Computing Approximate Radicals using Bezoutians (Extended Abstract)

Itnuit Janovitz-Freireich† Bernard Mourrain*
Lajos Rónyai‡ Ágnes Szántó†

Abstract

Consider $I \subset \mathbb{C}[x_1, \ldots, x_m]$, a zero dimensional complete intersection ideal, with $I = (f_1, \ldots, f_m)$. Assume that I has clusters of roots, each cluster of radius at most ε in the ∞-norm. We compute the "approximate radical" of I, i.e. an ideal which contains one root for each cluster, corresponding to the center of gravity of the points in the cluster, up to an error term asymptotically bounded by ε^2. The main bottleneck of our method is the computation of the "matrix of traces", a matrix with entries which are trace functions of the roots of I with respect to some basis of $\mathbb{C}[x_1, \ldots, x_m]/I$. We investigate how to compute a matrix of traces from the Bezoutian of $f_1, \ldots, f_m$ and their Jacobian J. We use work by Mourrain and Pan to reduce the Bezout matrix to a matrix of traces with respect to a certain canonical basis of $\mathbb{C}[x_1, \ldots, x_m]/I$.

1 Introduction

Let $f_1, \ldots, f_m \in \mathbb{C}[\mathbf{x}]$ be polynomials in m variables $\mathbf{x} = [x_1, \ldots, x_m]$ and assume that they have finitely many roots forming the clusters $C_1, \ldots, C_k$ such that each cluster C_i has n_i roots within a radius of ε in the ∞-norm for $i = 1, \ldots, k$. Let $n := \sum_{i=1}^{k} n_i$.

In [9, 10] a "global" method was devised to compute an *approximate radical* of $I := \langle f_1, \ldots, f_m \rangle$, denoted by $\widetilde{\sqrt{I}}$, i.e. a method that works simultaneously for

† Mathematics Department, North Carolina State University, Raleigh, NC, USA. Research supported by NSF grants CCR-0306406 and CCR-0347506.

‡ Computer and Automation Institute, Hungarian Academy of Sciences and Budapest University of Technology and Economics, Budapest, Hungary. Research supported in part by OTKA grants T42481 and T42706 and NK63066.

* GALAAD, INRIA, Sophia Antipolis, France.

all clusters and does not use any local information about the roots in the clusters, only the coefficients of the system of polynomials defining I. It was shown that the approximate radical has exactly one root for each cluster, corresponding to the arithmetic mean of the cluster up to an error bounded by ε^2.

The method to compute $\widetilde{\sqrt{I}}$ uses Gaussian elimination with complete pivoting or singular value decomposition of the $n \times n$ matrix of traces R (see definition in section 2). In [10] it is shown that a partial LU decomposition of R obtained by k steps of the Gaussian elimination with complete pivoting will result in a U matrix having almost vanishing entries of magnitude ε^2 in the last $n-k$ rows. Similarly, the last $n-k$ singular values of R are of the order of magnitude of ε^2.

The computationally most expensive part of the method in [9, 10] is the computation of the matrix of traces R. As pointed out, direct methods not involving the computation of the multiplication matrices are preferred since R is shown to be continuous with respect to root perturbations around multiplicities while multiplication matrices are generally not. Methods for computing the matrix of traces directly from the generating polynomials of I, without using multiplication matrices, include [2, 4, 5, 7, 1, 6].

Here we investigate how to compute matrices of traces using Bezoutians. Our approach is based on [13, 12]. The advantage of using Bezoutians for the computation of the matrix of traces over the methods mentioned above is that it is both conceptually and computationally simpler.

In the univariate case it is proved that the Bezoutian matrix of a univariate polynomial f and its derivative f' corresponds to 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 17). Unfortunately, the Bezout matrix cannot directly be expressed as a matrix of traces. However, in [13] 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 I.

Now the question is how to find the reduced version of the Bezout matrix above without further information on the structure of the quotient algebra $\mathbb{C}[x_1, \ldots, x_m]/I$, e.g. without Gröbner Bases or multiplication matrices. We can adapt the results of [12] to get an algorithm which computes the required identities in the ideal in order to reduce the Bezout matrix, using only Bezoutians of $f_1, \ldots, f_m$ and either one of the variables x_i, for $i = 1, \ldots, m$, or 1.

Combining these results gives an improvement to the approximate radical algorithm by explicitly addressing the computation of the matrix of traces using a well studied and conceptually simpler object such as the Bezoutian.

2 Radical and the Matrix of Traces

Our main construction is based on the following results describing the elements of the radical of an associative algebra A using traces of elements:

Theorem 1 (Dickson [8] pp.106-107)**.** *An element x of an associative algebra A over a field F of characteristic 0 is properly nilpotent if and only if $Tr(xy) = 0$ for every $y \in A$.*

The above theorem can be applied to the special case of commutative algebras which are quotients of polynomial rings. Consider the system of polynomial equations

$$\mathbf{f}(\mathbf{x}) = 0$$

where $\mathbf{f} = [f_1, \ldots, f_m]$ and each f_i is a polynomial in the variables $\mathbf{x} = [x_1, \ldots, x_m]$. Assume that the polynomials $f_1, \ldots, f_m$ have finitely many roots in $\mathbb{C}^m$, which implies that the algebra $A = \mathbb{C}[\mathbf{x}]/I$ is finite dimensional, where I is the ideal generated by the polynomials in $\mathbf{f}$. Denote the dimension of A over $\mathbb{C}$ by n and let $B = [b_1, \ldots, b_n]$ be a basis of A. By a slight abuse of notation we denote the elements of the basis B which are in A and some fixed preimages of them in $\mathbb{C}[x_1, \ldots, x_m]$ both by $b_1, \ldots, b_n$. Let $\{\mathbf{z}_1, \ldots, \mathbf{z}_n\} \subset \mathbb{C}^m$ be the set of common roots of the polynomials in $\mathbf{f}$, taken with the appropriate multiplicities which can be read from the primary decomposition of I. We will use the multiplication matrices M_g of $g \in A$ with respect to the basis B, defined as the matrix of the multiplication map

$$\begin{aligned} m_g : \ A &\longrightarrow A \\ [f] &\mapsto [fg] \end{aligned}$$

written in the basis B. Using the fact that

$$Rad(A) = \sqrt{I}/I \subseteq \mathbb{C}[\mathbf{x}]/I = A,$$

we can reword Theorem 1 in the following way:

Corollary 2. *Let $p \in \mathbb{C}[\mathbf{x}]$ and $\bar{p}$ be the image of p in A. Using the above notation, the following statements are equivalent:*

(i) $p \in \sqrt{I}$

(ii) $\bar{p} \in Rad(A)$

(iii) $Tr(M_{\bar{p}b_j}) = 0$ *for all* $j = 1, \ldots, n$.

We can now use the previous corollary to characterize the radical of A as the nullspace of a matrix defined as follows:

Definition 3. *The* matrix of traces *is the $n \times n$ symmetric matrix:*

$$R = \left[Tr(M_{b_i b_j})\right]_{i,j=1}^{n}$$

where $M_{b_i b_j}$ is the multiplication matrix of $b_i b_j$ as an element in A in terms of the basis $B = [b_1, \ldots, b_n]$ and Tr indicates the trace of a matrix.

Corollary 4. *An element*

$$r = \sum_{k=1}^{n} c_k b_k$$

of the quotient ring A with basis $B = [b_1, \ldots, b_n]$ is in the radical of A if and only if $[c_1, \ldots, c_n]$ is in the nullspace of the matrix of traces R.

We have the following result for the entries of the matrix of traces R expressed in terms of the roots of the polynomial system.

Proposition 5. *The matrix of traces R of the system $\mathbf{f}$ with respect to $B = [b_1, \ldots, b_n]$ can be expressed in terms of the common roots $\{\mathbf{z}_1, \ldots, \mathbf{z}_n\}$ of $\mathbf{f}$ as*

$$R = \left[\sum_{s=1}^{n} b_i b_j(\mathbf{z}_s)\right]_{i,j=1}^{n}$$

where $b_i b_j(\mathbf{z}_s)$ indicates the evaluation of the polynomial $b_i b_j$ at the point $\mathbf{z}_s$.

This implies that the matrix of traces is a continuous function of the roots, even if the system has possible root multiplicities. We remark here that the multiplication matrices are in general not continuous functions of the roots.

3 Approximate Case

In this section we will describe the results of [10]. In the rest of the paper we will assume that the size of the clusters is a parameter ε. More precisely, in the following definition we formally explain the mathematical setting where our results will hold.

Definition 6. *Let $\mathbf{z}_i = [z_{i,1}, \ldots, z_{i,m}] \in \mathbb{C}^m$ for $i = 1, \ldots, k$, and consider k clusters $C_1, \ldots, C_k$ of size $|C_i| = n_i$ such that $\sum_{i=1}^{k} n_i = n$, each of radius proportional to the parameter ε in the ∞-norm around $\mathbf{z}_1, \ldots, \mathbf{z}_k$:*

$$\begin{aligned} C_i(\varepsilon) =& \{[z_{i,1} + \delta_{i,1,1}\varepsilon, \ldots, z_{i,m} + \delta_{i,1,m}\varepsilon], \ldots, [z_{i,1} + \delta_{i,n_i,1}\varepsilon, \ldots, z_{i,m} + \delta_{i,n_i,m}\varepsilon]\} \\ =& \{\mathbf{z}_i + \vec{\delta}_{i,1}\varepsilon, \ldots, \mathbf{z}_i + \vec{\delta}_{i,n_i}\varepsilon\}, \end{aligned} \tag{1}$$

where $|\delta_{i,j,r}| < 1$ for all $i = 1, \ldots, k$, $j = 1, \ldots, n_i$, $r = 1, \ldots, m$.

We will need the following assumption throughout the paper:

Assumption 7. *Denote by $\mathbb{C}[V(\varepsilon)]$ the coordinate ring of $V(\varepsilon) := \bigcup_{i=1}^{k} C_i(\varepsilon)$. Throughout this paper we make the assumption that the basis B for $\mathbb{C}[V(\varepsilon)]$ is independent of ε for sufficiently small values of ε.*

The following proposition gives asymptotic bounds for the entries of the matrix obtained from a partial Gauss elimination with complete pivoting on the matrix of traces R for the case where the n roots of the system correspond to k clusters, each of them with n_i roots ($i = 1, \ldots, k$) and radius proportional to ε in the max-norm.

Proposition 8. *Let $B = [b_1, \ldots, b_n] \in \mathbb{C}[x_1, \ldots, x_m]^n$. Let $\{\mathbf{z}_1, \ldots, \mathbf{z}_k\} \in \mathbb{C}^m$ and the clusters $C_1, \ldots, C_k$ around $\{\mathbf{z}_1, \ldots, \mathbf{z}_k\}$ be as in Definition 6.*

Let R be the matrix of traces associated to $C_1 \cup \cdots \cup C_k$ and B (see Definition 3 and Proposition 5). Assume that there exist permutations of the rows and columns of $R_0 := R|_{\varepsilon=0}$ such that the resulting matrix has rank k and is regular. Then, after k steps of Gaussian elimination with complete pivoting on R we get a partially row reduced matrix U_k, such that its last $n-k$ rows satisfy

$$[U_k]_{i,j} = \begin{cases} 0, & \text{if } j \leq k \\ c_{i,j}\varepsilon^2 + h.o.t.(\varepsilon) \quad \in \mathbb{C}[[\varepsilon]] & \text{if } j > k \end{cases} \quad \text{for} \quad i = k+1, \ldots, n. \tag{2}$$

The values of $c_{i,j} \in \mathbb{C}$ depend on n, $\{\mathbf{z}_1, \ldots, \mathbf{z}_k\}$, $\{\vec{\delta}_{s,t}\}$ and B (we will give a bound for $c_{i,j}$ in Proposition 9). Here $h.o.t.(\varepsilon)$ denotes the higher order terms in ε. Moreover, the formal power series in (2) are convergent in a sufficiently small neighborhood of $\varepsilon = 0$.

The next proposition gives a bound for the coefficient $c_{i,j}$ of ε^2 in (2). It also gives an idea of the magnitude of the threshold one can use to decide on the numerical rank which would additionally indicate how small the size of the clusters need to be for our method to work.

Proposition 9. *Let $B = [b_1, \ldots, b_n] \in \mathbb{C}[x_1, \ldots, x_m]^n$. Let $\{\mathbf{z}_1, \ldots, \mathbf{z}_k\} \in \mathbb{C}^m$. Let the clusters $C_1, \ldots, C_k$ around $\{\mathbf{z}_1, \ldots, \mathbf{z}_k\}$ be as in (1) with $|\delta_{i,j,r}| \leq 1$ for all $i = 1, \ldots, k$, $j = 1, \ldots, n_i$, $r = 1, \ldots, m$. Let R be the matrix of traces associated to $C_1 \cup \cdots \cup C_k$ and B.*

Let $\mathbf{b}'$ be such that

$$\mathbf{b}' \geq max_{\{i,l,r\}} \left\{ \left| \frac{\partial b_l}{\partial x_r}(\mathbf{z}_i) \right| \right\}. \tag{3}$$

Assume that the GECP applied to R also implies complete pivoting on $R|_{\varepsilon=0}$. Then the bound for the coefficients $c_{i,j}$ of ε^2 in the U_k matrix, obtained after k steps of the GECP applied to the matrix of traces R, is given by

$$|c_{i,j}| \leq \alpha \cdot (\mathbf{b}')^2,$$

where $\alpha = 4(n-k)(k+1)^2 m^2$.

The next Proposition shows that the $k+1$-th singular value of R is asymptotically equal to ε^2.

Proposition 10. *Let R be the matrix of traces associated to $C_1 \cup \cdots \cup C_k$ and B where the clusters $C_1, \ldots, C_k$ around $\mathbf{z}_1, \ldots, \mathbf{z}_k \in \mathbb{C}^m$ are as in (1) and $B = [b_1, \ldots, b_n] \in \mathbb{C}[x_1, \ldots, x_m]^n$. Let $\sigma_1 \geq \cdots \geq \sigma_n$ be the singular values of R. Then*

$$\sigma_{k+1} = \Omega\varepsilon^2 + h.o.t.(\varepsilon)$$

where

$$\Omega \leq 4(n-k)^2(k+1)^2 m^2 \sqrt{\frac{2n+2nk-k^2-k}{2}}(\mathbf{b}')^2$$

and $\mathbf{b}'$ is defined in (3).

The above results show that we can use GECP or SVD to compute the numerical rank k of the matrix of traces R. Once we have the estimation on the number of clusters k we can define the *approximate radical* as follows:

Definition 11. *Let $B = [b_1, \ldots, b_n] \in \mathbb{C}[x_1, \ldots, x_m]^n$ and the clusters $C_1, \ldots, C_k$ be as in Definition 6. Let R be the matrix of traces associated to $C_1 \cup \cdots \cup C_k$ and B. Denote by $\tilde{R}$ the matrix obtained by applying the permutation on the rows and columns of R resulting from the Gaussian elimination with complete pivoting. By renaming the elements of B we can still assume that the columns of $\tilde{R}$ correspond to the basis vector B, but the rows will correspond to a permutation $\sigma(B) := [b_{\sigma(1)}, \ldots, b_{\sigma(n)}]$.*

We define the vectors $\mathbf{v}_{i,j} \in \mathbb{C}(\varepsilon)^k$ for $i = 1, \ldots m$ and $j = 1, \ldots k$, as the solutions of the following mk linear systems:

$$\tilde{R}^{(k)}\mathbf{v}_{i,j} = \mathbf{r}_{i,j} \quad i = 1, \ldots, m \quad j = 1, \ldots, k, \tag{4}$$

where the left hand sides are always the $k \times k$ principal submatrix of $\tilde{R}$, while for any fixed i and j the right hand side of (4) is defined as

$$\mathbf{r}_{i,j} := \begin{bmatrix} Tr(x_i b_j b_{\sigma(1)}) \\ \vdots \\ Tr(x_i b_j b_{\sigma(k)}) \end{bmatrix} \in \mathbb{C}^k. \tag{5}$$

Note that one can compute the vectors $\mathbf{r}_{i,j}$ the same way as the columns of the matrix of traces. Then we define the following mk polynomials:

$$f_{i,j} := x_i b_j - \left(\sum_{s=1}^{k} [\mathbf{v}_{i,j}]_s b_s\right) \quad i = 1, \ldots, m, \quad j = 1, \ldots, k. \tag{6}$$

We will call the approximate radical ideal of the clusters $C_1 \cup \cdots \cup C_k$ the ideal generated by

$$\widetilde{\sqrt{I}} := \langle f_{i,j} \ : \ i = 1, \ldots, m, \ j = 1, \ldots, k \rangle.$$

Finally, we prove that the common roots of the approximate radical ideal correspond to the arithmetic mean of the clusters modulo ε^2.

Proposition 12. *Let $B = [b_1, \dots, b_n]$, $\{\mathbf{z}_1, \dots, \mathbf{z}_k\}$ and for $i = 1, \dots, k$*

$$\begin{aligned} C_i =&\{[z_{i,1} + \delta_{i,1,1}\varepsilon, \dots, z_{i,m} + \delta_{i,1,m}\varepsilon], \dots, \\ &\dots [z_{i,1} + \delta_{i,n_i,1}\varepsilon, \dots, z_{i,m} + \delta_{i,n_i,m}\varepsilon]\} \end{aligned}$$

be as in Definition 6. Let $\vec{\xi_s} = [\xi_{s,1}, \dots, \xi_{s,m}]$ for $s = 1, \dots k$ be defined as

$$\xi_{s,i} := z_{s,i} + \frac{\sum_{r=1}^{n_s} \delta_{s,r,i}}{n_s}\varepsilon \quad i = 1, \dots, m. \tag{7}$$

Then $\vec{\xi_1}, \dots, \vec{\xi_k}$ satisfy modulo ε^2 the defining equations $\{f_{i,j}\}$ of the approximate radical ideal of $C_1 \cup \dots \cup C_k$ defined in Definition 11.

4 Matrix of Traces and the Bezoutian

The bottleneck of the computation of the approximate radical ideal using the method presented above is the computation of the matrix of traces. In this section we study how to obtain trace matrices using Bezoutians. First we discuss the univariate case as a motivation, after which we will describe the general multivariate case.

4.1 Univariate Case

In this section we will follow the work of Mourrain and Pan [13]. We start by defining the univariate Bezout matrix.

Definition 13. *Let $f, g \in \mathbb{C}[x]$ 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*

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

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

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

We will need the following definition:

Definition 14. *The* Horner basis *for the polynomial $f = f(x) = a_0 + a_1 x + \dots + a_d x^d$ is the set $\{H_{d-1}, \dots, H_0\}$ with*

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

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

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

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 15.

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

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

Theorem 15 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 16. *The smallest degree polynomial of the form* $\sum_{i=0}^{d-1} r_i H_i(x)$ *such that* $[r_0, \ldots, r_{d-1}]^T$ *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 [3] and [11] are good references for the Bezout (Dixon) matrix described below.

Definition 17. *Let*

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

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

$$X_1 = [x_1, \ldots, x_m], X_2 = [y_1, x_2, \ldots, x_m], \ldots, X_m = [y_1, y_2, \ldots, y_m].$$

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

$$\mathfrak{B}_{f_0}(\mathbf{x}, \mathbf{y}) := \det \begin{vmatrix} f_1(X_1) & \frac{f_1(X_1) - f_1(X_2)}{x_1 - y_1} & \cdots & \frac{f_1(X_{n-1}) - f_1(X_n)}{x_{n-1} - y_{n-1}} \\ f_2(X_1) & \frac{f_2(X_1) - f_2(X_2)}{x_1 - y_1} & & \frac{f_2(X_{n-1}) - f_2(X_n)}{x_{n-1} - y_{n-1}} \\ \vdots & \vdots & & \vdots \\ f_n(X_1) & \frac{f_n(X_1) - f_n(X_2)}{x_1 - y_1} & \cdots & \frac{f_n(X_{n-1}) - f_n(X_n)}{x_{n-1} - y_{n-1}} \end{vmatrix}. \quad (8)$$

The Bezout matrix *of the system* $[f_0, f_1, \ldots, f_n[$*, denoted by* B_{f_0}*, is the coefficient matrix of the Bezoutian, i.e. if we write*

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

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

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

Our goal is to compute a matrix of traces for the system $\mathbf{f} = [f_1, \ldots, f_m]$ from the Bezout matrix B_J of the system $[J, f_1, \ldots, f_m]$ 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 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 18. *Let $\mathbf{f} = [f_1, \ldots, f_m] \in \mathbb{C}[x_1, \ldots, x_m]^m$ and assume that the factor algebra $A(\mathbf{x}) := \mathbb{C}[\mathbf{x}]/I$ has dimension n over $\mathbb{C}$, where I is the ideal generated by the polynomials in $\mathbf{f}$. For some $f_0 \in \mathbb{C}[\mathbf{x}]$ 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*

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

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

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

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

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

In [13] the following expression was given for the reduced Bezout matrix $\overline{B}_J$ of the system $[J, f_1, \ldots, f_m]$ in terms of a matrix of traces of $f_1, \ldots, f_m$:

Theorem 19. *Let $\mathbf{f}$, $A(\mathbf{x})$, $A(\mathbf{y})$ and the bases B, B' be as in Definition 18. 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 B and B'. Then*

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

where the basis $[\omega_1, \ldots, \omega_n]$ of $A(\mathbf{x})$ is defined from the the reduced Bezoutian $\overline{\mathfrak{B}}_1$ of the system $[1, f_1, \ldots, f_m]$ with respect to the bases B and B' as follows:

$$\overline{\mathfrak{B}}_1(\mathbf{x}, \mathbf{y}) =: \sum_{b_i' \in B'} \omega_i(\mathbf{x}) b_i'(\mathbf{y}).$$

Using Theorem 19 and the results in Sections 2 and 3 one can define the approximate radical of an ideal with clusters in terms of the numerical kernel of the reduced Bezout matrix of $[J, f_1, \dots, f_m]$ using the basis $[\omega_1, \dots, \omega_n]$ obtained from $\overline{\mathfrak{B}}_1$.

The question that remains is how to compute the reduced Bezout matrix without computing Gröbner Bases or multiplication matrices for the ideal I.

In order to compute the reduced Bezout matrix $\overline{B}_{f_0}$ of the system $[f_0, \dots, f_m]$ with respect to some bases $B = [b_1, \dots, b_n]$ of $A(\mathbf{x})$ and $B' = [b'_1, \dots, b'_n]$ 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 $F, G \in I$, $c_b, c_{b'} \in \mathbb{C}$ and E and E' were defined in Definition 17. 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 $i = 1, \dots, n$, 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.

In [12], it was shown that the computation of the Bezoutians $\mathfrak{B}_{x_i}$ of the system $[x_i, f_1, \dots, f_m]$, for $i = 1, \dots, m$, as well as the Bezoutian $\mathfrak{B}_1$ of the system $[1, f_1, \dots, f_m]$, gives sufficient information of the structure of I in order to find the reduced Bezout matrix $\overline{B}_{f_0}$ for any $f_0 \in \mathbb{C}[\mathbf{x}]$. Here we describe a summary of the method in [12].

First notice that

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

The initial step of the method in [12] is to obtain ideal elements which are in V and W from $x_i \mathfrak{B}_1 - \mathfrak{B}_{x_i}$ and $y_i \mathfrak{B}_1 - \mathfrak{B}_{y_i}$.

In order to obtain additional ideal elements, the paper proposes the following steps to be repeated iteratively until no new elements of the ideal are found.

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

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 $I(\mathbf{x}) \cap V$, and also that the Bezout matrix B_1, written in terms of these new bases, has a lower block triangular structure. By writing the matrices B_{x_i} in terms of the new bases for V and W, one can obtain new elements in $I(\mathbf{x}) \cap V$.

Diagonalization step: After the column reduction step one can transform B_1 into a block diagonal form which, by repeating the same transformation on the matrices 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.

Using the above algorithm we can prove the following theorem:

Theorem 20. *Let $f_0, f_1, \dots, f_n$ be as above. Assume that upon termination, the algorithm outlined above computes new bases $[v_1, \dots, v_{|E|}]$ for V and $[w_1, \dots, w_{|E'|}]$ for W such that for some r and r'*

$$v_{r+1}, \dots, v_{|E|} \in I(\mathbf{x}) \cap V \quad \text{and} \quad w_{r'+1}, \dots, w_{|E|} \in I(\mathbf{y}) \cap W.$$

Then $r = r' = n$ and the $n \times n$ principal submatrix of B_{f_0}, written in the bases $[v_1, \dots, v_{|E|}]$ and $[w_1, \dots, w_{|E'|}]$, is equal to the reduced Bezout matrix $\overline{B}_{f_0}$ with respect to the bases $B = [v_1, \dots, v_n]$ of $A(\mathbf{x})$ and $B' = [w_1, \dots, w_n]$ and $A(\mathbf{y})$.

References

[1] Emmanuel Briand and Laureano Gonzalez-Vega, *Multivariate Newton sums: Identities and generating functions*, Communications in Algebra **30** (2001), no. 9, 4527–4547.

[2] J.P. Cardinal and B. Mourrain, *Algebraic approach of residues and applications*, Proceedings of AMS-Siam Summer Seminar on Math. of Numerical Analysis (Park City, Utah, 1995) (J. Reneger, M. Shub, and S. Smale, eds.), Lectures in Applied Mathematics, vol. 32, 1996, pp. 189–219.

[3] ______, *Algebraic approach of residues and applications*, Proc. AMS-SIAM Summer Seminar on Math. of Numerical Analysis, (Park City, Utah, 1995) (J. Renegar, M. Shub, and S. Smale, eds.), Lectures in Applied Math., vol. 32, American Mathematical Society Press, Providence, 1996, pp. 189–210.

[4] E. Cattani, A. Dickenstein, and B. Sturmfels, *Computing multidimensional residues*, Algorithms in algebraic geometry and applications (Santander, 1994), Progr. Math., vol. 143, Birkhäuser, Basel, 1996, pp. 135–164.

[5] Eduardo Cattani, Alicia Dickenstein, and Bernd Sturmfels, *Residues and resultants*, J. Math. Sci. Univ. Tokyo **5** (1998), no. 1, 119–148.

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

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

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

[9] Itnuit Janovitz-Freireich, Lajos Rónyai, and Ágnes Szántó, *Approximate radical of ideals with clusters of roots*, ISSAC '06: Proceedings of the 2006 international symposium on Symbolic and algebraic computation (New York, NY, USA), ACM Press, 2006, pp. 146–153.

[10] ———, *Approximate radical for clusters: a global approach using gaussian elimination or svd*, (2007), to appear in Mathematics in Computer Science, Vol. 1 Number 2.

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

[12] Bernard Mourrain, *Generalized normal forms and polynomial system solving*, ISSAC '05, 2005, pp. 253–260.

[13] Bernard Mourrain and Victor Y. Pan, *Multivariate polynomials, duality, and structured matrices*, J. Complex. **16** (2000), no. 1, 110–180.