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 roots of the equation system are represented as linear combinations of roots of several univariate polynomial equations. The main advantage of this representation is that the precision of the roots 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 equation system to a given precision. As a consequence, a root isolation 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 isolation

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 (14) and has been studied extensively in the past twenty years (1; 2; 4; 8; 9; 10; 11; 12; 13; 15; 19; 20; 24). 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 that $t = \sum_i c_i x_i = 0$ takes different values when evaluated at different roots of the polynomial equation system $\mathcal{P} = 0$. 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):

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

[1] Partially supported by a National Key Basic Research Project of China and by a grant from NSFC.

where $f \in \mathbb{Q}[t]$ and $R_i(t)$ are rational functions in t. As a consequence, solving multi-variate equation 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 (20) and the Magma package Kronecker by Giusti, Lecerf, and Salvy (11) are given.

The above approaches still have the following problem: for an isolation interval $[a, b]$ of a real root α of $f(u) = 0$, to determine the isolation 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.

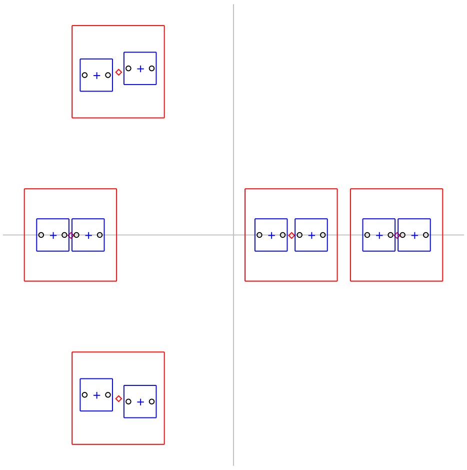

Fig. 1. The distribution of the roots of $T_i(x) = 0 (i = 1, 2, 3)$. The red diamonds (blue crosses, black circles) are roots of $T_1(x) = 0$ ($T_2(x) = 0$, $T_3(x) = 0$) and red (blue) boxes are neighborhoods for the red diamonds (blue crosses).

In the ISSAC paper (3), 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 equation systems with multiple roots. In this paper, we extend the method to solve general zero-dimensional polynomial systems. A local generic position for a polynomial equation system $\mathcal{P} = 0$ is also a linear combination of the variables to be solved: $t = \sum_i c_i x_i$ which satisfies two conditions. First, $t_k = \sum_{i=1}^{k} c_i x_i$ 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 $T_k(t_k) = 0$. Second, for a root $\xi = (\xi_1, \ldots, \xi_k)$ of $\mathcal{P}_k = 0$ represented by a root η of $T_k(t_k) = 0$, all the roots η_j of $T_{k+1}(t_{k+1}) = 0$ corresponding to the roots of $\mathcal{P}_{k+1} = 0$, say $\xi_j = (\xi, \xi_{k+1,j})$, "lifted" from ξ are projected into a fixed square neighborhood of η. This "local" property is illustrated in Figure 1. We prove that if $t_n = \sum_{i=1}^{n} c_i x_i$ is a local generic position for $\mathcal{P}$, then the roots of $\mathcal{P} = 0$ can be be represented as special linear combinations of the roots of univariate equations $T_k(t_k) = 0, k = 1, \ldots, n$:

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

where s_j are certain positive rational numbers and the 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 representation 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 $T_i(x) = 0$ 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 $T_i(x) = 0$ at most once. Another advantage of LUR is that when we isolate the roots of $T_{i+1}(x) = 0$, we need only to consider a fixed neighborhood of each root of $T_i(x) = 0$.

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 separating bounds for the roots of $\mathcal{P}_{k+1} = 0$ lifted from a root of $\mathcal{P}_k = 0$. 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 separating bounds for $\mathcal{P}_k = 0$ are obtained from the isolating boxes for the roots of the $T_k(x) = 0$. 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 $\mathcal{P} = 0$.

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 isolation 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 $\mathbb{Q}[x_1, \ldots, x_n]$, where $\mathbb{Q}$ is the field of rational numbers. Let

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

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 $|c_1 - c_2| \leq |c_1 - c_3| + |c_3 - c_2|$ for any complex number c_3. Let c_0 be a complex number and r a positive rational number.

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

Then the set of points having distance less than r with c_0, that is $\{c_1 \in \mathbb{C} \mid |c_1 - c_0| < r\}$, is an open square with c_0 as the center.

By an LUR, we mean a set like

$$\{T_1(x), \ldots, T_n(x), s_i, d_i, i = 1, \ldots, n-1\}, \tag{2}$$

where $T_i(x) \in \mathbb{Q}[x]$ are univariate polynomials, s_i and d_i are positive rational numbers. The **roots** of (2) are defined to be

$$\begin{aligned}&\{(\alpha_1, \frac{\alpha_2 - \alpha_1}{s_1}, \ldots, \frac{\alpha_n - \alpha_{n-1}}{s_1 \cdots s_{n-1}}) \mid T_i(\alpha_i) = 0, i = 1, \ldots, n \text{ and}\\ &|\alpha_{i+1} - \alpha_i| < s_1 \cdots s_{i-1} d_i, i = 1, \ldots, n-1\}\end{aligned} \tag{3}$$

where $s_0 = 1$. Geometrically, we match a root α_i of $T_i(x) = 0$ with those roots of $T_{i+1}(x) = 0$ inside a squared neighborhood centered at α_i. See Figure 1 for an illustration. An **LUR for** $\mathcal{P}$ is a set of form (2) 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 (2) be an LUR for a polynomial system $\mathcal{P} = 0$. If α_i is a root of $T_i(x) = 0 (1 \le i \le n)$ 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 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 $(i = 1, \ldots, n-1)$ be positive rational numbers satisfying

$$D_i = \min\{\frac{1}{2}|\alpha - \beta|, \forall \eta \in V_{\mathbb{C}}(\mathcal{I}_{i-1}), (\eta, \alpha), (\eta, \beta) \in V_{\mathbb{C}}(\mathcal{I}_i), \alpha \ne \beta\}, \tag{4}$$

$$d_i < \min\{D_i, \frac{d_{i-1}}{2 s_{i-1}}\}, \tag{5}$$

$$r_i > 2 \max\{|\alpha_i|, \forall (\alpha_1, \ldots, \alpha_i) \in V_{\mathbb{C}}(\mathcal{I}_i)\}, \tag{6}$$

$$s_i \le \frac{d_i}{r_{i+1}} \tag{7}$$

where $s_0 = 1, d_0 = +\infty$. 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 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.

For s_i satisfying (7), consider the ideal

$$\bar{\mathcal{I}}_i = (\mathcal{I}_i \cup \{x - x_1 - s_1 x_2 - \cdots - s_1 \cdots s_{i-1} x_i\}), \tag{8}$$

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

$$(\bar{\mathcal{I}}_i) \cap \mathbb{Q}[x] = (T_i(x)). \tag{9}$$

The following is the main result of this paper.

Theorem 2. *If d_i, s_i satisfy conditions (5), (7) and T_i is defined in (9), then the corresponding set (2) is an LUR for $\mathcal{P}$.*

We will prove two lemmas which will lead to a proof for the theorem. For a root η_i of $T_i(x) = 0$, let

$$\mathbb{S}_{\eta_i} = \{\eta \in \mathbb{C} \,|\, |\eta - \eta_i| < \rho_i\}, i = 1, \ldots, n \tag{10}$$

where $\rho_i = s_1 \cdots s_{i-1} d_i, (s_0 = 1)$. Note that $\mathbb{S}_{\eta_i}$ is an open square whose center is η_i and whose edge has length $2\rho_i$. With this notation, the roots of (2) can be written as

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

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

Lemma 3. *Under assumptions of Theorem 2, we have $\mathbb{S}_{\eta_{i+1}} \subset \mathbb{S}_{\eta_i}$,i=1,...,n-1, where $(\xi_1, \ldots, \xi_{i+1}) \in V_{\mathbb{C}}(\mathcal{I}_{i+1})$ and*

$$\eta_i = \xi_1 + s_1\xi_2 + \cdots + s_1 \cdots s_{i-1}\, \xi_i, \tag{12}$$

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

Proof. From the definition of $\bar{\mathcal{I}}_i$ in (8), η_i is a root of $T_i(x) = 0$, η_{i+1} is a root of $T_{i+1}(x) = 0$, and each root of $T_{i+1}(x) = 0$ has the form (13).

We first prove that $\eta_{i+1} \in \mathbb{S}_{\eta_i}$. Using (6) and (7), we have

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

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

We now prove that $\mathbb{S}_{\eta_{i+1}} \subset \mathbb{S}_{\eta_i}$. By (5), 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 $\eta \in \mathbb{S}_{\eta_{i+1}}$, by (14), we have $|\eta - \eta_i| \le |\eta - \eta_{i+1}| + |\eta_{i+1} - \eta_i| < \rho_{i+1} + \frac{1}{2}\rho_i < \rho_i$. Hence $\eta \in \mathbb{S}_{\eta_i}$ and the lemma is proved. ▌

For rational numbers a_j, we call $f_i = \Sigma_{j=1}^{i} a_j x_j$ a **separating element** of $\mathcal{I}_i$, if $\forall \alpha, \beta \in V_{\mathbb{C}}(\mathcal{I}_i)$, $\alpha \ne \beta$ implies $f_i(\alpha) \ne f_i(\beta)$ (see paper (20)).

Theorem 2 follows from (d) of the following lemma.

Lemma 4. *Under assumptions of Theorem 2, for $i = 1, \dots, n$, we have*

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

(b) Each root η_i of $T_i(x) = 0$ is in an $\mathbb{S}_{\eta_{i-1}}$ for a root η_{i-1} of $T_{i-1}(x) = 0$. Furthermore, if $\eta_{i-1} = \xi_1 + s_1 \xi_2 + \cdots + s_1 \cdots s_{i-2}\xi_{i-1}$, then all roots of $T_i(x) = 0$ in $\mathbb{S}_{\eta_{i-1}}$ are of the following form

$$\eta_i = \eta_{i-1} + s_1 \cdots s_{i-1} \xi_i \tag{15}$$

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

(c) $\mathbb{S}_{\eta_i}$ are disjoint for all roots η_i of $T_i(x) = 0$.

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

Proof. We will prove the lemma by induction on $k = i$. For $k = 1$, since $(\mathcal{I}_1) = (T_1(x))$, statements (a) and (d) are obviously true. We do not need prove (b). From (5), 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, $\mathbb{S}_{\eta_1}$ are disjoint for all roots η_1 of $T_1(x) = 0$. Statement (c) is proved.

Suppose that the result is correct 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 $\eta_i = \xi_1 + s_1\xi_2 + \cdots + s_1 \cdots s_{i-1}\xi_i$ 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, $\mathbb{S}_{\eta_i}$ and $\mathbb{S}_{\theta_i}$ are disjoint. By Lemma 3, $\eta_{i+1} = \eta_i + s_1 \cdots s_i\xi_{i+1} \in \mathbb{S}_{\eta_i}$ 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 $\eta_{i+1} \neq \theta_{i+1}$. In the second case, we have $(\xi_1, \dots, \xi_i) = (\beta_1, \dots, \beta_i)$. Then, $\eta_i = \theta_i$ and $\xi_{i+1} \neq \beta_{i+1}$. It is clear that $\eta_{i+1} = \eta_i + s_1 \cdots s_i\xi_{i+1}$ 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 3, we have $\eta_{i+1} \in \mathbb{S}_{\eta_i}$. Then, each root of $T_{i+1}(x) = 0$ is in an $\mathbb{S}_{\eta_i}$ for a root η_i of $T_i(x) = 0$. 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 $\mathbb{S}_{\eta_i}$. 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 η_i. By the induction hypothesis (c), $\mathbb{S}_{\eta_i}$ and $\mathbb{S}_{\theta_i}$ are disjoint which is impossible since by Lemma 3, $\theta_{i+1} \in \mathbb{S}_{\eta_i}$ and $\theta_{i+1} \in \mathbb{S}_{\theta_i}$. Thus, $(\beta_1, \dots, \beta_i) = (\xi_1, \dots, \xi_i)$ and hence $\theta_{i+1} = \eta_i + s_1 \cdots s_i\beta_{i+1}$. This proves equation (15) and hence statement (b).

We now prove statement (c). Use notations in (12) and (13). By Lemma 3, $\mathbb{S}_{\eta_{i+1}} \subset \mathbb{S}_{\eta_i}$. As a consequence, we need only to prove that the squares $\mathbb{S}_{\eta_{i+1}}$ contained in the same $\mathbb{S}_{\eta_i}$ are disjoint. Let η_{i+1}, θ_{i+1} be two roots of $T_{i+1}(x) = 0$ in $\mathbb{S}_{\eta_i}$. By statement (b) just proved, we have

$$\eta_{i+1} = \eta_i + s_1 \cdots s_i\xi_{i+1}, \theta_{i+1} = \eta_i + s_1 \cdots s_i\beta_{i+1}$$

where η_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 (5),

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

So, $\mathbb{S}_{\eta_{i+1}}$ and $\mathbb{S}_{\theta_{i+1}}$ 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 $\eta_j = \xi_1 + s_1\xi_2 + \cdots + s_1 \cdots s_{j-1}\xi_j, j = 1, \dots, i+1$. By the induction hypothesis, we have $(\xi_1, \dots \xi_i) = (\eta_1, \frac{\eta_2 - \eta_1}{s_1}, \dots, \frac{\eta_i - \eta_{i-1}}{s_1 \cdots s_{i-1}})$ where $|\eta_{j+1} - \eta_j| < s_1 \cdots s_{j-1}d_j, j = 1, \dots, i$. Note that the inequality is equivalent to that $\eta_{j+1} \in \mathbb{S}_{\eta_j}$. By (15), we can recover the ξ_{i+1} with the following equation

$$\xi_{i+1} = \frac{\eta_{i+1} - \eta_i}{s_1 \cdots s_i}.$$

From Lemma 3, we have $\eta_{i+1} \in \mathbb{S}_{\eta_i}$ or equivalently $|\eta_{i+1} - \eta_i| < s_1 \cdots s_{i-1} d_i$. Then the root $(\xi_1, \ldots \xi_{i+1}) = (\eta_1, \frac{\eta_2 - \eta_1}{s_1}, \ldots, \frac{\eta_{i+1} - \eta_i}{s_1 \cdots s_i})$ is a root of the LUR $(T_1(x), \ldots, T_{i+1}(x), s_j, d_j, j = 1, \ldots, i)$. We thus proved that the roots of $\mathcal{I}_{i+1}$ are the same as the roots of the LUR and hence statement (d). ▮

We have the following corollaries.

Corollary 5. *If (2) is an LUR for a polynomial system $\mathcal{P}$, then the roots of $\mathcal{I}_i = 0$ are in a one to one correspondence with the roots of $T_i(x) = 0$ for $i = 1, \ldots, n$.*

Proof. Let $\xi = (\xi_1, \ldots, \xi_i) \in V_{\mathbb{C}}(\mathcal{I}_i)$. Then $\eta_i = \xi_1 + s_1\xi_2 + \cdots + s_1 \cdots s_{i-1}\, \xi_i$ is a root of $T_i(x) = 0$. By (a) of Lemma 4, this mapping is injective. This mapping is clearly surjective. ▮

Corollary 6. *The real roots of $\mathcal{P} = 0$ are in a one to one correspondence with the real roots of $T_n(x) = 0$. More precisely, if α_n is a real root of $T_n(x) = 0$, 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 $T_i(x) = 0, i = 1, \ldots, n-1$.*

Proof. For each root η of $T_{i-1}(x) = 0$, let $\mathbb{S}_\eta$ be the open square neighborhood of η defined in (10). We claim that a real root of $T_i(x) = 0$ cannot be in $\mathbb{S}_\eta$ for a complex root η of $T_{i-1}(x) = 0$. Since $T_{i-1}(x)$ has rational numbers as coefficients, the complex roots of $T_{i-1}(x) = 0$ appear as pairs which are symmetric with the real axis and the open square neighborhoods for a pair of complex roots are disjoint. Then the open square neighborhood of any complex root has no intersection with the real axis. This proves the claim. As a consequence, if α_n is a real root of $T_n(x) = 0$, then α_n is in the open square neighborhood of a real root α_{n-1} of $T_{n-1}(x) = 0$. Repeating the process, we obtain a real root $(\alpha_1, \frac{\alpha_2 - \alpha_1}{s_1}, \ldots, \frac{\alpha_n - \alpha_{n-1}}{s_1 \cdots s_{n-1}})$ for $\mathcal{P} = 0$ where all α_i are real numbers. The other side is obvious: a real root of $\mathcal{P} = 0$ will correspond to a real root of $T_n(x) = 0$. ▮

From the lemma, we can consider the real roots of an LUR if we only interest 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 the roots of the system in $\mathbb{C}^n$ at the same time.

3.1. Complex isolation intervals and isolation boxes

We introduce some basic concepts of interval computation. For more details, we refer to (17).

Let $\square\mathbb{Q}$ denote the set of intervals of the form $[a, b]$, where $a \le b \in \mathbb{Q}$. The **length** of an interval $I = [a, b] \in \square\mathbb{Q}$ is defined to be $|I| = b - a$. Assuming $a_1 \le a_2$, we define the distance between two intervals as

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

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 $|\langle I, J\rangle| = \max\{|I|, |J|\}$. 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 **isolation 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 (5; 18; 22; 23).

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 **isolation 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-isolation boxes** of $\mathcal{P} = 0$. The aim of this paper is to compute a set of ϵ-isolation boxes for a zero-dimensional polynomial system $\mathcal{P}$.

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

In this subsection, we will show how to use Gröbner basis to compute r_i defined in (6) and $T_i(x)$ defined in (8) 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

$$\mathbf{B} = \{x_1^{t_1} \cdots x_n^{t_n} | x_1^{t_1} \cdots x_n^{t_n} \text{ is not divisible by the leading term of any element of } \mathcal{G}\}$$

forms a basis of $\mathcal{A}$ as a linear space over $\mathbb{Q}$, where t_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 (16).

Theorem 7 (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 (7) and

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

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

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

In fact, we can construct the matrixes for M_{x_i} and M_x based on $\mathbf{B}$ and $\mathcal{G}$, and $g_i(x_i)$ and $T_i(x)$ are the minimal polynomials for M_{x_i} and M_x, respectively (See reference (6)). Note that we can also use the method introduced in reference (7) to compute $g_i(x_i), T_i(x)$.

From Theorem 7 and (a) of Lemma 4, 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 $x=\sum_{j=1}^{i} s_1\cdots s_{j-1}x_j$ on the roots of $\mathcal{P}=0$ are roots of $T_i(x)=0$.

Now we show how to estimate r_i defined in (6). At first, compute $(g_i(x_i))=(\mathcal{P})\cap\mathbb{Q}[x_i]$. Then we have the following result.

Lemma 8. *Use the notations introduced before. Then*

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

satisfies the condition (6), 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 preparations 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 2.

We define the **isolation boxes** for an LUR defined in (2) 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 isolation boxes for the complex roots of $T_i(x)=0$ and $\rho_i=s_1\cdots s_{i-1}d_i$. In Theorem 16 to be proved below, we will give criteria under which the isolation boxes for $\mathcal{P}$ are the isolation 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-isolation boxes for the roots of $\mathcal{P}=0$ inductively.

At first, consider $i=1$. We compute $T_1(x)$ as defined in equation (17). Let $\mathcal{B}_1$ be a set of isolation intervals for the complex roots of $T_1(x)=0$. 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 $(T_1(x),\ldots,T_i(x),s_j,d_j,j=1,\ldots,i-1)$ for $\mathcal{I}_i$.
- A set of ϵ-isolation boxes for $\mathcal{I}_i$.
- The parameter d_i.

We will show how to compute r_{i+1}, s_i, $T_{i+1}(x)$, d_{i+1}, and a set of ϵ-isolation 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 (6) and (7). With s_i, we can compute $T_{i+1}(x)$ as defined in (17).

Here r_{i+1} can be computed with the method in Lemma 8. Note that d_i is known from the induction hypotheses. Then we can choose a rational number s_i such that condition (7) is valid. Finally, $T_{i+1}(x)$ can be computed with the methods mentioned below equation (17).

Step 2. We are going to compute the isolation 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 isolation intervals for $\xi_{i+1,j}$ with lengths no larger than ϵ, since we already have an ϵ-box for ξ.

Let

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

Then, η_i is a root of $T_i(x) = 0$. By (b) of Lemma 4 the roots θ_j of $T_{i+1}(x) = 0$ correspond to ζ_j are

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

We have

Lemma 9. *Let $I_i = \langle [a, b], [c, d] \rangle$ be an isolation interval for the root η_i of $T_i(x) = 0$ 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 $\mathbb{I}_\eta$ are disjoint for all roots η of $T_i(x) = 0$.

Proof. In Figure 2, let square $ABCD$ be $\mathbb{S}_{\eta_i} = \{\theta \in \mathbb{C} \,|\, |\theta - \eta_i| < \rho_i\}$ and square $A_1B_1C_1D_1 = \{\theta \in \mathbb{C} \,|\, |\theta - \eta_i| < \rho_i/2\}$. By equation (14), we know $|\theta_j - \eta_i| < \frac{1}{2}\rho_i$. 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 $A_3B_3C_3D_3$. 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 $|\theta - \eta_i| \le |\theta - P|$ 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, $\forall \theta \in \mathbb{I}_{I_i}$, $|\theta - \eta_i| \le \frac{3}{4}\rho_i$. Since $\mathbb{S}_{\eta_i}$ is the set of complex numbers satisfying $|\theta - \eta_i| < \rho_i$, we have $\mathbb{I}_{I_i} \subset \mathbb{S}_{\eta_i}$. By (c) of Lemma 4, $\mathbb{S}_{\eta_i}$ are disjoint for all roots of $T_i(x) = 0$. Then $\mathbb{I}_{I_i}$ are disjoint for all roots of $T_i(x) = 0$ too. ▮

The following lemma shows what is the precision needed to isolate the roots of $T_{i+1}(x) = 0$ in order for the isolation boxes to be contained in some $\mathbb{I}_{I_i}$. It can be seen as an effective version of the fact $\eta_{i+1} \in \mathbb{S}_{\eta_i}$ proved in Lemma 3.

Lemma 10. *Use the notations introduced in Lemma 9. Let $\{B_j, j = 1, \ldots, m\}$ be a set of $\frac{1}{4}\rho_i$-isolation boxes for the roots $\theta_j, j = 1, \ldots, m$ of $T_{i+1}(x) = 0$. Then, for all j*

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

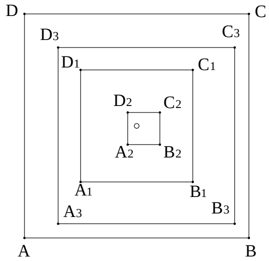

Fig. 2. The isolation intervals I_i, $\mathbb{S}_{\eta_i}$, $\mathbb{I}_{I_i}$ for a root η_i of $T_i(x) = 0$. η_i is represented by $\circ$.

Proof. From the proof of Lemma 9, the distance from η_i to line BC in Figure 2 is ρ_i and the distance from η_i to line B_3C_3 is less than $\frac{3}{4}\rho_i$. So, the distance between line BC and B_3C_3 is at least $\frac{1}{4}\rho_i$. This fact is also valid for the pairs of lines AD/A_3D_3, AB/A_3B_3, and CD/C_3D_3. Since the isolation 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 rectangle $A_2B_2C_2D_2$. Since θ_j is inside both B_j and rectangle $A_3B_3C_3D_3$ and the distance from η_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 $\rho_i/2$. ▌

Isolate the roots of $T_{i+1}(x) = 0$ with precision $\frac{1}{4}\rho_i$. By Lemma 10, all the roots are in one of the intervals $\mathbb{I}_I$ where I is an isolation interval for a root η of $T_i(x) = 0$.

Let $K_j = \langle [p_j, q_j], [g_j, h_j] \rangle (1 \leq j \leq m)$ be the isolation intervals for the roots θ_j of $T_{i+1}(x) = 0$ inside $\mathbb{I}_{I_i}$. Then from (21), the isolation intervals of $\xi_{i+1,j}(1 \leq j \leq m)$ 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 11. *With the notations introduced above, if the following conditions*

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

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

are valid, then $J_{i+1,j}$ defined in (24) are ϵ-isolation 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 $J_{i+1,j}, J_{i+1,k}(1 \leq k \neq j \leq m)$ 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-isolation 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 isolation 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 isolation intervals of the roots η_j, η_k of $T_{i+1}(x) = 0$. Here η_j, η_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 isolation intervals of $T_{i+1}(x)=0$. 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, S_{η_i} is the separation bound for the roots of $T_{i+1}(x)=0$ 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 $T_i(x)=0$.

Remark 12. 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 isolation interval I_i of $T_i(x)=0$ such that inequality (26) is true. After the refinement, all other conditions are still valid. We need to do this kind of refinement only once.

As a consequence of the above lemma, we have

Corollary 13. *Let $\mathbb{B}$ be an ϵ-isolation 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-isolation boxes for the roots ρ_j of $\mathcal{I}_{i+1}=0$, which are lifted from ξ.*

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

Lemma 14. *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 isolation intervals of $T_{i+1}(x)=0$. Then d_{i+1} satisfies conditions (5).

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

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

Therefore, $D_{i+1}=\min_{\eta\in V_{\mathbb{C}}(T_i(x))}\{\frac{S_\eta}{2s_1\cdots s_i}\}$ is the parameter defined in (4), where S_η 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 isolation intervals of $T_{i+1}(x)=0$. Then, the first condition in (5) is satisfied. In order for the second condition in (5) to be satisfied, we also require $d_{i+1}\le\frac{d_i}{2s_i}$. So the lemma is proved. ▮

We can summarize the result as the following theorem which is an interval version of Theorem 2.

Theorem 15. *Let (2) be an LUR such that d_i, r_i, and s_i satisfy (27), (6), and (7) respectively, $\mathcal{B}_i$ the ϵ_i-isolation boxes for the roots of $T_i(x) = 0$, 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-isolation boxes for $\mathcal{P}$.

Proof. We first explain the functions of the inequalities in (28). The first two inequalities in (28) are introduced in (25) to ensure the ϵ precision for the isolation boxes. The third inequality in (28) is introduced in Lemma 9 to ensure $\theta_j \in \mathbb{I}_{I_i}$ and $\mathbb{I}_{I_i}$ are disjoint. The fourth inequality is introduced in Lemma 10 to ensure the isolation intervals of the roots of $T_{i+1}(x) = 0$ are inside their corresponding interval $\mathbb{I}_{I_i}$. The last inequality is introduced in (26) to ensure the recovered isolation boxes of $\mathcal{P}$ are disjoint.

Now the theorem is a consequence of Corollary 13. Here, we give the explicit expression for the isolation 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 Theorems 2 and 15 by giving an explicit formula for ϵ_i.

Theorem 16. *Using the same notations as Theorem 15. 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 $i = 2, ..., n$, $s_0 = 1, s_n = 1$, $S_{n+1} = +\infty$. If we isolate the roots of $T_i(x) = 0$ with precision ϵ_i, then (19) is a set of ϵ-isolation 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 17. *If we compute the last univariate polynomial $T_n(x)$ in the LUR as the characteristic polynomial of M_x, then the multiplicities of the roots of $\mathcal{P} = 0$ are the multiplicities of the corresponding roots of $T_n(x) = 0$.*

Proof. By (a) of Lemma 4, $x = x_1 + s_1\, x_2 + \cdots + s_1 \cdots s_{n-1} x_n$ is a separating element. By Theorem 7, the characteristic polynomial of M_x 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 $\mathcal{P} = \{P_1, \ldots, P_t\}$ 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-isolation boxes for the roots of $\mathcal{P} = 0$.

S1 Compute a Gröbner basis $\mathcal{G}$ of $\mathcal{P}$ with the graded reverse lexicographic 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 $T_1(x)$ as defined in (17) with the method given in Section 3.2; compute a set of ϵ-isolation boxes $\mathcal{B}_1$ for the complex roots of $T_1(x) = 0$; 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 8. Select a rational number s_i such that condition (7) is valid.
S5 Compute $T_{i+1}(x)$ 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 $\frac{1}{4}\rho_i$-isolation boxes $\mathcal{B}_{i+1}$ for the complex roots of $T_{i+1}(x) = 0$
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 isolation boxes $\mathcal{B}_i$ of $T_i(x) = 0$ with precision ϵ_i; still denote the isolation boxes as $\mathcal{B}_i$.

Remark 18. From Lemma 9, the roots of $T_{i+1}(x) = 0$ are in the rectangle $\mathbb{I}_{I_i}$. So, we need only to isolate the roots of $T_i(x) = 0$ 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 numbers to compute the roots of $\mathcal{P} = 0$ if the floating point number can provide the required precision as shown in the following example.

Example 19. 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 $t = x$, we can compute:

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

The minimal polynomial of M_t is

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

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 $d_1 \leq 0.6365871918$. 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 $t = x + s_1\,y$. We can compute a matrix M_t and its minimal polynomial

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

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

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

Let $t = x + s_1\,y + s_1 s_2 z$. Compute M_t and its minimal polynomial

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

Computing its complex roots, we have

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

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 16, 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 $T_i(t) = 0$ 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:

$$[[T_1(t), T_2(t), T_3(t)], [s_1, s_2], [d_1, d_2]].$$

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 $T_i(t) = 0$ 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 (20).

Example 20. Consider the following example from paper (20). $\mathcal{P} := [24\,uz - u^2 - z^2 - u^2z^2 - 13, 24\,yz - y^2 - z^2 - y^2z^2 - 13, 24\,uy - u^2 - y^2 - u^2y^2 - 13]$. The coordinate order is (u, y, z).

The RUR is as follows.

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

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:

$$[[T_1(t), T_2(t), T_3(t)], [s_1, s_2], [d_1, d_2]] = [[T_1(t), T_2(t), T_3(t)], [1/200, 1/15], [0.2237374734, 2.146554200]],$$

where

$$
\begin{aligned}
T_1(t) = {} & 169 - 1820\,t^{2} + 2622\,t^{4} - 140\,t^{6} + t^{8}, \\
T_2(t) = {} & 120345526276040203089814411661970 - 133523438810776274535699687120000\,t^{2} \\
& +33425730556415688213871200000000\,t^{4} - 2564569716120853839360000000000000\,t^{6} \\
& +23629005541670400000000000000000\,t^{8} - 665288908800000000000000000000\,t^{10} \\
& +4096000000000000000000000000000\,t^{12}, \\
T_3(t) = {} & 39865812484275792282799017452589173402459809897080 1 \\
& -5057045016775809265742737650285696238919118781687500\,t^{2} \\
& +18306568462902747682078658662680830721818866699218750\,t^{4} \\
& -26971016274307991838575084944533427932357788085937500\,t^{6} \\
& +15563591910271113423505114668403939783573150634765625\,t^{8} \\
& -19364191550676931999611450263857841491699218750000000\,t^{10} \\
& +94190634217706926258139312267303466796875000000000\,t^{12} \\
& -18510481584396623075008392333984375000000000000000\,t^{14} \\
& +100225957576185464859008789062500000000000000000\,t^{16}.
\end{aligned}
$$

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 much clearer.

The main drawback of the LUR method is that when the parameters s_i becomes very small, the coefficients of $T_i(t)$ could become very large, which will slow down the algorithm. To improve the efficiency of the LUR algorithm is our future work.

References and Notes

[1] 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.

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

[3] 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.

[4] 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.

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

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

[7] 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.

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

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

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

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

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

[13] 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.

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

[15] 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.

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

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

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

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

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

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

[22] 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.

[23] 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.

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