Linear Algebra and its Applications 438 (2013) 1969–1989

Contents lists available at SciVerse ScienceDirect

Linear Algebra and its Applications

journal homepage: www.elsevier.com/locate/laa

Subresultants in multiple roots ☆

Carlos D'Andrea [a,*], Teresa Krick [b], Agnes Szanto [c]

[a] Universitat de Barcelona, Departament d'Àlgebra i Geometria, Gran Via 585, 08007 Barcelona, Spain
[b] Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires and IMAS, CONICET, Argentina
[c] Department of Mathematics, North Carolina State University, Raleigh, NC 27695, USA

ARTICLE INFO

Article history:
Received 21 December 2010
Accepted 5 November 2012
Available online 8 December 2012

Submitted by J. Queiro

Keywords:
subresultants
Sylvester sums
root multiplicity
Hermite interpolation

ABSTRACT

We extend our previous work on Poisson-like formulas for subresultants in roots to the case of polynomials with multiple roots in both the univariate and multivariate case, and also explore some closed formulas in roots for univariate polynomials in this multiple roots setting.

1. Introduction

In [8] we presented Poisson-like formulas for multivariate subresultants in terms of the roots of the system given by all but one of the input polynomials, provided that all the roots were *simple*, i.e. that the ideal generated by these polynomials is zero-dimensional and radical. Multivariate resultants were mainly introduced by Macaulay in [21], after earlier work by Euler, Sylvester and Cayley, while multivariate subresultants were first defined by González-Vega in [13,14], generalizing Habicht's method [16]. The notion of subresultants that we use in this text was introduced by Chardin in [5].

Later on, in [10,11], we focused on the classical univariate case and reworked the relation between subresultants and double Sylvester sums, always in the simple roots case (where double sums are actually well-defined). This is also the subject of the more recent articles [24,20]. As one of the referees

☆ Carlos D'Andrea is partially supported by the Research Project MTM2007-67493, Teresa Krick was partially supported by ANPCyT PICT 33671/05, CONICET PIP 2010-2012 and UBACyT Grants, and Agnes Szanto was partially supported by NSF Grants CCR-0347506 and CCF-1217557.

* Corresponding author.
E-mail addresses: cdandrea@ub.edu (C. D'Andrea), krick@dm.uba.ar (T. Krick), aszanto@ncsu.edu (A. Szanto).
URLs: http://atlas.mat.ub.es/personals/dandrea (C. D'Andrea), http://mate.dm.uba.ar/~krick (T. Krick), http://www4.ncsu.edu/~aszanto (A. Szanto).

http://dx.doi.org/10.1016/j.laa.2012.11.004

of the MEGA'2007 conference pointed out to us, working out these results for the case of polynomials with multiple roots would also be interesting.

This paper is a first attempt in that direction. We succeed in describing Poisson like formulas for univariate and multivariate subresultants in the presence of multiple roots, as well as to obtain formulas in roots in the univariate setting for subresultants of degree 1 and of degree immediately below the minimum of the degrees of the input polynomials: the two non-trivial extremal cases in the sequence of subresultants. We cannot generalize these formulas for other intermediate degrees, and it is still not clear for us which is the correct way of generalizing Sylvester double sums in the multiple roots case.

The paper is organized as follows: In Section 2 we recall the definitions of the classical univariate subresultants and Sylvester double sums, and of the generalized Wronskian and Vandermonde matrices. We then show how the Poisson formulas obtained in [17] for the subresultants in the case of simple roots extend to the multiple roots setting by means of these generalized matrices. We also obtain formulas in roots for subresultants in the two extremal non-trivial cases mentioned above. In Section 3 we present Poisson-like formulas for multivariate subresultants in the case of multiple roots, generalizing our previous results described in [8].

2. Univariate case: subresultants in multiple roots

2.1. Notation

We first establish a notation that will make the presentation of the problem and the state of the art simpler.

Set $d, e \in \mathbb{N}$ and let $A := (\alpha_1, \dots, \alpha_d)$ and $B := (\beta_1, \dots, \beta_e)$ be two (ordered) sets of d and e different indeterminates respectively.

For $m, n \in \mathbb{N}$, set $(d_1, \dots, d_m) \in \mathbb{N}^m$ and $(e_1, \dots, e_n) \in \mathbb{N}^n$ such that $d_1 + \cdots + d_m = d$ and $e_1 + \cdots + e_n = e$, and let

$$\overline{A} := \big((\alpha_1, d_1); \dots; (\alpha_m, d_m)\big) \quad \text{and} \quad \overline{B} := \big((\beta_1, e_1); \dots; (\beta_n, e_n)\big)$$

(these will be regarded as "limit sets" of A and B when roots are packed following the corresponding multiplicity patterns).

We associate to A and B the monic polynomials f and g of degrees d and e respectively, and the set $R(A, B)$, where

$$\begin{aligned} f(x) &:= \prod_{i=1}^{d}(x - \alpha_i) \quad \text{and} \quad g(x) := \prod_{j=1}^{e}(x - \beta_j), \\ R(A, B) &= \prod_{1 \leqslant i \leqslant d, 1 \leqslant j \leqslant e}(\alpha_i - \beta_j), = \prod_{1 \leqslant i \leqslant d} g(\alpha_i) \end{aligned}$$

with natural limits when the roots are packed

$$\begin{aligned} \overline{f}(x) &:= \prod_{i=1}^{m}(x - \alpha_i)^{d_i} \quad \text{and} \quad \overline{g}(x) := \prod_{j=1}^{n}(x - \beta_j)^{e_j}, \\ R(\overline{A}, \overline{B}) &= \prod_{1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n}(\alpha_i - \beta_j)^{d_i e_j} = \prod_{1 \leqslant i \leqslant m} \overline{g}(\alpha_i)^{d_i}. \end{aligned}$$

2.2. Subresultants and Sylvester double sums

We recall that for $0 \leqslant t \leqslant d < e$ or $0 \leqslant t < d = e$, the t-th subresultant of the polynomials $f = a_d x^d + \cdots + a_0$ and $g = b_e x^e + \cdots + b_0$, introduced by Sylvester in [26], is defined as

$$
\operatorname{Sres}_t(f,g) := \det \begin{array}{c} d+e-2t \\ \left|\begin{array}{cccccc} a_d & \cdots & \cdots & a_{t+1-(e-t-1)} & x^{e-t-1}f(x) \\ & \ddots & & \vdots & \vdots \\ & & a_d \; \cdots & a_{t+1} & x^0 f(x) \\ \hline b_e & \cdots & \cdots & b_{t+1-(d-t-1)} & x^{d-t-1}g(x) \\ & \ddots & & \vdots & \vdots \\ & & b_e \; \cdots & b_{t+1} & x^0 g(x) \end{array}\right| \end{array} \begin{array}{l} \\ e-t \\ \\ \\ d-t \\ \\ \end{array}
$$

with $a_\ell = b_\ell = 0$ for $\ell < 0$. When $t = 0$ we have $\operatorname{Sres}_t(f,g) = \operatorname{Res}(f,g)$.

In the same article Sylvester also introduced for $0 \leqslant p \leqslant d$, $0 \leqslant q \leqslant e$ the following *double-sum* expression in A and B,

$$
\operatorname{Sylv}^{p,q}(A,B;x) := \sum_{\substack{A' \subset A,\, B' \subset B \\ |A'|=p,\, |B'|=q}} R(x,A')\,R(x,B')\,\frac{R(A',B')\,R(A\backslash A',B\backslash B')}{R(A',A\backslash A')\,R(B',B\backslash B')},
$$

where by convention $R(A',B') = 1$ if $A' = \emptyset$ or $B' = \emptyset$. For instance

$$
\operatorname{Sylv}^{0,0}(A,B;x) = R(A,B) = \prod_{1\leqslant i\leqslant d,1\leqslant j\leqslant e} (\alpha_i - \beta_j) = \operatorname{Res}(f,g). \tag{1}
$$

We note that $\operatorname{Sylv}^{p,q}(A,B;x)$ only makes sense when $\alpha_i \neq \alpha_j$ and $\beta_i \neq \beta_j$ for $i \neq j$, since otherwise some denominators in $\operatorname{Sylv}^{p,q}(A,B;x)$ would vanish.

The following relation between these double sums and the subresultants (for monic polynomials with simple roots f and g) was described by Sylvester: for any choice of $0 \leqslant p \leqslant d$ and $0 \leqslant q \leqslant e$ such that $t := p + q$ satisfies $t < d \leqslant e$ or $t = d < e$, one has

$$
\operatorname{Sres}_t(f,g) = (-1)^{p(d-t)} \binom{t}{p}^{-1} \operatorname{Sylv}^{p,q}(A,B;x). \tag{2}
$$

This gives an expression for the subresultant in terms of the differences of the roots—generalizing the well-known formula (1)—*in case f and g have only simple roots*. However, when the roots are packed, i.e. when we deal with $\overline{A}$ and $\overline{B}$, the expression for the resultant is stable, i.e.

$$
\operatorname{Res}(\overline{f},\overline{g}) = \prod_{1\leqslant i\leqslant m,\, 1\leqslant j\leqslant n} (\alpha_i - \beta_j)^{d_i e_j},
$$

while not only there is no simple expression of what $\operatorname{Sres}_t(\overline{f},\overline{g})$ is in terms of differences of roots but moreover there is no simple definition of what $\operatorname{Sylv}^{p,q}(\overline{A},\overline{B};x)$ should be in order to preserve Identity (2). Of course, since $\operatorname{Sres}_t(\overline{f},\overline{g})$ is defined anyway, $\operatorname{Sylv}^{p,q}(\overline{A},\overline{B};x)$ could be defined as the result

$$
\operatorname{Sylv}^{p,q}(\overline{A},\overline{B};x) := (-1)^{p(d-t)} \binom{t}{p} \operatorname{Sres}_t(\overline{f},\overline{g})
$$

but this is not quite satisfactory because on one hand this does not clarify how Sres_t behaves in terms of the roots when these are packed, and on the other hand, $\mathrm{Sylv}^{p,q}(\overline{A}, \overline{B}; x)$ is defined for every $0 \leqslant p \leqslant d$ and $0 \leqslant q \leqslant e$ while Sres_t is only defined for $t := p + q \leqslant \min\{d, e\}$.

In what follows, we express some particular cases of the subresultant of two univariate polynomials in terms of the roots of the polynomials, when these polynomials have multiple roots. These are partial answers to the questions raised above, since we were not able to give a right expression for what the Sylvester double sums should be, even in the particular cases we could consider. Nevertheless the results we obtained give a hint of how complex it can be to give complete general answers, at least in terms of double or multiple sums, see Theorem 2.7 below.

2.3. Generalized Vandermonde and Wronskian matrices

We need to recall some facts on generalized Vandermonde and Wronskian matrices.

Notation 2.1. Set $u \in \mathbb{N}$. The *generalized Vandermonde* or *confluent* (non-necessarily square) $u \times d$ matrix $V_u(\overline{A})$ associated to $\overline{A} = ((\alpha_1, d_1); \ldots; (\alpha_m, d_m))$, [18], is

$$V_u(\overline{A}) = V_u\big((\alpha_1, d_1); \ldots; (\alpha_m, d_m)\big) := \begin{array}{c} d \\ \left[\begin{array}{c|c|c} V_u(\alpha_1, d_1) & \ldots & V_u(\alpha_m, d_m) \end{array}\right] \end{array} u\,,$$

where

$$V_u(\alpha_i, d_i) := \begin{array}{c} d_i \\ \left[\begin{array}{ccccc} 1 & 0 & 0 & \ldots & 0 \\ \alpha_i & 1 & 0 & \ldots & 0 \\ \alpha_i^2 & 2\alpha_i & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ \alpha_i^{u-1} & (u-1)\alpha_i^{u-2} & \binom{u-1}{2}\alpha_i^{u-3} & \ldots & \binom{u-1}{d_i-1}\alpha_i^{u-d_i} \end{array}\right] \end{array} u$$

with the convention that when $k < j$, $\binom{k}{j}\alpha_i^{k-j} = 0$.

When $d_i = 1$ for all i, this gives the usual Vandermonde matrix $V_u(A)$. When $u = d$, we omit the sub-index u and write $V(\overline{A})$ and $V(A)$.

For example

$$V\big((\alpha, 3); (\beta, 2)\big) = \left[\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & 0 \\ \alpha & 1 & 0 & \beta & 1 \\ \alpha^2 & 2\alpha & 1 & \beta^2 & 2\beta \\ \alpha^3 & 3\alpha^2 & 3\alpha & \beta^3 & 3\beta^2 \\ \alpha^4 & 4\alpha^3 & 6\alpha^2 & \beta^4 & 4\beta^3 \end{array}\right]$$

and

$$V_3((\alpha,3);(\beta,2)) = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ \alpha & 1 & 0 & \beta & 1 \\ \alpha^2 & 2\alpha & 1 & \beta^2 & 2\beta \end{bmatrix}.$$

The determinant of a square confluent matrix is non-zero, and satisfies, [1],

$$\det\big(V(\overline{A})\big) = \prod_{1\leqslant i<j\leqslant m} (\alpha_j-\alpha_i)^{d_i d_j}.$$

In the same way that the usual Vandermonde matrix $V(A)$ is related to the Lagrange Interpolation Problem on A, the generalized Vandermonde matrix $V(\overline{A})$ is associated with the Hermite Interpolation Problem on $\overline{A}$ [18]: Given $\{y_{i,j_i},\ 1\leqslant i\leqslant m,\ 0\leqslant j_i<d_i\}$, there exists a unique polynomial p of degree $\deg(p)<d$ which satisfies the following conditions:

$$\begin{cases} p(\alpha_1)=0!\,y_{1,0}, & p'(\alpha_1)=1!\,y_{1,1}, & \dots, & p^{(d_1-1)}(\alpha_1)=(d_1-1)!\,y_{1,d_1-1}, \\ \vdots & \vdots & \vdots & \vdots \\ p(\alpha_m)=0!\,y_{m,0}, & p'(\alpha_m)=1!\,y_{m,1}, & \dots, & p^{(d_m-1)}(\alpha_m)=(d_m-1)!\,y_{m,d_m-1}. \end{cases}$$

This Hermite polynomial $p=a_0+a_1x+\cdots+a_{d-1}x^{d-1}$ is given by the only solution of

$$(a_0\ a_1\ \dots\ a_{d-1})\cdot V(\overline{A}) = (y_{1,0}\ y_{1,1}\ \dots\ y_{m,d_m-1})$$

(here the right vector is indexed by the pairs (i,j_i) for $1\leqslant i\leqslant m$, $0\leqslant j_i<d_i$) and satisfies

$$\det\big(V(\overline{A})\big)\,p(x) = -\det \begin{array}{|c|c|c} \multicolumn{1}{c}{d} & \multicolumn{1}{c}{1} & \\ \cline{1-2} V(\overline{A}) & \begin{matrix}1\\ x\\ \vdots\\ x^{d-1}\end{matrix} & d \\ \cline{1-2} y_{1,0}\ y_{1,1}\ \dots\ y_{m,d_m-1} & 0 & 1 \\ \cline{1-2} \end{array}. \tag{3}$$

The polynomial p can also be viewed in a more suitable basis, where the corresponding “Vandermonde" matrix has more structure. We introduce the d polynomials in this basis.

Notation 2.2. For $1\leqslant i\leqslant m$ we set

$$\bar f_i := \prod_{j\neq i}(x-\alpha_j)^{d_j}$$

and, for $0\leqslant k_i<d_i$,

$$\bar f_{i,k_i} := \frac{\bar f}{(x-\alpha_i)^{d_i-k_i}} = (x-\alpha_i)^{k_i}\bar f_i.$$

Then, in this basis, the polynomial $p = \sum_{i,k_i} a_{i,k_i}\overline{f}_{i,k_i}$ is given by the only solution of

$$(a_{1,0}\ a_{1,1}\ \ldots\ a_{m,d_m-1}) \cdot V'(\overline{A}) = (y_{1,0}\ y_{1,1}\ \ldots\ y_{m,d_m-1})$$

where

$$V'(\overline{A}) := \begin{array}{c} \begin{array}{ccc} d_1 & & d_m \end{array} \\ \left[\begin{array}{c|c|c} V'(\alpha_1, d_1) & \mathbf{0} & \mathbf{0} \\ \hline \mathbf{0} & \ddots & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0} & V'(\alpha_m, d_m) \end{array}\right] \begin{array}{c} d_1 \\ \\ d_m \end{array} \end{array},$$

with

$$V'(\alpha_i, d_i) := \begin{array}{c} d_i \\ \left[\begin{array}{cccc} \overline{f}_i(\alpha_i) & \overline{f}_i'(\alpha_i) & \ldots & \frac{\overline{f}_i^{(d_i-1)}(\alpha_i)}{(d_i-1)!} \\ 0 & \overline{f}_i(\alpha_i) & \ldots & \frac{\overline{f}_i^{(d_i-2)}(\alpha_i)}{(d_i-2)!} \\ 0 & 0 & \ddots & \vdots \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \ldots & \overline{f}_i(\alpha_i) \end{array}\right] d_i \end{array}$$

and satisfies

$$\det\left(V'(\overline{A})\right) p(x) = -\det \begin{array}{c} \begin{array}{cc} d & 1 \end{array} \\ \left[\begin{array}{c|c} & \overline{f}_{1,0} \\ & \overline{f}_{1,1} \\ V'(\overline{A}) & \vdots \\ & \overline{f}_{m,d_m-1} \\ \hline y_{1,0}\ y_{1,1}\ \ldots\ y_{m,d_m-1} & 0 \end{array}\right] \begin{array}{c} d \\ 1 \end{array} \end{array}.$$

We note that

$$\det(V'(\overline{A})) = \prod_{1\leqslant i\leqslant m} \overline{f}_i(\alpha_i)^{d_i}$$
$$= (-1)^{\frac{m(m-1)}{2}} \left(\prod_{1\leqslant i<j\leqslant m} (\alpha_j - \alpha_i)^{d_i d_j}\right)^2 = (-1)^{\frac{m(m-1)}{2}} \det(V(\overline{A}))^2.$$

In particular $p = \sum_{i,j_i} y_{i,j_i} p_{i,j_i}$ where for $1 \leqslant i \leqslant m,\ 0 \leqslant j_i < d_i$, the *basic Hermite polynomials* p_{i,j_i} are the unique polynomials of degree $\deg(p_{i,j_i}) < d$ determined by the conditions for $1 \leqslant \ell \leqslant m,\ 0 \leqslant q_\ell < d_\ell$,

$$\begin{cases} p_{i,j_i}^{(q_\ell)}(\alpha_\ell) = j_i! \ \text{for} \ \ell = i \text{ and } q_\ell = j_i, \\ p_{i,j_i}^{(q_\ell)}(\alpha_\ell) = 0 \ \text{otherwise.} \end{cases} \tag{4}$$

When $\overline{A} = A = (\alpha_1, \ldots, \alpha_d)$, then, denoting $f_i := \overline{f}_i$, we have

$$p_{i,0} = \prod_{\ell \neq i} \frac{x - \alpha_\ell}{\alpha_i - \alpha_\ell} = \frac{1}{f_i(\alpha_i)} f_i \quad \text{for} \quad 1 \leqslant i \leqslant d,$$

while for $\overline{A} = (\alpha, d)$,

$$p_{1,j} = (x - \alpha)^j = \overline{f}_{1,j} \quad \text{for} \quad 0 \leqslant j < d.$$

The following proposition generalizes these two extremal formulas.

Proposition 2.3. *Fix $1 \leqslant i \leqslant m$ and $0 \leqslant j < d_i$. Then*

$$p_{i,j} = \frac{1}{\overline{f}_i(\alpha_i)} \sum_{k=0}^{d_i-1-j} (-1)^k \left(\sum_{k_1+\ldots+\widehat{k_i}+\ldots+k_m=k} \prod_{\ell \neq i} \frac{\binom{d_\ell - 1 + k_\ell}{k_\ell}}{(\alpha_i - \alpha_\ell)^{k_\ell}} \right) \overline{f}_{i,j+k}$$

where $k_1 + \cdots + \widehat{k_i} + \cdots + k_m$ denotes the sum without k_i. (When $m = 1$, the right expression under brackets is understood to equal 1 for $k = 0$ and 0 otherwise.)

Proof. Applying for instance [25, Theorem 1], we first remark that

$$p_{i,j} = \sum_{k=0}^{d_i-1-j} \frac{1}{k!} \left(\frac{1}{\overline{f}_i} \right)^{(k)} (\alpha_i) \overline{f}_{i,j+k}.$$

Then we plug into the expression the following, given by Leibnitz rule for the derivative of a product:

$$\left(\frac{1}{\overline{f}_i} \right)^{(k)} (\alpha_i) = (-1)^k \, k! \sum_{k_1+\ldots+\widehat{k_i}+\ldots+k_r=k} \prod_{\ell \neq i} \frac{\binom{d_\ell - 1 + k_\ell}{k_\ell}}{(\alpha_i - \alpha_\ell)^{d_\ell + k_\ell}}. \quad \square$$

The basic Hermite polynomials enable us to compute the inverse of the confluent matrix $V(\overline{A})$:

$$V(\overline{A})^{-1} = \begin{array}{c} d \\ \boxed{\begin{array}{c} V_1^* \\ \hline \vdots \\ \hline V_m^* \end{array}} \end{array} \begin{array}{l} d_1 \\ \\ d_m \end{array} \quad \text{where} \quad V_i^* := \begin{array}{c} d \\ \boxed{\begin{array}{c} \text{coefficients of } p_{i,1} \\ \vdots \\ \text{coefficients of } p_{i,d_i} \end{array}} \end{array} {}_{d_i}, \ 1 \leqslant i \leqslant r$$

(here the coefficients of $p_{i,j_i}(x)$ are written in the monomial basis $1, x, \ldots, x^{d-1}$).

Now we set the notation for a slight modification of a case of generalized Wronskian matrices.

Notation 2.4. Set $u \in \mathbb{N}$. Given a polynomial $h(z)$, the *generalized Wronskian* (non-necessarily square) $u \times d$ matrix $W_{h,u}(\overline{A})$ associated to $\overline{A} = \big((\alpha_1, d_1); \ldots; (\alpha_m, d_m)\big)$ is

$$W_{h,u}(\overline{A}) = W_{h,u}((\alpha_1, d_1); \dots; (\alpha_m, d_m)) := \begin{array}{cc} d & \\ \begin{array}{|c|c|c|}\hline W_{h,u}(\alpha_1, d_1) & \dots & W_{h,u}(\alpha_m, d_m) \\ \hline \end{array} & u \end{array},$$

where

$$W_{h,u}(\alpha_i, d_i) := \begin{array}{cc} d_i & \\ \begin{array}{|cccc|}\hline h(\alpha_i) & h'(\alpha_i) & \dots & \frac{h^{(d_i-1)}(\alpha_i)}{(d_i-1)!} \\ (zh)(\alpha_i) & (zh)'(\alpha_i) & \dots & \frac{(zh)^{(d_i-1)}(\alpha_i)}{(d_i-1)!} \\ \vdots & \vdots & & \vdots \\ (z^{u-1}h)(\alpha_i) & (z^{u-1}h)'(\alpha_i) & \dots & \frac{(z^{u-1}h)^{(d_i-1)}(\alpha_i)}{(d_i-1)!} \\ \hline \end{array} & u \end{array}.$$

When $u = d$, we omit the sub-index u and write $W_h(\overline{A})$.

For example for $h(z) = x - z$ and $\overline{A} = (\alpha, 3)$,

$$W_{x-z}(\alpha, 3) = W_{x-z,3}(\alpha, 3) = \begin{array}{cc} 3 & \\ \begin{array}{|ccc|}\hline x-\alpha & -1 & 0 \\ \alpha x - \alpha^2 & x - 2\alpha & -1 \\ \alpha^2 x - \alpha^3 & 2\alpha x - 3\alpha^2 & x - 3\alpha \\ \hline \end{array} & 3 \end{array}.$$

The determinant of a square Wronskian matrix is easily obtainable performing row operations in the case of one block, and by induction in the size of the matrix in general:

$$\det\left(W_h(\overline{A})\right) = \left(\prod_{1 \leqslant i < j \leqslant m} (\alpha_j - \alpha_i)^{d_i d_j}\right) h(\alpha_1)^{d_1} \cdots h(\alpha_m)^{d_m}.$$

2.4. Subresultants in multiple roots

In this section, we describe explicit formulas we can get for the non-trivial extremal cases of subresultants in terms of both sets of roots of $\overline{f} = (x-\alpha_1)^{d_1} \cdots (x-\alpha_m)^{d_m}$ and $\overline{g} = (x-\beta_1)^{e_1} \cdots (x-\beta_n)^{e_n}$ with $d = \sum_{i=1}^m d_i$ and $e = \sum_{j=1}^n e_j$. More precisely, we present formulas for $\operatorname{Sres}_t(\overline{f}, \overline{g})$ for the cases $t = d - 1 < e$ (Proposition 2.6 below) and $t = 1 < d \leqslant e$ (Theorem 2.7). We will derive them from Theorem 2.5 below, a generalization of [17, Theorem 3.1] and [10, Lemma 2] which includes the multiple roots case (and is also strongly related to a multiple roots case version of [11, Theorem 1]). The main drawback of this approach to obtain formulas for all cases of t is the fact that submatrices of generalized Vandermonde matrices are not always generalized Vandermonde matrices, so in general their determinants cannot be expressed as products of differences. This is why the search for nice formulas in double sums in the case of multiple roots is more challenging.

Theorem 2.5. *Set* $0 \leqslant t \leqslant d < e$ *or* $0 \leqslant t < d = e$. *Then*

$$\mathrm{Sres}_t(\bar f, \bar g) = (-1)^{d-t}\ \det\left(V(\bar A)\right)^{-1}\ \det \begin{array}{|c|c|l} \multicolumn{1}{c}{d} & \multicolumn{1}{c}{1} & \\ \cline{1-2} V_{t+1}(\bar A) & \begin{matrix}1\\ \vdots\\ x^t\end{matrix} & t+1 \\ \cline{1-2} W_{\bar g, d-t}(\bar A) & \mathbf{0} & d-t \\ \cline{1-2} \end{array}$$

$$= (-1)^{c}\ \det\left(V(\bar A)\right)^{-1}\ \det\left(V(\bar B)\right)^{-1}\ \det \begin{array}{|c|c|c|l} \multicolumn{1}{c}{d} & \multicolumn{1}{c}{e} & \multicolumn{1}{c}{1} & \\ \cline{1-3} V_{t+1}(\bar A) & \mathbf{0} & \begin{matrix}1\\ \vdots\\ x^t\end{matrix} & t+1 \\ \cline{1-3} V_{d+e-t}(\bar A) & V_{d+e-t}(\bar B) & \mathbf{0} & d+e-t \\ \cline{1-3} \end{array},$$

where $c := \max\{e \pmod 2, d-t \pmod 2\}$.

Proof. The proof is quite similar to the proofs of Lemmas 2 and 3 in [10], replacing the usual Vandermonde and Wronskian matrices by their generalized counterparts. We will thus omit the intermediate computations.

Let $\bar f = \sum_{i=0}^{d} a_i x^i$, where $a_d = 1$, and $\bar g = \sum_{j=0}^{e} b_j x_i$, where $b_e = 1$. We introduce the following matrices of [10]:

$$M_{\bar f} := \begin{array}{|ccccc|l} \multicolumn{5}{c}{d+e-t} & \\ \cline{1-5} a_0 & \dots & a_d & & & \\ & \ddots & & \ddots & & e-t \\ & & a_0 & \dots & a_d & \\ \cline{1-5} \end{array}, \quad M_{\bar g} := \begin{array}{|ccccc|l} \multicolumn{5}{c}{d+e-t} & \\ \cline{1-5} b_0 & \dots & b_e & & & \\ & \ddots & & \ddots & & d-t \\ & & b_0 & \dots & b_e & \\ \cline{1-5} \end{array}.$$

and

$$S_t := \begin{array}{|c|l} \multicolumn{1}{c}{d+e-t} & \\ \cline{1-1} M_{x-z} & t \\ \cline{1-1} M_{\bar f} & e-t \\ \cline{1-1} M_{\bar g} & d-t \\ \cline{1-1} \end{array} \quad \text{where} \quad M_{x-z} := \begin{array}{|cccccc|l} \multicolumn{6}{c}{d+e-t} & \\ \cline{1-6} x & -1 & 0 & \dots & \dots & 0 & \\ \ddots & \ddots & \ddots & & & \vdots & t \\ & x & -1 & 0 & \dots & 0 & \\ \cline{1-6} \end{array}.$$

We have [10, Lemma 1]:

$$\mathrm{Sres}_t(\bar f, \bar g) = (-1)^{(e-t)(d-t)} \det(S_t).$$

Also, exactly as in the proof of [10, Lemma 2],

$$\begin{array}{c|c|} \multicolumn{1}{c}{} & \multicolumn{1}{c}{d+e-t} \\ \cline{2-2} t & M_{x-z} \\ \cline{2-2} e-t & M_{\bar f} \\ \cline{2-2} d-t & M_{\bar g} \\ \cline{2-2} \end{array} \begin{array}{|c|c|c} \multicolumn{1}{c}{d} & \multicolumn{1}{c}{e-t} & \\ \hline & \mathbf{0} & d \\ \cline{2-2} V_{d+e-t}(\bar A) & & \\ & \mathrm{Id}_{e-t} & e-t \\ \hline \end{array} = \begin{array}{|c|c|c} \multicolumn{1}{c}{d} & \multicolumn{1}{c}{e-t} & \\ \hline W_{x-z,t}(\bar A) & * & t \\ \hline \mathbf{0} & M'_{\bar f} & e-t \\ \hline W_{\bar g,d-t}(\bar A) & * & d-t \\ \hline \end{array}.$$

This implies first the generalization of [10, Lemma 2] to the multiple roots case:

$$\det\left(V(\bar A)\right) \mathrm{Sres}_t(\bar f, \bar g) = \det \begin{array}{|c|c} \multicolumn{1}{c}{d} & \\ \hline W_{x-z,t}(\bar A) & t \\ \hline W_{\bar g,d-t}(\bar A) & d-t \\ \hline \end{array} = (-1)^{d-t} \det \begin{array}{|c|c|c} \multicolumn{1}{c}{d} & \multicolumn{1}{c}{1} & \\ \hline & 1 & \\ V_{t+1}(\bar A) & \vdots & t+1 \\ & x^t & \\ \hline W_{\bar g,d-t}(\bar A) & \mathbf{0} & d-t \\ \hline \end{array},$$

where the second equality is a consequence of obvious row and column operations. Next, we get as in the proof of [10, Lemma 3],

$$\det\left(V(\bar A)\right) \det\left(V(\bar B)\right) \mathrm{Sres}_t(\bar f, \bar g) = (-1)^c \det \begin{array}{|c|c|c|c} \multicolumn{1}{c}{d} & \multicolumn{1}{c}{e} & \multicolumn{1}{c}{1} & \\ \hline & & 1 & \\ V_{t+1}(\bar A) & \mathbf{0} & \vdots & t+1 \\ & & x^t & \\ \hline V_{d+e-t}(\bar A) & V_{d+e-t}(\bar B) & \mathbf{0} & d+e-t \\ \hline \end{array}. \qquad \square$$

We note that starting from the first equality above and applying similar arguments, we also get very simply

$$\det\left(V(\bar A)\right) \det\left(V(\bar B)\right) \mathrm{Sres}_t(\bar f, \bar g) = (-1)^{(d-t)e} \det \begin{array}{|c|c|c} \multicolumn{1}{c}{d} & \multicolumn{1}{c}{e} & \\ \hline W_{x-z}(\bar A) & \mathbf{0} & t \\ \hline V_{d+e-t}(\bar A) & V_{d+e-t}(\bar B) & d+e-t \\ \hline \end{array}. \tag{5}$$

As mentioned above, when $t = 0$ the formula in roots for $\mathrm{Sres}_0(f, g)$ specializes well when considering $\mathrm{Sres}_0(\bar f, \bar g)$. When $t = d < e$, the formula $\mathrm{Sres}_d(f, g) = \prod_{1 \leqslant i \leqslant d}(x - \alpha_i)$ also specializes well as $\mathrm{Sres}_d(\bar f, \bar g) = \prod_{1 \leqslant i \leqslant m}(x - \alpha_i)^{d_i}$. Our purpose now is to understand formulas in roots for the following extremal subresultants, i.e for Sres_1 and Sres_{d-1}, in case of multiple roots.

• The case $t = d - 1 < e$: When f has simple roots, it is known (or can easily be derived for instance from Sylvester's Identity (2) for $p = d - 1$ and $q = 0$) that

$$\mathrm{Sres}_{d-1}(f, \bar g) = \sum_{i=1}^{d} \bar g(\alpha_i) \left(\prod_{j \neq i} \frac{x - \alpha_j}{\alpha_i - \alpha_j} \right) = \sum_{i=1}^{d} \bar g(\alpha_i)\, p_i,$$

where p_i is the basic Lagrange interpolation polynomial of degree strictly bounded by d such that $p_i(\alpha_i) = 1$ and $p_i(\alpha_j) = 0$ for $j \neq i$. In other words, $\mathrm{Sres}_{d-1}(f, \bar g)$ is the Lagrange interpolation polynomial of degree strictly bounded by d which coincides with $\bar g$ in the d values $\alpha_1, \ldots, \alpha_d$. This formula does not apply when f has multiple roots, but we can show that we get the natural generalization of this fact, that is, that $\mathrm{Sres}_{d-1}(\bar{f},\bar{g})$ is the Hermite interpolation polynomial of degree strictly bounded by d which coincides with $\bar{g}$ and its derivatives up to the corresponding orders in the m values $\alpha_1,\dots,\alpha_m$:

Proposition 2.6.

$$\mathrm{Sres}_{d-1}(\bar{f},\bar{g}) = \sum_{i=1}^{m}\sum_{j_i=0}^{d_i-1}\frac{\bar{g}^{(j_i)}(\alpha_i)}{j_i!}\,p_{i,j_i},$$

where p_{i,j_i} is the basic Hermite interpolation polynomial defined by Condition (4) or Proposition 2.3 for $\bar{A}$.

Proof. In this case, applying the first statement of Theorem 2.5 we get

$$\mathrm{Sres}_{d-1}(\bar{f},\bar{g}) = -\,\det\left(V(\bar{A})\right)^{-1}\,\det \begin{array}{c|c|c} d & 1 & \\ \hline V_d(\bar{A}) & \begin{matrix}1\\ \vdots\\ x^{d-1}\end{matrix} & d \\ \hline W_{\bar{g},1}(\bar{A}) & \mathbf{0} & 1 \end{array}$$

where when following the sub-index notation of Formula (3), we note that

$$(W_{\bar{g},1}(\bar{A}))_{i,j_i} = \frac{\bar{g}^{(j_i)}(\alpha_i)}{j_i!}.$$

The conclusion follows by Formula (3). $\square$

For example, when $\bar{A}=(\alpha,d)$, we get

$$\mathrm{Sres}_{d-1}((x-\alpha)^d,\bar{g}) = \sum_{j=0}^{d-1}\frac{\bar{g}^{(j)}(\alpha)}{j!}\,(x-\alpha)^j,$$

the Taylor expansion of $\bar{g}$ up to order $d-1$.

• The case $t = 1 < d \leqslant e$: We keep Notation 2.2. When f has simple roots, it is known (or can easily be derived for instance from Sylvester's Identity (2) for $p=1$ and $q=0$) that

$$\begin{aligned}\mathrm{Sres}_1(f,\bar{g}) &= (-1)^{d-1}\sum_{i=1}^{d}\Big(\prod_{j\neq i}\frac{\bar{g}(\alpha_j)}{\alpha_i-\alpha_j}\Big)(x-\alpha_i) \\ &= (-1)^{d-1}\sum_{i=1}^{d}\frac{\prod_{j\neq i}\bar{g}(\alpha_j)}{f_i(\alpha_i)}\,(x-\alpha_i).\end{aligned} \tag{6}$$

The general situation is a bit less obvious, but in any case we can get an expression of $\mathrm{Sres}_1(\bar{f},\bar{g})$ by using the coefficients of the Hermite interpolation polynomial, in this case of the whole data

$$\bar{A}\cup\bar{B} := ((\alpha_1,d_1);\dots;(\alpha_m,d_m);(\beta_1,e_1);\dots;(\beta_n,e_n)).$$

We note that

$$\det\left(V(\bar{A}\cup\bar{B})\right) = \det\left(V(\bar{A})\right)\det\left(V(\bar{B})\right)R(\bar{B},\bar{A})$$

which holds even when $\alpha_i=\beta_j$ for some i,j.

Theorem 2.7.

$$\begin{aligned}\mathrm{Sres}_1(\bar f,\bar g) &= \sum_{i=1}^{m}(-1)^{d-d_i}\left(\frac{\prod_{j\neq i}\bar g(\alpha_j)^{d_j}}{\bar f_i(\alpha_i)}\right)\bar g(\alpha_i)^{d_i-1}\Big((x-\alpha_i)\\
&\quad\cdot \sum_{\substack{k_1+\cdots+\widehat{k_i}+\cdots\\ \cdots+k_{m+n}=d_i-1}}\ \prod_{\substack{1\leqslant j\leqslant m\\ j\neq i}}\frac{\binom{d_j-1+k_j}{k_j}}{(\alpha_i-\alpha_j)^{k_j}}\prod_{1\leqslant \ell\leqslant n}\frac{\binom{e_\ell-1+k_{m+\ell}}{k_{m+\ell}}}{(\alpha_i-\beta_\ell)^{k_{m+\ell}}}\\
&\quad+\min\{1,d_i-1\}\sum_{\substack{k_1+\cdots+\widehat{k_i}+\cdots\\ \cdots+k_{m+n}=d_i-2}}\ \prod_{\substack{1\leqslant j\leqslant m\\ j\neq i}}\frac{\binom{d_j-1+k_j}{k_j}}{(\alpha_i-\alpha_j)^{k_j}}\prod_{1\leqslant \ell\leqslant n}\frac{\binom{e_\ell-1+k_{m+\ell}}{k_{m+\ell}}}{(\alpha_i-\beta_\ell)^{k_{m+\ell}}}\Big).\end{aligned}$$

Proof. Setting $t=1$ in Expression (5) we get

$$\det\left(V(\bar A)\right)\det\left(V(\bar B)\right)\mathrm{Sres}_1(\bar f,\bar g) = (-1)^{(d-1)e}\det\begin{array}{cc} d & e & \\ \left[\begin{array}{c|c} W_{x-z,1}(\bar A) & \mathbf{0}\\ \hline V_{d+e-1}(\bar A) & V_{d+e-1}(\bar B)\end{array}\right] & \begin{array}{c}1\\ d+e-1\end{array}\end{array}$$

where

$$W_{x-z,1} = (\underbrace{x-\alpha_1,-1,0,\dots,0}_{d_1},\dots,\underbrace{x-\alpha_m,-1,0\dots,0}_{d_m}).$$

We expand the determinant w.r.t. the first row, and observe that when we delete the first row and column j, the matrix that survives coincides with $V(\bar A\cup\bar B)_{(d+e,j)}$, the submatrix of $V(\bar A\cup\bar B)$ obtained by deleting the last row and column j. Therefore,

$$\begin{aligned}&\det\left[\begin{array}{c|c} W_{x-z,1}(\bar A) & \mathbf{0}\\ \hline V_{d+e-1}(\bar A) & V_{d+e-1}(\bar B)\end{array}\right]\\
&=\sum_{j=1}^{m}(-1)^{\phi(j)-1}\Big(\det\left(V(\bar A\cup\bar B)|_{(d+e,\phi(j))}\right)(x-\alpha_j)+\det\left(V(\bar A\cup\bar B)|_{(d+e,\phi'(j))}\right)\Big),\end{aligned}$$

where $\phi(i)$ equals the number of the column corresponding to $(1,\alpha_i,\dots,\alpha_i^{d+e-1})$ in $V(\bar A\cup\bar B)$, and $\phi'(i)=\phi(i)+1$ if $d_i>1$ and 0 otherwise.

Now, from

$$\begin{aligned}\det\left(V(\bar A\cup\bar B)|_{(d+e,\phi(j))}\right) &= (-1)^{d+e-\phi(j)}\det\left(V(\bar A\cup\bar B)\right)V(\bar A\cup\bar B)^{-1}_{\phi(j),d+e},\\
\det\left(V(\bar A\cup\bar B)|_{(d+e,\phi'(j))}\right) &= (-1)^{d+e-\phi'(j)}\det\left(V(\bar A\cup\bar B)\right)V(\bar A\cup\bar B)^{-1}_{\phi'(j),d+e}\end{aligned}$$

(by the cofactor expression for the inverse) and

$$\det\left(V(\bar A\cup\bar B)\right) = (-1)^{de}\det\left(V(\bar A)\right)\det\left(V(\bar B)\right)R(\bar A,\bar B),$$

we first get, since $R(\bar A,\bar B)=\prod_{1\leqslant i\leqslant m}\bar g(\alpha_i)^{d_i}$, that

$$\mathrm{Sres}_1(\bar f,\bar g) = (-1)^{d-1}\left(\prod_{1\leqslant i\leqslant m}\bar g(\alpha_i)^{d_i}\right)\left(\sum_{i=1}^{m}V(\bar A\cup\bar B)^{-1}_{\phi(i),d+e}(x-\alpha_i)-\sum_{i=1}^{m}V(\bar A\cup\bar B)^{-1}_{\phi'(i),d+e}\right).$$

We set $\overline{h} := \overline{f}\,\overline{g}$, and for $i = 1, \ldots, m$, $\overline{h}_i := \overline{h}/(x-\alpha_i)^{d_i}$. In [7, Identity 9], it is shown that

$$V(\overline{A} \cup \overline{B})^{-1}_{\phi(i),d+e} = \frac{1}{(d_i-1)!}\left(\frac{1}{\overline{h}_i}\right)^{(d_i-1)}(\alpha_i),$$

and when $d_i > 1$,

$$V(\overline{A} \cup \overline{B})^{-1}_{\phi'(i),d+e} = \frac{1}{(d_i-2)!}\left(\frac{1}{\overline{h}_i}\right)^{(d_i-2)}(\alpha_i).$$

Therefore, we obtain the statement by applying Leibnitz rule

$$\left(\frac{1}{\overline{h}_i}\right)^{(k)} = (-1)^k\, k! \sum_{k_1+\cdots+\widehat{k_i}+\cdots+k_{m+n}=k} \prod_{\substack{1 \leqslant j \leqslant m \\ j \neq i}} \frac{\binom{d_j-1+k_j}{k_j}}{(x-\alpha_j)^{d_j+k_j}} \prod_{1\leqslant \ell \leqslant n} \frac{\binom{e_\ell-1+k_{m+\ell}}{k_{m+\ell}}}{(x-\beta_\ell)^{e_\ell+k_{m+\ell}}}. \qquad \square$$

Note that in the case that f has simple roots we immediately recover Identity (6) while when $\overline{f} = (x-\alpha)^d$ for $d \geqslant 2$, we recover Proposition 3.2 of [9]:

$$\begin{aligned} \mathrm{Sres}_1((x-\alpha)^d, \overline{g}) = \overline{g}(\alpha)^{d-1} \Bigg(& \sum_{k_1+\cdots+k_n=d-1} \Big(\prod_{\ell=1}^{n} \frac{\binom{e_\ell-1+k_\ell}{k_\ell}}{(\alpha-\beta_\ell)^{k_\ell}} \Big)(x-\alpha) \\ & + \sum_{k_1+\cdots+k_n=d-2} \prod_{\ell=1}^{n} \frac{\binom{e_\ell-1+k_\ell}{k_\ell}}{(\alpha-\beta_\ell)^{k_\ell}} \Bigg). \end{aligned}$$

3. Multivariate case: Poisson-like formulas for subresultants

We turn to the multivariate case, considering the definition of subresultants introduced in [5]. Our goal is to generalize Theorem 3.2 in [8]—that we recall below—to the case when the considered polynomials have multiple roots. We first fix the notation, referring the reader to [8] for more details.

3.1. Notation

Fix $n \in \mathbb{N}$ and set $D_i \in \mathbb{N}$ for $1 \leqslant i \leqslant n+1$. Let

$$f_i := \sum_{|\boldsymbol{\alpha}| \leqslant D_i} a_{i,\boldsymbol{\alpha}} \boldsymbol{x}^{\boldsymbol{\alpha}} \in K[x_1, \ldots, x_n],$$

be polynomials of degree D_i in n variables, where $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in (\mathbb{Z}_{\geqslant 0})^n$, $\boldsymbol{x}^{\boldsymbol{\alpha}} := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, $|\boldsymbol{\alpha}| = \alpha_1 + \cdots + \alpha_n$, and K is a field of characteristic zero, that we assume without loss of generality to be algebraically closed.

Fix $t \in \mathbb{N}$. Let $k := \mathcal{H}_{D_1\ldots D_{n+1}}(t)$ be the Hilbert function at t of a regular sequence of $n+1$ homogeneous polynomials in $n+1$ variables of degrees $D_1, \ldots, D_{n+1}$, i.e.

$$k = \#\{\boldsymbol{x}^{\boldsymbol{\alpha}} : |\boldsymbol{\alpha}| \leqslant t,\ \alpha_i < D_i,\ 1 \leqslant i \leqslant n,\ \text{and } t - |\boldsymbol{\alpha}| < D_{n+1}\}.$$

We set

$$\mathcal{S} := \{\boldsymbol{x}^{\boldsymbol{\gamma}_1}, \ldots, \boldsymbol{x}^{\boldsymbol{\gamma}_k}\} \subset K[\boldsymbol{x}]_t$$

a set of k monomials of degree bounded by t, and

$$\Delta_{\mathcal{S}}(f_1, \ldots, f_{n+1}) := \Delta^{(t)}_{\mathcal{S}^h}(f_1^h, \ldots, f_{n+1}^h),$$

for the *order t subresultant of* $f_1^h, \ldots, f_{n+1}^h$ *with respect to the family* $\mathcal{S}^h := \{\boldsymbol{x}^{\boldsymbol{\gamma}_1} x_{n+1}^{t-|\boldsymbol{\gamma}_1|}, \ldots, \boldsymbol{x}^{\boldsymbol{\gamma}_k} x_{n+1}^{t-|\boldsymbol{\gamma}_k|}\}$ defined in [5]. Here, f_i^h denotes the homogenization of f_i by the variable x_{n+1}.

We recall that the subresultant $\Delta_{\mathcal{S}}$ is a polynomial in the coefficients of the f_i^h of degree $\mathcal{H}_{D_1\ldots D_{i-1}D_{i+1}\ldots D_{n+1}}(t - D_i)$ for $1 \leqslant i \leqslant n+1$, having the following property: $\Delta_{\mathcal{S}} = 0$ if and only if $I_t \cup \mathcal{S}^h$ does not generate the space of all forms of degree t in $k[x_1, \ldots, x_{n+1}]$, where I_t denotes the degree t part of the ideal generated by the f_i^h's.

By [4] we know that

$$\det(M_{\mathcal{S}}) = \mathcal{E}(t)\,\Delta_{\mathcal{S}}, \tag{7}$$

where $M_{\mathcal{S}}$ denotes the Macaulay–Chardin matrix obtained from

$$\begin{bmatrix} M_{f_1} \\ \vdots \\ M_{f_{n+1}} \end{bmatrix} \tag{8}$$

by deleting the columns indexed by the monomials in $\mathcal{S}$, and $\mathcal{E}(t)$ is the extraneous factor defined as the determinant of a specific square submatrix of (8) (see [5,4,8]).

We set $\rho := (D_1 - 1) + \cdots + (D_n - 1)$ and for $j \geqslant 0$, $\tau_j := \mathcal{H}_{D_1\ldots D_n}(j)$, the Hilbert function at j of a regular sequence of n homogeneous polynomials in n variables of degrees $D_1, \ldots, D_n$. We define also

$$\mathcal{T}_j := \begin{cases} \textit{any} \text{ set of } \tau_j \text{ monomials of degree } j & \text{if } j \geqslant \max\{0, t - D_{n+1} + 1\} \\ \{\boldsymbol{x}^{\boldsymbol{\alpha}} : |\boldsymbol{\alpha}| = j, \alpha_i < D_i \text{ for } 1 \leqslant i \leqslant n\} & \text{if } 0 \leqslant j < t - D_{n+1} + 1, \end{cases} \tag{9}$$

and denote with $D := D_1 \cdots D_n$ the *Bézout number*, the number of common solutions in K^n of n generic polynomials.

Set $\mathcal{T} := \cup_{j \geqslant 0} \mathcal{T}_j$ and $\mathcal{T}^* := \cup_{j=t+1}^{\rho} \mathcal{T}_j$. Note that $|\mathcal{T}| = D$. We enumerate the elements of $\mathcal{T}$ as follows: $\mathcal{T} = \{\boldsymbol{x}^{\boldsymbol{\alpha}_1}, \ldots, \boldsymbol{x}^{\boldsymbol{\alpha}_D}\}$, and assume that for $s := |\mathcal{T}^*|$ we have $\mathcal{T}^* = \{\boldsymbol{x}^{\boldsymbol{\alpha}_1}, \ldots, \boldsymbol{x}^{\boldsymbol{\alpha}_s}\}$. Also set

$$\mathcal{R} := \{\boldsymbol{x}^{\boldsymbol{\beta}_1}, \ldots, \boldsymbol{x}^{\boldsymbol{\beta}_r}\} = \{\boldsymbol{x}^{\boldsymbol{\alpha}} : |\boldsymbol{\alpha}| \leqslant t, \alpha_i < D_i, 1 \leqslant i \leqslant n,\ t - |\boldsymbol{\alpha}| \geqslant D_{n+1}\}. \tag{10}$$

Finally, for $1 \leqslant i \leqslant n$, let $\widetilde{f}_i$ be the homogeneous component of degree D_i of f_i, and $\widetilde{\Delta}_{\mathcal{T}_j} := \Delta^{(j)}_{\mathcal{T}_j}(\widetilde{f}_1, \ldots, \widetilde{f}_n)$ be the order j subresultant of $\widetilde{f}_1, \ldots, \widetilde{f}_n$ with respect to $\mathcal{T}_j$.

3.2. Poisson-like formula for subresultants

From now on we assume that $f_1, \ldots, f_n$ are generic in the sense they have no roots at infinity (which implies by Bézout theorem that the quotient algebra $A := K[\boldsymbol{x}]/(f_1, \ldots, f_n)$ is a finitely dimensional K-vector space of dimension D, which equals the number of common roots in K^n of these polynomials, counted with multiplicity, see e.g. [6, Chapter 3, Theorem 5.5]), and that $\mathcal{T}$ is a basis of A.

In [8] we treated the case of general polynomials with indeterminate coefficients, which specializes well under our assumptions to the case when the common roots $\boldsymbol{\xi}_1, \ldots, \boldsymbol{\xi}_D$ of $f_1, \ldots, f_n$ in K^n are all *simple*. Set $Z := \{\boldsymbol{\xi}_1, \ldots, \boldsymbol{\xi}_D\}$. We introduced the Vandermonde matrix

$$V_{\mathcal{T}}(Z) := \boxed{\begin{matrix} \boldsymbol{\xi}_1^{\boldsymbol{\alpha}_1} & \cdots & \boldsymbol{\xi}_D^{\boldsymbol{\alpha}_1} \\ \vdots & & \vdots \\ \boldsymbol{\xi}_1^{\boldsymbol{\alpha}_D} & \cdots & \boldsymbol{\xi}_D^{\boldsymbol{\alpha}_D} \end{matrix}} \in K^{D\times D} \tag{11}$$

whose determinant is non-zero, since $\mathcal{T}$ is assumed to be a basis of A, and we defined

$$\mathcal{O}_{\mathcal{S}}(Z) := \begin{array}{c} D \\ \left|\begin{array}{ccc} \boldsymbol{\xi}_1^{\boldsymbol{\gamma}_1} & \cdots & \boldsymbol{\xi}_D^{\boldsymbol{\gamma}_1} \\ \vdots & & \vdots \\ \boldsymbol{\xi}_1^{\boldsymbol{\gamma}_k} & \cdots & \boldsymbol{\xi}_D^{\boldsymbol{\gamma}_k} \\ \hline \boldsymbol{\xi}_1^{\boldsymbol{\alpha}_1} & \cdots & \boldsymbol{\xi}_D^{\boldsymbol{\alpha}_1} \\ \vdots & & \vdots \\ \boldsymbol{\xi}_1^{\boldsymbol{\alpha}_s} & \cdots & \boldsymbol{\xi}_D^{\boldsymbol{\alpha}_s} \\ \hline \boldsymbol{\xi}_1^{\boldsymbol{\beta}_1} f_{n+1}(\boldsymbol{\xi}_1) & \cdots & \boldsymbol{\xi}_D^{\boldsymbol{\beta}_1} f_{n+1}(\boldsymbol{\xi}_D) \\ \vdots & & \vdots \\ \boldsymbol{\xi}_1^{\boldsymbol{\beta}_r} f_{n+1}(\boldsymbol{\xi}_1) & \cdots & \boldsymbol{\xi}_D^{\boldsymbol{\beta}_r} f_{n+1}(\boldsymbol{\xi}_D) \end{array}\right| \end{array} \begin{array}{l} k \\ \\ s \\ \\ r \end{array} \in K^{D\times D}. \tag{12}$$

Theorem 3.1 [8, Theorem 3.2]. *For any $t \in \mathbb{Z}_{\geqslant 0}$ and for any $\mathcal{S} = \{\boldsymbol{x}^{\boldsymbol{\gamma}_1}, \ldots, \boldsymbol{x}^{\boldsymbol{\gamma}_k}\} \subset K[\boldsymbol{x}]_t$ of cardinality $k = \mathcal{H}_{D_1\ldots D_{n+1}}(t)$, we have*

$$\Delta_{\mathcal{S}}(f_1, \ldots, f_{n+1}) = \pm \left(\prod_{j=t-D_{n+1}+1}^{t} \widetilde{\Delta}_{\mathcal{T}_j} \right) \frac{\det\left(\mathcal{O}_{\mathcal{S}}(Z)\right)}{\det\left(V_{\mathcal{T}}(Z)\right)}.$$

In order to generalize this result to systems with multiple roots, and obtain an expression for the subresultant in terms of the roots of the first n polynomials $f_1, \ldots, f_n$, we need to introduce notions of the multiplicity structure of the roots that are sufficient to define $(f_1, \ldots, f_n)$. To be more precise, in the case of multiple roots, the set of evaluation maps $\{\mathrm{ev}_{\boldsymbol{\xi}} : A \to K \mid \boldsymbol{\xi} \text{ common root of } f_1, \ldots, f_n\}$ is not anymore a basis of A^*, the dual of the quotient ring A as a K-vector space, though still linearly independent. Hence other forms must be considered in order to describe A^* and to get a non-singular matrix generalizing $V_{\mathcal{T}}(Z)$.

All along this section we will use the language of dual algebras to generalize Theorem 3.1 for the multiple roots case (see for instance in [19,2] and the references therein). In Theorem 3.4 below we show that any basis of the dual A^* gives rise to generalizations of Theorem 3.1, as long as we assume that $\mathcal{T}$ is a basis of A. This is the most general setting where a generalization of Theorem 3.1 will hold. However, this version of the Theorem, using general elements of the dual, does not give a formula for the subresultant in terms of the roots.

In order to obtain these expressions, we need to consider a specific basis of A^* which contains the evaluation maps described above. It turns out that one can define a basis for A^* in terms of linear combinations of higher order derivative operators evaluated at roots of $f_1, \ldots, f_n$. This is the content of the so called theory of “inverse systems” introduced by Macaulay in [22], and developed in a context closer to our situation under the name of “Gröbner duality " in [15,23,12] among others.

The following is a multivariate analogue of Definition 2.4:

Definition 3.2. Let $\Lambda := \{\Lambda_1, \ldots, \Lambda_D\}$ be a basis of A^* as a K-vector space. Given any set $E = \{\boldsymbol{x}^{\boldsymbol{\alpha}_1}, \ldots, \boldsymbol{x}^{\boldsymbol{\alpha}_u}\}$ of u monomials and given any polynomial $h \in K[\boldsymbol{x}]$, the *generalized Vandermonde matrix* $V_E(\Lambda)$ and the *generalized Wronskian matrix* $W_{h,E}(\Lambda)$ corresponding to E, Λ and h are the following $u \times D$ matrices:

$$V_E(\Lambda) = \begin{array}{c} D \\ \left[\begin{array}{ccc} \Lambda_1(\boldsymbol{x}^{\boldsymbol{\alpha}_1}) & \cdots & \Lambda_D(\boldsymbol{x}^{\boldsymbol{\alpha}_1}) \\ \vdots & & \vdots \\ \Lambda_1(\boldsymbol{x}^{\boldsymbol{\alpha}_u}) & \cdots & \Lambda_D(\boldsymbol{x}^{\boldsymbol{\alpha}_u}) \end{array}\right] \end{array} u, \quad W_{h,E}(\Lambda) = \begin{array}{c} D \\ \left[\begin{array}{ccc} \Lambda_1(\boldsymbol{x}^{\boldsymbol{\alpha}_1}h) & \cdots & \Lambda_D(\boldsymbol{x}^{\boldsymbol{\alpha}_1}h) \\ \vdots & & \vdots \\ \Lambda_1(\boldsymbol{x}^{\boldsymbol{\alpha}_u}h) & \cdots & \Lambda_D(\boldsymbol{x}^{\boldsymbol{\alpha}_u}h) \end{array}\right] \end{array} u.$$

We modify the definition of the matrix $\mathcal{O}_{\mathcal{S}}(Z)$ in (12) as follows:

Definition 3.3. Let $\mathcal{S} = \{\boldsymbol{x}^{\boldsymbol{\gamma}_1}, \ldots, \boldsymbol{x}^{\boldsymbol{\gamma}_k}\} \subset K[\boldsymbol{x}]_t$ be of cardinality $k = \mathcal{H}_{D_1 \ldots D_{n+1}}(t)$, $\mathcal{T}^* := \cup_{j=t+1}^{\rho} \mathcal{T}_j$ as in (9) and $\mathcal{R}$ as in (10). Then

$$\mathcal{O}_{\mathcal{S}}(\Lambda) := \begin{array}{c} D \\ \left[\begin{array}{c} V_{\mathcal{S}}(\Lambda) \\ \hline V_{\mathcal{T}^*}(\Lambda) \\ \hline W_{f_{n+1},\mathcal{R}}(\Lambda) \end{array}\right] \end{array} \begin{array}{l} k \\ s \\ r \end{array} \in K^{D \times D}.$$

Note that by our assumption on $\mathcal{T}$ being a basis of A and Λ being a basis of A^*, we have $\det\left(V_{\mathcal{T}}(\Lambda)\right) \neq 0$. The following is the extension of Theorem 3.1 to the multiple roots case.

Theorem 3.4. *Let $(f_1, \ldots f_{n+1}) \subset K[\boldsymbol{x}]$ and $\mathcal{T} := \cup_{j \geqslant 0} \mathcal{T}_j$ specified in (9) satisfying our assumptions, and Λ be an arbitrary basis of A^*. For any $t \in \mathbb{Z}_{\geqslant 0}$ and for any $\mathcal{S} = \{\boldsymbol{x}^{\boldsymbol{\gamma}_1}, \ldots, \boldsymbol{x}^{\boldsymbol{\gamma}_k}\} \subset K[\boldsymbol{x}]_t$ of cardinality $k = \mathcal{H}_{D_1 \ldots D_{n+1}}(t)$, we have*

$$\Delta_{\mathcal{S}}(f_1, \ldots, f_{n+1}) = \pm \left(\prod_{j=t-D_{n+1}+1}^{t} \widetilde{\Delta}_{\mathcal{T}_j} \right) \frac{\det\left(\mathcal{O}_{\mathcal{S}}(\Lambda)\right)}{\det\left(V_{\mathcal{T}}(\Lambda)\right)}.$$

Proof of Theorem 3.4. The proof is similar to the proof of Theorem 3.2 in [8], to which we refer for notations and details. Extra care must be taken however, as we are not anymore considering the polynomials $f_1, \ldots, f_n$ to have simple common roots.

Using the exact same argument as in the proof of Theorem 3.2 in [8] we can prove that

$$\pm\,\mathcal{E}(t)\,\Delta_{\mathcal{S}}(f_1, \ldots, f_{n+1})\,\det\left(V_{\mathcal{T}}(\Lambda)\right) = \pm\det(M')\det\left(\mathcal{O}_{\mathcal{S}}(\Lambda)\right),$$

where

$$M' := \left[\begin{array}{c} M'_{f_1} \\ \vdots \\ M'_{f_n} \end{array}\right], \tag{13}$$

is the submatrix of (8) obtained by removing the columns corresponding the monomials in $\mathcal{T}$. In [8] we also showed that

$$\det(M') = \pm\mathcal{E}(t)\left(\prod_{j=t-D_{n+1}+1}^{t} \widetilde{\Delta}_{\mathcal{T}_j}\right),$$

so the claim is proved when $\mathcal{E}(t) \neq 0$.

If $\mathcal{E}(t) = 0$, we consider a perturbation "à la Canny" as in [3], i.e. we replace f_i by $f_{i,\lambda} := f_i + \lambda\, x_i^{D_i} \in K(\lambda)[\boldsymbol{x}]$, where λ is a new parameter, for $1 \leqslant i \leqslant n$. It is easy to see that this perturbed system has no roots at infinity over the algebraic closure $\overline{K(\lambda)}$ of $K(\lambda)$, since the leading term in λ of the resultant of its homogeneous components of degrees $D_1, \ldots, D_n$ does not vanish, and hence the dimension of the quotient ring $A_\lambda := K(\lambda)[\boldsymbol{x}]/(f_{1,\lambda}, \ldots, f_{n,\lambda})$ as a $K(\lambda)$-vector space is also equal to D.

It can also be shown (see [3]) that $\mathcal{E}_\lambda(t) \neq 0$, where $\mathcal{E}_\lambda(t)$ denotes the extraneous factor in Macaulay's formulation applied to the polynomials $f_{i,\lambda},\ 1 \leqslant i \leqslant n$. Indeed, if E_t is the matrix whose determinant gives $\mathcal{E}(t)$ with rows and columns ordered properly, it is easy to see that the perturbed matrix is equal to $E_t + \lambda\, I$, where I is the identity matrix.

Therefore, the statement holds for this perturbed family:

$$\Delta_{\mathcal{S}}(f_{1,\lambda}, \ldots, f_{n,\lambda}, f_{n+1}) = \pm\left(\prod_{j=t-D_{n+1}+1}^{t} \widetilde{\Delta}_{\mathcal{T}_j,\lambda}\right)\frac{\det\left(\mathcal{O}_{\mathcal{S}}(\Gamma_\lambda)\right)}{\det\left(V_{\mathcal{T}}(\Gamma_\lambda)\right)} \tag{14}$$

for *any* basis Γ_λ of A_λ^* (here, $\widetilde{\Delta}_{\mathcal{T}_j,\lambda} = \Delta_{\mathcal{T}_j}^{(j)}(\widetilde{f}_{1,\lambda}, \ldots, \widetilde{f}_{n,\lambda})$).

The subresultants appearing in (14) are polynomials in λ, that, when evaluated in $\lambda = 0$, satisfy:

$$\Delta_{\mathcal{S}}(f_{1,\lambda}, \ldots, f_{n,\lambda}, f_{n+1})\big|_{\lambda=0} = \Delta_{\mathcal{S}}(f_1, \ldots, f_n, f_{n+1}),\ \ \widetilde{\Delta}_{\mathcal{T}_j,\lambda}\Big|_{\lambda=0} = \widetilde{\Delta}_{\mathcal{T}_j},\ \forall j.$$

So, in order to prove the claim, it is enough to show that there exists a basis of A_λ^* which "specializes" to Λ when setting $\lambda = 0$, i.e. to find a basis Λ_λ of A_λ^* such that

$$\left.\frac{\det\left(\mathcal{O}_{\mathcal{S}}(\boldsymbol{\Lambda}_\lambda)\right)}{\det\left(V_{\mathcal{T}}(\boldsymbol{\Lambda}_\lambda)\right)}\right|_{\lambda=0} = \frac{\det\left(\mathcal{O}_{\mathcal{S}}(\boldsymbol{\Lambda})\right)}{\det\left(V_{\mathcal{T}}(\boldsymbol{\Lambda})\right)}, \tag{15}$$

and then to apply Identity (14) to $\boldsymbol{\Lambda}_\lambda$ and to specialize it at $\lambda = 0$.

We now construct the basis Λ_λ: The monomial basis $\mathcal{T} = \{\boldsymbol{x}^{\boldsymbol{\alpha}_1}, \ldots, \boldsymbol{x}^{\boldsymbol{\alpha}_D}\}$ of A is also a monomial basis of A_λ, since clearly linearly independent, and therefore it defines the dual bases $\{\boldsymbol{y}_{\boldsymbol{\alpha}_1}, \ldots, \boldsymbol{y}_{\boldsymbol{\alpha}_D}\} \subset A^*$ and $\{\boldsymbol{y}_{\boldsymbol{\alpha}_1,\lambda}, \ldots, \boldsymbol{y}_{\boldsymbol{\alpha}_D,\lambda}\} \subset A_\lambda^*$, satisfying for $1 \leqslant j, k \leqslant D$,

$$\boldsymbol{y}_{\boldsymbol{\alpha}_k}(\boldsymbol{x}^{\boldsymbol{\alpha}_j}) = \boldsymbol{y}_{\boldsymbol{\alpha}_k,\lambda}(\boldsymbol{x}^{\boldsymbol{\alpha}_j}) = 1 \ \text{ if } \ k = j \ \text{ and } \ 0 \ \text{ otherwise}\,.$$

We write $\Lambda_i = \sum_{k=1}^{D} c_{ik}\boldsymbol{y}_{\boldsymbol{\alpha}_k}$ for $1 \leqslant i \leqslant D$, where $c_{ik} \in K$, and then set $\Lambda_\lambda := \{\Lambda_{1,\lambda}, \ldots, \Lambda_{D,\lambda}\}$, with $\Lambda_{i,\lambda} := \sum_{k=1}^{D} c_{ik}\boldsymbol{y}_{\boldsymbol{\alpha}_k,\lambda},\ 1 \leqslant i \leqslant D$. Note that

$$\Lambda_{i,\lambda}(\boldsymbol{x}^{\boldsymbol{\alpha}_j}) = \Lambda_i(\boldsymbol{x}^{\boldsymbol{\alpha}_j}) = c_{ij} \ \text{ for } \ 1 \leqslant i, j \leqslant D, \tag{16}$$

$$\det\left(V_{\mathcal{T}}(\Lambda_\lambda)\right) = \det\left(V_{\mathcal{T}}(\Lambda)\right) = \det\left(c_{ij}\right)_{1\leqslant i,j\leqslant D} \in K \setminus \{0\}, \tag{17}$$

as the matrix $(c_{ij})_{1\leqslant i,j\leqslant D}$ is invertible. This implies that Λ_λ is a basis of A_λ^*.

We claim now that, for every $\boldsymbol{\alpha} \in \mathbb{N}^n$, there exist polynomials $p_{\boldsymbol{\alpha}}$ and $A_{j,\boldsymbol{\alpha}},\ 1 \leqslant j \leqslant D$, in $K[\lambda]$ such that

$$p_{\boldsymbol{\alpha}}(\lambda)\,\boldsymbol{x}^{\boldsymbol{\alpha}} = \sum_{j=1}^{D} A_{j,\boldsymbol{\alpha}}(\lambda)\boldsymbol{x}^{\boldsymbol{\alpha}_j} \ \text{ in } \ A_\lambda, \quad \text{and} \quad p_{\boldsymbol{\alpha}}(0) \neq 0. \tag{18}$$

For this, it suffices to express the monomial $\boldsymbol{x}^{\boldsymbol{\alpha}}$ in terms of the basis $\mathcal{T}$ of A_λ and take $p_{\boldsymbol{\alpha}}(\lambda)$ as a common denominator when lifting the expression to $K[\lambda][\boldsymbol{x}]$, satisfying the condition $\gcd\left(p_{\boldsymbol{\alpha}},\, A_{j,\boldsymbol{\alpha}},\, 1 \leqslant j \leqslant D\right) = 1$. It is clear that $p_{\boldsymbol{\alpha}}(0) \neq 0$ because $\mathcal{T}$ is also a basis of A, and by assumption 0 is not a common root of $p_{\boldsymbol{\alpha}}$ and $A_{j,\boldsymbol{\alpha}}$, $1 \leqslant j \leqslant D$.

Applying $\Lambda_{i,\lambda}$ to Identity (18) and Λ_i to Identity (18) specialized at $\lambda = 0$, we then get by (16) for $1 \leqslant i \leqslant D$:

$$p_{\boldsymbol{\alpha}}(\lambda)\Lambda_{i,\lambda}(\boldsymbol{x}^{\boldsymbol{\alpha}}) = \sum_{j=1}^{D} c_{ij}A_{j,\boldsymbol{\alpha}}(\lambda) \text{ and } p_{\boldsymbol{\alpha}}(0)\Lambda_i(\boldsymbol{x}^{\boldsymbol{\alpha}}) = \sum_{j=1}^{D} c_{ij}A_{j,\boldsymbol{\alpha}}(0).$$

This implies that the entries of the matrix $\mathcal{O}_{\mathcal{S}}(\Lambda_\lambda)$ are the same K-linear combinations of the quotients $\frac{A_{j,\boldsymbol{\alpha}}(\lambda)}{p_{\boldsymbol{\alpha}}(\lambda)}$ as the entries of the matrix $\mathcal{O}_{\mathcal{S}}(\Lambda)$ in terms of $\frac{A_{j,\boldsymbol{\alpha}}(0)}{p_{\boldsymbol{\alpha}}(0)}$. This and Identity (17) implies (15), which proves the statement. $\square$

As we mentioned before, for an arbitrary basis Λ of A^* the expression in Theorem 3.4 may not provide a formula in terms of the roots of $f_1, \ldots, f_n$. In order to obtain one, we recall here the notion of Gröbner duality from [23].

For $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ define the differential operator

$$\partial_{\boldsymbol{\alpha}} := \frac{1}{\alpha_1! \cdots \alpha_n!}\, \frac{\partial^{|\boldsymbol{\alpha}|}}{\partial x_1^{\alpha_1} \cdots \partial x_n^{\alpha_n}}$$

and consider the ring $K[[\partial]] := \{\sum_{\boldsymbol{\alpha}\in\mathbb{N}^n} a_{\boldsymbol{\alpha}}\partial_{\boldsymbol{\alpha}} : a_{\boldsymbol{\alpha}} \in K\}$.

For $1 \leqslant i \leqslant n$ define the K-linear map

$$\sigma_i : K[[\partial]] \to K[[\partial]];\ \sigma_i\left(\partial_{\boldsymbol{\alpha}}\right) = \begin{cases} \partial_{(\alpha_1,\ldots,\alpha_i-1,\ldots,\alpha_n)} & \text{if } \alpha_i > 0, \\ 0 & \text{otherwise,} \end{cases}$$

and for $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$ define $\sigma_{\boldsymbol{\beta}} = \sigma_1^{\beta_1} \circ \cdots \circ \sigma_n^{\beta_n}$.

A K-vector space $V \subset K[[\partial]]$ is *closed* if $\dim_K(V)$ is finite and for all $\boldsymbol{\beta} \in \mathbb{N}^n$ and $\mathbf{D} \in V$ we have $\sigma_{\boldsymbol{\beta}}(\mathbf{D}) \in V$. Note that $K[[\partial]]$ and its closed subspaces have a natural $K[\boldsymbol{x}]$-module structure given by $\boldsymbol{x}^{\boldsymbol{\beta}}\mathbf{D}(f) := \mathbf{D}(\boldsymbol{x}^{\boldsymbol{\beta}}f) = \sigma_{\boldsymbol{\beta}}(\mathbf{D})(f)$.

Let $\boldsymbol{\xi} \in K^n$. For a closed subspace $V \subset K[[\partial]]$ define

$$\nabla_{\boldsymbol{\xi}}(V) := \{f \in K[\boldsymbol{x}] \ :\ \mathbf{D}(f)(\boldsymbol{\xi}) = 0,\quad \forall\, \mathbf{D} \in V\} \subset K[\boldsymbol{x}].$$

Let $\mathbf{m}_{\boldsymbol{\xi}} \subset K[\boldsymbol{x}]$ be the maximal ideal defining $\boldsymbol{\xi}$. For an ideal $J \subset \mathbf{m}_{\xi}$ define

$$\Delta_{\boldsymbol{\xi}}(J) := \{\mathbf{D} \in K[[\partial]] \ :\ \mathbf{D}(f)(\boldsymbol{\xi}) = 0,\quad \forall f \in J\} \subset K[[\partial]].$$

Then the following theorem gives the so called Gröbner duality:

Theorem 3.5 [15,23]. *Fix $\boldsymbol{\xi} \in K^n$. The correspondences between closed subspaces $V \subset K[[\partial]]$ and $\mathbf{m}_{\xi}$-primary ideals Q, $V \mapsto \nabla_{\boldsymbol{\xi}}(V)$ and $Q \mapsto \Delta_{\boldsymbol{\xi}}(Q)$ are 1-1 and satisfy $V = \Delta_{\boldsymbol{\xi}}(\nabla_{\boldsymbol{\xi}}(V))$ and $Q = (\nabla_{\boldsymbol{\xi}}(\Delta_{\boldsymbol{\xi}}(Q)))$. Moreover,*

$$\dim_K(\Delta_{\boldsymbol{\xi}}(Q)) = \mathrm{mult}(Q) \quad \textit{and} \quad \mathrm{mult}(\nabla_{\boldsymbol{\xi}}(V)) = \dim_K(V).$$

We set $Z := \{\boldsymbol{\xi}_1, \ldots, \boldsymbol{\xi}_D\}$ for the set of all common roots of $f_1, \ldots, f_n$ in K^n, with multiplicities, and $\mathbf{m}_{\xi_i} \subset K[\boldsymbol{x}]$ for the maximal ideal corresponding to $\boldsymbol{\xi}_i$ for $1 \leqslant i \leqslant m$.

Example 3.6 [12, Exemple 7.37]. Let $f_1 = 2x_1x_2^2 + 5x_1^4, f_2 = 2x_1^2x_2 + 5x_2^4 \in \mathbb{C}[x, y]$.

Then $Z = \{\mathbf{0}, \boldsymbol{\xi}_1, \boldsymbol{\xi}_2, \boldsymbol{\xi}_3, \boldsymbol{\xi}_4, \boldsymbol{\xi}_5\}$ where $\mathbf{0} = (0, 0)$ has multiplicity eleven and $\boldsymbol{\xi}_i = (\frac{-2}{5\xi^{2i}}, \frac{-2}{5\xi^{3i}})$ where ξ is a primitive 5-th root of unity, are all simple, $1 \leqslant i \leqslant 5$.

Denote by $Q_{\mathbf{0}}, Q_{\boldsymbol{\xi}_i}, 1 \leqslant i \leqslant 5$, the primary ideals corresponding to the roots, then $\Delta_{\boldsymbol{\xi}_i}(Q_{\boldsymbol{\xi}_i}) = \langle 1 \rangle$ for $1 \leqslant i \leqslant 5$ and if $\{\boldsymbol{e}_1, \boldsymbol{e}_2\}$ is the canonical basis of $\mathbb{Z}^2$,

$$\begin{aligned}\Delta_{\mathbf{0}}(Q_{\mathbf{0}}) =& \langle 1,\ \partial_{\boldsymbol{e}_1},\ \partial_{\boldsymbol{e}_2},\ \partial_{2\boldsymbol{e}_1},\ \partial_{\boldsymbol{e}_1+\boldsymbol{e}_2},\ \partial_{2\boldsymbol{e}_2},\ \partial_{3\boldsymbol{e}_1},\ \partial_{3\boldsymbol{e}_2},\\ & (4\partial_{4\boldsymbol{e}_1} - 5\partial_{\boldsymbol{e}_1+2\boldsymbol{e}_2}),\ (4\partial_{4\boldsymbol{e}_2} - 5\partial_{2\boldsymbol{e}_1+\boldsymbol{e}_2}), (3\partial_{2\boldsymbol{e}_1+3\boldsymbol{e}_2} - \partial_{5\boldsymbol{e}_1} - \partial_{5\boldsymbol{e}_2})\rangle.\end{aligned}$$

Using Gröbner duality, we are now able to give an expression for the subresultant in terms of the roots of $f_1, \ldots, f_n$. For $\mathbf{D} \in K[[\partial]]$and $\boldsymbol{\xi} \in K^n$, we denote by $\mathbf{D}|_{\boldsymbol{\xi}}$ the element of A^* defined as $\mathbf{D}|_{\boldsymbol{\xi}}(f) = \mathbf{D}(f)(\boldsymbol{\xi})$. In particular, under this notation, $1|_{\boldsymbol{\xi}} = \mathrm{ev}_{\boldsymbol{\xi}}$.

Corollary 3.7. *Using our previous assumptions, let $I = (f_1, \ldots, f_n)$ and*

$$I = Q_1 \cap \cdots \cap Q_m$$

be the primary decomposition of I, where Q_i is a $\mathbf{m}_{\boldsymbol{\xi}_i}$-primary ideal with $d_i := \mathrm{mult}(Q_i)$. For $1 \leqslant i \leqslant m$ let $V_i := \Delta_{\boldsymbol{\xi}_i}(Q_i) \subset K[[\partial]]$ be the corresponding closed subspace, and fix a basis $\{\mathbf{D}_{i,1}, \ldots, \mathbf{D}_{i,d_i}\}$ for V_i such that $\mathbf{D}_{i,1} = 1$. Then

$$\Lambda := \{\mathbf{D}_{1,1}|_{\boldsymbol{\xi}_1}, \ldots, \mathbf{D}_{1,d_1}|_{\boldsymbol{\xi}_1}, \ldots, \mathbf{D}_{m,1}|_{\boldsymbol{\xi}_m}, \ldots, \mathbf{D}_{m,d_m}|_{\boldsymbol{\xi}_m}\}$$

is a basis of A^* over K.

Note that the above choice for the dual basis Λ contains the evaluation maps for the roots of I, and using this Λ in Theorem 3.4 gives an expression for the subresultant in terms of the roots of I.

Example 3.8. This is a very simple example containing an expression for a subresultant in terms of the roots.

Let $f_1 := x_1x_2,\ f_2 := x_1^2 + (x_2 - 1)^2 - 1,\ f_3 := c_0 + c_1x_1 + c_2x_2$, with $c_0,\ c_1,\ c_2 \in \mathbb{C}$. Then $Z = \{(0, 0), (0, 2)\}$ where $(0, 0)$ has multiplicity 3 and $(0, 2)$ is simple. By computing explicitly, we check that $\mathcal{T} := \{1, x_1, x_2, x_2^2\}$ is a basis of $A = \mathbb{C}[x_1, x_2]/(f_1, f_2)$ and that

$$\Lambda := \left\{1|_{(0,0)}, \partial_{\boldsymbol{e}_1}|_{(0,0)}, (\partial_{\boldsymbol{e}_2} + 2\partial_{2\boldsymbol{e}_1})|_{(0,0)}, 1|_{(0,2)}\right\}$$

is a basis of A^*. We will use these bases to express the degree $t = \rho = 2$ subresultant $\Delta_{x_1^2}(f_1, f_2, f_3)$ with $\mathcal{S} = \{x_1^2\}$ in terms of the roots of f_1, f_2. First, $\Delta_{x_1^2}(f_1, f_2, f_3)$ is equal to the following 6×6 determinant (since here the extraneous factor is 1):

$$\Delta_{x_1^2}(f_1, f_2, f_3) = \det M_{\mathcal{S}} = \det \begin{vmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -2 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ c_0 & c_1 & c_2 & 0 & 0 & 0 \\ 0 & c_0 & 0 & c_1 & c_2 & 0 \\ 0 & 0 & c_0 & 0 & c_1 & c_2 \end{vmatrix} = c_0^3 + 2c_0^2c_2.$$

On the other hand, Theorem 3.4 gives the following expression:

$$\left(\prod_{j=2}^{2}\widetilde{\Delta}_{\mathcal{T}_j}\right)\frac{\det \mathcal{O}_{\mathcal{S}}(\Lambda)}{\det V_{\mathcal{T}}(\Lambda)} = \frac{\det\begin{vmatrix} 0 & 0 & 2 & 0 \\ c_0 & c_1 & c_2 & c_0+2c_2 \\ 0 & c_0 & 2c_1 & 0 \\ 0 & 0 & c_0 & 2c_0+4c_2 \end{vmatrix}}{\det\begin{vmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 4 \end{vmatrix}} = \frac{4(c_0^3+2c_0^2c_2)}{4},$$

using that $\mathcal{T}_2 = \{x_2^2\}$ is the degree 2 part of $\mathcal{T}$, and

$$\widetilde{\Delta}_{\mathcal{T}_2}(\widetilde{f}_1,\widetilde{f}_2) = \det\begin{vmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{vmatrix} = 1.$$

Acknowledgements

We wish to thank the referee for her/his careful reading and comments. A preliminary version of these results was presented at the MEGA 2009 Conference in Barcelona. Part of this work was done at the Fields Institute in Toronto while the authors were participating in the Fall 2009 Thematic Program on Foundations of Computational Mathematics.

References

[1] A.C. Aitken, Determinants and Matrices, Oliver and Boyd, Edinburgh, 1939. vii + 135 pp.
[2] E. Becker, J.P. Cardinal, M.-F. Roy, Z. Szafraniec, Multivariate Bezoutians, Kronecker symbol and Eisenbud–Levine formula, Progr. Math. 143 (1996) 79–104.
[3] J.F. Canny, Generalised characteristic polynomials, J. Symbolic Comput. 9 (1990) 241–250.
[4] Marc. Chardin, Formules à la Macaulay pour les sous-résultants en plusieurs variables, C. R. Acad. Sci. Paris Sér. I Math. 319 (5) (1994) 433–436.
[5] M. Chardin, Multivariate subresultants, J. Pure Appl. Algebra 101 (2) (1995) 129–138.
[6] D. Cox, J. Little, D. O'Shea, Using Algebraic Geometry, Graduate Text in Mathematics, vol. 185, Springer-Verlag, 1998.
[7] F.G. Csáki, Some notes on the inversion of confluent Vandermonde matrices, IEEE Trans. Automat. Control AC-20 (1975) 154–157.
[8] C. D'Andrea, T. Krick, A. Szanto, Multivariate subresultants in roots, J. Algebra 302 (1) (2006) 16–36.
[9] C. D'Andrea, T. Krick, A. Szanto, Subresultants in multiple roots (extended abstract), Effective Methods in Algebraic Geometry, MEGA'09, Barcelona.
[10] C. D'Andrea, H. Hong, T. Krick, A. Szanto, An elementary proof of Sylvester's double sums for subresultants, J. Symbolic Comput. 42 (3) (2007) 290–297.
[11] C. D'Andrea, H. Hong, T. Krick, A. Szanto, Sylvester's double sums: the general case, J. Symbolic Comput. 44 (9) (2009) 1164–1175.
[12] M. Elkadi, B. Mourrain, Introduction à la résolution des systèmes polynomiaux, Springer-Verlag, 2007.
[13] L. González-Vega, A subresultant theory for multivariate polynomials, Extracta Math. 5 (3) (1990) 150–152.
[14] L. González-Vega, Determinantal formulae for the solution set of zero-dimensional ideals, J. Pure Appl. Algebra 76 (1) (1991) 57–80.
[15] W. Gröbner, Algebraische Geometrie. 2. Teil: Arithmetische Theorie der Polynomringe, Bibliographisches Institut, Mannheim, 1970.
[16] W. Habicht, Zur inhomogenen Eliminationstheorie, Comment. Math. Helv. 21 (1948) 79–98.
[17] H. Hong, Subresultants in roots, Technical Report, Department of Mathematics, North Carolina State University, 1999.
[18] D. Kalman, The generalized Vandermonde matrix, Math. Mag. 57 (1) (1984) 15–21.
[19] M. Kreuzer, E. Kunz, Traces in strict Frobenius algebras and strict complete intersections, J. Reine Angew. Math. 381 (1987) 181–204.
[20] T. Krick, A. Szanto, Sylvester's double sums: an inductive proof of the general case, J. Symbolic Comput. 47 (2012) 942–953.
[21] F. Macaulay, Some formulae in elimination, Proc. London Math. Soc. 33 (1) (1902) 3–27.

[22] F. Macaulay, The Algebraic Theory of Modular Systems, Cambridge University Press, 1916.
[23] M.G. Marinari, T. Mora, H.M. Möller, Gröbner duality and multiplicities in polynomial system solving, in: ISSAC '95: Proceedings of the 1995 International Symposium on Symbolic and Algebraic Computation, ACM Press, New York, NY, USA, 1995, pp. 167–179.
[24] M.-F. Roy, A. Szpirglas, Sylvester double sums and subresultants, J. Symbolic Comput. 46 (2011) 385–395.
[25] A. Spitzbart, A generalization of Hermite's interpolation formula, Amer. Math. Monthly 67 (1960) 42–46.
[26] J.J. Sylvester, On a Theory of Syzygetic Relations of Two Rational Integral Functions, Comprising an Application to the Theory of Sturm's Function and that of the Greatest Agebraical Common Measure, Trans. Roy. Soc., London, 1853. Reprinted in: The Collected Mathematical Papers of James Joseph Sylvester, vol. 1, Chelsea Publ., New York, 1973, pp. 429–586.