SCIENCE CHINA
Mathematics

• ARTICLES •

June 2012 Vol. 55 No. 6: 1293–1302
doi: 10.1007/s11425-012-4404-0

Computing polynomial univariate representations of zero-dimensional ideals by Gröbner basis

MA XiaoDong, SUN Yao* & WANG DingKang

KLMM, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190*, China*
Email: maxiaodong@amss.ac.cn, sunyao@amss.ac.cn, dwang@mmrc.iss.ac.cn

Received May 24, 2011; accepted October 12, 2011

Abstract Rational Univariate Representation (RUR) of zero-dimensional ideals is used to describe the zeros of zero-dimensional ideals and RUR has been studied extensively. In 1999, Roullier proposed an efficient algorithm to compute RUR of zero-dimensional ideals. In this paper, we will present a new algorithm to compute Polynomial Univariate Representation (PUR) of zero-dimensional ideals. The new algorithm is based on some interesting properties of Gröbner basis. The new algorithm also provides a method for testing separating elements.

Keywords RUR, PUR, zero-dimensional ideals, Gröbner basis

MSC(2010) 12Y05, 13P10, 13P15, 33F10

Citation: Ma X D, Sun Y, Wang D K. Computing polynomial univariate representations of zero-dimensional ideals by Gröbner basis. Sci China Math, 2012, 55(6): 1293–1302, doi: 10.1007/s11425-012-4404-0

1 Introduction

An efficient algorithm for computing Rational Univariate Representation (RUR) was proposed by Rouillier in 1999 [10]. RUR is often used to describe the zeros of a zero-dimensional ideal. An RUR for a zero-dimensional ideal $I \subset K[x_1, \ldots, x_n]$, where K is a field with characteristic 0, has the following form:

$$f(t) = 0, \quad x_1 = \frac{g_1(t)}{g(t)}, \quad \ldots, \quad x_n = \frac{g_n(t)}{g(t)},$$

where t is an auxiliary variable different from the variables $x_1, \ldots, x_n$, and $f, g, g_1, \ldots, g_n$ are polynomials in $K[t]$.

For an RUR, we have

$$V(I) = \left\{ \left(\frac{g_1(\alpha)}{g(\alpha)}, \ldots, \frac{g_n(\alpha)}{g(\alpha)} \right) \middle| \alpha \in V(f(t)) \right\} \subset \mathbb{C}^n,$$

where $\mathbb{C}$ is an algebraic closure of K. Moreover, the geometrical information about I can also be reflected in this RUR. For example, the multiplicity of $(\frac{g_1(\alpha)}{g(\alpha)}, \ldots, \frac{g_n(\alpha)}{g(\alpha)})$ in $V(I) \subset \mathbb{C}^n$ is exactly the same as the multiplicity of α in $V(f(t)) \subset \mathbb{C}$. Therefore, with an RUR for I, one can easily obtain all the information about the zeros of I by simply solving $f(t) = 0$.

The RUR has been studied extensively since it was proposed. Noro and Yonoyama [8] proposed a modular method for computing RUR. Ouchi and Keyser [9] presented an approach to compute RUR via

*Corresponding author

toric resultants. Zeng and Xiao [13, 14] gave an algorithm for computing RUR by using Wu's methods. Tan and Zhang developed an improved algorithm for finding separating elements of zero-dimensional ideals [12]. Cheng et al. [2] also used linear univariate representation to isolate roots of zero-dimensional ideals. Many applications of RUR have been studied in [3, 7].

Polynomial Univariate Representation (PUR) is a special version of RUR, and a PUR can be easily transformed from an RUR. A PUR for a zero-dimensional ideal $I \subset K[x_1, \ldots, x_n]$ has the following form:

$$f(t) = 0, \quad x_1 = g_1(t), \quad \ldots, \quad x_n = g_n(t),$$

where $f, g, g_1, \ldots, g_n$ are polynomials of $K[t]$. A PUR for I also contains all the information about the zeros of I. The main work of this paper is to present a new method for computing Polynomial Univariate Representations for zero-dimensional ideals via the properties of Gröbner basis. Our new algorithm will use some new interesting properties of Gröbner basis.

Separating elements play an important role in the new algorithm. For a zero-dimensional ideal I, a polynomial $r(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ is a *separating element* on $V(I) \subset \mathbb{C}^n$, if $r(\alpha) \neq r(\beta)$ for any two different elements α, β in $V(I)$.

The basic idea of the new algorithm is as follows. Let $r(x_1, \ldots, x_n)$ be a separating element on $V(I)$. An auxiliary ideal $J = \langle f_1, \ldots, f_s, r - r(x_1, \ldots, x_n)\rangle \subset K[x_1, \ldots, x_n, r]$ can be constructed, where r is an auxiliary variable different from the variables $x_1, \ldots, x_n$. Note that J is a zero-dimensional ideal in $K[x_1, \ldots, x_n, r]$. Next, consider the linear map $m_r : [g] \longrightarrow [r(x_1, \ldots, x_n)g]$ defined on the quotient ring $K[x_1, \ldots, x_n]/I$, and let $P(\lambda)$ be the characteristic polynomial of m_r. Substituting λ by r in $P(\lambda)$, we have $P(r) \in J$ [11]. The new algorithm aims to find polynomials $D_i(r) \in K[r]$ such that

$$\sqrt{J} = \langle \text{sqrfree}(P(r)), x_1 - D_1(r), \ldots, x_n - D_n(r)\rangle,$$

where sqrfree$(P(r))$ is the square-free part of the polynomial $P(r)$. With these $D_i(r)$'s, we can show that

$$P(r) = 0, \quad x_1 = D_1(r), \quad \ldots, \quad x_n = D_n(r),$$

is a Polynomial Univariate Representation for I. To find these polynomials $D_i(r) \in K[r]$, we consider the Gröbner basis for the ideal $J \cap K[x_i, r]$ respectively. The properties of Gröbner basis will help us construct $D_i(r)$ for each x_i efficiently.

In the new algorithm, a separating element on $V(I)$ should be chosen at the beginning, so we need to check whether a randomly chosen $r(x_1, \ldots, x_n)$ is a separating element. Rouillier provides a method for this purpose in [10]. Unlike Rouillier's approach, the new algorithm also uses a new technique for checking whether $r(x_1, \ldots, x_n)$ is a separating element during the procedure of constructing $D_i(r)$'s.

This paper is organized as follows. In Section 2, some basic notations are introduced first, then some facts about Gröbner basis of zero-dimensional ideals in two variables are given. The method for computing a PUR for a zero-dimensional ideals is presented in Section 3. We discuss some aspects of implementation in Section 4. An illustrative example is provided in Section 5. Conclusion remarks come in Section 6.

2 Preliminaries

Let $K[x_1, \ldots, x_n]$ be a polynomial ring, where K is a field of characteristic 0 and $x_1, \ldots, x_n$ are variables. Given a term order, for any nonzero polynomial $f \in K[x_1, \ldots, x_n]$, the notations $\text{lm}(f)$, $\text{lc}(f)$ and $\text{lpp}(f)$ denote the leading monomial, leading coefficient and leading power product of f respectively, and it follows that $\text{lm}(f) = \text{lc}(f)\text{lpp}(f)$. The degree of f w.r.t. variable x_i is denoted as $\deg_{x_i}(f)$. Similarly, we use $\text{coeff}(f, x_i^m)$ to denote the coefficient of x_i^m in f. Usually, $\text{coeff}(f, x_i^m)$ is a polynomial in $K[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$.

The ideal generated by $\{f_1, \ldots, f_m\}$ is denoted as $\langle f_1, \ldots, f_m\rangle$. Let I be an ideal in $K[x_1, \ldots, x_n]$ and f be a polynomial, $\langle f, I\rangle$ stands for the ideal generated by f and I, and $\sqrt{I}$ refers to the radical ideal of I.

For two polynomials f and g in $K[x_1,\ldots,x_n]$, the notation $\gcd(f,g)$ stands for the greatest common divisor of f and g, and $\mathrm{sqrfree}(f)$ refers to the square-free part of f. We say $f \mid g$ if f divides g; and say $f \nmid g$ otherwise.

Let $G=\{g_1,\ldots,g_s\}$ be a finite set of polynomials in the ring $K[x_1,\ldots,x_n]$ and $t=x^\alpha$ be a term in $K[x_1,\ldots,x_n]$. For any polynomial $g\in K[x_1,\ldots,x_n]$, we say g has a **t-representation** w.r.t. G, if there exist polynomials $f_1,\ldots,f_s\in K[x_1,\ldots,x_n]$ such that $g=f_1g_1+\cdots+f_sg_s$ and $t\succeq \mathrm{lpp}(f_ig_i)$ for $i=1,\ldots,s$.

The following lemma gives a criterion to determine if a set of polynomials is a Gröbner basis by using t-representations. The proof of this lemma can be found in [1].

Lemma 2.1. *Let $G=\{g_1,\ldots,g_s\}$ be a set of polynomials in $K[x_1,\ldots,x_n]$. Then the set G itself is a Gröbner basis, if and only if the S-polynomial of g_i and g_j has a t-representation w.r.t. G with $t\prec \mathrm{lcm}(\mathrm{lpp}(g_i),\mathrm{lpp}(g_j))$ for any $1\leqslant i,j\leqslant s$.*

Some facts about zero-dimensional ideals in two variables are given below. Some extended results can be found in [5].

Lemma 2.2. *Let J_1 be a zero-dimensional ideal in $K[r,x_1]$, Let $G=\{p_0,g_1,\ldots,g_t\}$ be the reduced Gröbner basis of J_1 w.r.t. the lex order with $x_1>r$. Suppose polynomials in G have the following form:*

$$\begin{aligned} &p_0\in K[r],\\ &g_1=p_1x_1^{m_1}+g_1',\\ &\quad\cdots\cdots\\ &g_t=p_tx_1^{m_t}+g_t', \end{aligned}$$

where $\deg_{x_1}(g_i')<m_i$ for $i=1,\ldots,t$ and $0<m_1<\cdots<m_t$. Note that $p_1,\ldots,p_t$ are polynomials in $K[r]$ and $p_t=1$. Then the following assertions hold.

(i) *p_i divides p_{i-1} for each $1\leqslant i\leqslant t$.*

(ii) *p_i divides g_i for each $1\leqslant i\leqslant t$. In this case, let q_i's be the polynomials such that $g_i=p_iq_i$.*

(iii) *The set $\{p_i,g_{i+1},\ldots,g_t\}$ is a Gröbner basis for the ideal $\langle p_i,J_1\rangle$ w.r.t. the lex order with $x_1>r$ for each $1\leqslant i\leqslant t$.*

(iv) *$q_1\mid q_i \bmod (p_0/p_1)$ holds for $1<i\leqslant t$, i.e., there exists h_i such that $q_i-h_iq_1\in\langle p_0/p_1\rangle$. Moreover, $q_i\mid q_j \bmod (p_{i-1}/p_i)$ holds for all $1\leqslant i<j\leqslant t$.*

(v) *For any irreducible factor a of p_0, there exists a unique integer k $(1\leqslant k\leqslant t)$ such that $a\mid p_{k-1}$ and $a\nmid p_k$, and the set $\{a,q_k\}$ is a Gröbner basis for the ideal $\langle a,J_1\rangle$ w.r.t. the lex order with $x_1>r$.*

Proof. (i) First, we prove p_1 divides p_0. It suffices to show $\gcd(p_0,p_1)=p_1$, and we will prove this by contradiction. Since G is the reduced Gröbner basis for the ideal J_1, it follows that $\deg_r(p_1)<\deg_r(p_0)$. Suppose $\gcd(p_0,p_1)=p$ and $p\neq p_1$, which implies $\deg_r(p)<\deg_r(p_1)$. Since p is the greatest common divisor of p_0 and p_1, there exist s and t in $K[r]$ such that $p=sp_0+tp_1$. Let $f:=sx_1^{m_1}p_0+tg_1=sp_0x_1^{m_1}+t(p_1x_1^{m_1}+g_1')=px_1^{m_1}+tg_1'\in J_1$. Since G is the reduced Gröber basis for J_1 w.r.t. the lex order with $x_1>r$ and $\deg_r(p)<\deg_r(p_1)$, it follows that $\mathrm{lm}(p_0)$ divides $\mathrm{lm}(f)=x_1^{m_1}\mathrm{lm}(p)$ and hence $\mathrm{lm}(p_0)\mid\mathrm{lm}(p)$, which is a contradiction with $\deg_r(p)<\deg_r(p_0)$. So we must have $\gcd(p_0,p_1)=p_1$. The cases $i=2,\ldots,t$ can be proved similarly.

(ii) We prove this assertion by the induction on i.

First, we prove the case $i=1$. Let $h_1:=(p_0/p_1)g_1-x_1^{m_1}p_0=(p_0/p_1)g_1'\in J_1$. Since G is the reduced Gröbner basis for J_1 and $\deg_{x_1}(h_1)=\deg_{x_1}(g_1')<m_1$, then p_0 divides $h_1=(p_0/p_1)g_1'$. Hence there exists a polynomial $f\in K[x_1,r]$ such that $(p_0/p_1)g_1'=p_0f$, which means $p_0g_1'=p_0p_1f$ and p_1 divides g_1'. As $g_1=p_1x_1^{m_1}+g_1'$, we have p_1 divides g_1.

Second, we assume the assertion holds for cases $i<k$, i.e., p_i divides g_i for each $1\leqslant i\leqslant k-1$. We need to show the assertion also holds for the case $i=k$. Let $h_k:=(p_{k-1}/p_k)g_k-x_1^{m_k-m_{k-1}}g_{k-1}=(p_{k-1}/p_k)g_k'-x_1^{m_k-m_{k-1}}g_{k-1}'\in J_1$. Since G is the reduced Gröbner basis for J_1 w.r.t. the lex order with $x_1>r$ and $\deg_{x_1}(h_k)<m_k$, there exist polynomials $f_0,f_1,\ldots,f_{k-1}\in K[x_1,r]$ such that $h_k=f_0p_0+f_1g_1+\cdots+f_{k-1}g_{k-1}$. Lemma 2.2 shows that p_{k-1} divides p_i for each $0\leqslant i\leqslant k-1$, and

according to the induction assumption, we have $p_{k-1} \mid g_i$ for each $1 \leqslant i \leqslant k-1$, so p_{k-1} divides $h_k = (p_{k-1}/p_k)g'_k - x_1^{m_k - m_{k-1}} g'_{k-1}$. Note that $g_{k-1} = p_{k-1}x_1^{m_{k-1}} + g'_{k-1}$ and p_{k-1} divides g'_{k-1}. Then p_{k-1} divides $(p_{k-1}/p_k)g'_k$, which means there exists a polynomial $f \in K[x_1, r]$ such that $p_{k-1}g'_k = p_{k-1}p_k f$. Thus, p_k divides g'_k and hence p_k divides g_k.

(iii) To show the set $\{p_i, g_{i+1}, \ldots, g_t\}$ is a Gröbner basis for the ideal $\langle p_i, J_1\rangle$, we only need to prove the set $\{p_i, p_0, g_1, \ldots, g_t\}$ is a Gröbner basis for the ideal $\langle p_i, J_1\rangle$ w.r.t. the lex order with $x_1 > r$. For convenience, we assume $p_i, p_0, g_1, \ldots, g_t$ are all monic polynomials. In this proof, t-presentations and Lemma 2.1 are used. Since G is a Gröbner basis for the ideal J_1, p_i divides p_0, and p_i divides g_j for $1 \leqslant j \leqslant i$, we only need to show the S-polynomial $\mathrm{spoly}(p_i, g_j)$ has a t-representation w.r.t. the set $\{p_0, p_i, g_1, \ldots, g_t\}$ where $i+1 \leqslant j \leqslant t$.

Given j where $i+1 \leqslant j \leqslant t$, the S-polynomial of p_i and g_j is

$$\mathrm{spoly}(p_i, g_j) = x_1^{m_j} p_i - (p_i/p_j)g_j + ((p_i/p_j) - \mathrm{lm}(p_i/p_j))g_j.$$

Note that p_i divides g_i. Next, consider the S-polynomial of g_i and g_j:

$$\begin{aligned}\mathrm{spoly}(g_i, g_j) &= x_1^{m_j - m_i} g_i - (p_i/p_j)g_j + ((p_i/p_j) - \mathrm{lm}(p_i/p_j))g_j \\ &= x_1^{m_j - m_i}(p_i q_i) - (p_i/p_j)g_j + ((p_i/p_j) - \mathrm{lm}(p_i/p_j))g_j \\ &= x_1^{m_j} p_i - (p_i/p_j)g_j + ((p_i/p_j) - \mathrm{lm}(p_i/p_j))g_j + x_1^{m_j - m_i} p_i(q_i - x_1^{m_i}).\end{aligned}$$

According to the above two equations, we have

$$\mathrm{spoly}(p_i, g_j) = \mathrm{spoly}(g_i, g_j) - x_1^{m_j - m_i} p_i(q_i - x_1^{m_i}).$$

Since $\mathrm{spoly}(g_i, g_j)$ can be reduced to 0 by $\{p_0, g_1, \ldots, g_t\}$ which is a Gröbner basis, then $\mathrm{spoly}(g_i, g_j)$ has a t-representation w.r.t. $\{p_0, g_1, \ldots, g_t\}$ where $t \prec \mathrm{lcm}(\mathrm{lpp}(g_i), \mathrm{lpp}(g_j)) = \mathrm{lcm}(\mathrm{lpp}(p_i), \mathrm{lpp}(g_j))$. Combined with fact $\mathrm{lpp}(x_1^{m_j - m_i} p_i(q_i - x_1^{m_i})) \prec \mathrm{lcm}(\mathrm{lpp}(p_i), \mathrm{lpp}(g_j))$, the S-polynomial $\mathrm{spoly}(p_i, g_j)$ also has a t-representation w.r.t. $\{p_i, p_0, g_1, \ldots, g_t\}$ where $t \prec \mathrm{lcm}(\mathrm{lpp}(p_i), \mathrm{lpp}(g_j))$. Then Lemma 2.1 shows the set $\{p_i, p_0, g_1, \ldots, g_t\}$ is a Gröbner basis for the ideal $\langle p_i, p_0, g_1, \ldots, g_t\rangle = \langle p_i, J_1\rangle$.

(iv) In this proof, we regard q_i and q_1 as polynomials in $K[r][x_1]$. Dividing q_i by q_1 w.r.t. x_1, we have $q_i = h_i q_1 + r_i$ where $h_i, r_i \in K[r][x_1]$, $\deg_{x_1}(r_i) < \deg_{x_1}(q_1)$ and $\mathrm{lpp}(h_i) = x_1^{m_i - m_1}$. Multiplying both sides of the equation by p_1, we have $(p_1/p_i)g_i = p_1 q_i = p_1 h_i q_1 + p_1 r_i = h_i g_1 + p_1 r_i$. It follows that $p_1 r_i = (p_1/p_i)g_i - h_i g_1 \in J_1$. Since G is a Gröbner basis for J_1 and $\deg_{x_1}(r_i) < \deg_{x_1}(q_1)$, we have p_0 divides $p_1 r_i$, and hence (p_0/p_1) divides r_i. As $q_i = h_i q_1 + r_i$, it follows $q_i - h_i q_1 \in \langle p_0/p_1\rangle$, which means $q_1 \mid q_i \mod (p_0/p_1)$.

Lemma 2.2 shows that the set $\{p_i, g_{i+1}, \ldots, g_t\}$ is a Gröbner basis for the ideal $\langle p_i, J_1\rangle$ where $1 \leqslant i \leqslant t$. Then we can prove $q_i \mid q_j \mod (p_{i-1}/p_i)$ similarly where $1 \leqslant i < j \leqslant t$.

(v) Let a be an irreducible factor of p_0, then there exists a unique integer k $(1 \leqslant k \leqslant t)$ such that $a \mid p_{k-1}$ and $a \nmid p_k$, since $p_t = 1$ and p_i divides p_{i-1}. Note that the set $\{a, q_k\}$ itself is a Gröbner basis w.r.t. the lex order with $x_1 > r$, so it suffices to show $\langle a, J_1\rangle = \langle a, q_k\rangle$.

On the one hand, it follows that $\gcd(a, p_k) = 1$ since $a \nmid p_k$, so there exist polynomials $s, t \in K[r]$ such that $sa + tp_j = 1$. Consequently, $q_k = (sa + tp_k)q_k = sq_k a + tg_k \in \langle a, J_1\rangle$, which means $\langle a, q_k\rangle \subset \langle a, J_1\rangle$.

On the other hand, to prove $\langle a, J_1\rangle \subset \langle a, q_k\rangle$, we only need to show that $p_0, g_1, \ldots, g_t \in \langle a, q_k\rangle$. Since $a \mid p_i$ for $0 \leqslant i \leqslant k-1$, we have $p_0, g_1, \ldots, g_{k-1} \in \langle a, q_k\rangle$. The equation $g_k = p_k q_k$ indicates $g_k \in \langle a, q_k\rangle$. For each i where $k < i \leqslant t$, Lemma 2.2 shows that there exists a polynomial $h_i \in K[x_1, r]$ such that $q_i - h_i q_k \in \langle p_{k-1}/p_k\rangle$. Since a divides (p_{k-1}/p_k), we have $q_i - h_i q_k \in \langle a\rangle$, and hence, $g_i = p_i q_i = p_i(q_i - h_i q_k) + p_i h_i q_k \in \langle a, q_k\rangle$. To sum up, we have $\langle a, J_1\rangle \subset \langle a, q_k\rangle$.

Finally, we have $\langle a, J_1\rangle = \langle a, q_k\rangle$ and the set $\{a, q_k\}$ is a Gröbner basis for the ideal $\langle a, J_1\rangle$ w.r.t. the lex order with $x_1 > r$. □

3 A new method for computing a PUR for a zero-dimensional ideal

In this section, we will present a new method for computing a PUR for a zero-dimensional ideal. The following is the main theorem of this paper.

Theorem 3.1. *Let I be a zero-dimensional ideal in $K[x_1,\ldots,x_n]$, $r(x_1,\ldots,x_n)$ be a separating element on $V(I)$, and $J=\langle r-r(x_1,\ldots,x_n),I\rangle$ be an ideal in $K[x_1,\ldots,x_n,r]$, where r is an auxiliary variable. Let $p_0\in K[r]$ be a polynomial such that $J\cap K[r]=\langle p_0\rangle$. If there exist polynomials $D_1,\ldots,D_n\in K[r]$ such that $\sqrt{J_i}=\langle \mathrm{sqrfree}(p_0),x_i-D_i\rangle$ where $J_i=J\cap K[x_i,r]$, then*

$$\sqrt{J}=\langle \mathrm{sqrfree}(p_0),x_1-D_1,\ldots,x_n-D_n\rangle.$$

Moreover, let $m_r:[g]\longrightarrow[r(x_1,\ldots,x_n)g]$ be a linear map defined on the quotient ring $K[x_1,\ldots,x_n]/I$, and $P(\lambda)\in K[\lambda]$ be the characteristic polynomial of m_r. Then $\mathrm{sqrfree}(p_0)=\mathrm{sqrfree}(P(r))$ *and*

$$P(r)=0,x_1=D_1(r),\ldots,x_n=D_n(r),$$

is a Polynomial Univariate Representation of I.

Proof. First, we prove $\sqrt{J}=\langle \mathrm{sqrfree}(p_0),x_1-D_1,\ldots,x_n-D_n\rangle$. On the one hand, for each i where $1\leqslant i\leqslant n$, we have $J_i\subset J$, which implies $\sqrt{J_i}\subset\sqrt{J}$. And hence, $\mathrm{sqrfree}(p_0),x_i-D_i\in\sqrt{J}$ since $\langle \mathrm{sqrfree}(p_0),x_i-D_i\rangle=\sqrt{J_i}$. So we have $\langle \mathrm{sqrfree}(p_0),x_1-D_1,\ldots,x_n-D_n\rangle\subset\sqrt{J}$. On the other hand, for any $f\in\sqrt{J}$, consider the remainder of f w.r.t. the set $\{\mathrm{sqrfree}(p_0),x_1-D_1,\ldots,x_n-D_n\}$. That is, we can represent f as $f=\mathrm{sqrfree}(p_0)f_0+(x_1-D_1)f_1+\cdots+(x_n-D_n)f_n+g$, where $f_0,f_1,\ldots,f_n\in K[x_1,\ldots,x_n,r]$, $g\in K[r]$, and $g=0$ or $\deg_r(g)<\deg_r(\mathrm{sqrfree}(p_0))$. Since $f,\mathrm{sqrfree}(p_0),x_i-D_i\in\sqrt{J}$, we have $g\in\sqrt{J}$, and hence, there exists a positive integer m such that $g^m\in J$. Note that $g^m\in J\cap K[r]=\langle p_0\rangle$, so p_0 divides g^m, and hence, $\mathrm{sqrfree}(p_0)$ divides g, which implies g must be 0. Thus, $f=\mathrm{sqrfree}(p_0)f_0+(x_1-D_1)f_1+\cdots+(x_n-D_n)f_n\in\langle \mathrm{sqrfree}(p_0),x_1-D_1,\ldots,x_n-D_n\rangle$. Since f is any polynomial in $\sqrt{J}$, then we have $\sqrt{J}\subset\langle \mathrm{sqrfree}(p_0),x_1-D_1,\ldots,x_n-D_n\rangle$.

Second we show that $P(r)=0,x_1=D_1(r),\ldots,x_n=D_n(r)$ is a PUR for I. Since $\sqrt{J}=\langle \mathrm{sqrfree}(p_0),x_1-D_1,\ldots,x_n-D_n\rangle$, then we have

$$V(J)=V(\mathrm{sqrfree}(p_0),x_1-D_1,\ldots,x_n-D_n)=\{(D_1(\alpha),\ldots,D_n(\alpha),\alpha)\mid p_0(\alpha)=0\}\subset\mathbb{C}^{n+1}.$$

By the construction of the ideal J, we have $V(I)=\{(D_1(\alpha),\ldots,D_n(\alpha))\mid p_0(\alpha)=0\}\subset\mathbb{C}^n$ and $\alpha=r(D_1(\alpha),\ldots,D_n(\alpha))$. According to the knowledge of basic linear algebra, p_0 is the minimal polynomial of the linear map m_r, so $P(r)$ and p_0 share the same irreducible factors, i.e., $\mathrm{sqrfree}(P(r))=\mathrm{sqrfree}(p_0)$. Then $V(I)=\{(D_1(\alpha),\ldots,D_n(\alpha))\mid P(\alpha)=0\}$. Since $r(x_1,\ldots,x_n)$ is a separating element on $V(I)$, the point $(D_1(\alpha),\ldots,D_n(\alpha))$ in $V(I)$ has the same multiplicity as α in $V(P(r))$. For more details of this proof, interested readers please see [10]. Besides, when K is the rational number field or real number field, $D_i(\alpha)$ is real only if α is real. So

$$P(r)=0,x_1=D_1(r),\ldots,x_n=D_n(r),$$

is a PUR for I. □

In Theorem 3.1, the polynomials $D_1,\ldots,D_n$ always exist since J is a zero-dimensional ideal. But how to compute these D_i's is the key step of computing a PUR. In the following, we will present an efficient method to obtain these D_i's. Without loss of generality, we will describe in detail how to compute D_1 such that $\sqrt{J_1}=\langle \mathrm{sqrfree}(p_0),x_1-D_1\rangle$, and the other D_i's can be obtained similarly.

By Lemma 2.2, the polynomials in G can be reformulated in the following form:

$$p_0\in K[r],\ g_1=p_1q_1,\ \ldots,\ g_t=p_tq_t,$$

where $\mathrm{lm}(q_i)=x_1^{m_i}$ and $p_i\in K[r]$ for $i=1,\ldots,t$, and $0<m_1<\cdots<m_t$.

To compute a polynomial $D_1\in K[r]$ such that $\sqrt{J_1}=\langle \mathrm{sqrfree}(p_0),x_1-D_1\rangle$ where $\langle p_0\rangle=J_1\cap K[r]$, we need the following proposition.

Proposition 3.2. *Let I be a zero-dimensional ideal in $K[x_1,\ldots,x_n]$, $r(x_1,\ldots,x_n)$ be a polynomial in $K[x_1,\ldots,x_n]$, $J=\langle r-r(x_1,\ldots,x_n),I\rangle$ be an ideal in $K[x_1,\ldots,x_n,r]$ where r is an auxiliary variable and J_1 be the ideal $J\cap K[x_1,r]$. Let $p_0\in K[r]$ be a polynomial such that $J\cap K[r]=\langle p_0\rangle$, and $G=\{p_0,g_1,\ldots,g_t\}$ be the reduced Gröbner basis for the zero-dimensional ideal J_1 w.r.t. the lex order with $x_1>r$. Suppose the polynomials in G have the following form:*

$$p_0\in K[r],\ g_1=p_1q_1,\ \ldots,\ g_t=p_tq_t,$$

where $\mathrm{lm}(q_i)=x_1^{m_i}$ *and* $p_i\in K[r]$ *for* $i=1,\ldots,t$, *and* $0<m_1<\cdots<m_t$. *Then the following assertions hold.*

(i) *Let a be an irreducible factor of p_0, and k an integer such that $a\mid p_{k-1}$ and $a\nmid p_k$. If $r(x_1,\ldots,x_n)$ is a separating element on $V(I)$, then $\{a,(x_1-d_k)^{m_k}\}$ is a Gröbner basis for the ideal $\langle a,J_1\rangle$ w.r.t. the lex order with $x_1>r$ where $d_k=-\mathrm{coeff}(q_k,x_1^{m_k-1})/m_k$.*

(ii) *If $r(x_1,\ldots,x_n)$ is a separating element on $V(I)$, then $\{\mathrm{sqrfree}(p_{i-1}/p_i),x_1-d_i\}$ is a Gröbner basis for $\sqrt{\langle\mathrm{sqrfree}(p_{i-1}/p_i),J_1\rangle}$ w.r.t. the lex order with $x_1>r$ where $d_i=-\mathrm{coeff}(q_i,x_1^{m_i-1})/m_i$ for $1\leqslant i\leqslant t$.*

(iii) *Let Q be a polynomial in $K[r]$ and Q divides* $\mathrm{sqrfree}(p_{i-1}/p_i)$. *If $r(x_1,\ldots,x_n)$ is a separating element on $V(I)$, then $\{Q,x_1-d_i\}$ is a Gröbner basis for $\sqrt{\langle Q,J_1\rangle}$ w.r.t. the lex order with $x_1>r$ where $d_i=-\mathrm{coeff}(q_i,x_1^{m_i-1})/m_i$ for $1\leqslant i\leqslant t$.*

Proof. (i) Let a be an irreducible factor of p_0, then there exists a unique integer k $(1\leqslant k\leqslant t)$ such that $a\mid p_{k-1}$ and $a\nmid p_k$. Note that the set $\{a,(x_1-d_k)^{m_k}\}$ itself is a Grönber basis w.r.t. the lex order with $x_1>r$. To prove the set $\{a,(x_1-d_k)^{m_k}\}$ is a Grönber basis for the ideal $\langle a,J_1\rangle$, we need to show that $\langle a,J_1\rangle=\langle a,(x_1-d_k)^{m_k}\rangle$. Lemma 2.2 (v) indicates $\langle a,J_1\rangle=\langle a,q_k\rangle$, so it suffices to show $\langle a,q_k\rangle=\langle a,(x_1-d_k)^{m_k}\rangle$ which is equivalent to $q_k-(x_1-d_k)^{m_k}\in\langle a\rangle$.

Since a is an irreducible polynomial in $K[r]$, the quotient ring $K[r]/\langle a\rangle$ is in fact a field. Let L be an algebraic closed field which contains $K[r]/\langle a\rangle$. Equivalent class of q_k in $(K[r]/\langle a\rangle)[x_1]$ is denoted as $\bar{q}_k$. Then $\bar{q}_k$ has a factorization in $L[x_1]$:

$$\bar{q}_k=(x_1-\bar{u}_1)^{n_1}\cdots(x_1-\bar{u}_l)^{n_l},$$

where $\bar{u}_1,\ldots,\bar{u}_l\in L$ and $n_1+\cdots+n_l=m_k$.

We claim that $\bar{u}_1=\bar{u}_2=\cdots=\bar{u}_l$. To prove this claim, we only need to show $\bar{u}_1=\bar{u}_2$, and the other equations can be proved similarly. Assume $\bar{u}_1\neq\bar{u}_2$. We denote the equivalent class of r in $K[r]/\langle a\rangle$ as $\bar{r}$, then $a(\bar{r})=0\in L$.

First, we show that $(\bar{u}_1,\bar{r})\in V(J_1)\subset L^2$, where $J_1=\langle p_0,g_1,\ldots,g_t\rangle$. Since a is a factor of p_0, we have $p_0(\bar{r})=0$. As $g_i=p_iq_i$ and a divides p_i for $1\leqslant i\leqslant k-1$, then $g_i(\bar{u}_1,\bar{r})=0$. We also have $g_k(\bar{u}_1,\bar{r})=p_k(\bar{r})q_k(\bar{u}_1,\bar{r})=0$, since $x_1-\bar{u}_1$ is a factor of $\bar{q}_k$. For each i where $k<i\leqslant t$, Lemma 2.2 (iv) shows that there exists a polynomial $h_i\in K[x_1,r]$ such that $q_i-h_iq_k\in\langle p_{k-1}/p_k\rangle$, so we have $q_i-h_iq_k\in\langle a\rangle$ due to the fact $a\mid(p_{k-1}/p_k)$. Thus, $g_i(\bar{u}_1,\bar{r})=h_i(\bar{u}_1,\bar{r})q_k(\bar{u}_1,\bar{r})=0$. To sum up, we have $(\bar{u}_1,\bar{r})\in V(J_1)$.

Second, we can prove $(\bar{u}_2,\bar{r})\in V(J_1)$ similarly.

Since J is a zero-dimensional ideal, $(\bar{u}_1,\bar{r})$ and $(\bar{u}_2,\bar{r})$ can be extended to the points in $V(J)\subset L^{n+1}$ respectively. Let $(\bar{u}_1,\bar{b}_2,\ldots,\bar{b}_n,\bar{r}),(\bar{u}_2,\bar{c}_2,\ldots,\bar{c}_n,\bar{r})\in V(J)$ be the points extended from $(\bar{u}_1,\bar{r})$ and $(\bar{u}_2,\bar{r})$. Then we have $(\bar{u}_1,\bar{b}_2,\ldots,\bar{b}_n),(\bar{u}_2,\bar{c}_2,\ldots,\bar{c}_n)\in V(I)\subset L^n$ and $\bar{r}=r(\bar{u}_1,\bar{b}_2,\ldots,\bar{b}_n)=r(\bar{u}_2,\bar{c}_2,\ldots,\bar{c}_n)$ by the definition of J. But this contradicts with that $r(x_1,\ldots,x_n)$ is a separating element on $V(I)$. So we must have $\bar{u}_1=\bar{u}_2$, and the claim is proved.

Next, let $\bar{u}:=\bar{u}_1=\cdots=\bar{u}_l$, then $\bar{q}_k$ can be expanded as

$$\bar{q}_k=(x_1-\bar{u})^{m_k}=x_1^{m_k}-m_k\bar{u}x_1^{m_k-1}+\cdots+(-1)^{m_k}\bar{u}^{m_k}.$$

Let $\bar{d}_k$ be the equivalent class of d_k in $K[r]/\langle a\rangle$, then we have $\bar{u}=\bar{d}_k\in K[r]/\langle a\rangle$, and hence, $\bar{q}_k=(x_1-\bar{d}_k)^{m_k}$, which implies $q_k-(x_1-d_k)^{m_k}\in\langle a\rangle$.

(ii) We will only give the proof for the case $i = 1$, the proofs are the same for the others. Since the set $\{\text{sqrfree}(p_0/p_1), x_1 - d_1\}$ itself is a Gröbner basis w.r.t. the lex order with $x_1 > r$, it suffices to show that $\sqrt{\langle \text{sqrfree}(p_0/p_1), J_1\rangle} = \langle \text{sqrfree}(p_0/p_1), x_1 - d_1\rangle$. Suppose $\text{sqrfree}(p_0/p_1) = a_1 \dots a_s$, where $a_1, \dots, a_s$ are irreducible polynomials in $K[r]$.

First, we show that the following equation holds for each j where $1 \leqslant j \leqslant s$:

$$\sqrt{\langle a_j, J_1\rangle} = \langle a_j, x - d_1\rangle.$$

For each factor a_j, Proposition 3.2 (i) indicates that there exists a unique integer k $(1 \leqslant k \leqslant t)$ such that $a_j \mid p_{k-1}$ and $a_j \nmid p_k$, and the set $\{a_j, (x_1 - d_k)^{m_k}\}$ is a Gröbner basis for the ideal $\langle a_j, J_1\rangle$ w.r.t. the lex order with $x_1 > r$, where $d_k = -\text{coeff}(q_k, x_1^{m_k-1})/m_k$ and $q_k - (x_1 - d_k)^{m_k} \in \langle a_j\rangle$. Therefore $\langle a_j, J_1\rangle = \langle a_j, (x_1 - d_k)^{m_k}\rangle$, and $\sqrt{\langle a_j, J_1\rangle} = \langle a_j, x - d_k\rangle$ follows easily. By Lemma 2.2 (iv), we have $q_k - h_k q_1 \in \langle p_0/p_1\rangle \subset \langle a_j\rangle$, where $h_k \in K[x_1, r]$. As proved in Proposition 3.2 (i), $q_k - (x_1 - d_k)^{m_k} \in \langle a_j\rangle$ holds, so it follows that $(x_1 - d_k)^{m_k} - h_k q_1 \in \langle a_j\rangle$, which means $q_1 \mid (x_1 - d_k)^{m_k} \bmod a_j$. Since $(K[r]/\langle a_j\rangle)[x_1]$ is a unique factorization domain, we have $q_1 - (x_1 - d_k)^{m_1} \in \langle a_j\rangle$ where $m_1 = \deg_{x_1}(q_1)$. Note that $d_1 = -\text{coeff}(q_1, x_1^{m_1-1})/m_1$, so we have $d_1 - d_k \in \langle a_j\rangle$, and it follows that $\sqrt{\langle a_j, J_1\rangle} = \langle a_j, x_1 - d_k\rangle = \langle a_j, x_1 - d_1\rangle$.

Next, we show that

$$\sqrt{\langle a_1 \cdots a_s, J_1\rangle} = \sqrt{\langle a_1, J_1\rangle} \cap \cdots \cap \sqrt{\langle a_s, J_1\rangle}.$$

The inclusion " $\subset$ " holds obviously, and it suffices to show the inclusion " $\supset$ " also holds. Let h be a polynomial in $\sqrt{\langle a_1, J_1\rangle} \cap \cdots \cap \sqrt{\langle a_s, J_1\rangle}$, then $h \in \sqrt{\langle a_i, J_1\rangle}$ for each $1 \leqslant i \leqslant s$. Hence there exists a positive integer n_i such that $h^{n_i} \in \langle a_i, J_1\rangle$, and it follows that $h^{n_1+\cdots+n_s} \in \langle a_1 \cdots a_s, J_1\rangle$, which means $h \in \sqrt{\langle a_1 \cdots a_s, J_1\rangle}$.

Finally, since $\langle a_1 \cdots a_s, x - d_1\rangle = \langle a_1, x - d_1\rangle \cap \cdots \cap \langle a_s, x - d_1\rangle$, we have

$$\begin{aligned}\sqrt{\langle a_1 \cdots a_s, J_1\rangle} &= \sqrt{\langle a_1, J_1\rangle} \cap \cdots \cap \sqrt{\langle a_s, J_1\rangle} \\ &= \langle a_1, x - d_1\rangle \cap \cdots \cap \langle a_s, x - d_1\rangle \\ &= \langle a_1 \cdots a_s, x - d_1\rangle,\end{aligned}$$

which means $\sqrt{\langle \text{sqrfree}(p_0/p_1), J_1\rangle} = \langle \text{sqrfree}(p_0/p_1), x_1 - d_1\rangle$.

(iii) Since Q divides $\text{sqrfree}(p_{i-1}/p_i)$, the conclusion is direct from Proposition 3.2 (ii). □

In Theorem 3.1 and the above proposition, $r(x_1, \dots, x_n)$ is always needed to be a separating element on $V(I)$. The following remark is used to check whether a polynomial is a separating element on $V(I)$.

Remark 3.3. With notations defined above, let $d_i = -\text{coeff}(q_i, x_1^{m_i-1})/m_i$ for each $1 \leqslant i \leqslant t$. If there exists an integer k such that $\text{sqrfree}(p_{k-1}/p_k)$ does not divide the polynomial $q_k - (x_1 - d_k)^{m_k}$, then the polynomial $r(x_1, \dots, x_n)$ is not a separating element on $V(I)$.

The method based on the above remark for checking separating element can be integrated in the main process of computing D_i's and we do not need to test separating element before the computations of D_i's. Generally, the testing of separating element is usually redundant, since the probability that a randomly chosen polynomial is a separating element is 1.

Proposition 3.2 provides *a specific method* for computing the polynomial D_1 such that $\sqrt{J_1} = \langle \text{sqrfree}(p_0), x_1 - D_1\rangle$ where $\langle p_0\rangle = J_1 \cap K[r]$.

The basic ideal is that let $Q_1, \dots, Q_s$ be polynomials in $K[r]$ such that $\text{sqrfree}(p_0) = Q_1 \cdots Q_s$. We can obtain $d_1, \dots, d_s \in K[r]$ easily such that $\langle Q_i, x_1 - d_i\rangle = \sqrt{\langle Q_i, J_1\rangle}$. Note that $\gcd(Q_i, Q_j) = 1$ if $i \neq j$. Next, a polynomial D_1 such that $D_1 \equiv d_i \bmod Q_i$ can be constructed by Chinese Remainder Theorem. Then it is evident that $\sqrt{J_1} = \langle \text{sqrfree}(p_0), x_1 - D_1\rangle$. Specifically, the above Q_i's and d_i's can be obtained in the following way.

First, let $Q_1 := \text{sqrfree}(p_0/p_1)$ and $d_1 := -\text{coeff}(q_1, x_1^{m_1-1})/m_1$. Clearly, $Q_1 \neq 1$. If Q_1 does not divide $q_1 - (x_1 - d_1)^{m_1}$, then $r(x_1, \dots, x_n)$ is not a separating element by Remark 3.3, which means we have to choose another $r(x_1, \dots, x_n)$ and start from the beginning again; otherwise, we will have

$\langle Q_1, x_1 - d_1\rangle = \sqrt{\langle Q_1, J_1\rangle}$ by Proposition 3.2. Let $Q := \text{sqrfree}(p_0)/Q_1$ which contains the remaining factors of $\text{sqrfree}(p_0)$. If $Q = 1$, then all factors of $\text{sqrfree}(p_0)$ have been considered and the procedure for finding Q_i's and d_i's is over; otherwise, we should go to the next step.

Second, let k be the smallest integer such that $\gcd(Q, \text{sqrfree}(p_{k-1}/p_k)) \neq 1$. Then denote $Q_2 := \gcd(Q, \text{sqrfree}(p_{k-1}/p_k))$ and $d_2 := -\text{coeff}(q_k, x_1^{m_k-1})/m_k$. If Q_2 does not divide $q_k - (x_1 - d_2)^{m_k}$, we choose another $r(x_1, \ldots, x_n)$ and repeat all the procedures from the beginning; otherwise, we have $\langle Q_2, x_1 - d_2\rangle = \sqrt{\langle Q_2, J_1\rangle}$. Now we update Q by $Q := Q/Q_2$. If $Q = 1$, then the procedure is over; otherwise, we find another k such that $\gcd(Q, \text{sqrfree}(p_{k-1}/p_k)) \neq 1$, and repeat the above process.

The procedure must terminate in finite steps, since Q becomes its proper factor after each update.

Let D_1 be the polynomial constructed by Chinese Remainder Theorem such that $D_1 \equiv d_i \bmod Q_i$ for $i = 1, \ldots, s$ where Q_i and d_i are obtained by the above method. Clearly, Q_i divides $\text{sqrfree}(p_0)$, $\gcd(Q_i, Q_j) = 1$ for $i \neq j$, and $\text{sqrfree}(p_0) = Q_1 \cdots Q_s$ since for any irreducible factor a of $\text{sqrfree}(p_0)$, there always exists an integer k such that $a \mid p_{k-1}$ and $a \nmid p_k$, which means $a \in \text{sqrfree}(p_{k-1}/p_k)$. Therefore, we have $\langle Q_i, x_1 - d_i\rangle = \langle Q_i, x_1 - D_1\rangle = \sqrt{\langle Q_i, J_1\rangle}$, and hence $\langle \text{sqrfree}(p_0), x_1 - D_1\rangle = \sqrt{\langle \text{sqrfree}(p_0), J_1\rangle} = \sqrt{J_1}$.

Remark 3.4. A natural method for computing a PUR for zero-dimensional ideal is based on the following fact: $\langle \text{sqrfree}(p_{i-1})/\text{sqrfree}(p_i), J_1\rangle = \langle \text{sqrfree}(p_{i-1})/\text{sqrfree}(p_i), (x_1 - d_i)^{m_i}\rangle$ for $1 \leqslant i \leqslant n$ where $d_i = -\text{coeff}(q_i, x_1^{m_i-1})/m_i$. This approach is similar to solving systems of equations from the lex order Gröbner basis. However, this method is less efficient than the new technique presented in this paper, since $\text{sqrfree}(p_{i-1}/p_i)$ usually contains more factors than $\text{sqrfree}(p_{i-1})/\text{sqrfree}(p_i)$.

4 Some details in implementation

Let $I = \langle f_1, \ldots, f_s\rangle$ be a zero-dimensional ideal in $K[x_1, \ldots, x_n]$, G be a Gröbner basis for I, and $r(x_1, \ldots, x_n)$ be a random polynomial in $K[x_1, \ldots, x_n]$. Then the set $G \cup \{r - r(x_1, \ldots, x_n)\}$ is a Gröbner basis for $J = \langle f_1, \ldots, f_s, r - r(x_1, \ldots, x_n)\rangle \subset K[x_1, \ldots, x_n, r]$ w.r.t. a block order with $r > \{x_1, \ldots, x_n\}$, where r is an auxiliary variable.

If G is a Gröbner basis for the ideal J, then the Gröbner basis for the ideal $J \cap K[x_i, r]$ w.r.t. the lex order with $x_i > r$ can be obtained by the FGLM algorithm [4] or MMM algorithm [6] within polynomial time.

The probability that a random polynomial $r(x_1, \ldots, x_n)$ is a separating element on $V(I)$ is 1. This has been studied by many researchers, and we also give a proof for the following proposition in [11].

Proposition 4.1. *Let K be a field of characteristic 0 and I be a zero-dimensional ideal in $K[x_1, \ldots, x_n]$, then the probability that a random polynomial in $K[x_1, \ldots, x_n]$ is a separating element on $V(I)$ is 1. If the chosen polynomial is not a separating element, then a separating element can be obtained within finite steps.*

For the sake of efficiency, the polynomial $r(x_1, \ldots, x_n)$ is usually selected as a linear form of $\{x_1, \ldots, x_n\}$ with coefficients in the field of rational numbers, in practical implementation.

5 An example

In this section, we use an illustrative example to show how the new method works.

Example 5.1. Let $I = \langle x^2(x-1), (y-2)^2(y+1)\rangle$ be a zero-dimensional ideal of $\mathbb{Q}[x, y]$ where $\mathbb{Q}$ is the rational number field. The set $G = \{x^2(x-1), (y-2)^2(y+1)\}$ is a Gröbner basis for I w.r.t. the lex order with $x > y$.

Next, we use the new method to compute a PUR for I.

Let $r(x, y) := x + y$, then the set $\{x^2(x-1), (y-2)^2(y+1), r - x - y\}$ is a Gröbner basis for the ideal $J = \langle x^2(x-1), (y-2)^2(y+1), r - x - y\rangle$ w.r.t. the lex order with $r > x > y$.

Consider the linear map $m_r : [g] \longrightarrow [r(x,y)g]$ defined on the quotient ring $\mathbb{Q}[x,y]/I$, we can compute the characteristic polynomial $P(\lambda)$ of m_r. Substituting λ by r, we get

$$P(r) = r(r+1)^2(r-3)^2(r-2)^4.$$

First, we compute $D_x \in \mathbb{Q}[r]$ such that $\langle \text{sqrfree}(P(r)), x - D_x\rangle = \sqrt{\langle \text{sqrfree}(P(r)), J_x\rangle}$ where $J_x = J \cap \mathbb{Q}[x,r]$.

By using the MMM algorithm, we get the reduced Gröbner basis G_x for the ideal $J \cap K[x,r]$ w.r.t. the lex order with $x > r$. The set G_x consists of the following polynomials:

$$\begin{aligned}
p_0 &= r(r+1)^2(r-3)^2(r-2)^3,\\
g_1 &= (r-2)\left(x + \frac{1}{96}r^6 + \frac{1}{96}r^5 - \frac{25}{96}r^4 + \frac{11}{96}r^3 + r^2 - \frac{3}{8}r - 1\right),\\
g_2 &= x^2 + \frac{3}{32}r^7 - \frac{23}{32}r^6 + \frac{51}{32}r^5 + \frac{3}{32}r^4 - \frac{59}{16}r^3 + \frac{15}{8}r^2 + \frac{9}{4}r - 1.
\end{aligned}$$

Here $p_1 = r-2$, $p_2 = 1$, $q_1 = g_1/p_1$, $q_2 = g_2/p_2$, $m_1 = 1$ and $m_2 = 2$. Note that $\text{sqrfree}(P(r)) = \text{sqrfree}(p_0)$.

Let $Q_1 := \text{sqrfree}(p_0/p_1) = r(r+1)(r-2)(r-3)$ and $d_1 := -\text{coeff}(q_1, 1) = -\frac{1}{96}r^6 - \frac{1}{96}r^5 + \frac{25}{96}r^4 - \frac{11}{96}r^3 - r^2 + \frac{3}{8}r + 1$. Note that Q_1 divides $q_1 - (x - d_1)$. Then we have $\langle Q_1, x - d_1\rangle = \sqrt{\langle Q_1, J_x\rangle}$. Since $Q = \text{sqrfree}(p_0)/Q_1 = 1$, the polynomial d_1 is the desired D_x such that $\langle \text{sqrfree}(P(r)), x - D_x\rangle = \sqrt{\langle \text{sqrfree}(P(r)), J_x\rangle}$. Note that we can simplify d_1 via reducing d_1 by $\text{sqrfree}(p_0)$. At last, we get $D_x = \frac{1}{4}r^3 - \frac{3}{4}r^2 + 1$.

Similarly, we can compute $D_y = -\frac{1}{4}r^3 + \frac{3}{4}r^2 + r - 1$ such that

$$\langle \text{sqrfree}(P(r)), y - D_y\rangle = \sqrt{\langle \text{sqrfree}(P(r)), J_y\rangle}$$

where $J_y = J \cap \mathbb{Q}[y,r]$.

Finally, we obtain a Polynomial Univariate Representation of I:

$$P(r) = r(r+1)^2(r-3)^2(r-2)^4 = 0, \quad x = D_x = \frac{1}{4}r^3 - \frac{3}{4}r^2 + 1, \quad y = D_y = -\frac{1}{4}r^3 + \frac{3}{4}r^2 + r - 1.$$

In the above example, the polynomial $r(x,y) = x + y$ is a separating element on $V(I)$. However, what if $r(x,y)$ is not a separating element? For example, let $r(x,y) := 3x - y$.

The set $\{x^2(x-1), (y-2)^2(y+1), r - 3x + y\}$ is a Gröbner basis for the ideal $J = \langle x^2(x-1), (y-2)^2(y+1), r - 3x + y\rangle$ w.r.t. the lex order with $r > x > y$. The corresponding characteristic polynomial of m_r is $P(\lambda)$. By substituting λ with r, we get

$$P(r) = (r-4)(r+2)^4(r-1)^4.$$

Next, we compute $D_x \in \mathbb{Q}[r]$ such that $\langle \text{sqrfree}(P(r)), x - D_x\rangle = \sqrt{\langle \text{sqrfree}(P(r)), J_x\rangle}$ where $J_x = J \cap \mathbb{Q}[x,r]$. By using the MMM algorithm, the reduced Gröbner basis G_x for the ideal $J \cap K[x,r]$ w.r.t. the lex order with $x > r$, consists of:

$$\begin{aligned}
p_0 &= (r-4)(r-1)^2(r+2)^3,\\
g_1 &= (r+2)(r-1)^2\left(x - \frac{1}{6}r - \frac{1}{3}\right),\\
g_2 &= x^2 - \left(\frac{1}{3}r + \frac{2}{3}\right)x - \frac{1}{216}r^5 + \frac{5}{72}r^3 + \frac{11}{108}r^2 - \frac{1}{18}r - \frac{1}{9}.
\end{aligned}$$

Here $p_1 = (r+2)(r-1)^2, p_2 = 1$, $q_1 = g_1/p_1$, $q_2 = g_2/p_2$, $m_1 = 1$ and $m_2 = 2$.

Let $Q_1 := \text{sqrfree}(p_0/p_1) = (r-4)(r+2)$ and $d_1 := -\text{coeff}(q_1, 1) = \frac{1}{6}r + \frac{1}{3}$. Note that Q_1 divides $q_1 - (x - d_1)$, so we have $\langle Q_1, x - d_1\rangle = \sqrt{\langle Q_1, J_x\rangle}$. Since $Q = \text{sqrfree}(p_0)/Q_1 = r - 1 \neq 1$, we go to the next step.

Let $Q_2 := \gcd(Q, \text{sqrfree}(p_1/p_2)) = r - 1$ and $d_2 := -\text{coeff}(q_2, x)/2 = \frac{1}{6}r + \frac{1}{3}$. However, Q_2 *does not divide* $q_2 - (x - d_2)^2$, which means $r(x, y) = 3x - y$ is not a separating element on $V(I)$. In this case, we have to choose another $r(x, y)$ and start from the beginning again. Proposition 4.1 shows that by using a specific method for choosing $r(x, y)$, we can get a separating element within finite steps.

6 Conclusions and future works

A new method for computing a Polynomial Univariate Representation for a zero-dimensional ideal is presented in this paper. This method is based on some interesting properties of Gröbner basis of zero-dimensional ideals. If both the Gröbner basis of the zero-dimensional ideal and separating element are given, then the complexity of our method is of polynomial time. The new method also includes a new technique for testing separating elements. In our algorithm, we choose random polynomials as candidates of separating elements. Since any random polynomial is a separating element with probability 1, our method is quite efficient.

According to our experimental data, we usually have $\text{sqrfree}(p_0/p_1) = \text{sqrfree}(p_0)$ in practical examples, which means $d_1 = -\text{coeff}(q_1, x_1^{m_1})/m_1$ is just the polynomial D_1 such that $\langle \text{sqrfree}(p_0), x_1 - D_1 \rangle = \sqrt{\langle \text{sqrfree}(p_0), J_1 \rangle}$ where $J_1 = J \cap K[x_1, r]$. In this case, a PUR for I can be obtained quite efficiently. We guess the probability that $\text{sqrfree}(p_0/p_1) = \text{sqrfree}(p_0)$ happens is 1, and we may prove this in the future.

Some properties of Gröbner bases for zero-dimensional ideals in two variables are given in Lemma 2.2. It seems that these properties remain true even if the number of variables is bigger than two. We believe these properties can be further studied, and this will be included in our future work.

Acknowledgements This work was partially supported by National Key Basic Research Project of China (Grant No. 2011CB302400) and National Natural Science Foundation of China (Grant Nos. 10971217, 60821002/F02). The authors cordially thank Professor Ziming Li for his helpful suggestions and we also thank the anonymous referees for their careful reading and helpful comments.

References

1 Becker T, Weispfenning V. Gröbner Basis: A Computational Approach to Commutative Algebra. New York: Springer-Verlag, 1993
2 Cheng J S, Gao X S, Guo L L. Root isolation of zero-dimensional polynomial systems with linear univariate representation. J Symb Comp, 2012, 47: 843–8585
3 Emiris I Z, Pan V Y. Improved algorithms for computing determinants and resultants. J Complexity, 2005, 21: 43–71
4 Faugère J C, Gianni P, Lazard D, et al. Efficient computation of zero-dimensional Gröbner bases by change of ordering. J Symb Comp, 1993, 16: 329–344
5 Lazard D. Ideal bases and primary decomposition: case of two variables. J Symb Comp, 1985, 1: 261–270
6 Marinari M G, Möller H M, Mora T. Gröbner bases of ideals defined by functionals with an application to ideals of projective points. Appl Algebra Engrg Comm Comp, 1993, 4: 103–145
7 Mourrain B, Técourt J P, Teillaud M. On the computation of an arrangement of quadrics in 3D. Comp Geom, 2005, 30: 145–164
8 Noro M, Yokoyama K. A modular method to compute the rational univariate representation of zero-dimensional ideals. J Symb Comp, 1999, 28: 243–263
9 Ouchi K, Keyser J. Rational univariate reduction via toric resultants. J Symb Comp, 2008, 43: 811–844
10 Rouillier F. Solving zero-dimensional systems through the rational univariate representation. Appl Algebra Engrg Comm Comp, 1999, 9: 33–461
11 Sun Y, Wang D K. An efficient algorithm for factoring polynomials over algebraic extension field. Arxiv:0907.2300v2, 2009
12 Tan C, Zhang S G. Separating element computation for the rational univariate representation with short coefficients in zero-dimensional algebraic varieties. J Jilin Univ Sci, 2009, 47: 174–178
13 Xiao S J, Zeng G X. Algorithms for computing the global infimum and minimum of a polynomial function. Sci China Math, 2012, 55: 881–891
14 Zeng G X, Xiao S J. Computing the rational univariate representations for zero-dimensional systems by Wu's method (in Chinese). Sci Sin Math, 2010, 40: 999–1016