Received ; | Revised ; | Accepted
DOI: xxx/xxxx

ARTICLE TYPE

Analyzing the Dual Space of the Saturated Ideal of a Regular Set and the Local Multiplicities of its Zeros†

Xiaoliang Li[1] | Wei Niu*[2,3]

[1]School of Finance and Trade, City College of Dongguan University of Technology, Dongguan, China
[2]Beijing Advanced Innovation Center for Big Data and Brain Computing, Beihang University, Beijing, China
[3]Ecole Centrale de Pékin, Beihang University, Beijing, China

Correspondence
*Wei Niu Email: Wei.Niu@buaa.edu.cn

Present Address
Ecole Centrale de Pékin, Beihang University, Beijing, 100191, China

Summary

In this paper, we are concerned with the problem of counting the multiplicities of a zero-dimensional regular set's zeros. We generalize the squarefree decomposition of univariate polynomials to the so-called pseudo squarefree decomposition of multivariate polynomials, and then propose an algorithm for decomposing a regular set into a finite number of simple sets. From the output of this algorithm, the multiplicities of zeros could be directly read out, and the real solution isolation with multiplicity can also be easily produced. As a main theoretical result of this paper, we analyze the structure of dual space of the saturated ideal generated by a simple set as well as a regular set. Experiments with a preliminary implementation show the efficiency of our method.

KEYWORDS:
multiplicity, regular set, simple set, squarefree decomposition, triangular decomposition

1 | INTRODUCTION

Polynomial equations are widely used in science and engineering to describe various problems. The multiplicities of the solutions are crucial characteristics, which help us to intensively understand the algebraic structure behind equations.

The study of multiplicities at solutions of polynomial equations may be traced back to the foundation of algebraic geometry. After that, researchers did remarkable work on this topic. Based on the dual space theory, Marinari and others[1] proposed an algorithm for computing the multiplicity. Furthermore, the computation of multiplicity structure could be reduced to solving eigenvalues of the so-called multiplicity matrix, which is studied by Möller, Stetter[2,3] and others[4,5].

Example 1. Consider the univariate polynomial $F = x^5 - x^3$ for example. It is easy to verify that 0 is a zero of F and

$$F'(0) = 0, \quad F''(0) = 0, \quad F^{(3)}(0) \neq 0.$$

It follows that the multiplicity of 0 at F is 3. This is the fundamental idea of counting the multiplicities of zeros using the dual space theory.

Triangular decomposition is one of main elimination approaches for solving systems of multivariate polynomial equations. The first well-known method of triangular decomposition is called the *characteristic set* method, which was proposed by Wu[6,7] based on Ritt's work on differential ideals[8]. But the zero set of a characteristic set may be empty. To remedy this shortcoming, Kalkbrener[9], Yang and Zhang[10] introduced the notation of regular set. The properties of regular sets and relative algorithms have been intensively studied by many researchers such as Wang[11], Hubert[12], Lazard[13] and Moreno Maza[14]. The reader may refer to other literature[15,16,17,11,14,18,19,20,21,22,23] on triangular decomposition of polynomial systems.

†This is an example for title footnote.

Li[24] gave a method to count the multiplicities of a zero-dimensional polynomial system's zeros after decomposing the system into triangular sets. Motivated by his work, we consider a relative yet different problem: efficiently counting the multiplicities of a regular set's zeros. Our main idea is based on the observation that in Example 1, F can be rewritten as $F = x^3(x^2-1)$ with $\gcd(x, x^2-1) = 1$ and x, x^2-1 to be squarefree. Then the multiplicity of 0 can be directly read from the exponent of the factor $x - 0$ in F.

In this paper, we extend the above philosophy to the multivariate case. To be exact, we generalize the squarefree decomposition of univariate polynomials to the so-called pseudo squarefree decomposition of multivariate polynomials, and then propose an algorithm for computing the multiplicities of a regular set's zeros. The method proposed in this paper can also be used to produce the real solution isolation with multiplicity[25]. As a main theoretical result of this paper, we analyze the structure of dual space of the saturated ideal generated by a simple set as well as a regular set.

The rest of this paper is structured as follows. In section 2, basic notations and relative properties of multiplicity and triangular decomposition are revisited. In section 3, we introduce the pseudo squarefree decomposition of a multivariate polynomial and give a feasible algorithm to compute it. Based on the pseudo squarefree decomposition, in section 4 we propose the algorithm Reg2Sim with a regular set as its input, and the multiplicities of zeros can be easily obtained from the output. Section 5 shows the efficiency of our approach with extensive experiments.

2 | PRELIMINARIES

In what follows, we use $\boldsymbol{x}$ to denote variables $x_1, \dots, x_n$. $\mathbb{C}[x_1, \dots, x_n]$ or simply $\mathbb{C}[\boldsymbol{x}]$ represents the polynomial ring with a fixed variable ordering $x_1 < \cdots < x_n$.

2.1 | Multiplicity

Dayton and others[4,5] proposed methods for computing the multiplicity structure of zeros of a zero-dimensional polynomial system. Their approach is based on the theory of dual space. In this section, we revisit relative notations and theorems.

Let $\mathbb{N} = \{0, 1, 2, \dots\}$. For any index array $\boldsymbol{j} = [j_1, \dots, j_r] \in \mathbb{N}^r$, we define the differential operator

$$\partial_{\boldsymbol{j}} \equiv \partial_{j_1 \cdots j_r} \equiv \frac{1}{j_1! \cdots j_r!} \frac{\partial^{j_1 + \cdots + j_r}}{\partial x_1^{j_1} \cdots \partial x_s^{j_r}}.$$

Let $\boldsymbol{a}$ be a zero of the zero-dimensional ideal $\mathcal{I} \subseteq \mathbb{C}[\boldsymbol{x}]$. For any $\partial_{\boldsymbol{j}}$, we can define a functional $\partial_{\boldsymbol{j}}[\boldsymbol{a}] : \mathbb{C}[\boldsymbol{x}] \to \mathbb{C}$, where $\partial_{\boldsymbol{j}}[\boldsymbol{a}](F) = (\partial_{\boldsymbol{j}} F)(\boldsymbol{a})$ for $F \in \mathbb{C}[\boldsymbol{x}]$. Any element of the vector space over $\mathbb{C}$ spanned by $\partial_{\boldsymbol{j}}[\boldsymbol{a}]$ is called a *differential functional* at $\boldsymbol{a}$. All differential functionals at $\boldsymbol{a}$ that vanish on $\mathcal{I}$ form a subspace

$$\mathbb{D}_{\boldsymbol{a}}(\mathcal{I}) \equiv \left\{ \sum_{\boldsymbol{j} \in \mathbb{N}^r} c_{\boldsymbol{j}} \partial_{\boldsymbol{j}}[\boldsymbol{a}] \,:\, c_{\boldsymbol{j}} \in \mathbb{C}, \text{ and } \sum_{\boldsymbol{j} \in \mathbb{N}^r} c_{\boldsymbol{j}} \partial_{\boldsymbol{j}}[\boldsymbol{a}](F) = 0 \text{ for all } F \in \mathcal{I} \right\},$$

which is called the *dual space* of $\mathcal{I}$ at $\boldsymbol{a}$.

Definition 1 (Local Multiplicity)**.** Suppose that $\mathcal{I}$ ia a zero-dimensional ideal in $\mathbb{C}[\boldsymbol{x}]$, i.e. $\mathcal{I}$ has a finite number of complex zeros. Let $\boldsymbol{a}$ be a zero of $\mathcal{I}$. The dimension of the vector space $\mathbb{D}_{\boldsymbol{a}}(\mathcal{I})$ is called the *local multiplicity* or *multiplicity* for short of $\boldsymbol{a}$ in $\mathcal{I}$.

Let $\mathcal{S}$ be a multiplicatively closed subset of $\mathbb{C}[\boldsymbol{x}]$. We use $\mathcal{S}^{-1}\mathcal{I}$ to denote the localization of the polynomial ideal $\mathcal{I}$ at $\mathcal{S}$, i.e. $\mathcal{S}^{-1}\mathcal{I} \equiv \{F/G \,:\, F \in \mathcal{I},\, G \in \mathcal{S}\}$.

Theorem 1. [5] Under the assumption of Definition 1, the *local multiplicity* of $\boldsymbol{a}$ in $\mathcal{I}$ equals to the dimension of the quotient ring $\mathcal{S}^{-1}\mathbb{C}[\boldsymbol{x}]/\mathcal{S}^{-1}\mathcal{I}$ as a vector space over $\mathbb{C}$, where $\mathcal{S} = \mathbb{C}[\boldsymbol{x}] \setminus \mathcal{M}_{\boldsymbol{a}}$ and $\mathcal{M}_{\boldsymbol{a}}$ is the maximal ideal of $\boldsymbol{a}$.

2.2 | Triangular Decomposition

Let F and G be two polynomials in $\mathbb{C}[\boldsymbol{x}]$. The variable of biggest index appearing in F is called the *leading variable* of F and denoted by $\mathrm{lv}(F)$. The leading coefficient of F, viewed as a univariate polynomial in $\mathrm{lv}(F)$, is called the *initial* of F and denoted by $\mathrm{ini}(F)$. Moreover, $\mathrm{pquo}(F, G)$ and $\mathrm{prem}(F, G)$ are used to denote the *pseudo-quotient* and *pseudo-remainder* of F with respect to G in $\mathrm{lv}(G)$ respectively.

Definition 2. An ordered set $\mathcal{T} = [T_1, \ldots, T_r]$ of non-constant polynomials in $\mathbb{C}[\boldsymbol{x}]$ is called a *triangular set* if $\mathrm{lv}(T_i) < \mathrm{lv}(T_j)$ for all $i < j$.

Suppose that $\mathcal{T} = [T_1, \ldots, T_r]$ is a triangular set. We use y_i as an alias of $\mathrm{lv}(T_i)$ for each $i = 1, \ldots, r$. Moreover, $\boldsymbol{y}_i$ stands for $y_1, \ldots, y_i$ with $\boldsymbol{y} = \boldsymbol{y}_r$. The triangular set $\mathcal{T}$ is said to be zero-dimensional if $\boldsymbol{x} = \boldsymbol{y}$. We denote $\boldsymbol{u}$ the variables in $\boldsymbol{x}$ but not in $\boldsymbol{y}$.
Let $\tilde{\mathbb{C}}$ represent the transcendental extension field $\mathbb{C}(\boldsymbol{u})$. To avoid ambiguity, for any ideal $\mathcal{I} \subseteq \mathbb{C}[\boldsymbol{u}, \boldsymbol{y}_i]$, $\mathcal{I}_{\tilde{\mathbb{C}}}$ denotes the ideal generated by $\mathcal{I}$ in $\tilde{\mathbb{C}}[\boldsymbol{y}_i]$. The *saturated ideal* of $\mathcal{T}$ is defined as

$$\mathrm{sat}(\mathcal{T}) \equiv \langle \mathcal{T} \rangle : H^\infty \equiv \{F : \text{ there exits an integer } s \text{ such that } FH^s \in \langle \mathcal{T} \rangle\},$$

where H is the product of the initials of all polynomials in $\mathcal{T}$. Moreover, we define $\mathrm{sat}_i(\mathcal{T}) \equiv \mathrm{sat}([T_1, \ldots, T_i])$.

Definition 3. Let $\mathcal{T} = [T_1, \ldots, T_r] \subseteq \mathbb{C}[\boldsymbol{x}]$ be a triangular set. $\mathcal{T}$ is called a *regular set* in $\mathbb{C}[\boldsymbol{x}]$ if for each $i = 1, \ldots, r$, $\mathrm{ini}(T_i)$ is neither zero nor a zero divisor in quotient ring $\mathbb{C}[\boldsymbol{x}]/\,\mathrm{sat}_{i-1}(\mathcal{T})$.

The notation of regular set was introduced first by Kalkbrener[9], Yang and Zhang[10] simultaneously. In the following, we list two main properties of regular sets[9,10,12,26,11].

Proposition 1. [12] Let $\mathcal{T}$ be a regular set in $\mathbb{C}[\boldsymbol{x}]$. Then

1. $\mathrm{sat}(\mathcal{T}) \neq \mathbb{C}[\boldsymbol{x}]$;
2. $\mathcal{T}$ is zero-dimensional if and only if $\mathrm{sat}(\mathcal{T})$ is a zero-dimensional ideal;
3. $\mathrm{sat}(\mathcal{T})$ is an unmixed-dimensional ideal.

Proposition 2. [12] For any regular set $\mathcal{T} \subseteq \mathbb{C}[\boldsymbol{x}]$, $\mathrm{sat}(\mathcal{T})_{\tilde{\mathbb{C}}} = \langle \mathcal{T} \rangle_{\tilde{\mathbb{C}}}$. Furthermore, $\langle \mathcal{T} \rangle_{\tilde{\mathbb{C}}} \cap \mathbb{C}[\boldsymbol{x}] = \mathrm{sat}(\mathcal{T})$.

Proposition 2 plays a key role in this paper. By this property, we know that if the regular set $\mathcal{T}$ is zero-dimensional, then $\mathrm{sat}(\mathcal{T}) = \langle \mathcal{T} \rangle$.
Let F be a polynomial in $\mathbb{C}[\boldsymbol{u}, \boldsymbol{y}_i]$. Then F can also be viewed as an element in $\tilde{\mathbb{C}}[\boldsymbol{y}_i]$. For any prime ideal $\mathcal{P} \subseteq \tilde{\mathbb{C}}[\boldsymbol{y}_{i-1}]$, $\overline{F}^{\mathcal{P}}$ denotes the image of F in $(\tilde{\mathbb{C}}[\boldsymbol{y}_{i-1}]/\mathcal{P})[y_i]$ under the natural homomorphism. For any polynomial set $\mathcal{S} \in \tilde{\mathbb{C}}[\boldsymbol{y}_i]$, define $\overline{\mathcal{S}}^{\mathcal{P}} \equiv \{\overline{S}^{\mathcal{P}} : S \in \mathcal{S}\}$.

Definition 4. A regular set $\mathcal{T} = [T_1, \ldots, T_r]$ in $\mathbb{C}[\boldsymbol{x}]$ is called a *simple set* or said to be *simple* if for each $i = 1, \ldots, r$ and associated prime $\mathcal{P}$ of $\mathrm{sat}_{i-1}(\mathcal{T})_{\tilde{\mathbb{C}}}$, $\overline{T}_i^{\mathcal{P}}$ is a squarefree polynomial in $(\tilde{\mathbb{C}}[\boldsymbol{y}_{i-1}]/\mathcal{P})[y_i]$.

Simple set[27,17] is also called *squarefree regular chain*[12]. The following proposition reveals the most important property of simple sets.

Proposition 3. [28] Let $\mathcal{T}$ be a regular set in $\mathbb{C}[\boldsymbol{x}]$. Then the following statements are equivalent:

1. $\mathcal{T}$ is simple;
2. $\mathrm{sat}(\mathcal{T})$ is a radical ideal;
3. $\mathrm{sat}(\mathcal{T})_{\tilde{\mathbb{C}}}$ is a radical ideal.

3 | PSEUDO SQUAREFREE DECOMPOSITION MODULO A REGULAR SET

Let $\mathcal{I}$ and $\mathcal{I}_1, \ldots, \mathcal{I}_s$ be ideals in $\mathbb{C}[\boldsymbol{x}]$ with

$$\mathcal{I} = \mathcal{I}_1 \cap \cdots \cap \mathcal{I}_s. \tag{1}$$

We say (1) is an *irredundant decomposition* if, for any associated prime $\mathcal{P}$ of $\mathcal{I}$, there exists a unique i such that $\sqrt{\mathcal{I}_i} \subseteq \mathcal{P}$.

Theorem 2. [12,9,14,29] There exists an algorithm (named by pgcd) with a polynomial set $\mathcal{F}$ in $\mathbb{C}[\boldsymbol{x}][z]$ and a regular set $\mathcal{T}$ in $\mathbb{C}[\boldsymbol{x}]$ as its input, where $\mathbb{C}[\boldsymbol{x}][z]$ represents the polynomial ring with all variables in $\boldsymbol{x}$ smaller than z, such that the output $\{(G_1, \mathcal{A}_1), \ldots, (G_s, \mathcal{A}_s)\}$ satisfies the following conditions:

1. each $\mathcal{A}_i$ is a regular set in $\mathbb{C}[\boldsymbol{x}]$ and $\mathrm{sat}(\mathcal{T}) \subseteq \mathrm{sat}(\mathcal{A}_i)$;
2. $\sqrt{\mathrm{sat}(\mathcal{T})} = \sqrt{\mathrm{sat}(\mathcal{A}_1)} \cap \cdots \cap \sqrt{\mathrm{sat}(\mathcal{A}_s)}$ is an irredundant decomposition;

3. The ideal in $\mathrm{fr}(\mathbb{C}[\boldsymbol{x}]/\operatorname{sat}(\mathcal{A}_i))[z]$ generated by $\mathcal{F}$ equals to that generated by the polynomial G_i, where $\mathrm{fr}(\mathbb{C}[\boldsymbol{x}]/\operatorname{sat}(\mathcal{A}_i))$ is the total quotient ring of $\mathbb{C}[\boldsymbol{x}]/\operatorname{sat}(\mathcal{A}_i)$, i.e. the localization of $\mathbb{C}[\boldsymbol{x}]/\operatorname{sat}(\mathcal{A}_i)$ at the multiplicatively closed set of all its non-zerodivisors;

4. $G_i \in \langle \mathcal{F} \rangle + \operatorname{sat}(\mathcal{A}_i)$;

5. $G_i = 0$, or $\operatorname{lc}(G_i, z)$ is neither zero nor a zero divisor in quotient ring $\mathrm{fr}(\mathbb{C}[\boldsymbol{x}]/\operatorname{sat}(\mathcal{A}_i))$.

Remark 1. It is pointed out[12] that if $\mathcal{T}$ is a simple set, then all $\mathcal{A}_i$ in the output of $\mathsf{pgcd}(\mathcal{F}, \mathcal{T})$ are also simple sets. Furthermore, the ideal relation in 2 can be replaced with $\operatorname{sat}(\mathcal{T}) = \operatorname{sat}(\mathcal{A}_1) \cap \cdots \cap \operatorname{sat}(\mathcal{A}_s)$ in this case.

It is known that $\mathrm{fr}(\mathbb{C}[\boldsymbol{x}]/\operatorname{sat}(\mathcal{A}_i)) = \tilde{\mathbb{C}}[\boldsymbol{y}]/\operatorname{sat}(\mathcal{A}_i)_{\tilde{\mathbb{C}}}$. Then by 3, for any associated prime $\mathcal{P}$ of $\operatorname{sat}(\mathcal{A}_i)_{\tilde{\mathbb{C}}}$, we have that $\langle \overline{\mathcal{F}}^{\mathcal{P}} \rangle = \langle \overline{G_i}^{\mathcal{P}} \rangle$, i.e. $\gcd(\overline{\mathcal{F}}^{\mathcal{P}}) = \overline{G_i}^{\mathcal{P}}$. Therefore, the set $\{(G_1, \mathcal{A}_1), \ldots, (G_s, \mathcal{A}_s)\}$ satisfying the above five conditions is called the *pseudo gcd* of $\mathcal{F}$ modulo $\mathcal{T}$.

For any univariate polynomials A and B, the expression $A \sim B$ means that there exists a nonzero constant c such that $A = cB$. Let $F, A_1, \ldots, A_s$ be non-constant polynomial in $\mathbb{C}[x]$ and $a_1, \ldots, a_s$ be positive integers. We call $\{[A_1, a_1], \ldots, [A_s, a_s]\}$ the *squarefree decomposition* of F if the following conditions are satisfied:

- $F \sim A_1^{a_1} \cdots A_s^{a_s}$,
- $\gcd(A_i, A_j) = 1$ for all $i \neq j$,
- A_i is squarefree for all $i = 1, \ldots, s$.

The following example illustrates the philosophy of computing the squarefree decomposition of a univariate polynomial[30].

Example 2. Consider the univariate polynomial $F = 3\,x^5 - 3\,x^3 \in \mathbb{C}[x]$. First compute $\gcd(F, \mathrm{d}F/\mathrm{d}x)$ and store the result in P. It is easy to see that $P = x^2$, which is a factor of F. Let $Q = F/P = 3\,x^3 - 3\,x$. Further computing $\gcd(P, Q)$, one obtains x, which is also a factor of Q. Since $Q/x = 3\,x^2 - 3 \sim x^2 - 1$, we have $F \sim x^3(x^2 - 1)$, where x and $x^2 - 1$ are coprime and squarefree. As a result, the squarefree decomposition of F is $\{[x, 3], [x^2 - 1, 1]\}$.

The first author of this paper and the coworkers[28] generalized the squarefree decomposition of a univariate polynomial to the so-called pseudo squarefree decomposition of a multivariate polynomial modulo a simple set. We slightly modify the definition of pseudo squarefree decomposition as follows.

Definition 5. For any regular set $\mathcal{T} \subseteq \mathbb{C}[\boldsymbol{x}]$ and polynomial $F \in \mathbb{C}[\boldsymbol{x}][z] \setminus \mathbb{C}[\boldsymbol{x}]$, the set

$$\{(\{[P_{i1}, a_{i1}], \ldots, [P_{ik_i}, a_{ik_i}]\}, \mathcal{A}_i) : i = 1, \ldots, s\}$$

is called the *pseudo squarefree decomposition* of F modulo $\mathcal{T}$ if

1. each $\mathcal{A}_i$ is a regular set in $\mathbb{C}[\boldsymbol{x}]$ and $\operatorname{sat}(\mathcal{T}) \subseteq \operatorname{sat}(\mathcal{A}_i)$;
2. $\sqrt{\operatorname{sat}(\mathcal{T})} = \sqrt{\operatorname{sat}(\mathcal{A}_1)} \cap \cdots \cap \sqrt{\operatorname{sat}(\mathcal{A}_s)}$ is an irredundant decomposition;
3. each $\{[\overline{P_{i1}}^{\mathcal{P}}, a_{i1}], \ldots, [\overline{P_{ik_i}}^{\mathcal{P}}, a_{ik_i}]\}$ is the squarefree decomposition of $\overline{F}^{\mathcal{P}}$ for any associated prime $\mathcal{P}$ of $\operatorname{sat}(\mathcal{A}_i)_{\tilde{\mathbb{C}}}$.

Moreover, for any $F \in \mathbb{F}_q[\boldsymbol{x}][z]$ and any zero-dimensional simple set $\mathcal{T}$ in $\mathbb{F}_q[\boldsymbol{x}]$, where $\mathbb{F}_q$ is a finite field, an effective algorithm for computing the pseudo squarefree decomposition of F modulo $\mathcal{T}$ was designed by the first author[28]. In the sequel, we propose a new algorithm (Algorithm 1), obtained by modifying the original algorithm, for computing the pseudo squarefree decomposition of polynomials in $\mathbb{C}[\boldsymbol{x}][z]$.

Algorithm 1: Pseudo Squarefree Decomposition $\mathbb{S} := \mathsf{psqf}(F, \mathcal{T})$

Input: a polynomial F in $\mathbb{C}[\boldsymbol{x}][z] \setminus \mathbb{C}[\boldsymbol{x}]$; a regular set $\mathcal{T}$ in $\mathbb{C}[\boldsymbol{x}]$.
Output: the pseudo squarefree decomposition $\mathbb{S}$ of F modulo $\mathcal{T}$.

```
S := ∅; D := ∅;
for (C_1, C) ∈ pgcd({F, ∂F/∂z}, T) do
    B_1 := pquo(F, C_1);
    D := D ∪ {[B_1, C_1, C, ∅, 1]};
end
while D ≠ ∅ do
    [B_1, C_1, C, P, d] := pop(D);
    if deg(B_1, z) > 0 then
        for (B_2, A) ∈ pgcd({B_1, C_1}, C) do
            C_2 := pquo(C_1, B_2);
            P := pquo(B_1, B_2);
            if deg(P, z) > 0 then P := P ∪ {[P, d]};
            D := D ∪ {[B_2, C_2, A, P, d + 1]};
        end
    else
        S := S ∪ {(P, C)};
    end
end
return(S);
```

We use $\mathsf{pop}(\mathbb{D})$ to represent the operation of taking one element randomly and then delete it from $\mathbb{D}$. In Algorithm 1, $\mathbb{D}$ stores what to be processed. For each element $[B, C, \mathcal{C}, \mathbb{P}, d] \in \mathbb{D}$, one may see that $\mathcal{C}$ is a regular set over which later computation is to be performed, and $\mathbb{P}$ stores the squarefree components already obtained with exponent smaller than d.

It can be observed that the **while** loop is essentially a splitting procedure. Thus we may regard the running of Algorithm 1 as building trees with elements in $\mathbb{D}$ as their nodes. The roots of these trees are constructed in the first **for** loop. For each node $[B_1, C_1, \mathcal{C}, \mathbb{P}, d]$, its child $[B_2, C_2, \mathcal{A}, \mathbb{P}, d+1]$ is built when the statement "$\mathbb{D} := \mathbb{D} \cup \{[B_2, C_2, \mathcal{A}, \mathbb{P}, d+1]\}$" is executed. For any fixed path of one of the trees, we denote the node of depth i in the path by $[B(i), C(i), \mathcal{C}(i), \mathbb{P}(i), i]$.

Correctness. The conditions 1 and 2 of Definition 5 follow from 1 and 2 of Theorem 2 respectively.

To prove 3 of Theorem 2, the tool of localization may be helpful. Suppose that $[B(s), C(s), \mathcal{C}(s), \mathbb{P}(s), t]$ is a leaf node of the tree. For any associated prime $\mathcal{P}$ of $\mathrm{sat}(\mathcal{C}(t))_{\tilde{\mathbb{C}}}$, $\overline{F}^{\mathcal{P}}$ is a univariate polynomial over the field $\tilde{\mathbb{C}}[\boldsymbol{y}]/\mathcal{P}$. We can assume that $\overline{F}^{\mathcal{P}} = \prod_{i=1}^{t} P_i^i$, where P_i are squarefree polynomial in z and $\gcd(P_j, P_k) = 1$ for any $j \neq k$. It can be proved that

$$\overline{B(i)}^{\mathcal{P}} \sim P_i P_{i+1} \cdots P_t \qquad \text{and} \qquad \overline{C(i)}^{\mathcal{P}} \sim P_{i+1} P_{i+2}^2 \cdots P_t^{t-i}. \tag{2}$$

Thus $\overline{B(i)}^{\mathcal{P}} / \overline{B(i-1)}^{\mathcal{P}} = P_i$. Therefore $\mathbb{P}$ stores the squarefree decomposition of $\overline{F}^{\mathcal{P}}$. □

Termination. It suffices to prove that every path in the tree is finite, which is obvious by (2). □

4 | ANALYZING MULTIPLICITY

In this section, we propose algorithms for analyzing multiplicity of a regular set's zeros. As a preparation, the following algorithm is given first, which can be used to decompose any given regular set over $\mathbb{C}$ into a finite number of simple sets.

Algorithm 2: $\mathbb{S} := \mathsf{Reg2Sim}(\mathcal{T})$

Input: a regular set $\mathcal{T}$ in $\mathbb{C}[\boldsymbol{x}]$.

Output: a finite set $\mathbb{S}$ with elements of the form $(\mathcal{B}, P)$, where $\mathcal{B} = [B_1, \dots, B_r]$ is a simple set in $\mathbb{C}[\boldsymbol{x}]$ and $P = [p_1, \dots, p_r]$ is an array of integers. We use $\mathcal{B}^P$ to denote $[B_1^{p_1}, \dots, B_r^{p_r}]$ and call P the *multiplicity array* of $\mathcal{B}^P$. Furthermore, we have that

$$\operatorname{sat}(\mathcal{T}) = \bigcap_{(\mathcal{B},P)\in\mathbb{S}} \operatorname{sat}(\mathcal{B}^P), \tag{3}$$

which is an irredundant decomposition.

$\mathbb{S} := \emptyset$; $\mathbb{D} := \{(\mathcal{T}, [\,], [\,])\}$;
while $\mathbb{D} \neq \emptyset$ **do**
    $(\mathcal{A}, \mathcal{B}, P) := \mathsf{pop}(\mathbb{D})$;
    if $\mathcal{A} = \emptyset$ **then**
        $\mathbb{S} := \mathbb{S} \cup \{(\mathcal{B}, P)\}$;
    else
        $A :=$ the first polynomial in $\mathcal{A}$;
        for $(\{[C_1, c_1], \dots, [C_s, c_s]\}, \mathcal{Q}) \in \mathsf{psqf}(A, \mathcal{B})$ **do**
            $\mathbb{D} := \bigcup_{i=1}^{s} \{(\mathcal{A} \setminus \{A\}, \mathsf{append}(\mathcal{Q}, C_i), \mathsf{append}(P, c_i))\} \cup \mathbb{D}$;
        end
    end
end
$\mathsf{return}(\mathbb{S})$;

In Algorithm 2, $\mathsf{append}(L, a)$ returns the array obtained by appending the element a to the end of L. The termination is obvious. In order to prove the correctness, the following lemma is needed.

Lemma 1. Suppose that $\mathcal{T}$ is a simple set in $\mathbb{C}[\boldsymbol{x}]$ and F is a polynomial in $\mathbb{C}[\boldsymbol{x}][z]\backslash\mathbb{C}[\boldsymbol{x}]$. Let $\{(\{[P_{i1}, a_{i1}], \dots, [P_{ik_i}, a_{ik_i}]\}, \mathcal{A}_i) : i = 1, \dots, s\}$ be the output of $\mathsf{Reg2Sim}(F, \mathcal{T})$. Then all $\mathcal{A}_i$ are simple sets. Furthermore, $\operatorname{sat}(\mathcal{T}) = \operatorname{sat}(\mathcal{A}_1) \cap \cdots \cap \operatorname{sat}(\mathcal{A}_s)$.

Proof. It directly follows from Remark 1. □

Correctness(Algorithm 2)**.** For any element $(\mathcal{B}, P)$ in the output of $\mathsf{Reg2Sim}(\mathcal{T})$, one can easily know that $\mathcal{B}$ is a simple set by Lemma 1 and Definition 4.

The ideal relation (3) could be proved as follows. For each $(\mathcal{A}, \mathcal{B}, P) \in \mathbb{D}$ which satisfies that $\mathcal{A} \neq \emptyset$, the statement "$(\{[C_1, c_1], \dots, [C_s, c_s]\}, \mathcal{Q}) \in \mathsf{psqf}(A, \mathcal{B})$" in the **for** loop is then executed. It can be observed that

$$\langle \mathcal{A} \rangle_{\tilde{\mathbb{C}}} + \langle \mathcal{B}^P \rangle_{\tilde{\mathbb{C}}} = \bigcap_{(\{[C_1,c_1],\dots,[C_s,c_s]\},\mathcal{Q})\in\mathsf{psqf}(A,\mathcal{B})} \langle \mathcal{A} \rangle_{\tilde{\mathbb{C}}} + \langle \mathcal{Q}^P \rangle_{\tilde{\mathbb{C}}}.$$

Furthermore, for each $(\{[C_1, c_1], \dots, [C_s, c_s]\}, \mathcal{Q}) \in \mathsf{psqf}(A, \mathcal{B})$, we have that

$$\begin{aligned}
\langle \mathcal{A} \rangle_{\tilde{\mathbb{C}}} + \langle \mathcal{Q}^P \rangle_{\tilde{\mathbb{C}}} &= \langle \mathcal{A} \setminus \{A\} \rangle_{\tilde{\mathbb{C}}} + \langle \mathcal{Q}^P \cup \{A\} \rangle_{\tilde{\mathbb{C}}} \\
&= \langle \mathcal{A} \setminus \{A\} \rangle_{\tilde{\mathbb{C}}} + \langle \mathcal{Q}^P \cup \{\prod_{i=1}^{s} C_i^{c_i}\} \rangle_{\tilde{\mathbb{C}}} \\
&= \langle \mathcal{A} \setminus \{A\} \rangle_{\tilde{\mathbb{C}}} + \bigcap_{i=1}^{s} \langle \mathcal{Q}^P \cup \{C_i^{c_i}\} \rangle_{\tilde{\mathbb{C}}} \\
&= \bigcap_{i=1}^{s} \langle \mathcal{A} \setminus \{A\} \rangle_{\tilde{\mathbb{C}}} + \langle \mathcal{Q}^P \cup \{C_i^{c_i}\} \rangle_{\tilde{\mathbb{C}}}.
\end{aligned}$$

Thus in the **while** loop, we have the following invariant:

$$\langle \mathcal{T} \rangle_{\tilde{\mathbb{C}}} = \bigcap_{(\mathcal{A},\mathcal{B},P)\in\mathbb{D}} \langle \mathcal{A} \cup \mathcal{B}^P \rangle_{\tilde{\mathbb{C}}} \cap \bigcap_{(\mathcal{B},P)\in\mathbb{S}} \langle \mathcal{B}^P \rangle_{\tilde{\mathbb{C}}}.$$

When the **while** loop terminates, $\langle \mathcal{T} \rangle_{\tilde{\mathbb{C}}} = \bigcap_{(\mathcal{B},P)\in\mathbb{S}} \langle \mathcal{B}^P \rangle_{\tilde{\mathbb{C}}}$. Intersecting the left and right sides of this equation with $\mathbb{C}[\boldsymbol{x}]$, we obtain (3).

The irredundant property of the ideal decomposition in (3) follows from Definition 5 and the property of Algorithm 1. □

In what follows, we show how the multiplicity arrays in the output of $\mathsf{Reg2Sim}(\mathcal{T})$ are used to count the multiplicities at zeros of $\mathcal{T}$.

Lemma 2. Suppose that $[B_1, \ldots, B_r]$ is a zero-dimensional simple set in $\mathbb{C}[\boldsymbol{x}]$, and $[p_1, \ldots, p_r]$ is a list of integers. Let $\boldsymbol{a} = (a_1, \ldots, a_r)$ be a zero of $\mathcal{I} = \mathrm{sat}([B_1, \ldots, B_r])$ and $\partial_{j_1 \cdots j_r}$ be a differential functional with $j_i \geq p_i$ for some i's. Then there exists a polynomial $F_{j_1 \cdots j_r}$ in $\mathcal{I}$ such that $\partial_{j_1 \cdots j_r}[\boldsymbol{a}](F_{j_1 \cdots j_r}) \neq 0$.

Proof. Suppose that μ is the smallest integer among i's such that $j_i \geq p_i$. Let

$$F_{j_1 \cdots j_r} = \Big(\prod_{k \neq \mu} (x_k - a_k)^{j_k} \Big) (x_\mu - a_\mu)^{j_\mu - p_\mu} B_\mu^{p_\mu}.$$

It is obvious that $F_{j_1 \cdots j_r} \in \mathcal{I}$. For any polynomial $P \in \mathbb{C}[\boldsymbol{x}]$,

$$\partial_{j_1 \cdots j_r}[\boldsymbol{a}](P) = \partial_{j_\mu} \Big(\partial_{j_1 \cdots j_{\mu-1} j_{\mu+1} \cdots j_r}(P)|_{(a_1, \ldots, a_{\mu-1}, a_{\mu+1}, \ldots, a_r)} \Big)|_{x_\mu = a_\mu}. \tag{4}$$

Denote $\partial_{j_1 \cdots j_{\mu-1} j_{\mu+1} \cdots j_r}(F_{j_1 \cdots j_r})|_{(a_1, \ldots, a_{\mu-1}, a_{\mu+1}, \ldots, a_r)}$ by G. Since

$$\partial_{j_1 \cdots j_{\mu-1} j_{\mu+1} \cdots j_r} \Big(\prod_{k \neq \mu} (x_k - a_k)^{j_k} \Big) = 1,$$

we have

$$G = (x_\mu - a_\mu)^{j_\mu - p_\mu} \Big(B_\mu|_{(a_1, \ldots, a_{\mu-1}, a_{\mu+1}, \ldots, a_r)} \Big)^{p_\mu},$$

where $B_\mu|_{(a_1, \ldots, a_{\mu-1}, a_{\mu+1}, \ldots, a_r)}$ is a squarefree polynomial in $\mathbb{C}[x_\mu]$. It is known that $(a_1, \ldots, a_r)$ is a zero of $\mathcal{I}$ and $B_\mu \in \mathcal{I}$, thus one can assume that

$$B_\mu|_{(a_1, \ldots, a_{\mu-1}, a_{\mu+1}, \ldots, a_r)} = (x_\mu - a_\mu) \cdot A,$$

where $A \in \mathbb{C}[x_\mu]$ and $\gcd(x_\mu - a_\mu, A) = 1$. Therefore $G = (x_\mu - a_\mu)^{j_\mu} A^{p_\mu}$. By (4),

$$\partial_{j_1 \cdots j_r}[\boldsymbol{a}](F_{j_1 \cdots j_r}) = \partial_{j_\mu}(G)|_{x_\mu = a_\mu} = A^{p_\mu}|_{x_\mu = a_\mu} \neq 0,$$

which completes the proof. □

Proposition 4. Let $\mathcal{B} = [B_1, \ldots, B_r]$ be a zero-dimensional simple set in $\mathbb{C}[\boldsymbol{x}]$, and $P = [p_1, \ldots, p_r]$ be a list of integers. Then for any zero $\boldsymbol{a} = (a_1, \ldots, a_r)$ of $\mathcal{I} = \mathrm{sat}(\mathcal{B}^P)$, the dual space $\mathbb{D}_{\boldsymbol{a}}(\mathcal{I})$ is spanned by

$$S = \Big\{ \partial_{j_1 \cdots j_r}[\boldsymbol{a}] \, : \, 0 \leq j_i < p_i \text{ for all } i = 1, \ldots, r \Big\}.$$

Proof. Suppose that $\partial_{j_1 \cdots j_r}$ satisfies that $0 \leq j_i < p_i$ for all $i = 1, \ldots, r$. It is easy to verify that $B_i \mid \partial_{j_1 \cdots j_r}(B_i^{p_i})$, i.e. there exists a polynomial $A_i \in \mathbb{C}[\boldsymbol{x}]$ such that $\partial_{j_1 \cdots j_r}(B_i^{p_i}) = A_i B_i$. Since $\mathcal{B}^P$ is a zero-dimensional regular set, we know that

$$\mathrm{sat}(\mathcal{B}^P) = \langle B_1^{p_1}, \ldots, B_r^{p_r} \rangle.$$

For any $F \in \mathrm{sat}(\mathcal{B}^P)$, there exist $C_1, \ldots, C_r \in \mathbb{C}[\boldsymbol{x}]$ such that $F = \sum_{i=1}^r C_i B_i^{p_i}$. Thus

$$\partial_{j_1 \cdots j_r}(F) = \sum_{i=1}^r B_i [\partial_{j_1 \cdots j_r}(C_i) B_i^{p_i - 1} + A_i C_i].$$

Since $B_i(\boldsymbol{a}) = 0$, it follows that $\partial_{j_1 \cdots j_r}[\boldsymbol{a}](F) = 0$. Hence $\partial_{j_1 \cdots j_r}[\boldsymbol{a}] \in \mathbb{D}_{\boldsymbol{a}}(\mathcal{I})$.

On the other hand, suppose that $\sum_{i=1}^l c_{j_i} \partial_{j_i}[\boldsymbol{a}]$ ($c_{j_i} \in \mathbb{C}$) is a differential functional in $\mathbb{D}_{\boldsymbol{a}}(\mathcal{I})$. Without loss of generality, one may assume that $\partial_{j_i}[\boldsymbol{a}] \notin S$ for $i = 1, \ldots, m$ and $\partial_{j_i}[\boldsymbol{a}] \in S$ for $i = m+1, \ldots, l$. For each $\partial_{j_k}[\boldsymbol{a}]$, $k = 1, \ldots, m$, construct $F_{j_k} \in \mathcal{I}$ such that $\partial_{j_k}[\boldsymbol{a}](F_{j_k}) \neq 0$ in the same way as we did in the proof of Lemma 2. For any $i = m+1, \ldots, l$, it can be proved that $\partial_{j_i}[\boldsymbol{a}](F_{j_k}) = 0$. Furthermore, $\partial_{j_i}[\boldsymbol{a}](F_{j_k}) = 0$ if $i = 1, \ldots, m$ and $i \neq k$. It follows that

$$\sum_{i=1}^l c_{j_i} \partial_{j_i}[\boldsymbol{a}](F_{j_k}) = c_{j_k} \partial_{j_k}[\boldsymbol{a}](F_{j_k}) = 0, \text{ for } k = 1, \ldots, m.$$

Since $\partial_{j_k}[\boldsymbol{a}](F_{j_k}) \neq 0$, we know that $c_{j_1} = \cdots = c_{j_m} = 0$, which means that $\mathbb{D}_{\boldsymbol{a}}(\mathcal{I})$ is spanned by S. The proof is complete. □

Corollary 1. Let $\mathcal{B} = [B_1, \ldots, B_r]$ be a zero-dimensional simple set in $\mathbb{C}[\boldsymbol{x}]$, and $P = [p_1, \ldots, p_r]$ be a list of integers. Then the local multiplicity of any zero in $\mathrm{sat}(\mathcal{B}^P)$ is $\prod_{i=1}^r p_i$.

Proof. This is obvious by Definition 1 and Proposition 4. □

The following lemma states a classical result in commutative algebra.

Lemma 3. [31] Suppose that $\mathcal{S}$ is a multiplicatively closed subset of $\mathbb{C}[\boldsymbol{x}]$, and $\mathcal{I}$, $\mathcal{I}_1$, $\mathcal{I}_2$ are polynomials in $\mathbb{C}[\boldsymbol{x}]$.

1. $\mathcal{S}^{-1}(\mathcal{I}_1 \cap \mathcal{I}_2) = \mathcal{S}^{-1}\mathcal{I}_1 \cap \mathcal{S}^{-1}\mathcal{I}_2$.
2. If $\mathcal{S} \cap \mathcal{P} \neq \emptyset$ for every prime ideal $\mathcal{P} \supseteq \mathcal{I}$, then $\mathcal{S}^{-1}\mathcal{I} = \mathcal{S}^{-1}\mathbb{C}[\boldsymbol{x}]$.

Theorem 3 (Main Theorem)**.** Suppose that a zero-dimensional regular set $\mathcal{T} \subseteq \mathbb{C}[\boldsymbol{x}]$ is given. Let $\mathbb{S} = \{(\mathcal{B}_1, P_1), \ldots, (\mathcal{B}_k, P_k)\}$ be the output of $\mathsf{Reg2Sim}(\mathcal{T})$. For any zero $\boldsymbol{a} = (a_1, \ldots, a_r)$ of $\langle \mathcal{T} \rangle$, there exists one and only one element $([B_1, \ldots, B_r], [p_1, \ldots, p_r]) \in \mathbb{S}$ such that $B_1(\boldsymbol{a}) = 0, \ldots, B_r(\boldsymbol{a}) = 0$. Furthermore, the local multiplicity of $\boldsymbol{a}$ in $\langle \mathcal{T} \rangle$ is $\prod_{i=1}^{r} p_i$.

Proof. The existence of such $([B_1, \ldots, B_r], [p_1, \ldots, p_r]) \in \mathbb{S}$ is from (3). While the uniqueness is because the decomposition in (3) is irredundant.

Without loss of generality, we assume that

$$\{(\mathcal{B}_1, P_1), \ldots, (\mathcal{B}_k, P_k)\} = \mathsf{Reg2Sim}(\mathcal{T})$$

with $(\mathcal{B}_1, P_1) = ([B_1, \ldots, B_r], [p_1, \ldots, p_r])$. By Theorem 1 and Corollary 1, it suffices to prove $\mathcal{S}^{-1}\langle \mathcal{T} \rangle = \mathcal{S}^{-1} \operatorname{sat}(\mathcal{B}_1^{P_1})$, where $\mathcal{S} = \mathbb{C}[\boldsymbol{x}] \setminus \mathcal{M}_{\boldsymbol{a}}$ and $\mathcal{M}_{\boldsymbol{a}} = \langle x_1 - a_1, \ldots, x_r - a_r \rangle$.

We know that $\langle \mathcal{T} \rangle = \operatorname{sat}(\mathcal{T})$. By Lemma 3 and (3),

$$\mathcal{S}^{-1}\langle \mathcal{T} \rangle = \mathcal{S}^{-1} \operatorname{sat}(\mathcal{T}) = \bigcap_{i=1}^{k} \mathcal{S}^{-1} \operatorname{sat}(\mathcal{B}_i^{P_i}).$$

As $B_1(\boldsymbol{a}) = 0, \ldots, B_r(\boldsymbol{a}) = 0$, we have that $\operatorname{sat}(\mathcal{B}_1^{P_1}) = \langle \mathcal{B}_1^{P_1} \rangle \subseteq \mathcal{M}_{\boldsymbol{a}}$. Moreover, (3) is an irredundant decomposition, thus $\operatorname{sat}(\mathcal{B}_i^{P_i}) \nsubseteq \mathcal{M}_{\boldsymbol{a}}$ for any $i \neq 1$. Then it can be proved that $\mathcal{S} \cap \mathcal{P} \neq \emptyset$ for every prime ideal $\mathcal{P} \supseteq \operatorname{sat}(\mathcal{B}_i^{P_i})$, $i \neq 1$. By Lemma 3, $\mathcal{S}^{-1} \operatorname{sat}(\mathcal{B}_i^{P_i}) = \mathcal{S}^{-1}\mathbb{C}[\boldsymbol{x}]$ for any $i \neq 1$. Hence $\mathcal{S}^{-1}\langle \mathcal{T} \rangle = \mathcal{S}^{-1} \operatorname{sat}(\mathcal{B}_1^{P_1})$. □

By the above theorem, one can easily count the multiplicities at zeros of any given zero-dimensional regular set $\mathcal{T}$ from the output of $\mathsf{Reg2Sim}(\mathcal{T})$. The following example illustrates the idea.

Example 3. Consider the following regular set in $\mathbb{C}[x, y]$:

$$\mathcal{T} = [x^3 - x^2 + 2, (x^5 + x)y^3 - x^3 y^2].$$

Applying $\mathsf{Reg2Sim}$ to $\mathcal{T}$, we obtain the output of 4 branches:

$$\begin{aligned}
(\mathcal{B}_1, P_1) &= ([x^2 - 2\,x + 2, y],\ [1, 2]),\\
(\mathcal{B}_2, P_2) &= ([x + 1, 2\,y - 1,],\ [1, 1]),\\
(\mathcal{B}_3, P_3) &= ([x + 1, y],\ [1, 2]),\\
(\mathcal{B}_4, P_4) &= ([x^2 - 2\,x + 2, (3\,x - 3)y - 2],\ [1, 1]).
\end{aligned}$$

To count the multiplicity at, e.g., the complex zero $\boldsymbol{a} = (1 + \mathrm{i}, 0)$ of $\mathcal{T}$, one just check that $\boldsymbol{a}$ is a zero of $\mathcal{B}_1$. Then from P_1, we know that the multiplicity of $\boldsymbol{a}$ is 2.

We give a description of the input and output of the function for computing the multiplicity as follows without entering the details.

Algorithm 3: $M := \mathsf{RegMult}(\mathcal{T}, \boldsymbol{a})$

Input: a zero-dimensional regular set $\underline{\mathcal{T}}$ in $\mathbb{C}[\boldsymbol{x}]$; a zero $\underline{\boldsymbol{a}}$ of $\mathcal{T}$.
Output: the local multiplicity of $\boldsymbol{a}$ in $\operatorname{sat}(\mathcal{T})$.

It should be noted that $\mathsf{Reg2Sim}$ computes not the multiplicity of just one zero of a regular set, but essentially the multiplicities of all its zeros.

Remark 2. The multiplicity array produced by $\mathsf{Reg2Sim}$ may be more appropriate than the local multiplicity in Definition 1 for characterizing the multiplicity. For example, consider ideals $\langle x^2, y^3 \rangle$ and $\langle x^3, y^2 \rangle$ in $\mathbb{C}[x, y]$. It is easy to see that $(0, 0)$ is their unique zero, and the local multiplicities of $(0, 0)$ in these two ideal both equal to 6. But it is obvious that $\langle x^2, y^3 \rangle \neq \langle x^3, y^2 \rangle$, and their Gröbner bases are different under a same term order.

It is well known that the Gröbner basis is one of elimination methods that preserve the multiplicity. From the above example, we know that the multiplicity in the Gröbner sense differs from the local multiplicity, but is closer to the multiplicity array. For the above example, the multiplicity array $[2, 3]$ of $\langle x^2, y^3\rangle$ is distinct from the multiplicity array $[3, 2]$ of $\langle x^3, y^2\rangle$. It never occurs that ideals of zero-dimensional regular sets are different but with same zeros and same multiplicity arrays.

Remark 3. Zhang and others[25] proposed an approach for isolating real solutions of a zero-dimensional triangular set as well as counting their multiplicities. It should be noted that the real solution isolation with multiplicity of any given zero-dimensional regular set $\mathcal{T}$ can also be easily obtained from the output of $\mathsf{Reg2Sim}(\mathcal{T})$.

The first step is to compute the real solution isolation of $\mathcal{T}$, i.e. "boxes" of the form $\big[[a_1, b_1], \dots, [a_n, b_n]\big]$ with rational a_i and b_i such that each box contains exact one real zero of $\mathcal{T}$[32]. Let $[\mathcal{B}_1, P_1], \dots, [\mathcal{B}_k, P_k]$ be the output of $\mathsf{Reg2Sim}(\mathcal{T})$. For each box $\big[[a_1, b_1], \dots, [a_n, b_n]\big]$ that covers one zero (say $\boldsymbol{a}$) of $\mathcal{T}$, we just need to find the unique $\mathcal{B}_i$ with $\boldsymbol{a}$ as its zero[33]. Then the multiplicity of $\boldsymbol{a}$ can be directly read from P_i.

The approach by Zhang and others[25] computes the simple decomposition of a zero-dimensional generic triangular set with respect to its real solutions and multiplicities. On the other hand, ours can produce the simple decomposition of a zero-dimensional regular set with respect to all its solutions and multiplicities. However, the former method needs not to split triangular sets in the squarefree decomposition over algebraic extension fields, thus may be more efficient.

5 | EXPERIMENTAL RESULTS

Based on the RegularChains library in Maple 13, we have implemented the algorithms proposed in this paper. The Maple package Apatools[34] also provides us with a function for computing the multiplicity of a zero at any zero-dimensional ideal:

MultiplicityStructure(idealBases, variables, zero, threshold),

which is built on the dual space theory and can be executed symbolically or approximately. In order to be fair, we compare our implementation with the symbolic version of MultiplicityStructure by setting the parameter "threshold" to be 0.

All the experiments were running on a laptop with Intel Core i3-2350TM CPU 2.30 GHz, 2G RAM and Windows 7 OS. Table 1 records the timings of selected examples, which are listed in the appendix.

TABLE 1 Timings of MultiplicityStructure and RegMult (in seconds)

No.	Variables	Zero	Multiplicity	MultiplicityStructure	RegMult
$\mathcal{T}_1$	$[x, y]$	(1,1)	1	.109	.093
$\mathcal{T}_2$	$[x, y]$	(1,1)	20	41.840	.047
$\mathcal{T}_3$	$[x, y]$	(2,1)	50	10.593	240.990
$\mathcal{T}_4$	$[x, y]$	(2,1)	105	120.932	3.057
$\mathcal{T}_5$	$[u, s]$	(0,0)	6	0.187	.078
$\mathcal{T}_6$	$[u, s, t, x, y, z]$	(0,0,0,0,0,0)	6	out of memory	.266
$\mathcal{T}_7$	$[x, y, z]$	(0,0,0)	18	2.606	.046
$\mathcal{T}_8$	$[u, s, t, x, y, z]$	(0,0,0,0,0,0)	18	out of memory	.172
$\mathcal{T}_9$	$[u, s, t, x, y, z]$	(0,0,0,0,0,0)	4	34.383	1.263
$\mathcal{T}_{10}$	$[u, s, t, x, y, z]$	(0,0,0,0,0,0)	24	out of memory	1.076

From Table 1, we can observe that RegMult is much more efficient than MultiplicityStructure in most cases except $\mathcal{T}_3$. One possible reason of the low efficiency of our method on $\mathcal{T}_3$ is that the computation of $\mathsf{psqf}(F, \mathcal{T})$ may be quite heavy if the regular set $\mathcal{T}$ is complex and the factors of F have high exponents.

One can also see that the efficiency of MultiplicityStructure decreases rapidly with the multiplicity going up. Moreover, if the number of variables is big, the multiplicity matrix (the most important intermediate object in the execution of MultiplicityStructure) may become huge even though the involved regular set has simple structure. In this case, the computation of MultiplicityStructure could be fairly time-consuming and the needed memory space would be unimaginable. However, our new algorithms do not suffer from these problems.

ACKNOWLEDGMENTS

The authors wish to thank Dongming Wang and Bican Xia for beneficial discussions.

Financial disclosure

This work has been supported by National Natural Science Foundation of China (No. 11601023).

Conflict of interest

The authors declare no potential conflict of interests.

□

APPENDIX

A EXAMPLES IN TIMINGS

$\mathcal{T}_1 = [x(x-1), y^{20}(y-1)]$.
$\mathcal{T}_2 = [x(x-1)^{20}, y(y-1)]$.
$\mathcal{T}_3 = [1235556(x-2)^5(234156\,x^4 + 3456\,x + 23677134)^2, 23566234(x^3 + 23\,x)(y-1)^{10}(x^2y^3 + 2346234\,y)]$.
$\mathcal{T}_4 = [1235556(x-2)^{21}(234156\,x^4 + 3456\,x + 23677134)^2, 23566234(x^3 + 23\,x)(y-1)^5(x^2y^3 + 2346234\,y)]$.
$\mathcal{T}_5 = [u^2(u-1)(u^2+u+1), ((u+1)s^3-u)(s^4+1)]$.
$\mathcal{T}_6 = [u^2(u-1)(u^2+u+1), ((u+1)s^3-u)(s^4+1), t, x, y, z]$.
$\mathcal{T}_7 = [1275467\,x^3(23564882\,x - 60289123), 2892349145(y-x)^2(912318912759\,y + 29375\,x - 12366), (7987326611\,z^2 - 9712375656\,xy^2)z]$.
$\mathcal{T}_8 = [u, s, t, 1275467\,x^3(23564882\,x - 60289123), 2892349145(y-x)^2(912318912759\,y + 29375\,x - 12366), (7987326611\,z^2 - 9712375656\,xy^2)z]$.
$\mathcal{T}_9 = [u(u-1), (s-u)(s+u-1), (t-s)(t+u+s-1), (x-t)(x+u+s+t-1), (y-x)(y+u+s+t+x-1), (z-y)^4(z+u+s+t+x+y-1)]$.
$\mathcal{T}_{10} = [u^2(u-1), (s-u)(s+u-1), (t-s)^2(t+u+s-1), (x-t)^3(x+u+s+t-1), (y-x)^2(y+u+s+t+x-1), (z-y)(z+u+s+t+x+y-1)]$.

References

1. M. G. Marinari, T. Mora, H. M. Möller, Gröbner duality and multiplicities in polynomial system solving, in: A. H. M. Levelt (Ed.), Proceedings of the 1995 International Symposium on Symbolic and Algebraic Aomputation, ACM, New York, 1995, pp. 167–179.

2. H. M. Möller, H. J. Stetter, Multivariate polynomial equations with multiple zeros solved by matrix eigenproblems, Numerische Mathematik 70 (3) (1995) 311–329.

3. H. J. Stetter, Matrix eigenproblems are at the heart of polynomial system solving, ACM SIGSAM Bulletin 30 (4) (1996) 22–25.

4. B. H. Dayton, T.-Y. Li, Z. Zeng, Multiple zeros of nonlinear systems, Mathematics of Computation 80 (276) (2011) 2143–2168.

5. B. H. Dayton, Z. Zeng, Computing the multiplicity structure in solving polynomial systems, in: M. Kauers (Ed.), Proceedings of the 2005 International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2005, pp. 116–123.
6. W.-T. Wu, On zeros of algebraic equations: an application of Ritt principle, Kexue Tongbao 31 (1) (1986) 1–5.
7. W.-T. Wu, Basic principles of mechanical theorem proving in elementary geometries, Journal of Automated Reasoning 2 (3) (1986) 221–252.
8. J. F. Ritt, Differential Algebra, American Mathematical Society, Providence, 1950.
9. M. Kalkbrener, A generalized Euclidean algorithm for computing triangular representations of algebraic varieties, Journal of Symbolic Computation 15 (2) (1993) 143–167.
10. L. Yang, J.-Z. Zhang, Searching dependency between algebraic equations: an algorithm applied to automated reasoning, in: J. Johnson, S. McKee, A. Vella (Eds.), Artificial Intelligence in Mathematics, Oxford University Press, Oxford, 1994, pp. 147–156.
11. D. Wang, Computing triangular systems and regular systems, Journal of Symbolic Computation 30 (2) (2000) 221–236.
12. E. Hubert, Notes on triangular sets and triangulation-decomposition algorithms I: Polynomial systems, in: F. Winkler, U. Langer (Eds.), Symbolic and Numerical Scientific Computation, Vol. 2630 of Lecture Note in Computer Science, Springer, Berlin, 2003, pp. 143–158.
13. D. Lazard, A new method for solving algebraic systems of positive dimension, Discrete Applied Mathematics 33 (1–3) (1991) 147–160.
14. M. Moreno Maza, On triangular decompositions of algebraic varieties, Technical Report 4/99, NAG, UK, Presented at the MEGA-2000 Conference, Bath, UK.
15. C. Chen, M. Moreno Maza, Algorithms for computing triangular decompositions of polynomial systems, in: A. Leykin (Ed.), Proceedings of the 36th International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2011, pp. 83–90.
16. D. Wang, An elimination method for polynomial systems, Journal of Symbolic Computation 16 (2) (1993) 83–114.
17. D. Wang, Decomposing polynomial systems into simple systems, Journal of Symbolic Computation 25 (3) (1998) 295–314.
18. G. Gallo, B. Mishra, Wu-Ritt characteristic sets and their complexity, in: J. E. Goodman, R. D. Pollack, W. Steiger (Eds.), Discrete and Computational Geometry: Papers from the DIMACS Special Year, Vol. 6 of Discrete Mathematics and Theoretical Computer Science, American Mathematical Society, Providence, 1991, pp. 111–136.
19. G. Gallo, B. Mishra, Efficient algorithms and bounds for Wu-Ritt characteristic sets, in: T. Mora, C. Traverso (Eds.), Effective Methods in Algebraic Geometry, Vol. 94 of Progress in Mathematics, Birkhauser, Berlin, 1991, pp. 119–142.
20. X.-S. Gao, S.-C. Chou, On the dimension of an arbitrary ascending chain, Chinese Science Bulletin 38 (5) (1993) 396–399.
21. Z. Huang, Y. Sun, D. Lin, On the efficiency of solving boolean polynomial systems with the characteristic set method, Journal of Symbolic Computation 103 (2021) 66–94.
22. C. Mou, Y. B, J. Lai, Chordal graphs in triangular decomposition in top-down style, Journal of Symbolic Computation 102 (2021) 108–131.
23. D. Wang, R. Dong, C. Mou, Decomposition of polynomial sets into characteristic pairs, Mathematics of Computation 89 (2020) 1993–2015.
24. B. Li, A method to solve algebraic equations up to multiplicities via Ritt-Wu's characteristic sets, Acta Analysis Functionalis Applicata 5 (3) (2005) 98–109.
25. Z. Zhang, T. Fang, B. Xia, Real solution isolation with multiplicity of zero-dimensional triangular systems, Science China Information Sciences 54 (1) (2011) 60–69.

26. P. Aubry, D. Lazard, M. Moreno Maza, On the theories of triangular sets, Journal of Symbolic Computation 28 (1–2) (1999) 105–124.

27. J. M. Thomas, Differential Systems, American Mathematical Society, New York, 1937.

28. X. Li, C. Mou, D. Wang, Decomposing polynomial sets into simple sets over finite fields: The zero-dimensional case, Computers and Mathematics with Applications 60 (11) (2010) 2983–2997.

29. D. Kapur, D. Lu, M. B. Monagan, Y. Sun, D. Wang, Algorithms for computing greatest common divisors of parametric multivariate polynomials, Journal of Symbolic Computation 102 (2021) 3–20.

30. T. Mora, Solving Polynomial Equation Systems I: the Kronecker-Duval Philosophy, Encyclopedia of Mathematics and its Applications, Cambridge University Press, Cambridge, 2003.

31. M. F. Atiyah, I. G. Macdonald, Introduction to Commutative Algebra, Addison-Wesley Series in Mathematics, Addison-Wesley, Reading, Mass., 1969.

32. B. Xia, L. Yang, An algorithm for isolating the real solutions of semi-algebraic systems, Journal of Symbolic Computation 34 (5) (2002) 461–477.

33. B. Xia, X. Hou, A complete algorithm for counting real solutions of polynomial systems of equations and inequalities, Computers and Mathematics with Applications 44 (5–6) (2002) 633–642.

34. Z. Zeng, ApaTools: a software toolbox for approximate polynomial algebra, in: M. E. Stillman, N. Takayama, J. Verschelde (Eds.), Software for Algebraic Geometry, Springer, Berlin, 2008, pp. 149–167.