Article Submitted to Journal of Symbolic Computation

Solving over-determined systems by the subresultant method

Agnes Szanto*[1] and
with an appendix by Marc Chardin[2]

[1] *Department of Mathematics,*
North Carolina State University, Raleigh, USA
aszanto@ncsu.edu

[2] *C.N.R.S. & Institut Mathématique de Jussieu Université Pierre et Marie Curie*
Paris, France
chardin@math.jussieu.fr

Abstract

A general *subresultant method* is introduced to compute elements of a given ideal with few terms and bounded coefficients. This subresultant method is applied to solve over-determined polynomial systems by either finding a triangular representation of the solution set or by reducing the problem to eigenvalue computation. One of the ingredients of the subresultant method is the computation of a matrix that satisfies certain requirements, called the *subresultant properties*. Our general framework allows to use matrices of significantly smaller size than previous methods. We prove that certain previously known matrix constructions, in particular, Macaulay's, Chardin's and Jouanolou's resultant and subresultant matrices possess the subresultant properties. However, these results rely on some assumptions on the regularity of the over-determined system to be solved. The appendix, written by Marc Chardin, contains relevant results on the regularity of n homogeneous forms in n variables.

1. Introduction

Let $f_1, \ldots, f_n \in \mathcal{C}[x_1, \ldots, x_n]$ be an over-constrained system of homogeneous polynomials of degree $d_1, \ldots, d_n$ respectively. A prevalent symbolic method to find the common roots of a multivariate polynomial system is based on Poisson

*Research supported in part by PIMS while a postdoctoral fellow at Simon Fraser University, in part by EPRSC while a postdoctoral fellow at University of Kent, Canterbury, and in part with the support of NSF grants CCR-0306406 and CCR-0347506.

type product formulae for the projective resultant (see for example Cox *et al.* (11, Chapter 3))

$$\mathrm{Res}(f_1,\ldots,f_n) = R' \prod_{\gamma\in V(f_2^A,\ldots,f_n^A)} f_1^A(\gamma), \tag{1}$$

where

$$f_i^A(x_1,\ldots,x_{n-1}) := f_i(x_1,\ldots,x_{n-1},1) \quad i=1,\ldots,n,$$

and the product is taken over the set of finite solutions of $f_2^A,\ldots,f_n^A$ in $\mathcal{C}^{n-1}$. The extraneous factor R' is a polynomial in the coefficients of the polynomials $f_2|_{x_n=0},\ldots,f_n|_{x_n=0}$, and vanishes if and only if $f_2,\ldots,f_n$ has a root at infinity, i.e. at $x_n = 0$. The motivation for the present investigation stems from the observation that, even in the univariate case, the expressions derived from (1) for the coordinates of the common roots are not optimal, as the following example illustrates:

Let us apply the product formula (1) to the univariate case. Let Res_d be the Sylvester resultant of the polynomials $f_i = c_{i0} + c_{i1}x + \cdots + c_{id}x^d \quad i = 1,2$. Assume that f_1 and f_2 have exactly one common root $\alpha \in \mathcal{C}$. (To simplify the notation we dehomogenized the polynomials and assumed that they have an affine common root.) Then (1) implies the following formula:

$$(1 : \alpha : \ldots : \alpha^d) \;=\; (\frac{\partial \mathrm{Res}_d}{\partial c_{10}}(f_1,f_2) : \ldots : \frac{\partial \mathrm{Res}_d}{\partial c_{1d}}(f_1,f_2)), \tag{2}$$

thus

$$\alpha = \frac{(\partial \mathrm{Res}_d/\partial c_{11})(f_1,f_2)}{(\partial \mathrm{Res}_d/\partial c_{10})(f_1,f_2)}. \tag{3}$$

Therefore, we expressed the unique common root as the ratio of two polynomials in the coefficients of the f_i's of degree $\deg(\mathrm{Res}_d) - 1$.

Alternatively, we can find α using the univariate subresultant method (see Collins (9) for reference). If f_1 and f_2 have exactly one common root α then it is the solution of the homogeneous linear system with coefficient matrix

$$S_1 := \begin{array}{c} \overbrace{\qquad\qquad\qquad}^{2d-1} \\ \left|\begin{array}{ccccc} c_{10} & \ldots & c_{1d} & & \\ & \ddots & & \ddots & \\ & & c_{10} & \ldots & c_{1d} \\ c_{20} & \ldots & c_{2d} & & \\ & \ddots & & \ddots & \\ & & c_{20} & \ldots & c_{2d} \end{array}\right| \begin{array}{l} \\ d-1 \\ \\ \\ d-1 \\ \end{array} \end{array},$$

where the rows correspond to the polynomials $x^j \cdot f_1$ and $x^j \cdot f_2$ for $0 \le j < d-1$.

Therefore, α is the ratio of two $(2d-2)\times(2d-2)$ non-singular minors of S_1. Thus, we expressed α as the ratio of two polynomials in the coefficients of the f_i's of degree $\deg(\mathrm{Res}_d)-2$. This shows that the expression in (3) is not optimal, the numerator and the denominator must contain superfluous components.

The primary concern of the present paper is to find efficient methods to compute multivariate generalizations of the univariate subresultants and to use the resulting subresultant matrices to solve over-constrained polynomial systems. González-Vega (19) gives a multivariate generalization of the univariate subresultant method using a non-homogeneous construction of Habicht (22). He defines subresultants as subdeterminants of the Macaulay matrix, and he constructs a geometric representation of the zero-dimensional solution set of a given polynomial system using subresultants. Chardin (7) introduces a more general version of the subresultant, defined as the determinant of a homogeneous part of the Koszul complex, or equivalently, as the ratio of two subdeterminants of the Macaulay matrix. Chardin (8) proves that his subresultant construction satisfies certain universal properties. Earlier, Lazard (29) gave a method related to the one in the present paper which reduces the solution of polynomial systems to linear algebra using Koszul complexes, without explicitly defining the subresultants. Recently, D'Andrea and Jeronimo (14) use subresultants to test whether a given set of monomials is a bases of the factor space of a well-defined polynomial system. Other recent works on subresultants include Busé and D'Andrea (4) proving that certain subresultants are irreducible and (3) using subresultants in the inverse parametrization problem of rational surfaces.

In the present paper we first describe a general framework for subresultant matrices and study the so called "subresultant property" with respect to a given ideal. We show how to compute certain simple elements in the given ideal by solving non-singular linear systems with coefficient matrices having the subresultant property. We also introduce the notion of "strong subresultant property" with respect to sets of polynomial systems. We prove that if a matrix has the strong subresultant property with respect to some set of polynomial systems, then for any given system in the set, the polynomials computed via the subresultant method generate the same affine ideal as the given system.

Next we demonstrate that the solution of the polynomials computed by the subresultant method is usually easier than the solution of the original system. We show how to derive a triangular representation of their solution or express the coordinates of the solutions as eigenvalues of multiplication matrices: all we need is to set up small matrices from the coefficients of the polynomials, and take determinants. In the case when the given over-constrained system has a unique common root we give a determinantal formula for the coordinates of the root. González-Vega (20) gave a similar determinantal formula to find the solution set of zero dimensional algebraic sets, using subdeterminants of the Macaulay ma-

trix. Our general framework allows us to use matrices, described in the second half of the paper, of significantly smaller size than that of González-Vega (19), which can improve the efficiency of the computations.

The second half of the paper is devoted to the description of subresultant matrix constructions. We investigate on a subresultant matrix construction based on the resultant matrices introduced by Jouanolou (27). The subresultant construction using Jouanolou's resultant matrices was originally introduced in (35), and we call these matrices Jouanolou's subresultant matrices. Jouanolou's subresultant matrices are generalizations of the matrix constructions of (19) and (8), which we call here Macaulay's subresultant matrices, in the sense that for each Macaulay subresultant matrix (corresponding to a degree ν) there is a family of Jouanolou's subresultant matrices satisfying the same "universal properties", and among them the Macaulay subresultant matrix has the largest size. Informally, the universal property that all the degree ν subresultant matrices satisfy is the following: for a system of $(f_1, \ldots, f_n) \in \mathcal{C}[x_1, \ldots, x_n]^n$ of homogenous polynomials of degrees $\mathbf{d} = (d_1, \ldots, d_n)$, the corresponding degree ν subresultant matrices have full rank if and only if $\dim_{\mathcal{C}} \mathcal{C}[x_1, \ldots, x_n]_\nu / \mathcal{I}_\nu = \mathcal{H}_{\mathbf{d}}(\nu)$, where $\mathcal{I}$ is the ideal generated by $f_1, \ldots, f_n$, $\mathcal{I}_\nu$ is the set of degree ν polynomials in $\mathcal{I}$, and $\mathcal{H}_{\mathbf{d}}$ is the Hilbert function of a complete intersection in $\mathcal{C}[x_1, \ldots, x_n]$ of degrees $\mathbf{d} = (d_1, \ldots, d_n)$.

The main result of this paper is that simple modifications of Jouanolou's degree ν subresultant matrices satisfy the strong subresultant properties with respect to sets of homogeneous polynomial systems satisfying the following properties: they do not have roots at infinity, the cardinality of the roots (counting multiplicities) is between $\mathcal{H}_{\mathbf{d}}(\nu)$ and ν, and the regularity of the Hilbert function of the system is at most ν.

The last section of the paper together with the appendix written by Marc Chardin, is devoted to a discussion on the above assumptions, listing results either cited from the literature or proved here allowing to identify whether the above assumptions are satisfied, and/or handling the cases when they don't. These are meant to justify that the assumptions above do not constrain the practical applicability of the subresultant method applied to Jouanolou's subresultant.

To summarize, the subresultant method using Jouanolou's subresultant matrices presented in this paper is a more efficient alternative to methods using resultant matrices to solve polynomial systems. Our general framework could also allow in the future to consider other subresultant matrix constructions to improve efficiency, for example possible subresultant matrix constructions for sparse polynomial systems. Some work has been done in this direction, see for example (6; 13; 28).

Acknowledgments: I would like to thank Liz Mansfield for her continued support and helpful suggestions. I would like to acknowledge the helpful discussions related to this paper that I had with Laurent Busé, Marc Chardin, Carlos D'Andrea, Teresa Krick, Bernard Mourrain, Olivier Ruatta, Michael Singer and Martin Sombra.

2. Notation

First we need some notational conventions:

NOTATION 2.1: We use the following notation throughout the paper:

1. Let $\mathbf{f} = (f_1, \ldots, f_n)$ be homogeneous polynomials in $\mathbf{x} = (x_1, \ldots, x_n)$ for $n \geq 2$ and with coefficients from an integral domain $\mathbf{R}$ such that $\mathcal{Z} \subset \mathbf{R}$. Let $\mathbf{K}$ be the fraction field of $\mathbf{R}$, and denote the algebraic closure of $\mathbf{K}$ by $\bar{\mathbf{K}}$. The ideal generated by $f_1, \ldots, f_n$ is denoted by $\langle f_1, \ldots, f_n \rangle$.
2. For $p \in \mathbf{K}[x_1, \ldots, x_n]$ we denote by
$$p^A(x_1, \ldots, x_{n-1}) := p(x_1, \ldots, x_{n-1}, 1)$$
the affinization of p. Similarly, for an set $S \subset \mathbf{K}[x_1, \ldots, x_n]$, S^A denotes the set of its affine elements. For an ideal $\mathcal{I} \subset \mathbf{K}[x_1, \ldots, x_n]$ generated by $f_1, \ldots, f_n$, $\mathcal{I}^A$ denotes the ideal generated by $f_1^A, \ldots, f_n^A$ in $\mathbf{K}[x_1, \ldots, x_{n-1}]$.
3. $\mathbf{x}^\alpha$ denotes the monomial $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$.
4. In our matrix notation, if M is a matrix of a linear map Φ then each row of M corresponds to an element of the basis of the domain of Φ and each column correspond to an element of the basis of the image space. (Note that this is the transpose of the usual notation.)
5. Let $\mathbf{K}$ be a field and V be a vector space over $\mathbf{K}$. We denote by $\mathbf{K}\langle v_1, \ldots, v_m \rangle$ the subspace of V spanned by the elements $v_1, \ldots, v_m \in V$.

3. The subresultant method

In this section we describe the *subresultant method* to compute elements in a given ideal with few terms and bounded coefficients using solutions of nonsingular linear systems. We present the method in a general framework and presume that a matrix satisfying certain conditions is precomputed. In the next section we apply the subresultant method to compute a rational representation of the solution of over-constrained polynomial systems. In later sections we investigate on various matrix constructions that suit the requirements described in this section.

The first definition gives the properties that a rectangular matrix has to satisfy in order to be used in the subresultant method, called "subresultant properties".

DEFINITION 3.1: *Let* $\mathbf{R}$ *and* $\mathbf{K}$ *be as above and let* $\mathcal{I} \subset \mathbf{K}[x_1, \ldots, x_n]$ *be an ideal. Let* $l, m, r \in \mathbb{N}_+$ *such that*

$$1 < l \leq m \quad \text{and} \quad m - l < r. \tag{4}$$

Let $M \in \mathbf{R}^{r \times m}$ *be a matrix and let* $\mathbf{p} = (p_1, \ldots, p_l)$ *be a vector of polynomials in* $\mathbf{R}[x_1, \ldots, x_n]$. *We say that the pair* $(M, \mathbf{p})$ *has the* **subresultant property** *with respect to* $\mathcal{I}$ *if it satisfies the following conditions:*

(1) There exist $a_{l+1}, \ldots, a_m \in \mathbf{K}$ *such that for all* $i = 1, \ldots, r$

$$\sum_{j=1}^{l} M_{i,j} p_j + \sum_{j=l+1}^{m} M_{i,j} a_j \ \in \ \mathcal{I}, \tag{5}$$

where $M_{i,j}$ *is the* (i,j)*-th entry of* M.

(2) There exists $T \subset \{1, \ldots, m\}$ *with* $|T| = r$ *and* $\{l+1, \ldots, m\} \subset T$ *with the following properties:*

(a) the square submatrix of M *with columns corresponding to* T *is non-singular,*

(b) for each $i \notin T$ *and* $j = 1, \ldots, n-1$ *we have*

$$x_j p_i^A \in \mathbf{K}\langle p_1^A, \ldots p_l^A \rangle,$$

(c) $p_1^A, \ldots, p_l^A$ *generate* $\mathbf{K}[x_1, \ldots, x_{n-1}]$ *as an ideal.*

REMARK 3.2: Condition (1) of Definition 3.1 is trivially satisfied for pairs $(M, \mathbf{p})$ when $m = l$ and the entries of the vector $M \cdot \mathbf{p}$ are in the ideal $\mathcal{I}$. For example, the Macaulay subresultant matrix, together with the vector of monomials corresponding to its column, satisfies this weaker condition. On the other hand, the Jouanolou subresultant matrix only satisfies condition (1) above.
The second condition ensures that the ideal elements in (5) generate a sufficiently large ideal. Parts (b) and (c) of condition (2) is satisfied for example if for some $k \geq 0$ $\mathrm{Mon}_{n-1}(k) \subset \{p_1^A, \ldots, p_l^A\}$ and either $\{p_i^A \mid i \notin T\} \subset \mathrm{Mon}_{n-1}(k-1)$ or $\#\{p_i^A \mid i \notin T\} = m - r \leq k$. Here $\mathrm{Mon}_{n-1}(k)$ denotes the set of monomials of degrees at most k in $x_1, \ldots, x_{n-1}$.

In the next proposition we give an upper bound for $\dim \mathbf{K}[x_1, \ldots, x_{n-1}]/\mathcal{I}^A$ in terms of the corank of a matrix with the subresultant property with respect to $\mathcal{I}$.

PROPOSITION 3.3: *Let* $\mathbf{R}$ *and* $\mathbf{K}$ *as above and let* $\mathcal{I} \subset \mathbf{K}[x_1, \ldots, x_n]$ *be an ideal. Let* $l, m, r \in \mathbb{N}_+$, $M \in \mathbf{R}^{r \times m}$ *and* $\mathbf{p} = (p_1, \ldots, p_l) \in \mathbf{R}[x_1, \ldots, x_n]^l$ *be as in Definition 3.1, and assume that* $(M, \mathbf{p})$ *has the subresultant property w.r.t.* $\mathcal{I}$. *Then* $\mathcal{I}^A$ *is a zero dimensional ideal and*

$$\dim_{\mathbf{K}} \mathbf{K}[x_1, \ldots, x_{n-1}]/\mathcal{I}^A \leq m - r.$$

Proof: By (35, Lemma 3.2.5) we have that condition (1) of the subresultant property implies that for any $S \subset \{1,\ldots,m\}$ such that $|S| = r-1$ and $\{l+1,\ldots,m\} \subset S$ we have

$$\sum_{j\notin S} (-1)^{\sigma(j,S)}\, \mathcal{D}_{S\cup\{j\}}\, p_j \;\in\; \mathcal{I}, \tag{6}$$

where $\mathcal{D}_X$ denotes the determinant of the submatrix of M corresponding to the columns indexed by X, and $\sigma(j,S)$ denotes the ordinal number of j in the ordered set $S\cup\{j\}$. Let $T \subset \{1,\ldots,m\}$, $|T| = r$ as in condition (2) of the subresultant property, and let $\overline{T} \subset \{1,\ldots,l\}$ be its complement, which has cardinality $m-r$. Then $\mathcal{D}_T \neq 0$ by assumption, and by (6) we have that

$$\mathcal{D}_T p_i + \sum_{j\in\overline{T}} \pm \mathcal{D}_{T\cup\{j\}-\{i\}} p_j \;\in\; \mathcal{I} \quad \forall\, i \in \{1,\ldots,l\}\cap T. \tag{7}$$

After dividing the elements on the left hand side of (7) by $\mathcal{D}_T$ we get that $p_1,\ldots,p_l$ is generated by $B := \{p_j : j\in\overline{T}\}$ modulo $\mathcal{I}$ as a vector space over $\mathbf{K}$. This implies that $p_1^A,\ldots,p_l^A$ is generated by $B^A = \{p_j^A : j\in\overline{T}\}$ modulo $\mathcal{I}^A$ as a vector space over $\mathbf{K}$. To prove that $\mathbf{K}[x_1,\ldots,x_{n-1}]$ is generated by B^A modulo $\mathcal{I}^A$ as a vector space over $\mathbf{K}$, let $f\in\mathbf{K}[x_1,\ldots,x_{n-1}]$. Then by condition (2)(c) in Definition 3.1 and by the above argument we can write

$$f = \sum_{i=1}^{l} f_i p_i^A \equiv \sum_{j\in\overline{T}} g_j p_j^A \mod \mathcal{I}^A$$

for some $f_i, g_j \in \mathbf{K}[x_1,\ldots,x_{n-1}]$. If $\max_{j\in\overline{T}}(\deg_{\mathbf{x}}(g_j)) > 0$ then by condition (2)(b) of Definition 3.1 we can write

$$\sum_{j\in\overline{T}} g_j p_j^A = \sum_{i=1}^{n-1}\sum_{j\in\overline{T}} h_{ij} x_i p_j^A + \sum_{j\in\overline{T}} h_j p_j^A \equiv \sum_{j\in\overline{T}} \tilde{g}_j p_j^A \mod \mathcal{I}^A$$

where $\max_{j\in\overline{T}}(\deg_{\mathbf{x}}(\tilde{g}_j))$ is strictly smaller than $\max_{j\in\overline{T}}(\deg_{\mathbf{x}}(g_j))$. Therefore, using induction on $\max_{j\in\overline{T}}(\deg_{\mathbf{x}}(g_j))$, we can write

$$f \equiv \sum_{j\in\overline{T}} g_j p_j^A \mod \mathcal{I}^A$$

where $g_j \in \mathbf{K}$ for all $j\in\overline{T}$. This implies that

$$\dim \mathbf{K}[x_1,\ldots,x_{n-1}]/\mathcal{I}^A \leq m-r$$

as claimed. □

In the following definition we define the "subresultant method".

DEFINITION 3.4: *Let* $\mathbf{R}$ *and* $\mathbf{K}$ *be as above and assume that the ideal* $\mathcal{I} \subset \mathbf{K}[x_1, \ldots, x_n]$ *is given by a finite set* $F \subset \mathbf{R}[x_1, \ldots, x_n]$ *of generators as input. We call* **subresultant method** *the computation of the following objects:*

i. A matrix $M \in \mathbf{R}^{r \times m}$ *and a vector* $\mathbf{p} = (p_1, \ldots, p_l) \in \mathbf{K}[x_1, \ldots, x_n]^l$ *as in Definition 3.1 such that* $(M, \mathbf{p})$ *has the subresultant property for* $\mathcal{I}$*.*

ii. $T \subset \{1, \ldots, m\}$*,* $|T| = r$*,* $\{l+1, \ldots, m\} \subset T$ *such that* $\mathcal{D}_T \neq 0$*, where* $\mathcal{D}_T$ *denotes the determinant of the submatrix of* M *with columns corresponding to* T*.*

iii. The set of polynomials

$$\mathcal{S}(M, \mathbf{p}) := \{\mathbf{z}_i \cdot \mathbf{p} \mid i \in T \cap \{1, \ldots, l\}\} \tag{8}$$

where $\mathbf{z}_i = (z_{i1}, \ldots, z_{il}) \in \mathbf{K}^l$ *for* $i \in T \cap \{1, \ldots, l\}$ *are defined by*

$$z_{ij} = \begin{cases} -\delta_{i,j} & \text{if } j \in T \cap \{1, \ldots, l\} \\ (-1)^{\sigma(j, T-\{i\})} \frac{\mathcal{D}_{T-\{i\}\cup\{j\}}}{\mathcal{D}_T} & \text{if } j \notin T, \end{cases} \tag{9}$$

where $\sigma(j, T - \{i\})$ *denotes the ordinal number of* j *in the ordered set* $T \cup \{j\} \setminus \{i\}$*. Note that by the proof of Proposition 3.3 we have* $\mathcal{S}(M, \mathbf{p}) \subset \mathcal{I}$*.*

In the next proposition we relate the coefficients of the polynomials in $\mathcal{S}(M, \mathbf{p})$ defined in (9) to the dual of the column-nullspace of M. Since the parametric equations of the nullspace of a full rank matrix can be computed by the solution of non-singular linear systems, this observation allows to compute the set $\mathcal{S}(M, \mathbf{p})$ in the subresultant method using basic numerical linear algebra tools. The proof of the proposition is straightforward linear algebra, and we leave it to the reader. Before stating the proposition, we introduce the following notation:

NOTATION 3.5: Let $\mathbf{K}$ be a field and $M \in \mathbf{K}^{r \times m}$ be a matrix. The *column-nullspace* of M is defined as the subspace

$$\mathrm{cnull}(M) := \{\mathbf{w} \in \mathbf{K}^m \mid M \cdot \mathbf{w} = 0\} \tag{10}$$

and its dual is defined as

$$\mathrm{cnull}^{\perp}(M) := \{\mathbf{z} \in (\mathbf{K}^m)^* \mid \mathbf{z}(\mathrm{cnull}(M)) = 0\}. \tag{11}$$

Note that if $\mathrm{rank}(M) = r$ then $\dim(\mathrm{cnull}(M)) = m - r$ and $\dim(\mathrm{cnull}^{\perp}(M)) = r$.

PROPOSITION 3.6: *Let* M *be an* $s \times m$ *matrix with entries from a field* $\mathbf{K}$*. Let* $r := \mathrm{rank}(M)$*. Fix* $T \subset \{1, \ldots, m\}$ *such that* $|T| = r$ *and the columns of* M *corresponding to* T *are linearly independent. Then the set of vectors* $\{\mathbf{z}_i = (z_{i1}, \ldots, z_{im}) \mid 1 \leq i \leq r\}$ *defined as*

$$z_{ij} = \begin{cases} -\delta_{i,j} & \text{if } j \in T \\ (-1)^{\sigma(j, T-\{i\})} \frac{\mathcal{D}_{T-\{i\}\cup\{j\}}}{\mathcal{D}_T} & \text{if } j \notin T \end{cases}.$$

forms a basis for $\mathrm{cnull}^{\perp}(M)$. *Here* $\mathcal{D}_X$ *denotes the minor corresponding to the columns of* M *indexed by* X *for any set* $X \subset \{1,\ldots,m\}$ *with* $|X| = r$ *and* **any** *fixed* r *rows of* M *such that* $\mathcal{D}_T \neq 0$. *As above,* $\sigma(j, T - \{i\})$ *denotes the ordinal number of* j *in the ordered set* $T \cup \{j\} \setminus \{j\}$. *Moreover, once we fix the columns* T *as above, the values of* $\frac{\mathcal{D}_{T-\{i\}\cup\{j\}}}{\mathcal{D}_T}$ *(*$i \in T$, $j \notin T$*) do not depend on the choice of rows as long as* $\mathcal{D}_T \neq 0$. ■

Example 3.7: Let $n = 3$, $d = (3,3,2)$ and $\mathbf{f} = (f_1, f_2, f_3)$ be the following generic polynomial system in $\mathbf{x} := (x, y, z)$

$$\begin{aligned} f_1 &= a_0x^3 + a_1x^2y + a_2x^2z + a_3xy^2 + a_4xyz + a_5xz^2 + a_6y^3 + a_7y^2z + a_8yz^2 + a_9z^3 \\ f_2 &= b_0x^3 + b_1x^2y + b_2x^2z + b_3xy^2 + b_4xyz + b_5xz^2 + b_6y^3 + b_7y^2z + b_8yz^2 + b_9z^3 \\ f_3 &= c_0x^2 + c_1xy + c_2xz + c_3y^2 + c_4yz + c_5z^2. \end{aligned} \tag{12}$$

Define M to be the following 8×11 matrix (which is the Jouanolou subresultant matrix of $\mathbf{f}$ with $\eta = 2$ and $\nu = 4$, see later sections):

$$\begin{bmatrix} \mu_{u^2,x^3} & \mu_{u^2,x^2y} & \mu_{u^2,x^2z} & \mu_{u^2,xy^2} & \mu_{u^2,xyz} & \mu_{u^2,xz^2} & \mu_{u^2,y^3} & \mu_{u^2,y^2z} & \mu_{u^2,yz^2} & \mu_{u^2,z^3} & c_0 \\ \mu_{vu,x^3} & \mu_{vu,x^2y} & \mu_{vu,x^2z} & \mu_{vu,xy^2} & \mu_{vu,xyz} & \mu_{vu,xz^2} & \mu_{vu,y^3} & \mu_{vu,y^2z} & \mu_{vu,yz^2} & \mu_{vu,z^3} & c_1 \\ \mu_{v^2,x^3} & \mu_{v^2,x^2y} & \mu_{v^2,x^2z} & \mu_{v^2,xy^2} & \mu_{v^2,xyz} & \mu_{v^2,xz^2} & \mu_{v^2,y^3} & \mu_{v^2,y^2z} & \mu_{v^2,yz^2} & \mu_{v^2,z^3} & c_3 \\ a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & a_9 & 0 \\ c_0 & c_1 & c_2 & c_3 & c_4 & c_5 & 0 & 0 & 0 & 0 & 0 \\ b_0 & b_1 & b_2 & b_3 & b_4 & b_5 & b_6 & b_7 & b_8 & b_9 & 0 \\ 0 & c_0 & 0 & c_1 & c_2 & 0 & c_3 & c_4 & c_5 & 0 & 0 \\ 0 & 0 & c_0 & 0 & c_1 & c_2 & 0 & c_3 & c_4 & c_5 & 0 \end{bmatrix}$$

where $\mu_{\mathbf{u}^\beta,\mathbf{x}^\alpha}$ are coefficients of the "Morley forms" (see (27)) and are multilinear forms in the coefficients of f_1, f_2, f_3, for example

$$\mu_{uv,x^2y} = -a_1c_1b_5 + a_3c_0b_5 - a_0c_3b_5 + a_5b_1c_1 + a_5b_0c_3 - a_3b_0c_5 - a_5c_0b_3 + a_0b_3c_5.$$

Let $\mathbf{p}$ be the following vector of 10 polynomials of degree $\nu = 3$:

$$\mathbf{p} = \begin{pmatrix} x^3 & yx^2 & zx^2 & y^2x & zyx & z^2x & y^3 & y^2z & z^2y & z^3 \end{pmatrix}.$$

Define for $i = 1,\ldots,7$ and $j = 8,9,10$

$$d_{i,j} = (-1)^{j-1}\frac{\mathcal{D}_{\{1,\ldots,\hat{i},\ldots,7,11\}\cup\{j\}}}{\mathcal{D}_{\{1,\ldots,7,11\}}}$$

where $\mathcal{D}_X$ denotes the subdeterminant of M with columns indexed by the set $X \subset \{1,\ldots,11\}$, for $|X| = 8$. Note that $d_{i,j}$ are well defined in $\mathbf{K}$ since $\mathcal{D}_{\{1,\ldots,7,11\}} \neq 0$. Take the elements $\mathbf{z}_i = (z_{i1},\ldots,z_{i10})$ for $i = 1\ldots7$ defined as follows:

$$z_{ij} = \begin{cases} -\delta_{i,j} & \text{if } 1 \le i \le 7 \\ d_{i,j} & \text{if } j = 8,9,10 \end{cases}$$

where $\delta_{i,j}$ denotes the Kronecker symbol. Then, by definition, the following 7 polynomials will form the set $\mathcal{S}(M,\mathbf{p})$:

$$\begin{aligned} &\mathbf{z}_1\cdot\mathbf{p} = -x^3 + d_{1,8}y^2z + d_{1,9}z^2y + d_{1,10}z^3, && \mathbf{z}_2\cdot\mathbf{p} = -yx^2 + d_{2,8}y^2z + d_{2,9}z^2y + d_{2,10}z^3, \\ &\mathbf{z}_3\cdot\mathbf{p} = -zx^2 + d_{3,8}y^2z + d_{3,9}z^2y + d_{3,10}z^3, && \mathbf{z}_4\cdot\mathbf{p} = -y^2x + d_{4,8}y^2z + d_{4,9}z^2y + d_{4,10}z^3, \\ &\mathbf{z}_5\cdot\mathbf{p} = -zyx + d_{5,8}y^2z + d_{5,9}z^2y + d_{5,10}z^3, && \mathbf{z}_6\cdot\mathbf{p} = -z^2x + d_{6,8}y^2z + d_{6,9}z^2y + d_{6,10}z^3, \\ &\mathbf{z}_7\cdot\mathbf{p} = -y^3 + d_{7,8}y^2z + d_{7,9}z^2y + d_{7,10}z^3. \end{aligned} \tag{13}$$

As we shall see in the proof of Proposition 5.6, the pair $(M,\mathbf{p})$ satisfies the subresultant property, thus $\mathcal{S}(M,\mathbf{p}) \subset \mathcal{I} = \langle f_1, f_2, f_3\rangle$.

As we shall see in the next section, in many cases the computation of the common roots of the system $\mathcal{S}(M, \mathbf{p})$ is much easier than the solution of the original input system $F \subset \mathbf{R}[x_1, \ldots, x_n]$. As we noted earlier, the subresultant property implies that

$$\mathcal{S}(M, \mathbf{p}) \subset \mathcal{I}.$$

In the following proposition we prove that if the dimension of the factor algebra of $\mathcal{I}^A$ equals the corank of M then

$$\mathcal{S}(M, \mathbf{p})^A = \mathcal{I}^A. \tag{14}$$

PROPOSITION 3.8: *Let* $\mathbf{R}$, $\mathbf{K}$, $\mathcal{I}$, $\mathbf{p}$, *and* $M \in \mathbf{R}^{r \times m}$ *be as in Definition 3.1, and assume that* $(M, \mathbf{p})$ *has the subresultant property with respect to* $\mathcal{I}$. *Let* $\mathcal{S}(M, \mathbf{p})$ *be the set defined in Definition 3.4. Then*

$$\dim_{\mathbf{K}} \mathbf{K}[x_1, \ldots, x_{n-1}]/\mathcal{I}^A = m - r \tag{15}$$

implies that

$$\mathcal{I}^A = \mathcal{S}(M, \mathbf{p})^A.$$

Proof: Since $(M, \mathbf{p})$ has the subresultant property w.r.t. $\mathcal{I}$ we have $\mathcal{S}(M, \mathbf{p}) \subset \mathcal{I}$. This also implies that $\mathcal{S}(M, \mathbf{p})^A \subset \mathcal{I}^A$. Denote by J^A the ideal generated by $\mathcal{S}(M, \mathbf{p})^A$ in $\mathbf{K}[x_1, \ldots, x_{n-1}]$. It is sufficient to prove that

$$\dim \mathbf{K}[x_1, \ldots, x_{n-1}]/J^A \leq m - r.$$

Let $T \subset \{1, \ldots, m\}$, $|T| = r$ be such that the columns of M indexed by T form a non-singular matrix. Let $B^A := \{p_i^A \mid i \in \overline{T}\}$, where $\overline{T}$ is the complement of T and has cardinality $|\overline{T}| = m - r$. By the definition of $\mathbf{z}_i$ for $i \in T \cap \{1, \ldots, l\}$ in (9) we have that the equivalence classes of the elements in B^A generate the factor space

$$\frac{\mathbf{K}\langle p_1^A, \ldots, p_l^A \rangle}{\mathbf{K}\langle \mathbf{z}_i \cdot \mathbf{p}^A \mid i \in T \cap \{1, \ldots, l\} \rangle}.$$

Using the same argument as is the proof of Proposition 3.3 we can see that B^A also generates $\mathbf{K}[x_1, \ldots, x_{n-1}]/\mathcal{J}^A$ as a vector space over $\mathbf{K}$. This implies that

$$\dim \mathbf{K}[x_1, \ldots, x_{n-1}]/\mathcal{J}^A \leq m - r$$

as claimed. Note that by (15) we have that B^A forms a basis for $\mathbf{K}[x_1, \ldots x_{n-1}]/\mathcal{I}^A$. □

We finish this section by defining properties of "generic" matrices, i.e. matrices with parametric entries, such that they can be used to compute the solutions of families of specific polynomial systems via the subresultant method. Informally, we call a generic matrix a "strong subresultant matrix" with respect to a set of polynomial systems if for any given system in the set, the polynomials computed

via the subresultant method generate the same affine ideal as the given system. In the second part of the paper we study particular matrix constructions and prove that they are strong subresultant matrices with respect to certain sets of polynomial systems.

First we need the notion of "generic" and "specified" polynomial systems as well as a notion of "affine k-sets".

DEFINITION 3.9: *(i) Let*

$$f_1 = \sum_{|\alpha|=d_1} \mathcal{C}^{\bullet}_{\mathfrak{m}1,\alpha}\mathbf{x}^{\alpha}, \ldots, f_n = \sum_{|\alpha|=d_n} \mathcal{C}^{\bullet}_{\mathfrak{m}n,\alpha}\mathbf{x}^{\alpha} \in \mathbf{R}[x_1,\ldots,x_n]$$

be homogeneous polynomials with parametric coefficients $\mathcal{C}^{\bullet}_{\mathfrak{m}i,\alpha}$ where we assume that $\mathbf{R}$ is an integral domain containing $\mathcal{Z}[\mathcal{C}^{\bullet}_{\mathfrak{m}i,\alpha}]$. Then $\mathbf{f} = (f_1,\ldots,f_n)$ is called a **generic system of degrees** *$(d_1,\ldots,d_n)$.*

(ii) A **coefficient specialization** *is a ring homomorphism $\phi : \mathcal{Z}[\mathcal{C}^{\bullet}_{\mathfrak{m}i,\alpha}] \to \mathbf{k}$ for some field $\mathbf{k}$, sending each coefficient $\mathcal{C}^{\bullet}_{\mathfrak{m}i,\alpha}$ into its value. We usually denote the specialization of a generic system $\mathbf{f}$ by $\tilde{\mathbf{f}} = (\tilde{f}_1,\ldots,\tilde{f}_n)$ and by $\tilde{\mathcal{I}}$ the ideal generated by $\tilde{f}_1,\ldots,\tilde{f}_n$ in $\mathbf{k}[x_1,\ldots,x_n]$.*

(iii) Let $\mathbf{f}$ be a generic system of degrees $(d_1,\ldots,d_n)$ and let $k \geq 0$. We say that a set $\mathcal{F} \subset \mathbf{k}[\mathbf{x}]^n$ of coefficient specializations of $\mathbf{f}$ is an **affine k-set**, *if for all $\tilde{\mathbf{f}} = (\tilde{f}_1,\ldots,\tilde{f}_n) \in \mathcal{F}$,*

$$\dim_{\mathbf{k}} \mathbf{k}[x_1,\ldots,x_{n-1}]/\tilde{\mathcal{I}}^A = k,$$

where $\tilde{\mathcal{I}}^A$ is the ideal generated by $\tilde{f}_1^A,\ldots,\tilde{f}_n^A$.

Next we define the "strong subresultant property".

DEFINITION 3.10: *Let $\mathbf{R}$ be as in Definition 3.9 and let $\mathbf{K}$ be the fraction field of $\mathbf{R}$. Let $\mathbf{f} = (f_1,\ldots,f_n)$ be a generic system with degrees $(d_1,\ldots,d_n)$ in $\mathbf{R}[x_1,\ldots,x_n]$. For some $k,l,t,u \in \mathbb{N}$ let $M \in \mathbf{R}^{t\times u}$ be a matrix, $\mathbf{p} = (p_1,\ldots,p_l) \in \mathbf{R}[x_1,\ldots,x_n]^l$ be a list of polynomials, and let $\mathcal{F} \subset \mathbf{k}[x_1,\ldots,x_n]^n$ be an affine k-set of coefficients specializations of $\mathbf{f}$.*

*We say that the pair $(M,\mathbf{p})$ has the k–***strong subresultant property** *with respect to $\mathcal{F}$ if for all $\tilde{\mathbf{f}} \in \mathcal{F}$ there exists a submatrix $\tilde{M}'$ of $\tilde{M}$ of size $r \times m$ such that $r = m-k$ and $(\tilde{M}',\tilde{\mathbf{p}})$ has the subresultant property w.r.t. $\tilde{\mathcal{I}}$. Here $\tilde{\mathcal{I}}$ is the ideal generated by $\tilde{\mathbf{f}}$, and $\tilde{M} \in \mathbf{k}^{t\times u}$ and $\tilde{\mathbf{p}} \in \mathbf{k}[x_1,\ldots,x_n]^l$ denotes the coefficient specializations of M and $\mathbf{p}$ corresponding to $\tilde{\mathbf{f}}$, respectively.*

As a consequence of Propositions 3.3 and 3.8 we get the following corollary.

COROLLARY 3.11: *Let $\mathbf{f}$, M, $\mathbf{p}$ be as in Definition 3.10, and assume that $(M,\mathbf{p})$ has the k-strong subresultant property w.r.t. some affine k-set $\mathcal{F} \subset \mathbf{k}[x_1,\ldots,x_n]^n$ for some $k \geq 0$. For $\tilde{\mathbf{f}} \in \mathcal{F}$ let $(\tilde{M}',\tilde{\mathbf{p}})$ be the pair with the subresultant property that satisfies the conditions of Definition 3.10. Let $\tilde{\mathcal{J}}$ be the ideal generated by $\mathcal{S}(\tilde{M}',\tilde{\mathbf{p}})$ defined in Definition 3.4. Then*

$$\tilde{\mathcal{J}}^A = \tilde{\mathcal{I}}^A.$$

4. Solution of polynomial systems

In this section we follow an approach similar to the one in (20) and translate the subresultant method in Definition 3.4 into a tool for solving polynomial systems. We give a triangular representation of the common roots of $\mathcal{S}(M, \mathbf{p})$ defined in (8) in the case when the polynomials in $\mathbf{p} = (p_1, \ldots, p_l)$ satisfy certain conditions. We also give a method to compute the matrices of the multiplication maps of the coordinate functions. These matrices has the coordinates of the common roots as eigenvalues. The techniques described in this section are very simple, only using matrix multiplication and determinant computation on small matrices. In order to motivate the hypotheses and the construction, we first describe the method and the proof of correctness, and then we summarize the results in a proposition.

Let $\mathbf{p}^A = (p_1^A, \ldots, p_l^A)$ be a vector of polynomials in $\mathbf{k}[x_1, \ldots, x_n]$, and assume that the first k polynomials $p_1^A, \ldots p_k^A$ are linearly independent over $\mathbf{k}$ for some $k > 0$. Let $\mathbf{z}_i = (z_{i,1}, \ldots, z_{i,l}) \in \mathbf{k}^l$ $(i = 1, \ldots, l-k)$ be any vectors such that

$$z_{i,j} = \delta_{i,j-k} \quad \text{if } j = k+1, \ldots l, \tag{16}$$

where $\delta_{i,j-k}$ is the Kronecker delta. Then the equivalence classes of $[p_1^A], \ldots, [p_k^A]$ form a basis for the vector space

$$V := \frac{\mathbf{k}\langle p_1^A, \ldots, p_l^A \rangle}{\mathbf{k}\langle \mathbf{z}_1 \cdot \mathbf{p}^A, \ldots, \mathbf{z}_{l-k} \cdot \mathbf{p}^A \rangle}. \tag{17}$$

Let $q^A \in \mathbf{k}(x_1, \ldots, x_{n-1})$ be any rational function such that

$$q^A p_i^A \in \mathbf{k}\langle p_1^A, \ldots, p_l^A \rangle \quad i = 1, \ldots, k.$$

Define the linear transformation

$$\mu_{q^A} : V \to V, \quad [p_j^A] \mapsto [q^A p_j^A] \;\; j = 1, \ldots, k. \tag{18}$$

Then it is easy to see that the values $q^A(\xi_1), \ldots, q^A(\xi_k) \in \bar{\mathbf{k}}$ are eigenvalues of μ_{q^A}, where $\xi_1, \ldots, \xi_k$ are the common roots of the polynomials $\mathbf{z}_1 \cdot \mathbf{p}^A, \ldots, \mathbf{z}_{l-k} \cdot \mathbf{p}^A$. Moreover, if $q^A(\xi_1), \ldots, q^A(\xi_k)$ are all distinct, then they provide all eigenvalues of μ_{q^A} and the eigenvector corresponding to $q^A(\xi_j)$ is $\mathbf{v}(\xi_j) := (p_1^A(\xi_j), \ldots, p_k^A(\xi_j))$ for $j = 1, \ldots, k$, which are independent of q^A. Here the coordinates are taken with respect to the basis $\{[p_1^A], \ldots, [p_k^A]\}$ of V. Note also that if the values $q^A(\xi_1), \ldots, q^A(\xi_k)$ are not all distinct, i.e. $q^A(\xi_i)$ has multiplicity m_i (the roots are also counted with multiplicity), then $q^A(\xi_i)$ is an eigenvalue of μ_{q^A} with multiplicity m_i, and the generalized eigenspace corresponding to $q^A(\xi_i)$ is independent of q^A (see Cox *et al.* (11, Chapter 4)).

In the next corollary we state sufficient conditions on $\mathbf{p}$ so that we can easily compute the matrices of the multiplication maps μ_{x_i} for $i = 1, \ldots, n-1$. Computing the eigenvalues of these matrices simultaneously gives an algorithm to

find the common roots of $\mathbf{z}_1 \cdot \mathbf{p}^A, \ldots, \mathbf{z}_{l-k} \cdot \mathbf{p}^A$, together with their multiplicity. Many other authors give methods to compute the matrices of the multiplication maps (see for example (1; 36; 32; 10; 30; 33; 34; 24; 21; 17; 2)), here we show how to compute them from subresultant matrices.

COROLLARY 4.1: *Let* $\mathbf{p}^A = (p_1^A, \ldots, p_l^A) \in \mathbf{k}[x_1, \ldots, x_{n-1}]^l$ *be a vector of polynomials and let* $0 \leq k \leq l$. *For* $1 \leq i \leq l-k$ *let* $\mathbf{z}_i = (z_{i,1}, \ldots, z_{i,l}) \in \mathbf{k}^m$ *be vectors as in (16), and let* V *be defined as in (17). Assume that for all* $i = 1, \ldots, n-1$ *and* $j = 1, \ldots, k$ *there exist* $a_{j,t}^{(i)} \in \mathbf{k}$ $(1 \leq t \leq l)$ *such that*

$$x_i \cdot p_j^A = \sum_{t=1}^{l} a_{j,t}^{(i)} \, p_t^A. \tag{19}$$

Define the following matrices for $1 \leq i \leq n-1$*:*

$$A_i := \left(a_{j,t}^{(i)}\right)_{1,1}^{k,k} \quad B_i := \left(a_{j,t}^{(i)}\right)_{1,k+1}^{k,l} \qquad C := \left(z_{u,v}\right)_{1,1}^{l-k,k}.$$

Then the $k \times k$ *matrix* $A_i + B_i \cdot C$ *is the transformation matrix between the basis* $\{[p_1^A], \ldots, [p_k^A]\} \subset V$ *and the set* $\{[x_i p_1^A], \ldots, [x_i p_k^A]\} \subset V$*, thus it is the matrix of* μ_{x_i} *defined in (18).* ■

Another method to compute the coordinates of the common roots of $\mathbf{z}_1 \cdot \mathbf{p}^A, \ldots, \mathbf{z}_{l-k} \cdot \mathbf{p}^A$ is to find a triangular representation for them. To this end we first express the first coordinates of the common roots as the roots of the characteristic polynomial of the map μ_{x_1}. Then we also give expressions for the other coordinates of the common roots in terms of the first coordinates. We need the following assumption:

> The first coordinates of the common roots of $(\mathbf{z}_1 \cdot \mathbf{p}^A, \ldots, \mathbf{z}_{l-k} \cdot \mathbf{p}^A)$ are k distinct elements of $\bar{\mathbf{k}}$.

Note that the case when $(\mathbf{z}_1 \cdot \mathbf{p}^A, \ldots, \mathbf{z}_{l-k} \cdot \mathbf{p}^A)$ has k distinct common roots but the first coordinates are not distinct can be treated by a generic coordinate transformation. As we mentioned above, even if some of the first coordinates of the common roots have higher multiplicity, the eigenvalues of μ_{x_1} will have the same multiplicity. However, to compute the other coordinates of the common roots in terms of the first one is more complicated in this case, and we will not consider it here. For a method to handle this case without coordinate transformation see Díaz-Toca and González-Vega (15).

First of all, using the notation and the claim of Corollary 4.1 the first coordinates of the common roots of $(\mathbf{z}_1 \cdot \mathbf{p}^A, \ldots, \mathbf{z}_{l-k} \cdot \mathbf{p}^A)$ are the roots of the characteristic polynomial

$$\det\left(A_1 + B_1 \cdot C - x_1 \cdot I\right) = 0. \tag{20}$$

To express the other coordinates in terms of the first ones, fix a common

root $\zeta = (\zeta_1, \ldots, \zeta_{n-1})$ of $(\mathbf{z}_1 \cdot \mathbf{p}^A, \ldots, \mathbf{z}_{l-k} \cdot \mathbf{p}^A)$. We denote the eigenvector of $A_1 + B_1 \cdot C$ corresponding to ζ_1 by

$$\mathbf{v}(\zeta) = (v_1(\zeta), \ldots, v_k(\zeta)) = (p_1^A(\zeta), \ldots, p_k^A(\zeta)) \ \in \bar{\mathbf{k}}^k.$$

Therefore, using (19), we get that ζ_i for $2 \leq i \leq n-1$ satisfy

$$\zeta_i \cdot v_1(\zeta) = \mathbf{e}_1 \cdot (A_i + B_i \cdot C) \cdot \mathbf{v}(\zeta)^T$$

where $\mathbf{e}_1$ is the first canonical basis vector. We get a determinantal formula by observing that the eigenvector

$$(v(\zeta)_1 : \cdots : v(\zeta)_k) = (\mathcal{P}_{i,1}(\zeta) : \cdots : \mathcal{P}_{i,k}(\zeta)) \tag{21}$$

for some $1 \leq i \leq k$, where $\mathcal{P}_{i,j}$ is the determinant of the submatrix of $A_1 + B_1 \cdot C - x_1 \cdot I$ with the i-th row and the j-th column removed. If we assume that $\mathcal{P}_{1,1}$ and $\det(A_1 + B_1 \cdot C - x_1 \cdot I)$ have no common roots, then we can choose $i = 1$ for all eigenvalues of $A_1 + B_1 \cdot C$, and get the formula

$$x_i \cdot \ \mathcal{P}_{1,1} = \mathbf{e}_1 \cdot (A_i + B_i \cdot C) \cdot \ \mathcal{P}_1^T, \tag{22}$$

where $\mathcal{P}_1 = (\mathcal{P}_{1,1}, \ldots, \mathcal{P}_{1,k}) \in \mathbf{k}[x_1]^k$.

The application of equations (20) and (22) gives determinantal formulae for a triangular representation of the common roots of $\mathcal{S}(M, \mathbf{p})^A = \{\mathbf{z}_1 \cdot \mathbf{p}^A, \ldots, \mathbf{z}_{l-k} \cdot \mathbf{p}^A\}$.

We summarize the above construction in the following corollary:

COROLLARY 4.2: *Let* $\mathbf{p}^A = (p_1^A, \ldots, p_l^A)$, $\mathbf{z}_i = (z_{i,1}, \ldots, z_{i,l}) \in \mathbf{k}^m$ *for* $1 \leq i \leq l-k$ *and* A_i, B_i, C *for* $1 \leq i \leq n-1$ *be as in Corollary 4.1. Assume that* $(\mathbf{z}_1 \cdot \mathbf{p}^A, \ldots, \mathbf{z}_{l-k} \cdot \mathbf{p}^A)$ *has exactly* k *common roots in* $\bar{\mathbf{k}}^{n-1}$*, and the first coordinates of the common roots are all distinct. Then for the first coordinates of the common roots we have the defining equation*

$$\det(A_1 + B_1 \cdot C - x_1 \cdot I) = 0.$$

To find the other coordinates we define the univariate polynomials $\mathcal{P}_{1,j} \in \mathbf{k}[x_1]$ *to be the determinant of the submatrix of* $A_1 + B_1 \cdot C - x_1 \cdot I$ *with the first row and the* j*-th column removed. Define the vector*

$$\mathcal{P}_1 = (\mathcal{P}_{1,1}, \ldots, \mathcal{P}_{1,k}) \in \mathbf{k}[x_1]^k.$$

If

$$\gcd_{x_1}(\mathcal{P}_{1,1}, \ \det(A_1 + B_1 \cdot C - x_1 \cdot I)) = 1.$$

then for each $2 \leq i \leq n-1$ *we have the following determinantal formula for the* i*-th coordinates in terms of the first ones:*

$$x_i \cdot \ \mathcal{P}_{1,1} = \mathbf{e}_1 \cdot (A_i + B_i \cdot C) \cdot \ \mathcal{P}_1^T \tag{23}$$

where $\mathbf{e}_1$ *is the first canonical basis vector.* ■

Example 3.7 (cont)
In this example we specified our system of three homogeneous polynomials to have 3 common roots in the projective space:

$$\text{Roots } = \{(x = 2t, y = -t, z = -2t), (x = -t, y = -t, z = t), (x = t, y = -2t, z = 3t)\}.$$

The polynomial system $\tilde{\mathbf{f}}$ consists of the following three polynomials:

$$\begin{aligned}
\tilde{f_1} &:= -\frac{335}{8}x^3 - 53x^2y - 66x^2z - 37xy^2 - 23xyz - \frac{129}{8}xz^2 + 82y^3 - 42y^2z - 34yz^2 + 31z^3,\\
\tilde{f_2} &:= -76x^3 + 25x^2y - 65x^2z - 60xy^2 - 61xyz + 28xz^2 - 306y^3 - 289y^2z + 29yz^2 + 55z^3,\\
\tilde{f_3} &:= 78x^2 + 94xy + \frac{599}{12}xz - 222y^2 - 17yz + \frac{995}{12}z^2
\end{aligned}$$

The subresultant matrix $\tilde{M} \in \mathbb{Q}^{8\times 11}$ is the specialization of the matrix M defined in Example 3.7. The vector $\mathbf{p} \in \mathbb{Q}[x, y, z]^{10}$ is the same as in Example 3.7. We will prove in Proposition 5.6 that $(\tilde{M}, \mathbf{p})$ has the subresultant property w.r.t. $\tilde{\mathbf{f}}$. To demonstrate the method described in Proposition 4.2, we choose $\mathcal{B} := \{p_1, p_2, p_3\} = \{x^3, x^2y, x^2z\}$. Then the following polynomials — corresponding to elements in $\mathrm{cnull}^{\perp}(\tilde{M})$ — are all in the ideal $\langle \tilde{f_1}, \tilde{f_2}, \tilde{f_3}\rangle$:

$$\begin{array}{ll}
y^2z - (\frac{-1}{2}x^2y + \frac{19}{8}x^3 + \frac{23}{8}x^2z), & xz^2 - (3x^3 + 2x^2z),\\
yz^2 - (-4x^2z - 4x^3 + x^2y), & z^3 - (6x^3 + 7x^2z),\\
xyz - (-2x^3 - x^2y - 2x^2z), & y^3 - (-\frac{23}{16}x^3 + \frac{3}{4}x^2y - \frac{27}{16}x^2z),\\
xy^2 - (\frac{13}{8}x^3 + \frac{1}{2}x^2y + \frac{9}{8}x^2z). &
\end{array} \tag{24}$$

The set $\mathcal{S}(\tilde{M}, \mathbf{p})$ is defined as the set of polynomials in (24). By Proposition 3.8 we have that

$$\tilde{\mathcal{I}}^A = \mathcal{S}(\tilde{M}, \mathbf{p})^A,$$

where the affinization we use here is at $x = 1$. Since

$$y \cdot \mathcal{B}^A = \{y, y^2, yz\} \subset \mathbf{k}\langle x^3, x^2y, x^2z, xy^2, xyz, xz^2, y^3, y^2z, yz^2, z^3\rangle^A,$$

we can apply Proposition 4.2. Using (24), the transformation matrix between the bases $\mathcal{B}$ and $y \cdot \mathcal{B}$ modulo $\langle \mathcal{S}(\tilde{M}, \mathbf{p})\rangle$ is the 3×3 matrix

$$U = \begin{bmatrix} 0 & 1 & 0\\ \frac{13}{8} & \frac{1}{2} & \frac{9}{8}\\ -2 & -1 & -2 \end{bmatrix}$$

with characteristic polynomial $2\lambda^3 + 3\lambda^2 - 3\lambda - 2$. The eigenvalues, 1, $-\frac{1}{2}$ and -2, of U are the values of y at the common roots above.
We can find the values of z at the common roots by observing that the first row of the transformation matrix between the bases $\mathcal{B}$ and $z \cdot \mathcal{B}$ is $[0, 0, 1]$. Therefore, using the formula (23), we get that

$$\begin{vmatrix} \frac{1}{2} - \lambda & \frac{9}{8}\\ -1 & -2 - \lambda \end{vmatrix} z = \begin{vmatrix} \frac{13}{8} & \frac{1}{2} - \lambda\\ -2 & -1 \end{vmatrix}.$$

In other words, after substituting $\lambda = y$, we get the following triangular description of the common roots of $\tilde{\mathbf{f}}$:

$$\mathcal{S}(\tilde{M}, \mathbf{p})^A = \mathcal{V}\left(2y^3 + 3y^2 - 3y - 2,\ (-5/8 - 2y) - (1/8 + 3/2\,y + y^2)z\right).$$

Note that if we choose $\mathcal{B} := \{p_1, p_2, p_4\} = \{x^3, x^2y, xy^2\}$ then the polynomials in $\mathcal{S}(\tilde{M}, \mathbf{p})$ are

$$\begin{array}{ll}
xz^2 - 1/9\,x^3 + \frac{8}{9}x^2y - \frac{16}{9}xy^2, & x^2z + \frac{13}{9}x^3 + 4/9\,x^2y - \frac{8}{9}xy^2,\\
y^2z + \frac{16}{9}x^2y - \frac{23}{9}xy^2 + \frac{16}{9}x^3, & yz^2 - \frac{16}{9}x^3 - \frac{25}{9}x^2y + \frac{32}{9}xy^2,\\
xyz - \frac{8}{9}x^3 + 1/9\,x^2y + \frac{16}{9}xy^2, & y^3 - x^3 - 3/2\,x^2y + 3/2\,xy^2,\\
z^3 + \frac{37}{9}x^3 + \frac{28}{9}x^2y - \frac{56}{9}xy^2 &
\end{array}$$

and we can get a triangular representation directly from $\mathcal{S}(\tilde{M}, \mathbf{p})$ without using Proposition 4.2:

$$\left(y^3 - x^3 - 3/2\,x^2y + 3/2\,xy^2,\ \ x^2z + \frac{13}{9}x^3 + 4/9\,x^2y - \frac{8}{9}xy^2)\right).$$

In the following proposition we consider the case when the polynomial system has a unique common root. Similar expressions using subresultant matrices can be found in (19; 8).

PROPOSITION 4.3: *Let $\tilde{\mathbf{f}} = (\tilde{f}_1, \ldots, \tilde{f}_n) \in \mathbf{k}[x_1, \ldots, x_n]$ be homogeneous polynomials. Let $\tilde{M} \in \mathbf{k}^{r\times(r+1)}$ be a matrix and let $\tilde{\mathbf{p}} = (\tilde{p}_1, \ldots, \tilde{p}_l)$ be a vector of degree ν homogeneous polynomials in $\mathbf{k}[x_1, \ldots, x_n]$ such that $(\tilde{M}, \tilde{\mathbf{p}})$ has the subresultant property with respect to $\tilde{\mathcal{I}}$. Then $\tilde{f}_1, \ldots, \tilde{f}_n$ have either zero or one common root in $\mathbb{P}^{n-1}_{\bar{\mathbf{k}}}$. If $\tilde{f}_1, \ldots, \tilde{f}_n$ has one common root $\xi = (\xi_1 : \cdots : \xi_n) \in \mathbb{P}^{n-1}$, then we have the following equation in $\mathbb{P}^r_{\mathbf{k}}$:*

$$(\tilde{p}_1(\xi) : \cdots : \tilde{p}_l(\xi)) = \left(\mathcal{D}_{\{2,\ldots,r+1\}} : \cdots : (-1)^{l-1}\mathcal{D}_{\{1,\ldots,\hat{l}\ldots,r+1\}}\right) \tag{25}$$

where $\mathcal{D}_{\{1,\ldots,\hat{i}\ldots,r+1\}}$ denotes the maximal minor of $\tilde{M}$ with the i-th column removed. Moreover, if we assume that $\mathcal{D}_{\{1,\ldots\hat{n}\ldots,r\}} \neq 0$ and

$$x_i\tilde{p}_n = x_n\tilde{p}_i \quad \textit{for} \quad i = 1, \ldots n-1 \tag{26}$$

then the coordinates of ξ are given by

$$(\xi_1 : \cdots : \xi_n) = \left(\mathcal{D}_{\{2,\ldots,r+1\}} : \cdots : (-1)^{n-1}\mathcal{D}_{\{1,\ldots\hat{n}\ldots,r+1\}}\right). \tag{27}$$

Proof: First note that condition (2) of the subresultant property in Definition 3.1 implies that the right hand side of (25) defines a point in $\mathbb{P}^l_{\mathbf{k}}$. We can assume without loss of generality that $\mathcal{D}_{\{2,\ldots,r+1\}} \neq 0$. Consider the linear equation system L with unknowns $\zeta = (\zeta_1, \ldots, \zeta_l)$ given by

$$L := \{\zeta_i - (-1)^i \frac{\mathcal{D}_{\{1,\ldots\hat{i}\ldots,r+1\}}}{\mathcal{D}_{\{1,\ldots,r\}}}\, \zeta_1 = 0 \mid 2 \leq i \leq l\}.$$

Clearly L has a unique solution in $\mathbb{P}^r_{\mathbf{k}}$ which equals to

$$(\zeta_1 : \cdots : \zeta_l) = \left(\mathcal{D}_{\{2,\ldots,r+1\}} : \cdots : (-1)^r\mathcal{D}_{\{1,\ldots,\ldots\hat{l}\ldots,r+1\}}\right).$$

Since $(\tilde{M}, \tilde{\mathbf{p}})$ has the subresultant property w.r.t $\tilde{\mathbf{f}}$, $p_i - \frac{(-1)^i\mathcal{D}_{\{1,\ldots\hat{i}\ldots,r+1\}}}{\mathcal{D}_{\{2,\ldots,r+1\}}}p_1$ $(2 \leq i \leq l)$ is in the ideal generated by $\tilde{f}_1, \ldots, \tilde{f}_n$. Therefore, for any common root $\xi \in \mathbb{P}^{n-1}_{\bar{\mathbf{k}}}$ of $\tilde{f}_1, \ldots, \tilde{f}_n$ we have that $p_i(\xi) - \frac{(-1)^i\mathcal{D}_{\{1,\ldots\hat{i}\ldots,r+1\}}}{\mathcal{D}_{\{1,\ldots,r\}}}p_1(\xi) = 0$. This implies that $\tilde{f}$ has at most one common root in $\mathbb{P}^{n-1}_{\bar{\mathbf{k}}}$. In the case when $\tilde{f}$ has a common root we get the claimed equation (25).
The second claim (27) is an immediate consequence of (25) and (26). □

REMARK 4.4: As we mentioned in the introduction, there is a formula involving the partial derivatives of the resultant for the coordinates of the unique common root, generalizing (2) above (cf. Jouanolou (25); Jouanolou (26); Gelfand *et al.* (18); Jeronimo *et al.* (23)). If $\mathbf{f} = (f_1 = \sum_{j=1}^{t_1} c_{\alpha_{1,j}} x^{\alpha_{1,j}}, \ldots, f_n = \sum_{j=1}^{t_n} c_{\alpha_{n,j}} x^{\alpha_{n,j}})$ is a system of generic homogeneous polynomials of degree $\mathbf{d} = (d_1, \ldots, d_n)$ and

$\tilde{\mathbf{f}} \subset \mathbf{k}[x_1, \ldots, x_n]$ is a coefficient specialization of $\mathbf{f}$ such that $\tilde{\mathbf{f}}$ has a unique common root ξ then for all $1 \leq i \leq n$ we have

$$(\xi^{\alpha_{i,1}} : \cdots : \xi^{\alpha_{i,t_i}}) = \left(\frac{\partial \mathrm{Res}_{\mathbf{d}}}{\partial c_{\alpha_{i,1}}}(\tilde{f}) : \cdots : \frac{\partial \mathrm{Res}_{\mathbf{d}}}{\partial c_{\alpha_{i,t_i}}}(\tilde{f}) \right). \tag{28}$$

Note that

$$\deg_{c_{i,\alpha(j)}} \frac{\partial \mathrm{Res}_{\mathbf{d}}}{\partial c_{i,\alpha(j)}} = \mathcal{H}_{\hat{\mathbf{d}}^i}(\delta - d_i + 1) - 1 = \prod_{k \neq i} d_k - 1 \quad \forall\, 1 \leq j \leq t_i$$

where $\mathcal{H}_{\hat{\mathbf{d}}^i}$ denotes the Hilbert function of a regular sequence with $n-1$ homogeneous polynomials in n variables with degrees $\hat{\mathbf{d}}^i = (d_1, \ldots, d_{i-1}, d_{i+1}, \ldots, d_n)$ (for reference see for example D'Andrea and Dickenstein (12)), and $\delta = \sum_{i=1}^{n}(d_i - 1)$. On the other hand, if we apply Corollary 4.3 and the results of (19; 8) with the Macaulay or Jouanolou type subresultant matrices, then the determinants on the right hand side of (25) can be replaced by the subresultants, and their degree in the coefficients of f_i is $\mathcal{H}_{\hat{d}^i}(\delta - d_i)$ and we have

$$\mathcal{H}_{\hat{\mathbf{d}}^i}(\delta - d_i) \leq \mathcal{H}_{\hat{\mathbf{d}}^i}(\delta - d_i + 1) - n.$$

This shows that the use of subresultants improves methods using formulas analogous to (28) when solving polynomial systems. Note that (25) uses the determinants of subresultant matrices, which are multiples of the subresultants, but the extraneous factor is smaller than the extraneous factor for the determinants of resultant matrices.

5. Strong subresultant theory for Jouanolou type matrices

For homogeneous multivariate polynomial systems González-Vega (19) and Chardin (8) generalized the notion of univariate subresultants of Collins (9) using Macaulay matrices. As we mentioned in the introduction, these subresultant constructions are special cases of the Jouanolou type subresultant construction (c.f. Szanto (35)). Therefore, we only describe the latter, following the approach of Szanto (35).

First we recall the definition of the Jouanolou subresultant matrix $\mathbf{J}_{\eta,\nu}(f)$ defined in Szanto (35). As we shall see, the matrix $\mathbf{J}_{\eta,\nu}(f)$, together with a vector of monomials corresponding to its columns, form a pair satisfying the subresultant property. In the end of the subsection we give a modification of the matrix $\mathbf{J}_{\eta,\nu}(f)$ which, together with the vector of monomials corresponding to its columns, satisfies the k-strong subresultant property with respect to affine k-sets of polynomial systems $\mathcal{F}$, where the exact conditions on k and $\mathcal{F}$ are specified below.

Before the definition of the subresultant matrices, we define sets of monomials corresponding to columns and rows of the Jouanolou type resultant and subresultant matrices (c.f. Jouanolou (27, Section 3.10) and (35)).

DEFINITION 5.1: *Fix* $\mathbf{d} = (d_1, \ldots, d_n)$. *For* $\eta \geq 0$ *we define the following sets of monomials*

$$\begin{aligned} \mathrm{Mon}_n(\eta) &:= \{\mathbf{x}^\alpha \mid |\alpha| = \eta\} \\ \mathrm{Rep}_{\mathbf{d}}(\eta) &:= \{\mathbf{x}^\alpha \mid |\alpha| = \eta,\ \exists\, i\ \alpha_i \geq d_i\} \\ \mathrm{Dod}_{\mathbf{d}}(\eta) &:= \{\mathbf{x}^\alpha \mid |\alpha| = \eta,\ \exists\, i \neq j\ \alpha_i \geq d_i, \alpha_j \geq d_j\}. \end{aligned}$$

For $\eta < 0$ *we define all of the above sets to be the empty set. Also, we denote by* $\mathrm{Mon}_n^*(\eta)$ *the dual basis of* $\mathrm{Mon}_n(\eta)$ *in the dual* $\mathbf{R}$*-module* $\langle \mathrm{Mon}_n(\eta) \rangle^*$, *and similarly for* $\mathrm{Rep}_{\mathbf{d}}^*(\eta)$.
For $0 \leq \eta' \leq \eta$ *let*

$$\begin{aligned} \overline{\mathrm{Mon}}_n(\eta, \eta') &:= \{\mathbf{x}^\alpha \mid |\alpha| = \eta, \alpha_n \geq \eta'\} \\ \overline{\mathrm{Rep}}_{\mathbf{d}}(\eta, \eta') &:= \{\mathbf{x}^\alpha \in \overline{\mathrm{Mon}}_n(\eta, \eta') \mid \exists i \leq n-1\ \ \alpha_i \geq d_i \ \ \textit{or}\ \ \alpha_n \geq d_n + \eta'\}. \end{aligned}$$

We denote the sets of monomials corresponding to columns and rows of the subresultant matrix by

$$\begin{aligned} \mathrm{Mon}_n(\eta, \eta') &:= \mathrm{Mon}_n(\eta) - \overline{\mathrm{Mon}}_n(\eta, \eta') \\ \mathrm{Rep}_{\mathbf{d}}(\eta, \eta') &:= \mathrm{Rep}_{\mathbf{d}}(\eta) - \overline{\mathrm{Rep}}_{\mathbf{d}}(\eta, \eta'). \end{aligned}$$

We may omit n *and* $\mathbf{d}$ *from the subscript if it is clear from the context.*

NOTATION 5.2: We use the following notations and assumptions:

1. For $\nu \geq 0$ and $\mathbf{d} = (d_1, \ldots, d_n)$ we denote by $\mathcal{H}_{\mathbf{d}}(\nu)$ the Hilbert function of a regular sequence of n homogeneous polynomials in n variables of degrees $d_1, \ldots, d_n$.
2. Denote by δ the sum
$$\delta = \sum_{i=1}^{n} (d_i - 1).$$
3. Fix η and ν such that they satisfy the condition
$$0 \leq \delta - \nu \leq \eta \leq \delta - \eta \leq \nu \leq \delta. \tag{29}$$
Informally, η denotes the smaller one among η and $\delta - \eta$ in the definition of Jouanolou's matrix and ν is the analogue of the degree in the Macaulay type subresultant construction of Chardin (8). To simplify the notation, we also introduce
$$\eta' := \eta - (\delta - \nu).$$

Next we define the subresultant matrix $\mathbf{J}_{\eta,\nu}(f)$.

DEFINITION 5.3: *Let* $\mathbf{f} = (f_1, \ldots, f_n) \in \mathbf{R}[x_1, \ldots, x_n]$ *be generic homogeneous polynomials of degrees* $\mathbf{d} = (d_1, \ldots, d_n)$. *Fix* η *and* ν *such that they satisfy (29) and let* $\eta' = \eta - (\delta - \nu)$. *The* $\mathbf{R}$*-module homomorphism*

$$\mathbf{J}_{\eta,\nu}(\mathbf{f}) : \langle \mathrm{Mon}(\eta, \eta') \rangle^* \oplus \langle \mathrm{Rep}(\delta - \eta) \rangle \to \langle \mathrm{Mon}(\delta - \eta) \rangle \oplus \langle \mathrm{Rep}(\eta, \eta') \rangle^*$$

corresponding to the subresultant matrix is defined as follows. Let

$$\Omega_{\eta,\eta'} : \langle \mathrm{Mon}(\eta, \eta') \rangle^* \to \langle \mathrm{Mon}(\delta - \eta) \rangle, \qquad \mathbf{y}^\beta \mapsto \mathrm{Morl}_\beta(\mathbf{x}), \tag{30}$$

where $\mathrm{Morl}_\beta(\mathbf{x})$ *is the Morley form defined in Jouanolou (27, Section 3.10), a degree* $\delta - \eta$ *polynomial in* $\mathbf{R}[x_1, \ldots, x_n]$. *For* $t \geq 0$ *define*

$$\Phi_t : \langle \mathrm{Rep}(t) \rangle \to \langle \mathrm{Mon}(t) \rangle, \qquad \mathbf{x}^\alpha \mapsto \left(\frac{\mathbf{x}^\alpha}{x_{i(\alpha)}^{d_{i(\alpha)}}} \right) \cdot f_{i(\alpha)}, \tag{31}$$

where $i(\alpha)$ *denotes the smallest index such that* $\alpha_{i(\alpha)} \geq d_{i(\alpha)}$. *Let* $\Phi^*_{\eta,\eta'}$ *be the dual of the map* $\Phi_\eta|_{\langle \mathrm{Rep}_d(\eta,\eta') \rangle}$ *restricted to* $\langle \mathrm{Mon}(\eta, \eta') \rangle^*$. *Then* $\mathbf{J}_{\eta,\nu}(\mathbf{f})$ *is defined as*

$$\left(\mathbf{y}^\alpha, \mathbf{x}^\beta \right) \mapsto \left(\Omega_{\eta,\eta'}(\mathbf{y}^\alpha) + \Phi_{\delta-\eta}(\mathbf{x}^\beta), \;\; \Phi^*_{\eta,\eta'}(\mathbf{y}^\alpha) \right)$$

for $\mathbf{y}^\alpha \in \mathrm{Mon}(\eta, \eta')^*$ *and* $\mathbf{x}^\beta \in \mathrm{Rep}_d(\delta - \eta)$. *Abusing the notation, we denote the matrix of the map* $\mathbf{J}_{\eta,\nu}(\mathbf{f})$ *– in the given monomial bases – again by* $\mathbf{J}_{\eta,\nu}(\mathbf{f})$.

Permuting rows and columns, the matrix $\mathbf{J}_{\eta,\nu}(\mathbf{f})$ has the following structure:

$$\mathbf{J}_{\eta,\nu}(\mathbf{f}) = \begin{array}{c|c|c} & \mathrm{Mon}(\delta - \eta) & \mathrm{Rep}(\eta, \eta')^* \\ \hline & \Omega_{\eta,\eta'} & \Phi^*_{\eta,\eta'} \quad \mathrm{Mon}(\eta, \eta')^* \\ \hline & \Phi_{\delta-\eta} & 0 \quad \mathrm{Rep}(\delta - \eta) \end{array} \tag{32}$$

As we mentioned earlier, the subresultant matrix $\mathbf{J}_{\eta,\nu}(f)$ is a submatrix of Jouanolou's resultant matrix (cf. (27)), and for $\nu = \delta + 1$ we get the resultant matrix, which is square. The subresultant matrix is obtained from the resultant matrix by erasing the rows corresponding to the monomials in $\overline{\mathrm{Mon}}(\eta, \eta')$ and the columns corresponding to the monomials in $\overline{\mathrm{Rep}}(\eta, \eta')$. The difference between the number of columns and rows of $\mathbf{J}_{\eta,\nu}(f)$ is $\mathcal{H}_{\mathbf{d}}(\nu)$ (c.f. Szanto (35)).

Example 5.4: Let $n = 3$, $\mathbf{d} = (3, 3, 2)$ and $\mathbf{f} = (f_1, f_2, f_3)$ be polynomials in $\mathbf{x} := (x, y, z)$ as in Example 3.7. We set $\eta = 2$. We obtain Jouanolou's resultant matrix by taking $\nu = \delta + 1 = 6$, which is a 11×11 matrix $\mathbf{J}_{2,6}(\mathbf{f})$ with rows corresponding to the monomials

$$\left[\begin{array}{ccccccccccc} u^2 & uv & uw & v^2 & vw & w^2 & x^3 & z^2x & y^3 & z^2y & z^3 \end{array} \right]$$

and the columns corresponding to the monomials

$$[\ x^3 \quad yx^2 \quad zx^2 \quad y^2x \quad zyx \quad z^2x \quad y^3 \quad y^2z \quad z^2y \quad z^3 \quad w^2\ ],$$

using the variables u, v, w for the dual $\mathbf{R}$-algebra.

For $\nu = 5$ we have $\eta' = \eta - (\delta - \nu) = 2$, therefore we erase all rows of $\mathbf{J}_{2,6}(\mathbf{f})$ corresponding to monomials which have degree 2 in the variable w. That is, we erase the single row corresponding to w^2. Since $\overline{\mathrm{Rep}}(2,2) = \emptyset$, we do not erase any columns. Thus the subresultant matrix $\mathbf{J}_{2,5}(\mathbf{f})$ has size 10×11.

For $\nu = 4$ we have $\eta' = 1$, therefore we erase all rows which correspond to monomials of degree at least 1 in the variable w. Again, $\overline{\mathrm{Rep}}(2,1) = \emptyset$, so we do not erase any columns. Thus the subresultant matrix $\mathbf{J}_{2,4}(\mathbf{f})$ has size 8×11, with the rows corresponding to the monomials

$$[\ u^2 \quad vu \quad v^2 \quad x^3 \quad z^2x \quad y^3 \quad z^2y \quad z^3\ ],$$

while the columns still correspond to the monomials

$$[\ x^3 \quad yx^2 \quad zx^2 \quad y^2x \quad zyx \quad z^2x \quad y^3 \quad y^2z \quad z^2y \quad z^3 \quad w^2\ ]$$

In the next definition we define square submatrices of the Jouanolou subresultant matrix $\mathbf{J}_{\eta,\nu}(\mathbf{f})$ such that the ratios of their determinants give the subresultants.

DEFINITION 5.5: *Let* $\mathbf{f}$, $\mathbf{d}$, δ, η, ν, η' *and* $\mathbf{J}_{\eta,\nu}(\mathbf{f})$ *be as in Definition 5.3.*

1. *Let* $\mathcal{T} \subseteq \mathrm{Mon}(\delta - \eta)$ *of cardinality* $\mathcal{H}_{\mathbf{d}}(\nu)$. *Denote by* $\mathbf{M}_{\mathcal{T}}^{\eta,\nu}(\mathbf{f})$ *the maximal square submatrix of* $\mathbf{J}_{\eta,\nu}(\mathbf{f})$ *with columns not corresponding to* $\mathcal{T}$.
2. *Let* $\mathbf{E}_{\delta-\eta}$ *denote the submatrix of* $\Phi_{\delta-\eta}$ *(see (31)) with rows and columns corresponding to monomials in* $\mathrm{Dod}(\delta-\eta)$ *(see Definition 5.1). Let* $\mathbf{E}_{\eta,\eta'}$ *be the submatrix of* $\Phi^*_{\eta,\eta'}$ *(see Definition 5.3) such that its rows and columns correspond to* $\mathrm{Dod}(\eta) \cap \mathrm{Rep}(\eta, \eta')$.
3. *Let* $\mathcal{T} \subseteq \mathrm{Mon}(\delta-\eta)$ *of cardinality* $\mathcal{H}_{\mathbf{d}}(\nu)$. *We define the subresultant* $\Gamma_{\mathcal{T}}^{\eta,\nu}(\mathbf{f})$ *corresponding to* $\mathcal{T}$ *by*

$$\Gamma_{\mathcal{T}}^{\eta,\nu}(\mathbf{f}) := \frac{\det(\mathbf{M}_{\mathcal{T}}^{\eta,\nu})}{\det(\mathbf{E}_{\delta-\eta})\det(\mathbf{E}_{\eta,\eta'})}. \tag{33}$$

Note that the denominator of $\Gamma_{\mathcal{T}}^{\eta,\nu}(\mathbf{f})$ *do not depend on the choice of* $\mathcal{T}$.

Example 5.4 (cont)
To give an example when the denominator in (33) is nontrivial, we note that for $\mathbf{d} = (3,3,2)$ $\mathrm{Dod}_{\mathbf{d}}(t) = \emptyset$ for any $t < 5$, therefore, if $0 < \eta < 5$, then the denominator of (33) is 1. For $\eta = 0$, Jouanolou's matrix contains a single row of Bézoutian type, therefore there is only one possible subresultant matrix $\mathbf{J}_{0,5}$ obtained by removing this one row. Then $\mathbf{J}_{0,5}$ is a Macaulay type subresultant matrix, which has size 20×21. Note that for $\nu = \delta - \eta$ we always get a Macaulay type subresultant matrix. Since $\mathrm{Dod}_{(3,3,2)}(5) = \{x^3z^2, y^3z^2\}$, therefore $\mathbf{E}_5$ has size 2×2:

$$\begin{bmatrix} a_0 & a_6 \\ b_0 & b_6 \end{bmatrix}$$

Thus, for any $\mathcal{T} \subset \mathrm{Mon}(5)$, $|\mathcal{T}| = 1$, we have

$$\Gamma_{\mathcal{T}}^{0,5}(\mathbf{f}) = \frac{\det(\mathbf{M}_{\mathcal{T}}^{0,5})}{a_0b_6 - a_6b_0}.$$

In the following proposition we prove that the Jouanolou type subresultant matrices satisfy the conditions of the subresultant property (see Definition 3.1).

PROPOSITION 5.6: *Let* $\mathbf{f} = (f_1, \ldots, f_n)$ *be generic polynomials of degrees* $\mathbf{d} = (d_1, \ldots, d_n)$ *in* $\mathbf{R}[x_1, \ldots, x_n]$ *and let* δ, η, ν, η' *and* $\mathbf{J}_{\eta,\nu}(\mathbf{f})$ *be as in Definition 5.3. Moreover, let* $\mathbf{p}$ *be the following vector:*

$$\mathbf{p} := (\underbrace{x_n^{\eta'} \cdot \mathbf{x}^{\alpha(1)}, \ \ldots, \ x_n^{\eta'} \cdot \mathbf{x}^{\alpha(N)}}_{|\mathrm{Mon}(\delta-\eta)|}) \tag{34}$$

where $\mathbf{x}^{\alpha(i)} \in \mathrm{Mon}(\delta - \eta)$ *is the monomial corresponding to the* i*-th column of* $\mathbf{J}_{\eta,\nu}(\mathbf{f})$ *for* $1 \leq i \leq N := |\mathrm{Mon}(\delta-\eta)|$. *Assume that* $\mathcal{H}_{\mathbf{d}}(\nu) \leq \delta - \eta$. *Then the pair* $(\mathbf{J}_{\eta,\nu}(\mathbf{f}), \mathbf{p})$ *has the subresultant property with respect to* $\mathcal{I}$, *the ideal generated by* $f_1, \ldots, f_n$.

Proof: By Szanto (35, Proposition 3.1.6) there exists $\mathcal{T} \subset \mathrm{Mon}(\delta - \eta)$ of cardinality $\mathcal{H}_{\mathbf{d}}(\nu)$ such that $\mathbf{M}_{\mathcal{T}}^{\eta,\nu}$ is non-singular. Also, the assumption that $\mathcal{H}_{\mathbf{d}}(\nu) \leq \delta - \eta$ implies that for any $\mathcal{T} \subset \mathrm{Mon}(\delta - \eta)$ of cardinality $\mathcal{H}_d(\nu)$ conditions (2)(b) and (2)(c) of Definition 3.1 are satisfied (see Remark 3.2). Therefore, if T is the index set of the columns of $\mathbf{J}_{\eta,\nu}(\mathbf{f})$ not corresponding $\mathcal{T}$ then T satisfies condition (2) of the subresultant property.

To prove condition (1) of the subresultant property, we cite Szanto (35, Lemma 3.2.7), where it is proved that the column vector

$$\Omega_{\eta,\eta'} \cdot \mathbf{p} = \Big(x_n^{\eta'} \mathrm{Morl}_\beta(\mathbf{x}) \Big)_{\mathbf{y}^\beta \in \mathrm{Mon}^*(\eta,\eta')}$$

(see (32) and Definition 5.3) is in the column space of the matrix $\Phi^*_{\eta,\eta'}$ modulo the ideal $\mathcal{I}$. This implies that there exists $a_1, \ldots, a_R$ for $R := |\mathrm{Rep}(\eta, \eta')|$ such that if

$$\mathbf{q} := (\underbrace{x_n^{\eta'} \cdot \mathbf{x}^{\alpha(1)}, \ \ldots, \ x_n^{\eta'} \cdot \mathbf{x}^{\alpha(N)}}_{|\mathrm{Mon}(\delta-\eta)|}, \underbrace{a_1, \ldots, a_R}_{|\mathrm{Rep}(\eta,\eta')|})$$

then the entries of the vector $\mathbf{J}_{\eta,\nu}(\mathbf{f}) \cdot \mathbf{q}$ are in the ideal $\mathcal{I}$. This proves condition (1) of the subresultant property. □

We devote the rest of this section to give a modification of the Jouanolou type subresultant matrix which satisfies the strong subresultant property (see Definition 3.10). To understand the motivation for the construction what follows, we first informally explain why $(\mathbf{J}_{\eta,\nu}(f), \mathbf{p})$ do not have the strong subresultant property.

Let $\tilde{\mathbf{f}} = (\tilde{f}_1, \ldots, \tilde{f}_n)$ be a coefficient specialization of $\mathbf{f}$ such that there exists $\mathcal{T} \subset \mathrm{Mon}(\delta - \eta)$ of cardinality $|\mathcal{T}| = \mathcal{H}_d(\nu)$ so that $x_n^{\eta'}\mathcal{T}$ generates $\mathbf{k}[\mathbf{x}]_\nu / \tilde{\mathcal{I}}_\nu$. Then, by (35)

$$\Gamma_{\mathcal{T}}^{\eta,\nu}(\tilde{\mathbf{f}}) \neq 0.$$

But this does not imply that the matrix $\mathbf{J}_{\eta,\nu}(\tilde{\mathbf{f}})$ has maximal rank: if for example $\det(\mathbf{E}_{\delta-\eta}(\tilde{\mathbf{f}})) = 0$ (see Definition 5.5), then the rows of $\mathbf{J}_{\eta,\nu}(\tilde{\mathbf{f}})$ are dependent. On the other hand, in (35, Proposition 3.3.5) it is proved that $\Gamma_{\mathcal{T}}^{\eta,\nu}(\tilde{\mathbf{f}})$ is the determinant of a Koszul type complex of $\mathbf{k}$-spaces – there denoted by $K^\bullet(\tilde{\mathbf{f}}, \eta, \nu, \mathcal{T})$.

Thus, the non-vanishing of $\Gamma_{\mathcal{T}}^{\eta,\nu}(\tilde{\mathbf{f}})$ implies that $K^\bullet(\tilde{\mathbf{f}},\eta,\nu,\mathcal{T})$ is exact. This implies that the differential of $K^\bullet(\tilde{\mathbf{f}},\eta,\nu,\mathcal{T})$ at level 0 has the same rank as in the generic case, thus its matrix must have a submatrix which has the same size and rank as the generic Jouanolou type subresultant matrix $\mathbf{J}_{\eta,\nu}(\mathbf{f})$. This is the motivation of taking the larger matrix – corresponding to the matrix of the differential of $K^\bullet(\mathbf{f},\eta,\nu,\mathcal{T})$ at level 0 – instead of $\mathbf{J}_{\eta,\nu}(\mathbf{f})$.

In the next definition we give explicitly the matrix corresponding to the level 0 differential of $K^\bullet(\mathbf{f},\eta,\nu,\mathcal{T})$.

DEFINITION 5.7: *Let* $\mathbf{f}$, $\mathbf{d}$, ν, η, η' *be as Definition 5.3. The* $\mathbf{R}$*-module homomorphism* $\daleth_{\eta,\nu}(\mathbf{f})$:

$$\langle \mathrm{Mon}(\eta,\eta')\rangle^* \oplus \bigoplus_{i=1}^n \langle \mathrm{Mon}(\delta-\eta-d_i)\rangle \to \langle \mathrm{Mon}(\delta-\eta)\rangle \oplus \bigoplus_{i=1}^n \langle \mathrm{Mon}(\eta-d_i,\eta')\rangle^*$$

is defined as follows. For $t>0$ *let*

$$\phi_t : \bigoplus_{i=1}^n \langle \mathrm{Mon}(t-d_i)\rangle \longrightarrow \langle \mathrm{Mon}(t)\rangle, \quad (\mathbf{x}^{\beta(1)},\ldots,\mathbf{x}^{\beta(n)}) \mapsto \sum_{i=1}^n \mathbf{x}^{\beta(i)} f_i.$$

For $t \geq t' > 0$ *let*

$$\phi_{t,t'}^* : \langle \mathrm{Mon}(t,t')\rangle^* \longrightarrow \bigoplus_{i=1}^n \langle \mathrm{Mon}(t-d_i,t')\rangle^*$$

be the dual of $\phi_t|_{\bigoplus_{i=1}^n \langle \mathrm{Mon}(t-d_i,t')}$ *restricted to* $\langle \mathrm{Mon}(t,t')\rangle^*$. *Let* $\Omega_{\eta,\eta'}$ *be the same as in Definition 5.3.*
Then $\daleth_{\eta,\nu}(f)$ *is defined as*

$$\big(\mathbf{y}^\alpha, \mathbf{x}^{\beta(1)},\ldots,\mathbf{x}^{\beta(n)}\big) \mapsto \big(\Omega_{\eta,\eta'}(\mathbf{y}^\alpha) + \phi_{\delta-\eta}(\mathbf{x}^{\beta(1)},\ldots,\mathbf{x}^{\beta(n)}),\ \ \phi^*_{\eta,\eta'}(\mathbf{y}^\alpha)\big)$$

for $\mathbf{y}^\alpha \in \mathrm{Mon}(\eta,\eta')^*$ *and* $(\mathbf{x}^{\beta(1)},\ldots,\mathbf{x}^{\beta(n)}) \in \bigoplus_{i=1}^n \langle \mathrm{Mon}(t-d_i)\rangle$. *Abusing the notation, we denote the matrix of the map* $\daleth_{\eta,\nu}(\mathbf{f})$ – *in the monomial bases* – *again by* $\daleth_{\eta,\nu}(\mathbf{f})$.

Example 5.4 (cont)
This example demonstrates the possible difference between the subresultant matrices defined in Definition 5.3 and the matrix defined in Definition 5.7. We also show the possible difference between

$$\bigoplus_{i=1}^n \langle \mathrm{Mon}(t-d_i)\rangle \quad \text{and} \quad \langle \mathrm{Rep}_{\mathbf{d}}(t)\rangle.$$

As before, we consider 3 generic polynomials of degrees $\mathbf{d}=(3,3,2)$. If $0<\eta<5$ then for all ν the subresultant matrix $\mathbf{J}_{\eta,\nu}$ is the same as the matrix $\daleth_{\eta,\nu}$.

For $\eta=0$ and $\nu=5$ the subresultant matrix $\mathbf{J}_{0,5}$ has size 20×21 as we mentioned in a previous example. The matrix $\daleth_{0,5}$ defined in Definition 5.7 has size 22×21. Its rows correspond to the 22 monomials:

$$\left[x^2,\ xy,\ xz,\ y^2,\ yz,\ z^2,\ x^2,\ xy,\ xz,\ y^2,\ yz,\ z^2,\ x^3,\ x^2y,\ x^2z,\ xy^2,\ xyz,\ xz^2,\ y^3,\ y^2z,\ yz^2,\ z^3\right].$$

Note that $\mathrm{Rep}_{\mathbf{d}}(5)$ has the following 20 elements:

$$\left[x^5,\ x^4y,\ x^4z,\ x^3y^2,\ x^3yz,\ x^3z^2,\ y^3x^2,\ yx^2z^2,\ z^3x^2,\ y^4x,\ y^3xz,\ y^2xz^2,\ yxz^3,\ z^4x,\ y^5,\ y^4z,\ y^3z^2,\ y^2z^3,\ yz^4,\ z^5\right].$$

Dividing $\mathbf{x}^\alpha \in \mathrm{Rep}_d(5)$ by one of $\{x^3, y^3, z^2\}$ – the first one which divides $\mathbf{x}^\alpha$ – we get an injective, but not surjective, map of sets:

$$\mathrm{Rep}(5) \ \to\ \mathrm{Mon}(2)\ \cup^*\ \mathrm{Mon}(2)\ \cup^*\ \mathrm{Mon}(3).$$

In fact, the maps Φ_5 of Definition 5.3 and ϕ_5 of Definition 5.7 are related the same way: while Φ_5 first divides $\mathbf{x}^\alpha \in \mathrm{Rep}(5)$ by the first one of $[x^3, y^3, z^2]$ which divides it, and then multiplies with the corresponding f_i, the map ϕ_5 simply multiplies $x^\beta \in \mathrm{Mon}(5-d_i)$ by f_i. The maps $\Phi_{t,t'}$ and $\phi_{t,t'}$ relate similarly. The maps corresponding to the Morley forms are exactly the same.

In the next theorem we show that $(\beth_{\eta,\nu}(\mathbf{f}), \mathbf{p})$ has the k-strong subresultant property for all k values such that $\mathcal{H}_d(\nu) \le k \le \delta - \eta$ and with respect to an affine k-set $\mathcal{F}_{k,\nu}$ defined below. Here $\mathbf{p}$ is the same as was defined in (34) above. We use the notion of the dimension, degree and the regularity index of the Hilbert function of homogeneous ideals, which we define first:

DEFINITION 5.8: *Let $\mathcal{I} \subset \mathbf{k}[\mathbf{x}]$ be a homogeneous ideal, let $\mathcal{H}_\mathcal{I}$ and $\mathcal{H}_{\mathbf{k}[\mathbf{x}]/\mathcal{I}}$ be the Hilbert functions and let $\mathcal{P}_\mathcal{I}$ and $\mathcal{P}_{\mathbf{k}[\mathbf{x}]/\mathcal{I}}$ be the Hilbert polynomials of $\mathcal{I}$ and $\mathbf{k}[\mathbf{x}]/\mathcal{I}$, respectively. We denote by*

$$\sigma(\mathcal{I}) := \min\{t_0 : \mathcal{H}_\mathcal{I}(t) = \mathcal{P}_\mathcal{I}(t)\ \forall t \ge t_0\},$$

and we call $\sigma(\mathcal{I})$ the **regularity of the Hilbert function** *of $\mathcal{I}$. The* **dimension** *of $\mathcal{I}$, denoted by $\dim(\mathcal{I})$ is defined to be the degree of $\mathcal{P}_{\mathbf{k}[\mathbf{x}]/\mathcal{I}}$ (if $\mathcal{P}_{\mathbf{k}[\mathbf{x}]/\mathcal{I}} \equiv 0$ then $\dim(\mathcal{I}) := -1$). If we assume that $\dim(\mathcal{I}) = 0$ then $\mathcal{P}_{\mathbf{k}[\mathbf{x}]/\mathcal{I}}$ is a constant k, and the* **degree** *of $\mathcal{I}$ is*

$$\deg(\mathcal{I}) = k.$$

REMARK 5.9: *Classically, one either speaks of the dimension of projective varieties (or schemes) or the dimension of rings (Krull dimension). Our definition of the dimension of $\dim(\mathcal{I})$ coincides with the dimension of the projective variety $\mathrm{Proj}(\mathbf{k}[\mathbf{x}]/\mathcal{I}) \subset \mathbb{P}^{n-1}_{\overline{\mathbf{k}}}$ defined by $\mathcal{I}$. In this paper we assume that $\dim(\mathcal{I}) = 0$. On the other hand, this is equivalent to the Krull dimension of the ring $\mathbf{k}[\mathbf{x}]/\mathcal{I}$ being 1, which is also dimension of the affine variety defined by $\mathcal{I}$. This second notion of dimension is used in the Appendix. Note that the assumption that $\dim(\mathcal{I}) = 0$ implies that $\deg(\mathcal{I})$ equals to the number of common roots of $\mathcal{I}$ in $\mathbb{P}^{n-1}_{\overline{\mathbf{k}}}$, counted with multiplicity. (c.f. Cox* et al. *(11, Chapter 6.4)).*

THEOREM 5.10: *Let $\mathbf{f} = (f_1, \ldots, f_n) \subset \mathbf{R}[x_1, \ldots, x_n]$ be generic homogeneous polynomials of degree $\mathbf{d} = (d_1, \ldots, d_n)$ and let η, ν, η' satisfying (29) and the matrix $\beth_{\eta,\nu}(\mathbf{f})$ be as in Definition 5.7. Let $\mathbf{p}$ be the vector*

$$\mathbf{p} := (\underbrace{x_n^{\eta'} \cdot \mathbf{x}^{\alpha(1)}, \ldots, x_n^{\eta'} \cdot \mathbf{x}^{\alpha(N)}}_{|\mathrm{Mon}(\delta-\eta)|}) \tag{35}$$

as in (34). Assume that $\mathcal{H}_d(\nu) \leq \delta - \eta$. *Then for all* $k > 0$ *such that* $\mathcal{H}_d(\nu) \leq k \leq \delta - \eta$, *the pair* $(\mathfrak{Jac}_{\eta,\nu}(\mathbf{f}), \mathbf{p})$ *has the* k*-strong subresultant property with respect to the affine* k*-set* $\mathcal{F}$ *(see Definition 3.9) defined as*

$$\mathcal{F}_{k,\nu} := \{\tilde{\mathbf{f}} \mid \dim(\tilde{\mathcal{I}}) = 0,\ \dim_{\mathbf{k}} \mathbf{k}[\mathbf{x}]^A/\tilde{\mathcal{I}}^A = \deg(\tilde{\mathcal{I}}) = k \ \text{ and } \ \sigma(\tilde{\mathcal{I}}) \leq \nu\}.$$

Here $\tilde{\mathbf{f}} = (\tilde{f}_1, \ldots, \tilde{f}_n) \in \mathbf{k}[\mathbf{x}]^n$ *is a coefficient specialization of* $\mathbf{f}$, $\tilde{\mathcal{I}}$ *is the ideal generated by* $\tilde{f}_1, \ldots, \tilde{f}_n$ *in* $\mathbf{k}[\mathbf{x}]$, $\mathbf{k}[\mathbf{x}]^A = \mathbf{k}[x_1, \ldots, x_{n-1}]$, $\dim(\tilde{\mathcal{I}})$, $\deg(\tilde{\mathcal{I}})$ *and* $\sigma(\tilde{\mathcal{I}})$ *are defined in Definition 5.8.*

The Theorem follows from the following two lemmas:

LEMMA 5.11: *Let* $\mathcal{F}_{k,\nu}$, $\tilde{\mathbf{f}} \in \mathcal{F}_{k,\nu}$ *and* $\tilde{\mathcal{I}} \subset \mathbf{k}[\mathbf{x}]$ *be as in Theorem 5.10. Assume that there exists* $\mathcal{T} \subset \mathrm{Mon}(\delta - \eta)$ *with cardinality* $k := |\mathcal{T}| \leq \delta - \eta$ *such that* $\mathcal{S} := x_n^{\eta'}\mathcal{T}$ *generates* $\mathbf{k}[\mathbf{x}]_\nu/\tilde{\mathcal{I}}_\nu$. *Then there exists a submatrix* $\mathbf{J}'_{\eta,\nu}(\tilde{\mathbf{f}})$ *of* $\mathfrak{Jac}_{\eta,\nu}(\tilde{\mathbf{f}})$ *such that after removing the columns of* $\mathbf{J}'_{\eta,\nu}(\tilde{\mathbf{f}})$ *corresponding to* $\mathcal{T}$, *the resulting matrix is square and have full rank. Moreover, the pair* $(\mathbf{J}'_{\eta,\nu}(\tilde{\mathbf{f}}), \mathbf{p})$ *has the subresultant property with respect to* $\tilde{\mathcal{I}}$, *where* $\mathbf{p}$ *is defined in (35).*

Proof: We use the notation introduced in Definition 5.7. Let $B_1 \subset \bigoplus_{i=1}^n \mathrm{Mon}(\eta - d_i, \eta')^*$ be such that the corresponding columns of $\phi^*_{\eta,\eta'}$ form a basis for its column-space. First we will prove that the columns of $\mathfrak{Jac}_{\eta,\nu}(\tilde{\mathbf{f}})$ corresponding to $\mathrm{Mon}(\delta-\eta) - \mathcal{T} \cup B_1$ are linearly independent. Let $B_2 \subset \mathrm{Mon}(\delta-\eta) - \mathcal{T}$ be such that the columns of $\mathfrak{Jac}_{\eta,\nu}(\tilde{\mathbf{f}})$ corresponding to $B_1 \cup B_2$ form a basis for the space of columns of $\mathfrak{Jac}_{\eta,\nu}(\tilde{\mathbf{f}})$ not corresponding to $\mathcal{T}$. Let $C_2 := \mathrm{Mon}(\delta - \eta) - B_2 - \mathcal{T}$.

It is sufficient to prove that

$$\left(\mathbf{k}\langle\mathcal{S}\rangle \oplus \tilde{\mathcal{I}}_\nu\right) \ \cap \ \mathbf{k}\langle x_n^{\eta'} \cdot C_2\rangle = \{0\}, \tag{36}$$

since it implies that $C_2 = \emptyset$ since $\mathcal{S}$ generates $\mathbf{k}[\mathbf{x}]_\nu/\tilde{\mathcal{I}}_\nu$. To prove (36), assume that $x_n^{\eta'}q(\mathbf{x})$ is an element of the left hand side of (36). Then there exists $r(\mathbf{x}) \in \mathbf{k}\langle\mathrm{Mon}(\delta-\eta)\rangle$ such that

$$x_n^{\eta'}r(\mathbf{x}) = x_n^{\eta'}q(\mathbf{x}) + \sum_{\mathbf{x}^\alpha \in \mathcal{T}} c_\alpha x_n^{\eta'}\mathbf{x}^\alpha \in \tilde{\mathcal{I}}_\nu$$

for some $c_\alpha \in \mathbf{k}$. Then by (35, Proposition 3.2.8) there exists $p(\mathbf{x}) \in \tilde{\mathcal{I}}_{\delta-\eta}$ such that $(p(\mathbf{x}) + r(\mathbf{x}), \mathbf{0})$ are in the image of the map $\Omega_{\eta,\eta'} \oplus \phi^*_{\eta,\eta'}$. Here $\mathbf{0}$ denotes the zero vector in $\bigoplus_{i=1}^n \mathbf{k}\langle\mathrm{Mon}(\eta - d_i, \eta')\rangle^*$. However, $p(\mathbf{x})$ is in the image of the map $\phi_{\delta-\nu}$, therefore the coefficient vector of $(r(\mathbf{x}), \mathbf{0})$ is in the row space of $\mathfrak{Jac}_{\eta,\nu}(\tilde{\mathbf{f}})$. Therefore, the coefficient vector of $(q(\mathbf{x}), \mathbf{0})$ is generated by the rows of $\mathfrak{Jac}_{\eta,\nu}(\tilde{\mathbf{f}})$ with the columns corresponding to $\mathcal{T}$ removed. But this implies that $q(\mathbf{x}) = 0$, since $q(\mathbf{x}) \in \mathbf{k}\langle C_2\rangle$, thus the coefficient vector of $(q(\mathbf{x}), \mathbf{0})$ is zero outside of C_2, so by the definition of C_2 it must be identically zero.

This implies that the submatrix of $\mathfrak{Z}_{\eta,\nu}(\tilde{\mathbf{f}})$ with columns corresponding to $\mathrm{Mon}(\delta-\eta)\cup B_1$ has rank at least $|\mathrm{Mon}(\delta-\eta)|+|B_1|-k$. Thus there exists a subset of rows of cardinality $|\mathrm{Mon}(\delta-\eta)|+|B_1|-k$ which are linearly independent. The resulting matrix, which we denote by $\mathbf{J}'_{\eta,\nu}(\tilde{\mathbf{f}})$, clearly satisfies the first claim of the lemma. To prove the second claim, first note that the assumption that $|\mathcal{T}|\leq\delta-\eta$ implies that condition (2) of the subresultant property is satisfied. We will prove condition (1) similarly as in Proposition 5.6. Since B_1 generates the columns of $\mathfrak{Z}_{\eta,\nu}(\tilde{\mathbf{f}})$ corresponding to $\bigoplus_{i=1}^{n}\mathrm{Mon}(\eta-d_i,\eta')^*$, by Szanto (35, Lemma 3.2.7) we have that $\Omega_{\eta,\eta'}\cdot\mathbf{p}$ (see Definition 5.3) is in the space generated by the columns in B_1 modulo the ideal $\tilde{\mathcal{I}}$. This implies that there exists $a_1,\ldots,a_{|B_1|}$ such that if

$$\mathbf{q}:=(\underbrace{x_n^{\eta'}\cdot\mathbf{x}^{\alpha(1)},\ \ldots,\ x_n^{\eta'}\cdot\mathbf{x}^{\alpha(N)}}_{\mathbf{p}},\underbrace{a_1,\ldots,a_{|B_1|}}_{|B_1|})$$

then the entries of the vector $\mathbf{J}'_{\eta,\nu}(\tilde{\mathbf{f}})\cdot\mathbf{q}$ are in the ideal $\tilde{\mathcal{I}}$. This proves condition (1) of the subresultant property. □

Lemma 5.12: *Let $\mathcal{I}$ be a homogeneous ideal in $\mathbf{k}[x_1,\ldots,x_n]$ and for $\nu\geq 0$ let $\mathcal{I}_\nu$ be the degree ν homogeneous part of $\mathcal{I}$. Assume that all common roots of $\mathcal{I}$ are in the affine subspace defined by $x_n\neq 0$. Define*

$$k:=\deg(\mathcal{I})\quad\text{ and }\quad\nu_0:=\sigma(\mathcal{I}).$$

Then there exists a set of monomials $\mathcal{T}\subset\mathrm{Mon}(k)$ of cardinality k such that $x_n^{\nu-k}\mathcal{T}$ generates $\mathbf{k}[\mathbf{x}]_\nu/\mathcal{I}_\nu$ for all $\nu\geq\max(k,\nu_0)$.

Proof: Let $\{h_1,\ldots,h_N\}$ be a Gröbner basis for $\mathcal{I}$ w.r.t. the graded reverse lexicographic order. Let

$$\mathrm{sat}(\mathcal{I}):=\{f\in\mathbf{k}[\mathbf{x}]\mid\exists m\ \forall i\ \ x_i^m f\in\mathcal{I}\}\tag{37}$$

be the saturation of $\mathcal{I}$, which is equal to $(\mathcal{I}:x_n^\infty)$ (c.f. Eisenbud (16, Exercise 15.40)). Let

$$g_i:=\frac{h_i}{x_n^{m_i}}\quad i=1,\ldots,N,$$

where m_i is the highest power of x_n which divides h_i. Then, by (16, Proposition 15.12), $G:=\{g_1,\ldots,g_N\}$ forms a Gröbner basis for $\mathrm{sat}(\mathcal{I})$. Since all the roots of $\mathcal{I}$ satisfy $x_n\neq 0$, therefore $\deg(\mathrm{sat}(\mathcal{I}))=\deg(\mathcal{I})=k$. This and the fact that the regularity of a saturated ideal is at most its degree implies that

$$\dim\left(\mathbf{k}[\mathbf{x}]_\nu/\mathrm{sat}(\mathcal{I})_\nu\right)=k\ \ \forall\,\nu\geq k.$$

Let $\mathcal{N}$ be the (infinite) set of monomials not in $\langle\mathrm{lt}(G)\rangle$, the polynomials generated by the leading terms of the elements in G. Define $\mathcal{T}\subset\mathrm{Mon}(k)$ to be

$$\mathcal{T}:=\mathcal{N}_k$$

the degree k elements in $\mathcal{N}$. Then by (16, Theorem 15.26) $\mathcal{T}$ forms a basis for $\mathbf{k}[\mathbf{x}]_k/\mathrm{sat}(\mathcal{I})_k$.

Next we prove that $x_n^{\nu-k}\mathcal{T}$ forms a basis for $\mathbf{k}[\mathbf{x}]_\nu/\mathrm{sat}(\mathcal{I})_\nu$ for all $\nu \geq k$. First consider $\nu = k+1$. Let $\mathbf{x}^\alpha \in \mathrm{Mon}(k+1)$. If $x_n|\mathbf{x}^\alpha$, then it is clearly generated by $x_n\mathcal{T}$ modulo $\mathrm{sat}(\mathcal{I})_{k+1}$. Next assume that $x_n \not| \mathbf{x}^\alpha$. Let $\mathcal{T}^A := \mathcal{T}|_{x_n=1}$. Since

$$\dim_{\mathbf{k}} \frac{\mathbf{k}[x_1,\ldots,x_{n-1}]}{\mathrm{sat}(\mathcal{I})^A} = k$$

where $\mathrm{sat}(\mathcal{I})^A$ is generated by the polynomials in $\mathrm{sat}(\mathcal{I})$ after substituting $x_n = 1$, therefore $\mathcal{T}^A$ forms a basis for $\mathbf{k}[\mathbf{x}]^A/\mathrm{sat}(\mathcal{I})^A$. Since $\mathbf{x}^\alpha|_{x_n=1} = \mathbf{x}^\alpha$, we have that

$$\mathbf{x}^\alpha = \sum_{i=1}^N q_i^A g_i^A + \sum_{\mathbf{x}^\beta \in \mathcal{T}} c_\alpha \mathbf{x}^\beta|_{x_n=1}$$

where $\deg(g_i^A q_i^A) \leq |\alpha| = k+1$. Note that since the left hand side only contains a monomial of degree $k+1$, therefore all the monomials on the right hand side which have degree $\leq k$ must add up to 0. Also note that if $q_i^A \neq 0$ then $\deg(g_i) \leq k+1$, otherwise g_i would be divisible by a power of x_n, contrary to its definition. Let $\bar{q}_i$ be the homogenization of q_i^A multiplied by a power of x_n such that $\deg(\bar{q}_i g_i) = k+1$. Then all the terms which are divisible by x_n in

$$\sum_{i=1}^N \bar{q}_i g_i + \sum_{\mathbf{x}^\beta \in \mathcal{T}} c_\alpha x_n \mathbf{x}^\beta$$

must add up to 0. Thus we have that

$$\mathbf{x}^\alpha = \sum_{i=1}^N \bar{q}_i g_i + \sum_{\mathbf{x}^\beta \in \mathcal{T}} c_\alpha x_n \mathbf{x}^\beta,$$

which proves that $x_n\mathcal{T}$ generates $\mathbf{k}[\mathbf{x}]_{k+1}/\mathrm{sat}(\mathcal{I})_{k+1}$. For $\nu > k+1$ we can use induction and the proof is similar.

It remains to prove that $x_n^{\nu-k}\mathcal{T}$ also forms a basis for $\mathbf{k}[\mathbf{x}]_\nu/\mathcal{I}_\nu$ for all $\nu \geq \max(k, \nu_0)$. By our assumptions on $\mathcal{I}$ we have that $\dim \mathbf{k}[\mathbf{x}]_\nu/\mathcal{I}_\nu = k$, and since $\mathcal{I} \subseteq \mathrm{sat}(\mathcal{I})$ we must have that $\mathcal{I}_\nu \subseteq \mathrm{sat}(\mathcal{I})_\nu$. Thus $\mathcal{I}_\nu = \mathrm{sat}(\mathcal{I})_\nu$, and the same is true for their complement in $\mathbf{k}[\mathbf{x}]_\nu$. This concludes the proof. □

6. On affine k-sets and the regularity of Hilbert functions

In Theorem 5.10 we made certain assumptions about the polynomial systems for which the strong subresultant property of Jouanolou's subresultant matrices hold. These included assumptions on the dimension and location of the roots of the system, and on the regularity of its Hilbert function: all of these are in general difficult to verify without the computation of the structure of the factor algebra.

This section, together with the Appendix written by Marc Chardin, are devoted to a discussion on what can be said about the validity of these assumptions without the computation of the structure of the factor algebra. First recall the assumptions we needed in Theorem 5.10.

ASSUMPTION 6.1: *Let* $\mathbf{f} = (f_1, \ldots, f_n) \in \mathbf{k}[x_1, \ldots, x_n]^n$ *be homogeneous polynomials of degrees* $\mathbf{d} = (d_1, \ldots, d_n)$ *and let* $\mathcal{I}$ *be the ideal generated by* $f_1, \ldots, f_n$*. Let* ν, η *be as in Theorem 5.10. We assume that* $\mathbf{f}$ *satisfies the following conditions:*

A1. $\dim(\mathcal{I}) = 0$*, or equivalently the Krull dimension of the ring* $\mathbf{k}[x_1, \ldots, x_n]/\mathcal{I}$ *is* 1*.*

A2. $\mathcal{H}_{\mathbf{d}}(\nu) \leq \dim_{\mathbf{k}} \mathbf{k}[x_1, \ldots, x_{n-1}]/\mathcal{I}^A = \deg(\mathcal{I}) \leq \delta - \eta$*.*

A3. $\sigma(\mathcal{I}) \leq \nu$*.*

In the first part of this section we discuss assumptions A1 and A2 which are related to the dimension, cardinality and location of the common roots of $\mathbf{f}$. Considering assumption A3, as we mentioned earlier, the paper contains an Appendix, written by Marc Chardin, which proves upper bounds for the regularity of the Hilbert function using the fact that the system is "almost complete intersection", i.e. that there is only one extra polynomial to make the system over-constrained. In the second part of this section we relate the results of Marc Chardin on the regularity of the Hilbert function of I to the subresultant method.

Polynomial systems that satisfy assumptions A1 and A2 have a set of projective roots that is finite, non-empty and is in the affine space defined by $x_n \neq 0$. Unfortunately, these properties are often not inherited from the affine system to its homogenization: even if the affine system is zero dimensional, it often has common roots at infinity, and sometimes components with higher dimension. For example, the ideal generated by $\{x_1^3 - x_1, x_2 - x_1^2, x_3 - x_1^2\}$ is zero dimensional, but its homogenization by x_4 contains the projective line $(0 : 1 : t : 0)$ at infinity. (For more on computing the ideal defining the projective closure of an affine variety, see Eisenbud (16, Chapter 15).) The following notes are practical ways to handle the situation when assumptions A1 and A2 are not satisfied.

1. If $(f_1, \ldots, f_n)$ defines a zero dimensional projective variety, then there is a simple way to check whether it has roots at infinity: Let $g_1, \ldots, g_{n-1} \in \mathbf{k}[x_1, \ldots, x_n]$ and define

$$\overline{g}_i(x_1, \ldots, x_{n-1}) := g_i(x_1, \ldots, x_{n-1}, 0) \quad i = 1, \ldots, n-1.$$

Then

$$\mathrm{Res}(\overline{g}_1, \ldots, \overline{g}_{n-1}) \neq 0$$

if and only $g_1, \ldots, g_{n-1}$ has no common roots at infinity (i.e. at $x_n = 0$) (c.f. Cox *et al.* (11, Chapter 3, Theorem 3.4)). Here the resultant is taken with respect to the variables $x_1, \ldots, x_{n-1}$. From our n polynomials $(f_1, \ldots, f_n)$

to get $n-1$, we can form $n-1$ generic or random linear combinations $g_1, \ldots, g_{n-1}$ out of $f_1, \ldots, f_n$. (More precisely, either introduce $n(n-1)$ parameter values for the coefficients of the linear combinations, or use random integer coefficients.) This gives a deterministic or a randomized algorithm to check the condition A2 in Assumption 6.1.

2. If $(f_1, \ldots, f_n)$ defines a zero dimensional projective variety, then a random homogenous linear change of variables will turn all roots so that $x_n \neq 0$ with high probability.

3. For polynomial systems having positive dimensional components at infinity the straightforward application of resultant and subresultant based methods will not work. However, to find the isolated roots of a well-constrained system with higher dimensional components, the so called "generalized characteristic polynomials" method (see Canny (5)) extends the u-resultant method to handle this case. In this paper we do not consider the possible extension of the subresultant method to solve over-constrained systems with positive dimensional components.

We finish the paper by investigating on the regularity of the Hilbert function of $\mathcal{I}$. The following list contains facts and related results which might help to predict whether Assumption 6.1(3) is satisfied.

1. Assume that $(f_1, \ldots, f_n) \in \mathbf{k}[\mathbf{x}]^n$ is homogeneous of degree $(d_1, \ldots, d_n)$, and that $\dim(\mathcal{I}) = 0$ where $\mathcal{I}$ is the ideal generated by $f_1, \ldots, f_n$. Then the regularity of the Hilbert function of $\mathcal{I}$ in the worst case is at most δ (c.f. Appendix, Corollary 7.12). This implies that in the worst case we can use Jouanolou's subresultant matrices in degree δ: for all $1 \leq k \leq \delta - \eta$, $\beth_{\delta,\eta}$ has the k-strong subresultant property with respect to all systems satisfying assumptions A1 and A2. However, in many cases we have a priori knowledge about the regularity of the Hilbert function being smaller than in the worst case.

2. If the ideal $\mathcal{I}$ is saturated, i.e. $\mathrm{sat}(\mathcal{I}) = \mathcal{I}$ where $\mathrm{sat}(\mathcal{I})$ was defined in (37), then, as we mentioned earlier, $\sigma(\mathcal{I}) \leq \deg(\mathcal{I}) - 1$. Note that using Assumption 6.1(A2) and (29) we get that $\deg(\mathcal{I}) \leq \delta - \eta \leq \nu$, therefore assumption (3) is always satisfied for saturated ideals.

   Computing the saturation of an ideal, or its degree d components might require the computation of Gröbner bases (see Eisenbud (16, Chapter 15.10)), or the computation of H-bases originally introduced by Macaulay (see Möller and Sauer (31)). However, using Gröbner bases or H-bases one could directly compute the common roots.

3. Corollary 7.5 of the Appendix implies that if, in addition to Assumptions (A1) and (A2), we also have that the projective variety defined by $\mathcal{I}$ is not contained by any degree $\delta - \nu$ hypersurface, then ν is an upper bound for $\sigma(\mathcal{I})$, i.e. Assumption (A3) is also satisfied.

4. According Remark 7.8 of the Appendix, one of the equivalent conditions of Corollary 7.7 together with Assumptions (A1) and (A2) implies that the degree ν subresultant $\Gamma_{\mathcal{T}}^{\eta,\nu}(\mathbf{f})$ corresponding to the monomial set $\mathcal{T} := \{x_n^{2\nu-\delta}\mathbf{x}^\alpha \,:\, |\alpha| = \delta-\nu\}$ is not zero. This implies that the degree ν Jouanolou subresultant matrix $\mathbf{J}_{\eta,\nu}(\mathbf{f})$ have the subresultant property with respect to $\mathcal{I}$, unless the extraneous factor $\det(\mathbf{E}_{\delta-\eta})\det(\mathbf{E}_{\eta,\eta'})$ is zero at $\mathbf{f}$.

References

[1] Auzinger, W., Stetter, H. (1988). An elimination algorithm for the computation of all zeros of a system of multivariate polynomial equations. In *Proc. Intern. Conf. on Numerical Math., Intern. Series of Numerical Math., 86*, pages 12–30. Birkhauser Verlag, Basel.

[2] Bostan, A., Salvy, B., Schost, E. (2002). Fast algorithms for zero-dimensional polynomial systems using duality.

[3] Busé, L., D'Andrea, C. (2004). Inversion of parameterized hypersurfaces by means of subresultants. In *Proceedings of the 2004 international symposium on Symbolic and algebraic computation*, pages 65–71. ACM Press.

[4] Busé, L., D'Andrea, C. (2004). On the irreducibility of multivariate subresultants. *C. R., Math., Acad. Sci. Paris*, 338(4):287–290.

[5] Canny, J. (1989). Generalized characteristic polynomials. In *Symbolic and algebraic computation (Rome, 1988)*, volume 358 of *Lecture Notes in Comput. Sci.*, pages 293–299. Springer, Berlin.

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

[7] Chardin, M. (1994). Formules à la Macaulay pour les sous-résultants en plusiurs variables et application au d'un résultant réduit. *Comptes rendus de l Academie des Sciences serie I-Mathematique*, 319(5):433–436. French.

[8] Chardin, M. (1995). Multivariate subresultants. *Journal of Pure and Applied Algebra*, 101:129–138.

[9] Collins, G. E. (1967). Subresultants and reduced polynomial remainder sequences. *Journal of the ACM*, 14(1):128–142.

[10] Corless, R. M., Gianni, P. M., Trager, B. M., Watt, S. M. (1995). The singular value decomposition for polynomial systems. In *Proceedings of the International Symposium on Symbolic and Algebraic Computation*, pages 195–207.

[11] Cox, D., Little, J., O'Shea, D. (1998). *Using Algebraic Geometry*. Graduate Texts in Mathematics, 185. Springer-Verlag.

[12] D'Andrea, C., Dickenstein, A. (2001). Explicit formulas for the multivariate resultant. In *Proceedings of MEGA 2000, Special Issue of the Journal of Pure and Applied Algebra*, volume 164, pages 59–86.

[13] D'Andrea, C., Emiris, I. Z. (2002). Hybrid sparse resultant matrices for bivariate polynomials. *J. Symbolic Comput.*, 33(5):587–608. Computer algebra (London, ON, 2001).

[14] D'Andrea, C., Jeronimo, G. (2004). Subresultants and generic monomial bases. Revised version accepted for publication in the Journal of Symbolic Computation.

[15] Díaz-Toca, G. M., González-Vega, L. (2001). An explicit description for the triangular decomposition of a zero-dimensional ideal through trace computations. In Green, E. L., Hosten, S., Laubenbacher, R. C., Powers, V. A., editors, *Symbolic Computation: Solving Equations in Algebra, Geometry, and Engineering*. American Mathematical Society.

[16] Eisenbud, D. (1999). *Commutative algebra with a view toward algebraic geometry*. Springer.

[17] Emiris, I. Z., Pan, V. Y. (2002). Symbolic and numeric methods for exploiting structure in constructing resultant matrices. *J. Symbolic Comput.*, 33(4):393–413.

[18] Gelfand, I. M., Kapranov, M. M., Zelevinsky, A. V. (1994). *Discriminants, Resultants and Multidimensional Determinants*. Birkhäuser.

[19] González-Vega, L. (1991a). Determinantal formulae for the solution set of zero-dimensional ideals. *Journal of Pure and Applied Algebra*, 76:57–80.

[20] González-Vega, L. (1991b). A subresultant theory for multivariate polynomials. In *ISSAC '91*, pages 79–85. ACM Press.

[21] González-Vega, L. (2002). Dealing with approximate geometric problems with a symbolic-numeric approach. Invited lectures at the SCA (Symbolic and Computational Algebra) Conference held in London (Canada). `http://frisco.matesco.unican.es/~gvega/ficheros/SCA.pdf`.

[22] Habicht, V. W. (1948). Zur inhomogenen Eliminationstheorie. *Comment. Math. Helv.*, 21:79–98.

[23] Jeronimo, G., Krick, T., Sabia, J., Sombra, M. (2004). The computational complexity of the Chow form. *Found. Comput. Math.*, 4(1):41 –117.

[24] Jónsson, G., Vavasis, S. A. (2001). Accurate solution of polynomial equations using macaulay resultant matrices. `citeseer.nj.nec.com/424677.html`.

[25] Jouanolou, J.-P. (1980). Idéaux résultants. *Advances in Mathematics*, 37(3):212–238.

[26] Jouanolou, J.-P. (1991). Le formalisme du résultants. *Advances in Mathematics*, 90(2):117–243.

[27] Jouanolou, J. P. (1997). Formes d'inertie et résultant: un formulaire. *Adv. Math.*, 126(2):119–250.

[28] Khetan, A. (2003). The resultant of an unmixed bivariate system. *J. Symbolic Comput.*, 36(3-4):425–442. International Symposium on Symbolic and Algebraic Computation (ISSAC'2002) (Lille).

[29] Lazard, D. (1977). Algèbre linééaire sur $k[x_1, \cdots, x_n]$, et élimination. (French). *Bull. Soc. Math. France*, 105(2):165–190.

[30] Manocha, D., Demmel, J. (1995). Algorithms for intersecting parametric and algebraic curves ii: multiple intersections. *Graphical Models and Image Processing*, 57(2):81–100.

[31] Möller, H. M., Sauer, T. (2000). H-bases for polynomial interpolation and system solving. *Adv. Comput. Math.*, 12(4):335–362. Multivariate polynomial interpolation.

[32] Möller, H. M., Stetter, H. J. (1995). Multivariate polynomial equations with multiple zeros solved by matrix eigenproblems. *Numer. Math.*, 70(3):311–329.

[33] Mourrain, B. (1998). Computing the isolated roots by matrix methods. *J. Symbolic Comput.*, 26(6):715–738. Symbolic numeric algebra for polynomials.

[34] Mourrain, B. (1999). A new criterion for normal form algorithms. In *Applied algebra, algebraic algorithms and error-correcting codes (Honolulu, HI, 1999)*, volume 1719 of *Lecture Notes in Comput. Sci.*, pages 430–443. Springer, Berlin.

[35] Szanto, A. (2001). Multivariate subresultants using Jouanolou's resultant matrices. Accepted in the Journal of Pure and Applied Algebra.

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

7. Appendix: Castelnuovo-Mumford regularity of an almost complete intersection of dimension 1

by Marc Chardin

We give in this appendix a short account on the behavior of some invariants of an ideal of codimension $n-1$ in a polynomial ring in n variables over a field. We

study in particular the Castelnuovo-Mumford regularity of such an ideal, give some results on its Hilbert function or the one of its saturation. These results can be easily derived from more general results on this subject (see e.g. (CEU, 2.3) or (Ch, 5.8)).

Let $R := k[X_1, \ldots, X_n]$ be a polynomial ring in n variables over a field, with $n \geq 2$, $f := (f_1, \ldots, f_n)$ be a n-tuple of forms of degrees $d_1 \geq \cdots \geq d_n$, I be the ideal generated by the f_i's and J its saturation with respect to the ideal $\mathfrak{m} := (X_1, \ldots, X_n)$. Set $A := R/I$, $B := R/J$, $F := J/I = H^0_{\mathfrak{m}}(A)$, $\sigma := \sum_{i=1}^n d_i$ and $\delta := \sigma - n$.

Let $\mathcal{H}_P$ denotes the Hilbert function of a graded R-module P.

In this appendix we will assume that $\dim A = 1$ (equivalently $\dim B = 1$).

The Castelnuovo-Mumford regularity of a finitely generated graded R-module M can be defined in the following way using the local cohomology modules with support in $\mathfrak{m}$:

$$\operatorname{reg}(M) := \min\{\mu \mid H^i_{\mathfrak{m}}(M)_{\nu-i} = 0,\ \forall \nu > \mu, \forall i\}.$$

It can also be defined in terms of a minimal free R-resolution of M, or in terms of the initial degrees of the modules $\operatorname{Ext}^i_R(M, R)$ (see e.g. (Ei, 20.5)), from which it follows that $\operatorname{reg}(M) \geq \operatorname{indeg}(M)$. (The initial degree of a module M, denoted by $\operatorname{indeg}(M)$, is the infimum of the degrees of its non zero elements.)

We refer the reader to (BH) for standard facts on local cohomology, Koszul complexes, canonical modules, Hilbert series, etc.

Recall that, for $\nu \gg 0$, one has $\mathcal{H}_A(\nu) = \mathcal{H}_B(\nu) = \deg X$, where $X := \operatorname{Proj}(A) = \operatorname{Proj}(B)$ is the zero dimensional scheme defined by A (equivalently by B).

PROPOSITION 7.1: *For any $\nu \in \mathbf{Z}$,*
(i) $\mathcal{H}_A(\nu) = \mathcal{H}_B(\nu) + \mathcal{H}_F(\nu)$,
(ii) $\mathcal{H}_B(\nu) = \deg X - \mathcal{H}_{H^1_{\mathfrak{m}}(B)}(\nu)$,
(iii) $\mathcal{H}_{H^1_{\mathfrak{m}}(B)}(\nu) = \mathcal{H}_{\omega_B}(-\nu)$.

Proof. (i) follows from the graded exact sequence $0 \to F \to A \to B \to 0$, (ii) follows from (BH, 4.3.5) and (iii) from (BH, 3.6.19). □

Let K be the Koszul complex $K_\bullet(f; R)$ with its usual grading ($K_0 = R$, $K_n = R[-\sigma]$) and H_i be its i-th homology group.

Denote by $P_Q \in \mathbf{Z}[t^{-1}][[t]]$ the Hilbert Poincaré series of a finitely generated graded R-module Q: $P_Q(t) := \sum_{\nu \in \mathbf{Z}} \mathcal{H}_Q(\nu) t^\nu$.

PROPOSITION 7.2: *(i)* $H_i = 0$ *for* $i \neq 0, 1$,
(ii) $H_0 = A$ *and* $H_1 \simeq \operatorname{Ext}^{n-1}_R(A, R)[\sigma] \simeq \operatorname{Ext}^{n-1}_R(B, R)[\sigma] \simeq \omega_B[\delta]$,
(iii) $\sum_i (-i)^i P_{H_i}(t) = \sum_i (-i)^i P_{K_i}(t) = \prod_{i=1}^n (1 + t + \cdots + t^{d_i - 1}) = \sum_\nu \mathcal{H}_d(\nu) t^\nu$.

Proof. (i) and (ii) follows from (BH, 1.6.16, 1.6.9, 1.6.10, 3.6.12 and 3.6.14), and the fact that the canonical onto map $A \to B$ induces an isomorphism $\mathrm{Ext}_R^{n-1}(A,R) \simeq \mathrm{Ext}_R^{n-1}(B,R)$. In (iii), the first equality is standard and easy and the second is a classical exercise. □

PROPOSITION 7.3: *For any* $\nu \in \mathbf{Z}$, $\mathcal{H}_A(\nu) = \mathcal{H}_d(\nu) + \deg X - \mathcal{H}_B(\delta - \nu)$. *Therefore the following are equivalent :*
(i) $\mathcal{H}_A(\nu) = \mathcal{H}_d(\nu)$,
(ii) $\nu \leq \delta - \mathrm{reg}(B)$.

Proof. $\mathcal{H}_A(\nu) = \mathcal{H}_d(\nu) + \mathcal{H}_{H_1}(\nu) = \mathcal{H}_d(\nu) + \mathcal{H}_{\omega_B}(\nu - \delta)$ by Proposition 7.2. This proves the first claim together with Proposition 7.1 (ii) and (iii).

For the equivalence of (i) and (ii) recall that as $H^i_{\mathfrak{m}}(B) = 0$ for $i \neq 1$ and the Hilbert function of B strictly increases from 1 in degree 0 until it reaches $\deg(X)$, $\mathrm{reg}(B) = \min\{\mu \mid \mathcal{H}_B(\mu) = \deg(X)\}$ by Proposition 7.1 (ii). □

COROLLARY 7.4: $\mathcal{H}_F(\nu) = \mathcal{H}_F(\delta - \nu)$ *for any* ν. *Therefore,*

$$\mathrm{reg}(A) = \max\{\mathrm{reg}(B), \delta - \mathrm{indeg}(J/I)\}.$$

Proof. The first claim follows from Proposition 7.3 and Proposition 7.1 (i), using that $\mathcal{H}_d(\nu) = \mathcal{H}_d(\delta - \nu)$, which for instance follows from Proposition 7.2 (iii). To conclude, recall that $F = J/I = H^0_{\mathfrak{m}}(A)$ and $\mathrm{reg}(A) = \max\{\mathrm{reg}(B), \mathrm{end}(F)\}$. The symmetry $\mathcal{H}_F(\nu) = \mathcal{H}_F(\delta - \nu)$ shows that $\mathrm{end}(F) = \delta - \mathrm{indeg}(F)$. □

COROLLARY 7.5: *The following are equivalent :*
(i) $\mathcal{H}_A(\nu) = \mathcal{H}_B(\nu) = \deg X$,
(ii) either $\nu > \delta - \mathrm{indeg}(J)$ *or* $\nu < \mathrm{indeg}(J)$ *and* $\deg X = \binom{\nu+n-1}{n-1}$.

PROPOSITION 7.6: $\min\{\nu \mid \mathcal{H}_B(\nu) = \deg X\} = \mathrm{reg}(B) = \mathrm{reg}(J) - 1 \geq \mathrm{indeg}(J) - 1$.

Proof. The first equality follows from Proposition 7.1 (ii) as B is Cohen-Macaulay of dimension 1, the second is due to the equality $B = R/J$ and the third is evident. □

Notice that if $\nu < \mathrm{indeg}(J) \leq \mathrm{indeg}(I)$ then $A_\nu = B_\nu = R_\nu$, and therefore $\mathcal{H}_A(\nu) = \mathcal{H}_B(\nu) = \mathcal{H}_d(\nu)$.

COROLLARY 7.7: *Let* $\nu \geq \mathrm{indeg}(J)$. *The following are equivalent :*
(i) $\mathcal{H}_A(\nu) = \mathcal{H}_B(\nu) = \mathcal{H}_d(\nu) = \deg X$,
(ii) $\nu = \delta - \mathrm{indeg}(J) + 1$ *and* $\deg X = \binom{\mathrm{indeg}(J)+n-2}{n-1}$,
(iii) X is a scheme of degree $\mathcal{H}_R(\mu)$ *not contained in a hypersurface of degree* μ, *for some* $\mu < \mathrm{indeg}(I)$ *and* $\nu = \delta - \mu$.

Proof. If (i) holds, then $\nu > \delta - \mathrm{indeg}(J)$, by Corollary 7.5 and $\nu \leq \delta - \mathrm{reg}(B)$ by Proposition 7.3, this shows (ii) in view of Proposition 7.6.

Clearly (ii) implies (iii) with $\mu := \mathrm{indeg}(J) - 1$. On the other hand if $\deg(X) = \mathcal{H}_R(\mu)$ then $\mathrm{indeg}(J) \leq \mu + 1$ as $\mathcal{H}_B(\mu+1) \leq \deg(X) = \mathcal{H}_R(\mu) < \mathcal{H}_R(\mu+1)$, hence $\mu = \mathrm{indeg}(J) - 1$ if X is not contained in a hypersurface of degree μ, which shows (ii).

Notice that

$$\mathcal{H}_d(\delta - \nu) = \mathcal{H}_R(\mathrm{indeg}(J) - 1) = \mathcal{H}_B(\mathrm{indeg}(J) - 1) = \binom{\mathrm{indeg}(J) + n - 2}{n-1}.$$

If (ii) holds, then $\mathrm{reg}(B) = \mathrm{indeg}(J) - 1$ by Proposition 7.6, this implies (i) in view of Proposition 7.3 and Proposition 7.5. □

Remark 7.8: *If one of the equivalent conditions of Corollary 7.7 holds, for instance if (iii) holds, notice that if X does not meet the hyperplane $X_i = 0$, then X_i is a non zero divisor on B, hence the monomials $X_i^{\nu-\mu} X^\alpha$ with $|\alpha| = \mu$ form a basis of B_ν for all $\nu \geq \mu$. As $A_{\delta-\mu} \simeq B_{\delta-\mu}$, it follows that the subresultant associated to this collection of monomials in degree $\delta - \mu$ is not 0.*

Proposition 7.9: *Let $\mathfrak{b} := (g_1, \ldots, g_{n-1})$ be a complete intersection ideal contained in J. Then* $\mathrm{reg}(B) = \sum_{i=1}^{n-1} (\deg(g_i) - 1) - \mathrm{indeg}((\mathfrak{b} : J)/\mathfrak{b})$.

Proof. Set $\sigma' := \sum_{i=1}^{n-1} \deg(g_i)$. One has graded degree zero isomorphisms

$$(\mathfrak{b} : J)/\mathfrak{b} \simeq \mathrm{Hom}_B(R/J, R/\mathfrak{b}) \simeq \mathrm{Hom}_B(R/J, \omega_{R/\mathfrak{b}}[n - \sigma']) \simeq \omega_{R/J}[n - \sigma']$$

hence $\mathrm{indeg}((\mathfrak{b} : J)/\mathfrak{b}) = \mathrm{indeg}(\omega_{R/J}) - n + \sigma' = -\mathrm{end}(H^1_{\mathfrak{m}}(B)) - n + \sigma' = -\mathrm{reg}(B) + 1 - n + \sigma'$. The claim follows. □

Lemma 7.10: *Assume k is infinite. If $f_n \neq 0$, then the ideal I contains a complete intersection ideal of codimension $n-1$ defined by forms of degrees $d_n, d_1, \ldots, d_{n-2}$.*

Proof. The element f_n is a not a zero divisor on R. One then construct by induction a regular sequence $f_n, g_1, \ldots, g_i$ with $g_i = f_i + \sum_{j>i} a_{ij} f_j$ homogeneous not in any associated prime of $J_i := (f_n, g_1, \ldots, g_{i-1})$, for $i \leq n-2$, using that a complete intersection ideal is unmixed, so that the associated prime of J_i are all of codimension i. □

Corollary 7.11: *One has*

$$\mathrm{reg}(B) \leq \delta - d_{n-1}$$

unless $J = I$ is a complete intersection ideal and $\deg X = d_1 \cdots d_{n-2} d_n$, *in which case* $\mathrm{reg}(B) = \delta - d_{n-1} + 1$.

Proof. We may assume that k is infinite. It the follows from Proposition 7.9 in view of Lemma 7.10. □

COROLLARY 7.12: *Assume that I is a complete intersection ideal defined by forms of degrees $d_1, \ldots, d_{n-2}, d_n$. Then $\mathcal{H}_B(\nu) = \deg X$ for any $\nu \geq \delta - d_{n-1}$ and*

$$\operatorname{reg}(A) \leq \delta - \min\{d_{n-1}, \operatorname{indeg}(J/I)\}.$$

Moreover, equality holds if $\operatorname{indeg}(J/I) \leq d_{n-1}$.

Proof. This follows from Corollary 7.4 and Proposition 7.6 in view of Corollary 7.11. □

References

[BH] Bruns, Winfried; Herzog, Jürgen. *Cohen Macaulay rings.* Cambridge Studies in Advanced Mathematics, 39. Cambridge University Press, Cambridge, 1993.

[Ch] Chardin, Marc. Regularity of ideals and their powers. Prépublication 364, Insitut de Mathématiques de Jussieu, Mars 2004.

[CEU] Chardin, Marc; Eisenbud, David; Ulrich, Bernd. Hilbert functions, residual intersections, and residually S_2 ideals. Compositio Math. 125 (2001), no. 2, 193–219.

[Ei] Eisenbud, David. *Commutative algebra. With a view toward algebraic geometry.* Graduate Texts in Mathematics, 150. Springer-Verlag, New York, 1995.