Journal of Algebra 417 (2014) 72–94

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

An improved algorithm for deciding semi-definite polynomials

Shuijing Xiao [a], Xiaoning Zeng [b], Guangxing Zeng [a,*]

[a] *Department of Mathematics, Nanchang University, Nanchang 330031, China*
[b] *Department of Mathematics, Guangdong University of Eduction, Guangzhou 510303, China*

ARTICLE INFO

Article history:
Received 13 April 2013
Available online 16 July 2014
Communicated by Gerhard Hiss

Keywords:
Semi-definite polynomial
Semi-algebraic subset
Triangular decomposition
Regular chain
Transfer principle

ABSTRACT

In this paper, a new algorithm is presented for deciding the semi-definiteness of multivariate polynomials with coefficients in a computable ordered field, which admits an effective method of finding an isolating set for every non-zero univariate polynomial. This algorithm is an improvement of the method presented in Ref. [24]. The technique in this paper is to compute triangular decompositions of polynomial systems into regular chains.

1. Introduction

In the computational real algebraic geometry, the decision of semi-definite polynomials is an important topic, which is closely related to many areas, e.g. polynomial optimization, automated theorem proving in ordered geometry, control theory and the study of inequalities.

Let $(K, \leq)$ be a computable ordered field with real closure R, and $K[x_1, \ldots, x_n]$ the ring of polynomials in n variables over K. For a non-zero $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$,

* Corresponding author.
E-mail addresses: xiaoshjing@163.com (S. Xiao), zxn@gdei.edu.cn (X. Zeng), zenggx@ncu.edu.cn (G. Zeng).

http://dx.doi.org/10.1016/j.jalgebra.2014.06.021
0021-8693/

we say that f is positive (respectively negative) semi-definite on R if $f(a_1,\ldots,a_n) \geq 0$ (respectively $f(a_1,\ldots,a_n) \leq 0$) for any $a_1,\ldots,a_n \in R$. The decision of semi-definite polynomials is just to devise an algorithm for deciding whether or not a given polynomial is positive semi-definite.

The decision of semi-definite polynomials has been studied extensively by many researchers (for example, see [3,6,7,14]). In Ref. [24], based on the well-known Wu's Algorithm of computing the triangular decompositions of polynomial systems, an effective method was presented for deciding the semi-definiteness of multivariate polynomials with coefficients in a computable ordered field, if this field admits an effective method of finding isolating points for every non-zero univariate polynomial. By this method, the decision of the semi-definiteness of a multivariate polynomial may be reduced to testing some resulted polynomials in fewer variables, of which the total degrees and the term numbers do not exceed those of the given polynomial.

For an input polynomial $f(x_1,\ldots,x_n)$ in n variables, the key of the algorithm in [24] is to compute the triangular decompositions of such polynomial sets $\{f+t, \frac{\partial f}{\partial x_{j_1}},\ldots,\frac{\partial f}{\partial x_{j_k}}\}$ into irreducible ascending chains, where t is a new variable and $\{j_1,\ldots,j_k\}$ is taken over all the nonempty subsets of $\{1,\ldots,n\}$, see the description of the algorithm in §4 of [24]. The efficiency of this algorithm is thereby dependent on computing the irreducible ascending chains from these polynomial sets. In order to raise the efficiency, one attempt is to remove the polynomial $f+t$ from the involved polynomial sets.

In this paper, we present a new algorithm for deciding the semi-definiteness of multivariate polynomials with coefficients in a computable ordered field, which admits an effective method of finding an isolating set for every univariate polynomial. In this new algorithm, it is enough to compute the weaker triangular sets, the so-called regular chains, instead of irreducible ascending chains, and the involved polynomial sets don't contain the polynomial $f+t$.

Throughout this paper, the symbol K stands for a computable ordered field with real closed extension R. Hence, K and its extensions are fields of characteristic 0. For α, $\beta \in R$ with $\alpha < \beta$, write $]\alpha,\beta[_R$ (or $[\alpha,\beta[_R$) for the open interval $\{z \in R \mid \alpha < z < \beta\}$ (or the closed interval $\{z \in R \mid \alpha \leq z \leq \beta\}$). For a subset P of the polynomial ring $F[x_1,\ldots,x_n]$ over any field F in n variables, denote by (P) the ideal generated by P in $F[x_1,\ldots,x_n]$. Moreover, for a finite set (or sequence) S, $^{\#}S$ stands for the number of members in S.

2. Triangular decompositions of polynomial systems into regular chains

In this section, as some preliminaries, we recall some basic concepts and results on the triangular decompositions of polynomial systems, especially on the triangular decompositions of polynomial systems into regular chains.

The triangular decomposition of a polynomial system was introduced by Ritt in [18]. Ritt's decomposition relies on computing the so-called characteristic sets, which are some triangular sets of polynomials, of prime ideals, see [19]. So Ritt's decomposition

involves the factorization of polynomials in algebraic extensions. In order to avoid the factorization of polynomials, Wu provided an algorithm for solving polynomial systems by means of characteristic sets of not necessarily prime ideals in [20]. For the details of Wu's algorithm and its applications, we refer to [21].

Let F be an arbitrary field, let $F[x_1, \ldots, x_n]$ be the ring of polynomials over F in variables $x_1, \ldots, x_n$, and $x_{j_1}, \ldots, x_{j_n}$ an arrangement of the variables $x_1, \ldots, x_n$. For a non-constant polynomial $f \in F[x_1, \ldots, x_n]$, a variable x_{j_i} $(1 \leq i \leq n)$ is called the *main variable* of f with respect to the lexicographic order $x_{j_1} \prec \cdots \prec x_{j_n}$, if $f \in F[x_{j_1}, \ldots, x_{j_i}]$ but $f \notin F[x_{j_1}, \ldots, x_{j_{i-1}}]$. So f can be represented in the form

$$f := \ell x_{j_i}^d + u_1 x_{j_i}^{d-1} + \cdots + u_d,$$

where d is a positive integer, ℓ, $u_1, \ldots, u_d \in F[x_{j_1}, \ldots, x_{j_{i-1}}]$, and $\ell \neq 0$. The main variable x_{j_i} of f is denoted by $\mathrm{mv}(f)$, and the leading coefficient ℓ of f, as a polynomial over $F[x_{j_1}, \ldots, x_{j_{i-1}}]$ in one variable x_{j_i}, is called the initial of f. A sequence $C := [f_1, \ldots, f_s]$ of non-constant polynomials in $F[x_1, \ldots, x_n]$ is called a *chain* (*ascending chain* or *triangular set*) with respect to the lexicographic order $x_{j_1} \prec \cdots \prec x_{j_n}$, if $\mathrm{mv}(f_1) \prec \cdots \prec \mathrm{mv}(f_s)$.

Now let P and Q be two finite subsets of $F[x_1, \ldots, x_n]$, and E an arbitrary extension of F. Then we may obtain a subset of E^n as follows:

$$\mathrm{Zero}_E(P/Q) = \big\{\bar{\alpha} \in E^n \;\big|\; p(\bar{\alpha}) = 0 \text{ for all } p \in P, \text{ but } q(\bar{\alpha}) \neq 0 \text{ for all } q \in Q\big\}.$$

According to the so-called Zero-Decomposition Theorem (see Theorem 5.1 in [21]), for a finite subset P of $F[x_1, \ldots, x_n]$, a sequence $C_1, \ldots, C_r$ of chains in $F[x_1, \ldots, x_n]$ can be obtained by Wu's algorithm such that for an arbitrary extension E of F, the following equality holds:

$$\mathrm{Zero}_E(P) = \bigcup_{1 \leq i \leq r} \mathrm{Zero}_E(C_i/I_i),$$

where I_i is the set of the initials of members in C_i, $i = 1, \ldots, r$.

However, such a sequence of chains obtained by Wu's algorithm may include an inconsistent chain, i.e. there exists possibly a $j \in \{1, \ldots, r\}$ such that $\mathrm{Zero}_E(C_j/I_j) = \emptyset$ for all extension E of F. In order to solve the consistency problem, Kalkbrener [9,10] and Yang and Zhang [23] introduced independently particular triangular sets, named regular chains. The good properties of characteristic sets of prime ideals can be generalized to regular chains, see Theorem 6.1 in [1]. For a regular chain C in $F[x_1, \ldots, x_n]$, $\mathrm{Zero}_E(C_j/I_j) \neq \emptyset$ if E is an algebraically closed extension of F.

Definition 1. Let $C := [f_1, \ldots, f_s]$ be a chain in $F[x_1, \ldots, x_n]$ with respect to the lexicographic order $x_{j_1} \prec \cdots \prec x_{j_n}$, and put $\mathrm{Tv}(C) := \{x_1, \ldots, x_n\} \setminus \{\mathrm{mv}(f_i) \mid i = 1, \ldots, s\}$. Write Ω_C for the algebraic closure of $F(\mathrm{Tv}(C))$, the fraction field of the polynomial ring

$F[\mathrm{Tv}(C)]$. For $i = 1, \ldots, n$, define by induction the finite sequence $\mathrm{RZ}_i(C)$ of points in Ω_C^i as follows:

(1) If $F[x_{j_1}] \cap C = \emptyset$, $\mathrm{RZ}_1(C) := [x_{j_1}]$. If $F[x_{j_1}] \cap C = \{f_1(x_{j_1})\}$, $\mathrm{RZ}_1(C) := [\alpha_1, \ldots, \alpha_{d_1}]$ where d_1 is the degree of the univariate polynomial $f_1(x_{j_1})$ and $\alpha_1, \ldots, \alpha_{d_1}$ are all the roots of $f_1(x_{j_1})$ in Ω_C.

(2) Assume $i \in \{2, \ldots, n\}$. If $\mathrm{RZ}_{i-1}(C) = \emptyset$, $\mathrm{RZ}_i(C) := \emptyset$. Else, $\mathrm{RZ}_i(C)$ is defined as the union of the sequences $\Delta_{\bar{\alpha}_{i-1}}$, where $\bar{\alpha}_{i-1}$ runs over $\mathrm{RZ}_{i-1}(C)$, and $\Delta_{\bar{\alpha}_{i-1}}$ is defined as follows:
- If $(F[x_{j_1}, \ldots, x_{j_i}] \setminus F[x_{j_1}, \ldots, x_{j_{i-1}}]) \cap C = \emptyset$ (i.e. $x_{j_i} \in \mathrm{Tv}(C)$), $\Delta_{\bar{\alpha}_{i-1}} := [(\bar{\alpha}_{i-1}, x_{j_i})]$.
- If $(F[x_{j_1}, \ldots, x_{j_i}] \setminus F[x_{j_1}, \ldots, x_{j_{i-1}}]) \cap C = \{f_i(x_{j_1}, \ldots, x_{j_i})\}$ and $f_i(\bar{\alpha}_{i-1}, x_{j_i})$ is a polynomial of positive degree over Ω_C in one variable x_{j_i}, $\Delta_{\bar{\alpha}_{i-1}} := [(\bar{\alpha}_{i-1}, \alpha'_1), \ldots, (\bar{\alpha}_{i-1}, \alpha'_{d_i})]$, where d_i is the degree of the univariate polynomial $f_i(\bar{\alpha}_{i-1}, x_{j_i})$, and $\alpha'_1, \ldots, \alpha'_{d_i}$ are all the roots of $f_i(\bar{\alpha}_{i-1}, x_{j_i})$ in Ω_C.
- Else, $\Delta_{\bar{\alpha}_{i-1}} := \emptyset$.

In what follows, $\mathrm{RZ}_n(C)$ is simply denoted by $\mathrm{RZ}(C)$, and $\mathrm{Tv}(C)$ is called *the set of transcendental variables for* C.

The above definition of $\mathrm{RZ}_n(C)$ is slightly different from the set of regular zeros in §2.2 of [10], but both are algebraically equivalent. In a word, there is a one-to-one correspondence between $\mathrm{RZ}_n(C)$ and the set of regular zeros in §2.2 of [10] such that, for $(\alpha_1, \ldots, \alpha_n) \in \mathrm{RZ}(C)$ with corresponding zero $(\alpha'_1, \ldots, \alpha'_n)$, there exists an isomorphism of the field $F(\alpha_1, \ldots, \alpha_n)$ into $F(\alpha'_1, \ldots, \alpha'_n)$ such that $\alpha_i \mapsto \alpha'_i$ for $i = 1, \ldots, n$. As a sequence, it is possible that such an $\mathrm{RZ}(C)$ contains the same points in Ω_C^n, i.e. a point in $\mathrm{RZ}(C)$ might appear multiple times. Our definition is helpful for formulating the forthcoming propositions.

Remark. Let the notation be as in Definition 1, and assume $\mathrm{RZ}(C) \neq \emptyset$. It is easy to see that $x_{j_i} \in \mathrm{Tv}(C)$ if and only if $\alpha_i = x_{j_i}$ for all $(\alpha_1, \ldots, \alpha_n) \in \mathrm{RZ}(C)$. So, $f(\bar{\alpha}) = f$ for any polynomial $f \in F[\mathrm{Tv}(C)]$ and any $\bar{\alpha} \in \mathrm{RZ}(C)$.

Example. Let $\mathbb{Q}$ be the rational numbers, and let

$$C_1 := \{x_1^2 - x_2^2, (x_2 - x_1)x_3\}, \qquad C_2 := \{(x_1^2 - x_2^2)^2, (x_2 - x_1)x_3\},$$
$$C_3 := \{x_1^2 - 2, (x_2 - x_1)(x_1 - x_3)\}, \qquad C_4 := \{x_1 - x_2, (x_2 - x_1)x_3\},$$
$$C_5 := \{(x_1^2 - x_2^2)^2, x_2(x_3 - x_1)\}.$$

Obviously, these sequences are chains with respect to the lexicographic order $x_1 \prec x_2 \prec x_3$. According to Definition 1, we have $\mathrm{Tv}(C_1) = \{x_1\}$, $\mathrm{RZ}(C_1) = [x_1]$ and $\mathrm{RZ}_2(C_1) = [(x_1, x_1), (x_1, -x_1)]$. When $(x_1, x_2) = (x_1, -x_1)$, $(x_2 - x_1)x_3$ has the

only root 0 in the algebraic closure of the field $\mathbb{Q}(x_1)$. But $(x_2 - x_1)x_3 = 0$ when $(x_1, x_2) = (x_1, x_1)$. Hence $\mathrm{RZ}_3(C_1) = [(x_1, -x_1, 0)]$, i.e. $\mathrm{RZ}(C_1) = [(x_1, -x_1, 0)]$.

Likewise, according to Definition 1, we have

$$\mathrm{RZ}(C_2) := \big[(x_1, -x_1, 0), (x_1, -x_1, 0)\big], \qquad \mathrm{RZ}(C_3) = \big[(\sqrt{2}, x_2, \sqrt{2}), (-\sqrt{2}, x_2, -\sqrt{2})\big],$$
$$\mathrm{RZ}(C_4) = \emptyset, \qquad \mathrm{RZ}(C_5) = \big[(x_1, x_1, x_1), (x_1, x_1, x_1), (x_1, -x_1, x_1), (x_1, -x_1, x_1)\big].$$

According to the inductive definition of regular chains in §2.2 of [10], we give the following

Definition 2. Let $C := [f_1, \ldots, f_s]$ be a chain in $F[x_1, \ldots, x_n]$ with respect to the lexicographic order $x_{j_1} \prec \cdots \prec x_{j_n}$, and let ℓ_i and $x_{j_{m_i}}$ be the initial and main variable of f_i respectively, $i = 1, \ldots, s$. C is called regular if the following condition is satisfied:

- For $i = 2, \ldots, s$, $\ell_i(\bar{\alpha}_{m_i-1}) \neq 0$ for all $\bar{\alpha}_{m_i-1} \in \mathrm{RZ}_{m_i-1}(C)$.

In the above example, both C_3 and C_5 are regular, but C_1, C_2 and C_4 are not regular. It is easy to see that a chain $C := [f_1, \ldots, f_s]$ in $F[x_1, \ldots, x_n]$ is regular if and only if

$$^{\#}\,\mathrm{RZ}(C) = d_1 d_2 \cdots d_s,$$

where d_i is the degree of f_i relative to the variable $\mathrm{mv}(f_i)$, $i = 1, \ldots, s$.

Let $C := [f_1, \ldots, f_s]$ be a regular chain in $F[x_1, \ldots, x_n]$ with respect to some lexicographic order, and g another polynomial over an extension E of F in variables $x_1, \ldots, x_n$. Following [23], we get successively the resultants as follows:

$$\begin{aligned}
r_{s-1} &:= \mathrm{resultant}\big(g, f_s, \mathrm{mv}(f_s)\big),\\
r_{s-2} &:= \mathrm{resultant}\big(r_{s-1}, f_{s-1}, \mathrm{mv}(f_{s-1})\big),\\
&\cdots\cdots\cdots\\
r_1 &:= \mathrm{resultant}\big(r_2, f_2, \mathrm{mv}(f_2)\big),\\
r_0 &:= \mathrm{resultant}\big(r_1, f_1, \mathrm{mv}(f_1)\big).
\end{aligned}$$

Obviously, $r_0 \in E[x_{j_{s+1}}, \ldots, x_{j_n}]$, where $x_{j_{s+1}}, \ldots, x_{j_n}$ are all the variables in $\mathrm{Tv}(C)$. In what follows, r_0 is called *the resultant of C with respect to g*, and is denoted by $\mathrm{Res}(C; g)$ or $\mathrm{Res}(f_1, \ldots, f_s; g)$.

As an important result on regular chains, Lemma 3 in [23] may be stated in the following version:

Proposition 2.1. *Let $C := [f_1, \ldots, f_s]$ be a regular chain in $F[x_1, \ldots, x_n]$ with respect to the lexicographic order $x_{j_1} \prec \cdots \prec x_{j_n}$, and g another polynomial over an extension of F in variables $x_1, \ldots, x_n$. If $x_{j_{m_i}}$ is the main variable of f_i, $i = 1, \ldots, s$, then*

$$\operatorname{Res}(C;g)=\ell_1^{\nu_1}\Bigg(\prod_{\bar{\alpha}_1\in \mathrm{RZ}_{m_1}(C)}\ell_2^{\nu_2}(\bar{\alpha}_1)\Bigg)\cdots\Bigg(\prod_{\bar{\alpha}_{s-1}\in \mathrm{RZ}_{m_{s-1}}(C)}\ell_s^{\nu_s}(\bar{\alpha}_{s-1})\Bigg)\Bigg(\prod_{\bar{\alpha}\in \mathrm{RZ}(C)}g(\bar{\alpha})\Bigg),$$

where ℓ_i is the initial of f_i for $i=1,\dots,s$, ν_j is the degree of $\operatorname{Res}(f_{j+1},\dots,f_s;g)$ *relative to the variable $mv(f_j)$ for $j=1,\dots,s-1$, and ν_s is the degree of g relative to the variable $mv(f_s)$.*

As an immediate consequence of Proposition 2.1, we can establish the following

Proposition 2.2. *Let $C:=[f_1,\dots,f_s]$ be a regular chain in $F[x_1,\dots,x_n]$ with respect to the lexicographic order $x_{j_1}\prec\cdots\prec x_{j_n}$, and t a new variable. If $x_{j_{m_i}}$ is the main variable of f_i, $i=1,\dots,s$, then, for any $g\in F[x_1,\dots,x_n]$,* $\operatorname{Res}(C;g+t)$ *is a polynomial of positive degree in one variable t over $F[x_{j_{m_{s+1}}},\dots,x_{j_{m_n}}]$ where $\{m_{s+1},\dots,m_n\}$ is the complement of $\{m_1,\dots,m_s\}$ in $\{1,\dots,n\}$, and*

$$\begin{aligned}&\operatorname{Res}(C;g+t)\\&=\ell_1^{\nu_1}\Bigg(\prod_{\bar{\alpha}_1\in \mathrm{RZ}_{m_1}(C)}\ell_2^{\nu_2}(\bar{\alpha}_1)\Bigg)\cdots\Bigg(\prod_{\bar{\alpha}_{s-1}\in \mathrm{RZ}_{m_{s-1}}(C)}\ell_s^{\nu_s}(\bar{\alpha}_{s-1})\Bigg)\Bigg(\prod_{\bar{\alpha}\in \mathrm{RZ}(C)}\big(t+g(\bar{\alpha})\big)\Bigg),\end{aligned}$$

where the symbols are as in Proposition 2.1.

For $\bar{\alpha}\in\Omega_C^n$, we obtain the ideal of $F[x_1,\dots,x_n]$ as follows:

$$\mathfrak{P}_{\bar{\alpha}}:=\big\{g\in F[x_1,\dots,x_n]\;\big|\;g(\bar{\alpha})=0\big\}.$$

Obviously, $\mathfrak{P}_{\bar{\alpha}}$ is a prime ideal of $F[x_1,\dots,x_n]$ with generic point $\bar{\alpha}$ for $\bar{\alpha}\in\Omega_C^n$.

By a familiar fact about polynomial ideals and algebraic varieties (see Propositions 3.7 and 3.11 in [12]), there exists a one-to-one correspondence between prime ideals in $F[x_1,\dots,x_n]$ and irreducible F-varieties in Ω_C^n.

In [10], Kalkbrener presented an algorithm named **solve**$_n$. For a regular (possibly empty) chain D in $F[x_1,\dots,x_{n-1}]$ and a (nonempty) finite subset P of $F[x_1,\dots,x_n]$, Algorithm **solve**$_n$ returns a sequence $C_1,\dots,C_r$ of regular chains in $F[x_1,\dots,x_n]$ such that

$$\Bigg(\bigcap_{\bar{\beta}\in \mathrm{RZ}_{n-1}(D)}\mathfrak{P}_{\overline{(\beta,x_n)}}\Bigg)\cup\sqrt{(P)}\supseteq\bigcap_{\bar{\alpha}\in\Xi}\mathfrak{P}_{\bar{\alpha}}\supseteq\sqrt{(P)},$$

where $\sqrt{(P)}$ is the radical of the ideal (P) generated by P in $F[x_1,\dots,x_n]$, and $\Xi:=\mathrm{RZ}(C_1)\cup\cdots\cup\mathrm{RZ}(C_r)$. Observe that $\mathrm{RZ}_{n-1}(D)=\{(x_1,\dots,x_{n-1})\}$ and $\mathfrak{P}_{\overline{(x_1,\dots,x_{n-1},x_n)}}=\{0\}$ if D is the empty chain $[\,]$. So we have $\sqrt{(P)}=\bigcap_{\bar{\alpha}\in\Xi}\mathfrak{P}_{\bar{\alpha}}$ in the case when $D=[\,]$.

According to Algorithm **solve**$_n$ and the above argument, we give the following

Definition 3. Let P be a finite subset of $F[x_1,\ldots,x_n]$. A sequence $C_1,\ldots,C_r$ of regular chains in $F[x_1,\ldots,x_n]$ is called a regular decomposition of P, if the following equality holds:

$$\sqrt{(P)} = \bigcap_{\bar{\alpha}\in\Xi} \mathfrak{P}_{\bar{\alpha}},$$

where $\sqrt{(P)}$ is the radical of the ideal (P) generated by P in $F[x_1,\ldots,x_n]$, and $\Xi := \mathrm{RZ}(C_1)\cup\cdots\cup\mathrm{RZ}(C_r)$.

In [15], Moreno Maza introduced another kind of triangular decompositions of regular chains, which is said to be in the sense of Lazard. Such a regular decomposition as in Definition 3 is hence said to be in the sense of Kalkbrener. For a finite subset P of $F[x_1,\ldots,x_n]$, a sequence $C_1,\ldots,C_r$ of regular chains in $F[x_1,\ldots,x_n]$ is called a regular decomposition of P in the sense of Lazard, if it is a regular decompositions in the sense of Definition 3, and for an arbitrary extension E of F, $\mathrm{Zero}_E(P) = \bigcup_{1\le i\le r}\mathrm{Zero}_E(C_i/I_i)$, where I_i is the set of the initials of members in C_i, $i=1,\ldots,r$. The decompositions in the sense of Kalkbrener are weaker but less expensive to compute. In this paper, we only consider the regular decompositions in the sense of Kalkbrener, i.e. the regular decompositions in the sense of Definition 3. In the computer algebraic system **Maple 15 (or 14)**, the command **Triangularize** returns a regular decomposition (in the sense of Definition 3) for a given finite subset of polynomials.

Proposition 2.3. *Let P be a finite subset of $F[x_1,\ldots,x_n]$, let $C_1,\ldots,C_r$ be a regular decomposition of P with respect to the lexicographic order $x_{i_1}\prec\cdots\prec x_{i_n}$, and t a new variable. Then, for any $f\in F[x_1,\ldots,x_n]$, $C_1\cup\{f+t\},\ldots,C_r\cup\{f+t\}$ is a regular decomposition of $P\cup\{f+t\}$ with respect to the lexicographic order $x_{i_1}\prec\cdots\prec x_{i_n}\prec t$.*

Proof. Put $D_i := C_i\cup\{f+t\}$, $i=1,\ldots,r$. By Definitions 1 and 2, it is easy to see that, for $i=1,\ldots,r$, $\Omega_{D_i}=\Omega_{C_i}$, $\mathrm{RZ}(D_i) = [(\bar{\alpha},-f(\bar{\alpha}))\mid \bar{\alpha}\in\mathrm{RZ}(C_i)]$, and D_i is a regular chain with respect to the lexicographic order $x_{i_1}\prec\cdots\prec x_{i_n}\prec t$. Since $C_1,\ldots,C_r$ is a regular decomposition of P, we have

$$\sqrt{(P)} = \bigcap_{\bar{\alpha}\in\Xi} \mathfrak{P}_{\bar{\alpha}},$$

where $\Xi := \mathrm{RZ}(C_1)\cup\cdots\cup\mathrm{RZ}(C_r)$.

Obviously, $P\cup\{f+t\}\subset\mathfrak{P}_{(\bar{\alpha},-f(\bar{\alpha}))}$ for all $\bar{\alpha}\in\Xi$. So we have $\sqrt{(P\cup\{f+t\})}\subseteq\bigcap_{\bar{\alpha}\in\Xi}\mathfrak{P}_{(\bar{\alpha},-f(\bar{\alpha}))}$.

Now assume that $g\in\bigcap_{\bar{\alpha}\in\Xi}\mathfrak{P}_{(\bar{\alpha},-f(\bar{\alpha}))}$. Then $g(\bar{\alpha},-f(\bar{\alpha}))=0$ for all $\bar{\alpha}\in\Xi$. Denote by g^* the polynomial $g(x_1,\ldots,x_n,-f)$ in $F[x_1,\ldots,x_n]$. Then $g^*(\bar{\alpha}) = g(\bar{\alpha},-f(\bar{\alpha}))=0$ for all $\bar{\alpha}\in\Xi$. It follows that $g^*\in\bigcap_{\bar{\alpha}\in\Xi}\mathfrak{P}_{\bar{\alpha}} = \sqrt{(P)}\subset\sqrt{(P\cup\{f+t\})}$. It is easy to see that

$g - g^* = w(f+t)$ for some $w \in F[x_1, \ldots, x_n, t]$. It follows that $g - g^* \in \sqrt{(P \cup \{f+t\})}$. Hence $g = (g - g^*) + g^* \in \sqrt{(P \cup \{f+t\})}$. So we further have

$$\sqrt{(P \cup \{f+t\})} = \bigcap_{\bar{\alpha} \in \Xi} \mathfrak{P}_{(\bar{\alpha}, -f(\bar{\alpha}))}.$$

It is obvious that $\mathrm{RZ}(D_1) \cup \cdots \cup \mathrm{RZ}(D_r) = [(\bar{\alpha}, -f(\bar{\alpha})) \mid \bar{\alpha} \in \Xi]$. By Definition 3, the proposition is proved. □

3. Some theoretical results

In this section, we establish some theoretical results, which are useful for establishing our algorithms, see Proposition 3.3 and Theorem 3.4 below.

As usual, for a polynomial $f \in F[x_1, x_2, \ldots, x_n]$ where F is a field, write $\frac{\partial f}{\partial x_i}$ for the partial derivative of f relative to x_i for $i = 1, \ldots, n$. The following proposition can be found as the corollary of Proposition 1 in [24].

Proposition 3.1. *Let $f(x_1, x_2, \ldots, x_n) \in F[x_1, x_2, \ldots, x_n]$ where F is a field of characteristic 0, and I the ideal of $F[x_1, x_2, \ldots, x_n, z]$ generated by $z - f$ and $\frac{\partial f}{\partial x_i}$, $i = 1, \ldots, n$. Then $I \cap F[z] \neq \{0\}$.*

In the sequel, denote by $(K, \leq)$ a computable ordered field with real closure R. Now let f be a non-zero polynomial in $K[x_1, x_2, \ldots, x_n]$, and put

$$\mathfrak{N}_R(f, x_n) := \big\{a_n \in R \big| \text{ there are } a_1, \ldots, a_{n-1} \in R \text{ such that } f(a_1, a_2, \ldots, a_n) < 0\big\}.$$

It is easy to see that $\mathfrak{N}_R(f, x_n)$ is an open semi-algebraic subset of R. By Proposition 2.1.7 in [5], $\mathfrak{N}_R(f, x_n)$ consists of finitely many disjoint open intervals in R, if the polynomial f is not positive semi-definite on R. An endpoint a of an interval of $\mathfrak{N}_R(f, x_n)$ is called finite, if $a \neq -\infty$ and $a \neq +\infty$. Obviously, $\mathfrak{N}_R(f, x_n)$ possesses at least one finite endpoint if f is not positive semi-definite on R and $\mathfrak{N}_R(f, x_n) \neq R$.

The purpose of this section is to seek an effective method to find a finite subset U of $K[x_n]$ such that every finite endpoint of $\mathfrak{N}_R(f, x_n)$ is a root of some polynomial in U for an indefinite polynomial $f \in K[x_1, x_2, \ldots, x_n]$. For this purpose, we shall extend the real closed field R to an ordered field containing infinitely large elements and infinitesimal elements over R.

Let $\eta_1, \ldots, \eta_n$ be n indeterminates over R, and write $R(\eta_1, \ldots, \eta_i)$ for the fraction field of the polynomial ring $R[\eta_1, \ldots, \eta_i]$ for $i = 1, \ldots, n$. Then the ordering $\leq$ of R may be extended to an ordering of $R(\eta_1, \ldots, \eta_n)$, still denoted by $\leq$, in the following manner:

$$\text{For non-zero } g, h \in R[\eta_1, \ldots, \eta_n],\ \frac{g}{h} < 0, \quad \text{if and only if} \quad \mathrm{lc}(gh; \eta_1, \ldots, \eta_n) < 0,$$

where $\mathrm{lc}(u; \eta_1, \ldots, \eta_n)$ stands for the leading coefficient of u with respect to the lexicographic order $\eta_1 \prec \cdots \prec \eta_n$ for non-zero $u \in R[\eta_1, \ldots, \eta_n]$.

It is easy to see that η_i is a positive and infinitely large element over the subfield $R(\eta_1,\ldots,\eta_{i-1})$ in the sense that $w<\eta_i$ for all $w\in R(\eta_1,\ldots,\eta_{i-1})$, $i=1,\ldots,n$.

According to Theorem 3.10 in [17], denote by $\mathcal{R}$ the real closure of the ordered field $(R(\eta_1,\ldots,\eta_n),\leq)$. Now let ϵ be an indeterminate over $\mathcal{R}$, and write $\mathcal{R}(\epsilon)$ for the fraction field of the polynomial ring $\mathcal{R}[\epsilon]$. Then the ordering $\leq$ of $\mathcal{R}$ may be further extended to an ordering of $\mathcal{R}(\epsilon)$, still denoted by $\leq$, in the following manner:

$$\text{For non-zero } g,h\in\mathcal{R}[\epsilon],\ \frac{g}{h}<0,\quad \text{if and only if}\quad \mathrm{tc}(gh;\epsilon)<0,$$

where $\mathrm{tc}(u;\epsilon)$ stands for the trailing coefficient (the coefficient of lowest term) of u as a polynomial over $\mathcal{R}$ in one variable ϵ for non-zero $u\in\mathcal{R}[\epsilon]$.

It is easy to see that ϵ is a positive and infinitesimal element over $\mathcal{R}$ in the sense that $0<\epsilon<\alpha$ for all positive $\alpha\in\mathcal{R}$.

Denote by $\mathcal{R}$ the real closure of the ordered field $(\mathcal{R}(\epsilon),\leq)$. Now, we construct the four subsets of $\mathcal{R}$ as follows:

$$\begin{aligned}
\mathcal{A}&:=\{z\in\mathcal{R}\mid \text{For some positive element } d\in R,\ -d\leq z\leq d\},\\
\mathcal{M}&:=\{z\in\mathcal{R}_1\mid \text{For every positive element } d\in R, -d\leq z\leq d\}.\\
\mathcal{A}_1&:=\{z\in\mathcal{R}_1\mid \text{For some positive element } \delta\in\mathcal{R}, -\delta\leq z\leq \delta\},\\
\mathcal{M}_1&:=\{z\in\mathcal{R}_2\mid \text{For every positive element } \delta\in\mathcal{R}, -\delta\leq z\leq \delta\}.
\end{aligned}$$

Hence, $\mathcal{M}$ (or $\mathcal{M}_1$) consists of all elements in $\mathcal{R}_1$ which are "infinitesimal" over R (or $\mathcal{R}$). Obviously, $R\subset\mathcal{A}\subset\mathcal{A}_1$, $\mathcal{R}\subset\mathcal{A}_1$, but $\mathcal{M}_1\subset\mathcal{M}$. By the definition of $\leq$, we further have $\eta_i^{-1}\in M$ for $i=1,\ldots,n$, and $\epsilon\in\mathcal{M}_1$.

By a familiar result on real valuations (see Proposition 1.3 in [11] or the relevant theorems in §5 of [13]), $\mathcal{A}$ is a valuation ring of $\mathcal{R}_1$ with maximal ideal $\mathcal{M}$, and $\mathcal{A}_1$ is another valuation ring of $\mathcal{R}_1$ with maximal ideal $\mathcal{M}_1$. Moreover, both $(\mathcal{A},\mathcal{M})$ and $(\mathcal{A}_1,\mathcal{M}_1)$ are compatible with the ordering $\leq$, in other words, $\mathcal{A}$, $\mathcal{M}$, $\mathcal{A}_1$ and $\mathcal{M}_1$ are convex in $\mathcal{R}_1$ with respect to the ordering $\leq$. Observe that the residue field $\mathcal{A}/\mathcal{M}$ of $\mathcal{A}$ is isomorphic to R and the residue field $\mathcal{A}_1/\mathcal{M}_1$ of $\mathcal{A}_1$ is isomorphic to $\mathcal{R}$. Thereby, there is a homomorphism π of $\mathcal{A}$ onto R such that $\pi(a)=a$ for all $a\in R$, $\pi(\epsilon)=0$ and $\pi(\eta_i^{-1})=0$ for $i=1,\ldots,n$, and there is a homomorphism π_1 of $\mathcal{A}_1$ onto $\mathcal{R}$ such that $\pi_1(\alpha)=\alpha$ for all $\alpha\in\mathcal{R}$ and $\pi(\epsilon)=0$.

Denote by $K_{\langle n+1\rangle}$ the subfield $K(\epsilon,\eta_1,\ldots,\eta_n)$ of $\mathcal{R}_1$. Obviously, $K_{\langle n+1\rangle}$ is also a computable ordered field with respect to its inherited ordering.

Let S be any nonempty semi-algebraic subset of $\mathcal{R}_1$. By Proposition 2.1.7 in [5], S consists of finitely many disjoint (open or closed or half open-closed) intervals and points in $\mathcal{R}_1$. For $\alpha\in\mathcal{R}_1$, write $[\alpha,\alpha]_{\mathcal{R}_1}:=\{\alpha\}$. Thereby, a singleton may be considered as a closed interval with the same endpoints. Moreover, we may assume that a closed endpoint of an interval is not the same as an open endpoint of another interval for any two intervals of S; otherwise, they can be combined into a larger interval. So, every

semi-algebraic subset of $\mathcal{R}_1$ consists of finitely many disjoint (open or closed or half open-closed) intervals in $\mathcal{R}_1$.

For $g_1, \ldots, g_r \in K_{\langle n+1\rangle}[x_{j_1}, \ldots, x_{j_k}, x_n]$ where $\{j_1, \ldots, j_k\}$ is a nonempty subset of $\{1, \ldots, n-1\}$, denote by $\mathcal{V}_{R_1}(g_1, \ldots, g_r; x_n)$ the subset of $\mathcal{R}_1$ as follows:

$$\big\{a_n \in \mathcal{R}_1 \mid \text{there are } a_{j_1}, \ldots, a_{j_k} \in \mathcal{R}_1 \text{ such that } g_i(a_{j_1}, \ldots, a_{j_k}, a_n) = 0,\ i = 1, \ldots, r\big\}.$$

Obviously, $\mathcal{V}_{\mathcal{R}_1}(g_1, \ldots, g_r; x_n)$ is a semi-algebraic subset of $\mathcal{R}_1$.

The following proposition may be considered as a combination version of Lemmas 1, 2 and 3 in [24]. Here, a simpler proof is given.

Proposition 3.2. *Let the notation be as above, and $f \in K[x_1, \ldots, x_n]$. If a is a finite open endpoint of $\mathfrak{N}_R(f, x_n)$, then one of the following statements is true:*

(1) *$e(a) = 0$ where $e(x_n) \in K[x_n]$ be the leading coefficient of f as a polynomial over $K[x_n]$ in variables $x_1, \ldots, x_{n-1}$ with respect to the lexicographic order $x_1 \prec \cdots \prec x_{n-1}$.*

(2) *For some nonempty subset $\{j_1, \ldots, j_k\}$ of $\{1, \ldots, n-1\}$ with complement $\{j_{k+1}, \ldots, j_{n-1}\}$ and certain $\varrho_{k+1}, \ldots, \varrho_{n-1} \in \{1, -1\}$, the set*

$$\mathcal{V}_{\mathcal{R}_1}\left(g + \epsilon, \frac{\partial g}{\partial x_{j_1}}, \ldots, \frac{\partial g}{\partial x_{j_k}}; x_n\right),$$

where g is the polynomial over $K_{\langle n+1\rangle}$ obtained from f by substituting $x_{j_i} = \varrho_i \eta_{j_i}$ for $i = k+1, \ldots, n-1$, contains a point β such that the following conditions are satisfied:

(i) *$\beta - a \in \mathcal{M}$.*

(ii) *$\beta \notin \mathcal{R}$, i.e. β is transcendental over $\mathcal{R}$.*

Proof. Without loss of generality, we may assume that a is a left finite endpoint of $\mathfrak{N}_R(f, x_n)$. In this case, there is a $c \in R$ with $a < c$ such that $]a, c[_R \subseteq \mathfrak{N}_R(f, x_n)$, where $]a, c[_R$ is the open interval in R with endpoints a, c.

Consider the semi-algebraic subset T of $\mathcal{R}_1^n$ as follows:

$$T := \big\{(\alpha_1, \ldots, \alpha_n) \in \mathcal{R}_1^n \mid f(\alpha_1, \ldots, \alpha_n) + \epsilon = 0, \text{ and } -\eta_i \le \alpha_i \le \eta_i,\ i = 1, \ldots, n\big\}.$$

Obviously, T is closed and bounded in $\mathcal{R}_1^n$. By Proposition 2.5.7 in [5], T_{x_n} is closed and bounded in $\mathcal{R}_1$ where

$$T_{x_n} := \big\{\alpha \in \mathcal{R}_1 \mid \text{ there exist } \alpha_1, \ldots, \alpha_{n-1} \in \mathcal{R}_1 \text{ such that } (\alpha_1, \ldots, \alpha_{n-1}, \alpha) \in T\big\}.$$

By the above argument, T_{x_n} consists of a finite number of disjoint closed intervals. Suppose that $a \in T_{x_n}$. Then $f(\zeta_1, \ldots, \zeta_{n-1}, a) + \epsilon = 0$ for some $\zeta_1, \ldots, \zeta_{n-1} \in \mathcal{R}_1$. Hence

$f(\zeta_1,\dots,\zeta_{n-1},a)=-\epsilon<0$, and the following sentence is valid in the real closed field $\mathcal{R}_1$:

$$\exists(x_1,\dots,x_{n-1})\big(f(x_1,\dots,x_{n-1},a)<0\big).$$

Observe that all the constants in the above sentence belong to R. By the familiar Transfer principle for real closed fields (see Theorem 2.78 in [2] or Proposition 5.2.3 in [5]), the sentence also is valid in the real closed field R. This yield a contradiction that $a\in\mathfrak{N}_R(f,x_n)$. Thus $a\notin T_{x_n}$.

Let δ be any positive element in R such that $\delta<c-a$. Then $a+\delta\in\,]a,c[_R\subseteq\mathfrak{N}_R(f,x_n)$. Hence there exist $b_1,\dots,b_{n-1}$ in R such that $f(b_1,\dots,b_{n-1},a+\delta)<0$. Since $a\notin\mathfrak{N}_R(f,x_n)$, we have $f(b_1,\dots,b_{n-1},a)\geq 0$. By the definition of the ordering $\leq$ of $\mathcal{R}_1$, we have $f(b_1,\dots,b_{n-1},a+\delta)+\epsilon<0$, but $f(b_1,\dots,b_{n-1},a)+\epsilon>0$. By the intermediate value theorem for polynomials over real closed fields, there exists a ξ in $\mathcal{R}_1$ such that $a<\xi<a+\delta$ and $f(b_1,\dots,b_{n-1},\xi)+\epsilon=0$. It follows that $(b_1,\dots,b_{n-1},\xi)\in T$ and $\xi\in T_{x_n}$. So, there is a closed interval $[\omega,\gamma]_{\mathcal{R}_1}$ of T_{x_n} such that $\xi\in[\omega,\gamma]_{\mathcal{R}_1}$. Obviously, $\omega-a\leq\xi-a<(a+\delta)-a=\delta$. Since $a<\xi$ but $a\notin[\omega,\gamma]_{\mathcal{R}_1}$, we have $a<\omega$. This implies that ω is a closed endpoint of T_{x_n} such that $\omega-a>0$.

Let β be the closed endpoint of T_{x_n} such that $\beta-a>0$ and $\beta-a$ is minimal. Then $0<\beta-a\leq\omega-a<\delta$. By the arbitrariness of δ, we get $\beta-a\in\mathcal{M}$, and $\pi(\beta)=\pi(a)=a$.

Since $\beta\in T_{x_n}$, there exist $\alpha_1,\dots,\alpha_{n-1}\in\mathcal{R}_1$ such that $f(\alpha_1,\dots,\alpha_{n-1},\beta)+\epsilon=0$. Put

$$\Gamma:=\{j\mid 1\leq j\leq n-1,\ \text{and}\ -\eta_j<\alpha_j<\eta_j\},$$

and denote by k the number of subscripts in Γ. Then $0\leq k\leq n-1$.

Assume that $k=0$. Then $\Gamma=\emptyset$, and $\alpha_i=\varrho_i\eta_i$ for some $\varrho_i\in\{1,-1\}$, $i=1,\dots,n-1$. It follows that $f(\varrho_1\eta_1,\dots,\varrho_{n-1}\eta_{n-1},\beta)+\epsilon=0$. Observe that $\beta=a+(\beta-a)\in\mathcal{A}\subset\mathcal{A}_1$. By the homomorphism π_1, we have

$$f\big(\varrho_1\eta_1,\dots,\varrho_{n-1}\eta_{n-1},\pi_1(\beta)\big)=\pi_1\big(f(\varrho_1\eta_1,\dots,\varrho_{n-1}\eta_{n-1},\beta)+\epsilon\big)=0.$$

Represent f in the form as follows:

$$f=e(x_n)x_1^{d_1}\cdots x_{n-1}^{d_{n-1}}+e_1(x_n)x_1^{d_{11}}\cdots x_{n-1}^{d_{1,n-1}}+\cdots+e_m(x_n)x_1^{d_{m1}}\cdots x_{n-1}^{d_{m,n-1}},$$

where $e_i(x_n)\in K[x_n]$, $i=1,\dots,m$, and $e(x_n)$ is the leading coefficient of f as a polynomial over $K[x_n]$ in variables $x_1,\dots,x_{n-1}$ with respect to the lexicographic order $x_1\prec\cdots\prec x_{n-1}$.

By the above representation, we have

$$e\big(\pi_1(\beta)\big)+\mu_1+\cdots+\mu_m=\frac{f(\varrho_1\eta_1,\dots,\varrho_{n-1}\eta_{n-1},\pi_1(\beta))}{(\varrho_1\eta_1)^{d_1}\cdots(\varrho_{n-1}\eta_{n-1})^{d_{n-1}}}=0,$$

where $\mu_i:=e_i(\pi_1(\beta))\cdot\frac{(\varrho_1\eta_1)^{d_{i1}}\cdots(\varrho_{n-1}\eta_{n-1})^{d_{i,n-1}}}{(\varrho_1\eta_1)^{d_1}\cdots(\varrho_{n-1}\eta_{n-1})^{d_{n-1}}}$, $i=1,\dots,m$.

Since $\pi_1(\beta) - a = (\pi_1(\beta) - \beta) + (\beta - a) \in \mathcal{M}_1 + \mathcal{M} \subseteq \mathcal{M}$, we have $\pi(\pi_1(\beta)) = a$. Moreover, it is easy to prove that $\mu_i \in M$ for $i = 1, \ldots, m$. By the homomorphism π, we further have

$$e(a) = \pi\big(e\big(\pi_1(\beta)\big) + \mu_1 + \cdots + \mu_m\big) = \pi(0) = 0.$$

Now assume that $1 \leq k \leq n-1$, $\Gamma = \{j_1, \ldots, j_k\}$, and $\{j_{k+1}, \ldots, j_n\}$ is the complement of Γ in $\{1, \ldots, n\}$. Then, $-\eta_{j_i} < \alpha_{j_i} < \eta_{j_i}$ for $i = 1, \ldots, k$, but $\alpha_{j_i} = \varrho_i \eta_{j_i}$ for some $\varrho_i \in \{1, -1\}$, $i = k+1, \ldots, n-1$. Write g for the polynomial over $K_{\langle n+1 \rangle}$ obtained from f by substituting $x_{j_i} = \varrho_i \eta_{j_i}$ for $i = k+1, \ldots, n-1$. Then $g \in K_{\langle n+1 \rangle}[x_{j_1}, \ldots, x_{j_k}, x_n]$ and $g(\alpha_{j_1}, \ldots, \alpha_{j_k}, \beta) + \epsilon = 0$.

Suppose that $\frac{\partial g}{\partial x_{j_1}}(\alpha_{j_1}, \ldots, \alpha_{j_k}, \beta) \neq 0$. Observe that $\frac{\partial (g+\epsilon)}{\partial x_{j_1}} = \frac{\partial g}{\partial x_{j_1}}$. By the implicit function theorem for real closed fields (see Corollary 2.9.8 in [5]), there exist an open neighborhood Δ of $(\alpha_{j_2}, \ldots, \alpha_{j_k}, \beta)$ in the topological space $\mathcal{R}_1^k$, an open neighborhood Δ_1 of α_{j_1} in $\mathcal{R}_1$ and a continuous function (mapping) ψ of Δ into Δ_1 such that $\psi(\alpha_{j_2}, \ldots, \alpha_{j_k}, \beta) = \alpha_{j_1}$ and for every $(y_1, \ldots, y_k, y_n) \in \Delta_1 \times \Delta$, $g(y_1, \ldots, y_k, y_n) + \epsilon = 0$ if and only if $y_1 = \psi(y_2, \ldots, y_k, y_n)$.

Since $\Delta_1 \cap]-\eta_{j_1}, \eta_{j_1}[_{\mathcal{R}_1}$ is an open neighborhood of α_{j_1}, $\psi^{-1}(\Delta_1 \cap]-\eta_{j_1}, \eta_{j_1}[_{\mathcal{R}_1})$ is an open neighborhood of $(\alpha_{j_2}, \ldots, \alpha_{j_k}, \beta)$. By the topological structure of $\mathcal{R}_1^k$, there is a positive element $\lambda \in \mathcal{R}_1$ such that $\{(\alpha_{j_2}, \ldots, \alpha_{j_k})\} \times]\beta - \lambda, \beta + \lambda[_{\mathcal{R}_1} \subseteq \psi^{-1}(\Delta_1 \cap]-\eta_{j_1}, \eta_{j_1}[_{\mathcal{R}_1})$. This implies that $\psi(\alpha_{j_2}, \ldots, \alpha_{j_k}, z) \in]-\eta_{j_1}, \eta_{j_1}[_{\mathcal{R}_1}$ for all $z \in]\beta - \lambda, \beta + \lambda[_{\mathcal{R}_1}$. Put $\gamma_z := \psi(\alpha_{j_2}, \ldots, \alpha_{j_k}, z)$. Then $g(\gamma_z, \alpha_{j_2}, \ldots, \alpha_{j_k}, z) + \epsilon = 0$, i.e. $f(\alpha'_1, \ldots, \alpha'_{n-1}, z) + \epsilon = 0$ where $\alpha'_{j_1} := \gamma_z$, $\alpha'_{j_i} := \alpha_{j_i}$ for $i = 2, \ldots, k$, and $\alpha'_{j_i} := \varrho_i \eta_{j_i}$ for $i = k+1, \ldots, n-1$. It follows that $z \in T_{x_n}$ for all $z \in]\beta - \lambda, \beta + \lambda[_{\mathcal{R}_1}$. This is a contradiction, because β is a closed endpoint of T_{x_n}. Hence, $\frac{\partial g}{\partial x_{j_1}}(\alpha_{j_1}, \ldots, \alpha_{j_k}, \beta) = 0$. It is similar to prove $\frac{\partial g}{\partial x_{j_i}}(\alpha_{j_1}, \ldots, \alpha_{j_k}, \beta) = 0$ for $i = 2, \ldots, k$.

It remains to prove $\beta \notin \mathcal{R}$. From the equality $g(\alpha_{j_1}, \ldots, \alpha_{j_k}, \beta) + \epsilon = 0$, it follows that $g(\alpha_{j_1}, \ldots, \alpha_{j_k}, \beta) < 0$. So the following sentence is valid in the real closed field $\mathcal{R}_1$:

$$\exists (x_{j_1}, \ldots, x_{j_k}) \big(g(x_{j_1}, \ldots, x_{j_k}, \beta) < 0 \wedge -\eta_{j_1} < x_{j_1} < \eta_{j_1} \wedge \cdots \wedge -\eta_{j_k} < x_{j_k} < \eta_{j_k}\big).$$

Suppose that $\beta \in \mathcal{R}$. Then all the constants in the above sentence belong to $\mathcal{R}$. By the Transfer principle for real closed fields, this sentence also is valid in the real closed field $\mathcal{R}$. Hence there exist $\beta_{j_1}, \ldots, \beta_{j_k} \in \mathcal{R}$ such that $g(\beta_{j_1}, \ldots, \beta_{j_k}, \beta) < 0$ and $-\eta_{j_i} < \beta_{j_i} < \eta_{j_i}$ for $i = 1, \ldots, k$. By the continuity of the polynomial function $g(\beta_{j_1}, \ldots, \beta_{j_k}, x)$, there exists a positive element $\theta \in \mathcal{R}$ such that $\theta < \beta - a$ and $g(\beta_{j_1}, \ldots, \beta_{j_k}, \beta - \theta) < 0$. By the definition of the ordering $\leq$ of $\mathcal{R}_1$, we have $g(\beta_{j_1}, \ldots, \beta_{j_k}, \beta - \theta) + \epsilon < 0$, i.e. $f(\beta'_1, \ldots, \beta'_{n-1}, \beta - \theta) + \epsilon < 0$ where $\beta'_{j_i} := \beta_{j_i}$ for $i = 1, \ldots, k$, and $\beta'_{j_i} := \varrho_i \eta_{j_i}$ for $i = k+1, \ldots, n-1$. Observe that $a \notin \mathfrak{N}_R(f; x_n)$. By the Transfer principle for real closed fields, we may get $f(\beta'_1, \ldots, \beta'_{n-1}, a) \geq 0$, and $f(\beta'_1, \ldots, \beta'_{n-1}, a) + \epsilon > 0$. Observe that $a < \beta - \theta$. By the intermediate value theorem for univariate polynomials, there exists a $\zeta \in \mathcal{R}_1$ such that $a < \zeta < \beta - \theta$ and $f(\beta'_1, \ldots, \beta'_{n-1}, \zeta) + \epsilon = 0$. This yields

$\zeta \in T_{x_n}$. Hence there is a closed interval $[\omega', \gamma']_{\mathcal{R}_1}$ of T_{x_n} such that $\zeta \in [\omega', \gamma']_{\mathcal{R}_1}$. Likewise, $\omega' - a > 0$. Moreover, $\omega' - a \leq \zeta - a < (\beta - \theta) - a < \beta - a$; this contradicts the minimality of $\beta - a$. Thus $\beta \notin \mathcal{R}$. This completes the proof. □

Let D is a unique factorization domain with fraction field F, and $h(x)$ a non-zero polynomial in $F[x]$. According to Lemma 1 on page 152 in [8], $h(x)$ may be represented in the form $h(x) = ah_0(x)$ where $a \in F$ and $h_0(x) \in D[x]$ is a primitive polynomial. Moreover, such a primitive polynomial $h_0(x)$ is determined by h up to unit multipliers in D. For sake of convenience, in what follows, such a primitive polynomial $h_0(x)$ is called *a primitive part* of h over D.

Proposition 3.3. *Let $f \in K[x_1, \ldots, x_n]$, let $\{j_1, \ldots, j_k\}$ be a nonempty subset of $\{1, \ldots, n-1\}$ with complement $\{j_{k+1}, \ldots, j_{n-1}\}$, and $\varrho_{k+1}, \ldots, \varrho_{n-1} \in \{-1, 1\}$. If $C_1, \ldots, C_s$, $C_{s+1}, \ldots, C_r$ is a regular decomposition of $\{\frac{\partial f}{\partial x_{j_1}}, \ldots, \frac{\partial f}{\partial x_{j_k}}\}$ with respect to the lexicographic order $x_n \prec x_{j_{n-1}} \prec \cdots \prec x_{j_1}$ such that $C_i \cap K[x_{j_{k+1}}, \ldots, x_{j_{n-1}}, x_n] = \emptyset$ for $i = 1, \ldots, s$, but $C_i \cap K[x_{j_{k+1}}, \ldots, x_{j_{n-1}}, x_n] \neq \emptyset$ for $i = s+1, \ldots, r$, then the following statements are true:*

(1) *For $i = 1, \ldots, s$, $\frac{\mathrm{Res}(C_i; f+t)}{L_i} \in K(x_{j_{k+1}}, \ldots, x_{j_{n-1}}, x_n)[t]$ where L_i is the leading coefficient of $\mathrm{Res}(C_i; f+t)$ as a polynomial over $K[Tv(C_i)]$ in one variable t.*
(2) *If β is an element, transcendental over $\mathcal{R}$, in the set*

$$\mathcal{V}_{\mathcal{R}_1}\left(g + \epsilon, \frac{\partial g}{\partial x_{j_1}}, \ldots, \frac{\partial g}{\partial x_{j_k}}; x_n\right)$$

where g is the polynomial over $K_{\langle n+1 \rangle}$ obtained from f by substituting $x_{j_i} = \varrho_i \eta_{j_i}$ for $i = k+1, \ldots, n-1$, then

$$\Phi_\ell(\varrho_{k+1}\eta_{j_{k+1}}, \ldots, \varrho_{n-1}\eta_{j_{n-1}}, \beta, \epsilon) = 0 \quad \text{for some } \ell \in \{1, \ldots, s\},$$

where $\Phi_\ell \in K[x_{j_{k+1}}, \ldots, x_{j_{n-1}}, x_n, t]$ is a primitive part of $\frac{\mathrm{Res}(C_\ell; f+t)}{L_\ell}$ over $K[x_{j_{k+1}}, \ldots, x_{j_{n-1}}, x_n]$.

Proof. Put $G_i := \frac{\mathrm{Res}(C_i; f+t)}{L_i}$ for $i = 1, \ldots, r$, and write J for the ideal generated by $P \cup \{f + t\}$ in $K[x_1, \ldots, x_n, t]$ where $P := \{\frac{\partial f}{\partial x_{j_1}}, \ldots, \frac{\partial f}{\partial x_{j_k}}\}$. Denote by J^e the extended ideal of J in $K(x_{j_{k+1}}, \ldots, x_{j_{n-1}}, x_n)[x_{j_1}, \ldots, x_{j_k}, t]$. By Proposition 3.1, $J^e \cap K(x_{j_{k+1}}, \ldots, x_{j_{n-1}}, x_n)[t] \neq \{0\}$. Since $K(x_{j_{k+1}}, \ldots, x_{j_{n-1}}, x_n)[t]$ is a principal ideal ring, $J^e \cap K(x_{j_{k+1}}, \ldots, x_{j_{n-1}}, x_n)[t] = (u)$ for some non-zero $u \in K(x_{j_{k+1}}, \ldots, x_{j_{n-1}}, x_n)[t]$. Then there exists a non-zero polynomial $v \in K[x_{j_{k+1}}, \ldots, x_{j_{n-1}}, x_n]$ such that $uv \in J$. Put $h := uv$. Then $h \in J \cap K[x_{j_{k+1}}, \ldots, x_{j_{n-1}}, x_n, t]$, and $J^e \cap K(x_{j_{k+1}}, \ldots, x_{j_{n-1}}, x_n)[t] = (h)$.

By Proposition 2.2, we have

$$G_i = \prod_{\bar{\alpha}\in \mathrm{RZ}(C_i)} \big(t + f(\bar{\alpha})\big), \quad i = 1, \ldots, r. \tag{1}$$

Since $C_1, \ldots, C_s$, $C_{s+1}, \ldots, C_r$ be a regular decomposition of P with respect to the lexicographic order $x_n \prec x_{j_{n-1}} \prec \cdots \prec x_{j_1}$, by Proposition 2.3 and its proof, we have

$$\sqrt{J} = \bigcap_{\bar{\alpha}\in \Xi} \mathfrak{P}_{(\bar{\alpha}, -f(\bar{\alpha}))}, \tag{2}$$

where $\Xi := \mathrm{RZ}(C_1) \cup \cdots \cup \mathrm{RZ}(C_r)$.

(1) Let $i \in \{1, \ldots, s\}$ and $\bar{\alpha} \in \mathrm{RZ}(C_i)$. By the hypothesis, $C_i \cap K[x_{j_{k+1}}, \ldots, x_{j_{n-1}}, x_n] = \emptyset$, and $\{x_{j_{k+1}}, \ldots, x_{j_{n-1}}, x_n\} \subseteq \mathrm{Tv}(C_i) \subset \Omega_{C_i}$. This implies that

$$\bar{\alpha} = (x_n, x_{j_{n-1}}, \ldots, x_{j_{k+1}}, \alpha_1, \ldots, \alpha_k) \quad \text{where } \alpha_1, \ldots, \alpha_k \in \Omega_{C_i}.$$

By equality (2), $h \in J \subseteq \mathfrak{P}_{(\bar{\alpha}, -f(\bar{\alpha}))}$. So we have $h(\bar{\alpha}, -f(\bar{\alpha})) = 0$, i.e.

$$h\big(x_{j_{k+1}}, \ldots, x_{j_{n-1}}, x_n, -f(\bar{\alpha})\big) = 0.$$

Hence $f(\bar{\alpha})$ is algebraic over the field $K(x_{j_{k+1}}, \ldots, x_{j_{n-1}}, x_n)$. By equality (1), all the coefficients of G_i, as a polynomial in one variable t, are algebraic over $K(x_{j_{k+1}}, \ldots, x_{j_{n-1}}, x_n)$. Observe that $G_i \in K(x_1, \ldots, x_n)[t]$ and $K(x_{j_{k+1}}, \ldots, x_{j_{n-1}}, x_n)$ is algebraically closed in $K(x_1, \ldots, x_n)$. So we get $G_i \in K(x_{j_{k+1}}, \ldots, x_{j_{n-1}}, x_n)[t]$.

(2) Observe that $x_{j_1}, \ldots, x_{j_k}$, $\eta_{j_{k+1}}, \ldots, \eta_{j_{n-1}}$, x_n, ϵ are algebraically independent over K. There is a K-isomorphism σ of the ring $K(x_{j_1}, \ldots, x_{j_k}, x_{j_{k+1}}, \ldots, x_{j_{n-1}}, x_n)[t]$ onto $K(x_{j_1}, \ldots, x_{j_k}, \eta_{j_{k+1}}, \ldots, \eta_{j_{n-1}}, x_n)[\epsilon]$ such that

$$(x_{j_1}, \ldots, x_{j_k}, x_{j_{k+1}}, \ldots, x_{j_{n-1}}, x_n, t) \mapsto (x_{j_1}, \ldots, x_{j_k}, \varrho_{k+1}\eta_{j_{k+1}}, \ldots, \varrho_{n-1}\eta_{j_{n-1}}, x_n, \epsilon).$$

Obviously, $\sigma(J)$ is just the ideal generated by $\{g+\epsilon, \frac{\partial g}{\partial x_{j_1}}, \ldots, \frac{\partial g}{\partial x_{j_k}}\}$ in $K[\eta_{j_{k+1}}, \ldots, \eta_{j_{n-1}}, x_n, x_{j_1}, \ldots, x_{j_k}, \epsilon]$, and $\sigma(h) \in \sigma(J) \cap K[\eta_{j_{k+1}}, \ldots, \eta_{j_{n-1}}, x_n, \epsilon]$.

Since $\beta \in \mathcal{V}_{\mathcal{R}_1}(g + \epsilon, \frac{\partial g}{\partial x_{j_1}}, \ldots, \frac{\partial g}{\partial x_{j_k}}; x_n)$, there exists a $(\beta_{j_1}, \ldots, \beta_{j_k}) \in \mathcal{R}_1^k$ such that $(\beta_{j_1}, \ldots, \beta_{j_k}, \beta)$ is a zero of $\sigma(J)$. This implies that $(\beta_{j_1}, \ldots, \beta_{j_k}, \varrho_{k+1}\eta_{j_{k+1}}, \ldots, \varrho_{n-1}\eta_{j_{n-1}}, \beta, \epsilon)$ is a zero of J and is hence a zero of $\sqrt{J}$. By equality (2), $(\beta_{j_1}, \ldots, \beta_{j_k}, \varrho_{k+1}\eta_{j_{k+1}}, \ldots, \varrho_{n-1}\eta_{j_{n-1}}, \beta, \epsilon)$ is a zero of $\mathfrak{P}_{(\bar{\alpha}_1, -f(\bar{\alpha}_1))}$ for some $\bar{\alpha}_1 \in \Xi$. Since $\Xi = \mathrm{RZ}(C_1) \cup \cdots \cup \mathrm{RZ}(C_r)$, there exists an $\ell \in \{1, \ldots, r\}$ such that $\bar{\alpha}_1 \in \mathrm{RZ}(C_\ell)$. Suppose that $C_\ell \cap K[x_{j_{k+1}}, \ldots, x_{j_{n-1}}, x_n] \neq \emptyset$. Then, there is a polynomial w in $C_\ell \cap K[x_{j_{k+1}}, \ldots, x_{j_{n-1}}, x_n]$. Obviously, $w \in \mathfrak{P}_{(\bar{\alpha}_1, -f(\bar{\alpha}_1))}$. Hence $(\beta_{j_1}, \ldots, \beta_{j_k}, \varrho_{k+1}\eta_{j_{k+1}}, \ldots, \varrho_{n-1}\eta_{j_{n-1}}, \beta, \epsilon)$ is a zero of w, and $w(\varrho_{k+1}\eta_{j_{k+1}}, \ldots, \varrho_{n-1}\eta_{j_{n-1}}, \beta) = 0$. This contradicts the hypothesis that β is transcendental over $\mathcal{R}$. Thus $C_\ell \cap K[x_{j_{k+1}}, \ldots, x_{j_{n-1}}, x_n] = \emptyset$, and $\ell \in \{1, \ldots, s\}$.

Moreover, $h \in J \subseteq \mathfrak{P}_{(\bar{\alpha}_1, -f(\bar{\alpha}_1))}$, and $(\beta_{j_1}, \ldots, \beta_{j_k}, \varrho_{k+1}\eta_{j_{k+1}}, \ldots, \varrho_{n-1}\eta_{j_{n-1}}, \beta, \epsilon)$ is a zero of h. It follows that $h(\varrho_{k+1}\eta_{j_{k+1}}, \ldots, \varrho_{n-1}\eta_{j_{n-1}}, \beta, \epsilon) = 0$. This implies that

h is a non-constant polynomial in $K[x_{j_{k+1}},\dots,x_{j_{n-1}},x_n,t]$. Let $h = h_1h_2\cdots h_m$, where $h_1,\dots,h_m$ are irreducible polynomials in $K[x_{j_{k+1}},\dots,x_{j_{n-1}},x_n,t]$. Then, $h_{i_0} \in \mathfrak{P}_{(\bar{\alpha}_1,-f(\bar{\alpha}_1))}$ for some $i_0 \in \{1,\dots,m\}$. Without loss of generality, we assume that $h_1 \in \mathfrak{P}_{(\bar{\alpha}_1,-f(\bar{\alpha}_1))}$. So we have

$$h_1(\varrho_{k+1}\eta_{j_{k+1}},\dots,\varrho_{n-1}\eta_{j_{n-1}},\beta,\epsilon) = 0.$$

Observe that $x_{j_{k+1}},\dots,x_{j_{n-1}},x_n \in \mathrm{Tv}(C_\ell) \subset \Omega_{C_\ell}$. Hence, $\bar{\alpha}_1 = (x_n,x_{j_{n-1}},\dots,x_{j_{k+1}},\alpha'_1,\dots,\alpha'_k)$ where $\alpha'_1,\dots,\alpha'_k \in \Omega_{C_i}$. So we get

$$h_1\big(x_{j_{k+1}},\dots,x_{j_{n-1}},x_n,-f(\bar{\alpha}_1)\big) = h_1\big(\bar{\alpha}_1,-f(\bar{\alpha}_1)\big) = 0.$$

Since $G_\ell = \prod_{\bar{\alpha}\in \mathrm{RZ}(C_\ell)}(t+f(\bar{\alpha}))$ and $G_\ell \in K(x_{j_{k+1}},\dots,x_{j_{n-1}},x_n)[t]$, G_ℓ and $h_1(x_{j_{k+1}},\dots,x_{j_{n-1}},x_n,t)$ have the same root $-f(\bar{\alpha}_1)$, and Φ_ℓ and h_1 have the same root $-f(\bar{\alpha}_1)$. Since h_1 is irreducible in $K(x_{j_{k+1}},\dots,x_{j_{n-1}},x_n)[t]$, h_1 divides Φ_ℓ in $K(x_{j_{k+1}},\dots,x_{j_{n-1}},x_n)[t]$. This implies that h_1 divides Φ_ℓ in $K[x_{j_{k+1}},\dots,x_{j_{n-1}},x_n,t]$, because h_1 is primitive as a polynomial over $K[x_{j_{k+1}},\dots,x_{j_{n-1}},x_n]$ in one variable t. Observe that $(\varrho_{k+1}\eta_{j_{k+1}},\dots,\varrho_{n-1}\eta_{j_{n-1}},\beta,\epsilon)$ is a zero of h_1. It follows that $\Phi_\ell(\varrho_{k+1}\eta_{j_{k+1}},\dots,\varrho_{n-1}\eta_{j_{n-1}},\beta,\epsilon) = 0$. This completes the proof. □

For the sake of convenience, we need the following

Definition 4. Let D be a commutative ring, and let $\{j_{k+1},\dots,j_{n-1}\}$ be a subset of $\{1,\dots,n-1\}$ where $1 \le k < n-1$. The lexicographic order $x_{j_{k+1}} \prec \cdots \prec x_{j_{n-1}}$ in $D[x_{j_{k+1}},\dots,x_{j_{n-1}}]$ is called the natural order of the set $\{x_{j_{k+1}},\dots,x_{j_{n-1}}\}$ of variables if $j_{k+1} < \cdots < j_{n-1}$. In the case when $k = n-1$, we adopt the convention that the leading coefficient of a is itself with respect to the natural order of the empty set $\{x_{j_{k+1}},\dots,x_{j_{n-1}}\}$ for every non-zero $a \in D$.

Based on Propositions 3.2 and 3.3, the following result may be established.

Theorem 3.4. *Let $f \in K[x_1,\dots,x_n]$, and let a be a finite open endpoint of $\mathfrak{N}(f;x_n)$. Then, one of the following statements is true:*

(1) *$e(a) = 0$ where $e(x_n) \in K[x_n]$ is the leading coefficient of f as a polynomial over $K[x_n]$ in variables $x_1,\dots,x_{n-1}$ with respect to the lexicographic order $x_1 \prec \cdots \prec x_{n-1}$.*
(2) *There is a nonempty subset $\{j_1,\dots,j_k\}$ of $\{1,\dots,n-1\}$ with complement $\{j_{k+1},\dots,j_{n-1}\}$ such that the following condition is satisfied:*

If $C_1,\dots,C_r$ is a regular decomposition of $\{\frac{\partial f}{\partial x_{j_1}},\dots,\frac{\partial f}{\partial x_{j_k}}\}$ with respect to the lexicographic order $x_n \prec x_{j_{n-1}} \prec \cdots \prec x_{j_{k+1}} \prec x_{j_k} \prec \cdots \prec x_{j_1}$, then, for some

$C \in \{C_1, \ldots, C_r\}$ with $C \cap K[x_{j_{k+1}}, \ldots, x_{j_{n-1}}, x_n] = \emptyset$, $e_C(a) = 0$ where $e_C(x_n)$ is the univariate polynomial obtained by the following computations:

- *Compute a primitive part Φ_C of $\frac{\mathrm{Res}(C; f+t)}{L}$ over $K[x_{j_{k+1}}, \ldots, x_{j_{n-1}}, x_n]$, where L is the leading coefficient of $\mathrm{Res}(C; f + t)$ as a polynomial over $K[Tv(C)]$ in one variable t.*
- *Extract the trailing coefficient ρ_C of Φ_C as a polynomial over $K[x_{j_{k+1}}, \ldots, x_{j_{n-1}}, x_n]$ in one variable t.*
- *Extract the leading coefficient $e_C(x_n)$ of ρ_C as a polynomial over $K[x_n]$ in variables $x_{j_{k+1}}, \ldots, x_{j_{n-1}}$ with respect to the natural order of $\{x_{j_{k+1}}, \ldots, x_{j_{n-1}}\}$.*

Proof. By Proposition 3.2, one of the following statements is true:

(i) $e(a) = 0$ where $e(x_n) \in K[x_n]$ be the leading coefficient of f as a polynomial over $K[x_n]$ in variables $x_1, \ldots, x_{n-1}$ with respect to the lexicographic order $x_1 \prec \cdots \prec x_{n-1}$.

(ii) For some nonempty subset $\{j_1, \ldots, j_k\}$ of $\{1, \ldots, n-1\}$ with complement $\{j_{k+1}, \ldots, j_{n-1}\}$ and certain $\varrho_{k+1}, \ldots, \varrho_{n-1} \in \{1, -1\}$, the set

$$\mathcal{V}_{\mathcal{R}_1}\left(g + \epsilon, \frac{\partial g}{\partial x_{j_1}}, \ldots, \frac{\partial g}{\partial x_{j_k}}; x_n\right),$$

where g is the polynomial over $K_{\langle n+1\rangle}$ obtained from f by substituting $x_{j_i} = \varrho_i \eta_{j_i}$ for $i = k+1, \ldots, n-1$, contains a point β such that the following conditions are satisfied:

(ii-1) $\beta - a \in \mathcal{M}$.

(ii-2) $\beta \notin \mathcal{R}$, i.e. β is transcendental over $\mathcal{R}$.

Now assume that statement (ii) is true, and adopt the symbols in Proposition 3.3. By Proposition 3.3, $\Phi_C(\varrho_{k+1}\eta_{j_{k+1}}, \ldots, \varrho_{n-1}\eta_{j_{n-1}}, \beta, \epsilon) = 0$ for some $C \in \{C_1, \ldots, C_r\}$ with $C \cap K[x_{j_{k+1}}, \ldots, x_{j_{n-1}}, x_n] = \emptyset$. Write Φ_C in the form $\Phi_C = t^m \Psi_C$ where $m \geq 0$ and $\Psi_C \in K[x_{j_{k+1}}, \ldots, x_{j_{n-1}}, x_n, t]$ with $\Psi_C(x_{j_{k+1}}, \ldots, x_{j_{n-1}}, x_n, 0) \neq 0$. Then $\rho_C = \Psi_C(x_{j_{k+1}}, \ldots, x_{j_{n-1}}, x_n, 0)$, and $\Psi_C(\varrho_{k+1}\eta_{j_{k+1}}, \ldots, \varrho_{n-1}\eta_{j_{n-1}}, \beta, \epsilon) = 0$. It is easy to see that $\beta \in \mathcal{A}_1$ and $\epsilon \in \mathcal{M}_1$. Using the homomorphism π_1 and putting $\beta' := \pi_1(\beta)$, we have

$$\begin{aligned}
\rho_C\big(\varrho_{k+1}\eta_{j_{k+1}}, \ldots, \varrho_{n-1}\eta_{j_{n-1}}, \beta'\big) &= \Psi_C\big(\varrho_{k+1}\eta_{j_{k+1}}, \ldots, \varrho_{n-1}\eta_{j_{n-1}}, \beta', 0\big) \\
&= \Psi_C\big(\varrho_{k+1}\eta_{j_{k+1}}, \ldots, \varrho_{n-1}\eta_{j_{n-1}}, \pi_1(\beta), \pi_1(\epsilon)\big) \\
&= \pi_1\big(\Psi_C(\varrho_{k+1}\eta_{j_{k+1}}, \ldots, \varrho_{j_{n-1}}\eta_{n-1}, \beta, \epsilon)\big) \\
&= \pi_1(0) = 0.
\end{aligned}$$

As in the proof of Proposition 3.2, represent ρ in the following form

$$\rho_C = e_C(x_n)x_{j_{k+1}}^{d_{k+1}}\cdots x_{j_{n-1}}^{d_{n-1}} + e_1(x_n)x_{j_{k+1}}^{d_{1,k+1}}\cdots x_{j_{n-1}}^{d_{1,n-1}} + \cdots + e_m(x_n)x_{j_{k+1}}^{d_{m,k+1}}\cdots x_{j_{n-1}}^{d_{m,n-1}},$$

where $e_i(x_n) \in K[x_n]$, $i = 1,\ldots,m$, and $e_C(x_n)$ is the leading coefficient of ρ_C as a polynomial over $K[x_n]$ in variables $x_{j_{k+1}},\ldots,x_{j_{n-1}}$ with respect to the natural order of $\{x_{j_{k+1}},\ldots,x_{j_{n-1}}\}$.

By the above representation, we have

$$e_C\big(\beta'\big) + \mu_1 + \cdots + \mu_m = \frac{\rho_C(\varrho_{k+1}\eta_{j_{k+1}},\ldots,\varrho_{n-1}\eta_{j_{n-1}},\beta')}{(\varrho_1 j_{k+1})^{d_{k+1}}\cdots(\varrho_{n-1}\eta_{j_{n-1}})^{d_{n-1}}} = 0,$$

where $\mu_i := e_i(\beta')\cdot\frac{(\varrho_1\eta_{j_{k+1}})^{d_{i,k+1}}\cdots(\varrho_{n-1}\eta_{j_{n-1}})^{d_{i,n-1}}}{(\varrho_1 j_{k+1})^{d_{k+1}}\cdots(\varrho_{n-1}\eta_{j_{n-1}})^{d_{n-1}}}$, $i = 1,\ldots,m$.

Since $\beta' - a = (\pi_1(\beta) - \beta) + (\beta - a) \in \mathcal{M}_1 + \mathcal{M} \subseteq \mathcal{M}$, we have $\pi(\beta') = a$. It is easy to prove that $\mu_i \in M$ for $i = 1,\ldots,m$. By the homomorphism π, we further have

$$e_C(a) = \pi\big(e_C\big(\beta'\big) + \mu_1 + \cdots + \mu_m\big) = \pi(0) = 0.$$

This completes the proof. □

4. Algorithms and examples

In the final section, we establish two algorithms based on Theorem 3.4. In order to compare with the original algorithm in [24], we use the new algorithm to treat several examples with the aid of the computer algebraic system **Maple 15**. Our new algorithms have been embedded into a general program, named **DecidePsd**, to decide the semi-definiteness of a polynomial with rational coefficients. The software named **DecidePsd** can be found in [22].

In our new algorithms, the involved ordered fields are assumed to admit an effective method of finding an isolating set for every non-zero univariate polynomial. For a finite set U of non-zero univariate polynomials in $K[x]$, a finite subset Γ of K is called an isolating set for U, if the following conditions are satisfied: (1) For every $a \in \Gamma$ and any $f \in U$, $f(a) \neq 0$; (2) If α is a zero of a polynomial $f(x) \in U$ in R, there are a, $b \in \Gamma$ with $a < b$ such that $]a,b[_R \cap \mathrm{Root}_R(U) = \{\alpha\}$ where $\mathrm{Root}_R(U) := \{z \in R \mid u(z) = 0$ for some $u \in U\}$. For the sake of convenience, we define $\{0\}$ to be the only isolating set of U if $\mathrm{Root}_R(U) = \emptyset$. So, every isolating set is nonempty for any finite set of non-zero univariate polynomials. According to Theorem 8.115 in [4] or Theorem 8.5.7 in [16], the field $\mathbb{Q}$ of rational numbers admits an effective method of finding an isolating set for every finite set of non-zero univariate polynomials.

Algorithm 4.1 *(The elimination method for semi-definiteness).*
Structure: a computable ordered field $(K,\leq)$ admitting an effective method of finding isolating sets for univariate polynomials.
Input: a polynomial $f \in K[x_1,\ldots,x_n]$ containing really the variable x_n where $n \geq 2$.
Output: a finite subset Γ of K such that

- f is positive semi-definite if and only if so is $f(x_1, \ldots, x_{n-1}, \gamma)$ for all $\gamma \in \Gamma$.

Procedure:

Step 1. For every nonempty subset $\{j_1, \ldots, j_k\}$ of $\{1, \ldots, n-1\}$ with complement $\{j_{k+1}, \ldots, j_{n-1}\}$, create a finite subset $S_{j_1 \ldots j_k}$ of $K[x_n]$ by the following computations:

Step 1.1. Compute a regular decomposition $C_{j_1 \ldots j_k,1}, \ldots, C_{j_1 \ldots j_k, r_{j_1 \ldots j_k}}$ of $\{\frac{\partial f}{\partial x_{j_i}} \mid 1 \leq i \leq k\}$ with respect to the lexicographic order $x_n \prec x_{j_{n-1}} \prec \cdots \prec x_{j_1}$, pick out all the chains $C_{j_1 \ldots j_k,1}, \ldots, C_{j_1 \ldots j_k, s_{j_1 \ldots j_k}}$ that are disjoint with $K[x_{j_1}, \ldots, x_{j_k}, x_n]$, and compute $\mathrm{Res}(C_{j_1 \ldots j_k,i}; f + t)$ for $i = 1, \ldots, s_{j_1 \ldots j_k}$.

Step 1.2. For $i = 1, \ldots, s_{j_1 \ldots j_k}$, extract the leading coefficient $L_{j_1 \ldots j_k,i}$ of $\mathrm{Res}(C_{j_1 \ldots j_k,i}; f + t)$ as a polynomial in one variable t. (Note: By Proposition 3.3, $\frac{\mathrm{Res}(C_{j_1 \ldots j_k,i}; f+t)}{L_{j_1 \ldots j_k,i}} \in K(x_{j_1}, \ldots, x_{j_k}, x_n)[t]$, $i = 1, \ldots, s_{j_1 \ldots j_k}$.)

Step 1.3. For $i = 1, \ldots, s_{j_1 \ldots j_k}$, compute a primitive part $\Phi_{j_1 \ldots j_k,i}$ of $\frac{\mathrm{Res}(C_{j_1 \ldots j_k,i}; f+t)}{L_{j_1 \ldots j_k,i}}$ over $K[x_{j_1}, \ldots, x_{j_k}, x_n]$, extract the trailing coefficient $\rho_{j_1 \ldots j_k,i}$ of $\Phi_{j_1 \ldots j_k,i}$ as a polynomial in one variable t, and extract the leading coefficient $e_{j_1 \ldots j_k,i}(x_n)$ of $\rho_{j_1 \ldots j_k,i}$ as a polynomial over $K[x_n]$ with respect to the natural order of $\{x_{j_{k+1}}, \ldots, x_{j_{n-1}}\}$. Set $S_{j_1 \ldots j_k} := \{e_{j_1 \ldots j_k,i}(x_n) \mid i = 1, \ldots, s_{j_1 \ldots j_k}\}$.

Step 2. Find an isolating set Γ for the set $\{e(x_n)\} \cup \bigcup_\lambda S_\lambda$ where $e(x_n)$ is the leading coefficient of f as a polynomial over $K[x_n]$ with respect to the lexicographic order $x_1 \prec \cdots \prec x_{n-1}$, and λ runs over all the nonempty subsets of $\{1, \ldots, n-1\}$.

Step 3. RETURN(Γ).

Proof of correctness. Assume that $f(x_1, \ldots, x_{n-1}, \gamma)$ is not positive semi-definite for some $\gamma \in \Gamma$. Then it is obvious that $f(x_1, \ldots, x_{n-1}, x_n)$ is not positive semi-definite.

Conversely, assume that $f(x_1, \ldots, x_n)$ is not positive semi-definite. Then $\mathfrak{N}_R(f; x_n) \neq \emptyset$. In the case when $\mathfrak{N}_R(f; x_n) = R$, $f(x_1, \ldots, x_{n-1}, \gamma)$ is not positive semi-definite for any $\gamma \in \Gamma$. In the case when $\mathfrak{N}_R(f; x_n) \neq R$, $\mathfrak{N}_R(f; x_n)$ possesses at least one finite open endpoint a. Denote by U the set of univariate polynomials indicated in Step 2, i.e. $U := \{e(x_n)\} \cup \bigcup_\lambda S_\lambda$ where $e(x_n)$ is the leading coefficient of f as a polynomial over $K[x_n]$ with respect to the lexicographic order $x_1 \prec \cdots \prec x_{n-1}$, and λ runs over all the nonempty subsets of $\{1, \ldots, n-1\}$. According to Theorem 3.4 and the commutations in Step 1, all the finite endpoints of $\mathfrak{N}_R(f; x_n)$ are contained in $\mathrm{Root}_R(U)$. Of course, $a \in \mathrm{Root}_R(U)$. Since Γ is an isolating set for U, there are $b, c \in \Gamma$ with $b < c$ such that $]b, c[_R \cap \mathrm{Root}_R(U) = \{a\}$. Thus the open interval $]b, c[_R$ contains only the endpoint a of $\mathfrak{N}_R(f; x_n)$. Thereby either $b \in \mathfrak{N}_R(f; x_n)$ or $c \in \mathfrak{N}_R(f; x_n)$. This implies that either $f(x_1, \ldots, x_{n-1}, b)$ or $f(x_1, \ldots, x_{n-1}, c)$ is not positive semi-definite. The correctness of Algorithm 4.1 is verified. □

Based on Algorithm 4.1, the following algorithm is easily established. For the sake of convenience, we adopt the convention that $D^0 := \{(\,)\}$ for any set D.

Algorithm 4.2 *(Deciding the semi-definiteness of multivariate polynomials).*
Structure: a computable ordered field $(K, \leq)$ admitting an effective method of finding isolating sets for univariate polynomials
Input: a polynomial $f \in K[x_1, \ldots, x_n]$ where $n \geq 2$.
Output: the word "**true**" if f is positive semi-definite, or a point $(a_1, \ldots, a_n) \in K^n$ such that $f(a_1, \ldots, a_n) < 0$.

Procedure:

Step 1. Compute inductively a finite subset Δ_i of $K[x_1, \ldots, x_{n-i}] \times K^i$ for $i = 0, 1, n-1$ as follows:

- $\Delta_0 := \{(f, (\,))\}$.
- Assume that Δ_{i-1} has been obtained, where $1 \leq i < n-1$. For every $(g, \bar{b}) \in \Delta_{i-1}$, compute by Algorithm 4.1 a finite subset $\Gamma_{(g,\bar{b})}$ such that g is positive semi-definite if and only if $g(x_1, \ldots, x_{n-i}, a)$ is positive semi-definite for all $a \in \Gamma_{(g,\bar{b})}$. Put $\Delta_{(g,\bar{b})} := \{(g(x_1, \ldots, x_{n-i}, a), (a, \bar{b})) \mid a \in \Gamma_{(g,\bar{b})}\}$, and put

$$\Delta_i := \bigcup_{(g,\bar{b}) \in \Delta_{i-1}} \Delta_{(g,\bar{b})}.$$

Step 2. Assume that $\Delta_{n-1} = \{(h_1(x_1), \bar{b}_1), \ldots, (h_m(x_1), \bar{b}_m)\}$. For i from 1 to m, find an isolating set Γ_i for $h_i(x_1)$. If $h_i(a) < 0$ for some i and some $a \in \Gamma_i$, RETURN $((a, \bar{b}_i))$. Else, RETURN (**true**).

Proof of correctness. It follows from Algorithm 4.1 and the following obvious fact:

- If Γ is an isolating set of a univariate polynomial $h(x)$, then $h(x)$ is positive semi-definite if and only if $h(a) > 0$ for all $a \in \Gamma$. □

As an illustration of Algorithm 4.2, we proceed to investigate the following example.

Example 1. Let $f(x, y, z) = 4x^2z^2y^2 + 8z^2xy + 4z^2 + 4x^2zy^2 + 8xzy + 4z + 2x^2y^2 + 4xy + x^4y^2 + 2x^3y + x^2 + 2x^3y^2 + 4x^2y + 2x + 1$. Decide whether or not $f(x, y, z)$ is positive semi-definite.

Process of Computing. All the partial derivatives of $f(x, y, z)$ are computed as follows:

$$\frac{\partial f}{\partial x} = 8xz^2y^2 + 8z^2y + 8xzy^2 + 8zy + 4xy^2 + 4y + 4x^3y^2 + 6x^2y + 2x + 6x^2y^2 + 8xy + 2,$$

$$\frac{\partial y}{\partial y} = 8x^2z^2y + 8z^2x + 8x^2zy + 8xz + 4x^2y + 4x + 2x^4y + 2x^3 + 4x^3y + 4x^2,$$
$$\frac{\partial f}{\partial z} = 8x^2zy^2 + 16xzy + 8z + 4x^2y^2 + 8xy + 4.$$

According to Algorithm 4.2, we proceed to perform the following computations:

(1) (Eliminate the variable z) Observe that all the nonempty subsets of $\{x, y\}$ are $\{x, y\}$, $\{x\}$ and $\{y\}$.

(1.1) With respect to the lexicographic order $z \prec y \prec x$, compute a regular decomposition of $\{\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\}$ as follows:

$$C_1 := [xy + 1], \qquad C_2 := \big[\big(4z^2 + 4z + 2\big)y + 1, x\big], [2z + 1, x + 1].$$

Observing that $[2z + 1, x + 1] \cap \mathbb{Q}[z] \neq \emptyset$, we only consider C_1 and C_2, and get

$$\mathrm{Res}(C_1; f + t) = -y^4 + ty^4, \qquad \mathrm{Res}(C_2; f + t) = 1 + 4z^2 + 4z + t.$$

Observe that the leading coefficient of $-y^4 + ty^4$, as a polynomial in one variable t, is y^4, and $\frac{-y^4+ty^4}{y^4} = t - 1$. Extracting the trailing coefficients of $t - 1$ and $1 + 4z^2 + 4z + t$ as polynomials in one variable t, we get -1 and $1 + 4z^2 + 4z$ respectively.

(1.2) With respect to the lexicographic order $z \prec y \prec x$, compute a regular decomposition of $\{\frac{\partial f}{\partial x}\}$ as follows:

$$C_3 := [xy + 1], \qquad C_4 := \big[2x^2y + (3y + 1)x + \big(4z^2 + 4z + 2\big)y + 1\big].$$

So we get

$$\mathrm{Res}(C_3; f + t) = -y^4 + ty^4, \quad \text{and} \quad \mathrm{Res}(C_4; f + t) = \Phi_4(y, z, t),$$

where Φ_4 is a polynomial of 52 terms in $\mathbb{Q}[y, z, t]$.

Extracting the trailing coefficients of $-y^4 + ty^4$ and $\Phi_4(y, z, t)$ as polynomials in one variable t, we get $-y^4$ and $\psi_4(y, z)$ respectively, where $\psi_4(y, z)$ is a polynomial of 38 terms in $\mathbb{Q}[y, z]$. By extracting the leading coefficients of $-y^4$ and $\psi_4(y, z)$ as polynomials in one variable y, we get -1 and $8 + 80z + 368z^2 + 1024z^3 + 1888z^4 + 2368z^5 + 1984z^6 + 1024z^7 + 256z^8$ respectively.

(1.3) With respect to the lexicographic order $z \prec x \prec y$, compute a regular decomposition of $\{\frac{\partial f}{\partial y}\}$ as follows:

$$C_5 := [xy + 1], [x], \big[2x + x^2 + 4z + 4z^2 + 2\big].$$

Since both $[x]$ and $[2x + x^2 + 4z + 4z^2 + 2]$ meet $\mathbb{Q}[x, z]$, we only consider C_5, and get

$$\mathrm{Res}(C_5; f + t) = -x^2 + x^2t.$$

Extract the trailing coefficients $-x^2$ of $-x^2+x^2t$ as a polynomial in one variable t, and extract the leading coefficients -1 of $-x^2$.

(1.4) Extract the leading coefficient 1 of f as a polynomial over $\mathbb{Q}[z]$ respect to the lexicographic order $y \prec x$, and find such an isolating set Γ_1 of $\{1, -1, 1+4z^2+4z, 8+80z+368z^2+1024z^3+1888z^4+2368z^5+1984z^6+1024z^7+256z^8\}$ as follows:

$$\Gamma_1 = \left\{-\frac{3}{2}, \frac{1}{2}\right\}.$$

So we get

$$\Delta_1 := \left\{\left(g(x,y), \left(-\frac{3}{2}\right)\right), \left(g(x,y), \left(\frac{1}{2}\right)\right)\right\}$$

where $g := f(x,y,-\frac{3}{2})(= f(x,y,\frac{1}{2})) = 5x^2y^2+10xy+4+x^4y^2+2x^3y+x^2+2x^3y^2+4x^2y+2x$.

(2) (Eliminate the variable y) Observe that $\{x\}$ is the only nonempty subset of $\{x\}$.

(2.1) With respect to the lexicographic order $y \prec x$, compute a regular decomposition of $\{\frac{\partial g}{\partial x}\}$ as follows:

$$C_6 := [xy+1], \qquad C_7 := \left[2x^2y+(3y+1)x+5y+1\right].$$

So we get $\mathrm{Res}(C_6; g+t) = -y^4+y^4t$, and $\mathrm{Res}(C_7; g+t) = \Phi_7(y,t)$, where $\Phi_7(y,t) = y^2(3-20y-4yt+38y^2-108y^3-164y^3t+587y^4-600y^5+t+54y^2t-47y^4t+500y^6+16y^2t^2)$.

Extracting the trailing coefficients of $-y^4+ty^4$ and $\Phi_7(y,t)$ as polynomials in one variable t, we get $-y^4$ and $y^2(3-108y^3-20y+587y^4+38y^2-600y^5+500y^6)$ respectively.

(2.2) Extract the leading coefficient y^2 of g as a polynomial over $\mathbb{Q}[y]$ in one variable x, and find such an isolating set Γ_2 of $\{y^2, -y^4, y^2(3-108y^3-20y+587y^4+38y^2-600y^5+500y^6)\}$ as follows:

$$\Gamma_2 = \{-1, 1\}.$$

So we get

$$\Delta_2 := \left\{\left(h_1(x), \left(-1, -\frac{3}{2}\right)\right), \left(h_1(x), \left(-1, \frac{1}{2}\right)\right), \left(h_2(x), \left(1, -\frac{3}{2}\right)\right), \left(h_2(x), \left(1, \frac{1}{2}\right)\right)\right\}$$

where $h_1(x) := g(x,-1) = 2x^2-8x+4+x^4$ and $h_2(x) := g(x,1) = 10x^2+12x+4+x^4+4x^3$.

(3) Finding an isolating set of $h_1(x)$, we get $\Gamma_3 = \{-\frac{1}{2}, 1, \frac{5}{2}\}$. Computing the values of $h_1(x)$ at $x = -\frac{1}{2}$, 1, $\frac{5}{2}$, we get $h_1(-\frac{1}{2}) = \frac{137}{16} > 0$ but $h_1(1) = -1 < 0$.

According to Algorithm 4.2, $f(x,y,z)$ is not positive semi-definite, and $f(1,-1,-\frac{3}{2}) < 0$.

Now we use the software **DecidePsd** to treat several examples. The following examples were done on an Intel(R) Core(TM)2 Quad CPU computer with 2 GB RAM.

Example 2. Decide the positive semi-definiteness of the following polynomials.

(1) $f_1 = x^4 + 2x^2z + x^2 - 2xyz + 2y^2z^2 - 2yz^2 + 2z^2 - 2x + 2yz + 1/2$;

(2) $f_2 = x^4 + 2x^2z + x^2 - 2xyz + 2y^2z^2 - 2yz^2 + 2z^2 - 2x + 2yz + 1$;

(3) $f_3 = x^4y^4 - 2x^5y^3z^2 + x^6y^2z^4 + 2x^2y^3z - 4x^3y^2z^3 + 2x^4yz^5 + y^2z^2 - 2xyz^4 + x^2z^6$;

(4) $f_4 = x^4y^4 - 2x^5y^3z^2 + x^6y^2z^4 + 2x^2y^3z - 4x^3y^2z^3 + 2x^4yz^5 + y^2z^2 - 2xyz^4 + \frac{99}{100}x^2z^6$;

(5) $f_5 = x^4 + y^4 + z^4 + w^6 + 2z^2w^3 + 2x^2w + 2x^2z + 3x^2 + w^2 + 2zw + z^2 + 2z + 2w + 1$;

(6) $f_6 = x^4 + 4x^2y^2 + 2xyz^2 + 2xyw^2 + y^4 + z^4 + w^4 + 2z^2w^2 + 2x^2w + 2y^2w + 2xy + 3w^2 + 2z^2 + 1$;

(7) $f_7 = x^4 + 4x^2y^2 + 2xyz^2 + 2xyw^2 + y^4 + z^4 + w^4 + 2z^2w^2 + 2x^2w + 2y^2w + 2xy + 3w^2 - 2z^2 + 1$;

(8) $f_8 = x^6 + y^6 + z^6 + w^6 + 2z^2w^3 + x^4 + y^4 + z^4 + 2x^2w + 2x^2z + 3x^2 + w^2 + 2zw + z^2 + 2z + 2w + 1$;

(9) $f_9 = 2x_1^4 + 2x_1^2 + 2x_1^2x_4 - 2x_1^2x_2 + 2x_4 - 2x_2 + x_4^2 - 2x_4x_2 + x_2^2 + x_3^2x_4^2 + 2x_3x_4x_5 + 2x_5^2 - 2x_1^2x_2^2 + 2x_1^2x_5 + x_2^4 - 2x_2^2x_5 + 1$;

(10) $f_{10} = 2x_1^4 + 2x_1^2 + 2x_1^2x_4 - 2x_1^2x_2 + 2x_4 - 2x_2 + x_4^2 - 2x_4x_2 + x_2^2 + x_3^2x_4^2 + 2x_3x_4x_5 + 2x_5^2 - 2x_1^2x_2^2 + 2x_1^2x_5 + x_2^4 - 2x_2^2x_5 + \frac{9999}{10\,000}$.

Let $[\cdot]_1, \ldots, [\cdot]_{10}$ stand for the lexicographic orders $[x, y, z]$, $[x, y, z]$, $[x, y, z]$, $[x, y, z]$, $[x, y, z, w]$, $[x, y, z, w]$, $[x, y, z, w]$, $[x, y, z, w]$, $[x_1, x_2, x_3, x_4, x_5]$ and $[x_1, x_2, x_3, x_4, x_5]$ respectively. By Calling **DecidePsd**$(f_i, [\cdot]_i)$ for $i = 1, \ldots, 10$, the respective outputs are

$$\left[-\frac{13}{8}, 1, -\frac{41}{16}\right], \quad \text{“true”}, \quad \text{“true”}, \quad [-1, 1, -1], \quad \text{“true”}, \quad \text{“true”},$$

$$\left[\frac{3}{4}, -\frac{3}{4}, -\frac{49}{32}, -\frac{1}{8}\right], \quad \text{“true”}, \quad \text{“true”} \quad \text{and} \quad \left[0, -1, \frac{1}{2}, -2, 1\right].$$

Table 1 gives a comparison with the original algorithm in [24] in respect of the CPU times. It shows that the efficiency of the new algorithm is higher for polynomials in more than two variables. In the table, the CPU times are given in seconds.

Table 1
Table of CPU times.

Example	1	2	3	4	5	6	7	8	9	10
Original	1.015	0.937	1.156	2.046	139.2	> 500	> 500	> 500	> 500	> 500
New	0.968	0.718	0.921	0.968	0.937	1.359	2.375	2.515	4.062	17.71

⋆ “> 500” means that there is no result in 500 seconds.

Acknowledgments

This work is partially supported by the National Natural Science Foundation of China (Grant Nos. 11161034, 11371143). The authors are very grateful to the referees for their valuable suggestions.

References

[1] P. Aubry, D. Lazard, M. Moreno Maza, On the theories of triangular sets, J. Symbolic Comput. 28 (1999) 105–124.
[2] S. Basu, R. Pollack, M.-F. Roy, Algorithms in Real Algebraic Geometry, Algorithms and Computation in Math., vol. 10, Springer-Verlag, Berlin, 2003.
[3] E. Becker, V. Powers, T. Wörmann, Deciding Positivity of Real Polynomials, Real Algebraic Geometry and Ordered Fields, Contemporary Math., vol. 253, Amer. Math. Soc., Providence, 2000, pp. 19–23.
[4] T. Becker, V. Weispfenning, H. Kredel, Gröbner Bases: A Computational Approach to Commutative Algebra, Springer-Verlag, New York, Berlin, Heidelberg, 1993.
[5] J. Bochnak, M. Coste, M.-F. Roy, Real Algebraic Geometry, Springer-Verlag, New York, Berlin, Heidelberg, 1998.
[6] H.K. Bose, E.I. Jury, Inner algorithm to test for positive definiteness of arbitrary binary forms, IEEE Trans. Automat. Control 20 (1) (1975) 169–170.
[7] N.K. Bose, A.R. Modarressi, General procedure for multivariable polynomial positivity test with control applications, IEEE Trans. Automat. Control 21 (5) (1976) 696–701.
[8] N. Jacobson, Basic Algebra I, 2nd edition, W.H. Freeman and Company, New York, 1985.
[9] M. Kalkbrener, Three contributions of elimination theory, Ph.D. thesis, University of Linz, Austria, 1991.
[10] M. Kalkbrener, A generalized Euclidean algorithm for computing triangular representations of algebraic varieties, J. Symbolic Comput. 15 (1993) 143–167.
[11] M. Knebusch, On the extension of real places, Comment. Math. Helv. 48 (1973) 354–369.
[12] E. Kunz, Introduction to Commutative Algebra and Algebraic Geometry, Birkhäuser, Boston, Basel, Stuttgart, 1985.
[13] T.Y. Lam, The Theory of Ordered Fields, Lecture Notes in Pure and Appl. Math., vol. 55, M. Dekker, New York, 1980.
[14] S. Liang, J. Zhang, A complete discrimination system for polynomials with complex coefficients and its automatic generation, Sci. China Ser. E 42 (1999) 113–128.
[15] M. Moreno Maza, On triangular decompositions of algebraic varieties, MEGA-2000 conference, Bath, UK, England, 2000.
[16] B. Mishra, Algorithmic Algebra, Texts and Monographs in Computer Science, Springer-Verlag, New York, Berlin, Heidelberg, 1993.
[17] A. Prestel, Lectures on Formally Real Fields, Lecture Notes in Math., vol. 1093, Springer-Verlag, Berlin, Heidelberg, New York, 1984.
[18] J. Ritt, Differential Equations from the Algebraic Standpoint, vol. 14, American Mathematical Society, New York, 1932.
[19] J. Ritt, Differential Algebra, Dover Publications, New York, 1950.
[20] W.T. Wu, On zeros of algebraic equations—an application of Ritt principle, Kexue Tongbao 31 (1) (1986) 1–5.
[21] W.T. Wu, Mathematics Mechanization: Mechanical Geometry Theorem-Proving, Mechanical Geometry Problem-Solving and Polynomial Equations-Solving, Science Press/Kluwer Academic Publishers, Beijing/Dordrecht, Boston, London, 2000.
[22] S. Xiao, The software **DecidePsd**, http://www.gmail.com, 2013, mailbox: algebrajournal@gmail.com, password: referee2013.
[23] L. Yang, J. Zhang, Searching dependency between algebraic equations: an algorithm applied to automated reasoning, Technical Report IC/91/6, International Atomic Energy Agency, Miramare, Trieste, Italy, 1991.
[24] G. Zeng, X. Zeng, An effective decision method for semidefinite polynomials, J. Symbolic Comput. 37 (2004) 83–99.