Radical computations of zero-dimensional ideals and real root counting

IMACS Symposium SC-1993

E. Becker, T. Wörmann*
Universität Dortmund, Fachbereich Mathematik, Lehrstuhl VI
44221 Dortmund, Fed. Rep. of Germany

Abstract: The computation of the radical of a zero-dimensional ideal plays an important role in various areas of computer algebra. A bunch of different methods have been published to meet this task (see e.g. [FII], [GP], [GTZ], [KL1], [L1], [L4], [LL], [N]). The method presented in this paper is strongly connected to a recent approach to the real root counting problem as described in [PRS] and [BW]. It provides a lot of information for real root counting already in the process of calculating the radical. In this sense this approach is well-suited for real root counting problems.

Keywords: Trace form, radical of an ideal, decomposition of algebras

1 Outline of the method

Let $F$ be a field of characteristic 0 and $I \subseteq F[X_1, \ldots, X_n]$ a zero-dimensional ideal of the polynomial ring, $V(I)$ the zeros of $I$ in $\mathbb{F}^n$, $\mathbb{F}$ the algebraic closure of $F$. We further denote by $A = F[X_1, \ldots, X_n]/I$ the coordinate algebra which is a finite-dimensional $\mathbb{F}$-algebra. $\text{rad}(A)$ denotes the reduced $\mathbb{F}$-algebra $A/\text{Nil}(A) \cong F[X_1, \ldots, X_n]/\sqrt{I}$ which in turn is isomorphic to $A_{\text{red}}$, the $\mathbb{F}$-subalgebra of $A$ of all separable elements of $A$. Thus we have the Wedderburn decomposition $A = A_{\text{red}} \otimes_{\mathbb{F}} \text{Nil}(A)$. $A_{\text{red}} = A_{\text{red}}(A)$ via $a \mapsto a + \text{Nil}(A)$.

The trace of an element $x \in A$ is defined to be the trace of the $F$-linear multiplication by $x$.

By $tr_r < g >$ for $g \in A$ we denote the symmetric bilinear form defined by

$$tr_r < g > := tr(gxy)$$

for all $x, y \in A$.

This bilinear form is used for counting real roots in the following way. Let $F$ be an ordered field with real closure $K$. Set $V_r(I) := K^n \cap V(I)$. Then

$$\text{sign}(tr_r < g >) = \# \{ \alpha \in V_r(I) \mid g(\alpha) > 0 \} - \# \{ \alpha \in V_r(I) \mid g(\alpha) < 0 \},$$

where on the right hand side, $g \in A$ is understood as a function on $V_r(I)$ of $\text{fro}$/ [PRS]/[BW]. In general, the bilinear forms $tr_r < g >$ are degenerate. Therefore for actual computations it seems advisable to start by reducing these forms modulo their radical

$$\text{rad}(A) = \{ x \in A \mid \phi(x, y) = 0 \forall y \in A \}.$$

Since the trace vanishes on $\text{Nil}(A)$ we get $\text{Nil}(A) \subseteq \text{rad}(A)$ for every form $\phi$. Consequently by passing from $A$ to its factor algebra $A_{\text{red}}$ and from $\phi$ to $\phi_{\text{red}}$ accordingly, the signatures of the forms in question are not changed: $\text{sign} \phi_{\text{red}} = \text{sign} \phi$.

Now, $\phi$ lives on an algebra of lower dimension. Hence calculations in $A_{\text{red}}$ are generally cheaper than in $A$ itself. However the epimorphism $A \to A_{\text{red}}$ is needed in an explicit form. Theoretically this is achieved by the so-called Shape Lemma.

Theorem (Shape Lemma): Let $I$ be an ideal which is in general position w.r.t. $X_0$, i.e. the projection $V(I) \to \mathbb{R}$ onto the $X_0$-coordinate is injective. Then $I$ has a lexicographical Gröbner basis w.r.t. $X_n < X_{n-1} < \ldots < X_1$ of the form

$$\sqrt{I} = \langle f(X_n), X_{n-1} - g_{n-1}(X_n), \ldots, X_1 - g_1(X_n) \rangle,$$

where $f$ is a squarefree polynomial and the degree of $g_i$ does not exceed the degree of $f$.

For a proof see e.g. [BW] or [L1].

Having $\sqrt{I}$ generated as in the Shape Lemma the epimorphism $A \to A_{\text{red}}$ is given by

$$A/F[X_1, \ldots, X_n]/I \to A_{\text{red}} = F[X_1, \ldots, X_n]/\sqrt{I} = F[X_n]/(f(X_n)).$$
where
\[ G(X_1, \ldots, X_n) + f = G(g_1(X_n), \ldots, g_{n-1}(X_n), X_n) + (f(X_n)). \]

Moreover, and this is of great computational importance, the structure of the reduced algebra allows to apply univariate techniques for the real root counting, either by signature of bilinear forms or by Sturm-Habicht sequences (see [GLR] or [G]). However, to derive the lexicographical Gröbner basis above directly by the Buchberger algorithm usually amounts to high computational expenses, if possible at all.

The trace form \( \text{tr}^* < 1 \) on \( A \) or rather its representing symmetric matrix \( M \) can be used to determine the radical \( N(f)(A) \) as a vectorspace by linear algebra methods as proposed by various authors, e.g. [R], [GMT], [G]. Knowing \( N(f)(A) \) as a vectorspace further calculations, e.g. by Gröbner basis techniques, will then yield the required set of generators of \( \sqrt{J} \). In our method, however, we don't need the whole matrix \( M \) of size \( N \times N, N = \dim_{\mathbb{F}} A \). Instead, \( M \) is replaced by a smaller matrix of size \( m \times m \) where \( m \leq \dim_{\mathbb{F}} A_{x,d} \) which, additionally, also provides candidates for the polynomials \( g_i(X_n), i = 1, \ldots, n - 1 \). An implementation is being prepared.

2 The algorithm

Input: A set of generators for the ideal \( I \).
Output: \( f(X_n), g_1(X_n), \ldots, g_{n-1}(X_n) \) as in the Skaspe lemma (possibly after a linear change of variables).

0) Compute a Gröbner basis of the ideal with respect to any admissible term ordering. Check whether the ideal is zero-dimensional, if not leave the algorithm. Determine \( N = \dim_{\mathbb{F}} A \) and the multiplication table of \( A \).

1) Determine the minimal polynomial \( f \) of \( x_n \in A \) and its squarefree kernel \( f' \).

2) If \( \deg f = \dim_{\mathbb{F}} A = N \) determine \( x_i = g_i(x_n), g_i \in f \mod f \), STOP.

3) If \( d := \deg f < N \) determine \( g_1, \ldots, g_{n-1}, \) polynomials of degree \( \leq d - 1 \) subject to
\[ \text{tr}((x_i - g_i(x_n)) : x_n^k) = 0 \forall j = 0, \ldots, d - 1. \]

Or if we write \( g_i(X) = a_0^i + \ldots + a_{d-1}^i X^{d-1} \), we get the systems of linear equations:
\[
\begin{pmatrix}
\text{tr}(1) & \text{tr}(x_n) & \cdots & \text{tr}(x_n^{d-1}) \\
\text{tr}(g_1) & \text{tr}(g_2) & \cdots & \text{tr}(g_2^{d-1}) \\
\vdots & \vdots & \ddots & \vdots \\
\text{tr}(g_{n-1}) & \text{tr}(g_{n-1}^2) & \cdots & \text{tr}(g_{n-1}^{d-1})
\end{pmatrix}
\begin{pmatrix}
a_0^1 \\
a_0^2 \\
\vdots \\
a_0^{d-1}
\end{pmatrix} = 0.
\]

4) If \( (x_i - g_i(x_n))^{N-d+1} = 0, \forall i = 1, \ldots, d - 1 \) then STOP.

5) If \( (x_i - g_i(x_n))^{N-d+1} \neq 0 \) for some \( i \) then choose at random an \( \alpha \in \mathbb{F} \) and a linear change of coordinates \( X_1, \ldots, X_{n-1}, X_n + \alpha X_1 \).

Start again at 0) with the new variables.

3 Cyclic algebras

In this and the subsequent section we will present the mathematical background of our algorithm.

An algebra \( A \) is called cyclic (see [SchS]) if \( A = F[x] \) for some \( x \). To determine some properties of generating elements of a cyclic algebra we need the following special case of the elementary divisor theorem:

Proposition: Let \( V \) be a vectorspace of dimension \( n \) over the field \( F \), \( f \in \text{End}_F(V) \) a fixed vectorspace endomorphism. Then the following statements are equivalent:

i) \( V \) is cyclic w.r.t. \( f \), i.e., there exists an \( x \in V \) such that \( x, f(x), \ldots, f^{n-1}(x) \) is a basis of \( V \).

ii) There exists a basis of \( V \) such that \( f \) has a matrix of the form
\[
\begin{pmatrix}
0 & \cdots & 0 & -a_0 \\
1 & \cdots & 0 & -a_1 \\
\vdots & \ddots & \vdots & \vdots \\
0 & \cdots & 1 & -a_{n-1}
\end{pmatrix}
\]

iii) All Eigenspaces of \( f := f \otimes id \in \text{End}_F(V \otimes F) \) have dimension 1 (in [AS] this criterion is used to compute numerically the zeroes).

iv) Characteristic and minimal polynomial of \( f \) coincide.

v) The degree of the minimal polynomial is \( n \).

Proof: i) \( \Rightarrow \) ii) is trivial, ii) \( \Rightarrow \) iii) is a trivial rank-computation. iii) \( \Rightarrow \) iv): In the Jordan normal form all Jordan blocks contain pairwise distinct Eigenvalues. The minimal (characteristic) polynomial is the lcm (product) of the minimal (characteristic) polynomials of those blocks. Hence the lcm and the product coincide. iv) \( \Rightarrow \) v) is trivial again and v) \( \Rightarrow \) i) is clear by the following

Lemman: Assume the same conditions as in the Proposition. If \( \mu_f \) is the minimal polynomial of \( f \)
then there exists an $z \in V$, such that $\mu_z$ is equal to the monic polynomial $p$ of smallest degree with $p(f)(x) = 0$.

**Proof:** see [Ga] or [SchSt]

In the $F$-algebra $A$ the characteristic (minimal) polynomial of an element $x \in A$ coincides with the characteristic (minimal) polynomial of the $F$-linear multiplication by $x$. The characteristic polynomial $\lambda_x$ and the minimal polynomial $\mu_x$ differ by a factor $p$, which is the gcd of the minors of size $n - 1$ of the matrix of $\lambda_x - X - id$ (see [Gi]), where $\lambda_x$ denotes the multiplication with $x$ in the $n$-dimensional algebra $A$. The relation is:

$$\lambda_x = F \cdot \mu_x.$$

Then we have the following

**Corollary:** The following statements are equivalent:

i) $x \in A$ is a generating element of $A$, i.e. $A = F[x]$.

ii) The minimal polynomial of $x$ is of degree $n$.

iii) The gcd of all minors of size $n - 1$ of a matrix of $\lambda_x - X - id$ is 1.

If $A$ is known to be cyclic, it is easy to find a generating element due to the following

**Lemma:** Let $A$ be cyclic. For almost every choice of $x \in A$, $x$ is a generating element.

**Proof:** Let $v_1, \ldots, v_n \in A$ be a vectorspace basis of $A$. Take a generic linear combination $x := \sum_{i=1}^{n} a_i v_i$ and denote by $M \in M(n \times n, F[a_1, \ldots, a_n])$ the following matrix. The columns of $M$ are the coefficient vectors of $1, \ldots, z^{n-1}$. Then we have that $x$ is a generating element of $A$ if $\text{det}(M) \neq 0$. But this equation defines a hypersurface in the space of coefficients.

So the lemma gives a probabilistic method to decide whether $A$ is cyclic or not: Just check for an random element $x \in A$ if it generates $A$ or not. If it doesn't, the algebra is not cyclic in general.

Let $y \in A$. Then $F[y] = F[Y]/(f(Y))$ where $f(Y)$ denotes the minimal polynomial of $y$. If $\text{sq}(f)$ is the squarefree kernel of $f$, then $\text{sq}(f)$ is the minimal polynomial of $y_{\text{sep}}$, the separable part of $y$ in the unique decomposition $y = y_{\text{sep}} + y_{\text{sep}}$, where $y_{\text{sep}} \in A_{\text{sep}}$. $y_{\text{sep}} \in \text{Nil}(A)$. Since $F[y_{\text{sep}}]$ is generated by a separable element, it is separable and hence a semisimple $F$-subalgebra of $A$.

We have the following interesting

**Proposition:**

$$\text{dim}_F(F[y_{\text{sep}}]) = \text{deg}(\text{sq}(f)) = \#y(V_F(I))$$

**Proof:** W.l.o.g. we may assume that $F$ is algebraically closed and $A = A_{\text{sep}}$, $y \in A$.

If $N$ denotes the cardinality of the variety $V(I)$, we have the following isomorphism:

$$A \longrightarrow F^N$$

with

$$f \longmapsto (f(x_1), \ldots, f(x_N)).$$

so we get

$$F[y] \cong F[[y(x_1), \ldots, y(x_N))],$$

where $V(F) = \{x_1, \ldots, x_N\}$.

There is a one-to-one correspondence between the $F$-subalgebras of $F^N$ and the equivalence relations on $\{1, \ldots, N\}$ in the following way: If $R$ is an $F$-subalgebra of $F^N$, we get an equivalence relation by:

$$i \sim j \iff h_i = h_j \forall (h_1, \ldots, h_N) \in B$$

If vice versa we are given an equivalence relation $\sim$ on $\{1, \ldots, N\}$, we have a basis of a subalgebra by $e_R = \sum_{i \in R} e_i$, $e_i \in \{0, \ldots , 1, \ldots, 0\}$ where $R$ runs through all equivalence classes on $\{1, \ldots, N\}$ (see [SchSt], Theorem 2.34a).

This observation completes the proof.

We have an easy

**Corollary:**

i) $A_{\text{sep}}$, hence $A_{\text{reg}}$, is cyclic.

ii) $F[y_{\text{sep}}] = A_{\text{sep}} \iff \text{all } y(x), x \in V(I)$ are pairwise distinct.

Moreover we get that if an $F$-algebra $F[x,y]$ is separable then $F[x,y] = F[x + \alpha \cdot y]$ for all but finitely many $\alpha \in F$, using e.g. that a separable algebra has only finitely many subalgebras (see the proof above).

## 4 A decomposition of the algebra

We start with the following

**Theorem:** Let $B \subseteq A$ be a semisimple $F$-subalgebra of $A$ then $B^{\times} \cap B_{\times}B$ is non-degenerate.

**Proof:** Since $B$ is semisimple, it is a finite product of finite separable field extensions of $F$:

$$B \cong L_1 \oplus \cdots \oplus L_m$$

as $F$-algebra.

If we denote by $e_i = (0, \ldots , 1, \ldots , 0), i = 1, \ldots, m$ the irreducible idempotents of $B$, we have $e_i e_j = \delta_{ij}$ and $1 = \sum_{i=1}^{m} e_i$.

Since for any $a \in A$ we have $a = 1_a a + \cdots + 1_m a$, hence

$$A = \sum_{i=1}^{m} A_i.$$
with $A_i := a_i A$. But this sum is also direct, for if $0 = a_1 e_1 + \ldots + a_n e_n$, multiplication by $e_i$ yields $ae_i = 0$. $A_i$ is the $L_i$-module hence an $L_i$-vectorspace.

For calculating $tr^* < 1 > |_{B^* B}$ we omit the indices since $e_i e_j = 0$ for $i \neq j$. We get for $z, y \in L_1$:

$$tr_{A_1}r^* < 1 > (z,y) = tr_{A_1}f(z) = \sum_{M} M,$$

where $M$ is a matrix of the multiplication by $z$ in $L_1$ as an $F$-linear mapping.

Now we can conclude:

$$tr^* < 1 > |_{B^* B} = \sum_{i} tr_{A_i}r^* < 1 > \otimes < dim_{L_i} A_i >.$$

Since $L_i / F$ is a separable field extension and therefore $tr_{F_i}r^* < 1 >$ is non-degenerate and $dim_{L_i} A_i > 0$ we end the proof.

**Corollary:** $rad tr^* < 1 > = \sqrt{I} / I = Nil(A)$

**Proof:** We have the Wedderburn-decomposition

$$A \cong A / Nil(A) \oplus Nil(A),$$

as $F$-vectorspaces. Because $A / Nil(A) \cong A_{sep}$ is clearly semisimple applying the theorem yields the desired result.

**Remark:** This is no longer true for a perfect field of characteristic greater than zero (see [10]).

### 4.1 The decomposition

If $d$ is the degree of $s(f)$ the two vectorspaces $span(1, x, \ldots, x^{d-1})$ and $span(1, x, \ldots, x^{d-1}) = F[x_{d+1}]$ are isometric, since the trace of a nilpotent element is zero. By the first theorem the latter space is non-degenerate hence the first one as well. Therefore it can be split off orthogonally:

$$A = span(1, y, \ldots, y^{d-1}) \perp V_1 \perp Nil(A),$$

where

$$V_0 := span(1, y, \ldots, y^{d-1}) = F[y] / (s(f)(Y))$$

and

$$span(1, y, \ldots, y^{d-1}) \perp V_1 \cong A_{sep}.$$  

Here $V_1$ is also non-degenerate since $A_{sep}$ is of this type. The symbol $\cong$ means isometry.

### 5 Correctness and Performance

#### 5.1 Correctness

The homomorphism $F[X_n] \rightarrow A, x_n \mapsto x_n$ induces $F[X_n] / (f) \rightarrow F[x_n] \rightarrow A$

$$\begin{array}{ccc}
\pi & \rightarrow & \pi \\
\downarrow & & \downarrow \\
\pi & & \pi \\
F[X_n] / (f) & \rightarrow & F[x_n]/(x_n) = A
\end{array}$$

If $\deg f = N$, i.e. $A = F[x_n]$ then $x_n = g(x_n)$, yielding $\pi(x_i) = g_i(x_n)$ for $i = 1, \ldots, n - 1$, and finally $\pi = (f(X_n), X_n) = g_{n-1}(X_n), \ldots, X_1 = g_1(X_n))$. Now we assume $\dim_{A} < N$. We consider the decomposition in 4.1:

$$A = span(1, x_n, \ldots, (x_n)^{d-1}) \perp V_1 \perp Nil(A),$$

and compute $g(x_n)$ satisfying

$$x_n - g(x_n) \in V_0 = V_1 \perp Nil(A),$$

or equivalently solve the systems of linear equations given in the algorithm. If all the $x_i - g_i(x_n)$ are nilpotent then

$$A / Nil(A) \cong F[x_n] / (F[x_n] \cap Nil(A)) \cong F[x_n]_{sep}$$

Since $dim_{F} Nil(A) \leq N - d$ we get that $x_i - g_i(x_n)$ is nilpotent if $x_i - g_i(x_n)^{N-d+1} = 0$.

Assume next that, say, $x_i - g_i(x_n)$ is not nilpotent. Then the subalgebra $B := F[x_n, x_i]$ has a reduced algebra $B_{red} = F[x_n, x_i] \cap A_{red}$, which is strictly larger than $F[x_n] = F[x_n]_{sep}$ since $x_i \notin F[x_n]$.

From section 3 we know that $F[x_n, x_i]$ is cyclic and generated by an element of the type $e + \alpha \cdot z$ where $\alpha$ is chosen at random.

Hence, after considering the new generator $x_i, \ldots, x_{d+1}, x_{d+1}$, we have enlarged the dimension of $F[x_n] / (x_n) \cong A_{red}$ at least by one. After at most $N - d$ steps we have found $x_n$ satisfying $F[x_n] / (x_n) = A_{red}$, i.e. $dim_{F} V_0 = dim_{F} A_{red}$ yielding $V_1 = 0$ and $x_i - g_i(x_n) \in Nil(A)$ necessarily.

#### 5.2 Performance

There are several possibilities of computing the minimal polynomial $f$, e.g. some [FGLM] technique or directly by computing an appropriate Gröbner basis etc.

For computing the solutions of the linear systems in step 3) we need only to invert one Hankel matrix of size $d \times d$ which can be done in $O(d^3)$-time (see [HR]). This is clearly better than working with a matrix of size $N \times N$.

The check for nilpotency of the $x_i - g_i(x_n)$ can be done by using fast exponentiation taking $(n - 1) \cdot \log(N - d + 1)$ multiplications.
The algorithm terminates for sure after \( N - d \) loops. But since a generic linear change of coordinates puts the variety in general position we are almost always done after one loop. In any case, the complexity of the algorithm is clearly dominated by the computation of the Gröbner base in step 0.

6 Variants

Some special cases are given by requiring that the difference between the vectorspace dimensions of \( A \) (known after the first step of the algorithm) and \( F[x_n] \) (computed in step 1) is 1 or 2. Then there are explicit formulæ for the structure of the algebra \( A \) which will be described in a forthcoming paper.

We next study the case of a Frobenius algebra. Suppose that \( A \) is a Frobenius algebra with an explicitly given or constructed Frobenius linear form \( f \), i.e., the bilinear form \( x, y \mapsto f(xy) \) is non-degenerate. E.g. this is the case when \( A = F[X_1, \ldots, X_n]/(f_1, \ldots, f_n) \) is a complete intersection, see [Ske81], [Sch82] and [Ca].

In this case the radical can be computed by the following method which also accounts for a simplification of our algorithm.

Let \( \{ e_i \} \) and \( \{ \tilde{e}_j \} \) be a pair of dual bases of \( A \), i.e., both are bases and we have

\[
T(e_i \tilde{e}_j) = \delta_{ij}.
\]

Set \( \tilde{J} := \sum e_i \tilde{e}_i \). Then we have a

**Proposition:** \( \text{tr}_{A^P}(x) = (Jx) \) for every \( x \in A \).

**Proof:** We calculate \( \text{tr}(e_i) \) by means of the basis \( \{ \tilde{e}_j \} \). First we note that \( e_i \tilde{e}_j = \sum_k T(e_i e_k \cdot \tilde{e}_j) \).

Consequently

\[
\text{tr}(e_i) = \sum_j (e_i \tilde{e}_j) = \sum_j \tilde{J} e_i \tilde{e}_j.
\]

This holds for every \( e_i \), hence the claim is proved.

**Corollary:**

\( \text{Nil}(A) = \text{Ann}(\tilde{J}) = (A\tilde{J})^{-1} \)

**Proof:** \( \text{Nil}(A) = \text{Ann}(\tilde{J}) \) follows from the non-degeneracy of the bilinear form \( \phi : x, y \mapsto f(xy) \). This fact also yields that, given any ideal \( T \subset A \), we have \( \text{Ann}(T) = T^{-1} \) (relative to \( \phi \)).

**Remark:** The calculation of \((A\tilde{J})^{-1}\) is clearly a matter of linear algebra.

Now take any coordinate function \( x_n \in A \). In the present situation of a Frobenius algebra the algorithm can be modified using the following

**Corollary:** The following statements are equivalent:

i) \( A_{x_n} = F[x_n] \)

ii) for every \( i = 1, \ldots, n - 1 \) the equation

\[
x_i \tilde{J} = g_i(x_n) \tilde{J}
\]

is solvable.

**Proof:** It remains to prove ii) \( \Rightarrow \) i). From \( x_i - g_i(x_n) \tilde{J} = 0 \) we derive \( x_i - g_i(x_n) \in \text{Nil}(A) \). Hence \( A_{x_n} = F[x_n] \) as was to be shown.

Note that we may bound the degree of the \( g_i \) by the degree of the minimal polynomial of \( x_n \).

References:


