Available online at www.sciencedirect.com
SCIENCE DIRECT®

Journal of Symbolic Computation 39 (2005) 259–277

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Subresultants and generic monomial bases

Carlos D'Andrea[a,*], Gabriela Jeronimo[b]

[a] *Miller Institute for Basic Research in Science and Department of Mathematics, University of California, Berkeley CA 94720-3840, USA*

[b] *Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Ciudad Universitaria, Pabellón I, 1428 Buenos Aires, Argentina*

Received 14 August 2003; accepted 1 November 2004

Abstract

Given n polynomials in n variables of respective degrees $d_1, \ldots, d_n$, and a set of monomials of cardinality $d_1 \cdots d_n$, we give an explicit subresultant-based polynomial expression in the coefficients of the input polynomials whose non-vanishing is a necessary and sufficient condition for this set of monomials to be a basis of the ring of polynomials in n variables modulo the ideal generated by the system of polynomials. This approach allows us to clarify the algorithms for the Bézout construction of the resultant.

Keywords: Multivariate resultants; Multivariate subresultants; Determinant of complexes; Monomial bases

1. Introduction

Consider a system of n polynomials in n variables with coefficients in a field $\mathbb{K}$, $f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)$, with respective degrees $d_1, \ldots, d_n$. Generically, this system has $\mathbf{d} := d_1.d_2 \ldots d_n$ roots in the algebraic closure of $\mathbb{K}$. This is the very well-known *Bézout formula* which appeared in Bézout (1779) (see Cox et al. (1996) for a modern treatment of this).

* Corresponding author.
E-mail addresses: cdandrea@math.berkeley.edu (C. D'Andrea), jeronimo@dm.uba.ar (G. Jeronimo).

0747-7171/$ - see front matter
doi:10.1016/j.jsc.2004.11.003

One can say something more about what "generic" means above: let $V(f_1, \ldots, f_n) \subset \overline{\mathbb{K}}^n$ be the set of common zeros of the polynomials $f_1, \ldots, f_n$, and set

$$f_i := \sum_{j=0}^{d_i} f_{ij}, \qquad i = 1, \ldots, n,$$

where f_{ij} is the homogeneous component of f_i of degree j. Then, it turns out that $V(f_1, \ldots, f_n)$ is a finite set and its cardinality (counting multiplicities) is $\mathbf{d}$ if and only if the system of homogeneous equations

$$f_{1d_1} = 0, \; f_{2d_2} = 0, \ldots, f_{nd_n} = 0 \tag{1}$$

has no solution in projective space $\mathbb{P}^{n-1}$—see Cox et al. (1998, Chapter 3, Theorem 5.5) for a proof of this result and also Cox et al. (1998, Chapter 4, Definition 2.1) for the definition of multiplicity of a zero of a polynomial system.

From a more algebraic point of view, if we set $I := (f_1, \ldots, f_n)$ for the ideal generated by the f_i's in $\mathbb{K}[x_1, \ldots, x_n]$, the fact that $V(I) \subset \overline{\mathbb{K}}^n$ has $\mathbf{d}$ points counted with multiplicity means that the $\mathbb{K}$-algebra $\mathcal{A} := \mathbb{K}[x_1, \ldots, x_n]/I$ is a $\mathbb{K}$-vector space of dimension $\mathbf{d}$. As $\mathcal{A}$ is generated by the set of (the images in $\mathcal{A}$ of) all monomials in $\mathbb{K}[x_1, \ldots, x_n]$, one can always find a basis of monomials for $\mathcal{A}$ (finite or not).

In this paper, we will focus our attention on the following problem: given a set $\mathbb{M}$ of $\mathbf{d}$ monomials, how can we decide if they are a basis of $\mathcal{A}$ or not?

We could use Gröbner bases for solving this problem, but we would like our answer to be a function on the input set $\mathbb{M}$ only, and not depending on an extra monomial ordering and other intermediate steps that are needed in Gröbner bases algorithms.

One of the main results of this paper is a polynomial expression in the coefficients of $f_1, \ldots, f_n$ which vanishes if and only if the set $\mathbb{M}$ fails to be a basis of $\mathcal{A}$. The expression we get can be described in terms of resultants and subresultants of homogeneous polynomials obtained from the input system, which is the algebraic counterpart of this problem in the homogeneous case (see Cox et al., 1998; Chardin, 1995; Szanto, in press).

The problem of deciding whether a given set of monomials $\mathbb{M}$ is a basis of $\mathcal{A}$ or not is important in elimination theory due to the fact that algorithms for computing resultants, Bézout identities, reduction modulo an ideal and explicit versions of the Shape Lemma can be reduced to linear algebra computations in the quotient ring, avoiding the use of Gröbner bases, if one succeeds in finding such a basis $\mathbb{M}$.

Bézout (1779) was the first to work following this approach, which was extended by Macaulay (1902), who answered this question in the case $\mathbb{M} = \{x_1^{\alpha_1} \ldots x_n^{\alpha_n}, \; 0 \leq \alpha_i \leq d_i - 1\}$ by means of a polynomial expression in the coefficients of the input polynomials (see also Macaulay, 1916). Our results, when applied to Macaulay's case, recover his original formulation.

In this direction, some results were obtained by Chardin (1994b), provided that all the f_i's are generic and homogeneous. If the input system is generic and sparse, a generalization of the case we are dealing with here, partial results were obtained by Emiris and Rege (1994) and Pedersen and Sturmfels (1996) for $\mathbb{M}$'s constructed by means of regular triangulations of polytopes.

A different approach based on recursive linear algebra is provided in Bikker and Uteshev (1999) for specific $\mathbb{M}$. In Section 7, we will compare our results with those obtained in this article.

The paper is organized as follows. Some preliminary results are stated in Section 2. In Section 3, we recall the definition and basic properties of multivariate subresultants, as introduced in Chardin (1995). We relate subresultants with our problem in Section 4, associating with any given set $\mathbb{M}$ a polynomial whose non-vanishing is equivalent to the fact that $\mathbb{M}$ is a basis of $\mathcal{A}$. In Section 5, we show that, for certain $\mathbb{M}$'s, this polynomial expression depends only on the coefficients of $f_{1d_1}, \ldots, f_{nd_n}$, and moreover, it can be decomposed into factors. Then, we give in Section 6 some rational expressions for generalized Vandermonde determinants. These results, along with those presented in Section 5, allow us a better understanding of the recursive algorithm proposed in Bikker and Uteshev (1999). Finally, we conclude by comparing our results with those obtained in Bikker and Uteshev (1999) in Section 7.

2. Preliminary results

Let $\mathrm{Res}_{d_1,\ldots,d_n}(\cdot)$ be the homogeneous resultant operator, as defined in Macaulay (1902), van der Waerden (1950) and Cox et al. (1998). We recall the following well-known result (see Cox et al., 1998, for a proof):

Proposition 2.1. *The system* (1) *has a nontrivial solution in* $\overline{\mathbb{K}}^n$ *if and only if* $\mathrm{Res}_{d_1,\ldots,d_n}(f_{1d_1}, \ldots, f_{nd_n}) = 0$.

Remark 2.2. This proposition, together with our previous remarks about the quotient ring $\mathcal{A}$, gives a proof for the Choice Conjecture stated in Bikker and Uteshev (1999): The condition $\mathrm{Res}_{d_1,\ldots,d_n}(f_{1d_1}, \ldots, f_{nd_n}) \neq 0$ is necessary and sufficient for the existence of a set $\mathbb{M}$ of $\mathbf{d}$ monomials which is a basis of $\mathcal{A}$ (and hence, any polynomial can be reduced with respect to this set). Of course, the hard problem is to find such an $\mathbb{M}$!

Let $\mathbb{K}$ be a field, $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$ and

$$\mathbb{M} := \{m_1, \ldots, m_{\mathbf{d}}\} \subset \mathbb{K}[x_1, \ldots, x_n]$$

be a set of $\mathbf{d}$ monomials. Set $\rho := d_1 + \cdots + d_n - n$, and

$$\delta := \delta(\mathbb{M}) = \max\{\deg(m_i),\ i = 1, \ldots, \mathbf{d}\}.$$

Let x_0 be a new variable. For every polynomial $p(x_1, \ldots, x_n) \in \mathbb{K}[x_1, \ldots, x_n]$ we define

$$p^0(x_0, x_1, \ldots, x_n) := x_0^{\deg(p)} p\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right),$$

i.e., p^0 is the homogenization of p with a new variable x_0, and for every $t \geq \delta$, we set

$$\mathbb{M}_t := \{m x_0^{t-\deg(m)},\ m \in \mathbb{M}\}.$$

Let $\mathcal{A}_0$ be the quotient ring $\mathbb{K}[x_0, \ldots, x_n]/(f_1^0, \ldots, f_n^0)$. It is a graded ring of the form $\mathcal{A}_0 = \bigoplus_{i=0}^{\infty} \mathcal{A}_{0i}$.

Set $H_{(d_1,\dots,d_n)}(\tau)$ for the coefficients of the power series

$$\sum_{\tau=0}^{\infty} H_{(d_1,\dots,d_n)}(\tau)T^{\tau} = \frac{\prod_{j=1}^{n}(1-T^{d_j})}{(1-T)^{n+1}}. \tag{2}$$

It turns out that $H_{(d_1,\dots,d_n)}$ is the Hilbert function of $\mathbb{K}[x_0, x_1, \dots, x_n]/J$ when J is an ideal generated by a regular sequence of n homogeneous polynomials of degrees $d_1, \dots, d_n$, that is, $H_{(d_1,\dots,d_n)}(\tau)$ is the dimension as a $\mathbb{K}$-vector space of the piece of degree τ in $\mathbb{K}[x_0, x_1, \dots, x_n]/J$; see Macaulay (1902) and Chardin (1995).

Remark 2.3. From the right-hand side of identity (2), it is easy to check that $H_{(d_1,\dots,d_n)}(\tau) < \mathbf{d}$ if $\tau < \rho$, and $H_{(d_1,\dots,d_n)}(\tau) = \mathbf{d}$ if $\tau \geq \rho$.

If $\operatorname{Res}_{d_1,\dots,d_n}(f_{1d_1}, \dots, f_{nd_n}) \neq 0$ holds, Proposition 2.1 implies that the family of polynomials $f_1^0, \dots, f_n^0, x_0$ has no common roots in projective space and so, $\operatorname{Res}_{d_1,\dots,d_n,1}(f_1^0, \dots, f_n^0, x_0) \neq 0$. But this implies that $f_1^0, \dots, f_n^0, x_0$ is a regular sequence in $\mathbb{K}[x_0, \dots, x_n]$ and, in particular, $f_1^0, \dots, f_n^0$ is also a regular sequence in that ring. Therefore, $\dim(\mathcal{A}_{0\tau}) = H_{(d_1,\dots,d_n)}(\tau)$.

The next proposition shows a relationship between a monomial basis of the affine ring $\mathcal{A}$ and bases of certain graded parts of the ring $\mathcal{A}_0$. This will allow us to state the condition for an arbitrary set $\mathbb{M}$ to be a basis of $\mathcal{A}$.

Proposition 2.4. *If* $\operatorname{Res}_{d_1,\dots,d_n}(f_{1d_1}, \dots, f_{nd_n}) \neq 0$*, then the following conditions are equivalent:*

(1) $\mathbb{M}$ *is a basis of* $\mathcal{A}$ *as a* $\mathbb{K}$*-vector space.*
(2) *There exists* $t_0 \geq \max\{\delta, \rho\}$ *such that* $\mathbb{M}_{t_0}$ *is a basis of* $\mathcal{A}_{0t_0}$ *as a* $\mathbb{K}$*-vector space.*
(3) *For every* $t \geq \max\{\delta, \rho\}$, $\mathbb{M}_t$ *is a basis of* $\mathcal{A}_{0t}$ *as a* $\mathbb{K}$*-vector space.*

Remark 2.5. We will see in Corollary 2.6 that a necessary condition for $\mathbb{M}$ to be a basis of $\mathcal{A}$ is that $\delta \geq \rho$. Therefore, in the statement of Proposition 2.4 we can replace $\max\{\delta, \rho\}$ with δ.

Now we will prove Proposition 2.4.

Proof. Recall that the assumption $\operatorname{Res}_{d_1,\dots,d_n}(f_{1d_1}, \dots, f_{nd_n}) \neq 0$ implies that $f_1^0, \dots, f_n^0$ is a regular sequence in $\mathbb{K}[x_0, \dots, x_n]$.

$\boxed{(1) \Longrightarrow (3)}$ Let $t \geq \max\{\delta, \rho\}$ and consider a linear combination of vectors in $\mathbb{M}_t$ which lies in the ideal $(f_1^0, \dots, f_n^0)$:

$$\sum_{i=1}^{\mathbf{d}} \lambda_i m_i x_0^{t-\deg(m_i)} = \sum_{j=1}^{n} A_j(x_0, \dots, x_n) f_j^0. \tag{3}$$

Setting $x_0 = 1$ we get a linear combination of elements in $\mathbb{M}$ which lies in I. So, if $\mathbb{M}$ is linearly independent, we get that $\mathbb{M}_t$ is linearly independent. As $t \geq \rho$ and $f_1^0, \dots, f_n^0$ is a regular sequence, the dimension of $\mathcal{A}_{0t}$ is $\mathbf{d}$, and therefore we conclude that $\mathbb{M}_t$ is a basis of $\mathcal{A}_{0t}$.

(3) $\implies$ (1) Consider a linear combination of $\mathbb{M}$ as follows:

$$\sum_{i=1}^{\mathbf{d}} \lambda_i m_i = \sum_{j=1}^{n} a_j(x_1, \ldots, x_n) f_j.$$

Let $t_0 := \max\{\delta,\ \rho,\ \deg(a_j f_j),\ j = 1, \ldots, n\}$. Homogenizing the linear combination up to degree t_0, we have an equality like (3) with t_0 instead of t. As $\mathbb{M}_{t_0}$ is linearly independent, it turns out that $\lambda_i = 0$ for $i = 1, \ldots, \mathbf{d}$. Then, $\mathbb{M}$ is a linearly independent set. Taking into account that $\dim(\mathcal{A}) = \mathbf{d}$ it follows that it is a basis of $\mathcal{A}$.

(3) $\implies$ (2) Obvious.

(2) $\implies$ (3) Consider the following exact complex of vector spaces:

$$0 \to \ker \phi_t \to \mathcal{A}_{0t} \xrightarrow{\phi_t} \mathcal{A}_{0(t+1)} \to \left(\mathbb{K}[x_0, \ldots, x_n]/(x_0,\ f_1^0, \ldots,\ f_n^0)\right)_{t+1} \to 0,$$

where $\phi_t(m) = x_0.m$. As $\mathrm{Res}_{1,d_1,\ldots,d_n}(x_0,\ f_1^0, \ldots,\ f_n^0) \neq 0$, it turns out that $\left(\mathbb{K}[x_0, \ldots, x_n]/(x_0,\ f_1^0, \ldots,\ f_n^0)\right)_{t+1} = 0$ if $t \geq \rho$. In addition, for $t \geq \rho$, we have that $\dim(\mathcal{A}_{0t}) = \dim(\mathcal{A}_{0(t+1)})$. So, ϕ_t is an isomorphism if $t \geq \max\{\delta, \rho\}$, and furthermore, $\phi_t(\mathbb{M}_t) = \mathbb{M}_{t+1}$. Then, $\mathbb{M}_{t_0}$ is a basis of $\mathcal{A}_{0t_0}$ for some $t_0 \geq \max\{\delta, \rho\}$ if and only if $\mathbb{M}_t$ is a basis of $\mathcal{A}_{0t}$ for every $t \geq \max\{\delta, \rho\}$. □

The following result, which follows immediately from the proof of Proposition 2.4, gives us a lower bound of the maximal degree one may expect from a monomial basis of $\mathcal{A}$.

Corollary 2.6. *If $\mathbb{M}$ is a basis of $\mathcal{A}$, then $\delta(\mathbb{M}) \geq \rho$.*

Proof. Let $t < \rho$, and suppose that $\mathbb{M}$ is a basis of $\mathcal{A}$ with $\delta = t$. Proceeding as in the proof of (1) $\implies$ (3) in Proposition 2.4, it follows that $\mathbb{M}_t$ is linearly independent in $\mathcal{A}_{0t}$. But, from Remark 2.3, we have that $\dim(\mathcal{A}_{0t}) < \mathbf{d}$ if $t < \rho$, which is a contradiction. □

Example 2.7. Let $f_1,\ f_2,\ f_3$ be generic polynomials of degree two in $\mathbb{K}[x_1, x_2, x_3]$. In this case, $\mathbf{d} = 2.2.2 = 8$. It is well-known that

$$\mathbb{M} := \{1, x_1, x_2, x_3, x_1x_2, x_1x_3, x_2x_3, x_1x_2x_3\}$$

is a basis of $\mathcal{A}$ (see for instance Macaulay (1902)). Observe that $\delta = 3 = \rho$ in this case. On the other hand, Corollary 2.6 implies that there are no eight monomials linearly independent in the set

$$\{1, x_1, x_2, x_3, x_1^2, x_2^2, x_3^2, x_1x_2, x_1x_3, x_2x_3\}.$$

This can be explained as follows. As $f_1^0,\ f_2^0,\ f_3^0$ is a regular sequence, they must be linearly independent. So, the dimension of the $\mathbb{K}$-vector space they generate is 3, and hence the dimension of $\mathcal{A}_{02}$ is $10 - 3 = 7$.

3. Subresultants by means of Koszul complexes

In this section we recall the theory of multivariate subresultants for homogeneous polynomials as formulated in Chardin (1995); see also Demazure (1984).

First, we are going to introduce the crucial notion involved in the definition of subresultants.

3.1. *The determinant of an exact complex of vector spaces*

Let K be a field and let $\mathbf{C}$ be an exact complex of finitely generated K-vector spaces $F_i = K^{B_i}$, with bases B_i, of the form

$$\mathbf{C} : 0 \to F_n \stackrel{\partial_n}{\to} F_{n-1} \stackrel{\partial_{n-1}}{\to} \cdots \stackrel{\partial_2}{\to} F_1 \stackrel{\partial_1}{\to} F_0 \to 0.$$

Then, there exists a decomposition of the K-vector spaces F_i which enables us to associate with the complex $\mathbf{C}$ an element $\Delta \in K$. This element Δ is called the *determinant* of the complex (see Gel'fand et al., 1994, Appendix A). In order to obtain the decomposition, we can proceed as in Demazure (1984), Chardin (1995) and Gel'fand et al. (1994):

ASCENDING DECOMPOSITION

- Set $I_1 := B_0$ and $V_1 := K^{I_1}$.
- Since ∂_1 is onto, there exists a non-zero maximal minor of the matrix of ∂_1. Choose such a non-zero minor, and set I_1' for the subset of B_1 corresponding to the elements indexing the columns of the chosen submatrix and $I_2 := B_1 - I_1'$. Then, if $V_1' := K^{I_1'}$ and $V_2 := K^{I_2}$, we have $F_1 = V_2 \oplus V_1'$, and $\partial_1|_{V_1'} : V_1' \to V_1$ is an isomorphism.
- For $i \geq 2$, consider $\partial_i^* := \pi_{i-1} \circ \partial_i : F_i \to V_i$, where π_{i-1} is the projection from F_{i-1} to V_i. The map ∂_i^* is onto, due to the exactness of $\mathbf{C}$ and the chosen decomposition of F_{i-1}. Then, we can choose a non-zero maximal minor of the matrix of ∂_i^* and consider the subset I_i' of B_i indexing the columns of the chosen submatrix and $I_{i+1} := B_i - I_i'$. Setting $V_i' := K^{I_i'}$ and $V_{i+1} := K^{I_{i+1}}$ we obtain a decomposition $F_i = V_{i+1} \oplus V_i'$ such that the restriction $\partial_i^*|_{V_i'} : V_i' \to V_i$ is an isomorphism.
- In the last step, we obtain a square matrix for ∂_n^*, due to the fact that $\sum_{i=0}^n (-1)^i \dim(F_i) = 0$.

For every $1 \leq i \leq n$, let $\phi_i := \partial_i^*|_{V_i'} : V_i' \to V_i$. The *determinant* of the complex $\mathbf{C}$ (relative to the bases B_i) is defined to be

$$\Delta := \prod_{i=0}^{n-1} \det(\phi_{i+1})^{(-1)^i}.$$

We remark that Δ is (up to a sign) independent of the choices made to perform the decomposition.

A second procedure to obtain a decomposition of a complex which also enables us to compute its determinant, is the following:

DESCENDING DECOMPOSITION

- Set $I_n := B_n$ and $V_n := K^{I_n}$.

- Since ∂_n is into, there exists a non-zero maximal minor of the matrix of ∂_n. Choose such a minor and define $I_{n-1} \subset B_{n-1}$ to be the subset of elements of B_{n-1} indexing the rows not involved in this minor and $I'_n := B_{n-1} - I_{n-1}$. Then we have a decomposition $F_{n-1} = V'_n \oplus V_{n-1}$, where $V'_n := K^{I'_n}$ and $V_{n-1} := K^{I_{n-1}}$.
- Note that, for $i \geq 1$, the previous construction for $i-1$ implies that $\mathrm{Im}(\partial_{n-i+1}) \cap V_{n-i} = 0$, and therefore $\mathrm{Ker}(\partial_{n-i}) \cap V_{n-i} = 0$, that is, the restriction of ∂_{n-i} to V_{n-i} is into. Then we can iterate the process and choose a maximal non-zero minor of the matrix of $\partial_{n-i}|_{V_{n-i}}$, and define I'_{n-i} to be the subset of B_{n-i-1} indexing the rows of the chosen submatrix and I_{n-i-1} to be its complement in B_{n-i-1}. We obtain a decomposition $F_{n-i-1} := V'_{n-i} \oplus V_{n-i-1}$, where $V'_{n-i} := K^{I'_{n-i}}$ and $V_{n-i-1} := K^{I_{n-i-1}}$.
- In the last step a square matrix is obtained, due to the exactness of the complex.

As before, for every $1 \leq i \leq n$, we define $\phi_i := \partial_i^*|_{V_i} : V_i \to V'_i$. It turns out that (Gel'fand et al., 1994; Chardin, 1995) the determinant of $\mathbf{C}$ relative to the bases B_i can also be computed as

$$\Delta := \prod_{i=0}^{n-1} \det(\phi_{i+1})^{(-1)^i}.$$

3.2. Subresultants

Multivariate subresultants are defined as determinants of generically exact Koszul complexes. Let $s \leq n+1$ and let $P_1, \ldots, P_s$ be generic homogeneous polynomials in $n+1$ variables $x_0, \ldots, x_n$ of respective degrees $d_1, \ldots, d_s$:

$$P_i(x_0, \ldots, x_n) := \sum_{|\alpha|=d_i} c_{i,\alpha} x^\alpha, \qquad i = 1, \ldots, s,$$

where the $c_{i,\alpha}$'s are new variables.

In this case, K is the field of fractions of $A := \mathbb{Z}[c_{i,\alpha}, |\alpha| = d_i, i = 1, \ldots, s]$. Set $R := A[x_0, x_1, \ldots, x_n]$.

Let $\mathfrak{M}_t$ be the set of all monomials of degree t in the variables $x_0, \ldots, x_n$, and let S be a family of $H_{d_1,\ldots,d_s}(t)$ monomials in $\mathfrak{M}_t$. With this data we can construct a complex $\mathbf{C} = \mathbf{C}_t^s$ which is obtained by modifying the degree t part of the Koszul complex associated with $P_1, \ldots, P_s$ as follows:

$$0 \to (\wedge^s R^s)_t \xrightarrow{\partial_s} (\wedge^{s-1} R^s)_t \xrightarrow{\partial_{s-1}} \cdots \xrightarrow{\partial_2} (\wedge^1 R^s)_t \xrightarrow{\varphi} A\langle \mathfrak{M}_t \setminus S \rangle \to 0$$

equipped with the bases $B_k := \bigcup_{1 \leq i_1 < \cdots < i_k \leq s} \bigcup_{x^\alpha \in \mathbf{M}_{t-d_{i_1}-\cdots-d_{i_k}}} X^\alpha e_{i_1} \wedge \cdots \wedge e_{i_k}$.

If this complex is generically exact (i.e., $\mathbf{C} \otimes K$ is exact as a complex of K-vector spaces), then the *subresultant of S with respect to the polynomials* $P_1, \ldots, P_s$, which will be denoted with Δ_S^t, is defined to be the determinant of $\mathbf{C} \otimes K$ with respect to the monomial bases; otherwise we set $\Delta_S^t := 0$. As we have $H_i(\mathbf{C}_t^s) = 0$ for $i > 0$ (Jouanolou, 1980; Chardin, 1995), it turns out that Δ_S^t is a *polynomial* in the coefficients of the P_i's which satisfies the following property (Chardin, 1995, Theorem 2): Let $\mathbf{k}$ be any field, and

$\tilde{P}_i \in \mathbf{k}[x_0, \ldots, x_n]_{d_i}$, $i = 1, \ldots, s$. Then

$$\Delta^t_S(\tilde{P}_1, \ldots, \tilde{P}_s) \neq 0 \iff J_t + \mathbf{k}\langle S\rangle = \mathbf{k}[x_0, \ldots, x_n]_t,$$

where J_t is the degree t part of the ideal generated by the $\tilde{P}_i$'s.

4. Monomial bases and subresultants

In this section, we will relate our problem with multivariate subresultants.

We set $s = n$, and let $P_1, \ldots, P_n$ be the homogeneous polynomials $f_1^0, \ldots, f_n^0$ defined above. The following may be regarded as the main result of this section.

Theorem 4.1. *Let $\mathbb{M} \subset \mathbb{K}[x_1, \ldots, x_n]$ be a set of* **d** *monomials, and set $t := \delta(M)$. Let $\Delta^t_{\mathbb{M}_t}$ be the subresultant of $\mathbb{M}_t$ with respect to $f_1^0, \ldots, f_n^0$. Then, $\mathbb{M}$ is a basis of $\mathcal{A}$ if and only if*

$$P_{\mathbb{M},d_1,\ldots,d_n} := \mathrm{Res}_{d_1,\ldots,d_n}(f_{1d_1}, \ldots, f_{nd_n})\Delta^t_{\mathbb{M}_t} \neq 0. \tag{4}$$

Proof. If $\mathbb{M}$ is a basis of $\mathcal{A}$, the family $f_1, \ldots, f_n$ has all its zeros in $\overline{\mathbb{K}}^n$, and therefore, $\mathrm{Res}_{d_1,\ldots,d_n}(f_{1d_1}, \ldots, f_{nd_n}) \neq 0$. In addition, from Corollary 2.6 and Proposition 2.4 it follows that $\mathbb{M}_t$ is a basis of $\mathcal{A}_{0t}$, which implies that $\Delta^t_{\mathbb{M}_t} \neq 0$.

In order to prove the converse, we can apply Proposition 2.4, as $\mathrm{Res}_{d_1,\ldots,d_n}(f_{1d_1}, \ldots, f_{nd_n}) \neq 0$. The condition $\Delta^t_{\mathbb{M}_t} \neq 0$ implies that $\mathbb{M}_t$ is a basis of $\mathcal{A}_{0t}$, and then we conclude that $\mathbb{M}$ is a basis of $\mathcal{A}$. $\square$

Example 4.2. For $i = 1, 2, 3$, let $f_i := \sum_{|\alpha|\leq 2} c_{i,\alpha} x^\alpha$ be generic polynomials of degree two in $\mathbb{K}[x_1, x_2, x_3]$, and let $\mathbb{M}$ be as in Example 2.7. The subresultant $\Delta^3_{\mathbb{M}_3}$ can be computed as the product of the determinants of the following two matrices:

$$\begin{pmatrix} c_{1,2,0,0} & c_{1,0,2,0} & c_{1,0,0,2} \\ c_{2,2,0,0} & c_{2,0,2,0} & c_{2,0,0,2} \\ c_{3,2,0,0} & c_{3,0,2,0} & c_{3,0,0,2} \end{pmatrix}$$

and

$$\begin{pmatrix}
c_{1,2,0,0} & 0 & 0 & c_{1,1,1,0} & c_{1,1,0,1} & 0 & c_{1,0,0,2} & 0 & c_{1,0,1,1} \\
0 & c_{1,0,2,0} & 0 & c_{1,2,0,0} & 0 & c_{1,0,1,1} & 0 & c_{1,0,0,2} & c_{1,1,1,0} \\
0 & 0 & c_{1,0,0,2} & 0 & c_{1,2,0,0} & c_{1,0,2,0} & c_{1,1,0,1} & c_{1,0,1,1} & 0 \\
c_{2,2,0,0} & 0 & 0 & c_{2,1,1,0} & c_{2,1,0,1} & 0 & c_{2,0,0,2} & 0 & c_{2,0,1,1} \\
0 & c_{2,0,2,0} & 0 & c_{2,2,0,0} & 0 & c_{2,0,1,1} & 0 & c_{2,0,0,2} & c_{2,1,1,0} \\
0 & 0 & c_{2,0,0,2} & 0 & c_{2,2,0,0} & c_{2,0,2,0} & c_{2,1,0,1} & c_{2,0,1,1} & 0 \\
c_{3,2,0,0} & 0 & 0 & c_{3,1,1,0} & c_{3,1,0,1} & 0 & c_{3,0,0,2} & 0 & c_{3,0,1,1} \\
0 & c_{3,0,2,0} & 0 & c_{3,2,0,0} & 0 & c_{3,0,1,1} & 0 & c_{3,0,0,2} & c_{3,1,1,0} \\
0 & 0 & c_{3,0,0,2} & 0 & c_{3,2,0,0} & c_{3,0,2,0} & c_{3,1,0,1} & c_{3,0,1,1} & 0
\end{pmatrix}.$$

For a proof of this fact, see Theorem 5.2 below.

5. Factorization of subresultants

For several sets $\mathbb{M}$, the polynomial $P_{\mathbb{M},d_1,\ldots,d_n}$ defined in (4) depends only on the coefficients of $f_{1d_1}, \ldots, f_{nd_n}$ and factorizes as a product of more than two terms. For instance, Macaulay (1902) showed that one can decide whether

$$\mathbb{M}^0 := \{x_1^{\alpha_1} \cdots x_n^{\alpha_n}, 0 \le \alpha_i \le d_i - 1\} \tag{5}$$

is a basis of $\mathcal{A}$ by applying linear algebra on the coefficients of the highest terms of $f_1, \ldots, f_n$ (see also Bikker and Uteshev, 1999). The same has been done by Bikker and Uteshev (1999) with

$$\mathbb{M}^1 := \{x_1^{\alpha_1} x_2^{\alpha_2}, 0 \le \alpha_1 < d_1, 0 \le \alpha_2 \le d_1 + d_2 - 2\alpha_1 - 2\}, \tag{6}$$

and with

$$\begin{aligned}\{x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3},\ 0 \le \alpha_1 < d_1,\ 0 \le \alpha_2 < \min(d_1, d_2, 2(d_1 - \alpha_1) - 1),\\ 0 \le \alpha_3 < d_1 + d_2 + d_3 - 2(\alpha_1 + \alpha_2 + 1)\},\end{aligned}$$

for $n = 2$ and $n = 3$ respectively. This is not always the case, as the following cautionary example shows.

Example 5.1. Consider $n = 3$. Set $d_1 = d_2 = d_3 = 2$ and write $f_i := \sum_{|\alpha| \le 2} c_{i,\alpha} x^\alpha$ for $i = 1, 2, 3$. Take

$$\mathbb{M} := \{x_1^3, x_1, x_2, x_3, x_1x_2, x_1x_3, x_2x_3, x_1x_2x_3\}.$$

Then, $\Delta^3_{\mathbb{M}_3}$ is the determinant of the following matrix:

$$\begin{pmatrix}
c_{1,0,0,0} & 0 & 0 & 0 & c_{2,0,0,0} & 0 & 0 & 0 & c_{3,0,0,0} & 0 & 0 & 0\\
0 & 0 & c_{1,0,2,0} & 0 & 0 & 0 & c_{2,0,2,0} & 0 & 0 & 0 & c_{3,0,2,0} & 0\\
0 & 0 & 0 & c_{1,0,0,2} & 0 & 0 & 0 & c_{2,0,0,2} & 0 & 0 & 0 & c_{3,0,0,2}\\
c_{1,2,0,0} & c_{1,1,0,0} & 0 & 0 & c_{2,2,0,0} & c_{2,1,0,0} & 0 & 0 & c_{3,2,0,0} & c_{3,1,0,0} & 0 & 0\\
c_{1,0,2,0} & 0 & c_{1,0,1,0} & 0 & c_{2,0,2,0} & 0 & c_{2,0,1,0} & 0 & c_{3,0,2,0} & 0 & c_{3,0,1,0} & 0\\
c_{1,0,0,2} & 0 & 0 & c_{1,0,0,1} & c_{2,0,0,2} & 0 & 0 & c_{2,0,0,1} & c_{3,0,0,2} & 0 & 0 & c_{3,0,0,1}\\
0 & c_{1,1,1,0} & c_{1,2,0,0} & 0 & 0 & c_{2,1,1,0} & c_{2,2,0,0} & 0 & 0 & c_{3,1,1,0} & c_{3,2,0,0} & 0\\
0 & c_{1,1,0,1} & 0 & c_{1,2,0,0} & 0 & c_{2,1,0,1} & 0 & c_{2,2,0,0} & 0 & c_{3,1,0,1} & 0 & c_{3,2,0,0}\\
0 & c_{1,0,2,0} & c_{1,1,1,0} & 0 & 0 & c_{2,0,2,0} & c_{2,1,1,0} & 0 & 0 & c_{3,0,2,0} & c_{3,1,1,0} & 0\\
0 & c_{1,0,0,2} & 0 & c_{1,1,0,1} & 0 & c_{2,0,0,2} & 0 & c_{2,1,0,1} & 0 & c_{3,0,0,2} & 0 & c_{3,1,0,1}\\
0 & 0 & c_{1,0,0,2} & c_{1,0,1,1} & 0 & 0 & c_{2,0,0,2} & c_{2,0,1,1} & 0 & 0 & c_{3,0,0,2} & c_{3,0,1,1}\\
0 & 0 & c_{1,0,1,1} & c_{1,0,2,0} & 0 & 0 & c_{2,0,1,1} & c_{2,0,2,0} & 0 & 0 & c_{3,0,1,1} & c_{3,0,2,0}
\end{pmatrix}.$$

With the aid of `Maple` we have computed this determinant, which is an irreducible polynomial depending on all the variables $c_{i,\alpha}$.

Set

$$\sum_{\tau=0}^{\infty} h_{(d_1,\ldots,d_n)}(\tau) T^\tau = \frac{\prod_{j=1}^{n} (1 - T^{d_j})}{(1 - T)^n}. \tag{7}$$

It turns out that $h_{d_1,\dots,d_n}$ is the Hilbert function of the ideal generated by a regular sequence of n homogeneous polynomials in n variables of degrees $d_1, \dots, d_n$ respectively.

The following is the main result of this section:

Theorem 5.2. *Let $P_{\mathbb{M},d_1,\dots,d_n}$ be the polynomial defined in (4). Then, if $P_{\mathbb{M},d_1,\dots,d_n}$ is not identically zero, the following conditions are equivalent:*

- *$P_{\mathbb{M},d_1,\dots,d_n}$ depends only on the coefficients of $f_{1d_1}, \dots, f_{nd_n}$.*
- *For every $t = 0, 1, \dots, \rho$, the cardinality of $\mathbb{M} \cap \mathbb{K}[x_1, \dots, x_n]_t$ equals $h_{(d_1,\dots,d_n)}(t)$.*

If any of the above conditions hold, we have the following factorization:

$$\Delta^{\delta}_{\mathbb{M}_\delta} = \prod_{t=\min\{d_i\}}^{\rho} D^t_{\mathbb{M}\cap\mathbb{K}[x_1,\dots,x_n]_t}, \tag{8}$$

where D^t_S denotes the subresultant in n variables of S with respect to $f_{1d_1}, \dots, f_{nd_n}$.

Proof. If $P_{\mathbb{M},d_1,\dots,d_n}$ depends only on the coefficients of $f_{1d_1}, \dots, f_{nd_n}$, we can set to zero all the coefficients of $f_1, \dots, f_n$ not appearing in these leading forms and work with this family of homogeneous polynomials instead of $f_1, \dots, f_n$. As $P_{\mathbb{M},d_1,\dots,d_n}$ is not identically zero, we have that $\Delta^{\delta}_{\mathbb{M}_\delta}$ is not identically zero either and this implies that $\mathbb{M}$ is a basis of the homogeneous quotient ring $\mathbb{K}[x_1, \dots, x_n]/(f_{1d_1}, \dots, f_{nd_n})$. As the family $f_{1d_1}, \dots, f_{nd_n}$ is a regular sequence in $\mathbb{K}[x_1, \dots, x_n]$, it turns out that $\#(\mathbb{M} \cap \mathbb{K}[x_1, \dots, x_n]_t) = h_{(d_1,\dots,d_n)}(t)$ for any $t = 0, \dots, \rho$, and we are done.

In order to prove the other implication, we will work with generic homogeneous polynomials. For each $i = 1, \dots, n$ and $\alpha \in \mathbb{N}_0^n$ with $|\alpha| \leq d_i$, introduce a variable $c_{i,\alpha}$. Set

$$f_i(x_1, \dots, x_n) := \sum_{|\alpha|\leq d_i} c_{i,\alpha}\, x^\alpha, \qquad i = 1, \dots, n. \tag{9}$$

We shall work in the field $\mathbb{K} := \mathbb{Q}(c_{i,\alpha})$. In this situation we have that $\mathrm{Res}_{d_1,\dots,d_n}(f_{1d_1}, \dots, f_{nd_n}) \neq 0$ (see for instance Cox et al. (1998)) and, due to the universal property of subresultants (Chardin, 1995), if $P_{\mathbb{M},d_1,\dots,d_n} \neq 0$ for a given family of polynomials in *any* field, then it will not be zero for the generic family (9).

As before, set f_i^0 for the homogenization of the polynomial f_i in $\mathbb{K}[x_0, \dots, x_n]$. Consider the following $\mathbb{K}$-linear map:

$$\begin{array}{rccc} \phi^\rho: & S^1_{\rho-d_1} \oplus \cdots \oplus S^n_{\rho-d_n} & \to & S_\rho \\ & (p_1, \dots, p_n) & \mapsto & \sum_{i=1}^n p_i\, f_i^0, \end{array} \tag{10}$$

where $S_\rho := \mathbb{K}[x_0, x_1, \dots, x_n]_\rho$, and for each $i = 1, \dots, n$,

$$S^i_{\rho-d_i} := \left\langle x_0^{\alpha_0} \cdots x_n^{\alpha_n}, \sum_{j=0}^{n} \alpha_j = \rho - d_i, \alpha_1 < d_1, \dots, \alpha_{i-1} < d_{i-1} \right\rangle.$$

Let M be the matrix obtained from the matrix of ϕ^ρ in the monomial bases by deleting the columns[1] indexed by the elements in $\mathbb{M}$ and let M' be the matrix obtained in the same way but using the set

$$S := \{x_0^{\alpha_0} \cdots x_n^{\alpha_n}, |\alpha| = \rho, \alpha_i < d_i, i = 1, \ldots, n\} \tag{11}$$

instead of $\mathbb{M}$. It is well-known that $\det(M') \neq 0$ (Macaulay, 1902; Chardin, 1995).

As the subresultant of S with respect to $f_1^0, \ldots, f_n^0$ is the determinant of $\mathbf{C}_t^S$, it turns out that $\det(M')$ may be regarded as a non-zero maximal minor in the last morphism of the complex whose determinant is Δ_S^ρ.

Starting with this maximal minor and using the ascending decomposition of the Koszul complex, it turns out that there exists an element $\mathcal{E} \in \mathbb{K}$, which is actually a polynomial in the $c_{i,\alpha}$, such that $\det(M') = \mathcal{E}\, \Delta_S^\rho$. As $\det(M') \neq 0$, then $\mathcal{E} \neq 0$.

This $\mathcal{E}$ is a product of complementary minors in $\mathbf{C}_t^S$. Starting now with these minors from the left and applying the descending decomposition of the Koszul complex, one can see that, as in Chardin (1995), $\det(M) = \mathcal{E}\, \Delta_{\mathbb{M}}^\rho$, as the complex whose determinant is $\Delta_{\mathbb{M}}^\rho$ is the same as the one whose determinant is Δ_S^ρ except in the last map.

Set $\mathbb{M}(t) := \mathbb{M} \cap \mathbb{K}[x_1, \ldots, x_n]_t$, $t = 0, 1, \ldots, \rho$, and suppose w.l.o.g. that $d_1 \leq d_i$, $i = 2, \ldots, n$. As $\#\mathbb{M}(t) = h_{d_1,\ldots,d_n}(t)$, proceeding as in Macaulay (1902), it follows that—ordering appropriately its rows and columns—the matrix M has the following block structure:

$$\begin{pmatrix} M_\rho & * & * & * \\ 0 & M_{\rho-1} & * & * \\ 0 & 0 & \ddots & * \\ 0 & 0 & \cdots & M_{d_1} \end{pmatrix}, \tag{12}$$

where M_t is the square matrix obtained by deleting the columns indexed by the monomials in $\mathbb{M}(t)$ in the matrix of the $\mathbb{K}$-linear map:

$$\begin{aligned} \phi_t : S_{t-d_1}^{1*} \oplus \cdots \oplus S_{t-d_n}^{n*} &\to S_t^* \\ (p_1, \ldots, p_n) &\mapsto \sum_{i=1}^n p_i\, f_{id_i}. \end{aligned}$$

Here $S_t^* := \mathbb{K}[x_1, \ldots, x_n]_t$, and for each $i = 1, \ldots, n$,

$$S_{t-d_i}^{i*} := \left\langle x_1^{\alpha_1} \cdots x_n^{\alpha_n}, \sum_{k=1}^n \alpha_k = t - d_i,\ \alpha_1 < d_1, \ldots, \alpha_{i-1} < d_{i-1} \right\rangle.$$

Then, we have that $\det(M) = \prod_{t=d_1}^\rho \det(M_t)$, which shows that $\det(M)$ depends only on the coefficients of $f_{id_i}, i = 1, \ldots, n$. Furthermore, $\det(M_t) = \mathcal{E}_t D^t_{\mathbb{M}\cap\mathbb{K}[x_1,\ldots,x_n]_t}$ for $t = 0, \ldots, \rho$, and the extraneous factor $\mathcal{E}$ has also a block structure compatible with the one given in (12), that is, $\mathcal{E} = \prod_{t=d_1}^\rho \mathcal{E}_t$; see Macaulay (1902) and Chardin (1994a). This completes the proof of the theorem. □

[1] As in Macaulay (1902), the rows of M are indexed by the monomial basis of the domain.

Corollary 5.3. *If $P_{\mathbb{M},d_1,\ldots,d_n}$ is not identically zero and depends only on the coefficients of $f_{1d_1},\ldots,f_{nd_n}$, then $\delta(\mathbb{M})=\rho$.*

6. Simple roots and generalized Vandermonde determinants

In this section, we will study a result by Macaulay (1902) concerning the structure of a generalized Vandermonde determinant associated with the monomial set $\mathbb{M}^0$ and, with the aid of subresultants, we will extend it to arbitrary sets of monomials with cardinality $\mathbf{d}$. This will make apparent the relationship between the non-vanishing of the generalized Vandermonde determinant associated with a set of monomials $\mathbb{M}$ and the fact that $\mathbb{M}$ is a basis of the quotient algebra $\mathcal{A}$ in the case of a polynomial system with simple roots.

We will work in the generic field $\mathbb{K}=\mathbb{Q}(c_{i,\alpha})$, and with the family (9). Let $V(f_1,\ldots,f_n)=\{\xi_1,\ldots,\xi_{\mathbf{d}}\}\subset\overline{\mathbb{K}}^n$, and set $\mathbb{M}^0=\{m_1,\ldots,m_{\mathbf{d}}\}$ (recall that $\mathbb{M}^0$ was defined in (5)). Let M_0 be the $\mathbf{d}\times\mathbf{d}$ matrix whose rows (resp. columns) are indexed by the elements of $V(f_1,\ldots,f_n)$ (resp. $\mathbb{M}^0$), such that the element indexed by (ξ_i,m_j) is the evaluation of m_j at ξ_i, that is, $M_0:=\big(m_j(\xi_i)\big)_{1\le i,j\le n}$.

In (Macaulay, 1902, Section 10), it is proven that

$$\det(M_0)^2=\mathbf{c}\,\mathcal{J}\frac{\Big(\Delta^{\rho}_{\mathbb{M}^0_\rho}\Big)^2}{\mathrm{Res}_{(d_1,\ldots,d_n)}(f_{1d_1},\ldots,f_{nd_n})^{\rho+1}},\tag{13}$$

where $\mathcal{J}:=\prod_{i=1}^{\mathbf{d}}J(\xi_i)$ (here $J:=\det\big(\partial f_i/\partial x_j\big)_{1\le i,j\le n}$ is the Jacobian of the sequence $f_1,\ldots,f_n$), and $\mathbf{c}\in\mathbb{Q}$ is a numerical constant depending only on n and the degrees $d_1,\ldots,d_n$.

The constant $\mathbf{c}$ in (13) has an explicit expression in terms of $d_1,\ldots,d_n$:

Lemma 6.1.

$$\mathbf{c}=(-1)^{E_n(d_1,\ldots,d_n)},$$

where

$$E_n(d_1,\ldots,d_n):=\sum_{j=1}^{n}d_1\cdots d_{j-1}\frac{(d_j-1)d_j}{2}d_{j+1}\cdots d_n.$$

Proof. First, observe that a system $f_1,\ldots,f_n$ having the property that $f_{id_i}=x_i^{d_i}$ for $i=1,\ldots,n$, verifies $\mathrm{Res}_{(d_1,\ldots,d_n)}(f_{1d_1},\ldots,f_{nd_n})=1$ and $(\Delta^{\rho}_{\mathbb{M}^0_\rho})^2=1$, as both polynomials depend only on the coefficients of $f_{1d_1},\ldots,f_{nd_n}$ (see Theorem 5.2 above). Therefore, the numerical factor $\mathbf{c}$ can be obtained from identity (13) by specializing the coefficients of f_i in such a way that $f_{id_i}=x_i^{d_i}$, $i=1\ldots,n$. If this is the case, we get

$$\mathbf{c}=\frac{\det(M_0)^2}{\mathcal{J}}.\tag{14}$$

The theorem will be proved by induction on n.

First, we fix some notation. We denote by $c_n(d_1,\ldots,d_n)$ the numerical factor associated with n and degrees $d_1,\ldots,d_n$. If $f_1,\ldots,f_n$ is a system of polynomials in n variables of degrees $d_1,\ldots,d_n$, we denote by $\mathcal{M}_n(f_1,\ldots,f_n)$ the matrix M_0 associated with the system $f_1,\ldots,f_n$ and the set $\mathbb{M}^0$, and we set $\mathcal{J}_n(f_1,\ldots,f_n) := \prod_{i=1}^{\mathbf{d}} J(\xi_i)$.

For $n = 1$, set $d_1 = d$ for a positive integer and let $f_1 := x_1^d - 1$. We have that $V(f_1) = \{\xi_1,\ldots,\xi_d\}$ is the set of dth roots of unity. The matrix M_0 is the Vandermonde matrix associated with the roots of f_1, and so, $\det(M_0)^2 = \mathrm{disc}(f_1) = (-1)^{d-1+\frac{d(d-1)}{2}} d^d$. In addition, $\mathcal{J} = (-1)^{d-1} d^d$. Then we conclude from identity (14) that

$$c_1(d) = (-1)^{\frac{d(d-1)}{2}}.$$

Assume now that the formula holds for systems of n polynomials in n variables and consider $n+1$ polynomials in $n+1$ variables.

- For degrees $d_1,\ldots,d_n,1$: Set $f_i := x_i^{d_i} - 1$ for $i = 1,\ldots,n$, and $f_{n+1} := x_{n+1}$. We have

  $$V(f_1,\ldots,f_{n+1}) = \{(\eta_1,\ldots,\eta_n,0) : \eta_i^{d_i} = 1,\ 1 \le i \le n\},$$

  and so, it is straightforward to check that

  $$\mathcal{M}_{n+1}(f_1,\ldots,f_n,f_{n+1}) = \mathcal{M}_n(x_1^{d_1}-1,\ldots,x_n^{d_n}-1),$$
  $$\mathcal{J}_{n+1}(f_1,\ldots,f_n,f_{n+1}) = \mathcal{J}_n(x_1^{d_1}-1,\ldots,x_n^{d_n}-1).$$

  Identity (14) implies

  $$c_{n+1}(d_1,\ldots,d_n,1) = c_n(d_1,\ldots,d_n),$$

  and the formula holds.
- For degrees $d_1,\ldots,d_n,d_{n+1}+1$: Set $f_i := x_i^{d_i}-1$ for $1 \le i \le n$, and $f_{n+1} := x_{n+1}^{d_{n+1}+1} - x_{n+1}$. Then, $V(f_1,\ldots,f_{n+1}) = V_1 \cup V_2$, where $V_1 = V(x_1^{d_1}-1,\ldots,x_n^{d_n}-1) \times \{0\}$ and $V_2 = V(x_1^{d_1}-1,\ldots,x_n^{d_n}-1) \times \{\eta \in \overline{\mathbb{K}} : \eta^{d_{n+1}} = 1\}$. Arranging the monomials in $\mathbb{M}^0$ so that those which do not depend on the variable x_{n+1} come first and the roots of the system so that those in V_1 come first, it follows that $\mathcal{M}_{n+1}(f_1,\ldots,f_{n+1})$ has the following block structure:

  $$\begin{pmatrix} \mathcal{M}_n(x_1^{d_1}-1,\ldots,x_n^{d_n}-1) & 0 \\ * & \mathcal{M}'_{n+1}(x_1^{d_1}-1,\ldots,x_n^{d_n}-1,x_{n+1}^{d_{n+1}}-1) \end{pmatrix}$$

  where $\mathcal{M}'_{n+1}(x_1^{d_1}-1,\ldots,x_n^{d_n}-1,x_{n+1}^{d_{n+1}}-1)$ is a matrix differing from $\mathcal{M}_{n+1}(x_1^{d_1}-1,\ldots,x_n^{d_n}-1,x_{n+1}^{d_{n+1}}-1)$ only in a factor by a d_{n+1}-th root of unity in each row. Moreover, each root of unity appears in exactly $d_1\cdots d_n$ rows. Taking into account that the product of all the d_{n+1}th roots of unity equals $(-1)^{d_{n+1}-1}$, it follows that $\big(\det\mathcal{M}_{n+1}(f_1,\ldots,f_{n+1})\big)^2$ equals the product

  $$\big(\det\mathcal{M}_n(x_1^{d_1}-1,\ldots,x_n^{d_n}-1)\big)^2\big(\det\mathcal{M}_{n+1}(x_1^{d_1}-1,\ldots,x_n^{d_n}-1,x_{n+1}^{d_{n+1}}-1)\big)^2.$$

On the other hand, the Jacobian of the polynomial system $f_1, \ldots, f_n, f_{n+1}$ is $J = d_1 x_1^{d_1-1} \cdots d_n x_n^{d_n-1}((d_{n+1}+1)x_{n+1}^{d_{n+1}}-1)$ and then, for every $\xi \in V_1$, $J(\xi) = (-1) J(x_1^{d_1}-1, \ldots, x_n^{d_n}-1)(\xi)$ and, for every $\xi \in V_2$, $J(\xi) = \xi_{n+1} J(x_1^{d_1}-1, \ldots, x_{n+1}^{d_{n+1}}-1)(\xi)$. Then, it follows easily that

$$\prod_{\xi \in V_1} J(\xi) = (-1)^{d_1 \cdots d_n} \mathcal{J}_n(x_1^{d_1}-1, \ldots, x_n^{d_n}-1),$$

$$\prod_{\xi \in V_2} J(\xi) = (-1)^{d_1 \cdots d_n (d_{n+1}-1)} \mathcal{J}_{n+1}(x_1^{d_1}-1, \ldots, x_n^{d_n}-1, x_{n+1}^{d_{n+1}}-1)$$

and so, $\mathcal{J}_{n+1}(f_1, \ldots, f_{n+1})$ equals

$$(-1)^{d_1 \cdots d_n d_{n+1}} \mathcal{J}_n(x_1^{d_1}-1, \ldots, x_n^{d_n}-1) \mathcal{J}_{n+1}(x_1^{d_1}-1, \ldots, x_n^{d_n}-1, x_{n+1}^{d_{n+1}}-1).$$

From the expressions for $\mathcal{M}_{n+1}$ and $\mathcal{J}_{n+1}$, we deduce:

$$c_{n+1}(d_1, \ldots, d_n, d_{n+1}+1) = (-1)^{d_1 \cdots d_n d_{n+1}} c_n(d_1, \ldots, d_n) c_{n+1}(d_1, \ldots, d_n, d_{n+1}).$$

Thus, the inductive assumption implies that $c_{n+1}(d_1, \ldots, d_n, d_{n+1}+1) = \pm 1$. More precisely, the exponent $E_{n+1}(d_1, \ldots, d_n, d_{n+1}+1)$ giving the sign equals

$$\begin{aligned} &d_1 \cdots d_n d_{n+1} + E_n(d_1, \ldots, d_n) + E_{n+1}(d_1, \ldots, d_n, d_{n+1}) \\ &\quad = \sum_{j=1}^{n+1} d_1 \cdots d_{j-1} \frac{(d_j-1)d_j}{2} d_{j+1} \cdots d_n d_{n+1}. \quad \square \end{aligned}$$

Let $\mathbb{M}$ be any set of monomials of cardinality **d**, and let $M := M(\mathbb{M})$ be the matrix defined as M_0 but with the columns indexed by the elements of $\mathbb{M}$. The main result of this section is an expression similar to (13) for M:

Theorem 6.2.

$$\det(M(\mathbb{M}))^2 = \pm \mathcal{J} \frac{(\Delta^{\delta}_{\mathbb{M}_\delta})^2}{\mathrm{Res}_{(d_1,\ldots,d_n)}(f_{1d_1}, \ldots, f_{nd_n})^{2\delta-\rho+1}}.$$

The following result will be needed in the proof of Theorem 6.2.

Lemma 6.3. *For any $t \geq \delta = \delta(\mathbb{M})$,*

$$\Delta^t_{\mathbb{M}_t} = \Delta^{\delta}_{\mathbb{M}_\delta} \mathrm{Res}_{(d_1,\ldots,d_n)}(f_{1d_1}, \ldots, f_{nd_n})^{t-\delta}.$$

Proof. It is enough to prove the result for $t = \delta + 1$ and $\delta \geq \rho$ (otherwise, both subresultants are identically zero and the claim holds).

Consider the morphisms for computing $\Delta^{\delta}_{\mathbb{M}_\delta}$ and $\Delta^{\delta+1}_{\mathbb{M}_{\delta+1}}$ as in (10):

$$\begin{array}{ccc} S^1_{\delta-d_1} \oplus \cdots \oplus S^n_{\delta-d_n} & \overset{\phi^\delta}{\rightarrow} & S_\delta \\ \downarrow & & \downarrow \\ S^1_{\delta+1-d_1} \oplus \cdots \oplus S^n_{\delta+1-d_n} & \overset{\phi^{\delta+1}}{\rightarrow} & S_{\delta+1}, \end{array} \tag{15}$$

where the vertical maps are multiplication by x_0. It is straightforward to check that the diagram (15) commutes. For $i = \delta, \delta+1$, let M^i be the matrix of ϕ^i where we have deleted the columns indexed by those $m \in \mathbb{M}_i$. If we order the rows and columns of $M^{\delta+1}$ in such a way that the monomials having degree zero in x_0 come first, it is easy to see that this matrix has the following structure:

$$\begin{pmatrix} M_{\delta+1} & * \\ 0 & M^{\delta} \end{pmatrix},$$

where $M_{\delta+1}$ has been defined in the proof of Theorem 5.2.

As $\delta + 1 > \rho$, there exists a polynomial $\mathcal{E}_1 \in \mathbb{Q}[c_{i,\alpha}]$ such that $\det(M_{\delta+1}) = \mathrm{Res}_{(d_1,\ldots,d_n)}(f_{1d_1}, \ldots, f_{nd_n})\mathcal{E}_1$ (Macaulay, 1902). Besides, there are also elements $\mathcal{E}_2$ and $\mathcal{E}$ such that $\det(M^{\delta}) = \Delta^{\delta}_{\mathbb{M}_\delta}\mathcal{E}_2$ and $\det(M^{\delta+1}) = \Delta^{\delta+1}_{\mathbb{M}_{\delta+1}}\mathcal{E}$. As in the proof of Theorem 5.2, we use the block structure of the extraneous factor $\mathcal{E}$ (Macaulay, 1902; Chardin, 1994a), and it turns out that $\mathcal{E} = \mathcal{E}_1\mathcal{E}_2$. $\square$

Proof of Theorem 6.2. Let $\delta = \delta(\mathbb{M})$. If $\Delta^{\delta}_{\mathbb{M}_\delta} = 0$, it follows that the same holds for $\det(M(\mathbb{M}))$.

If this is not the case, consider the following complex of $\overline{\mathbb{K}}$-vector spaces:

$$0 \to S^1_{\delta-d_1} \oplus \cdots \oplus S^n_{\delta-d_n} \xrightarrow{\phi} S_\delta \xrightarrow{\psi} \overline{\mathbb{K}}^{\mathbf{d}} \to 0, \tag{16}$$

where $S_\delta := \overline{\mathbb{K}}[x_0, x_1, \ldots, x_n]_\delta$ and, as before,

$$S^i_{\delta-d_i} := \langle x_0^{\alpha_0}\cdots x_n^{\alpha_n},\ \sum_{j=0}^{n}\alpha_j = \delta - d_i,\ \alpha_1 < d_1, \ldots, \alpha_{i-1} < d_{i-1}\rangle_{\overline{\mathbb{K}}},$$
$$\phi(p_1, \ldots, p_n) := \sum_{i=1}^{n} p_i\, f_i^0,$$
$$\psi(p(x)) := (p(1, \xi_1), \ldots, p(1, \xi_{\mathbf{d}})).$$

It is easy to see that the complex (16) is exact. If $\mathbb{M}'$ is another set of $\mathbf{d}$ elements such that $\delta(\mathbb{M}') \le \delta(\mathbb{M})$ and $\det(M(\mathbb{M}')) \neq 0$, we denote with $D(\mathbb{M}'_\delta)$ (resp. $D(\mathbb{M}_\delta)$) the determinant of the matrix of ϕ in the monomial bases where we have deleted the columns indexed by those monomials lying in $\mathbb{M}'_\delta$ (resp. $\mathbb{M}_\delta$). Then, considering the determinant of the complex (16), we have the following:

$$\frac{D(\mathbb{M}_\delta)}{\det(M(\mathbb{M}))} = \pm\frac{D(\mathbb{M}'_\delta)}{\det(M(\mathbb{M}'))}.$$

As in the proof of Theorem 5.2, it turns out that $D(\mathbb{M}'_\delta) = \mathcal{E}\,\Delta^{\delta}_{\mathbb{M}'_\delta}$ and $D(\mathbb{M}_\delta) = \mathcal{E}\,\Delta^{\delta}_{\mathbb{M}_\delta}$, with the same extraneous factor $\mathcal{E}$. Therefore

$$\frac{\Delta^{\delta}_{\mathbb{M}_\delta}}{\det(M(\mathbb{M}))} = \pm\frac{\Delta^{\delta}_{\mathbb{M}'_\delta}}{\det(M(\mathbb{M}'))}.$$

Taking as $\mathbb{M}'$ the set $\mathbb{M}^0$, it follows that

$$\left(\frac{\Delta^{\delta}_{\mathbb{M}_\delta}}{\det(M(\mathbb{M}))}\right)^2 = \left(\frac{\Delta^{\delta}_{\mathbb{M}^0_\delta}}{\det(M_0)}\right)^2 = \left(\frac{\Delta^{\rho}_{\mathbb{M}^0_\rho}\operatorname{Res}_{(d_1,\ldots,d_n)}(f_{1d_1},\ldots,f_{nd_n})^{\delta-\rho}}{\det(M_0)}\right)^2,$$

where the last equality holds for Lemma 6.3.

Now, the claim is an immediate consequence of identity (13) and Lemma 6.1. □

7. An overview of the Bézout construction of the resultant

In this section we will compare several results obtained by Bikker and Uteshev (1999) with ours. This will allow us to clarify the Bézout construction of the resultant.

In Bikker and Uteshev (1999, Section 4), the matrix M_0 defined at the beginning of Section 6 is introduced (it is denoted as V) and the structure of $\det(M_0)^2$ is studied. Following Macaulay (1902), it is stated that

$$\det(M_0)^2 = \Upsilon\mathcal{J},$$

where $\mathcal{J}$ is as defined in Section 6 of this paper. Furthermore, it is claimed that Υ is a rational function in the coefficients of the leading forms of the polynomials $f_1,\ldots,f_n$ whose numerator is a product of ρ polynomials in these coefficients.

In our notation, identity (13) and Lemma 6.1 imply that

$$\Upsilon = \pm\frac{(\Delta^{\rho}_{\mathbb{M}^0_\rho})^2}{\operatorname{Res}_{(d_1,\ldots,d_n)}(f_{1d_1},\ldots,f_{nd_n})^{\rho+1}}.$$

Moreover, the fact stated in Bikker and Uteshev (1999) about the factorization of the numerator of Υ is Theorem 5.2 of the present paper applied to $\mathbb{M}^0$ (see also Macaulay, 1902, Section 10). Finally, let us observe that the irreducible factors of the numerator and the denominator of Υ and of the polynomial $P_{\mathbb{M}^0,d_1,\ldots,d_n}$ defined in Theorem 4.1 are the same and, therefore, due to our main result we have that $\Upsilon \neq 0$ if and only if $\mathbb{M}^0$ is a basis of $\mathcal{A}$.

Also, the structure of $\det(M(\mathbb{M}^1))^2$ is studied in Bikker and Uteshev (1999, Theorem 5.1) in the bivariate case (see the definition of $\mathbb{M}^1$ in (6)). We point out a mistake in formula (5.30) of Bikker and Uteshev (1999), which is incorrect if the degrees of the input polynomials are different. This follows straightforwardly due to the fact that $\det(M(\mathbb{M}^1))^2$ has degree zero in the coefficients of $f_1,\ldots,f_n$, and if $n=2$, then $\mathcal{J}$ has degree $2d_1d_2$ in these coefficients and the kth classical subresultant has degree d_1+d_2-2k, $k=1,\ldots,\min(d_1,d_2)$. If $d_1 < d_2$, it turns out that the kth classical subresultant is the multivariate subresultant of $\mathbb{M}^1_{\rho-k+1}$ with respect to f_{1d_1}, f_{2d_2} if $1 \le k \le d_1 - 1$ (Chardin, 1995). It remains to compute the multivariate subresultant of $\mathbb{M}^1_t$ for those degrees t such that $d_1 \le t < d_2$. This is easily seen to be equal to $c^{t+1-d_1}_{1,(d_1,0)}$. Hence, we have the following

Proposition 7.1.

$$\Upsilon = \mathbf{c}\frac{(\mathcal{R}_1 \ldots \mathcal{R}_{d_1-1})^2 c_{1,(d_1,0)}^{(d_2-d_1)(d_2-d_1+1)}}{\mathrm{Res}_{(d_1,d_2)}(f_{1d_1}, f_{2d_2})^{\rho+1}},$$

where $\mathcal{R}_i$ is the classical i-subresultant and $\mathbf{c}$ *is the constant of Lemma* 6.1.

Concerning the reducibility problem (that is, given a family of polynomials $f_1, \ldots, f_n$ with respective degrees $d_1, \ldots, d_n$ and a set of monomials $\mathbb{M}$ with cardinality $\mathbf{d} = d_1 \ldots d_n$, decide whether every polynomial is a linear combination of $\mathbb{M}$ when reduced modulo the ideal $(f_1, \ldots, f_n)$), in Section 5 of Bikker and Uteshev (1999), a reduction algorithm with respect to $\mathbb{M}^0$ and $\mathbb{M}^1$ is presented by solving a succession of linear systems whose coefficients depend rationally on the leading forms of the input polynomials. One can easily check that the matrices of these linear systems can be regarded as subresultant matrices. Indeed, in Bikker and Uteshev (1999, Theorem 5.1), reduction modulo $\mathbb{M}^1$ is completely characterized in terms of the classical subresultants if $n = 2$.

In Bikker and Uteshev (1999, Theorem 5.2) it is claimed that, for three polynomials of equal degree d, it is sufficient for reducibility that $2d - 1$ determinants are non-zero. However, as a result of Theorem 5.2, we get that $2d - 2$ conditions suffice. This can be verified following the approach by Bikker and Uteshev (1999) in detail: it turns out that the linear systems they consider have determinants which are rational functions involving subresultants, and that the condition arising in the last system in their algorithm is redundant. Also, in Bikker and Uteshev (1999, Theorem 5.3) it is shown that the first d conditions of the $2d - 1$ needed in their reduction algorithm can be rewritten in terms of the nested minors of the Macaulay matrix of the initial forms of the polynomials. This follows straightforwardly in our framework, due to the structure of the Macaulay matrix given in (12) and the fact that, for $d \le t \le 2d - 1$, $\det(M_t) = D^t_{\mathbb{M}\cap\mathbb{K}[x_1,\ldots,x_n]_t}$, i.e., there are no extraneous factors (Macaulay, 1902).

Similar remarks can be made about the general approach they present in Bikker and Uteshev (1999, Section 5.3.).

Finally, we will answer negatively the Rank Conjecture posted in Bikker and Uteshev (1999, Section 4). Let $f_1, \ldots, f_n$ be polynomials such that $\mathbb{M}^0$ is a basis of $\mathcal{A}$. Let $g \in \mathbb{K}[x_1, \ldots, x_n]$, and let us denote with $\mathcal{B}$ the matrix of the following linear map in the basis $\mathbb{M}^0$:

$$\begin{array}{ccc} \mathcal{A} & \to & \mathcal{A} \\ p(x) & \mapsto & p(x)\, g(x). \end{array} \tag{17}$$

It is a well-known fact (see Cox et al., 1998; Bikker and Uteshev, 1999) that, if $V(g) \cap V(f_1, \ldots, f_n) = \emptyset$, then the determinant of $\mathcal{B}$ equals the dense resultant of the family $f_1, \ldots, f_n, g$ up to a constant. Suppose now that $V(g) \cap V(f_1, \ldots, f_n) = \{p_1, \ldots, p_s\}$, and for each $i = 1, \ldots, s$, we denote with l_i the minimum between the multiplicity of p_i as a zero of $V(f_1, \ldots, f_n)$ and the multiplicity of p_i as a zero of g. The Rank Conjecture asserts that the rank of $\mathcal{B}$ should be equal to $\mathbf{d} - \sum_{i=1}^{s} l_i$.

This conjecture is not true in general. For instance, we can take $f_1, \ldots, f_n$ homogeneous polynomials of respective degrees $d_1, \ldots, d_n$ such that the specialization of $P_{\mathbb{M}^0,d_1,\ldots,d_n}$ in the coefficients of this family is not identically zero. This implies that the only zero of the affine variety $V(f_1, \ldots, f_n)$ is the zero vector with multiplicity $\mathbf{d}$. Moreover, $\mathbb{M}^0$ is a basis of $\mathcal{A}$, which is a graded ring of finite dimension with $\mathcal{A}_t = 0$ for $t > \rho$. Let g be any homogeneous polynomial of degree d. According to the Rank Conjecture, the kernel of $\mathcal{B}$ should have dimension equal to $\min\{\mathbf{d}, d\}$, which is true if $d = 0$ or $d > \mathbf{d}$, but not in general. A straightforward computation shows that $\mathcal{A}_t \subset \ker(\mathcal{B})$ if $t > \rho - d$, so

$$\dim(\ker(\mathcal{B})) \geq \sum_{j=\rho-d+1}^{\rho} h_{(d_1,\ldots,d_n)}(j),$$

and this number may be greater than d. For instance, if $d = 2,\ d_i > 3$, we have that

$$h_{(d_1,\ldots,d_n)}(\rho - 1) + h_{(d_1,\ldots,d_n)}(\rho) = n + 1,$$

which is greater than 2 unless $n = 1$.

Acknowledgements

We are grateful to P. Bikker and A. Yu. Uteshev for providing us with updated versions of their joint work, to Laurent Busé for helpful comments on a preliminary version of this paper, and to the anonymous referees for their useful suggestions.

The first author was supported by the Miller Institute for Basic Research in Science, in the form of a Miller Research Fellowship (2002–2005). The second author was partially supported by CONICET, grant PIP 2461 (2000-2002), and Universidad de Buenos Aires, grant X198 (2001-2003).

References

Bézout, É., 1779. Théorie générale des équations algébriques. Ph.D. Pierres, Paris.

Bikker, P., Uteshev, A.Yu., 1999. On the Bézout construction of the resultant. J. Symbolic Comput. 28 (1–2), 45–88.

Chardin, M., 1994a. Formules à la Macaulay pour les sous-résultants en plusieurs variables. C. R. Acad. Sci. Paris Sér. I Math. 319 (5), 433–436.

Chardin, M., 1994b. Sur l'indépendance linéaire de certains monômes modulo des polynômes génériques. C. R. Acad. Sci. Paris Sér. I Math. 319 (10), 1033–1036.

Chardin, M., 1995. Multivariate subresultants. J. Pure Appl. Algebra 101 (2), 129–138.

Cox, D., Little, J., O'Shea, D., 1996. Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra. In: Undergraduate Texts in Mathematics. Springer, New York, NY, p. xiii.

Cox, D., Little, J., O'Shea, D., 1998. Using Algebraic Geometry. In: Graduate Texts in Mathematics, vol. 185. Springer-Verlag, New York.

Demazure, M., 1984. Une définition constructive du résultant. Notes Informelles de Calcul Formel 2, prépublication du Centre de Mathématiques de l'École Polytechnique.

Emiris, I.Z., Rege, A., 1994. Monomial bases and polynomial system solving. In: Proceedings of International Symposium on Symbolic and Algebraic Computation, Oxford. ACM, New York, pp. 114–122.

Gel'fand, I.M., Kapranov, M.M., Zelevinsky, A.V., 1994. Discriminants, resultants, and multidimensional determinants. In: Mathematics: Theory and Applications. Birkhäuser Boston, Inc., Boston, MA.

Jouanolou, J.P., 1980. Idéaux résultants. Adv. Math. 37 (3), 212–238.

Macaulay, F., 1902. Some formulae in elimination. Proc. London Math. Soc. 1 33, 3–27.

Macaulay, F., 1916. The Algebraic Theory of Modular Systems. Cambridge University Press.

Pedersen, P., Sturmfels, B., 1996. Mixed monomial bases. In: Algorithms in Algebraic Geometry and Applications. Santander, 1994. In: Progr. Math., vol. 143. Birkhäuser, Basel, pp. 307–316.
Szanto, A., 2005. Multivariate subresultants using Jouanolou's resultant matrices. J. Pure Appl. Algebra (in press) (preprint).
van der Waerden, B.L., 1950. Modern Algebra, 3rd edition. F. Ungar Publishing Co., New York.