Bezoutian and quotient ring structure

B. Mourrain

GALAAD, INRIA
BP 93, 06902 Sophia Antipolis, France

Abstract

In this paper, we present different results related to bezoutian and residue theory. We consider, in particular, the problem of computing the structure of the quotient ring by an affine complete intersection, and an algorithm to obtain it, as conjectured in [9]. We analyze it in detail and prove the validity of the conjecture, for a modification of the initial method. Direct applications of the results in effective algebraic geometry are given.

1 Introduction

The bezoutian is a fundamental tool which, surprisingly, appears in many areas of constructive algebra.

It was introduced implicitly by E. Bézout (around 1756) and also studied by Euler, at the premise of resultant theory. Later on, this method was revisited and analyzed in detail by A. Cayley [12], yielding an alternative approach to the well-known formulation of S. Sylvester for the resultant of two univariate polynomials. We also find the Bezoutian construction in the work of A. Dixon [15] on resultants for bivariate polynomials.

Indeed, the bezoutian plays a central role in elimination theory, as it can be observed in the work of J.P. Jouanolou [28], where its also named Morley form. It is involved in projective resultant constructions [29], [14] or toric resultants [34], and more recently in their generalization of resultants over parameterized varieties [6], or residual resultant [7], [8]. See also [32], [30], [33], [31] for projection operators.

Email address: mourrain@sophia.inria.fr (B. Mourrain).

Preprint submitted to special issue of J. Symb. Comp. 20 February 2004
The bezoutian is naturally connected to the theory of residue, as we will see. In complex analysis, it appears explicitly in different contexts (eg. [27](p. 657)), involving Cauchy formula and properness properties in order to obtain explicit representation formulae [5], [4], [16]. This theory of residue has also an algebraic facet, which relies mainly on the works of G. Scheja and U. Storch [43], and E. Kunz [37], where the foundations of the algebraic theory of residues were settled. Some related works and algorithmic extensions were presented in [3], [10], [17]. The algebraic approach of residue theory is also involved in works related to complexity analysis and polynomial representation formulae. See for instance [22], [42], [35], [23], [24], [36], [11], [20], [38], [1], [26].

The problem we are concerned with in this paper, is the computation of the structure of the quotient ring 
\[ A = \mathbb{R}/(f_1, \ldots, f_n) \] when \((f_1, \ldots, f_n)\) is an affine complete intersection. A new algorithm, contrasting with the classical Gröbner or triangular set approaches was described in [9]. It was conjectured that the matrices obtained at the end of this algorithm are the matrices of multiplication by the variables in a basis of \( A \). This was corroborated by the experimentations. Though this work induced an active focus of the community on the topic, the conjecture remained unsolved. The aim of the paper is to describe the problem and to specify it in details, in order to give a positive answer to the conjecture, for a modification of the initial algorithm. We deduce some direct applications of this result in effective algebraic geometry.

The paper is organized as follows. In the next section, we give the definitions that are used through the paper. In section 3, we recall the important algebraic properties of the bezoutian. In section 4, we describe the algorithm and in section 5, we prove the conjecture under some hypothesis. In the last section, we give some direct applications.

2 Definitions

Let \( K \) be a field. Let \( R = K[x_1, \ldots, x_n] = K[\mathbf{x}] \) be the ring of polynomials in the variables \( \mathbf{x} = (x_1, \ldots, x_n) \) with coefficients in \( K \). By convention, we set \( x_0 = 1 \). For any \( \alpha \in \mathbb{N}^n \), we denote by \( x^\alpha \) the monomial \( x_1^{\alpha_1} \cdots x_n^{\alpha_n} \). For any subset \( \mathbf{a} \) of \( R \), we denote by \( \langle \mathbf{a} \rangle \) the vector space of \( R \) generated by \( \mathbf{a} \).

For any vector space \( K \subset R \), we denote by \( K^+ \), the vector space \( K^+ = K + x_1 K + \cdots + x_n K \). The notation \( K^{[p]} \) means \( p \) iterations of the operator +, starting from \( K \).

A vector space \( V \subset R \), is said to be connected to \( e \in V \), if for any \( v \in V - \langle e \rangle \), there exists \( l > 0 \) such that \( v \in \langle e \rangle^{[l]} \) and \( v = v_0 + \sum_{i=1}^{n} x_i v_i \) with \( v_i \in \langle e \rangle^{[l-1]} \cap V \) for \( i = 0, \ldots, n \).
We denote by \( \hat{R} = \text{Hom}_K(R, K) \) the set of \( K \)-linear forms from the polynomial ring \( R \) to \( K \). This vector space has a natural structure of an \( R \)-module. For any linear form \( \Lambda \in \hat{R} \) and \( r \in R \), we define \( r \cdot \Lambda \) by \( r \cdot \Lambda : x \mapsto \Lambda(r \cdot x) \).

We denote by \( R \otimes R = K[x_1, \ldots, x_n, y_1, \ldots, y_n] = K[x, y] \). An element \( \Delta = \Delta(x, y) \) of \( R \otimes R \) is of the form

\[
\Delta = \sum_i a_i \otimes b_i = \sum_i a_i(x) b_i(y),
\]

with \( a_i, b_i \in R \).

**Definition 2.1** Assume that the monomials of \( R \) are sorted according to a given total order. For any

\[
\Delta = \sum_{\alpha \in a, \beta \in b} \Delta_{\alpha, \beta} x^\alpha y^\beta \in R \otimes R
\]

where \( a \) and \( b \) are ordered set of monomials, the matrix associated to \( \Delta \) is

\[
[\Delta] := (\Delta_{\alpha, \beta})_{\alpha \in a, \beta \in b}.
\]

If \( a \) and \( b \) are the minimal sets for which such a decomposition is possible, we say that \( [\Delta] \) is minimal.

Notice that \([\Delta] \) is the matrix of the restriction of the following operator:

\[
\Delta| : \hat{R} \to R
\]

\[
\Lambda \mapsto (\Delta|\Lambda) := \sum_{\alpha \in a, \beta \in b} \Delta_{\alpha, \beta} x^\alpha \Lambda(y^\beta),
\]

expressed in the dual basis \((y^\beta)_{\beta \in b}\) and in \((x^\alpha)_{\alpha \in a}\). Indeed, the mapping \( \Delta \mapsto \Delta| \) allows us to identify naturally \( R \otimes_K R \) with \( \text{Hom}_K(\hat{R}, R) \). Similarly, we define

\[
|\Delta : \hat{R} \to R
\]

\[
\Lambda \mapsto (\Lambda|\Delta) := \sum_{\alpha \in a, \beta \in b} \Delta_{\alpha, \beta} \Lambda(x^\alpha)y^\beta.
\]

Denoting by \( a(x) \) and \( b(y) \) the vector of ordered monomials \((x^\alpha)_{\alpha \in a}\) and \((y^\beta)_{\beta \in b}\), we have

\[
a(x)^t [\Delta] b(y) = \Delta(x, y).
\]

We extend this definition for any ordered set \( a \), \( b \) of linearly independent polynomials, in which \( \Delta \) can be decomposed. We will say that the polynomials of \( a \) (resp. \( b \)) are indexing the rows (resp. columns) of \([\Delta]\)
Given an ideal $I$ of $R$ and $A, B \in R \otimes R$, we will say that the equation $A = B$ holds modulo $I(x)$ if it is valid modulo the ideal $I \otimes R$. It will be denoted hereafter by $A = B + I(x)$. Similarly an equation in $R \otimes R$ holds modulo $I(y)$ if it is valid modulo $R \otimes I$.

The fundamental object of our study is the bezoutian defined as follows.

**Definition 2.2** Let $f_0, \ldots, f_n \in R$. The bezoutian polynomial associated with $f_0, \ldots, f_n$ is the element of $R \otimes R$ defined by

$$B(f_0, \ldots, f_n) = \frac{\prod_{i=1}^{n} (y_i - x_i)}{f_0(x_1, \ldots, x_n) f_0(y_1, x_2, \ldots, x_n) \cdots f_0(y_1, \ldots, y_n) \cdots f_n(x_1, \ldots, x_n) f_n(y_1, x_2, \ldots, x_n) \cdots f_n(y_1, \ldots, y_n)}.$$ 

This construction gives a symmetric role to the variables $x$ and $y$. Here is a non symmetric construction, with the same symmetric result:

**Lemma 2.3** We have

$$B(f_0, \ldots, f_n) = \frac{\prod_{i=1}^{n} (y_i - x_i)}{f_0(x_1, \ldots, x_n) \delta_1(f_0) \cdots \delta_n(f_0) \cdots f_n(x_1, \ldots, x_n) \delta_1(f_n) \cdots \delta_n(f_n)}.$$ 

where $\delta_i(f) = \frac{f(y_1, \ldots, y_i, x_{i+1}, \ldots, x_n) - f(y_1, \ldots, y_{i-1}, x_1, \ldots, x_n)}{y_i - x_i}$.

**Proof.** By subtracting the $i^{th}$ column from the $(i+1)^{th}$, and dividing the result by $y_i - x_i$, we obtain the first determinantal expression. Since for any polynomial $f \in R$, we have

$$f(y) - f(x) = \delta_1(f) \times (y_1 - x_1) + \ldots + \delta_n(f) \times (y_n - x_n),$$

we deduce that

4
For any \( f \) denote by \( \hat{R}/I \) the ideal that they generate. The quotient ring \( R/I \) will be denoted by \( B \).

Hereafter, we will denote by \( B \). This implies in particular that if \( I \) is the ideal generated by the polynomials \( f_1(x), \ldots, f_n(x) \) (resp. \( f_1(y), \ldots, f_n(y) \)) in \( R \otimes R \) is denoted by \( I(x) \) (resp. \( I(y) \)). Notice that \( \mathcal{A} \otimes_K \mathcal{A} = K[x, y]/(I(x), I(y)) \).

**Proposition 2.4** We have \( \mathcal{B}(f_0) \equiv f_0(x)\mathcal{B}_0 + I(x) \) and \( \mathcal{B}(f_0) \equiv f_0(y)\mathcal{B}_0 + I(y) \).

**Proof.** By expansion of the determinant \( \mathcal{B}(f_0) \) (lemma 2.3) along the first column and modulo \( (f_1(x), \ldots, f_n(x)) \), we check that \( \mathcal{B}(f_0) \equiv f_0(x)\mathcal{B}(1) + I(x) \). Using lemma 2.3, a similar proof applies for the \( y \). \( \square \)

This implies in particular that if \( \mathcal{B}_0 = \mathcal{B}(1) = \sum_{\alpha \in a, \beta \in b} \mathcal{B}_{\alpha, \beta}(1)x^\alpha y^\beta \) and \( \mathcal{B}(f_0) = \sum_{\alpha \in a, \beta \in b} \mathcal{B}_{\alpha, \beta}(f_0)x^\alpha y^\beta \), we have for all \( \beta \in b \)

\[
\sum_{\alpha \in a} \mathcal{B}_{\alpha, \beta}(f_0)x^\alpha \equiv f_0(x) \left( \sum_{\alpha \in a} \mathcal{B}_{\alpha, \beta}(1)x^\alpha \right) + I(x),
\]

and similarly \( \forall \alpha \in a, \)

\[
\sum_{\beta \in b} \mathcal{B}_{\alpha, \beta}(f_0)y^\beta \equiv f_0(y) \left( \sum_{\beta \in b} \mathcal{B}_{\alpha, \beta}(1)y^\beta \right) + I(y).
\]
Notice in particular that, for \( p = 1, \ldots, n \), we have

\[
\mathfrak{B}_p - x_p \mathfrak{B}_0 = \begin{vmatrix} 0 & 0 & 1 & 0 \\ f_1(x) & \delta_1(f_1) & \cdots & \delta_p(f_1) \\ \vdots & \vdots & \ddots & \vdots \\ f_n(x) & \delta_1(f_n) & \cdots & \delta_p(f_n) \end{vmatrix} = \sum_l k_p^l(x)y^{\beta_l},
\]

and

\[
\mathfrak{B}_p - y_p \mathfrak{B}_0 = \begin{vmatrix} 0 & 0 & 1 & 0 \\ f_1(y) & \delta_1(f_1) & \cdots & \delta_p(f_1) \\ \vdots & \vdots & \ddots & \vdots \\ f_n(y) & \delta_1(f_n) & \cdots & \delta_p(f_n) \end{vmatrix} = \sum_l x^\alpha_l h_p^l(y).
\]

with \( k_p^l(x) \in I(x) \) and \( h_p^l(y) \in I(y) \).

**Definition 2.5** Let \( K_0 \) (resp. \( H_0 \)) be the vector space generated by the polynomials \( k_p^l(x) \) (resp. \( h_p^l(y) \)).

By proposition 2.4, \( K_0 \) and \( H_0 \) are subvector spaces of the ideal \( I \). Hereafter \( \Delta_p := \mathfrak{B}_p - x_p \mathfrak{B}_0 \).

3 Algebraic properties of the Bezoutian

In this section, we assume that \((f_1, \ldots, f_n)\) defines an affine complete intersection. Therefore, \( \mathcal{A} = \mathbb{K}[x_1, \ldots, x_n]/(f_1, \ldots, f_n) \) is a finite dimensional \( \mathbb{K} \)-vector space.

3.1 Gorenstein algebra

Let \( dx_i = x_i - y_i = x_i \otimes 1 - 1 \otimes x_i \in R \otimes R \) and let \( \mathfrak{D} = (dx_1, \ldots, dx_n) \) be the ideal of \( R \otimes R \) generated by the elements \( dx_i \) (or equivalently by all the polynomials \( q(x) - q(y) = q \otimes 1 - 1 \otimes q \), for \( q \in R \)). Let us recall that the annihilator of an ideal \( \mathfrak{I} \) of the ring \( \mathfrak{A} \) is by definition \( \text{Ann}_{\mathfrak{A} \otimes \mathfrak{A}}(\mathfrak{I}) = \{ b \in \mathfrak{A} \otimes \mathfrak{A}; b \mathfrak{I} = 0 \} \).

Using the identification between \( R \otimes \mathbb{K} R \) and \( \text{Hom}_\mathbb{K}(\hat{R}, R) \), we also identify \( \text{Hom}_\mathfrak{A}(\hat{\mathfrak{A}}, \mathfrak{A}) \) (that is the set of \( \mathfrak{A} \)-homomorphism from \( \hat{\mathfrak{A}} \) to \( \mathfrak{A} \)) and \( \text{Ann}_{\mathfrak{A} \otimes \mathfrak{A}}(\mathfrak{D}) \) as follows:
\[ \Delta \in \text{Ann}_{A \otimes A}(D) \iff \forall s \in A, \Delta (s \otimes 1 - 1 \otimes s) = 0 \]
\[ \iff \forall s \in A, \forall \Lambda \in \hat{A}, (s \Delta | \Lambda) = (\Delta | s \cdot \Lambda) \iff \Delta | \in \text{Hom}_A(\hat{A}, A) \]

See [37] (p. 362, p. 357, ex. 3) and [43] for more details.

According to proposition 2.4, for any \( f_0 \in A \), we have in \( A \otimes A \),
\[ \mathfrak{B}_0 (f_0(x) - f_0(y)) \equiv 0 + (I(x), I(y)), \]
so that \( \mathfrak{B}_0 \in \text{Ann}_{A \otimes A}(D) \). In other words, it defines an \( A \)-homomorphism from \( \hat{A} \) to \( A \).

Assuming now that \( (f_1, \ldots, f_n) \) defines an affine complete intersection and therefore that \( A \) is a Gorenstein algebra, [3], the bezoutian \( \mathfrak{B}_0 \) has important properties, that we describe now.

**Theorem 3.1** Assume that \( (f_1, \ldots, f_n) \) defines an affine complete intersection. Then we have the following equivalent properties:

1. \( \text{Hom}_A(\hat{A}, A) \) is a free \( A \)-module of basis \( \Delta \).
2. \( \mathfrak{B}_0| \) is \( A \)-isomorphism from \( \hat{A} \) to \( A \).
3. \( \hat{A} \) is a free \( A \)-module of basis \( \tau = \mathfrak{B}_0|^{-1}(1) \).
4. The bilinear form of \( A \) defined by \( \langle a, b \rangle \mapsto \langle a, b \rangle := \tau(ab) \) is non-degenerate.
5. \( \mathfrak{B}_0 \equiv \sum_{i=1}^{D} a_i \otimes b_i \) in \( A \otimes A \) where \((a_i)_{i=1, \ldots, D}\) and \((b_i)_{i=1, \ldots, D}\) are bases of \( A \).

Moreover, for any element \( \Delta \in R \otimes R \), as soon as one of these points is satisfied, so are any of the other points, and conversely. For more details on this result involving Wiebe’s lemma, see [37](p. 352), [43](p. 182-184), [18].

We deduce a simple corollary, which will be used hereafter.

**Corollary 3.2** Assume that \( f_1, \ldots, f_n \) is a complete intersection. Then the set of polynomials indexing the rows (resp. columns) of \( \mathfrak{B}_0 \) is a generating family of \( A = R/(f_1, \ldots, f_n) \).

**Proof.** Since \( \mathfrak{B}_0| \) defines an isomorphism between \( \hat{A} = I^1 \) and \( A = R/I \), any element \( f \in R \) is equal, modulo \( I \), to an element in the image of \( \mathfrak{B}_0| \), that is to a linear combination of the polynomials indexing the rows of \( \mathfrak{B}_0 \). Equivalently, this set of polynomials is a generating family of \( A = R/I \). By symmetry, the result also holds for the polynomial indexing the columns. \( \square \)
3.2 The residue

The residue of analytic functions $f_1, \ldots, f_n$ of complex variables over $K = \mathbb{C}$ is defined by integration of differential forms \[5\] over a compact domain. Its impact in complex analysis is ubiquitous. In the context of polynomial functions, we have the following definition:

**Definition 3.3** Assume that $(f_1, \ldots, f_n)$ is a complete intersection. Then, the residue of $(f_1, \ldots, f_n)$ is the unique linear form $\tau \in \hat{K}$, such that

1. $\tau$ vanishes on $I = (f_1, \ldots, f_n)$,
2. $(\mathcal{B}_0|\tau) \equiv 1 + I$.

By theorem 3.1 (point 4), we have the following duality theorem (see [27] (p. 659)):

\[ b \in I \iff \forall a \in B, \tau(a b) = 0. \]

By theorem 3.1 (point 3), for all $\Lambda \in \hat{A}$, we have $\Lambda = a \cdot \tau$ with $a = (\Delta|\Lambda) \in A$, since $(\Delta|a \cdot \tau) = a(\Delta|\tau) = a$.

Let $\Delta = \sum_{i=1}^D a_i \otimes b_i$ be a decomposition of $\mathcal{B}_0$ in $A \otimes A$, such that $(a_i)_{i=1,\ldots,D}$ and $(b_i)_{i=1,\ldots,D}$ are bases of $A$. Then noticing that $(\Delta|a_i \cdot \tau) = a_i$, we easily check the dual basis of $(a_i)_{i=1,\ldots,D}$ for $\langle \cdot \rangle$ is $(b_i)_{i=1,\ldots,D}$, that is $\langle a_i, b_j \rangle = \delta_{i,j}$. In other words, $\hat{a}_i := b_i \cdot \tau$ $(i = 1, \ldots, D)$ is the dual basis in $\hat{A}$, of the basis $a_i$ $(i = 1, \ldots, D)$. This implies the following interpolation formula or Cauchy formula (see [37], [5]):

\[ b = \sum_{i=1}^d \langle b, b_i \rangle a_i = \sum_{i=1}^d \langle b, a_i \rangle b_i. \]

(1)

As a consequence, the residue $\tau$ of $f_1, \ldots, f_n$ encodes not only the complete structure of $\hat{A}$ but also the algebraic structure of the quotient algebra $A$. The knowledge of the decomposition $\Delta = \sum_{i=1}^D a_i \otimes b_i$ yields a complete view on $A$ and its dual $\hat{A}$. We are going to see now how to compute effectively such a decomposition.

4 Algorithmic ingredients

The algorithm that we are going to describe yields the algebraic structure of $A$, that is

- a basis of $A$ as $K$-vector space,
- and its multiplication tables by the variables $x_i, i = 1, \ldots, n$, in this basis.
The outline of this algorithm consists in extending the relations $K_0$ and $H_0$ (see definition 2.5), by adding new independent vectors to the generating sets of $K_0$ and $H_0$, in order to get a *normalizing set* of relations in the ideal $I$. This set of normalizing relations will allow us, for any variable $x_i$ and any element $a$ of the basis, to rewrite $x_i a$ as a linear combination of the elements of the basis. Thus it yields the multiplication tables by the variables $x_i$ in this basis.

Let us recall that $\mathcal{B}_p \ (p = 0, \ldots, n)$ are the matrices of the bezoutian polynomials $\mathcal{B}_p$, decomposed with respect to the same set of polynomials in $x$ and $y$. These set of polynomials in $x$ and in $y$ are denoted respectively by $a(x)$ and $b(y)$. They are indexing the rows and columns of the matrices $\mathcal{B}_p$. More precisely, we have the relations

$$a(x)^t \mathcal{B}_p b(y) = \mathcal{B}_p, \; p = 0, \ldots, n.$$ 

The vector space generated by the polynomials in $a(x)$ (resp. $b(y)$) will be denoted by $V$ (resp. $W$). Hereafter, the matrices $M_p$ will be submatrices of $\mathcal{B}_p$ ($p = 1, \ldots, n$).

We are going to operate simultaneously on the matrices $\mathcal{B}_0, \mathcal{B}_1, \ldots, \mathcal{B}_n$ by applying invertible transformations $P, Q$ on the rows and columns of these matrices:

$$P \mathcal{B}_0 Q, P \mathcal{B}_1 Q, \ldots, P \mathcal{B}_n Q.$$ 

After such a transformation, the new set of polynomials indexing the rows and columns are respectively $P^{-t} a(x)$ and $Q^{-1} b(y)$. Let us describe now more precisely the basic operations that we are going to perform.

### 4.1 Column reduction step

Assume that we are given two subspaces $\hat{K} \subset V \cap I$ and $\hat{H} \subset W \cap I$. Let $A$ be a supplementary space of $\hat{K}$ in $V$ so that $V = A \oplus \hat{K}$. Let $B = (\hat{K}^\perp | \mathcal{B}_0)$ and $H' \subset I$ a supplementary space of $B$ in $W$ so that $W = B \oplus H'$. Notice that the supplementary space $H'$ can be chosen as a subset of $I$, since by theorem 3.1, $B = (\hat{K}^\perp | \mathcal{B}_0) \supset (I^\perp | \mathcal{B}_0)$ is a generating set of $A$. Based on these direct sums in $V$ and $W$, we obtain the following block decomposition of the generalized pencil:

$$
\begin{pmatrix}
M_0' & 0 \\
H_0' & L_0'
\end{pmatrix},
\begin{pmatrix}
M_1' & K_1' \\
H_1' & L_1'
\end{pmatrix}, \ldots,
\begin{pmatrix}
M_n' & K_n' \\
H_n' & L_n'
\end{pmatrix},
$$

where the block $M_i'$ have rows and columns indexed respectively by the bases of $A$ and $B$. By construction of $B$, the number of columns of $M_0'$ equals its rank, which is the dimension of $B$. 


By proposition 2.4, if a column of $B_0$ represents a polynomial $f(x)$, the corresponding column of $B_p$ is $x_p f(x)$ modulo $I$. We deduce that the polynomials represented by the columns of \[
abla p \begin{pmatrix} K_p' \\ L_p' \end{pmatrix}\] and thus of the submatrices $K_p'$ are in $I$.

The column reduction step consists in extending $\tilde{K}$, by adding to its generating family, these new polynomials associated with the blocks $K_p', p = 0, \ldots, n$.

4.2 Row reduction step

We assume that we are given two subspaces $\tilde{K} \subset V \cap I$ and $\tilde{H} \subset W \cap I$. We operate symmetrically on the columns of the matrices $B_p$. In this case, the vector space $\tilde{H}$ may be extended by new polynomials in $I$.

4.3 Saturation step

This step consists in replacing $\tilde{K}$ by $\tilde{K}^+ \cap V$. Its purpose is to ensure the connectivity of the vector space of relations that are used to reduce. It is an important step for the proof of correctness of the algorithm.

4.4 Diagonalisation step

Assume that we have decomposed the matrix pencil as

\[
\begin{pmatrix} M_0 & 0 \\ H_0 & L_0 \end{pmatrix}, \quad \begin{pmatrix} M_1 & K_1 \\ H_1 & L_1 \end{pmatrix}, \ldots, \begin{pmatrix} M_n & K_n \\ H_n & L_n \end{pmatrix},
\]

with the rank of $M_0$ equal to $r$ its number of columns, the last rows (resp. columns) indexed by polynomials in $\tilde{K}$ (resp. $\tilde{H}$). Then, there exists a matrix $M_0^*$ such that $M_0^* M_0 = \text{Id}_r$ is the $r \times r$ identity matrix. By multiplying the pencil on the left by the invertible matrix

\[
\begin{pmatrix} \text{Id} & 0 \\ -H_0 M_0^* \text{Id} \end{pmatrix},
\]

we obtain the following decomposition:

\[
\begin{pmatrix} M_0 & 0 \\ 0 & L_0 \end{pmatrix}, \quad \begin{pmatrix} M_1 & K_1 \\ H_1' & L_1' \end{pmatrix}, \ldots, \begin{pmatrix} M_n & K_n \\ H_n' & L_n' \end{pmatrix}.
\]
This corresponds to a change of basis in $V$, for which we add to the $r$ first polynomials indexing the rows of the matrices, polynomials in $\tilde{K}$.

4.5 Compatibility step

For a variant of the main algorithm, described in the next section, we also consider the following operations.

We assume here that $M_0 = \text{Id}$ and that the matrices $M_p$ ($p = 1, \ldots, D$) commute. We denote by $A$, the vector space generated by the polynomials indexing their rows. For $i = 1, \ldots, n$, we denote by $f_i(M_1, \ldots, M_n)$ the matrix obtained by substituting the variable $x_p$ by $M_p$. The compatibility step consists in adding to $\tilde{K}$ (resp. $\tilde{H}$) the polynomials corresponding to the non-zero columns (resp. rows) of these matrices $f_i(M_1, \ldots, M_n)$. Its aim is to ensure that at the end of the loop, the matrices $M_p$ satisfy the polynomial relations $f_i = 0$.

4.6 Algorithm

We describe now the algorithm, given in [9] in other terms, with an additional saturation step.

Quotient structure algorithm:

- Compute the bezoutian matrices $B_0, \ldots, B_n$ of $1, x_1, \ldots, x_n$ and $f_1, \ldots, f_n$.
- Let $\tilde{K} := K_0$; $\tilde{H} := H_0$; $M_p := B_p$ ($p = 1, \ldots, n$); $\textbf{notsat} := \text{true}$.
- While $\textbf{notsat}$
  - Apply the saturation step on $\tilde{K}$;
  - Apply the column reduction step;
  - Apply the diagonalisation step;
  - Apply the row reduction step;
  - If this extends strictly $\tilde{K}$; or $\tilde{H}$, let $\textbf{notsat} := \text{true}$,
    otherwise let $\textbf{notsat} := \text{false}$.
- Check that $M_0$ is invertible and output $\bar{M}_i := M_0^{-1}M_i$ for $i = 1, \ldots, n$.

The algorithm operates in-place, transforming the initial matrices $B_p$ by multiplication on the left and on the right by invertible matrices. It eventually stops, since the dimension of the vector spaces $\tilde{K}$ or $\tilde{H}$ increases and is bounded by the dimension of $V$ or $W$. We will check that at the end of the algorithm, the matrix $M_0$ is invertible. Due to the saturation step, we have $\tilde{K}^+ \cap V = \tilde{K}$. We denote by $D$ the size of the matrices $M_p$. 
Main theorem: At the end of the algorithm, the matrices $M_i$ of size $D = \dim_K(\mathcal{A})$, are the matrices of multiplication by the variables $x_p$ ($p = 1, \ldots, n$) in the basis $a(x)$ of $\mathcal{A}$, indexing the rows of $M_0$.

This result was conjectured in [9], without the saturation step. The reason why we need to introduce this saturation step, is that if we multiply all the bezoutian polynomials by an element of the form $1 + f(x)g(y)$, with $f, g \in R$ conveniently chosen, we could obtain matrices of the form

$$\begin{pmatrix} B_p & 0 \\ 0 & B_p \end{pmatrix}.$$ 

Applying only the reduction and compression steps, as described in [9], would not allow us to avoid the duplication of the structure of $A$. Moreover, if $f$ and $g$ are in $I$, the polynomials $(1+f(x)g(y))B_p$ share the same properties modulo $I$, as the bezoutians $B_p$. To handle this problem, we add this saturation step, which will "connect" the two blocks, provided that the vector space $V$ is connected to an element $e$. This is the hypothesis that will be made hereafter to prove the main theorem.

This hypothesis is easy to check in practice, and usually we have $e = 1$. Moreover, it is satisfied when the polynomials $f_i$ are monomials $x^{\alpha_i}$. We do not have a proof that this extends by linearity to any polynomial $f_i$.

4.7 Example

We illustrate the algorithm on a small example in two variables, where the reduction steps are simple to perform. We consider $f_1 = x_1x_2 - x_1$, $f_2 = x_1x_2^2 - 2$ and $I = (f_1, f_2) \subset K[x_1, x_2]$. The initial bezoutian matrices are

$$M_0 := \begin{bmatrix} 0 & 0 & -1 \\ 0 & -1 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \quad M_1 := \begin{bmatrix} 0 & -2 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad M_2 := \begin{bmatrix} -2 & -2 & 0 \\ 2 & 0 & -1 \\ 0 & -1 & 1 \end{bmatrix}.$$ 

The rows are indexed by the monomials $[1, x_2, x_2^2]$ and the columns by $[1, y_1, y_1y_2]$, which are sets connected to 1. In this example, we even start with $K = 0$, $H = 0$ and change the order in which the operations are performed, to simplify the illustration.

The column reduction step yields the polynomial $-y_1 + y_1y_2$ corresponding to the last row $[0, -1, 1]$ of $M_2$. This polynomial is added to $H$. The row reduction step yields polynomial $1 - x_2$ corresponding to the first column $[-2, 2, 0]^t$ of
$M_2$. It is added to $\tilde{K}$. After these reduction steps, we obtain the following matrices

$$M_0 \equiv \begin{bmatrix} 0 & -1 \\ 0 & 0 \end{bmatrix}, M_1 \equiv \begin{bmatrix} 0 & -2 \\ 0 & 0 \end{bmatrix}, M_2 \equiv \begin{bmatrix} 0 & -3 \\ 0 & 0 \end{bmatrix}.$$  

The saturation step does not introduce new elements in $\tilde{H}$ and $\tilde{K}$, which can be used for the reduction. The diagonalisation step yields the matrices

$$M_0 \equiv [-2], M_1 \equiv [-2], M_2 \equiv [-1],$$

which ends the loop. From these matrices, we deduce easily the coordinates of the single solution of our system: $x_1 = 2, x_2 = 1$.

5 Proof of the main theorem

The algorithm decomposes the initial vector spaces $V$ and $W$ generated by the monomials indexing the rows and columns of the bezoutian matrices $\mathcal{B}(x_p)$ into the sum of a subspace of the ideal generated by the equations $f_1, \ldots, f_n$ and a supplementary vector space.

**Definition 5.1** Let $K$ (resp. $H$) be the vector space containing $\tilde{K}$ (resp. $\tilde{H}$), generated by polynomials of $I$ and supplementary to $A$ (resp. $B$) in $V$ (resp. $W$), which we get at the end of the algorithm.

By construction, we have $K^+ \cap V = K$ and $V = A \oplus K$. The proof of the result is based on the following properties:

**Lemma 5.2** There exist linearly independent polynomials $\{a_1, \ldots, a_D, \ldots\}$ of $V$, with $a_{D+1}, \ldots \in K$ and a basis $\{b_1, \ldots, b_D, \ldots\}$ of $W$, with $b_{D+1}, \ldots \in H$ in which the bezoutian matrices $\mathcal{B}_p$ have the following decomposition:

$$\begin{pmatrix} \text{Id} & 0 \\ 0 & L_0 \end{pmatrix}, \begin{pmatrix} \tilde{M}_1 & 0 \\ 0 & L_1 \end{pmatrix}, \ldots, \begin{pmatrix} \tilde{M}_n & 0 \\ 0 & L_n \end{pmatrix},$$

where $\text{Id}$ is the $D \times D$ identity matrix, and the $\tilde{M}_p$ are the output of the algorithm.

**Proof.** Assume that we are at the end of the algorithm and let us decompose the bezoutian matrices $\mathcal{B}_p$ of $\mathcal{B}_p$ in the bases $x^\alpha$ and $y^\beta$ which are given by
the algorithm and go through the column reduction step again:

\[
\begin{pmatrix}
M_0 & 0 \\
H_0 & L_0
\end{pmatrix},
\begin{pmatrix}
M_1 & K_1 \\
H_1 & L_1
\end{pmatrix}, \ldots, \begin{pmatrix}
M_n & K_n \\
H_n & L_n
\end{pmatrix}.
\]

The last rows are indexed by polynomials in \(K\). Since \(K\) is not extended in this column reduction step, we deduce that \(K_p = 0\) for \(p = 1, \ldots, n\).

Apply now the diagonalisation step so that we obtain the following decomposition:

\[
\begin{pmatrix}
M_0 & 0 \\
0 & L_0
\end{pmatrix}, \begin{pmatrix}
M_1 & 0 \\
H'_1 & L_1
\end{pmatrix}, \ldots, \begin{pmatrix}
M_n & 0 \\
H'_n & L_n
\end{pmatrix},
\]

and consider the row reduction step. Since this operation does not extend \(H\), we have \(H'_p = 0\), for \(p = 1, \ldots, n\) and \(M_0\) is invertible.

By multiplying by the inverse of \(M_0\), we finally obtain the decomposition:

\[
\begin{pmatrix}
\text{Id} & 0 \\
0 & L_0
\end{pmatrix}, \begin{pmatrix}
\bar{M}_1 & 0 \\
0 & L_1
\end{pmatrix}, \ldots, \begin{pmatrix}
\bar{M}_n & 0 \\
0 & L_n
\end{pmatrix}.
\]

We denote by \(\{a_1, \ldots, a_D, \ldots\}\) (resp. \(\{b_1, \ldots, b_D, \ldots\}\)) the polynomial indexing the rows (resp. columns) of these matrices. By construction, the polynomials \(a_{D+1}, \ldots\) are in \(K\) and \(b_{D+1}, \ldots\) in \(H\).

\[\qed\]

We denote by \(A = \langle a_1, \ldots, a_D \rangle\) (resp. \(B = \langle b_1, \ldots, b_D \rangle\)) the vector space generated by the first \(D\) polynomials indexing the rows (resp. columns) of \(M_0\) and by \(a = [a_1, \ldots, a_D]\) (resp. \(b = [b_1, \ldots, b_D]\)) the corresponding vector of polynomials. The entries of the matrices \(\bar{M}_p\) will be denoted by \(m_{p,j}^i\): \(\bar{M}_p = (m_{p,j}^i)_{1 \leq i, j \leq D}\).

**Proposition 5.3** For \(p = 1 \ldots n, i = 1 \ldots D\), we have

\[
x_p a_i = \sum_{j=1}^{D} m_{p,j}^i a_j + \kappa_p^i \quad \text{with} \quad \kappa_p^i \in K.
\]

**Proof.** We have \(\mathfrak{B}(x_p) = x_p \mathfrak{B}(1) + k(x, y)\), with \(k(x, y) \in K_0 \otimes R\) of the form

\[
k(x, y) = \sum_{i=0}^{D} k_i^p(x)b_i(y) + \sum_{l \geq D+1} k_l^p(x)b_l(y),
\]

where \(k_l^p(x) \in K_0\). By identifying the coefficients of \(b_i(y)\), for \(i = 1, \ldots, D\), we deduce that
Proposition 5.4

For $p < q$, we have

$$\mathcal{B}(x_p x_q) = \sum_{1 \leq i, j, k \leq D} m^q_{i,j} m^p_{j,k} a_i \otimes b_k + K \otimes H + x_q K \otimes H + y_p K \otimes H \quad (2)$$

**Proof.** Assume that $p < q$. By definition of $\mathcal{B}(x_p x_q)$, we have

$$\begin{align*}
x_p x_q & = x_q (x_p) = x_q \mathcal{B}(x_p) + y_p (\mathcal{B}(x_q) - x_q \mathcal{B}(1)) \\
& = \sum_{1 \leq i, j \leq D} m^p_{i,j} a_i \otimes b_j + x_q K \otimes H + x_q K \otimes H \\
& \quad + y_p \sum_{1 \leq i \leq D} \kappa^q_i \otimes b_i + y_p K \otimes H \\
& = \sum_{1 \leq i, j \leq D} m^p_{i,j} \left( \sum_{1 \leq k \leq D} m^q_{k,i} a_k - \kappa^q_i \right) \otimes b_j \\
& \quad + \sum_{1 \leq i \leq D} \kappa^q_i \otimes \left( \sum_{1 \leq l \leq D} m^p_{i,l} b_l - \sigma^p_i \right) + x_q K \otimes H + y_p K \otimes H \\
& = \sum_{1 \leq i, j, k \leq D} m^q_{k,i} m^p_{i,j} a_k \otimes b_j \\
& \quad - \sum_{1 \leq i, j \leq D} m^p_{i,j} \kappa^q_i \otimes b_j + \sum_{1 \leq i, j \leq D} m^p_{i,j} \kappa^q_i \otimes b_l \\
& \quad + K \otimes H + x_q K \otimes H + y_p K \otimes H \\
& = \sum_{1 \leq i, j, k \leq D} m^q_{k,i} m^p_{i,j} a_k \otimes b_j + K \otimes H + x_q K \otimes H + y_p K \otimes H.
\end{align*}$$

We deduce that

$$\mathcal{B}(x_p x_q) = x_q \mathcal{B}(x_p) + y_p (\mathcal{B}(x_q) - x_q \mathcal{B}(1))$$

with $\kappa^q_i \in K$. \qed
Proposition 5.5 For $p < q$, we have
\[
\mathcal{B}(x_p x_q) = \sum_{1 \leq i,j,k \leq D} m_{i,j}^p m_{j,k}^q a_i \otimes b_k + K \otimes H + x_p K \otimes H + y_q K \otimes H \quad (3)
\]

Proof. We apply a similar proof, exchanging the role of $x$ and $y$, and using the identity:
\[
\mathcal{B}(x_p x_q) = y_p \mathcal{B}(x_q) + x_q(\mathcal{B}(x_p) - y_p \mathcal{B}(1)).
\]

Proposition 5.6 The matrices $\tilde{M}_p = (m_{i,j}^p)_{1 \leq i,j \leq D}$ commute.

Proof. We identify the coefficients in $A \otimes B$ in the two expansions of propositions 5.4 and 5.5.

Abusing notations, we will also denote by $\tilde{M}_p$, the map $\tilde{M}_p : A \to A$ such that for all $i = 1, \ldots, D$,
\[
\tilde{M}_p(a_i) = \sum_{j=1}^D m_{i,j}^p a_j.
\]

It corresponds to the multiplication by $x_p$, modulo $K$. Since these operators commute, for any polynomial $f(x_1, \ldots, x_n) \in R$, we define $f(\tilde{M}) = f(\tilde{M}_1, \ldots, \tilde{M}_n)$ as the operator obtained by substituting the variable $x_p$ by $\tilde{M}_p$, for $p = 1, \ldots, n$.

In order to prove the main theorem, we will suppose that $V$ is connected to a polynomial $e \in V$. To simplify the proof, we will assume hereafter that $e = 1$. The proof can be extended to any $e$, by showing that, in this case, $e$ is invertible in $A$ and by dividing by $e$.

Proposition 5.7 The ideal $(K)$ generated by the elements of $K$ is equal to $I = (f_1, \ldots, f_n)$.

Proof. By construction, we have $K \subset I$.

As $V = A \oplus K$ is connected to 1, there exist $\mu_1, \ldots, \mu_D \in K$ and $\kappa \in K$ such that
\[
\sum_{i=1}^D \mu_i a_i = u = 1 - \kappa.
\]

This implies that $u$ is invertible in $A = R/I$. We also deduce that there exists $\Lambda \in \hat{R}$, such that $(\mathcal{B}_0|\Lambda) = u$. On the other hand, for $i = 1, \ldots, n$, we have
by definition
\[ \mathfrak{B}(f_i) = 0 = f_i(x)\mathfrak{B}_0 - \delta_1(f_i)\Delta_1 + \cdots + \delta_n(f_i)\Delta_n, \]
with \( \Delta_j \in K \otimes R \). Therefore,
\[ f_i(x)(\mathfrak{B}_0|\Lambda) = f_i(x)(1 - \kappa) = (\delta_1(f_i)|\Delta_1|\Lambda) - \cdots \mp (\delta_n(f_i)|\Delta_n|\Lambda) \in (K), \]
which implies that \( f_i(x) \in (K) \). Consequently \( I (K) \), which proves that \( I = (K) \).

We have now all the ingredients to prove our main theorem, following the approach and results of \([40]\). See also \([41]\).

**Theorem 5.8** Assume that \( V \) is connected to 1. Then, the sets of polynomials \((a_i)_{1 \leq i \leq D}\) and \((b_j)_{1 \leq j \leq D}\) are bases of \( A = R/(f_1, \ldots, f_n) \), and \( M_p \) and \( M^* \) are the matrices of multiplication by \( x_p \) in the corresponding bases.

**Proof.** If \( 1 \in K \subset I \), we have \( A = \{0\} \) and by the saturation step \( K = V \), so that the theorem is satisfied in this case. Otherwise, since \( V \) is connected to 1 and \( K \) does not contain 1, we may assume that 1 is an element of the basis of \( A \). For any \( f \in R \), let \( N(f) = f(M)(1) \). This defines a map from \( R \) to \( A \). We are going to prove by induction that the restriction of \( N \) on \( V \) is the projection on \( A \) along \( K \).

Let us assume that for any \( g \in \langle 1 \rangle^{[l-1]} \cap V \), we have \( g = g(M)(1) \in K \). Let \( f \in \langle 1 \rangle^{[l]} \cap V \). Since \( V \) is connected to 1, \( f \) is of the form \( f = \sum_{i=1}^{n} x_i g_i \) with \( l_i \in \{1, \ldots, n\} \) and \( g_i \in \langle 1 \rangle^{[l-1]} \cap V \). We have
\[ f - f(M)(1) = \sum_{i=1}^{n} x_i (g_i - g_i(M)(1)) + \left( x_i g_i(M)(1) - M_l g_i(M)(1) \right). \]

By induction hypothesis, \( (g_i - g_i(M)(1)) \in K \). By proposition 2.4, we have \( \left( x_i g_i(M)(1) - M_l g_i(M)(1) \right) \in K \). Therefore \( f - f(M)(1) \in K^+ \cap V \). Due to the saturation step of the algorithm, we have \( K^+ \cap V = K \), which proves that \( f - f(M)(1) \in K \). Since the induction hypothesis is true for \( f = 1 \), we deduce that it is valid for all \( f \in V \).

We also prove by induction, that for any \( f \in R \), the polynomial \( f - f(M)(1) \) is in the ideal generated by \( K \). The proof is similar to the previous one.

For any polynomials \( a \in A \) and \( k \in K \), we have
- \( a - a(M)(1) \in K \cap A = \{0\} \) and
- \( k(M)(1) = (k(M)(1) - k) + k \in K \cap A = \{0\} \),
which implies that for all $a \in A$, $N(a) = a$ and that $N(K) = 0$. Thus, the restriction of $N$ on $V = A \oplus K$ is the projection on $A$ along $K$.

Consider now the exact sequence of vector spaces

$$0 \to J \to R \to A \to 0$$

where $J$ is the kernel of $N$. It is an ideal of $R$.

Since $K \subset \text{Ker}(N) = J$ and $J$ is an ideal of $R$, we have $(K) \subset J$. Conversely, as shown above, for any $f \in R$, $f - N(f) \in (K)$. Therefore the kernel $J$ of $N$ is a sub-ideal of $(K)$, which proves that $J = (K)$ and by proposition 5.7 that $J = I$.

Moreover, the image of $N$ is $A$, which proves that $A \sim R/I = \mathcal{A}$ and concludes the proof of the theorem.

\[\square\]

6 Applications

We give some first consequences of this result. Hereafter, the degree of the polynomial $f_i$ is $d_i$ ($i = 1, \ldots, n$) and $d = \max_i \{d_i\}$. A bound on the size of the bezoutian matrices $B_p$ is denoted by $\nu$, which is at most the number of monomials of degree $\leq d_1 + \cdots + d_n - n + 1$, that is $O(e^\nu d^n)$ by Stirling’s formula.

**Proposition 6.1** Assume that $V$ is connected to 1. A basis of $\mathcal{A}$ formed by polynomials of degree $\leq d_1 + \cdots + d_n - n$ can be computed in $O(n \nu^4)$ arithmetic operations.

**Proof.** The basis produced by the algorithm involves polynomials of degree $\leq d_1 + \cdots + d_n - n$ because the polynomials indexing the rows or columns of $B_0$ are of degree $\leq d_1 + \cdots + d_n - n$ (see definition 2.2 and lemma 2.3).

In the loop of the algorithm, each linear operation on the $n$ matrices of size at most $\nu$ involves at most $O(n \nu^3)$ arithmetic operations. The number of loops is bounded by the size of the matrices, that is $\nu$, so that the complexity of the algorithm is bounded by $O(n \nu^4)$.

\[\square\]

From the output of this algorithm, we can construct a generator of the $\mathcal{A}$-module $\hat{A}$, as follows. We take the inverse image of 1 by $B_0|$, which is the
residue of $f_1, \ldots, f_n$.

The multiplication tables by the variables $x_p$ in a basis of $A$ yield many interesting results for solving the system of equations $f_1 = 0, \ldots, f_n = 0$. As described for instance in [2] and in [39], the roots can be recovered from the eigenvalues or eigenspaces of the matrices $M_p$. From the determinant $\det(u_0 + u_1 M_1 + \cdots + u_n M_n)$, we can also recover a rational univariate representation of the roots [25], [19]. Indeed the complete geometry of the roots of the system, can be deduced from the knowledge of the structure of $A$. See [13], [21] for more details.

**Theorem 6.2** For any $f \in R$ of degree $d$, the membership problem "$f \in (f_1, \ldots, f_n)$?" can be tested, in $O(n^\nu^4 L)$ arithmetic operations, where $L$ is a bound for the cost of evaluation of $f_i (i = 1, \ldots, n)$ and $f$.

**Proof.** We replace the saturation step by the compatibility step in the main loop of the algorithm but do not require any hypothesis on $V$. In this case, at the end of the algorithm, we have

$$f_i(M) = 0, (i = 1, \ldots, n).$$

Consider the map $\sigma$ defined by

$$0 \to J' \to R \to K^{D \times D} \to f(M)$$

The kernel $J'$ of this map is an ideal which contains $f_i (i = 1, \ldots, n)$. Thus $I \subset J'$. On the other hand, let $u \in V$ be such that $u = (B_0 | \tau) = 1 + I$ (corollary 3.2) and $f \in J'$. Then, we have

$$f(x) - f(M)(u) = f(x) \in (K) \subset I,$$

so that $J' \subset I$ and $J' = I$. Thus, in order to test if a polynomial $f$ is in $I$, we check whether $f(M) = 0$. The cost for computing the matrices $M_p$ is bounded by $O(n^\nu^4)$ plus $\nu$ times the cost for evaluation the matrices $f_i(M)$ in the compatibility steps. The cost for computing the matrices $f_i(M), f(M)$ is bounded by $O(\nu^3 L)$. So that the total cost of this algorithm is bounded by $O(n^\nu^4 L)$.

Another consequence of this algorithm is that the membership problem can be tested and representation formulae can be computed in small degree. Let $f$ be a polynomial of $R$. We add to the bezoutian matrices $B_p (p = 0, \ldots, n)$ the bezoutian matrix $B(f)$ of $f$. Let us still denote by $V$ and $W$, the vector spaces generated by the rows and columns indexing these matrices. Assuming that $V$ is connected to 1, and applying the algorithm 4.6, we compute a basis
of $\mathcal{A}$, the matrices $M_p$ of multiplication by the variables $x_p$ in this basis and
the matrix $M_f$ of multiplication by $f$ in $\mathcal{A}$. Then $f \in I$, if and only if, $M_f = 0$.
The number of arithmetic operations for computing these matrices is bounded
by $O(\gamma^4)$ where $\gamma$ bounds the dimension of $V$ and $W$. We have $\gamma = O(e^nd^n)$
where $d = \max\{\deg(f_i), \deg(f)\}$. By expansion of $\mathfrak{B}(f)$ along the first column,
we have

$$\mathfrak{B}(f) = f(x)\mathfrak{B}(1) + f_1(x)\Delta_1(x, y) + \cdots + f_n(x)\Delta_n(x, y).$$

By proposition 2.4, for any $\Lambda \in I^\perp$ and $f \in I$, we have $(\mathfrak{B}(f)|\Lambda) = 0$, so that
we obtain the decomposition

$$f(x)(\mathfrak{B}|\Lambda) = f_1(x)(\Delta_1|\Lambda) + \cdots + f_n(x)(\Delta_n|\Lambda).$$

where $u^\Lambda(x) = (\mathfrak{B}_0|\Lambda)$ and $g_i^\Lambda(x) = -(\Delta_i|\Lambda)$ ($i = 1, \ldots, n$) of degree $\leq$ $d_1 + \cdots + d_n + d - n - d_i$. In particular, replacing $\Lambda$ by the residue $\tau$, we get
the representation :

$$f(x) u(x) = f_1(x)g_1^\tau(x) + \cdots + f_n(x)g_n^\tau(x),$$

where $u(x) = (\mathfrak{B}|\tau) \equiv 1$ is invertible in $\mathcal{A}$ and $\deg(e) \leq d_1 + \cdots + d_n - n$
and $\deg(f_i, g_i) \leq d_1 + \cdots + d_n + d - n$.

Acknowledgments: I would like to thank especially J.-P. Cardinal, with
whom I spent a lot of time, discussing, and investigating the properties of be-
zoutian matrices. My gratitude also goes to Marie-Francoise Roy, who initiated
this work.

References

formulas for systems of nonlinear algebraic equations and some of their

Conf. on Numerical Math., volume 86 of Int. Series of Numerical Math, pages

Kronecker symbol and Eisenbud-Levin formula. In L. González-Vega and
T. Recio, editors, Algorithms in Algebraic Geometry and Applications, volume


