An effective decision method for semidefinite polynomials

Zeng Guangxing\textsuperscript{a,}\textsuperscript{*}, Zeng Xiaoning\textsuperscript{b}

\textsuperscript{a}Department of Mathematics, Nanchang University, Nanchang, 330047, China
\textsuperscript{b}Department of Mathematics, Guangdong Education Institute, Guangzhou 510303, China

Received 7 September 2002; accepted 16 February 2003

Abstract

The purpose of this paper is to present an effective method of deciding the semidefiniteness 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. Based on this method, the decision of the semidefiniteness 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. With the aid of the computer algebra system Maple, our method is used to solve several examples.

© 2003 Elsevier Ltd. All rights reserved.

1. Introduction

The study of semidefinite polynomials should be traced to the well-known Hilbert’s 17th problem (see Hilbert, 1901). As his solution to Hilbert’s 17th problem, Artin (1927) affirmed the representation of positive semidefinite polynomials as sums of squares of rational functions. However, Artin did not give an effective method for deciding whether or not a given polynomial is semidefinite, since his solution is only a qualitative conclusion. Theoretically, the Tarski–Seidenberg principle (see Tarski, 1951; Seidenberg, 1954) gives a decision method for semidefinite polynomials, but it would induce so many systems of equalities and inequalities as to hardly work in practice. The question of deciding the semidefiniteness of multivariate polynomials arises in many areas, e.g. automated theorem proving in ordered geometry, the study of inequalities and the computation of real radicals of polynomial ideals. The decision of semidefinite polynomials has been studied extensively by many researchers (for example, see Becker et al., 2000; Bose and Jury, 1975;
Bose and Modarressi, 1976; Liang and Zhang, 1999). However, either these algorithms are valid only for binary polynomials, or these algorithms involve complicated calculations so that some examples cannot be computed in a reasonable amount of time.

In this paper, we shall give an effective method of deciding the semidefiniteness 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. Based on our method, the decision of the semidefiniteness 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.

Let \((K, \leq)\) be a computable ordered field with real closure \(R\), and \(K[X] := K[x_1, \ldots, x_n]\) the polynomial ring in \(n\) variables over \(K\). For a non-zero \(f(X) \in K[X]\), we say that \(f\) is positive (respectively negative) semidefinite on \(R\) if \(f(a_1, \ldots, a_n) \geq 0\) (respectively \(f(a_1, \ldots, a_n) \leq 0\)) for any \(a_1, \ldots, a_n \in R\). \(f\) is called positive (respectively negative) definite on \(R\) if \(f(a_1, \ldots, a_n) > 0\) (respectively \(f(a_1, \ldots, a_n) < 0\)) for any \(a_1, \ldots, a_n \in R\). As a main result in this paper, we establish the following theorem:

**Theorem 1.** Let \((K, \leq)\) be a computable ordered field with real closure \(R\), let \(f(x_1, \ldots, x_n)\) be a polynomial in \(n\) variables over \(K\), and \(n \geq 2\). Then a non-zero univariate polynomial \(p(x_n)\) over \(K\) may be effectively computed such that for any isolating set \(\Gamma^*\) for \(p(x_n)\), \(f(x_1, \ldots, x_n)\) is positive semidefinite on \(R\) if and only if \(f(x_1, \ldots, x_{n-1}, a)\) is positive semidefinite on \(R\) for every \(a \in \Gamma^*\).

For a non-zero univariate polynomial \(f(x) \in K[x]\) with zeros in \(R\), a finite subset \(\Gamma\) of \(K\) is called an isolating set for \(f(x)\), if the following conditions are satisfied: (1) For every \(a \in \Gamma\), \(f(a) \neq 0\); (2) For any zero \(\alpha\) of \(f(x)\) in \(R\), there are \(a, b \in \Gamma\) with \(a < b\) such that the open interval \(]a, b[\) contains only the zero \(\alpha\) of \(f(x)\). For the sake of convenience, we define \([0]\) to be the only isolating set of \(f(x)\) for every non-zero \(f(x) \in K[x]\) without zeros in \(R\). Hence, every isolating set is non-empty for any non-zero univariate polynomial. According to Theorem 8.115 in Becker et al. (1993), the field \(\mathbb{Q}\) of rational numbers admits an effective method of finding an isolating set for every non-zero univariate polynomial. Hence, our conclusion applies to testing the semidefiniteness of multivariate polynomials over \(\mathbb{Q}\). As applications of our decision method, we make use of the computer algebra system Maple 7 to treat several examples in the cases of ternary and quaternary polynomials. In this paper, the well-known Wu’s method (see Wu, 1984) plays an important role. The efficiency of our method is mainly dependent on that of Wu’s method.

2. Preliminaries

In this section, we will establish some results on polynomial ideals over a field of characteristic 0, which are useful for the coming discussion. Note that every field extension of \(K\) is of characteristic 0, if \((K, \leq)\) is a computable ordered field.

Denote by \(F\) a field of characteristic 0 with algebraic closure \(A\), and \(F[X]\) the polynomial ring over \(F\) in \(n\) variables \(x_1, \ldots, x_n\). As usual, for a polynomial \(f \in F[X]\), \(f\) is called non-singular, if the system of equations \(f = 0, \partial f/\partial x_i = 0, i = 1, \ldots, n,\)
has no solution in $A$, equivalently $1 \in I$, where $I$ is the ideal of $F[X]$ generated by $f$ and $\partial f/\partial x_i = 0$, $i = 1, \ldots, n$.

**Proposition 1.** Let $f(x_1, x_2, \ldots, x_n) \in F[X]$ be non-singular, and $I$ the ideal of $F[X]$ generated by $f$ and $\partial f/\partial x_i$, $i = 1, \ldots, n - 1$. Then $I \cap F[x_n] \neq \{0\}$.

**Proof.** Write $\mathcal{V}_A(f)$ for the variety of $f$ in $A^n$. Then, we have a regular map $\pi$ of $\mathcal{V}_A(f)$ into the affine space $A$ such that $\pi(y_1, \ldots, y_n) = y_n$ for every $(y_1, \ldots, y_n) \in \mathcal{V}_A(f)$. Let $\mathcal{W}$ be the closure of $\pi(\mathcal{V}_A(f))$ for the Zariski topology of $A$. By the second Bertini theorem (see Theorem 2, Section 6, Chapter II, Shafarevich, 1994), there exists a dense open set $O \subseteq \mathcal{W}$ such that the fibre $\pi^{-1}(y)$ is non-singular for every $y \in O$. Then $\mathcal{W} \setminus O$ is a closed subset of $A$ for the Zariski topology such that $\mathcal{W} \setminus O \neq A$. According to the structure of closed subsets of $A$ (cf. Example 3 on page 23, Shafarevich, 1994), $\mathcal{W} \setminus O = \mathcal{V}_A(g)$, where $g(x_n) \in F[x_n]$ is a non-zero univariate polynomial.

Observe that $\pi(\mathcal{V}_A(I)) \cap O = \emptyset$, where $\mathcal{V}_A(I)$ is the variety of $I$ in $A^n$; otherwise there exists a $y' \in \pi(\mathcal{V}_A(I)) \cap O$ such that $\pi^{-1}(y')$ is non-singular. So we have $\pi(\mathcal{V}_A(I)) \subseteq \mathcal{W} \setminus O$. This implies $g(y_n) = 0$ for all $(y_1, \ldots, y_n) \in \mathcal{V}_A(I)$. By the Hilbert Nullstellensatz, $g^k \in I$ for some positive integer $s$. Obviously, $g^k \in I \cap F[x_n]$. This completes the proof. □

Obviously, $z - f \in F[X, z]$ is non-singular for all $f \in F[X]$. Thereby, we may establish the following result as an immediate consequence of Proposition 1.

**Corollary.** Let $f(x_1, x_2, \ldots, x_n) \in F[X]$, and $I$ the ideal of $F[X, z]$ generated by $z - f$ and $\partial f/\partial x_i$, $i = 1, \ldots, n$. 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 polynomial of degree $> 0$ in $K[X]$, and put $S_R(f, x_n) := \{a_n \in R \mid$ there are $a_1, \ldots, a_{n-1} \in R$ such that $f(a_1, a_2, \ldots, a_n) < 0\}$. It is easy to see that $S_R(f, x_n)$ is an open semialgebraic subset of $R$. By Proposition 2.1.7 in Bochnack et al. (1998), $S_R(f, x_n)$ consists of finitely many disjoint open intervals in $R$, if the polynomial $f(X)$ is not positive semidefinite on $R$. An endpoint $a$ of an interval of $S_R(f, x_n)$ is called finite, if $a \neq -\infty$ and $+\infty$. Obviously, $S_R(f, x_n)$ possesses at least one finite endpoint if $S_R(f, x_n) \neq R$. The purpose of this section is to seek an effective method to find out a finite subset of $R$ containing all finite endpoints of $S_R(f, x_n)$ for an indefinite polynomial $f \in K[X]$. For this purpose, we shall extend the original ordered field $K$ with real closure $R$ to an ordered field $K(m)$ with real closure $R(m)$, where $K(m)$ is a computable non-Archimedean ordered field containing infinitesimal positive elements $\epsilon_0, \epsilon_1, \ldots, \epsilon_m$.

For a non-negative integer $m$, put $K(m) := K(\epsilon_0, \ldots, \epsilon_m)$, where $\epsilon_0, \ldots, \epsilon_m$ are $m + 1$ indeterminates over $K$. Then the ordering $\leq$ of $K$ may be uniquely extended to an ordering of $K(m)$, still denoted by $\leq$, such that $\epsilon_0$ is positive and infinitesimal over $R$, and $\epsilon_k$ is positive and infinitesimal over $K(\epsilon_0, \ldots, \epsilon_{k-1})$, $k = 1, \ldots, m$. Obviously, the ordered field $(K(m), \leq)$ is also computable. Indeed, for a non-zero element $f/g \in K(m)$ with $f$, $g \in K[\epsilon_0, \epsilon_1, \ldots, \epsilon_m]$, $f/g < 0$ if and only if the coefficient of the lowest term of $fg$ is negative for the lexicographic order $\epsilon_0 < \cdots < \epsilon_m$. Denote the real closure of $(K(m), \leq)$ by $R(m)$. Of course, we may assume $R \subset R(m)$. Moreover, for $k = 0, \ldots, m - 1$, write $R(k)$
for the algebraic closure of $K$ in $R$. By Lemma 3.13 in Prestel (1984), $R$ is actually the real closure of $K$ with respect to the ordering ≤. Evidently, $R \subseteq R(0) \subseteq \cdots \subseteq R(n)$.

For a fixed $n \in \mathbb{N}$, construct the two subsets of $R(n)$ as follows:

$$A := \{ z \in R(n) | \text{ for some } d \in R \text{ with } d > 0, -d \leq z \leq d \},$$

$$M := \{ z \in R(n) | \text{ for every } d \in R \text{ with } d > 0, -d \leq z \leq d \}.$$

Likewise, we may construct the two subsets of $R(n)$ as follows:

$$A_{(0)} := \{ z \in R(n) | \text{ for some } d \in R(0) \text{ with } d > 0, -d \leq z \leq d \},$$

$$M_{(0)} := \{ z \in R(n) | \text{ for every } d \in R(0) \text{ with } d > 0, -d \leq z \leq d \}.$$

Obviously, $M$ consists of all elements in $R(n)$ infinitesimal over $R$, and $M_{(0)}$ consists of all elements in $R(n)$ infinitesimal over $R(0)$. According to the structure of $\leq, R \subseteq A \subseteq R(n)$, $R(0) \subseteq A_{(0)} \subseteq R(n)$, $\epsilon_0, \epsilon_1, \ldots, \epsilon_n \in M$, and $\epsilon_1, \ldots, \epsilon_n \in M_{(0)}$. By a familiar result on real valuations (see Proposition 1.3 in Knebusch (1973) or the relevant theorems in Section 5 of Lam (1980)), $A$ is a valuation ring of $R(n)$ with maximal ideal $M$, and $A_{(0)}$ is a valuation ring of $R(n)$ with maximal ideal $M_{(0)}$. Moreover, both $(A, M)$ and $(A_{(0)}, M_{(0)})$ are compatible with the ordering $\leq$, in other words, both $A$ and $M$ are convex in $R(n)$ with respect to $\leq$, and both $A_{(0)}$ and $M_{(0)}$ are convex in $R(n)$ with respect to $\leq$. Observe that the residue field $A/M$ of $A$ is isomorphic to $K$ and the residue field $A_{(0)}/M_{(0)}$ of $A_{(0)}$ is isomorphic to $R_{(0)}$. Thereby, there is a homomorphism $\pi$ of $A$ into $R$ such that $\pi(f(\epsilon_0, \ldots, \epsilon_n)) = f(0, \ldots, 0)$ for every $f \in R[\epsilon_0, \ldots, \epsilon_n]$, and there is a homomorphism $\pi_{(0)}$ of $A_{(0)}$ into $R_{(0)}$ such that $\pi_{(0)}(g(\epsilon_1, \ldots, \epsilon_n)) = g(0, \ldots, 0)$ for every $g \in R_{(0)}[\epsilon_1, \ldots, \epsilon_n]$.

For every $g \in K_0[\overline{X}]$, obviously $g \in K_0[\overline{X}]$, $k = 1, \ldots, n$. For $k = 0, 1, \ldots, n$, denote by $V_{R_{(k)}(g, x_n)}$ the subset of $R_{(k)}$ as follows:

$$\{ a_n \in R_{(k)} | \text{ there are } a_1, \ldots, a_{n-1} \in R_{(k)} \text{ such that } g(a_1, a_2, \ldots, a_n) = 0 \}.$$
Proof.

(1) $\implies$ (2): Since $f$ is not semidefinite on $R$, there are $(a_1, \ldots, a_n)$, $(b_1, \ldots, b_n) \in R^n$ such that $f(a_1, \ldots, a_n) > 0$ but $f(b_1, \ldots, b_n) < 0$. Observing that $a_0$ is infinitesimal over $R$, we have $f(a_1, \ldots, a_n) + a_0 > 0$ but $f(b_1, \ldots, b_n) + a_0 < 0$. Put $\Phi(z) := f(a_1 + z(b_1 - a_1), \ldots, a_n + z(b_n - a_n)) + a_0$, where $z$ is a new variable. Then $\Phi(z)$ is a univariate polynomial over $R_{\langle k \rangle}$ such that $\Phi(0) > 0$ but $\Phi(1) < 0$. By the intermediate value theorem for $R_{\langle k \rangle}$, $\Phi(z)$ has a root in $R_{\langle k \rangle}$. This implies that $f_+^+$ has a zero in $R_{\langle k \rangle}$.

(2) $\implies$ (3): Obvious.

(3) $\implies$ (1): Assume that $f_+$ has a zero $\alpha$ in $R^n_{\langle k \rangle}$, where $0 \leq k \leq n$. Then $f(\alpha) = -\epsilon_0 < 0$. By the transfer principle for real closed fields (cf. Proposition 5.2.3 in Bochnack et al. (1998)), there exist $a_1, \ldots, a_n \in R$ such that $f(a_1, \ldots, a_n) < 0$. Observe that the leading coefficient of $f$ is positive. Thereby, there exist $b_1, \ldots, b_n \in R$ such that $f(b_1, \ldots, b_n) > 0$. This implies that $f$ is not semidefinite on $R$. The proof is completed.

Now, we proceed to establish the following lemmas:

Lemma 1. Let the notations be as above, and let $I$ be the ideal of $K[t, \overline{X}]$ generated by $f + t$ and $\partial f / \partial x_i$, $i = 1, \ldots, k$, where $t$ is another variable, and $0 \leq k \leq n - 1$. Then we have

(1) $I \cap K[t, x_{k+1}, \ldots, x_n] \neq \{0\};$

(2) if $a_n^* \in K_{\langle n \rangle}$ is a closed endpoint of

$$\mathcal{V}_{R_{\langle n-k \rangle}}(f_+(x_1, \ldots, x_k, \epsilon_1^{-1}, \ldots, \epsilon_{n-k-1}^{-1} x_{n-k-1}, x_n), x_n),$$

where $\epsilon_i = \pm 1$, $i = 1, \ldots, n - k - 1$, then

$$g(\epsilon_0, \epsilon_1^{-1}, \ldots, \epsilon_{n-k-1}^{-1} a_n^*) = 0$$

for any non-zero polynomial $g(t, x_{k+1}, \ldots, x_n) \in I \cap K[t, x_{k+1}, \ldots, x_n]$.

Proof. (1) Denote the extended ideal of $I$ in $K(x_{k+1}, \ldots, x_n)[x_1, \ldots, x_k, t]$ by $I^c$.

By the corollary of Proposition 1, $I^c \cap K(x_{k+1}, \ldots, x_n)t \neq \{0\}$. Necessarily $I \cap K[t, x_{k+1}, \ldots, x_n] \neq \{0\}$.

(2) Put $h := f_+(x_1, \ldots, x_k, \epsilon_1^{-1}, \ldots, \epsilon_{n-k-1}^{-1} x_{n-k-1}, x_n)$. Obviously, $h$ is a non-zero polynomial in $K_{\langle n-k-1 \rangle}[x_1, \ldots, x_k, x_n]$. Assume that $a_n^*$ is a closed endpoint of $\mathcal{V}_{R_{\langle n-k \rangle}}(h, x_n)$. Then there exist $a_1^*, \ldots, a_k^* \in R_{\langle n-k-1 \rangle}$ such that $h(a_1^*, \ldots, a_k^*, a_n^*) = 0$. Since $a_n^*$ is not an interior point of $\mathcal{V}_{R_{\langle n-k \rangle}}(h, x_n)$, we have $S \nsubseteq \mathcal{V}_{R_{\langle n-k \rangle}}(h, x_n)$ for every open neighbourhood $S$ of $a_n^*$. Suppose that $\frac{\partial h}{\partial \epsilon_j}(a_1^*, \ldots, a_k^*, a_n^*) \neq 0$ for some $j \in \{1, \ldots, k\}$. Without loss of generality, assume $j = 1$. By the implicit function theorem for real closed fields (see Corollary 2.9.8 in Bochnack et al. (1998)), there exist an open neighbourhood $\Delta$ of $(a_2^*, \ldots, a_k^*, a_n^*)$ in the topological space $R_{\langle n-k-1 \rangle}^k$, an open neighbourhood $T$ of $a_1^*$ and a function (mapping) $\psi$ of $\Delta$ into $T$ such that $\psi(a_1^*, a_2^*, \ldots, a_k^*, a_n^*) = a_1^*$ and for every $(y_1, \ldots, y_k, y_n) \in \Delta \times T$, $h(y_1, \ldots, y_k, y_n) = 0$ if and only if $y_1 = \psi(y_2, \ldots, y_k, y_n)$. By the topological structure of $R_{\langle n-k-1 \rangle}^k$, for each
\[ \pi(S_8) \]

**Proof.** Without loss of generality, we may assume that over \( R \).

By definition of \( \pi(S_8) \), for some interval \( \Omega \) is positive. Thus, for an arbitrary positive element \( \pi(S_8) \) of \( \mathcal{V}_{R_{\infty}}(f, x_n) \) such that \( \pi(a^*) = a, i.e. a^* - a \) is infinitesimal over \( R \).

**Lemma 2.** Let the notations be as above, and let \( e(x_n) \in K[x_n] \) be the leading coefficient of \( f \) as a polynomial in \( K(x_n)[x_1, \ldots, x_{n-1}] \) with respect to the lexicographic order \( x_1 < \cdots < x_{n-1} \). If \( a \) is a finite open endpoint of \( \mathcal{S}_R(f, x_n) \), then either \( e(a) = 0 \) or there exists a finite endpoint \( a^* \) of \( \mathcal{V}_{R_{\infty}}(f, x_n) \) such that \( \pi(a^*) = a, i.e. a^* - a \) is infinitesimal over \( R \).

**Proof.** Without loss of generality, we may assume that \( a \) is a left finite endpoint of \( \mathcal{S}_R(f, x_n) \) such that \( e(a) \neq 0 \). In this case, there is a \( c \in R \) with \( a < c \) such that \( [a, c] \subseteq \mathcal{S}_R(f, x_n) \), where \([a, c]\) is the open interval in \( R \) with endpoints \( a, c \). Namely, \( e(a) > 0 \); otherwise \( a \in \mathcal{S}_R(f, x_n) \). Since every polynomial function is continuous on \( R \), there is a positive element \( \delta \) of \( R \) such that \( e(a_0) > 0 \) for all \( a_0 \in [a, a + 2\delta) \). Since \( \delta \) may be taken as a sufficiently small element, we may assume \( [a + \delta, a + 2\delta) \subseteq [a, c) \) where \([a + \delta, a + 2\delta) \) is the closed interval in \( R \) with endpoints \( a + \delta, a + 2\delta \).

Denote by \([a + \delta, a + 2\delta]_{R_{\infty}} \) the closed interval in \( R_{\infty} \) with endpoints \( a + \delta, a + 2\delta \). Let \( a_n^* \in [a + \delta, a + 2\delta]_{R_{\infty}} \). Then \( a_n^* \in \mathcal{S}_R(f, x_n) \). Putting \( a_n^* := \pi(a_n^*) \), we have \( a_n^* \in R \). Moreover, we have \( a_n^* - a_n^* \in M \), as \( \pi(a_n - a_n^*) = 0 \).

Thus, for an arbitrary positive element \( d \) in \( R \), \( -d + a + \delta < (a_n - a_n^*) \) is infinitesimal on \( R \). By the arbitrariness of \( d \), we get \( a + \delta \leq a_n^* \). Since \( \pi(a_n^*) \) is not positive semidefinite on \( R \) and \( a_n^* \in [a, a + 2\delta) \), then \( f(x_1, \ldots, x_{n-1}, a_n^*) \) is positive. Therefore \( f(b_1, \ldots, b_{n-1}, a_n^*) > 0 \) for some \( (b_1, \ldots, b_{n-1}) \in R^{n-1} \).

From the equality \( \pi(f(a_1, \ldots, a_{n-1}, a_n^*) + e_0 - f(a_1, \ldots, a_{n-1}, a_n)) = 0 \), it follows that \( f(a_1, \ldots, a_{n-1}, a_n^*) + e_0 - f(a_1, \ldots, a_{n-1}, a_n) \) is infinitesimal on \( R \). So we have \( f(a_1, \ldots, a_{n-1}, a_n^*) + e_0 - f(a_1, \ldots, a_{n-1}, a_n) < -f(a_1, \ldots, a_{n-1}, a_n) \), and \( f(a_1, \ldots, a_{n-1}, a_n^*) + e_0 < 0 \). Similarly, we have \( f(b_1, \ldots, b_{n-1}, a_n^*) + e_0 > 0 \). By the intermediate value theorem for polynomials over real closed fields, we have \( a_n^* \in \mathcal{V}_{R_{\infty}}(f, x_n) \). This implies \([a + \delta, a + 2\delta]_{R_{\infty}} \subseteq \mathcal{V}_{R_{\infty}}(f, x_n) \). Hence \([a + \delta, a + 2\delta]_{R_{\infty}} \subseteq \Omega \) for some interval \( \Omega \) of \( \mathcal{V}_{R_{\infty}}((f_1, x_n) \). Denote by \( a^* \) the left endpoint of \( \Omega \). Then \( a^* \leq a + \delta \). Suppose \( a^* < a \). Then \( a \in \mathcal{V}_{R_{\infty}}(f_1, x_n) \), i.e. \( f_1(d_{n-1}^*, \ldots, d_n^*) - a = 0 \) for some \( (d_1^*, \ldots, d_n^*) \in \mathcal{V}_{R_{\infty}}(f_1, x_n) \). So we have \( f(d_1^*, \ldots, d_n^*, a) = -e_0 < 0 \). By the transfer principle, \( f(d_1, \ldots, d_{n-1}, a) < 0 \) for some \( (d_1, \ldots, d_{n-1}) \in R^{n-1} \); this yields such a contradiction as follows: \( a \in \mathcal{S}_R(f, x_n) \). So we have \( a + a^* < a + \delta \) and \( 0 \leq a^* - a < \delta \). This implies \( a^* - a \in M \), since \( \delta \) may be taken as a sufficiently small element. Namely, \( \pi(a^* - a) = 0 \), and \( \pi(a^*) = a \). The proof is completed. \( \square \)

**Lemma 3.** Let the notations be as above, and \( \text{g}(X) \in K(0)_{\infty}(X) \). If \( a \) is a finite open endpoint of \( \mathcal{V}_{R_{\infty}}(g, x_n) \), then for some tuple \( (j_1, \ldots, j_k) \) of integers with
1 ≤ j_1 < ⋅ ⋅ ⋅ < j_k ≤ n − 1 and certain \( q_1, \ldots, q_k \in [1, -1] \), there exists a closed endpoint \( a^* \) of \( V_{R,0}(h, x_n) \) such that \( \pi_0(a^*) = a \), where \( h \) is the polynomial over \( K(k) \) obtained by substituting \( x_{j_i} = q_i \epsilon_i^{-1} \) in \( g \) for \( i = 1, \ldots, k \).

**Proof.** Without loss of generality, we may assume that \( a \) is a left finite open endpoint of \( V_{R,0}(g, x_n) \). Obviously \( a \notin V_{R,0}(g, x_n) \), and there is a \( c \in R(0) \) such that \( a < c \) and \( [a, c[ \subseteq V_{R,0}(g, x_n) \). For every \( \delta \in R(0) \) with \( 0 < \delta < c - a \) and every \( i \in \{1, \ldots, n - 1\} \), construct the subset of \( R(0) \) as follows:

\[
W_{\delta, i}(g; a) = \{z_i \in R(0) \mid \text{there exist } a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n \in R(0) \text{ such that } a < a_n < a + \delta, \text{ and } g(a_1, \ldots, a_{i-1}, z_i, a_{i+1}, \ldots, a_n) = 0\}.
\]

For the sake of convenience, we call the variable \( x_{j_i} \) is bounded for \( g \) when \( x_n \rightarrow a \), if for some \( \delta \in R(0) \) with \( 0 < \delta < c - a \), \( W_{\delta, i}(g; a) \) is a bounded subset of \( R(0) \). In this case, we may assert that there exists a \( j \in \{1, \ldots, n - 1\} \) such that \( x_{j_i} \) is not bounded for \( g \) when \( x_n \rightarrow a \). Indeed, if not, there are some \( \delta, D \in R(0) \) with \( 0 < \delta < c - a \) and \( 0 < D \) such that \( -D < z < D \) for all \( z \in \bigcup_{i=1}^{n-1} W_{\delta, i}(g; a) \). Then, the following sentence is valid in \( R(0) \):

\[
\forall(x_1, \ldots, x_n) \quad \left(g(x_1, \ldots, x_n) = 0 \land a < x_n < a + \delta \implies \bigwedge_{i=1}^{n-1} (-D < x_i < D)\right).
\]

Clearly, \( [a, a + \delta[ \subseteq V_{R,0}(g, x_n) \). Thereby, the following sentence is also valid in \( R(0) \):

\[
\forall x_n \quad (a < x_n < a + \delta \implies \exists(x_1, \ldots, x_{n-1})(g(x_1, \ldots, x_{n-1}, x_n) = 0)).
\]

Observe that \( R(0) \subseteq R(1) \). By the transfer principle for real closed fields, the above sentences are valid in \( R(1) \). Putting \( a = a + \epsilon_1 \), we have \( a \in R(1) \) and \( a < a + \epsilon_1 < a + \delta \). According to the second sentence, \( a \in V_{R,1}(g, x_n) \), i.e. there exist \( a_1, \ldots, a_{n-1} \in R(1) \) such that \( g(a_1, \ldots, a_{n-1}, a) = 0 \). From the first sentence, it follows that \( -D < a_i < D \) for every \( i = 1, \ldots, n - 1 \). Hence \( a_i \in A(0) \), \( i = 1, \ldots, n - 1 \). This yields \( g(\pi_0(a_1), \ldots, \pi_0(a_{n-1}), \pi_0(a)) = \pi_0(g(a_1, \ldots, a_{n-1}, a)) = 0 \), i.e. \( g(\pi_0(a_1), \ldots, \pi_0(a_{n-1}), a) = 0 \), where \( \pi_0(a_i) \in R(0) \), \( i = 1, \ldots, n - 1 \). This implies \( a \in V_{R,0}(g, x_n) \), a contradiction.

Let \( j \) be the minimal natural number such that \( x_{j_i} \) is not bounded for \( g \) when \( x_n \rightarrow a \). Then the following sentence is valid in \( R(0) \):

\[
\forall(\delta, D) \quad (0 < \delta < c - a \land 0 < D) \implies \exists(x_1, \ldots, x_n)(g(x_1, \ldots, x_n) = 0 \land x_n < a + \delta).\]

Likewise, by the transfer principle, the above sentence is valid in \( R(1) \). Observe that \( 0 < \epsilon_1 < c - a \) and \( 0 < \epsilon_1^{-1} \). By the above sentence, there exist \( b_1, \ldots, b_n \in R(1) \) such that \( g(b_1, \ldots, b_n) = 0, \epsilon_1^{-2} < b_{j_i}^2, \) and \( a < b_n < a + \epsilon_1 \). Since \( \epsilon_1 \) is positive and infinitesimal over \( R(0) \), \( \epsilon_1 b_{j_i}^{-1} \) is also positive and infinitesimal over \( R(0) \), where \( \partial_1 = 1 \) if \( 0 < b_{j_i} \) or \( \partial_1 = -1 \) if \( b_{j_i} < 0 \). Denote by \( \theta \) the \( R(0) \)-isomorphism of \( R(0)(b_{j_i}) \) onto \( R(0)(\epsilon_1) \) such that \( \theta(b_{j_i}) = \partial_1 \epsilon_1^{-1} \). It is clear that \( \theta \) is order-preserving. Observe that \( R(1) \)
is the real closure of both $R_0(b_{j_1})$ and $R_0(\epsilon_1)$. Therefore $\theta$ can be extended to an order-preserving automorphism of $R_{[1]}$. Put $a_1 := \theta(b_n)$, and write $g_1$ for the polynomial over $R_{[1]}$ obtained by substituting $x_{j_1} = q_1 \epsilon_1^{-1}$ in $g$. Then $a_1 \in \mathcal{V}_{R_{[1]}}(g_1, x_n)$. By the inequality $0 < b_n - a < \epsilon_1$, it is clear that $b_n - a$ is positive and infinitesimal over $R_{[0]}$. Thereby, $a_1 - a$ is positive and infinitesimal over $R_{[0]}$.

By Proposition 2.1.7 in Bochnack et al. (1998), there exists an interval $\Omega$ of $\mathcal{V}_{R_{[1]}}(g_1, x_n)$ such that $a_1 \in \Omega$. Write $a^*_1$ for the left endpoint of $\Omega$. Necessarily $a^*_1 \leq a_1$. Suppose $a^*_1 < a$. Then $a \in \mathcal{V}_{R_{[1]}}(g_1, x_n)$. According to the transfer principle, we have $a \in \mathcal{V}_{R_{[0]}}(g, x_n)$, a contradiction. Hence $a \leq a^*_1 \leq a_1$, and $a^*_1 - a$ is non-negative and infinitesimal over $R_{[0]}$. Moreover, we may prove the following claim:

Claim. For $g_1, x_i$ is bounded when $x_n \rightarrow a^*_1, i \in \{1, \ldots, j_1 - 1\}$.

Indeed, by the choice of $j_1$, $x_i$ is bounded for $g$ when $x_n \rightarrow a$. Then, for some $\delta$, $D \in R_{[0]}$ with $0 < \delta < c - a$ and $0 < D, -D < z < D$ for all $z \in \bigcup_{i=1}^{j_1-1} W_{g_1}(g; a)$. Thereby, the following sentence is valid in $R_{[0]}$:

$$\mathcal{V}(x_1, \ldots, x_n) \left( g(x_1, \ldots, x_n) = 0 \land a < x_n < a + \delta \Rightarrow \bigwedge_{i=1}^{j_1-1} (D < x_i < D) \right).$$

By the transfer principle, the above sentence is also valid in $R_{[1]}$. Since $a^*_1 - a$ is non-negative and infinitesimal over $R_{[0]}$, we have $a \leq a^*_1 < a^*_1 + \frac{\delta}{2} < a + \delta$. By the validity of the above sentence in $R_{[1]}$, it is easy to check $-D < z < D$ for all $z \in \bigcup_{i=1}^{j_1-1} W_{g_1}(g_1, a^*_1)$. Hence, the claim above is verified.

If $a^*_1$ is a closed endpoint of $\mathcal{V}_{R_{[1]}}(g_1, x_n)$, then our proof is completed. Now assume that $a^*_1$ is an open endpoint of $\mathcal{V}_{R_{[1]}}(g_1, x_n)$. By repeating the preceding argument, there is the minimal number $j_2$ in $\{1, \ldots, n - 1\} \setminus \{j_1\}$ such that $x_{j_2}$ is not bounded for $g_1$ when $x_n \rightarrow a^*_1$. By the claim above, $j_1 < j_2$. Write $g_2$ for the polynomial over $R_{[2]}$ obtained by substituting $x_{j_2} = q_2 \epsilon_2^{-1}$ in $g_1$, where $q_2 = 1$ or $-1$ as determined as above. Similarly, we can prove the facts as follows: (1) There exists a finite endpoint $a^*_2$ of $\mathcal{V}_{R_{[2]}}(g_2, x_n)$ such that $a^*_2 - a^*_1$ is non-negative and infinitesimal over $R_{[1]}$; hence over $R_{[0]}$; (2) For $g_2, x_i$ is bounded when $x_n \rightarrow a^*_1, i \in \{1, 2, \ldots, j_2 - 1\} \setminus \{j_1\}$.

Whenever $a^*_2$ is an open endpoint of $\mathcal{V}_{R_{[2]}}(g_2, x_n)$, our argument about $g_2$ may be similarly continued. Finally, after repeating some $k$th argument, we can obtain a tuple $(j_1, \ldots, j_k)$ of integers with $1 \leq j_1 < \cdots < j_k \leq n - 1$ and a sequence $a^*_1, \ldots, a^*_k$ satisfying the conditions as follows: (1) $a^*_k$ is a closed endpoint of $\mathcal{V}_{R_{[k]}}(g_k, x_n)$, where $g_k$ is the polynomial over $K(k)$ obtained by substituting $x_{j_i} = q_i \epsilon_i^{-1}$ in $g$ ($i = 1, \ldots, k$) for certain determined $q_1, \ldots, q_k \in \{1, -1\}$; (2) All elements $a^*_i - a, a^*_i - a^*_i, \ldots, a^*_k - a^*_k - 1$ are non-negative and infinitesimal over $R_{[0]}$. By condition (2), $a^*_k - a$ is infinitesimal over $R_{[0]}$, and $\pi_0(a^*_k) = a$. This completes the proof. □

In order to obtain non-zero polynomials in $I \cap K[t, x_{k+1}, \ldots, x_n]$ as in Lemma 1, the well-known Wu’s method is an effective tool. The well-known Wu’s theorem (see Wu, 1984) may be cited as follows:
Wu’s Theorem. Let $F$ be a field, and let $P$ be a finite set of polynomials in $F[\overline{X}]$. Then there is an effective algorithm to construct a set $C_1, \ldots, C_r$ of irreducible ascending chains such that

$$\operatorname{Zero}(P) = \bigcup_{1 \leq j \leq r} \operatorname{Zero}(C_j/I_j).$$

where $I_j$ is the initial set of $C_j$, $\operatorname{Zero}(P)$ denotes the set of all zeros of $P$ in an arbitrary algebraically closed extension of $F$, and $\operatorname{Zero}(C_j/I_j)$ denotes the set of all zeros of $C_j$ which are not zeros of any member in $I_j$.

It should be pointed out that Wu’s method has been programmed into some computer software to create irreducible ascending chains for polynomials with rational numbers as their coefficients.

Lemma 4. Let $F$ be a field, let $P$ be a finite set of polynomials in $F[\overline{X}]$, and let $I$ be the ideal of $F[\overline{X}]$ generated by $P$ such that $I \cap F[x_1, \ldots, x_r] \neq \{0\}$ for some $r$ with $1 \leq r \leq n$. If $C_1, \ldots, C_r$ is a set of irreducible ascending chains obtained from $P$ with respect to the order $x_1 \prec \cdots \prec x_r \prec x_{r+1} \prec \cdots \prec x_n$ as in Wu’s theorem, and $\phi_j$ is the first member in $C_j$, $j = 1, \ldots, r$, then there is an $s \in \mathbb{N}$ such that $\left(\prod_{1 \leq j \leq r} \phi_j\right)^s$ is a non-zero polynomial in $I \cap F[x_1, \ldots, x_r]$.

Proof. First we prove $\phi_j \in F[x_1, \ldots, x_r]$, $j = 1, \ldots, r$. Suppose that $\phi_k \notin F[x_1, \ldots, x_r]$ for some $k \in \{1, \ldots, r\}$. Put $C_k = \{g_1, \ldots, g_m\}$ with $g_1 = \phi_k$, and denote by $x_j$ the main variable of $g_i$, $i = 1, \ldots, m$. Necessarily $r < j_1 < \cdots < j_m$. Without loss of generality, we may assume $x_{j_i} = x_{r+i}$, $i = 1, \ldots, m$. By the definition of irreducible ascending chains, we have a tower of field extensions as follows:

$$K_0 = F(V), \quad K_1 = K_0[x_{r+1}]/(g_1), \ldots, K_m = K_{m-1}[x_{r+m}]/(g_m)$$

where $V = \{x_1, \ldots, x_r, x_{r+m+1}, \ldots, x_n\}$, and $(g_i)$ is the ideal of $K_{i-1}[x_{r+i}]$ generated by $g_i$, $i = 1, \ldots, m$.

Denote by $\tilde{x}_i$ the image of $x_i$ under the canonical homomorphism of $F[\overline{X}]$ into $K_m$, $i = 1, \ldots, n$. Obviously, $(\tilde{x}_1, \ldots, \tilde{x}_n) \in \operatorname{Zero}(C_k/I_k) \subseteq \operatorname{Zero}(P)$. Thereby, $(\tilde{x}_1, \ldots, \tilde{x}_n)$ is a zero of $I$. By the hypothesis, there exists a non-zero polynomial $h$ in $I \cap F[x_1, \ldots, x_r]$. This yields

$$h(\tilde{x}_1, \ldots, \tilde{x}_r) = h(\tilde{x}_1, \ldots, \tilde{x}_n) = 0.$$

However, $\tilde{x}_1, \ldots, \tilde{x}_r$ are obviously algebraically independent over $F$, a contradiction. Hence, $\phi_j \in F[x_1, \ldots, x_r]$, $j = 1, \ldots, r$.

By Wu’s theorem, we have $\prod_{1 \leq j \leq r} \phi_j(\alpha) = 0$ for every $\alpha \in \operatorname{Zero}(P)$. According to the familiar Hilbert Nullstellensatz, the proof may be completed. □

3. Main results

In this section, we shall prove Theorem 1 in the introduction and establish some relevant results.
By the lemmas in Section 2, we first establish the following theorem:

**Theorem 2.** Let \( f(\overline{x}) \in \mathcal{K}(\overline{x}) \) be a non-zero polynomial. Then a univariate polynomial \( p(x_n) \) may be effectively computed such that \( p(a) = 0 \) for every finite open endpoint \( a \) of \( S_R(f, x_n) \).

**Proof.** According to the lemmas in Section 2, we may implement the effective computations as follows:

1. With the aid of Wu’s method, we may obtain a set \( C_1, \ldots, C_r \) of irreducible ascending chains from \( \{ f + t, \frac{\partial f}{\partial x_i}, i = 1, 2, \ldots, n - 1 \} \) with respect to the lexicographic order \( t < x_n < \{ x_1, \ldots, x_{n-1} \} \). Denote by \( \phi_i \) the first member in \( C_i, i = 1, \ldots, r \), and put \( \phi = \prod_{1 \leq i \leq r} \phi_i \). By Lemmas 1 and 4, \( \phi^* \) is a non-zero polynomial in \( I \cap \mathcal{K}[t, x_n] \) for some \( s \in \mathbb{N} \). Write \( e(x_n) \) for the trailing coefficient of \( \phi \) as a polynomial over \( \mathcal{K}[x_n] \) in one variable \( t \). Obviously, \( e(x_n) \in \mathcal{K}[x_n] \).

2. For every tuple \( (j_1, \ldots, j_k) \) with \( 1 \leq j_1 < \cdots < j_k \leq n - 1 \), by Lemma 1 we have \( I \cap \mathcal{K}[t, x_{j_1}, \ldots, x_{j_k}, x_n] \neq \{0\} \), where \( I \) is the ideal of \( \mathcal{K}[t, \overline{x}] \) generated by \( \{ f + t, \frac{\partial f}{\partial x_i}, i = 1, 2, \ldots, n - 1 \} \backslash \{ j_1, \ldots, j_k \} \). With the aid of Wu’s method, we may obtain a set \( C_1, \ldots, C_r \) of irreducible ascending chains from \( \{ f + t, \frac{\partial f}{\partial x_i}, i = 1, 2, \ldots, n - 1 \} \backslash \{ j_1, \ldots, j_k \} \) with respect to the lexicographic order \( t < x_n < \{ x_{j_1}, \ldots, x_{j_k} \} < \{ x_1, \ldots, x_{n-1} \} \backslash \{ j_1, \ldots, j_k \} \). Pick out the first member \( \psi_i \) in \( C_i, i = 1, \ldots, r \), and put \( \psi_{j_1 \cdots j_k} = \prod_{1 \leq i \leq r} \psi_i \). By Lemma 4, \( \psi_{j_1 \cdots j_k}^* \) is a non-zero polynomial in \( I \cap \mathcal{K}[t, x_{j_1}, \ldots, x_{j_k}, x_n] \) for some \( s_{j_1 \cdots j_k} \in \mathbb{N} \).

3. For every polynomial \( \psi_{j_1 \cdots j_k}^* \) obtained in the procedure (2), write \( u_{j_1 \cdots j_k}^* (x_n, t) \) for the leading coefficient of \( \psi_{j_1 \cdots j_k}^* \) as a polynomial over \( \mathcal{K}(x_n, t) \) with respect to the lexicographic order \( x_{j_1} < \cdots < x_{j_k} \). Further write \( e_{j_1 \cdots j_k}^* (x_n) \) for the trailing coefficient of \( u_{j_1 \cdots j_k}^* (x_n, t) \) as a polynomial over \( \mathcal{K}[x_n] \) in one variable \( t \). Obviously, \( e_{j_1 \cdots j_k}^* (x_n) \in \mathcal{K}[x_n] \).

Put \( p(x_n) := e(x_n) \prod \lambda e_{i}(x_n) \), where \( \lambda \) runs over all tuples \( (j_1, \ldots, j_k) \) of integers with \( 1 \leq j_1 < \cdots < j_k \leq n - 1 \). Then we may assert that \( p(x_n) \) is as required. Indeed, \( e_{1 \cdots (n-1)}^* (x_n) \) is obviously the leading coefficient of \( f \) with respect to the lexicographic order \( x_1 < \cdots < x_{n-1} \). For every finite endpoint \( a \) of \( S_R(f, x_n) \), by Lemma 2 either \( e_{1 \cdots (n-1)}^* (a) = 0 \) or there exists a finite endpoint \( a^* \) of \( \mathcal{V}_{R_{\overline{0}}} (f_+ + x_n) \) such that \( a^* - a \) is infinitesimal over \( R \). Obviously \( p(a) = 0 \) if \( e_{1 \cdots (n-1)}^* (a) = 0 \). Now assume that \( a^* - a \) is infinitesimal over \( R \) for some finite endpoint \( a^* \) of \( \mathcal{V}_{R_{\overline{0}}} (f_+ + x_n) \).

When \( a^* \) is a closed endpoint of \( \mathcal{V}_{R_{\overline{0}}} (f_+ + x_n) \), by Lemma 1 we have \( \phi^* (\epsilon_0, a^*) = 0 \), and \( \phi(\epsilon_0, a^*) = 0 \). Let \( t^m (m \geq 0) \) be the trailing term of \( \phi(t, x_n) \) as a polynomial over \( \mathcal{K}[x_n] \) in one variable \( t \). Then \( \phi(t, x_n) = t^m \phi_0(t, x_n) \) where \( \phi_0(t, x_n) \in \mathcal{K}[t, x_n] \). So we have \( e_0^m \phi_0(\epsilon_0, a^*) = 0 \), and \( \phi_0(\epsilon_0, a^*) = 0 \). Hence \( e(a) = \phi_0(0, a) = \phi_0(\pi(\epsilon_0), \pi(a^*)) = \pi(\phi_0(\epsilon_0, a^*)) = 0 \). Now consider the case when \( a^* \) is an open endpoint of \( \mathcal{V}_{R_{\overline{1}}} (f_+ + x_n) \). By Lemma 3, for some tuple \( (j_1, \ldots, j_k) \) of integers with \( 1 \leq j_1 < \cdots < j_k \leq n - 1 \) and certain \( \epsilon_1, \ldots, \epsilon_k \in \{ 1, -1 \} \), there exists a closed endpoint \( a^*_{\overline{1}} \) of \( \mathcal{V}_{R_{\overline{1}}} (h, x_n) \) such that \( \pi_0(a^*_{\overline{1}}) = a^* \), where \( h \) is the polynomial over \( \mathcal{K} \) obtained by substituting \( x_{j_k} = \phi_t \epsilon_i^{-1} \) in \( f_+ \), \( 1 = i, \ldots, k \). According to Lemma 1, we have
\[ \psi_{j_1 \ldots j_k}(\epsilon_0, \epsilon_1^{-1}, \ldots, \epsilon_k^{-1}, a_n^*) = 0, \] and \( \psi_{j_1 \ldots j_k}(\epsilon_0, \epsilon_1^{-1}, \ldots, \epsilon_k^{-1}, a_n^*) = 0. \) Suppose that \( u_{j_1 \ldots j_k}(\epsilon_0, a_n^*) \) is not infinitesimal over \( R(0) \). Then \( u_{j_1 \ldots j_k}(\epsilon_0, a_n^*)^2 > d \) for some positive element \( d \) in \( R(0) \). Obviously, the polynomial \( \psi_{j_1 \ldots j_k}(t, q_1x_1, \ldots, q_kx_k, x_n) \) can be expressed in the following form:

\[
\psi_{j_1 \ldots j_k}(t, q_1x_1, \ldots, q_kx_k, x_n) = \pm u_{j_1 \ldots j_k}(t, x_n) x_{j_1}^{n_1} \cdots x_{j_k}^{n_k} + \sum_{i_1 \cdots i_k} w_{i_1 \cdots i_k}(t, x_n) x_{i_1}^{n_1} \cdots x_{i_k}^{n_k},
\]

where \( u_{j_1 \ldots j_k}(t, x_n) x_{j_1}^{n_1} \cdots x_{j_k}^{n_k} \) is the leading term of \( \psi_{j_1 \ldots j_k} \) as a polynomial over \( K(x_n, t) \) with respect to the lexicographic order \( x_{j_1} < \cdots < x_{j_k} \), and \( w_{i_1 \cdots i_k}(t, x_n) \in K[t, x_n] \).

Then, by the equality \( \psi_{j_1 \ldots j_k}(\epsilon_0, \epsilon_1^{-1}, \ldots, \epsilon_k^{-1}, a_n^*) = 0 \), we have

\[
d < u_{j_1 \ldots j_k}(\epsilon_0, a_n^*)^2 = \pm u_{j_1 \ldots j_k}(\epsilon_0, a_n^*) \sum_{i_1 \cdots i_k} w_{i_1 \cdots i_k}(\epsilon_0, a_n^*) \epsilon_1^{n_1-i_1} \cdots \epsilon_k^{n_k-i_k}.
\]

This is impossible, because \( u_{j_1 \ldots j_k}(\epsilon_0, a_n^*)w_{i_1 \cdots i_k}(\epsilon_0, a_n^*)\epsilon_1^{n_1-i_1} \cdots \epsilon_k^{n_k-i_k} \) is infinitesimal over \( R(0) \) for every tuple \((i_1, \ldots, i_k)\) corresponding to the lower term \( x_{j_1}^{n_1} \cdots x_{j_k}^{n_k} \). Hence \( u_{j_1 \ldots j_k}(\epsilon_0, a_n^*) \) is infinitesimal over \( R(0) \). Therefore, \( \tau_0(u_{j_1 \ldots j_k}(\epsilon_0, a_n^*)) = 0 \), and \( u_{j_1 \ldots j_k}(\epsilon_0, a_n^*) = 0 \). Let \( t^m \) (\( m \geq 0 \)) be the trailing term of \( u_{j_1 \ldots j_k}(t, x_n) \) as a polynomial over \( K[x_n] \) in one variable \( t \). Then \( u_{j_1 \ldots j_k}(t, x_n) = t^m v(t, x_n) \) where \( v(t, x_n) \in K[t, x_n] \). So we have \( \epsilon_0^m v(\epsilon_0, a^*) = 0 \), and \( v(\epsilon_0, a^*) = 0 \). Hence \( \epsilon_1(\epsilon_0, a^*) = v(\epsilon_0, a^*) = 0 \).

So we always have \( p(a) = 0 \) in either case. This completes the proof.

Now we can give without difficulty the proof of Theorem 1 in the introduction as follows:

**Proof of Theorem 1.** By Theorem 2, a univariate polynomial \( p(x_n) \) may be effectively computed such that \( p(a) = 0 \) for every finite open endpoint \( a \) of \( \mathcal{S}_R(f, x_n) \). Now let \( \Gamma \) be an arbitrary isolating set for \( p(x_n) \).

Clearly, \( f(\overline{x}) \) is not positive semidefinite if \( f(x_1, \ldots, x_{n-1}, a) \) is not positive semidefinite for some \( a \in \Gamma \). Now assume that \( f(\overline{x}) \) is not positive semidefinite. Then \( \mathcal{S}_R(f, x_n) \neq \emptyset \). In the case when \( \mathcal{S}_R(f, x_n) = R \), \( f(x_1, \ldots, x_{n-1}, a) \) is not positive semidefinite for every \( a \in \Gamma \). In the case when \( \mathcal{S}_R(f, x_n) \neq R \), there is at least one finite endpoint \( a \) of \( \mathcal{S}_R(f, x_n) \). Of course, \( a \) is a zero of \( p(x_n) \). Hence there are \( b, c \in \Gamma \) with \( b < c \) such that the open interval \( ]b, c[ \) contains only the endpoint \( a \) of \( \mathcal{S}_R(f, x_n) \). Thereby either \( b \in \mathcal{S}_R(f, x_n) \) or \( c \in \mathcal{S}_R(f, x_n) \). This implies that either \( f(x_1, \ldots, x_{n-1}, b) \) or \( f(x_1, \ldots, x_{n-1}, c) \) is not positive semidefinite. The proof is completed.

As two initial stages of deciding the semidefiniteness of polynomials, we consider the special cases of ternary polynomials and binary polynomials.

Let \( f(x, y, z) \) be a non-zero ternary polynomial over \( K \), and denote \( f_x = \partial f/\partial x \) and \( f_z = \partial f/\partial y \). By Wu's method, we can obtain a set \( C_1, \ldots, C_r \) of irreducible ascending chains from \( \{f + t, f_x, f_z\} \) with respect to the order \( z < y < x \). Put \( \Phi = \prod_{1 \leq j \leq r} \phi_j \), where \( \phi_j \) is the first member in \( C_j \), \( j = 1, \ldots, r \). By Lemmas 1 and 4, \( \phi \in K[t, z] \).

Write \( u(z) \) for the trailing coefficient of \( \phi \) as a polynomial over \( K[z] \) in one variable \( t \).
Moreover, write $\text{Res}(f + t, f_x; x)$ for the resultant of $f + t$ and $f_x$ relative to $x$, and $\text{Res}(f + t, f_y; y)$ for the resultant of $f + t$ and $f_y$ relative to $y$. Observe that $f + t$ is irreducible in $K[t, x, y, z]$. It is easy to see that $\text{Res}(f + t, f_x; x), \text{Res}(f + t, f_y; y)$ are non-zero polynomials in $K[t, y, z], K[t, x, z]$ respectively. Denote by $h_1(t, z), h_2(t, z)$ the leading coefficients of $\text{Res}(f + t, f_x; x), \text{Res}(f + t, f_y; y)$ as polynomials over $K[t, z]$ respectively, and write $v(z)$ for the trailing coefficient of $h_1(t, z)h_2(t, z)$ as a polynomial over $K[z]$ in one variable $t$. Then we have the following

**Theorem 3.** Let the notations be as above, and $e(z)$ the leading coefficient of $f(x, y, z)$ as a polynomial over $K[z]$ with respect to the lexicographic order $x < y$. If $\Gamma$ is an isolating set for $e(z)u(z)v(z)$ in $K$, then $f(x, y, z)$ is positive semidefinite if and only if $f(x, y, a)$ is positive semidefinite for every $a \in \Gamma$.

**Proof.** Denote by $J_1$ and $J_2$ the ideals of $K[x, y, z, t]$ generated by $\{f + t, f_x\}$ and $\{f + t, f_y\}$ respectively. By a familiar fact about resultants of polynomials (cf. Lemma 7.2.1, Mishra, 1993), $\text{Res}(f + t, f_x; x) \in J_1 \cap K[t, z, y]$ and $\text{Res}(f + t, f_y; y) \in J_2 \cap K[t, z, x]$. According to Theorems 1 and 2 and their proofs, $e(z)u(z)v(z)$ is just a univariate polynomial as required in Theorem 1. The proof of Theorem 3 is completed.

Now we consider the case of binary polynomials. Let $f(x, y) \in K[x, y]$ be a polynomial in which $x$ really appears. Put $f_x = \frac{\partial f(x, y)}{\partial x}$, and write $\text{Res}(f + t, f_x; x)$ for the resultant of $f + t$ and $f_x$ relative to $x$. Likewise, $\text{Res}(f + t, f_y; x) \neq 0$. Denote by $v(y)$ the trailing coefficient of $\text{Res}(f + t, f_x; x)$ as a polynomial over $K[y]$ in one variable $t$. Then we can establish the following theorem, which is an improvement of Proposition 9.1 in Liang and Zhang (1999).

**Theorem 4.** Let $f(x, y), f_x$ and $v(y)$ be as above. If $\Gamma$ is an isolating set for the polynomial $v(y)$ in $K$, then $f(x, y)$ is positive semidefinite on $R$ if and only if $f(x, a)$ is positive semidefinite on $R$ for every $a \in \Gamma$.

**Proof.** Denote by $I$ the ideal of $K[t, x, y]$ generated by $f + t$ and $f_x$. By Lemma 7.2.1 in Mishra (1993), we have $\text{Res}(f + t, f_x; x) \in I \cap K[t, y]$. Denote by $e(y)$ the leading coefficient of $f$ as a polynomial over $K[y]$. According to Theorem 2 and its proof, $v(y)u(y)$ is just a univariate polynomial as required in Theorem 2. Clearly, $e(y)$ is also the leading coefficient of $f + t$ as a polynomial over $K[t, y]$ in one variable $x$. Thereby, for every root $\alpha$ of $e(y), \text{Res}(f + t, f_x; x) \equiv 0$ whenever $y = \alpha$. This implies that $v(\alpha) = 0$ for every root $\alpha$ of $e(y)$. Hence, $\Gamma$ is also an isolating set for $e(y)v(y)$.

By Theorem 1 and its proof, $f(x, y)$ is positive semidefinite on $R$ if and only if $f(x, a)$ is positive semidefinite on $R$ for every $a \in \Gamma$. This completes the proof.

### 4. Algorithm and examples

In view of Theorems 1 and 2 and their proofs, we have an algorithm to reduce a given multivariate polynomial to some polynomials in fewer variables in the decision of semidefinite polynomials. For an input $f \in K[x_1, \ldots, x_n]$ containing really the variable $x_n$, our algorithm consists of the steps as follows:
(1) With the aid of Wu’s method, we may obtain a set $C_1, \ldots, C_r$ of irreducible ascending chains from $\{f + t, \frac{\partial f}{\partial x_i}, t = 1, 2, \ldots, n - 1\}$ with respect to the lexicographic order $t < x_n < \{x_1, \ldots, x_{n-1}\}$. Pick out the first member $\phi_j$ in $C_j$, $j = 1, \ldots, r$, and put $\phi = \prod_{1 \leq j \leq r} \phi_j$. By Lemmas 1 and 4, $\phi$ is a non-zero polynomial in $K[t, x_n]$. Write $e(x_n)$ for the trailing coefficient of $\phi$ as a polynomial over $K[x_n]$ in one variable $t$.

(2) For every tuple $(j_1, \ldots, j_k)$ of integers with $1 \leq j_1 < \cdots < j_k \leq n - 1$, by Lemma 1 we have $I \cap K[t, x_{j_1}, \ldots, x_{j_k}, x_n] \neq \{0\}$, where $I$ is the ideal of $K[t, x_n]$ generated by $\{f + t, \frac{\partial f}{\partial x_i}, i \in \{1, 2, \ldots, n-1\}\{j_1, \ldots, j_k\}\}$. With the aid of Wu’s method, we may obtain a set $C_1, \ldots, C_r$ of irreducible ascending chains from $\{f + t, \frac{\partial f}{\partial x_i}, i \in \{1, 2, \ldots, n-1\}\{j_1, \ldots, j_k\}\}$ with respect to the lexicographic order $t < x_n < \{x_{j_1}, \ldots, x_{j_k}\} < \{x_1, \ldots, x_{n-1}\}\{x_{j_1}, \ldots, x_{j_k}\}$. By Lemma 4, $\psi_j \in K[t, x_{j_1}, \ldots, x_{j_k}, x_n]$ and $\psi_j \neq 0$, where $\psi_j$ is the first member in $C_j$, $j = 1, \ldots, r$. Put $\psi_{j_1 \cdots j_k} = \prod_{1 \leq j \leq r} \psi_j$.

(3) For every polynomial $\psi_{j_1 \cdots j_k}$ obtained in the procedure (2), write $u_{j_1 \cdots j_k}(x_n, t)$ for the leading coefficient of $\psi_{j_1 \cdots j_k}$ as a polynomial over $K(x_n, t)$ with respect to the lexicographic order $x_{j_1} < \cdots < x_{j_k}$. Moreover, write $e_{j_1 \cdots j_k}(x_n)$ for the trailing coefficient of $u_{j_1 \cdots j_k}(x_n, t)$ as a polynomial over $K[x_n]$ in one variable $t$.

(4) Determine an isolating set $I'$ for $e(x_n) \prod_{\lambda} e_\lambda(x_n)$, where $\lambda$ runs over all tuples $(j_1, \ldots, j_k)$ of integers with $1 \leq j_1 < \cdots < j_k \leq n - 1$.

As the output, we obtain the set $\{f(x_1, \ldots, x_{n-1}, \alpha) \mid \alpha \in I'\}$ of polynomials in $n - 1$ variables such that $f$ is positive (or negative) semidefinite if and only if so is every member in $\{f(x_1, \ldots, x_{n-1}, \alpha) \mid \alpha \in I'\}$.

It should be pointed out that the desirable polynomials $\phi$ and $\psi_{j_1 \cdots j_k}$ may also be obtained by the computation of Gröbner bases in the steps (1) and (2).

Based on the elimination above, the decision of semidefiniteness of multivariate polynomials may be finally reduced to testing univariate polynomials. Observe that the semidefiniteness of a polynomial is invariant for the deletion of its even factors, and the deletion of even factors is an effective process with squarefree polynomial as output. Thereby, the semidefiniteness of a univariate polynomial may be easily tested according to the following proposition:

Proposition 3. Let $f(x)$ be a non-zero polynomial over $K$ in one variable $x$, and $g(x)$ the polynomial obtained by deleting even factors in the decomposition of $f(x)$ into irreducible factors. Then the following statements are equivalent:

(1) $f(x)$ is not semidefinite on $R$;
(2) $f(x)$ has a root of odd multiplicity in $R$;
(3) $g(x)$ has a root in $R$.

As an application of our algorithm, we give the following example, which was studied by Becker et al. (2000) in another way.

Example 1. (1) Decide whether or not $f(x, y)$ is semidefinite, where $f(x, y) = 2x^6 - 3x^4y^2 + y^6 + x^2y^2 - 6y + 5$. 
(2) Find all real numbers $z$ such that $f_z(x, y) = 2x^6 - 3x^4y^2 + y^6 + zx^2y^2 - 6y + 5$ is positive semidefinite.

**Process of computing**

(1) According to Theorem 4, we proceed to perform the following computations:

(1.1) Compute the resultant of $f + t$ and $\frac{\partial f}{\partial x}$ relative to $x$ as follows:

$$
\text{Res} \left( f + t, \frac{\partial f}{\partial x}; x \right) = (y^6 - 6y + 5 + t)(43200 + 8768y^6 + 8640y^4 - 103680y^3 + 1728y^{10} - 144y^8 - 10368y^5 + 1728y^4t - 10368y^7 + 62208y^2 - 20736yt + 1728y^6t + 1728y^2)^2.
$$

(1.2) As a polynomial over $\mathbb{Q}[y]$ in one variable $t$, the trailing coefficient of $\text{Res}(f + t, \frac{\partial f}{\partial x}; x)$ is as follows:

$$
u(y) := (y^6 - 6y + 5)(43200 + 8768y^6 + 8640y^4 - 103680y^3 + 1728y^{10} - 144y^8 - 10368y^5 + 1728y^4t - 10368y^7 + 62208y^2 - 20736yt + 1728y^6t + 1728y^2)^2.
$$

(1.3) Find such an isolating set $I'$ for $\nu(y)$ as follows:

$$I' = \{15, 31, 21, 43\}.\]$$

(1.4) For every $a \in I'$, decide whether or not the polynomial $f(x, a)$ is positive semidefinite. By the computation, we have

$$f(x, \frac{31}{32}) = 2x^6 - \frac{2883}{1024}x^4 + \frac{961}{1024}x^2 + \frac{15088449}{1073741824}.$$

It is easy to see that $f(x, \frac{31}{32})$ has a simple real root. This implies that $f(x, \frac{31}{32})$ is not positive semidefinite. Therefore, $f(x, y)$ is not positive semidefinite.

(2) Regarding $f_z$ as a ternary polynomial in the variables $x$, $y$ and $z$, we proceed to catch the open endpoints of $\mathcal{S}_R(f_z, z)$.

(2.1) Put $r_1 := \text{Res}(f_z + t, \frac{\partial f_z}{\partial y}; x)$, and $r_2 := \text{Res}(f_z + t, \frac{\partial f_z}{\partial y}; x)$. According to Lemma 7.2.1 in Mishra (1993), it is easy to see $\text{Res}(r_1, r_2; y) \in I \cap \mathbb{Q}[t, z]$, where $I$ is the ideal of $\mathbb{Q}[x, y, z, t]$ generated by $f_z + t, \frac{\partial f_z}{\partial y}$ and $\frac{\partial f_z}{\partial y}$. As a polynomial over $\mathbb{Q}[z]$ in one variable $t$, the trailing coefficient of $\text{Res}(r_1, r_2; y)$ is computed as follows:

$$u(z) = cz^{60}(8z - 9)^4u_2^2u_3^8u_4^4,$$

where $c$ is a non-zero integer,

$$u_1 = 10000z^{12} - 3240000z^{10} + 7123248z^9 + 634230000z^7 + 11994212700z^6 - 28067958000z^5 + 2213491131000z^4 + 4039965639000z^3 + 5767463452500z^2 + 20548904377500z + 35017791564375.$$
\[ u_2 = 2500z^{11} - 54000z^9 + 4442796z^8 + 48600z^7 - 681615000z^6 \\
+ 4941617625z^5 + 12567595500z^4 - 998715420000z^3 \\
+ 2659763790000z^2 + 6224945580000z \\
- 7748409780000, \]

and

\[ u_3 = 473169920000z^{17} + 532316160000z^{16} \\
- 211196436480000z^{15} - 69198374780928z^{14} \\
- 107455596447744z^{13} + 4196210555826288z^{12} \\
+ 5612147860359744z^{11} + 19532734205579712z^{10} \\
- 471655404355120992z^9 - 262317250242182016z^8 \\
+ 2026961820539255232z^7 + 11752913474703306216z^6 \\
- 2050929259840192632z^5 + 20464147147184520192z^4 \\
+ 9233080209928459016z^3 - 171459029679888593232z^2 \\
- 443852372703358599696z + 646998885493749662967. \]

(2.2) Denote by \( h_1(t, z) \) the leading coefficient of \( \text{Res}(f_z + t \frac{\partial f_z}{\partial x}; x) \) as a polynomial over \( \mathbb{Q}(t, z) \) in one variable \( y \). Then, as a polynomial over \( \mathbb{Q}[z] \) in one variable \( t \), the trailing coefficient of \( h_1(t, z) \) is computed as follows:

\[ v_1(z) = 2985984z^2. \]

(2.3) Denote by \( h_2(t, z) \) the leading coefficient of \( \text{Res}(f_z + t \frac{\partial f_z}{\partial y}; y) \) as a polynomial over \( \mathbb{Q}(t, z) \) in one variable \( x \). Then, as a polynomial over \( \mathbb{Q}[z] \) in one variable \( t \), the trailing coefficient of \( h_2(t, z) \) is computed as follows:

\[ v_2(z) = 1492992z^2. \]

(2.4) Observe that the leading coefficient of \( f_z \) is 1 with respect to the lexicographic order \( x \prec y \).

By Theorem 2 and its proof, \( z(8z - 9)u_1u_2u_3 \) is just a univariate polynomial as required in Theorem 2. By computation, the polynomial \( z(8z - 9)u_1u_2u_3 \) has exactly four real roots \( \alpha_1, \alpha_2, \alpha_3 \) and \( \alpha_4 \) such that \( -\frac{991}{128} < \alpha_1 < -\frac{195}{64} < 0 < \alpha_3 = \frac{9}{8} < \frac{77}{64} < \alpha_4 < \frac{155}{128} \) and \( u_2(\alpha_4) = u_3(\alpha_1) = 0 \). According to Theorem 4, it is easy to see that \( f_{\frac{77}{64}} \) is not positive semidefinite, but \( f_{\frac{155}{128}} \) is positive semidefinite. This implies that \( S_R(f_z, z) \) is just the open interval \( -\infty, \alpha_4 \). Therefore, \( f_z(x, y) \) is positive semidefinite if and only if \( z \geq \alpha_4 \), where \( \alpha_4 \) is the only real root of \( u_2 \).

With the aid of the computer algebra system Maple 7, the algorithm above has been made into a general program for multivariate polynomials with coefficients in the field of rational numbers. The following examples were done on a Pentium IV computer with 128 MB RAM:
Examples of ternary polynomials

1. $x^6 + y^6 + z^6 - 3x^2y^2z^2$;
2. $x^4 + y^4 + z^4 + 1 - 4xyz$;
3. $x^4 + 2x^2z + x^2 - 2xyz + 2y^2z^2 - 2yz^2 + 2z^2 - 2x + 2yz + 1/2$;
4. $x^4 + 2x^2z + x^2 - 2xyz + 2y^2z^2 - 2yz^2 + 2z^2 - 2x + 2yz + 1$;
5. $x^4y^4 - 2x^5y^3z - x^6y^2z^4 + 2x^7y^3z^2 - 4x^3y^2z^3 + 2x^4yz^5 + z^2y^2 - 2z^4yx + z^6x^2$;
6. $x^4y^4 - 2x^5y^3z + x^6y^2z^4 + 2x^7y^3z^2 - 4x^3y^2z^3 + 2x^4yz^5 + z^2y^2 - 2z^4yx + 99/100z^6x^2$.

The respective answers are “true”, “true”, “[1/2, 2, 1/2]”, “true”, “true” and “[-1, 1, -1]”, where the word “true” means that the corresponding polynomial is positive semidefinite, but the tuple “[a, b, c]” of numbers means that the value of the corresponding polynomial is negative when $[x, y, z] = [a, b, c]$. The respective CPU times are 0.2, 0.1, 0.4, 0.2, 0.3 and 18.5 s.

Examples of quaternion polynomials

1. $x^4 + y^4 + z^4 + w^4 - 5xyzw + x^2 + y^2 + z^2 + w^2 + 1$;
2. $x^4 + 4x^3y^2 + 2xyz^2 + 2xyw^2 + y^4 + z^4 + w^4 + 2z^2w^2 + 2x^2w + 2y^2w + 2xy + 3w^2 + 2z^2 + 1$;
3. $x^4 + 4x^3y^2 + 2xyz^2 + 2xyw^2 + y^4 + z^4 + w^4 + 2z^2w^2 + 2x^2w + 2y^2w + 2xy + 3w^2 - 2z^2 + 1$;
4. $w^6 + 2x^2w^3 + x^4 + y^4 + z^4 + 2x^2w + 2x^2z + 3x^2 + w^2 + 2z + 2 + 2 + w + 1$.

The respective answers are “true”, “true”, “[1/2, 1/2, 1/2]”, “true”, “[1/2, 1/2, 1/2]”, and “true”, where the word “true” means that the corresponding polynomial is positive semidefinite, but the tuple “[a, b, c, d]” of numbers means that the value of the corresponding polynomial is negative when $[x, y, z, w] = [a, b, c, d]$. The respective CPU times are 2.6, 4.4, 33.4, and 30.9 s.

Acknowledgements

This work is supported by the NKBRSF (Grant No. G1998030600) and the National Natural Science Foundation of China (Grant No. 19661002).

References