ELSEVIER Journal of Pure and Applied Algebra 124 (1998) 261–280

JOURNAL OF
PURE AND
APPLIED ALGEBRA

Computation of real radicals of polynomial ideals – II

Rolf Neuhaus *

Universität Dortmund, Fachbereich Mathematik, D-44221 Dortmund, Germany

Communicated by M.-F. Roy; received 27 January 1995; revised 1 August 1995

Abstract

In the present paper we describe an algorithm for the computation of real radicals of polynomial ideals. Moreover, results concerning the computational requirements and the complexity as well as some theoretical consequences are presented. © 1998 Elsevier Science B.V.

1. Introduction

This paper is a sequel to the work of Becker and Neuhaus [2] where an algorithm for the computation of the real radical was published for the first time. For the convenience of the reader we present this algorithm in a revised form together with more background material. The issue of complexity is dealt with and further theoretical and algorithmical studies are included. The term "computation of an ideal J from a given input ideal I" has to be understood in the following strong sense: Given any finite set $f_1,\dots,f_s$ of generators of the input ideal I a finite set of generators of the ideal J is constructed algorithmically.

In classical algebraic geometry Hilbert's Nullstellensatz is of fundamental importance: Let k be a field with algebraic closure $\bar{k}$ and I some ideal of the polynomial ring $k[X_1,\dots,X_n]$. We set

$$\mathscr{V}_{\bar{k}}(I) = \{\underline{x} \in \bar{k}^n \mid f(\underline{x}) = 0 \text{ for all} f \in I\}$$

for the set of zeros of I over $\bar{k}$. Then – according to Hilbert's Nullstellensatz – the vanishing ideal

$$\mathscr{I}_k(V) = \{f \in k[X_1,\dots,X_n] \mid f(\underline{x}) = 0 \text{ for all } \underline{x} \in V\}$$

* Tel.:+49 6227 342965; fax; +49 6227 343390; e-mail: rolf.neuhaus@sap-ag.de.

0022-4049/98/$19.00 © 1998 Elsevier Science B.V. All rights reserved
PII S0022-4049(96)00103-X

of the variety $V := \mathscr{V}_{\bar{k}}(I)$ equals the radical

$$\sqrt{I} = \{f \in k[X_1,\ldots,X_n] \mid f^r \in I \text{ for some } r \in \mathbb{N}\}.$$

Because of the one-to-one correspondence between the irreducible k-varieties of the affine space $\bar{k}^n$ and the prime ideals of $k[X_1,\ldots,X_n]$ the variety $\mathscr{V}_{\bar{k}}(I)$ can be studied by means of $\sqrt{I}$. This explains the demand for an algorithm to compute radicals in polynomial rings over a field. Already Hermann was dealing with that problem in her treatise "Die Frage der endlich vielen Schritte in der Theorie der Polynomideale" (Mathematische Annalen, Vol. 95) which was published in 1926. Since then many papers about radical computations have been published in the literature (cf. [1, 6, 9, 14, 23]). As a sample, let us mention the algorithms described in [9, 14]: Given as input a finite set of generators $f_1,\ldots,f_r$ of some ideal $I \trianglelefteq k[X_1,\ldots,X_n]$, a finite set of generators $g_1,\ldots,g_s$ of the radical $\sqrt{I}$ is constructed by means of localizations and calculation of square-free parts. Thereby the degree of the output polynomials $g_1,\ldots,g_s$ can be bounded by a function of type $\max\{\deg f_i \mid 1 \le i \le r\}^{2^{O(n^2)}}$. Moreover, these algorithms can be realized algorithmically – at least in the case of $\mathrm{Char}(k) = 0$ – if the field k is effectively given, i.e. if the elements of k can be coded effectively and if the operations $+, -, \cdot, .^{-1}, =$ can be realized upon this codification.

In the present paper we are dealing with the corresponding problems in real algebraic geometry. Thereby the situation is as follows: Let k be a formally real field and τ a preordering of k, i.e. $\tau \subseteq k$ such that

$$\tau + \tau \subseteq \tau,\ \tau \cdot \tau \subseteq \tau,\ k^2 \subseteq \tau \text{ and } -1 \notin \tau.$$

As usual $\bar{k}$ denotes a fixed algebraic closure of k. Now, if $I \trianglelefteq k[X_1,\ldots,X_n]$ then we set

$$\mathscr{V}_\tau(I) = \bigcup_R \mathscr{V}_R(I)$$

for the set of τ-real points of I where R ranges over all real closed intermediate fields of $\bar{k} \mid k$ satisfying $\tau \subseteq R^2 = \{x^2 \mid x \in R\}$. According to the Real Nullstellensatz which was proved independently by Krivine et al. (cf. [15, 5, 21]) in the 1960s the vanishing ideal of $\mathscr{V}_\tau(I)$ in $A := k[X_1,\ldots,X_n]$ equals the τ-radical

$$\sqrt[\tau]{I} = \left\{ f \in A \middle| f^{2r} + \sum_{i=1}^{m} s_i\ a_i^2 \in I \text{ for some } r \in \mathbb{N},\ m \in \mathbb{N}_0,\ s_i \in \tau,\right.$$
$$\left. a_i \in A (i = 1 \ldots m) \right\}.$$

Similarily to the situation over an algebraically closed field, the set $\mathscr{V}_\tau(I)$ can be studied by means of its vanishing ideal $\mathscr{I}_k(\mathscr{V}_\tau(I)) = \sqrt[\tau]{I}$: for example the geometric Zariski-dimension of $\mathscr{V}_\tau(I)$ equals the Krull-dimension of $\sqrt[\tau]{I}$ (see [2, Proposition 7] for detail). From this fact arises the interest in an algorithm for the computation of

τ-radicals as it is described in the present paper. But before giving a short overview over the following sections let us recall once more that this method was essentially presented at the MEGA-92 conference in Nice (cf. [2]). However, in the following sections the algorithm is described in a conciser way. In particular, the complicated recursion technique has been simplified. Moreover, we are able to present theoretical consequences of this algorithm which solve some open problems formulated in [2].

In Section 2 we start by defining the set $\mathscr{V}_\tau(I)$ of τ-real points as well as the τ-radical $\sqrt[\tau]{I}$. Next we examine the compatibility of the $\sqrt[\tau]{.}$-operator with the calculation of ideal intersections and the extension of ideals in quotient rings. Preparatory to the Real Nullstellensatz which is presented at the end of that section a characterization of τ-real prime ideals is given.

In Section 3 the concept of isolated real points is introduced. Thereby a point $\underline{x} \in \mathscr{V}_{\bar{k}}(I)$ is called isolated if it is isolated in the topological space $\mathscr{V}_R(I)$ (with respect to the order topology) for some real closed intermediate field R of $\bar{k} \mid k$. The set of all these isolated real points is denoted by $\mathscr{V}_{\text{iso}}(I)$. We prove that the vanishing ideal $I_{\text{iso}} = \mathscr{I}_k(\mathscr{V}_{\text{iso}}(I))$ of these isolated real points is the (finite) intersection of maximal ideals $M_1,\ldots,M_r$ such that any zero-dimensional component of $\sqrt[\tau]{I}$ occurs among the M_i. This fact allows the construction of the zero-dimensional components of $\sqrt[\tau]{I}$: Although we do not know how to compute I_{iso} exactly we are able to give an iterative method for the construction of an ideal J such that $\dim J \leq 0$ and $I \subseteq J \subseteq I_{\text{iso}}$ which meets our requirements in connection with the calculation of τ-radicals.

In Section 4 the algorithm for the computation of τ-radicals is presented. We start with the univariate case in some polynomial ring $k(Y_1,\ldots,Y_m)[X]$ which can be handled via polynomial factorization and the sign change criterion. Next we show how to extend this method to the general zero-dimensional case. A central result of Section 4 is the equality

$$\sqrt[\tau]{I} = \bigcap_{S \subseteq \{X_1,\ldots,X_n\}} \left(\sqrt[\tau]{(I \cdot k(S))_{\text{iso}}} \cap k[X_1,\ldots,X_n] \right).$$

Thus $\sqrt[\tau]{I}$ is completely determined by the τ-radicals of the ideals $(I \cdot k(S))_{\text{iso}}$ describing the finitely many real isolated points of its extension ideals $I \cdot k(S)$, $S \subseteq \{X_1,\ldots,X_n\}$. Combining the equality with the results obtained so far we immediately get a method to construct the τ-radical of polynomial ideals of arbitrary dimension.

Following the algorithm for the computation of real radicals we demonstrate in Section 5 that for any preordering τ of k the τ-radical of an ideal $I = (f_1,\ldots,f_r) \trianglelefteq k[X_1,\ldots,X_n]$ is generated by polynomials of degree less than $\max\{\deg fi \mid 1 \leq i \leq r\}^{2^{O(n^2)}}$.

In Section 6, preparing Section 7 but also of interest in its own, a constructive proof of the Open-Mapping Theorem of Elman, Lam and Wadsworth is presented. Given any finitely generated extension $F \mid k$ of formally real fields satisfying certain computational conditions this proof makes it feasible to compute the restriction of any constructible subset $C \subseteq X(F)$ to k.

The dependence of the α-radical $\sqrt[\alpha]{I}$ on the ordering $\alpha \in X(k)$ is the subject of Section 7. It is proved that for any ideal I of some affine k-algebra A the space of orderings $X(k)$ is a finite union of constructible subsets $C_1, \dots, C_r \subseteq X(k)$ such that the mapping $\alpha \longmapsto \sqrt[\alpha]{I}$ is constant on any C_i. Moreover, using the results of Section 6 a description of the C_i can be obtained algorithmically under certain computational conditions.

2. Real radicals

Throughout this paper a *k-algebra* is associative, commutative, and has a unit.

Definition 2.1. Let (k,τ) be a preordered field and I an ideal of some k-algebra A.

(a) The τ-radical of I is defined by

$$\sqrt[\tau]{I} = \left\{ f \in A \mid f^{2r} + \sum_{i=1}^{m} s_i a_i^2 \in I \text{ for some } r \in \mathbb{N},\ m \in \mathbb{N}_0,\ s_i \in \tau,\ a_i \in A \right\}$$

In the case $\tau = \sum k^2$ we simply write $\sqrt[re]{I}$ instead of $\sqrt[\tau]{I}$ for the so-called *real radical* of I.

(b) I is called *τ-real iff* $\sqrt[\tau]{I} = I$. Finally, I is called *real iff* $\sqrt[re]{I} = I$.

It is elementary to prove that $\sqrt[\tau]{I}$ is a radical ideal. Moreover, $\sqrt[\tau]{I}$ is the (with respect to inclusion) smallest τ-real ideal containing I. Next we observe that the calculation of τ-radicals is compatible with the calculation of ideal intersections and the extension in quotient rings.

Lemma 2.2. *Let (k,τ) be a preordered field, I, J ideals of some k-algebra A and S a multiplicatively closed subset of A satisfying $1 \in S$ and $0 \notin S$. Then we have:*

(a) $\sqrt[\tau]{I \cap J} = \sqrt[\tau]{I} \cap \sqrt[\tau]{J}$,

(b) $\sqrt[\tau]{I_S} = \sqrt[\tau]{I}_S$.

Thereby $\sqrt[\tau]{I_S}$ denotes the τ-radical of the extension ideal I_S of I in the quotient ring A_S which naturally is a k-algebra.

We point out that our algorithm for the computation of τ-radicals strongly relies on the elementary properties stated above.

Lemma 2.3. *Let (k,τ) be a preordered field and I a τ-real ideal of some k-algebra A. Then all minimal primes of I are τ-real as well.*

Proof. Let P be a minimal prime of I and $f \in \sqrt[\tau]{P}$, e.g. $f^{2r} + s \in P$ for some $r \in \mathbb{N}$, $s \in \sum \tau A^2$. We have to prove that $f \in P$.

Since PA_P is the only minimal prime of the radical ideal I_P in the local ring A_P we have $I_P = PA_P$ and thus $I_{(P)} = P$. From $f^{2r}+s\in P = I_{(P)}$ we derive that $t(f^{2r}+s)\in I$ for some $t\in A\backslash P$. But then $(tf)^{2r}+t^{2r}s\in I$ and finally $tf\in\sqrt[\tau]{I}=I\subseteq P$. Since $t\notin P$ we conclude that $f\in P$. □

Corollary 2.4. *Let (k,τ) be a preordered field and I an ideal of some k-algebra A. Then $\sqrt[\tau]{I}=\bigcap P$, where P ranges over all τ-real primes containing I.*

Proof. As a τ-real ideal $\sqrt[\tau]{I}$ is radical and thus the intersection of its minimal primes. These are τ-real by Lemma 2.3. □

For any formally real field k we denote by $X(k)$ its set of orderings.

Proposition 2.5. *Let (k,τ) be a preordered field and P a prime ideal of some k-algebra A. Then the following statements are equivalent:*

(a) *P is τ-real.*

(b) *There is some $\alpha\in X(k)$ satisfying $\alpha\supseteq\tau$ which can be extended to an ordering $\tilde{\alpha}$ of the function field $k(P)=\mathrm{Quot}(A/P)$.*

(c) *There is some $\alpha\in X(k)$ satisfying $\alpha\supseteq\tau$ such that P is α-real.*

Moreover, if A is an affine k-algebra *and P* a *maximal ideal of A then the statements* (a) – (c) *are equivalent to:*

(d) *There is some $\alpha\in X(k)$ satisfying $\alpha\supseteq\tau$ such that $k(P)$ can be embedded into some real closure of (k,α).*

Proof.

(a) $\Longrightarrow$ (b): Let $\tilde{\tau}$ denote the quadratic semiring

$$\tilde{\tau} := \left\{\sum_{i=1}^{m} s_i a_i^2 \in k(P)\,|\, m\in\mathbb{N}_0,\ s_1,\ldots,s_m\in\tau,\ a_1,\ldots,a_m\in k(P)\right\}$$

generated by τ in $k(P)$. Then P is τ-real iff $\tilde{\tau}$ is a preordering of $k(P)$, i.e. $-1\notin\tilde{\tau}$. By choosing an ordering $\tilde{\alpha}\in X(k(P))$ extending $\tilde{\tau}$ we obtain via $\alpha:=\tilde{\alpha}\cap k$ an element of $X(k)$ as required.

(b) $\Longrightarrow$ (c): Let be $f\in\sqrt[\alpha]{P}$, e.g. $f^{2r}+\sum_{\text{finite}} s_i a_i^2\in P$ for some $r\in\mathbb{N}$, $s_i\in\alpha$, $a_i\in A$. Taking residues modulo P we obtain the equation $\bar{f}^{2r}+\sum_{\text{finite}} s_i\bar{a}_i^2=0$ in the ordered field $(k(P),\tilde{\alpha})$ from which we conclude that $\bar{f}=0$ in $k(P)$, i.e. $f\in P$.

(c) $\Longrightarrow$ (a): The assertion immediately follows from the inclusion chain $P\subseteq\sqrt[\tau]{P}\subseteq\sqrt[\alpha]{P}=P$.

Finally, we remark that in the case of an affine k-algebra A for any maximal ideal P of A the function field $k(P)=A/P$ is a finite (algebraic) extension of k. □

Proposition 2.6. *Let (k,τ) be a preordered field and I an ideal of some affine k-algebra A. Then we have $\sqrt[\tau]{I}=\bigcap M$, where M ranges over all τ-real maximal ideals of A containing I.*

Proof. Let be $f \in A \setminus \sqrt[\tau]{I}$. By Corollary 2.4 we conclude that $f \notin P$ for some τ-real prime P containing I. We proceed by demonstrating that there is some τ-real maximal ideal M of A such that $M \supseteq P(\supseteq I)$ and $f \notin M$.

From Proposition 2.5 we obtain that there is an $\alpha \in X(k)$ satisfying $\alpha \supseteq \tau$ which can be extended to some $\tilde{\alpha} \in X(k(P))$. Now let R be a real closure of (k, α). Then the Artin–Lang Theorem (cf. [19, Ch. XI, Section 3, Theorem 5]) yields the existence of some k-homomorphism

$$\varphi : B := A/P\left[\frac{1}{f}\right] \longrightarrow R.$$

It remains to verify that the kernel of the k-homomorphism

$$\Phi : A \xrightarrow{\pi} A/P \xrightarrow{i} B \xrightarrow{\varphi} R$$

is a maximal ideal of A as required. □

Given any field k we write $\bar{k}$ for its algebraic closure.

Definition 2.7. Let (k, τ) be a preordered field and $I \trianglelefteq k[X_1, \dots, X_n]$. Then

$$\mathscr{V}_\tau(I) := \{\underline{x} \in \mathscr{V}_{\bar{k}}(I) \mid \underline{x} \in R^n \text{ for some real closure } R \text{ of } k \text{ extending an order } \alpha \supseteq \tau\}$$

denotes the set of *τ-real points of I*.

Theorem 2.8. *Let (k, τ) be a preordered field and $I \trianglelefteq k[X_1, \dots, X_n]$. Then we have $\mathscr{I}_k(\mathscr{V}_\tau(I)) = \sqrt[\tau]{I}$.*

Proof. It is easy to verify that any $f \in \sqrt[\tau]{I}$ vanishes on $\mathscr{V}_\tau(I)$. Thus let be $f \in A \setminus \sqrt[\tau]{I}$. We have to show that there is some $\underline{x} \in \mathscr{V}_\tau(I)$ such that$f(\underline{x}) \neq 0$.

By Proposition 2.6 there exists some τ-real maximal ideal M of A satisfying $M \supseteq I$ and $f \notin M$ whereby the function field $k(M)$ can be embedded into some real closure R of (k, α), $\alpha \in X(k)$ such that $\alpha \supseteq \tau$, by Proposition 2.5. Now, if $\bar{\cdot} : A \longrightarrow A/M = k(M)$ denotes the canonical epimorphism then the point $\underline{x} := (\overline{X}_1, \dots, \overline{X}_n) \in k(M)^n \subseteq R^n \subseteq \bar{k}^n$ has the demanded properties. □

Lemma 2.9. *Let (k, τ) be a preordered field and $P \in \operatorname{Spec}(k[X_1, \dots, X_n])$. Then the following statements are equivalent*:

(a) *P is τ-real.*

(b) *There is an ordering $\alpha \in X(k)$ satisfying $\alpha \supseteq \tau$ and a prime Q in $R[X_1, \dots, X_n]$, where R is the real closure of (k, α), such that $P = Q \cap k[X_1, \dots, X_n]$.*

Proof. The implication (b) $\Longrightarrow$ (a) is easy to verify. We restrict ourselves to prove that (a) implies (b).

Let P be τ-real. Then there is some $\alpha \in X(k)$, $\alpha \supseteq \tau$, such that $\sqrt[\alpha]{P} = P$ (Proposition 2.5). If R is a real closure of (k, α) then (as a consequence of the Real Nullstellensatz 2.8)

$$P = \sqrt[\alpha]{P} = \sqrt[re]{P \cdot R} \cap k[X_1, \dots, X_n]$$

and thus $P = Q \cap k[X_1, \dots, X_n]$ for some minimal prime Q of $\sqrt[re]{P \cdot R}$ in $R[X_1, \dots, X_n]$. But as a minimal prime of the real ideal $\sqrt[re]{P \cdot R}$ the ideal Q is real as well (Lemma 2.3). □

3. Isolated real points

In the sequel any real closed field R will be understood as a topological field under its order topology, and the affine space R^n will be endowed with the product topology.

Definition 3.1. Let F be a formally real field with algebraic closure $\bar{F}$ and $I \trianglelefteq F[X_1, \dots, X_n]$.

(a) *A point* $\underline{x} \in \mathcal{V}_{\bar{F}}(I)$ *is called* isolated real point of I if there is some real closure R of F such that $\underline{x}$ is isolated in the topological space $\mathcal{V}_R(I) \subseteq R^n$.

(b) The set of all isolated real points will be denoted by $\mathcal{V}_{\text{iso}}(I)$.

(c) Finally, we define $I_{\text{iso}} := \mathcal{I}_F(\mathcal{V}_{\text{iso}}(I))$ (the ideal describing the F-Zariski-closure of $\mathcal{V}_{\text{iso}}(I)$).

Obviously, I_{iso} is a real ideal. The importance of I_{iso} in connection with the computation of real radicals is due to the following fact.

Proposition 3.2. *Let* $(F, \tilde{\tau})$ *be a preordered field and* $I \trianglelefteq F[X_1, \dots, X_n]$. *Then* I_{iso} *is contained in any zero-dimensional component of* $\sqrt[\tilde{\tau}]{I}$.

Proof. Let M be a zero-dimensional component of $\sqrt[\tilde{\tau}]{I}$. Then M is $\tilde{\tau}$-real by Lemma 2.3. Using Lemma 2.9, M can be extended to a (necessarily) maximal ideal $\tilde{M} \lhd R[X_1, \dots, X_n]$ whereby R denotes a real closure of $(F, \tilde{\alpha})$, $\tilde{\alpha} \in X(F)$ such that $\tilde{\alpha} \supseteq \tilde{\tau}$. The reality of $\tilde{M}$ implies that $\tilde{M}$ has a zero $\underline{x} \in R^n$.

Next we claim that $\tilde{M}$ is a component of $\sqrt[re]{I \cdot R}$. If not we would find a further real prime $\tilde{Q}$ between $\sqrt[re]{I \cdot R}$ and $\tilde{M}$. But then

$$\sqrt[\tilde{\tau}]{I} \subseteq \tilde{Q} \cap F[X_1, \dots, X_n] =: Q \subseteq M.$$

Since M is a minimal prime of $\sqrt[\tilde{\tau}]{I}$ we get $Q = M$ and (because $R[X_1, \dots, X_n] | F[X_1, \dots, X_n]$ is an integral extension) $\tilde{Q} = \tilde{M}$ – a contradiction.

As a component of $\sqrt[re]{I \cdot R}$ the ideal $\tilde{M}$ occurs in the primary decomposition of $\sqrt[re]{I \cdot R}$, e.g. $\sqrt[re]{I \cdot R} = \bigcap_i \tilde{P}_i \cap \tilde{M}$. Now choose $f \in \left(\bigcap_i \tilde{P}_i\right) \setminus \tilde{M}$. Then $\mathcal{V}_R(I) \cap \{f \neq 0\} = \{\underline{x}\}$, i.e. $\underline{x}$ is isolated in $\mathcal{V}_R(I)$ and $\mathcal{V}_R(\tilde{M}) = \{\underline{x}\} \subseteq \mathcal{V}_{\text{iso}}(I)$. Applying $\mathcal{I}_F(.)$ we finally obtain

$$I_{\text{iso}} = \mathcal{I}_F(\mathcal{V}_{\text{iso}}(I)) \subseteq \mathcal{I}_F(\underline{x}) = M. \qquad \square$$

Lemma 3.3. *Let R be a real closed field with algebraic closure $\bar{F} = R(\sqrt{-1})$, Q a prime of $\bar{F}[X_1,\dots,X_n]$ and $P := Q \cap R[X_1,\dots,X_n] \in \operatorname{Spec}(R[X_1,\dots,X_n])$. Then $P \cdot \bar{F} = Q \cap \sigma(Q)$ whereby $\sigma \in \operatorname{Aut}(\bar{F} \mid R)$ denotes the conjugation.*

The assertion is verified by a straightforward calculation.

Proposition 3.4. *Let F be a formally real field, $I \lhd F[X_1,\dots,X_n]$ and R a real closed intermediate field of $\bar{F} \mid F$. Moreover, let Q be a minimal prime of the extension ideal $I \cdot \bar{F}$ satisfying $d := \dim\, Q > 0$ and $\underline{x} \in \mathcal{V}_R(Q)$. If $\underline{x}$ is a regular point of $\mathcal{V}_{\bar{F}}(I)$ then $\underline{x}$ is not isolated in the topological space $\mathcal{V}_R(I)$.*

Proof. Without loss of generality , we may assume that $d = \dim Q \in \{1, \dots, n-1\}$.

Let $\sigma \in \operatorname{Aut}(\bar{F} \mid R)$ denote the conjugation. Then it follows from $\underline{x} \in \mathcal{V}_{\bar{F}}(Q) \cap R^n$ that $\underline{x} = \sigma(\underline{x}) \in \mathcal{V}_{\bar{F}}(\sigma(Q))$ whereby $\sigma(Q)$ is a minimal prime of $\sigma(I \cdot \bar{F}) = I \cdot \bar{F}$.

If $Q \neq \sigma(Q)$ then $\underline{x}$ would be a zero of the two distinct irreducible components $\mathcal{V}_{\bar{F}}(Q)$, $\mathcal{V}_{\bar{F}}(\sigma(Q))$ of $\mathcal{V}_{\bar{F}}(I)$ and thus a singular point of $\mathcal{V}_{\bar{F}}(I)$ contrary to the assumption. We conclude that $Q = \sigma(Q)$ and – because of Lemma 3.3 – $P := Q \cap R[X_1,\dots,X_n] \in \operatorname{Spec}(R[X_1,\dots,X_n])$ with $P \cdot \bar{F} = Q$. Note that $\dim P = \dim Q = d$ and $\underline{x} \in \mathcal{V}_R(P)$.

Now let $f_1,\dots,f_r$ be a set of generators of P. Then $Q = P \cdot \bar{F} = (f_1,\dots,f_r)\, \bar{F}[X_1,\dots,X_n]$, and because of the regularity of $\underline{x}$ in $\mathcal{V}_{\bar{F}}(I)$ the Jacobian $(\partial f_i / \partial X_j(\underline{x}))_{i=1\dots r, j=1\dots n}$ has maximal rank $n-d$ (cf. [16, Ch. VI, Proposition 1.5]). This fact implies that $\underline{x}$ is a regular point of P and thus $P = \sqrt[re]{P}$ (cf. [3, Proposition 3.3.15]).

According to [3, Proposition 3.3.7] there exist $n-d$ polynomials $g_1,\dots,g_{n-d} \in P$ as well as a neighbourhood U of $\underline{x}$ in R^n such that

$$\mathcal{V}_R(g_1,\dots,g_{n-d}) \cap U = \mathcal{V}_R(P) \cap U \quad \text{and} \quad \operatorname{Rank}\left(\frac{\partial g_i}{\partial X_j}(\underline{x})\right)_{i=1\dots n-d,\, j=1\dots n} = n-d.$$

But now the theorem of implicit functions (cf. [3, Corollary 2.9.6]) yields that $\underline{x}$ is not isolated in $\mathcal{V}_R(g_1,\dots,g_{n-d}) \cap U \subseteq \mathcal{V}_R(I)$, thus not isolated in $\mathcal{V}_R(I)$. □

Using Proposition 3.4, it can easily be verified that I_{iso} equals the unit ideal or has dimension zero.

Proposition 3.5. *Let F be a formally real field and $I \trianglelefteq F[X_1,\dots,X_n]$. Then we have $\dim I_{\text{iso}} \leq 0$, i. e. $I_{\text{iso}} = \bigcap_{i=1}^{r} M_i$ for some real maximal ideals $M_1,\dots,M_r$.*

The importance of I_{iso} in connection with the computation of $\sqrt[r]{I}$ relies on the fact that (according to Proposition 3.2) any zero-dimensional component M of $\sqrt[r]{I}$ occurs among the M_i.

For the sake of easy reference the following notations will be used: If $I \trianglelefteq F[X_1,\dots,X_n]$ then

$$\mathcal{V}_{\text{sing}}(I) := \{\underline{x} \in \mathcal{V}_{\bar{F}}(I) \mid \underline{x} \text{ a singular point of } \mathcal{V}_{\bar{F}}(I)\}$$

denotes the singular locus of $\mathcal{V}_{\bar{F}}(I)$ and

$$I_{\text{sing}} := \mathcal{I}_F\left(\mathcal{V}_{\text{sing}}(I)\right)$$

its vanishing ideal. Now let $I \lhd F[X_1,\dots,X_n]$ be a radical ideal of dimension $d \in \{0, \dots, n-1\}$ and $I^{(d)} = (f_1,\dots,f_r)$ its d-dimensional equidimensional component, i.e. the intersection of its d-dimensional minimal primes. Then the Jacobian criterion (cf. [16, Ch. VI, Proposition 1.5]) yields

$$\mathcal{V}_{\text{sing}}\left(I^{(d)}\right) = \mathcal{V}_{\bar{F}}(J(I^{(d)}, n-d)) \quad \text{and} \quad I^{(d)}_{\text{sing}} = \sqrt{J(I^{(d)}, n-d)},$$

where $J(I^{(d)}, n-d)$ denotes the ideal generated by $I^{(d)}$ and all $(n-d)\times(n-d)$-minors of the Jacobian $\left(\partial f_i/\partial X_j\right)_{i=1\dots r, j=1\dots n}$ in $F[X_1,\dots,X_n]$. Note that because of Krull's principal ideal theorem (cf. [16, Ch. V, Theorem 3.4]) $n-d \leq r$ holds.

Corollary 3.6. *Let F be a formally real field and $I \lhd F[X_1,\dots,X_n]$ a radical ideal of dimension $d \in \{1, \dots, n-1\}$. If $I = \bigcap_{e=0}^{d} I^{(e)}$ is the equidimensional decomposition of I, i.e. $I^{(e)}$ the intersection of the e-dimensional minimal primes of I, then the ideal $J := \bigcap_{e=0}^{d-1} I^{(e)} \cap I^{(d)}_{\text{sing}}$ has the following properties:*

(a) $I \subset J$ *and* $\dim J < d$,

(b) $\mathcal{V}_{\text{iso}}(I) \subseteq \mathcal{V}_{\text{iso}}(J)$,

(c) $J_{\text{iso}} \subseteq I_{\text{iso}}$.

Proof. It suffices to prove (b): Let $\underline{x} \in \mathcal{V}_{\text{iso}}(I)$, i.e. $\underline{x}$ is isolated in $\mathcal{V}_R(I)$ for some real closed intermediate field R of $\bar{F} \mid F$. Then

$$\begin{aligned}
\underline{x} &\in \bigcup_{e=0}^{d-1} \mathcal{V}_{\bar{F}}\left(I^{(e)}\right) \cup \mathcal{V}_{\text{iso}}\left(I^{(d)}\right) \\
&\overset{3.4}{\subseteq} \bigcup_{e=0}^{d-1} \mathcal{V}_{\bar{F}}\left(I^{(e)}\right) \cup \mathcal{V}_{\text{sing}}\left(I^{(d)}\right) \\
&= \mathcal{V}_{\bar{F}}\left(\bigcap_{e=0}^{d-1} I^{(e)} \cap I^{(d)}_{\text{sing}}\right) \\
&= \mathcal{V}_{\bar{F}}(J),
\end{aligned}$$

and the fact that $\underline{x}$ is isolated in $\mathcal{V}_R(I)$ implies that $\underline{x}$ is isolated in $\mathcal{V}_R(J)$, especially $\underline{x} \in \mathcal{V}_{\text{iso}}(J)$. □

Iterated application of Corollary 3.6 immediately yields:

Proposition 3.7. *Let F be an effectively given formally real field and $I \trianglelefteq F[X_1,\dots,X_n]$. Then we are able to construct an ideal $J \trianglelefteq F[X_1,\dots,X_n]$ satisfying* $\dim J \leq 0$ *and* $I \subseteq J \subseteq I_{\text{iso}}$.

The construction of J is described in more details in the proof of Lemma 5.4.

4. Computation of real radicals

Lemma 4.1. *Let R be a real closure of an ordered field (k,α) and p an irreducible polynomial of $k[Y_1,\dots,Y_m,X]$ $(m \in \mathbb{N}_0)$ such that $\deg_X p > 0$. Then the following statements are equivalent:*

(a) *$(p)k(Y_1,\dots,Y_m)[X]$ is α-real.*

(b) *$(p)k[Y_1,\dots,Y_m,X]$ is α-real.*

(c) *The ordering α can be extended to $k(p) = \mathrm{Quot}(k[Y_1,\dots,Y_m,X]/(p))$.*

(d) *p is indefinite over R, i. e. there are points $\underline{x}$, $\underline{x}' \in R^{m+1}$ satisfying $p(\underline{x})\cdot p(\underline{x}') < 0$ (in R).*

Lemma 4.1 is an immediate consequence of Proposition 2.5 and the sign change criterion [11, Ch. II, Section 12, Theorem 4].

To cope with an arbitrary polynomial $f \in k(Y_1,\dots,Y_m)[X]$ we now introduce the following computational assumptions: The preordered field (k,τ) should be effectively given and it should allow

(F) polynomial factorization of multivariate polynomials over k as well as

(R) an algorithm to test if a given irreducible polynomial $p \in k[Y_1,\dots,Y_m,X]$ is τ-real over $k(Y_1,\dots,Y_m)$, i.e. if $\sqrt[\tau]{(p)} = (p)$ in $k(Y_1,\dots,Y_m)[X]$.

Remark 4.2. (a) It is well known that the assumption (F) is equivalent to univariate factorization (cf. [22]).

(b) According to Lemma 4.1 the test demanded in (R) can be realized in many cases via quantifier elimination (see [2] for details).

Lemma 4.3. *Let (k,τ) be a preordered field meeting the computational assumptions (F) and (R) stated above. Then there is an algorithm to compute the τ-radical in $k(Y_1,\dots,Y_m)[X]$.*

Proof. Let $F := k(Y_1,\dots,Y_m)$ and $f \in F[X]$, without loss of generality, $f \notin F$. First of all, the factorization of f in $F[X]$ can be carried out using (F) (cf. [22, p. 289]). Next, let p be an irreducible factor of f in $F[X]$. Without loss of generality, we may assume $p \in k[Y_1,\dots,Y_m,X]$. In view of Lemma 4.1, the assumption (R) allows us to decide whether the τ-real part of p over F equals p or 1, i.e. whether $(p)F[X]$ is τ-real or not. Now, if $f = c \cdot \prod p_i^{n_i}$ is the prime factorization of f in $F[X]$ then

$$\sqrt[\tau]{(f)F[X]} = \left(\prod_{p_i\ \tau-\text{real}} p_i \right). \qquad \square$$

We stress the fact that the reduction method described in the following which reduces the multivariate to the univariate case does not need the requirements (F) and (R). Thus these strong additional computational conditions imposed on k are exclusively demanded for the handling of the univariate case. However, in Proposition 4.7 we will show that – at least in the case of an ordered field (k,α) – these assumptions are essentially necessary.

Lemma 4.4. *Let (k,τ) be a preordered field satisfying the computational assumptions* (F) *and* (R) *and I a zero-dimensional ideal of the polynomial ring $k(Y_1,\dots,Y_m)[X_1,\dots,X_n]$. Then it is possible to compute $\sqrt[\tau]{I}$.*

Proof. Let be $F := k(Y_1,\dots,Y_m)$. Because of $\sqrt{I}\subseteq\sqrt[\tau]{I}$ we may assume that I is already radical (for the computation of $\sqrt{I}$ see [6, 8, 12, 17, 22, Lemma 92]). Then for "almost all" vectors $c=(c_2,\dots,c_n)\in\mathbb{Q}^{n-1}$, i.e. excluding the points of a finite union of proper affine linear subspaces of $\mathbb{Q}^{n-1}$, the automorphism

$$\varphi := \varphi_c : \begin{cases} F[X_1,\dots,X_n] \longrightarrow F[X_1,\dots,X_n], \\ f(X_1,\dots,X_n) \longmapsto f\left(X_1+\sum_{i=2}^{n} c_iX_i, X_2,\dots,X_n\right) \end{cases}$$

puts $\varphi(I)$ into general position with respect to X_1 (cf. [8, 9]). Alternatively, it is well known that a suitable vector c can be computed deterministically. However, from a practical point of view the strategy of "guessing and testing" seems to be superior.

In accordance with the Shape-Lemma the reduced Gröbner basis G of $\varphi(I)$ with respect to the pure lexicographical ordering with $X_1<\dots<X_n$ has the form

$$G=\{X_j-g_j(X_1)\,(j=2\dots n),\ g_1(X_1)\}$$

with a square-free polynomial $g_1(X_1)$ (cf. [8]). If $g_1=\prod p_i$ is the prime factorization of g_1 in $F[X_1]$, then the

$$M_i := \left(X_j-g_j(X_1)\,(j=2\dots n),\ p_i(X_1)\right)$$

are the maximal ideals in the primary decomposition $\varphi(I)=\bigcap_i M_i$. We have

$$F[X_1,\dots,X_n]/M_i \simeq F[X]/(p_i(X))$$

via

$$f(X_1,\dots,X_n)+M_i \mapsto f(X, g_2(X),\dots,g_n(X))+(p_i(X)).$$

Hence M_i is a τ-real ideal of $F[X_1,\dots,X_n]$ iff $(p_i(X))$ is a τ-real ideal of $F[X]$. Therefore, we obtain

$$\sqrt[\tau]{\varphi(I)} = \bigcap_{M_i\ \tau\text{-real}} M_i = \left(X_j-g_j(X_1)\,(j=2\dots n),\ \tilde{g_1}(X_1)\right),$$

where $\tilde{g_1}(X_1)$ is the τ-real part of $g_1(X_1)$ in $F[X_1]$. Finally, we have

$$\sqrt[\tau]{I}=\varphi^{-1}\left(\sqrt[\tau]{\varphi(I)}\right). \qquad \square$$

Preparatory to Theorem 4.5 let us define $(I\cdot k(X_1,\dots,X_n))_{\text{iso}} := I\cdot k(X_1,\dots,X_n)$ for $S=\{X_1,\dots,X_n\}$, in addition to Definition 3.1 and compatible with Proposition 3.2.

Theorem 4.5. *Let (k,τ) be a preordered field and $I \trianglelefteq A := k[X_1,\dots,X_n]$. For any subset $S \subseteq \{X_1,\dots,X_n\}$ let $J^{(S)}$ denote an ideal of the quotient ring $A \cdot k(S)$ satisfying* $\dim J^{(S)} \leq 0$ *and* $I \cdot k(S) \subseteq J^{(S)} \subseteq (I \cdot k(S))_{\text{iso}}$. *Then*

$$\sqrt[\tau]{I} = \bigcap_{S \subseteq \{X_1,\dots,X_n\}} \left(\sqrt[\tau]{J^{(S)}} \cap A\right).$$

Proof. ($\subseteq$) For any subset $S \subseteq \{X_1,\dots,X_n\}$ we have

$$\sqrt[\tau]{I} \subseteq \left(\sqrt[\tau]{I} \cdot k(S)\right) \cap A = \sqrt[\tau]{I \cdot k(S)} \cap A \subseteq \sqrt[\tau]{J^{(S)}} \cap A.$$

($\supseteq$) Since $\sqrt[\tau]{I}$ is radical it is sufficient to prove that $\bigcap_S \left(\sqrt[\tau]{J^{(S)}} \cap A\right)$ is contained in any minimal prime ideal P of $\sqrt[\tau]{I}$: Let S_0 be a maximal subset of $\{X_1,\dots,X_n\}$ independent mod P (cf. [13]) and $T := k[S_0] \setminus \{0\}$. Then P_T is a zero-dimensional component of $\sqrt[\tau]{I}_T = \sqrt[\tau]{I_T}$. Thus we conclude in consideration of Proposition 3.2

$$\bigcap_S \left(\sqrt[\tau]{J^{(S)}} \cap A\right) \subseteq \sqrt[\tau]{J^{(S_0)}} \cap A \subseteq \sqrt[\tau]{(I_T)_{\text{iso}}} \cap A \subseteq \sqrt[\tau]{P_T} \cap A = \sqrt[\tau]{P}_{(T)} = P_{(T)} = P. \quad \square$$

Because of Theorem 4.5 the concept of real isolated points seems to be crucial for the theory of real radicals. The representation given above will be used in Section 5 and Section 7.

As a consequence of Theorem 4.5, Lemma 4.4 and Proposition 3.7 we obtain:

Theorem 4.6. *Let (k,τ) be a preordered field satisfying the computational assumptions* (F) *and* (R) *and I an arbitrary ideal of $k[X_1,\dots,X_n]$. Then it is possible to compute $\sqrt[\tau]{I}$.*

For the computation of the contraction ideals and ideal intersections in the formula of Theorem 4.5 see [9, Corollary 3.8].

Finally, let us return to the computational conditions imposed on (k,τ). Naturally, it has to be required that the coefficient domain k is effectively given, i.e. the arithmetic operations and the comparison between elements can be performed. This assumption is already sufficient for the computation of the ordinary radical in $k[X_1,\dots,X_n]$ if k has zero characteristic (cf. [9, 14]). For the construction of τ-radicals in $k[X_1,\dots,X_n]$ our algorithm requires in addition the validity of (F) and (R). Obviously, any algorithm computing τ-radicals in polynomial rings over k supplies an algorithm to test if a given irreducible $p \in k[Y_1,\dots,Y_m,X]$ is τ-real over $k(Y_1,\dots,Y_m)$ while it remains an open question if there is any preordered field (k,τ) allowing the construction of τ-radicals but not meeting the factorization assumption. However, as was pointed out to us by Tomas Sander the factorization assumption cannot be omitted in the case of an ordering $\tau = \alpha \in X(k)$. For an arbitrary preordering this problem is still unsolved.

Proposition 4.7. *Let (k,α) be an ordered field allowing the computation of α-radicals in $k[X_1,\dots,X_n]$ (for arbitrary n). Then k permits polynomial factorization as well.*

Proof. Let R be a real closure of (k,α) coded à la Thom (cf. [3, Proposition 2.5.4]). Since R allows polynomial factorization (cf. [3, p. 9]) it is sufficient to prove that k is a decidable subset of R, i.e. for any $x \in R$ it can be decided if $x \in k$.

Let $x \in R$ be coded by the system $f_0 = 0$, $f_1 > 0, \ldots, f_r > 0$, the $f_i \in k[X] \setminus k$. Then the roots of the ideal $I := \left(f_0,\ T_1^2 \cdot f_1 - 1, \ldots, T_r^2 \cdot f_r - 1\right) k[X, T_1, \ldots, T_r]$ over R are exactly the 2^r points

$$\left(x,\ \pm\frac{1}{\sqrt{f_1(x)}}, \ldots, \pm\frac{1}{\sqrt{f_r(x)}}\right) \in R^{r+1}$$

whose vanishing ideal $\mathscr{I}_k(\mathscr{V}_R(I)) = \sqrt[\alpha]{I}$ we are able to construct according to the assumption. Using the technique of Gröbner bases it is possible to compute a generator g of the non-trivial principal ideal $\sqrt[\alpha]{I} \cap k[X]$. Note that $0 \neq f_0 \in \sqrt[\alpha]{I} \cap k[X]$ and $1 \notin \sqrt[\alpha]{I}$ because of $\mathscr{V}_R(I) \neq \emptyset$. But then $x \in k$ iff $\deg g = 1$. □

5. Complexity

Let (k,τ) be a preordered field and $I = (f_1, \ldots, f_r) \trianglelefteq k[X_1, \ldots, X_n]$. Following our algorithm for the computation of $\sqrt[\tau]{I}$ we will show that $\sqrt[\tau]{I}$ is generated by polynomials of degree less than

$$\max\{\deg f_i \mid 1 \leq i \leq r\}^{2^{O(n^2)}}.$$

Since the computation of $\sqrt[\tau]{I}$ is performed by

- calculation of τ-real parts over rational function fields $k(X_1, \ldots, X_m)$, $0 \leq m < n$, and
- computation of ideal operations in $k(X_1, \ldots, X_m)[X_{m+1}, \ldots, X_n]$ such as intersections, contractions, etc., which again are realizable by Gröbner basis computations in polynomial rings over k

it is crucial to control the increase of polynomial degrees caused by the Buchberger-algorithm. But before we cite a result from [10, 20] resp. [4] on this topic let us define, for the sake of easy reference,

$$\operatorname{Deg} F := \begin{cases} \max\{\deg f \mid f \in F\}, & F \neq \emptyset, \\ 0, & F = \emptyset \end{cases}$$

for any finite subset $F \subset k[X_1, \ldots, X_n]$ and

$$\operatorname{Deg} I := \min\{\operatorname{Deg} F \mid F \subset k[X_1, \ldots, X_n] \text{ finite, } (F) = I\}$$

for $I \trianglelefteq k(X_1, \ldots, X_m)[X_{m+1}, \ldots, X_n]$, $0 \leq m < n$.

Note that any ideal $I \trianglelefteq k(X_1, \ldots, X_m)[X_{m+1}, \ldots, X_n]$ with $\operatorname{Deg} I \leq 1$ is trivial or a prime ideal generated by linear forms $\sum_{i=1}^n a_i X_i + c$ $(a_1, \ldots, a_n, c \in k)$.

Lemma 5.1. *Let I be an ideal of $k[X_1,\dots,X_n]$ and $\le$ an admissible ordering on the terms in $X_1,\dots,X_n$. Then there is a (not necessarily reduced) Gröbner basis G of I with respect to $\le$ such that*

$$\operatorname{Deg} G \le (\operatorname{Deg} I)^{2^{O(n)}}.$$

Proof. [10, 20] or [4]. □

Remark 5.2. It seems difficult to compute Deg I. Nevertheless, we make use of this concept in stating the result. For algorithmic purpose it may be more suitable to deal with Deg F where $I = (F)$.

In an algorithmic setting Lemma 5.1 can be formulated alternatively as follows: Given any finite set $F \subset k[X_1,\dots,X_n]$ generating I, a Gröbner basis G of I with respect to $\le$ can be constructed out of F such that $\operatorname{Deg} G \le (\operatorname{Deg} F)^{2^{O(n)}}$.

The following statements can be rephrased in the same manner. In Lemmas 5.3–5.8 and Theorem 5.9 we list bounds obtained by applying Lemma 5.1 to some fundamental algorithms described in [9, 14] or [22] (see the references given below) and then to our algorithm for the computation of τ-radicals.

Lemma 5.3. *Let k be a field of characteristic 0 and $I \lhd A := k(X_1,\dots,X_m)[X_{m+1},\dots,X_n]$, $0 \le m \le n-2$ and $d := \dim I \in \{1, \dots, n-m-1\}$. If $I^{(e)}$ denotes the intersection of the e–dimensional minimal primes of I $(e = 0\dots d)$ then:*

(a) $\operatorname{Deg} I^{(d)} \le (\operatorname{Deg} I)^{2^{O(n)}}$

(b) *There is an ideal $J \trianglelefteq A$ with $\dim J < d$ and $\sqrt{I} \subset \sqrt{J} \subseteq \bigcap_{e=0}^{d-1} I^{(e)}$ such that* $\operatorname{Deg} J \le (\operatorname{Deg} I)^{2^{O(n)}}$.

Proof. [14, Section 2] and Lemma 5.1. □

Lemma 5.4. *Let k be a formally real field and $I \trianglelefteq A := k(X_1,\dots,X_m)[X_{m+1},\dots,X_n]$, $0 \le m < n$. Then there is an ideal $J \trianglelefteq A$ with $\dim J \le 0$ and $I \subseteq J \subseteq I_{\text{iso}}$ such that*

$$\operatorname{Deg} J \le (\operatorname{Deg} I)^{2^{O(n^2)}}.$$

Proof. Without loss of generality, $\dim I \in \{1, \dots, n-m-1\}$ and $\operatorname{Deg} I \ge 2$ may be assumed. We proceed by defining inductively ideals $I_0 := I, I_1, \dots, I_l \trianglelefteq A$ satisfying $\dim I_i > \dim I_{i+1}$, $(I_i)_{\text{iso}} \supseteq (I_{i+1})_{\text{iso}}$ $(i = 0\dots l-1)$ and $\dim I_l \le 0$ where $l \le \dim I < n-m$. Defining $J := I + I_l$ we obtain an ideal as required whereby the asserted degree bound follows from $\operatorname{Deg} I_i \le (\operatorname{Deg} I)^{2^{i\cdot O(n)}}$ $(i = 0\dots l)$.

Let $0 \le i < l$ and $1 \le d_i := \dim I_i < n-m$. For $e = 0\dots d_i$ let $I_i^{(e)}$ denote the intersection of the e–dimensional minimal primes of I_i. Then I_{i+1} is constructed out of I_i by setting $I_{i+1} := J_i \cdot J(I_i^{(d_i)}, n-m-d_i)$, where

- $J_i \trianglelefteq A$ with $\dim J_i < d_i$ and $\sqrt{I_i} \subset \sqrt{J_i} \subseteq \bigcap_{e=0}^{d_i-1} I_i^{(e)}$ such that $\operatorname{Deg} J_i \le (\operatorname{Deg} I_i)^{2^{O(n)}}$ (Lemma 5.3(b)),

- $J(I_i^{(d_i)}, n-m-d_i) \trianglelefteq A$ generated by $I_i^{(d_i)}$ and all $(n-m-d_i) \times (n-m-d_i)$-minors of the Jacobian $\left(\partial f_\mu / \partial X_\nu\right)$, the $f_\mu \in k[X_1,\dots,X_n]$ generators of $I_i^{(d_i)}$ satisfying $\deg f_\mu \le \operatorname{Deg} I_i^{(d_i)} \le (\operatorname{Deg} I_i)^{2^{O(n)}}$ (Lemma 5.3(a)). □

Lemma 5.5. *Let k be a field of characteristic* 0 *and $I \lhd k(X_1,\dots,X_m)[X_{m+1},\dots,X_n]$ zero-dimensional,* $0 \le m < n$. *Then*

$$\operatorname{Deg} \sqrt{I} \le (\operatorname{Deg} I)^{2^{O(n)}}.$$

Proof. By [22, Lemma 92; 9, Proposition 3.1] and Lemma 5.1. □

Lemma 5.6. *Let (k,τ) be a preordered field and $I \lhd k(X_1,\dots,X_m)[X_{m+1},\dots,X_n]$ zero-dimensional,* $0 \le m < n$. *Then*

$$\operatorname{Deg} \sqrt[\tau]{I} \le (\operatorname{Deg} I)^{2^{O(n)}}.$$

Proof. By Lemmas 4.4 and 5.5. □

Lemma 5.7. *Let be $I \trianglelefteq k(X_1,\dots,X_m)[X_{m+1},\dots,X_n]$,* $0 \le m < n$. *Then*

$$\operatorname{Deg}(I \cap k[X_1,\dots,X_n]) \le (\operatorname{Deg} I)^{2^{O(n)}}.$$

Proof. By [9, Corollary 3.8] and Lemma 5.1. □

Lemma 5.8. *Let be $I_1,\dots,I_{2^l} \trianglelefteq k[X_1,\dots,X_n]$, $l \in \mathbb{N}$. Then*

$$\operatorname{Deg}\left(\bigcap_{i=1}^{2^l} I_i\right) \le \max\{2, \operatorname{Deg} I_1, \dots, \operatorname{Deg} I_{2^l}\}^{2^{O(ln)}}.$$

Proof. By [9, Corollary 3.2] and Lemma 5.1. □

Combining Lemmas 5.4, 5.6–5.8 with Theorem 4.5 we finally obtain:

Theorem 5.9. *Let (k,τ) be a preordered field and $I \trianglelefteq k[X_1,\dots,X_n]$. Then*

$$\operatorname{Deg} \sqrt[\tau]{I} \le (\operatorname{Deg} I)^{2^{O(n^2)}}.$$

We end with a remark on the time complexity in the sense of sequential arithmetical networks over k where the k-operations are measured with unit costs: Let (k,τ) be a preordered field such that the τ-real part of any polynomial $f \in k[X_1,\dots,X_{m+1}]$ over $k(X_1,\dots,X_m)$, $0 \le m < n$, is computable within time $(\deg f)^{2^{O(n^2)}}$, e.g. $k = \mathbb{Q}$. Then the number of k-operations necessary to construct $\sqrt[\tau]{(f_1,\dots,f_r)k[X_1,\dots,X_n]}$ out of $f_1,\dots,f_r$ can be bounded by a function of type $\max\{\deg f_i \mid 1 \le i \le r\}^{2^{O(n^2)}}$ as well.

6. Computational aspects of the Open-Mapping Theorem

This section is preparatory to Section 7 where we analyze the dependence of the α-radical $\sqrt[\alpha]{I}$ on the ordering $\alpha \in X(k)$. To begin with let us recall some basic definitions and notations.

Let k be a formally real field and $X(k)$ its space of orderings. Then the *Harrison-sets*

$$H_k(a_1,\ldots,a_r) := \{\alpha \in X(k) \mid a_1 >_\alpha 0, \ldots , a_r >_\alpha 0\} \subseteq X(k)$$

$(a_1,\ldots,a_r \in k)$ form a basis of the so-called *Harrison-topology* on $X(k)$. Note that the sets $H_k(a_1,\ldots,a_r)$ are clopen with respect to this topology.

A subset $C \subseteq X(k)$ is called *constructible* if it can be obtained from Harrison-sets $H_k(a_1,\ldots,a_r)$ by applying a finite number of boolean operations, i.e. taking finite unions, intersections and complements in $X(k)$. Via induction on these boolean expressions it can easily be demonstrated that the constructible subsets of $X(k)$ are exactly the finite unions of Harrison-sets $H_k(a_1,\ldots,a_r)$, the $a_i \in k$.

The set of all constructible subsets of $X(k)$ is denoted by $C(k)$. We point out that any $C \in C(k)$ is representable as a (formal) boolean expression involving finitely many Harrison-sets $H_1,\ldots,H_s$ whereby any $H_i = H_k(a_1,\ldots,a_r)$ can be coded by the vector $(a_1,\ldots,a_r) \in k^r$.

Finally, we define $C_k(I) := \{\alpha \in X(k) \mid I \ \alpha\text{-real}\}$ for any ideal I of some k-algebra A.

Now let $F \mid k$ be a finitely generated extension of formally real fields where $X(F)$ and $X(k)$ are endowed with the Harrison-topology. The Open-Mapping Theorem (cf. [7, Theorem 4.9]) states that the restriction $\mathrm{res}_{F|k} : X(F) \longrightarrow X(k)$, $\alpha \longmapsto \alpha \cap k$ is an open mappping. As $\mathrm{res}_{F|k}$ is a closed map (cf. [7, Theorem 4.1]) and $X(k)$ is quasi-compact (cf. [18, Theorem 4.1]) this implies that $\mathrm{res}_{F|k}\, C \in C(k)$ for any $C \in C(F)$. Following [7, pp. 16–18] a constructive proof of this fact will be outlined demonstrating that the restriction of any constructible subset $C \in C(F)$ to k can be realized algorithmically under certain computational conditions via symbolic manipulation on the boolean expressions mentioned above (see Theorem 6.5). In this sense the statement "$C \in C(k)$" also means that *a subset $C \subseteq X(k)$ can be constructed algorithmically.* We assume that k allows factorization of polynomials. The referee has pointed out that the following results could possibly be obtained under weaker assumptions.

Lemma 6.1. *Let k be a formally real field and p an irreducible polynomial of $k[X]$. Then $C_k((p)k[X]) \in C(k)$.*

Proof. For any $\alpha \in X(k)$ we have $\alpha \in C_k((p)k[X])$ iff $p(X)$ has a root in some real closure of (k,α). Thus the leading coefficients of the polynomials in the Sturm sequence of p yield a description of $C_k((p)k[X])$ as required (cf. [3, Corollary 1.2.10]). □

Lemma 6.2. *Let k be a formally real field, $\Theta \in \bar{k}$ and $a_1,\ldots,a_r \in k(\Theta)$. Then*

$$\mathrm{res}_{k(\Theta)|k}\, H_{k(\Theta)}(a_1,\ldots,a_r) \in C(k).$$

Proof. Without loss of generality, $a_1,\dots,a_r \neq 0$ may be assumed. We start by constructing a primitive element ϑ of the finite (algebraic) extension $k(\Theta,\sqrt{a_1},\dots,\sqrt{a_r})\,|\,k$ with minimal polynomial $p \in k[X]$. Then

$$\begin{aligned}\operatorname{res}_{k(\Theta)|k} H_{k(\Theta)}(a_1,\dots,a_r) &= \operatorname{im}\big(\operatorname{res}_{k(\Theta,\sqrt{a_1},\dots,\sqrt{a_r})|k}\big)\\ &= \operatorname{im}\big(\operatorname{res}_{k(\vartheta)|k}\big)\\ &= C_k((p)k[X]) \overset{6.1}{\in} C(k).\end{aligned}$$

Thereby the last equality holds because of

$$\begin{aligned}\alpha \in \operatorname{im}\big(\operatorname{res}_{k(\vartheta)|k}\big) &\iff \alpha \text{ can be extended to } k(\vartheta) \simeq_k k[X]/(p) = k(p)\\ &\iff (p)k[X] \text{ is } \alpha\text{–real}\\ &\iff \alpha \in C_k((p)k[X]). \qquad \square\end{aligned}$$

Lemma 6.3. *Let k be a formally real field and $f_1,\dots,f_r \in k[Y]\setminus\{0\}$, $f_i = g_i \cdot h_i^2$ where $g_i, h_i \in k[Y]\setminus\{0\}$ and g_i squarefree $(i = 1\dots r)$. If $\zeta_1,\dots,\zeta_s$ are the pairwise distinct roots of $g_1,\dots,g_r$ in $\bar{k}$ and*

$$V := \{0\} \cup \{\,\zeta_\mu \pm 1 \mid 1 \le \mu \le s\,\} \cup \{\,\tfrac{1}{2}(\zeta_\mu + \zeta_\nu) \mid 1 \le \mu < \nu \le s\,\} \subset \bar{k}$$

then

$$\operatorname{res}_{k(Y)|k} H_{k(Y)}(f_1(Y),\dots,f_r(Y)) = \bigcup_{\Theta\in V} \operatorname{res}_{k(\Theta)|k} H_{k(\Theta)}(g_1(\Theta),\dots,g_r(\Theta)) \in C(k).$$

Proof. The equality

$$\operatorname{res}_{k(Y)|k} H_{k(Y)}(f_1(Y),\dots,f_r(Y)) = \bigcup_{\Theta\in V} \operatorname{res}_{k(\Theta)|k} H_{k(\Theta)}(g_1(\Theta),\dots,g_r(\Theta))$$

can be verified following the second proof of [7, Theorem 4.9]. The constructibility of the right-hand side then follows from Lemma 6.2. □

Theorem 6.4. *Let $F\,|\,k$ be a finitely generated extension of formally real fields. Then $\operatorname{res}_{F|k} C \in C(k)$ for any $C \in C(F)$. In particular, $\operatorname{res}_{F|k} : X(F) \longrightarrow X(k)$ is an open mapping.*

Proof. By induction it suffices to prove the assertion for a simple extension $F = k(y)\,|\,k$: If y is algebraic over k then Lemma 6.2 can be applied, otherwise we are done by Lemma 6.3. □

In an algorithmic setting the proofs given above demonstrate the following fact.

Theorem 6.5. *Let $F = k(y_1,\dots,y_n)\,|\,k$ be a finitely generated extension of formally real fields which is given in such a way that for any y_i $(1 \le i \le n)$ which is* *algebraic over $k(y_1,\dots,y_{i-1})$ its minimal polynomial is known. If k allows polynomial factorization then the restriction of any constructible subset $C \in C(F)$ to k can be realized algorithmically.*

7. Variation of orderings

By combining Theorem 4.5 with the methods described in Section 6 we are able to examine the dependence of the α-radical $\sqrt[\alpha]{I}$ on the ordering $\alpha \in X(k)$. The central result of this section is the following one: Let I be an ideal of some affine k-algebra A and $\sim_I$ the equivalence relation on $X(k)$ defined by

$$\alpha \sim_I \beta \;:\Longleftrightarrow\; \sqrt[\alpha]{I} = \sqrt[\beta]{I}.$$

Then there are only finitely many equivalence classes with respect to $\sim_I$, and all these classes are constructible subsets of $X(k)$. Moreover, an upper bound for $|X(k)/\sim_I|$ can be obtained.

Lemma 7.1. *Let k be a formally real field and $I \trianglelefteq k(Y_1,\dots,Y_m)[X]$, $m \in \mathbb{N}_0$. Then the partition of $X(k)$ induced by $\sim_I$ consists of a finite number of constructible subsets.*

Proof. Without loss of generality, we may assume that I is a non-trivial ideal generated by a polynomial $f = c \cdot \prod_{i=1}^{r} p_i^{m_i}$ with irreducible factors $p_1,\dots,p_r$. For $i = 1\dots r$ we define

$$C_i := C_k((p_i)F[X]) = \mathrm{res}_{F|k}\, C_F((p_i)F[X]) \overset{6.1,\,6.4}{\in} C(k)$$

where $F := k(Y_1,\dots,Y_m)$. Then the sets $D_1 \cap \dots \cap D_r$ with $D_i = C_i$ or $D_i = X(k) \setminus C_i$ form a partition of $X(k)$, and on any of these sets $D_1 \cap \dots \cap D_r$ (which may be empty) the mapping $\alpha \longmapsto \sqrt[\alpha]{I}$ is constant (Lemma 4.3). □

Lemma 7.2. *Let k be a formally real field and $I \lhd k(Y_1,\dots,Y_m)[X_1,\dots,X_n]$ zero-dimensional, $m \in \mathbb{N}_0$. Then the partition of $X(k)$ induced by $\sim_I$ consists of a finite number of constructible subsets.*

Proof. Let φ be a linear F-automorphism of $F[X_1,\dots,X_n]$ putting I into general position with respect to X_1 where $F := k(Y_1,\dots,Y_m)$. If g_1 is a generator of the non-trivial principal ideal $\sqrt{\varphi I} \cap F[X_1]$ then

$$\sqrt[\alpha]{I} = \varphi^{-1}\left(\sqrt[\alpha]{(g_1)F[X_1]},\ \sqrt{\varphi I}\right)$$

for any $\alpha \in X(k)$ (Lemma 4.4). Thus, the assertion follows from Lemma 7.1. □

Theorem 7.3. *Let k be a formally real field and I an ideal of some affine k-algebra A. Then the partition of $X(k)$ induced by $\sim_I$ consists of a finite number of constructible subsets.*

Proof. Since any affine k-algebra is k-isomorphic to some quotient algebra $k[X_1,\dots,X_n]/J$ and $\sqrt[\tau]{I/J} = \sqrt[\tau]{I}/J$ for any ideal $I \trianglelefteq k[X_1,\dots,X_n]$ containing J we may restrict ourselves to the case $A = k[X_1,\dots,X_n]$. But then the assertion follows from Theorem 4.5 and Lemma 7.2. □

By combining the results of Section 5 with the proofs of 7.1–7.3 we obtain the following result.

Proposition 7.4. *Let k be a formally real field and $I \trianglelefteq k[X_1,\dots,X_n]$. Then the number $|X(k)/\sim_I|$ of equivalence classes can be bounded by a function of type*

$$2^{(\mathrm{Deg}\ I)^{2^{O(n^2)}}}.$$

Moreover, if k allows polynomial factorization then the equivalence classes with respect to $\sim_I$ can be constructed algorithmically (whereby some of the classes computed may be empty subsets of $X(k)$).

In [2, Corollary 3] we proved that for any ideal I of some noetherian k-algebra A and for any preordering τ of k there are finitely many orderings $\alpha_1,\dots,\alpha_N \supseteq \tau$ such that $\sqrt[\tau]{I} = \bigcap_{i=1}^{N} \sqrt[\alpha_i]{I}$. By using Theorem 7.3 it is evident that suitable orderings $\alpha_1,\dots,\alpha_N \in X(k)$ can be chosen from a (finite) set of representatives of $X(k)/\sim_I$:

Corollary 7.5. *Let k be a formally real field, I an ideal of some affine k-algebra A and $\{\alpha_1,\dots,\alpha_r\} \subseteq X(k)$ a system of representatives of the equivalence classes $[\alpha_1],\dots,[\alpha_r]$ given by $\sim_I$. Then for any preordering τ of k we have*

$$\sqrt[\tau]{I} = \bigcap\left\{ \sqrt[\alpha_i]{I} \mid i = 1\dots r,\ \alpha \supseteq \tau \textit{ for some } \alpha \in [\alpha_i]\right\}.$$

Remark 7.6. The referee added the interesting remark that the decision "I is α-radical" can be done without referring to polynomial factorization. Instead one can use elimination of quantifiers where no factorization requirement is needed.

Acknowledgements

Many thanks to E. Becker and T. Sander.

References

[1] M.E. Alonso, T. Mora and M. Raimondo, Local decomposition algorithms, Proc. AAECC-8, Tokyo, Japan, August 1990, Lecture Notes in Computer Science, Vol. 508 (Springer, Berlin, 1990) 208–221.

[2] E. Becker and R. Neuhaus, Computation of real radicals of polynomial ideals, Proc. MEGA-92, Nice, France, April 1992 (Birkhäuser, Basel, 1993) 1–20.

[3] J. Bochnak, M. Coste and M.-F. Roy, Géométrie algébrique réelle, in: Ergebnisse der Mathematik und ihrer Grenzgebiete, Folge 3, Vol. 12 (Springer, Berlin, 1987).

[4] T.W. Dubé, Quantitative analysis of problems in computer algebra: Gröbner bases and the nullstellensatz, (New York University, Courant Institute of Mathematical Sciences, 1989).

[5] D.W. Dubois, A nullstellensatz for ordered fields, Ark. Mat. 8 (1969) 111–114.

[6] D. Eisenbud and C. Huneke, A Jacobian method for finding the radical of an ideal, preprint, 1989.

[7] R. Elman, T.Y. Lam and A.R. Wadsworth, Orderings under field extensions, J. Reine Angewandte Math. 306 (1979) 7–27.

[8] P. Gianni and T. Mora, Algebraic solution of systems of polynomial equations using Gröbner bases, Proc. AAECC-5, June 1987, Lecture Notes in Computer Science, Vol. 356 (Springer, Berlin, 1987) 247–257.

[9] P. Gianni, B. Trager and G. Zacharias, Gröbner bases and primary decomposition of polynomial ideals, in: Computational Aspects of Commutative Algebra (Academic Press, New York, 1989) 15–33.

[10] M. Giusti, Some effectivity problems in polynomial ideal theory, Proc. Eurosam 84, Cambridge, England, July 1984, Lecture Notes in Computer Science, Vol. 174 (Springer, Berlin, 1984) 159–171.

[11] M. Knebusch and C. Scheiderer, Einführung in die reelle Algebra, Vieweg-Studium, Vol. 63 (Vieweg, Braunschweig, 1989).

[12] H. Kobayashi, S. Moritsugu and R.W. Hogan, On radical zero-dimensional ideals, J. Symbolic Comput. 8 (1989) 545–552.

[13] H. Kredel and V. Weispfenning, Computing dimension and independent sets for polynomial ideals, in: Computational Aspects of Commutative Algebra (Academic Press, New York, 1989) 97–113.

[14] T. Krick and A. Logar, An algorithm for the computation of the radical of an ideal in the ring of polynomials, Proc. AAECC-9, New Orleans, LA, October 1991, Lecture Notes in Computer Science, Vol. 539 (Springer, Berlin, 1991) 195–205.

[15] J.L. Krivine, Anneaux préordonnés, J. Anal. Math. 12 (1964) 307–326.

[16] E. Kunz, Einführung in die kommutative Algebra und algebraische Geometrie, Vieweg-Studium, Vol. 46 (Vieweg, Braunschweig, 1979).

[17] Y.N. Lakshman, On the complexity of computing a Gröbner basis for the radical of a zero dimensional ideal, Proc. 22nd ACM Symp. on Theory of Computing, May 1990.

[18] T.Y. Lam, An introduction to real algebra, Rocky Mountain J. Math. 14 (1984) 767–814.

[19] S. Lang, Algebra (Addison-Wesley, Reading, MA, 6th edn., 1974).

[20] H.M. Möller and F. Mora, Upper and lower bounds for the degree of Gröbner bases, Proc. Eurosam 84, Cambridge, England, Lecture Notes in Computer Science, Vol. 174 (Springer, Berlin, 1984) 172–183.

[21] J.-J. Risler, Une caractérisation des idéaux des variétés algébriques réelles, CRAS Paris Sér. A 271 (1970) 1171–1173.

[22] A. Seidenberg, Constructions in algebra, Trans. Amer. Math. Soc. 197 (1974) 273–313.

[23] W.V. Vasconcelos, Jacobian matrices and constructions in algebra, Proc. AAECC-9, New Orleans, LA, USA, October 1991, Lecture Notes in Computer Science, Vol. 539 (Springer, Berlin, 1991) 48–64.