Moment Matrices, Trace Matrices and the Radical of Ideals

Itnuit Janovitz-Freireich, Ágnes Szántó *
North Carolina State University
Campus Box 8205
Raleigh, NC, 27695
USA
{ijanovi2, aszanto}@ncsu.edu

Bernard Mourrain †
GALAAD
INRIA,
Sophia Antipolis,
France
mourrain@sophia.inria.fr

Lajos Rónyai ‡
MTA SZTAKI
1111 Budapest,
Lágymányosi u. 11
Hungary
lajos@csillag.ilab.sztaki.hu

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. Assume that the factor algebra $\mathcal{A} = \mathbb{K}[x_1, \ldots, x_m]/\mathcal{I}$ is Gorenstein and that we have a bound $\delta > 0$ such that a basis for $\mathcal{A}$ can be computed from multiples of $f_1, \ldots, f_s$ of degrees at most δ. We propose a method using Sylvester or Macaulay type resultant matrices of $f_1, \ldots, f_s$ and J, where J is a polynomial of degree δ generalizing the Jacobian, to compute moment matrices, and in particular matrices of traces for $\mathcal{A}$. These matrices of traces in turn allow us to compute a system of multiplication matrices $\{M_{x_i} | i = 1, \ldots, m\}$ of the radical $\sqrt{\mathcal{I}}$, following the approach in the previous work by Janovitz-Freireich, Rónyai and Szántó. Additionally, we give bounds for δ for the case when $\mathcal{I}$ has finitely many projective roots in $\mathbb{P}^m_{\mathbb{K}}$.

Categories and Subject Descriptors

I.1.2 [**Computing Methodologies**]: Algebraic Manipulations—*Algebraic Algorithms*

General Terms

Algorithms, Theory

Keywords

Moment Matrices, Matrices of Traces, Radical Ideal, Solving polynomial systems

*Affiliation: North Carolina State University, Department of Mathematics. Research supported by NSF grant CCR-0347506.

†Affiliation: GALAAD, INRIA, Sophia Antipolis, France. Research partially supported by the ANR GECKO

‡Affiliation: Computer and Automation Institute of the Hungarian Academy of Sciences, and Budapest University of Technology and Economics. Research supported in part by OTKA grant NK63066.

1. INTRODUCTION

This paper is a continuation of our previous investigation in [22, 23] to compute the approximate radical of a zero dimensional ideal which has zero clusters. 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 [22, 23] was Dickson's lemma [14], 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 14): in [22, 23] we studied numerical 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.

It turns out that the computationally most expensive part of the method in [22, 23] is the computation of the matrix of traces. We address this problem in the present paper, and give a simple algorithm using only Sylvester or Macaulay type resultant matrices and elementary linear algebra to compute matrices of traces of zero dimensional ideals satisfying certain conditions.

More precisely, we need the following assumptions: let $\mathbf{f} = [f_1, \ldots, f_s]$ be a system of polynomials of degrees $d_1 \geq \cdots \geq d_s$ in $\mathbb{K}[\mathbf{x}]$, with $\mathbf{x} = [x_1, \ldots, x_m]$, 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 a bound $\delta > 0$ such that a basis $S = [b_1, \ldots, b_N]$ of $\mathcal{A}$ can be obtained by taking a linear basis of the space of polynomials of degree at most δ factored by the subspace generated by the multiples of $f_1, \ldots, f_s$ of degrees at most δ. By slight abuse of notation we denote the elements of the basis S which are in $\mathcal{A}$ and some fixed preimages of them in $\mathbb{K}[\mathbf{x}]$ both by $b_1, \ldots, b_N$. Thus we can assume that the basis S consists of monomials of degrees at most δ. Note that we can prove bounds $\delta = \sum_{i=1}^{m+1} d_i - m$

(or $\delta = \sum_{i=1}^{m} d_i - m$ if $s = m$) if $\mathcal{I}$ has only finitely many *projective* common roots in $\mathbb{P}^m_{\mathbb{K}}$ and have no common roots at infinity, using a result of Lazard [33] (see Theorem 3).

Furthermore, we also assume that $\mathcal{A}$ is Gorenstein over $\mathbb{K}$ (see Definition 1). Note that in practice we can easily detect if $\mathcal{A}$ is not Gorenstein (see Remark 10). Also, a random change of projective variables can eliminate roots at infinity with high probability when they are in finite number, but we will address the necessity of this assumption in an upcoming paper.

The main ingredient of our method is a Macaulay type resultant matrix $\mathrm{Mac}_\Delta(\mathbf{f})$, which is defined to be a maximal row-independent submatrix of the transpose matrix of the degree Δ Sylvester map $(g_1, \ldots, g_s) \mapsto \sum_{i=1}^{s} f_i g_i \in \mathbb{K}[\mathbf{x}]_\Delta$ for $\Delta \leq 2\delta + 1$ (see Definition 5). Using our assumptions on $\mathcal{A}$, we can compute a basis S of $\mathcal{A}$ using $\mathrm{Mac}_\Delta(\mathbf{f})$, and we also prove that a random element $\mathbf{y}$ of the nullspace of $\mathrm{Mac}_\Delta(\mathbf{f})$ provides a non-singular $N \times N$ moment matrix $\mathfrak{M}_S(\mathbf{y})$ with high probability (similarly as in [31]). 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 $f_1, \ldots f_s$ in the case when $s = m$. The main result of the paper now can be formulated as follows:

THEOREM *Let $S = [b_1, \ldots, b_N]$ be a basis of $\mathcal{A}$ with $\deg(b_i) \leq \delta$. With J as above, let $\mathrm{Syl}_S(J)$ 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*

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

where X is the unique extension of the matrix $\mathfrak{M}_S(\mathbf{y})$ 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 $R_{x_k} := [Tr(x_k b_i b_j)]_{i,j=1}^{N} = \mathrm{Syl}_S(x_k J) \cdot X$ for $k = 1, \ldots, m$, we can use the results of [22, 23] 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 [23] 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} 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.

We also note here that in a follow up paper we will consider an extension of our present results which works also in the non-Gorenstein case to compute the matrices of traces. Furthermore, that paper will also extend our results to the *affine* complete intersection case using Bezout matrices.

2. RELATED WORK

The motivation for this work was the papers [31, 32] 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 [32] they double up the machinery for the real case to obtain the radical of the complex ideal. However, in [31] 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 [31] they cite our previous work [22] 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 $S = [b_1, \ldots, b_N]$ by simply eliminating the terms not in S 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 S contains the monomials $1, x_1, \ldots, x_m$, one eigenvector computation yield 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 [18, 5] 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 [19] 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 [17, 26, 10, 20]). The advantage of the latter is that it can be generalized for higher dimensional ideals (see for example [25]). 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 [23]. Other methods to compute the radical of zero dimensional ideals include [24, 16, 28, 29, 30, 39]. Applications of computing the radical include [21], 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 [13, 6] where they use Newton Sums, [7, 8, 9] where they use residues and [12] using resultants. Besides computing the radical of an ideal, matrices of traces have numerous applications mainly in real algebraic geometry [2, 35, 4], or in [36] where trace matrices are applied to find separating linear forms deterministically.

3. MOMENT MATRICES AND MATRICES OF TRACES

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. [27, 37, 15, 31]). Note that these algebras are also referred to as Frobenius in the literature, see for example [3].

DEFINITION 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 2. *Throughout the paper we assume that $\mathcal{A}$ is Gorenstein. Furthermore, we also assume that we have a bound $\delta > 0$ such that*

$$N := \dim_{\mathbb{K}} \mathbb{K}[\mathbf{x}]_\delta / \langle f_1, \ldots, f_s \rangle_\delta = \dim_{\mathbb{K}} \mathbb{K}[\mathbf{x}]_d / \langle f_1, \ldots, f_s \rangle_d \quad (1)$$

for all $d \geq \delta$ and that

$$N = \dim \mathcal{A}. \quad (2)$$

Here

$$\langle f_1, \ldots, f_s \rangle_d := \left\{ \sum_i f_i p_i \ : \ \deg(p_i) \leq d - d_i \right\}. \quad (3)$$

We fix $S = [b_1, \ldots, b_N]$ a monomial basis for $\mathcal{A}$ such that $\deg(b_i) \leq \delta$ for all $i = 1, \ldots, N$. Let D be the maximum degree of the monomials in S. Thus $D \leq \delta$.

We have the following theorem giving bounds for δ in the case when $\mathbf{f}$ has finitely many projective roots.

THEOREM 3. *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 $f_1, \ldots, f_s$ has finitely many projective common roots in $\mathbb{P}^m_{\mathbb{K}}$. Assume further that $f_1, f_2, \ldots, f_s$ have no common roots at infinity. Then:*

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

PROOF. For the first assertion let $\mathbf{f}^h$ 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 [38], we can now calculate the Hilbert series of B, defined by $H(B,\lambda) = \sum_d \mathcal{H}_B(d)\lambda^d$, where $\mathcal{H}_\mathcal{B}$ 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 $B_d \to \mathbb{K}[\mathbf{x}]_d / \langle f_1, \ldots, f_s \rangle_d$, 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 $d \geq \delta$ $\dim_{\mathbb{K}} \mathbb{K}[\mathbf{x}]_d / \langle f_1, \ldots, f_s \rangle_d = \dim_{\mathbb{K}} \mathcal{A} = N$, which implies (1) and (2).

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 [15, 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 [33, Theorem 3.3] implies that

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

From here we obtain (1) and (2) as in the Case 1.

□

REMARK 4. *Note that in general $\mathcal{I}_d \neq \langle f_1, \ldots, f_s \rangle_d$, where I_d is the set of elements of I with degree at most d and $\langle f_1, \ldots, f_s \rangle_d$ was defined in (3). This can happen when the system has a root at infinity, for example, if $f_1 = x+1$, $f_2 = x$ then $\mathcal{I}_0 = \text{span}_{\mathbb{K}}(1)$ 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 $\dim \mathbb{K}[\mathbf{x}]_d / \langle f_1, \ldots, f_s \rangle_d$ for large enough d, because above $\dim \mathcal{A} = 0$ but $\dim \mathbb{K}[x,y]_d / \langle f_1, f_2 \rangle_d = 1$ for all $d \geq 0$.*

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

DEFINITION 5. *Define*

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

where δ and D are defined in Assumption 2.

Let $\text{Syl}_\Delta(\mathbf{f})$ be the transpose matrix of the linear map

$$\begin{aligned} \bigoplus_i \mathbb{K}[\mathbf{x}]_{\Delta - d_i} &\longrightarrow \mathbb{K}[\mathbf{x}]_\Delta \quad (4) \\ (g_1, \ldots, g_s) &\mapsto \sum_{i=1}^s f_i g_i \end{aligned}$$

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

Let $\mathrm{Mac}_\Delta(\mathbf{f})$ *be a row submatrix of* $\mathrm{Syl}_\Delta(\mathbf{f})$ *of maximal size with linearly independent rows.*

REMARK 6. *In the case where* $s = m$*, for generic* $\mathbf{f}$ *we can directly construct* $\mathrm{Mac}_\Delta(\mathbf{f})$ *by taking the restriction of the map (4) to*

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

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

Here $\mathrm{Mac}_\Delta(\mathbf{f})$ *is a submatrix of the classical Macaulay matrix of the homogenization of* $\mathbf{f}$ *and some* f_{m+1}^h*, where* f_{m+1}^h *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 $f_1, \ldots, f_m$ *has finitely many projective roots, we have that* $\mathrm{Mac}_\Delta(\mathbf{f})$ *has column corank* $N := \prod_{i=1}^m d_i$.

Since $\Delta \geq \delta$, by Assumption 2 the corank of $\mathrm{Mac}_\Delta(\mathbf{f}) = N$, where N is the dimension of $\mathcal{A}$. Also, we can assume that the elements of the basis S of $\mathcal{A}$ are monomials of degree at most δ, and that the first columns of $\mathrm{Mac}_\Delta(\mathbf{f})$ correspond to the basis S of $\mathcal{A}$.

Fix an element

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

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

DEFINITION 7. *Let* S *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* $\Lambda_\mathbf{y}(g) := \sum_{\mathbf{x}^\alpha \in S} y_\alpha g_\alpha$*, where* $g = \sum_{\mathbf{x}^\alpha \in S} g_\alpha \mathbf{x}^\alpha \in \mathcal{A}$*. 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 $\mathfrak{M}_S(\mathbf{y})$ *to be the* $N \times N$ *matrix given by*

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

where α *and* β *run through the exponents of the monomials in* S*. Note that* $\mathfrak{M}_S$ *is only a submatrix of the usual notion of moment matrices in the literature, see for example [11].*

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 8. *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* $g, h \in \mathcal{A}$

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

where $\mathrm{coeff}_S(p)$ *denotes the vector of coefficients of* $p \in \mathcal{A}$ *in the basis* S*.*

The following proposition is a simple corollary of [31, Prop 3.3 and Cor. 3.1].

PROPOSITION 9. *Let* $\mathbf{y}$ *be a random element of the vector space* $\mathrm{Null}(\mathrm{Mac}_\Delta(\mathbf{f}))$*. With high probability,* $\mathfrak{M}_S(\mathbf{y})$ *is non-singular.*

REMARK 10. *Using the above proposition, one can detect whether the algebra* $\mathcal{A}$ *is not Gorenstein with high probability by simply computing the rank of* $\mathfrak{M}_S(\mathbf{y})$ *for (perhaps several) random elements* $\mathbf{y}$ *in* $\mathrm{Null}(\mathrm{Mac}_\Delta(\mathbf{f}))$*.*

REMARK 11. *By [31, 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* $\mathfrak{M}_S(\mathbf{y})$ *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 $S = [b_1, \ldots, b_N]$ with respect to the moment matrix $\mathfrak{M}_S(\mathbf{y})$. 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 12. *From now on we fix* $\mathbf{y} \in \mathrm{Null}(\mathrm{Mac}_\Delta(\mathbf{f}))$ *such that* $\mathfrak{M}_S(\mathbf{y})$ *is invertible and we will denote by* Λ *the corresponding element* $\Lambda_\mathbf{y} \in \mathcal{A}^*$*. We define*

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

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* $\mathfrak{M}_S^{-1}(\mathbf{y})$ *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*

$$J := \sum_{i=1}^{N} b_i b_i^* \mod \mathcal{I} \tag{5}$$

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

REMARK 13. *Note that since* $\sum_{i=1}^N b_i b_i^*$ *has degree at most* $2D$*, and* $\Delta > 2D$*, we can use* $\mathrm{Mac}_\Delta(\mathbf{f})$ *to find its reduced form, which is* J*. Because of this reduction, we have that* $\deg(J) \leq D \leq \delta$*.*

Also note that the notion of generalized Jacobian was also introduced in [3]. Its name come from the fact that if $s = m$ *and if* Λ *is the so called residue (c.f. [15]), 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 [23].

DEFINITION 14. *Let* $p \in \mathcal{A}$*. The multiplication matrix* M_p *is the transpose of the matrix of the multiplication map*

$$M_p : \mathcal{A} \longrightarrow \mathcal{A}$$
$$g \mapsto pg$$

written in the basis S*.*

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

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

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* $S = [b_1, \ldots, b_N]$ *and* Tr *indicates the trace of a matrix.*

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

PROPOSITION 15. *Let* M_J *be the multiplication matrix of* J *with respect to the basis* S*. 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 12. For any $h \in \mathcal{A}$ we have that

$$h = \sum_{j=1}^{N} \Lambda(hb_j)b_j^* = \sum_{j=1}^{N} \Lambda(hb_j^*)b_j$$

$$\Rightarrow \quad hb_i = \sum_{j=1}^{N} \Lambda(hb_j^* b_i)b_j = M_h[i,j] = \Lambda(hb_j^* b_i)$$

$$\Rightarrow \quad Tr(h) = \sum_{i=1}^{N} \Lambda(hb_i^* b_i) = \Lambda(h\sum_{i=1}^{N} b_i^* b_i).$$

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

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

□

COROLLARY 16.

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

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

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

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

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

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

LEMMA 17. *There exists a unique matrix* $\mathfrak{R}_S(\mathbf{y})$ *of size* $|\mathrm{Mon}_{\leq}(\Delta) - S| \times |S|$ *such that*

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

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

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

where the columns of B are indexed by the monomials in S. Note here that by Assumption 2 the rows of $\mathrm{Mac}_\Delta(\mathbf{f})$ span $\mathcal{I}_\Delta$, and the monomials in S span the factor space $\mathbb{K}[\mathbf{x}]_\Delta/\mathcal{I}_\Delta$. These together imply that the (square) submatrix A is invertible.

Then

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

which implies that

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

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

□

By construction, the column of $\mathfrak{M}_S(\mathbf{y})$ indexed by $b_j \in S$ corresponds to the values of $b_j \cdot \Lambda \in \mathcal{A}^*$ on $b_1, \ldots, b_N$. The same column in $\mathfrak{R}_S(\mathbf{y})$ 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 18. *Let* $S = [b_1, \ldots, b_N]$ *be the basis of* $\mathcal{A}$ *as above, and let* $P \in \mathbb{K}[\mathbf{x}]$ *be a polynomial of degree at most* $D + 1$.

Define $\mathrm{Syl}_S(P)$ *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* $\deg(b_i P) \leq 2D + 1 \leq \Delta$*).*

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

THEOREM 19.

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

PROOF. Since the j-th column of the matrix

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

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 $\mathrm{Syl}_S(J)$ is the coefficient matrix of $b_i J$, we have

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

$$= [\Lambda(Jb_i b_j)]_{i,j=1}^{N}$$

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

□

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 [23, 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 20. *Let* $\tilde{R}$ *be a maximal non-singular submatrix of the matrix of traces* R*. Let* r *be the rank of* $\tilde{R}$*, and* $T := [b_{i_1}, \ldots, b_{i_r}]$ *be the monomials corresponding to*

the columns of $\tilde{R}$. Then T 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

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

is the multiplication matrix of x_k for $\sqrt{\mathcal{I}}$ with respect to T. Here $\tilde{R}_{x_k}$ 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 $\tilde{R}$.

ALGORITHM 21. 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 they satisfy the conditions in Assumption 2. An optional input is $D \leq \delta$, which by default is set to be δ.*

OUTPUT*: A basis T 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 T.*

1. *Compute $\mathrm{Mac}_\Delta(\mathbf{f})$ for $\Delta := \max(2D+1, \delta)$*
2. *Compute a basis S of $\mathbb{K}[\mathbf{x}]_\Delta / \langle \mathbf{f} \rangle_\Delta$ such that the polynomials in S have degrees at most D. Let $S = [b_1, \ldots, b_N]$.*
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 $\mathfrak{M}_S(\mathbf{y})$ defined in Definition 7 and $\mathfrak{R}_S(\mathbf{y})$ defined in Lemma 17.*
5. *Compute $\mathfrak{M}_S^{-1}(\mathbf{y})$ and the basis $[b_1^*, \ldots, b_N^*]$ defined in Definition 12.*
6. *Compute $J = \sum_{i=1}^N b_i b_i^* \mod \mathcal{I}$ using $\mathrm{Mac}_\Delta(\mathbf{f})$.*
7. *Compute $\mathrm{Syl}_S(J)$ and $\mathrm{Syl}_S(x_k J)$ for $k = 1, \ldots, m$ defined in Definition 18.*
8. *Compute*

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

and

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

for $k = 1, \ldots, m$.

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

REMARK 22. *Since the bound given in Theorem 3 might be too high, it seems reasonable to design the algorithm in an iterative fashion, similarly to the algorithms in [31, 32, 40], 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 23. *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 $|\mathrm{Mon}_{\leq}(\Delta)| \times |S|$ matrix X such that it has full rank and $\mathrm{Mac}_\Delta(\mathbf{f}) \cdot X = \mathbf{0}$ in the place of*

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

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 $\mathrm{Syl}_S(J) \cdot X$, and $\tilde{Q}_{x_k}$ is the submatrix of $\mathrm{Syl}_S(x_k J) \cdot X$ 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 T as the above Algorithm.

REMARK 24. *As M_{x_k} is the matrix of multiplication by x_k modulo the radical ideal $\sqrt{\mathcal{I}}$, its eigenvectors are (up to a non-zero scalar) the interpolation polynomials at the roots of $\mathcal{I}$. Similarly the eigenvectors of the transposed matrix $M_{x_k}^t$ are (up to a non-zero scalar) the evaluation at the roots ζ of $\mathcal{I}$ (see [34, 15] for more details). The vector which represents this evaluation at ζ in the dual space $\mathcal{A}^*$ is the vector of values of $[b_1, \ldots, b_N]$ at ζ. To obtain these vectors, we solve the generalized eigenvalue problem $(\tilde{R}_{x_k}^t - z\tilde{R}^t)\, w = 0$ and compute $v = \tilde{R}^t w$. The vectors v will be of the form $[b_1(\zeta), \ldots, b_N(\zeta)]$ for ζ a root of $\mathcal{I}$. If $b_1 = 1, b_2 = x_1, \ldots, b_{m+1} = x_m$, we can read directly the coordinates of ζ from this vector.*

4. EXAMPLES

In this section we present three examples. Each of them has three polynomials in two variables. The first one is a system which has roots with multiplicities, the second one is a system which has clusters of roots, and the third one is a system obtained by perturbing the coefficients of the first one. For each of them we compute the Macaulay matrix $\mathrm{Mac}_\Delta(\mathbf{f})$, the vector $\mathbf{y}$ in its nullspace, the moment matrix $\mathfrak{M}_S(\mathbf{y})$, the polynomial J, the matrix of traces R and the (approximate) multiplication matrices of the (approximate) radical, following Algorithm 21.

The exact system:

$$\mathbf{f} = \begin{cases} 3x_1^2 + 18x_1x_2 - 48x_1 + 21x_2^2 - 114x_2 + 156 \\ x_1^3 - \frac{259}{4}x_1^2x_2 + \frac{493}{4}x_1^2 - \frac{611}{4}x_1x_2^2 + \frac{2423}{4}x_1x_2 - \frac{1175}{2}x_1 \\ \quad -5x_2^3 + 6x_2^2 + x_2 + 5 \\ x_1^3 + \frac{81}{4}x_1^2x_2 - \frac{163}{4}x_1^2 + \frac{21}{4}x_1x_2^2 + \frac{87}{4}x_1x_2 - \frac{151}{2}x_1 - x_2^3 \\ \quad +4x_2^2 + 2x_2 + 3 \end{cases}$$

$\mathbf{f}$ has common roots $(-1, 3)$ of multiplicity 3 and $(2, 2)$ of multiplicity 2.

The system with clusters:

$$\bar{\mathbf{f}} = \begin{cases} 3x_1^2 + 17.4x_1x_2 - 46.5x_1 + 23.855x_2^2 - 127.977x_2 + 171.933 \\ x_1^3 - 72.943x_1^2x_2 + 139.617x_1^2 - 8.417x_1x_2^2 - 124.161x_1x_2 \\ \quad +295.0283x_1 - 5x_2^3 + 6x_2^2 + x_2 + 5 \\ x_1^3 + 21.853x_1^2x_2 - 43.658x_1^2 - 27.011x_1x_2^2 + 185.548x_1x_2 \\ \quad -274.649x_1 - x_2^3 + 4x_2^2 + 2x_2 + 3 \end{cases}$$

$\bar{\mathbf{f}}$ has two clusters: $(-1, 3)$, $(-0.9, 3)$, $(-1.01, 3.1)$ and $(2, 2)$, $(1.9, 2)$ each of radius 10^{-1}.

The perturbed system:

$$\hat{\mathbf{f}} = \begin{cases} 3x_1^2 + 18x_1x_2 - 48x_1 + 21.001x_2^2 - 113.999x_2 + 156.001 \\ 1.001x_1^3 - 64.751x_1^2x_2 + 123.250x_1^2 - 152.750x_1x_2^2 \\ \quad +605.751x_1x_2 - 587.500x_1 - 4.999x_2^3 + 6.0001x_2^2 + x_2 + 5 \\ x_1^3 + 20.249x_1^2x_2 - 40.750x_1^2 + 5.249x_1x_2^2 + 21.749x_1x_2 \\ \quad -75.5x_1 - 1.001x_2^3 + 4x_2^2 + 2x_2 + 3 \end{cases}$$

is obtained from $\mathbf{f}$ by a random perturbation of size 10^{-3}. This system has no common roots.

We set $\delta = 6$, $D = 2$ and $\Delta = 6$. The Sylvester matrices in all three cases were size 28×28 and in the first two cases they had rank 23 while in the last case it was full rank. In the first two cases the fact that the corank is 5 indicates that there are 5 solutions, counting multiplicities. For these cases we computed a basis $S := [1, x_1, x_2, x_1x_2, x_1^2]$ for the factor algebra by taking maximum rank submatrices of the Macaulay matrices. In the third case, we simply erased the columns of the Macaulay matrix corresponding to the monomials in S. From here, we chose random elements in the nullspaces of the (cropped) Macaulay matrices to compute the moment matrices:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{-6}{7} & \frac{-34}{7} \\ 0 & 0 & \frac{-52}{7} & \frac{10}{7} & \frac{-6}{7} \\ 0 & \frac{-6}{7} & \frac{10}{7} & \frac{-40}{7} & \frac{-36}{7} \\ 0 & \frac{-34}{7} & \frac{-6}{7} & \frac{-36}{7} & \frac{-276}{7} \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1.787 & -20.059 \\ 0 & 0 & -7.207 & 1.219 & 1.787 \\ 0 & 1.787 & 1.219 & 7.702 & -43.499 \\ 0 & -20.059 & 1.787 & -43.499 & -43.644 \end{bmatrix} \text{ and}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -0.858 & -4.848 \\ 0 & 0 & -7.428 & 1.428 & -0.858 \\ 0 & -0.858 & 1.428 & -5.719 & -5.125 \\ 0 & -4.848 & -0.858 & -5.125 & -39.404 \end{bmatrix}.$$

The polynomials J, computed from the moment matrices are:

$$\begin{aligned} J &= 5 - \frac{3}{10}x_1 - \frac{26}{15}x_2 - \frac{1}{30}x_1x_2 - \frac{1}{5}x_1^2 \\ \bar{J} &= 5 + 0.916x_1 - 1.952x_2 - 0.636x_1x_2 - 0.106x_1^2 \\ \hat{J} &= 4.999 - 0.306x_1 - 1.733x_2 - 0.030x_1x_2 - 0.200x_1^2. \end{aligned}$$

After computing the matrices $\mathrm{Syl}_S(J)$ and $\mathfrak{R}_S(\mathbf{y})$, we obtain the matrices of traces:

$$\begin{bmatrix} 5 & 1 & 13 & -1 & 11 \\ 1 & 11 & -1 & 25 & 13 \\ 13 & -1 & 35 & -11 & 25 \\ -1 & 25 & -11 & 59 & 23 \\ 11 & 13 & 25 & 23 & 35 \end{bmatrix},$$

$$\begin{bmatrix} 4.999 & 0.990 & 13.100 & -1.031 & 10.440 \\ 0.990 & 10.440 & -1.031 & 23.812 & 12.100 \\ 13.100 & -1.031 & 35.610 & -11.206 & 23.812 \\ -1.031 & 23.812 & -11.206 & 56.533 & 21.337 \\ 10.440 & 12.100 & 23.812 & 21.337 & 31.729 \end{bmatrix} \text{ and}$$

$$\begin{bmatrix} 5 & 0.995 & 13.002 & -1.017 & 11.003 \\ 0.995 & 10.999 & -1.015 & 25.019 & 12.913 \\ 13.002 & -1.017 & 35.013 & -11.064 & 25.029 \\ -1.017 & 25.0256 & -11.061 & 59.129 & 22.770 \\ 11.003 & 12.870 & 25.0519 & 22.644 & 34.968 \end{bmatrix}.$$

The first matrix R has rank 2, while $\bar{R}$ and $\hat{R}$ have rank 5. In the first case we follow steps 9 and 10 of Algorithm 21 to obtain the multiplication matrices of the radical with respect to its basis $T = [1, x_1]$:

$$\begin{bmatrix} 1 & 1 \\ 2 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} \frac{7}{3} & \frac{-1}{3} \\ \frac{-2}{3} & \frac{8}{3} \end{bmatrix},$$

with respective eigenvalues $[2, -1]$ and $[2, 3]$.

For the second case we use the method described in [22, 23] to compute the approximate multiplication matrices of the approximate radical of the clusters. Using Gaussian Elimination with complete pivoting, we found that the almost vanishing pivot elements were of the order of magnitude of 10^{-1} which clearly indicated the numerical rank. Using the submatrices obtained from the complete pivoting algorithm we got the following approximate multiplication matrices of the approximate radical with respect to the basis $T = [x_1x_2, x_2]$:

$$\begin{bmatrix} 0.976 & 1 \\ 1.895 & -4.623 \times 10^{-7} \end{bmatrix} \text{ and } \begin{bmatrix} 2.346 & -0.354 \\ -0.671 & 2.691 \end{bmatrix}.$$

The norm of the commutator of these matrices is 0.002 and their eigenvalues are respectively $[1.949, -0.972]$ and $[2.001, 3.036]$. Note that the corresponding roots $[1.949, 2.001]$ and $[-0.972, 3.036]$ are within 10^{-2} distance from the centers of gravity of the clusters, as was shown in [22, 23] (recall that the radius of the clusters was 10^{-1}).

In the third case, the numerical rank was not easy to determine using either SVD or complete pivoting. However, when we assume that the numerical rank of R is 2, and we cut the matrix R using the output of the complete pivoting algorithm, then we obtain the multiplication matrices with respect to the basis $T = [x_1x_2, x_2]$:

$$\begin{bmatrix} 1.005 & 0.992 \\ 1.992 & 0.005 \end{bmatrix} \text{ and } \begin{bmatrix} 2.327 & -0.330 \\ -0.663 & 2.664 \end{bmatrix}.$$

The norm of the commutator of these matrices is 0.010 and their eigenvalues are respectively $[1.997, -0.987]$ and $[1.999, 2.993]$ (recall that the perturbation of the polynomials was of size 10^{-3}).

5. CONCLUSION

In this paper 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. A follow-up paper will consider 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 $\sqrt{\mathcal{I}}$.

6. REFERENCES

[1] I. Armendáriz and P. 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] E. 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.

[3] E. Becker, J. P. Cardinal, M.-F. 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.

[4] E. Becker and T. 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.

[5] E. 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.

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

[7] J. Cardinal and B. 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.

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

[9] E. Cattani, A. Dickenstein, and B. Sturmfels. Residues and resultants. *J. Math. Sci. Univ. Tokyo*, 5(1):119–148, 1998.

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

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

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

[13] G. M. Díaz-Toca and L. 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.

[14] L. Dickson. *Algebras and Their Arithmetics*. University of Chicago Press, 1923.

[15] M. Elkadi and B. Mourrain. *Introduction à la résolution des systèmes polynomiaux*, volume 59 of *Mathématiques et Applications*. 2007.

[16] P. Gianni and T. 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.

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

[18] L. 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.

[19] L. González-Vega and G. 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.

[20] G.-M. Greuel and G. Pfister. *A* **Singular** *introduction to commutative algebra*. 2002. With contributions by Olaf Bachmann, Christoph Lossen and Hans Schönemann, With 1 CD-ROM (Windows, Macintosh, and UNIX).

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

[22] I. Janovitz-Freireich, L. 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.

[23] I. Janovitz-Freireich, L. 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.

[24] H. Kobayashi, S. Moritsugu, and R. W. Hogan. On radical zero-dimensional ideals. *J. Symbolic Comput.*, 8(6):545–552, 1989.

[25] T. Krick and A. 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.

[26] T. Krick and A. 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.

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

[28] Y. 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.

[29] Y. 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.

[30] Y. N. Lakshman and D. 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.

[31] J. B. Lasserre, M. Laurent, and P. Rostalski. A unified approach to computing real and complex zeros of zero-dimensional ideals. *preprint*, 2007.

[32] J. B. Lasserre, M. Laurent, and P. Rostalski. Semidefinite characterization and computation of zero-dimensional real radical ideals. *to appear in Foundations of Computational Mathematics*, 2007.

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

[34] B. 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.

[35] P. Pedersen, M.-F. Roy, and A. 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.

[36] F. 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.

[37] G. Scheja and U. Storch. Über Spurfunktionen bei vollständigen Durschnitten. *J. Reine Angew Mathematik*, 278:174–190, 1975.

[38] R. P. Stanley. *Combinatorics and commutative algebra*, volume 41 of *Progress in Mathematics*. Birkhäuser, 1996.

[39] K. Yokoyama, M. Noro, and T. Takeshima. Solutions of systems of algebraic equations and linear maps on residue class rings. *J. Symbolic Comput.*, 14(4):399–417, 1992.

[40] L. Zhi and G. 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.