HAL
archives-ouvertes.fr

On the Computation of Matrices of Traces and Radicals of Ideals

Itnuit Janovitz-Freireich, Bernard Mourrain, Lajos Ronayi, Agnes Szanto

▶ **To cite this version:**

Itnuit Janovitz-Freireich, Bernard Mourrain, Lajos Ronayi, Agnes Szanto. On the Computation of Matrices of Traces and Radicals of Ideals. Journal of Symbolic Computation, Elsevier, 2012, 47 (1), pp.102-122. <10.1016/j.jsc.2011.08.020>. <inria-00354120>

HAL Id: inria-00354120
https://hal.inria.fr/inria-00354120

Submitted on 19 Jan 2009

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

ON THE COMPUTATION OF MATRICES OF TRACES AND RADICALS OF IDEALS

ITNUIT JANOVITZ-FREIREICH, BERNARD MOURRAIN, LAJOS RÓNYAI, AND ÁGNES SZÁNTÓ

Abstract. Let $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_m]$ be a system of polynomials generating a zero-dimensional ideal $\mathcal{I}$, where $\mathbb{K}$ is an arbitrary algebraically closed field. We study the computation of "matrices of traces" for the factor algebra $\mathcal{A} := \mathbb{K}[x_1, \ldots, x_m]/\mathcal{I}$, i.e. matrices with entries which are trace functions of the roots of $\mathcal{I}$. Such matrices of traces in turn allow us to compute a system of multiplication matrices $\{M_{x_i} | i = 1, \ldots, m\}$ of the radical $\sqrt{\mathcal{I}}$.

We first propose a method using Macaulay type resultant matrices of $f_1, \ldots, f_s$ and a polynomial J to compute moment matrices, and in particular matrices of traces for $\mathcal{A}$. Here J is a polynomial generalizing the Jacobian. We prove bounds on the degrees needed for the Macaulay matrix in the case when $\mathcal{I}$ has finitely many projective roots in $\mathbb{P}^m_{\mathbb{K}}$. We also extend previous results which work only for the case where $\mathcal{A}$ is Gorenstein to the non-Gorenstein case.

The second proposed method uses Bezoutian matrices to compute matrices of traces of $\mathcal{A}$. Here we need the assumption that $s = m$ and $f_1, \ldots, f_m$ define an affine complete intersection. This second method also works if we have higher dimensional components at infinity. A new explicit description of the generators of $\sqrt{\mathcal{I}}$ are given in terms of Bezoutians.

Keyword: matrix of traces; radical of an ideal;

1. Introduction

This paper is a continuation of our previous investigation in [25, 26] to compute the approximate radical of a zero dimensional ideal which has zero clusters. It turns out that the computationally most expensive part of the method in [25, 26] is the computation of the matrix of traces. We address this problem in the present paper. Some of the results of this paper also appeared earlier in [24], however here we present generalized versions of those results and also add new results, as described below.

The computation of the radical of a zero dimensional ideal is a very important problem in computer algebra since a lot of the algorithms for solving polynomial systems with finitely many solutions need to start with a radical ideal. This is also the case in many numerical approaches, where Newton-like methods are used. From a symbolic-numeric perspective, when we are dealing with approximate polynomials, the zero-clusters create great numerical instability, which can be eliminated by computing the approximate radical.

The theoretical basis of the symbolic-numeric algorithm presented in [25, 26] was Dickson's lemma [15], which, in the exact case, reduces the problem of computing the radical of a zero dimensional ideal to the computation of the nullspace of the so called matrices of traces (see Definition 3.17): in [25, 26] we studied numerical

This research was partly supported by the Marie-Curie Initial Training Network SAGA.

properties of the matrix of traces when the roots are not multiple roots, but form small clusters. Among other things we showed that the direct computation of the matrix of traces (without the computation of the multiplication matrices) is preferable since the matrix of traces is continuous with respect to root perturbations around multiplicities while multiplication matrices are generally not.

In the present paper, first we give a simple algorithm using only Macaulay type resultant matrices and elementary linear algebra to compute matrices of traces of zero dimensional ideals which have finitely many projective roots. We also extend the method presented in [24] to handle systems which might have roots at infinity or for which the quotient algebra is non-Gorenstein.

In the second part of the paper, we investigate how to compute matrices of traces using Bezoutians in the affine complete intersection case. Our approach in that case is based on [40, 39].

For the method using Macaulay matrices we need the following assumptions: let $\mathbf{f} = [f_1, \dots, f_s]$ be a system of polynomials of degrees $d_1 \geq \cdots \geq d_s$ in $\mathbb{K}[\mathbf{x}]$, with $\mathbf{x} = [x_1, \dots, x_m]$, generating an ideal $\mathcal{I}$ in $\mathbb{K}[\mathbf{x}]$, where $\mathbb{K}$ is an arbitrary algebraically closed field. We assume that the algebra $\mathcal{A} := \mathbb{K}[\mathbf{x}]/\mathcal{I}$ is finite dimensional over $\mathbb{K}$ and that we have bounds $\delta > 0$ and $0 \leq k \leq \delta$ such that a basis $B = [b_1, \dots, b_N]$ of $\mathcal{A}$ can be obtained by taking a linear basis of the space

$$\mathbb{K}[\mathbf{x}]_k / \langle f_1, \dots, f_s \rangle_\delta \cap \mathbb{K}[\mathbf{x}]_k$$

where $\mathbb{K}[\mathbf{x}]_k$ is the set of polynomials of degree at most k and $\langle f_1, \dots, f_s \rangle_\delta = \{\sum_{i=1}^s q_i f_i \ : \ \deg q_i \leq \delta - d_i\}$. We can assume that the basis B consists of monomials of degrees at most k by a slight abuse of notation. In our earlier work [24], we gave bounds for k and δ in the case where there were no roots at infinity using a result of Lazard [37] (see Theorem 3.4). Here we extend those results to the case where $\mathcal{I}$ has finitely many *projective* common roots in $\mathbb{P}^m_{\mathbb{K}}$ (see Theorem 3.5). Furthermore, we now extend the method presented in [24], which only addressed the case where $\mathcal{A}$ is Gorenstein over $\mathbb{K}$ (see Definition 3.1), to handle non-Gorenstein algebras.

The main ingredient of our first method is a Macaulay type resultant matrix $\mathrm{Mac}_\Delta(\mathbf{f})$, which is defined from the transpose matrix of the degree Δ Sylvester map $(g_1, \dots, g_s) \mapsto \sum_{i=1}^s f_i g_i \in \mathbb{K}[\mathbf{x}]_\Delta$ for $\Delta \leq 2\delta + 1$ using simple linear algebra (see Definition 3.8). Using our results, we can compute a basis B of $\mathcal{A}$ using $\mathrm{Mac}_\Delta(\mathbf{f})$. We also prove that a random element $\mathbf{y}$ of the nullspace of $\mathrm{Mac}_\Delta(\mathbf{f})$ provides an $N \times N$ moment matrix $\mathfrak{M}_B(\mathbf{y})$ which has the maximal possible rank with high probability (similarly as in [35]). Note that in the Gorenstein case the moment matrix $\mathfrak{M}_B(\mathbf{y})$ is non-singular. This will no longer be true in the non-Gorenstein case. This moment matrix allows us to compute the other main ingredient of our algorithm, a polynomial J of degree at most δ, such that J is the generalization of the Jacobian of $f_1, \dots f_s$ in the case when $s = m$. The main result of the paper now can be formulated as follows:

THEOREM *Let $B = [b_1, \dots, b_N]$ be a basis of $\mathcal{A}$ with $\deg(b_i) \leq k$. With J as above, let $\mathrm{Syl}_B(J)$ be the transpose matrix of the map $\sum_{i=1}^N c_i b_i \mapsto J \cdot \sum_{i=1}^N c_i b_i \ \in \mathbb{K}[x]_\Delta$ for $c_i \in \mathbb{K}$. Then*

$$[Tr(b_i b_j)]_{i,j=1}^N = \mathrm{Syl}_B(J) \cdot X,$$

where X is the unique extension of the matrix $\mathfrak{M}_B(\mathbf{y})$ such that $\mathrm{Mac}_\Delta(\mathbf{f}) \cdot X = 0$.

Once we compute the matrix of traces $R := [Tr(b_i b_j)]_{i,j=1}^N$ and the matrices $R_{x_k} := [Tr(x_k b_i b_j)]_{i,j=1}^N = \mathrm{Syl}_B(x_k J) \cdot X$ for $k = 1, \ldots, m$, we can use the results of [25, 26] to compute a system of multiplication matrices for the (approximate) radical of $\mathcal{I}$ as follows: if $\tilde{R}$ is a (numerical) maximal non-singular submatrix of R and $\tilde{R}_{x_k}$ is the submatrix of R_{x_k} with the same row and column indices as in $\tilde{R}$, then the solution M_{x_k} of the linear matrix equation

$$\tilde{R} M_{x_k} = \tilde{R}_{x_k}$$

is an (approximate) multiplication matrix of x_k for the (approximate) radical of $\mathcal{I}$. See [26] for the definition of (approximate) multiplication matrices. Note that a generating set for the radical $\sqrt{\mathcal{I}}$ can be obtained directly from the definition of multiplication matrices, in particular, it corresponds to the rows of the matrices $M_{x_1}, \ldots, M_{x_m}$.

We also point out that in the $s = m$ case these multiplication matrices M_{x_k} of $\sqrt{\mathcal{I}}$ can be obtained even more simply using the nullspace of $\mathrm{Mac}_\Delta(\mathbf{f})$ and the Jacobian J of $\mathbf{f}$, without computing the matrices of traces.

In the last section we investigate the use of Bezoutians to compute matrices of traces of systems $f_1, \ldots, f_m$ which form an affine complete intersection. In this particular setting, our method allows systems that may have higher dimensional projective components.

In the univariate case it is proved in [40] that the Bezoutian matrix of a univariate polynomial f and its derivative f' is a matrix of traces with respect to the Horner basis of f (see subsection 4.1). Therefore, applying the method to compute the approximate or exact radical from the matrix of traces provided by the Bezoutian will give us an approximate or exact square-free factorization of f. The question that naturally arises is how this method relates to computing the square-free factor as $\frac{f}{gcd(f,f')}$. We show here that the two algorithms are computationally equivalent.

The generalization to the multivariate case is not quite as straightforward. The goal would be to express the Bezout matrix of $f_1, \ldots, f_m$ and their Jacobian J as a matrix of traces with respect to some basis, generalizing the univariate case (see the definition of the Bezout matrix – sometimes also referred as the Dixon matrix – in Definition 4.5). Unfortunately, the Bezout matrix cannot directly be expressed as a matrix of traces. However, in [40] it is shown that a reduced version of the Bezout matrix of $f_1, \ldots, f_m$, and J is equal to the matrix of traces of $f_1, \ldots, f_m$ with respect to the so called canonical basis, obtained from the reduced Bezout matrix of $f_1, \ldots, f_m$, and 1. The required reduction of the Bezout matrix involves reducing polynomials modulo $\mathcal{I}$.

Now the question is how to find the reduced version of the Bezout matrix without further information on the structure of the quotient algebra $\mathbb{C}[x_1, \ldots, x_m]/\mathcal{I}$, e.g. without Gröbner Bases or multiplication matrices. First we show that we can obtain a set of generating polynomials for the radical $\sqrt{I}$ from the *non-reduced* Bezoutian matrices (see Theorem 4.9). Secondly, we give an algorithm which computes a system of multiplication matrices $M_{x_1}, \ldots, M_{x_m}$ for $\sqrt{I}$. This algorithm adapts the results of [39] to find the required reduced Bezout matrices using only elements in $\sqrt{I}$ which were obtained from non-reduced Bezout matrices.

2. Related Work

The motivation for this work was the papers [35, 36] where they use moment matrices to compute the radical of real and complex ideals. They present two versions of the method for the complex case: first, in [36] they double up the machinery for the real case to obtain the radical of the complex ideal. However, in [35] they significantly simplify their method and show how to use moment matrices of maximal rank to compute the multiplication matrices of an ideal between $\mathcal{I}$ and its radical $\sqrt{\mathcal{I}}$. In particular, in the Gorenstein case they can compute the multiplication matrices of $\mathcal{I}$. In fact, in [35] they cite our previous work [25] to compute the multiplication matrices of $\sqrt{\mathcal{I}}$ from the multiplication matrices of $\mathcal{I}$, but the method proposed in the present paper is much simpler and more direct.

Note that one can also obtain the multiplication matrices of $\mathcal{I}$ with respect to the basis $B = [b_1, \ldots, b_N]$ by simply eliminating the terms not in B from $x_k b_i$ using $\mathrm{Mac}_{\delta+1}(\mathbf{f})$. The advantage of computing multiplication matrices of the radical $\sqrt{\mathcal{I}}$ is that it returns matrices which are always simultaneously diagonalizable, and possibly smaller than the multiplication matrices of $\mathcal{I}$, hence easier to work with. Moreover, if B contains the monomials $1, x_1, \ldots, x_m$, one eigenvector computation yields directly the coordinates of the roots.

Computation of the radical of zero dimensional complex ideals is very well studied in the literature: methods most related to ours include [20, 3] where matrices of traces are used in order to find generators of the radical, and the matrices of traces are computed using Gröbner Bases; also, in [1] they use the traces to give a bound for the degree of the generators of the radical and use linear solving methods from there; in [21] they describe the computation of the radical using symmetric functions which are related to traces. One of the most commonly quoted method to compute radicals is to compute the projections $\mathcal{I} \cap \mathbb{K}[x_i]$ for each $i = 1, \ldots, m$ and then use univariate squarefree factorization (see for example [19, 30, 11, 22]). The advantage of the latter is that it can be generalized for higher dimensional ideals (see for example [29]). We note here that an advantage of the method using matrices of traces is that it behaves stably under perturbation of the roots of the input system, as was proved in [26]. Other methods to compute the radical of zero dimensional ideals include [28, 18, 32, 33, 34, 45]. Applications of computing the radical include [23], where they show how to compute the multiplicity structure of the roots of $\mathcal{I}$ once the radical is computed.

Methods for computing the matrix of traces directly from the generating polynomials of $\mathcal{I}$, without using multiplication matrices, include [14, 6] where they use Newton Sums, [8, 9, 10] where they use residues and [13] using resultants. Besides computing the radical of an ideal, matrices of traces have numerous applications mainly in real algebraic geometry [4, 41, 5], or in [42] where trace matrices are applied to find separating linear forms deterministically.

3. Ideals with Finitely Many Projective Roots

3.1. **The Gorenstein Case.** Some of the results of this subsection appeared in [24]. We included them here for completeness.

Let $\mathbf{f} = [f_1, \ldots, f_s]$ be a system of polynomials of degrees $d_1 \geq \cdots \geq d_s$ in $\mathbb{K}[\mathbf{x}]$, where $\mathbf{x} = [x_1, \ldots, x_m]$ and $\mathbb{K}$ is an arbitrary algebraically closed field. Let

$\mathcal{I}$ be the ideal generated by $f_1, \ldots, f_s$ in $\mathbb{K}[\mathbf{x}]$ and define $\mathcal{A} := \mathbb{K}[\mathbf{x}]/\mathcal{I}$. We assume throughout the paper that $\mathcal{A}$ is a finite dimensional vector space over $\mathbb{K}$ and let $\mathcal{A}^*$ denote the dual space of $\mathcal{A}$.

Let us first recall the definition of a Gorenstein algebra (c.f. [31, 43, 17, 35]). Note that these algebras are also referred to as Frobenius in the literature, see for example [2].

Definition 3.1. *A finite dimensional $\mathbb{K}$-algebra $\mathcal{A}$ is Gorenstein (over $\mathbb{K}$) if there exists a nondegenerate $\mathbb{K}$-bilinear form $B(x, y)$ on $\mathcal{A}$ such that*

$$B(ab, c) = B(a, bc) \text{ for every } a, b, c \in \mathcal{A}.$$

Note that this is equivalent to the fact that $\mathcal{A}$ and $\mathcal{A}^*$ are isomorphic as $\mathcal{A}$ modules. It is also equivalent to the existence of a $\mathbb{K}$-linear function $\Lambda : \mathcal{A} \to \mathbb{K}$ such that the bilinear form $B(a, b) := \Lambda(ab)$ is nondegenerate on $\mathcal{A}$.

Assumption 3.2. *Throughout this subsection we assume that $\mathcal{A}$ is Gorenstein. Furthermore, we also assume that we have a bound $\delta > 0$ and $0 \leq k \leq \delta$ such that*

$$\dim_{\mathbb{K}} \mathbb{K}[\mathbf{x}]_k/\langle f_1, \ldots, f_s\rangle_\delta \cap \mathbb{K}[\mathbf{x}]_k = \dim_{\mathbb{K}} \mathbb{K}[\mathbf{x}]_k/\langle f_1, \ldots, f_s\rangle_d \cap \mathbb{K}[\mathbf{x}]_k \tag{1}$$

for all $d \geq \delta$. Here $\mathbb{K}[\mathbf{x}]_k := \{p \in \mathbb{K}[\mathbf{x}] \ : \ \deg(p) \leq k\}$ and

$$\langle f_1, \ldots, f_s\rangle_d := \left\{ \sum_i f_i q_i \ : \ \deg(q_i) \leq d - d_i \right\}. \tag{2}$$

Theorem 3.3. *Assume that δ and k satisfy the condition (1). Then*

$$\dim_{\mathbb{K}}(\mathcal{A}) = \dim_{\mathbb{K}} \mathbb{K}[\mathbf{x}]_k/\langle f_1, \ldots, f_s\rangle_\delta \cap \mathbb{K}[\mathbf{x}]_k.$$

Proof. Assume that δ and k satisfy the condition (1) and let $B := [b_1, \ldots, b_N]$ be a basis for $\mathbb{K}[\mathbf{x}]_k/\langle f_1, \ldots, f_s\rangle_\delta \cap \mathbb{K}[\mathbf{x}]_k$. Taking pre-images, we can assume that $b_1, \ldots, b_N$ are polynomials in $\mathbb{K}[\mathbf{x}]_k$. We claim that B is a basis for $\mathcal{A} = \mathbb{K}[\mathbf{x}]/\langle f_1, \ldots, f_s\rangle$. Since $\langle f_1, \ldots, f_s\rangle_\delta \subseteq \langle f_1, \ldots, f_s\rangle_d$ if $\delta \leq d$, B is clearly a generator set for $\mathcal{A}$. On the other hand, assume that B is not linearly independent in $\mathcal{A}$, i.e. there exist $c_1, \ldots, c_N \in \mathbb{K}$ such that $\sum_{i=1}^N c_i b_i$ is in $\langle f_1, \ldots, f_s\rangle$. Then there exists $d \geq \delta$ such that $\sum_{i=1}^N c_i b_i \in \langle f_1, \ldots, f_s\rangle_d$. But $\sum_{i=1}^N c_i b_i$ is also in $\mathbb{K}[\mathbf{x}]_k$, so B is linearly dependent in $\mathbb{K}[\mathbf{x}]_k/\langle f_1, \ldots, f_s\rangle_d \cap \mathbb{K}[\mathbf{x}]_k$, which contradicts condition (1). □

We have the following theorems giving bounds for δ in the case when $\mathbf{f}$ has finitely many projective roots. First we assume that $\mathbf{f}$ has no roots at infinity.

Theorem 3.4. *Let $\mathbf{f} = [f_1, \ldots, f_s]$ be a system of polynomials of degrees $d_1 \geq \cdots \geq d_s$ in $\mathbb{K}[\mathbf{x}]$. Assume that the corresponding system of homogenous polynomials $f_1^h, \ldots, f_s^h$ has finitely many projective common roots in $\mathbb{P}^m_{\mathbb{K}}$. Assume further that $f_1, \ldots, f_s$ have no common roots at infinity. Then:*

1. *If $s = m$ then for $\delta = k := \sum_{i=1}^m (d_i - 1)$ condition (1) is satisfied. Furthermore, in this case $\mathcal{A}$ is always Gorenstein.*
2. *If $s > m$ then for $\delta = k := \sum_{i=1}^{m+1} d_i - m$ condition (1) is satisfied.*

Proof. For the first assertion let $\mathbf{f}^h = [f_1^h, \ldots, f_m^h]$ be the homogenization of $\mathbf{f}$ using a new variable x_{m+1}. Using our assumption that $\mathbf{f}^h$ has finitely many roots in $\mathbb{P}^m_{\mathbb{K}}$ and $s = m$, one can see that $(\mathbf{f}^h)$ is a regular sequence in $R := \mathbb{K}[x_1, \ldots, x_m, x_{m+1}]$.

Define the graded ring $B := R/\langle \mathbf{f}^h \rangle$. Following the approach and notation in [44], we can now calculate the Hilbert series of B, defined by $H(B,\lambda) = \sum_d \mathcal{H}_B(d)\lambda^d$, where $\mathcal{H}_B$ is the Hilbert function of B. We have

$$H(R,\lambda) = \frac{H(B,\lambda)}{(1-\lambda^{d_1})\cdots(1-\lambda^{d_m})},$$

and using the simple fact that

$$H(R,\lambda) = \frac{1}{(1-\lambda)^{m+1}}$$

we obtain that

$$\begin{aligned} H(B,\lambda) &= \frac{(1+\lambda+\cdots+\lambda^{d_1-1})\cdots(1+\lambda+\cdots+\lambda^{d_m-1})}{(1-\lambda)} \\ &= g(\lambda)(1+\lambda+\ldots), \end{aligned}$$

where

$$g(\lambda) = (1+\lambda+\cdots+\lambda^{d_1-1})\cdots(1+\lambda+\cdots+\lambda^{d_m-1}).$$

This implies that the Hilbert function

$$\mathcal{H}_B(\delta) = \mathcal{H}_B(\delta+1) = \mathcal{H}_B(\delta+2) = \ldots$$

Note that dehomogenization induces a linear isomorphism $B_d \to \mathbb{K}[\mathbf{x}]_d/\langle f_1,\ldots,f_m\rangle_d$, where B_d stands for the degree d homogeneous part of B. From this, using that there are no common roots at infinity, we infer that for $d \geq \delta$ $\dim_{\mathbb{K}} \mathbb{K}[\mathbf{x}]_d/\langle f_1,\ldots,f_m\rangle_d = \dim_{\mathbb{K}} \mathcal{A} = N$, which implies (1).

Note that the common value $N = \mathcal{H}_B(\delta)$ is the sum of the coefficients of g, which is

$$g(1) = \prod_{i=1}^{m} d_i.$$

To prove that $\mathcal{A}$ is Gorenstein, we cite [17, Proposition 8.25, p. 221] where it is proved that if $f_1,\ldots,f_m$ is an affine complete intersection then the Bezoutian $B_{1,f_1,\ldots,f_m}$ defines an isomorphism between $\mathcal{A}^*$ and $\mathcal{A}$.

To prove the second assertion we note that [37, Theorem 3.3] implies that

$$\dim_{\mathbb{K}} B_\delta = \dim_{\mathbb{K}} B_{\delta+1} = \ldots.$$

From here we obtain (1) as in the Case 1. □

The following theorem generalizes the previous result for systems which may have roots at infinity.

Theorem 3.5. *Let $\mathbf{f} = [f_1,\ldots,f_s]$ be a system of polynomials of degrees $d_1 \geq \cdots \geq d_s$ in $\mathbb{K}[\mathbf{x}]$. Assume that the corresponding system of homogenous polynomials $f_1^h,\ldots,f_s^h$ has finitely many projective common roots in $\mathbb{P}^m_{\mathbb{K}}$ and let $\mathcal{J} := \langle f_1^h,\ldots,f_s^h\rangle$ be the ideal they generate in $R := \mathbb{K}[x_1,\ldots,x_n,x_{n+1}]$. Then:*

1. *If $s = m$ then for $k := \sum_{i=1}^m (d_i-1)$ and $\delta := k+1$ condition (1) is satisfied.*
2. *If $s > m$ then for $k := \sum_{i=1}^{m+1} d_i - m$ and $\delta := k+1$ condition (1) is satisfied.*

Proof. Assume that $\mathbf{f}$ has N affine roots and N' roots at infinity, counted with multiplicity. In this proof only, for a homogeneous ideal $J \subseteq R$, J_t denotes the elements of J of degree *equal* to t, abusing the notation. By the proof of Theorem 3.4 and [37], we have that for k defined above (in both cases) and for all $d \geq 0$,

$R_{k+d}/\mathcal{J}_{k+d}$ (resp. $R_{k+d}/(\mathcal{J}+(x_{m+1}))_{k+d}$) is of dimension $N+N'$ (resp. N'). Consider the exact sequence

$$0 \to (\mathcal{J} : x_{m+1})_k/\mathcal{J}_k \to R_k/\mathcal{J}_k \stackrel{\mathcal{M}_{m+1}}{\longrightarrow} R_{k+1}/\mathcal{J}_{k+1} \to R_{k+1}/(\mathcal{J}+x_{m+1})_{k+1} \to 0$$

where $\mathcal{M}_{m+1}$ is the multiplication by x_{m+1}. Using the relation on the dimensions of the vector spaces of this exact sequence, we deduce that

$$\dim_{\mathbb{K}}((\mathcal{J} : x_{m+1})_k/\mathcal{J}_k) = (N+N') - (N+N') + N' = N'.$$

Thus we can choose a basis $[b_1^h, \ldots, b_{N+N'}^h]$ of $R_k/\mathcal{J}_k$ such that $b_1^h, \ldots, b_{N'}^h \in (\mathcal{J} : x_{m+1})_k$. Moreover, we can even assume that $b_{N'+1}^h, \ldots, b_{N+N'}^h \in \langle x_{m+1}\rangle_k$, since

$$\operatorname{span}(b_1^h, \ldots, b_{N+N'}^h) = \operatorname{span}(b_1^h, \ldots, b_{N'}^h) + \langle x_{m+1}\rangle_k \ + \ \mathcal{J}_k.$$

If $x_{m+1}^k \in (\mathcal{J} : x_{m+1})_k$ then $x_{m+1}^{k+1} \in \mathcal{J}$, all the roots are at infinity, $N = 0$, and $(\mathcal{J} : x_{m+1})_k = R_k$ modulo $\mathcal{J}_k$ which shows that $x_{m+1}R_k \subset \mathcal{J}_{k+1}$. After dehomogeneization all polynomials of degree $\leq k$ are in $\langle f_1, \ldots, f_s\rangle_{k+1}$. So condition (1) is satisfied for $\delta = k+1$.

Suppose now that $x_{m+1}^k \notin (\mathcal{J} : x_{m+1})_k$, so that we can take $b_{N'+1}^h = x_{m+1}^k$.

As $x_{m+1}(\mathcal{J} : x_{m+1}) \subset \mathcal{J}$, we deduce that $x_{m+1}\, b_1^h = \cdots = x_{m+1}\, b_{N'}^h = 0$ modulo $\mathcal{J}_{k+1}$ and that

$$\dim_{\mathbb{K}} \left(\operatorname{span}\left(x_{m+1}\, b_1^h, \ldots, x_{m+1}\, b_{N+N'}^h\right)/\mathcal{J}_{k+1}\right) \leq N.$$

As we have

$$R_k = \operatorname{span}\left(b_1^h, \ldots, b_{N+N'}^h\right) + \mathcal{J}_k$$

and $x_{m+1}\, b_i^h \in \mathcal{J}_{k+1}$ for $1 \leq i \leq N'$, we deduce that

$$x_{m+1}\, R_k = \operatorname{span}\left(x_{m+1}b_{N'+1}^h, \ldots, x_{m+1}b_{N+N'}^h\right) \ + \ \mathcal{J}_{k+1}.$$

After dehomogeneization, we obtain a family $B = [b_{N'+1}, ..., b_{N+N'}]$ of N elements of degree $< k$ (because $b_i^h \in \langle x_{m+1}\rangle_k$ for $N' < i \leq N+N'$) such that

$$\mathbb{K}[x_1, \ldots, x_m]_k = \operatorname{span}(B) + \langle f_1, \ldots, f_s\rangle_{k+1} \cap \mathbb{K}[x_1, \ldots, x_m]_k$$

(here we use the notation of Assumption 3.2 again). Thus any polynomial of degree $\leq k$ can be rewritten, modulo $\langle f_1, \ldots, f_s\rangle_{k+1}$, as a linear combination of elements in B of degree $< k$. As B contains 1 since $b_{N'+1}^h = x_{m+1}^k$, this shows that B is a generating set of $\mathcal{A}$. As $\mathcal{A}$ is of dimension N, B is in fact a basis of $\mathcal{A}$, and thus $\delta := k+1$ and k satisfy the conditions in (1). □

Remark 3.6. *Note that in general*

$$\langle f_1, \ldots, f_s\rangle \cap \mathbb{K}[\mathbf{x}]_d \ \neq \langle f_1, \ldots, f_s\rangle_d,$$

where $\langle f_1, \ldots, f_s\rangle_d$ was defined in (2). Inequality can happen when the system has a root at infinity, for example, if $f_1 = x+1$, $f_2 = x$ then $\langle f_1, f_2\rangle \cap \mathbb{K}[\mathbf{x}]_0 = \mathbb{K}$ but $\langle f_1, f_2\rangle_0 = \{0\}$. However, using the homogenization $f_1^h, \ldots, f_s^h$, the degree d part of the homogenized ideal is always equal to the space spanned by the multiples of $f_1^h, \ldots, f_s^h$ of degree d. The above example also demonstrates that $\dim \mathcal{A}$ is not always the same as $\dim \mathbb{K}[\mathbf{x}]_d/\langle f_1, \ldots, f_s\rangle_d$ even for large d, because above $\dim \mathcal{A} = 0$ but $\dim \mathbb{K}[x,y]_d/\langle f_1, f_2\rangle_d = 1$ for all $d \geq 0$.

Definition 3.7. *Let $N := \dim_{\mathbb{K}}(\mathcal{A})$ and fix $B = [b_1, \ldots, b_N]$ a monomial basis for $\mathcal{A}$ such that $\deg(b_i) \leq k$ for all $i = 1, \ldots, N$. We define D to be the maximum degree of the monomials in B. Thus $D \leq k \leq \delta$.*

Next we will define Sylvester and Macaulay type resultant matrices for $f_1, \dots f_s$.

Definition 3.8. *Define*

$$\Delta := \max(\delta - 1, 2D)$$

where δ and D are defined in Assumption 3.2 and Definition 3.7.

Let $\mathrm{Syl}_{\Delta+1}(\mathbf{f})$ *be the transpose matrix of the linear map*

$$\begin{aligned} \bigoplus_i \mathbb{K}[\mathbf{x}]_{\Delta-d_i+1} &\longrightarrow \mathbb{K}[\mathbf{x}]_{\Delta+1} \\ (g_1, \dots, g_s) &\mapsto \sum_{i=1}^{s} f_i g_i \end{aligned} \tag{3}$$

written in the monomial bases. So, in our notation, $\mathrm{Syl}_{\Delta+1}(\mathbf{f})$ *will have rows which correspond to all polynomials $f_i x^\alpha$ of degree at most Δ.*

Let $\mathrm{Mac}_\Delta(\mathbf{f})$ *be the matrix with rows corresponding to a basis of $\langle f_1, \dots, f_s\rangle_{\Delta+1} \cap \mathbb{K}[\mathbf{x}]_\Delta$, obtained by eliminating coefficients of terms of degree $\Delta+1$ in the matrix* $\mathrm{Syl}_{\Delta+1}(\mathbf{f})$ *using Gaussian elimination, and then taking a maximal linearly independent set among the eliminated rows.*

Remark 3.9. *In the case where $s = m$, for generic $\mathbf{f}$ with no roots at infinity, we can directly construct* $\mathrm{Mac}_\Delta(\mathbf{f})$ *by taking the restriction of the map (3) to*

$$\bigoplus_{i=1}^{m} \mathcal{S}_i(\Delta) \longrightarrow \mathbb{K}[\mathbf{x}]_\Delta$$

where $\mathcal{S}_i(\Delta) = \mathrm{span}\{\mathbf{x}^\alpha : |\alpha| \le \Delta - d_i, \forall j < i,\, \alpha_j < d_j\}$.

Here $\mathrm{Mac}_\Delta(\mathbf{f})$ *is a submatrix of the classical Macaulay matrix of the homogenization of $\mathbf{f}$ and some f^h_{m+1}, where f^h_{m+1} is any homogeneous polynomial of degree $\Delta - \delta$: we only take the rows corresponding to the polynomials in $\mathbf{f}$. Since the Macaulay matrix is generically non-singular,*
$\mathrm{Mac}_\Delta(\mathbf{f})$ *will also be generically full rank.*

Note that with our assumption that $f_1, \dots, f_m$ has no roots at infinity, we have that $\mathrm{Mac}_\Delta(\mathbf{f})$ *has column* corank $\dim \mathcal{A} = \prod_{i=1}^m d_i$.

Since $\Delta \ge \delta - 1$, by Assumption 3.2 and Theorem 3.5, the corank of $\mathrm{Mac}_\Delta(\mathbf{f}) = N$, where N is the dimension of $\mathcal{A}$. Also, we can assume that the first columns of $\mathrm{Mac}_\Delta(\mathbf{f})$ correspond to a basis B of $\mathcal{A}$.

Fix an element

$$\mathbf{y} = [y_\alpha : \alpha \in \mathbb{N}^m,\ |\alpha| \le \Delta]^T$$

of the nullspace $\mathrm{Null}(\mathrm{Mac}_\Delta(\mathbf{f}))$, i.e. $\mathrm{Mac}_\Delta(\mathbf{f}) \cdot \mathbf{y} = 0$.

Definition 3.10. *Let $B = [b_1, \dots, b_N]$ be the basis of $\mathcal{A}$ as above, consisting of monomials of degree at most D. Using $\mathbf{y}$ we can define $\Lambda_{\mathbf{y}} \in \mathcal{A}^*$ by $\Lambda_{\mathbf{y}}(g) := \sum_{\mathbf{x}^\alpha \in B} y_\alpha g_\alpha$, where $g = \sum_{\mathbf{x}^\alpha \in B} g_\alpha \mathbf{x}^\alpha \in \mathcal{A}$. Note that every $\Lambda \in \mathcal{A}^*$ can be defined as $\Lambda_{\mathbf{y}}$ for some $\mathbf{y} \in \mathrm{Null}(\mathrm{Mac}_\Delta(\mathbf{f}))$ or more generally with an element of $\mathbb{K}[\mathbf{x}]^*$ which vanishes on the ideal $\mathcal{I}$.*

Define the moment matrix $\mathfrak{M}_B(\mathbf{y})$ *to be the $N \times N$ matrix given by*

$$\mathfrak{M}_B(\mathbf{y}) = [y_{\alpha+\beta}]_{\alpha,\beta},$$

where α and β run through the exponents of the monomials in B. Note that $\mathfrak{M}_B$ is only a submatrix of the usual notion of moment matrix, see for example [12].

For $p \in \mathcal{A}$, we define the linear function $p \cdot \Lambda \in \mathcal{A}^*$ as $p \cdot \Lambda(g) := \Lambda(pg)$ for all $g \in \mathcal{A}$.

Remark 3.11. *If one considers a linear function Λ on $\mathcal{A}$, such that the bilinear form $(x, y) \mapsto \Lambda(xy)$ is nondegenerate on $\mathcal{A}$, then the moment matrix corresponding to this Λ will be the one whose (i, j)-th entry is just $\Lambda(b_i b_j)$. Moreover, for $g, h \in \mathcal{A}$*

$$\Lambda_{\mathbf{y}}(gh) = \operatorname{coeff}_B(g)^T \cdot \mathfrak{M}_B(\mathbf{y}) \cdot \operatorname{coeff}_B(h)$$

where $\operatorname{coeff}_B(p)$ denotes the vector of coefficients of $p \in \mathcal{A}$ in the basis B.

The following proposition is a simple corollary of [35, Prop 3.3 and Cor. 3.1].

Proposition 3.12. *Let $\mathbf{y}$ be a random element of the vector space $\operatorname{Null}(\operatorname{Mac}_\Delta(\mathbf{f}))$. With high probability, $\mathfrak{M}_B(\mathbf{y})$ is non-singular.*

Remark 3.13. *Using the above proposition, one can detect whether the algebra $\mathcal{A}$ is not Gorenstein with high probability by simply computing the rank of $\mathfrak{M}_B(\mathbf{y})$ for (perhaps several) random elements $\mathbf{y}$ in $\operatorname{Null}(\operatorname{Mac}_\Delta(\mathbf{f}))$.*

Remark 3.14. *By* [35, Theorem 2.6 and Lemma 3.2] *one can extend $\mathbf{y}$ to $\tilde{\mathbf{y}} \in \mathbb{K}^{\mathbb{N}^m}$ such that the infinite moment matrix $\mathfrak{M}(\tilde{\mathbf{y}}) := [\tilde{y}_{\alpha+\beta}]_{\alpha,\beta\in\mathbb{N}^m}$ has the same rank as $\mathfrak{M}_B(\mathbf{y})$ and the columns of $\mathfrak{M}(\tilde{\mathbf{y}})$ vanish on all the elements of the ideal $\mathcal{I}$.*

Next we define a basis dual to $B = [b_1, \ldots, b_N]$ with respect to the moment matrix $\mathfrak{M}_B(\mathbf{y})$. Using this dual basis we also define a polynomial J which is in some sense a generalization of the Jacobian of a well-constrained polynomial system.

Definition 3.15. *From now on we fix $\mathbf{y} \in \operatorname{Null}(\operatorname{Mac}_\Delta(\mathbf{f}))$ such that $\mathfrak{M}_B(\mathbf{y})$ is invertible and we will denote by Λ the corresponding element $\Lambda_{\mathbf{y}} \in \mathcal{A}^*$. We define*

$$\mathfrak{M}_B^{-1}(\mathbf{y}) =: [c_{ij}]_{i,j=1}^N.$$

Let $b_i^* := \sum_{j=1}^N c_{ji} b_j$. Then $[b_1^*, \ldots, b_N^*]$ corresponds to the columns of the inverse matrix $\mathfrak{M}_B^{-1}(\mathbf{y})$ and they also form a basis for $\mathcal{A}$. Note that we have $\Lambda(b_i b_j^*) = 1$, if $i = j$, and 0 otherwise.

Define the generalized Jacobian *by*

$$J := \sum_{i=1}^N b_i b_i^* \mod \mathcal{I} \tag{4}$$

expressed in the basis $B = [b_1, \ldots, b_N]$ of $\mathcal{A}$.

Remark 3.16. *Note that since $\sum_{i=1}^N b_i b_i^*$ has degree at most $2D$, and $\Delta \geq 2D$, we can use $\operatorname{Mac}_\Delta(\mathbf{f})$ to find its reduced form, which is J. Because of this reduction, we have that $\deg(J) \leq D \leq \delta$.*

Note that the notion of generalized Jacobian was also introduced in [2]*. Its name come from the fact that if $s = m$ and if Λ is the so called residue (c.f.* [17]*), then $\sum_{i=1}^N b_i b_i^* = J$ is the Jacobian of $f_1, \ldots, f_m$.*

We now recall the definition of the multiplication matrices and the matrix of traces as presented in [26].

Definition 3.17. *Let $p \in \mathcal{A}$. The multiplication matrix M_p is the transpose of the matrix of the multiplication map*

$$\begin{aligned} \mathcal{M}_p : \mathcal{A} &\longrightarrow \mathcal{A} \\ g &\mapsto pg \end{aligned}$$

written in the basis B.

The matrix of traces *is the $N \times N$ symmetric matrix:*

$$T = [Tr(b_i b_j)]_{i,j=1}^N$$

where $Tr(pq) := Tr(M_{pq})$, M_{pq} is the multiplication matrix of pq as an element in $\mathcal{A}$ in terms of the basis $B = [b_1, \ldots, b_N]$ and Tr indicates the trace of a matrix.

The next results relate the multiplication by J matrix to the matrix of traces T.

Proposition 3.18. *Let M_J be the multiplication matrix of J with respect to the basis B. We then have that*

$$M_J = [Tr(b_i b_j^*)]_{i,j=1}^N.$$

Proof. Let $\Lambda \in \mathcal{A}^*$ be as in Definition 3.15. For any $h \in \mathcal{A}$ we have that

$$\begin{aligned} & h = \sum_{j=1}^N \Lambda(h b_j) b_j^* = \sum_{j=1}^N \Lambda(h b_j^*) b_j \\ \Rightarrow \quad & h\, b_i = \sum_{j=1}^N \Lambda(h\, b_i\, b_j^*) b_j \Rightarrow M_h[j,i] = \Lambda(h\, b_i\, b_j^*) \\ \Rightarrow \quad & Tr(h) = \sum_{i=1}^N \Lambda(h\, b_i\, b_i^*) = \Lambda(h \sum_{i=1}^N b_i\, b_i^*). \end{aligned}$$

Since $J = \sum_{i=1}^N b_i^* b_i$ in $\mathcal{A}$, we have $Tr(h) = \Lambda(hJ)$. Therefore

$$M_J[j,i] = \Lambda(J\, b_i\, b_j^*) = Tr(b_i\, b_j^*)$$

□

Corollary 3.19.

$$M_J \cdot \mathfrak{M}_B(\mathbf{y}) = [Tr(b_i b_j)]_{i,j=1}^N = T,$$

or equivalently $J \cdot \Lambda = Tr$ in $\mathcal{A}^*$.

Proof. The coefficients of b_i^* in the basis $B = [b_1, \ldots, b_N]$ are the columns of $\mathfrak{M}_B^{-1}(\mathbf{y})$, which implies that

$$M_J = [Tr(b_i b_j^*)]_{i,j=1}^N = [Tr(b_i b_j)]_{i,j=1}^N \cdot \mathfrak{M}_B^{-1}(\mathbf{y}).$$

Therefore we have that $M_J \cdot \mathfrak{M}_B(\mathbf{y}) = [Tr(b_i b_j)]_{i,j=1}^N$. □

Finally, we prove that the matrix of traces T can be computed directly from the Macaulay matrix of $f_1, \ldots, f_s$ and J, without using the multiplication matrix M_J. First we need a lemma.

Lemma 3.20. *There exists a unique matrix $\mathfrak{R}_B(\mathbf{y})$ of size $|\mathrm{Mon}_{\leq}(\Delta) - B| \times |B|$ such that*

$$\mathrm{Mac}_\Delta(\mathbf{f}) \cdot \begin{array}{|c|}\hline \mathfrak{M}_B(\mathbf{y}) \\ \hline \mathfrak{R}_B(\mathbf{y}) \\ \hline \end{array} = 0$$

Proof. By our assumption that the first columns of $\mathrm{Mac}_\Delta(\mathbf{f})$ correspond to B we have

$$\begin{array}{|c|}\hline \mathrm{Mac}_\Delta(\mathbf{f}) \\ \hline \end{array} = \begin{array}{|c|c|}\hline \mathtt{B} & \mathtt{A} \\ \hline \end{array},$$

where the columns of B are indexed by the monomials in B. Note here that by Definition 3.8 and Assumption 3.2 the rows of $\mathrm{Mac}_\Delta(\mathbf{f})$ span $\mathcal{I}_{\Delta+1} \cap \mathbb{K}[\mathbf{x}]_\Delta$, and the monomials in B span the factor space $\mathbb{K}[\mathbf{x}]_\Delta/(\mathcal{I}_{\Delta+1} \cap \mathbb{K}[\mathbf{x}]_\Delta)$. These together imply that the (square) submatrix $\mathtt{A}$ is invertible.

Then

$$\begin{array}{|c|c|}\hline \mathtt{B} & \mathtt{A} \\ \hline \end{array} \cdot \begin{array}{|c|}\hline Id_{N\times N} \\ \hline -\mathtt{A}^{-1}\mathtt{B} \\ \hline \end{array} = 0$$

which implies that

$$\mathrm{Mac}_\Delta(\mathbf{f}) \cdot \begin{array}{|c|}\hline \mathfrak{M}_B(\mathbf{y}) \\ \hline \mathfrak{R}_B(\mathbf{y}) \\ \hline \end{array} = 0,$$

where $\mathfrak{R}_B(\mathbf{y}) = -\mathtt{A}^{-1}\mathtt{B} \cdot \mathfrak{M}_B(\mathbf{y})$. □

By construction, the column of $\mathfrak{M}_B(\mathbf{y})$ indexed by $b_j \in B$ corresponds to the values of $b_j \cdot \Lambda \in \mathcal{A}^*$ on $b_1, \ldots, b_N$. The same column in $\mathfrak{R}_B(\mathbf{y})$ corresponds to the values of $b_j \cdot \Lambda$ on the complementary set of monomials of $\mathrm{Mon}_{\leq}(\Delta)$. The column in the stacked matrix corresponds to the value of $b_j \cdot \Lambda$ on all the monomials in $\mathrm{Mon}_{\leq}(\Delta)$. To evaluate $b_j \cdot \Lambda(p)$ for a polynomial p of degree $\leq \Delta$, we simply compute the inner product of the coefficient vector of p with this column.

Definition 3.21. *Let $B = [b_1, \ldots, b_N]$ be the basis of $\mathcal{A}$ as above, and let $P \in \mathbb{K}[\mathbf{x}]$ be a polynomial of degree at most D.*

Define $\mathrm{Syl}_B(P)$ to be the matrix with rows corresponding to the coefficients of the polynomials $(b_1 P), \ldots, (b_N P)$ in the monomial basis $\mathrm{Mon}_{\leq}(\Delta)$ (we use here that $\deg(b_i) \leq D$, thus $\deg(b_i P) \leq 2D \leq \Delta$).

Furthermore, we assume that the monomials corresponding to the columns of $\mathrm{Syl}_B(P)$ are in the same order as the monomials corresponding to the columns of $\mathrm{Mac}_\Delta(\mathbf{f})$.

Theorem 3.22.

$$\boxed{\mathrm{Syl}_B(J)} \cdot \begin{array}{|c|}\hline \mathfrak{M}_B(\mathbf{y}) \\ \hline \mathfrak{R}_B(\mathbf{y}) \\ \hline \end{array} = [Tr(b_i b_j)]_{i,j=1}^N$$

Proof. Since the j-th column of the matrix

$$\begin{array}{|c|}\hline \mathfrak{M}_B(\mathbf{y}) \\ \hline \mathfrak{R}_B(\mathbf{y}) \\ \hline \end{array}$$

represents the values of $b_j \cdot \Lambda$ on all the monomials of degree less than or equal to Δ, and the i-th row of $\mathrm{Syl}_B(J)$ is the coefficient vector of $b_i J$, we have

$$\begin{aligned} \boxed{\mathrm{Syl}_B(J)} \cdot \begin{array}{|c|}\hline \mathfrak{M}_B(\mathbf{y}) \\ \hline \mathfrak{R}_B(\mathbf{y}) \\ \hline \end{array} &= [(b_j \cdot \Lambda)(b_i J)]_{i,j=1}^N \\ &= [\Lambda(J b_i b_j)]_{i,j=1}^N \\ &= [Tr(b_i b_j)]_{i,j=1}^N. \end{aligned}$$

□

We can now describe the algorithm to compute a set of multiplication matrices M_{x_i}, $i = 1, \ldots, m$ of the radical $\sqrt{\mathcal{I}}$ of $\mathcal{I}$ with respect to a basis of $\mathbb{K}[\mathbf{x}]/\sqrt{\mathcal{I}}$. To prove that the algorithm below is correct we need the following result from [26, Proposition 8.3] which is the consequence of the fact that the kernel of the matrix of traces corresponds to the radical of $\mathcal{A}$:

Proposition 3.23. *Let $\tilde{T}$ be a maximal non-singular submatrix of the matrix of traces T. Let r be the rank of $\tilde{T}$, and $\tilde{B} := [b_{i_1}, \ldots, b_{i_r}]$ be the monomials corresponding to the columns of $\tilde{T}$. Then $\tilde{B}$ is a basis of the algebra $\mathbb{K}[\mathbf{x}]/\sqrt{\mathcal{I}}$ and for each $k = 1, \ldots, m$, the solution M_{x_k} of the linear matrix equation*

$$\tilde{T} M_{x_k} = \tilde{T}_{x_k}$$

is the multiplication matrix of x_k for $\sqrt{\mathcal{I}}$ with respect to $\tilde{B}$. Here $\tilde{T}_{x_k}$ is the $r \times r$ submatrix of $[Tr(x_k b_i b_j)]_{i,j=1}^N$ with the same row and column indices as in $\tilde{T}$.

Algorithm 3.24 (Radical ideal using Macaulay matrices and traces)**.**
INPUT*: $\mathbf{f} = [f_1, \ldots, f_s] \in \mathbb{K}[\mathbf{x}]$ of degrees $d_1, \ldots, d_s$ generating an ideal $\mathcal{I}$ and $\delta > 0$ such that for $k := \delta - 1$ they satisfy the conditions in Assumption 3.2. An optional input is $D \leq \delta$, which by default is set to be δ.*

OUTPUT: *A basis* $\tilde{B}$ *for the factor algebra* $\mathbb{K}[\mathbf{x}]/\sqrt{\mathcal{I}}$ *and a set of multiplication matrices* $\{M_{x_i} | i = 1, \ldots, m\}$ *of* $\sqrt{\mathcal{I}}$ *with respect to the basis* $\tilde{B}$.

(1) *Compute* $\mathrm{Mac}_\Delta(\mathbf{f})$ *for* $\Delta := \max(2D, \delta - 1)$ *as in Definition 3.8.*
(2) *Compute a basis* B *of* $\mathbb{K}[\mathbf{x}]_\Delta/(\langle \mathbf{f} \rangle_{\Delta+1} \cap \mathbb{K}[\mathbf{x}]_\Delta)$ *such that the polynomials in* B *have degrees at most* D. *Let* $B = [b_1, \ldots, b_N]$.
(3) *Compute a random combination* $\mathbf{y}$ *of the elements of a basis of* $Null(\mathrm{Mac}_\Delta(\mathbf{f}))$.
(4) *Compute the moment matrix* $\mathfrak{M}_B(\mathbf{y})$ *defined in Definition 3.10 and* $\mathfrak{R}_B(\mathbf{y})$ *defined in Lemma 3.20.*
(5) *Compute* $\mathfrak{M}_B^{-1}(\mathbf{y})$ *and the basis* $[b_1^*, \ldots, b_N^*]$ *defined in Definition 3.15.*
(6) *Compute* $J = \sum_{i=1}^N b_i b_i^*$ *mod* $\mathcal{I}$ *using* $\mathrm{Mac}_\Delta(\mathbf{f})$.
(7) *Compute* $\mathrm{Syl}_B(J)$ *and* $\mathrm{Syl}_B(x_k J)$ *for* $k = 1, \ldots, m$ *defined in Definition 3.21.*
(8) *Compute*

$$T = [Tr(b_i b_j)]_{i,j=1}^N = \boxed{\mathrm{Syl}_B(J)} \cdot \begin{array}{|c|}\hline \mathfrak{M}_B(\mathbf{y}) \\ \hline \mathfrak{R}_B(\mathbf{y}) \\ \hline \end{array}$$

and

$$T_{x_k} := [Tr(x_k b_i b_j)]_{i,j=1}^N = \boxed{\mathrm{Syl}_B(x_k J)} \cdot \begin{array}{|c|}\hline \mathfrak{M}_B(\mathbf{y}) \\ \hline \mathfrak{R}_B(\mathbf{y}) \\ \hline \end{array} \quad \text{for } k = 1, \ldots, m.$$

(9) *Compute* $\tilde{T}$, *a maximal non-singular submatrix of* T. *Let* r *be the rank of* $\tilde{T}$, *and* $\tilde{B} := [b_{i_1}, \ldots, b_{i_r}]$ *be the monomials corresponding to the columns of* $\tilde{T}$.
(10) *For each* $k = 1, \ldots, m$ *solve the linear matrix equation* $\tilde{T} M_{x_k} = \tilde{T}_{x_k}$, *where* $\tilde{T}_{x_k}$ *is the submatrix of* T_{x_k} *with the same row and column indices as in* $\tilde{T}$.

Remark 3.25. *Since the bound given in Theorem 3.5 might be too high, it seems reasonable to design the algorithm in an iterative fashion, similarly to the algorithms in* [35, 36, 46]*, in order to avoid nullspace computations for large matrices. The bottleneck of our algorithm is doing computations with* $\mathrm{Mac}_\Delta(\mathbf{f})$, *since its size exponentially increases as* Δ *increases.*

Remark 3.26. *Note that if* $s = m$ *then we can use the conventional Jacobian of* $f_1, \ldots, f_m$ *in the place of* J, *and any* $|\mathrm{Mon}_{\leq}(\Delta)| \times |B|$ *matrix* X *such that it has full rank and* $\mathrm{Mac}_\Delta(\mathbf{f}) \cdot X = \mathbf{0}$ *in the place of*

$$\begin{array}{|c|}\hline \mathfrak{M}_B(\mathbf{y}) \\ \hline \mathfrak{R}_B(\mathbf{y}) \\ \hline \end{array}.$$

Even though this way we will not get matrices of traces, a system of multiplication matrices of the radical $\sqrt{\mathcal{I}}$ can still be recovered: if $\tilde{Q}$ denotes a maximal non-singular submatrix of $\mathrm{Syl}_B(J)\cdot X$, and $\tilde{Q}_{x_k}$ is the submatrix of $\mathrm{Syl}_B(x_kJ)\cdot X$ with the same row and column indices as in $\tilde{Q}$, then the solution M_{x_k} of the linear matrix equation $\tilde{Q}M_{x_k}=\tilde{Q}_{x_k}$ gives the same multiplication matrix of $\sqrt{\mathcal{I}}$ w.r.t. the same basis $\tilde{B}$ as the above Algorithm.

Remark 3.27. *As M_{x_k} is the transpose matrix of multiplication by x_k modulo the radical ideal $\sqrt{\mathcal{I}}$, its eigenvectors are (up to a non-zero scalar) the evaluation at the roots ζ of $\mathcal{I}$ (see* [38, 17] *for more details). The vector which represents this evaluation at ζ in the dual space $\mathcal{A}^*$ is the vector of values of $[b_1,\dots,b_N]$ at ζ. To obtain these vectors, we solve the generalized eigenvalue problem $(\tilde{T}_{x_k}-z\tilde{T})\,w=0$ and compute $v=\tilde{T}\,w$. The vectors v will be of the form $[b_1(\zeta),\dots,b_N(\zeta)]$ for ζ a root of $\mathcal{I}$. If $b_1=1, b_2=x_1,\dots,b_{m+1}=x_m$, we can read directly the coordinates of ζ from this vector.*

3.2. **The Non-Gorenstein Case.** We will now consider the case where $\mathcal{A}$ is not Gorenstein. The main idea of the algorithm is the same as in the Gorenstein case, except we will obtain as an output a matrix of traces with respect to an algebra $\mathcal{B}$ which is a maximal Gorenstein factor of $\mathcal{A}$. This will still allow us to compute the multiplication matrices of the radical of $\mathcal{I}$ since the maximal non-singular submatrix of the trace matrix corresponding to $\mathcal{B}$ is the same as that of the trace matrix of $\mathcal{A}$. First we will need some results to define a maximal Gorenstein factor $\mathcal{B}$ of $\mathcal{A}$ from a random element of the nullspace of $\mathrm{Mac}_\Delta(\mathbf{f})$.

Let $\mathbb{K}$ be an arbitrary algebraically closed field. All algebras we consider will be finite dimensional commutative $\mathbb{K}$-algebras. A local $\mathbb{K}$-algebra here is an $\mathbb{K}$-algebra $\mathcal{B}$, with unique maximal ideal (which we denote by $\mathcal{M}$) such that $\mathcal{B}/\mathcal{M}$ is isomorphic to $\mathbb{K}$. Note that due to the fact that $\mathbb{K}$ is algebraically closed, no other residue class field is possible.

Definition 3.28. *Fix $\mathbf{y}\in\mathrm{Null}(\mathrm{Mac}_\Delta(\mathbf{f}))$ and let $\Lambda:=\Lambda_{\mathbf{y}}\in\mathcal{A}^*$ defined as in Definition 3.10. We define*

$$\mathcal{R}(\Lambda):=\{a\in A,\Lambda(ab)=0 \text{ holds for all } b\in A\}.$$

Note that $\mathcal{R}(\Lambda)=0$ iff $\Lambda(xy)$ is a nondegenerate bilinear form on $\mathcal{A}$. Also, an easy calculation shows that $\mathcal{R}(\Lambda)$ is an ideal in $\mathcal{A}$.

Define

$$\mathcal{B}:=\mathcal{A}/\mathcal{R}(\Lambda).$$

First we need the following technical lemmas.

Lemma 3.29. *$\mathcal{R}(\Lambda)$ is an ideal of $\mathcal{A}$, in fact, it is the largest ideal of $\mathcal{A}$ which is in* $\ker(\Lambda)$.

Here $\ker(\Lambda)$ *is the set of elements $a\in\mathcal{A}$, such that $\Lambda(a)=0$.*

Proof. An easy calculation shows that $\mathcal{R}(\Lambda)$ is an ideal. Clearly it is in $\ker(\Lambda)$. Conversely, if $\mathcal{J}$ is an ideal of $\mathcal{A}$ which is in $\ker(\Lambda)$, then $\mathcal{J}$ is in $\mathcal{R}(\Lambda)$. Note that the sum of ideals is an ideal again, hence there exists a unique largest ideal of $\mathcal{A}$ which is a subset of $\ker(\Lambda)$. □

Lemma 3.30. *(Structure Theorem on Artininan Rings, specialized to our setting, see Atiyah-MacDonald) A $\mathbb{K}$-algebra $\mathcal{B}$ is the direct product of finitely many local $\mathbb{K}$-algebras.*

Lemma 3.31. *Suppose that the $\mathbb{K}$-algebra $\mathcal{B}$ is the direct product of the local $\mathbb{K}$-algebras $\mathcal{B}_i, (i = 1, \ldots, k)$. Then $\mathcal{B}$ is Gorenstein iff all the $\mathcal{B}_i$ are Gorenstein.*

Proof. Note that the $\mathcal{B}_i$ can be viewed as ideals of $\mathcal{B}$, moreover $\mathcal{B}$ is the direct sum of these (as $\mathbb{K}$-subspaces).

Let Λ be a linear function on $\mathcal{B}$ such that the form $\Lambda(xy)$ is nondegenerate. Then the resctriction Λ_i of Λ on $\mathcal{B}_i$ will define a nondegenerate bilinear form on $\mathcal{B}_i$. Let a be a nonzero element of $\mathcal{B}_i$. Then there exists a $b \in \mathcal{B}$ such that $\Lambda(ab) \neq 0$. Write now b as $b = \sum b_j$, with $b_j \in \mathcal{B}_j$ for $(j = 1, \ldots, k)$. Note that we have $ab_j = 0$ if $j \neq i$, hence

$$0 \neq \Lambda(ab) = \Lambda(ab_i) = \Lambda_i(ab_i),$$

hence $\Lambda_i(xy)$ is nondegenerate.

Conversely, assume that we have linear functions $\Lambda_i : \mathcal{B}_i \to \mathbb{K}$ such that the form $\Lambda_i(xy)$ is nondegenerate on $\mathcal{B}_i$. We define Λ as follows. Let $a \in \mathcal{B}$ with $a = a_1 + \cdots + a_k$, where $a_i \in \mathcal{B}_i$. Note that a uniquely determines the a_i, and the map $a \mapsto a_i$ is an $\mathbb{K}$-algebra morphism from $\mathcal{B}$ to $\mathcal{B}_i$. This implies that $\Lambda(a) := \Lambda_1(a_1)+\cdots+\Lambda_k(a_k)$ is a correct definition and Λ is a linear function on $\mathcal{B}$. Moreover, it is easily seen that $\Lambda(xy)$ is nondegenerate. □

Lemma 3.32. *Λ induces a linear function Λ' on the factor $\mathcal{B} = \mathcal{A}/\mathcal{R}(\Lambda)$. For the function Λ' on $\mathcal{B}$ we have that $\mathcal{R}(\Lambda') = 0$, hence $\mathcal{B}$ is Gorenstein.*

Proof. We set $\Lambda'(a + \mathcal{R}(\Lambda)) = \Lambda(a)$. It is routine to check that Λ' is a correctly defined linear function on $\mathcal{B}$. Suppose that $a + \mathcal{R}(\Lambda)$ is in $\mathcal{R}(\Lambda')$. Then $\Lambda(ac) = 0$ holds for every $c \in \mathcal{A}$, hence $a \in \mathcal{R}(\Lambda)$ and therefore $a + \mathcal{R}(\Lambda) = 0$ in $\mathcal{B}$. □

Lemma 3.33. *Every Gorenstein factor $\mathcal{B}$ of an $\mathbb{K}$-algebra $\mathcal{A}$ can be obtained via a linear function Λ on $\mathcal{A}$, as outlined by Lemma 3.32.*

Proof. Let $\mathcal{B} = \mathcal{A}/\mathcal{J}$ be a Gorenstein factor of $\mathcal{A}$. Let Λ' be a linear function on $\mathcal{B}$ with $\mathcal{R}(\Lambda') = 0$. We define Λ on $\mathcal{A}$ as follows. Let $\Lambda(a) := \Lambda'(a + \mathcal{J})$ for $a \in \mathcal{A}$. Clearly Λ will be a linear function on $\mathcal{A}$. Let $a \in \mathcal{A}$ such that $\Lambda(ab) = 0$ for every $b \in \mathcal{A}$. Then $0 = \Lambda(ab) = \Lambda'(ab + \mathcal{J}) = \Lambda'((a + \mathcal{J})(b + \mathcal{J}))$, giving that $a + \mathcal{J} \in \mathcal{R}(\Lambda')$, hence $a \in \mathcal{J}$. This shows that $\mathcal{R}(\Lambda) \subseteq \mathcal{J}$. The reverse containment is immediate, therefore $\mathcal{R}(\Lambda) = \mathcal{J}$. Now one can directly check that Λ' is obtained from Λ via the factor construction of Lemma 3.32. □

Lemma 3.34. *Let $\mathcal{A}$ be an $\mathbb{K}$-algebra. Then the maximal dimensional Gorenstein factors of $\mathcal{A}$ are obtained as follows: from every direct factor $\mathcal{A}_i$ (this is local) factor out an ideal $\mathcal{J}_i$ so that $\mathcal{A}_i/\mathcal{J}_i$ is a maximal Gorenstein factor of $\mathcal{A}_i$.*

Proof. Any ideal $\mathcal{J}$ of $\mathcal{A}$ is the direct sum of the ideals $\mathcal{J}_j = \mathcal{A}_j \cap \mathcal{J}$. On the other hand $\mathcal{A}/\mathcal{J}$ is Gorenstein iff the local factors $\mathcal{A}_i/\mathcal{J}_i$ are (Lemma 3.31). □

The following Theorem shows that we can get maximal Gorenstein factors of $\mathcal{A}$ from random linear forms on $\mathcal{A}$ with high probability, similarly as in the Gorenstein case.

Theorem 3.35. *The maximal Gorenstein factors of $\mathcal{A}$ can be obtained with high probability as $\mathcal{B} := \mathcal{A}/\mathcal{R}(\Lambda)$, where Λ is a random linear function on $\mathcal{A}$.*

Proof. Let $a_1, \ldots, a_m$ be a basis of $\mathcal{A}$ over $\mathbb{K}$. Then for a linear function $\Lambda : \mathcal{A} \to \mathbb{K}$ the dimension of $\mathcal{A}/\mathcal{R}(\Lambda)$ is the rank of the matrix $[\Lambda(a_i a_j)]$. Thus, maximal Gorenstein factors are obtained if the rank of the matrix is maximal (as Λ ranges over the $\mathbb{K}$-dual of $\mathcal{A}$). If one fixes a dual basis of $\mathcal{A}$, and writes Λ as a linear combination of these basis functions, then, the entries of the matrix $[\Lambda(a_i a_j)]$ will be linear polynomials of the coordinates $\gamma_1, \ldots, \gamma_m$ of Λ. Now consider a Λ which achieves the maximal rank k, and consider a corresponding $k \times k$ minor of the matrix that has a nonzero determinant. This determinant is not identically zero, as a function of the γ_j, hence it will be nonzero on a Zariski open set. The linear functions corresponding to the points in this set will define maximal Gorenstein factors. □

We now show that any maximal Gorenstein factor will allow us to compute the radical of $\mathcal{A}$.

Theorem 3.36. *Assume that Λ is such that the corresponding bilinear form on $\mathcal{A}$ has maximal rank. Then*

$$\mathcal{R}(\Lambda) \subseteq \mathrm{Rad}(\mathcal{A}).$$

Proof. By Lemma 3.34, we can assume that $\mathcal{A}$ is local. By Lemma 3.29, $\mathcal{R}(\Lambda)$ is an ideal. Since $\mathcal{A}/\mathrm{Rad}(\mathcal{A}) \cong \mathbb{K}$ is Gorenstein and $\mathcal{B}$ is the maximal Gorenstein factor of $\mathcal{A}$ we have that $\mathcal{R}(\Lambda) \neq \mathcal{A}$. Therefore $\mathcal{R}(\Lambda)$ is a subset of the unique maximal ideal $\mathcal{M} = \mathrm{Rad}(\mathcal{A})$. □

Using the previous results, we are now ready to define the main ingredients of our algorithm in the non-Gorenstein case, which are analogous to the Gorenstein case except that instead of working in $\mathcal{A}$ we are going to work in $\mathcal{B}$. We will use the notation of the previous subsection.

We can obtain a basis for $\mathcal{B}$ as follows. Let $B = [b_1, \ldots, b_N]$ be a basis for $\mathcal{A}$ and $\mathbf{y} \in \mathrm{Null}(\mathrm{Mac}_\Delta(\mathbf{f}))$ such that the moment matrix $\mathfrak{M}_B(\mathbf{y})$ has maximal rank. Since the columns of $\mathfrak{M}_B(\mathbf{y})$ correspond to B, taking a maximal nonsingular minor of this matrix will define a subset $B_\alpha = [b_{\alpha_1}, \ldots, b_{\alpha_r}]$ of B corresponding to the columns of this submatrix. Then B_α will form a basis for $\mathcal{B}$ as we prove in the following proposition.

Proposition 3.37. *$B_\alpha = [b_{\alpha_1}, \ldots, b_{\alpha_r}]$ forms a basis for $\mathcal{B}$.*

Proof. Consider the moment matrix $\mathfrak{M}_B(\mathbf{y})$ with columns corresponding to B and let r be its rank. Since B_α corresponds to a set of basic columns of $\mathfrak{M}_B(\mathbf{y})$, there exists a basis $\mathbf{v}_1, \ldots, \mathbf{v}_{N-r}$ for $\mathrm{Null}(\mathfrak{M}_B(\mathbf{y}))$ which can be extended to a basis of $\mathbb{K}^N$ by adding the unit vectors $\mathbf{e}_{\alpha_i} := [\delta_{\alpha_i, j}]_{j=1}^N$ for $i = 1, \ldots, r$.

Let v_i be the element of $\mathcal{A}$ obtained by taking the linear combination of $b_1, \ldots, b_N$ corresponding to the coordinates of $\mathbf{v}_i$ for $i = 1, \ldots, N - r$. Then it is easy to see that $v_i \in \mathcal{R}(\Lambda)$. Thus the elements of B_α correspond to a basis of $\mathcal{A}/\mathcal{R}(\Lambda) = \mathcal{B}$. □

Here we need to define the moment matrix.

Definition 3.38. *Let B_α be defined as above. Define*

$$J_\alpha := \sum_{i=1}^{k} b_{\alpha_i} b_{\alpha_i}^*$$

similarly as in 4.

Theorem 3.39. $[Tr(b_{\alpha_i} b_{\alpha_j})]_{i,j=1}^{k} = \boxed{\mathrm{Syl}_{B_\alpha}(J_\alpha)} \cdot \begin{array}{|c|}\hline \mathfrak{M}_{B_\alpha}(\mathbf{y}) \\ \hline \mathfrak{R}_{B_\alpha}(\mathbf{y}) \\ \hline \end{array}$.

Using the following theorem we get that the maximal nonsingular minor of the smaller trace matrix $[Tr(b_{\alpha_i} b_{\alpha_j})]_{i,j=1}^{k}$ suffices to compute the radical.

Theorem 3.40. *Let $B = [b_1, \ldots, b_N]$ be a basis for $\mathcal{A}$ and $B_\alpha = [b_{\alpha_1}, \ldots, b_{\alpha_r}]$ a basis for $\mathcal{B}$, where $\alpha_1 < \cdots < \alpha_r$ are in $\{1, \ldots, N\}$. Then*

$$\operatorname{rank}[Tr(b_{\alpha_i} b_{\alpha_j})]_{i,j=1}^{r} = \operatorname{rank}[Tr(b_i b_j)]_{i,j=1}^{N}.$$

(As before, by a slight abuse of notation, we use the same notation for elements in $\mathcal{A}$, in $\mathcal{B}$, and their common preimages in $\mathbb{K}[\mathbf{x}]$.)

Proof. This follows from Theorem 3.36 and the fact that the rank of the trace matrix is $\dim \mathcal{A}/\mathrm{Rad}(\mathcal{A}) = \dim \mathcal{B}/\mathrm{Rad}(\mathcal{B})$. □

4. Affine Complete Intersection Ideals

4.1. **Univariate Case.** In this section we will follow the work of Mourrain and Pan [40]. We start by defining the univariate Bezout matrix.

Definition 4.1. *Let $f, g \in \mathbb{K}[x]$ be two univariate polynomials such that $\deg g \leq \deg f = d$, and let y be a new variable. Then the Bezoutian $\Theta_{f,g}$ of f and g is the polynomial*

$$\mathfrak{B}_{f,g}(x, y) = \frac{f(x)g(y) - f(y)g(x)}{x - y} = \sum_{0 \leq i,j \leq d-1} c_{ij} x^i y^j.$$

The Bezout Matrix $B_{f,g}$ of f and g is the $d \times d$ matrix

$$[B_{f,g}]_{ij} = c_{ij}.$$

We will need the following definition:

Definition 4.2. *The* Horner basis *for the polynomial f is the set $\{H_{d-1}, \ldots, H_0\}$ with*

$$H_i(x) = a_{i+1} + \cdots + a_d x^{d-i-1} \qquad \text{for } i = 0, \ldots, d-1.$$

Note that in terms of the Horner polynomials, we have that

$$\mathfrak{B}_{f,1}(x, y) = \sum_{i=0}^{d-1} x^i H_i(y).$$

The following theorem connects the Bezoutian of f and its derivative f' with the matrix of traces of f with respect to the Horner basis.

Theorem 4.3.

$$B_{f,f'} = [Tr(H_i H_j)]_{i,j=0}^{d-1},$$

where $[Tr(H_i H_j)]_{i,j=0}^{d-1}$ is the matrix of traces of f in the Horner basis (see eg. [7], [40]*).*

Theorem 4.3 implies that using Dickson's Lemma one can compute the square-free factor of f by simply computing the kernel of $B_{f,f'}$. It's natural to ask how our method based on Dickson's lemma relates to computing the square-free factor of f via computing $\frac{f}{gcd(f,f')}$. The following proposition shows that computing $f/\gcd(f,f')$ to get the square-free factor using the Bezout matrix is computationally equivalent to using Dickson's Lemma.

Proposition 4.4. *The smallest degree polynomial of the form $\sum_{i=0}^{d-1} r_i H_i(x)$ such that $[r_0,\dots,r_{d-1}]^T$ is in the kernel of $B_{f,f'}$, is equal to $f/\gcd(f,f')$.*

4.2. **Multivariate Case.** For the multivariate case we will first define the multivariate analogue of the Bezout matrix (also referred to as Dixon matrix in the literature). The papers [8] and [27] are good references for the Bezout (Dixon) matrix described below.

Definition 4.5. *Let*

$$\mathbf{f} := [f_1,\dots,f_m] \in \mathbb{K}[x_1,\dots,x_m]^m$$

and consider an additional polynomial $f_0 \in \mathbb{K}[x_1,\dots,x_m]$. We use the notation $\mathbf{x} = [x_1,\dots,x_m]$, $\mathbf{y} = [y_1,\dots,y_m]$ and

$$X_0 = [x_1,\dots,x_m], X_1 = [y_1,x_2,\dots,x_m],\dots,X_m = [y_1,y_2,\dots,y_m].$$

The Bezoutian *of the system $[f_0,f_1,\dots,f_n]$, denoted by $\mathfrak{B}_{f_0}$, is a polynomial in the variables $\mathbf{x}$ and $\mathbf{y}$ defined as follows:*

$$\mathfrak{B}_{f_0}(\mathbf{x},\mathbf{y}) := \det \begin{vmatrix} f_0(X_0) & \frac{f_0(X_0)-f_0(X_1)}{x_1-y_1} & \dots & \frac{f_0(X_{m-1})-f_0(X_m)}{x_m-y_m} \\ f_1(X_1) & \frac{f_1(X_0)-f_1(X_1)}{x_1-y_1} & & \frac{f_1(X_{m-1})-f_1(X_m)}{x_m-y_m} \\ \vdots & \vdots & & \vdots \\ f_m(X_1) & \frac{f_m(X_0)-f_m(X_1)}{x_1-y_1} & \dots & \frac{f_m(X_{m-1})-f_m(X_m)}{x_m-y_m} \end{vmatrix}.$$

The Bezout matrix *of the system $[f_0,f_1,\dots,f_m]$, denoted by $\mathcal{B}_{f_0}$, is the coefficient matrix of the Bezoutian, i.e. if we write*

$$\mathfrak{B}_{f_0}(\mathbf{x},\mathbf{y}) = \sum_{\alpha\in E,\ \beta\in E'} c_{\alpha,\beta}(f_0)\ \mathbf{x}^\alpha \mathbf{y}^\beta$$

where E and E' are subsets of $\mathbb{N}^m$ and $c_{\alpha,\beta}(f_0) \in \mathbb{K}$, then the Bezout matrix of $[f_0,f_1\dots,f_m]$ is the $|E'|\times|E|$ matrix

$$\mathcal{B}_{f_0} := (c_{\beta,\alpha}(f_0))_{\beta\in E',\ \alpha\in E}.$$

We denote by $\mathfrak{B}^{\mathbf{x}}_{f_0}$ the map

$$\mathfrak{B}^{\mathbf{x}}_{f_0} : (\lambda_\beta)_{\beta\in E'} \mapsto \sum_{\alpha\in E,\ \beta\in E'} c_{\alpha,\beta}(f_0)\ \mathbf{x}^\alpha \lambda_\beta \tag{6}$$

and by $\mathfrak{B}^{\mathbf{y}}_{f_0}$ the map

$$\mathfrak{B}^{\mathbf{y}}_{f_0} : (\lambda_\alpha)_{\alpha\in E} \mapsto \sum_{\alpha\in E,\ \beta\in E'} c_{\alpha,\beta}(f_0)\ \lambda_\alpha \mathbf{y}^\beta. \tag{7}$$

Our goal is to compute a matrix of traces for the system $\mathbf{f} = [f_1,\dots,f_m]$ from the Bezout matrix $\mathcal{B}_J$ of the system $[J,f_1,\dots,f_m]$ analogously to the univariate

case, where J is the Jacobian of $f_1, \ldots, f_m$. As we mentioned in the introduction, in general the Bezout matrix $\mathcal{B}_J$ is not a matrix of traces, which can be easily seen by comparing sizes. However, to obtain a matrix of traces of $\mathbf{f}$ one can define a reduced version of the Bezoutian and the Bezout matrix as follows.

Definition 4.6. *Let $\mathbf{f} = [f_1, \ldots, f_m] \in \mathbb{K}[x_1, \ldots, x_m]^m$ and assume that the factor algebra $\mathcal{A}(\mathbf{x}) := \mathbb{K}[\mathbf{x}]/\mathcal{I}$ has dimension N over $\mathbb{K}$, where I is the ideal generated by the polynomials in $\mathbf{f}$. For some $f_0 \in \mathbb{K}[\mathbf{x}]$ let $\mathfrak{B}_{f_0}(\mathbf{x}, \mathbf{y})$ be the Bezoutian of the system $f_0, f_1, \ldots, f_m$. Let $B = [b_1, \ldots, b_N]$ and $B' = [b'_1, \ldots b'_N]$ be bases for $A(\mathbf{x})$ and $A(\mathbf{y})$, respectively. Then we can uniquely write*

$$\mathfrak{B}_{f_0}(\mathbf{x}, \mathbf{y}) = \sum_{b \in B, b' \in B'} \beta_{b,b'}(f_0)\, b(\mathbf{x}) b'(\mathbf{y}) + F(\mathbf{x}, \mathbf{y})$$

where $F(\mathbf{x}, \mathbf{y}) \in (I(\mathbf{x}), I(\mathbf{y}))$ and $\beta_{b,b'}(f_0) \in \mathbb{K}$. We define the reduced Bezoutian $\overline{\mathfrak{B}}_{f_0}$ *with respect to the bases B and B' as*

$$\overline{\mathfrak{B}}_{f_0} := \sum_{b \in B, b' \in B'} \beta_{b,b'}(f_0)\, b(\mathbf{x}) b'(\mathbf{y})$$

and the reduced Bezout matrix $\overline{\mathcal{B}}_{f_0}$ *with respect to the bases B and B' to be the $N \times N$ matrix*

$$\overline{\mathcal{B}}_{f_0}^{B,B'} := \left(\beta_{b,b'}(f_0)\right)_{b \in B, b' \in B'}.$$

We are going to use the following theorem [16]:

Theorem 4.7. *There exists (dual) bases $\Theta := [\theta_1(\mathbf{x}), \ldots, \theta_N(\mathbf{x})]$ and $\Omega := [\omega_1(\mathbf{y}), \ldots, \omega_N(\mathbf{y})]$ of $A(\mathbf{x})$ and $A(\mathbf{y})$ such that for all polynomial $f \in \mathbb{K}[\mathbf{x}]$, we have*

$$\mathfrak{B}_f := \sum_{i,j} \beta_{i,j}(f)\, \theta_i(\mathbf{x})\, \omega_j(\mathbf{y}) + F(\mathbf{x}, \mathbf{y}),$$

with $F(\mathbf{x}, \mathbf{y}) \in I(\mathbf{x}) \otimes I(\mathbf{y})$ and such that

$$\overline{\mathfrak{B}}_1 = \sum_i \theta_i(\mathbf{x})\, \omega_i(\mathbf{y}).$$

In [40] the following expression was given for the reduced Bezout matrix $\overline{\mathcal{B}}_J$ of the system $[J, f_1, \ldots, f_m]$ in terms of a matrix of traces of $f_1, \ldots, f_m$:

Theorem 4.8. *Let $\mathbf{f}$, $A(\mathbf{x})$, $A(\mathbf{y})$ and the bases $\Theta = (\theta_i)$, $\Omega = (\omega_i)$ be as in Definition 4.6 and Theorem 4.7. Let J be the Jacobian of $f_1, \ldots, f_m$, and consider the reduced Bezout matrix $\overline{\mathfrak{B}}_J$ with respect to the bases Θ and Θ. Then*

$$\overline{\mathcal{B}}_J^{\Theta,\Theta} = [Tr(\omega_i \omega_j)]_{i,j=1}^N.$$

Using the relation $\overline{\mathcal{B}}_J^{\Theta,\Theta} = \overline{\mathcal{B}}_J^{\Theta,\Omega}\, \overline{\mathcal{B}}_1^{\Theta,\Theta}$, we deduce that

$$\overline{\mathcal{B}}_J^{\Theta,\Omega} = [Tr(\omega_i\, \theta_j)]_{i,j=1}^N,$$

so that $\lambda = [\lambda_i] \in \ker \overline{\mathcal{B}}_J^{\Theta,\Omega}$ iff

$$Tr(\omega_i\, (\sum_{j=1}^N \lambda_j\, \theta_j)) = 0,\ i = 1, \ldots, N,$$

or equivalently iff

$$r := \sum_{j=1}^{N} \lambda_j \, \theta_j(\mathbf{x}) \in \sqrt{I}.$$

Because of the block diagonal form of the Bezoutian matrices in a common basis (Theorem 4.7), we deduce that if Λ is an element of $\ker(\mathfrak{B}_J)$ then

$$\mathfrak{B}_1^{\mathbf{x}}(\Lambda) = r(\mathbf{x}) + h(\mathbf{x}),$$

where $h \in I$, $\mathfrak{B}_1$ is the Bezoutian matrix of 1 in the (monomial) bases $(\mathbf{x}^\alpha)_{\alpha\in E}$, $(\mathbf{y}_\beta)_{\beta\in E'}$, $\mathfrak{B}_1^{\mathbf{x}}$ is the corresponding map defined in (6), and $\mathrm{im}(\mathfrak{B}_1^{\mathbf{y}})$ is the space generated by the coefficient vectors with respect to $(\mathbf{y}^\beta)_{\beta\in E'}$ of the polynomials in the image of the map $\mathfrak{B}_1^{\mathbf{y}}$ (see (7)). Then, we have the following theorem:

Theorem 4.9. *Using the previous notation we have that*

$$\sqrt{I} = \mathfrak{B}_1^{\mathbf{x}}(\ker(\mathfrak{B}_J^{\mathbf{x}})) + I(\mathbf{x}).$$

Proof. Because of the block diagonal form of the Bezoutian matrices in a common basis (Theorem 4.7) and the previous discussion, we deduce that if Λ is an element of $\ker(\mathfrak{B}_J)$ then

$$\mathfrak{B}_J^{\mathbf{x}}(\Lambda) = \sum_{i,j} \beta_{i,j}(J) \, \theta_i(\mathbf{x}) \, \Lambda(\omega_j(\mathbf{y})) + F^\Lambda(\mathbf{x}) = 0$$

where $F^\Lambda(\mathbf{x}) \in I$. By the previous discussions,

$$\sum_j \theta_j(\mathbf{x}) \, \Lambda(\omega_j(\mathbf{y})) = \mathfrak{B}_1^{\mathbf{x}}(\Lambda) \in \sqrt{I}.$$

□

Note that the role of $\mathbf{x}$ and $\mathbf{y}$ can be exchanged in this theorem. Note also that $\ker(\mathfrak{B}_J^{\mathbf{x}})$ can be replaced by $\ker(\mathfrak{B}_J^{\mathbf{x}}) \cap \ker(\mathfrak{B}_1^{\mathbf{x}})^\perp$ in this theorem.

A question that remains is how to compute the multiplication matrices $M_{x_1}, \ldots, M_{x_m}$ of the radical $\sqrt{I}$.

In order to compute the reduced Bezout matrix $\overline{\mathcal{B}}_{f_0}$ of the system $[f_1, \ldots, f_m]$ with respect to some bases $[a_1, \ldots, a_r]$ of $A(\mathbf{x})$ and $[b_1, \ldots, b_r]$ of $A(\mathbf{y})$, it is sufficient to find expressions of the form

$$\mathbf{x}^\alpha = \sum_{b\in B} c_b b(\mathbf{x}) + F(\mathbf{x}), \text{ for all } \alpha \in E \quad \text{and}$$
$$\mathbf{y}^\beta = \sum_{b'\in B'} c_{b'} b'(\mathbf{y}) + G(\mathbf{y}), \text{ for all } \beta \in E'$$

where $F, G \in I$, $c_b, c_{b'} \in \mathbb{K}$ and E and E' were defined in Definition 4.5. Define

$$V := \langle \mathbf{x}^\alpha | \alpha \in E \rangle \quad \text{and} \quad W := \langle \mathbf{y}^\beta | \beta \in E' \rangle.$$

Assuming that $b_i \in V$ and $b'_i \in W$ for $i = 1, \ldots, l$, the task is to find enough linear combinations of the monomials corresponding to the rows and the columns of the Bezout matrices which belong to the ideal I.

We follow the approach described in [39], where it was shown that the computation of the Bezoutians $\mathfrak{B}_{x_i}$ of the system $[x_i, f_1, \ldots, f_m]$, for $i = 1, \ldots, m$, as well as the Bezoutian $\mathfrak{B}_1$ of the system $[1, f_1, \ldots, f_m]$, gives sufficient information of the structure of I in order to find the reduced Bezout matrix $\overline{\mathcal{B}}_{f_0}$ for any $f_0 \in \mathbb{K}[\mathbf{x}]$. In

order to get the structure of $\sqrt{I}$ we simply have to add the polynomials in $\mathbf{x}$ (resp. $\mathbf{y}$), obtained from Theorem 4.9.

Here we describe a summary of this method. First notice that

$$x_i\mathfrak{B}_1 - \mathfrak{B}_{x_i} \in I(\mathbf{x}) \quad \text{and} \quad y_i\mathfrak{B}_1 - \mathfrak{B}_{y_i} \in I(\mathbf{y}) \quad i = 1, \ldots, m.$$

The **initial step** of the method is to obtain ideal elements in $\sqrt{I}(\mathbf{x})$ (resp. $\sqrt{I}(\mathbf{x})$) which are in V (resp. W) from $x_i\mathfrak{B}_1 - \mathfrak{B}_{x_i}$ (resp. $y_i\mathfrak{B}_1 - \mathfrak{B}_{y_i}$) and also from $\mathfrak{B}_1^{\mathbf{x}}(\ker(\mathfrak{B}_J^{\mathbf{x}}))$ (resp. $\mathfrak{B}_1^{\mathbf{y}}(\ker(\mathfrak{B}_J^{\mathbf{y}}))$). The elements in $\sqrt{I}(\mathbf{x}) \cap \mathbf{V}$ obtained by the initial step are denote K_0, and the ones in $\sqrt{I}(\mathbf{y}) \cap \mathbf{W}$ are denoted by H_0.

For any vector space $K \subset R$, we denote by K^+, the vector space $K^+ = K + x_1K + \cdots + x_mK$. The notation $K^{[n]}$ means n iterations of the operator $+$, starting from K.

To prove that we get the quotient structure by the radical ideal $\sqrt{I}$, we will assume that V is connected to 1, that is, V contains 1 and for any $v \in V - \langle 1 \rangle$, there exists $l > 0$ such that $v \in \text{span}(1)^{[l]}$ and $v = v_0 + \sum_{i=1}^m x_i v_i$ with $v_i \in \text{span}(1)^{[l-1]} \cap V$ for $i = 0, \ldots, m$.

In order to obtain additional ideal elements, the following steps are used [39]:

Saturation step: Finds new ideal elements by multiplying the already computed ideal elements by the variables x_i for all $i = 1, \ldots, m$.

Column reduction step: Finds new bases for the vector spaces V and W such that the new basis for V contains previously computed elements in $\sqrt{I}(\mathbf{x}) \cap V$, and also that the Bezout matrix $\mathcal{B}_1$, written in terms of these new bases, has a lower block triangular structure. By writing the matrices $\mathcal{B}_{x_i}$ in terms of the new bases for V and W, one can obtain new elements in $\sqrt{I}(\mathbf{x}) \cap V$.

Diagonalization step: After the column reduction step one can transform $\mathcal{B}_1$ into a block diagonal form which, by repeating the same transformation on the matrices $\mathcal{B}_{x_i}$, can possibly reveal new ideal elements.

Row reduction step: Same as the column reduction step, with the roles of $\mathbf{x}$ and $\mathbf{y}$ interchanged.

They are used in the following iterative algorithm:

Algorithm 4.10 (Radical of an affine complete intersection)**.**
INPUT*:* $\mathbf{f} = [f_1, \ldots, f_m] \in \mathbb{K}[\mathbf{x}]$ *generating an ideal* I*, which have a finit number of complex roots.*
OUTPUT*:* $M_{x_1}, \ldots, M_{x_m}$ *a system of multiplication matrices for the radical ideal* $\sqrt{I}$*.*

- *Compute the Bezoutian matrices* $\mathcal{B}_1, \mathcal{B}_{x_1}, \ldots, \mathcal{B}_{x_m}$ *of* $1, x_1, \ldots, x_m$ *and* $f_1, \ldots, f_m$ *and* $\mathcal{B}_J$*.*
- *Using the initial step, define* $K := K_0$*;* $H := H_0$*;* **notsat** `:= true`*.*
- *While* **notsat**
  - *Apply the saturation step on* K *and* H*;*
  - *Apply the column reduction step;*
  - *Apply the diagonalisation step;*
  - *Apply the row reduction step;*
  - *If this extends strictly* K*; or* H*, then*
    let **notsat** `:= true`*, otherwise let* **notsat** `:= false`*.*

- *Return*

$$M_{x_i} := N_1^{-1} N_{x_i},\ i = 1, \dots, m \tag{8}$$

where N_{x_i} is the matrix reduced from $\mathcal{B}_{x_i}$, at the end of the loop.

The loop terminantes because the size of the matrices are decreasing. If it ends with matrices of non-zero size, N_1 is necessarily invertible. At the initial step and all along the computation, we have $K \subset \sqrt{I}(\mathbf{x}), H \subset \sqrt{I}(\mathbf{y})$, since the different steps are valid modulo $I \subset \sqrt{I}$. We denote by $[a_1, \dots, a_r]$ (resp. $[b_1, \dots, b_r]$) the linearly independent polynomials indexing the rows (resp. columns) of M_i and A (resp. B) the vector space they span. By construction, the vector space V (resp. W) decomposes as $V = A + \mathrm{span}(K)$ (resp. $W = B + \mathrm{span}(H)$) where K and H are the sets of relations in $\sqrt{I}$ updated in the reduction steps during the algorithm. We complete $a_i, i = 1, \dots, r$ (resp. $b_i, i = 1, \dots, r$) in a basis $a_1, \dots, a_{|E|}$ of V (resp. $b_1, \dots, b_{|E'|}$ of W) with $a_i \in K$ (resp. $b_i \in H$) for $i > r$.

We have the following theorem, which allow us to compute the radical of an affine complete inetrsection, based on simple algebra tools:

Theorem 4.11. *Let $f_1, \dots, f_m$ be as above. Upon termination, Algorithm 4.10 computes new bases $[a_1, \dots, a_{|E|}]$ for V and $[b_1, \dots, b_{|E'|}]$ for W, such that*

- *$[a_1, \dots, a_r]$ (resp. $[b_1, \dots, b_r]$) is a basis of $\mathbb{K}[\mathbf{x}]/\sqrt{I}(\mathbf{x})$ (resp. $\mathbb{K}[\mathbf{y}]/\sqrt{I}(\mathbf{y})$),*
- *the ouput matrices M_i are the (resp. transpose) matrix of multiplication of x_i with respect to the basis $[a_1, \dots, a_r]$ (resp. $[b_1, \dots, b_r]$) for $i = 1, \dots m$,*
- *$a_{r+1}, \dots, a_{|E|} \in \sqrt{I}(\mathbf{x}) \cap V$ and $b_{r+1}, \dots, b_{|E'|} \in \sqrt{I}(\mathbf{y}) \cap W$.*

Proof. The proofs of [39][Lemma 5.3, Proposition 5.3-5.6] apply also here in order to show that the matrices M_{x_i} commute. Moreover, by construction, $K \subset V \cap \sqrt{I}(\mathbf{x})$ such that $V = A \oplus \mathrm{span}(K)$, and K satisfies the following relations: $f_i \in \langle K \rangle$ for $i = 1, \dots, m$ (same proof as in [39] [Proposition 5.7]), $\langle K \rangle \subset \sqrt{I}$ by definition of the reduction steps, $B_1^{\mathbf{x}}(\ker B_J^{\mathbf{x}}) \subset \langle K_0 \rangle \subset \langle K \rangle$. Therefore, by Theorem 4.9, this shows that $\langle K \rangle = \sqrt{I}$. As in [39] [Theorem 5.8], we can assume that $1 \in A$ and that we have an exact sequence:

$$\begin{array}{rcl} 0 \to \langle K \rangle \to \mathbb{K}[\mathbf{x}] & \to & A \to 0 \\ f & \mapsto & f(\mathbf{M})(1) \end{array}$$

where $f(\mathbf{M}) := f(M_{x_1}, \dots, M_{x_m})$ is the linear operator of A, obtain by replacing the variable x_i by M_{x_i}. As $\langle K \rangle = \sqrt{I}$, this shows that $A \sim \mathbb{K}[\mathbf{x}]/\sqrt{I}$ and the basis of A is a basis in $\mathbb{K}[\mathbf{x}]/\sqrt{I}$. □

5. Conclusion

In an earlier work we gave an algorithm to compute matrices of traces and the radical of an ideal $\mathcal{I}$ which has finitely many projective common roots, none of them at infinity and its factor algebra is Gorenstein. The present paper considers an extension of the above algorithm which also works in the non-Gorenstein case and for systems which have roots at infinity, as well as an alternative method using Bezout matrices for the affine complete intersection case to compute the radical $\sqrt{\mathcal{I}}$.

References

[1] Inés Armendáriz and Pablo Solernó. On the computation of the radical of polynomial complete intersection ideals. In *AAECC-11: Proceedings of the 11th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, pages 106–119, 1995.

[2] Eberhard Becker, Jean-Paul Cardinal, Marie-Françoise Roy, and Z. Szafraniec. Multivariate Bezoutians, Kronecker symbol and Eisenbud-Levine formula. In *Algorithms in algebraic geometry and applications (Santander, 1994)*, volume 143 of *Progr. Math.*, pages 79–104.

[3] Eberhard Becker and T. Wörmann. Radical computations of zero-dimensional ideals and real root counting. In *Selected papers presented at the international IMACS symposium on Symbolic computation, new trends and developments*, pages 561–569, 1996.

[4] Eberhard Becker. Sums of squares and quadratic forms in real algebraic geometry. In *De la géométrie algébrique réelle (Paris, 1990)*, volume 1 of *Cahiers Sém. Hist. Math. Sér. 2*, pages 41–57. 1991.

[5] Eberhard Becker and Thorsten Wörmann. On the trace formula for quadratic forms. In *Recent advances in real algebraic geometry and quadratic forms*, volume 155 of *Contemp. Math.*, pages 271–291. 1994.

[6] Emmanuel Briand and Laureano Gonzalez-Vega. Multivariate Newton sums: Identities and generating functions. *Communications in Algebra*, 30(9):4527–4547, 2001.

[7] Jean-Paul Cardinal On two iterative methods for approximating the roots of a polynomial. In *Proc. AMS-SIAM Summer Seminar on Math. of Numerical Analysis, (Park City, Utah, 1995)*, volume 32 of *Lectures in Applied Math.*, pages 165–188. American Mathematical Society, 1996.

[8] Jean-Paul Cardinal and Bernard Mourrain. Algebraic approach of residues and applications. In J. Reneger, M. Shub, and S. Smale, editors, *Proceedings of AMS-Siam Summer Seminar on Math. of Numerical Analysis (Park City, Utah, 1995)*, volume 32 of *Lectures in Applied Mathematics*, pages 189–219, 1996.

[9] Eduardo Cattani, Alicia Dickenstein, and Bernd Sturmfels. Computing multidimensional residues. In *Algorithms in algebraic geometry and applications (Santander, 1994)*, volume 143 of *Progr. Math.*, pages 135–164. 1996.

[10] Eduardo Cattani, Alicia Dickenstein, and Bernd Sturmfels. Residues and resultants. *J. Math. Sci. Univ. Tokyo*, 5(1):119–148, 1998.

[11] David A. Cox, John B. Little, and Don O'Shea. *Using Algebraic Geometry*, volume 185 of *Graduate Texts in Mathematics*. Springer-Verlag, NY, 1998. 499 pages.

[12] Raúl E. Curto and Lawrence A. Fialkow. Solution of the truncated complex moment problem for flat data. *Mem. Amer. Math. Soc.*, 119(568):x+52, 1996.

[13] Carlos D'Andrea and Gabriela Jeronimo. Rational formulas for traces in zero-dimensional algebras. *http://arxiv.org/abs/math.AC/0503721*, 2005.

[14] Gema M. Díaz-Toca and Laureano González-Vega. An explicit description for the triangular decomposition of a zero-dimensional ideal through trace computations. In *Symbolic computation: solving equations in algebra, geometry, and engineering (South Hadley, MA, 2000)*, volume 286 of *Contemp. Math.*, pages 21–35. 2001.

[15] Leonard E. Dickson. *Algebras and Their Arithmetics*. University of Chicago Press, 1923.

[16] Mohamed Elkadi and Bernard Mourrain. A new algorithm for the geometric decomposition of a variety. In S. Dooley, editor, *Proc. Intern. Symp. on Symbolic and Algebraic Computation*, pages 9–16, 1999.

[17] Mohamed Elkadi and Bernard Mourrain. *Introduction à la résolution des systèmes polynomiaux*, volume 59 of *Mathématiques et Applications*. 2007.

[18] Patrizia Gianni and Teo Mora. Algebraic solution of systems of polynomial equations using Gröbner bases. In *Applied algebra, algebraic algorithms and error-correcting codes (Menorca, 1987)*, volume 356 of *Lecture Notes in Comput. Sci.*, pages 247–257. 1989.

[19] Patrizia Gianni, Barry Trager, and Gail Zacharias. Gröbner bases and primary decomposition of polynomial ideals. *J. Symbolic Comput.*, 6(2-3):149–167, 1988. Computational aspects of commutative algebra.

[20] Laureano González-Vega. The computation of the radical for a zero dimensional ideal in a polynomial ring through the determination of the trace for its quotient algebra. *Preprint*, 1994.

[21] Laureano González-Vega and Guadalupe Trujillo. Using symmetric functions to describe the solution set of a zero-dimensional ideal. In *Applied algebra, algebraic algorithms and error-correcting codes (Paris, 1995)*, volume 948 of *Lecture Notes in Comput. Sci.*, pages 232–247.

[22] Gert-Martin Greuel and Gerhard Pfister. *A Singular introduction to commutative algebra*. 2002. With contributions by Olaf Bachmann, Christoph Lossen and Hans Schönemann.

[23] Werner Heiß, Ulrich Oberst, and Franz Pauer. On inverse systems and squarefree decomposition of zero-dimensional polynomial ideals. *J. Symbolic Comput.*, 41(3-4):261–284, 2006.

[24] Itnuit Janovitz-Freireich, Bernard Mourrain, Lajos Rónyai, and Ágnes Szántó. Moment matrices, trace matrices and the radical of ideals. *ISSAC '08: Proceedings of the 2008 International Symposium on Symbolic and Algebraic Computation*, pages 125–132, 2008.

[25] Itnuit Janovitz-Freireich, Lajos Rónyai, and Ágnes Szántó. Approximate radical of ideals with clusters of roots. In *ISSAC '06: Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computation*, pages 146–153, 2006.

[26] Itnuit Janovitz-Freireich, Lajos Rónyai, and Ágnes Szántó. Approximate radical for clusters: a global approach using gaussian elimination or svd. *Mathematics in Computer Science*, 1(2):393–425, 2007.

[27] Deepar Kapur, Tushar Saxena, and Lu Yang. Algebraic and geometric reasoning using Dixon resultants. In *ISSAC '94*, pages 99–107, 1994.

[28] Hidetsune Kobayashi, Shuichi Moritsugu, and Robert W. Hogan. On radical zero-dimensional ideals. *J. Symbolic Comput.*, 8(6):545–552, 1989.

[29] Teresa Krick and Alessandro Logar. An algorithm for the computation of the radical of an ideal in the ring of polynomials. In *Applied algebra, algebraic algorithms and error-correcting codes (New Orleans, LA, 1991)*, volume 539 of *Lecture Notes in Comput. Sci.*, pages 195–205.

[30] Teresa Krick and Alessandro Logar. Membership problem, representation problem and the computation of the radical for one-dimensional ideals. In *Effective methods in algebraic geometry (Castiglioncello, 1990)*, volume 94 of *Progr. Math.*, pages 203–216. 1991.

[31] Ernst Kunz. *Kähler differentials*. Advanced lectures in Mathematics. Friedr. Vieweg and Sohn, 1986.

[32] Yagati N. Lakshman. On the complexity of computing a Gröbner basis for the radical of a zero-dimensional ideal. In *In Proceedings of the Twenty Second Symposium on Theory of Computing*, pages 555–563, 1990.

[33] Yagati N. Lakshman. A single exponential bound on the complexity of computing Gröbner bases of zero-dimensional ideals. In *Effective methods in algebraic geometry (Castiglioncello, 1990)*, volume 94 of *Progr. Math.*, pages 227–234. 1991.

[34] Yagati N. Lakshman and Daniel Lazard. On the complexity of zero-dimensional algebraic systems. In *Effective methods in algebraic geometry (Castiglioncello, 1990)*, volume 94 of *Progr. Math.*, pages 217–225. 1991.

[35] Jean Bernard Lasserre, Monique Laurent, and Philipp Rostalski. A unified approach to computing real and complex zeros of zero-dimensional ideals. *preprint*, 2007.

[36] Jean Bernard Lasserre, Monique Laurent, and Philipp Rostalski. Semidefinite characterization and computation of zero-dimensional real radical ideals. *to appear in Foundations of Computational Mathematics*, 2007.

[37] Daniel Lazard. Résolution des systèmes d'équations algébriques. *Theoret. Comput. Sci.*, 15(1):77–110, 1981.

[38] Bernard Mourrain. Computing isolated polynomial roots by matrix methods. *J. of Symbolic Computation, Special Issue on Symbolic-Numeric Algebra for Polynomials*, 26(6):715–738, Dec. 1998.

[39] Bernard Mourrain. Bezoutian and quotient ring structure. *J. of Symbolic Comput.*, 39:397–415, 2005.

[40] Bernard Mourrain and Victor Y. Pan. Multivariate polynomials, duality, and structured matrices. *J. Complex.*, 16(1):110–180, 2000.

[41] Paul Pedersen, Marie-Françoise Roy, and Aviva Szpirglas. Counting real zeros in the multivariate case. In *Computational algebraic geometry (Nice, 1992)*, volume 109 of *Progr. Math.*, pages 203–224. Boston, MA, 1993.

[42] Fabrice Rouiller. Solving zero-dimensional systems through the rational univariate representation. In *AAECC: Applicable Algebra in Engineering, Communication and Computing*, volume 9, pages 433–461, 1999.

[43] Günter Scheja and Uwe Storch. Über Spurfunktionen bei vollständigen Durschnitten. *J. Reine Angew Mathematik*, 278:174–190, 1975.
[44] Richard P. Stanley. *Combinatorics and commutative algebra*, volume 41 of *Progress in Mathematics*. Birkhäuser, 1996.
[45] Kazuhiro Yokoyama, Masayuki Noro, and Taku Takeshima. Solutions of systems of algebraic equations and linear maps on residue class rings. *J. Symbolic Comput.*, 14(4):399–417, 1992.
[46] Lihong Zhi and Greg Reid. Solving nonlinear polynomial systems via symbolic-numeric elimination method. In *In Proceedings of the International Conference on Polynomial System Solving*, pages 50–53, 2004.

Itnuit Janovitz-Freireich, Departamento de Matemáticas, Centro de Investigación y Estudios Avanzados del I.P.N., Mexico City, Mexico
E-mail address: janovitz@math.cinvestav.mx

Bernard Mourrain, GALAAD, INRIA, Sophia Antipolis, France
E-mail address: mourrain@sophia.inria.fr

Lajos Rónyai, Computer and Automation Institute, Hungarian Academy of Sciences and Budapest University of Technology and Economics, Budapest, Hungary
E-mail address: lajos@csillag.ilab.sztaki.hu

Ágnes Szántó, Mathematics Department, North Carolina State University, Raleigh, NC, USA
E-mail address: aszanto@ncsu.edu