An Improvement of the Rational Representation for High-Dimensional Systems*

XIAO Fanghui · LU Dong · MA Xiaodong · WANG Dingkang

DOI: 10.1007/s11424-020-9316-4
Received: 20 November 2019 / Revised: 10 March 2020

Abstract Based on the rational univariate representation of zero-dimensional polynomial systems, Tan and Zhang proposed the rational representation theory for solving a high-dimensional polynomial system, which uses so-called rational representation sets to describe all the zeros of a high-dimensional polynomial system. This paper is devoted to giving an improvement for the rational representation. The idea of this improvement comes from a minimal Dickson basis used for computing a comprehensive Gröbner system of a parametric polynomial system to reduce the number of branches. The authors replace the normal Gröbner basis G satisfying certain conditions in the original algorithm (Tan-Zhang's algorithm) with a minimal Dickson basis G_m of a Gröbner basis for the ideal, where G_m is smaller in size than G. Based on this, the authors give an improved algorithm. Moreover, the proposed algorithm has been implemented on the computer algebra system Maple. Experimental data and its performance comparison with the original algorithm show that it generates fewer branches and the improvement is rewarding.

Keywords Comprehensive Gröbner systems, high-dimensional polynomial system, rational representation, rational univariate representation.

XIAO Fanghui
KLMM, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190*, China; School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing* 100049*, China.*
Email: xiaofanghui@amss.ac.cn.
LU Dong (Corresponding author)
Beijing Advanced Innovation Center for Big Data and Brain Computing, Beihang University, Beijing 100191*, China; School of Mathematical Sciences, Beihang University, Beijing* 100191*, China.*
Email: donglu@amss.ac.cn.
MA Xiaodong
College of Science, China Agricultural University, Beijing 100083*, China.* Email: maxiaodong@cau.edu.cn.
WANG Dingkang
KLMM, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190*, China; School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing* 100049*, China.*
Email: dwang@mmrc.iss.ac.cn.

*This research was supported by the National Natural Science Foundation of China under Grant No. 11801558, the Chinese Universities Scientific Funds under Grant No. 15059002 and the CAS Key Project QYZDJ-SSW-SYS022.

◇*This paper was recommended for publication by Editor FENG Ruyong.*

1 Introduction

Polynomial system solving is a very classic problem in mathematics, which plays an extremely important role in scientific research and engineering applications, such as robot design, geometric modelling, game theory and computational economics. For nonlinear polynomial systems, there are three main symbolic computation methods, that is, Wu's method[1], Gröbner basis method[2] and resultant-based method[3]. With further research, the eigenvalue methods[4, 5] based on resultant or Gröbner basis have been developed to solve polynomial equation systems. For more work on the problem of solving polynomial systems, please refer to [6–10].

In order to better describe the solution of the equations, in 1999, Rouillier[11] proposed the rational univariate representation (RUR) to solve zero-dimensional polynomial systems, which can represent the solutions as rational functions at the zeros of an univariate polynomial. Since then, it has been extensively studied. Noro and Yokoyama[12] used modular method to compute the rational univariate representation of zero-dimensional ideal. Ouchi and Keyser[13] proposed an approach for computing the rational univariate representation via toric resultants. Zeng and Xiao[14] used Wu's method to compute the rational univariate representation. Ma, et al.[15] presented a method based on properties of Gröbner basis to compute the rational univariate representation.

In 2009, Tan and Zhang[16, 17] generalized the rational univariate representation theory of zero-dimensional polynomial systems to high dimensionality and proposed the rational representation theory for solving a high-dimensional polynomial system. The rational representation theory uses a finite number of rational representation sets to describe all the solutions of a high-dimensional polynomial system. The idea is reducing the ideal to zero dimension by placing the independent variables in the base field, then by means of the rational univariate representation of zero-dimensional ideal and Wu's method all the solutions can be expressed. Along this, Shang, et al.[18] proposed a simplified rational representation for solving positive-dimensional ideals, which uses less rational representation sets to represent the variety. They found zeros represented by some rational representation sets can get from the others by taking limit, then it avoids the generation of some rational representation sets. Also worth mentioning is that there is a concept similar to rational representation, namely rational parametrization (also known as geometric resolution). In 2003, Schost[19] proposed parametric geometric resolution which gives a description of the generic solutions for parametric polynomial systems. From the point of view of an end-user, a rational parametrization is certainly the most friendly simplification for a parametric system. The rational parametrization or geometric resolution can be applied to real algebraic geometry. Safey El Din, et al.[20] used rational parametrizations to represent all irreducible components of the real algebraic set.

Inspired by the idea of reducing the number of branches for computing the comprehensive Gröbner system of a parametric polynomial system in [21] which is based on the research of Kalkbrener[22], Montes[23], Suzuki and Sato[24], Nabeshima[25] on comprehensive Gröbner systems, we apply a minimal Dickson basis to the rational representation and make an improvement of the rational representation. In Tan-Zhang's algorithm, computing the rational representation set of a high-dimensional ideal I needs to compute a Gröbner basis G for ideal I^e which is a zero-dimensional ideal obtained by placing the independent variables of ideal I in the base field, and G is required to be a basis of I. The improvement we make is to replace the basis G with a minimal Dickson basis G_m of a Gröbner basis for the ideal I. Precisely, G_m is a minimal Gröbner basis of ideal I^e, but not a basis of I. We prove the improvement is correct and give the improved algorithm for computing the rational representation. What's more, we have implemented the improved algorithm on Maple.

This paper is organized as follows. In Section 2, some notations and concepts for polynomial systems are introduced, and the related knowledge of the rational univariate representation is reviewed. In Section 3, we introduce the rational representation theory for high-dimensional ideals proposed by Tan and Zhang, and give an improvement for the rational representation to reduce the number of rational representation sets. The improved algorithm is described in Section 4, and we give an example to illustrate this algorithm in Section 5. The implementation of the algorithm and the performance comparison with the original algorithm in [17] are presented in Section 6. Finally, we conclude this paper.

2 Preliminaries

In this section, we will introduce some notations and concepts for polynomial systems, and also briefly review main contents of the rational univariate representation theory for zero-dimensional ideals.

Let k be a field of characteristic 0, and L its algebraic closure. $k[X]$ is the polynomial ring over k in the variables $X = \{x_1, x_2, \cdots, x_n\}$, I is an ideal of $k[X]$ and $\mathbb{V}_L(I)$ is the variety of I in L^n. We denote by $A_k(I) = k[X]/I$ the k-algebra.

2.1 Basis Knowledge

Now we introduce the multiplication map of quotient rings $A_k(I)$, the characteristic polynomial and the Hermite's quadratic form which are related to computing the rational univariate representation of a zero-dimensional ideal I. The details can refer to [3] and [11].

Definition 2.1 Let $I \subset k[X]$ be a zero-dimensional ideal. For all $h \in k[X]$, we denote by $m_h^{A_k(I)}$ the k-linear map:

$$\begin{aligned} m_h^{A_k(I)}:\ A_k(I) &\longrightarrow A_k(I) \\ \overline{f} &\longmapsto \overline{hf}, \end{aligned}$$

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

We denote by M_h the matrix representation of $m_h^{A_k(I)}$ w.r.t. a basis in quotient rings $A_k(I)$. And we call $m_h^{A_k(I)}$ the multiplication map and M_h the multiplication matrix w.r.t. h.

Theorem 2.2 (see [3]) *Let $I \subset k[X]$ be a zero-dimensional ideal, $m_h^{A_k(I)}$ be the multiplication map. Then the eigenvalues of $m_h^{A_k(I)}$ are exactly the scalars $h(\alpha)$ with respective multiplicities $\sum_{\beta\in\mathbb{V}_L(I),h(\beta)=h(\alpha)} \mu(\beta)$, where $\alpha \in \mathbb{V}_L(I)$, $\mu(\beta)$ denotes the multiplicity of β.*

This theorem shows that for any $h \in k[X]$, the set of eigenvalues of $m_h^{A_k(I)}$ coincides with the set of values of the h at the points in $\mathbb{V}_L(I)$.

The main consequences following from above theorem are as follows.

Proposition 2.3 (see [11]) *Let $I \subset k[X]$ be a zero-dimensional ideal, $m_h^{A_k(I)}$ be the multiplication map. Then*

- *$Det(m_h^{A_k(I)}) = \prod_{\alpha \in \mathbb{V}_L(I)} h(\alpha)^{\mu(\alpha)}$, where $\mu(\alpha)$ is the multiplicity of α.*
- *$Trace(m_h^{A_k(I)}) = \sum_{\alpha \in \mathbb{V}_L(I)} \mu(\alpha) h(\alpha)$.*
- *The characteristic polynomial of $m_h^{A_k(I)}$ is (if it is supposed to be monic):*

$$\mathcal{X}_h = \prod_{\alpha \in \mathbb{V}_L(I)} (T - h(\alpha))^{\mu(\alpha)}.$$

- *For any $h \in k[X]$, $\mathcal{X}_h(h) \in I$.*

We below introduce a method to compute the number of distinct complex roots of a polynomial system.

Definition 2.4 Let $I \subset k[X]$ be a zero-dimensional ideal and $h \in k[X]$. The Hermite's quadratic form associated to h is defined by

$$\begin{aligned} q_h^{A_k(I)}:\ A_k(I) &\longrightarrow \quad k \\ f \quad &\longmapsto \mathrm{Trace}(m_{\overline{hf^2}}^{A_k(I)}). \end{aligned}$$

Theorem 2.5 (see [11]) *For any $h \in k[X]$, the Hermite's quadratic form $q_h^{A_k(I)}$ associated to h satisfies:*

$$\rho(q_h^{A_k(I)}) = \sharp\{\alpha \in \mathbb{V}_L(I) :\ h(\alpha) \neq 0\},$$

where $\rho(q_h^{A_k(I)})$ denotes the rank of $q_h^{A_k(I)}$.

2.2 RUR for Zero-Dimensional Ideals

First, we review the definition of separating elements which plays an important role in rational univariate representation theory, the study of the roots of polynomial systems and the study of the k-algebra $A_k(I)$.

Definition 2.6 Let $I \subset k[X]$ be a zero-dimensional ideal. A polynomial $t \in k[X]$ separates $\mathbb{V}_L(I)$, if

$$\alpha, \beta \in \mathbb{V}_L(I), \quad \alpha \neq \beta \Rightarrow t(\alpha) \neq t(\beta).$$

We also call t a separating element of I.

Obviously, such polynomials exist. The following lemma was proved in [11].

Lemma 2.7 *Let $V \subset L^n$ be a finite set, $\sharp V = D$, where D is a non-negative integer. Then the finite set of linear form $L = \{x_1 + cx_2 + \cdots + c^{n-1}x_n \mid 0 \le c \le (n-1)D(D-1)/2\}$ contains at least one separating element.*

By Theorem 2.2 and the definition of separating elements, we get the following corollary used for the determination of separating elements.

Corollary 2.8 *An element t in $k[X]$ is a separating element of zero-dimensional ideal $I \subset k[X]$ if and only if degree($\overline{\mathcal{X}_t}$)=$\sharp\mathbb{V}_L(I)$, where $\overline{\mathcal{X}_t}$ is the squarefree part of the characteristic polynomial $\mathcal{X}_t$ of $m_t^{A_k(I)}$.*

According to Theorem 2.5, $\sharp\mathbb{V}_L(I) = \rho(q_1^{A_k(I)})$. In practice, we express $q_1^{A_k(I)}$ with its matrix Q_1 w.r.t the standard basis $\mathcal{B} = \{X^{\alpha(1)}, X^{\alpha(2)}, \cdots, X^{\alpha(D)}\}$ of $A_k(I)$: $Q_1[i,j] = \text{Trace}(m^{A_k(I)}_{X^{\alpha(i)}X^{\alpha(j)}})$, $i,\ j = 1, 2, \cdots, D$. We can compute the rank of matrix Q_1, and choose a polynomial t from the set $L = \{x_1 + cx_2 + \cdots + c^{n-1}x_n \mid 0 \le c \le (n-1)D(D-1)/2\}$. If the degree of $\overline{\mathcal{X}_t}$ is equal to the rank of matrix Q_1, then t is a separating element. Otherwise, re-select one from L. So that we can pick out a separating element.

Next, let's look at the rational univariate representation theory for zero-dimensional ideals proposed by Rouillier[11].

Definition 2.9 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 $m_t^{A_k(I)}$. For any $v \in k[X]$, we define:

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

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

$$\{\mathcal{X}_t(T), g_t(1,T), g_t(x_1,T), \cdots, g_t(x_n,T)\}.$$

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

Theorem 2.10 (see [11]) *Let $I \subset k[X]$ be a zero-dimensional ideal, an RUR of I associated to a separating element t has the following properties:*

- *$\mathcal{X}_t(T), g_t(1,T), g_t(x_1,T), \cdots, g_t(x_n,T)$ are polynomials in $k[T]$.*
- *The variety of I can be represented as*

$$\mathbb{V}_L(I) = \left\{\left(\frac{g_t(x_1,t(\alpha))}{g_t(1,t(\alpha))}, \frac{g_t(x_2,t(\alpha))}{g_t(1,t(\alpha))}, \cdots, \frac{g_t(x_n,t(\alpha))}{g_t(1,t(\alpha))}\right) \;\middle|\; t(\alpha) \in \mathbb{V}_L(\mathcal{X}_t(T))\right\},\ \alpha \in \mathbb{V}_L(I).$$

Since the elements in the representation matrix M_t of $m_t^{A_k(I)}$ are in k, $\mathcal{X}_t(T) \in k[T]$. Suppose $\overline{\mathcal{X}_t} = \prod_{y\in\mathbb{V}_L(\mathcal{X}_t)}(T-y)$, then

$$\frac{g_t(v,T)}{\overline{\mathcal{X}_t}} = \sum_{\alpha\in\mathbb{V}_L(I)} \frac{\mu(\alpha)v(\alpha)}{T-t(\alpha)} = \sum_{i\ge0} \frac{\sum_{\alpha\in\mathbb{V}_L(I)} \mu(\alpha)v(\alpha)t(\alpha)^i}{T^{i+1}}$$
$$= \sum_{i\ge0} \frac{Trace(m^{A_k(I)}_{vt^i})}{T^{i+1}}.$$

Let $\overline{\mathcal{X}_t} = \sum_{j=0}^{d} a_j T^{d-j}$. Multiplying both sides of the above formula by $\overline{\mathcal{X}_t}$, according to $g_t(v,T) \in L[T]$ we have: $g_t(v,T) = \sum_{i=0}^{d-1}\sum_{j=0}^{d-i-1} Trace(m_{vt^i}^{A_k(I)}) a_j T^{d-i-j-1}$. We denote by $H_j(T) = \sum_{i=0}^{j} a_i T^{j-i}$ the j-th Horner's polynomial associated to $\overline{\mathcal{X}_t}$, then

$$g_t(v,T) = \sum_{i=0}^{d-1} Trace(m_{vt^i}^{A_k(I)}) H_{d-i-1}(T) \in k[T].$$

In addition,

$$g_t(v,t(\alpha)) = \sum_{\beta\in\mathbb{V}_L(I), t(\beta)=t(\alpha)} \mu(\beta)v(\beta) \prod_{y\in t(\mathbb{V}_L(I))\setminus\{t(\alpha)\}} (t(\alpha)-y).$$

If t separates $\mathbb{V}_L(I)$, then $v(\alpha) = \frac{g_t(v,t(\alpha))}{g_t(1,t(\alpha))}$.

Remark 2.11 From Corollary 2.8 and Theorem 2.10, we know only when t is a separating element can a bijection between the roots of a univariate polynomial (the characteristic polynomial $\mathcal{X}_t(T)$) and those of the considered ideal be constructed. In the RUR of I, $g_t(1,T)$ is the denominator of each coordinate expression, so it must not be zero (for zero-dimensional situation, $g_t(1,T)$ and $\mathcal{X}_t(T)$ are coprime according to the definition of $g_t(1,T)$). In other words, there are two key points to note: The choice of a separating element and the denominator $g_t(1,T)$ cannot be zero.

3 RR for High-Dimensional Ideals and Improvement

In this section, we first review the rational representation theory for solving high-dimensional ideals proposed by Tan and Zhang in [17]. And then we will give an improvement for the rational representation by applying the idea of reducing the number of branches for computing a comprehensive Gröbner system (CGS) of a parametric polynomial system in [21].

All notations are as before, we will introduce some related new notations below.

Now let $U = \{x_{i_1}, x_{i_2}, \cdots, x_{i_d}\} \subset X$ be a maximally independent set modulo I, $V = X\setminus U = \{x_{i_{d+1}}, x_{i_{d+2}}, \cdots, x_{i_n}\}$. $T(V)$ and $T(X)$ denote the sets of all monomials in V and X. Let $\prec_{U,V}$ be an admissible block monomial order on $T(X)$ such that $U \ll V$, and $\prec_V$ be the restriction of $\prec_{U,V}$ to $T(V)$. For $f \in k[X]$, we denote by $\mathrm{LC}_{\prec_V}(f)$, $\mathrm{LM}_{\prec_V}(f)$ the leading coefficient and the leading monomial of f w.r.t. $\prec_V$.

3.1 Rational Representation Theory

Let I^e be the extension of I to $k(U)[V]$, and for point $p \in L^d$, I_p be the ideal generated by $\{f|_{U=p} \in L[V] \mid f \in I\}$ in $L[V]$. Suppose the finite polynomial set $G = \{g_1, g_2, \cdots, g_m\} \subset I$ such that G is a Gröbner basis of I^e w.r.t. $\prec_V$ and a basis of ideal I, then G_p is a generator set of ideal I_p. Set $\mathcal{F} = \mathrm{LCM}\{\mathrm{LC}_{\prec_V}(g_i) | 1 \le i \le m\} \in k[U]$, where $\mathrm{LC}_{\prec_V}(g_i) \in k[U]$ and LCM denotes the least common multiple.

Since U is a maximally independent set modulo I, I^e is a zero-dimensional ideal. According to the RUR of zero-dimensional ideals, we choose a separating element $t \in k[V]$ of I^e and obtain the RUR of I^e.

Definition 3.1 Let $I \subset k[X]$ be an ideal, $U = \{x_{i_1}, x_{i_2}, \cdots, x_{i_d}\} \subset X$ be a maximally independent set modulo I, $V = X \setminus U = \{x_{i_{d+1}}, x_{i_{d+2}}, \cdots, x_{i_n}\}$ and I^e be the extension of I to $k(U)[V]$. Suppose that $t \in k[V]$ and $\{\mathcal{X}_{U,t}(T), \mathcal{G}_{U,t}(1,T), \mathcal{G}_{U,t}(x_{i_{d+1}}, T), \cdots, \mathcal{G}_{U,t}(x_{i_n}, T)\}$ are a separating element of I^e and the RUR of I^e associated to t, respectively. Then the set

$$\mathcal{R}_t^U \;=\; \{\mathcal{F}(U)\triangle_t(U), \mathcal{X}_{U,t}(T), \mathcal{G}_{U,t}(1,T), \mathcal{G}_{U,t}(x_{i_{d+1}}, T), \cdots, \mathcal{G}_{U,t}(x_{i_n}, T)\}$$

is called a rational representation set (RRS) of I associated to U and t, where $\triangle_t(U) \in k[U]$ is the numerator of the resultant of $\overline{\mathcal{X}_{U,t}(T)}$ and its derivative $\overline{\mathcal{X}_{U,t}(T)}'$ w.r.t. the variable T.

Particularly, if dim$I$=0, then the RUR of zero-dimensional ideal I associated to separating element t is called a rational representation set.

Theorem 3.2 (see [17]) *Let $I \subset k[X]$ be an ideal, $\mathbb{V}_L(I)$ is the variety of I in L^n. Then there is*

$$\mathbb{V}_L(I) = \bigcup_{j=1}^{s} \mathcal{W}_j$$

such that $\mathcal{W}_j$ can be represented by a rational representation set $\mathcal{R}_j$. Moreover, $\cup_{j=1}^{s}\mathcal{R}_j$ is called a rational representation (RR) of $\mathbb{V}_L(I)$. For convenience, we also call $\cup_{j=1}^{s}\mathcal{R}_j$ an RR of I. A rational representation set $\mathcal{R}_j$ is seen as a branch.

The main idea of the rational representation theory proposed by Tan and Zhang for describing all the solutions of a high-dimensional ideal is reducing ideal I to zero dimension by placing the independent variables U in the base field. Then combining the RUR for zero-dimension ideals and Wu's method, the solutions of I in L^n can be expressed.

It can be seen from Definition 3.1 that we get the expression of $n-d$ coordinates through U and I^e. However, $I \subset I^e \in k(U)[V]$ and the roots of I^e is in $L(U)^{n-d}$. Therefore, we take $p \in L^d$ as the value of U, and consider ideal I_p and two key points of Remark 2.11. Tan and Zhang[17] proved that when $p \notin \mathbb{V}_L(\mathcal{F}\triangle_t)$, I_p is a zero-dimensional ideal, $t \in k[V]$ is a separating element of I_p and $\mathcal{G}_{U,t}(1, t(\alpha))|_{U=p}$ is not zero, where $t(\alpha) \in \mathbb{V}_L(\mathcal{X}_{U,t}(T)|_{U=p})$, $\alpha \in \mathbb{V}_L(I_p)$. Consequently, $\mathcal{R}_t^U$ can represent the point set

$$\mathcal{W}_t^U = \Bigg\{(x_1, x_2, \cdots, x_n) \in L^n \mid (x_{i_1}, x_{i_2}, \cdots, x_{i_d}) = p,\ x_{i_j} = \left.\frac{\mathcal{G}_{U,t}(x_{i_j}, t(\alpha))}{\mathcal{G}_{U,t}(1, t(\alpha))}\right|_{U=p},\ d+1 \le j \le n,$$
$$p \in L^d,\ p \notin \mathbb{V}_L(\mathcal{F}\triangle_t) \subset L^d,\ t(\alpha) \in \mathbb{V}_L(\mathcal{X}_{U,t}(T)|_{U=p}),\ \alpha \in \mathbb{V}_L(I_p)\Bigg\}.$$

Obviously, $\mathcal{W}_t^U = \mathbb{V}_L(I) \setminus \mathbb{V}_L(\mathcal{F}\triangle_t)$ forms a branch of $\mathbb{V}_L(I)$. Then considering other branches: $\mathbb{V}_L(\langle I, \mathcal{F}\rangle)$ and $\mathbb{V}_L(\langle I, \triangle_t\rangle)$, the computations just repeat the above steps. Finally, $\mathbb{V}_L(I)$ can be represented by a finite number of RRS.

3.2 Improvement

In order to present the improvement for rational representations, let us introduce some necessary knowledge points. The details can refer to [21].

A specialization of $k[U]$ is a homomorphism $\sigma : k[U] \to L$. In this paper, we consider the specializations induced by the elements in L^d. That is, for $p \in L^d$, the induced specialization

σ_p is defined as

$$\sigma_p : f \to f(p),$$

where $f \in k[U]$. Every specialization σ: $k[U] \to L$ extends canonically to a specialization σ: $k[U][V] \to L[V]$ by applying σ coefficient-wise.

Definition 3.3 Given a polynomial set $\widehat{G} \subset k[Y, Z]$ and an admissible block order $\prec_{Y,Z}$ with $Y \ll Z$, we say $F \subset k[Y, Z]$, denoted as $\mathrm{MDBasis}(\widehat{G})$, is a Minimal Dickson Basis of $\widehat{G}$, if

1) F is a subset of $\widehat{G}$, and

2) for every polynomial $g \in \widehat{G}$, there is some polynomial $f \in F$ such that $\mathrm{LM}_{\prec_Z}(g)$ is a multiple of $\mathrm{LM}_{\prec_Z}(f)$, i.e., $\langle \mathrm{LM}_{\prec_Z}(F)\rangle = \langle \mathrm{LM}_{\prec_Z}(\widehat{G})\rangle$, and

3) for any two distinct $f_1, f_2 \in F$, neither $\mathrm{LM}_{\prec_Z}(f_1)$ is a multiple of $\mathrm{LM}_{\prec_Z}(f_2)$ nor $\mathrm{LM}_{\prec_Z}(f_2)$ is a multiple of $\mathrm{LM}_{\prec_Z}(f_1)$.

Theorem 3.4 (see [21]) *Let $\widehat{G}$ be a Gröbner basis of the ideal $\langle F\rangle \subset k[Y, Z]$ w.r.t. an admissible block order $\prec_{Y,Z}$ with $Y \ll Z$. Let $\widehat{G}_r = \widehat{G} \cap k[Y]$ and $\widehat{G}_m = \mathrm{MDBasis}(\widehat{G} \setminus \widehat{G}_r)$. If σ is a specialization from $k[Y]$ to L such that*

1) $\sigma(g) = 0$ for $g \in \widehat{G}_r$, and

2) $\sigma(h) \neq 0$, where $h = \prod_{g\in\widehat{G}_m} \mathrm{LC}_{\prec_Z}(g) \in k[Y]$,

then $\sigma(\widehat{G}_m)$ is a (minimal) Gröbner basis of $\langle\sigma(F)\rangle$ in $L[Z]$ w.r.t. $\prec_Z$.

Remark 3.5 When $\widehat{G}_r = \emptyset$ (i.e., Y is a maximally independent set modulo ideal $\langle F\rangle$), then $\widehat{G}_m$ is actually a Gröbner basis of the ideal $\langle F\rangle_{k(Y)[Z]}$ generated by F in $k(Y)[Z]$.

According to Theorem 3.4, we now suppose $\widehat{G}$ is a Gröbner basis of the ideal $I \subset k[U, V]$ w.r.t. a block order $\prec_{U,V}$ with $U \ll V$, where U is a maximally independent set modulo I. Set $G_m = \mathrm{MDBasis}(\widehat{G}) = \{\widehat{g}_1, \widehat{g}_2, \cdots, \widehat{g}_l\} \subset I$. Then G_m is a Gröbner basis of I^e w.r.t. $\prec_V$, but it is not necessarily a basis of ideal I (unlike G being a basis of ideal I in Subsection 3.1). Let $\mathcal{F}_m = \mathrm{LCM}\{\mathrm{LC}_{\prec_V}(\widehat{g}_i) | 1 \leq i \leq l\} \in k[U]$. When $p \notin \mathbb{V}_L(\mathcal{F}_m) \subset L^d$ and the specialization σ_p acts on I and G_m, as a consequence, G_{mp} is a Gröbner basis of I_p, where $G_{mp} = \{\widehat{g}|_{U=p} \in L[V] \mid \widehat{g} \in G_m\}$.

Further, it is noted that G_m and G_{mp} are the minimal Gröbner basis of I^e and I_p w.r.t. $\prec_V$, respectively.

Remark 3.6 In [17], $G \subset k[U, V]$ is a Gröbner basis of I^e w.r.t. $\prec_V$, and it is also required to be a basis of ideal I. The purpose is to make G_p a Gröbner basis of ideal I_p ($p \notin \mathbb{V}_L(\mathcal{F})$), then the standard bases of $A_{k(U)}(I^e) = k(U)[V]/I^e$ and $A_L(I_p) = L[V]/I_p$ are the same. So we can establish a correspondence between the RRS of I^e and the RRS of I_p through specialization σ_p. However, we have found a point: There exists a $G^* \subset k[U, V]$, which is a Gröbner basis of I^e but not a basis of ideal I, such that G^*_p is a Gröbner basis of ideal I_p, when $p \notin \mathbb{V}_L(\mathcal{F}^*)$. Surprisingly, G_m mentioned above is just such a G^*, then it can be used to establish the connection between I^e and I_p.

As follows, we give a theorem similar to Theorem 3.2 in [17], which is a main theorem of this paper. The proof of the theorem is basically the same as the proof of Theorem 3.2 in [17], except that in the process of proving $\sharp\mathbb{V}_L(I_p) \leq \sharp\mathbb{V}_L(I^e)$, "the contraction I^{ec} of I^e to $k[X]$

equals $I : \mathcal{F}^{\infty}$" needs to be replaced with "the contraction I^{ec} of I^e to $k[X]$ equals $\langle G_m\rangle : \mathcal{F}_m^{\infty}$, and $\langle G_m\rangle \subset I$" (see [2] for more details of the contraction of an ideal). For the sake of the rigor of the argument and the ease of understanding, here we still give a proof.

Theorem 3.7 *Suppose that G_m and $\mathcal{F}_m$ are as above, $t \in k[V]$ is a separating element of I^e, and $\{\mathcal{X}_{U,t}(T), \mathcal{G}_{U,t}(1,T), \mathcal{G}_{U,t}(x_{i_{d+1}}, T), \cdots, \mathcal{G}_{U,t}(x_{i_n}, T)\}$ is the RUR of I^e associated to t. If $p \notin \mathbb{V}_L(\mathcal{F}_m \triangle_t(U)) \subset L^d$, then $t \in k[V]$ is also a separating element of I_p. Furthermore,*

$$\{\mathcal{X}_{U,t}(T)|_{U=p}, \mathcal{G}_{U,t}(1,T)|_{U=p}, \mathcal{G}_{U,t}(x_{i_{d+1}}, T)|_{U=p}, \cdots, \mathcal{G}_{U,t}(x_{i_n}, T)|_{U=p}\}$$

is the RUR of I_p associated to t, where $\triangle_t(U) \in k[U]$ is the numerator of the resultant of $\overline{\mathcal{X}_{U,t}(T)}$ and its derivative $\overline{\mathcal{X}_{U,t}(T)}'$ w.r.t. the variable T.

Proof First we have to prove:

$$\sharp\mathbb{V}_L(I_p) \leq \sharp\mathbb{V}_L(I^e), \quad p \notin \mathbb{V}_L(\mathcal{F}_m) \subset L^d.$$

From the above we know that when $p \notin \mathbb{V}_L(\mathcal{F}_m)$, G_{mp} is a Gröbner basis of I_p and $\mathrm{LC}_{\prec_V}(\widehat{g})|_{U=p} \neq 0$ for $\widehat{g} \in G_m$. This means $A_{k(U)}(I^e) = k(U)[V]/I^e$ and $A_L(I_p) = L[V]/I_p$ have the same standard bases $\mathcal{B}$. Therefore I_p is zero-dimensional since I^e is a zero-dimensional ideal. Assume that $h \in k[V]$ is a separating element of I_p and $\mathcal{X}_{U,h}$ is the characteristic polynomial of multiplication map $m_h^{A_{k(U)}(I^e)}$, then $\mathcal{X}_{U,h}(h) \in I^e$. It follows that there exists $l \in \mathbb{N}$ such that $\overline{\mathcal{X}_{U,h}}^{l}(h) \in I^e$. Now let $\overline{\mathcal{X}_{U,h}}$ be multiplied by the least common multiple of all denominators appearing in its coefficients and the result is written as P_h. We have

$$P_h^l(h) \in I^e \cap k[X] = I^{ec}.$$

By the contraction theory of ideals (see [2] for more details),

$$I^{ec} = \langle G_m\rangle : \mathcal{F}_m^{\infty},$$

where $\langle G_m\rangle$ is an ideal generated by G_m in $k[X]$. Then there exists $k \in \mathbb{N}$ such that $\mathcal{F}_m^k P_h^l(h) \in \langle G_m\rangle \subset I$. This implies $\mathcal{F}_m P_h(h) \in \sqrt{I}$. Hence $(\mathcal{F}_m P_h(h))|_{U=p} \in \sqrt{I}_p$. Since $\sqrt{I}_p \subset \sqrt{I_p}$ and $0 \neq \mathcal{F}_m|_{U=p} \in L$,

$$P_h(h)|_{U=p} = P_h|_{U=p}(h) \in \sqrt{I_p}.$$

And $\mathrm{LC}_{\prec_V}(P_h)(p) \neq 0$, so $P_h|_{U=p}(h)$ is not a zero polynomial. Thus,

$$\sharp\mathbb{V}_L(I_p) \leq \mathrm{degree}(P_h|_{U=p}) = \mathrm{degree}(\overline{\mathcal{X}_{U,h}}|_{U=p}) \leq \mathrm{degree}(\overline{\mathcal{X}_{U,h}}) \leq \sharp\mathbb{V}_L(I^e).$$

Now let us show that t is a separating element of I_p if $p \notin \mathbb{V}_L(\mathcal{F}_m \triangle_t(U))$. Let M_t and $\overline{M}_t$ be the multiplication matrices of t w.r.t. $\mathcal{B}$ in quotient rings $A_{k(U)}(I^e)$ and $A_L(I_p)$, respectively. By the definition of multiplication matrices and that $A_{k(U)}(I^e)$ and $A_L(I_p)$ have the same standard bases $\mathfrak{B}$, $\overline{M}_t = M_t|_{U=p}$. Then $\mathcal{X}_{U,t}|_{U=p}$ is the characteristic polynomial of $\overline{M}_t$. According to Corollary 2.8, we just need to prove that

$$\mathrm{degree}(\overline{\mathcal{X}_{U,t}|_{U=p}}) = \sharp\mathbb{V}_L(I_p).$$

Suppose the square-free decomposition of $\mathcal{X}_{U,t}$ is as follows:

$$\mathcal{X}_{U,t} = P_1 P_2^2 \cdots P_l^l.$$

Then

$$\begin{aligned}\overline{\mathcal{X}_{U,t}}|_{U=p} &= (P_1|_{U=p})(P_2|_{U=p}) \cdots (P_l|_{U=p}),\\ \mathcal{X}_{U,t}|_{U=p} &= (P_1|_{U=p})(P_2|_{U=p})^2 \cdots (P_l|_{U=p})^l.\end{aligned}$$

Obviously, $\overline{\mathcal{X}_{U,t}|_{U=p}}\Big|\overline{\mathcal{X}_{U,t}}|_{U=p}$. Since $\triangle_t(p) \neq 0$, $\overline{\mathcal{X}_{U,t}}|_{U=p}$ is square-free, which implies that

$$\overline{\mathcal{X}_{U,t}|_{U=p}} = \overline{\mathcal{X}_{U,t}}|_{U=p}.$$

Hence,

$$\sharp\mathbb{V}_L(I_p) \geq \text{degree}(\overline{\mathcal{X}_{U,t}|_{U=p}}) = \text{degree}(\overline{\mathcal{X}_{U,t}}|_{U=p}) = \sharp\mathbb{V}_L(I^e).$$

Together with $\sharp\mathbb{V}_L(I_p) \leq \sharp\mathbb{V}_L(I^e)$, we have degree$(\overline{\mathcal{X}_{U,t}|_{U=p}}) = \sharp\mathbb{V}_L(I_p)$, So t is a separating element of I_p.

In addition, if $\overline{\mathcal{X}_{U,t}} = \sum_{j=0}^{d} a_j T^{d-j}$, then

$$g_t(v,T) = \sum_{i=0}^{d-1}\sum_{j=0}^{d-i-1} \text{Trace}(M_{vt^i}) a_j T^{d-i-j-1}.$$

Moreover, $\mathcal{X}_{U,t}|_{U=p}$ is the characteristic polynomial of $\overline{M}_t$. Both $\overline{\mathcal{X}_{U,t}|_{U=p}} = \overline{\mathcal{X}_{U,t}}|_{U=p}$ and $\overline{M}_{vt^i} = M_{vt^i}|_{U=p}$. It follows that the RUR of I^e associated to t under the specialization σ_p is the RUR of I_p associated to t.

Naturally, we have the RRS of I associated to U and t:

$$\widehat{\mathcal{R}}_t^U = \{\mathcal{F}_m(U)\triangle_t(U), \mathcal{X}_{U,t}(T), \mathcal{G}_{U,t}(1,T), \mathcal{G}_{U,t}(x_{i_{d+1}},T), \cdots, \mathcal{G}_{U,t}(x_{i_n},T)\}.$$

Correspondingly,

$$\begin{aligned}\widehat{\mathcal{W}}_t^U = \Bigg\{(x_1,x_2,\cdots,x_n) \in L^n \Bigg| &(x_{i_1},x_{i_2},\cdots,x_{i_d}) = p, p \in L^d, p \notin \mathbb{V}_L(\mathcal{F}_m\triangle_t) \subset L^d, d+1 \leq j \leq n,\\ &x_{i_j} = \frac{\mathcal{G}_{U,t}(x_{i_j},t(\alpha))}{\mathcal{G}_{U,t}(1,t(\alpha))}\Bigg|_{U=p},\ t(\alpha) \in \mathbb{V}_L(\mathcal{X}_{U,t}(T)|_{U=p}),\ \alpha \in \mathbb{V}_L(I_p)\Bigg\}.\end{aligned}$$

Similarly, there exists a decomposition:

$$\begin{aligned}\mathbb{V}_L(I) &= \mathbb{V}_L(I) \setminus \mathbb{V}_L(\mathcal{F}_m\triangle_t) \cup \mathbb{V}_L(\langle I, \mathcal{F}_m\rangle) \cup \mathbb{V}_L(\langle I, \triangle_t\rangle)\\ &= \widehat{\mathcal{W}}_t^U \cup \mathbb{V}_L(\langle I, \mathcal{F}_m\rangle) \cup \mathbb{V}_L(\langle I, \triangle_t\rangle).\end{aligned}$$

It can be clearly seen from the above that we replace the basis G with a minimal Dickson basis G_m of a Gröbner basis of the ideal I, so $\mathcal{F}$ becomes $\mathcal{F}_m$. As should be evident from the definition of minimal Dickson basis and Theorem 3.4, G_m is much smaller in size than G, thus $\mathcal{F}_m$ is "smaller" than $\mathcal{F}$. For example, $G = \{ax, bx^2\}$, $G_m = \{ax\}$, $U = \{a, b\}$, then $\mathcal{F} = ab$, $\mathcal{F}_m = a$. Note that although we replace G and $\mathcal{F}$ with G_m and $\mathcal{F}_m$ respectively, the standard basis $\mathcal{B}$ of $A_{k(U)}(I^e)$ is still the same. Therefore $\mathcal{X}_{U,t}$, $\mathcal{G}_{U,t}(1, T)$ and $\mathcal{G}_{U,t}(x_{i_j}, T)$ $(d+1 \leq j \leq n)$ are the same. So, in general $\{\mathcal{F}_m\triangle_t, \mathcal{X}_{U,t}, \cdots\}$ can represent more solutions than $\{\mathcal{F}\triangle_t, \mathcal{X}_{U,t}, \cdots\}$. More importantly, branching is done based on the least common multiple $\mathcal{F}_m$ instead of $\mathcal{F}$. As a result, the number of branches (i.e the number of rational representational sets) generated by the following algorithm based on the improvement is smaller than that of the branches in the algorithm of [17] presented by Tan and Zhang. $\blacksquare$

4 Algorithm

Based on Theorems 3.4 and 3.7, we are now ready to give the improved algorithm for computing a rational representation of a high-dimensional ideal, which reduces the number of branches in the algorithm of [17]. In this paper, we regard the Tan-Zhang algorithm of [17] as the original algorithm. In order to enable everyone to understand the algorithm more intuitively, we deliberately avoid tricks and optimizations, such as the selection of separating elements, choosing a minimal Dickson basis and factoring $\mathcal{X}_{U,t}(T)$ to simplify the output expression. We remind that the improved algorithm for finding separating elements of a zero-dimensional ideal proposed by Tan in [16] can also be used in high-dimensional cases.

Of course, the way of iteration or recursion can be changed. In [17], the iteration of the original algorithm is divided into two lines:

$$\mathbb{V}_L(\langle I, \mathcal{F}\rangle) = \mathbb{V}_L(\langle I, \mathcal{F}\rangle) \setminus \mathbb{V}_L(\mathcal{F}_1\triangle_{t_1}) \cup \mathbb{V}_L(\langle I, \mathcal{F}_1\rangle) \cup \mathbb{V}_L(\langle I, \triangle_{t_1}\rangle);$$
$$\mathbb{V}_L(\langle I, \triangle_t\rangle) = \mathbb{V}_L(\langle I, \triangle_t\rangle) \setminus \mathbb{V}_L(\mathcal{F}_2\triangle_{t_2}) \cup \mathbb{V}_L(\langle I, \mathcal{F}_2\triangle_{t_2}\rangle).$$

Here, we use an iterative approach different from the iteration of the original algorithm. In this paper, that we compare the performance of the improved algorithm and the original algorithm is performed under the same iteration or recursion approach. That is to say, we modify the iteration of the original algorithm to be the same as the iteration of our improved algorithm.

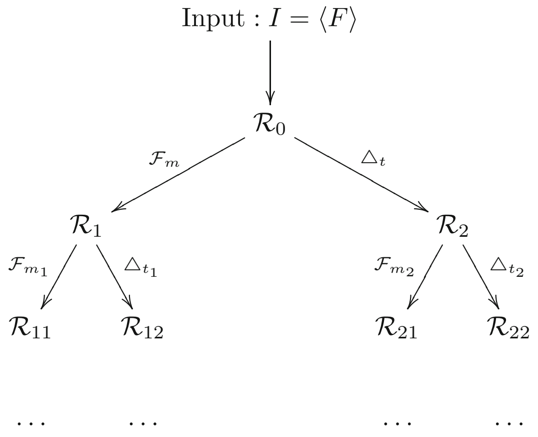
The following Algorithm RR(F) is the main algorithm for computing rational representations, where $\langle F\rangle$ denotes the ideal generated by the set F on $k[X]$.

```
Algorithm RR(F)
Input $F$, a finite subset of $k[X]$.
Output $\mathcal{R}$, a rational representation of $\mathbb{V}_L(\langle F\rangle)$.
1. Set $I := \langle F\rangle$;
2. If dim($I$)=0, then return $\mathcal{R}$:=the RUR of zero-dimensional ideal $I$; Else,
3. Compute a rational representation set of $I = \langle F\rangle$:
   $\mathcal{R} := RRS(F) = \{\mathcal{F}_m\triangle_t(U), \mathcal{X}_{U,t}(T), \mathcal{G}_{U,t}(1, T), \mathcal{G}_{U,t}(x_{i_{d+1}}, T), \cdots, \mathcal{G}_{U,t}(x_{i_n}, T)\}$;
4. Return $\mathcal{R} := \mathcal{R} \cup RR(F \cup \{\mathcal{F}_m\}) \cup RR(F \cup \{\triangle_t\})$.
```

In the above algorithm, RRS(F) is the a subroutine which is to compute a rational representation set and whose details are as follows.

```
Algorithm RRS(F)
Input $F$, a finite subset of $k[X]$.
Output $\mathcal{R}_t^U$, a rational representation set of $I = \langle F \rangle$.
1. Set $I := \langle F \rangle$;
2. If dim($I$)=0, then return the RUR $\mathcal{R}_t^U$ of zero-dimensional ideal $I$; Else,
3. Compute a maximally independent set $U$ modulo $I$, and the set $V := X \setminus U$ ;
4. Compute a Gröbner basis $G$ of $I$ w.r.t. an admissible block order $\prec_{U,V}$ with $U \ll V$;
5. Set $G_m$:=MDBasis($G$) as a Gröbner basis of $I^e$ w.r.t. $\prec_V$;
6. Compute $\mathcal{F}_m := \mathrm{LCM}\{\mathrm{LC}_{\prec_V}(g) | g \in G_m\}$;
7. Choose a separating element $t \subset k[V]$ of $I^e$;
8. Compute an RUR of $I^e$: $\{\mathcal{X}_{U,t}(T), \mathcal{G}_{U,t}(1,T), \mathcal{G}_{U,t}(x_{i_{d+1}},T), \cdots, \mathcal{G}_{U,t}(x_{i_n},T)\}$ associated to $t$;
9. Compute $\triangle_t(U) \in k[U]$: the numerator of $Res_T(\overline{\mathcal{X}_{U,t}(T)}, \overline{\mathcal{X}_{U,t}(T)}')$ ;
10. Return $\mathcal{R}_t^U := \{\mathcal{F}_m(U)\triangle_t(U), \mathcal{X}_{U,t}(T), \mathcal{G}_{U,t}(1,T), \mathcal{G}_{U,t}(x_{i_{d+1}},T), \cdots, \mathcal{G}_{U,t}(x_{i_n},T)\}$.
```

It can be known from the above algorithm that the this algorithm uses recursion. The simple schematic diagram of the algorithm is as follows.



Herein, we need to explain the termination of the algorithm.

Theorem 4.1 *The above Algorithm RR(F) terminates in a finite number of steps.*

Proof When dim(I)=0, $\mathcal{R}$ is the RUR of zero-dimensional ideal I and the algorithm terminates. Now we consider that dim(I)> 0. We have the decomposition:

$$\mathbb{V}_L(I) = \mathbb{V}_L(I) \setminus \mathbb{V}_L(\mathcal{F}_m\triangle_t) \cup \mathbb{V}_L(\langle I, \mathcal{F}_m\rangle) \cup \mathbb{V}_L(\langle I, \triangle_t\rangle).$$

Write

$$I_1 = \langle I, \mathcal{F}_m \rangle,$$
$$I_2 = \langle I, \triangle_t \rangle.$$

The constructions of $\mathcal{F}_m$ and $\triangle_t$ imply that $\mathcal{F}_m, \triangle_t \notin I$. So $I \subsetneqq I_i$, $i = 1, 2$. Then

$$\mathbb{V}_L(I_1) = \mathbb{V}_L(I_1) \setminus \mathbb{V}_L(\mathcal{F}_{m_1}\triangle_{t_1}) \cup \mathbb{V}_L(\langle I, \mathcal{F}_{m_1}\rangle) \cup \mathbb{V}_L(\langle I, \triangle_{t_1}\rangle);$$
$$\mathbb{V}_L(I_2) = \mathbb{V}_L(I_2) \setminus \mathbb{V}_L(\mathcal{F}_{m_2}\triangle_{t_2}) \cup \mathbb{V}_L(\langle I, \mathcal{F}_{m_2}\rangle) \cup \mathbb{V}_L(\langle I, \triangle_{t_2}\rangle).$$

Write

$$I_{11} = \langle I_1, \mathcal{F}_{m_1}\rangle, \quad I_{12} = \langle I_1, \triangle_{t_1}\rangle,$$
$$I_{21} = \langle I_2, \mathcal{F}_{m_2}\rangle, \quad I_{22} = \langle I_2, \triangle_{t_2}\rangle,$$

where $I_i \subsetneqq I_{ij}$, $i, j \in \{1, 2\}$.

Go on like this, we get strictly ascending ideal chains:

$$I \subsetneqq I_i \subsetneqq I_{ij} \subsetneqq I_{ijl} \subsetneqq \cdots$$

According to the ascending chain condition, they must terminate in a zero-dimensional ideal. From $I_{i\cdots j}$ to $I_{i\cdots jl}$, it only creates finite branches.

In summary, 1) in each step, the algorithm only creates finite branches; 2) each branch terminates after finite steps. According to König's Lemma, the algorithm terminates in a finite number of steps. ▮

5 An Illustrative Example

The proposed improved algorithm to compute a rational representation for a high-dimensional ideal is illustrated on an example.

Example 5.1 Consider the ideal: $I = \langle F\rangle \subset \mathbb{C}[x, y, z, w], F = \{f_1, f_2\}$, where

$$f_1 = xyw^3 - z,$$
$$f_2 = xw^3 + yw + z,$$

and $X = \{x, y, z, w\}$. We compute the Gröbner basis under a block order $\prec_{U,V}$ with $U \ll V$ $(U, V \subset X)$; within each block, $\prec_U$ and $\prec_V$ are graded lexicographic orders.

1) dim(I)≠0, we compute a rational representation set of I: A maximally independent set $U = \{z, w\}$, $V = X \setminus U = \{x, y\}$, the reduced Gröbner basis of I w.r.t.$\prec_{U,V}$ is $G = \{xw^3 + yw + z, y^2w + yz + z, xyzw^2 + xzw^2 + yz, xyz^2w + xz^2w + xzw^2 - y^2z + yz, xyz^3 + xz^3 + xz^2w + 2xzw^2 + y^3z - 2y^2z + 2yz\}$, then $G_m = \{xw^3 + yw + z, y^2w + yz + z\}, \mathcal{F}_m = w^3$; choosing a separating element $t = x$, then $\mathcal{X}_{U,t}(T) = T^2 + zT/w^3 + z/w^5$, $\triangle_t = z(4w - z)$, $\mathcal{G}_{U,t}(1, T) = 2T + z/w^3$, $\mathcal{G}_{U,t}(x, T) = (-zw^2T - 2z)/w^5$, $\mathcal{G}_{U,t}(y, T) = (2zw - zw^3T - z^2)/w^4$. A rational representation set of I is $\mathcal{R}_0 = \{\mathcal{F}_m\triangle_t, \mathcal{X}_{U,t}, \mathcal{G}_{U,t}(1, T), \mathcal{G}_{U,t}(x, T), \mathcal{G}_{U,t}(y, T)\}$.

2) deg($\mathcal{F}_m$)≠0 and dim($\langle I, \mathcal{F}_m\rangle$)≠0, we compute a rational representation set of $I_1 = \langle I, \mathcal{F}_m\rangle$: A maximally independent set $U_1 = \{x, y\}$, $V_1 = \{z, w\}$, the reduced Gröbner basis of I_1 w.r.t. $\prec_{U_1,V_1}$ is $G_1 = \{yw, z, w^3\}$, then $G_{m_1} = \{yw, z\}, \mathcal{F}_{m_1} = y$; choosing a separating element $t_1 = z$, then $\mathcal{X}_{U_1,t_1}(T) = T$, $\triangle_{t_1} = 1$. A rational representation set of I_1 is $\mathcal{R}_1 = \{\mathcal{F}_{m_1}\triangle_{t_1}, \mathcal{X}_{U_1,t_1}, \mathcal{G}_{U_1,t_1}(1, T), \mathcal{G}_{U_1,t_1}(z, T), \mathcal{G}_{U_1,t_1}(w, T)\} = \{y, T, 1, 0, 0\}$.

3) $\deg(\mathcal{F}_{m_1})\neq 0$ and $\dim(\langle I_1, \mathcal{F}_{m_1}\rangle)\neq 0$, we compute a rational representation set of $I_{11} = \langle I_1, \mathcal{F}_{m_1}\rangle$: $U_{11} = \{x\}$, $V_{11} = \{y, z, w\}$, the reduced Gröbner basis $G_{11} = \{z, y, w^3\}$, then $G_{m_{11}} = \{z, y, w^3\}, \mathcal{F}_{m_{11}} = 1$; choosing a separating element $t_{11} = w$, then $\mathcal{X}_{U_{11},t_{11}}(T) = T^3$, $\triangle_{t_{11}} = 1$. A rational representation set of I_{11} is $\mathcal{R}_{11} = \{\mathcal{F}_{m_{11}}\triangle_{t_{11}}, \mathcal{X}_{U_{11},t_{11}}, \mathcal{G}_{U_{11},t_{11}}(1,T), \mathcal{G}_{U_{11},t_{11}}(y,T), \mathcal{G}_{U_{11},t_{11}}(z,T), \mathcal{G}_{U_{11},t_{11}}(w,T)\} = \{1, T^3, 3, 0, 0, 0\}$.

Here, $\triangle_{t_1}=1$, $\mathcal{F}_{m_{11}}=1$, and $\triangle_{t_{11}}=1$, so the rational representation set of $\langle I_1, \triangle_{t_1}\rangle$, $\langle I_2, \mathcal{F}_{m_{11}}\rangle$, and $\langle I_2, \triangle_{t_{11}}\rangle$ are $\emptyset$. Then no new branches are generated.

4) $\deg(\triangle_t)\neq 0$ and $\dim(\langle I, \triangle_t\rangle)\neq 0$, we compute a rational representation set of $I_2 = \langle I, \triangle_t\rangle$: $U_2 = \{x, y\}$, $V_2 = \{z, w\}$, $\mathcal{F}_{m_2} = y^3(y+2)^2$; choosing a separating element $t_2 = z$, then $\mathcal{X}_{U_2,t_2}(T) = T$, $\triangle_{t_2} = 1$. A rational representation set of I_2 is $\mathcal{R}_2 = \{\mathcal{F}_{m_2}\triangle_{t_2}, \mathcal{X}_{U_2,t_2}, \mathcal{G}_{U_2,t_2}(1,T), \mathcal{G}_{U_2,t_2}(z,T), \mathcal{G}_{U_2,t_2}(w,T)\} = \{y^3(y+2)^2, T, 1, 0, 0\}$.

5) $\deg(\mathcal{F}_{m_2})\neq 0$ and $\dim(\langle I_2, \mathcal{F}_{m_2}\rangle)\neq 0$, we compute a rational representation set of $I_{21} = \langle I_2, \mathcal{F}_{m_2}\rangle$: $U_{21} = \{w\}$, $V_{21} = \{x, y, z\}$, $\mathcal{F}_{m_{21}} = w^3$; choosing a separating element $t_{21} = y$, then $\mathcal{X}_{U_{21},t_{21}}(T) = T^2(T+2)^2$, $\triangle_{t_{21}} = -4$. A rational representation set of I_{21} is $\mathcal{R}_{21} = \{\mathcal{F}_{m_{21}}\triangle_{t_{21}}, \mathcal{X}_{U_{21},t_{21}}, \mathcal{G}_{U_{21},t_{21}}(1,T), \mathcal{G}_{U_{21},t_{21}}(x,T), \mathcal{G}_{U_{21},t_{21}}(y,T), \mathcal{G}_{U_{21},t_{21}}(z,T)\} = \{-4w^3, T^2(T+2)^2, 4T+4, -4T/w^2, -4T, 8wT\}$.

6) $\deg(\mathcal{F}_{m_{21}})\neq 0$ and $\dim(\langle I_{21}, \mathcal{F}_{m_{21}}\rangle)\neq 0$, we compute a rational representation set of $I_{211} = \langle I_{21}, \mathcal{F}_{m_{21}}\rangle$: $U_{211} = \{x\}$, $V_{211} = \{y, z, w\}$, $\mathcal{F}_{m_{211}} = 1$; choosing a separating element $t_{211} = y$, then $\mathcal{X}_{U_{211},t_{211}}(T) = T^5(T+2)^2$, $\triangle_{t_{211}} = -4$. A rational representation set of I_{211} is $\mathcal{R}_{211} = \{\mathcal{F}_{m_{211}}\triangle_{t_{211}}, \mathcal{X}_{U_{211},t_{211}}, \mathcal{G}_{U_{211},t_{211}}(1,T), \mathcal{G}_{U_{211},t_{211}}(y,T), \mathcal{G}_{U_{211},t_{211}}(z,T), \mathcal{G}_{U_{211},t_{211}}(w,T)\} = \{-4, T^5(T+2)^2, 7T+10, -4T, 0, 0\}$.

$\triangle_{t_2} = 1$, $\triangle_{t_{21}} = -4$, $\mathcal{F}_{m_{211}} = 1$ and $\triangle_{t_{211}} = -4$, so no other branches are created and the algorithm terminates.

Thus, we obtain a rational representation of $\mathbb{V}_L(I)$:

$$\bigcup_{i=0}^{5} \mathcal{R}_i = \mathcal{R}_0 \cup \mathcal{R}_1 \cup \mathcal{R}_{11} \cup \mathcal{R}_2 \cup \mathcal{R}_{21} \cup \mathcal{R}_{211},$$

where $\mathcal{R}_3 = \mathcal{R}_{11}, \mathcal{R}_4 = \mathcal{R}_{21}, \mathcal{R}_5 = \mathcal{R}_{211}$ as above.

However, if we use the original algorithm to compute, we can get a rational representation of $\mathbb{V}_L(I)$ which has nine branches:

$$\begin{aligned}
\mathcal{R}'_0 = \{&\mathcal{F}\triangle_t = w^3z^3(4w-z),\ \mathcal{X}_{U,t} = T^2 + zT/w^3 + z/w^5,\ \mathcal{G}_{U,t}(1,T) = 2T + z/w^3,\\
&\mathcal{G}_{U,t}(x,T) = (-zw^2T - 2z)/w^5,\ \mathcal{G}_{U,t}(y,T) = (2zw - zw^3T - Z^2)/w^4\};\\
\mathcal{R}'_1 = \{&\mathcal{F}_1\triangle_{t_1} = xy^6,\ \mathcal{X}_{U_1,t_1} = T,\ \mathcal{G}_{U_1,t_1}(1,T) = 1,\ \mathcal{G}_{U_1,t_1}(z,T) = 0,\ \mathcal{G}_{U_1,t_1}(w,T) = 0\};\\
\mathcal{R}'_{11} = \{&\mathcal{F}_{11}\triangle_{t_{11}} = x,\ \mathcal{X}_{U_{11},t_{11}} = T^{18},\ \mathcal{G}_{U_{11},t_{11}}(1,T) = 1,\ \mathcal{G}_{U_{11},t_{11}}(y,T) = 0,\\
&\mathcal{G}_{U_{11},t_{11}}(z,T) = 0,\ \mathcal{G}_{U_{11},t_{11}}(w,T) = 0\};\\
\mathcal{R}'_{111} = \{&\mathcal{F}_{111}\triangle_{t_{111}} = y,\ \mathcal{X}_{U_{111},t_{111}} = T,\ \mathcal{G}_{U_{111},t_{111}}(1,T) = 1,\ \mathcal{G}_{U_{111},t_{111}}(x,T) = 0,\\
&\mathcal{G}_{U_{111},t_{111}}(z,T) = 0,\ \mathcal{G}_{U_{111},t_{111}}(w,T) = 0\};
\end{aligned}$$

$$\begin{aligned}
\mathcal{R}'_{1111} = \{&\mathcal{F}_{1111}\triangle_{t_{1111}} = 1,\ \mathcal{X}_{U_{1111},t_{1111}} = T,\ \mathcal{G}_{U_{1111},t_{1111}}(1,T) = 1,\ \mathcal{G}_{U_{1111},t_{1111}}(x,T) = 0,\\
&\mathcal{G}_{U_{1111},t_{1111}}(y,T) = 0,\ \mathcal{G}_{U_{1111},t_{1111}}(z,T) = 0\};\\
\mathcal{R}'_{2} = \{&\mathcal{F}_{2}\triangle_{t_{2}} = xy^3(y+2)^2,\ \mathcal{X}_{U_{2},t_{2}} = T,\ \mathcal{G}_{U_{2},t_{2}}(1,T) = 1,\ \mathcal{G}_{U_{2},t_{2}}(z,T) = 0,\\
&\mathcal{G}_{U_{2},t_{2}}(w,T) = 0\};\\
\mathcal{R}'_{21} = \{&\mathcal{F}_{21}\triangle_{t_{21}} = y^3(y+2)^2,\ \mathcal{X}_{U_{21},t_{21}} = T,\ \mathcal{G}_{U_{21},t_{21}}(1,T) = 1,\ \mathcal{G}_{U_{21},t_{21}}(z,T) = 0,\\
&\mathcal{G}_{U_{21},t_{21}}(w,T) = 0\};\\
\mathcal{R}'_{211} = \{&\mathcal{F}_{211}\triangle_{t_{211}} = -4w^3,\ \mathcal{X}_{U_{211},t_{211}} = T^2(T+2)^2,\ \mathcal{G}_{U_{211},t_{211}}(1,T) = 4T+4,\\
&\mathcal{G}_{U_{211},t_{211}}(x,T) = -4T/w^2,\ \mathcal{G}_{U_{211},t_{211}}(y,T) = -4T,\ \mathcal{G}_{U_{211},t_{211}}(z,T) = 8wT\};\\
\mathcal{R}'_{2111} = \{&\mathcal{F}_{2111}\triangle_{t_{2111}} = -4,\ \mathcal{X}_{U_{2111},t_{2111}} = T^5(T+2)^2,\ \mathcal{G}_{U_{2111},t_{2111}}(1,T) = 7T+10,\\
&\mathcal{G}_{U_{2111},t_{2111}}(y,T) = -4T,\ \mathcal{G}_{U_{2111},t_{2111}}(z,T) = 0,\ \mathcal{G}_{U_{2111},t_{2111}}(w,T) = 0\}.
\end{aligned}$$

We can see that in the first step $\mathcal{F}_m = w^3$, but $\mathcal{F} = z^2w^3$. And in fact, $\mathcal{R}'_0 = \mathcal{R}_0$, $\mathcal{R}'_{211} = \mathcal{R}_{21}$, $\mathcal{R}'_{2111} = \mathcal{R}_{211}$, $\mathcal{R}'_1 \cup \mathcal{R}'_{111} = \mathcal{R}_1$, $\mathcal{R}'_2 \cup \mathcal{R}'_{21} = \mathcal{R}_2$. Obviously, our improved algorithm generates fewer branches than the original algorithm.

6 Implementation and Comparative Performance

The improved algorithm and the original algorithm for computing a rational representation of the variety of a high-dimensional ideal have been implemented on the computer algebra system Maple. The codes and examples are available on the web: http://www.mmrc.iss.ac.cn /dwang/software.html. We randomly generate ten high-dimensional polynomial systems in $\mathbb{C}[X]$ to compare the performance of our algorithm and the original algorithm.

Ten examples are as follows. For all these examples, we compute the Gröbner basis of ideals under the block order $\prec_{U,V}$ with $U \ll V$, where U is a maximally independent set modulo the ideal, and $V = X \setminus U$; within each block, $\prec_U$ and $\prec_V$ are graded reverse lexicographic orders.

- $F_1 = \{-x_1x_2x_5^2, x_1x_5^2x_4 - x_5^2x_4^2 - 2x_4^3\}$;
- $F_2 = \{3x_1x_2x_5^2, 3x_1^2x_2x_4 + 2x_5x_2x_3^2 - x_1x_2x_4\}$;
- $F_3 = \{x_1^2x_3x_4 - x_5x_2 + 2x_2x_3, x_1^3x_5 - 3x_5x_4x_3\}$;
- $F_4 = \{x_1^3 + 2, -x_1x_2x_4^2, -x_4x_3^3 + x_1x_2x_3^2 - x_2^2x_3\}$;
- $F_5 = \{-3x_4x_1x_3^2 + x_3, 2x_5x_1^3 + 2x_4x_1x_3^2 + 3x_5x_2x_3\}$;
- $F_6 = \{x_3x_4, -x_4^2x_1^2 + 2x_4^2x_2^2 - 2x_4^2x_2, 2x_4^2x_2^2 - 2x_4x_2^2 + x_1x_2\}$;
- $F_7 = \{3x_1x_3^3 - x_1^2x_3, 3x_4^2x_3^2 + x_4^2x_3 - x_4x_1, x_4^2x_2x_3 - 2x_4x_1, 3x_4^4 - 3x_1^2x_2^2\}$;
- $F_8 = \{-2x_4^3x_2 + x_4^3x_3, -2x_4x_1x_3 - 3x_2x_3, 2x_1^2x_2^2 + 2x_2x - 3, -x_4^2x_1x_3 + 3x_4x_3^3 - 3x_4^2x_2\}$;
- $F_9 = \{(1-x_2)x_3^2 - x_2x_4^2 - x_6x_3 + x_2x_7x_3x_4 + 1, (1-x_1)x_4^2 - x_1x_3^2 - x_5x_4 + x_1x_7x_3x_4 + 1\}$.

- $F_{10} = \{3x_4x_1x_2^2 - 3x_4x_3^3 + 2x_4x_3^2, -3x_4x_1x_2^2 + 3x_1^3, 2x_4x_2^2x_3 - 3x_4^2x_1 - 2x_4x_1x - 3, -x_4^2x_2x_3 - 2x_4x_2 + x_1x_2\}$;

The following tables show the comparison of our improved algorithm with the original algorithm in the number of branches and running time in seconds. In algorithm implementation, we tried to do some optimization on the recursive process, such as taking the squarefree parts of $\mathcal{F}_m$ and $\triangle_t$, and factoring $\mathcal{F}_m\triangle_t$.

In Tables 1 and 2, the entries labeled with "New" and "Original" are our improved algorithm and the original algorithm (i.e., the Tan-Zhang's algorithm in [17]), respectively; "(1)" stands for in each step $\mathcal{F}_m$ and $\triangle_t$ do not perform any optimization processing; "(2)" stands for taking the squarefree parts of $\mathcal{F}_m$ and $\triangle_t$ instead of $\mathcal{F}_m$ and $\triangle_t$ to perform the recursive process; "(3)" stands for taking all the factors of the squarefree parts of $\mathcal{F}_m\triangle_t$ instead of $\mathcal{F}_m$ and $\triangle_t$ to perform the recursive process; ">1h " means that the computation does not terminate whithin one hour. Timings were obtained on a Core i7-4790 3.60GHz with 8GB Memory running Windows 7.

As is evident from Tables 1 and 2, our algorithms usually generate fewer branches, and the running times are less. It is because G_m is much smaller in size than G and branching is done based on $\mathcal{F}_m$ instead of $\mathcal{F}$, which lead to reducing the number of branches and then avoiding expensive Gröbner basis computation along branches. In addition, we can see that the optimization of taking the squarefree part can further reduce the number of branches and running times. For the optimization of factoring $\mathcal{F}_m\triangle_t$, although the number of branches may increase, the operation is simpler, which results in less times and simpler expressions. Exceptionally, New(3) has fewer branches than New(2) on examples F_2 and F_4, because $\mathcal{F}_m$ and $\triangle_t$ have common factors. On the whole, our improved algorithm has the better performance in contrast to the original algorithm in [17].

Table 1 Branches

Examples	New(1)	New(2)	New(3)	Original
F_1	10	5	7	14
F_2	21	17	14	∞
F_3	∞	19	25	∞
F_4	7	6	5	7
F_5	3	3	5	13
F_6	7	7	8	11
F_7	8	8	13	8
F_8	13	11	13	13
F_9	5	5	7	∞
F_{10}	8	8	22	∞

Table 2 Timings (sec)

Examples	New(1)	New(2)	New(3)	Original
F_1	0.780	0.062	0.062	2.356
F_2	1.404	0.234	0.093	>1h
F_3	>1h	0.172	0.343	>1h
F_4	23.181	0.764	0.624	23.198
F_5	0.031	0.031	0.031	0.250
F_6	0.062	0.047	0.078	0.561
F_7	2.199	0.344	0.109	8.315
F_8	0.359	0.141	0.109	109.076
F_9	0.062	0.063	0.062	>1h
F_{10}	8.222	1.685	0.343	>1h

7 Concluding Remarks

In the paper, we have presented an improvement of the rational representation for high-dimensional polynomial systems, which is based on the replacement of Gröbner basis for ideal I^e, that is, replacing a normal Gröbner basis G satisfying certain conditions with a minimal Dickson basis G_m. We proved the improvement is correct and gave the improved algorithm for computing the rational representation. Moreover, we proposed some optimizations on the recursive process. The performance comparison on implementation between our improved algorithm and the original algorithm is reported, and preliminary experiments show the efficiency of our proposed improvement in reducing the number of branches and running times.

What needs to be added is this improvement is also suitable for the simplified rational representation proposed by Shang, et al. in [18].

References

[1] Wu W T, *Basic Principles of Mechanical Theorem Proving in Geometries*, Vol. I: Part of Elementary Geometries, Science Press, Beijing, 1984 (in Chinese).

[2] Becker T and Weispfenning V, *Gröbner Bases*, Springer-Verlag, New York, 1993.

[3] Cox D, Little J, and O'shea D, *Using Algebra Geometry*, 2nd Edition, Springer, New York, 2005.

[4] Auzinger W and Stetter H J, An elimination algorithm for the computation of all zeros of a system of multivariate polynomial equations, *Inter., Series of Number. Math.*, 1988, **86**: 11–30.

[5] Stetter H J, Matrix eigenproblem are at the heart of polynomial system solving, *ACM SIGSAM Bull.*, 1996, **30**(4): 27–36.

[6] Kobayashi H, Fujise T, and Furukawa A, Solving systems of algebraic equations, *Poceedings of the ISSAC'*88, Springer Lecture Notes in Computer Science, 1988, **358**: 139–149.

[7] Yokoyama K, Noro M, and Takeshima T, Solutions of systems of algebraic equations and linear maps on residue class rings, *J. Symbolic Comput.*, 1992, **14**: 399–417.

[8] Lazard D, Résolution des systèmes d'équations algébriques, *Theor. Comp. Sci.*, 1981, **15**(1): 77–110.

[9] Lazard D, Gröbner bases, Gaussian elimination and resolution of system of algebraic equations, *Proc. EUROCAL*'83, Springer Lecture Notes in Computer Science, 1983, **162**: 146–156.

[10] Lazard D, Solving zero-dimensional algebraic systems, *J. Symbolic Comput.*, 1992, **13**: 117–133.

[11] Rouillier F, Solving zero-dimensional systems through the rational univariate representation, *Appl. Algebra ENngrg. Comm. Comput.*, 1999, **9**(5): 433–461.

[12] Noro M and Yokoyama K, A modular method to compute the rational univariate representation of zero-dimensional ideals, *J. Symbolic Comput.*, 1999, **28**: 243–263.

[13] Ouchi K and Keyser J, Rational univariate reduction via toric resultants, *J. Symbolic Comput.*, 2008, **43**(11): 811–844.

[14] Zeng G X and Xiao S J, Computing the rational univariate representations for zero-dimensional systems by Wu's method, *Sci. Sin. Math.*, 2010, **40**(10): 999–1016.

[15] Ma X D, Sun Y, and Wang D K, Computing polynomial univariate representations of zero-dimensional ideals by Gröbner basis, *Sci. China Math.*, 2012, **55**(6): 1293–1302.

[16] Tan C, The rational representation for solving polynomial systems, Ph.D. thesis, Jilin University, Changchun, 2009 (in Chinese).

[17] Tan C and Zhang S G, Computation of the rational representation for solutions of high-dimensional systems, *Comm. Math. Res.*, 2010, **26**(2): 119–130.

[18] Shang B X, Zhang S G, Tan C, et al., A simplified rational representation for positive-dimensional polynomial systems and SHEPWM equation solving, *Journal of Systems Science & Complexity*, 2017, **30**(6): 1470–1482.

[19] Schost É, Computing parametric geometric resolutions, *Applicable Algebra in Engineering*, Communication and Computing, 2003, **13**(5): 349–393.

[20] Safey El Din M, Yang Z H, and Zhi L H, On the complexity of computing real radicals of polynomial systems, *Proceedings of the ISSAC*'2018, New York, USA, 351–358.

[21] Kapur D, Sun Y, and Wang D K, An efficient algorithm for computing a comprehensive Gröbner system of a parametric polynomial systems, *J. Symbolic Comput.*, 2013, **49**: 27–44.

[22] Kalkbrener M, On the stability of Gröbner bases under specializations, *J. Symbolic Comput.*, 1997, **24**: 51–58.

[23] Montes A, A new algorithm for discussing Gröbner basis with parameters, *J. Symbolic Comput.*, 2002, **33**: 183–208.

[24] Suzuki A and Sato Y, A simple algorithm to compute comprehensive Gröbner bases using Gröbner bases, *Poceedings of the ISSAC*'2006, New York, 2006, 326–331.

[25] Nabeshima K, A speed-up of the algorithm for computing comprehensive Gröbner systems, *Poceedings of the ISSAC*'2007, New York, 2007, 299–306.