Computer Science Journal of Moldova, vol.**16**, no.1(46), 2008

A zero-dimensional approach to compute real radicals

Silke J. Spang

Abstract

The notion of real radicals is a fundamental tool in Real Algebraic Geometry. It takes the role of the radical ideal in Complex Algebraic Geometry. In this article I shall describe the zero-dimensional approach and efficiency improvement I have found during the work on my diploma thesis at the University of Kaiserslautern (cf. [6]). The main focus of this article is on maximal ideals and the properties they have to fulfil to be real. New theorems and properties about maximal ideals are introduced which yield an heuristic `prepare_max` which splits the maximal ideals into three classes, namely real, not real and the class where we can't be sure whether they are real or not. For the latter we have to apply a coordinate change into general position until we are sure about realness. Finally this constructs a randomized algorithm for real radicals. The underlying theorems and algorithms are described in detail.

1 Introduction

The original task arose from an article by Becker and Neuhaus written in 1998 (see [1]), where they present an idea to compute the real radical of a polynomial ideal. The following article speeds up the computation time of the algorithm which they described there:

Becker and Neuhaus idea was a coordinate change to reduce to the univariate case. Such coordinate changes cause a coefficient growth which slows down the computation.

Our idea is to study the properties of maximal ideals M and find a heuristic to decide whether they are real, i. e. if $\sqrt[re]{M} = M$ or not. This arose from the fact that the primary decomposition in SINGULAR is well implemented and very efficient in the average case.

The article is structured in three parts:

Section 1 gives a short overview of and motivation for the notion of τ-radicals. In particular the real radical is recalled. Some theory on how the $\sqrt[re]{}$-functor behaves and first properties of K-algebras A are stated. The real radical commutes with intersection and localisation. For an arbitrary ideal $I \trianglelefteq A$, we know $\sqrt[re]{I} = \sqrt[re]{\sqrt[re]{I}}$, and $\sqrt[re]{I}$ is a radical ideal by definition. A special form of the Real Nullstellensatz over $\mathbb{Q}$ is stated. One of the fundamental statements is Theorem 1 which tells us that the real radical of I is the intersection of all real prime ideals P containing I. In fact, giving rise to all real points, the real radical of I is the intersection of all real maximal ideals M containing I. The section finishes by sketching how the one-to-one correspondences from algebraic geometry over algebraically closed fields are translated to real algebraic geometry by means of the real radical. Thus a real maximal ideal corresponds to a zero-dimensional real zero-set which can be seen as finitely many conjugate points in the field extension of $\mathbb{Q}$ to $\mathbb{R}_{alg}$ (or $\mathbb{R}$ by the Tarski Seidenberg principle).

Prime ideals correspond to irreducible $\mathbb{Q}$-varieties in $\mathbb{R}^n$ and the primary decomposition is just the decomposition of a $\mathbb{Q}$-variety $V_{re}(I) \subset \mathbb{R}^n$ into its irreducible components.

The univariate case of polynomials $f \in \mathbb{Q}(y_1, \ldots, y_m)[x]$ which is a special case of zero-dimensional ideals is explained in Section 2. The main idea is the following: Let

$$f = \varepsilon \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}.$$

If we could decide whether a prime polynomial p_i is real or not, then the real radical of the principal ideal $\langle f \rangle \trianglelefteq \mathbb{Q}(y_1, \ldots, y_m)[x]$ is

$$\sqrt[re]{\langle f \rangle} = \langle \prod_{p_i \text{ is real}} p_i \rangle.$$

This provides an idea how to compute the real radical of a univariate polynomial.

After describing the machinery for the univariate case, an algorithm for computing the zero-dimensional radical is explained in section 3. In contrast to the article of Becker and Neuhaus, the decision was to compute the primary decomposition of the zero-dimensional input and to give a heuristic for deciding whether a maximal ideal is real or not. This heuristic yields a procedure `prepare_max` which prepares a maximal ideal in such a way that we can avoid a coordinate change into general position as often as possible. If a coordinate change can't be avoided we use the procedure `GeneralPos`. Its input is a list of maximal ideals where a change can't be avoided. Here a suitably randomised coordinate change is computed such that we can check the properties of `prepare_max` for the transformed maximal ideals and afterwards we intersect all real maximal ideals of this list. The procedure `RealZero` gets a zero-dimensional input I and computes its primary decomposition. Then it considers separately every maximal ideal and tests if a change is needed to compute the real part. Afterwards it intersects the real radicals of all these 'nice' maximal ideals and restarts the procedure `GeneralPos` for the list of 'bad' ideals. To conclude the article section 3 is finished with one important Theorem of Becker and Neuhaus ([1] Theorem 4.5.) which explains the computation real radicals of general polynomial ideals via a reduction to the zero-dimensional case.

I would like to thank Dr. Anne Frühbis-Krüger and Prof. Dr. Gerhard Pfister for many fruitful discussions. I want to thank the SINGULAR team of the University in Kaiserslautern, especially Dr. Hans Schönemann, for supporting me with my SINGULAR problems while implementing the algorithms for my diploma thesis and giving good advise on the computation.

2 τ-real ideals and the real radical

This section uses some basics in real algebra which can be found in [5]. We define τ-radicals for pre-orderings σ of real fields K.

Definition 1 (τ-radicals and the real radical) *Let K be a formally real field and τ a pre-ordering of K. For any K-algebra A, we define the τ-radical of an ideal $I \trianglelefteq A$ by*

$$\sqrt[\tau]{I} = \{f \in A \ : \ f^{2r} + \sum_{i=1}^{m} a_i g_i^2 \in I \text{ with } r, m \in \mathbb{N}, g_i \in A \text{ and } a_i \in \tau \ \forall i\}.$$

An ideal I with the property $I = \sqrt[\tau]{I}$ is called τ-real.
If $\tau = \sum K^2 =: re$, then $\sqrt[re]{I}$ is called the real radical of I.

We can easily verify that $\sqrt[\tau]{I}$ is an ideal. For the special case of subfields K of $\mathbb{R}$ we get the following definition.

Definition 2 (Real radical) *Let A be an affine K-algebra, $I \trianglelefteq A$ any ideal. We define the real radical of I to be*

$$\begin{aligned}\sqrt[re]{I} := \langle f \in A : \exists r, m \in \mathbb{N} : \\ f^{2r} + \sum_{i=1}^{m} k_i g_i^2 \in I, \ k_i \in K_{\geq 0}, g_i \in A \rangle\end{aligned}$$

*I is called **real** if and only if $\sqrt[re]{I} = I$.*

To see that both definitions do not differ for $\mathbb{Q} \subseteq K \subseteq \mathbb{R}$ and the special case $\tau = re = \sum \mathbb{Q}^2$ we prove the following lemma:

Lemma 1 *Let $K = \mathbb{Q}$, then $re = \sum K^2 = K_{\geq 0}$ is an ordering of K.*

Proof 1 *$\sum \mathbb{Q}^2 \subseteq \mathbb{Q}_{\geq 0}$ is clear.*
Let $\frac{p}{q} \in \mathbb{Q}_{>0}$. Then

$$\frac{p}{q} = \frac{pq}{q^2} = \sum_{i=1}^{pq} \left(\frac{1}{q}\right)^2 \in \sum \mathbb{Q}^2.$$

Hence $\mathbb{Q}$ has a unique real closure and this closure is $\mathbb{R}_{alg} := \overline{\mathbb{Q}} \cap \mathbb{R}$, so we get the following corollary.

Corollary 1 *For every algebraic extension K of $\mathbb{Q}$ which is in $\mathbb{R}$ there exists only one possible ordering, i. e. $\sum K^2 = K_{\geq 0}$.*

2.1 Some properties of the $\sqrt[\tau]{}$-functor

For this subsection see Chapter 2 of [1].

Theorem 1 *Let (K,τ) be a pre-ordered field, I, J ideals in some K-algebra A and S a multiplicative 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) $\sqrt[\tau]{I_S} = (\sqrt[\tau]{I})_S$

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

For prime ideals and prime polynomials we get the following properties:

Lemma 2 *Let (K,τ) be a pre-ordered field and I a τ-real ideal of some K-algebra A. Then all minimal primes of I are τ-real as well.*

Corollary 2 *Let (K,τ) be a pre-ordered 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 2 *The τ-real ideal $\sqrt[\tau]{I}$ is radical and thus the intersection of its minimal primes. These are τ-real by Lemma 2.*

The most important proposition which describes the relation between τ-realness and the possibility to extend pre-orderings is stated below.

Proposition 1 *Let (K,τ) be a pre-ordered fields 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 $\alpha \in X(K)$ (which is the set of all orderings for any formally real field K.) satisfying $\alpha \supseteq \tau$ which can be extended to an ordering $\overline{\alpha}$ of the function field $k(P) := Q(A/P)$.*

(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 closed field containing the real closure of (K, τ).

Finally the real radical describes a real variety as a collection of all real points respectively. conjugated points.

Proposition 2 *Let (K, τ) be a pre-ordered field and I an ideal of some affine K-algebra A. Then $\sqrt[r]{I} = \bigcap M$, where M ranges over all τ-real maximal ideals of A containing I.*

2.1.1 The behaviour of prime polynomials

The well-known **sign change criterion** of D. Dubois and G. Elfroymson (see [5] Chapter 2 12 Theorem 4) is:

Theorem 2 *Let (K, τ) be an ordered field with its unique real closure R and $f \in K[x_1, \ldots, x_n]$ be an irreducible polynomial. Then the following are equivalent:*

(a) The ordering τ can be extended to an ordering $\overline{\alpha}$ over the function field $k(f) = Q(K[x_1, \ldots, x_n]/\langle f \rangle)$.

(b) f is indefinite over R, i. e. there exists $a, b \in R^n$ such that $f(a) \cdot f(b) < 0$.

This leads us directly to the following remark about the situation over the special case that $K = \mathbb{Q}$.

Remark 1 *Let $f \in \mathbb{Q}[x_1, \ldots, x_n]$ be an irreducible polynomial. Then f is real (i. e. $\langle f \rangle$ is real) if and only if f is indefinite over $\mathbb{R}_{alg}$ and thus by the Tarski-Seidenberg principle indefinite over $\mathbb{R}$.*

Proof 3 *f is real if and only if the ordering $re = \mathbb{Q}_{\geq}$ can be extended in $Q(\mathbb{Q}[x_1, \ldots, x_n]/\langle f \rangle)$ by Proposition 1. By the sign change criterion this can be extended if and only if f is indefinite over $\mathbb{R}_{alg}$.*

As another remark for polynomials over $\mathbb{Q}(y_1, \ldots, y_m)$ we get:

Remark 2 *Let $f \in \mathbb{Q}(y_1, \ldots, y_m)[x_1, \ldots, x_n]$ be an irreducible polynomial. Then f is real if and only if there exists an ordering α of $\mathbb{Q}(y_1, \ldots, y_m)$ such that f is indefinite over the corresponding real closure R_α.*

Proof 4 *Let $F := \mathbb{Q}(y_1, \ldots, y_m)$.*
Let us first observe that since f is irreducible the ideal $\langle f \rangle$ is a prime ideal. Let now $\alpha \in X(F)$ be an ordering such that f is indefinite over R_α. This ordering α of F can be extended to an ordering $\overline{\alpha}$ in $k(f) = F[x_1, \ldots, x_n]/\langle f \rangle$. By Proposition 1 (b) this is equivalent to the statements that $\langle f \rangle$ is real. Thus f is real.

2.2 The Real Nullstellensatz

We now state the Real Nullstellensatz which was proved by Krivine in the 60s. We first recall the set of real points. For more detailed information see [5] or ([1] Definition 2.7 and Theorem 2.8)

Definition 3 *Let (K, τ) be a pre-ordered field and $I \trianglelefteq K[x_1, \ldots, x_n]$. For a ordering $\alpha \supseteq \tau$ let R_α denote the unique real closure of (K, α). Then we define the set of all τ-real points V_τ as follows:*

$$V_\tau(I) = \cup_{\alpha \supseteq \tau} V_{R_\alpha}(I).$$

Especially the set of all real points is denoted by $V_{re}(I)$.

We get the general Real Nullstellensatz:

Theorem 3 (The general Real Nullstellensatz) *Let (K, τ) be a pre-ordered field and $I \trianglelefteq K[x_1, \ldots, x_n]$ be an ideal. Then we have*

$$I_K(V_\tau(I)) = \sqrt[\tau]{I}.$$

The following lemma is useful for the computation in real closed fields. Note that it is a kind of specialisation of the Weak Nullstellensatz over algebraically closed fields.

Lemma 3 *Let R be any real closed field and $M \lhd \cdot R[x_1, \ldots, x_n]$ be a maximal ideal. Then we have the following 2 cases.*

i. M is not real, so $V_R(M) = \varnothing$.

ii. M is real and $V_R(M)$ consists of only one point.

Proof 5 *As M is a maximal ideal $R' := R[x_1, \ldots, x_n]/M$ is a field extension of R. As R is real closed, we know that $\overline{R} = R(i)$ and $[\overline{R} : R] = 2$. So we have the following 2 cases.*

$[R' : R] = 1$ *Then $R' = R$ and every zero of M is real thus M is real. Let $a = (a_1, a_2, \ldots, a_n) \in R^n$ so $a \in V_R(M)$. Now $I_R(a) = \langle x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n \rangle$ is a maximal ideal which contains M as $\langle x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n \rangle = I_R(a) \subset I_R(V_R(M)) = M$. Thus $M = \langle x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n \rangle$. And hence $V_R(M) = \{a\}$ is exactly one point.*

$[R' : R] = 2$ *Then $R' = \overline{R}$ and $\overline{R}$ is not real, thus M is not real by Proposition 1. Hence by the Real Nullstellensatz (Theorem 3) $V_R(M) = \varnothing$.*

2.3 One-to-one correspondences in real algebraic geometry

Let K be any subfield of $\mathbb{R}$ and $A = K[x_1, \ldots, x_n]$. Here the following special form of Theorem 3 holds:

Theorem 4 (Special Real Nullstellensatz) *Let $J \trianglelefteq K[x_1, \ldots, x_n]$, then:*

$$I_K(V_{\mathbb{R}}(J)) = \sqrt[re]{J}$$

This yields the well-known one-to-one correspondences.

$$\begin{aligned}
\text{real ideals} &\overset{1:1}{\longleftrightarrow} K\text{-varieties in } \mathbb{R}^n \\
\text{real prime ideals} &\overset{1:1}{\longleftrightarrow} \text{irreducible } K\text{-varieties in } \mathbb{R}^n \\
\text{real maximal ideals} &\overset{1:1}{\longleftrightarrow} \text{irreducible 0-dim. } K\text{-varieties in } \mathbb{R}^n
\end{aligned}$$

So every correspondence over $\mathbb{C}$ occurs in a natural way by means of real radicals in real algebraic geometry.

3 The univariate case

To obtain an algorithm for the zero-dimensional case, we first consider the univariate case, i. e. ideals in the principal ideal domain $F[x]$ where $F = \mathbb{Q}(y_1, \ldots, y_m)$. The main idea for the univariate case is the following: If we compute the real radical of $\langle f \rangle \trianglelefteq K[x]$, we know that factorising f corresponds to a primary decomposition. So if

$$f = \varepsilon p_1^{m_1} \cdot p_2^{m_2} \cdots p_r^{m_r}$$

then the $\langle p_i \rangle$, for all $i = 1, \ldots, r$ are precisely the minimal primes of $\langle f \rangle$. Such a minimal prime is real if and only if $V_{\mathbb{R}}(p_i) \neq \varnothing$, i. e. if p has a real root. So $\langle p_i \rangle$ is real if and only if p_i is real.

Hence the real radical of $\langle f \rangle$ is:

$$\sqrt[re]{\langle f \rangle} = \langle \prod_{p_i \text{ real}} p_i \rangle.$$

This leads us directly to the demand of a criterion to know whether an irreducible polynomial p is real or not.

Here we have two cases:

In the easier first case $F = \mathbb{Q}$ i.e. $m = 0$; the general case $m > 0$ requires more knowledge of real algebra.

3.1 The special univariate case

Definition 4 *Let $p \in \mathbb{Q}[x]$ be an irreducible polynomial. We call p* ***real*** *if p has a real root $\alpha \in \mathbb{R}$. Then p is the minimal polynomial of this root α.*

Note that p is real if and only if $V_{\mathbb{R}}(p) \neq \varnothing$, that is p is real if and only if $\langle p \rangle$ is real, since $\langle p \rangle$ is a maximal ideal and $\sqrt[re]{\langle p \rangle} \supseteq \langle p \rangle$. Hence the decision of being real for prime polynomials reduces to a root counting problem.

The solution to this problem is the following:
If the degree of p is odd the fundamental theorem of algebra over $\mathbb{R}$ states that p has a real root. But if the degree of p is even, we can't be sure if p has a real root. In this case we use the theorem of Sturm, which counts the number of all distinct real roots of a non–constant polynomial $f \in K[x]$ in an interval $[a, b]$, where $a < b$. The best a and b can be found by computing the Cauchy bound for polynomials. For detailed description of Sturm's theorem and its applications see [2].

3.2 The general univariate case

Contrary to the special case $F = \mathbb{Q}$ the general case of polynomials in $\mathbb{Q}(y_1, \ldots, y_m)[x]$ is not a real root counting problem as we do not know about sign or when a root is real. Thus we need some tools of real algebra.

The following special form of Lemma 4.1 in [1] gives a solution to the decision problem of realness for prime polynomials:

Lemma 4 *Let $p \in \mathbb{Q}[y_1, \ldots, y_m, x]$, where $m \in \mathbb{N}_0$ and $\deg_x p > 0$ be an irreducible polynomial. Then the following conditions are equivalent:*

(a) $\langle p \rangle \cdot \mathbb{Q}(y_1, \ldots, y_m)[x]$ *is real.*

(b) $\langle p \rangle \cdot \mathbb{Q}[y_1, \ldots, y_m, x]$ *is real.*

(c) p is indefinite over $\mathbb{R}$, i. e. there are points $\underline{a}, \underline{b} \in \mathbb{R}^{m+1}$ satisfying $p(\underline{a}) \cdot p(\underline{b}) < 0$.

This reduces our problem to decision whether a polynomial has a sign change i. e. whether it is indefinite or not. For a detailed solution of this problem see the article of G. Zeng and X. Zeng [4].

3.3 Example for the procedure `RealPoly`

The algorithm `RealPoly` (cf. SINGULAR Release 3-0-3) computes the real part of a polynomial in the univariate case. We conclude this section with some examples.

Example 1 *1. Let* $f = x^9+x^7+2x^6+x^5+2x^4-7x^3+4x^2-8x+4 \in \mathbb{Q}[x]$. *Factorising yields* $f = (x-1)\cdot(x^3+x^2+x-1)\cdot(x3+4)\cdot(x^2+1) = p_1\cdot p_2\cdot p_3\cdot p_4$. *The prime factors* p_1, p_2, p_3 *are real as they have real roots by the fundamental theorem of algebra, but* p_4 *has no real root. Hence* p_4 *is not real. So the real part of* f *is:* $\overline{f} = p_1\cdot p_2\cdot p_3 = x7+2x4+x3-8x+4$.

Let

$$\begin{aligned} f =& x^8y^2z^4 - 2x^7y^3z^2 + x6y^4z^4 + x^6y^4 + x^6y^2z^4 + 2x^6yz^5 - 2x^5y^5z^2 - \\ & 2x^5y^3z^2 - 4x^5y^2z^3 + x^4y^6 + x^4y^4 + 2x^4y^3z^5 + 2x^4y^3z + 2x^4yz^5 + \\ & x4z^6 - 4x^3y^4z^3 - 4x^3y^2z^3 - 2x^3yz^4 + 2x^2y^5z + 2x^2y^3z + x^2y^2z^6 + \\ & x^2y^2z^2 + x^2z^6 - 2xy^3z^4 - 2xyz^4 + y^4z^2 + y^2z^2 \in \mathbb{Q}(y,z)[x]. \end{aligned}$$

Factorising yields that

$$f = (x^2y+z)^2\cdot(xz^2-y)^2\cdot(x^2+y^2+1) = p_1^2\cdot p_2^2\cdot p_3.$$

As p_1 *and* p_2 *have odd degree in* z *(resp. in* y*) they are indefinite and thus real.* x^2+y^2+1 *is positive semi-definite. The real polynomial computed from* f *is* $g = p_1\cdot p_2 = x^3yz^2 - x^2y^2 + xz^3 - yz$.

4 The zero-dimensional radical computation

To explain the main idea used in the algorithm for the zero-dimensional real radical via reduction to the univariate case consider the following example. Let $F := \mathbb{Q}(y_1,\ldots,y_m)$ as in the last section.

Example 2 *Let* $I = \langle x_1 - g_1(x_n), x_2 - g_2(x_n), \ldots, x_{n-1} - g_{n-1}(x_n), g_n(x_n)\rangle \trianglelefteq F[x_1, \ldots, x_n]$ *be given. If* $\overline{g_n}$ *is the real part of* g_n *obtained by the procedure* `RealPoly` *the real radical of* I *is:*

$$\sqrt[re]{I} = \langle x_1 - g_1(x_n), x_2 - g_2(x_n), \ldots, x_{n-1} - g_{n-1}(x_n), \overline{g_n}(x_n)\rangle$$

Proof 6 *Let* $g_n = \prod_{i=1}^{r} p_i^{\alpha_i}$ *be the factorisation of* g_n *in* $F[x_n]$*. Then every ideal* $\langle x_1 - g_1, x_2 - g_2, \ldots, x_{n-1} - g_{n-1}, p_i\rangle$ *is maximal because of the isomorphism*

$$F[x_1, \ldots, x_n]/\langle x_1 - g_1, x_2 - g_2, \ldots, x_{n-1} - g_{n-1}, p_i\rangle \cong F[x_n]/\langle p_i\rangle.$$

As p_i *is prime we conclude that* $F[x_1, \ldots, x_n]/\langle x_1 - g_1, x_2 - g_2, \ldots, x_{n-1} - g_{n-1}, p_i\rangle$ *is a field.*
Now $\langle x_1 - g_1, x_2 - g_2, \ldots, x_{n-1} - g_{n-1}, p_i\rangle$ *is real if and only if* p_i *is real because* $F[x_n]/\langle p_i\rangle$ *is real if and only if* p_i *is real by Propostion 1. Hence*

$$\begin{aligned}
\sqrt[re]{I} &\overset{Cor.2}{=} \bigcap_{M \in \mathrm{Min}(I)\ \text{real}} M \\
&= \bigcap_{p_i \text{ is real}} \langle x_1 - g_1, x_2 - g_2, \ldots, x_{n-1} - g_{n-1}, p_i\rangle \\
&= \langle x_1 - g_1, x_2 - g_2, \ldots, x_{n-1} - g_{n-1}, \prod_{p_i \text{ is real}} p_i\rangle \\
&= \langle x_1 - g_1(x_n), x_2 - g_2(x_n), \ldots, x_{n-1} - g_{n-1}(x_n), \overline{g_n}(x_n)\rangle
\end{aligned}$$

The most important theorem for the zero-dimensional computation in the article of Becker and Neuhaus is the Shape lemma which gives a detailed information on the shape of the reduced Gröbner basis of a radical ideal satisfying the property of being in general position in some way, so that we can obtain the position of an ideal given in the example above.

Lemma 5 (Shape-Lemma) *Let* I *be a zero-dimensional radical ideal in* $F[x_1, \ldots, x_n]$ *with all* d *roots in* $\overline{F}^n$ *having distinct* x_n *coordinates.*

Then the reduced Gröbner basis of I in the lexicographical ordering has the shape

$$G = \{x_1 - g_1(x_n), x_2 - g_2(x_n), \ldots, x_{n-1} - g_{n-1}(x_{n-1}), g_n(x_n)\},$$

where g_n is a square-free polynomial of degree d and the g_i, $i < n$, are polynomials of degree $d - 1$.

Proof 7 *See Lemma 4.5 of [6].*

A naive idea for an algorithm could be:

1. Compute the radical $\sqrt{I}$ of the given ideal I.
2. Test if $\sqrt{I}$ fulfils the shape condition with respect to one variable x_i and compute a reduced Gröbner basis of $\sqrt[re]{I}$ w. r. t. a lexicographical ordering with lowest variable x_i. If not use a random change into general position until this condition is fulfilled.
3. Compute the real radical of $\sqrt{I}$ as described in Example 2 and undo the coordinate change.

As a coordinate change into general position causes a growth of coefficients and terms which slows down the Gröbner bases computations it is important to avoid this change as often as possible. Therefore we give some heuristics, i. e. some kinds of special cases in which we do not have to apply a random coordinate change.

The idea for the algorithm due to Becker and Neuhaus ([1]) has been presented in Example 2 and Lemma 5. In the rest of this section I will present my own algorithm:

As in SINGULAR the primary decomposition of zero-dimensional ideal, in the average case, is very efficient, we can use this algorithm as a black box. The main idea of the primary decomposition due to Gianni/Trager/Zacharias (the command is `primdecGTZ`) was presented in [3] chapter 4.2. Hence we can assume the maximality of all ideals we are dealing with. The next subsection presents some properties for maximal ideals I found.

4.1 How to decide whether a maximal ideal is real

For a maximal ideal there are only two possibilities – either it is real or its real radical is the whole ring. This is the reason why getting criteria for maximal ideals is not difficult. The main idea of this section is to find an heuristic which fulfils the following criteria:

1. Its costs have to be lower in the average case than the costs that a random coordinate change would cost.

2. The decision of realness must be an easy test, i. e. it shouldn't cost too many operations.

3. Our heuristic must cancel out maximal ideals M which are not real as early as possible in the computations.

Here are some properties of maximal ideals that I found during the work on my diploma thesis ([6]). For the definition of orderings and real closed fields I refer to [5].

One obvious property of real maximal ideals is the following corollary.

Corollary 3 *Let $M \lhd \cdot F[x_1, \ldots, x_n]$ be maximal and $f_1, \ldots, f_n$ be the univariate polynomials such that $\langle f_i \rangle = M \cap F[x_i]$. If M is real then every f_i is real too.*

Another simple remark is:

Remark 3 *If $M = \langle f_1, \ldots f_n \rangle \lhd \cdot \mathbb{Q}[x_1, \ldots, x_n]$ is a maximal ideal with every $f_i \in \mathbb{Q}[x_i]$ real, then M is real.*

Proof 8 *This is clear as every f_i has a zero a_i in the common real closed field $\mathbb{R}$. Thus $(a_1, \ldots, a_n) \in \mathbb{R}^n$ is in the real zeros of M.*

Note that this simple remark for the rational numbers is not true for an arbitrary real field F. This remains only true if F is an ordered field. The problem for arbitrary real fields is the following:
A polynomial $f_i \in F[x_i]$ is real if and only if there exist orderings

$\alpha_1, \ldots, \alpha_r$ and the corresponding real closures $R_{\alpha_1}, \ldots, R_{\alpha_r}$ such that f_i has zeros in every R_{α_i}.

But these orderings α_i could occur in a way that there exists no common real closed ground field R_α and no corresponding ordering α of F such that the polynomials f_i all have a root in R_α, which would yield that M is real. The following counter-example for arbitrary real fields clarifies the problem:

Example 3 *Let $M = \langle x^2 + 1 + t, y^2 - t\rangle \lhd \cdot\mathbb{Q}(t)[x, y]$. Then $m_1 = x^2+1+t$ is real in every real closed extension R_α of $\mathbb{Q}(t)$ which admits an ordering α in which $t < -1$ (note that we conclude that m_1 is real as it is indefinite over $\mathbb{R}$), $m_2 = y^2 - t$ is real in every real closed extension R_β which admits an ordering β satisfying $t > 0$. Both types of orderings, the α– and β-orderings, contradict each other.*
In fact M is not real as

$$1^2 + x^2 + y^2 = m_1 + m_2 \in M$$

and hence $1 \in \sqrt[re]{M}$.

Analogous to the Shape Lemma, there holds a stronger property for maximal ideals that can be tested very easily:

Proposition 3 *Let $M \lhd \cdot F[x_1, \ldots, x_n]$ be a maximal ideal and $G = \{g_1, \ldots, g_n\}$ the reduced Gröbner basis of M with respect to any lexicographical ordering with smallest variable x_i. If G has the following properties:*

- *$g_1 \in F[x_i]$ and g_1 is real.*[1]
- *every g_i for $i = 2, \ldots, n$ has odd degree in its leading variable*[2]*.*

[1] G is a triangular set as it is a reduced lexicographical Gröbner basis, wlog we can assume that the univariate polynomial in smallest variable in G is g_1.

[2] Let $f \in \mathbb{Q}[x_1, \ldots, x_n]$. The leading variable of f (short $lvar(f)$) is the largest variable in f, i. e. if

$$f = a_s(x_1, \ldots, x_{k-1})x_k^s + a_{s-1}(x_1, \ldots, x_{k-1})x_k^{s-1} + \ldots + a_0(x_1, \ldots, x_{k-1}),$$

$a_s \in \mathbb{Q}[x_1, \ldots, x_{k-1}] \setminus \{0\}$, for a $k \leq n$, then $lvar(f) = x_k$ and the pseudo leading coefficient of f is $ini(f) = a_s(x_1, \ldots, x_{k-1})$.

Then the maximal ideal M is real.

Proof 9 *Assume for simplicity that $G = \{g_1, \ldots, g_n\}$ is a Gröbner basis satisfying the properties above w. r. t. the ordering $x_1 < x_2 < \ldots < x_n$.*
As $g_1 \in F[x_1]$ is real there exists a real closed field $R \supset F$ such that g_1 has a zero $\alpha_1 \in R$. Now $g_2(x_2, \alpha_1) \in R[x_2]$ has odd degree and thus has a zero α_2 in R by the fundamental theorem of algebra. By the same reason $g_3(x_3, \alpha_2, \alpha_1) \in R[x_3]$ has a zero $\alpha_3 \in R$. Inductively there exists an $\alpha \in V_{R^n}(M)$.
Thus $V_R(M) \neq \varnothing$ and hence, by the definition of the real zero-set of M, $V_{re}(M) \neq \varnothing$. Now by the Real Nullstellensatz $\sqrt[re]{M} = I_F(V_R(M)) = I_F(\alpha) \subset M$. As M is maximal and $V_{re}(M) \neq \varnothing$ we conclude the realness of M.

A last non-trivial condition to test the realness of M is:

Lemma 6 *Let $M = \langle m_1, \ldots, m_n \rangle$ be a maximal ideal in $F[x_1, \ldots, x_n]$ written as a reduced lexicographical Gröbner basis w.r.t to the ordering $x_1 < x_2 < \ldots < x_n$. If M is real, every generator m_i is real.*

Proof 10 *Assume contrary: Thus let i be the smallest index such that m_i is not real. As M is a lexicographical Gröbner basis we get the following cases:*

Case 1: $i = 1$ then $m_1 \in F[x_1]$ and has no real root. So

$$\langle 1 \rangle = \sqrt[re]{m_1} \subset \sqrt[re]{\langle m_1, \ldots, m_n \rangle} = \sqrt[re]{M}.$$

Thus M is not real which is a contradiction.

Case 2: $i > 1$. Let R be an arbitrary real closure of (F, α) w. r. t. an ordering α of F such that $a = (a_1, \ldots, a_n) \in R^n$ is a real point of M (i. e. $a \in V_{re}(M)$). Then we have the following situation:

- *$M' := \langle m_1, \ldots, m_i \rangle = M \cap F[x_1, \ldots, x_i] \lhd \cdot F[x_1, \ldots x_i]$ is real since $(a_1, \ldots, a_i) \in V_R(M') \subset V_{re}(M')$.*

- $M'' := \langle m_1, \ldots, m_{i-1} \rangle = M \cap F[x_1, \ldots, x_{i-1}] \lhd \cdot F[x_1, \ldots x_{i-1}]$ *is real since* $(a_1, \ldots, a_{i-1}) \in V_R(M'') \subset V_{re}(M'')$.

As M' is real, the ordering α of F can be extended in $k(M) = F[x_1, \ldots, x_n]/M$, i. e. $k(M)$ is a formally real field (see Proposition 1). From the first isomorphism theorem, we get:

$$\begin{aligned} F[x_1, \ldots, x_i]/M' \cong & (F[x_1, \ldots, x_{i-1}, x_i]/M'')/(M'/M'') \\ = & ((F[x_1, \ldots, x_{i-1}]/M'')[x_i])/((\langle m_i \rangle + M'')/M''). \end{aligned}$$

Now as $(a_1, \ldots, a_{i-1})$ is a (real) root of the maximal M'' we get that

$$F[x_1, \ldots, x_{i-1}]/M'' \cong F(a_1, \ldots, a_{i-1})$$

which is ordered by $F(a_1, \ldots, a_{i-1}) \cap R^2$. Hence

$$k(M) \cong F(a_1, \ldots, a_{i-1})[x_i]/\langle m_i(a_1, \ldots, a_{i-1}, x_i) \rangle$$

and $k(M)$ is real. Thus the ordering $F(a_1, \ldots, a_{i-1}) \cap R^2$ can be extended to $F(a_1, \ldots, a_{i-1}, a_i) \cap R^2$ (as a_i is a real root of $m_i(a_1, \ldots, a_{i-1}, x_i)$ by the definition of a). But then $m_i(a_1, \ldots, a_{i-1}, x_i)$ is indefinite over R by the sign change criterion (Theorem 2) and thus $m_i(x_1, \ldots, x_i)$ is indefinite over R, too. Now we get from Remark 2 that m_i is real which contradicts the assumption.

Lemma 6 is no equivalence as we can see in the following example:

Example 4 *Let $M = \langle x^3 - 2, y^2 + x^2 - x \rangle \lhd \cdot \mathbb{Q}[x, y]$. Now $x^3 - 2$ is real since $\sqrt[3]{2}$ is in $\mathbb{R}$ and $y^2 + x^2 - x$ is real by Lemma 4 as it is indefinite. But M is not real as $y^2 + \sqrt[3]{2}^2 - \sqrt[3]{2}$ has no real root since $\sqrt[3]{2}^2 - \sqrt[3]{2} > 0$.*

The following corollary is useful to test the realness of prime polynomials $f \in F[x_1, \ldots, x_n]$.

Corollary 4 *Let $f \in \mathbb{Q}[y_1, \ldots, y_m, x_1, \ldots, x_n]$ be an irreducible polynomial. Then f is real considered as polynomial in $F[x_1, \ldots, x_n]$ if and only if f considered as a polynomial in $\mathbb{Q}[y_1, \ldots, y_m, x_1, \ldots, x_n]$ is real.*

Proof 11 $\Rightarrow$**:** *As* $\langle f\rangle F[x_1,\ldots,x_n]$ *is real in* $F[x_1,\ldots,x_n]$*, there exists an* x_i *such that* $\deg_{x_i} f > 0$*. Without loss of generality let* x_n *be this* x_i*. By Theorem 1 we conclude that* $\langle f\rangle F(x_1,\ldots,x_{n-1})[x_n] = \langle f\rangle \mathbb{Q}(y_1,\ldots,y_m,x_1,\ldots,x_{n-1})[x_n]$ *is real. Thus by Lemma 4* $\langle f\rangle \mathbb{Q}\ [y_1,\ldots,y_m,x_1,\ldots,x_n]$ *is real and hence* f *is real considered over* $\mathbb{Q}[x_1,\ldots,x_n,y_1,\ldots,y_m]$*.*

$\Leftarrow$**:** *This is clear as reality commutes with localisation (see Lemma 1).*

Combining all these conditions yields a good heuristic to decide the property of being real for maximal ideals M. Let us first consider a large example in which it was possible to avoid the change into general position completely.

Example 5 *Let*

$$I = \langle (y^3+3y^2+y+1)(y^2+4y+4)(x^2+1),\\ (x^2+y)(x^2-y^2)(x^2+2xy+y2)(y^2+y+1)\rangle \trianglelefteq \mathbb{Q}[x,y]$$

The primary decomposition of I *yields 10 maximal ideals.*

1. $M_1 = \langle y^2+1, x-y\rangle$ *which is not real as* y^2+1 *is not real. Hence it does not satisfy the conditions in Proposition 3 and Corollary 3.*

2. $M_2 = \langle y-1, x^2+1\rangle$ *does not satisfy the Corollary 3 and is thus not real.*

3. $M_3 = \langle y^2+y+1, x^2+1\rangle$ *does not satisfy Corollary 3 and is thus not real.*

4. $M_4 = \langle y^2+1, x+y\rangle$ *does not satisfy Corollary 3 and is thus not real.*

5. $M_5 = \langle y+2, x-2\rangle$ *is real by Proposition 3 or Remark 3.*

6. $M_6 = \langle y+2, x^2-2\rangle$ *is real by Proposition 3 for the ordering* $x < y$ *with the reduced Gröbner basis* $G = \{x^2-2, y+2\}$*.*

7. *$M_7 = \langle y+2, x+2\rangle$ is real by Proposition 3 or Remark 3.*

8. *$M_8 = \langle y^3+3y^2+y+1, x+y\rangle$ is real by Proposition 3 w. r. t. the ordering $y < x$ under which M is a reduced Gröbner bases.*

9. *$M_9 = \langle y^3+3y^2+y+1, x^2+y\rangle$. Here it is not obvious to see if M_9 is real or not. So we have to compute the Gröbner bases w. r. t. both orderings $x < y$ and $y < x$.*
   The Gröbner basis w. r. t. to the lexicographical ordering $x < y$ of M_9 is
   $$G_M = \langle x^6 - 3x^4 + x^2 - 1, y + x^2\rangle.$$
   First we have to test if $x^6 - 3x^4 + x^2 - 1$ is real. We know that $x^6 - 3x^4 + x^2 - 1$ is prime and after applying the `RealPoly` procedure introduced in the last section we get that $x^6-3x^4+x^2-1$ is real. Now we know that M_9 is real by Proposition 3 w. r. t. to the ordering $x < y$.

10. *$M_{10} = \langle y^3+3y^2+y+1, x-y\rangle$ is real by Proposition 3.*

So the real radical of I is

$$\begin{aligned}\sqrt[re]{I} &= M_5 \cap M_6 \cap M_7 \cap M_8 \cap M_9 \cap M_{10} \\ &= \langle y^4+5y^3+7y^2+3y+2, x^4 - x^2y^2 + x^2y - y^3\rangle\end{aligned}$$

In the next subsection I describe a procedure using the criteria introduced above.

After giving this procedure it is easy to describe the algorithm for the zero-dimensional case using a coordinate change into general position.

4.1.1 The procedure `prepare_max`

The procedure `prepare_max` which uses the properties introduced above acts in the following way:

It gets as input a maximal ideal M and returns a list $erg = \overline{M}, j$, where

$$\overline{M} = \begin{cases} \sqrt[re]{M} & \text{if } j = 1, \text{ the change into general position can be avoided} \\ M & \text{if } j = 0, \text{ the change into general position cannot be avoided} \end{cases}$$

I explain my algorithm in pseudo-code. The proof of the correctness of this algorithm follows from the criteria explained above. In the algorithm itself there is no need to check Corollary 3 explicitly. This criterion is checked implicitly in the check of Proposition 3 as we will see.

The procedure `prepare_max` is written as follows:

Algorithm 1
(An heuristic to check if a coordinate change can be avoided)

proc *prepare_max(M)*

INPUT : *a maximal ideal* $M \lhd \cdot F[x_1, \ldots, x_n]$

OUTPUT: *a list* $erg = (\overline{M}, j)$ *s.t.:*

$$\overline{M} = \begin{cases} \sqrt[re]{M} & \text{if } j = 1, \text{ the change into general position can be avoided} \\ M & \text{if } j = 0, \text{ the change into general position can't be avoided} \end{cases}$$

BEGIN

Initialise $P := \{\lambda : \lambda \text{ is a permutation of the variables } \{x_1, \ldots, x_n\}\}$

while $(P \neq \varnothing)$ *do* {

Choose a $\lambda = (x_{j_1}, x_{j_2}, \ldots, x_{j_n}) \in P$

$P := P \setminus \{\lambda\}$

Compute the lexicographical Gröbner basis $M_\lambda = \{f_1, f_2, \ldots, f_n\}$ *of* M *w. r. t. the ordering* $x_{j_1} < x_{j_2} < \ldots < x_{j_n}$. *Now* f_1 *is univariate in the variable* x_{j_1}.

Let $\overline{f_1} :=$ `RealPoly`(f_1) *the real part of* f_1. *As* f_i *is prime there are two possibilities* $\overline{f_1} = 1$ *or* $\overline{f_1} = f_1$.

if $(\overline{f_1} = 1)$

{

$erg := \langle 1 \rangle, 1$

$return(erg)$;

}

According to Proposition 3 search the first position $k \geq 2$ *such that* m_k *has even degree in* x_{j_k}. *Set* $k = n+1$ *if there exists none.*

if $(k > n)$

{

$erg := M, 1$; *(Correctness is clear from Prop. 3)*

$return(erg)$;

}

According to Lemma 6 search from position $(k+1)$ *in* M_λ, *the first non-real generator* m_i.

If there exists a position $i \leq n$ *set* $erg = \langle 1 \rangle, 1$ *and return erg.*

}

If F *is non parametric, i. e.* $F = \mathbb{Q}$ *and every generator of* M *is univariate use Remark 3 and return* $erg := M, 1$.

$erg := M, 0$;

$return(erg)$;

END

In many cases the realness of maximal ideals can be checked only using the procedure `prepare_max`. But it may happen that an ideal fails this test, i. e. the result of $prepare\_max(M)$ is $erg = M, 0$. In this case we have to apply a coordinate change into general position.

Here I used the already well-optimised coordinate change implemented in the primdec.lib.

The method I implemented during my diploma thesis is called `GeneralPos`. It gets a list of maximal ideals which failed the test `prepare_max` as input and returns the intersection of all real maximal ideals of this input.

Let us consider an example. An ideal in which we have to apply a coordinate change into general position was presented in Example 3. Lets have a look at this.

Example 6 *Let* $M = \langle x^2 + 1 + t, y^2 - t\rangle \lhd \cdot\mathbb{Q}(t)[x, y]$. *Choosing the coordinate change*

$$\begin{aligned}\varphi : \mathbb{Q}(t)[x, y] &\to \mathbb{Q}(t)[x, y]\\ x &\mapsto x\\ y &\mapsto y + x + t\end{aligned}$$

we get:

$$\begin{aligned}\varphi(M) &= \langle x^2 + 1 + t, (y + x + t)^2 - t\rangle\\ &= \langle x^2 + 1 + t, x^2 + 2xy + 2tx + y^2 + 2ty + t^2 - t\rangle\end{aligned}$$

Its lexicographical Gröbner basis w. r. t. the ordering $y < x$ *is:*

$$\begin{aligned}G_\varphi = \{&y^4 + 4ty^3 + (6t^2 + t)y^2 + (4t^3 + 4t)y + (t^4 + 6t^2 + 4t + 1),\\ &(-4t - 2)x - y^3 + (-3t)y^2 + (-3t^2 - 2t - 3)y + (-t^3 - 2t^2 - 3t)\}.\end{aligned}$$

Now $y^4 + 4ty^3 + (6t^2 + 2)y^2 + (4t^3 + 4t)y + (t^4 + 6t^2 + 4t + 1)$ *is not real in* $\mathbb{Q}(t)[y]$ *as* $y^4 + 4ty^3 + (6t^2 + 2)y^2 + (4t^3 + 4t)y + (t^4 + 6t^2 + 4t + 1)$ *is positive semi-definite (which can be seen using Lemma 4). Hence as in Example 3 we get that* M *is not real.*

In all my tests it didn't happen often that I had to change into general position for the test of being real. In fact the only examples I found in which there is a need to apply this change are ideals over

transcendent extensions of $\mathbb{Q}$ which are of the form in Example 3, i. e. every generator is univariate and real. For these cases I have not yet found any property to check realness without applying this change. A simple example for an ideal in which this change yields the realness of a maximal ideal is the following:

Example 7 *Let* $M = \langle x^2 + 1 - t, y^2 - t\rangle \lhd \cdot\mathbb{Q}(t)[x, y]$. *Here the same coordinate change as in the example above yields:*

$$\begin{aligned}\varphi(M) &= \langle x^2 + 1 - t, (y + x + t)^2 - t\rangle \\ &= \langle x^2 + 1 - t, x^2 + 2xy + 2tx + y^2 + 2ty + t^2 - t\rangle\end{aligned}$$

Here the Gröbner basis w. r. t. the lexicographical ordering $y < x$ *is:*

$$\begin{aligned}G_\varphi =&\{y^4 + 4ty^3 + (6t^2 - 4t + 2)y^2 + (4t^3 - 8t^2 + 4t)y + (t^4 - 4t^3 + \\ &+ 2t^2 + 1), 2x + y^3 + 3ty^2 + (3t^2 - 4t + 3)y + (t^3 - 4t^2 + 3t)\}.\end{aligned}$$

Now $y^4 + 4ty^3 + (6t^2 - 4t + 2)y^2 + (4t^3 - 8t^2 + 4t)y + (t^4 - 4t^3 + 2t^2 + 1)$ *is real as it is indefinite and the degree of* $2x + y^3 + 3ty^2 + (3t^2 - 4t + 3)y + (t^3 - 4t^2 + 3t)$ *in* x *is odd. Hence* $\varphi(M)$ *is real by Proposition 3, thus* M *is real. In fact* M *is* α*-real in every ordering* α *of* $\mathbb{Q}(t)$ *satisfying the condition* $t \geq 1$.

To see the algorithm `GeneralPos` I recommend looking at Algorithm 4.2 in [6].

4.2 An algorithm to compute the zero-dimensional radical

From the explanation in the last subsections, it is not difficult to get an algorithm which computes the real radical of a zero-dimensional ideal J in $F[x_1, \ldots, x_n]$.

Algorithm 2

proc *RealZero(I)*

INPUT : *a zero-dimensional ideal* $I \trianglelefteq F[x_1, \ldots, x_n]$

OUTPUT: *an ideal* $\overline{J}$ *s.th.* $\overline{J} = \sqrt[re]{I}$

Simplify the ideal $I = \langle f_1, \ldots, f_r \rangle$ *to* $J = \langle g_1, \ldots, g_r \rangle$ *as described in [6] Remark 4.16,*[4]

Compute the associated primes of $Max := \mathrm{Min}(I)$ *with* `primdecGTZ` *or* `primdecSY`*. (This depends on which algorithm is faster.*[4]*).*

Initialise $Prep := \varnothing$ *and* $NonPrep := \varnothing$

while $Max \neq \varnothing$ *do*

{

Choose an $M \in Max$

$Max := Max \setminus \{M\}$

Compute $erg = \overline{M}, j$ *with Algorithm 1.*

If $j = 1$ *and* $\overline{M} \neq \langle 1 \rangle$

{

$Prep := Prep \cup \{\overline{M}\}$

}

else

{

$NonPrep := NonPrep \cup \{\overline{M}\}$

}

$Prepared := \bigcap_{\overline{M} \in Prep} \overline{M}$*:*

$NonPrepared := GeneralPos(NonPrep)$*;*[5]

[4]These operations are applied with a time limit by the aid of the `watchdog` command. watchdog(command, timer) returns the result of the command if the time for the command finishes before the timer.

[5]The idea of this approach was explained with 2 examples in the previous subsection.

According to Theorem 1 we get that

$$\sqrt[re]{I} = \sqrt[re]{J} = Prepared \cap NonPrepared =: \overline{J}.$$

$return(\overline{J})$;

To finish this chapter I give an example in which every path of Algorithm 2 is taken.

Example 8 *Let*

$$\begin{aligned} I = \langle & (x^2y^3 - tx^2y + y^6 - y^5 - ty^4 + t^2 + 1) \cdot (y^3 - t^2y^2 + (-t^3 + t^2 - \\ & - t)y + t^3), (-2t)x^4 - 4tx^2 + (-t + 1)y^6 + (-t^2 + t)y^5 + (t^2 - \\ & - t)y^4 + (-t^4 + t^3)y^2 + (t^4 - t^3)y + (t^5 - t^4 + 2t^3 - 2t), y^7 + \\ & + t^2y^4 - t^2y^3 - t^4, (-t)x^2y^2 + t^2x^2 - y^6 - ty^5 + ty^4 + (-t^3 + \\ & + t^2 - t)y^2 + t^3y + (t^4 - t^3 + t^2)\rangle. \end{aligned}$$

Then every generator of I is simplified in the sense of Remark 4.16.

1. *The primary decomposition of I provides 4 minimal primes which are*

   - $M_1 = \langle x^2 + 1 - t, y^3 + t^2 \rangle$
   - $M_2 = \langle x^2 + t^2 + 1, y^2 + t \rangle$
   - $M_3 = \langle x^2 + 1 - t, y^2 - t \rangle$
   - $M_4 = \langle x^2 + 1 + t, y^2 - t \rangle$

   We set $Max := \{M_1, M_2, M_3, M_4\}$.

2. *$Prep := \varnothing$ and $NonPrep := \varnothing$*

3. *As Max is not empty choose $M_1 \in Max$ and set*

$$Max := Max \setminus \{M_1\} = \{M_2, M_3, M_4\}.$$

4. *prepare_max*$(M_1) = M_1, 1$ *because of Proposition 3. Hence set:*

$$Prep := Prep \cup \{M_1\} = \{M_1\}$$
$$NonPrep := NonPrep = \varnothing$$

5. *As* Max *is not empty choose* $M_2 \in Max$ *and set*

$$Max := Max \setminus \{M_2\} = \{M_3, M_4\}.$$

6. *prepare_max*$(M_2) = \langle 1 \rangle, 1$ *by [6] Lemma 3.2 w. r. t. the lexicographical ordering* $y < x$*. Hence set:*

$$Prep := Prep = \{M_1\}$$
$$NonPrep := NonPrep = \varnothing$$

7. *As* Max *is not empty choose* $M_3 \in Max$ *and set*

$$Max := Max \setminus \{M_3\} = \{M_4\}.$$

8. *prepare_max*$(M_3) = M_3, 0$*. Hence we have to apply a coordinate change and set:*

$$Prep := Prep = \{M_1\}$$
$$NonPrep := NonPrep \cup \{M_3\} = \{M_3\}$$

9. *As* Max *is not empty choose* $M_4 \in Max$ *and set*

$$Max := Max \setminus \{M_4\}.$$

10. *prepare_max*$(M_4) = M_4, 0$*. Hence we have to apply a coordinate change and set:*

$$Prep := Prep = \{M_1\}$$
$$NonPrep := NonPrep \cup \{M_4\} = \{M_3, M_4\}$$

11. *Now* Max *is empty and we set* $Prep = \{M_1\}$.

12. *From the examples 6 and 7 we conclude with the coordinate change* φ *satisfying* $\varphi(x) = x, \varphi(y) = y + x + t$ *that* M_3 *is real and* M_4 *is not real. Hence*

$$NonPrep = \{M_3\}$$

13. *Set*

$$\begin{aligned}\overline{J} &= Prep \cap NonPrep = M_1 \cap M_3 \\ &= \langle y^5 - ty^3 + t^2y^2 - t^3, x^2 + (-t+1)\rangle\end{aligned}$$

Hence the real radical of I *is*

$$\overline{J} = \langle y^5 - ty^3 + t^2y^2 - t^3, x^2 + (-t+1)\rangle.$$

4.3 The general case as reduction

To conclude I shall explain shortly how to compute the real radical with the preparations of this article.

The main theorem for the higher dimensional computation, adapted from [1] Theorem 4.5., is:

Theorem 5 *Let* $I \trianglelefteq F[x_1, \ldots, x_n]$. *For any* $S \subsetneq \{x_1, \ldots, x_n\}$ *let* $J^{(S)}$ *denote an ideal of the quotient ring* $F[x_1, \ldots, x_n] \cdot F(S)$ *satisfying*

$$\dim J^{(S)} \leq 0 \text{ and } I \cdot F(S) \subseteq J^{(S)} \subseteq (I \cdot F(S))_{Iso}.$$

Then

$$\sqrt[re]{I} = \bigcap_{S \subsetneq \{x_1,\ldots,x_n\}} (\sqrt[re]{J^{(S)}} \cap F[x_1, \ldots, x_n])$$

As every $J^{(S)}$ has a dimension less then equal zero we are able to compute there real radicals. Theorem 5 now tells us how to intersect all these ideals properly so that our result will be the real radical. The theory of finding the $J^{(S)}$ uses real isolated points for arbitrary formally real fields. It is explained in detail in [1] chapter 4 or in chapter 5 of [6].

5 Conclusions

Following a short introduction of the basics on real algebra and real radicals, I described how to compute the real radical in the univariate case and in the zero-dimensional case. The univariate case corresponds to the leaves of the reduction tree for computing real radicals. While the univariate case uses theory which can already be found in literature, like Sturm's Theorem (cf. [2]) or the decision of indefiniteness (cf. [4]), section 4, the zero-dimensional case, introduces newly found properties. The decision was to compute the primary decomposition of the zero-dimensional input and to give a heuristic for deciding whether a maximal ideal is real or not. This heuristic yield a procedure `prepare_max` which prepares a maximal ideal in such a way that we can avoid a coordinate change into general position as often as possible. If we can not avoid a coordinate change we use the procedure `GeneralPos`. Its input is a list of maximal ideals where a change can't be avoided. Here a suitably randomised coordinate change is computed such that we can check the properties of `prepare_max` for the transformed maximal ideals and afterwards we intersect all real maximal ideals of this list. Finally, the procedure `RealZero` gets a zero-dimensional input I and computes its primary decomposition. Then it considers separately every maximal ideal and tests if a change is needed to compute the real part. Afterwards it intersects the real radicals of all these 'nice' maximal ideals and restarts the procedure `GeneralPos` for the list of 'bad' ideals. Since the primary decomposition is well-optimised in SINGULAR the advantage of this is a time improvement during the computations. This is because coordinate changes into general position cause a growth of coefficients and terms which slows the Gröbner bases computations down. The idea presented in this abstract avoid such changes as often as possible. Finally the article closes with the description how to compute the arbitrary radical as a reduction to the zero-dimensional case. We have presented an algorithm to compute real radicals which uses the new introduced heuristic `prepare_max` and is thus a time improvement to the algorithm presented by Becker and Neuhaus in [1].

References

[1] E. Becker and R. Neuhaus. On the computation of the real radical. *Journal of Pure and Applied Algebra*, 124:261–280, 1998.

[2] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[3] Gert-Martin Greuel and Gerhard Pfister. *A* **Singular** *introduction to commutative algebra*. Springer-Verlag, Berlin, 2002. With contributions by Olaf Bachmann, Christoph Lossen and Hans Schönemann, With 1 CD-ROM (Windows, Macintosh, and UNIX).

[4] Zeng Guangxing and Zeng Xiaoning. An effective decision method for semidefinite polynomials. *J. Symb. Comput.*, 37(1):83–99, 2004.

[5] Manfred Knebusch and Claus Scheiderer. *Einführung in die reelle Algebra*, volume 63 of *Vieweg Studium: Aufbaukurs Mathematik [Vieweg Studies: Mathematics Course]*. Friedr. Vieweg & Sohn, Braunschweig, 1989.

[6] Silke J. Spang. *On the Computation of the real radical*. Diploma Thesis. University of Kaiserslautern, March 2007.

Silke J. Spang,

Received November 9, 2007

Fraunhofer Institute for Industrial Mathematics (ITWM)
Department System Analysis, Prognosis and Control
Kaiserslautern, Germany
E–mail: *silke.spang@itwm.fraunhofer.de*