Rational Univariate Representation of Zero-Dimensional Ideals with Parameters

Dingkang Wang
[1]KLMM, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China
[2]School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing 100049, China
dwang@mmrc.iss.ac.cn

Jingjing Wei
Beijing ETown Academy, Beijing 100176, China
weijingjing18@mails.ucas.ac.cn

Fanghui Xiao
MOE-LCSM, School of Mathematics and Statistics, Hunan Normal University, Changsha 410081, China
xiaofanghui@hunnu.edu.cn

Xiaopeng Zheng
[1]KLMM, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China
[2]School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing 100049, China
zhengxiaopeng@amss.ac.cn

ABSTRACT

An algorithm for computing the rational univariate representation of zero-dimensional ideals with parameters is presented in the paper. Different from the rational univariate representation of zero-dimensional ideals without parameters, the number of zeros of zero-dimensional ideals with parameters under various specializations is different, which leads to choosing and checking the separating element, the key to computing the rational univariate representation, is difficult. In order to pick out the separating element, by partitioning the parameter space we can ensure that under each branch the ideal has the same number of zeros. Subsequently based on the extended subresultant theorem for parametric cases, the separating element corresponding to each branch is chosen with the further partition of parameter space. Finally, with the help of parametric greatest common divisor theory a finite set of the rational univariate representation of zero-dimensional ideals with parameters can be obtained.

CCS CONCEPTS

• **Computing methodologies** → **Symbolic and algebraic algorithms**; **Algebraic algorithms**; **Symbolic calculus algorithms**; **Equation and inequality solving algorithms**;

KEYWORDS

Rational univariate representation, Parametric zero-dimensional ideal, Comprehensive Gröbner system

ISSAC '22, July 4–7, 2022, Villeneuve-d'Ascq, France

ACM ISBN 978-1-4503-8688-3/22/07…$15.00
https://doi.org/10.1145/3476446.3535496

ACM Reference Format:
Dingkang Wang, Jingjing Wei, Fanghui Xiao, and Xiaopeng Zheng. 2022. Rational Univariate Representation of Zero-Dimensional Ideals with Parameters. In *Proceedings of the 2022 International Symposium on Symbolic and Algebraic Computation (ISSAC '22), July 4–7, 2022, Villeneuve-d'Ascq, France.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3476446.3535496

1 INTRODUCTION

Solving multivariate polynomial equations has always been a classical algebraic problem, which plays an important role in many fields. The rapid development of computer technology makes the function of computer algebra system perfect. Thus, it provides a new opportunity for the solution of polynomial equations. Many new methods for solving polynomial equations have emerged in computer algebra and algebraic geometry, such as Wu's method [26], Gröbner basis method [2], resultant-based method [3]and eigenvalue methods [1, 20]. These new theories and methods inject new vitality into the solution of polynomial equations, making them more and more widely used in computer-aided design, computer vision, cybernetics, robot trajectory design, curve and surface design and modeling.

Rouillier [16] in 1999 proposed the rational univariate representation (RUR) to solve zero-dimensional polynomial systems and presented an efficient algorithm for computing rational univariate representations. The rational univariate representation consists in expressing all the coordinates of the roots for zero-dimensional ideal $I \subset k[x_1, \ldots, x_n]$ (where k is a field of characteristic 0) as rational functions of the roots of an univariate polynomial. That is, the roots of I can be represented in the following way:

$$\mathbb{V}_L(I) = \left\{ \left(\frac{g_1(\beta)}{g(\beta)}, \ldots, \frac{g_n(\beta)}{g(\beta)} \right) \middle| \, \beta \in \mathbb{V}_L(\mathcal{X}(T)) \right\},$$

where $\mathcal{X}, g, g_1, \ldots, g_n \in k[T]$ are univariate polynomials, L is an algebraic closure of k, $\mathbb{V}_L(I)$ is the variety of I in L^n. Since then, it has been extensively studied. Noro and Yokoyama [14] used modular method to compute the rational univariate representation of zero-dimensional ideal. Ouchi and Keyser [15] based on toric resultants gave the computation of the rational univariate representation. Tan

and Zhang [23] presented an improved algorithm for finding separating elements of zero-dimensional ideals. Zeng and Xiao [28] proposed a method for computing the rational univariate representation by Wu's method. Ma, et al. [8] presented an approach to compute the rational univariate representation via properties of Gröbner basis.

Tan and Zhang [22, 24] generalized the rational univariate representation theory to high-dimensional polynomial systems and proposed the rational representation theory. Along this, Shang, et al. [19] proposed a simplified rational representation and Xiao et al. [27] presented an improvement of the rational representation by introducing minimal Dickson basis proposed by [7]. Similar to rational representation, Schost [18] proposed parametric geometric resolution and Safey El Din et al. [17] used rational parametrizations to represent all irreducible components of real algebraic sets.

Although the rational representation of polynomial systems has formed a relatively perfect theory, the research on the rational representation of polynomial systems with parameters as the method of solving parametric multivariate polynomial equations is still blank. In this paper, we extend the rational univariate representation of zero-dimensional ideals to the parametric case. Given an ideal $I = \langle f_1(U,X), \ldots, f_l(U,X)\rangle \subset k[U,X]$ with variables X and parameters U. The considered problem is to find finite sets $E_i, N_i \subset k[U]$, $i \in \{1,\ldots,s\}$ such that for all $\bar{u} \in \mathbb{V}_L(E_i)\backslash\mathbb{V}_L(N_i)$, $I(\bar{u}) = \langle f_1(\bar{u},X), \ldots, f_l(\bar{u},X)\rangle \subset L[X]$ is a zero-dimensional ideal and give an RUR of $I(\bar{u})$ to express the variety:

$$\mathbb{V}_L(I(\bar{u})) = \left\{ \left(\frac{g_{i1}(\bar{u},\beta)}{g_i(\bar{u},\beta)}, \ldots, \frac{g_{in}(\bar{u},\beta)}{g_i(\bar{u},\beta)} \right) \Big| \ \beta \in \mathbb{V}_L(\mathcal{X}_i(\bar{u},T)) \right\},$$

where $g_i, g_{i1}, \ldots, g_{in}, \mathcal{X}_i \in k(U)[T]$. That is to compute a finite set:

$$\{(E_1, N_1, \mathcal{X}_1, g_1, g_{11}, \ldots, g_{1n}), \ldots, (E_s, N_s, \mathcal{X}_s, g_s, g_{s1}, \ldots, g_{sn})\}.$$

The idea is based on the partition of parameter space, which contains four steps. First, by means of comprehensive Gröbner systems (see [5, 7, 11, 12, 21, 25]) and Finiteness theorem, we pick out the zero-dimensional branches which satisfy the ideal is zero-dimensional under parametric specializations. Different from the rational univariate representation of zero-dimensional ideals without parameters, the number of zeros for zero-dimensional ideals with parameters under various specializations is different, which leads to choosing and checking the separating element, the premise and the key to computing the rational univariate representation, is difficult. Thus, the second step is to determine the number of zeros by partitioning of the parameter space such that each branch of parameter space has the same number of zeros. Subsequently, we use extended subresultant theorem [10] for parametric cases to choose the separating element corresponding to each branch with the further partition of parameter space. Finally, with the help of parametric greatest common divisor theory [6, 13] a finite set of which each branch shares the same expression of rational univariate representation can be obtained.

This paper is organized as follows. In Section 2, we introduce some notations and definitions, and extend the subresultant theorem to parametric cases. The main content is presented in Section 3. We use comprehensive Gröbner systems, the extended subresultant theorem and parametric greatest common divisors to give the rational univariate representation of zero-dimensional ideals with parameters. In Section 4, we proposed the algorithm for computing rational univariate representations of parametric zero-dimensional ideals and give an example to illustrate this algorithm. We end with some concluding remarks in Section 5.

2 PRELIMINARIES

In this section we will introduce some notations and definitions to prepare for the discussion of this article.

Let k be a field of characteristic 0, and L be its algebraic closure. $k[X]$ is the polynomial ring over k in the variables $X = \{x_1, \ldots, x_n\}$ and $k[U,X]$ is the parametric polynomial ring with the parameters $U = \{u_1, \ldots, u_m\}$ and variables X. I is an ideal of $k[X]$ and $\mathbb{V}_L(I)$ is the variety of I in L^n.

2.1 Rational univariate representation

Let $I \subset k[X]$ be a zero-dimensional ideal. Since I is zero-dimensional, $k[X]/I$ is a linear space over k by Finiteness theorem. For all $t \in k[X]$, we denote by m_t the $k-$linear map:

$$\begin{aligned} m_t : k[X]/I &\to k[X]/I \\ \overline{f} &\mapsto \overline{tf}, \end{aligned}$$

where $\overline{f}$ denotes the residue class in $k[X]/I$ of any polynomial $f \in k[X]$.

We denote by M_t the matrix representation of m_t w.r.t. a basis in quotient ring $k[X]/I$. And we call m_t the multiplication map and M_t the multiplication matrix.

Theorem 2.1 ([16]). *Let $I \subset k[X]$ be a zero-dimensional ideal, $t \in k[X]$ and m_t be the multiplication map. Then the eigenvalues of M_t are $\{t(p) : p \in \mathbb{V}_L(I)\}$. More specifically, the characteristic polynomial of m_t is*

$$\mathcal{X}_t(T) = \prod_{p \in \mathbb{V}_L(I)} (T - t(p))^{\mu(p)},$$

where $\mu(p)$ is the multiplicity of p in $\mathbb{V}_L(I)$.

Similarly, given the polynomial $h \in k[X]$, we can construct a bilinear form

$$S_h(f,g) = \mathrm{Tr}(m_{hf} \cdot m_g) = \mathrm{Tr}(m_{hfg}).$$

Suppose that $B = \{X^{\alpha_1}, \ldots, X^{\alpha_s}\}$ is a basis of $k[X]/I$. Let Q_h be the matrix of S_h w.r.t. B, i.e., $Q_h = (S_h(X^{\alpha_i}, X^{\alpha_j}))_{1 \le i,j \le s} \in k^{s \times s}$. Q_h is called the Hermite's quadratic form associated h w.r.t. B in quotient ring $k[X]/I$.

Theorem 2.2 ([4], Page 71, Theorem 5.2). *Let $I \subset k[X]$ be a zero-dimensional ideal. Then the number of points in $\mathbb{V}_L(I)$ is equal to the rank of Q_1.*

Next, we review the definition of separating elements which plays an important role in rational univariate representation theory.

Definition 2.3. Let $I \subset k[X]$ be a zero-dimensional ideal. A polynomial $t \in k[X]$ separates $\mathbb{V}_L(I)$, if

$$p_1, p_2 \in \mathbb{V}_L(I), p_1 \neq p_2 \Rightarrow t(p_1) \neq t(p_2).$$

We also call t a separating element of I.

Definition 2.4. Let $I \subset k[X]$ be a zero-dimensional ideal, and $t \in k[X]$. $\mathcal{X}_t$ is the characteristic polynomial of multiplication map m_t. For any $v \in k[X]$, we define:

$$g(v,T) = \sum_{\alpha \in \mathbb{V}_L(I)} \mu(\alpha) v(\alpha) \prod_{y \neq t(\alpha), y \in \mathbb{V}_L(\mathcal{X}_t)} (T - y).$$

For any $t \in k[X]$, the t-representation of I is the $(n+2)$-tuple:

$$\{\mathcal{X}_t(T), g(1,T), g(x_1,T), \ldots, g(x_n,T)\}.$$

If t separates $\mathbb{V}_L(I)$, the t-representation of I is called the **Rational Univariate Representation** (RUR) of I associated to t.

In [16], Rouillier proposed an algorithm to compute the RUR of a zero-dimensional ideal.

Algorithm for Computing the RUR

Input: $I = \langle f_1, \ldots, f_l \rangle \subset k[X]$ is a zero-dimensional ideal.

(1) Compute the Gröbner basis of I with a monomial order $\prec$ and a basis B of $k[X]/I$ over k.
(2) Compute the rank of Q_1 with respect to B.
(3) Set $d = \mathrm{rank}(Q_1)$ and choose $t \in S = \{x_1 + ix_2 + \cdots + i^{n-1}x_n, i = 1, \ldots, nd(d-1)/2\}$ randomly, then compute the characteristic polynomial $\mathcal{X}_t$ of m_t.
(4) Let $\overline{\mathcal{X}_t} = \mathcal{X}_t / \gcd\left(\mathcal{X}_t', \mathcal{X}_t\right)$. If $\deg(\overline{\mathcal{X}_t}) \neq \mathrm{rank}(Q_1)$, then goto (3).
(5) Suppose that $\overline{\mathcal{X}_t} = \sum_{j=0}^{d} a_j T^{d-j}$. Compute

$$g(T) = \sum_{i=0}^{d-1} \sum_{j=0}^{d-i-1} \mathrm{Tr}(m_{t^i}) a_j T^{d-i-j-1}, \tag{1}$$

$$g_k(T) = \sum_{i=0}^{d-1} \sum_{j=0}^{d-i-1} \mathrm{Tr}(m_{x_k t^i}) a_j T^{d-i-j-1}, k = 1, \ldots, n. \tag{2}$$

Output: $\{\mathcal{X}_t(T), g(T), g_1(T), \ldots, g_n(T)\} \subset k[T]$.

By the above algorithm, the variety of I can be represented as

$$\mathbb{V}_L(I) = \left\{ \left(\frac{g_1(\beta)}{g(\beta)}, \ldots, \frac{g_n(\beta)}{g(\beta)} \right) \middle| \, \beta \in \mathbb{V}_L(\mathcal{X}_t(T)) \right\}.$$

There are some remarks:

- The Step (4) is aimed to check whether t is a separating element of I. According to Definition 2.3, Theorem 2.1 and Theorem 2.2, t is a separating element of I if and only if $\deg(\overline{\mathcal{X}_t}) = \mathrm{rank}(Q_1)$. In [16], it has been proved that S contains at least one element that separates $\mathbb{V}_L(I)$.
- We can use Formula (1) and (2) to compute $g(T)$ and $g_i(T)$ only if t is a separating element.
- The RUR of I computed by this algorithm is not unique. It depends on the choice of the separating element.

2.2 Comprehensive Gröbner System and Parametric Greatest Common Divisor

In order to deal with the polynomial system with parameters, we will introduce the comprehensive Gröbner system. Fix a monomial order $\prec_X$ in $k[X]$ and monomial order $\prec_U$ in $k[U]$. Let $\prec_{X,U}$ be a block order, $U \prec\prec X$, within $\prec_U$ and $\prec_X$. For convenience, we often omit writing the order if there is no confusion.

Definition 2.5 ([25]). Let $I = \langle f_1, \ldots, f_l \rangle \subset k[U,X]$, S be a subset of L^m, $G_i = \{g_{i1}, \ldots, g_{it}\} \subset k[U,X]$ and $E_i, N_i \subset k[U]$ for $i = 1, \ldots, s$ such that $S = \bigcup_{i=1}^{l} \mathbb{V}_L(E_i) \backslash \mathbb{V}_L(N_i)$. A finite set

$$\mathcal{G} = \{(E_1, N_1, G_1), \ldots, (E_s, N_s, G_s)\}$$

is called a comprehensive Gröbner system (CGS) on S for I if for every $i \in \{1, \ldots, s\}$, $G_i(\bar{u}) = \{g_{i1}(\bar{u}, X), \ldots, g_{it}(\bar{u}, X)\}$ is a Gröbner basis of $I(\bar{u}) = \langle f_1(\bar{u}, X), \ldots, f_l(\bar{u}, X) \rangle \subset L[X]$ for $\bar{u} \in \mathbb{V}_L(E_i) \backslash \mathbb{V}_L(N_i)$. Each (E_i, N_i, G_i) is called a branch of $\mathcal{G}$. In particular, if $S = L^m$, then $\mathcal{G}$ is called a comprehensive Gröbner system for I.

Definition 2.6. A comprehensive Gröbner system $\mathcal{G} = \{(E_1, N_1, G_1), \ldots, (E_s, N_s, G_s)\}$ on S for I is said to be minimal, if for each $i = 1, \ldots, s$,

(1) $\mathbb{V}_L(E_i) \backslash \mathbb{V}_L(N_i) \neq \emptyset$, and furthermore, whenever $i \neq j$,
$$\mathbb{V}_L(E_i) \backslash \mathbb{V}_L(N_i) \cap \mathbb{V}_L(E_j) \backslash \mathbb{V}_L(N_j) = \emptyset;$$
(2) $G_i(\bar{u})$ is a minimal Gröbner basis for $I(\bar{u}) \subset L[X]$ for $\bar{u} \in \mathbb{V}_L(E_i) \backslash \mathbb{V}_L(N_i)$;
(3) for each $g \in G_i$, assume that $c_1 = \mathrm{LC}_X(g)$ is the leading coefficient of g w.r.t. X, then $c_1(\bar{u}) \neq 0$ for any $\bar{u} \in \mathbb{V}_L(E_i) \backslash \mathbb{V}_L(N_i)$.

For computing the minimal comprehensive Gröbner system, we can refer to the algorithm proposed by Kapur et al. [7].

Based on the comprehensive Gröbner system, Kapur et al. [6] proposed an efficient algorithm for computing the greatest common divisor of polynomials with parameters.

Definition 2.7. For $F = \{f_1, \ldots, f_l\} \subset k[U][X]$ and $S \subset L^m$, we call $\{(E_1, N_1, g_1), \ldots, (E_r, N_r, g_r)\}$ a parametric GCD of F on S, if for each $i = 1, \ldots, r$, $g_i(\bar{u}, X) \in L[X]$ is a greatest common divisor of $\{f_1(\bar{u}, X), \ldots, f_l(\bar{u}, X)\} \subset L[X]$ for $\bar{u} \in \mathbb{V}_L(E_i) \backslash \mathbb{V}_L(N_i)$, where $E_i, N_i \subset k[U]$, $g_i \in k[U][X]$ for $i = 1, \ldots, r$ and $S = \cup_{i=1}^{r} \mathbb{V}_L(E_i) \backslash \mathbb{V}_L(N_i)$. If $S = k^m$, we simply call it a parametric GCD of F.

2.3 Subresultant and Common Divisor

In the process of computing the RUR, we can see that it is necessary to compute $\gcd(\mathcal{X}_t', \mathcal{X}_t)$. Therefore, if the polynomial system is with parameters, we need to discuss the relationship between $\gcd(\mathcal{X}_t', \mathcal{X}_t)$ and the value of parameters. In the following, we will build the connection between the degree of $\gcd(\mathcal{X}_t', \mathcal{X}_t)$ and the parameters U by using the subresultant theory.

First, we review the theorem of the subresultant.

Theorem 2.8 ([10]). *Let S be a unique factorization domain with identity, and $A(x), B(x) \in S[x]$ be univariate polynomials of positive degrees m and n, respectively. Then for all $0 \leq i < \min(m,n)$, the following three statements are equivalent:*

(1) *$A(x)$ and $B(x)$ have a common divisor with degree $> i$;*
(2) $(\forall j \leq i) \left[\mathrm{SubRes}_j(A,B) = 0\right]$;
(3) $(\forall j \leq i) \left[\mathrm{PSC}_j(A,B) = 0\right]$.

where $SubRes_j(A,B)$ denotes the ith subresultant of A and B, $PSC_j(A,B)$ denotes the leading coefficient of $SubRes_j(A,B)$.

Now we extend this result to the case for parameters and obtain the relationship between the degree of $\gcd(\mathcal{X}_t', \mathcal{X}_t)$ and the values of parameters.

Lemma 2.9. *Let $\mathcal{X}(U,T) = \sum_{i=0}^{l} c_i(U)T^i \in k[U,T]$ and $E, N \subset k[U]$. Suppose that for $\bar{u} \in \mathbb{V}_L(E)\backslash\mathbb{V}_L(N)$, $c_l(\bar{u}) \neq 0$, then there exist $E_0, \ldots, E_{l-1}, N_0, \ldots, N_{l-1} \subset k[U]$ such that for each $0 \leq i \leq l-1$ and for all $\bar{u} \in \mathbb{V}_L(E)\backslash\mathbb{V}_L(N)$,*

$$\deg\left(\gcd(\mathcal{X}(\bar{u},T), \mathcal{X}'(\bar{u},T))\right) = i \iff \bar{u} \in \mathbb{V}_L(E_i)\backslash\mathbb{V}_L(N_i).$$

where $\mathcal{X}' \in k[U,T]$ is the derivation of $\mathcal{X}$ w.r.t. T.

Proof. We regard $\mathcal{X}$ and $\mathcal{X}'$ as polynomials in $S[T]$, where $S = k[U]$. Then $\mathrm{PSC}_j(\mathcal{X}, \mathcal{X}') \in k[U]$. For $\bar{u} \in \mathbb{V}_L(E)\backslash\mathbb{V}_L(N)$, $c_l(\bar{u}) \neq 0$, so

$$\deg_T(\mathcal{X}(U,T)) = \deg(\mathcal{X}(\bar{u},T)) \text{ and } \deg_T(\mathcal{X}'(U,T)) = \deg(\mathcal{X}'(\bar{u},T)).$$

It implies that the degree of $\mathcal{X}(U,T)$ and $\mathcal{X}'(U,T)$ w.r.t. T does not change under $\bar{u} \in \mathbb{V}_L(E)\backslash\mathbb{V}_L(N)$. By the definition, for $\bar{u} \in \mathbb{V}_L(E)\backslash\mathbb{V}_L(N)$,

$$\mathrm{PSC}_j(\mathcal{X}, \mathcal{X}')(\bar{u}) = \mathrm{PSC}_j(\mathcal{X}(\bar{u},T), \mathcal{X}'(\bar{u},T)), j = 0, 1, \ldots, l-1.$$

Let $\lambda = l - 1$ and

$$E_i = E \cup \{\mathrm{PSC}_j(\mathcal{X}, \mathcal{X}') |\ j < i\},\ 0 \leq i \leq \lambda,$$

$$N_i = N \times \{\mathrm{PSC}_i(\mathcal{X}, \mathcal{X}')\},\ 0 \leq i < \lambda, \text{ and } N_\lambda = N,$$

where $N \times \{f\} = \{gf |\ g \in N\}$). By Theorem 2.8, for each $0 \leq i < \lambda$ and $\bar{u} \in \mathbb{V}_L(E)\backslash\mathbb{V}_L(N)$, the following statements are equivalent:

(1) $\deg\left(\gcd(\mathcal{X}(\bar{u},T), \mathcal{X}'(\bar{u},T))\right) = i$;
(2) $(\forall j < i)$ $[\mathrm{PSC}_j(\mathcal{X}(\bar{u},T), \mathcal{X}'(\bar{u},T)) = 0]$ and $\mathrm{PSC}_i(\mathcal{X}(\bar{u},T), \mathcal{X}'(\bar{u},T)) \neq 0$;
(3) $(\forall j < i)$ $[\mathrm{PSC}_j(\mathcal{X}, \mathcal{X}')(\bar{u}) = 0]$ and $\mathrm{PSC}_i(\mathcal{X}, \mathcal{X}')(\bar{u}) \neq 0$;
(4) $\bar{u} \in \mathbb{V}_L(E_i)\backslash\mathbb{V}_L(N_i)$.

Moreover, it is easy to verify that the conclusion is also true when $i = \lambda$. □

3 RUR OF ZERO-DIMENSIONAL IDEAL WITH PARAMETERS

In the section, we will consider the RUR of zero-dimensional ideal with parameters U. Let $I = \langle f_1(U,X), \ldots, f_l(U,X)\rangle \in k[U,X]$ and $E, N \subset k[U]$. For $f \in k[U]$, $N \times \{f\} = \{gf |\ g \in N\}$. For every $\bar{u} \in \mathbb{V}_L(E)\backslash\mathbb{V}_L(N)$, the ideal generated by $f_1(\bar{u},X), \ldots, f_l(\bar{u},X)$ is denoted by $I(\bar{u})$. We want to find finite sets $E_i, N_i \subset k[U]$, $i \in \{1, \ldots, s\}$ such that for $\bar{u} \in \mathbb{V}_L(E_i)\backslash\mathbb{V}_L(N_i)$, $I(\bar{u})$ is a zero-dimensional ideal and give an RUR of $I(\bar{u})$ to express

$$\mathbb{V}_L(I(\bar{u})) = \left\{ \left(\frac{g_{i1}(\bar{u},\beta)}{g_i(\bar{u},\beta)}, \ldots, \frac{g_{in}(\bar{u},\beta)}{g_i(\bar{u},\beta)} \right) \middle|\ \beta \in \mathbb{V}_L(\mathcal{X}_i(\bar{u},T)) \right\},$$

where $g_i, g_{i1}, \ldots, g_{in}, \mathcal{X}_i \in k(U)[T]$.

The idea is based on the partition of parameter space, which contains four steps.

Step 1. Pick zero-dimensional branches. That is to compute $E_i, N_i \subset k[U]$, $i = 1, \ldots, s$, such that $I(\bar{u})$ is a zero-dimensional ideal if and only if $\bar{u}$ belongs to some $\mathbb{V}_L(E_i)\backslash\mathbb{V}_L(N_i)$.

Step 2. Determine the number of zeros. For each E_i, N_i in Step 1, compute $E_{ij}, N_{ij} \subset k[U]$ such that $\mathbb{V}_L(E_i)\backslash\mathbb{V}_L(N_i) = \bigcup_{j=1}^{s_1} \mathbb{V}_L(E_{ij})\backslash\mathbb{V}_L(N_{ij})$ and for each $j \in \{1, \ldots, s_1\}$, $I(\bar{u})$ has the same number of zeros for all $\bar{u} \in \mathbb{V}_L(E_{ij})\backslash\mathbb{V}_L(N_{ij})$.

Step 3. Choose and check the separating element. For each E_{ij}, N_{ij} in Step 2, compute $E_{ijk}, N_{ijk} \subset k[U]$ such that $\mathbb{V}_L(E_{ij})\backslash\mathbb{V}_L(N_{ij}) = \bigcup_{k=1}^{s_2} \mathbb{V}_L(E_{ijk})\backslash\mathbb{V}_L(N_{ijk})$ and for each $k \in \{1, \ldots, s_2\}$, $I(\bar{u})$ shares the same separating element for all $\bar{u} \in \mathbb{V}_L(E_{ijk})\backslash\mathbb{V}_L(N_{ijk})$.

Step 4. Give the RUR for each branch. For each E_{ijk}, N_{ijk} in Step 3, compute $E_{ijkl}, N_{ijkl} \subset k[U]$ such that $\mathbb{V}_L(E_{ijk})\backslash\mathbb{V}_L(N_{ijk}) = \bigcup_{l=1}^{s_3} \mathbb{V}_L(E_{ijkl})\backslash\mathbb{V}_L(N_{ijkl})$ and for each $l \in \{1, \ldots, s_3\}$, for all $\bar{u} \in \mathbb{V}_L(E_{ijkl})\backslash\mathbb{V}_L(N_{ijkl})$, $I(\bar{u})$ shares the same expression of rational univariate representation.

3.1 Partition according to the Gröbner basis

In fact, Step 1 is easy to be achieved by comprehensive Gröbner system and Finiteness Theorem.

Theorem 3.1 (Finiteness Theorem [4]). *Let $I \subset k[X]$ be an ideal. Then the following conditions are equivalent:*

(1) *The algebra $A = k[x_1, \ldots, x_n]/I$ is finite-dimensional over k.*
(2) *The variety $\mathbb{V}_L(I) \subset L^n$ is a finite set.*
(3) *If G is a Gröbner basis for I, then for each $1 \leq i \leq n$, there is an $m_i \geq 0$ such that $x_i^{m_i} = \mathrm{LM(g)}$ for some $g \in G$, where $\mathrm{LM}(g)$ is the leading monomial of g.*

An ideal satisfying any of the above conditions is said to be zero-dimensional.

Theorem 3.2. *Let $I = \langle f_1(U,X), \ldots, f_l(U,X)\rangle \subset k[U,X]$. There exists a finite set $\{(E_1, N_1, G_1), \ldots, (E_s, N_s, G_s)\}$, such that:*

(1) *$I(\bar{u})$ is a zero-dimensional ideal if and only if*

$$\bar{u} \in \bigcup_{i=1}^{s} \mathbb{V}_L(E_i)\backslash\mathbb{V}_L(N_i).$$

(2) *For $\bar{u} \in \mathbb{V}_L(E_i)\backslash\mathbb{V}_L(N_i)$, $G_i(\bar{u}) = \{g_{i1}(\bar{u},X), \ldots, g_{ie}(\bar{u},X)\}$ is a Gröbner basis of $I(\bar{u})$.*

Proof. We only need to compute the minimal comprehensive Gröbner system $\mathcal{G} = \left\{(E_1, N_1, G_1), \ldots, \left(E_{s_0}, N_{s_0}, G_{s_0}\right)\right\}$ for I. Choose the branches $\left\{\left(E_{i_1}, N_{i_1}, G_{i_1}\right), \ldots, \left(E_{i_l}, N_{i_l}, G_{i_l}\right)\right\}$ which satisfy for each $1 \leq j \leq n$, $k[x_j] \cap \mathrm{LM}_X(G_{i_\upsilon}) \neq \emptyset$ $(\upsilon = 1, \ldots, l)$. By Finiteness Theorem and the definition of minimal comprehensive Gröbner system, $\left\{\left(E_{i_1}, N_{i_1}, G_{i_1}\right), \ldots, \left(E_{i_l}, N_{i_l}, G_{i_l}\right)\right\}$ satisfies the conclusion. □

Remark 1. *For each branch (E_i, N_i, G_i) in Theorem 3.2, and for $\bar{u} \in \mathbb{V}_L(E_i)\backslash\mathbb{V}_L(N_i)$,*

$$\mathrm{LM}(G_i(\bar{u})) = \{\mathrm{LM}(g_{i1}(\bar{u},X)), \ldots, \mathrm{LM}(g_{ie}(\bar{u},X))\}.$$

Therefore, for all $\bar{u} \in \mathbb{V}_L(E_i)\backslash\mathbb{V}_L(N_i)$, $L[X]/I(\bar{u})$ shares the same basis:

$$B_i = \{X^{\alpha_1}, \ldots, X^{\alpha_r} |\ X^{\alpha_j} \notin \langle \mathrm{LM}_X(G_i)\rangle, j = 1, \ldots, r\},$$

where $\mathrm{LM}_X(G)$ is a set of the leading monomials of all elements in G w.r.t. X.

3.2 Partition according to the number of zeros

Actually, Step 2 is a preparation for Step 3. For non-parametric cases, $t \in k[X]$ is a separating element of I if and only if $\deg(\overline{\mathcal{X}_t}) = \mathrm{rank}(Q_1)$, where $\overline{\mathcal{X}_t} = \mathcal{X}_t/\gcd\left(\mathcal{X}_t', \mathcal{X}_t\right)$. As for parametric cases, Q_1 and $\mathcal{X}_t$ are both with parameters. Therefore, choosing a $t \in k[X]$, it should discuss when dose $\deg(\overline{\mathcal{X}_t}) = \mathrm{rank}(Q_1)$ hold with the change of the parameters. First, we need to determine $\mathrm{rank}(Q_1)$, equally the number of zeros for I, under parametric specializations.

Let (E, N, G) be one of the branches obtained in Theorem 3.2 and $G = \{g_1, \ldots, g_e\} \subset k[U, X]$. Then (E, N, G) satisfies that for any $\bar{u} \in \mathbb{V}_L(E)\backslash\mathbb{V}_L(N)$,

(1) $I(\bar{u})$ is zero-dimensional and $G(\bar{u})$ is a Gröbner basis of $I(\bar{u})$;
(2) for each $g \in G$, $c_1(\bar{u}) \neq 0$, where c_1 is the leading coefficient of g w.r.t. X.

Assume that $B = \{X^{\alpha_1}, \ldots, X^{\alpha_r}\}$ be a basis of $L[X]/I(\bar{u})$. For $t \in k[X]$, let R_i be a remainder of $t \cdot X^{\alpha_1}$ on division by G in $k(U)[X]$, i.e.,

$$t \cdot X^{\alpha_i} = \sum_{j=1}^{e} q_{ij} g_j + R_i,\ i = 1, \ldots, r.$$

where $q_{ij}, R_i \in k(U)[X]$ and their denominators are the products of some factors of the leading coefficient of $g_j \in G$ w.r.t. X. So they are not equal to zero under $\bar{u} \in \mathbb{V}_L(E)\backslash\mathbb{V}_L(N)$. Therefore, we have

$$t \cdot X^{\alpha_i} = \sum_{j=1}^{e} q_{ij}(\bar{u}, X) g_j(\bar{u}, X) + R_i(\bar{u}, X),\ i = 1, \ldots, r.$$

The remainder of $t \cdot X^{\alpha_1}$ on division by $G(\bar{u})$ in $L[X]$ is equal to $R_i(\bar{u}, X)$. Let $M_t^I \in k(U)^{r\times r}$ be the matrix satisfying

$$(R_1, \ldots, R_r) = B \cdot M_t^I,$$

For any $\bar{u} \in \mathbb{V}_L(E)\backslash\mathbb{V}_L(N)$,

$$(R_1(\bar{u}, X), \ldots, R_r(\bar{u}, X)) = B \cdot M_t^I(\bar{u}).$$

Assume that $M_t^{I(\bar{u})}$ is the multiplication matrix of t w.r.t. B in quotient ring $L[X]/I(\bar{u})$. Then $M_t^I(\bar{u}) = M_t^{I(\bar{u})}$. Therefore, we obtain the following lemma.

Lemma 3.3. *Let (E, N, G), B and $M_t^I \in k(U)^{r\times r}$ be as defined above. For any $\bar{u} \in \mathbb{V}_L(E)\backslash\mathbb{V}_L(N)$,*

(1) *The multiplication matrix $M_t^{I(\bar{u})}$ of t w.r.t. B in quotient ring $L[X]/I(\bar{u})$ is equal to $M_t^I(\bar{u})$.*
(2) *Assume that the characteristic polynomial of M_t^I over $k(U)$ is $\mathcal{X}_t(U, T)$, then the characteristic polynomial of $M_t^{I(\bar{u})}$ over L is $\mathcal{X}_t(\bar{u}, T)$.*
(3) *Let $h \in k[X]$, $Q_h^I \triangleq (Tr(M^I_{hX^{\alpha_i}X^{\alpha_j}}))_{1\le i,j\le r}$ be a $r \times r$ matrix over $k(U)$. Then the Hermite's quadratic form associated h w.r.t. B in quotient ring $L[X]/I(\bar{u})$ is equal to $Q_h^I(\bar{u})$.*

By the above analysis, first we compute $Q_1^I \in k(U)^{r\times r}$ defined above. For all $\bar{u} \in \mathbb{V}_L(E)\backslash\mathbb{V}_L(N)$, $Q_1^{I(u)} = Q_1^I(u)$ by Lemma 3.3 and the number of points in $\mathbb{V}_L(I(\bar{u}))$ is equal to $\mathrm{rank}(Q_1^{I(u)})$ by Theorem 2.2.

Theorem 3.4. *Let (E, N, G) be one of the branches in Theorem 3.2. Then there exists a finite set*

$$\{(E_1, N_1, k_1), \ldots, (E_s, N_s, k_s)\},\ E_i,\ N_i \subset k[U],\ k_i \in \mathbb{Z}_{>0},$$

such that $\mathbb{V}_L(E)\backslash\mathbb{V}_L(N) = \cup_{i=1}^{s} \mathbb{V}_L(E_i)\backslash\mathbb{V}_L(N_i)$ and for each $i \in \{1, \ldots, s\}$ and all $\bar{u} \in \mathbb{V}_L(E_i)\backslash\mathbb{V}_L(N_i)$, the number of points in $\mathbb{V}_L(I(\bar{u}))$ is equal to k_i.

Proof. We first compute $Q_1^I \in k(U)^{r\times r}$ as defined above. It suffices to discuss $\mathrm{rank}(Q_1^I(\bar{u}))$ for $\bar{u} \in \mathbb{V}_L(E)\backslash\mathbb{V}_L(N)$. Let D is the least common multiple of all denominators of entries in Q_1^I. Then $D \in k[U]$ and $D(\bar{u}) \neq 0$ for any $\bar{u} \in \mathbb{V}_L(E)\backslash\mathbb{V}_L(N)$. Let $Q = D \cdot Q_1^I \in k[U]^{r\times r}$. It suffices to discuss $\mathrm{rank}(Q(\bar{u}))$.

Assume that $Q = (f_{ij})_{1\le i,j\le r}$. Using the method in [9], we construct polynomial $f_i = \sum_{j=1}^{r} f_{ij} z_j \in k[U][Z], Z = \{z_1, \ldots, z_r\}$, $i = 1, \ldots, r$. Compute the minimal comprehensive Gröbner system $\mathcal{G} = \{(E_1, N_1, G_1), \ldots, (E_s, N_s, G_s)\}$ of $F = \{f_1, \ldots, f_r\}$ where U is the parameters. By Theorem 1 and Theorem 2 in [9], for any $\bar{u} \in \mathbb{V}_L(E_i)\backslash\mathbb{V}_L(N_i)$, the rank of $Q(\bar{u})$ is equal to the number of elements in G_i. Let k_i denote the number of elements in G_i, $\{(E_1, N_1, k_1), \ldots, (E_s, N_s, k_s)\}$ satisfies the conditions we need. □

3.3 Partition according to separating elements

Choosing the separating element is the key to obtain the rational univariate representation. In the following, we will analyze each branch in Theorem 3.4. Assume that for all $\bar{u} \in \mathbb{V}_L(E)\backslash\mathbb{V}_L(N)$, the number of points in $\mathbb{V}_L(I(\bar{u}))$ is the same, denoted by k_0.

If $k_0 = 1$, we can choose $t = 1$ which is a separating element of $I(\bar{u})$ for $\bar{u} \in \mathbb{V}_L(E)\backslash\mathbb{V}_L(N)$. Otherwise, choose randomly a $t \in \{x_1 + ix_2 + \cdots + i^{n-1}x_n, i = 1 \ldots nk_0(k_0-1)/2\}$. $\mathbb{V}_L(E)\backslash\mathbb{V}_L(N)$ can be divided into two parts, $\mathbb{V}_L(E_i)\backslash\mathbb{V}_L(N_i)$, $i = 1, 2$, where

(1) t is a separating element of $I(\bar{u})$ for $\bar{u} \in \mathbb{V}_L(E_1)\backslash\mathbb{V}_L(N_1)$.
(2) t is not a separating element of $I(\bar{u})$ for $\bar{u} \in \mathbb{V}_L(E_2)\backslash\mathbb{V}_L(N_2)$.

We will prove in fact the second part is "small enough" in numbers of points. Thus we first find a separating element for the most part of $\mathbb{V}_L(E)\backslash\mathbb{V}_L(N)$. For the small part, we will choose another $t \in k[X]$. Sequentially, it does a recursive procedure.

Theorem 3.5. *Let $I = \langle f_1(U, X), \ldots, f_l(U, X)\rangle \subset k[U, X], E, N \subset k[U], G \subset k[U, X]$. Assume that for all $\bar{u} \in \mathbb{V}_L(E)\backslash\mathbb{V}_L(N)$,*

(1) *$I(\bar{u})$ is zero-dimensional and $G(\bar{u})$ is a Gröbner basis of $I(\bar{u})$;*
(2) *for each $g \in G$, $c_1(\bar{u}) \neq 0$, where c_1 is the leading coefficient of g w.r.t. X;*
(3) *the number of points in $\mathbb{V}_L(I(\bar{u}))$ is equal to $k_0 \neq 1$.*

Suppose that $t \in k[X]$, $\mathcal{X}_t(U, T) \in k(U)[T]$ is the characteristic polynomial as defined in Lemma 3.3. Let $\mathcal{X}(U, T) \in k[U][T]$ (briefly, $\mathcal{X}$)be the product of $\mathcal{X}_t(U, T)$ and the least common multiple of all denominators of $\mathcal{X}_t(U, T)$. Then t is separating element of $I(\bar{u})$ if and only if $\bar{u} \in \mathbb{V}_L(E)\backslash\mathbb{V}_L(N \times \{\mathrm{PSC}_d(\mathcal{X}, \mathcal{X}')\}) \neq \emptyset$.

Proof. By Definition 2.3 and Theorem 2.1, for $\bar{u} \in \mathbb{V}_L(E)\backslash\mathbb{V}_L(N)$, t is a separating element of $I(\bar{u})$ if and only

$$\deg\left(\frac{\mathcal{X}(\bar{u}, T)}{\gcd(\mathcal{X}'(\bar{u}, T), \mathcal{X}(\bar{u}, T))}\right) = k_0,$$

which is equivalent to

$$\deg(\gcd\left(\mathcal{X}'(\bar{u}, T), \mathcal{X}(\bar{u}, T)\right)) = \deg(\mathcal{X}(\bar{u}, T)) - k_0.$$

Since $\deg_T(\mathcal{X}) = \deg(\mathcal{X}(\bar{u}, T))$, the above equation becomes

$$\deg(\gcd\left(\mathcal{X}'(\bar{u}, T), \mathcal{X}(\bar{u}, T)\right)) = \deg_T(\mathcal{X}) - k_0.$$

Let $d = \deg_T(\mathcal{X}) - k_0$. By Theorem 2.1, for any $\bar{u} \in \mathbb{V}_L(E)\backslash\mathbb{V}_L(N)$, $\mathcal{X}(\bar{u}, T)$ has at most k_0 distinct roots. It implies that

$$\deg(\gcd\left(\mathcal{X}'(\bar{u}, T), \mathcal{X}(\bar{u}, T)\right)) \geq d.$$

Since $k_0 \neq 1$, $\deg_T(\mathcal{X}') = \deg_T(\mathcal{X}) - 1 > \deg_T(\mathcal{X}) - k_0 = d$. By Theorem 2.8 and the proof of Lemma 2.9,

$$\deg(\gcd\left(\mathcal{X}'(\bar{u}, T), \mathcal{X}(\bar{u}, T)\right)) \leq d \iff \mathrm{PSC}_d(\mathcal{X}, \mathcal{X}')(\bar{u}) \neq 0.$$

Let $N_1 = N \times \{\mathrm{PSC}_d(\mathcal{X}, \mathcal{X}')\}$. Then,

$$\deg(\gcd(\mathcal{X}'(\bar{u}, T), \mathcal{X}(\bar{u}, T))) = d \iff \bar{u} \in \mathbb{V}_L(E)\backslash\mathbb{V}_L(N_1) \neq \emptyset.$$

Thus, t is separating element of $I(\bar{u})$ if and only if $\bar{u} \in \mathbb{V}_L(E)\backslash\mathbb{V}_L(N \times \{\mathrm{PSC}_d(\mathcal{X}, \mathcal{X}')\}) \neq \emptyset$. □

Remark 2. (1) *For non-parametric cases, choosing t from S randomly, t is a separating element of some zero-dimensional ideal with probability 1. Therefore, it is easy to choose a t satisfying Theorem 3.5.*
(2) *For $E, N \in k[U]$, we can use the method in [7] to check whether $\mathbb{V}_L(E)\backslash\mathbb{V}_L(N) = \emptyset$.*

Theorem 3.6. *Let $I = \langle f_1(U, X), \ldots, f_l(U, X)\rangle \subset k[U, X], E, N \subset k[U]$, $G \subset k[U, X]$. Assume that for all $\bar{u} \in \mathbb{V}_L(E)\backslash\mathbb{V}_L(N)$,*

(1) *$I(\bar{u})$ is zero-dimensional and $G(\bar{u})$ is a Gröbner basis of $I(\bar{u})$;*
(2) *for each $g \in G$, $c_1(\bar{u}) \neq 0$, where c_1 is the leading coefficient of g w.r.t. X;*
(3) *the number of points in $\mathbb{V}_L(I(\bar{u}))$ is equal to k_0.*

Then there is a finite set

$$\{(E_1, N_1, t_1), \ldots, (E_s, N_s, t_s)\},\ E_i, N_i \subset k[U],\ t_i \in k[X],$$

such that $\mathbb{V}_L(E)\backslash\mathbb{V}_L(N) = \cup_{i=1}^{s}\mathbb{V}_L(E_i)\backslash\mathbb{V}_L(N_i)$ and for each $i \in \{1, \ldots, s\}$, t_i is a separating element of $I(\bar{u})$ for $\bar{u} \in \mathbb{V}_L(E_i)\backslash\mathbb{V}_L(N_i)$.

Proof. If $k_0 = 1$, then $t_1 = 1$, $E_1 = E$, $N_1 = N$ and it is done. When $k_0 \neq 1$, we choose $t \in S = \{x_1 + ix_2 + \cdots + i^{n-1}x_n, i = 1 \ldots nk_0(k_0-1)/2\}$. By Theorem 3.5, if $\mathbb{V}_L(E)\backslash\mathbb{V}_L(N \times \{\mathrm{PSC}_d(\mathcal{X}, \mathcal{X}')\}) = \emptyset$, pick another t from S; otherwise, let $t_1 = t, E_1 = E, N_1 = N \times \{\mathrm{PSC}_d(\mathcal{X}, \mathcal{X}')\}, E_{10} = E \cup \{\mathrm{PSC}_d(\mathcal{X}, \mathcal{X}')\}, N_{10} = N$. Then

$$\mathbb{V}_L(E)\backslash\mathbb{V}_L(N) = \mathbb{V}_L(E_1)\backslash\mathbb{V}_L(N_1) \cup \mathbb{V}_L(E_{10})\backslash\mathbb{V}_L(N_{10})$$

and t_1 is a separating element of $I(\bar{u})$ for $\bar{u} \in \mathbb{V}_L(E_1)\backslash\mathbb{V}_L(N_1)$. If $\mathbb{V}_L(E_{10})\backslash\mathbb{V}_L(N_{10}) = \emptyset$, it is done. Otherwise, it implies from $\mathbb{V}_L(E_1)\backslash\mathbb{V}_L(N_1) \neq \emptyset$ that $\mathrm{PSC}_d(\mathcal{X}, \mathcal{X}') \notin \langle E\rangle$. Thus $\langle E\rangle \subsetneq \langle E_{10}\rangle$. Continually, using Theorem 3.5 to (E_{10}, N_{10}) and choosing $t_2 \in S$, we have

$$\mathbb{V}_L(E_{10})\backslash\mathbb{V}_L(N_{10}) = \mathbb{V}_L(E_2)\backslash\mathbb{V}_L(N_2) \cup \mathbb{V}_L(E_{20})\backslash\mathbb{V}_L(N_{20})$$

and t_2 is a separating element of $I(\bar{u})$ for $\bar{u} \in \mathbb{V}_L(E_2)\backslash\mathbb{V}_L(N_2)$. If $\mathbb{V}_L(E_{20})\backslash\mathbb{V}_L(N_{20}) = \emptyset$, it is done. Otherwise, $\langle E_{10}\rangle \subsetneq \langle E_{20}\rangle$. Go on like this, we get strictly ascending ideal chains:

$$E \subsetneq E_{10} \subsetneq E_{20} \subsetneq E_{30} \subsetneq \cdots.$$

According to the ascending chains condition, it must stop in finite steps. Thus, we obtain a finite set

$$\{(E_1, N_1, t_1), \ldots, (E_s, N_s, t_s)\},\ E_i, N_i \subset k[U],\ t_i \in k[X],$$

such that $\mathbb{V}_L(E)\backslash\mathbb{V}_L(N) = \cup_{i=1}^{s}\mathbb{V}_L(E_i)\backslash\mathbb{V}_L(N_i)$ and for each $i \in \{1, \ldots, s\}$, t_i is a separating element of $I(\bar{u})$ for $\bar{u} \in \mathbb{V}_L(E_i)\backslash\mathbb{V}_L(N_i)$. □

3.4 Partitions according to GCDs of $\mathcal{X}_t$ and $\mathcal{X}'_t$

Suppose that (E, N, t) is one of branches in Theorem 3.6. That is, t is a separating element of $I(\bar{u})$ for any $\bar{u} \in \mathbb{V}_L(E)\backslash\mathbb{V}_L(N)$. We know if one obtain the RUR then you have to compute the GCD of $\mathcal{X}_t$ and $\mathcal{X}'_t$. However, for different $\bar{u} \in \mathbb{V}_L(E)\backslash\mathbb{V}_L(N)$, the GCD of $\mathcal{X}_t(\bar{u}, T)$ and $\mathcal{X}'_t(\bar{u}, T)$ may be different. In order to obtain the RUR with parameters, one needs to use parametric GCD algorithm in [6]. $\mathbb{V}_L(E)\backslash\mathbb{V}_L(N)$ will be divided into finite branches. In each branch the GCD of $\mathcal{X}_t$ and $\mathcal{X}'_t$ has the same expression, then by adjusting Formula (1), (2) in Section 2.1 to $k(U)[T]$, we can compute $g(U, T)$, $g_1(U, T), \ldots, g_n(U, T)$ and obtain an RUR for each branch.

Theorem 3.7. *Let $I = \langle f_1(U, X), \ldots, f_l(U, X)\rangle \subset k[U, X], E, N \subset k[U]$, $G \subset k[U, X]$, $t \in k[X]$. Assume that for all $\bar{u} \in \mathbb{V}_L(E)\backslash\mathbb{V}_L(N)$,*

(1) *$I(\bar{u})$ is zero-dimensional and $G(\bar{u})$ is a Gröbner basis of $I(\bar{u})$;*
(2) *for each $g \in G$, $c_1(\bar{u}) \neq 0$, where c_1 is the leading coefficient of g w.r.t. X;*
(3) *t is a separating element of $I(\bar{u})$.*

Let $\mathcal{X}_t(U, T) \in k(U)[T]$ be the characteristic polynomial as defined in Lemma 3.3. Then there is a finite set

$$\{(E_1, N_1, \mathcal{X}_t, g_1, g_{11}, \ldots, g_{1n}), \ldots, (E_s, N_s, \mathcal{X}_t, g_s, g_{s1}, \ldots, g_{sn})\},$$

such that $\mathbb{V}_L(E)\backslash\mathbb{V}_L(N) = \bigcup_{i=1}^{s}\mathbb{V}_L(E_i)\backslash\mathbb{V}_L(N_i)$ and for each $i \in \{1, \ldots, s\}$ and for each $\bar{u} \in \mathbb{V}_L(E_i)\backslash\mathbb{V}_L(N_i)$,

$$\mathbb{V}_L(I(\bar{u})) = \left\{\left(\frac{g_{i1}(\bar{u}, \beta)}{g_i(\bar{u}, \beta)}, \ldots, \frac{g_{in}(\bar{u}, \beta)}{g_i(\bar{u}, T)}\right) \middle|\ \beta \in \mathbb{V}_L(\mathcal{X}_t(\bar{u}, T))\right\},$$

where $E_i, N_i \in k[U], \mathcal{X}_t, g_i, g_{i1}, \ldots, g_{in} \in k(U)[T]$.

Proof. Let $\mathcal{X}(U, T) \in k[U][T]$ be the product of $\mathcal{X}_t(U, T)$ and the least common multiple of all denominators of $\mathcal{X}_t(U, T)$. By the parametric GCD algorithm in [6], we can obtain the parametric GCDs of $\mathcal{X}(U, T)$ and $\mathcal{X}'(U, T)$ on $\mathbb{V}_L(E)\backslash\mathbb{V}_L(N)$ and assume that it is

$$\{(E_1, N_1, d_1), \ldots, (E_s, N_s, d_s)\},$$

where $\mathbb{V}_L(E)\backslash\mathbb{V}_L(N) = \cup_{i=1}^{r}\mathbb{V}_L(E_i)\backslash\mathbb{V}_L(N_i)$, $d_1, \ldots, d_r \in k[U][T]$ and for every $i = 1, \ldots, s$, $d_i(\bar{u}, T)$ is a greatest common divisor of $\mathcal{X}(\bar{u}, T)$ and $\mathcal{X}'(\bar{u}, T)$ for any $\bar{u} \in \mathbb{V}_L(E_i)\backslash\mathbb{V}_L(N_i)$. Moreover, the leading coefficient of d_i w.r.t. T is not zero under $\bar{u} \in \mathbb{V}_L(E_i)\backslash\mathbb{V}_L(N_i)$. Therefore, we can divide d_i by the leading coefficient of d_i and make $d_i \in k(U)[T]$ monic. For $\bar{u} \in \mathbb{V}_L(E_i)\backslash\mathbb{V}_L(N_i)$, we have

$$\gcd(\mathcal{X}_t(\bar{u}, T), \mathcal{X}'_t(\bar{u}, T)) = \gcd(\mathcal{X}(\bar{u}, T), \mathcal{X}'(\bar{u}, T)) = d_i(\bar{u}, T).$$

For each $i = 1, \ldots, s$, using divide algorithm in $k(U)[T]$, we get

$$\mathcal{X}_t(U, T) = q_i(U, T)d_i(U, T) + r_i(U, T),\ \deg_T(r_i) < \deg_T(d_i),$$

Since $d_i(\bar{u}, T)$ divides $\mathcal{X}_t(\bar{u}, T)$, for all $\bar{u} \in \mathbb{V}_L(E_i)\backslash\mathbb{V}_L(N_i)$, $r_i(U, T) = 0$. Therefore,

$$\frac{\mathcal{X}_t(\bar{u}, T)}{\gcd(\mathcal{X}'_t(\bar{u}, T), \mathcal{X}_t(\bar{u}, T))} = q_i(\bar{u}, T).$$

Let $\overline{\mathcal{X}_t}(U, T) = q_i(U, T) = \sum_{j=0}^{d} a_j T^{d-j} \in k(U)[T]$. Compute

$$g_i(U, T) = \sum_{i=0}^{d-1}\sum_{j=0}^{d-i-1} \mathrm{Tr}(M^I_{t^i})a_j T^{d-i-j-1}, \tag{3}$$

$$g_{ij}(U, T) = \sum_{i=0}^{d-1}\sum_{j=0}^{d-i-1} \mathrm{Tr}(M^I_{x_k t^i})a_j T^{d-i-j-1}, j = 1, \ldots, n. \tag{4}$$

Then

$$\{\mathcal{X}_t(\bar{u}, T), g_i(\bar{u}, T), g_{i1}(\bar{u}, T), \ldots, g_{in}(\bar{u}, T)\}$$

is an RUR of $I(\bar{u})$ for $\bar{u} \in \mathbb{V}_L(E_i)\backslash\mathbb{V}_L(N_i)$. □

4 ALGORITHMS AND EXAMPLE

We are now ready to give the algorithm for computing a rational representation with parameters of a ideal in $k[U,X]$, where we deliberately avoid tricks and optimizations, such as the selection of separating elements, reducing $\mathcal{X}$ or g_i by E_i.

Algorithm for computing RURs with parameters

Input: $I = \langle f_1, \ldots, f_l \rangle \subset k[U,X]$.

(1) Compute a comprehensive Gröbner system of I with $\prec_{X,U}$. Choose the zero-dimensional branches by Theorem 3.2 and denote them by $\mathcal{G} = \{(E_1, N_1, G_1), \ldots, (E_s, N_s, G_s)\}$.
(2) $B_2 := \emptyset$. For each branch (E_i, N_i, G_i) in (1) do:
  (a) Compute $Q_1^I = (p_{ij}/q_{ij}) \in k(U)^{r\times r}$ defined in Lemma 3.3. Let $Q = D \cdot Q_1^I$, where $D = \mathrm{lcm}(\{q_{ij} : i,j = 1,\ldots,r\})$.
  (b) Assume that $Q = (f_{ij})_{1\le i,j\le r}$. Construct polynomial $f_i = \sum_{j=1}^r f_{ij} z_j$. Compute the minimal Comprehensive Gröbner system $\mathcal{G} = \{(E_{i1}, N_{i1}, G_{i1}), \ldots, (E_{is_i}, N_{is_i}, G_{is_i})\}$ of $\{f_1, \ldots, f_r\}$. Set $A_i := \{(E_{i1}, N_{i1}, k_{i1}), \ldots, (E_{is_i}, N_{is_i}, k_{is_i})\}$, where k_{ij} is equal to number of element in $G_{ij}, j = 1, \ldots, s_i$.
  (c) $B_2 := B_2 \cup A_i$.
(3) $B_3 := \emptyset$. For each branch $(E_{ij}, N_{ij}, k_{ij}) \in B_2$ do:
  (a) If $k_{ij} = 1$ then $A_{ij} := \{(E_{ij}, N_{ij}, 1)\}$ and goto (3.d); else $A_{ij} := \emptyset, S := \{x_1 + ix_2 + \cdots + i^{n-1}x_n, i = 1, \ldots, nk_{ij}(k_{ij} - 1)/2\}$.
  (b) Randomly choose $t \in S$. Compute $M_t^I \in k(U)^{r\times r}$, $\mathcal{X}_t \in k(U)[T]$. Let $\mathcal{X} = D' \cdot \mathcal{X}_t$. Compute $\mathrm{PSC}_d(\mathcal{X}, \mathcal{X}')$, where D' is the least common multiple of all denominators of $\mathcal{X}_t$ and $d = \deg_T(\mathcal{X}) - k_{ij}$.
  (c) If $\mathbb{V}_L(E_{ij}) \backslash \mathbb{V}_L(N_{ij} \times \mathrm{PSC}_d(\mathcal{X}, \mathcal{X}')) = \emptyset$, then $S := S \backslash \{t\}$ and goto (3.b); else, $A_{ij} := A_{ij} \cup \{(E_{ij}, N_{ij} \times \mathrm{PSC}_d(\mathcal{X}, \mathcal{X}'), t)\}$. Update $E_{ij} := E_{ij} \cup \{\mathrm{PSC}_d(\mathcal{X}, \mathcal{X}')\}$ and $S := S \backslash \{t\}$. If $\mathbb{V}_L(E_{ij}) \backslash \mathbb{V}_L(N_{ij}) \neq \emptyset$, then goto (3.b).
  (d) $B_3 := B_3 \cup A_{ij}$.
(4) $B_4 := \emptyset$. For each branch $(E_{ijk}, N_{ijk}, t_{ijk})$ in (3) do:
  (a) Compute parametric GCDs of $\mathcal{X}$ and $\mathcal{X}'$, denoted by
  $$\{(E_{ijkl}, N_{ijkl}, d_{ijkl}) : l = 1, \ldots, v\},$$
  where $\mathcal{X}_t \in k(U)[T]$ and $\mathcal{X} \in k[U][T]$ are the polynomials computed in (3.b) corresponding to t_{ijk}.
  (b) For each $(E_{ijkl}, N_{ijkl}, d_{ijkl})$ do:
  $A_{ijkl} := \emptyset$. Compute $\overline{\mathcal{X}_t}$. By Formula (3), (4) compute $g_{ijkl}(U,T), g_{ijkl1}(U,T), \ldots, g_{ijkln}(U,T)$. $A_{ijkl} := A_{ijkl} \cup \{(E_{ijkl}, N_{ijkl}, \mathcal{X}_t, g_{ijkl}, g_{ijkl1}, \ldots, g_{ijkln})\}$
  (c) $B_4 := B_4 \cup A_{ijkl}$.

Output: a finite set B_4 of the rational univariate representations with parameters, renumbering it by

$$\{(E_1, N_1, \mathcal{X}_1, g_1, g_{11}, \ldots, g_{1n}), \ldots, (E_s, N_s, \mathcal{X}_s, g_s, g_{s1}, \ldots, g_{sn})\}.$$

For each $i \in \{1, \ldots, s\}$, it satisfies that : for all $\bar{u} \in \mathbb{V}_L(E_i) \backslash \mathbb{V}_L(N_i)$,

$$\mathbb{V}_L(I(\bar{u})) = \left\{ \left(\frac{g_{i1}(\bar{u},\beta)}{g_i(\bar{u},\beta)}, \ldots, \frac{g_{in}(\bar{u},\beta)}{g_i(\bar{u},\beta)} \right) \,\middle|\, \beta \in \mathbb{V}_L(\mathcal{X}_i(\bar{u},T)) \right\},$$

where $I(\bar{u}) = \langle f_1(\bar{u},X), \ldots, f_l(\bar{u},X) \rangle \subset k[X]$, $\mathcal{X}_i(\bar{u},T) \in k[T]$.

Theorem 4.1. *The above algorithm works correctly and terminates in a finite number of steps.*

Proof. The correctness and the termination of the algorithm directly follows from Theorems 3.2, 3.4, 3.6 and 3.7. □

We use the following simple example to illustrate the steps in the above proposed algorithm.

Example 4.2. Let $I = \langle u_1x_1^2 + u_2x_2 + u_2, u_2x_2^2 + u_1x_2 + u_1 \rangle \subset \mathbb{C}[u_1, u_2, x_1, x_2]$ with $\prec_U$ and $\prec_X$ being graded lexicographic order,

(1) Compute the minimal comprehensive Gröbner system for I:

$$\begin{aligned}\mathcal{G} =& \{(\{0\}, \{u_1u_2\}, \{u_2x_2^2 + u_1x_2 + u_1, u_1x_1^2 + u_2x_2 + u_2\}),\\ & (\{u_1\}, \{u_2, u_2u_1\}, \{1\}), (\{u_2\}, \{u_1\}, \{u_1x_1^2, u_1x_2 + u_1\}),\\ & (\{u_1, u_2\}, \{1\}, \{0\})\}.\end{aligned}$$

By Finiteness Theorem, $(\{0\}, \{u_1u_2\}, \{u_2x_2^2 + u_1x_2 + u_1, u_1x_1^2 + u_2x_2 + u_2\})$ and $(\{u_2\}, \{u_1\}, \{u_1x_1^2, u_1x_2 + u_1\})$ are two zero-dimensional branches. For briefness, we only consider the first branch.

(2) For $(\{0\}, \{u_1u_2\}, \{u_2x_2^2 + u_1x_2 + u_1, u_1x_1^2 + u_2x_2 + u_2\})$, we compute $Q_1^I(U)$ as defined in Theorem 3.4:

$$Q_1^I(U) = \begin{bmatrix} 4 & -\frac{2u_1}{u_2} & 0 & 0 \\ -\frac{2u_1}{u_2} & \frac{2u_1(u_1-2u_2)}{u_2^2} & 0 & 0 \\ 0 & 0 & \frac{2(u_1-2u_2)}{u_1} & -\frac{2(-3u_2+u_1)}{u_2} \\ 0 & 0 & \frac{2(3u_2-u_1)}{u_2} & \frac{2\left(u_1^2-4u_1u_2+2u_2^2\right)}{u_2^2} \end{bmatrix}.$$

Then $D = u_1u_2^2$ be the least common multiple of all denominators of Q_1^I. Let $Q = D \cdot Q_1^I$. Denote the entries of Q by f_{ij} and set $f_i = \sum_{j=1}^4 f_{ij}z_j$, $i = 1, \ldots, 4$. We compute the minimal comprehensive Gröbner system of $\{f_1, f_2, f_3, f_4\}$ on $\mathbb{C}^2 \setminus \mathbb{V}_{\mathbb{C}}(u_1u_2)$: $\{(\{0\}, \{(u_1 - 4u_2)u_2u_1\}, \{(u_1^3u_2 - 4u_1^2u_2^2)z_2, (u_1^2u_2^3 - 4u_1u_2^4)z_4, 2u_1u_2^2z_1 - u_1^2u_2z_2, 2u_2^4z_3 - u_1u_2^3z_4\}), (\{u_1 - 4u_2\}, \{u_1u_2\}, \{u_2^3z_1 - 2u_2^3z_2, u_2^3z_3 - 2u_2^3z_4\})\}$. Therefore,

$$\begin{aligned}B_2 =& \{(E_{11}, N_{11}, k_{11}), (E_{12}, N_{12}, k_{12})\}\\ =& \{(\{0\}t, \{u_1u_2(u_1 - 4u_2)\}, 4), (\{u_1 - 4u_2\}, \{u_1u_2\}, 2)\}.\end{aligned}$$

(3) Let $B_3 = \emptyset$. For the branch $(E_{11}, N_{11}, k_{11}) = (\{0\}, \{u_1u_2(u_1 - 4u_2)\}, 4)$, let $A_{11} = \emptyset$. Randomly choose $t = x_1 \in S$. By computation,

$$M_t^I = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -\frac{u_2}{u_1} & -\frac{u_2}{u_1} & 0 & 0 \\ 1 & \frac{u_1-u_2}{u_1} & 0 & 0 \end{bmatrix}, \quad \mathcal{X}_t = T^4 - \frac{(u_1 - 2u_2)T^2}{u_1} + \frac{u_2^2}{u_1^2}. \quad .$$

Then $\mathcal{X} = u_1^2T^4 - u_1(u_1 - 2u_2)T^2 + u_2^2$, $\mathcal{X}' = 4u_1^2T^3 - 2u_1(u_1 - 2u_2)T$, $\mathrm{PSC}_0(\mathcal{X}, \mathcal{X}') = 16u_1^6u_2^2(u_1 - 4u_2)^2$. By check, $\mathbb{C}^2 \backslash \mathbb{V}_{\mathbb{C}}(u_1u_2(u_1 - 4u_2) \cdot \mathrm{PSC}_0(\mathcal{X}, \mathcal{X}')) \neq \emptyset$, x_1 is a separating element of $I(\bar{u})$ under $\bar{u} \in \mathbb{C}^2 \backslash \mathbb{V}_{\mathbb{C}}(16u_1^7u_2^3(u_1 - 4u_2)^3)$. Now

$$A_{11} := A_{11} \cup \{(\{0\}, \{16u_1^7u_2^3(u_1 - 4u_2)^3\}, x_1)\}.$$

Update $E_{11} = E_{11} \cup \{\mathrm{PSC}_0(\mathcal{X}, \mathcal{X}')\}$. We can check $\mathbb{V}_{\mathbb{C}}(E_{11}) \backslash \mathbb{V}_{\mathbb{C}}(N_{11}) = \emptyset$. Then this branch has been done and

$$B_3 := B_3 \cup A_{11} = \{(\{0\}, \{16u_1^7u_2^3(u_1 - 4u_2)^3\}, x_1)\}.$$

For the branch $(E_{12}, N_{12}, k_{12}) = (\{u_1 - 4u_2\}, \{u_1u_2\}, 2)$, let $A_{12} = \emptyset$. We also choose $t = x_1$. Then $M_t^I, \mathcal{X}_t, \mathcal{X}, \mathcal{X}'$ are the same as above. By computation,

$$\mathrm{PSC}_2(\mathcal{X}, \mathcal{X}') = -8u_1^3(u_1 - 2u_2).$$

We can check that $\mathbb{V}_{\mathbb{C}}(u_1 - 4u_2) \backslash \mathbb{V}_{\mathbb{C}}(u_1u_2 \cdot \mathrm{PSC}_2(\mathcal{X}, \mathcal{X}')) \neq \emptyset$, then

$$A_{12} := A_{12} \cup \{(\{u_1 - 4u_2\}, \{-8u_1^4u_2(u_1 - 2u_2)\}, x_1)\}.$$

Update $E_{12} = E_{12} \cup \{\mathrm{PSC}_2(\mathcal{X}, \mathcal{X}')\} = \{u_1 - 4u_2, -8u_1^3(u_1 - 2u_2)\}$. By check, $\mathbb{V}_{\mathbb{C}}(E_{12}) \backslash \mathbb{V}_{\mathbb{C}}(N_{12}) = \emptyset$. This branch has been done and

$$B_3 := B_3 \cup A_{12}$$
$$= \{(\{0\}, \{u_1^7 u_2^3 (u_1 - 4u_2)^3\}, x_1), (\{u_1 - 4u_2\}, \{-8u_1^4 u_2 (u_1 - 2u_2)\}, x_1)\}.$$

(4) For the branch $(\{0\}, \{u_1^7 u_2^3 (u_1 - 4u_2)^3\}, x_1)$, we compute the parametric GCDs of $\mathcal{X}$ and $\mathcal{X}'$ corresponding to $t = x_1$. That is $\{(\{0\}, \{u_2 u_1 (u_1 - 4u_2)\}, 1)\}$. Then $\overline{\mathcal{X}_t} = \mathcal{X}_t$. By Formula (3),(4), $g_1 = 4T^3 - \frac{2(u_1 - 2u_2)T}{u_1}$, $g_{11} = \frac{2(u_1 - 2u_2)}{u_1} T^2 - \frac{4u_2^2}{u_1^2}$, $g_{12} = -\frac{2u_1}{u_2} T^3 + 2T$. Let $\mathcal{X}_1 = \mathcal{X}_t = T^4 - \frac{u_1 - 2u_2}{u_1} T^2 + \frac{u_2^2}{u_1^2}$, we obtain the RUR with parameters of this branch is $(\{0\}, \{u_1 u_2 (u_1 - 4u_2)\}, \mathcal{X}_1, g_1, g_{11}, g_{12})$.

For the branch $(\{u_1 - 4u_2\}, \{-8u_1^4 u_2 (u_1 - 2u_2)\}, x_1)$, we compute the parametric GCDs of $\mathcal{X}, \mathcal{X}'$ corresponding to $t = x_1$. That is

$$(\{u_1 - 4u_2\}, \{(u_1 - 2u_2) u_1 u_2\}, 4T^2 u_2^2 - u_2^2)$$

By computation, $\overline{\mathcal{X}_t} = T^2 - \frac{3u_1 - 8u_2}{4u_1}$, $g_2 = 4T$, $g_{21} = \frac{2(u_1 - 2u_2)}{u_1}$, $g_{22} = -\frac{2u_1 T}{u_2}$. Let $\mathcal{X}_2 = \mathcal{X}_t$. In this case, we can reduce $\mathcal{X}_2, g_2, g_{21}, g_{22}$ by the relation $u_1 - 4u_2 = 0$. Then we have $\mathcal{X}_2 = T^4 - \frac{1}{2} T^2 + \frac{1}{16}$, $g_2 = 4T, g_{21} = 1, g_{22} = -8T$. Thus, the RUR with parameters of this branch is $(\{u_1 - 4u_2\}, \{(u_1 - 2u_2) u_1 u_2\}, \mathcal{X}_2, g_2, g_{21}, g_{22})$.

In conclusion, we obtain two RURs of I under the parameter branch $(\{0\}, \{u_1 u_2\})$. That is $(\{0\}, \{u_1 u_2 (u_1 - 4u_2)\}, \mathcal{X}_1, g_1, g_{11}, g_{12})$ and $(\{u_1 - 4u_2\}, \{(u_1 - 2u_2) u_1 u_2\}, \mathcal{X}_2, g_2, g_{21}, g_{22})$. Therefore,

(i) For all $\bar{u} = (\bar{u}_1, \bar{u}_2) \in \mathbb{C}^2 \backslash \mathbb{V}_{\mathbb{C}}(u_1 u_2 (u_1 - 4u_2))$,

$$\mathbb{V}_{\mathbb{C}}(I(\bar{u})) = \left\{ \left(\frac{g_{11}(\bar{u}, \beta)}{g_1(\bar{u}, \beta)}, \frac{g_{12}(\bar{u}, \beta)}{g_1(\bar{u}, \beta)} \right) \Big| \, \beta \in \mathbb{V}_{\mathbb{C}} \left(T^4 - \frac{\bar{u}_1 - 2\bar{u}_2}{\bar{u}_1} T^2 + \frac{\bar{u}_2^2}{\bar{u}_1^2} \right) \right\}$$
$$= \left\{ \left(\frac{(\bar{u}_1^2 - 2\bar{u}_1 \bar{u}_2)\beta^2 - 2\bar{u}_2^2}{2\beta^3 \bar{u}_1^2 - (\bar{u}_1 - 2\bar{u}_2)\bar{u}_1 \beta}, \frac{-\bar{u}_1^2 \beta^2 + \bar{u}_1 \bar{u}_2}{2\beta^2 \bar{u}_1 \bar{u}_2 - \bar{u}_2 (\bar{u}_1 - 2\bar{u}_2)} \right) \Big| \right.$$
$$\left. \beta \in \mathbb{V}_{\mathbb{C}} \left(T^4 - \frac{\bar{u}_1 - 2\bar{u}_2}{\bar{u}_1} T^2 + \frac{\bar{u}_2^2}{\bar{u}_1^2} \right) \right\}.$$

(ii) For all $\bar{u} = (\bar{u}_1, \bar{u}_2) \in \mathbb{V}_{\mathbb{C}}(u_1 - 4u_2) \backslash \mathbb{V}_{\mathbb{C}}(u_1 u_2)$,

$$\mathbb{V}_{\mathbb{C}}(I(\bar{u})) = \left\{ \left(\frac{1}{4\beta}, -2 \right) \Big| \, \beta \in \mathbb{V}_{\mathbb{C}} \left(T^4 - \frac{1}{2} T^2 + \frac{1}{16} \right) \right\},$$

5 CONCLUDING REMARKS

The rational univariate representation of zero-dimensional ideals with parameters has been considered in the paper. Because the number of zeros for zero-dimensional ideals with parameters under parametric specializations is different, the choosing of separating elements which is the premise and the key to computing the rational univariate representation is quite difficult. By means of comprehensive Gröbner systems to divide the parameter space, we make the ideal under each branch have the same number of zeros. Moreover, we extended the subresultant theorem to parametric cases, and based on it we choose the separating element corresponding to each branch, which further divides the parameter space. As a result, making use of rational univariate representation and parametric greatest common divisors we obtained a finite set of which each branch shares the same expression of rational univariate representation and proposed the algorithm for computing rational univariate representations of parametric zero-dimensional ideals.

ACKNOWLEDGMENTS

This research was supported by the National Natural Science Foundation of China under Grant No. 12171469, and the National Key Research and Development Project 2020YFA0712300.

REFERENCES

[1] W. Auzinger and H.J. Stetter. 1988. An elimination algorithm for the computation of all zeros of a system of multivariate polynomial equations. *International Series of Numerical Mathematics* 86 (1988), 11–30.
[2] T. Becker and V. Weispfenning. 1993. *Gröbner Bases.* Springer-Verlag.
[3] D. Cox, J. Little, and D. O'shea. 2005. *Using Algebraic Geometry.* Springer.
[4] David A Cox, John Little, and Donal O'shea. 2006. *Using algebraic geometry.* Vol. 185. Springer Science & Business Media.
[5] M. Kalkbrener. 1997. On the Stability of Gröbner Bases Under Specializations. *Journal of Symbolic Computation* 24, 1 (1997), 51–58.
[6] D. Kapur, D. Lu, M. Monagan, Y. Sun, and D.K. Wang. 2018. An Efficient Algorithm for Computing Parametric Multivariate Polynomial GCD. In *Proceedings of the 2018 International Symposium on Symbolic and Algebraic Computation.* 239–246.
[7] D. Kapur, Y. Sun, and D.K. Wang. 2013. An efficient algorithm for computing a comprehensive Gröbner system of a parametric polynomial systems. *Journal of Symbolic Computation* 49 (2013), 27–44.
[8] X.D. Ma, Y. Sun, and D.K. Wang. 2012. Computing polynomial univariate representations of zero-dimensional ideals by Gröbner basis. *Science China Mathematics* 55, 6 (2012), 1293–1302.
[9] X.D. Ma, Y. Sun, D.K. Wang, and Y.S. Xue. 2017. On Checking Linear Dependence of Parametric Vectors. In *Intelligent Computing Theories and Application.* 188–196.
[10] Bhubaneswar Mishra. 1993. *Algorithmic algebra.* Springer-Verlag, New York.
[11] A. Montes. 2002. A new algorithm for discussing Gröbner basis with parameters. *Journal of Symbolic Computation* 33 (2002), 183–208.
[12] K. Nabeshima. 2007. A speed-up of the algorithm for computing comprehensive Gröbner systems. In *Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation.* 299–306.
[13] K. Nagasaka. 2017. Parametric Greatest Common Divisors using Comprehensive Gröbner Systems. In *Proceedings of the 2017 International Symposium on Symbolic and Algebraic Computation.* 341–348.
[14] M. Noro and K. Yokoyama. 1999. A modular method to compute the rational univariate representation of zero-dimensional ideals. *Journal of Symbolic Computation* 28, 1-2 (1999), 243–263.
[15] K. Ouchi and J. Keyser. 2008. Rational univariate reduction via toric resultants. *Journal of Symbolic Computation* 43, 11 (2008), 811–844.
[16] F. Rouillier. 1999. Solving zero-dimensional systems through the rational univariate representation. *Applicable Algebra in Engineering Communication and Computing* 9, 5 (1999), 433–461.
[17] M. Safey El Din, Z.H. Yang, and L.H. Zhi. 2018. On the complexity of computing real radicals of polynomial systems. In *Proceedings of the 2018 International Symposium on Symbolic and Algebraic Computation.* 351–358.
[18] É. Schost. 2003. Computing parametric geometric resolutions. *Applicable Algebra in Engineering Communication and Computing* 13, 5 (2003), 349–393.
[19] B.X. Shang, S.G. Zhang, C. Tan, and P. Xia. 2017. A simplified rational representation for positive-dimensional polynomial systems and SHEPWM equation solving. *Journal of Systems Science and Complexity* 30 (2017), 1470–1482.
[20] H.J. Stetter. 1996. Matrix eigenproblem are at the heart of polynomial system solving. *ACM SIGSAM Bull.* 30 (1996), 27–36.
[21] A. Suzuki and Y. Sato. 2006. A simple algorithm to compute comprehensive Gröbner bases using Gröbner bases. In *Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computation.* 326–331.
[22] C. Tan. 2009. *The rational representation for solving polynomial systems (in Chinese).* Ph.D. Dissertation.
[23] C. Tan and S.C. Zhang. 2009. Separating element computation for the rational univariate representation with short coefficients in zero-dimensional algebraic varieties. *Journal of Jilin University (Science Edition)* 47 (2009), 174–178.
[24] C. Tan and S.G. Zhang. 2010. Computation of the rational representation for solutions of high-dimensional systems. *Communications in Mathematical Research* 26, 2 (2010), 119–130.
[25] V. Weispfenning. 1992. Comprehensive Gröbner bases. *Journal of Symbolic Computation* 14, 1 (1992), 1–29.
[26] W.T. Wu. 1984. *Basic Principles of Mechanical Theorem Proving in Geometries (in Chinese), Vol. I:Part of Elementary Geometries.* Science Press.
[27] F.H. Xiao, D. Lu, X.D. Ma, and D.K. Wang. 2021. An Improvement of the Rational Representation for High-Dimensional Systems. *Journal of Systems Science and Complexity* 34, 6 (2021), 2410–2427.
[28] G.X. Zeng and S.J. Xiao. 2010. Computing the rational univariate representations for zero-dimensional systems by Wu's method. *Science China Mathematics(Chinese)* 40, 10 (2010), 999–1016.