Root Isolation of Zero-dimensional Polynomial Systems with Linear Univariate Representation[1]

Jin-San Cheng, Xiao-Shan Gao, Leilei Guo

KLMM, Institute of Systems Science, AMSS, Chinese Academy of Sciences
Email: xgao@mmrc.iss.ac.cn,jcheng@amss.ac.cn

Abstract

In this paper, a linear univariate representation for the roots of a zero-dimensional polynomial equation system is presented, where the complex roots of the polynomial system are represented as linear combinations of the roots of several univariate polynomial equations. The main advantage of this representation is that the precision of the roots of the system can be easily controlled. In fact, based on the linear univariate representation, we can give the exact precisions needed for isolating the roots of the univariate equations in order to obtain the roots of the polynomial system to a given precision. As a consequence, a root isolating algorithm for a zero-dimensional polynomial equation system can be easily derived from its linear univariate representation.

Key words: Zero-dimensional polynomial system, linear univariate representation, local generic position, root isolating

1. Introduction

Solving polynomial equation systems is a basic problem in the field of computational science and has important engineering applications. In most cases, we consider zero-dimensional polynomial systems. We will discuss how to solve this kind of systems in this paper. In particular, we will consider how to isolate the complex roots for such a system.

One of the basic methods to solve polynomial equation systems is based on the concept of separating elements, which can be traced back to Kronecker (1882) and has been studied extensively in the past twenty years: Alonso et al (1996); Canny (1988); Cheng et al (2009); Gao and Chou (1999); Gianni and Mora (1989); Giusti and Heintz (1991); Giusti et al (2001); Keyser et al (2005); Kobayashi, Moritsugu and Hogan (1988); Kobayashi, Fujise and Furukawa (1988); Lakshman and Lazard (1991); Renegar (1992); Rouillier (1999); van der Waerden (1950); Yokoyama et al (1989). The idea of the method is to introduce a new variable $t = \sum_i c_i x_i$ which is a linear combination of the variables to be solved such

[1] The work is partially supported by a NKBRPC (2011CB302400) and China-France cooperation project EXACTA. The first author is partially supported by NSFC Grant 11001258.

that $t = \sum_i c_i x_i$ takes different values when evaluated at different complex roots of the polynomial equation system $0 = \mathcal{P} \subset \mathbb{Q}[x_1, \ldots, x_n]$, where $c_i' s$ are rational numbers and $\mathbb{Q}$ is the field of rational numbers. In such a case, we say that t is a **separating element** for $\mathcal{P} = 0$. If $t = \sum_i c_i x_i$ is a separating element for $\mathcal{P} = 0$, the roots of $\mathcal{P} = 0$ have the following rational univariate representation (RUR):

$$f(t) = 0, x_i = R_i(t), i = 1, ..., n,$$

where $f \in \mathbb{Q}[t]$ and $R_i(t)$ are rational functions in t. As a consequence, solving multi-variate polynomial systems is reduced to solving a univariate equation $f(t) = 0$ and to substituting the roots of $f(t) = 0$ into rational functions $R_i(t)$. Along this line, better complexity bounds and effective software packages for solving polynomial equations such as the Maple package RootFinding by Rouillier (1999) and the Magma package Kronecker by Giusti et al (2001) are given.

The above approaches still have the following problem: for an isolating interval $[a, b]$ of a real root α of $f(t) = 0$, to determine the isolating interval of $x_i = R_i(\alpha)$ under a given precision is not a trivial task. In this paper, we propose a new representation for the roots of a polynomial system which will remedy this drawback.

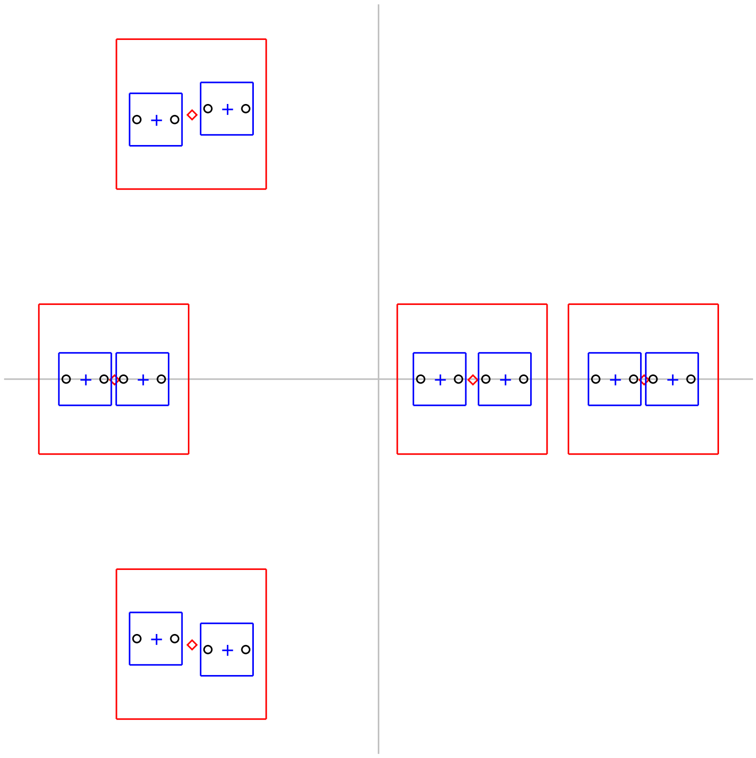

Fig. 1. The distribution of the roots of $T_i(x) = 0 (i = 1, 2, 3)$ in the complex plane. The red diamonds (blue crosses, black circles) are roots of $T_1(x) = 0$ ($T_2(x) = 0$, $T_3(x) = 0$) and red (blue) boxes are neighborhoods for the red diamonds (blue crosses).

In the ISSAC paper Cheng et al (2009), based on ideas similar to separating elements, a local generic position method is introduced to solve bivariate polynomial systems and experimental results show that the method is quite efficient for solving polynomial systems with multiple roots. In this paper, we extend the local generic position method to solve general zero-dimensional polynomial systems in complex field. We introduce the concept of local separating elements for a zero-dimensional polynomial system.

Definition 1. A linear polynomial $t = \sum_i c_i x_i$ for a polynomial equation system $\mathcal{P} = 0$ is called **a local separating element** for $\mathcal{P} = 0$ if it satisfies the following conditions.

(1) $t_1 = x_1$ is defined to be a local separating element of $\mathcal{P}_1$.

(2) $t_k = t_{k-1} + c_k\, x_k$ is a separating element of

$$\mathcal{P}_k = (\mathcal{P}) \cap \mathbb{Q}[x_1, \ldots, x_k]$$

for $k = 2, \ldots, n$, and the roots of $\mathcal{P}_k = 0$ have a one-to-one correspondence with the roots of a univariate equation $T_k(t_k) = 0$.

(3) for $k = 1, \ldots, n-1$, for a root $\xi = (\xi_1, \ldots, \xi_k)$ of $\mathcal{P}_k = 0$ represented by a root α of $T_k(t_k) = 0$, all the roots η_j's of $T_{k+1}(t_{k+1}) = 0$ corresponding to the roots of $\mathcal{P}_{k+1}(\xi, x_{i+1}) = 0$, say $\xi_j = (\xi, \xi_{k+1,j})$, "lifted" from ξ are projected into a fixed square neighborhood of α, where

$$\eta_j = \sum_{m=1}^{k} c_m\, \xi_m + c_{k+1}\xi_{k+1,j}.$$

This "local" property is illustrated in Figure 1. In fact, it is a special kind of separating elements method which originates from Kronecker. We prove that if $t_n = \sum_{i=1}^{n} c_i x_i$ is a local separating element for $\mathcal{P}$, then the roots of $\mathcal{P} = 0$ can be be represented as special linear combinations of the roots of univariate equations $T_k(t_k) = 0$:

$$\{(\alpha_1, \frac{\alpha_2 - \alpha_1}{s_1}, \ldots, \frac{\alpha_n - \alpha_{n-1}}{s_1 \cdots s_{n-1}}) \,|\, T_k(\alpha_k) = 0, k = 1, \ldots, n\},$$

where s_j are certain positive rational numbers and α_{j+1} matching α_j are in certain square neighborhood of α_j to be defined in Section 2. Such a representation is called a **linear univariate representation** (LUR for short) of the polynomial system.

The main advantage of the LUR is that the precision of the roots can be easily controlled. For RUR, computing solutions with a given precision is not a trivial task as we mentioned before. It is not easy to know with which precision to isolate the roots of $f(t) = 0$ is enough in order for the roots of the system $x_i = R_i(t)$ to satisfy a given precision. For LUR, precision control becomes very easy. We can give an explicit formula for the precision of the roots of $T_i(t_i) = 0$ in order to obtain the roots of the system with a given precision. So we can obtain the solutions of the system by refining the roots of $T_i(t_i) = 0$ at most once. The reason why we can achieve the given precision easily is that LUR method need only to evaluate the roots to a linear polynomial representation but RUR method to a rational non-linear polynomial representation. Another advantage of LUR is that for a fixed root $(\xi_1, \ldots, \xi_k)$ of $\mathcal{P}_k = 0$, we can easily know the roots of $\mathcal{P}_m = 0 (k + 1 \leq m \leq n)$ on the fiber of $(x_1, \ldots, x_k) = (\xi_1, \ldots, \xi_k)$. This property is useful especially for determining the topology of algebraic curves and surfaces, for example, Berbericha et al (2010); Cheng et al (2005).

We propose an algorithm to compute an LUR for a zero-dimensional polynomial system. The key ingredients of the algorithm are to estimate the root bounds of $\mathcal{P} = 0$ and to estimate the separation bounds for the roots of $\mathcal{P}_{k+1} = 0$ lifted from a root of $\mathcal{P}_k = 0$. The existing bounds for these values are not computable in practice (Emiris et al (2010); Yap, pp.341 (2000)). We adopt a computational approach to estimate such bounds in order to obtain tight bound values. For the root bounds of $\mathcal{P}=0$, we use Gröbner basis computation to obtain the generating polynomial of the principal ideal $(\mathcal{P})\cap\mathbb{Q}[x_i]$ and use this polynomial to estimate the root bound for the x_i coordinates of the roots of $\mathcal{P}=0$. The separation bounds for $\mathcal{P}_k=0$ are obtained from the isolating boxes for the roots of the $T_k(t_k)=0$. These bounds in turn will be used to compute the isolating boxes for the roots of $\mathcal{P}_{k+1}=0$. Hence, the algorithm to compute an LUR also gives a set of isolating boxes for the roots of $\mathcal{P}=0$.

Though we need to isolate n univariate equations comparing to RUR method, we only need to isolate the roots of $T_{i+1}(t_{i+1})=0$ in a fixed neighborhood of each root of $T_i(t_i)=0$. But usually, the roots of $T_i(t_i)=0$ will become dense and dense and the bitsize of $T_i(t_i)=0$ will become large and large when i increases.

The paper is organized as follows. In Section 2, we give the definition of LUR and the main result of the paper. In Section 3, we present an algorithm to compute an LUR of a zero-dimensional polynomial system as well as a set of isolating boxes of the roots of the equation system. In Section 4, we provide some illustrative examples. We conclude the paper in Section 5.

2. Linear univariate representation

In this section, we will define LUR and prove its main properties. Let

$$\mathcal{P}=\{f_1(x_1,\ldots,x_n),\ldots,f_s(x_1,\ldots,x_n)\}$$

be a zero-dimensional polynomial system in $\mathbb{Q}[x_1,\ldots,x_n]$. Let

$$\mathcal{I}_i=(\mathcal{P}_i)=(\mathcal{P})\cap\mathbb{Q}[x_1,\ldots,x_i], i=1,\ldots,n,$$

where $(\mathcal{P})$ is the ideal generated by $\mathcal{P}$. We use $V_{\mathbb{C}}(\mathcal{P})$ to denote its complex roots in $\mathbb{C}^n$.

Since we will use rectangles to isolate complex numbers, we adopt the following norm for a complex number $c=x+yi$:

$$|c|=\max\{|x|,|y|\}. \tag{1}$$

The "distance [*]" between two complex numbers c_1 and c_2 is defined to be $|c_1-c_2|$. It is easy to check that this is indeed a distance satisfying the inequality $|c_1-c_2|\le|c_1-c_3|+|c_3-c_2|$ for any complex number c_3. Let c_0 be a complex number and r a positive rational number. Then the set of points having distance less than r with c_0, denoted as

$$\mathbb{S}_{c_0,r}=\{c_1\in\mathbb{C}\,|\,|c_1-c_0|<r\}, \tag{2}$$

is an open square with c_0 as the center. We can simply denote it as $\mathbb{S}_{c_0}$ if r is clear.

Definition 2. By an **LUR**, we mean a set like

$$\{T_1(t_1),\ldots,T_n(t_n),s_i,d_i,i=1,\ldots,n-1\}, \tag{3}$$

[*] The results in this section are also valid if we use the usual distance for complex numbers.

where $T_i(t_i) \in \mathbb{Q}[t_i]$ are univariate polynomials, s_i and d_i are positive rational numbers. The **roots** of (3) are defined to be

$$\{(\alpha_1, \frac{\alpha_2-\alpha_1}{s_1}, \ldots, \frac{\alpha_n-\alpha_{n-1}}{s_1\cdots s_{n-1}}) \,|\, T_i(\alpha_i)=0, i=1,\ldots,n \text{ and}$$
$$|\alpha_{i+1}-\alpha_i| < s_1\cdots s_{i-1}d_i, i=1,\ldots,n-1\}. \tag{4}$$

Geometrically, we match a root α_i of $T_i(t_i)=0$ with those roots of $T_{i+1}(t_{i+1})=0$ inside a squared neighborhood centered at α_i. See Figure 1 for an illustration. An **LUR for** $\mathcal{P}$ is a set of form (3) whose roots are exactly the roots of $\mathcal{P}=0$.

It is clear that an LUR represents the roots of $\mathcal{P}$ as linear combinations of the roots of some univariate polynomial equations. The LUR representation has the following advantage: we can easily derive the precision of the roots of $\mathcal{P}=0$ from that of the univariate equations as shown by the following lemma.

Lemma 1. *Let (3) be an LUR for a polynomial system $\mathcal{P}=0$. If α_i is a root of $T_i(t_i)=0 (1\le i\le n)$ and $\overline{\alpha}_i$ is an approximation of α_i with precision ϵ_i, then the approximate root $(\overline{\alpha}_1, \frac{\overline{\alpha}_2-\overline{\alpha}_1}{s_1}, \ldots, \frac{\overline{\alpha}_n-\overline{\alpha}_{n-1}}{s_1\cdots s_{n-1}})$ of $\mathcal{P}=0$ has a precision* $\max\{\epsilon_1, \frac{\epsilon_2+\epsilon_1}{s_1}, \ldots, \frac{\epsilon_n+\epsilon_{n-1}}{s_1\cdots s_{n-1}}\}$.

Proof. Since $x_i = \frac{\alpha_i-\alpha_{i-1}}{s_1\cdots s_{i-1}}$ and the approximate root $\overline{\alpha}_i$ of α_i has precision ϵ_i, the approximate root $\overline{x}_i = \frac{\overline{\alpha}_i-\overline{\alpha}_{i-1}}{s_1\cdots s_{i-1}}$ has precision no larger than $\frac{\epsilon_i+\epsilon_{i-1}}{s_1\cdots s_{i-1}}$. ▮

For a zero-dimensional polynomial system $\mathcal{P}$, let d_i, r_i $(i=1,\ldots,n)$, and s_i $(1\le i\le n-1)$ be positive rational numbers satisfying

$$D_i = \min\{\frac{1}{2}|\alpha-\beta|, \forall\eta\in V_{\mathbb{C}}(\mathcal{I}_{i-1}), (\eta,\alpha),(\eta,\beta)\in V_{\mathbb{C}}(\mathcal{I}_i), \alpha\ne\beta\}, \tag{5}$$
$$d_i < \min\{D_i, \frac{d_{i-1}}{2s_{i-1}}\}, \tag{6}$$
$$r_i > 2\max\{|\gamma_i|, \forall(\gamma_1,\ldots,\gamma_i)\in V_{\mathbb{C}}(\mathcal{I}_i)\}, \tag{7}$$
$$s_i \le \frac{d_i}{r_{i+1}}, \tag{8}$$

where $s_0=1, d_0=+\infty, \mathcal{I}_0=(x_0)$. Geometrically, D_i is half of the root separation bound for roots of $\mathcal{I}_i$ considered as points on a "fiber" over each root of $\mathcal{I}_{i-1}$, r_i is twice of the root bound for the i-th coordinates of the roots of $\mathcal{I}_i$, and s_i, the inverse of the slope of certain line, is a key parameter to be used in our method. If $\forall\eta\in V_{\mathbb{C}}(\mathcal{I}_{i-1})$, $\#\{\alpha|(\eta,\alpha)\in V_{\mathbb{C}}(\mathcal{I}_i)\}=1$, we can choose any positive number as d_i.

The following lemma is to illustrate the worst cases of the bounds of D_i and r_i. The related results can be found in Yap, pp.341 (2000).

Lemma 2 (Emiris et al (2010))**.** *Let $\Sigma=\{f_1,\ldots,f_n\}\subset\mathbb{C}[x_1^{\pm},\ldots,x_n^{\pm}]$ be a zero-dimensional Laurent polynomial system. And $\deg(f_i)\le d$, $\mathcal{L}(f_i)\le\tau$ is the maximum bitsize of the coefficients of f (including a bit for the sign). Then the root separation bound $sep(\Sigma)$ and root bound $rb(\Sigma)$ of $\Sigma=0$ satisfy the following inequalities.*

$$2D_i > sep(\Sigma) \geq 2^{-2\,d^{2n} - n(2\,n\,\lg d + \tau)d^{2n-1}},$$
$$r_i/2 < rb(\Sigma) \leq 2^{d^n + n(\tau + n\,lgd+1)d^{n-1}}.$$

We can find that the bounds are too large or small to be used in practice.

For s_i satisfying (8), consider the ideal

$$\bar{\mathcal{I}}_i = (\mathcal{I}_i \cup \{t_i - x_1 - s_1x_2 - \cdots - s_1 \cdots s_{i-1}x_i\}), \tag{9}$$

where t_i is a new variable. It is clear that $\bar{\mathcal{I}}_i$ is a zero-dimensional ideal in $\mathbb{Q}[x_1, \ldots, x_i, t_i]$. And the elimination ideal $(\bar{\mathcal{I}}_i) \cap \mathbb{Q}[t_i]$ is principal. Let $T_i(t_i)$ be the generator of this ideal:

$$(\bar{\mathcal{I}}_i) \cap \mathbb{Q}[t_i] = (T_i(t_i)). \tag{10}$$

The following is the main result of this paper.

Theorem 3. *If d_i, s_i satisfy conditions (6), (8) and T_i is defined in (10), then the corresponding set (3) is an LUR for $\mathcal{P}$.*

We will prove two lemmas which will lead to a proof for the theorem. For a root α_i of $T_i(t_i) = 0$, $\mathbb{S}_{\alpha_i,\rho_i}$ (see equation (2) for definition) is an open square whose center is α_i and whose edge has length $2\rho_i$, where $\rho_i = s_1 \cdots s_{i-1}d_i$. In the rest of the paper, we simply denote it as $\mathbb{S}_{\alpha_i}$ since ρ_i is fixed for α_i. With this notation, the roots of (3) can be written as

$$\{(\alpha_1, \frac{\alpha_2 - \alpha_1}{s_1}, \ldots, \frac{\alpha_n - \alpha_{n-1}}{s_1 \cdots s_{n-1}}) \,|\, T_i(\alpha_i) = 0, i = 1, \ldots, n \text{ and}$$
$$\alpha_{i+1} \in \mathbb{S}_{\alpha_i}, i = 1, \ldots, n-1\}. \tag{11}$$

In Figure 1, $\mathbb{S}_{\alpha_i}$ are interior parts of the squares. We have

Lemma 4. *Under assumptions of Theorem 3, we have $\mathbb{S}_{\alpha_{i+1}} \subset \mathbb{S}_{\alpha_i}$,i=1,...,n-1, where $(\xi_1, \ldots, \xi_{i+1}) \in V_{\mathbb{C}}(\mathcal{I}_{i+1})$ and*

$$\alpha_i = \xi_1 + s_1\xi_2 + \cdots + s_1 \cdots s_{i-1}\,\xi_i, \tag{12}$$
$$\alpha_{i+1} = \xi_1 + s_1\xi_2 + \cdots + s_1 \cdots s_{i-1}\,\xi_i + s_1 \cdots s_i\,\xi_{i+1} = \alpha_i + s_1 \cdots s_i\,\xi_{i+1}. \tag{13}$$

Proof. From the definition of $\bar{\mathcal{I}}_i$ in (9), α_i is a root of $T_i(t_i) = 0$, α_{i+1} is a root of $T_{i+1}(t_{i+1}) = 0$, and each root of $T_{i+1}(t_{i+1}) = 0$ has the form (13).

We first prove that $\alpha_{i+1} \in \mathbb{S}_{\alpha_i}$. Using (7) and (8), we have

$$|\alpha_{i+1} - \alpha_i| = s_1 \cdots s_i|\xi_{i+1}| < \frac{1}{2}s_1 \cdots s_i r_{i+1} \leq \frac{1}{2}s_1 \cdots s_{i-1}d_i = \frac{1}{2}\rho_i. \tag{14}$$

As a consequence, α_{i+1} is in $\mathbb{S}_{\alpha_i}$.

We now prove that $\mathbb{S}_{\alpha_{i+1}} \subset \mathbb{S}_{\alpha_i}$. By (6), we have $\rho_{i+1} = s_1 \cdots s_i d_{i+1} < \frac{1}{2}s_1 \cdots s_{i-1}d_i = \frac{1}{2}\rho_i$. Therefore, for any $\alpha \in \mathbb{S}_{\alpha_{i+1}}$, by (14), we have $|\alpha - \alpha_i| \leq |\alpha - \alpha_{i+1}| + |\alpha_{i+1} - \alpha_i| < \rho_{i+1} + \frac{1}{2}\rho_i < \rho_i$. Hence $\alpha \in \mathbb{S}_{\alpha_i}$ and the lemma is proved. ∎

Theorem 3 follows from (d) of the following lemma.

Lemma 5. *Under assumptions of Theorem 3, for $i = 1, \dots, n$, we have*

(a) $t_i = x_1 + s_1 x_2 + \cdots + s_1 \cdots s_{i-1} x_i$ is a separating element of $\mathcal{I}_i$.

(b) Each root α_i of $T_i(t_i) = 0$ is in a box $\mathbb{S}_{\alpha_{i-1}}$ for a root α_{i-1} of $T_{i-1}(t_{i-1}) = 0$. Furthermore, if $\alpha_{i-1} = \xi_1 + s_1 \xi_2 + \cdots + s_1 \cdots s_{i-2} \xi_{i-1}$, then all roots of $T_i(t_i) = 0$ in $\mathbb{S}_{\alpha_{i-1}}$ are of the following form

$$\alpha_i = \alpha_{i-1} + s_1 \cdots s_{i-1} \xi_i \tag{15}$$

where $(\xi_1, \dots, \xi_{i-1}, \xi_i) \in V_{\mathbb{C}}(\mathcal{I}_i)$.

(c) $\mathbb{S}_{\alpha_i}$ are disjoint for all roots α_i of $T_i(t_i) = 0$.

(d) $(T_1(t_1), \dots, T_i(t_i), s_j, d_j, j = 1, \dots, i-1)$ is an LUR for $\mathcal{I}_i$.

Proof. We will prove the lemma by induction on $k = i$. For $k = 1$, since $(\mathcal{I}_1) = (T_1(t_1))$, statements (a) and (d) are obviously true. We do not need prove (b). From (6), we have $d_1 < \min\{\frac{1}{2}|\alpha - \beta|, \forall \alpha, \beta \in V_{\mathbb{C}}(\mathcal{I}_1) = V_{\mathbb{C}}(T_1), \alpha \neq \beta\}$. As a consequence, $\mathbb{S}_{\alpha_1}$ are disjoint for all roots α_1 of $T_1(t_1) = 0$. Statement (c) is proved.

Assume the statements are true for $k = 1, \dots, i$. We will prove the result for $k = i + 1$.

We first prove statement (a). Let $\xi = (\xi_1, \dots, \xi_{i+1})$ and $\beta = (\beta_1, \dots, \beta_{i+1})$ be two distinct elements in $V_{\mathbb{C}}(\mathcal{I}_{i+1})$. We consider two cases. If $(\xi_1, \dots, \xi_i)$ is different from $(\beta_1, \dots, \beta_i)$, then by the induction hypothesis $\alpha_i = \xi_1 + s_1\xi_2 + \cdots + s_1 \cdots s_{i-1}\xi_i$ is also different from $\theta_i = \beta_1 + s_1\beta_2 + \cdots + s_1 \cdots s_{i-1}\beta_i$. By (c) of the induction hypothesis, $\mathbb{S}_{\alpha_i}$ and $\mathbb{S}_{\theta_i}$ are disjoint. By Lemma 4, $\alpha_{i+1} = \alpha_i + s_1 \cdots s_i \xi_{i+1} \in \mathbb{S}_{\alpha_i}$ and $\theta_{i+1} = \theta_i + s_1 \cdots s_i \beta_{i+1} \in \mathbb{S}_{\theta_i}$. Then, in this case we have $\alpha_{i+1} \neq \theta_{i+1}$. In the second case, we have $(\xi_1, \dots, \xi_i) = (\beta_1, \dots, \beta_i)$. Then, $\alpha_i = \theta_i$ and $\xi_{i+1} \neq \beta_{i+1}$. It is clear that $\alpha_{i+1} = \alpha_i + s_1 \cdots s_i \xi_{i+1}$ is different from $\theta_{i+1} = \theta_i + s_1 \cdots s_i \beta_{i+1}$. Thus, (a) is proved.

We now prove statement (b). Use notations in (12) and (13). By Lemma 4, we have $\alpha_{i+1} \in \mathbb{S}_{\alpha_i}$. Then, each root of $T_{i+1}(t_{i+1}) = 0$ is in a box $\mathbb{S}_{\alpha_i}$ for a root α_i of $T_i(t_i) = 0$. Let $(\beta_1, \dots, \beta_{i+1}) \in V_{\mathbb{C}}(\mathcal{I}_{i+1})$ such that $\theta_{i+1} = \beta_1 + s_1\beta_2 + \cdots + s_1 \cdots s_i \beta_{i+1}$ is another element in $\mathbb{S}_{\alpha_i}$. We claim that $(\beta_1, \dots, \beta_i)$ must be the same as $(\xi_1, \dots, \xi_i)$. Otherwise, by the induction hypothesis (a), $\theta_i = \beta_1 + s_1\beta_2 + \cdots + s_1 \cdots s_{i-1}\beta_i$ is different from α_i. By the induction hypothesis (c), $\mathbb{S}_{\alpha_i}$ and $\mathbb{S}_{\theta_i}$ are disjoint which is impossible since by Lemma 4, $\theta_{i+1} \in \mathbb{S}_{\alpha_i}$ and $\theta_{i+1} \in \mathbb{S}_{\theta_i}$. Thus, $(\beta_1, \dots, \beta_i) = (\xi_1, \dots, \xi_i)$ and hence $\theta_{i+1} = \alpha_i + s_1 \cdots s_i \beta_{i+1}$. This proves equation (15) and hence statement (b).

We now prove statement (c). Use notations in (12) and (13). By Lemma 4, $\mathbb{S}_{\alpha_{i+1}} \subset \mathbb{S}_{\alpha_i}$. As a consequence, we need only to prove that the squares $\mathbb{S}_{\alpha_{i+1}}$ contained in the same $\mathbb{S}_{\alpha_i}$ are disjoint. Let $\alpha_{i+1}, \theta_{i+1}$ be two roots of $T_{i+1}(t_{i+1}) = 0$ in $\mathbb{S}_{\alpha_i}$. By statement (b) just proved, we have

$$\alpha_{i+1} = \alpha_i + s_1 \cdots s_i \xi_{i+1}, \theta_{i+1} = \alpha_i + s_1 \cdots s_i \beta_{i+1}$$

where α_i is defined in (12) and $(\xi_1, \dots, \xi_i, \xi_{i+1})$, $(\xi_1, \dots, \xi_i, \beta_{i+1})$ are roots of $\mathcal{I}_{i+1}$. Then, by (6),

$$|\alpha_{i+1} - \theta_{i+1}| = s_1 \cdots s_i |\xi_{i+1} - \beta_{i+1}| > 2\, s_1 \cdots s_i\, d_{i+1} = 2\rho_{i+1}.$$

So, $\mathbb{S}_{\alpha_{i+1}} = \mathbb{S}_{\alpha_{i+1}, \rho_{i+1}}$ and $\mathbb{S}_{\theta_{i+1}} = \mathbb{S}_{\theta_{i+1}, \rho_{i+1}}$ are disjoint. Statement (c) is proved.

Finally, we prove statement (d). Let $\xi = (\xi_1, \dots, \xi_{i+1}) \in V_{\mathbb{C}}(\mathcal{I}_{i+1})$ and $\alpha_j = \xi_1 + s_1\xi_2 + \cdots + s_1 \cdots s_{j-1} \xi_j, j = 1, \dots, i+1$. By the induction hypothesis, we have $(\xi_1, \dots \xi_i) = (\alpha_1, \frac{\alpha_2 - \alpha_1}{s_1}, \dots, \frac{\alpha_i - \alpha_{i-1}}{s_1 \cdots s_{i-1}})$ where $|\alpha_{j+1} - \alpha_j| < s_1 \cdots s_{j-1} d_j, j = 1, \dots, i$. Note that the inequality is equivalent to that $\alpha_{j+1} \in \mathbb{S}_{\alpha_j}$. By (15), we can recover ξ_{i+1} with the following equation

$$\xi_{i+1} = \frac{\alpha_{i+1} - \alpha_i}{s_1 \cdots s_i}.$$

From Lemma 4, we have $\alpha_{i+1} \in \mathbb{S}_{\alpha_i}$ or equivalently $|\alpha_{i+1}-\alpha_i| < s_1 \cdots s_{i-1} d_i$. Then the root $(\xi_1, \ldots \xi_{i+1}) = (\alpha_1, \frac{\alpha_2-\alpha_1}{s_1}, \ldots, \frac{\alpha_{i+1}-\alpha_i}{s_1 \cdots s_i})$ is a root of the LUR: $(T_1(t_1), \ldots, T_{i+1}(t_{i+1}), s_j, d_j, j = 1, \ldots, i)$. We thus proved that the roots of $\mathcal{I}_{i+1}$ are the same as the roots of the LUR and hence statement (d). ▮ ▮

Remark: From (a) and (b) of the lemma, we know that $t_i = x_1 + s_1 x_2 + \cdots + s_1 \cdots s_{i-1} x_i$ is also a local separating element for $\mathcal{I}_i = 0$.

From the remark above, we have the following corollaries.

Corollary 6. *If (3) is an LUR for a polynomial system $\mathcal{P}$, where d_i, s_i satisfy (6),(8), then the roots of $\mathcal{I}_i = 0$ are in a one to one correspondence with the roots of $T_i(t_i) = 0$ for $i = 1, \ldots, n$.*

Corollary 7. *The real roots of $\mathcal{P} = 0$ are in a one to one correspondence with the real roots of $T_n(t_n) = 0$. More precisely, if α_n is a real root of $T_n(t_n) = 0$, then in the corresponding root $(\alpha_1, \frac{\alpha_2-\alpha_1}{s_1}, \ldots, \frac{\alpha_n-\alpha_{n-1}}{s_1 \cdots s_{n-1}})$ of $\mathcal{P} = 0$, α_i is a real root of $T_i(t_i) = 0, i = 1, \ldots, n-1$.*

From the lemma, we can consider the real roots of an LUR if we are only interested in the real roots of $\mathcal{P} = 0$.

3. Algorithm for computing an LUR and roots isolation

In this section, we will present an algorithm to compute an LUR for a zero-dimensional polynomial system. The algorithm will isolate synchronously the roots of the system in $\mathbb{C}^n$.

3.1. Complex isolating intervals and isolating boxes

We will introduce the basic concepts of complex isolating intervals, isolating boxes and interval computation of (complex) isolating intervals (For more details, we refer to Neumaier (1990) and Moore (1966)).

Let $\square\mathbb{Q}$ denote the set of intervals of the form $[a, b]$, where $a \leq b \in \mathbb{Q}$. The **length** of an interval $I = [a, b] \in \square\mathbb{Q}$ is defined to be $|I| = b - a$. A pair of intervals $\langle I, J \rangle$ is called a **complex interval**, which represents a rectangle in the complex plane. A complex number $\langle \alpha, \beta \rangle = \alpha + \beta \mathrm{i}$ ($\mathrm{i}^2 = -1$) is said to be in a complex interval $\langle I, J \rangle$ if $\alpha \in I$ and $\beta \in J$. The length of a complex interval $\langle I, J \rangle$ is defined to be $|\langle I, J \rangle| = \max\{|I|, |J|\}$. Let $I_i = [a_i, b_i] \in \square\mathbb{Q}, i = 1, 2$, then

$$I_1 - I_2 = [a_1 - b_2, b_1 - a_2].$$

Let $\langle I_i, J_i \rangle, i = 1, 2$, then

$$\langle I_1, J_1 \rangle - \langle I_2, J_2 \rangle = \langle I_1 - I_2, J_1 - J_2 \rangle.$$

Definition 3. Assuming $a_1 \leq a_2$, we define the **distance between two intervals** as

$$\mathrm{Dis}([a_1, b_1], [a_2, b_2]) = \begin{cases} a_2 - b_1, & \text{if } [a_1, b_1] \cap [a_2, b_2] = \emptyset, \\ 0, & \text{otherwise.} \end{cases}$$

We define the **distance between two complex intervals** as

$$\mathrm{Dis}(\langle [a_1, b_1], [p_1, q_1] \rangle, \langle [a_2, b_2], [p_2, q_2] \rangle) = \max\{\mathrm{Dis}([a_1, b_1], [a_2, b_2]), \mathrm{Dis}([p_1, q_1], [p_2, q_2])\}. \quad (16)$$

A set $\mathcal{S}$ of disjoint complex intervals is called **isolating intervals** of $T(x) = 0$ if each interval in $\mathcal{S}$ contains only one root of $T(x) = 0$ and each root of $T(x) = 0$ is contained in one interval in $\mathcal{S}$. Methods to isolate the complex roots of a univariate polynomial equation are given in Collins and Krandick (1996); Pinkert (1976); Sagraloff and Yap (2009); Wilf (1978).

Let $\square\mathbb{C}$ denote the set of complex intervals. An element $\langle I_1^{\mathbb{R}}, I_1^{\mathbb{I}}\rangle \times \cdots \times \langle I_n^{\mathbb{R}}, I_n^{\mathbb{I}}\rangle$ in $\square\mathbb{C}^n$ is called a **complex box**. A set $\mathcal{S}$ of **isolating boxes** for a zero-dimensional polynomial system $\mathcal{P}$ in $\mathbb{Q}[x_1, \ldots, x_n]$ is a set of disjoint complex boxes in $\square\mathbb{C}^n$ such that each box in $\mathcal{S}$ contains only one root of $\mathcal{P} = 0$ and each root of $\mathcal{P} = 0$ is in one of the boxes. Furthermore, if each box $\mathbf{B} = \langle I_1^{\mathbb{R}}, I_1^{\mathbb{I}}\rangle \times \cdots \times \langle I_n^{\mathbb{R}}, I_n^{\mathbb{I}}\rangle$ in $\mathcal{S}$ satisfies $\max_i\{|I_i^{\mathbb{R}}|, |I_i^{\mathbb{I}}|\} \leq \epsilon$, then $\mathcal{S}$ is called an **ϵ-isolating boxes** of $\mathcal{P} = 0$. The aim of this paper is to compute a set of ϵ-isolating boxes for a zero-dimensional polynomial system $\mathcal{P}$.

3.2. Gröbner basis and computation of r_i and $T_i(t_i)$

In this subsection, we will show how to use Gröbner basis to compute r_i defined in (7) and $T_i(t_i)$ defined in (10) supposing the parameters s_i are given.

Let $\mathcal{P} \subset \mathbb{Q}[x_1, \ldots, x_n]$ be a zero-dimensional polynomial system. Then $\mathcal{A} = \mathbb{Q}[x_1, \ldots, x_n]/(\mathcal{P})$ is a finite dimensional linear space over $\mathbb{Q}$. Let $\mathcal{G}$ be a Gröbner basis of $\mathcal{P}$ with any ordering. Then the set of remainder monomials

$$\mathbf{B} = \{x_1^{\gamma_1} \cdots x_n^{\gamma_n} | x_1^{\gamma_1} \cdots x_n^{\gamma_n} \text{ is not divisible by the leading term of any element of } \mathcal{G}\}$$

forms a basis of $\mathcal{A}$ as a linear space over $\mathbb{Q}$, where γ_i are non-negative integers.

Let $f \in \mathbb{Q}[x_1, \ldots, x_n]$. Then f gives a multiplication map

$$M_f : \mathcal{A} \longrightarrow \mathcal{A}$$

defined by $M_f(p) = fp$ for $p \in \mathcal{A}$. It is clear that M_f is a linear map. We can construct the matrix representation for M_f from $\mathbf{B}$ and $\mathcal{G}$. The following theorem is a basic property for M_f (Lazard (1981)) and one can find similar result in Cox et al (2004) § 4, Chapter 1 or Basu et al (2006) pp.150.

Theorem 8 (Stickelberger's Theorem)**.** *Assume that $\mathcal{P} \subset \mathbb{Q}[x_1, \ldots, x_n]$ has a finite positive number of solutions over $\mathbb{C}$. The eigenvalues of M_f are the values of f at the roots of $\mathcal{P} = 0$ over $\mathbb{C}$ with respect to multiplicities of the roots of $\mathcal{P} = 0$.*

Let s_i be rational numbers satisfying (8) and

$$\mathcal{F}_i = \mathcal{P} \cup \{t_i - x_1 - s_1 x_2 - \cdots - s_1 \cdots s_{i-1} x_i\}.$$

We can compute $g_i(x_i)$ and $T_i(t_i)$ such that

$$(g_i(x_i)) = \mathbb{Q}[x_i] \cap (\mathcal{P}) \text{ and } (T_i(t_i)) = \mathbb{Q}[t_i] \cap (\mathcal{F}_i). \tag{17}$$

In fact, we can construct the matrixes for M_{x_i} and M_{t_i} based on $\mathbf{B}$ and $\mathcal{G}$, and $g_i(x_i)$ and $T_i(t_i)$ are the minimal polynomials for M_{x_i} and M_{t_i}, respectively (See reference Cox (2005)). Note that we can also use the method introduced in reference Faug et al (1993) to compute $g_i(x_i), T_i(t_i)$.

From Theorem 8 and (a) of Lemma 5, the i-th coordinates of all the roots of $\mathcal{P} = 0$ are roots of $g_i(x_i) = 0$, and all the possible values of $t_i = \sum_{j=1}^{i} s_1 \cdots s_{j-1} x_j$ on the roots of $\mathcal{P} = 0$ are roots of $T_i(t_i) = 0$.

Now we show how to estimate r_i defined in (7). At first, compute $(g_i(x_i)) = (\mathcal{P}) \cap \mathbb{Q}[x_i]$. Then we have the following result.

Lemma 9. *Use the notations introduced before. Then*

$$r_i = 2\max\{\mathrm{RB}(g_i(x_i))\} \tag{18}$$

satisfies the condition (7), where $\mathrm{RB}(g)$ *is the root bound of a univariate polynomial equation* $g = 0$.

Proof. The lemma is obvious since for any root $(\xi_1, \ldots, \xi_i) \in V_{\mathbb{C}}(\mathcal{I}_i)$, ξ_i is a root of $g_i(x_i) = 0$. ∎

3.3. Theoretical ingredients for the algorithm

In this subsection, we will outline an algorithm to compute an LUR for $\mathcal{P}$ and to isolate the roots of $\mathcal{P} = 0$ under a given precision ϵ. The algorithm is based on an interval version of Theorem 3.

The isolating boxes for an LUR defined in (3) can be written as:

$$\{B_1 \times \frac{B_2 - B_1}{s_1} \times \cdots \times \frac{B_n - B_{n-1}}{s_1 \cdots s_{n-1}} \mid B_i \in \mathcal{B}_i, \mathrm{Dis}(B_{i+1}, B_i) < \rho_i/2, 1 \le i \le n-1\}, \tag{19}$$

where $\mathcal{B}_i$ is a set of isolating boxes for the complex roots of $T_i(t_i) = 0$ and $\rho_i = s_1 \cdots s_{i-1} d_i$. In Theorem 17 to be proved below, we will give criteria under which conditions the isolating boxes for $\mathcal{P}$ are the isolating boxes of an LUR.

Let $\mathcal{P} \subset \mathbb{Q}[x_1, \ldots, x_n]$ be a zero-dimensional polynomial system. We will compute an LUR for $\mathcal{P}$ and a set of ϵ-isolating boxes for the roots of $\mathcal{P} = 0$ inductively.

At first, consider $i = 1$. We compute $T_1(t_1)$ as defined in equation (17). Let $\mathcal{B}_1$ be a set of isolating intervals for the complex roots of $T_1(t_1) = 0$. Then, we can set d_1 to be the minimal distance between any two intervals in $\mathcal{B}_1$.

For i from 1 to $n-1$, assuming that we have computed

- An LUR $(T_1(t_1), \ldots, T_i(t_i), s_j, d_j, j = 1, \ldots, i-1)$ for $\mathcal{I}_i$.
- A set of ϵ-isolating boxes for $\mathcal{I}_i$.
- The parameter d_i.

We will show how to compute r_{i+1}, s_i, $T_{i+1}(t_{i+1})$, d_{i+1}, and a set of ϵ-isolating boxes of the roots of $\mathcal{I}_{i+1} = 0$. The procedure consists of three steps.

Step 1. We will compute r_{i+1}, s_i as introduced in (7) and (8). With s_i, we can compute $T_{i+1}(t_{i+1})$ as defined in (17).

Here r_{i+1} can be computed with the method in Lemma 9. Note that d_i is known from the induction hypotheses. Then we can choose a rational number s_i such that condition (8) is valid. Finally, $T_{i+1}(t_{i+1})$ can be computed with the methods mentioned below equation (17).

Step 2. We are going to compute the isolating intervals of the roots of $\mathcal{I}_{i+1} = 0$. Let $\xi = (\xi_1, \ldots, \xi_i)$ be a root of $\mathcal{I}_i = 0$. We are going to find the roots of $\mathcal{I}_{i+1} = 0$ "lifted" from ξ, that is, roots of the form

$$\zeta_j = (\xi_1, \ldots, \xi_i, \xi_{i+1,j}), j = 1, \ldots, m. \tag{20}$$

To do that, we need only to find a set of isolating intervals for $\xi_{i+1,j}$ with lengths no larger than ϵ, since we already have an ϵ-box for ξ.

Let

$$\alpha_i = \xi_1 + s_1\xi_2 + \cdots + s_1 \cdots s_{i-1}\xi_i.$$

Then, α_i is a root of $T_i(t_i) = 0$. By (b) of Lemma 5 the roots θ_j of $T_{i+1}(t_{i+1}) = 0$ correspond to ζ_j are

$$\theta_j = \alpha_i + s_1 \cdots s_i\xi_{i+1,j}, j = 1, \ldots, m. \tag{21}$$

We have

Lemma 10. *Let $I_i = \langle [a, b], [c, d]\rangle$ be an isolating interval for the root α_i of $T_i(t_i) = 0$ such that $|I_i| < \frac{1}{4}\rho_i$ where $\rho_i = s_1 \cdots s_{i-1}d_i$. Then all θ_j in (21) are in the following complex interval*

$$\mathbb{I}_{I_i} = \langle (a - \rho_i/2, b + \rho_i/2), (c - \rho_i/2, d + \rho_i/2)\rangle. \tag{22}$$

Furthermore, the intervals $\mathbb{I}_{I_\alpha}$'s are disjoint for all the isolating intervals I_α of the roots α's of $T_i(t_i) = 0$.

Proof. In Figure 2, let the square $ABCD$ be $\mathbb{S}_{\alpha_i} = \{\theta \in \mathbb{C} \mid |\theta - \alpha_i| < \rho_i\}$ and the square $A_1B_1C_1D_1 = \{\theta \in \mathbb{C} \mid |\theta-\alpha_i| < \rho_i/2\}$. By equations (14) and (21), we know $|\theta_j-\alpha_i| < \frac{1}{2}\rho_i$. So, θ_j is inside $A_1B_1C_1D_1$. Let rectangle $A_2B_2C_2D_2$ be the complex interval I_i and rectangle $A_3B_3C_3D_3$ the complex interval $\mathbb{I}_{I_i}$ which is obtained by adding $\rho_i/2$ in each direction of the rectangle $A_2B_2C_2D_2$. Then, $\mathbb{I}_{I_i}$ contains $A_1B_1C_1D_1$ and hence θ_j is inside $\mathbb{I}_{I_i}$.

For any $\theta \in \mathbb{I}_{I_i}$, we have $|\theta - \alpha_i| \le |\theta - P|$, where P is one of the points A_2, B_2, C_2, D_2 to make $|\theta-P|$ maximal. It is clear that $|\theta-P| \le \rho_i/2+|I_i| = \frac{3}{4}\rho_i$. So, $\forall\theta \in \mathbb{I}_{I_i}$, $|\theta-\alpha_i| \le \frac{3}{4}\rho_i$. Since $\mathbb{S}_{\alpha_i}$ is the set of complex numbers satisfying $|\theta - \alpha_i| < \rho_i$, we have $\mathbb{I}_{I_i} \subset \mathbb{S}_{\alpha_i}$. By (c) of Lemma 5, $\mathbb{S}_{\alpha_i}$ are disjoint for all the roots of $T_i(t_i) = 0$. Then $\mathbb{I}_{I_i}$ are disjoint for all the roots of $T_i(t_i) = 0$ too. ∎

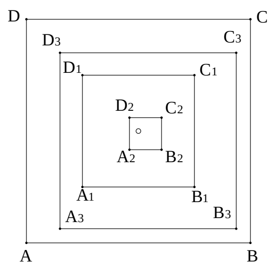

Fig. 2. The isolating intervals I_i, $\mathbb{S}_{\alpha_i}$, $\mathbb{I}_{I_i}$ for a root α_i of $T_i(t_i) = 0$. α_i is represented by $\circ$.

The following lemma shows what is the precision needed to isolate the roots of $T_{i+1}(t_{i+1}) = 0$ in order for the isolating boxes to be contained in some $\mathbb{I}_{I_i}$. It can be seen as an effective version of the fact $\alpha_{i+1} \in \mathbb{S}_{\alpha_i}$ proved in Lemma 4.

Lemma 11. *Use the notations introduced in Lemma 10. Let* $\{B_j, j = 1, \ldots, m\}$ *be a set of* $\frac{1}{4}\rho_i$*-isolating boxes for the roots* $\theta_j, j = 1, \ldots, m$ *of* $T_{i+1}(t_{i+1}) = 0$*. Then, for all* j

$$B_j \subset \mathbb{I}_{I_i} \text{ and } \mathrm{Dis}(B_j, I_i) < \rho_i/2. \tag{23}$$

Proof. From the proof of Lemma 10, the distance from α_i to the line BC in Figure 2 is ρ_i and the distance from α_i to the line B_3C_3 is less than $\frac{3}{4}\rho_i$. So, the distance between the line BC and B_3C_3 is at least $\frac{1}{4}\rho_i$. This fact is also valid for the pairs of the lines AD/A_3D_3, AB/A_3B_3, and CD/C_3D_3. Since the isolating boxes B_j are of size smaller than $\rho_i/4$ and their centers are inside $A_3B_3C_3D_3$, the boxes B_j must be inside $ABCD$. Note that I_i is the rectangle $A_2B_2C_2D_2$. Since θ_j is inside both B_j and the rectangle $A_3B_3C_3D_3$ and the distance from α_i to each edge of $A_3B_3C_3D_3$ is $\rho_i/2$, the distance between B_j and I_i must be smaller than $\rho_i/2$. ∎

If we isolate the roots of $T_{i+1}(t_{i+1}) = 0$ with precision $\frac{1}{4}\rho_i$, by Lemma 11, all the roots are in one of the intervals $\mathbb{I}_I$, where I is an isolating interval for a root α of $T_i(t_i) = 0$.

Let $K_j = \langle [p_j, q_j], [g_j, h_j] \rangle (1 \le j \le m)$ be the isolating intervals for the roots θ_j of $T_{i+1}(t_{i+1}) = 0$ inside $\mathbb{I}_{I_i}$. Then from (21), the isolating intervals of $\xi_{i+1,j} (1 \le j \le m)$ are

$$J_{i+1,j} = \frac{K_j - I_i}{s_1 \cdots s_i} = \frac{\langle [p_j - b, q_j - a], [g_j - d, h_j - c] \rangle}{s_1 \cdots s_i}. \tag{24}$$

We have

Lemma 12. *With the notations introduced above, if the following conditions*

$$(q_j - p_j) + (b - a) < s_1 \cdots s_i \epsilon, \ \ (h_j - g_j) + (d - c) < s_1 \cdots s_i \epsilon \tag{25}$$

$$T_{\alpha_i} = \min_{1 \le k \ne j \le m} \mathrm{Dis}(\langle [p_k, q_k], [g_k, h_k] \rangle, \langle [p_j, q_j], [g_j, h_j] \rangle) > \max\{b - a, d - c\}. \tag{26}$$

are valid, then $J_{i+1,j}$ *defined in (24) are* ϵ*-isolating intervals of* $\xi_{i+1,j}$ *in equation (20).*

Proof. It is clear that condition (25) is used to ensure the precision: $|J_{i+1,j}| < \epsilon$.

We consider (26) below. Assume that $J_{i+1,j}, J_{i+1,k} (1 \le k \ne j \le m)$ are any two intervals defined in (24) for the $(i+1)$-th coordinates of the roots $(\xi_1, \ldots, \xi_i, \xi_{i+1,j})$, $(\xi_1, \ldots, \xi_i, \xi_{i+1,k})$ of $\mathcal{I}_{i+1} = 0$, respectively. Since we have derived the ϵ-isolating boxes for the roots of $\mathcal{I}_i = 0$, we need only to ensure that the intervals of the $(i+1)$-th coordinates of the roots of $\mathcal{I}_{i+1} = 0$ lifted from a fixed root of $\mathcal{I}_i = 0$ are isolating intervals. That is, to show $\mathrm{Dis}(J_{i+1,j}, J_{i+1,k}) > 0$.

Assume that $K_j = \langle [p_j, q_j], [g_j, h_j] \rangle$ and $K_k = \langle [p_k, q_k], [g_k, h_k] \rangle$ are the isolating intervals of the roots α_j, α_k of $T_{i+1}(t_{i+1}) = 0$. Here α_j, α_k correspond to $(\xi_1, \ldots, \xi_i, \xi_{i+1,j})$, $(\xi_1, \ldots, \xi_i, \xi_{i+1,k})$, respectively. So K_j, K_k correspond to $J_{i+1,j}, J_{i+1,k}$, respectively. Assume that $p_j \le p_k, g_j \le g_k$. Then we have

$$\mathrm{Dis}(J_{i+1,j}, J_{i+1,k}) = \frac{\max\{\mathrm{Dis}([p_j - b, q_j - a], [p_k - b, q_k - a]), \mathrm{Dis}([g_j - d, h_j - c], [g_k - d, h_k - c])\}}{s_1 \cdots s_i},$$

and

$$\mathcal{L}_1 = \mathrm{Dis}([p_j - b, q_j - a], [p_k - b, q_k - a]) = \begin{cases} (p_k - q_j) - (b - a), & \text{if } (p_k - q_j) - (b - a) > 0, \\ 0, & \text{otherwise,} \end{cases}$$

$$\mathcal{L}_2 = \mathrm{Dis}([g_j - d, h_j - c], [g_k - d, h_k - c]) = \begin{cases} (g_k - h_j) - (d - c), & \text{if } (g_k - h_j) - (d - c) > 0, \\ 0, & \text{otherwise.} \end{cases}$$

K_j and K_k are disjoint since they are isolating intervals of $T_{i+1}(t_{i+1}) = 0$. So

$$\mathrm{Dis}(K_j, K_k) = \max\{p_k - q_j, g_k - h_j\} > 0.$$

It is clear that $\mathrm{Dis}(J_{i+1,j}, J_{i+1,k}) > 0$ if $\mathcal{L}_1 > 0$ or $\mathcal{L}_2 > 0$. Then we conclude if inequality (26) is true, then $\mathrm{Dis}(J_{i+1,j}, J_{i+1,k}) > 0$. This proves the lemma. ∎

Geometrically, T_{α_i} is the separation bound for the roots of $T_{i+1}(t_{i+1}) = 0$ corresponds to those roots of $\mathcal{I}_{i+1}$ lifted from the root of $\mathcal{I}_i = 0$ corresponding to the root η_i of $T_i(t_i) = 0$.

Remark 13. Note that in (26), we obtain $I_i = \langle [a, b], [c, d] \rangle$ first and $K_j = \langle [p_j, q_j], [g_j, h_j] \rangle$ later. We will refine the isolating interval I_i of $T_i(t_i) = 0$ such that inequality (26) is true. After the refinement, all other conditions are still valid. We need to do this kind of refinement at most once.

As a consequence of the above lemma, we have

Corollary 14. *Let $\mathbb{B}$ be an ϵ-isolating box for the root ξ of $\mathcal{I}_i = 0$ and $J_{i+1,j}$ defined in (24). If (25), (26) are valid, then $\mathbb{B} \times J_{i+1,j}, j = 1, \ldots, m$ are ϵ-isolating boxes for the roots $(\xi_1, \ldots, \xi_i, \xi_{i+1,j})$ of $\mathcal{I}_{i+1} = 0$, which are lifted from $(\xi_1, \ldots, \xi_i)$.*

Step 3. We will show how to compute d_{i+1} from the isolating intervals of $T_{i+1}(t_{i+1}) = 0$.

Lemma 15. *Let*

$$d_{i+1} = \min\{\frac{S_{i+1}}{2s_1 \cdots s_i}, \frac{d_i}{2s_i}\}, \tag{27}$$

where S_{i+1} is the minimal distance between any two isolating intervals of $T_{i+1}(t_{i+1}) = 0$. Then d_{i+1} satisfies conditions (6).

Proof. Let α_j and α_k be two different roots of $T_{i+1}(t_{i+1}) = 0$ defined in (21). Then we have

$$\xi_{i+1,j} - \xi_{i+1,k} = \frac{\alpha_j - \alpha_k}{s_1 \ldots s_i}.$$

Therefore, $D_{i+1} = \min_{\alpha_i \in V_{\mathbb{C}}(T_i(t_i))}\{\frac{T_{\alpha_i}}{2s_1 \cdots s_i}\}$ is the parameter defined in (5), where T_{α_i} is determined as in (26). It is clear that D_{i+1} is not larger than S_{i+1} which is the minimal distance between any two isolating intervals of $T_{i+1}(t_{i+1}) = 0$. Then, the first condition in (6) is satisfied. In order for the second condition in (6) to be satisfied, we also require $d_{i+1} \leq \frac{d_i}{2s_i}$. So the lemma is proved. ∎

We can summarize the result as the following theorem which is an interval version of Theorem 3.

Lemma 16. *Let (3) be an LUR such that d_i, r_i, and s_i satisfy (27), (7), and (8) respectively, $\mathcal{B}_i$ the ϵ_i-isolating boxes for the roots of $T_i(t_i) = 0$, and $S_i = \min\{\mathrm{Dis}(B_1, B_2) \mid B_1, B_2 \in \mathcal{B}_i, B_1 \neq B_2\}$. If*

$$\epsilon_1 \leq \epsilon, \epsilon_i + \epsilon_{i+1} \leq s_1 \cdots s_i \epsilon,\ \epsilon_i \leq \frac{\rho_i}{4}, \epsilon_{i+1} \leq \frac{\rho_i}{4}, \epsilon_i \leq S_{i+1}, \tag{28}$$

where $\rho_i = s_1 \cdots s_{i-1} d_i$, then (19) is a set of ϵ-isolating boxes for $\mathcal{P} = 0$.

Proof. We first explain what the function of each inequality is for the inequalities in (28). Then we can find that the theorem is clear. The first two inequalities in (28) are introduced in (25) to ensure the ϵ precision for the isolating boxes. The third inequality in (28) is introduced in Lemma 10 to ensure $\theta_j \in \mathbb{I}_{I_i}$ and $\mathbb{I}_{I_i}$ are disjoint. The fourth inequality is introduced in Lemma 11 to ensure the isolating intervals of the roots of $T_{i+1}(t_{i+1}) = 0$ are inside their corresponding interval $\mathbb{I}_{I_i}$. The last inequality is introduced in (26) to ensure the recovered isolating boxes of $\mathcal{P}$ are disjoint.

Now the lemma is a consequence of Corollary 14. Here, we give the explicit expression for the isolating boxes. The expression for interval $J_{i+1,j}$ in (24) is directly given. The matching condition $\mathrm{Dis}(B_{i+1}, B_i) < \rho_i/2$ is from condition (23). ∎

We have the following effective version of Theorem 3 and Lemma 16 by giving an explicit formula for ϵ_i.

Theorem 17. *Use the same notations as Lemma 16. Let ϵ be the given precision to isolate the roots of $\mathcal{P}$. Let*

$$\begin{aligned} \epsilon_1 &= \min\{\epsilon, \frac{s_1\epsilon}{2}, \frac{d_1}{4}, S_2\}, \\ \epsilon_i &= \min\{\frac{s_1 \cdots s_{i-1}\epsilon}{2}, \frac{s_1 \cdots s_i\epsilon}{2}, \frac{s_1 \cdots s_{i-1}d_i}{4}, \frac{s_1 \cdots s_{i-2}d_{i-1}}{4}, S_{i+1}\}, \end{aligned} \tag{29}$$

where $i = 2, ..., n$, $s_n = 1$, $S_{n+1} = +\infty$. If we isolate the roots of $T_i(t_i) = 0$ with precision ϵ_i, then (19) is a set of ϵ-isolating boxes for $\mathcal{P} = 0$.

Proof. By (29), we have $\epsilon_i \leq \frac{s_1 \cdots s_i \epsilon}{2}$ and $\epsilon_{i+1} \leq \frac{s_1 \cdots s_i \epsilon}{2}$. Then the second inequality in (28), $\epsilon_i + \epsilon_{i+1} \leq s_1 \cdots s_i \epsilon$, is valid. All other inequalities in (28) are clearly satisfied and the theorem is proved. ∎

We can also compute the multiplicities of the roots with the LUR algorithm.

Corollary 18. *If we compute the last univariate polynomial $T_n(t_n)$ in the LUR as the characteristic polynomial of M_{t_n}, then the multiplicities of the roots of $\mathcal{P} = 0$ are the multiplicities of the corresponding roots of $T_n(t_n) = 0$.*

Proof. By (a) of Lemma 5, $t_n = x_1 + s_1 x_2 + \cdots + s_1 \cdots s_{n-1} x_n$ is a separating element. By Theorem 8, the characteristic polynomial of M_{t_n} keeps the multiplicities of the roots of the system. The corollary is proved. ∎

3.4. Algorithm

Now, we can give the full algorithm based on LUR.

Algorithm 1. The input is a zero dimensional polynomial system $\mathcal{P} = \{f_1, \ldots, f_s\}$ in $\mathbb{Q}[x_1, \ldots, x_n]$ and a positive rational number ϵ. The output is an LUR for $\mathcal{P}$ and a set of ϵ-isolating boxes for the roots of $\mathcal{P} = 0$.

S1 Compute a Gröbner basis $\mathcal{G}$ of $\mathcal{P}$ with any order and a monomial basis $\mathbf{B}$ for linear space $\mathcal{A} = \mathbb{Q}[x_1, \ldots, x_n]/(\mathcal{P})$ over $\mathbb{Q}$.
S2 Compute $T_1(t_1)$ as defined in (17) with the method given in Section 3.2; compute a set of ϵ-isolating boxes $\mathcal{B}_1$ for the complex roots of $T_1(t_1) = 0$; set $d_1 = \min\{\mathrm{Dis}(B_1, B_2) \mid B_1, B_2 \in \mathcal{B}_1, B_1 \neq B_2, \}$.
S3 For $i = 1, \ldots, n-1$, do steps **S4-S9**; output the set of boxes (19).
S4 Compute r_{i+1} with the method in Lemma 9. Select a rational number s_i such that condition (8) is valid.
S5 Compute $T_{i+1}(t_{i+1})$ as defined in (17) with the method given in Section 3.2.
S6 Set $\rho_i = s_1 \cdots s_{i-1} d_i$ and compute a set of $\frac{1}{4}\rho_i$-isolating boxes $\mathcal{B}_{i+1}$ for the complex roots of $T_{i+1}(t_{i+1}) = 0$
S7 Set $S_{i+1} = \min\{\mathrm{Dis}(B_1, B_2) \mid B_1, B_2 \in \mathcal{B}_{i+1}, B_1 \neq B_2\}$.
S8 Compute d_{i+1} with formula (27).
S9 Compute ϵ_i with formula (29); refine the isolating boxes $\mathcal{B}_i$ of $T_i(t_i) = 0$ with the precision ϵ_i; still denote the isolating boxes as $\mathcal{B}_i$.

Remark 19. From Lemma 10, the roots of $T_{i+1}(t_{i+1}) = 0$ are in the rectangle $\mathbb{I}_{I_i}$. So, we need only to isolate the roots of $T_i(t_i) = 0$ inside these rectangles. This property is very useful in practice, see Figure 1 for an illustration.

4. Examples

In this section, we will give some examples to illustrate our method.

We first use the following example to show how to isolate the roots of a system with our method. Note that with an LUR, we can also use floating point number type to compute the roots of $\mathcal{P} = 0$ if the floating point numbers can provide the required precision as shown in the following example.

Example 20. Consider the system $\mathcal{P} := [x^2 + y^2 + z^2 - 3, x^2 + 2y^2 - 3z + 1, x + y - z]$. The coordinate order is (x, y, z).

The Gröbner basis $\mathcal{G}$ with the graded reverse lexicographic order $z > y > x$ of $\mathcal{P}$ is:

$$[-x - y + z, x^2 + 2\,yx + 3\,x - 4 + 3\,y, -3\,x + x^2 + 1 - 3\,y + 2\,y^2, 6\,x^3 - 30 + 9\,x^2 + 25\,y + 5\,x].$$

The leading monomials of the basis are $\{z, x\,y, y^2, x^3\}$. So the monomial basis of the quotient algebra $\mathcal{A} = \mathbb{Q}[x_1, ..., x_n]/(\mathcal{P})$ is $\mathbf{B} = [1, x, y, x^2]$.

Let $t_1 = x$, we can compute:

$$M_{t_1} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 2 & -3/2 & -3/2 & -1/2 \\ 5 & -5/6 & -\frac{25}{6} & -3/2 \end{bmatrix}.$$

The minimal polynomial of M_{t_1} is

$$T_1(t_1) = 5 - 60\,t_1 + 6\,t_1^2 + 18\,t_1^3 + 6\,t_1^4.$$

Compute its complex roots with the function "Analytic" in Maple package [RootFinding], we obtain

$$R_1 = [-2.22081423399575 - 1.53519779646152\,\mathrm{i}, -2.22081423399575 \\ +1.53519779646152\,\mathrm{i}, 0.0842270424726020, 1.35740142551890].$$

Computing the roots distance with formula (16), we obtain $d_1 \le 0.6365871918$. We can set

$$d_1 = \frac{1}{2}.$$

In a similar way, we compute M_y and its minimal polynomial $g_2(y) = -29 - 66\,y + 60\,y^2 + 12\,y^4$. The root bound of $g_2(y)$ is 3. So we have $r_2 = 6$. Since $\frac{d_1}{r_2} = \frac{1}{12}$, we set

$$s_1 = \frac{1}{20}.$$

Let $t_2 = x + s_1\,y$. We can compute a matrix M_{t_2} and its minimal polynomial

$$T_2(t_2) = 863337 - 6119640\,t_2 + 360000\,t_2^2 + 1920000\,t_2^3 + 640000\,t_2^4.$$

Computing its complex roots, we have

$$R_2 = [-2.24194942371773 - 1.41342395552762\mathrm{i}, -2.24194942371773 \\ +1.41342395552762\mathrm{i}, 0.143249906267126, 1.34064894116850].$$

Computing the minimal distance between any two roots, we have $S_2 = 0.5986995174$. From equation (27), we can obtain

$$d_2 = \min\{\frac{S_2}{2\,s_1}, \frac{d_1}{2\,s_1}\} = 5.$$

Compute M_z and its minimal polynomial $g_3(z) = 121 - 132z - 36z^2 + 36z^3 + 12z^4$. Then the root bound of $g_3(z)$ is 5. We have $r_3 = 10$. We can set

$$s_2 = \frac{1}{2} \le \frac{d_2}{r_3} = \frac{1}{2}.$$

Let $t_3 = x + s_1\,y + s_1 s_2 z$. Compute M_{t_3} and its minimal polynomial

$$T_3(t_3) = 53294617 - 309903360\,t_3 + 11884800\,t_3^2 + 94464000\,t_3^3 + 30720000\,t_3^4.$$

Computing its complex roots, we have

$$R_3 = [-2.30803737442857 - 1.39091697997219\,\mathrm{i}, -2.30803737442857 \\ +1.39091697997219\,\mathrm{i}, 0.174867014226204, 1.36620773463121].$$

We use $R_1[i]$ to represent the i-th element of R_1. $R_2[i], R_3[i]$ are similarly defined. Since $R_2[1] - R_1[1] = -0.021135190 + 0.121773840\mathrm{i}$ and the absolute values of its real part and imaginary part are lese than $1/2$, $(R_1[1], \frac{R_2[1]-R_1[1]}{s_1})$ is a root of $\mathcal{P} \cap \mathbb{Q}[x, y]$. But $R_2[2] - R_1[1] = -0.021135190 + 2.948621752\mathrm{i}$ and its imaginary part is larger than $1/2$. Then $R_2[2]$ does not correspond to $R_1[1]$. $R_3[1] - R_2[1] = -0.066087950 + 0.022506976\mathrm{i}$ and the absolute values of its real part and imaginary part are lese than $1/4$, so

$$\begin{aligned} &(R_1[1], \frac{R_2[1]-R_1[1]}{s_1}, \frac{R_3[1]-R_2[1]}{s_1 s_2}) \\ = &(-2.22081423399575 - 1.53519779646152\,\mathrm{i}, -0.42270380 + 2.43547680\,\mathrm{i}, \\ &-2.64351800 + 0.90027904\,\mathrm{i}) \end{aligned}$$

is a root of $\mathcal{P} = 0$. In a similar way, we can find all other complex roots of $\mathcal{P} = 0$. And from Theorem 17, we can set $\epsilon_1 = \frac{1}{40}\epsilon, \epsilon_2 = \epsilon_3 = \frac{1}{80}\epsilon$, where ϵ is the given precision. So if we refine the roots of $T_i(t_i) = 0$ to five digits, we can obtain the roots of $\mathcal{P} = 0$ with three digits.

We also obtain an LUR for $\mathcal{P}$ as follows:

$$[[T_1(t_1), T_2(t_2), T_3(t_3)], [s_1, s_2], [d_1, d_2]].$$

The roots of $\mathcal{P} = 0$ are:

$$[(\alpha, 20(\beta - \alpha), 40(\gamma - \beta)) | T_1(\alpha) = 0, T_2(\beta) = 0, T_3(\gamma) = 0, |\beta - \alpha| < 1/2, |\gamma - \beta| < 1/4].$$

Assuming that the final precision for the real roots of the system is $\epsilon = 1/2^{10}$ and isolating the real roots of $T_i(t_i) = 0$ with precision $\epsilon_1 = \frac{1}{40}\epsilon, \epsilon_2 = \epsilon_3 = \frac{1}{80}\epsilon$, respectively, we can obtain the following two real roots of $\mathcal{P} = 0$ with the given precision:

$$[\frac{5519}{65536}, \frac{345}{4096}] \times [\frac{4835}{4096}, \frac{38695}{32768}] \times [\frac{20715}{16384}, \frac{20725}{16384}],\ [\frac{44479}{32768}, \frac{88959}{65536}] \times [\frac{-10985}{32768}, \frac{-5485}{16384}] \times [\frac{16745}{16384}, \frac{16755}{16384}].$$

In the next example, we will compare our method with RUR in Rouillier (1999).

Example 21. Consider the following example from paper Rouillier (1999). $\mathcal{P} := [24\,uz - u^2 - z^2 - u^2z^2 - 13, 24\,yz - y^2 - z^2 - y^2z^2 - 13, 24\,uy - u^2 - y^2 - u^2y^2 - 13]$. The coordinate order is (u, y, z).

The RUR is as follows and its corresponding separating element is $t = x + 2\,y + 4\,z$.

$$f(x) = 0,\ u = \frac{g(u, x)}{g(1, x)},\ y = \frac{g(y, x)}{g(1, x)},\ z = \frac{g(z, x)}{g(1, x)},$$

where

$$
\begin{aligned}
f(x) = {} & x^{16} - 5656\,x^{14} + 12508972\,x^{12} - 14213402440\,x^{10} + 9020869309270\,x^{8} \\
& -3216081009505000\,x^{6} + 606833014754230732\,x^{4} \\
& -51316296630855044152\,x^{2} + 1068130551224672624689, \\
g(1,x) = {} & x^{15} - 4949\,x^{13} + 9381729\,x^{11} - 8883376525\,x^{9} + 4510434654635\,x^{7} \\
& -1206030378564375\,x^{5} + 151708253688557683\,x^{3} - 6414537078856880519\,x, \\
g(u,x) = {} & 116\,x^{14} - 483592\,x^{12} + 784226868\,x^{10} - 634062241592\,x^{8} \\
& +270086313707548\,x^{6} - 58355579408017944\,x^{4} + 5520988105236180668\,x^{2} \\
& -131448117382500870952, \\
g(y,x) = {} & 86\,x^{14} - 418870\,x^{12} + 759804846\,x^{10} - 670485664238\,x^{8} + 307445009725282\,x^{6} \\
& -71012402366579778\,x^{4} + 7099657810552674458\,x^{2} - 168190996202566563226, \\
g(z,x) = {} & 71\,x^{14} - 355135\,x^{12} + 673508751\,x^{10} - 633214359791\,x^{8} + 314815356659869\,x^{6} \\
& -79677638700441717\,x^{4} + 8618491509948092045\,x^{2} - 205956089289536014429.
\end{aligned}
$$

An LUR of $\mathcal{P}$ is as follows:

$$
\begin{aligned}
& [[T_1(t_1), T_2(t_2), T_3(t_3)], [s_1, s_2], [d_1, d_2]] \\
= {} & [[T_1(t_1), T_2(t_2), T_3(t_3)], [1/200, 1/15], [0.2237374734, 2.146554200]],
\end{aligned}
$$

where

$$
\begin{aligned}
T_1(t_1) = {} & 169 - 1820\,{t_1}^{2} + 2622\,{t_1}^{4} - 140\,{t_1}^{6} + {t_1}^{8}, \\
T_2(t_2) = {} & 1203455262760402030898144116 6197 - 13352343881077627453569968 7120000\,{t_2}^{2} \\
& +334257305564156882138712000000000\,{t_2}^{4} - 2564569716120853839360000000000000\,{t_2}^{6} \\
& +2362900554167040000000000000000000\,{t_2}^{8} - 665288908800000000000000000000000\,{t_2}^{10} \\
& +40960000000000000000000000000\,{t_2}^{12}, \\
T_3(t_3) = {} & 3986581248427579228279901745258917340245980989708 01 \\
& -50570450167758092657427376502856962389191187816875 00\,{t_3}^{2} \\
& +18306568462902747682078658662680830721818866699218750\,{t_3}^{4} \\
& -26971016274307991838575084944533427932357788085937500\,{t_3}^{6} \\
& +15563591910271113423505114668403939783573150634765625\,{t_3}^{8} \\
& -19364191550676931999611450263857841491699218750000000\,{t_3}^{10} \\
& +941906342177069262581393122673034667968750000000000\,{t_3}^{12} \\
& -185104815843966230750083923339843750000000000000000\,{t_3}^{14} \\
& +10022595757618546485900878906250000000000000000000\,{t_3}^{16}.
\end{aligned}
$$

And its local separating elements are $t_1 = x, t_2 = x + y/200, t_3 = x + y/200 + z/3000$.

The roots of $\mathcal{P}$ are: $\{(u, y, z) = (\alpha, 200(\beta-\alpha), 3000(\gamma-\beta)) | T_1(\alpha) = 0, T_2(\beta) = 0, T_3(\gamma) = 0, |\beta - \alpha| < 0.2237374734, |\gamma - \beta| < 0.01073277100\}$.

5. Conclusion

We give a new representation, LUR, for the roots of a zero-dimensional polynomial system $\mathcal{P}$ and propose an algorithm to isolate the roots of $\mathcal{P}$ under a given precision ϵ. For the LUR, the roots of the system are represented as a linear combination of the roots of some univariate polynomial equations. The main advantage of LUR is that precision control of the roots of the system is more clear.

The main drawback of the LUR method is that when the parameters s_i becomes very small, the coefficients of $T_i(t_i)$ could become very large, which will slow down the algorithm. To improve the efficiency of the LUR algorithm is our future work. A possible way is to choose proper s_i such that $1/s_i$ in the form of $m\,2^n$, $m > 0$, m, n are integers and the bit size of $m\,2^n$ is as small as possible.

References and Notes

M. E. Alonso, E. Becker, M. F. Roy, and T. Wörmann. Zeros, multiplicities, and idempotents for zerodimensional systems. In *Algorithms in Algebraic Geometry and Applicatiobns*, 1–15. Birkhauser, 1996.

S. Basu, R. Pollack, and M. F. Roy. *Algorithms in Real Algebraic Geometry.* Springer, 2nd edition, 2006.

E. Berbericha, M. Kerbera and M. Sagraloffa, An efficient algorithm for the stratification and triangulation of an algebraic surface, *Computational Geometry* Volume 43, Issue 3, April 2010, Pages 257-278, Special Issue on 24th Annual Symposium on Computational Geometry (SoCG'08).

J. F. Canny. Some algebraic and geometric computation in pspace. In *ACM Symp. on Theory of Computing*, 460–469. SIGACT, 1988.

J. S. Cheng, X. S. Gao, J. Li, Root isolation for bivariate polynomial systems with local generic position method. *Proc. ISSAC 2009*, 103-109, ACM Press, 2009.

J.-S. Cheng, X.-S. Gao, M. Li, Determining the topology of real algebraic surfaces, in: R. Martin, H. Bez, M. Sabin (Eds.), 11 IMA Conference on the Mathematics of Surfaces, in: LNCS, vol. 3604, 2005, pp. 121–146.

J. S. Cheng, X. S. Gao, and C. K. Yap. Complete numerical isolation of real roots in zero-dimensional triangular systems. *Journal of Symbolic Computation*, 44(7): 768–785, 2009.

G. E. Collins and W. Krandick. A tangent-secant method for polynomial complex root calculation. *Proc. ISSAC 1996*, 137-141, ACM Press, 1996.

D. A. Cox. Solving equations via algebras. In *Solving Polnomial Equations*, Editors: Alicia Dichenstein & Ioannis Z. Emiris, Springer, 2005.

D. A. Cox, J. Little, and D. O'Shea. Using algebraic geometry, Second edition, Springer-Verlag, 2004.

I. Z. Emiris, B. Mourrain, and E. P. Tsigaridas. The DMM bound: multivariate (aggregate) separation bounds. In Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation (ISSAC '10). ACM, New York, NY, USA, 243-250.

J. C. Faugère, P. Gianni, d. Lazard, and T. Mora, Efficient computation of zero-dimensional Gröbner basis by changing of order. *Journal of Symbolic Computation*, 16(4): 329-344, 1993.

X. S. Gao and S. C. Chou. On the theory of resolvents and its applications. *Sys. Sci. and Math. Sci.*, 12: 17–30, 1999.

P. Gianni and T. Mora. Algebraic solution of systems of polynomial equations using Groebner bases. *AAECC5*, LNCS 356, 247-257, 1989.

M. Giusti and J. Heintz. Algorithmes - disons rapides -pour la dècomposition d'une varièté algébrique en composantes irréducibles et équidimensionnelles. In *Proc MEGA' 90*, pages 169–193. Birkhäuser, 1991.

M. Giusti, G. Lecerf, and B. Salvy, A Gröbner free alternative for polynomial system solving. *Journal of Complexity*, 17: 154-211, 2001.

J. Keyser, J.M. Rojas and K. Ouchi. The exact rational univariate representation and its application. AMS/DIMACS Volume on Computer Aided Design and Manufacturing. American Mathematical Society/Center for Discrete Mathematics and Computer Science, 2005.

H. Kobayashi, S. Moritsugu, and R. W. Hogan. Solving systems of algebraic equations. *Proc. ISSAC 1988*, 139–149, ACM Press, 1988.

H. Kobayashi, T. Fujise, and A. Furukawa. Solving systems of algebraic equations by a general elimination method. *Journal of Symbolic Computation*, 5(3): 303–320, 1988.

L. Kronecker. Grundzüge einer arithmetischen theorie der algebraischen grössen. *J. Reine Angew. Math.* 92: 1-22,1882.

Y.N. Lakshman and D. Lazard, On the complexity of zero-dimensional algebraic systems. In "Effecitve Methods in Algebraic Geometry," Progess in Mathematics, 94: 217-225, Birkhäuser,Basel, 1991.

D. Lazard. Resolution des Systemes d'Equations Algebriques. *Theoretical Computer Science*, 15: 77-110, 1981.

R. E. Moore. Interval Analysis. Prentice Hall, Englewood Cliffs, NJ, 1966.

A. Neumaier. Interval methods for systems of equations. Cambridge University Press, 1990.

J. R. Pinkert. An exact method for finding the roots of a complex polynomial. *ACM Transactions on Mathematical Software* 2(4): 351-363, 1976.

J. Renegar, On the computaional complexity and geometry of the first-order theoery of the reals. Part I, *Journal of Symbolic Computation*, 13: 255-299, 1992.

F. Rouillier. Solving zero-dimensional systems through the rational univariate representation. *Applicable Algebra in Engineering, Communication and Computing*, 9(5): 433–461, 1999.

F. Rouillier and P. Zimmermann. Efficient isolation of polynomial real roots. *J. of Comp. and App. Math.*, 162(1): 33-50, 2003.

M. Sagraloff and C. K. Yap. An efficient exact subdivision algorithm for isolating complex roots of a polynomial and its complexity analysis. Submitted, Oct. 2009.

B. van der Waerden. Modern Algebra. F. Ungar Publishing Co., New York, 3rd edition, 1950.

H. S. Wilf. A global bisection algorithm for computing the zeros of polynomials in the complex plane. *Journal of the ACM*, 25(3): 415-420, 1978.

C. K. Yap. *Fundamental problems of algorithmic algebra.* Oxford Press, 2000.

K. Yokoyama, M. Noro, and T. Takeshima. Computing primitive elements of extension fields. *Journal of Symbolic Computation*, 8(6): 553–580, 1989.