}^4 - 2\,{x_1}^3{x_2}^2 + {x_1}^3. \end{aligned}$$

$m_1 = {x_1}^2, q_1 = x_1\, x + x_2, m_0 = w_1 = p_1 = 1, m_2 = (-x_1 + {x_2}^2)^2, q_2 = -{x_1}^2x + x_1{x_2}^2x + 2\,x_1x_2 - {x_2}^3 - {x_1}^5 - {x_1}^3{x_2}^2 + {x_1}^3$, $w_2 = p_2 = 1$. By Corollary 13, we have the following decomposition.

$$\mathbb{M}(f_1, f_2) = \mathbb{M}(f_4, f_3) + \mathbb{M}(m_1, q_1) - \mathbb{M}(m_2, f_3).$$

Simplifying the algebraic cycles, using Theorem 10, we have

$$\begin{aligned} \mathbb{M}(m_1, q_1) &= 2\,\mathbb{M}(x_1, x_1\, x + x_2) = 2\,\mathbb{M}(x_1, x_2), \\ \mathbb{M}(m_2, f_3) &= 2\,\mathbb{M}(x_2^2 - x_1, {x_1}^4 + {x_1}^2{x_2}^2 - {x_1}^2 - x_2) \\ &= 2\,\mathbb{M}(x_2^2 - x_1, x_1^4 + x_1^3 - x_1^2 - x_2) \\ &= 2\,\mathbb{M}(x_1, x_2) + 2\,\mathbb{M}(x_1 - 1, x_2 - 1) + 2\,\mathbb{M}(h_1, h_2), \end{aligned}$$

where $h_1 = {x_1}^6 + 3\,{x_1}^5 + 2\,{x_1}^4 + {x_1}^2 + x_1 + 1$, $h_2 = x_2 - {x_1}^4 - {x_1}^3 + x_1^2$. Both $\mathbb{M}(m_1, q_1)$ and $\mathbb{M}(m_2, f_3)$ have an algebraic cycle $\mathbb{M}(x_1, x_2)$ with multiplicity 2. With the method in Theorem 15, we can find that $\mathbb{M}(x_1 - 1, x_2 - 1)$, $\mathbb{M}(h_1, h_2)$, and $\mathbb{M}(f_4, f_3)$ are square free and disjoint. So we have the following disjoint decomposition for $\mathbb{M}(f_1, f_2)$:

$$\mathbb{M}(f_1, f_2) = \mathbb{M}(f_4, f_3) - 2\mathbb{M}(x_1 - 1, x_2 - 1) - 2\mathbb{M}(h_1, h_2).$$

Note that the component with negative multiplicity cannot be removed if using the triangular form. The last two algebraic cycles are zero-dimensional in $\mathbb{C}^2$, but they are 1-dimensional in $\mathbb{C}^3$. It is clear that $\mathbb{M}(f_4, f_3)$ contains the vertical lines defined by $\mathbb{M}(x_1 - 1, x_2 - 1), \mathbb{M}(h_1, h_2)$.

From this example, we can find that we can use our result to study the intersection of two algebraic hypersurfaces, for example, algebraic space curves. It is our future work.

5 Multiplicity Preserving Decomposition of Two Bivariate Polynomials

In this section, we will consider the triangular set decomposition of a zero-dimensional bivariate polynomial system with two polynomials, that is, $\Sigma = \{f, g\} \subset K[x, y]$. The method provided here is complete for a zero-dimensional bivariate polynomial system with two polynomials.

5.1 The Algorithm

In the bivariate case, we have the following triangular set decomposition.

Lemma 16 *Using the similar notations as Corollary* 6, *if* $\gcd(f_1, f_2) = 1$, *we have*

$$\mathbb{M}(f_1, f_2) = \mathbb{M}(f_{k+1}, f_{k+2}) + \sum_{i=1}^{k} \mathbb{M}(p_i, f_{i+1}) - \sum_{i=1}^{k} \mathbb{M}(w_i, f_{i+1}) - \mathbb{M}(m_k, f_{k+1}). \tag{27}$$

Proof The lemma is a consequence of Corollary 13. Note that $\mathbb{M}(m_i, \frac{m_{i-1}}{w_i}) = \mathbb{M}(m_i, p_i) = \mathbb{M}(m_i, q_i) = \emptyset$ since $\gcd(m_i, p_i)$, $\gcd(m_i, \frac{m_{i-1}}{w_i})$, and $\gcd(m_i, q_i)$ are constants. ∎

The following corollary is useful.

Corollary 17 *If* $w_i (1 \le i \le k)$ *are constants and* $f_{k+1} = l_1(x)\, y^t + l_0(x)$ *for* $t > 0$ *and* $l_0, l_1 \in K[x]$ *in* (27), *then we have*

$$\mathbb{M}(f_1, f_2) = \mathbb{M}(f_{k+1}, f_{k+2}) + \sum_{i=1}^{k} \mathbb{M}(p_i, f_{i+1}). \tag{28}$$

Furthermore, if $p_i (1 \le i \le k)$ *are constants, we have*

$$\mathbb{M}(f_1, f_2) = \mathbb{M}(f_{k+1}, f_{k+2}). \tag{29}$$

Proof Since $f_{k+1} = l_1(x)\, y^t + l_0(x)$ and $\mathrm{Cont}(f_{k+1}, y) = 1$, $\mathbb{M}(m_k, f_{k+1}) = \emptyset$. Note that m_k is a factor of l_1^n for some positive integer n. Thus $\mathbb{M}(m_0, f_2) = \emptyset$, $\mathbb{M}(m_k, f_{k+1}) = \emptyset$. So from (27), we have (28). If $p_i = 1$, (29) is a consequence of (28). ∎

Lemma 16 gives a multiplicity-preserving triangular decomposition of a bivariate polynomial system. But there exist some triangular sets with negative multiplicities. A special property of bivariate polynomials is that there is no vertical components, that is, the zero set defined by the coefficients of a bivariate primitive polynomial in the main variable is empty. Thus we can remove the negative components for bivariate polynomial systems. The following result gives an algorithm to remove the triangular sets with negative multiplicities.

Theorem 18 *There exists an algorithm to decompose a zero-dimensional bivariate polynomial system* $\{f_1, f_2\} \subset K[x, y]$ *into a set of square free and disjoint triangular sets, i.e.,*

$$\mathbb{M}(f_1, f_2) = \sum_{i=1}^{N} m_i\, \mathbb{M}(g_i, h_i), \tag{30}$$

such that $m_i > 0$, $M(g_i, h_i)$ *is square free,* $\mathbb{M}(g_i, h_i) \cap \mathbb{M}(g_j, h_j) = \emptyset, 1 \le i \ne j \le N$, *where* $g_i \in K[x], h_i \in K[x, y]$.

Proof In the case $f_1 = h_1 f_1', f_2 = h_2 f_2'$ having factors in $K[x]$ but $\gcd(f_1, f_2) = 1$, where $h_i = \mathrm{Cont}(f_i, y), i = 1, 2$, we have

$$\mathbb{M}(f_1, f_2) = \mathbb{M}(h_1, f_2') + \mathbb{M}(f_1', h_2) + \mathbb{M}(f_1', f_2'). \tag{31}$$

Since $\gcd(h_1 f_1', h_2 f_2') = 1$, $\mathbb{M}(h_1, h_2) = \emptyset$.

By Theorem 15, we can decompose $\mathbb{M}(h_1, f_2'), \mathbb{M}(f_1', h_2)$, and $\mathbb{M}(f_1', f_2')$ into a square free and disjoint algebraic cycles in triangular forms. ∎

Remark 2 The method in [36] can be used to decompose a triangular sets into irreducible ones. Thus we can have a stronger decomposition. We can simplify the computation by the following techniques. For some $\mathbb{M}(g, h)$ in the triangular form, ensure that h is unchanged after modulo g. Theorem 10 can be used to simplify the algebraic cycles (into lower degree).

We will give a multiplicity-preserving algorithm to decompose a bivariate polynomial system into zeros in triangular forms as well as their multiplicities based on the theory above. At first, we give the following basic subalgorithm below.

Algorithm 1 DisjointDecompositon$(S, t_1\mathbb{M}(h, F_{t+1}), t_2\mathbb{M}(h, F_{t+2}))$, where $S = \{m_i, F_i, q_i, g_i,$ for $i = 1, 2, \cdots, t\} \subset K[x, y]$, $m_i F_i + q_i F_{i+1} = g_i F_{i+2}$ satisfying the condition as (5), and $\gcd(h, m_i) = \gcd(h, g_i) = 1$ for $i = 1, 2, \cdots, t$. $t = 0$ if S is an empty set. This algorithm is to decompose $t_1\mathbb{M}(h, F_1) + t_2\mathbb{M}(h, F_2)$ ($t_1, t_2 \in \mathbb{Z}$ are integers and may be negative) into disjoint algebraic cycles in triangular forms.

Input $S, h, F_{t+1}, F_{t+2}, t_1, t_2$ as mentioned above.

Output a group of algebraic cycles in triangular forms $\mathscr{P} = \{l_i\mathbb{M}(g_i(x), h_i(x, y)),\ i = 1, 2, \cdots, n\}$ such that

- $\mathbb{M}(g_i(x), h_i(x, y)), i = 1, 2, \cdots, n$ are disjoint.
- $t_1\mathbb{M}(h, F_1) + t_2\mathbb{M}(h, F_2) = \sum_{i=1}^{n} l_i\,\mathbb{M}(g_i, h_i)$.

1) $\mathbb{M}_o = \emptyset$, $\{f_1, f_2\} = \{F_{t+1}, F_{t+2}\}$ such that $\deg(f_1, y) \geq \deg(f_2, y)$.

2) While $\deg(f_2, y) > 0$, do

   - Let $r = \gcd(l, h)$, where l is the leading coefficient of f_2 in y. If $r \notin K$, $\mathbb{M}_o \leftarrow$ DisjointDecompositon$(S, t_1\,\mathbb{M}(r, f_1), t_2\,\mathbb{M}(r, \mathrm{Prem(f_2, r, x)}))$, where "$A \leftarrow \{B\}$" means for each element B_1 of B, do the disjoint decomposition of B_1 and one element A_1 of A, for the resulting elements of DisjointDecompositon$(\emptyset, B_1, A_1)$ from B_1, do the disjoint decomposition for them and one element in $A = A \setminus A_1$, respectively. Do the similar operation until A is empty, and still denote all the resulting elements as A. And $h = h/r$.
   - By pseudo-division, we have $m\,f_1 + q\,f_2 = f_3$ and $g = \mathrm{Cont}(f_3, y)$. $f_3 = \frac{f_3}{g}, v = \gcd(m, g)$, $m = \frac{m}{v}, g = \frac{g}{v}$. If $f_3 = 1$, $f_3 = g, g = 1$. Else, $S \leftarrow \{m, f_1, q, g\}$.
   - Let $s = \gcd(g, h)$. If $h \nmid g$ and $s \notin K$,
     $\mathbb{M}_o \leftarrow$ DisjointDecompositon$(S, t_1\mathbb{M}(h/s, f_2), t_2\mathbb{M}(h/s, f_3))$. And $h = s$.

- If $h \mid g$, we have two formulae as (25), (26), where $\mathbb{M}(h, m_i) = \emptyset$. $\mathbb{M}_o \leftarrow \{t_1\mathbb{M}(h, Q_1), t_2\mathbb{M}(h, Q_2), (t_1 + t_2)\mathbb{M}(h, f_{k+1})\}$. $f_3 = 0$.
- $f_1 = f_2, f_2 = f_3$.

3) If $\deg(f_2, y) = 0$ and f_2 is not a constant, then: $\mathbb{M}_o \leftarrow \{t_1\mathbb{M}(h, F_1), t_2\mathbb{M}(h, F_2)\}$.

4) Output $\mathbb{M}_o$.

Proof The termination and correctness of the algorithm are guaranteed by Lemma 14. ∎

In order to derive a square free decomposition for a triangular set $\{h, f\}$, where $h \in K[x], f \in K[x, y]$, we can ensure that $\{h, f\}, \{h, \frac{\partial f}{\partial y}\}$ are disjoint at first. Thus we have a decomposition for $\{h, f\}$. And then decompose the non-square free part recursively with the same steps. In the end, we can obtain a square free and disjoint decomposition for $\{h, f\}$. We denote the operation on $\{h, f\}$ as SqrfreeDecompositon($t\,\mathbb{M}(h, f)$) in the rest of the paper, where $t \in \mathbb{Z}$.

Based on the subalgorithms above, we have the main algorithm, where "$A \leftarrow \{B\}$" has the same meaning as in Algorithm 5.1, and we also require the triangular sets added into A to be regular, that is, do a regular decomposition for these triangular sets before adding into A.

Algorithm 2

Input a zero-dimensional bivariate polynomial system $\mathscr{P}_1 = \{F_1(x, y), F_2(x, y)\} \in K[x, y]$.

Output a group of algebraic cycles in triangular forms $\mathscr{P} = \{m_i\,\mathbb{M}(g_i(x), h_i(x, y)),\ i = 1, 2, \cdots, n\}$ such that $\mathbb{M}(F_1, F_2) = \Sigma_{i=1}^{n}\, m_i\,\mathbb{M}(g_i, h_i)$, $m_i > 0$ and $\{g_i, h_i\}$ is irreducible and regular.

1) $\mathbb{M}_o = \emptyset$. $\{f_1, f_2\} = \{F_1, F_2\}$ such that $\deg(f_1, y) \geq \deg(f_2, y)$.

2) Let $h_i = \mathrm{Cont}(f_i, y), f_i = f_i/h_i, i = 1, 2$. $\mathbb{M}_o \leftarrow \{\mathbb{M}(h_1, f_2), \mathbb{M}(h_2, f_1)\}$.

3) Let $m_0 = 1$. While $\deg(f_2, y) > 0$, do

- By pseudo-division, we have $m_1 f_1 + q_1 f_2 = f_3$ and $h = \mathrm{Cont}(f_3, y)$. $f_3 = \frac{f_3}{h}, v = \gcd(m_1, h)$, $m_1 = \frac{m_1}{v}, h = \frac{h}{v}$. Let $q = \gcd(m_0, h)$, $w = \frac{m_0}{q}$, $p = \frac{h}{q}$. If $f_3 = 1$, $f_3 = p, p = 1$. If $p \notin K$, $\mathbb{M}_o \leftarrow \{\mathbb{M}(p, f_2)\}$. If $w \notin K$, $\mathbb{M}_o \leftarrow \{-\mathbb{M}(w, f_2)\}$.
- $f_1 = f_2, f_2 = f_3, m_0 = m_1$.

4) If $\deg(f_1, y) > 1$, $\mathbb{M}_o \leftarrow \{-\mathbb{M}(m_0, f_1)\}$.

5) Let $\mathbb{M}'_o = \emptyset$. For any element A of $\mathbb{M}_o$, $\mathbb{M}'_o \leftarrow$ SqrfreeDecompositon(A).

6) Output $\mathbb{M}'_o$.

Proof The termination of the algorithm is clear since the degrees of f_1 and f_2 are finite. The correctness of the algorithm is guaranteed by Theorem 18 and Lemma 16. ∎

Remark 3 $-\mathbb{M}(w, f_2)$ and $-\mathbb{M}(m_0, f_1)$ in Steps 3) and 4) mean the multiplicities are negative.

Example 2 Let $\mathcal{C}$ be the curve defined by

$$f = 2\,y^4 - 3\,y^2x + x^2 - 2\,x^3 + x^4.$$

We will compute the y-critical points ($f = \frac{\partial f}{\partial y} = 0$) of $\mathcal{C}$.

$$f_y = \frac{\partial f}{\partial y} = 8\,y^3 - 6\,yx.$$

Delete the content 2, $f_y = \frac{f_y}{2}$. In the following, we will solve the system $\Sigma = \{f, f_y\}$. Following our algorithm, we have

$$m_1\,f + q_1\,f_y = p_1\,f_3,$$

where $m_1 = 4, p_1 = x, q_1 = -y, f_3 = -3\,y^2 + 2\,x - 4\,x^2 + 2\,x^3$. Thus we have $\mathbb{M}_o = \{\mathbb{M}(p_1, f_y)\}$. Simplifying $\mathbb{M}(p_1, f_y)$, we have $\mathbb{M}(x, y^3)$. Taking a square free decomposition for $\mathbb{M}_o$, we have $\mathbb{M}_o = \{\mathbb{M}(x, y) + \mathbb{M}(x, y) + \mathbb{M}(x, y)\}$. We do not know the three elements in $\mathbb{M}_o$ are the same or not until we use Algorithm 5.1. So we have $\mathbb{M}_o = \{3\,\mathbb{M}(x, y)\}$. Continuing to compute with the algorithm, we have

$$m_2\,f_y + q_2\,f_3 = p_2\,f_4,$$

where $m_2 = 3, q_2 = 4\,y, p_2 = x\,(-1 - 16\,x + 8\,x^2), f_4 = y$. Note that here $w_2 = 4$. We ignore it since it is a constant. We have a new algebraic cycle $\mathbb{M}(p_2, f_3)$. We would like to illustrate the decomposition of $\mathbb{M}(p_2, f_3)$, which is not square free. Note that $\frac{\partial f_3}{\partial y} = -6\,y$, denote its primitive part y as f_3'. Then we have

$$1\,f_3 - 3\,y f_3' = 2\,x\,(x-1)^2.$$

We can find that $p_2 \nmid r = 2\,x\,(x-1)^2$ but $\gcd(p_2, r) = x$. So we can split $\mathbb{M}(p_2, f_3)$:

$$\mathbb{M}(p_2, f_3) = \mathbb{M}(x, f_3) + \mathbb{M}(-1 - 16\,x + 8\,x^2, f_3).$$

Thus by disjoint and square free decomposition, we have

$$\mathbb{M}(x, f_3) = \mathbb{M}(x, -3\,y) + \mathbb{M}(x, y) - \mathbb{M}(x, 1) = 2\,\mathbb{M}(x, y).$$

Since f_3 modulo $-1 - 16\,x + 8\,x^2$ equals $48\,(-4\,y^2 + 3\,x)$,

$$\mathbb{M}(-1 - 16\,x + 8\,x^2, f_3) = \mathbb{M}(-1 - 16\,x + 8\,x^2, -4\,y^2 + 3\,x).$$

Thus we have

$$\mathbb{M}(p_2, f_3) = 2\mathbb{M}(x, y) + \mathbb{M}(-1 - 16\,x + 8\,x^2, -4\,y^2 + 3\,x).$$

Adding these algebraic cycles into $\mathbb{M}_o$, we have

$$\mathbb{M}_o = 5\mathbb{M}(x, y) + \mathbb{M}(-1 - 16\,x + 8\,x^2, -4\,y^2 + 3\,x).$$

Continuing the computation, we have

$$m_3\, f_3 + q_3\, f_4 = f_5,$$

where $m_3 = 1, q_3 = 3\,y, f_5 = 2\,x\,(x-1)^2$. Similarly, we ignore $w_3 = 3$. We have an algebraic cycle $\mathbb{M}(f_5, f_4)$ which should be added into $\mathbb{M}_o$. Decomposing it, we have

$$\mathbb{M}(f_5, f_4) = \mathbb{M}(x\,(x-1), y) + \mathbb{M}(x-1, y) = \mathbb{M}(x, y) + 2\,\mathbb{M}(x-1, y).$$

Adding them into $\mathbb{M}_o$ by Algorithm 5.1, we have the disjoint and square free multiplicity-preserving decomposition for $\mathbb{M}(f, f_y)$:

$$\mathbb{M}(f, f_y) = 6\,\mathbb{M}(x, y) + 2\,\mathbb{M}(x-1, y) + \mathbb{M}(-1 - 16\,x + 8\,x^2, -4\,y^2 + 3\,x).$$

We find that $\mathbb{M}(x, y)$ and $\mathbb{M}(x-1, y)$ are zeros with multiplicities 6, 2, respectively. And the other zeros are with multiplicity 1.

5.2 Complexity Analysis

Now we will consider the complexity of our method under the condition of Lemma 16. Then we can directly obtain the complexity under Corollary 17. We consider this case due to two reasons. First, it is usually the case for almost all zero-dimensional bivariate polynomial systems with two polynomials. Second, it is easy to see that the bottleneck computation in our algorithm is to compute the primitive polynomial remainder sequence of f_1 and f_2. Therefore, Corollary 8 represents the complexity of the bottleneck step of the algorithm. So the result is interesting.

At first, we need to introduce some notations, which can be found in [37]. Let $\mathcal{L}(f)$ bound the bitsize of the coefficients of $f \in K[x, y]$ (including a bit for the sign). We assume $\lg(\deg(f)) = \mathcal{O}(\mathcal{L}(f))$. For $a \in \mathbb{Q}$, $\mathcal{L}(a)$ is the maximum bitsize of a's numerator and denominator. Let $M(\tau)$ denote the bit complexity of multiplying two integers of size τ, and $M(d, \tau)$ the complexity of multiplying two univariate polynomials of degrees $\leq d$ and coefficient bitsize $\leq \tau$. Using FFT, $M(\tau) = \widetilde{\mathcal{O}}_B(\tau)$ and $M(d, \tau) = \widetilde{\mathcal{O}}_B(d\tau)$.

Lemma 19 (see [37, 38]) *Let $f, g \in \mathbb{Z}[x]$, $\deg(f), \deg(g) \leq n$, and $\mathcal{L}(f), \mathcal{L}(g) \leq \tau$. We can compute* $\gcd(f, g)$ *in $\widetilde{\mathcal{O}}_B(n^2\tau)$.*

Lemma 20 (see [37, 38]) *Let $f, g \in \mathbb{Z}[x, y]$, $\deg(f), \deg(g) \leq n$, and $\mathcal{L}(f), \mathcal{L}(g) \leq \tau$. We can compute the subresultant sequence of f and g in $\widetilde{\mathcal{O}}_B(n^6\tau)$.*

Theorem 21 *Let $K = \mathbb{Z}$. We can decompose a zero-dimensional bivariate system with two polynomials into multiplicity-preserving triangular sets as Lemma* 16 *in $\widetilde{\mathcal{O}}_B(n^7\tau)$.*

Proof We can compute a subresultant sequence of f and g at first. It can be computed in $\widetilde{\mathcal{O}}_B(n^6\tau)$ by Lemma 20. Then we simplify each pseudo-division step to derive (7) from the highest degree of the sequence in y to the lowest degree. Let $\{F_1, F_2, \cdots, F_{k+2}\}$ be the subresultant sequence of f and g. We need only consider the case of regular subresultant sequence since we can find below that the complexity of the regular case also bounds the

degenerate case. Consider the formula

$$l_{i+1}^2 F_i + Q_i F_{i+1} = l_i^2 F_{i+2}. \tag{32}$$

Assume that we have computed the contents of F_i and F_{i+1}, say r_i, r_{i+1}. F_1, F_2 are f_1, f_2. And the contents of f or g can be computed in $\widetilde{\mathcal{O}}_B(n^3\tau)$ by Lemma 19, which can be ignored comparing to $\widetilde{\mathcal{O}}_B(n^6\tau)$. For each F_i, it is well known that $\deg(F_i) \le n^2, \mathcal{L}(F_i) = \mathcal{O}(n\tau)$ (for reference see [37]). And $\deg(F_i, y) \le n-1$ for $i \ge 3$. Thus for any coefficient of F_i, say $h \in \mathbb{Z}[x]$, we have $\deg(h) \le n^2, \mathcal{L}(h) = \mathcal{O}(n\tau)$. So to compute the content of F_i with $\deg(F_i, y) = m$, we need to compute at most m gcd each in $\widetilde{\mathcal{O}}_B(n^5\tau)$. Let $r_{i+2} = \mathrm{Cont}(F_{i+2}, y)$. In order to derive (7), we need to delete $\gcd(l_{i+1}^2 F_i, Q_i F_{i+1}, l_i^2 F_{i+2})$ from the two sides of (32). So we need to bound $\gcd(l_{i+1}^2\, r_i, l_i^2\, r_{i+2})$. Note that $\deg(s) \le n^2, \mathcal{L}(s) = \mathcal{O}(n\tau)$ holds for $s = l_i$ or $s = l_{i+1}$ and we can not optimize the degree of l_{k+1}. But we can compute $r = \gcd(l_i, l_{i+1})$, which is bounded by $\widetilde{\mathcal{O}}_B(n^5\tau)$. And $\gcd((\frac{l_i}{r})^2, r_i)$ can be bounded by $2\,\widetilde{\mathcal{O}}_B(n^5\tau)$ as below. We can compute $w = \gcd(\frac{l_i}{r}, r_{i+2})$, and then $\gcd(\frac{l_i}{r}, \frac{r_{i+2}}{w})$. Similarly, $\gcd((\frac{l_{i+1}}{r})^2, r_i)$ is bounded by $2\,\widetilde{\mathcal{O}}_B(n^5\tau)$. So to delete $\gcd(l_{i+1}^2 F_i, Q_i F_{i+1}, l_i^2 F_{i+2})$ from (32) for $\deg(F_i, y) = m$, we need $(m+5)\widetilde{\mathcal{O}}_B(n^5\tau)$. Note that the computations of those divisions can be ignored comparing to the gcd's computation. Then we can decide m_i, g_i in (5). In order to derive (7), we only need to compute $\gcd(m_{i-1}, g_i)$ and two divisions. The computation of $l = \gcd(m_{i-1}, g_i)$ can be bounded by $9\,\widetilde{\mathcal{O}}_B(n^5\tau)$. In fact, from the analysis above, both m_{i-1} and g_i can be split into three factors each bounded by the degree n^2 and the coefficients bitsize $\mathcal{O}(n\tau)$, corresponding to $l_i^2\, r_{i-1}$ and $l_i^2\, r_{i+2}$. Denoted as $m_{i-1} = u_1\, u_2\, u_3$, $g_i = v_1\, v_2\, v_3$. The computation of $e_1 = \gcd(u_1, v_1)$ is bounded by $\widetilde{\mathcal{O}}_B(n^5\tau)$. And the computations of $e_2 = \gcd(\frac{u_1}{e_1}, v_2)$ and $e_3 = \gcd(\frac{u_1}{e_1\, e_2}, v_3)$ are also bounded by $\widetilde{\mathcal{O}}_B(n^5\tau)$. In the end, we can find that the computations of $w_i = \frac{m_{i-1}}{l}$ and $p_i = \frac{g_i}{l}$ are bounded by $9\,\widetilde{\mathcal{O}}_B(n^5\tau)$. Thus in each pseudo-division step for $\deg(F_i, y) = m$ to obtain (7), we need $(m+14)\widetilde{\mathcal{O}}_B(n^5\tau)$. When m changes from n to 1, we can bound it by $\frac{1}{2}\,n^2 + \frac{29}{2}\,n\,\widetilde{\mathcal{O}}_B(n^5\tau)$, that is, $\widetilde{\mathcal{O}}_B(n^7\tau)$. Then the total complexity is $\widetilde{\mathcal{O}}_B(n^7\tau)$. ∎

The following corollary is obvious.

Corollary 22 *Let $K = \mathbb{Z}$. We can decompose a zero-dimensional bivariate system with two polynomials under the conditions of Corollary* 17 *into positive algebraic cycles in triangular forms in $\widetilde{\mathcal{O}}_B(n^7\tau)$.*

For many $f, g \in K[x, y]$, the last two elements of the subresultant sequence F_{k+1}, F_{k+2} form a multiplicity-preserving triangular decomposition of f, g. Thus, we can compute the decomposition in $\widetilde{\mathcal{O}}_B(n^6\tau)$.

5.3 Implementation and Comparison

We implemented our algorithm in Maple. We compare the computing times of our method with several other related methods. One is the regular chains method[7, 14] (package RegularChains in Maple 13), one is characteristic set method in Epsilon[39], the other is a package Wsolve (see [40]). All the results are collected on a PC with 2.83 GHz quad CPU, 3.37 GB memory, and running Microsoft Windows XP. We use Maple 13 in the experiments.

We run 100 examples in each case and compute their average computing time in seconds. The results are in Tables 1–3. The timings in the tables are in seconds. Here MPTD means the method provided in this paper, RC means the regular chains method of the function "Triangularize", CS means the characteristic set method ("charsets") in Epsilon, and WS means Wsolve method. The first column represents the methods. "-" means out of memory or out of time (half an hour). In Table 1, we take random dense polynomials with coefficients bounded by $[-100, 100]$ for each example.

Table 1 Timings for different methods on the examples with simple roots

$[\deg(f), \deg(g)]$	[7, 5]	[9,7]	[13, 11]	[19, 17]	[20,19]	[25,23]	[33,31]
MPTD	0.021	0.080	1.446	21.024	26.818	152.846	834.740
RC	0.062	0.141	1.451	18.073	22.184	126.325	618.865
CS	0.795	19.305	-	-	-	-	-
WS	3.324	396.870	-	-	-	-	-

In order to study the influence of multiple zeros to the methods, we test second group of examples. For these examples, we take $h(x, y, z)$ as a random dense polynomial with bounded coefficients and bounded total degree. And set f be the discriminant of h w.r.t. z, g the derivative of f w.r.t. y and ensure that $\{f, g\}$ is zero-dimensional. Then we decompose $\{f, g\}$ into triangular sets with the methods above. "Ceoff. bound (10^m)" means the coefficients of f and g are bounded by 10^m. We set $\deg(h) = d = 3, 4, 5$ and the coefficients of h are bounded by 10. Timings for these examples are given in Table 2.

Table 2 Timings for different methods on the examples with multiple roots

$\deg(h)$	$[\deg(f), \deg(g)]$	Ceoff. bound (10^m)	MPTD	RC	CS	WS
3	[6, 5]	7	0.028	0.154	0.854	4.197
4	[12,11]	11	2.664	10.790	-	-
5	[20,19]	15	104.949	477.142	-	-

In order to study the influence of the coefficients of f, g on the timings, we take the third group of examples, where the total degree of f and g are unchanged, $\deg(f) = 20, \deg(g) = \deg(\frac{\partial f}{\partial y}) = 19$. We generate f, g here in the same way as that in Table 2. The total degrees of h's are set to be 5. And the coefficients of h's are bounded by $i = 10, 4, 3, 2, 1$ respectively. Thus the coefficients of f, g are bounded by different numbers. Testing these examples for MPTD and RC, we have Table 3.

Table 3 Timings for examples with same type but different coefficient ranges

Ceoff. range of h	$-10..10$	$-4..4$	$-3..3$	$-2..2$	$-1..1$
Ceoff. bound (10^m)	15	12	11	10	8
MPTD	104.949	73.673	65.484	50.561	39.111
RC	477.142	317.093	287.366	212.213	163.102

We need to mention that only MPTD can compute the multiplicities of the zeros of the bivariate polynomial system. MPTD is only for bivariate polynomial system but other methods work for general systems. Note that MPTD can give a multiplicity-preserving triangular decomposition for systems with two multivariate polynomials.

We can conclude from the tables that MPTD are always faster than RC, CS, and WS for systems with many multiple roots. MPTD is a little faster than RC for systems without multiple roots and with low degree. It is a little slower than RC for systems without multiple roots and with high degree. The bitsizes of the coefficients of the systems influence much for both MPTD and RC.

6 Conclusion

We present an algorithm to decompose the zero set for a polynomial system consisting of two polynomials into algebraic cycles in triangular forms. Different from the existing methods for triangular decomposition, our method preserves the multiplicity of the zeros or components of the systems based on the concept of algebraic cycles. We can obtain the decomposition by computing a primitive polynomial remainder sequence once. We implement the method for bivariate polynomial systems. We will extend the method to the systems with more polynomials in the future.

References

[1] Ritt J, *Differential Algebra*, New York, Dover Publications, 1966.

[2] Wu W T, Basic principles of mechanical theorem-proving in elementary geometries, *Journal Automated Reasoning*, 1986, **2**: 221–252.

[3] Wu W T, *Basic Principle of Mechanical Theorem Proving in Geometries*, Science Press, Beijing, 1984; Springer, Wien, 1994 (in Chinese).

[4] Aubry P, Lazard D, and Moreno Maza M, On the theories of triangular sets, *J. Symb. Comput.*, 1999, **28**(1–2): 105–124.

[5] Chen C, Golubitsky O, Lemaire F, Moreno Maza M, and Pan W, Comprehensive triangular decomposition, *CASC*, 2007, 73–101.

[6] Chou S C and Gao X S, Ritt-Wu's decomposition algorithm and geometry theorem proving, *CADE*'10, ed. by Stickel M E, Lecture Notes in Computer Science, Springer-Verlag, 1990, **449**: 207–220.

[7] Dahan X, Moreno Maza M, Schost É, Wu W, and Xie Y, Lifting techniques for triangular decompositions, *Proceedings of the* 2005 *International Symposium on Sympolic and Algebraic Computation, ACM*, Beijing, 2005.

[8] Gao X S and Chou S C, On the dimension of an arbitrary ascending chain, *Chinese Sci. Bull.*, 1993, **38**: 799–804.

[9] Gerdt V P and Blinkov Y A, Involutive bases of polynomial ideals, *Mathematics and Computers in Simulation*, 1998, **45**(5–6): 519–541.

[10] Golubitsky O, Kondratieva M, Ovchinnikov A, and Szanto A, A bound for orders in differential Nullstellensatz. *Journal of Algebra*, 2009, **322**: 3852–3877.

[11] Hubert E, Notes on triangular sets and triangulation-decomposition algorithms I: Polynomial systems, Chapter of Symbolic and Numerical Scientific Computations Edited by Langer U and Winkler F, Lecture Notes in Computer Science, Springer-Verlag Heidelberg, 2003, **2630**: 1–39.

[12] Lazard D, A new method for solving algebraic systems of positive dimension, *Discrete Appl. Math.*, 1991, **33**: 147–160.

[13] Li X, Moreno Maza M, and Schost É, Fast arithmetic for triangular sets: From theory to practice, *Proceedings of the* 2007 *International Symposium on Sympolic and Algebraic Computation, ACM*, 2007, 269–276.

[14] Moreno Maza M, On triangular decompositions of algebraic varieties, *MEGA*-2000 *Conference*, Bath, England, 2000.

[15] Kalkbrener M, A generalized euclidean algorithm for computing triangular representations of algebraic varieties, *J. Symb. Comput.*, 1993, **15**(2): 143–167.

[16] Kalkbrener M, Primitive polynomial remainder sequence in elimination theory, *Applicable Algebra in Engineering, Communication and Computing*, 1995, **6**: 65–79.

[17] Kalkbrener M, Algorithmic properties of polynomial rings, *J. Symb. Comput.*, 1998, **26**(5): 525–581.

[18] Wang D, Computing triangular systems and regular systems, *J. Symb. Comput.*, 2000, **30**(2): 221–236.

[19] Wu W T, On a linear equations method of non-linear polynomial equations-solving, *Systems Science and Mathematical Sciences*, 1993, **6**(1): 1–12.

[20] Yang L and Zhang J, Searching dependency between algebraic equations: An algorithm applied to automated reasoning, *Artificial Intelligence in Mathematics*, Oxford University Press, 1994, 147–156.

[21] Lazard D, Solving zero-dimensional algebraic systems, *J. Symb. Comput.*, 1992, **13**: 117–131.

[22] Li B H, A method to solve algebraic equations up to multiplicities via Ritt-Wu's characteristic sets, *Acta Analysis Functionalis Applicata*, 2003, **5**(3): 98–109.

[23] Li Y, Xia B, and Zhang Z, Zero decomposition with multiplicity of zero-dimensional polynomial systems (in Chinese), The Third Computer Mathematics Conference of China, Shanghai, China, October, 2010, 19–22.

[24] Bates D, Peterson C, and Sommese A J, A numerical-symbolic algorithm for computing the multiplicity of a component of an algebraic set, *Journal of Complexity*, 2006, **22**(4): 475–489.

[25] Dayton B and Zeng Z, Computing the multiplicity structure in solving polynomial systems, *Proceedings of the* 2005 *International Symposium on Sympolic and Algebraic Computation, ACM*, 2005.

[26] Lazard D, Ideal bases and primary decomposition: Case of two variables, *J. Symb. Comput.*, 1985, **1**: 261–270.

[27] Brown W S, The subresultant PRS algorithm, *ACM Trans. on Mathematical Software*, 1978, **4**: 237–249.

[28] Hodge W V D and Pedoe D, *Methods of Algebraic Geometry*, Volume II, University Press Cambridge, ISBN 0 521 46901 5 paperback, 1994.

[29] Gel'fand I M, Kapranov M, and Zelevinsky A. *Discriminants, Resultants and Multidimensional Determinants*, Boston, Birkhäuser, 1994.

[30] Cox D A, Little J, and O'Shea D, *Using Algebraic Geometry*, Springer, Second Edition, 2004.

[31] Hodge W V D and Pedoe D, Methods of algebraic geometry, Volume I, University Press Cambridge, ISBN 0 521 469007 4 paperback, 1994.

[32] Macaulay F S, *The Algebraic Theory of Modular Systems*, Cambridge University Press, 1916, reprint 1994.

[33] Fulton W, *Algebraic Curves*, The third version, online, 2008.

[34] Boulier F, Lemaire F, and Moreno Maza M, Well known theorems on triangular systems and the D5 principle, *Transgressive Computing*, Granada, Spain, 2006.

[35] Dora J D, Discrescenzo C, and Duval D, About a new method method for computing in algebraic number fields, EUROCAL'85, Lecture Notes in Computer Science, Springer-Verlag, 1985, **204**: 289–290.

[36] Sun Y and Wang D K, An efficient algorithm for factoring polynomials over algebraic extension field, arXiv:0907.2300v2 [cs.SC].

[37] Diochnos D I, Emiris I Z, and Tsigaridas E P, On the asymptotic and practical complexity of solving bivariate systems over the reals, *J. Symb. Comput.*, 2009, **44**: 818–835.

[38] Reischert D, Asymptotically fast computation of subresultants, *Proceedings of the* 1997 *International Symposium on Sympolic and Algebraic Computation, ACM*, 1997, 233–240.

[39] Wang D, *Elimination Practice, Software Tools, and Applications*, Imperial College Press, 2004.

[40] Wang D K, Zero decomposition for system of polynomial equations, *Proc. ASCM*, World Scientific, 2000, 67–70.