Computing real radicals and $S$-radicals of polynomial systems

Mohab Safey El Din

Sorbonne Université, CNRS, INRIA, Laboratoire d’Informatique de Paris 6, LIP6, Équipe PolSys,
4 place Jussieu, F-75252, Paris Cedex 05, France

Zhi-Hong Yang

Department of Mathematics, North Carolina State University, Raleigh, NC, USA
Department of Computer Science, Duke University, Durham, NC, USA

Lihong Zhi

KLMM, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China;
University of Chinese Academy of Sciences, Beijing 100049, China

Abstract

Let $f = (f_1, \ldots, f_s)$ be a sequence of polynomials in $\mathbb{Q}[X_1, \ldots, X_n]$ of maximal degree $D$ and $V \subseteq \mathbb{C}^n$ be the algebraic set defined by $f$ and $r$ be its dimension. The real radical $\sqrt{\langle f \rangle}$ associated to $f$ is the largest ideal which defines the real trace of $V$. When $V$ is smooth, we show that $\sqrt{\langle f \rangle}$ has a finite set of generators with degrees bounded by $\deg V$. Moreover, we present a probabilistic algorithm of complexity $s \cdot n \cdot D \cdot n^2 \cdot \text{O}(1)$ to compute the minimal primes of $\sqrt{\langle f \rangle}$. When $V$ is not smooth, we give a probabilistic algorithm of complexity $s \cdot O(1) \cdot (n D)^O(\log n)$ to compute rational parametrizations for all irreducible components of the real algebraic set $V \cap \mathbb{R}^n$.

Let $(g_1, \ldots, g_p)$ in $\mathbb{Q}[X_1, \ldots, X_n]$ and $S$ be the basic closed semi-algebraic set defined by $g_1 \geq 0, \ldots, g_p \geq 0$. The $S$-radical of $\langle f \rangle$, which is denoted by $\sqrt{\langle f \rangle}$, is the ideal associated to the Zariski closure of $V \cap S$. We give a probabilistic algorithm to compute rational parametrizations of all irreducible components of that Zariski closure, hence encoding $\sqrt{\langle f \rangle}$. Assuming now that $D$ is the maximum of the degrees of the $f_i$'s and the $g_i$'s, this algorithm runs in time $2^p(s + p)^{O(1)}(n D)^{O(\log n)}$. Experiments are performed to illustrate and show the efficiency of our approaches on computing real radicals.

Keywords: Polynomial system; Real radical; $S$-radical ideal; Semi-algebraic set; Real Algebraic Geometry

1. Introduction

Let $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ be the fields of rational, real and complex numbers and $X = (X_1, \ldots, X_n)$ be a sequence of variables.

Preprint submitted to Journal of Symbolic Computation November 26, 2018
For \( f = (f_1, \ldots, f_s) \) in \( \mathbb{Q}[X] = \mathbb{Q}[X_1, \ldots, X_s] \), we denote by \( \langle f \rangle \) the ideal generated by \( f \) in \( \mathbb{Q}[X] \). For \( \mathbb{K} = \mathbb{C} \) or \( \mathbb{R} \), we let \( V_{\mathbb{K}}(f) = \{ x \in \mathbb{K}^s \mid f_i(x) = 0, \ldots, f_s(x) = 0 \} \). The real radical \( \sqrt{\langle f \rangle} \) of \( \langle f \rangle \) in \( \mathbb{Q}[X] \) is defined as (Krivine [1964], Dubois [1969], Risler [1970]):

\[
\sqrt{\langle f \rangle} = \left\{ h \in \mathbb{Q}[X] \mid h^{2m} + \sum_{i=1}^{s} a_i^2 \in \langle f \rangle \text{ for some } m, l \in \mathbb{N} \text{ and } a_i \in \mathbb{Q}[X] \right\}.
\]

An ideal \( I \subset \mathbb{Q}[X] \) is said to be real if it equals its real radical, that is, \( I = \sqrt{\mathbb{I}} \).

Let \( g = (g_1, \ldots, g_p) \) be another polynomial sequence in \( \mathbb{Q}[X] \), \( S = \{ x \in \mathbb{R}^s \mid g_1(x) \geq 0, \ldots, g_p(x) \geq 0 \} \) and \( V_S(f) = V_{\mathbb{R}}(f) \cap S \). Denote \( g^\alpha = g_1^{a_1} g_2^{a_2} \cdots g_p^{a_p} \), where \( a_i \in \{0, 1\} \) and \( \alpha = (a_1, \ldots, a_p) \). The \( S \)-radical of \( \langle f \rangle \) is defined as (Stengle [1974], Definition 5):

\[
\sqrt{\langle f \rangle} = \left\{ h \in \mathbb{Q}[X] \mid h^{2m} + \sum_{\alpha \in \{0, 1\}^p} \sigma_\alpha g^\alpha, m \in \mathbb{N} \text{ and } \sigma_\alpha \in \mathbb{Q}[X] \right\}.
\]

An ideal \( I \) is called \( S \)-radical if \( I = \sqrt{\mathbb{I}} \). It is proved in (Stengle [1974]) that \( \sqrt{\langle f \rangle} \) is an \( S \)-radical ideal.

The Real Nullstellensatz (see e.g. (Krivine [1964], Dubois [1969], Risler [1970], Neuhaus [1998], Bochnak et al. [1998])) states that \( \sqrt{\langle f \rangle} \) is equal to the vanishing ideal of \( V_{\mathbb{R}}(f) \). The semi-algebraic Nullstellensatz (Stengle [1974]) states that \( S \)-radical coincides with the vanishing ideal of \( V_S(f) \). Hence, representing the real radical associated to \( f \) and the \( S \)-radical of \( f \) provides some insight on the geometry of \( V_{\mathbb{R}}(f) \) and \( V_S(f) \).

Further, we let \( D \) be the maximum of the degrees of the \( f_i \)'s and the \( g_i \)'s.

Computing real radicals has attracted much attention both on the symbolic and numerical side. Symbolic algorithms were developed at first in (Becker and Neuhaus [1993]). Later (Neuhaus [1998]) proposed a revised form of this algorithm and gave an upper bound \( D^{re\alpha^{2m}} \) for the degree of the generators of \( \sqrt{\langle f \rangle} \). Spang (2007, 2008) implemented this algorithm and improved its efficiency by avoiding some linear changes of coordinates. This algorithm is based on properties of isolated points of real algebraic sets and computation of real radicals of zero-dimensional ideals. Instead of computing real radicals, (Chen et al. [2010], [2013], [2011]) provide a method to decompose semi-algebraic systems into regular semi-algebraic systems.

On the numerical side, algorithms have been developed for computing real radicals and \( S \)-radicals. (Lasserre et al. [2008], [2013]) presented an algorithm based on moment relaxations to compute zero-dimensional real radicals and \( S \)-radicals in \( \mathbb{R}[X] \). Subsequently, (Ma et al. [2016]) generalized this algorithm to positive dimensional cases. (Brake et al. [2016]) gave a method based on numerical algebraic geometry and cuts of squares programming to certify that a set of polynomials generates a real radical. Finally, we refer to (Sekiguchi et al. [2013]) for an SDP-based approach for computing \( S \)-radical ideals.

We emphasize that these algorithms compute real radicals in \( \mathbb{R}[X] \) and hence return approximate encodings of those radicals. To see this, consider a univariate polynomial \( f \in \mathbb{Q}[X_1] \) with a single irrational real root \( \rho \). The real radical of \( \langle f \rangle \) is generated by \( X_1 - \rho \). The aforementioned algorithms based on numerical computations use an approximation of \( \rho \) to encode the output. By contrast, symbolic algorithms return real radicals with base field \( \mathbb{Q} \) and in the example we just considered would simply return \( f \).

In this paper, we focus on symbolic algorithms for computing generators or lazy representations (see Definition 2) for real radicals and \( S \)-radicals in \( \mathbb{Q}[X] \) with a focus on complexity issues.
Main results. All in all, we improve the complexity bound $D^{2n^2r^2}$ for computing real radicals. When $V_C(f)$ is smooth, we use polynomial system solving techniques in (Jeronimo et al., 2004; Blanco et al. 2004; Safey El Din, 2005) to obtain an algorithm with complexity $(snD^r)^{O(1)}$. When $V = V_C(f)$ is not smooth, we obtain an algorithm using $s^{O(1)}(nD)^{O(n^2r^2)}$ arithmetic operations in $\mathbb{Q}$ to represent the irreducible components of $\sqrt[\delta]{f}$. Here $r$ is the dimension of the ideal $(f)$. Hence for fixed dimension $r$, it is singly exponential in $n$ by contrast to previous results. We also extend our results for computing $\delta$-radicals with the complexity bound $2^n(s + p)^{O(1)}(nD)^{O(n^2r^2)}$.

Theorem 1. Let $f = (f_1, \ldots, f_s) \subset \mathbb{Q}[X_1, \ldots, X_n]$ with $D = \max(\deg(f_i), i = 1, \ldots, s)$ encoded by a straight-line program $\Gamma$. Assume that $V_C(f)$ is smooth, of dimension $r$ and of degree $\delta$. There exists a probabilistic algorithm which takes as input $\Gamma$ and returns generators of each minimal associated prime of $\sqrt[\delta]{f}$ with maximum degree $\delta$. In case of success, the algorithm uses $(snD^r)^{O(1)}$ arithmetic operations in $\mathbb{Q}$.

The difficulty in the non-smooth case is that the real algebraic set $V_\delta(f)$ might be embedded in the singular locus of $V$, or even worse, in the singular locus of the singular locus of $V$, etc. Using the Jacobian criterion and general complexity estimates to compute the vanishing ideal of the singular locus of $V$, would result in the complexity $D^{2n^2r^2}$ as in (Neuhaus, 1998). To bypass complexity issues, we use techniques developed in the last decades to represent algebraic sets. Such techniques, which are now standard in computer algebra, consist in representing an equidimensional algebraic set $V \subset \mathbb{C}^n$ outside a Zariski closed set, hence often restricting to a subset of $V$ which is a complete intersection. There are two main such representations, either triangular sets (Wu, 1984; Wang, 1998) (also known as regular chains (Kalkbrener, 1991), tower of simple extensions (Lazard, 1991), regular set (Moreno Maza, 1997)) or rational parametrizations, also known as geometric resolutions (see e.g. (Giusti et al., 2001; Lecerf, 2003; Schost, 2003; Safey El Din and Schost, 2017). The following definition is folklore.

Definition 2. An $r$-dimensional rational parametrization $\mathcal{Q} = ((w, v_1, \ldots, v_0), \ell)$ in $\mathbb{Q}[T_1, \ldots, T_{r+1}]$ of degree $\delta$ consists of the following:

- a sequence of polynomials $(w, v_1, \ldots, v_0)$ in $\mathbb{Q}[T_1, \ldots, T_{r+1}]$ such that the following holds: the variables $T_1, \ldots, T_{r+1}$ are new and $w$ is square-free and monic and of degree $\delta$ in each variable $T_1, \ldots, T_{r+1}$ and, for $1 \leq i \leq n$, $\deg(v_i, T_{r+1}) < \deg(w, T_{r+1})$.
- $\ell = (\lambda_1, \ldots, \lambda_r)$ is a sequence of linear forms in variables $X_1, \ldots, X_n$ such that $\lambda_i(v_1, \ldots, v_0) = T_i \mod w$.

The corresponding algebraic set $Z(\mathcal{Q}) \subset \mathbb{C}^n$ is the Zariski closure of the locally closed set of points $(x_1, \ldots, x_n) \in \mathbb{C}^n$ such that $\exists \theta \in \mathbb{C}^{r+1}, w(\theta) = 0, \frac{\partial w}{\partial T_i}(\theta) \neq 0, x_i = v_i(\theta) \mod w$. Observe that $Z(\mathcal{Q})$ is equidimensional (using the Jacobian criterion) and that the Zariski closure of the image of $Z(\mathcal{Q})$ by the map $x \mapsto (\lambda_1(x), \ldots, \lambda_r(x))$ is defined by $w = 0$. Furthermore, the polynomial $w$ is called the eliminating polynomial of the parametrization. Besides, the degree of $w$ coincides with the degree of $Z(\mathcal{Q})$ (see (Giusti et al., 2001; Lecerf, 2003)). Finally, observe also that the parametrization $(1)$ encodes the empty set. Equidimensional decompositions of algebraic sets whose components are represented by such parametrizations can be efficiently computed using (Lecerf, 2000). This is a key ingredient for the proof of the result below.

Theorem 3. Let $f = (f_1, \ldots, f_s) \subset \mathbb{Q}[X_1, \ldots, X_n]$ of degrees bounded by $D$. Let $r$ be the maximum of 1 and the dimension of the algebraic set $V_C(f)$. Then, there exists a probabilistic algorithm LazyRealRadical which takes as input $f$ and returns rational parametrizations of the minimal associated primes of $\sqrt[\delta]{f}$ using $s^{O(1)}(nD)^{O(n^2r^2)}$ arithmetic operations in $\mathbb{Q}$. 

Let \( g = (g_1, \ldots, g_p) \) be another polynomial sequence in \( \mathbb{Q}[X] \), \( D \) be the maximal degree of \( f \) and \( g \) and \( r \) be the dimension of the ideal \( \langle f \rangle \). Following the approach for computing real radicals, we give a probabilistic algorithm to compute rational parametrizations of all minimal primes \( \sqrt{\langle f \rangle} \).

**Theorem 4.** Let \( f = (f_1, \ldots, f_s) \) and \( g = (g_1, \ldots, g_p) \) be two polynomial sequences in the ring \( \mathbb{Q}[X_1, \ldots, X_n] \), and \( D \) be the maximal degree of polynomials in \( f \) and \( g \). Let \( S = \{ x \in \mathbb{R}^n \mid g_1 \geq 0, \ldots, g_p \geq 0 \} \) and \( \sqrt{\langle f \rangle} \) be the \( S \)-radical of \( \langle f \rangle \). Assume that the algebraic set \( V_C(f) \) has dimension \( r \). There exists a probabilistic algorithm \texttt{LazySRadical} which takes as input \( f \) and \( g \), and returns rational parametrizations for all minimal primes of \( \sqrt{\langle f \rangle} \) using \( 2^p(s + p)^{(n^2)} \) arithmetic operations in \( \mathbb{Q} \).

**Plan of the paper.** In Section \( \texttt{2} \) we introduce some basic notions that will be used throughout the paper. In Section \( \texttt{3} \) we present an algorithm for computing generators of real radicals under the smoothness assumption and show the correctness and the complexity of the algorithm. In Section \( \texttt{4} \) we give a probabilistic algorithm to compute rational parametrizations for all irreducible components of an arbitrarily given real algebraic set. In Section \( \texttt{5} \) we generalize the results of Section \( \texttt{4} \) to the semi-algebraic case. Section \( \texttt{6} \) is devoted to practical experiments.

### 2. Preliminaries

#### 2.1. Ideals and varieties

For basic notions related to affine and projective spaces, ideals and algebraic sets (and their irreducible components), as well as equidimensionality we refer to \( \text{Cox et al.}[1992] \). For basic definitions on real algebraic sets and semi-algebraic sets, we refer to \( \text{Bochnak et al.}[1998] \). In the sequel, we use the following notations.

We denote by \( \mathbb{P}^n(\mathbb{C}) \) the \( n \)-dimensional projective space over \( \mathbb{C} \). A subset of \( \mathbb{P}^n(\mathbb{C}) \) is called a projective algebraic set if it is the set of common zeros of some homogeneous polynomials in \( \mathbb{Q}[X_0, X_1, \ldots, X_n] \).

Let \( S \subset \mathbb{C}^n \), we denote by \( \overline{S} \) the Zariski closure of \( S \) which is the smallest algebraic set containing \( S \); we denote by \( I(S) \) the vanishing ideal of \( S \) which is the set of all polynomials in \( \mathbb{Q}[X_0, X_1, \ldots, X_n] \) vanishing identically over \( S \).

Let \( V \subset \mathbb{C}^n \) be an algebraic set. Let \( I(V) = (f_1, \ldots, f_s) \subset \mathbb{Q}[X] \) and \( p \) be a point of \( V \). The tangent space of \( V \) at \( p \), denoted by \( T_p(V) \), is given by \( T_p(V) = \bigcap_{i=1}^s \left\{ x \in \mathbb{C}^n \mid \sum_{i=1}^n \frac{\partial f_i}{\partial x_i}(p)x_i = 0 \right\} \).

The dimension of \( V \) at \( p \), denoted by \( \dim_p V \), is the maximum dimension of an irreducible component of \( V \) containing \( p \). The point \( p \) is said to be non-singular (or regular) at \( V \) if \( \dim T_p(V) = \dim V \). Otherwise, \( p \) is called a singular point of \( V \). The singular locus of \( V \) is the set \( \text{Sing}(V) := \{ p \in V \mid p \text{ is a singular point of } V \} \). We say that \( V \) is smooth if \( V \) has no singular point, that is, \( \text{Sing}(V) = \emptyset \).

All the notions above can be similarly defined for real algebraic sets in \( \mathbb{R}^n \) and projective algebraic sets in \( \mathbb{P}^n(\mathbb{C}) \).

Let \( W \subset \mathbb{C}^n \) be an irreducible algebraic set and \( r := \dim W \). The degree \( \deg W \) of \( W \) is \( \sup\{\deg(H_1 \cap \ldots \cap H_r \cap W)\} \) where \( H_1, \ldots, H_r \) are hyperplanes in \( \mathbb{C}^n \) meeting \( W \) at finitely many points. If \( W \) is not irreducible, then its degree is defined to be the sum of the degrees of all its irreducible components.
2.2. Chow forms

We recall the definition of Chow forms (Gelfand et al., 1994, Chapter 3). Let $V \subset \mathbb{P}^n(\mathbb{C})$ be an irreducible projective algebraic set and $r = \dim V$. For $i = 0, \ldots, r$, we denote by $U_i = (U_{i0}, \ldots, U_{in})$ a group of $n + 1$ variables and $U = (U_0, \ldots, U_r)$. Let $L_i = U_{i0}X_0 + \cdots + U_{in}X_n$, $i = 0, \ldots, r$. The Chow form of the projective set $V$ is the unique (up to a scalar factor) irreducible polynomial $\mathcal{F}_V \in \mathbb{Q}[U]$ such that for any $u_0, \ldots, u_r \in \mathbb{C}^{n+1}$,

$$\mathcal{F}_V(u_0, \ldots, u_r) = 0 \iff V \cap (L_0(u_0, X) = 0, \ldots, L_r(u_r, X) = 0) \neq \emptyset$$

where $L_i(u_i, X) = u_{i0}X_0 + \cdots + u_{in}X_n$, $i = 0, \ldots, r$.

Let $W \subset \mathbb{P}^r(\mathbb{C})$ be an equidimensional projective set and $W_i$ be its irreducible components ($1 \leq i \leq \ell$). The Chow form of $W$ is defined as $\mathcal{F}_W = \prod_{i=1}^\ell \mathcal{F}_{W_i}$, where $\mathcal{F}_{W_i}$ is the Chow form of $W_i$.

This definition can be extended to equidimensional affine algebraic sets in $\mathbb{C}^n$. Assume that we are given a finite sequence of polynomials $f = (f_1, \ldots, f_s)$ in $\mathbb{Q}[X_1, \ldots, X_n]$ and let $f^b_i$ be the homogenization of $f_i$ using the new variable $X_0$. Denote $f^b = (f^b_1, \ldots, f^b_s)$. Then the affine algebraic set $V = V_\mathbb{C}(f)$ can be identified with a subset of $\mathbb{P}^n(\mathbb{C})$ which is $V_\mathbb{C}(f^b) \setminus V_\mathbb{C}(X_0)$, and the projective closure of $V$ is the smallest projective algebraic set containing $V_\mathbb{C}(f^b) \setminus V_\mathbb{C}(X_0)$ (see Cox et al., 1992, Chapter 8). The Chow form of $V$ is defined to be the Chow form of its projective closure in $\mathbb{P}^n(\mathbb{C})$ (see Jeronimo et al., 2004, Section 1.1).

3. Algorithm for the smooth case

3.1. Preliminary results

Let $V$ be a smooth and equidimensional algebraic set in $\mathbb{C}^n$ defined by polynomials in $\mathbb{Q}[X]$ and let $m = (n - \dim V)(1 + \dim V)$. It has been shown in (Blanco et al., 2004, Theorem 10 and Corollary 17) that there exist polynomials $g_1, \ldots, g_m$ with deg $g_i \leq \deg V$ such that $g_1, \ldots, g_m$ generate the ideal $I(V)$. Moreover, the polynomials $g_1, \ldots, g_m$ can be obtained by specializing the Chow form of $V$ at some generic linear forms with rational coefficients (see (Blanco et al., 2004, Section 4) for details). We slightly generalize this result.

**Theorem 5.** Let $V$ be a smooth algebraic set in $\mathbb{C}^n$ of degree $\delta$. There exists a finite set of polynomials $G = (g_1, \ldots, g_m) \subset \mathbb{Q}[X]$ with max($\deg(g_i), i = 1, \ldots, s) \leq \delta$ such that $(G) = I(V)$.

**Proof.** Set $r = \dim(V)$ and $V = \bigcup_{i=0}^r V_i$ be the minimal equidimensional decomposition of $V$, where $V_i$ is either empty or $i$-equidimensional. Let $m_i = (n - i)(i + 1)$, for $i = 0, \ldots, r$. By (Blanco et al., 2004, Theorem 10 and Corollary 17), there exist polynomials $g^{(i)}_1, \ldots, g^{(i)}_{m_i}$ with degrees bounded by $\deg V_i$ such that $I(V_i) = (g^{(i)}_1, \ldots, g^{(i)}_{m_i})$, for $i = 0, \ldots, r$. Since $V$ is smooth, according to (Cox et al., 1992) §9.6, Theorem 8), we have $V_i \cap V_j = \emptyset$ for any $0 \leq i < j \leq r$. Then $I(V_i) + I(V_j) = (1)$ for all $0 \leq i < j \leq r$. Therefore $I(V) = \bigcap_{i=0}^r I(V_i)$ which equals \( \{ (g^{(i)}_{j_0} \cdots g^{(i)}_{j_r}) \mid 1 \leq j_0 \leq m_0, \ldots, 1 \leq j_r \leq m_r \} \).

Moreover, deg $(g^{(i)}_{j_0} \cdots g^{(i)}_{j_r}) \leq \deg V_0 + \cdots + \deg V_r = \delta$. Let $G = \{ (g^{(i)}_{j_0} \cdots g^{(i)}_{j_r}) \mid 1 \leq j_0 \leq m_0, \ldots, 1 \leq j_r \leq m_r \}$.

We have $(G) = I(V) = \sqrt{I}$ and deg$(g) \leq \delta$ for all $g \in G$. \( \square \)
We recall now a well-known criterion for testing whether a given prime ideal is real.

**Proposition 6.** ([Bochnak et al.](1998) Proposition 3.3.16) ([Marshall](2008) Theorem 12.6.1) Let $I$ be a prime ideal in $\mathbb{Q}[X]$, then $I$ is real if and only if $I$ has a non-singular real zero.

**Theorem 7.** Let $f$ be a finite polynomial sequence of $\mathbb{Q}[X]$ and $V = V_C(f)$ of degree $\delta$. If $V$ is smooth, then $\sqrt{(f)}$ has a finite set of generators $G \subset \mathbb{Q}[X]$ with $\deg(g) \leq \delta$ for $g \in G$.

**Proof.** Let $V = \bigcup_{i=1}^t V_i$ be the minimal irreducible decomposition of $V$. Note that for $i = 1, \ldots, t$, $V_i$ is smooth (because $V$ is) and $I(V_i)$ is prime. W.l.o.g. we assume that $V \cap \mathbb{R}^n \neq \emptyset$ since otherwise the conclusion is trivial. Let $\Omega = \{V_j \mid V_j \cap \mathbb{R}^n \neq \emptyset, 1 \leq j \leq t\}$. If $V_j \in \Omega$, then the prime ideal $I(V_j)$ has at least one non-singular real zero because $V_j$ is smooth and $V_j \cap \mathbb{R}^n \neq \emptyset$. Therefore, according to Proposition 6, $I(V_j)$ is real for every $V_j \in \Omega$. Now we have $I(V \cap \mathbb{R}^n) = I(V) \cap \mathbb{R}^n = I(\bigcup_{V_j \in \Omega} (V_j \cap \mathbb{R}^n))$, and the last ideal equals to $\bigcap_{V_j \in \Omega} I(V_j \cap \mathbb{R}^n)$.

Here, $V \cap \mathbb{R}^n$ is the Zariski closure of $V \cap \mathbb{R}^n$ in $\mathbb{C}^n$. Note that the first equality holds because for any subset $S$ of $\mathbb{C}^n$, $S$ and its Zariski closure $\overline{S}$ have the same vanishing ideal (see [Cox et al.](1992) §4.4). For $V_j \in \Omega$, $I(V_j \cap \mathbb{R}^n) = I(V_j)$ because $I(V_j)$ is real. In the end, we have $I(V \cap \mathbb{R}^n) = \bigcap_{V_j \in \Omega} I(V_j)$. It follows that $I(V \cap \mathbb{R}^n)$ and $\bigcap_{V_j \in \Omega} I(V_j)$ define the same algebraic set, that is, $V \cap \mathbb{R}^n = \bigcup_{V_j \in \Omega} V_j$. Then,

$$\deg(V \cap \mathbb{R}^n) = \sum_{V_j \in \Omega} \deg V_j \leq \sum_{i=1}^t \deg V_i = \deg V. \quad (1)$$

By the Real Nullstellensatz, $\sqrt{(f)} = I(V \cap \mathbb{R}^n)$. We already observed that $I(V \cap \mathbb{R}^n) = I(V) \cap \mathbb{R}^n$.

Hence, we have $\sqrt{(f)} = I(V \cap \mathbb{R}^n)$. Moreover, $V \cap \mathbb{R}^n$ is smooth because $V$ is smooth. The conclusion follows from Theorem 5 and the inequality (1).

### 3.2. Algorithm description

Let $f = (f_1, \ldots, f_s) \in \mathbb{Q}[X]$, and assume that $V = V_C(f)$ is smooth of dimension $r$. Write the minimal equidimensional decomposition of $V$ as $V = \bigcup_{i=1}^r V_i$, where $V_i$ is either empty or is $i$-equidimensional. Denote by $f_1^h, \ldots, f_r^h$ the homogenizations of $f_1, \ldots, f_s$ using the new variable $X_0$. Our algorithm uses several subroutines for computing generators of real radicals when $V = V_C(f)$ is smooth.

- **PointsPerComponents.** It takes as input polynomial equations $f_1 = 0, \ldots, f_s = 0$ and returns a set of real points meeting every connected component of $V_S(f_1, \ldots, f_s)$ (see [Safey El Din](2005)).
- **Equidim.** It takes as input homogeneous polynomials $f_1^h, \ldots, f_s^h, g \in \mathbb{Q}[X_0, \ldots, X_n]$ and returns the Chow forms of all equidimensional components of $V_C(f_1^h, \ldots, f_s^h) \setminus V_C(g)$ (see [Jeronimo et al.](2004)).
- **Generators.** It takes as input a Chow form $\mathcal{F}_{V_i}$ of some equidimensional algebraic set $V_i$ and returns a set of generators of the radical ideal $I(V_i)$ (see [Blanco et al.](2004)).
Let $V_i \subset \mathbb{C}^n$ be an equidimensional component of $V$ and $V_i^h \subset \mathbb{P}^n$ denote the projective closure of $V_i$. Let $V_i = \bigcup_{j=1}^{m_i} V_{ij}$ be the minimal irreducible decomposition of $V_i$. Then $V_i^h = \bigcup_{j=1}^{m_i} V_{ij}^h$, where $V_{ij}^h$ is the projective closure of $V_{ij}$. We can compute the Chow form $F_{ij}$ of $V_{ij}$ by the subroutine $\text{Equidim}$. According to the definition of the Chow form, $F_{V_i} = \bigcap_{j=1}^{m_i} F_{V_{ij}}$. Therefore we can compute the Chow forms of all the irreducible components of $V_i$ by factorizing $F_{V_i}$ over $\mathbb{Q}$. The following is the algorithm mentioned in Theorem 1.

**RealRadicalSmooth($f$)**

1. $S = \text{PointsPerComponents}(f = 0)$;
2. if $S = \emptyset$, then return $\{1\}$;
3. $\{F_{V_0}, \ldots, F_{V_k}\} = \text{Equidim}(f^h, X_0)$;
4. for $0 \leq i \leq r$ do
   $\{F_{V_i}, \ldots, F_{V_{m_i}}\} \leftarrow$ irreducible factors of $F_{V_i}$;
5. $\Omega = \emptyset$;
6. for $0 \leq i \leq r$ and $1 \leq j \leq m_i$ do
   $G_{ij} = \text{Generators}(F_{V_{ij}})$;
   if $V_C(G_{ij}) \cap S \neq \emptyset$ then $\Omega = \Omega \cup \{G_{ij}\}$;
7. return $\Omega$.

3.3. **Proof of Theorem 1**

**Probabilistic aspects.** The algorithms used in Step 1,3,4,6 are probabilistic. The probability of success of these algorithms depends on choices of points in $\mathbb{Q}^{m_i^n}$, and there exists a Zariski open set in $\mathbb{Q}^{m_i^n}$ such that for all choices in this set yield correct answers for these algorithms in $\text{RealRadicalSmooth}$. In the following, we assume that all the probabilistic calls mentioned above perform correctly.

**Correctness of algorithm RealRadicalSmooth.** Let $V_{ij} = V_C(G_{ij})$. Since $V$ is smooth, by [Cox et al., 1992, §9.6, Theorem 8], its irreducible components $V_{ij}$ do not intersect each other. Hence for each nonempty real algebraic set $V_{ij} \cap \mathbb{R}^n$, it contains at least one connected component of $V_C(f)$, which implies that $V_{ij} \cap \mathbb{R}^n \neq \emptyset$ if and only if $V_{ij} \cap S \neq \emptyset$. On the other hand, the prime ideal $I(V_{ij})$ is real if and only if $V_{ij} \cap \mathbb{R}^n \neq \emptyset$ (see the proof of Theorem 1). Thus, $I(V_{ij})$ is real if and only if $V_{ij} \cap S \neq \emptyset$. Then we have $\sqrt[\mathbb{Q}]{f} = \bigcap_{V_{ij} \cap S \neq \emptyset} I(V_{ij})$. Finally, the ideals $I(V_{ij})$ are exactly the prime components of $\sqrt[\mathbb{Q}]{f}$ since $V_{ij}$ are irreducible components of $V_C(f)$. The correctness of the algorithm is proved.

**Complexity analysis.** The first step of $\text{RealRadicalSmooth}$ computes a finite set $S$ of real points meeting every connected component of the real algebraic set $V_C(f)$. Many algorithms can be used (see [Safey El Din and Schost, 2003, 2004; Safey El Din, 2005, 2007b,a]). Using [Safey El Din, 2007a] and by the complexity analysis in [Safey El Din, 2005], Step 1 uses $sL(nD)^{O(1)}$ arithmetic operations in $\mathbb{Q}$ where $L$ is the length of the straight-line program $\Gamma$.

Next, by [Jeronimo et al., 2003, Theorem 1], computing the Chow forms of all equidimensional components of $V_C(F_1^n, \ldots, F_p^n) \setminus V_C(X_0)$ requires at most $sL(nD)^{O(1)}$ arithmetic operations.
in \( \mathbb{Q} \). The Chow forms \( \{ F_{X_0}, \ldots, F_{X_n} \} \) computed in Step 3 are encoded by straight-line programs of length bounded by \( sL(nD^p)^{(k)} \) (Jeronimo et al., 2004, Section 3.5).

Suppose that the straight-line program encoding \( F_{X_i} \) has length \( L_i \), then the cost of factorizing \( F_{X_i} \) over \( \mathbb{Q} \) is polynomial in \( L_i \) and the total degree of \( F_{X_i} \) (Kaltofen, 1989; Kaltofen and Trager, 1990). Note that the total degree of \( F_{X_i} \) is bounded by \((i+1)D_p\), so Step 4 can be done using at most \((sLn(r+1)D_p)^{(k)}\) arithmetic operations in \( \mathbb{Q} \). Observe that \( r \leq n-1 \), we can bound \((sLn(r+1)D_p)^{(k)}\) by \((sLnD^n)^{(k)}\).

The cost of computing generators \( G_{ij} \) of \( I \{ V_{ij} \} \) from the Chow form \( F_{X_i} \), does not increase the order of the complexity of Step 4 (Blanco et al., 2004, Section 5.5). Deciding the emptiness of \( V_C(\{ G_{ij} \} \cap S) \) is done by evaluating the polynomials of \( G_{ij} \) at all points of \( S \), and its cost is negligible. Observe that \( L \) is bounded by \( O(sD + n)^p \) (see e.g. (Krick, 2002)). Therefore, in case of success, the algorithm \texttt{RealRadicalSmooth} uses \((snD^n)^{(k)}\) arithmetic operations in \( \mathbb{Q} \).

4. Lazy representations and non-smooth case

4.1. Preliminary results

The following result is folklore and extracted from (Durvy and Lecerf, 2008, Lecerf, 2003).

**Lemma 8.** Let \( V \subseteq \mathbb{C}^n \) be an equi-dimensional algebraic set defined over \( \mathbb{Q} \) of dimension \( r \). There exists a non-empty Zariski open set \( \mathcal{O}(V) \subseteq \mathbb{C}^{n(r+1)} \) such that for \( \ell \in \mathcal{O}(V) \cap \mathbb{Q}^{n(r+1)} \) the following holds. There exists a sequence of polynomials \( (w, v_1, \ldots, v_n) \) in \( \mathbb{Q}[T_1, \ldots, T_{r+1}] \) such that \( Z(\mathcal{O}) = V \) with \( \mathcal{O} = ((w, v_1, \ldots, v_n), \ell) \).

Let \( \mathcal{O} = ((w, v_1, \ldots, v_n), \ell = (\lambda_1, \ldots, \lambda_{r+1})) \) be a rational parametrization. We define the polynomial \( \sigma_{\mathcal{O}} \) as the one obtained by substituting the variables \( T_1, \ldots, T_{r+1} \) with the \( \lambda_1, \ldots, \lambda_{r+1} \) in \( \frac{\partial w}{\partial T_{r+1}} \). We denote by \( S(\mathcal{O}) \) the intersection of \( Z(\mathcal{O}) \) with \( V_C(\sigma_{\mathcal{O}}) \). The following lemma is pointed out as a remark in the conclusion of (Lecerf, 2000).

**Lemma 9.** Under the above notations, the ideal associated to \( Z(\mathcal{O}) \) in \( \mathbb{Q}[X_1, \ldots, X_n] \) is prime if and only if \( w \) is irreducible over \( \mathbb{Q} \).

**Lemma 10.** Assume that the vanishing ideal of \( Z(\mathcal{O}) \) in \( \mathbb{Q}[X] \) is prime. Then, it is real if and only if one of the following equivalent conditions are satisfied:

(i) \( Z(\mathcal{O}) \) contains a real regular point;

(ii) the semi-algebraic set defined by \( w = 0, \frac{\partial w}{\partial T_{r+1}} \neq 0 \) is non-empty.

In particular, if the vanishing ideal of \( Z(\mathcal{O}) \) is not real, then \( Z(\mathcal{O}) \cap \mathbb{R}^n \) coincides with \( S(\mathcal{O}) \cap \mathbb{R}^n \).

**Proof.** We denote \( h = \frac{\partial w}{\partial T_{r+1}} \) and \( I \) the vanishing ideal of \( Z(\mathcal{O}) \). By Proposition 6, \( I \) is real if and only if it has a regular real zero which is equivalent to the assertion that \( Z(\mathcal{O}) \) contains a regular real point.

Now we prove that the condition (ii) holds if and only if \( I \) is real. Without loss of generality, we assume that the linear forms \( \lambda_i = X_i \) for \( i = 1, \ldots, r+1 \). Then \( T_i = X_i \) for \( i = 1, \ldots, r+1 \).

If the semi-algebraic set defined by \( w = 0, h \neq 0 \) is not empty, that is, there exists \( \theta \in \mathbb{R}^{r+1} \) such that \( w(\theta) = 0 \) and \( h(\theta) \neq 0 \), then we have a real point \( x = \left( \frac{1}{n}(\theta), \ldots, \frac{1}{n}(\theta) \right) \in Z(\mathcal{O}) \). It follows from the definition of \( Z(\mathcal{O}) \) and the Hilbert Nullstellensatz that the polynomials
Corollary 11. Under the above notations, assume that \( Z(\mathcal{D}) \) is irreducible, then \( S(\mathcal{D}) \) has dimension strictly less than \( \dim(Z(\mathcal{D})) \).

4.2. Subroutines

In this paragraph, we describe the subroutines used in the main algorithm.

Subroutine IrreducibleDecomposition. This subroutine aims at performing the following. Given a straight-line program of length \( L \) which evaluates a sequence of polynomials \( f = (f_1, \ldots, f_s) \) in \( \mathbb{Q}[X] \), it outputs a list of rational parametrizations encoding the irreducible components of \( V_C(f) \). This computation simply consists of calling the equidimensional decomposition algorithm in \( \text{[Lecerf, 2000]} \) which uses \( (sLnD^r)^O(1) \) operations in \( \mathbb{Q} \) to return zero-dimensional parametrizations of generic points in \( V_C(f) \). Combined with the Hensel lifting technique in \( \text{[Giusti et al., 2001]} \) (which are actually used in \( \text{[Lecerf, 2000]} \)), that algorithm allows to recover \( r \)-equidimensional parametrizations for the components of dimension \( r \). The total cost becomes \( (snD^r_{\max}(1,r)^O(1)) \). Computing the irreducible components from equidimensional parametrizations can be done by factorizing the eliminating polynomials of the parametrizations (the one which vanishes in the representation); the cost of this latter step is negligible (Kaltofen [1989], Kaltofen and Trager [1990]).

Lemma 12. Let \( f = (f_1, \ldots, f_s) \) be a sequence of polynomials in \( \mathbb{Q}[X] \) of degree bounded by \( D \) and \( V \) be the algebraic set defined by \( f \) with \( r = \dim(V) \). There exists a probabilistic algorithm which computes a list of rational parametrizations encoding the irreducible components of \( V \) using \( (snD^r_{\max}(1,r)^O(1)) \) operations in \( \mathbb{Q} \).

Subroutine IsReal. Let \( \mathcal{D} \) be a rational parametrization in \( \mathbb{Q}[T_1, \ldots, T_{r+1}] \) of degree \( \delta \) with \( Z(\mathcal{D}) \) irreducible, the subroutine \( \text{IsReal} \) decides if \( Z(\mathcal{D}) \) contains a real regular point in time \( \delta^{O(\epsilon)} \).

Lemma 13. Let \( \mathcal{D} = (w, v_1, \ldots, v_n, t) \) be a rational parametrization in \( \mathbb{Q}[T_1, \ldots, T_{r+1}] \) of degree \( \delta \) such that \( Z(\mathcal{D}) \) is irreducible. There exists an algorithm \( \text{IsReal} \) which returns true if \( Z(\mathcal{D}) \) contains real regular points or false otherwise. It uses \( \delta^{O(\max(1,\epsilon))} \) arithmetic operations in \( \mathbb{Q} \).

Proof. By Lemma 10, it suffices to decide if the semi-algebraic system \( w = 0, \frac{\partial w}{\partial v_r} \neq 0 \) has a real solution. Using (Basu et al. [2006] Chapter 14), this can be done using \( \delta^{O(\max(1,\epsilon))} \) arithmetic operations in \( \mathbb{Q} \).
Subroutine ChangeSeparatingElement. We describe now a subroutine which takes as input a rational parametrization encoding an equidimensional algebraic set \( Z \) using linear forms \( \ell \) and returns a new sequence of linear forms \( \ell' \) and which computes a new rational parametrization still encoding \( Z \) but using \( \ell' \).

Lemma 14. Let \( \mathcal{D} = ((w, v_1, \ldots, v_n), \ell) \) be a rational parametrization of degree \( \delta \) encoding a \( r \)-equidimensional algebraic set \( Z \) and \( \ell \) in the non-empty Zariski open set \( \mathcal{G}(Z) \) defined in Lemma 8.

Then, there exists a routine ChangeSeparatingElement which computes a rational parametrization \( \mathcal{D}' = ((w', v'_1, \ldots, v'_n), \ell') \) using \( (r + 1)(n\delta)^{O(\max(1, r))} \) arithmetic operations in \( \mathbb{Q} \).

Proof. The algorithm for changing one linear form works as in the proof of (Safey El Din and Schost [2017] Lemma J.8 of the electronic Appendix). It simply consists in using the algorithm underlying (Poteaux and Schost [2013] Lemma 2) which performs this operation in the zero-dimensional case in time \( (n\delta)^{O(1)} \).

Here, we deal with positive dimensional situations. In (Safey El Din and Schost [2017] Lemma J.8 of the Appendix), the one dimensional situation is tackled by performing operations in a univariate power series ring \( \mathbb{Q}[\![T_1 - y_1]\!] \) (where \( y_1 \) is chosen randomly) by applying (Poteaux and Schost [2013] Lemma 2). Doing this allows us to use the algorithm designed for the zero-dimensional case but performing operations in \( \mathbb{Q}[\![T_1 - y_1]\!] \) and truncate computations up to degree \( 2 \delta + 1 \). The extra cost of such a strategy is just the extra cost induced by the arithmetics in \( \mathbb{Q}[\![T_1 - y_1]\!] \). To tackle the \( r \)-dimensional case, we do the same but using power series ring \( \mathbb{Q}[\![T_1 - y_1, \ldots, T_r - y_r]\!] \) where \( y_1, \ldots, y_r \) are chosen randomly and truncating computations again up to the degree of \( \mathcal{D} \). Again the extra cost comes from arithmetic operations in \( \mathbb{Q}[\![T_1 - y_1, \ldots, T_r - y_r]\!] \) which is dominated by \( (n\delta)^{O(1)} \) since computations are truncated up to degree \( 2 \delta + 1 \).

Now, changing \( r + 1 \) linear forms requires to perform the above operations \( r + 1 \) times.

Subroutine Intersect. Let \( \mathcal{D} = ((w, v_1, \ldots, v_n), \ell) \) with \( \ell = (\lambda_1, \ldots, \lambda_{r+1}) \) be a rational parametrization in \( \mathbb{Q}[T_1, \ldots, T_{r+1}] \) and \( g \in \mathbb{Q}[T_1, \ldots, T_{r+1}] \). We denote by \( g_{\mathcal{D}} \) the polynomial \( g(\lambda_1, \ldots, \lambda_{r+1}) \in \mathbb{Q}[X] \). A key step for our algorithm is to compute \( Z(\mathcal{D}) \cap V_\mathcal{G}(g_{\mathcal{D}}) \)

Lemma 15. Let \( \mathcal{D} = ((w, v_1, \ldots, v_n), \ell) \) be a rational parametrization in \( \mathbb{Q}[T_1, \ldots, T_{r+1}] \) encoding an equidimensional algebraic set \( Z = Z(\mathcal{D}) \subset \mathbb{C}^n \) of dimension \( r \geq 1 \) and degree \( \delta \) and let \( g \) be a polynomial in \( \mathbb{Q}[T_1, \ldots, T_{r+1}] \) of degree \( \delta' \). Assume that the intersection of \( Z \) with \( V_\mathcal{G}(g_{\mathcal{D}}) \) has dimension \( r - 1 \). There exists an algorithm Intersect which on input \( (\mathcal{D}, g) \) outputs a list of rational parametrizations encoding the irreducible components of \( Z \cap V_\mathcal{G}(g_{\mathcal{D}}) \) in time \( n \max(\delta, \delta')^{O(1)} \).

Proof. The algorithm starts by choosing randomly a sequence of \( r + 1 \) linear forms \( \ell' = (\lambda'_1, \ldots, \lambda'_{r+1}) \) in \( X_1, \ldots, X_n \) assuming that \( \ell' \) lies in the non-empty Zariski open set \( \mathcal{G}(Z) \) (defined in Lemma 8).

Recall that \( Z \) is \( r \)-equidimensional. Observe that by Krull’s theorem (Eisenbud [1995]), \( Z \cap V_\mathcal{G}(g_{\mathcal{D}}) \) is either empty or has dimension greater than or equal to \( r - 1 \) and hence none of its irreducible components has dimension less than \( r - 1 \). Since, by assumption, \( \dim(Z \cap V_\mathcal{G}(g_{\mathcal{D}})) = r - 1 \), we deduce that \( Z \cap V_\mathcal{G}(g_{\mathcal{D}}) \) is equidimensional (of dimension \( r - 1 \)).

Hence, it makes sense to assume additionally that the first \( r \) linear forms of \( \ell' \) lie in the non-empty Zariski open set \( \mathcal{G}(Z \cap V_\mathcal{G}(g_{\mathcal{D}})) \) (see again Lemma 8). Another assumption of the same nature will be done and stated precisely below.
Next, one computes a rational parametrization \( \mathcal{L}' = ((u', v'_1, \ldots, v'_{r+1}), \ell') \) defining \( Z \). For clarity, we denote by \( T'_1, \ldots, T'_{r+1} \) the variables involved in \( \mathcal{L}' \). Lemma 14 establishes that this step can be performed using \((r + 1)(n\delta)^{O(r)}\) arithmetic operations in \( \mathbb{Q} \).

Now, we want to compute a rational parametrization of the intersection of \( Z = Z(\mathcal{L}') \) with \( V_C(g, \omega) \). The process we would like to mimic is as follows:

1. substitute in \( g \) the variables \( T_1, \ldots, T_{r+1} \) by the linear forms \( \lambda_1, \ldots, \lambda_{r+1} \) used in \( \mathcal{L} \) (hence yielding an explicit representation of \( g, \omega \));
2. substitute the \( X_i \)'s by their parametrizations in \( \mathcal{L}' \), hence obtaining a rational fraction \( g' \) (it lies in \( \mathbb{Q}(T'_1, \ldots, T'_{r+1}) \));
3. compute a representation of the intersection of the vanishing sets of the numerator of \( g' \) and \( u' \) (through subresultant computations as in \cite{Giusti2001} and deduce from that a rational representation of \( Z \cap V_C(g, \omega) \)).

Carrying out directly these steps without taking care of denominators does not allow us to obtain the announced complexity statement.

To achieve the announced complexity bound, we use a classical evaluation interpolation technique: that will allow us to obtain a better control on the monomial combinatorics and handle the presence of denominators.

Instead of computing an explicit representation of \( g, \omega \), we will actually build a straight-line program \( \Gamma \) evaluating it. Since \( g \) is a polynomial of degree \( \delta' \) involving \( r + 1 \) variables and since \( \ell \) is composed of \( r + 1 \) linear forms in \( X_1, \ldots, X_n \) which are equal to \( T_1, \ldots, T_{r+1} \), the length of such a straight-line program is bounded by \((r\delta')^{O(r)} + O(nr)\).

Evaluating the rational fraction \( g' \) defined above is then obtained by stacking to \( \Gamma \) the parametrizations \( \lambda_i = \frac{v'_i}{\omega'_{i-1}} \). Evaluating all parametrizations can be done using \((n\delta)^{O(r)}\) arithmetic operations in \( \mathbb{Q} \) (because the polynomials in \( \mathcal{L}' \) have degree \( \leq \delta' \) and involve \( r + 1 \) variables). In the end, one can evaluate \( g' \) using \((r\delta')^{O(r)} + O(nr) + (n\delta)^{O(r)}\) arithmetic operations in \( \mathbb{Q} \).

Now take \( y = (y_1, \ldots, y_{r-1}) \) in \( \mathbb{Q}^{r-1} \). Substituting the variables \( T'_1, \ldots, T'_{r-1} \) by \( y_1, \ldots, y_{r-1} \) in \( g' \) is done thanks to the procedure described above in time \((r\delta')^{O(r)} + O(nr) + (n\delta)^{O(r)}\).

For \( y \) as above, we denote by \( g'_y \) the obtained rational fraction. Similarly, \( \mathcal{L}'_y \) denotes the rational parametrization obtained by substituting the variables \( T'_1, \ldots, T'_{r-1} \) with \( y_1, \ldots, y_{r-1} \) in \( \mathcal{L}' \).

Using the intersection algorithm of \cite{Giusti2001} with input \( \mathcal{L}'_y \) and the numerator of \( g'_y \), one computes a zero-dimensional rational parametrization encoding \( Z \cap V_C(g, \omega) \cap V_C(\ell') \).

Since, by Bézout’s theorem, the intersection of \( Z \) with \( V_C(g, \omega) \) has degree bounded by \( \delta' \delta \), it is sufficient to repeat this process \((\delta' \delta)^{O(\delta)}\) times to interpolate a rational parametrization for \( Z \cap V_C(g, \omega) \). The last step consists in extracting from that parametrization the irreducible components of \( Z \cap V_C(g, \omega) \) by factoring the eliminating polynomial of \( \mathcal{L}' \). The complexity statement follows easily.

**Subroutine RemoveRedundantComponents.** Let \( \mathcal{L} = (\mathcal{L}_1, \ldots, \mathcal{L}_t) \) be a list of rational parametrizations such that, for \( 1 \leq i \leq t \), \( Z(\mathcal{L}_i) \) is irreducible. The subroutine RemoveRedundantComponents returns a subset of \( \mathcal{L} \) say, \( \mathcal{L}_{i_1}, \ldots, \mathcal{L}_{i_u} \) such that, \( Z(\mathcal{L}_{i_1}) \cup \cdots \cup Z(\mathcal{L}_{i_u}) = Z(\mathcal{L}_1) \cup \cdots \cup Z(\mathcal{L}_t) \) and, for \( u \neq v \), \( Z(\mathcal{L}_{i_u}) \not\subseteq Z(\mathcal{L}_{i_v}) \).
Lemma 16. Let \( \mathcal{L} = (\mathcal{Q}_1, \ldots, \mathcal{Q}_t) \) be a list of rational parametrizations with \( \delta_i \) being the degree of \( \mathcal{Q}_i \) and \( \delta \) be the maximum of \( \delta_1, \ldots, \delta_t \). Assume that for \( 1 \leq i \leq t \), \( Z(\mathcal{Q}_i) \) is irreducible of dimension \( r_i \); let \( r \) be the maximum of \( 1 \) and \( r_1, \ldots, r_t \).

There exists an algorithm RemoveRedundantComponents which on input \( \mathcal{L} \) returns a subset \( \mathcal{Q}_{i_1}, \ldots, \mathcal{Q}_{i_k} \) of \( \mathcal{L} \) such that, the following holds:

- \( Z(\mathcal{Q}_{i_1}) \cup \cdots \cup Z(\mathcal{Q}_{i_k}) = Z(\mathcal{Q}_1) \cup \cdots \cup Z(\mathcal{Q}_t) \);
- for \( u \neq v \), \( Z(\mathcal{Q}_{i_u}) \not\subset Z(\mathcal{Q}_{i_v}) \).

It uses \( t(r + 1)(n\delta)^{O(r)} \) operations in \( \mathbb{Q} \).

Proof. The algorithm starts by sorting (in ascending order) the rational parametrizations according to their dimension. Up to renumbering, one may assume that \( \mathcal{Q}_1, \ldots, \mathcal{Q}_t \) are already sorted by nondecreasing dimension (i.e. \( r_i \leq r_{i+1} \)). The algorithm starts by choosing randomly \( r + 1 \) linear forms \( \ell = (\lambda_1, \ldots, \lambda_{r+1}) \) and call the routine ChangeSeparatingElement with input \( \mathcal{Q}_i \) and \( (\lambda_1, \ldots, \lambda_{r+1}) \). According to Lemma 14 this step uses \( t(r + 1)(n\delta)^{O(r)} \) operations in \( \mathbb{Q} \). To keep notations simple, we keep on naming \( \mathcal{Q}_1, \ldots, \mathcal{Q}_t \) for the obtained rational parametrizations. Since, by assumption, the rational parametrizations define irreducible algebraic sets, one only needs to decide if \( Z(\mathcal{Q}_i) \subset Z(\mathcal{Q}_j) \) for \( i < j \) and \( r_i < r_j \). Thanks to the change of separating element, it then suffices to pick a random rational point in \( \mathbb{Q}^{r-1} \) and specialize both in \( \mathcal{Q}_i \) and \( \mathcal{Q}_j \) the parameters corresponding to \( \lambda_1, \ldots, \lambda_{r_i} \). Hence, we are led to decide the inclusion of a finite set of points in an algebraic set: both are given by a rational parametrization. This boils down to standard Euclidean remainder computations (see (Lecerf, 2003)). \( \square \)

4.3. Description of main algorithm

The algorithm takes as input a sequence \( f = (f_1, \ldots, f_s) \) of polynomials in \( \mathbb{Q}[X_1, \ldots, X_n] \) of degree bounded by \( D \).

It returns a list of rational parametrizations, each of which defining a prime component of the real radical ideal generated by \( f \).

The algorithm starts by calling IrreducibleDecomposition to compute a finite sequence of rational parametrizations \( \mathcal{R}_1, \ldots, \mathcal{R}_t \) encoding the irreducible components of \( V_C(f) \). Next, for \( 1 \leq i \leq t \), one computes a list of rational parametrizations encoding the irreducible components of the real radical associated to \( \mathcal{R}_i \). This is done by calling a routine called LazyRealRadicalRec which is described further. Finally, the routine RemoveRedundantComponents is called with input the list of all previously computed rational parametrizations to remove redundancies.

LazyRealRadicalRec(\( f \))

1. \( (\mathcal{R}_1, \ldots, \mathcal{R}_t) = \text{IrreducibleDecomposition}(f) \);
2. if \( t = 1 \) and \( \mathcal{R}_1 = ((1)) \) then return \( ((1)) \);
3. \( \text{res} = {} \);
4. for \( 1 \leq i \leq t \) do
   - \( \text{res} = \text{res} \cup \text{LazyRealRadicalRec}(\mathcal{R}_i) \);
5. return RemoveRedundantComponents(res).
We describe now the routine LazyRealRadicalRec. It takes as input a rational parametrization \( \mathcal{Q} \) and outputs a list of rational parametrizations encoding the irreducible algebraic sets defined by the prime components of the real radical associated to \( Z(\mathcal{Q}) \).

It works as follows. First, it decides if \( Z(\mathcal{Q}) \) contains real regular points using the routine IsReal. If this is the case, then it returns \( \mathcal{Q} \), else it computes rational parametrizations encoding the prime components of the set \( S(\mathcal{Q}) \) and performs a recursive call with input these parametrizations.

**LazyRealRadicalRec(\( \mathcal{Q} \))**

1. if \( \mathcal{Q} = ((1)) \) then return \( ((1)) \);
2. if IsReal(\( \mathcal{Q} \)) then return \( (\mathcal{Q}) \);
3. let \( w \) be the eliminating polynomial of \( \mathcal{Q} \) in \( \mathbb{Q}[T_1, \ldots, T_{r+1}] \);
4. \((\mathcal{Q}'_1, \ldots, \mathcal{Q}'_k) = \text{Intersect}(\mathcal{Q}, \frac{\partial w}{\partial T_{r+1}})\);
5. for \( 1 \leq \ell \leq k \) do
   - \( \text{res} = \text{res} \cup \text{LazyRealRadicalRec}(\mathcal{Q}'_\ell) \);
6. return RemoveRedundantComponents(res).

### 4.4. Proof of Theorem 3

We start by proving correctness and termination.

**Proof.** On input \( f \), LazyRealRadical starts by computing an irreducible decomposition of the algebraic set defined by \( f \) by means of rational parametrizations \( \mathcal{R}_1, \ldots, \mathcal{R}_t \). The next step consists in computing rational parametrizations encoding the prime components of the real radical associated to \( Z(\mathcal{R}_i) \) for \( 1 \leq i \leq t \).

This is done through the call to the routine LazyRealRadicalRec. Hence, the main step for proving correctness of LazyRealRadical consists in proving the correctness of LazyRealRadicalRec. Recall that it takes as input a rational parametrization \( \mathcal{Q} \) encoding an irreducible algebraic set. We prove its correctness by decreasing induction on the dimension of \( Z(\mathcal{Q}) \). The case where the \( Z(\mathcal{Q}) \) is finite is immediate; hence we assume below that \( Z(\mathcal{Q}) \) has positive dimension, say \( r \), and LazyRealRadicalRec terminates and is correct on inputs encoding algebraic sets of dimension less than \( r \).

The routine LazyRealRadicalRec decides if the prime ideal associated to \( Z(\mathcal{Q}) \) is real by calling the routine IsReal. If this is the case, \( \mathcal{Q} \) is returned as expected. Else, it computes a decomposition of \( S(\mathcal{Q}) \) following Lemma 10. Besides, Corollary 11 establishes that \( S(\mathcal{Q}) \) has dimension strictly less than \( \dim(Z(\mathcal{Q})) \). Termination and correctness follow by the induction assumption.

We can now prove the complexity statement.

**Proof.** The first step of LazyRealRadical consists in calling the routine IrreducibleDecomposition which uses \( (\text{snD}^{\omega})^{O(1)} \) arithmetic operations in \( \mathbb{Q} \) (Lemma 12) where \( r \) is the the maximum of 1 and the dimension of the algebraic set defined by the input \( f \). By Bézout’s theorem, the sum
of the degrees of the irreducible components encoded by the output is bounded by \( D^r \). Hence, we have \( t \leq D^r \) and for \( 1 \leq i \leq t \), the degree of \( \mathcal{O}_i \) is bounded by \( D^r \).

Next, one enters in the loop and call \( t \) times \( \text{LazyRealRadicalRec} \) with \( \mathcal{O}_i \) as input (for \( 1 \leq i \leq t \)). Below, we prove that running \( \text{LazyRealRadicalRec} \) with input a rational parametrization, say \( \mathcal{O} \), of degree \( \delta \) encoding an irreducible algebraic set of dimension \( \rho \) takes \( (n\delta)^{O(2)} \) arithmetic operations in \( \mathbb{Q} \) and the sum of the degrees of the rational parametrizations it outputs lies in \( (n\delta)^{O(2)} \). Hence, the whole cost of the “for loop” is \( (nD)^{O(2)} \).

The last step consists in calling the routine \( \text{RemoveRedundantComponents} \). Lemma 16 allows to estimate the complexity of this step. All in all, the total cost is bounded by \( s^{O(1)}(nD)^{O(2)} \).

We prove now the claim on the complexity of \( \text{LazyRealRadicalRec} \). The first step consists in calling subroutine \( \text{IsReal} \) on input \( \mathcal{O} \). This call takes \( O(Q) \delta \) arithmetic operations in \( \mathbb{Q} \) (Lemma [15]). When it returns true, \( \mathcal{O} \) is returned else a call to \( \text{Intersect} \) is performed with input \( \mathcal{O} \) and \( \delta \omega \), where \( \omega \) is the eliminating polynomial of \( \mathcal{O} \). By Lemma 15 this uses \( (n\delta)^{O(\rho)} \) arithmetic operations in \( \mathbb{Q} \).

The sum of the degrees of the output is bounded by \( \delta^2 \) but the dimension of these output rational parametrizations is \( \rho - 1 \). Hence, denoting by \( T(\delta, \rho) \) the cost of \( \text{LazyRealRadicalRec} \) on input a rational parametrization of degree \( \delta \) encoding an irreducible algebraic set of dimension \( \rho \), the following recurrence formula holds:

\[
T(\delta, \rho) \leq (n\delta)^{O(\rho)} + T(\delta^2, \rho - 1).
\]

Solving this recurrence formula yields a complexity \( (n\delta)^{O(2)} \). The same formula occurs for the degree bounds on the output. Hence, we are done.

As for algorithm \( \text{RealRadicalSmooth} \), most of subroutines which are used in \( \text{LazyRealRadical} \) are probabilistic: they rely on either generic specialization points or generic choices of linear changes of variables (or linear forms).

5. Semi-algebraic case

5.1. Algorithm description

Let \( f = (f_1, \ldots, f_s) \) and \( g = (g_1, \ldots, g_d) \) be two polynomial sequences in \( \mathbb{Q}[X_1, \ldots, X_n] \). Let \( S = \{ x \in \mathbb{R}^n \mid g_i(x) \geq 0, \ldots, g_d(x) \geq 0 \} \) and \( V_C(f) = V_C(f) \cap S \). We will write the equations \( f_i = 0, \forall f_i \in f \) as \( f = 0 \) and write the inequalities \( g_j \geq 0, \forall g_j \in g \) as \( g \geq 0 \). Similar notations will be used for inequalities involved \( >, < \) and \( \leq \).

The semi-algebraic set \( S \) is equal to the union of \( 2^n \) sets of the form: \( S_A = \{ x \in \mathbb{R}^n \mid g_A = 0, \hat{g}_A > 0 \} \) where \( g_A \) is a subset of \( g \) and \( \hat{g}_A = g \setminus g_A \), if \( g_A = \emptyset \), then take \( S_A = V_R(g) \).

The routine \( \text{LazySRadical}(f, g) \) takes \( f, g \subset \mathbb{Q}[X_1, \ldots, X_n] \) as input, and returns rational parametrizations of all minimal primes of the vanishing ideal of \( \{ x \in \mathbb{R}^n \mid f = 0, g \geq 0 \} \).

\( \text{LazySRadical}(f, g) \)

1. if \( g = \emptyset \) then return \( \text{LazyRealRadical}(f) \);
2. \( \text{res} = \{ \} \);
3. \( \Lambda = \{ g_A \mid g_A \subset g \} \);

14
4. for every $g_i \in \Lambda$ do
   • $f_i = f \cup g_i$, $\hat{g}_i = g \setminus g_i$;
   • $(\mathcal{R}_1, \ldots, \mathcal{R}_t) = \text{IrreducibleDecomposition}(f_i)$;
   • for $1 \leq i \leq t$ do
     – res = res $\cup$ LazySRadicalRec($\mathcal{R}_i$, $\hat{g}_i$);

5. return RemoveRedundantComponents(res).

The subroutine LazySRadicalRec$(\mathcal{D}, g)$ takes a rational parametrization $\mathcal{D}$ and a polynomial sequence $g \subset \mathbb{Q}[X_1, \ldots, X_n]$ as input, where $\mathcal{D}$ encodes an irreducible algebraic set of dimension $r$. This subroutine returns rational parametrizations of the minimal primes of the vanishing ideal of $Z(\mathcal{D}) \cap \{x \in \mathbb{R}^n \mid g > 0\}$.

LazySRadicalRec$(\mathcal{D}, g)$

1. if $\mathcal{D} = ((1))$ then return $((1))$;
2. if $g = \emptyset$ then return LazyRealRadicalRec$(\mathcal{D})$;
3. let $((w, v_1, \ldots, v_n), \ell) = \mathcal{D}$;
4. $g_{\mathcal{D}} = \{g(v_1, \ldots, v_n) \mid g \in g\}$;
5. $Z = \text{PointsPerComponents}(w = 0, g_{\mathcal{D}} > 0)$;
6. if $Z = \emptyset$ then return $((1))$;
7. if $\exists \theta \in Z$ such that $\frac{\partial w}{\partial T_{r+1}}(\theta) \neq 0$ then return \mathcal{D};
8. $(\mathcal{D}_1', \ldots, \mathcal{D}_k') = \text{Intersect}(\mathcal{D}, \frac{\partial w}{\partial T_{r+1}})$;
9. for $1 \leq i \leq k$ do
   • res = res $\cup$ LazySRadicalRec$(\mathcal{D}_i', g)$;
10. return RemoveRedundantComponents(res).

5.2. Proof of Theorem 4

Termination and correctness. With the notations in LazySRadical, the set $S$ is the union of all the sets $Z(\mathcal{R}_i) \cap \{x \in \mathbb{R}^n \mid \hat{g}_i > 0\}$, where $i = 1, \ldots, t$ and $\hat{g}_i$ is a subset of $g$. Therefore, the termination and correctness of LazySRadical reduces to that of LazyRealRadicalRec since the final call to RemoveRedundantComponents will remove those returned components which are contained in other components of higher dimension.

Let $\mathcal{D}$ be a rational parametrization encoding an irreducible algebraic set of dimension $r$. We prove that with input $(\mathcal{D}, g)$, the subroutine LazySRadicalRec will terminate after a finite number of steps and return rational parametrizations of the minimal primes of the vanishing ideal of the set $A = Z(\mathcal{D}) \cap \{x \in \mathbb{R}^n \mid g > 0\}$.

If $g$ is empty then it reduces to the correctness of the subroutine LazyRealRadicalRec$(\mathcal{D})$ which has been shown in the proof of Theorem 3. By Lemma 10, the set $\{x \in \mathbb{R}^n \mid g > 0\}$ contains a regular real point of $Z(\mathcal{D})$ if and only if the polynomial system $g_{\mathcal{D}} > 0$, $w = 0$, $\frac{\partial w}{\partial T_{r+1}} \neq 0$.
has real solutions. On the other hand, if the set \( \{ x \in \mathbb{R}^n \mid g > 0 \} \) contains a regular real point of \( \mathbb{Z}(\mathcal{D}) \), then the Zariski closure of \( A \) is a nonempty Zariski dense subset of \( \mathbb{Z}(\mathcal{D}) \) since \( \mathbb{Z}(\mathcal{D}) \) is irreducible. Therefore, the Zariski closure of \( A \) is equal to \( \mathbb{Z}(\mathcal{D}) \). Thus, in Step 7 of LazySRadicalRec, \( \mathcal{D} \) is returned. Else, the set \( A \) only contains some singular points of \( \mathbb{Z}(\mathcal{D}) \).

Proving the correctness of the recursive call which is then performed is very similar to the one for LazyRealRadicalRec and we do not repeat it here.

**Complexity Analysis.** We first estimate the complexity and degree bound for the output of LazySRadicalRec. Let \( T(\delta, \rho) \) be the complexity of LazySRadicalRec with input \( (\mathcal{D}, g) \), where \( \delta \) is the degree of \( \mathcal{D} \) and \( \rho \) is the dimension of \( \mathbb{Z}(\mathcal{D}) \). Assume that the degrees of the polynomials in \( g \) are less than or equal to \( \delta \).

Without loss of generality, we assume that \( g \) is not empty (otherwise, \( T(\delta, \rho) \) is the complexity of LazyRealRadicalRec). The subroutine PointsPerComponents is called with input \( (w = 0, g, \mathcal{D}, \mathcal{D}_0 > 0) \) to compute the sample points set \( Z \), which uses \( (p + 1)(\rho D^\delta)^{O(\rho)} \) [Basu et al. 2006]. If the set \( Z \) contains a regular real point of \( \mathbb{Z}(\mathcal{D}) \) then \( \mathcal{D} \) is returned. Otherwise, the subroutine Intersect is called with input \( w \) and \( \frac{\partial w}{\partial x_i} \), which uses \( (n\delta)^{O(\rho)} \) arithmetic operations in \( \mathbb{Q} \) (Lemma 15). Now we have the following recurrence formula:

\[
T(\delta, \rho) \leq (p + 1)(\rho D^\delta)^{O(\rho)} + (n\delta)^{O(\rho)} + T(\delta^2, \rho - 1).
\]

Solving this recurrence formula gives that \( T(\delta, \rho) \) is bounded by \( p\delta^{O(\rho^2)} + (n\delta)^{O(\rho^2)} \). The degree bounds for the output of LazySRadicalRec follow the same formula as (2), and so the final output has degrees bounded by \( (n\delta)^{O(\rho^2)} \).

Next, we estimate the complexity of LazySRadical.

For every \( f_i = f \cup g_i \), the algebraic set \( V_C(f_i) \) has at most \( D^\rho \) irreducible components, which means the \( t \) in Step 4 of LazySRadical is bounded by \( D^\rho \). With input \( f_i \), the subroutine IrreducibleDecomposition uses \( ((s + p)n D^\rho)^{O(1)} \) arithmetic operations in \( \mathbb{Q} \) (By Lemma 12). In the second “for loop” of LazySRadical, the subroutine LazySRadicalRec(\( \mathcal{A}_i \)), \( g_i \)) uses \( p\delta^{O(\rho^2)} \) arithmetic operations in \( \mathbb{Q} \), where \( \delta_i \) is the degree of \( \mathcal{A}_i \), and \( \rho_i \) is the dimension of \( \mathcal{A}_i \). By Bézout’s theorem, every \( \delta_i \) is bounded by \( D^\rho \). Observe that every \( \rho_i \) is bounded by \( r \). Thus the whole cost of the Step 4 of LazySRadical is bounded by \( 2^p \cdot ((s + p)n D^\rho)^{O(1)} + 2^p D^r (p D^\rho)^{O(1)} \), which is \( 2^p (s + p)^{O(1)} (nD)^{O(n^2)} \). The final step is to remove redundant components. By Lemma 16 the complexity of this step is bounded by \( (nD)^{O(n^2)} \) since the output parametrizations of LazySRadicalRec have degrees bounded by \( (nD)^{O(n^2)} \). To summarize, the whole complexity of LazySRadical is \( 2^p (s + p)^{O(1)} (nD)^{O(n^2)} \).

**Example 17.** Let \( f = X^3 - X^2 - Y^2 \), \( g = -X + \frac{1}{2} \) and \( S = \{(x, y) \in \mathbb{R}^2 \mid g \geq 0\} \). The polynomial \( f \) is taken from [Bochnak et al. 1998 Example 3.1.2 b)].

- Let \( S_0 = \{(x, y) \in \mathbb{R}^2 \mid g > 0\} \). Taking \( (f = 0, g > 0) \) as input of PointsPerComponents, we obtain one point \((0, 0)\). Since \((0, 0)\) is a singular zero of \( f \), it is necessary to do a recursive call on the singular locus of \( V_C(f) \). The vanishing ideal of the singular locus of \( V_C(f) \) is \( \langle X, Y \rangle \). Replacing \( f \) by \( (X, Y) \) and repeating this process on \( (X, Y) \) and \( S_0 \), we obtain that the vanishing ideal of \( V_C(f) \cap S_0 \) is \( \langle X, Y \rangle \).

- Let \( S_1 = \{(x, y) \in \mathbb{R}^2 \mid g = 0\} \). By computation we have \( V_C(f) \cap S_1 = \emptyset \), so its vanishing ideal is \( \emptyset \).

Therefore, the \( S \)-radical of \( f \) in \( \mathbb{Q}[X, Y] \) is \( \sqrt{f} = \langle X, Y \rangle \).
6. Experiments

We give several examples to show the efficiency of our approach on computing real radicals. All the examples given below are beyond the reach of the Singular library realrad implemented by Spang (Spang, 2007) which is, up to our knowledge, the single available implementation of the algorithm given by Becker and Neuhaus (1993); Neuhaus (1998). That implementation is based on Gröbner bases.

Observe that one can use Singular functionalities to compute equidimensional/prime decompositions and intersections of ideals as well as elimination ideals, by means of Gröbner bases. Hence, one can “simulate” LazyRealRadical using those functionalities combined with the HasRealSolutions function in the Maple library RAGlib (Safey El Din, 2007a).

In a word, taking a polynomial sequence \( f \) as input, we will obtain generators of the minimal associated primes of \( \sqrt[\mathbb{R}]{\langle f \rangle} \).

The computations were performed on an Intel(R) Xeon(R) CPU E7-4809 v2 @ 1.90GHz and 756GB of RAM.

**Example 18** (Vor1). *The following polynomial comes from (Everett et al., 2009):*

\[
\text{Vor1} = (a^2 + \beta^2 + 1)a^2 x^4 - 2a(2\alpha^2 \beta^2 + a\beta + a\alpha x - \beta a + 2a + 2a\alpha^2 - \beta a^2)\lambda^3 + (\beta^2 + 6a^2 \beta^2 - 2\beta x a^3 - 6\beta a x^3 + 6\beta a^2 - 6a\beta x + 6a\alpha x^2 + y^2 a^2 - 2a a y + x^2 a^2 - 2ya a^3 + 6a^2 \alpha^2 + a^4 \alpha^2 + 4a^2)^2 - 2(x a - y a^2 - 2\beta a^2 - \beta + 2a a + a a^3)(x a - y - \beta + a a)\lambda + (1 + a^3)(x a - y - \beta + a a)\lambda ^2.
\]

This polynomial is a sum of squares (Kaltofen et al., 2008), thus the ideal \( \langle \text{Vor1} \rangle \) is not real. Take Vor1 as input and we obtain in 9 sec. the minimal primes of the real radical \( \sqrt[\mathbb{R}]{\langle \text{Vor1} \rangle} \):

\[
P_1 = \langle a a - a x + \beta - y, \lambda + 1 \rangle, P_2 = \langle a a + a x - \beta - y, \lambda \rangle, P_3 = \langle 2\beta \lambda + \beta + y, a \rangle.
\]

**Example 19.** Consider the discriminant \( D \) of the characteristic polynomial of the following linear symmetric matrix:

\[
\begin{pmatrix}
1 & 1 & 1 \\
1 & y & 1 \\
1 & 1 & z
\end{pmatrix}
\]

Figure 1: Example17 Vc(f) ∩ S
It has been proved that $\mathcal{D}$ is a sum of squares \cite{Lax2005}. On input $\mathcal{D}$, our algorithm computed in 4 sec. the real radical $\sqrt[\mathbb{R}]{\mathcal{D}}$. It has only one minimal prime which is $(y - z, g)$ where
\[
g = -19y^{12} + 228y^{11}z - 1254y^{10}z^2 + 4180y^9z^3 - 9405y^8z^4 + 15048y^7z^5 - 17556y^6z^6 + 15048y^5z^7 - 9405y^4z^8 + 4180y^3z^9 - 1254y^2z^{10} + 228yz^{11} - 19z^{12} - 606y^{10}z + 6060y^9z - 27270y^8z^2 + 72720y^7z^3 - 127260y^6z^4 + 152712y^5z^5 - 127260y^4z^6 + 72720y^3z^7 - 27270y^2z^8 + 6060yz^9 - 606z^{10} - 6732y^8 + 53856y^7z - 188496y^6z^2 + 376992y^5z^3 - 471240y^4z^4 + 376992y^3z^5 - 188496y^2z^6 + 53856yz^7 - 6732z^8 - 35370z^9 + 530550z^3 + 707400z^5 \]
\[
- 530550y^2z^4 + 212220yz^5 - 35370y^6 - 116073y^4 + 464292y^3z - 696438y^2z^2 + 464292yz^3 - 116073z^4 - 77760y^2 + 155520yz - 77760z^2 + 139968x - 69984y - 69984z.
\]

Example 20 (Homotopy-1). This example is taken from \cite{Chen2013}: 
\[
f_1 = x^3y^2 + c_1x^3y + y^2 + c_2x + c_3, \quad f_2 = c_4x^4y^2 - x^2y + y + c_5, \quad f_3 = c_4 - 1.
\]

Take the sequence $f = (f_1, f_2, f_3)$ as input and we obtain in a single second that $\sqrt[\mathbb{R}]{(f)}$ has only one minimal prime which is the ideal $(f)$. This shows that the ideal $(f)$ is prime and real.

Example 21 (Cinquin-3-4). This is also an example taken from \cite{Chen2013}:
\[
f_1 = s - x_1(1 + x_2^4 + x_3^4), \quad f_2 = s - x_2(1 + x_1^4 + x_3^4), \quad f_3 = s - x_3(1 + x_1^4 + x_2^4).
\]

We obtain in 47 sec. the minimal primes of $\sqrt[\mathbb{R}]{(f)}$ for $f = (f_1, f_2, f_3)$:
\[
P_1 = \left( x_1 - x_2 - x_3, -x_1^4, x_1 - x_2, s \right),
\]
\[
P_2 = \left( x_1 - x_2, x_2^2x_1 + x_2x_3^2 + x_1^2x_3 - x_1^4 - 1, -x_1^4x_3 - x_1^2x_3 - x_1 + s \right),
\]
\[
P_3 = \left( x_1 - x_2, x_2^2x_1 + x_2x_3^2 + x_3^2x_3 - x_3^4 - 1, -x_2^4x_3 - x_2x_3 - x_2 + s \right),
\]
\[
P_4 = \left( x_1 - x_2, x_2^2x_1 + x_2x_3^2 + x_3^2x_3 - x_3^4 - 1, -x_2^4x_3 - x_2x_3 - x_2 + s \right).
\]

Example 22 (Essential Variety). This is an example taken from \cite{Floydstad2017}. Let $E$ be the essential variety defined as:
\[
E = \left\{ M \in \mathbb{R}^{3 \times 3} \mid \det(M) = 0, 2(MM^T)M - \text{tr}(MM^T)M = 0 \right\},
\]
where $\det(M)$ is the determinant of $M$ and $\text{tr}(MM^T)$ is the trace of $MM^T$.

If we write the matrix $M$ as
\[
\begin{bmatrix}
a & b & c \\
u & v & w \\
x & y & z
\end{bmatrix},
\]

18
then the 10 cubics defining $E$ are:

\[
\begin{align*}
&avz -awy -bwx + cuy - cvx, \\
&(2a^2 + 2b^2 + 2c^2)a + (2au + 2bv + 2cw)u + (2ax + 2by + 2cz)x - ga, \\
&(2a^2 + 2b^2 + 2c^2)b + (2au + 2bv + 2cw)v + (2ax + 2by + 2cz)y - gb, \\
&(2a^2 + 2b^2 + 2c^2)c + (2au + 2bv + 2cw)w + (2ax + 2by + 2cz)z - gc, \\
&(2au + 2bv + 2cw)a + (2a^2 + 2v^2 + 2w^2)u + (2ux + 2vy + 2wz)x - gu, \\
&(2au + 2bv + 2cw)b + (2a^2 + 2v^2 + 2w^2)v + (2ux + 2vy + 2wz)y - gv, \\
&(2au + 2bv + 2cw)c + (2a^2 + 2v^2 + 2w^2)w + (2ux + 2vy + 2wz)z - gw, \\
&(2ax + 2by + 2cz)a + (2ux + 2vy + 2wz)u + (2x^2 + 2y^2 + 2z^2)x - gx, \\
&(2ax + 2by + 2cz)b + (2ux + 2vy + 2wz)v + (2x^2 + 2y^2 + 2z^2)y - gy, \\
&(2ax + 2by + 2cz)c + (2ux + 2vy + 2wz)w + (2x^2 + 2y^2 + 2z^2)z - gz,
\end{align*}
\]

where $g = (a^2 + b^2 + c^2 + u^2 + v^2 + w^2 + x^2 + y^2 + z^2)$. Let $I$ denote the ideal generated by these 10 cubics. Take these 10 cubics as input and we obtain in 800 sec. only one minimal prime of $\overline{\sqrt{I}}$, which is the ideal $I$ itself. Thus $I$ is a real ideal.

Acknowledgments

We thank the referees for their valuable advises. We thank Yue Ren for his generous help with the implementation of our algorithms. We thank Erich L. Kaltofen for his valuable suggestions on the complexity of factorizing multivariate polynomials.

Mohab Safey El Din is supported by the ANR grant ANR-17-CE40-0009 GALOOP and the PGMO/FMJH grant GAMMA. Zhi-Hong Yang is supported in part by NSF Grant CCF-1717100. Lihong Zhi is supported in part by the National Key Research Project of China 2018YFA0306702 and the National Natural Science Foundation of China under Grants 11571350.

References


Safey El Din, M., 2007a. RAGLib (Real Algebraic Geometry Library), Maple package.
Safey El Din, M., Schost, É., 2004. Properness defects of projections and computation of at least one point in each


