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 $\boldsymbol{f} = (f_1, \ldots, f_s)$ be a sequence of polynomials in $\mathbb{Q}[X_1, \ldots, X_n]$ of maximal degree D and $V \subset \mathbb{C}^n$ be the algebraic set defined by $\boldsymbol{f}$ and r be its dimension. The real radical $\sqrt[re]{\langle \boldsymbol{f} \rangle}$ associated to $\boldsymbol{f}$ is the largest ideal which defines the real trace of V. When V is smooth, we show that $\sqrt[re]{\langle \boldsymbol{f} \rangle}$, has a finite set of generators with degrees bounded by $\deg V$. Moreover, we present a probabilistic algorithm of complexity $(snD^n)^{O(1)}$ to compute the minimal primes of $\sqrt[re]{\langle \boldsymbol{f} \rangle}$. When V is not smooth, we give a probabilistic algorithm of complexity $s^{O(1)}(nD)^{O(nr2^r)}$ 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 $\langle \boldsymbol{f} \rangle$, which is denoted by $\sqrt[S]{\langle \boldsymbol{f} \rangle}$, 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 $\sqrt[S]{\langle \boldsymbol{f} \rangle}$. 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 $2^p(s + p)^{O(1)}(nD)^{O(rn2^r)}$. 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.

Email addresses: `mohab.safey@lip6.fr` (Mohab Safey El Din), `zyang28@ncsu.edu` (Zhi-Hong Yang), `lzhi@mmrc.iss.ac.cn` (Lihong Zhi)

URL: `https://www-polsys.lip6.fr/~safey/` (Mohab Safey El Din), `http://www.mmrc.iss.ac.cn/~lzhi/` (Lihong Zhi)

For $\boldsymbol{f} = (f_1, \ldots, f_s)$ in $\mathbb{Q}[X] = \mathbb{Q}[X_1, \ldots, X_n]$, we denote by $\langle \boldsymbol{f} \rangle$ the ideal generated by $\boldsymbol{f}$ in $\mathbb{Q}[X]$. For $\mathbb{K} = \mathbb{C}$ or $\mathbb{R}$, we let $V_{\mathbb{K}}(\boldsymbol{f}) = \{x \in \mathbb{K}^n \mid f_1(x) = 0 \ldots, f_s(x) = 0\}$. The real radical $\sqrt[re]{\langle \boldsymbol{f} \rangle}$ of $\langle \boldsymbol{f} \rangle$ in $\mathbb{Q}[X]$ is defined as (Krivine, 1964; Dubois, 1969; Risler, 1970):

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

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

Let $\boldsymbol{g} = (g_1, \ldots, g_p)$ be another polynomial sequence in $\mathbb{Q}[X]$, $S = \{x \in \mathbb{R}^n \mid g_1(x) \geq 0, \ldots, g_p(x) \geq 0\}$ and $V_S(\boldsymbol{f}) = V_{\mathbb{R}}(\boldsymbol{f}) \cap S$. Denote $\boldsymbol{g}^\alpha = g_1^{\alpha_1} g_2^{\alpha_2} \cdots g_p^{\alpha_p}$, where $\alpha_i \in \{0, 1\}$ and $\alpha = (\alpha_1, \ldots, \alpha_p)$. The S-radical of $\langle \boldsymbol{f} \rangle$ is defined as (Stengle, 1974, Definition 5):

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

An ideal I is called S-radical if $I = \sqrt[S]{I}$. It is proved in (Stengle, 1974) that $\sqrt[S]{\langle \boldsymbol{f} \rangle}$ 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 $\sqrt[re]{\langle \boldsymbol{f} \rangle}$ is equal to the vanishing ideal of $V_{\mathbb{R}}(\boldsymbol{f})$. The semi-algebraic Nullstellensatz (Stengle, 1974) states that S-radical coincides with the vanishing ideal of $V_S(\boldsymbol{f})$. Hence, representing the real radical associated to $\boldsymbol{f}$ and the S-radical of $\boldsymbol{f}$ provides some insight on the geometry of $V_{\mathbb{R}}(\boldsymbol{f})$ and $V_S(\boldsymbol{f})$.

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 $D^{2^{O(n^2)}}$ for the degree of the generators of $\sqrt[re]{\langle \boldsymbol{f} \rangle}$. (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 sums 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 ρ. The real radical of $\langle f \rangle$ is generated by $X_1 - \rho$. The aforementioned algorithms based on numerical computations use an approximation of ρ 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 $D^{2^{O(n^2)}}$ for computing real radicals. When $V_{\mathbb{C}}(\boldsymbol{f})$ 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 $(snD^n)^{O(1)}$. When $V = V_{\mathbb{C}}(\boldsymbol{f})$ is not smooth, we obtain an algorithm using $s^{O(1)}(nD)^{O(nr2^r)}$ arithmetic operations in $\mathbb{Q}$ to represent the irreducible components of $\sqrt[re]{\langle \boldsymbol{f}\rangle}$. Here r is the dimension of the ideal $\langle \boldsymbol{f}\rangle$. Hence for fixed dimension r, it is singly exponential in n by contrast to previous results. We also extend our results for computing S-radicals with the complexity bound $2^p(s+p)^{O(1)}(nD)^{O(rn2^r)}$.

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

The difficulty in the non-smooth case is that the real algebraic set $V_{\mathbb{R}}(\boldsymbol{f})$ 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 $D^{2^{O(n^2)}}$ 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 folkore.

Definition 2. *An r-dimensional rational parametrization $\mathscr{Q} = ((w, v_1, \dots, v_n), \boldsymbol{\ell})$ in $\mathbb{Q}[T_1, \dots, T_{r+1}]$ of degree δ consists of the following:*

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

The corresponding algebraic set $Z(\mathscr{Q}) \subset \mathbb{C}^n$ is the Zariski closure of the locally closed set of points $(x_1, \dots, x_n) \in \mathbb{C}^n$ such that $\exists \vartheta \in \mathbb{C}^{r+1}, w(\vartheta) = 0, \frac{\partial w}{\partial T_{r+1}}(\vartheta) \neq 0, x_i = \frac{v_i}{\partial w / \partial T_{r+1}}(\vartheta)$. Observe that $Z(\mathscr{Q})$ is equidimensional (using the Jacobian criterion) and that the Zariski closure of the image of $Z(\mathscr{Q})$ by the map $x \to (\lambda_1(x), \dots, \lambda_{r+1}(x))$ 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 $Z(\mathscr{Q})$ (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 $\boldsymbol{f} = (f_1, \dots, f_s) \subset \mathbb{Q}[X_1, \dots, X_n]$ of degrees bounded by D. Let r be the maximum of 1 and the dimension of the algebraic set $V_{\mathbb{C}}(\boldsymbol{f})$. Then, there exists a probabilistic algorithm* LazyRealRadical *which takes as input $\boldsymbol{f}$ and returns rational parametrizations of the minimal associated primes of $\sqrt[re]{\langle \boldsymbol{f}\rangle}$ using $s^{O(1)}(nD)^{O(nr2^r)}$ arithmetic operations in $\mathbb{Q}$.*

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

Theorem 4. *Let $\boldsymbol{f} = (f_1, \ldots, f_s)$ and $\boldsymbol{g} = (g_1, \ldots, g_p)$ be two polynomial sequences in the ring $\mathbb{Q}[X_1, \ldots, X_n]$, and D be the maximal degree of polynomials in $\boldsymbol{f}$ and $\boldsymbol{g}$. Let $S = \{x \in \mathbb{R}^n \mid g_1 \geq 0, \ldots, g_p \geq 0\}$ and $\sqrt[S]{\langle \boldsymbol{f} \rangle}$ be the S-radical of $\langle \boldsymbol{f} \rangle$. Assume that the algebraic set $V_{\mathbb{C}}(\boldsymbol{f})$ has dimension r. There exists a probabilistic algorithm* LazySRadical *which takes as input $\boldsymbol{f}$ and $\boldsymbol{g}$, and returns rational parametrizations for all minimal primes of $\sqrt[S]{\langle \boldsymbol{f} \rangle}$ using $2^p(s+p)^{O(1)}(nD)^{O(rn2^r)}$ arithmetic operations in $\mathbb{Q}$.*

Plan of the paper. In Section 2, we introduce some basic notions that will be used throughout the paper. In Section 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 4, we give a probabilistic algorithm to compute rational parametrizations for all irreducible components of an arbitrarily given real algebraic set. In Section 5, we generalize the results of Section 4 to the semi-algebraic case. Section 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 (Cox et al., 1992). For basic definitions on real algebraic sets and semi-algebraic sets, we refer to (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 $\mathbb{Q}[X_1, \ldots, X_n]$ vanishing identically over S.

Let $V \subset \mathbb{C}^n$ be an algebraic set. Let $I(V) = \langle f_1, \ldots, f_s \rangle \subset \mathbb{Q}[X]$ and p be a point of V. The *tangent space* of V at p, denoted by $T_p(V)$, is given by $T_p(V) = \bigcap_{j=1}^{s} \left\{ x \in \mathbb{C}^n \;\middle|\; \sum_{i=1}^{n} \frac{\partial f_j}{\partial X_i}(p) x_i = 0 \right\}$. 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 $\dim T_p(V) = \dim_p V$. Otherwise, p is called a *singular point* of V. The *singular locus* of V is the set $\mathrm{Sing}(V) := \{p \in V \mid p \text{ is a singular point of } V\}$. We say that V is *smooth* if V has no singular point, that is, $\mathrm{Sing}(V) = \emptyset$.

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 $\sup\{\#(H_1 \cap \ldots \cap H_r \cap W)\}$ 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 $L_i = U_{i0}X_0 + \ldots + U_{in}X_n,\ i = 0, \ldots, r$. 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 $u_0, \ldots, u_r \in \mathbb{C}^{n+1}$,

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

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

Let $W \subset \mathbb{P}^n(\mathbb{C})$ 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 $\boldsymbol{f} = (f_1, \ldots, f_s)$ in $\mathbb{Q}[X_1, \ldots, X_n]$ and let f_i^h be the homogenization of f_i using the new variable X_0. Denote $\boldsymbol{f}^h = (f_1^h, \ldots, f_s^h)$. Then the affine algebraic set $V = V_{\mathbb{C}}(\boldsymbol{f})$ can be identified with a subset of $\mathbb{P}^n(\mathbb{C})$ which is $V_{\mathbb{C}}(\boldsymbol{f}^h) \setminus V_{\mathbb{C}}(X_0)$, and the *projective closure* of V is the smallest projective algebraic set containing $V_{\mathbb{C}}(\boldsymbol{f}^h) \setminus V_{\mathbb{C}}(X_0)$ (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 δ. 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 $\langle G \rangle = I(V)$.*

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 $g_1^{(i)}, \ldots, g_{m_i}^{(i)}$ with degrees bounded by $\deg V_i$ such that $I(V_i) = \langle g_1^{(i)}, \ldots, g_{m_i}^{(i)} \rangle$, 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 $I(V_i) + I\left(V_j\right) = \langle 1 \rangle$ for all $0 \leq i < j \leq r$. Therefore $I(V) = \bigcap_{i=0}^{r} I(V_i)$ which equals $\left\langle \left\{ g_{j_0}^{(0)} \cdots g_{j_r}^{(r)} \mid 1 \leq j_0 \leq m_0, \ldots, 1 \leq j_r \leq m_r \right\} \right\rangle$.

Moreover, $\deg\left(g_{j_0}^{(0)} \cdots g_{j_r}^{(r)}\right) \leq \deg\ V_0 + \cdots + \deg\ V_r = \delta$. Let

$$G = \left\{ g_{j_0}^{(0)} \cdots g_{j_r}^{(r)} \mid 1 \leq j_0 \leq m_0, \ldots, 1 \leq j_r \leq m_r \right\}.$$

We have $\langle G \rangle = I(V) = \sqrt{I}$ and $\deg(g) \leq \delta$ for all $g \in G$. □

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 $\boldsymbol{f}$ be a finite polynomial sequence of $\mathbb{Q}[X]$ and $V = V_{\mathbb{C}}(\boldsymbol{f})$ of degree δ. If V is smooth, then $\sqrt[re]{\langle \boldsymbol{f} \rangle}$ 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 $\Omega = \left\{V_j \mid V_j \cap \mathbb{R}^n \neq \emptyset,\ 1 \leq j \leq t\right\}$. If $V_j \in \Omega$, then the prime ideal $I\left(V_j\right)$ 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, $I\left(V_j\right)$ is real for every $V_j \in \Omega$. Now we have $I\left(\overline{V \cap \mathbb{R}^n}\right) = I(V \cap \mathbb{R}^n) = I\left(\bigcup_{V_j \in \Omega}\left(V_j \cap \mathbb{R}^n\right)\right)$, and the last ideal equals to $\bigcap_{V_j \in \Omega} I\left(V_j \cap \mathbb{R}^n\right)$. Here, $\overline{V \cap \mathbb{R}^n}$ 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 $V_j \in \Omega$, $I\left(V_j \cap \mathbb{R}^n\right) = I\left(V_j\right)$ because $I\left(V_j\right)$ is real. In the end, we have $I\left(\overline{V \cap \mathbb{R}^n}\right) = \bigcap_{V_j \in \Omega} I\left(V_j\right)$. It follows that $I\left(\overline{V \cap \mathbb{R}^n}\right)$ and $\bigcap_{V_j \in \Omega} I\left(V_j\right)$ define the same algebraic set, that is, $\overline{V \cap \mathbb{R}^n} = \bigcup_{V_j \in \Omega} V_j$. Then,

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

By the Real Nullstellensatz, $\sqrt[re]{\langle \boldsymbol{f} \rangle} = I(V \cap \mathbb{R}^n)$. We already observed that $I\left(\overline{V \cap \mathbb{R}^n}\right) = I(V \cap \mathbb{R}^n)$. Hence, we have $\sqrt[re]{\langle \boldsymbol{f} \rangle} = I\left(\overline{V \cap \mathbb{R}^n}\right)$. Moreover, $\overline{V \cap \mathbb{R}^n}$ is smooth because V is smooth. The conclusion follows from Theorem 5 and the inequality (1). □

3.2. Algorithm description

Let $\boldsymbol{f} = (f_1, \ldots, f_s) \subset \mathbb{Q}[X]$, and assume that $V = V_{\mathbb{C}}(\boldsymbol{f})$ is smooth of dimension r. Write the minimal equidimensional decomposition of V as $V = \bigcup_{i=0}^{r} V_i$, where V_i is either empty or is i-equidimensional. Denote by $f_1^h, \ldots, f_s^h$ 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 $V = V_{\mathbb{C}}(\boldsymbol{f})$ 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 $V_{\mathbb{R}}(f_1, \ldots, f_s)$ (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 $V_{\mathbb{C}}(f_1^h, \ldots, f_s^h) \setminus V_{\mathbb{C}}(g)$ (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 $\mathcal{F}_{V_i}$ of V_i by the subroutine Equidim. According to the definition of the Chow form, $\mathcal{F}_{V_i} = \prod_{j=1}^{m_i} \mathcal{F}_{V_{ij}}$. Therefore we can compute the Chow forms of all the irreducible components of V_i by factorizing $\mathcal{F}_{V_i}$ over $\mathbb{Q}$. The following is the algorithm mentioned in Theorem 1.

RealRadicalSmooth($\boldsymbol{f}$)

1. S = PointsPerComponents($\boldsymbol{f} = 0$);
2. if $S = \emptyset$, then return $\{1\}$;
3. $\{\mathcal{F}_{V_0}, \ldots, \mathcal{F}_{V_r}\}$ = Equidim($\boldsymbol{f}^h, X_0$);
4. for $0 \le i \le r$ do

   $\{\mathcal{F}_{V_{i1}}, \ldots, \mathcal{F}_{V_{im_i}}\} \leftarrow$ irreducible factors of $\mathcal{F}_{V_i}$;
5. $\Omega = \{\}$;
6. for $0 \le i \le r$ and $1 \le j \le m_i$ do

   G_{ij} = Generators($\mathcal{F}_{V_{ij}}$);

   if $V_{\mathbb{C}}(G_{ij}) \cap S \neq \emptyset$ then $\Omega = \Omega \cup \left\{G_{ij}\right\}$;
7. return Ω.

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 $\mathbb{Q}^{n^{O(1)}}$, and there exists a Zariski open set in $\mathbb{Q}^{n^{O(1)}}$ such that for all choices in this set yield correct answers for these algorithms in RealRadicalSmooth. In the following, we assume that all the probabilistic calls mentioned above perform correctly.

Correctness of algorithm RealRadicalSmooth**.** Let $V_{ij} = V_{\mathbb{C}}(G_{ij})$. 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 $V_{\mathbb{R}}(\boldsymbol{f})$, 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 $I\left(V_{ij}\right)$ is real if and only if $V_{ij} \cap \mathbb{R}^n \neq \emptyset$ (see the proof of Theorem 7). Thus, $I\left(V_{ij}\right)$ is real if and only if $V_{ij} \cap S \neq \emptyset$. Then we have $\sqrt[re]{\langle \boldsymbol{f} \rangle} = \bigcap_{V_{ij} \cap S \neq \emptyset} I\left(V_{ij}\right)$ (Neuhaus, 1998, Lemma 2.2(a)). Finally, the ideals $I\left(V_{ij}\right)$ are exactly the prime components of $\sqrt[re]{\langle \boldsymbol{f} \rangle}$ since V_{ij} are irreducible components of $V_{\mathbb{C}}(\boldsymbol{f})$. The correctness of the algorithm is proved.

Complexity analysis. The first step of RealRadicalSmooth computes a finite set S of real points meeting every connected component of the real algebraic set $V_{\mathbb{R}}(\boldsymbol{f})$. 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 $sL(nD^n)^{O(1)}$ arithmetic operations in $\mathbb{Q}$ where L is the length of the straight-line program Γ.

Next, by (Jeronimo et al., 2004, Theorem 1), computing the Chow forms of all equidimensional components of $V_{\mathbb{C}}(f_1^h, \ldots, f_s^h) \setminus V_{\mathbb{C}}(X_0)$ requires at most $sL(nD^n)^{O(1)}$ arithmetic operations in $\mathbb{Q}$. The Chow forms $\{\mathcal{F}_{V_0}, \ldots, \mathcal{F}_{V_r}\}$ computed in Step 3 are encoded by straight-line programs of length bounded by $sL(nD^n)^{O(1)}$ (Jeronimo et al., 2004, Section 3.5).

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

The cost of computing generators G_{ij} of $I\left(V_{ij}\right)$ from the Chow form $\mathcal{F}_{V_{ij}}$ does not increase the order of the complexity of Step 4 (Blanco et al., 2004, Section 5.5). Deciding the emptiness of $V_{\mathbb{C}}(G_{ij}) \cap S$ 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 $O(s(D+n)^n)$ (see e.g. (Krick, 2002)). Therefore, in case of success, the algorithm RealRadicalSmooth uses $(snD^n)^{O(1)}$ arithmetic operations in $\mathbb{Q}$.

4. Lazy representations and non-smooth case

4.1. Preliminary results

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

Lemma 8. *Let $V \subset \mathbb{C}^n$ be an equi-dimensional algebraic set defined over $\mathbb{Q}$ of dimension r. There exists a non-empty Zariski open set $\mathscr{G}(V) \subset \mathbb{C}^{n\times(r+1)}$ such that for $\boldsymbol{\ell} \in \mathscr{G}(V) \cap \mathbb{Q}^{n\times(r+1)}$ 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 $Z(\mathscr{Q}) = V$ with $\mathscr{Q} = ((w, v_1, \ldots, v_n), \boldsymbol{\ell})$.*

Let $\mathscr{Q} = ((w, v_1, \ldots, v_n), \boldsymbol{\ell} = (\lambda_1, \ldots, \lambda_{r+1}))$ be a rational parametrization. We define the polynomial $\sigma_{\mathscr{Q}}$ 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 $\mathcal{S}(\mathscr{Q})$ the intersection of $Z(\mathscr{Q})$ with $V_{\mathbb{C}}(\sigma_{\mathscr{Q}})$. 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 $Z(\mathscr{Q})$ 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 $Z(\mathscr{Q})$ in $\mathbb{Q}[X]$ is prime. Then, it is real if and only if one of the following equivalent conditions are satisfied:*

(i) $Z(\mathscr{Q})$ 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 $Z(\mathscr{Q})$ is not real, then $Z(\mathscr{Q}) \cap \mathbb{R}^n$ coincides with $\mathcal{S}(\mathscr{Q}) \cap \mathbb{R}^n$.

Proof. We denote $h = \frac{\partial w}{\partial T_{r+1}}$ and I the vanishing ideal of $Z(\mathscr{Q})$. By Proposition 6, I is real if and only if it has a regular real zero which is equivalent to the assertion that $Z(\mathscr{Q})$ 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 $\vartheta \in \mathbb{R}^{r+1}$ such that $w(\vartheta) = 0$ and $h(\vartheta) \neq 0$, then we have a real point $x = \left(\frac{v_1}{h}(\vartheta), \ldots, \frac{v_n}{h}(\vartheta)\right) \in Z(\mathscr{Q})$. It follows from the definition of $Z(\mathscr{Q})$ and the Hilbert Nullstellensatz that the polynomials

$w, hX_{r+2} - v_{r+2}, \ldots, hX_n - v_n$ belong to I. Then x is a regular real zero of I because the Jacobian matrix of $w, hX_{r+2} - v_{r+2}, \ldots, hX_n - v_n$ has rank $n - r$ at the point x. Thus the ideal I is real.

Conversely, if the set $\left\{\vartheta \in \mathbb{R}^{r+1} \mid w(\vartheta) = 0, h(\vartheta) \neq 0\right\}$ is empty, then we have $Z(\mathscr{Q}) \cap \mathbb{R}^n \subset Z(\mathscr{Q}) \cap V_{\mathbb{C}}(\sigma_{\mathscr{Q}})$. On the other hand, $Z(\mathscr{Q}) \cap V_{\mathbb{C}}(\sigma_{\mathscr{Q}})$ has dimension less than $\dim(Z(\mathscr{Q}))$ (since $Z(\mathscr{Q})$ is irreducible and $Z(\mathscr{Q}) \cap V_{\mathbb{C}}(\sigma_{\mathscr{Q}})$ is strictly contained in $Z(\mathscr{Q})$). Hence $Z(\mathscr{Q}) \cap \mathbb{R}^n$ has dimension less than $\dim(Z(\mathscr{Q}))$, which implies that the vanishing ideal of $Z(\mathscr{Q})$ is not real. □

From the proof of Lemma 10, we immediately have the following corollary:

Corollary 11. *Under the above notations, assume that* $Z(\mathscr{Q})$ *is irreducible, then* $\mathcal{S}(\mathscr{Q})$ *has dimension strictly less than* $\dim(Z(\mathscr{Q}))$.

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 $\boldsymbol{f} = (f_1, \ldots, f_s)$ in $\mathbb{Q}[X]$, it outputs a list of rational parametrizations encoding the irreducible components of $V_{\mathbb{C}}(\boldsymbol{f})$. This computation simply consists of calling the equidimensional decomposition algorithm in (Lecerf, 2000) which uses $(sLnD^n)^{O(1)}$ operations in $\mathbb{Q}$ to return zero-dimensional parametrizations of generic points in $V_{\mathbb{C}}(\boldsymbol{f})$. Combined with the Hensel lifting technique in (Giusti et al., 2001) (which are actually used in (Lecerf, 2000)), that algorithm allows to recover r-equidimensional parametrizations for the components of dimension r. The total cost becomes $(snD^{n\max(1,r)})^{O(1)}$. 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* $\boldsymbol{f} = (f_1, \ldots, f_s)$ *be a sequence of polynomials in* $\mathbb{Q}[X]$ *of degree bounded by* D *and* V *be the algebraic set defined by* $\boldsymbol{f}$ *with* $r = \dim(V)$. *There exists a probabilistic algorithm which computes a list of rational parametrizations encoding the irreducible components of* V *using* $(snD^{n\max(1,r)})^{O(1)}$ *operations in* $\mathbb{Q}$.

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

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

Proof. By Lemma 10, it suffices to decide if the semi-algebraic system $w = 0, \frac{\partial w}{\partial T_{r+1}} \neq 0$ has a real solution. Using (Basu et al., 2006, Chapter 14), this can be done using $\delta^{O(\max(1,r))}$ 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 $\boldsymbol{\ell}$ and returns a new sequence of linear forms $\boldsymbol{\ell}'$ and which computes a new rational parametrization still encoding Z but using $\boldsymbol{\ell}'$.

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

Then, there exists a routine ChangeSeparatingElement *which computes a rational parametrization $\mathscr{Q} = ((w', v'_1, \ldots, v'_n), \boldsymbol{\ell}')$ 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 $\deg(\mathscr{Q}) + 1$. 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 $\mathscr{Q}$. Again the extra cost comes from arithmetic operations in $\mathbb{Q}[[T_1 - y_1, \ldots, T_r - y_r]]$ which is dominated by $(n\delta)^{O(r)}$ since computations are truncated up to $\deg(\mathscr{Q}) + 1$.

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

Subroutine Intersect. Let $\mathscr{Q} = ((w, v_1, \ldots, v_n), \boldsymbol{\ell})$ with $\boldsymbol{\ell} = (\lambda_1, \ldots, \lambda_{r+1})$ 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 $g_{\mathscr{Q}}$ the polynomial $g(\lambda_1, \ldots, \lambda_{r+1}) \in \mathbb{Q}[X]$. A key step for our algorithm is to compute $Z(\mathscr{Q}) \cap V_{\mathbb{C}}(g_{\mathscr{Q}})$

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

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

Recall that Z is r-equidimensional. Observe that by Krull's theorem (Eisenbud, 1995), $Z \cap V_{\mathbb{C}}(g_{\mathscr{Q}})$ 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, $\dim(Z \cap V_{\mathbb{C}}(g_{\mathscr{Q}})) = r-1$, we deduce that $Z \cap V_{\mathbb{C}}(g_{\mathscr{Q}})$ is equidimensional (of dimension $r-1$).

Hence, it makes sense to assume additionally that the first r linear forms of $\boldsymbol{\ell}'$ lie in the non-empty Zariski open set $\mathscr{G}(Z \cap V_{\mathbb{C}}(g_{\mathscr{Q}}))$ (see again Lemma 8). Another assumption of the same nature will be done and stated precisely below.

Next, one computes a rational parametrization $\mathscr{Q}' = ((w', v'_1, \dots, v'_n), \boldsymbol{\ell}')$ defining Z. For clarity, we denote by $T'_1, \dots, T'_{r+1}$ the variables involved in $\mathscr{Q}'$. 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 $Z = Z(\mathscr{Q}')$ with $V_{\mathbb{C}}(g_{\mathscr{Q}})$. The process we would like to mimic is as follows:

1. substitute in g the variables $T_1, \dots, T_{r+1}$ by the linear forms $\lambda_1, \dots, \lambda_{r+1}$ used in $\mathscr{Q}$ (hence yielding an explicit representation of $g_{\mathscr{Q}}$);

2. substitute the X_i's by their parametrizations in $\mathscr{Q}'$, hence obtaining a rational fraction g' (it lies in $\mathbb{Q}(T'_1, \dots, T'_{r+1})$);

3. compute a representation of the intersection of the vanishing sets of the numerator of g' and w' (through subresultant computations as in (Giusti et al., 2001)) and deduce from that a rational representation of $Z \cap V_{\mathbb{C}}(g_{\mathscr{Q}})$.

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 $g_{\mathscr{Q}}$, we will actually build a straight-line program Γ evaluating it. Since g is a polynomial of degree δ' involving $r+1$ variables and since $\boldsymbol{\ell}$ is composed of $r+1$ linear forms in $X_1, \dots, X_n$ which are equal to $T_1, \dots, T_{r+1}$, 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 Γ the parametrizations $X_i = \frac{v'_i}{\partial w'/\partial T'_{r+1}}$. Evaluating all parametrizations can be done using $(n\delta)^{O(r)}$ operations in $\mathbb{Q}$ (because the polynomials in $\mathscr{Q}'$ 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 $y = (y_1, \dots, y_{r-1})$ in $\mathbb{Q}^{r-1}$. Substituting the variables $T'_1, \dots, T'_{r-1}$ by $y_1, \dots, y_{r-1}$ 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, $\mathscr{Q}'_y$ denotes the rational parametrization obtained by substituting the variables $T'_1, \dots, T'_{r-1}$ with $y_1, \dots, y_{r-1}$ in $\mathscr{Q}'$.

Using the intersection algorithm of (Giusti et al., 2001) with input $\mathscr{Q}'_y$ and the numerator of g'_y, one computes a zero-dimensional rational parametrization encoding $Z \cap V_{\mathbb{C}}(g_{\mathscr{Q}}) \cap V_{\mathbb{C}}(\boldsymbol{\ell}'_y)$.

Since, by Bézout's theorem, the intersection of Z with $V_{\mathbb{C}}(g_{\mathscr{Q}})$ has degree bounded by $\delta'\delta$, it is sufficient to repeat this process $(\delta'\delta)^{O(r)}$ times to interpolate a rational parametrization for $Z \cap V_{\mathbb{C}}(g_{\mathscr{Q}})$. The last step consists in extracting from that parametrization the irreducible components of $Z \cap V_{\mathbb{C}}(g_{\mathscr{Q}})$ by factoring the eliminating polynomial of $\mathscr{Q}$. The complexity statement follows easily. $\square$

Subroutine RemoveRedundantComponents. Let $\mathscr{L} = (\mathscr{Q}_1, \dots, \mathscr{Q}_t)$ be a list of rational parametrizations such that, for $1 \leq i \leq t$, $Z(\mathscr{Q}_i)$ is irreducible. The subroutine RemoveRedundantComponents returns a subset of $\mathscr{L}$ say, $\mathscr{Q}_{i_1}, \dots, \mathscr{Q}_{i_k}$ such that, $Z(\mathscr{Q}_{i_1}) \cup \cdots \cup Z(\mathscr{Q}_{i_k}) = Z(\mathscr{Q}_1) \cup \cdots \cup Z(\mathscr{Q}_t)$ and, for $u \neq v$, $Z(\mathscr{Q}_{i_u}) \not\subset Z(\mathscr{Q}_{i_v})$.

Lemma 16. *Let $\mathscr{L} = (\mathscr{Q}_1, \ldots, \mathscr{Q}_t)$ be a list of rational parametrizations with δ_i being the degree of $\mathscr{Q}_i$ and δ be the maximum of $\delta_1, \ldots, \delta_t$. Assume that for $1 \le i \le t$, $Z(\mathscr{Q}_i)$ 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 $\mathscr{L}$ returns a subset $\mathscr{Q}_{i_1}, \ldots, \mathscr{Q}_{i_k}$ of $\mathscr{L}$ such that, the following holds:*

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

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 $\mathscr{Q}_1, \ldots, \mathscr{Q}_t$ are already sorted by nondecreasing dimension (i.e. $r_i \le r_{i+1}$). The algorithm starts by choosing randomly $r+1$ linear forms $\boldsymbol{\ell} = (\lambda_1, \ldots, \lambda_{r+1})$ and call the routine ChangeSeparatingElement with input $\mathscr{Q}_i$ and $(\lambda_1, \ldots, \lambda_{r_i+1})$. 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 $\mathscr{Q}_1, \ldots, \mathscr{Q}_t$ for the obtained rational parametrizations. Since, by assumption, the rational parametrizations define irreducible algebraic sets, one only needs to decide if $Z(\mathscr{Q}_i) \subset Z(\mathscr{Q}_j)$ 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 $\mathbb{Q}^{r_i-1}$ and specialize both in $\mathscr{Q}_i$ and $\mathscr{Q}_j$ 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 $\boldsymbol{f} = (f_1, \ldots, f_s)$ 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 $\boldsymbol{f}$.

The algorithm starts by calling IrreducibleDecomposition to compute a finite sequence of rational parametrizations $\mathscr{R}_1, \ldots, \mathscr{R}_t$ encoding the irreducible components of $V_{\mathbb{C}}(\boldsymbol{f})$. Next, for $1 \le i \le t$, one computes a list of rational parametrizations encoding the irreducible components of the real radical associated to $Z(\mathscr{R}_i)$. 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.

LazyRealRadical($\boldsymbol{f}$)

1. $(\mathscr{R}_1, \ldots, \mathscr{R}_t) =$ IrreducibleDecomposition($\boldsymbol{f}$);
2. if $t = 1$ and $\mathscr{R}_1 = ((1))$ then return ((1));
3. res = {};
4. for $1 \le i \le t$ do
   - res = res $\cup$ LazyRealRadicalRec($\mathscr{R}_i$);
5. return RemoveRedundantComponents(res).

We describe now the routine LazyRealRadicalRec. It takes as input a rational parametrization $\mathscr{Q}$ and outputs a list of rational parametrizations encoding the irreducible algebraic sets defined by the prime components of the real radical associated to $Z(\mathscr{Q})$.

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

LazyRealRadicalRec($\mathscr{Q}$)

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

4.4. Proof of Theorem 3

We start by proving correctness and termination.

Proof. On input $\boldsymbol{f}$, LazyRealRadical starts by computing an irreducible decomposition of the algebraic set defined by $\boldsymbol{f}$ by means of rational parametrizations $\mathscr{R}_1, \ldots, \mathscr{R}_t$. The next step consists in computing rational parametrizations encoding the prime components of the real radical associated to $Z(\mathscr{R}_i)$ 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 $\mathscr{Q}$ encoding an irreducible algebraic set. We prove its correctness by decreasing induction on the dimension of $Z(\mathscr{Q})$. The case where the $Z(\mathscr{Q})$ is finite is immediate; hence we assume below that $Z(\mathscr{Q})$ 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 $Z(\mathscr{Q})$ is real by calling the routine IsReal. If this is the case, $\mathscr{Q}$ is returned as expected. Else, it computes a decomposition of $\mathcal{S}(\mathscr{Q})$ following Lemma 10. Besides, Corollary 11 establishes that $\mathcal{S}(\mathscr{Q})$ has dimension strictly less than $\dim(Z(\mathscr{Q}))$. 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 routing IrreducibleDecomposition which uses $(snD^{nr})^{O(1)}$ 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 $\boldsymbol{f}$. By Bézout's theorem, the sum of the degrees of the irreducible components encoded by the output is bounded by D^n. Hence, we have $t \leq D^n$ and for $1 \leq i \leq t$, the degree of $\mathscr{R}_i$ is bounded by D^n.

Next, one enters in the loop and call t times LazyRealRadicalRec with $\mathscr{R}_i$ as input (for $1 \leq i \leq t$). Below, we prove that running LazyRealRadicalRec with input a rational parametrization, say $\mathscr{Q}$, of degree δ encoding an irreducible algebraic set of dimension ρ takes $(n\delta)^{O(2^\rho)}$ arithmetic operations in $\mathbb{Q}$ and the sum of the degrees of the rational parametrizations it outputs lies in $(n\delta)^{O(2^\rho)}$. Hence, the whole cost of the "for loop" is $(nD)^{O(n2^r)}$.

The last step consists in calling the routine RemoveRedundantComponents. Lemma 16 allows to estimate the complexity of this step. All in all, the total cost is bounded by $s^{O(1)}(nD)^{O(nr2^r)}$.

We prove now the claim on the complexity of LazyRealRadicalRec. The first step consists in calling subroutine IsReal on input $\mathscr{Q}$. This call takes $\delta^{O(\rho)}$ arithmetic operations in $\mathbb{Q}$ (Lemma 13). When it returns true, $\mathscr{Q}$ is returned else a call to Intersect is performed with input $\mathscr{Q}$ and $\frac{\partial w}{\partial T_{\rho+1}}$ where w is the eliminating polynomial of $\mathscr{Q}$. 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 δ^2 but the dimension of these output rational parametrizations is $\rho - 1$. Hence, denoting by $T(\delta, \rho)$ the cost of LazyRealRadicalRec on input a rational parametrization of degree δ encoding an irreducible algebraic set of dimension ρ, the following recurrence formula holds:

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

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

As for algorithm RealRadicalSmooth, most of subroutines which are used in 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 $\boldsymbol{f} = (f_1, \ldots, f_s)$ and $\boldsymbol{g} = (g_1, \ldots, g_p)$ be two polynomial sequences in $\mathbb{Q}[X_1, \ldots, X_n]$. Let $S = \{x \in \mathbb{R}^n \mid g_1(x) \geq 0, \ldots, g_p(x) \geq 0\}$ and $V_S(\boldsymbol{f}) = V_{\mathbb{C}}(\boldsymbol{f}) \cap S$. We will write the equations $f_i = 0, \forall f_i \in \boldsymbol{f}$ as $\boldsymbol{f} = 0$ and write the inequalities $g_j \geq 0, \forall g_j \in \boldsymbol{g}$ as $\boldsymbol{g} \geq 0$. Similar notations will be used for inequalities involved $>$, $<$ and $\leq$.

The semi-algebraic set S is equal to the union of 2^p sets of the form: $S_\lambda = \{x \in \mathbb{R}^n \mid \boldsymbol{g}_\lambda = 0, \hat{\boldsymbol{g}}_\lambda > 0\}$ where $\boldsymbol{g}_\lambda$ is a subset of $\boldsymbol{g}$ and $\hat{\boldsymbol{g}}_\lambda = \boldsymbol{g} \setminus \boldsymbol{g}_\lambda$ (if $\boldsymbol{g}_\lambda = \emptyset$, then take $S_\lambda = \{x \in \mathbb{R}^n \mid \boldsymbol{g} > 0\}$; if $\hat{\boldsymbol{g}}_\lambda = \emptyset$ then take $S_\lambda = V_{\mathbb{R}}(\boldsymbol{g})$).

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

LazySRadical($\boldsymbol{f}, \boldsymbol{g}$)

1. if $\boldsymbol{g} = \emptyset$ then return LazyRealRadical($\boldsymbol{f}$);
2. res = {};
3. $\Lambda = \{\boldsymbol{g}_\lambda \mid \boldsymbol{g}_\lambda \subset \boldsymbol{g}\}$;

4. for every $\boldsymbol{g}_\lambda \in \Lambda$ do
   - $\boldsymbol{f}_\lambda = \boldsymbol{f} \cup \boldsymbol{g}_\lambda$, $\hat{\boldsymbol{g}}_\lambda = \boldsymbol{g} \setminus \boldsymbol{g}_\lambda$;
   - $(\mathscr{R}_1, \ldots, \mathscr{R}_t) = \mathsf{IrreducibleDecomposition}(\boldsymbol{f}_\lambda)$;
   - for $1 \leq i \leq t$ do
     - res = res $\cup$ $\mathsf{LazySRadicalRec}(\mathscr{R}_i, \hat{\boldsymbol{g}}_\lambda)$;
5. return $\mathsf{RemoveRedundantComponents}$(res).

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

$\mathsf{LazySRadicalRec}(\mathscr{Q}, \boldsymbol{g})$

1. if $\mathscr{Q} = ((1))$ then return $((1))$;
2. if $\boldsymbol{g} = \emptyset$ then return $\mathsf{LazyRealRadicalRec}(\mathscr{Q})$;
3. let $((w, v_1, \ldots, v_n), \boldsymbol{\ell}) = \mathscr{Q}$;
4. $\boldsymbol{g}_{\mathscr{Q}} = \{g(v_1, \ldots, v_n) \mid g \in \boldsymbol{g}\}$;
5. $Z = \mathsf{PointsPerComponents}(w = 0, \boldsymbol{g}_{\mathscr{Q}} > 0)$;
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 $\mathscr{Q}$;
8. $(\mathscr{Q}'_1, \ldots, \mathscr{Q}'_k) = \mathsf{Intersect}(\mathscr{Q}, \frac{\partial w}{\partial T_{r+1}})$;
9. for $1 \leq i \leq k$ do
   - res = res $\cup$ $\mathsf{LazySRadicalRec}(\mathscr{Q}'_i, \boldsymbol{g})$;
10. return $\mathsf{RemoveRedundantComponents}$(res).

5.2. *Proof of Theorem 4*

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

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

If $\boldsymbol{g}$ is empty then it reduces to the correctness of the subroutine $\mathsf{LazyRealRadicalRec}(\mathscr{Q})$ which has been shown in the proof of Theorem 3. By Lemma 10, the set $\{x \in \mathbb{R}^n \mid \boldsymbol{g} > 0\}$ contains a regular real point of $Z(\mathscr{Q})$ if and only if the polynomial system $\boldsymbol{g}_{\mathscr{Q}} > 0$, $w = 0$, $\frac{\partial w}{\partial T_{r+1}} \neq 0$

has real solutions. On the other hand, if the set $\{x \in \mathbb{R}^n \mid \boldsymbol{g} > 0\}$ contains a regular real point of $Z(\mathscr{Q})$, then the Zariski closure of A is a nonempty Zariski dense subset of $Z(\mathscr{Q})$ since $Z(\mathscr{Q})$ is irreducible. Therefore, the Zariski closure of A is equal to $Z(\mathscr{Q})$. Thus, in Step 7 of LazySRadicalRec, $\mathscr{Q}$ is returned. Else, the set A only contains some singular points of $Z(\mathscr{Q})$. Proving the correctness of the recursive call which is then performed is very similar to the one for LazyRealRadical($\mathscr{Q}$) 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 $(\mathscr{Q}, \boldsymbol{g})$, where δ is the degree of $\mathscr{Q}$ and ρ is the dimension of $Z(\mathscr{Q})$. Assume that the degrees of the polynomials in $\boldsymbol{g}$ are less than or equal to δ.

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

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

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

Next, we estimate the complexity of LazySRadical.

For every $\boldsymbol{f}_\lambda = \boldsymbol{f} \cup \boldsymbol{g}_\lambda$, the algebraic set $V_{\mathbb{C}}(\boldsymbol{f}_\lambda)$ has at most D^n irreducible components, which means the t in Step 4 of LazySRadical is bounded by D^n. With input $\boldsymbol{f}_\lambda$, the subroutine IrreducibleDecomposition uses $((s+p)nD^{nr})^{O(1)}$ arithmetic operations in $\mathbb{Q}$ (By Lemma 12). In the second "for loop" of LazySRadical, the subroutine LazySRadicalRec($\mathscr{R}_i$, $\hat{\boldsymbol{g}}_\lambda$) uses $p\delta_i^{O(2^{\rho_i})} + (n\delta_i)^{O(2^{\rho_i})}$ arithmetic operations in $\mathbb{Q}$, where δ_i is the degree of $\mathscr{R}_i$ and ρ_i is the dimension of $\mathscr{R}_i$. By Bézout's theorem, every δ_i is bounded by D^n. Observe that every ρ_i is bounded by r. Thus the whole cost of the Step 4 of LazySRadical is bounded by $2^p \cdot ((s+p)nD^{nr})^{O(1)} + 2^p D^n (pD^{O(n2^r)} + (nD)^{O(n2^r)})$, which is $2^p(s+p)^{O(1)}(nD)^{O(n2^r)}$. The final step is to remove redundant components. By Lemma 16, the complexity of this step is bounded by $(nD)^{O(rn2^r)}$ since the output parametrizations of LazySRadicalRec have degrees bounded by $(nD)^{O(n2^r)}$. To summarize, the whole complexity of LazySRadical is $2^p(s+p)^{O(1)}(nD)^{O(rn2^r)}$.

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 $V_{\mathbb{C}}(\boldsymbol{f})$. The vanishing ideal of the singular locus of $V_{\mathbb{C}}(\boldsymbol{f})$ 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 $V_{\mathbb{C}}(\boldsymbol{f}) \cap S_0$ is $\langle X, Y\rangle$.
- Let $S_1 = \{(x, y) \in \mathbb{R}^2 \mid g = 0\}$. By computation we have $V_{\mathbb{C}}(f) \cap S_1 = \emptyset$, so its vanishing ideal is $\langle 1\rangle$.

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

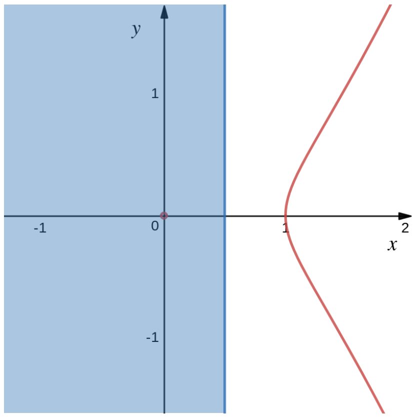

Figure 1: Example 17 $V_{\mathbb{C}}(\boldsymbol{f}) \cap S$

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 $\boldsymbol{f}$ as input, we will obtain generators of the minimal associated primes of $\sqrt[re]{\langle \boldsymbol{f} \rangle}$.

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):*

$$\begin{aligned}\mathrm{Vor1} =&(\alpha^2+\beta^2+1)a^2\lambda^4 - 2a(2a\beta^2+ay\beta+a\alpha x-\beta\alpha+2a+2a\alpha^2-\beta\alpha a^2)\lambda^3\\&+(\beta^2+6a^2\beta^2-2\beta x a^3-6\beta\alpha a^3+6y\beta a^2-6a\beta\alpha-2a\beta x+6\alpha x a^2+y^2a^2\\&-2a\alpha y+x^2a^2-2y\alpha a^3+6a^2\alpha^2+a^4\alpha^2+4a^2)\lambda^2\\&-2(xa-ya^2-2\beta a^2-\beta+2a\alpha+\alpha a^3)(xa-y-\beta+a\alpha)\lambda+(1+a^2)(xa-y-\beta+a\alpha)^2.\end{aligned}$$

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

$$P_1 = \langle a\alpha - ax+\beta-y, \lambda+1\rangle, P_2 = \langle a\alpha+ax-\beta-y, \lambda\rangle, P_3 = \langle 2\beta\lambda+\beta+y, a\rangle.$$

Example 19. *Consider the discriminant $\mathcal{D}$ of the characteristic polynomial of the following linear symmetric matrix:*

$$\begin{pmatrix} x & 1 & 1\\ 1 & y & 1\\ 1 & 1 & z\end{pmatrix}.$$

It has been proved that $\mathcal{D}$ is a sum of squares (Lax, 2005). On input $\mathcal{D}$, our algorithm computed in 4 sec. the real radical $\sqrt[re]{\langle \mathcal{D} \rangle}$. It has only one minimal prime which is $\langle y - z, g\rangle$ where

$$
\begin{aligned}
g = & - 19y^{12} + 228y^{11}z - 1254y^{10}z^2 + 4180y^9z^3 - 9405y^8z^4 + 15048y^7z^5 - 17556y^6z^6 + 15048y^5z^7 \\
& - 9405y^4z^8 + 4180y^3z^9 - 1254y^2z^{10} + 228yz^{11} - 19z^{12} - 606y^{10} + 6060y^9z - 27270y^8z^2 \\
& + 72720y^7z^3 - 127260y^6z^4 + 152712y^5z^5 - 127260y^4z^6 + 72720y^3z^7 - 27270y^2z^8 + 6060yz^9 \\
& - 606z^{10} - 6732y^8 + 53856y^7z - 188496y^6z^2 + 376992y^5z^3 - 471240y^4z^4 + 376992y^3z^5 \\
& - 188496y^2z^6 + 53856yz^7 - 6732z^8 - 35370y^6 + 212220y^5z - 530550y^4z^2 + 707400y^3z^3 \\
& - 530550y^2z^4 + 212220yz^5 - 35370z^6 - 116073y^4 + 464292y^3z - 696438y^2z^2 + 464292yz^3 \\
& - 116073z^4 - 77760y^2 + 155520yz - 77760z^2 + 139968x - 69984y - 69984z.
\end{aligned}
$$

Example 20 (Homotopy-1)**.** *This example is taken from Chen et al. (2013):*

$$f_1 = x^3y^2 + c_1x^3y + y^2 + c_2x + c_3,\ f_2 = c_4x^4y^2 - x^2y + y + c_5,\ f_3 = c_4 - 1.$$

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

Example 21 (Cinquin-3-4)**.** *This is also an example taken from Chen et al. (2013):*

$$f_1 = s - x_1(1 + x_2^4 + x_3^4),\ f_2 = s - x_2(1 + x_1^4 + x_3^4),\ f_3 = s - x_3(1 + x_1^4 + x_2^4).$$

We obtain in 47 sec. the minimal primes of $\sqrt[re]{\langle \boldsymbol{f} \rangle}$ for $\boldsymbol{f} = (f_1, f_2, f_3)$:

$$
\begin{aligned}
P_1 &= \left\langle x_3 - x_1, x_2 - x_1, -x_3^4x_1 - x_2^4x_1 - x_1 + s \right\rangle, \\
P_2 &= \left\langle x_3 - x_1, x_2^3x_1 + x_2^2x_1^2 + x_2x_1^3 - x_1^4 - 1, -x_3^4x_1 - x_2^4x_1 - x_1 + s \right\rangle, \\
P_3 &= \left\langle x_2 - x_1, x_3^3x_1 + x_3^2x_1^2 + x_3x_1^3 - x_1^4 - 1, -x_3^4x_1 - x_2^4x_1 - x_1 + s \right\rangle, \\
P_4 &= \left\langle x_3 - x_2, x_2^4 - x_2^3x_1 - x_2^2x_1^2 - x_2x_1^3 + 1, -x_3^4x_1 - x_2^4x_1 - x_1 + s \right\rangle.
\end{aligned}
$$

Example 22 (Essential Variety)**.** *This is an example taken from Fløystad et al. (2017). Let $\mathcal{E}$ be the essential variety defined as:*

$$\mathcal{E} = \left\{ M \in \mathbb{R}^{3\times3} \mid \det(M) = 0, 2(MM^T)M - \operatorname{tr}(MM^T)M = 0 \right\},$$

where $\det(M)$ *is the determinant of M and* $\operatorname{tr}(MM^T)$ *is the trace of MM^T.*

If we write the matrix M as

$$\begin{pmatrix} a & b & c \\ u & v & w \\ x & y & z \end{pmatrix},$$

then the 10 cubics defining $\mathcal{E}$ are:

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

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 $\sqrt[re]{I}$, 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 Galop 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

Basu, S., Pollack, R., Roy, M.-F., 2006. Algorithms in Real Algebraic Geometry. Springer Berlin Heidelberg, Berlin, Heidelberg.

Becker, E., Neuhaus, R., 1993. Computation of real radicals of polynomial ideals. In: Eyssette, F., Galligo, A. (Eds.), Computational Algebraic Geometry. Vol. 109. Birkhäuser, Boston, MA, pp. 1–20.

Blanco, C., Jeronimo, G., Solernó, P., 2004. Computing generators of the ideal of a smooth affine algebraic variety. Journal of Symbolic Computation 38 (1), 843–872.

Bochnak, J., Coste, M., Roy, M.-F., 1998. Real algebraic geometry. Vol. 36. Springer, Berlin, Heidelberg.

Brake, D. A., Hauenstein, J. D., Liddell, Jr., A. C., 2016. Validating the completeness of the real solution set of a system of polynomial equations. In: Proceedings of the 2016 International Symposium on Symbolic and Algebraic Computation. ISSAC'16. ACM, New York, NY, USA, pp. 143–150.

Chen, C., Davenport, J. H., May, J. P., Maza, M. M., Xia, B., Xiao, R., 2010. Triangular decomposition of semi-algebraic systems. In: Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation. ISSAC'10. ACM, New York, NY, USA, pp. 187–194.

Chen, C., Davenport, J. H., May, J. P., Maza, M. M., Xia, B., Xiao, R., 2013. Triangular decomposition of semi-algebraic systems. Journal of Symbolic Computation 49, 3–26.

Chen, C., Davenport, J. H., Moreno Maza, M., Xia, B., Xiao, R., 2011. Computing with semi-algebraic sets represented by triangular decomposition. In: Proceedings of the 36th International Symposium on Symbolic and Algebraic Computation. ISSAC'11. ACM, New York, NY, USA, pp. 75–82.

Cox, D., Little, J., O'shea, D., 1992. Ideals, varieties, and algorithms. Vol. 3. Springer.
Dubois, D., 1969. A nullstellensatz for ordered fields. Arkiv för Matematik 8 (2), 111–114.
Durvye, C., Lecerf, G., 2008. A concise proof of the Kronecker polynomial system solver from scratch. Expositiones Mathematicae 26 (2), 101–139.
Eisenbud, D., 1995. Commutative Algebra: with a View Toward Algebraic Geometry. Vol. 150. Springer New York, New York, NY.
Everett, H., Lazard, D., Lazard, S., Safey El Din, M., 2009. The Voronoi diagram of three lines. Discrete & Computational Geometry 42 (1), 94–130.
Fløystad, G., Kileel, J., Ottaviani, G., 2017. The Chow form of the essential variety in computer vision. Journal of Symbolic Computation.
Gelfand, I. M., Kapranov, M. M., Zelevinsky, A. V., 1994. Discriminants, Resultants, and Multidimensional Determinants. Birkhäuser Boston, Boston, MA.
Giusti, M., Lecerf, G., Salvy, B., 2001. A Gröbner free alternative for polynomial system solving. Journal of complexity 17 (1), 154–211.
Jeronimo, G., Krick, T., Sabia, J., Sombra, M., 2004. The computational complexity of the Chow form. Foundations of Computational Mathematics 4 (1), 41–117.
Kalkbrener, M., 1991. Three contributions to elimination theory. Ph.D. thesis, Johannes Kepler University, Linz.
Kaltofen, E., 1989. Factorization of polynomials given by straight-line programs. Randomness and Computation 5, 375–412.
Kaltofen, E., Li, B., Yang, Z., Zhi, L., 2008. Exact certification of global optimality of approximate factorizations via rationalizing sums-of-squares with floating point scalars. In: Proceedings of the Twenty-first International Symposium on Symbolic and Algebraic Computation. ISSAC'08. ACM, New York, NY, USA, pp. 155–164.
Kaltofen, E., Trager, B. M., 1990. Computing with polynomials given by black boxes for their evaluations: greatest common divisors, factorization, separation of numerators and denominators. Journal of Symbolic Computation 9 (3), 301–320.
Krick, T., 2002. Straight-line programs in polynomial equation solving. Foundations of computational mathematics: Minneapolis 312, 96–136.
Krivine, J.-L., 1964. Anneaux préordonnés. Journal d'analyse mathématique 12 (1), 307–326.
Lasserre, J.-B., Laurent, M., Mourrain, B., Rostalski, P., Trébuchet, P., 2013. Moment matrices, border bases and real radical computation. Journal of Symbolic Computation 51, 63–85.
Lasserre, J. B., Laurent, M., Rostalski, P., 2008. Semidefinite characterization and computation of zero-dimensional real radical ideals. Foundations of Computational Mathematics 8 (5), 607–647.
Lax, P., 2005. On the discriminant of real symmetric matrices. Selected Papers Volume II, 577–586.
Lazard, D., 1991. A new method for solving algebraic systems of positive dimension. Discrete Applied Mathematics 33 (1-3), 147–160.
Lecerf, G., 2000. Computing an equidimensional decomposition of an algebraic variety by means of geometric resolutions. In: Proceedings of the 2000 International Symposium on Symbolic and Algebraic Computation. ISSAC'00. ACM, New York, NY, USA, pp. 209–216.
Lecerf, G., 2003. Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers. Journal of Complexity 19 (4), 564–596.
Ma, Y., Wang, C., Zhi, L., 2016. A certificate for semidefinite relaxations in computing positive-dimensional real radical ideals. Journal of Symbolic Computation 72, 1–20.
Marshall, M., 2008. Positive polynomials and sums of squares. No. 146. American Mathematical Soc.
Moreno Maza, M., 1997. Calculs de pgcd au-dessus des tours d'extensions simples et résolution des systèmes d'équations algébriques. Ph.D. thesis, Université Paris 6.
Neuhaus, R., 1998. Computation of real radicals of polynomial ideals – II. Journal of Pure and Applied Algebra 124 (1), 261–280.
Poteaux, A., Schost, É., 2013. On the complexity of computing with zero-dimensional triangular sets. Journal of Symbolic Computation 50 (Supplement C), 110 – 138.
Risler, J.-J., 1970. Une caractérisation des idéaux des variétés algébriques réelles. CR Acad. Sci. Paris 271, 1171–1173.
Safey El Din, M., 2005. Finding sampling points on real hypersurfaces is easier in singular situations. MEGA (Effective Methods in Algebraic Geometry) Electronic proceedings.
Safey El Din, M., 2007a. RAGLib (Real Algebraic Geometry Library), Maple package.
Safey El Din, M., 2007b. Testing sign conditions on a multivariate polynomial and applications. Mathematics in Computer Science 1 (1), 177–207.
Safey El Din, M., Schost, É., 2003. Polar varieties and computation of one point in each connected component of a smooth real algebraic set. In: Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation. ISSAC'03. ACM, New York, NY, USA, pp. 224–231.
Safey El Din, M., Schost, É., 2004. Properness defects of projections and computation of at least one point in each

connected component of a real algebraic set. Discrete & Computational Geometry 32 (3), 417–430.
Safey El Din, M., Schost, É., 2017. A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets. Journal of the ACM 63 (6), 48:1–48:37.
URL `http://doi.acm.org/10.1145/2996450`
Schost, É., 2003. Computing parametric geometric resolutions. Applicable Algebra in Engineering, Communication and Computing 13 (5), 349–393.
Sekiguchi, Y., Takenawa, T., Waki, H., Jun 2013. Real ideal and the duality of semidefinite programming for polynomial optimization. Japan Journal of Industrial and Applied Mathematics 30 (2), 321–330.
URL `https://doi.org/10.1007/s13160-013-0104-6`
Spang, S. J., 2007. On the computation of the real radical. Ph.D. thesis, Technische Universität Kaiserslautern.
Spang, S. J., 2008. A zero-dimensional approach to compute real radicals. The Computer Science Journal of Moldova 16 (1), 64–92.
Stengle, G., 1974. A Nullstellensatz and a Positivstellensatz in semialgebraic geometry. Mathematische Annalen 207 (2), 87–97.
Wang, D., 1998. Decomposing polynomial systems into simple systems. Journal of Symbolic Computation 25 (3), 295–314.
Wu, W.-T., 1984. Basic principles of mechanical theorem proving in elementary geometries. Journal of Systems Science and Mathematical Sciences 4, 207–235.