Peer-reviewed version available at Mathematics 2018, 6, 166; doi:10.3390/math6090166

A Heuristic Method for Certifying Isolated Zeros of Polynomial Systems

Jin-San Cheng, Xiaojie Dou
KLMM, Academy of Mathematics and Systems Science
Chinese Academy of Sciences, Beijing, 100190
University of Chinese Academy of Sciences, Beijing, 100190
jcheng@amss.ac.cn, xjdou@amss.ac.cn

Abstract

We construct a real square system related to a given over-determined real system. We prove that the simple real zeros of the over-determined system are the simple real zeros of the related square system and the real zeros of the two systems are one-to-one correspondence with the constraint that the value of the sum of squares of the polynomials in the over-determined system at the real zeros is identically zero. After certifying the simple real zeros of the related square system with the interval methods, we assert that the certified zero is a local minimum of the sum of squares of the input polynomials. If the value of the sum of the squares of the input polynomials at the certified zero is equal to zero, it is a zero of the input system. As an application, we also consider the heuristic verification of the isolated zeros of polynomial systems and their multiplicity structures. Notice that a complex system with complex zeros can be transformed into a real system with real zeros.

Key words: over-determined polynomial system; isolated zeros; minimum point; sum of squares; interval methods.

1 Introduction

Finding zeros of polynomial systems is a fundamental problem in scientific computing. Newton's method is widely used to solve this problem. For a fixed approximate solution of a system, we can use the α-theory [3, 12, 33], the interval methods or the optimization methods [13, 18, 22, 25, 30, 34] to completely determine whether it is related to a zero of the system. However, the α-theory or the interval methods focuses mainly on a simple zero of a square system, that is, a system with n equations and n unknowns.

Some special certifications of a rational solution of rational polynomials with certified sum of squares decompositions are considered [2, 15, 17, 24, 28, 29, 32].

How about singular zeros of a well-constrained polynomial system? Usually, an over-determined system which contains the same zero as a simple one is constructed by introducing new equations. The basic idea is the deflation techniques [1, 6, 7, 9, 10, 26, 27, 35]. In some references [4, 14, 19, 20, 23, 31], new variables are also included. Moreover, some authors verify that a perturbed system possesses an isolated singular solution within a narrow and computed error bound. The multiplicity structures of singular zeros of a polynomial system are also studied [6, 10, 23]. Though it is in a theoretical sense and global sense, the method in [1] provides a sufficient condition that a zero is exactly a zero of a zero-dimensional polynomial system with rational coefficients.

For the deflation methods mentioned above, on one hand, to be a zero of the perturbed systems does not mean being a zero of the input system considering the difference between the two systems; on the other hand, although the over-determined systems without introducing new variables have the same zeros as the input systems, the verification methods, such as the α-theory or the interval methods, could not be used directly on the over-determined systems in general.

In [8], the authors extend the α-theory from well-constrained systems to over-determined systems. A main result about Newton's method given in their paper is Theorem 4 [8], which says that under the condition of $2\alpha_1(g,\zeta) < 1$, where $g = (g_1,\dots,g_m) \in (\mathbb{C}[x_1,\dots,x_n])^m (m \geq n)$, ζ is an attractive fixed point for Newton's method and simultaneously, a strict local minimum for $\|g\|^2 = \sum\limits_{j=1}^{m} \|g_j\|^2$. However, as they stated, whether the attracting fixed points for Newton's method are always local minima of $\|g\|^2$, or the zeros of the input system, is unknown.

In this paper, we consider the problem of certifying the simple real zeros of an over-determined polynomial system. Given $\Sigma = \{f_1,\dots,f_m\} \in (\mathbb{R}[x_1,\dots,x_n])^m (m \geq n)$, we construct a new square system $\Sigma' = \{\frac{\partial f}{\partial x_1},\dots,\frac{\partial f}{\partial x_n}\}$ with $f = \sum\limits_{i=1}^{m} f_i^2$. After transforming the input over-determined system into a square one, we can use both the α-theory and the interval methods to certify its simple zeros. In this paper, we only consider using the interval methods to certify the simple real zeros of the over-determined system. We prove that the simple real zeros of the input system are local minima of the sum of squares of the input polynomials. We also give the condition that the local minimum is a simple zero of the input system.

Let $\mathbb{R}$ be the field of real numbers. Denote $\mathbb{R}[\mathbf{x}] = \mathbb{R}[x_1,\dots,x_n]$ as the polynomial ring. Let $\mathbf{F} = \{f_1,\dots,f_m\} \subset \mathbb{R}[\mathbf{x}]$ be a polynomial system. Let $\mathbf{p} = (p_1,\dots,p_n) \in \mathbb{R}^n$.

The following theorem is our main result of this paper.

Theorem 1. *Let $\Sigma = \{f_1,\dots,f_m\} \subset \mathbb{R}[\mathbf{x}]$ $(m \geq n)$ and $f = \sum\limits_{i=1}^{m} f_i^2$. Then, we have:*

1. *If $\mathbf{p} \in \mathbb{R}^n$ is an isolated simple real zero of Σ, $\mathbf{p}$ is a local minimum of f;*
2. *$\mathbf{p}$ is a simple real zero of Σ if and only if $(\mathbf{p},0)$ is a simple real zero of the square system $\Sigma_r = \{\mathbf{J}_1(f),\dots,\mathbf{J}_n(f), f - r\}$, where $\mathbf{J}_i(f) = \frac{\partial f}{\partial x_i}$ and r is a new variable.*

In the above theorem, we get a necessary and sufficient condition to certify the simple real zeros of the input system Σ by certifying the simple real zeros of the square system Σ_r. Therefore, to certify that $\mathbf{p}$ is a simple real zero of Σ, the key point is verifying that $f(\mathbf{p}) = 0$.

However, it is difficult to decide numerically if a point is a zero of a polynomial. Thus we can not use the necessary and sufficient condition to certify the simple real zeros of Σ by certifying the simple real zeros of Σ_r.

As an alterative, we refine and certify the simple real zeros of Σ by refining and certifying a new square system $\Sigma' = \{\mathbf{J}_1(f), \ldots, \mathbf{J}_n(f)\}$ with the interval methods and get a verified inclusion $\mathbf{X}$, which contains a unique simple real zero $\hat{\mathbf{x}}$ of Σ'. In fact, $\hat{\mathbf{x}}$ is a local minimum of f, which also is a necessary condition for the certification. On one hand, if $f(\hat{\mathbf{x}}) = 0$, by Theorem 1, $(\hat{\mathbf{x}}, 0)$ is a simple real zero of Σ_r, and then $\hat{\mathbf{x}}$ is a simple real zero of Σ. Thus, we certified the input system Σ. On the other hand, if $f(\hat{\mathbf{x}}) \neq 0$, we can only assert that Σ_r has a unique zero in the verified inclusion $\mathbf{X} \times [0, f(\hat{\mathbf{x}})]$, which means we certified the system Σ_r.

As an application of our method, we also give a heuristic method for certifying not only the isolated singular zeros of polynomial systems, but also the multiplicity structures of the isolated singular zeros of polynomial systems.

This paper is an extended version of the CASC'17 conference paper [5].

The paper is organized as below. We will introduce some notations and preliminaries in the next section. In Section 3, we will give a method to show how to transform an over-determined system into a square one. The interval verification method on the obtained square system is considered in Section 4. At last, we give two applications of our method in Section 5.

2 Preliminaries

Let $\mathbb{C}$ be the field of complex numbers. Denote $\mathbb{C}[\mathbf{x}] = \mathbb{C}[x_1, \ldots, x_n]$ as the polynomial ring. Let $\mathbf{F} = \{f_1, \ldots, f_m\} \subset \mathbb{C}[\mathbf{x}]$ be a polynomial system. Let $\mathbf{p} = (p_1, \ldots, p_n) \in \mathbb{C}^n$. $\mathbf{F}(\mathbf{p}) = \mathbf{0}$ denotes that $\mathbf{p}$ is a zero of $\mathbf{F}(\mathbf{x}) = \mathbf{0}$.

Let A be a matrix. Denote A^T as the transpose of A and $\operatorname{rank}(A)$ as the rank of A. Let $Mat(a_{i,j})$ denote the matrix whose i-th row j-th column element is $a_{i,j}$.

Let $\Sigma = \{f_1, \ldots, f_m\} \subset \mathbb{C}[\mathbf{x}]$ be a polynomial system. Denote $\mathbf{J}(\Sigma)$ as the Jacobian matrix of Σ. That is,

$$\mathbf{J}(\Sigma) = \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial x_1} & \cdots & \frac{\partial f_m}{\partial x_n} \end{pmatrix}.$$

For a polynomial $f \in \mathbb{C}[\mathbf{x}]$, let $\mathbf{J}(f)$ denote $(\frac{\partial f}{\partial x_1}, \frac{\partial f}{\partial x_2}, \ldots, \frac{\partial f}{\partial x_n})$, $\mathbf{J}_i(f) = \frac{\partial f}{\partial x_i}$ and $\mathbf{J}_{i,j}(f) = \mathbf{J}_j(\mathbf{J}_i(f)) = \frac{\partial^2 f}{\partial x_j \partial x_i}$. Denote $\Sigma_r = \{\mathbf{J}_1(f), \ldots, \mathbf{J}_n(f), f - r\}$ with $f = \sum_{j=1}^{m} f_j^2$.

We denote the value of a function matrix $A \in \mathbb{C}[\mathbf{x}]^{n \times n}$ at a point $\mathbf{p} \in \mathbb{C}^n$ as $A(\mathbf{p})$. Let $\mathbf{J}(\mathbf{F})(\mathbf{p})$ denote the value of a function matrix $\mathbf{J}(\mathbf{F})$ at a point $\mathbf{p}$, similarly for $\mathbf{J}(f)(\mathbf{p})$.

Definition 2. *An* **isolated solution** *of* $\mathbf{F}(\mathbf{x}) = \mathbf{0}$ *is a point* $\mathbf{p} \in \mathbb{C}^n$ *which satisfies:*

$$\exists\ \varepsilon > 0 : \{\mathbf{y} \in \mathbb{C}^n : \|\mathbf{y} - \mathbf{p}\| < \varepsilon\} \cap \mathbf{F}^{-1}(\mathbf{0}) = \{\mathbf{p}\}.$$

Definition 3. *We call an isolated solution* $\mathbf{p} \in \mathbb{C}^n$ *of* $\mathbf{F}(\mathbf{x}) = \mathbf{0}$ *a* **singular solution** *if and only if*

$$\operatorname{rank}(\mathbf{J}(\mathbf{F})(\mathbf{p})) < n.$$

Else, we call $\mathbf{p}$ *a* **simple solution**.

Definition 4. *A* **stationary point** *of a polynomial function* $f(\mathbf{x}) \in \mathbb{C}[\mathbf{x}]$ *is a point* $\mathbf{p} \in \mathbb{C}^n$*, which satisfies:*

$$\frac{\partial f}{\partial x_i}(\mathbf{p}) = 0,\ \forall\ i = 1, \ldots, n.$$

We can find the following lemma in many undergraduate text books about linear algebra (see Example 7 on page 224 in [21] for example).

Lemma 5. *Let* $A \in \mathbb{R}^{m\times n}$ *be a real matrix with* $m \geq n$ *and* $B = A^T A$*. Then the ranks of* A *and* B *are the same, especially for the case that* A *is of full rank.*

In the following, we will consider the real zeros of the systems with real coefficients. It is reasonable since for a system (m equations and n unknowns) with complex coefficients, we can rewrite the system into a new one with $2\,m$ equations and $2\,n$ unknowns by splitting the unknowns $x_i = x_{i,1} + \mathbf{i}\,x_{i,2}$ and equations $f_j(x_1, \ldots, x_n) = g_{j,1}(x_{1,1}, x_{1,2}, \ldots, x_{n,1}, x_{n,2}) + \mathbf{i}\,g_{j,2}(x_{1,1}, x_{1,2}, \ldots, x_{n,1}, x_{n,2})$, where $\mathbf{i}^2 = -1$, $f_j \in \mathbb{C}[\mathbf{x}], g_{j,1}, g_{j,2} \in \mathbb{R}[\mathbf{x}]$, $j = 1, \ldots, m$, and find out the complex zeros of the original system by finding out the real zeros of the new system.

3 Transforming Over-determined Polynomial Systems into Square Ones

In this section, we will show how to transform an over-determined polynomial system into a square one with their zeros having a one-to-one correspondence, especially for the simple zeros.

By Definition 4, we have the following lemma:

Lemma 6. *Given a polynomial system* $\Sigma = \{f_1, \ldots, f_m\} \subset \mathbb{R}[\mathbf{x}]$ *(*$m \geq n$*). Let* $f = \sum\limits_{i=1}^{m} f_i^2$ *and* $\Sigma' = \{\mathbf{J}_1(f), \mathbf{J}_2(f), \ldots, \mathbf{J}_n(f)\}$*. If* $\mathbf{p} \in \mathbb{R}^n$ *is an isolated real zero of* Σ'*, then* $\mathbf{p}$ *is a stationary point of* f*.*

Lemma 7. *Let* $\Sigma = \{f_1, \ldots, f_m\} \subset \mathbb{R}[\mathbf{x}]$ *(*$m \geq n$*),* $\Sigma' = \{\mathbf{J}_1(f), \mathbf{J}_2(f), \ldots, \mathbf{J}_n(f)\}$ *with* $f = \sum\limits_{i=1}^{m} f_i^2$*. If* $\mathbf{p} \in \mathbb{R}^n$ *is an isolated real zero of* Σ*, then we have:*

1. $\mathbf{p}$ *is an isolated real zero of* Σ'*;*

2. $\mathrm{rank}(\mathbf{J}(\Sigma)(\mathbf{p})) = \mathrm{rank}(\mathbf{J}(\Sigma')(\mathbf{p})$.

Proof. It is clear that $\mathbf{p}$ is an isolated real zero of Σ' providing that $\mathbf{p}$ is an isolated real zero of Σ, since $\mathbf{J}_i(f) = 2\sum_{k=1}^{m} f_k\,\mathbf{J}_i(f_k)$.

To prove the second part of this lemma, we rewrite $\mathbf{J}_i(f)$ as follows.

$$\mathbf{J}_i(f) = 2\,\langle f_1,\dots,f_m\rangle\,\langle \mathbf{J}_i(f_1),\dots,\mathbf{J}_i(f_m)\rangle^T, \tag{1}$$

where $\langle\,\cdot\,\rangle^T$ is the transpose of a vector or a matrix $\langle\,\cdot\,\rangle$. Then

$$\begin{aligned}\mathbf{J}_{i,j}(f) = \mathbf{J}_j(\mathbf{J}_i(f)) = \mathbf{J}_j(2\sum_{k=1}^{m} f_k\,\mathbf{J}_i(f_k)) &= 2\sum_{k=1}^{m}(\mathbf{J}_j(f_k)\mathbf{J}_i(f_k) + f_k\,\mathbf{J}_{i,j}(f_k))\\ &= 2\,\langle \mathbf{J}_j(f_1),\dots,\mathbf{J}_j(f_m)\rangle\,\langle \mathbf{J}_i(f_1),\dots,\mathbf{J}_i(f_m)\rangle^T + 2\sum_{k=1}^{m} f_k\,\mathbf{J}_{i,j}(f_k).\end{aligned} \tag{2}$$

Then the Jacobian matrix of Σ' is

$$\mathbf{J}(\Sigma') = \begin{pmatrix} \mathbf{J}_{1,1}(f) & \dots & \mathbf{J}_{1,n}(f)\\ \vdots & \ddots & \vdots\\ \mathbf{J}_{n,1}(f) & \dots & \mathbf{J}_{n,n}(f)\end{pmatrix} = \mathrm{Mat}(\mathbf{J}_{i,j}(f)).$$

We rewrite

$$\mathrm{Mat}(\mathbf{J}_{i,j}(f)) = 2\,A^TA + 2\,\mathrm{Mat}(\sum_{k=1}^{m} f_k\,\mathbf{J}_{i,j}(f_k)), \tag{3}$$

where

$$A = \begin{pmatrix} \mathbf{J}_1(f_1) & \dots & \mathbf{J}_n(f_1)\\ \vdots & \ddots & \vdots\\ \mathbf{J}_1(f_m) & \dots & \mathbf{J}_n(f_m)\end{pmatrix}$$

is an $m \times n$ matrix which is exactly the Jacobian matrix of Σ, that is, $\mathbf{J}(\Sigma) = A$. Then we have

$$\mathbf{J}(\Sigma')(\mathbf{p}) = 2A(\mathbf{p})^TA(\mathbf{p}). \tag{4}$$

By Lemma 5, the second part of the lemma is true. This ends the proof. □

Remark. In our construction of f and Σ', the degrees of the polynomials almost be doubled compared to the original one. However, to evaluate the Jacobian matrix of Σ', we evaluate the Jacobian matrix of the original system plus m^2n numerical products. One can find it from Eq. (4) in the above proof. In fact, to get $\mathbf{J}(\Sigma')(\mathbf{p})$, we only need to compute $A(\mathbf{p})$, which does not increase our actual computing degree.

As a byproduct, thanks to the doubled degree of the polynomials, our final certified accuracy is also improved in Lemma 11.

The following is the proof of Theorem 1:

Proof. In fact, by fixing the real zero $\mathbf{p}$ as an isolated simple zero in Lemma 7, we have $\mathbf{p}$ is an isolated simple real zero of $\Sigma' = \{\mathbf{J}_1(f), \ldots, \mathbf{J}_n(f)\}$. Since $\mathbf{p}$ is an isolated simple zero of Σ, $A(\mathbf{p})$ is a column full rank matrix. Therefore, it's easy to verify that $\mathbf{J}(\Sigma')(\mathbf{p}) = 2\,A(\mathbf{p})^T A(\mathbf{p})$ is a positive definite matrix. Thus, $\mathbf{p}$ is a local minimum of f and the first part of the theorem is true . Now we consider the second part.

First, it's easy to verify that $\mathbf{p}$ is the real zero of Σ if and only if $(\mathbf{p}, 0)$ is the real zero of Σ_r. With the same method as proving Lemma 7, we can get

$$\operatorname{rank}(\mathbf{J}(\Sigma)(\mathbf{p})) = \operatorname{rank}(\mathbf{J}(\Sigma_r)(\mathbf{p}, 0)) - 1, \tag{5}$$

which means that $\mathbf{J}(\Sigma_r)(\mathbf{p}, 0)$ is of full rank if and only if $\mathbf{J}(\Sigma)(\mathbf{p})$ is of full rank. Thus, $\mathbf{p}$ is an isolated simple zero of Σ if and only if $(\mathbf{p}, 0)$ is an isolated simple zero of Σ_r. The second part is true. We have finished the proof. □

From Theorem 1, we know that the simple real zeros of Σ and Σ_r are in one to one correspondence with the constraint that the value of the sum of squares of the polynomials in Σ at the simple real zeros is identically zero. Thus we can transform an over-determined polynomial system into a square system Σ_r.

We will show a simple example to illustrate the theorem below.

Example 1. *The simple zero* $\mathbf{p} = (0, 0)$ *of the over-determined system* $\Sigma = \{f_1, f_2, f_3\}$ *corresponds to a simple zero of a square system* $\Sigma_r = \{\mathbf{J}_1(f), \mathbf{J}_2(f), f - r\}$*, where* $f = f_1^2 + f_2^2 + f_3^2$ *with*

$$f_1 = x^2 - 2\,y, f_2 = y^2 - x, f_3 = x^2 - 2\,x + y^2 - 2\,y.$$

We can verify simply that $(\mathbf{p}, 0)$ *is a simple zero of* Σ_r*.*

Though the simple real zeros of Σ and Σ_r have a one to one correspondence, it can not be used directly to do certification of the simple zeros of Σ since we can not certify $r = 0$ numerically. But we can certify the zeros of $\Sigma' = \{\mathbf{J}_1(f), \mathbf{J}_2(f), \ldots, \mathbf{J}_n(f)\}$ as an alternative, which is a necessary condition for the certification.

We will discuss it in next section.

4 Certifying Simple Zeros of Over-determined Systems

In this section, we consider certifying the over-determined system with the interval methods. We will prove the same local minimum result as [8].

The classical interval verification methods are based on the following theorem:

Theorem 8. *[18, 22, 30, 31] Let* $\mathbf{f} = (f_1, \ldots, f_n) \in (\mathbb{R}[\mathbf{x}])^n$ *be a polynomial system,* $\tilde{x} \in \mathbb{R}^n$*, real interval vector* $X \in \mathbb{IR}^n$ *with* $\mathbf{0} \in X$ *and real matrix* $R \in \mathbb{R}^{n\times n}$ *be given. Let an interval matrix* $M \in \mathbb{IR}^{n\times n}$ *be given whose i-th row* M_i *satisfies*

$$\{\nabla f_i(\zeta) : \zeta \in \tilde{x} + X\} \subseteq M_i.$$

Denote by I the $n \times n$ identity matrix and assume

$$-R\mathbf{f}(\tilde{x}) + (I - RM)X \subseteq int(X),$$

where $int(X)$ denotes the interior of X. Then, there is a unique $\hat{x} \in \tilde{x} + X$ with $\mathbf{f}(\hat{x}) = \mathbf{0}$. Moreover, every matrix $\tilde{M} \in M$ is nonsingular. In particular, the Jacobian $\mathbf{J}(\mathbf{f})(\hat{x})$ is nonsingular.

About interval matrices, there is an important property in the following theorem.

Theorem 9. *[16] A symmetric interval matrix A^I is positive definite if and only if it is regular and contains at least one positive definite matrix.*

Given an over-determined polynomial system $\Sigma = \{f_1, \ldots, f_m\} \subset \mathbb{R}[\mathbf{x}]$ with an isolated simple real zero, we can compute a related square system

$$\Sigma' = \{\frac{\partial f}{\partial x_1}, \frac{\partial f}{\partial x_2}, \ldots, \frac{\partial f}{\partial x_n}\} \text{ with } f = \sum_{j=1}^{m} f_j^2.$$

Based on Lemma 7, a simple zero of Σ is a simple zero of Σ'. Thus, we can compute the approximate simple zero of Σ by computing the approximate simple zero of Σ'. Using Newton's method, we can refine these approximate simple zeros with quadratic convergence to a relative higher accuracy. Then, we can certify them with the interval method mentioned before and get a verified inclusion $\mathbf{X}$, which possesses a unique certified simple zero of the system Σ' by Theorem 8, denoting as $\hat{\mathbf{x}} \in \mathbf{X}$.

However, even though we get a certified zero $\hat{\mathbf{x}}$ of the system Σ', considering Lemma 6, we cannot say $\hat{\mathbf{x}}$ is a zero of the input system Σ. Because the certified zero $\hat{\mathbf{x}}$ is just a stationary point of f. Considering Theorem 1 and the difference between Σ' and Σ_r, we have the following theorem.

Theorem 10. *Let Σ, Σ', Σ_r, f, $\hat{\mathbf{x}}$ and the interval $\mathbf{X}$ be given as above. Then, we have:*

1. *$\hat{\mathbf{x}}$ is a local minimum of f;*

2. *there exists a verified inclusion $\mathbf{X} \times [0, f(\hat{\mathbf{x}})]$, which possesses a unique simple zero of the system Σ_r. Especially, if $f(\hat{\mathbf{x}}) = 0$, the verified inclusion $\mathbf{X}$ possesses a unique simple zero of the input system Σ.*

Proof. First, it's easy to see that computing the value of the matrix $\mathbf{J}(\Sigma')$ at the interval $\mathbf{X}$ will give a symmetric interval matrix, denoting as $\mathbf{J}(\Sigma')(\mathbf{X})$. By Theorem 8, we know that for every matrix $M \in \mathbf{J}(\Sigma')(\mathbf{X})$, M is nonsingular. Therefore, the interval matrix $\mathbf{J}(\Sigma')(\mathbf{X})$ is regular. Especially, the matrix $\mathbf{J}(\Sigma')(\hat{\mathbf{x}})$, which is the Hessian matrix of f, is full rank and therefore, is positive definite. Thus, $\hat{\mathbf{x}}$ is a local minimum of f. By Theorem 9, we know that $\mathbf{J}(\Sigma')(\mathbf{X})$ is positive definite. Thus, for every point $\mathbf{q} \in \mathbf{X}$, $\mathbf{J}(\Sigma')(\mathbf{q})$ is a positive definite matrix. Considering Theorem 8, it's trivial that for the verified inclusion $\mathbf{X} \times [0, f(\hat{\mathbf{x}})]$, there exists a unique simple zero of the system Σ_r. If $f(\hat{\mathbf{x}}) = 0$, by Theorem 1, the verified inclusion $\mathbf{X}$ of the system Σ' is a verified inclusion of the original system Σ. □

Remarks. 1. In the above proof, we know that for every point $\mathbf{q} \in \mathbf{X}$, $\mathbf{J}(\Sigma')(\mathbf{q})$ is a positive definite matrix.

2. By Theorem 8, we know that there is a unique $\hat{\mathbf{x}} \in \mathbf{X}$ with $\Sigma'(\hat{\mathbf{x}}) = \mathbf{0}$. However, we could not know what the exact $\hat{\mathbf{x}}$ is. According to the usual practice, in actual computation, we will take the midpoint $\hat{\mathbf{p}}$ of the inclusion $\mathbf{X}$ as $\hat{\mathbf{x}}$ and verify whether $f(\hat{\mathbf{p}}) = 0$ or not. Considering the uniqueness of $\hat{\mathbf{x}}$ in $\mathbf{X}$, therefore, if $f(\hat{\mathbf{p}}) = 0$, we are sure that the verified inclusion $\mathbf{X}$ possesses a unique simple zero of the input system Σ. If $f(\hat{\mathbf{p}}) \neq 0$, we can only claim that there is a local minimum of f in the inclusion $\mathbf{X}$ and $\mathbf{X} \times [0, f(\hat{\mathbf{p}})]$ is a verified inclusion for the system Σ_r.

Considering the expression of Σ and f and for the midpoint $\hat{\mathbf{p}}$ of $\mathbf{X}$, we have a trivial result below.

Lemma 11. *Denote* $\epsilon = \max_{j=1}^{m} |f_j(\hat{\mathbf{p}})|$. *Under the conditions of Theorem 10, we have* $|f(\hat{\mathbf{p}})| \leq m\epsilon^2$.

Based on the above idea, we give an algorithm below. In the verification steps, we will apply the algorithm **verifynlss** in INTLAB [31], which is based on Theorem 8, to compute a verified inclusion $\mathbf{X}$ for the related square system Σ'. For simplicity, denote the interval $\mathbf{X} = [\underline{x}_1, \overline{x}_1], \cdots, [\underline{x}_m, \overline{x}_m]$ and the midpoint of $\mathbf{X}$ as $\hat{\mathbf{p}} = [(\underline{x}_1 + \overline{x}_1)/2, \ldots, (\underline{x}_m + \overline{x}_m)/2]$.

Algorithm 1 VSPS : verifying a simple zero of a polynomial system

Input: an over-determined polynomial system $\Sigma := \{f_1, \cdots, f_m\} \subset \mathbb{R}[\mathbf{x}]$ and an approximate simple zero $\tilde{\mathbf{p}} = (\tilde{p}_1, \cdots, \tilde{p}_n) \in \mathbb{R}^n$.

Output: a verified inclusion $\mathbf{X}$ and a small non-negative number.

```
Compute $f$ and $\Sigma'$;
Compute $\tilde{\mathbf{p}}' := \mathbf{Newton}(\Sigma', \tilde{\mathbf{p}})$;
Compute $\mathbf{X} := \mathbf{verifynlss}(\Sigma', \tilde{\mathbf{p}}')$ and $f(\hat{\mathbf{p}})$;
if $f(\hat{\mathbf{p}}) = 0$, then
    return $(\mathbf{X}, 0)$;
else
    return $(\mathbf{X}, f(\hat{\mathbf{p}}))$.
end if
```

The correctness and the termination of the algorithm is obvious by the above analysis.

We give two examples to illustrate our algorithm.

Example 2. *Continue Example 1. Given an approximate zero* $\tilde{\mathbf{p}} = (0.0003528, 0.0008131)$. *Using Newton's method, we will get a higher accuracy approximate zero*

$$\tilde{\mathbf{p}}' = 10^{-11} \cdot (-0.104224090958505, -0.005858368844383).$$

Compute $f = f_1^2 + f_2^2 + f_3^2$ *and* $\Sigma' = \{\mathbf{J}_1(f), \mathbf{J}_2(f)\}$. *After applying the algorithm* **verifynlss** *on* Σ', *we have a verified inclusion:*

$$\mathbf{X} = \begin{pmatrix} [-0.11330049261083, \ 0.11330049261083] \\ [-0.08866995073891, \ 0.08866995073891] \end{pmatrix} \cdot 10^{-321}.$$

Based on Theorem 8, we know that there exists a unique $\hat{\mathbf{x}} \in \mathbf{X}$, s.t. $\Sigma'(\hat{\mathbf{x}}) = \mathbf{0}$.

Let $\Sigma_r = \{\mathbf{J}_1(f), \mathbf{J}_2(f), f - r\}$. By Theorem 1, we can certify the simple zero of Σ by certifying the simple zero of Σ_r theoretically. Considering the difference between Σ' and Σ_r, we check first whether the value of f at some point in the interval $\mathbf{X}$ is zero. According to the usual practice, we consider the midpoint $\hat{\mathbf{p}}$ of $\mathbf{X}$, which equals $(0, 0)$ and further, $f(\hat{\mathbf{p}})$ is zero. Therefore, we are sure that there exists a unique $\hat{\mathbf{x}} = (\hat{x}, \hat{y}) \in \mathbf{X}$, s.t. $\Sigma_r((\hat{\mathbf{x}}, 0)) = \mathbf{0}$ and then, there exists a unique simple zero $(\hat{x}, \hat{y}) \in \mathbf{X}$ of the input system Σ, which means we certified the input system Σ.

Example 3. *Let $\Sigma = \{f_1 = x_1^2 + 3\,x_1x_2 + 3\,x_1x_3 - 3\,x_3^2 + 2\,x_2 + 2\,x_3, f_2 = -3\,x_1x_2 + x_1x_3 - 2\,x_2^2 + x_3^2 + 3\,x_1 + x_2, f_3 = 2\,x_2x_3 + 3\,x_1 - 3\,x_3 + 2, f_4 = -6\,x_2^2x_3 + 2\,x_2x_3^2 + 6\,x_2^2 + 15\,x_2x_3 - 6\,x_3^2 - 9\,x_2 - 7\,x_3 + 6\}$ be an over-determined system. Consider an approximate zero*

$$\tilde{\mathbf{p}} = (-1.29655, 0.47055, -0.91761).$$

Using Newton's method, we get a higher accuracy zero

$$\tilde{\mathbf{p}}' = (-1.296687216045438, 0.470344502045004, -0.917812633399457).$$

Compute

$$f = f_1^2 + f_2^2 + f_3^2 + f_4^2 \text{ and } \Sigma' = \{\mathbf{J}_1(f), \mathbf{J}_2(f), \mathbf{J}_3(f)\}.$$

After applying the algorithm **verifynlss** *on Σ', we have a verified inclusion:*

$$\mathbf{X} = \begin{pmatrix} [-1.29668721603974, & -1.29668721603967] \\ [\quad 0.47034450205107, & 0.47034450205114] \\ [-0.91781263339256, & -0.91781263339247] \end{pmatrix}.$$

Similarly, based on Theorem 8, we know that there exists a unique $\hat{\mathbf{x}} \in \mathbf{X}$, s.t. $\Sigma'(\hat{\mathbf{x}}) = \mathbf{0}$.

Proceeding as in the above example, we consider the midpoint $\hat{\mathbf{p}}$ of $\mathbf{X}$ and compute $f(\hat{\mathbf{p}}) = 3.94 \cdot 10^{-31} \neq 0$. Thus, by Theorem 10, we get a verified inclusion $\mathbf{X} \times [0, f(\hat{\mathbf{p}})]$, which contains a unique simple zero of the system Σ_r. It means that $\mathbf{X}$ may contain a zero of Σ. Even if $\mathbf{X}$ does not contain a zero of Σ, it contains a local minimum of f, which has a minimum value no larger than $f(\hat{\mathbf{p}})$.

5 Two Applications

As an application, we consider certifying isolated singular zeros of over-determined systems heuristically. Generally, dealing with the multiple zeros of polynomial systems directly is difficult. The classical method to deal with the isolated singular zeros of polynomial systems is the deflation technique, which constructs a new system owing the same singular zero as an isolated simple one. Although the deflation method can be used to refine or verify the isolated zero of the original system, it is a pity that the multiplicity information of the isolated zero is missed. In this section, as an application of the method of converting an over-determined system into a square system in previous section, we give a heuristic method for certifying isolated singular zeros of polynomial systems and their multiplicity structures.

5.1 Certifying Isolated Singular Zeros of Polynomial systems

Recently, Cheng et al. [5] propose a new deflation method to reduce the multiplicity of an isolated singular zero of a polynomial system to get a final system, which owns the isolated singular zero of the input system as a simple one. Different from the previous deflation methods, they consider the deflation of isolated singular zeros of polynomial systems from the perspective of linear combination.

In this section, we first give a brief introduction of their deflation method and then, show how our method is applied to certify the isolated singular zeros of the input system in a heuristic way.

Definition 12. *Let $f \in \mathbb{C}[\mathbf{x}]$, $\tilde{\mathbf{p}} \in \mathbb{C}^n$ and a tolerance $\theta > 0$, s.t. $|f(\tilde{\mathbf{p}})| < \theta$. We say f is* θ-**singular** *at $\tilde{\mathbf{p}}$ if*

$$\left| \frac{\partial f(\tilde{\mathbf{p}})}{\partial x_j} \right| < \theta, \forall 1 \leq j \leq n.$$

Otherwise, we say f is θ-**regular** *at $\tilde{\mathbf{p}}$.*

Let $\mathbf{F} = \{f_1, \ldots, f_n\} \subset \mathbb{C}[\mathbf{x}]$ be a polynomial system. $\tilde{\mathbf{p}} \in \mathbb{C}^n$ is an approximate isolated zero of $\mathbf{F} = \mathbf{0}$. Consider a tolerance θ. First, we can compute the polynomials of all $f_i (i = 1, \ldots, n)$, which is θ-regular at the approximate zero $\tilde{\mathbf{p}}$. That's to say, we compute a polynomial set

$$\mathbf{G} = \{\mathbf{d}_{\mathbf{x}}^{\gamma}(f) | \mathbf{d}_{\mathbf{x}}^{\gamma}(f) \text{ is } \theta\text{-regular at } \tilde{\mathbf{p}}, f \in \mathbf{F}\}.$$

Then, put $\mathbf{G}$ and $\mathbf{F}$ together and compute a subsystem $\mathbf{H} = \{h_1, \ldots, h_s\} \subset \mathbf{G} \cup \mathbf{F}$, whose Jacobian matrix at $\tilde{\mathbf{p}}$ has a maximal rank s. If $s = n$, we get the final system $\widetilde{\mathbf{F}}' = \mathbf{H}$. Else, we choose a new polynomial $h \in \mathbf{G} \cup \mathbf{F} \setminus \mathbf{H}$ and compute

$$g = h + \sum_{i=1}^{s} \alpha_i h_i, \ g_j = \frac{\partial h}{\partial x_j}, \ j = 1, \ldots, n,$$

where $\alpha_j, \ j = 1, \ldots, n$ are new introduced variables. Next, we check if

$$\operatorname{rank}(\mathbf{J}(\mathbf{H}, g_1, \ldots, g_n)(\tilde{\mathbf{p}})) = n + s. \tag{6}$$

If (6) holds, we get the final system $\widetilde{\mathbf{F}}' = \mathbf{H} \cup \{g_1, \ldots, g_n\}$. Else, let $\mathbf{H} := \mathbf{H} \cup \{g_1, \ldots, g_n\} \subset \mathbb{C}[\mathbf{x}, \boldsymbol{\alpha}]$ and repeat again until (6) holds.

Now, we give an example to illustrate the above idea.

Example 4. *Consider a polynomial system* $\mathbf{F} = \{f_1 = -\frac{9}{4} + \frac{3}{2}\,x_1 + 2\,x_2 + 3\,x_3 + 4\,x_4 - \frac{1}{4}\,x_1^2, f_2 = x_1 - 2\,x_2 - 2\,x_3 - 4\,x_4 + 2\,x_1x_2 + 3\,x_1x_3 + 4\,x_1x_4, f_3 = 8 - 4\,x_1 - 8\,x_4 + 2\,x_4^2 + 4\,x_1x_4 - x_1x_4^2, f_4 = -3 + 3\,x_1 + 2\,x_2 + 4\,x_3 + 4\,x_4\}$. *Consider an approximate singular zero*

$$\tilde{\mathbf{p}} = (\tilde{p}_1, \tilde{p}_2, \tilde{p}_3, \tilde{p}_4) = (1.00004659, -1.99995813, -0.99991547, 2.00005261)$$

of $\mathbf{F} = \mathbf{0}$ *and the tolerance* $\varepsilon = 0.005$.

First, we have the Taylor expansion of f_3 at $\tilde{\mathbf{p}}$:

$$f_3 = 3 \cdot 10^{-9} - 3 \cdot 10^{-9}(x_1 - \tilde{p}_1) + 0.00010522(x_4 - \tilde{p}_4) + 0.99995341(x_4 - \tilde{p}_4)^2$$
$$-0.00010522(x_1 - \tilde{p}_1)(x_4 - \tilde{p}_4) - (x_1 - \tilde{p}_1)(x_4 - \tilde{p}_4)^2.$$

Consider the tolerance $\theta = 0.05$. Since

$$|f_3(\tilde{\mathbf{p}})| < \theta, \ \left|\frac{\partial f_3}{\partial x_i}(\tilde{\mathbf{p}})\right| < \theta(i = 1, 2, 3, 4), \ \left|\frac{\partial^2 f_3}{\partial x_4^2}(\tilde{\mathbf{p}})\right| > \theta,$$

we get a polynomial

$$\frac{\partial f_3}{\partial x_4} = -8 + 4\,x_1 + 4\,x_4 - 2\,x_1 x_4,$$

which is θ-regular at $\tilde{\mathbf{p}}$. Similarly, by the Taylor expansion of f_1, f_2, f_4 at $\tilde{\mathbf{p}}$, we have that f_1, f_2, f_4 are all θ-regular at $\tilde{\mathbf{p}}$.

Thus, we have

$$\mathbf{G} = \{f_1, f_2, -8 + 4\,x_1 + 4\,x_4 - 2\,x_1 x_4, f_4\}.$$

Compute

$$r = \operatorname{rank}(\mathbf{J}(\mathbf{G})(\tilde{\mathbf{p}}), \varepsilon) = 3.$$

We can choose

$$\mathbf{H} = \{h_1 = f_1, h_2 = f_2, h_3 = -8 + 4\,x_1 + 4\,x_4 - 2\,x_1 x_4\}$$

from $\mathbf{G} \cup \mathbf{F}$. To $h = f_4 \in \mathbf{G} \cup \mathbf{F} \setminus \mathbf{H}$, let

$$g = h + \alpha_1 h_1 + \alpha_2 h_2 + \alpha_3 h_3.$$

By solving a Least Square problem:

$$LeastSquares((\mathbf{J}(\mathbf{H}, h)(\tilde{\mathbf{p}}))^T [\alpha_1, \alpha_2, \alpha_3, -1]^T = 0),$$

we get an approximate value:

$$(\tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{\alpha}_3) = (-1.000006509, -0.9997557989, 0.000106178711).$$

Then, compute

$$\begin{cases} g_1 = \dfrac{\partial g}{\partial x_1} = 3 + \dfrac{3}{2}\alpha_1 + \alpha_2 + 4\alpha_3 - \dfrac{1}{2}\alpha_1 x_1 + 2\alpha_2 x_2 + 3\alpha_2 x_3 + 4\alpha_2 x_4 - 2\alpha_3 x_4, \\ g_2 = \dfrac{\partial g}{\partial x_2} = 2 + 2\alpha_1 - 2\alpha_2 + 2\alpha_2 x_1, \\ g_3 = \dfrac{\partial g}{\partial x_3} = 4 + 3\alpha_1 - 2\alpha_2 + 3\alpha_2 x_1, \\ g_4 = \dfrac{\partial g}{\partial x_4} = 4 + 4\alpha_1 - 4\alpha_2 + 4\alpha_3 + 4\alpha_2 x_1 - 2\alpha_3 x_1, \end{cases}$$

and we get a polynomial set

$$\mathbf{H}' = \{h_1, h_2, h_3, g_1, g_2, g_3, g_4\},$$

which satisfies

$$\operatorname{rank}(\mathbf{J}(\mathbf{H}')(\tilde{\mathbf{p}}, \tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{\alpha}_3), \varepsilon) = 7.$$

Thus, we get the final system $\widetilde{\mathbf{F}}'(\mathbf{x}, \boldsymbol{\alpha}) = \mathbf{H}'$.

In the above example, given a polynomial system $\mathbf{F}$ with an isolated singular zero $\mathbf{p}$, by computing the derivatives of the input polynomials directly or the linear combinations of the related polynomials, we compute a new system $\widetilde{\mathbf{F}}'$, which has a simple zero. However, generally, the final system $\widetilde{\mathbf{F}}'$ do not contain all $f_i (i = 1, \ldots, n)$. Thus, in order to ensure that the simple zero or parts of the simple zero of the square system $\widetilde{\mathbf{F}}'$ really correspond to the isolated singular zero of the original system, we put $\mathbf{F}$ and $\widetilde{\mathbf{F}}'$ together and consider certifying the over-determined system $\mathbf{F} \cup \widetilde{\mathbf{F}}'$ in the following.

Example 5. *Continue with Example 4. we put* $\mathbf{F}$ *and* $\widetilde{\mathbf{F}}'$ *together and get the over-determined system* $\Sigma = \mathbf{F} \cup \widetilde{\mathbf{F}}'$*. According to our method in Section 4, let*

$$f = \sum_{j=1}^{4} f_j^2 + h_3^2 + \sum_{j=1}^{4} g_j^2.$$

Then, we compute

$$\Sigma' = \{\frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_4}, \frac{\partial f}{\partial \alpha_1}, \ldots, \frac{\partial f}{\partial \alpha_3}\} \text{ and } \Sigma_r = \{\Sigma', \ f - r\}.$$

After applying the algorithm **verifynlss** *on* Σ' *at* $(\tilde{\mathbf{p}}, \tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{\alpha}_3)$*, we have a verified inclusion:*

$$\mathbf{X} = \begin{bmatrix} [\ \ 0.99999999999979, & 1.00000000000019] \\ [-2.00000000000060, & -1.99999999999945] \\ [-1.00000000000040, & -0.99999999999956] \\ [\ \ 1.99999999999998, & 2.00000000000002] \\ [-1.00000000000026, & -0.99999999999976] \\ [-1.00000000000022, & -0.99999999999975] \\ [-0.00000000000012, & 0.00000000000010] \end{bmatrix}$$

By Theorem 8, we affirm that there is a unique isolated simple zero $\hat{\mathbf{x}} \in \mathbf{X}$*, s.t.* $\Sigma'(\hat{\mathbf{x}}) = \mathbf{0}$.

Next, as what we do in Example 2 and Example 3, we consider the midpoint $(\hat{\mathbf{p}}, \hat{\boldsymbol{\alpha}})$ *of* $\mathbf{X}$ *and compute* $f(\hat{\mathbf{p}}, \hat{\boldsymbol{\alpha}}) = 4.0133 \cdot 10^{-28}$*. Thus, by Theorem 10, we get a verified inclusion* $\mathbf{X} \times [0, f(\hat{\mathbf{p}}, \hat{\boldsymbol{\alpha}})]$*, which contains a unique simple zero of the system* Σ_r*. It means that* $\mathbf{X}$ *may contain a zero of* Σ*. Even if* $\mathbf{X}$ *does not contain a zero of* Σ*, it contains a local minimum of* f*, which has a minimum value no larger than* $f(\hat{\mathbf{p}}, \hat{\boldsymbol{\alpha}})$*.*

In the above example, we get the verified inclusion $\mathbf{X} \times [0, f(\hat{\mathbf{p}}, \hat{\boldsymbol{\alpha}})]$ of the system Σ_r. Noticing that $f(\hat{\mathbf{p}}, \hat{\boldsymbol{\alpha}}) \neq 0$, according to Theorem 10, we are not sure if the verified inclusion $\mathbf{X}$ contains a unique simple zero of the system Σ. While, considering the value of $f(\hat{\mathbf{p}}, \hat{\boldsymbol{\alpha}})$ is very small, under certain numerical tolerance condition(for example 10^{-25}), we can deem that the verified inclusion $\mathbf{X}$ contains a simple zero of the system Σ. That's to say, we certified the over-determined system Σ and further certified the original system $\mathbf{F}$.

5.2 Certifying the Multiplicity Structures of Isolated Singular Zeros of Polynomial Systems

In recent years, Mourrain et al.[10, 11] propose a new deflation method, which can be used to refine the accuracy of an isolated singular zero and the parameters introduced simultaneously and what's more, the parameters can describe the multiplicity structure at the zero. They also prove that the number of equations and variables in this deflation method depends polynomially on the number of variables and equations of the input system and the multiplicity of the singular zero. However, although they also show that the isolated simple zeros of the extended polynomial system correspond to zeros of the input system, the extended system is usually an over-determined system. Therefore, the problem of knowing the multiplicity structure of the isolated singular zero exactly becomes the problem of solving or certifying the isolated simple zero of the over-determined system.

In this section, we first give a brief introduction of their deflation method and then, show how our method is applied to certify the multiplicity structure of the isolated singular zero of the input system heuristically.

Let $\mathbf{F} = \{f_1, \ldots, f_m\} \subset \mathbb{C}[\mathbf{x}]$. Let $\mathbf{p} = (p_1, \ldots, p_n) \in \mathbb{C}^n$ be an isolated multiple zero of $\mathbf{F}$. Let $I = \langle f_1, \ldots, f_m \rangle$, $\mathfrak{m}_{\mathbf{p}}$ be the maximal ideal at $\mathbf{p}$ and Q be the primary component of I at $\mathbf{p}$ so that $\sqrt{Q} = \mathfrak{m}_{\mathbf{p}}$.

Consider the ring of power series $\mathbb{C}[[\boldsymbol{\partial}_{\mathbf{p}}]] := \mathbb{C}[[\partial_{1,\mathbf{p}}, \ldots, \partial_{n,\mathbf{p}}]]$ and we use the notation for $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$:

$$\boldsymbol{\partial}_{\mathbf{p}}^{\beta}(f) := \partial_{1,\mathbf{p}}^{\beta_1} \cdots \partial_{n,\mathbf{p}}^{\beta_n} = \frac{\partial^{|\beta|} f}{\partial x_1^{\beta_1} \cdots \partial x_n^{\beta_n}}(\mathbf{p}), \text{ for } f \in \mathbb{C}[\mathbf{x}].$$

The deflation method based on the orthogonal primal-dual pairs of bases for the space $\mathbb{C}[\mathbf{x}]/Q$ and its dual $\mathscr{D} \subset \mathbb{C}[\boldsymbol{\partial}]$, which is illustrated in the following lemma.

Lemma 13. *Let* $\mathbf{F}$, $\mathbf{p}$, Q, $\mathscr{D}$ *be as in the above and* δ *be the multiplicity of* $\mathbf{F}$ *at* $\mathbf{p}$. *Then there exists a primal-dual basis pair of the local ring* $\mathbb{C}[\mathbf{x}]/Q$ *with the following properties:*

(a) The primal basis of the local ring $\mathbb{C}[\mathbf{x}]/Q$ *has the form*

$$B := \{(\mathbf{x} - \mathbf{p})^{\alpha_0}, (\mathbf{x} - \mathbf{p})^{\alpha_1}, \ldots, (\mathbf{x} - \mathbf{p})^{\alpha_{\delta-1}}\}.$$

We can assume that $\alpha_0 = 0$ *and that the monomials in* B *are connected to 1. Define the set of exponents in* B

$$E := \{\alpha_0, \ldots, \alpha_{\delta-1}\}.$$

Peer-reviewed version available at *Mathematics* **2018**, *6*, 166; doi:10.3390/math6090166

(b) The unique dual basis $\mathbf{\Lambda} = \{\Lambda_0, \Lambda_1, \ldots, \Lambda_{\delta-1}\} \subset \mathscr{D}$ orthogonal to B has the form:

$$\begin{aligned}
\Lambda_0 &= \boldsymbol{\partial}_{\mathbf{p}}^{\alpha_0} = 1_{\mathbf{p}},\\
\Lambda_1 &= \frac{1}{\alpha_1!}\boldsymbol{\partial}_{\mathbf{p}}^{\alpha_1} + \sum_{\substack{|\beta|<|\alpha_1|\\ \beta\notin E}} \nu_{\alpha_1,\beta}\frac{1}{\beta!}\boldsymbol{\partial}_{\mathbf{p}}^{\beta},\\
&\vdots\\
\Lambda_{\delta-1} &= \frac{1}{\alpha_{\delta-1}!}\boldsymbol{\partial}_{\mathbf{p}}^{\alpha_{\delta-1}} + \sum_{\substack{|\beta|<|\alpha_{\delta-1}|\\ \beta\notin E}} \nu_{\alpha_{\delta-1},\beta}\frac{1}{\beta!}\boldsymbol{\partial}_{\mathbf{p}}^{\beta},
\end{aligned}$$

The above lemma says that once given a primal basis B of the local ring $\mathbb{C}[\mathbf{x}]/Q$, there exists a unique dual basis $\mathbf{\Lambda}$, which can be used to determine the multiplicity structure of $\mathbf{p}$ in $\mathbf{F}$ and further the multiplicity δ of $\mathbf{p}$, orthogonal to B. Based on the known primal basis B, Mourrain et.al construct the following parametric multiplication matrices, which can be used to determine the coefficients of the dual basis $\mathbf{\Lambda}$.

Definition 14. *Let B as defined in Lemma 13 and denote the exponents in B by $E := \{\alpha_0, \ldots, \alpha_{\delta-1}\}$ as above. Let*

$$E^+ := \bigcup_{i=1}^{n}(E + \mathbf{e}_i)$$

with $E + \mathbf{e}_i = \{(\gamma_1, \ldots, \gamma_i + 1, \ldots, \gamma_n) : \gamma \in E\}$ and we denote $\partial(E) = E^+ \setminus E$. We define an array $\boldsymbol{\mu}$ of length $n\delta(\delta-1)/2$ consisting of 0's, 1's and the variables $\mu_{\alpha_i,\beta}$ as follows: for all α_i, $\alpha_k \in E$ and $j \in \{1, \ldots, n\}$ the corresponding entry is

$$\mu_{\alpha_i,\alpha_l+\mathbf{e}_j} = \begin{cases} 1, & if\ \alpha_i = \alpha_k + \mathbf{e}_j\\ 0, & if\ \alpha_k + \mathbf{e}_j \in E,\ \alpha_i \neq \alpha_k + \mathbf{e}_j\\ \mu_{\alpha_i,\alpha_l+\mathbf{e}_j}, & if\ \alpha_k + \mathbf{e}_j \notin E. \end{cases}$$

The parametric multiplication matrices corresponding to E are defined for $i = 1, \ldots, n$ by

$$\mathtt{M}_i^t(\boldsymbol{\mu}) := \begin{array}{|ccccc|} 0 & \mu_{\alpha_1,\mathbf{e}_i} & \mu_{\alpha_2,\mathbf{e}_i} & \cdots & \mu_{\alpha_{\delta-1},\mathbf{e}_i}\\ 0 & 0 & \mu_{\alpha_2,\alpha_1+\mathbf{e}_i} & \cdots & \mu_{\alpha_{\delta-1},\alpha_1+\mathbf{e}_i}\\ \vdots & \vdots & & & \vdots\\ 0 & 0 & 0 & \cdots & \mu_{\alpha_{\delta-1},\alpha_{\delta-2}+\mathbf{e}_i}\\ 0 & 0 & 0 & \cdots & 0 \end{array}.$$

Definition 15. *(Parametric normal form). Let $\mathbb{K} \subset \mathbb{C}$ be a field. We define*

$$\begin{aligned}
\mathcal{N}_{z,\boldsymbol{\mu}} : \mathbb{K}[\mathbf{x}] &\longrightarrow \mathbb{K}[\mathbf{z}, \boldsymbol{\mu}]^{\delta}\\
f &\longmapsto \mathcal{N}_{\mathbf{z},\boldsymbol{\mu}}(f) := f(\mathbf{z} + \mathtt{M}(\boldsymbol{\mu}))[1] = \sum_{\gamma\in\mathbb{N}^n}\frac{1}{\gamma!}\boldsymbol{\partial}_{\mathbf{z}}^{\gamma}(f)\mathtt{M}(\boldsymbol{\mu})^{\gamma}[1].
\end{aligned}$$

where $[1] = [1, 0, \ldots, 0]$ is the coefficient vector of 1 in the basis B.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 July 2018 doi:10.20944/preprints201807.0271.v1

Peer-reviewed version available at *Mathematics* **2018**, *6*, 166; doi:10.3390/math6090166

Based on the above lemma and definitions, the multiplicity structure are characterized by polynomial equations in the following theorem.

Theorem 16. *[11] Let $\mathbb{K} \subset \mathbb{C}$ be any field, $\mathbf{F} \subset \mathbb{K}[\mathbf{x}]$, and let $\mathbf{p} \in \mathbb{C}^n$ be an isolated zero of $\mathbf{F}$. Let Q be the primary ideal at $\mathbf{p}$ and assume that B is a basis for $\mathbb{K}[\mathbf{x}]/Q$ satisfying the conditions of Lemma 13. Let $E \subset \mathbb{N}^n$ be as in Lemma 13 and $\mathtt{M}_i(\boldsymbol{\mu})$ for $i = 1, \ldots, n$ be the parametric multiplication matrices corresponding to E as in Definition 14 and $\mathcal{N}_{\mathbf{z},\boldsymbol{\mu}}$ be the parametric form as in Definition 15. Then $(\mathbf{z}, \boldsymbol{\mu}) = (\mathbf{p}, \boldsymbol{\nu})$ is an isolated zero with multiplicity one of the polynomial system in $\mathbb{K}[\mathbf{z}, \boldsymbol{\mu}]$:*

$$\begin{cases} \mathcal{N}_{\mathbf{z},\boldsymbol{\mu}}(f_k) = 0, \ \ for\ k = 1, \ldots, m, \\ \mathtt{M}_i(\boldsymbol{\mu}) \cdot \mathtt{M}_j(\boldsymbol{\mu}) - \mathtt{M}_j(\boldsymbol{\mu}) \cdot \mathtt{M}_i(\boldsymbol{\mu}) = 0, \ \ for\ i, j = 1, \ldots, n. \end{cases} \tag{7}$$

The second equation of (7) gives a pairwise commutation relationship of the parametric multiplication matrices. What's more, Theorem 16 makes sure that Equation (7) has an isolated zero $(\mathbf{p}, \boldsymbol{\nu})$ of multiplicity one. Thus, it can be used to deflate the isolated zero $\mathbf{p}$ of the input system $\mathbf{F}$ and simultaneously determine the multiplicity structure of $\mathbf{p}$.

Now, we show an example to illustrate how their method works.

Example 6. *Let $\mathbf{F} = \{f_1 = x_1 + x_2 + x_1^2, f_2 = x_1 + x_2 + x_2^2\}$ be a polynomial system with an 3-fold isolated zero $\mathbf{p} = (0, 0)$. Given the primal basis $B = \{1, x_1, x_1^2\}$, which satisfies the properties of Lemma 13, we can compute the parametric multiplication matrices:*

$$\mathtt{M}_1^t(\boldsymbol{\mu}) = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \ \mathtt{M}_2^t(\boldsymbol{\mu}) = \begin{bmatrix} 0 & \mu_1 & \mu_2 \\ 0 & 0 & \mu_3 \\ 0 & 0 & 0 \end{bmatrix}.$$

Thus, Equation (7) generates the following polynomials:

1). $\mathcal{N}(f_1) = 0$ gives the polynomials $x_1 + x_2 + x_1^2, \ 1 + 2x_1 + \mu_1, \ 1 + \mu_2$;

2). $\mathcal{N}(f_2) = 0$ gives the polynomials $x_1 + x_2 + x_2^2, \ 1 + (1 + 2x_2)\mu_1, \ (1 + 2x_2)\mu_2 + \mu_1\mu_3$;

3). $\mathtt{M}_1\mathtt{M}_2 - \mathtt{M}_2\mathtt{M}_1 = 0$ gives the polynomial $\mu_3 - \mu_1$.

Furthermore, Theorem 16 promises that $(\mathbf{p}, \nu_1, \nu_2, \nu_3)$ is an isolated zero with multiplicity one of the system $\mathbf{F}' = \{f_1, \ f_2, \ 1 + 2x_1 + \mu_1, \ 1 + \mu_2, \ 1 + (1 + 2x_2)\mu_1, \ (1 + 2x_2)\mu_2 + \mu_1\mu_3, \ \mu_3 - \mu_1\}$.

On one hand, from the above example, we can see that given a polynomial system $\mathbf{F}$ with an isolated zero $\mathbf{p}$, by Theorem 16, we will get an extended system $\mathbf{F}' \subset \mathbb{C}[\mathbf{x}, \boldsymbol{\mu}]$, which owns an isolated zero $(\mathbf{p}, \boldsymbol{\nu})$ with multiplicity one. What's more, by Lemma 13, we have the dual basis

$$\boldsymbol{\Lambda} = \{1, \ \partial_1 + \nu_1\partial_2, \ \frac{1}{2}\partial_1^2 + \nu_2\partial_2 + \nu_3\partial_1\partial_2 + \frac{1}{2}\nu_1\nu_3\partial_2^2\},$$

which corresponds to the primal basis $B = \{1, \ x_1, \ x_1^2\}$.

On the other hand, it is not hard to see that Equation (7) defined in Theorem 16 usually gives an over-determined extended system $\mathbf{F}'$. Once given an approximate zero $(\tilde{\mathbf{p}}, \tilde{\boldsymbol{\nu}})$, as what the authors say in Corollary 4.12 in [23], we can use random linear combinations of the polynomials in $\mathbf{F}'$ to produce a square system, which will have a simple zero at $(\mathbf{p}, \boldsymbol{\nu})$ with high probability. Furthermore, Newton's method can be used on this square system to refine $(\tilde{\mathbf{p}}, \tilde{\boldsymbol{\nu}})$ to a higher accuracy. However, this operation can only return an approximate multiplicity structure of the input system $\mathbf{F}$ with a higher accuracy. Next, we consider employing our certification method to certify the multiplicity structure of $\mathbf{F}$.

Example 7. *Continue to consider Example 6. Let* $\Sigma = \mathbf{F}' = \{f_1,\ f_2,\ g_1 = 1 + 2x_1 + \mu_1,\ g_2 = 1 + \mu_2,\ g_3 = 1 + (1 + 2x_2)\mu_1,\ g_4 = (1 + 2x_2)\mu_2 + \mu_1\mu_3,\ g_5 = \mu_3 - \mu_1\}$. *Given an approximate zero*

$$(\tilde{\mathbf{p}}, \tilde{\boldsymbol{\nu}}) = (0.15, 0.12, -1.13, -1.32, -1.47).$$

By Algorithm 1, with Newton's method, we will get a higher accuracy zero

$$(\tilde{\mathbf{p}}', \tilde{\boldsymbol{\nu}}') = (0.000000771, 0.000001256, -1.000002523, -1.000000587, -1.000001940).$$

Then, let

$$f = f_1^2 + f_2^2 + \sum_{j=1}^{5} g_j^2$$

and compute

$$\Sigma' = \{\mathbf{J}_1(f), \mathbf{J}_2(f), \mathbf{J}_{\mu_1}(f), \mathbf{J}_{\mu_2}(f), \mathbf{J}_{\mu_3}(f)\}.$$

After applying the algorithm **verifynlss** *on* Σ' *at* $(\tilde{\mathbf{p}}', \tilde{\boldsymbol{\nu}}')$, *we have a verified inclusion:*

$$\mathbf{X} = \begin{pmatrix} [-0.00000000000001, & 0.00000000000001] \\ [-0.00000000000001, & 0.00000000000001] \\ [-1.00000000000001, & -0.99999999999999] \\ [-1.00000000000001, & -0.99999999999999] \\ [-1.00000000000001, & -0.99999999999999] \end{pmatrix}.$$

Based on Theorem 8, we know that there exists a unique $(\hat{\mathbf{x}}, \hat{\boldsymbol{\mu}}) \in \mathbf{X}$, *s.t.* $\Sigma'(\hat{\mathbf{x}}, \hat{\boldsymbol{\mu}}) = \mathbf{0}$.

Similarly, as what we do in Example 2 and Example 3, we consider the midpoint $(\hat{\mathbf{p}}, \hat{\boldsymbol{\nu}})$ *of* $\mathbf{X}$ *and compute* $f(\hat{\mathbf{p}}, \hat{\boldsymbol{\nu}}) = 0$. *Thus, by Theorem 10, we are sure that there exists a unique simple zero* $(\hat{x}_1, \hat{x}_2, \hat{\boldsymbol{\nu}}_1, \hat{\boldsymbol{\nu}}_2, \hat{\boldsymbol{\nu}}_3)$ *of the input system* Σ *in the interval* $\mathbf{X}$, *which means we certified the input system* Σ.

According to the analysis in the above example, we know that after applying our Algorithm 1 on the extended system $\Sigma = \mathbf{F}'$, we get a verified inclusion $\mathbf{X}$, which possesses a unique simple zero of $\mathbf{F}'$. Noticing that the values of the variables μ_1, μ_2, μ_3 in $\mathbf{F}'$ determine the coefficients of the dual basis $\boldsymbol{\Lambda}$, thus, certifying the extended system $\mathbf{F}'$ means certifying the multiplicity structure of the input system $\mathbf{F}$ at $\mathbf{p}$. So, by Theorem 10, as long as $f(\hat{\mathbf{x}}, \hat{\boldsymbol{\mu}}) = 0$, we are sure that we certified not only the isolated singular zero of the input system $\mathbf{F}$, but also its multiplicity structure.

Acknowledgement

The work is partially supported by NSFC Grants 11471327.

References

[1] Akogul, T. A.; Hauenstein, J. D.; Szanto, A. Certifying solutions to overdetermined and singular polynomial systems over $\mathbb{Q}$, J. Symb. Comput.,2018, 84:147-171.

[2] Allamigeon, X.; Gaubert, S.; Magron, V.; Werner. B. Formal proofs for nonlinear optimization. Journal of Formalized Reasoning. 2015, 8(1).

[3] Blum, L.; Cucker, F.; Shub, M.; Smale, S. Complexity and real computation. Springer-Verlag, New York, 1998.

[4] Dayton, B.; Li, T.; Zeng, Z. Multiple zeros of nonlinear systems, *Mathematics of Computation*, 2011, 80: 2143–2168.

[5] Cheng, J.S.; Dou, X. Certifying simple zeros of over-determined polynomial systems, In: Gerdt V, Koepf W, Seiler W et al. (eds) Computer Algebra in Scientific Computing. CASC'17. Lecture Notes in Computer Science,2017, pp. 55-76.

[6] Dayton, B.; Zeng, Z. Computing the multiplicity structure in solving polynomial systems, in Proceedings of the 2005 International Symposium on Symbolic and Algebraic Computation, M. Kauers, ed., ISSAC 05, New York, NY, USA, ACM, 2005, pp. 116–123.

[7] Giusti, M.; Lecerf, G.; Salvy, B.; Yakoubsohn, J.-C. On location and approximation of clusters of zeros: case of embedding dimension one, *Foundations of Computational Mathematics*,2007, 7: 1–58.

[8] Dedieu, J.P.; Shub, M. Newton's method for overdetermined systems of equations. *Mathematics of Computation*, 1999 , 69(231): 1099-1115.

[9] Hauenstein, J. D.; Wampler, C. W. Isosingular sets and deflation. *Foundations of Computational Mathematics*, 2013, 13(3): 371–403.

[10] Hauenstein, J. D.; Mourrain, B.; Szant, A. Certifying isolated singular points and their multiplicity structure, In Proceedings of the Twenty-first International Symposium on Symbolic and Algebraic Computation, ISSAC' 15, 2015, 213–220.

[11] Hauenstein, J. D.; Mourrain, B.; Szanto, A. On deflation and multiplicity structure. J. Symb. Comput., 2017, 83:228-253.

[12] Hauenstein, J. D.; Sottile, F. Algorithm 921: alphaCertified: Certifying Solutions to Polynomial Systems, *ACM Transactions on Mathematical Software*, 2012, Volume 38 Issue 4.

[13] Kanzawa, Y.; Kashiwagi, M.; Oishi, S. An algorithm for finding all solutions of parameter-dependent nonlinear equations with guaranteed accuracy. *Electronics and Communications in Japan (Part III: Fundamental Electronic Science)*, 1999, 82(10): 33–39.

[14] Kanzawa, Y.; Oishi, S. Approximate singular solutions of nonlinear equations and a numerical method of proving their existence. Sūrikaisekikenkyūsho Kōkyūroku, 1997, (990): 216-223. *Theory and application of numerical calculation in science and technology*, II (Japanese) (Kyoto, 1996).

[15] Kaltofen, E.; Li, B.; Yang, Z.; Zhi, L. Exact certification of global optimality of approximate factorizations via rationalizing sums-of-squares with floating point scalars. In Proceedings of the Twenty-first International Symposium on Symbolic and Algebraic Computation, ISSAC 08, 2008, pp. 155–164, New York, NY, USA, ACM.

[16] Rohn, J. Positive definiteness and stability of interval matrices, *SIAM Journal on Matrix Analysis and Applications*, 1994, 15, 175-184.

[17] Kaltofen, E.L.; Li, B.; Yang, Z.; Zhi, L. Exact certification in global polynomial optimization via sums-of-squares of rational functions with rational coefficients. *Journal of Symbolic Computation*, 2012, 47(1): 1–15.

[18] Krawczyk, R. Newton-Algorithmen zur Bestimmung von Nullstellen mit Fehlherschranken, Computing, 1969, 4: 247–293.

[19] Leykin, A.; Verschelde, J.; Zhao, A. Newton's method with deflation for isolated singularities of polynomial systems. *Theoretical Computer Science*, 2006, 359: 111–122.

[20] Li, N.; Zhi, L. Verified Error Bounds for Isolated Singular Solutions of Polynomial Systems. *SIAM J. Numerical Analysis* 2014, 52(4): 1623–1640.

[21] Li, S. Linear Algebra, Higher Education Press, 2006, ISBN 978-7-04-019870-6.

[22] Moore, R.E. A test for existence of solutions to nonlinear systems, SIAM Journal on Numerical Analysis, 1977, 14: 611-615.

[23] Mantzaflaris, A.; Mourrain, B. Deflation and certified isolation of singular zeros of polynomial systems. In *Proc. ISSAC 2011*, 2011, 249-256.

[24] Monniaux, D.; Corbineau, P. On the generation of positivstellensatz witnesses in degenerate cases. In M. van Eekelen, H. Geuvers, J. Schmaltz, and F. Wiedijk, editors, Interactive Theorem Proving, LNCS 6898, 2011, 249–264. Springer Berlin Heidelberg.

[25] Nakaya, Y.; Oishi, S.; Kashiwagi, M.; Kanzawa, Y. Numerical verification of nonexistence of solutions for separable nonlinear equations and its application

to all solutions algorithm. *Electronics and Communications in Japan (Part III: Fundamental Electronic Science)*, 2003 , 86(5): 45–53.

[26] Ojika, T. A numerical method for branch points of a system of nonlinear algebraic equations, *Applied Numerical Mathematics*,1988, 4: 419–430.

[27] Ojika, T.; Watanabe, S.; Mitsui, T. Deflation algorithm for the multiple roots of a system of nonlinear equations, *Journal of Mathematical Analysis and Applications*, 1983, 96: 463–479.

[28] Peyrl, H.; Parrilo, P.A. A Macaulay2 package for computing sum of squares decompositions of polynomials with rational coefficients. *In Proceeding of SNC 2007*, 2007, pp. 207–208.

[29] Peyrl, H.; Parrilo, P.A. Computing sum of squares decompositions with rational coefficients. *Theoretical Computer Science*, 2008, 409(2): 269–281.

[30] Rump, S.M. Solving algebraic problems with high accuracy, *Proc. of the symposium on A new approach to scientific computation*,1983, pp 51–120, Academic Press Professional, Inc., San Diego, CA, USA.

[31] Rump, S.M.; Graillat, S. Verified error bounds for multiple roots of systems of nonlinear equations. *Numerical Algorithms*,2010, 54(3): 359–377.

[32] Safey, M.; Din, El; Zhi, L. Computing rational points in convex semialgebraic sets and sum of squares decompositions. *SIAM Journal on Optimization*, 2010, 20(6): 2876–2889.

[33] Smale, S. Newton's Method Estimates from Data at One Point, in : The Merging of Disciplines : New Directions in Pure, *Applied and Computational Mathematics*, R. Ewing, K. Gross, C. Martin Eds., Springer 1986.

[34] Yamamura, K.; Kawata, H.; Tokue, A. Interval solution of nonlinear equations using linear programming. *BIT Numerical Mathematics*, 1998, 38(1): 186–199.

[35] Zeng, Z. Computing multiple roots of inexact polynomials. *Mathematics of Computation*, 2005, 74: 869–903.