Multivariate Subresultants in Roots

Carlos D' Andrea [1]

Department of Mathematics, University of California at Berkeley, CA 94720 USA.

Teresa Krick [2]

Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, 1428 Buenos Aires, Argentina

Agnes Szanto [*,3]

Department of Mathematics, North Carolina State University, Raleigh, NC 27695 USA

Abstract

We give a rational expression for the subresultants of $n+1$ generic polynomials $f_1, \ldots, f_{n+1}$ in n variables as a function of the coordinates of the common roots of $f_1, \ldots, f_n$ and their evaluation in f_{n+1}. We present a simple technique to prove our results, giving new proofs and generalizing the classical Poisson product formula for the projective resultant, as well as the expressions of Hong for univariate subresultants in roots.

Key words: subresultants, Poisson product formula, Vandermonde determinants.

1 Introduction

The classical Poisson product formula for resultants of univariate polynomials can be stated as follows: if f and g are two univariate polynomials of degrees

* Corresponding author.
Email addresses: `cdandrea@math.berkeley.edu` (Carlos D' Andrea), `krick@dm.uba.ar` (Teresa Krick), `aszanto@ncsu.edu` (Agnes Szanto).

[1] Research supported by the Miller Institute for Basic Research in Science, UC Berkeley
[2] Research supported by grants CONICET PIP 2461/01 and UBACYT X-112.
[3] Research supported by NSF grants CCR-0306406 and CCR-0347506.

d_1 and d_2 respectively, with $g = b_{d_2}(x-\xi_1)\cdots(x-\xi_{d_2})$, then the resultant of f and g can be expressed as

$$\mathrm{Res}(f,g) = (-1)^{d_1 d_2}\, b_{d_2}^{d_1} \prod_{j=1}^{d_2} f(\xi_j). \tag{1}$$

The main result of this paper is a generalization of Formula (1) for univariate and multivariate subresultants (see Theorems 2.2 and 3.2). Although most of the results in the univariate case already appeared in [17,18,23,9], here we present simple techniques that enable us to reobtain them (see Theorem 2.2 and Corollary 2.6) and allow us to generalize them to the multivariate case.

Resultants and subresultants of two univariate polynomials go back to Leibniz, Euler, Bézout and Jacobi. We refer to [12] for historical references. In their modern form, subresultants were introduced by Sylvester in [26]. They have been used to give an efficient and parallelizable algorithm for computing the greatest common divisor of two polynomials [7,3,15,10,19,20,25]. More recently they were also applied in symbolic-numeric computation [11,31,22,30].

Multivariate resultants were mainly introduced by Macaulay in [24], after earlier work by Euler, Sylvester and Cayley, while multivariate subresultants were first defined by Gonzalez-Vega in [13,14], generalizing Habicht's method [16]. The notion of subresultants that we use in the present paper was introduced by Chardin in [5]. It works as follows: let $f_1^h,\dots,f_s^h$ be a system of generic homogeneous polynomials in $K[x_0,x_1,\dots,x_n]$ of degrees $d_i = \deg(f_i^h)$ with parametric coefficients, where $s \le n+1$ and K is the coefficient field of $f_1^h,\dots,f_s^h$. Let $\mathcal{H}_{d_1,\dots,d_s} : \mathbb{N} \to \mathbb{N}$ be the Hilbert function of a complete intersection given by s homogeneous polynomials in $n+1$ variables of degrees $d_1,\dots,d_s$. Fix $t \in \mathbb{N}$ and let $\mathcal{S}$ be a set of $\mathcal{H}_{d_1,\dots,d_s}(t)$ monomials of degree t. The *subresultant* $\Delta_{\mathcal{S}}$ is a polynomial in K whose degree in the coefficients of f_i^h is $\mathcal{H}_{d_1,\dots,d_{i-1},d_{i+1},\dots,d_s}(t-d_i)$ for $i=1,\dots,s$, having the following universal property: $\Delta_{\mathcal{S}}$ vanishes at a particular coefficient specialization $\tilde{f}_1^h,\dots,\tilde{f}_s^h \in \mathbb{C}[x_0,\dots,x_n]$ if and only if $I_t \cup \mathcal{S}$ does not generate the space of all forms of degree t. Here, I_t is the degree t part of the ideal generated by the $\tilde{f}_i^h$'s (see [5]).

The constructions in [13,5] generalize the classical univariate subresultants in the sense that they provide the coefficients of certain polynomials in I_t, which in the univariate case include the greatest common divisor of two given polynomials.

Theoretical properties and applications of multivariate subresultants are active areas of research. A series of recent publications explored: their application to solve zero dimensional [14] and over-constrained polynomial systems [28], in the inverse parametrization problem of rational surfaces [1]; their irreducibility and connection with residual resultants [2]; the generalization of their universal properties to the affine well-constrained case [8]; as well as generalizations of matrix constructions for subresultants [27].

Multivariate subresultants also encapsulate as a particular case the classical projective resultant $\operatorname{Res}(f_1^h, \ldots, f_{n+1}^h)$, which is defined to be an irreducible polynomial in the coefficients of the f_i^h's which vanishes at a particular coefficient specialization $\tilde{f}_1^h, ..., \tilde{f}_{n+1}^h \in \mathbb{C}[x_0, \ldots, x_n]$ if and only if $\tilde{f}_1^h, ..., \tilde{f}_{n+1}^h$ have a common root in the complex projective space $\mathbb{P}_{\mathbb{C}}^n$.

There is an affine interpretation of the resultant that can be stated as follows: Set

$$f_i := f_i^h(1, x_1, \ldots, x_n),\ \overline{f}_i := f_i^h(0, x_1, \ldots, x_n),\ i = 1, \ldots n+1.$$

Due to Bézout's Theorem, the cardinality of the set

$$V(f_1, \ldots, f_n) := \{\xi \in \overline{K}^n : f_1(\xi) = f_2(\xi) = \ldots = f_n(\xi) = 0\}$$

equals $d_1 \ldots d_n$ (here, overline denotes algebraic closure), and the classical Poisson product formula [29,6,21], which generalizes (1), states that the following identity holds in $\overline{K}$

$$\operatorname{Res}(f_1^h, ..., f_{n+1}^h) = \operatorname{Res}(\overline{f}_1, \ldots, \overline{f}_n)^{d_{n+1}} \prod_{\xi \in V(f_1, \ldots, f_n)} f_{n+1}(\xi). \tag{2}$$

In order to make this formula a generalization of (1), we have to define resultants of non-homogeneous polynomials. The obvious generalization is $\operatorname{Res}(g_1, \ldots, g_{n+1}) := \operatorname{Res}(g_1^h, ..., g_{n+1}^h)$, where g_j^h is the homogenization of g_j. The same extension to affine polynomials holds for subresultants. It should also be mentioned that the Poisson formula (2) is a particular case of the determinant of a multiplication map in a quotient ring (see [21, Prop. 2.7]).

In Theorem 3.2 we generalize (2) and give an expression for *any* multivariate subresultant as a ratio of two determinants times a function of the coefficients of $\overline{f}_1, \ldots, \overline{f}_n$. The determinant in the denominator is a Vandermonde type determinant depending on the common roots of $f_1, \ldots, f_n$, while the determinant in the numerator depends on evaluations of the common roots of $f_1, \ldots, f_n$ in the last polynomial f_{n+1}.

The paper is structured as follows: in Section 2, we present in detail the univariate case, showing how to derive with our techniques Hong's expressions for subresultants of two univariate polynomials in the roots of one of them and the coefficients of the other. The details in the univariate case are essential for the generalization to the multivariate case: they allow to identify the extraneous factor which is non-trivial in the multivariate case and they also allow to handle the generality of the monomial sets appearing in the definition of multivariate subresultants. In Section 3, we deal with the general case.

In order to keep coherence with the classical literature and previous works, the presentation in the univariate case is done in the traditional way, i.e. for non-homogeneous polynomials, while in the multivariate case the reader should be aware that the notions involve homogeneous polynomials.

Acknowledgements: This work started during a visit of the first two authors to North Carolina State University in the Fall Semester 2004. We would like to thank the Department of Mathematics for their hospitality and for the stimulating working atmosphere it provided. A previous version of this paper was presented in Mega'05. We thank the anonymous referees of that previous version for introducing us to discrete Wrónskians as presented in [23] and for pointing us other related references.

2 The univariate case

Classical scalar and polynomial subresultants

We review here the definition and some well-known properties of the classical univariate resultant and scalar subresultants and polynomial subresultants.

Let $f = a_{d_1}x^{d_1} + \ldots + a_0$ and $g := b_{d_2}x^{d_2} + \ldots + b_0 = b_{d_2}(x - \xi_1)\cdots(x - \xi_{d_2})$, $a_{d_1} \neq 0$, $b_{d_2} \neq 0$, be two polynomials of degrees d_1 and d_2 respectively with coefficients in a field K and roots in the algebraic closure $\overline{K}$.

The *scalar subresultant* $S_k^{(j)}$ of f and g is defined for $0 \leq j \leq j \leq \min\{d_1, d_2\}$ as the following determinant:

$$S_k^{(j)} := \det \overbrace{\left|\begin{array}{ccccc} a_{d_1} & \cdots & \cdots & a_{k+1-(d_2-k-1)} & a_{j-(d_2-k-1)} \\ & \ddots & & \vdots & \vdots \\ & & a_{d_1} \cdots & a_{k+1} & a_j \\ \hline b_{d_2} & \cdots & \cdots & b_{k+1-(d_1-k-1)} & b_{j-(d_1-k-1)} \\ & \ddots & & \vdots & \vdots \\ & & b_{d_2} \cdots & b_{k+1} & b_j \end{array}\right|}^{d_1+d_2-2k} \begin{array}{l} d_2 - k \\ \\ \\ d_1 - k \end{array} \qquad (3)$$

where $a_\ell = b_\ell = 0$ for $\ell < 0$.

The *subresultant polynomial* $\mathrm{Sres}_k(f,g)$ is defined for $0 \le k \le \min\{d_1, d_2\}$ as

$$\mathrm{Sres}_k(f,g) := \sum_{j=0}^{k} S_k^{(j)} x^j.$$

When $k=0$, $\mathrm{Sres}_0(f,g) = S_0^{(0)}$ coincides with the classical *resultant* $\mathrm{Res}(f,g)$ which arose historically when checking if f and g have a common factor:

$$\gcd(f,g) = 1 \iff \mathrm{Res}(f,g) \neq 0.$$

In an analogous way, the scalar subresultants satisfy the following property:

$$\deg \gcd(f,g) = k \quad \iff \quad S_\ell^{(\ell)} = 0 \text{ for } 0 \le \ell < k \text{ and } S_k^{(k)} \neq 0,$$

and the polynomial subresultants $\mathrm{sres}_k(f,g)$ are determinant expressions for modified remainders in the Euclidean algorithm. In particular, for the first k such that $S_k^{(k)} \neq 0$, the monic gcd of f and g satisfies:

$$\gcd(f,g) = (S_k^{(k)})^{-1} \mathrm{sres}_k(f,g).$$

There is a generalization of the univariate Poisson product formula (1) for the polynomial subresultant $\mathrm{sres}_k(f,g)$, as shown by Hong in [17, Th. 3.1], see also [23, Formula 9.3.2] and [9, Sec. 5]:

$$\mathrm{sres}_k(f,g) = (-1)^{(d_1-k)(d_2-k)} b_{d_2}^{d_1-k} \frac{\begin{vmatrix} (x-\xi_1)\xi_1^0 & \cdots & (x-\xi_{d_2})\xi_{d_2}^0 \\ \vdots & & \vdots \\ (x-\xi_1)\xi_1^{k-1} & \cdots & (x-\xi_{d_2})\xi_{d_2}^{k-1} \\ \xi_1^0 f(\xi_1) & \cdots & \xi_{d_2}^0 f(\xi_{d_2}) \\ \vdots & & \vdots \\ \xi_1^{d_2-k-1} f(\xi_1) & \cdots & \xi_{d_2}^{d_2-k-1} f(\xi_{d_2}) \end{vmatrix}}{\begin{vmatrix} \xi_1^0 & \cdots & \xi_{d_2}^0 \\ \vdots & & \vdots \\ \xi_1^{d_2-1} & \cdots & \xi_{d_2}^{d_2-1} \end{vmatrix}}. \qquad (4)$$

(Here the sign is due to the fact that we consider f on the roots of g instead of g on the roots of f as done in [17].)

Notations:

As we mentioned earlier, most of the results we obtain in this section are not new. However, we consider important to illustrate our technique by applying it to the univariate case, since it helps to understand its generalization to the multivariate setting. The choices of notations we made here are accordingly motivated by their coherence with the multivariate case. They correspond to Chardin's notion of subresultants [5] applied to the univariate case, a slight generalization of the usual notion of scalar subresultants.

- $f := a_0 + a_1 x + \ldots + a_{d_1} x^{d_1}$ and $g := b_0 + b_1 x + \ldots + b_{d_2} x^{d_2}$ in $K[x]$, where $K := \mathbb{Q}(a_0, \ldots, a_{d_1}, b_0, \ldots, b_{d_2})$, with $a_0, \ldots, a_{d_1}, b_0, \ldots, b_{d_2}$ algebraically independent variables over $\mathbb{Q}$ (representing the indeterminate coefficients of two generic polynomials f and g of degrees d_1 and d_2 respectively).
- $\{\xi_1, \ldots, \xi_{d_2}\}$ denotes the set of roots of g in $\overline{K}$ (recall that overline denotes algebraic closure), and $\mathcal{V}_{d_2} := \det(\xi_j^{i-1})_{1 \le i,j \le d_2}$ the Vandermonde determinant associated to this set.
- For any $j \in \mathbb{Z},\ K[x]_j := \{0\} \cup \{f \in K[x] : \deg f \le j\}$. Note that if $j < 0$, then $K[x]_j = \{0\}$.
- We set $t \in \mathbb{Z}$ such that $0 \le t \le d_1 + d_2 - 1$, and let $t^* := \max\{d_2 - 1, t\}$.
- $M_f \in K^{(t-d_1+1)\times(t^*+1)}$ and $M_g \in K^{(t-d_2+1)\times(t^*+1)}$ denote the transposes of the matrices in the monomial bases of the composition of the Sylvester multiplication maps and the inclusion $K[x]_t \to K[x]_{t^*}$:

$$\begin{array}{rcl} \mu_f : K[x]_{t-d_1} & \to & K[x]_{t^*} \\ x^\alpha & \mapsto & x^\alpha f(x) \end{array} \quad \text{and} \quad \begin{array}{rcl} \mu_g : K[x]_{t-d_2} & \to & K[x]_{t^*} \\ x^\beta & \mapsto & x^\beta g(x) \end{array},$$

  where the monomials indexing the rows and columns of these matrices are ordered "increasingly" $1,\ x,\ x^2,\ \ldots$. Namely

$$M_f = \left[\begin{array}{ccc|c} a_0 \ldots a_{d_1} & & & \\ \ddots & & \ddots & \mathbf{0} \\ & & a_0 \ldots a_{d_1} & \end{array}\right],\ M_g = \left[\begin{array}{ccc|c} b_0 \ldots b_{d_2} & & & \\ \ddots & & \ddots & \mathbf{0} \\ & & b_0 \ldots b_{d_2} & \end{array}\right].$$

  Note that if $t < d_1$ then $M_f = \emptyset$ (the empty matrix), and if $t < d_2$ then $M_g = \emptyset$.
- We set

$$\begin{aligned} k &:= t + 1 - \dim\left(K[x]_{t-d_1}\right) - \dim\left(K[x]_{t-d_2}\right) \\ &= t + 1 - \max\{0, t - d_1 + 1\} - \max\{0, t - d_2 + 1\} \\ &= t + 1 - \max\{0, t - d_1 + 1\} - (t^* - d_2 + 1). \end{aligned} \tag{5}$$

  Note that $k \ge 0$ since $t \le d_1 + d_2 - 1$.
- $\mathcal{S} := \{x^{\gamma_1}, \ldots, x^{\gamma_k};\ 0 \le \gamma_1 < \cdots < \gamma_k \le t\} \subset K[x]_t$, a fixed set of k monomials of degree bounded by t.

- $\mathrm{sg}(\mathcal{S}) := (-1)^{\sigma}$ where σ is a number of transpositions needed to bring $(1, x, x^2, \ldots, x^{t^*})$ to

$$(x^{\gamma_1}, \ldots, x^{\gamma_k}, x^{t+1}, \ldots, x^{t^*}, 1, x, \ldots, x^{\gamma_1 - 1}, x^{\gamma_1 + 1}, \ldots, x^{\gamma_2 - 1}, x^{\gamma_2 + 1}, \ldots, x^{t}).$$

- $\Delta_{\mathcal{S}} := \Delta_{\mathcal{S}}^{(t)}(f, g)$ denotes the *order t subresultant of f, g with respect to $\mathcal{S}$*, i.e. the determinant of the matrix whose $\max\{0, t - d_1 + 1\}$ first rows are M_f, whose $\max\{0, t - d_2 + 1\}$ following rows are M_g and from which one deletes the $k + t^* - t$ columns indexed by $\mathcal{S} \cup \{x^{t+1}, \ldots, x^{t^*}\}$.

Remark 2.1 The order t subresultant of f, g with respect to $\mathcal{S}$ coincides (up to a sign) with the scalar subresultant when making special choices of t and $\mathcal{S}$:

(1) When $t = d_1 + d_2 - 1$, then $k = t + 1 - d_2 - d_1 = 0$ and $\mathcal{S} = \emptyset$. In that case, from the definitions of $\mathrm{Res}(f, g)$ and $\Delta_{\emptyset}$ one gets that $\Delta_{\emptyset} = (-1)^{d_1 d_2}\,\mathrm{Res}(f, g)$.

(2) For $0 \le k \le \min\{d_1, d_2\}$ and $t := d_1 + d_2 - k - 1$, we can take $\mathcal{S}_j := \{x^i, 0 \le i \le k, i \ne j\}$. In that case, from the definition of $\Delta_{\mathcal{S}_j}$ and (3) one gets that $\Delta_{\mathcal{S}_j} = (-1)^{(d_1 - k)(d_2 - k)} S_k^{(j)}$.

The main statement of this section corresponds to (a slight generalization of) Hong's theorem [18, Th. 3.1]. It expresses $\Delta_{\mathcal{S}}$ as the ratio of discrete Wrónskians: we refer to [23, Sec. 9.3] for an introduction to the subject. Here we present a new simple proof of this result, that we generalize in the next section to the multivariate setting.

Theorem 2.2 *Let $f, g \in K[x]$ and $\{\xi_1, \ldots, \xi_{d_2}\}$ be the set of roots of g in $\overline{K}$. Then, under the previous notations, for any fixed t, $0 \le t \le d_1 + d_2 - 1$, and for any $\mathcal{S} = \{x^{\gamma_1}, \ldots, x^{\gamma_k}\} \subset K[x]_t$ of cardinality k, with k defined in (5), the order t subresultant $\Delta_{\mathcal{S}}$ of f, g with respect to $\mathcal{S}$ satisfies:*

$$\Delta_{\mathcal{S}} = sg(\mathcal{S})\, b_{d_2}^{t^* - d_2 + 1}\, \frac{|\mathcal{O}_{\mathcal{S}}|}{\mathcal{V}_{d_2}},$$

where

$$\mathcal{O}_{\mathcal{S}} = \left[\begin{array}{ccc} \xi_1^{\gamma_1} & \cdots & \xi_{d_2}^{\gamma_1} \\ \vdots & & \vdots \\ \xi_1^{\gamma_k} & \cdots & \xi_{d_2}^{\gamma_k} \\ \hline \xi_1^{t+1} & \cdots & \xi_{d_2}^{t+1} \\ \vdots & & \vdots \\ \xi_1^{t^*} & \cdots & \xi_{d_2}^{t^*} \\ \hline \xi_1^{0} f(\xi_1) & \cdots & \xi_{d_2}^{0} f(\xi_{d_2}) \\ \vdots & & \vdots \\ \xi_1^{t-d_1} f(\xi_1) & \cdots & \xi_{d_2}^{t-d_1} f(\xi_{d_2}) \end{array}\right] \in \overline{K}^{d_2 \times d_2}.$$

Proof. First, $\mathcal{O}_\mathcal{S}$ is a square matrix since by (5) we have

$$d_2 = k + (t^* - t) + \max\{0, t - d_1 + 1\}.$$

Let $I_\mathcal{S} \in K^{(k+t^*-t)\times(t^*+1)}$ be the transpose of the matrix of the immersion of the K-vector space generated by $\mathcal{S} \cup \{x^{t+1}, \dots, x^{t^*}\}$ into $K[x]_{t^*}$ ($I_\mathcal{S}$ is an identity $(k+t^*-t)$-square matrix plugged into (t^*+1) zero columns), and set

$$M_\mathcal{S} := \left[\begin{array}{c} I_\mathcal{S} \\ \hline M_f \\ \hline M_g \end{array}\right]. \tag{6}$$

Since it is straightforward to check by (5) that we have

$$k + t^* - t + \max\{0, t - d_1 + 1\} + \max\{0, t - d_2 + 1\} = t^* + 1,$$

therefore $M_\mathcal{S}$ is a (t^*+1)-square matrix.

Furthermore, it is immediate to verify that $|M_\mathcal{S}| = \mathrm{sg}(\mathcal{S})\Delta_\mathcal{S}$, and we are left to prove that $|M_\mathcal{S}| = b_{d_2}^{t^*-d_2+1}\,|\mathcal{O}_\mathcal{S}|/\mathcal{V}_{d_2}$.

We set

$$V_{t^*} := \begin{bmatrix} \xi_1^0 & \cdots & \xi_{d_2}^0 \\ \vdots & & \vdots \\ \xi_1^{t^*} & \cdots & \xi_{d_2}^{t^*} \end{bmatrix} \in \overline{K}^{(t^*+1)\times d_2}, \; V_{d_2} := \left[\begin{array}{c|c} & \mathbf{0} \\ V_{t^*} & \\ & Id \end{array}\right] \in \overline{K}^{(t^*+1)\times(t^*+1)}$$

and we observe that $\mathcal{V}_{d_2} = |V_{d_2}|$. Now, we perform the product $M_\mathcal{S} V_{d_2}$:

$$M_\mathcal{S} V_{d_2} = \begin{array}{|c|}\hline I_\mathcal{S} \\ \hline M_f \\ \hline M_g \\ \hline \end{array} \cdot \begin{array}{|c|c|}\hline & \mathbf{0} \\ \xi_j^{i-1} & \\ & Id \\ \hline \end{array} = \begin{array}{|c|c|}\hline \xi_j^{\gamma_i} & * \\ \hline \xi_j^{t+i} & * \\ \hline \xi_j^{i-1} f(\xi_j) & * \\ \hline \mathbf{0} & \begin{matrix} b_{d_2} & & \mathbf{0} \\ & \ddots & \\ * & & b_{d_2} \end{matrix} \\ \hline \end{array}.$$

Therefore $|M_\mathcal{S}|\,\mathcal{V}_{d_2} = b_{d_2}^{t^*-d_2+1}|\mathcal{O}_\mathcal{S}|$, which proves the Theorem. $\square$

The following examples illustrate how the formula works in a couple of cases.

Example 2.3 $d_1 = 5$, $d_2 = 2$, $t = 4$. Now we have $t = t^*$, $k = 2$, and

$$M_f = \emptyset, \ \ M_g = \begin{bmatrix} b_0 & b_1 & b_2 & 0 & 0 \\ 0 & b_0 & b_1 & b_2 & 0 \\ 0 & 0 & b_0 & b_1 & b_2 \end{bmatrix}.$$

Set $\mathcal{S} := \{x, x^4\}$. Here $\Delta_{\mathcal{S}}$ does not coincide with any of the scalar subresultants $S_2^{(j)}$, $0 \leq j \leq 2$. However, it is straightforward to check that $\Delta_{\mathcal{S}} = b_0 b_1^2 - b_0^2 b_2$. On the other hand, since $\mathrm{sg}(\mathcal{S}) = 1$, by Theorem 2.2 we have that

$$\begin{aligned} \mathrm{sg}(\mathcal{S})\, b_2^{4-2+1} \frac{\begin{vmatrix} \xi_1 & \xi_2 \\ \xi_1^4 & \xi_2^4 \end{vmatrix}}{\begin{vmatrix} 1 & 1 \\ \xi_1 & \xi_2 \end{vmatrix}} &= b_2^3\, \xi_1 \xi_2 \frac{\xi_2^3 - \xi_1^3}{\xi_2 - \xi_1} \\ &= b_2^3\, \xi_1 \xi_2 [(\xi_1 + \xi_2)^2 - \xi_1 \xi_2] \\ &= b_2^3\, (b_0/b_2)\, [(b_1/b_2)^2 - (b_0/b_2)]. \end{aligned}$$

□

Next example deals with a case when $t < d_2$ in which case we need to use $t^* = d_2 - 1$ instead of t.

Example 2.4 $d_1 = 2$, $d_2 = 5$, $t = 3$. Here $k = 2$. The scalar subresultants associated to this value of k are $S_2^{(2)} = a_2^3$, $S_2^{(1)} = a_2^2 a_1$ and $S_2^{(0)} = a_2^2 a_0$, while for $t = 3 < d_2$ we have $t^* = d_2 - 1 = 4$. Thus we have

$$M_f = \begin{bmatrix} a_0 & a_1 & a_2 & 0 & 0 \\ 0 & a_0 & a_1 & a_2 & 0 \end{bmatrix}, \quad M_g = \emptyset.$$

For $\mathcal{S} := \{1, x\}$, $\Delta_{\mathcal{S}} = a_2^2$, and Theorem 2.2 still works in this case: since $\mathrm{sg}(\mathcal{S}) = 1$ and $b_5^{4-5+1} = 1$, one has

$$\frac{\begin{vmatrix} 1 & 1 & 1 & 1 & 1 \\ \xi_1 & \xi_2 & \xi_3 & \xi_4 & \xi_5 \\ \xi_1^4 & \xi_2^4 & \xi_3^4 & \xi_4^4 & \xi_5^4 \\ f(\xi_1) & f(\xi_2) & f(\xi_3) & f(\xi_4) & f(\xi_5) \\ \xi_1 f(\xi_1) & \xi_2 f(\xi_2) & \xi_3 f(\xi_3) & \xi_4 f(\xi_4) & \xi_5 f(\xi_5) \end{vmatrix}}{\begin{vmatrix} 1 & 1 & 1 & 1 & 1 \\ \xi_1 & \xi_2 & \xi_3 & \xi_4 & \xi_5 \\ \xi_1^2 & \xi_2^2 & \xi_3^2 & \xi_4^2 & \xi_5^2 \\ \xi_1^3 & \xi_2^3 & \xi_3^3 & \xi_4^3 & \xi_5^3 \\ \xi_1^4 & \xi_2^4 & \xi_3^4 & \xi_4^4 & \xi_5^4 \end{vmatrix}} = a_2^2 \frac{\begin{vmatrix} 1 & 1 & 1 & 1 & 1 \\ \xi_1 & \xi_2 & \xi_3 & \xi_4 & \xi_5 \\ \xi_1^4 & \xi_2^4 & \xi_3^4 & \xi_4^4 & \xi_5^4 \\ \xi_1^2 & \xi_2^2 & \xi_3^2 & \xi_4^2 & \xi_5^2 \\ \xi_1^3 & \xi_2^3 & \xi_3^3 & \xi_4^3 & \xi_5^3 \end{vmatrix}}{\begin{vmatrix} 1 & 1 & 1 & 1 & 1 \\ \xi_1 & \xi_2 & \xi_3 & \xi_4 & \xi_5 \\ \xi_1^2 & \xi_2^2 & \xi_3^2 & \xi_4^2 & \xi_5^2 \\ \xi_1^3 & \xi_2^3 & \xi_3^3 & \xi_4^3 & \xi_5^3 \\ \xi_1^4 & \xi_2^4 & \xi_3^4 & \xi_4^4 & \xi_5^4 \end{vmatrix}}.$$

□

We end this section by showing how simple it is to derive from Theorem 2.2 both the Poisson product formula (1) and Hong's formula (4) for subresultant polynomials in roots, together with its generalization to a larger class of determinant polynomials that we call here generalized subresultant polynomials.

Observation 2.5 *(Poisson product formula)* Applying the previous theorem to Remark 2.1(1), one obtains

$$\begin{aligned}
\operatorname{Res}(f,g) &= (-1)^{d_1 d_2}\Delta_\emptyset \\
&= (-1)^{d_1 d_2} b_{d_2}^{d_1} \frac{\begin{vmatrix} \xi_1^0 f(\xi_1) & \cdots & \xi_{d_2}^0 f(\xi_{d_2}) \\ \vdots & & \vdots \\ \xi_1^{d_2-1} f(\xi_1) & \cdots & \xi_{d_2}^{d_2-1} f(\xi_{d_2}) \end{vmatrix}}{\begin{vmatrix} \xi_1^0 & \cdots & \xi_{d_2}^0 \\ \vdots & & \vdots \\ \xi_1^{d_2-1} & \cdots & \xi_{d_2}^{d_2-1} \end{vmatrix}} \\
&= (-1)^{d_1 d_2} b_{d_2}^{d_1} \prod_{j=1}^{d_2} f(\xi_j).
\end{aligned}$$

□

Observation 2.6 *([17, Th. 3.1], [23, Id. 9.3.2])* We derive Hong's Formula (4) applying Theorem 2.2 to Remark 2.1(2):

$$\begin{aligned}
\operatorname{sres}_k(f,g) &= \sum_{j=0}^{k} S_k^{(j)} x^j = (-1)^{(d_1-k)(d_2-k)} \sum_{j=0}^{k} \Delta_{\mathcal{S}_j} x^j \\
&= (-1)^{(d_1-k)(d_2-k)} b_{d_2}^{d_1-k} \mathcal{V}_{d_2}^{-1} \sum_{j=0}^{k} \operatorname{sg}(\mathcal{S}_j) |\mathcal{O}_{\mathcal{S}_j}|\, x^j.
\end{aligned}$$

We observe that in this case $t^* = t$, $\operatorname{sg}(\mathcal{S}_k) = \operatorname{sg}\{1, \ldots, x^{k-1}\} = 1$ and $\operatorname{sg}(\mathcal{S}_j) = (-1)^{k-j}$, and thus, by column expansion of the determinant we get:

$$\sum_{j=0}^{k} \operatorname{sg}(\mathcal{S}_j) |\mathcal{O}_{\mathcal{S}_j}|\, x^j = \begin{vmatrix} (-1)^k & \xi_1^0 & \cdots & \xi_{d_2}^0 \\ (-1)^k x & \xi_1^1 & \cdots & \xi_{d_2}^1 \\ \vdots & \vdots & & \vdots \\ (-1)^k x^k & \xi_1^k & \cdots & \xi_{d_2}^k \\ 0 & \xi_1^0 f(\xi_1) & \cdots & \xi_{d_2}^0 f(\xi_{d_2}) \\ \vdots & \vdots & & \vdots \\ 0 & \xi_1^{d_2-k-1} f(\xi_1) & \cdots & \xi_{d_2}^{d_2-k-1} f(\xi_{d_2}) \end{vmatrix}$$

$$= (-1)^k \begin{vmatrix} 1 & \xi_1^0 & \dots & \xi_{d_2}^0 \\ 0 & \xi_1^1 - x\xi_1^0 & \dots & \xi_{d_2}^1 - x\xi_{d_2}^0 \\ \vdots & \vdots & & \vdots \\ 0 & \xi_1^k - x\xi_1^{k-1} & \dots & \xi_{d_2}^k - x\xi_{d_2}^{k-1} \\ 0 & \xi_1^0 f(\xi_1) & \cdots & \xi_{d_2}^0 f(\xi_{d_2}) \\ \vdots & \vdots & & \vdots \\ 0 & \xi_1^{d_2-k-1} f(\xi_1) & \cdots & \xi_{d_2}^{d_2-k-1} f(\xi_{d_2}) \end{vmatrix}$$

$$= \begin{vmatrix} (x-\xi_1)\xi_1^0 & \dots & (x-\xi_{d_2})\xi_{d_2}^0 \\ \vdots & & \vdots \\ (x-\xi_1)\xi_1^{k-1} & \dots & (x-\xi_{d_2})\xi_{d_2}^{k-1} \\ \xi_1^0 f(\xi_1) & \cdots & \xi_{d_2}^0 f(\xi_{d_2}) \\ \vdots & & \vdots \\ \xi_1^{d_2-k-1} f(\xi_1) & \cdots & \xi_{d_2}^{d_2-k-1} f(\xi_{d_2}) \end{vmatrix}.$$

□

One can straightforwardly generalize Hong's result to a larger class of determinant polynomials

$$s(x) := \sum_{j=0}^{k} \Delta_{\mathcal{S}_j} x^{\gamma_j}, \tag{7}$$

corresponding to an arbitrary set of monomials $\mathcal{S} := \{x^{\gamma_j}, 0 \leq j \leq k\} \subset K[x]_t$ and $\mathcal{S}_j := S \setminus \{x^{\gamma_j}\}$, where $d_2 \leq t \leq d_1 + d_2 - 1$ and $k := d_2 - \max\{0, t - d_1 + 1\}$. We call such a polynomial a *generalized subresultant polynomial.*

The usual proof that shows that $\mathrm{sres}_k(f, g)$ belongs to the ideal (f, g) generated by f and g extends to showing that $s \in (f, g)$ and the following expression in terms of roots holds (we omit the proof which is essentially the same than the proof of Observation 2.6).

Corollary 2.7 *Let $f, g \in K[x]$ and $s(x)$ be the generalized subresultant polynomial defined in (7). Then, we have*

$$s(x) = b_{d_2}^{t-d_2+1} \mathcal{V}_{d_2}^{-1} x^{\gamma_0} \begin{vmatrix} (x^{\gamma_1-\gamma_0} - \xi_1^{\gamma_1-\gamma_0})\xi_1^{\gamma_0} & \cdots & (x^{\gamma_1-\gamma_0} - \xi_{d_2}^{\gamma_1-\gamma_0})\xi_{d_2}^{\gamma_0} \\ \vdots & & \vdots \\ (x^{\gamma_k-\gamma_{k-1}} - \xi_1^{\gamma_k-\gamma_{k-1}})\xi_1^{\gamma_{k-1}} & \cdots & (x^{\gamma_k-\gamma_{k-1}} - \xi_{d_2}^{\gamma_k-\gamma_{k-1}})\xi_{d_2}^{\gamma_{k-1}} \\ \xi_1^0 f(\xi_1) & \cdots & \xi_{d_2}^0 f(\xi_{d_2}) \\ \vdots & & \vdots \\ \xi_1^{d_2-k-1} f(\xi_1) & \cdots & \xi_{d_2}^{d_2-k-1} f(\xi_{d_2}) \end{vmatrix}.$$

□

3 The multivariate case

In this section we generalize Theorem 2.2 to Chardin's multivariate subresultants [5], after introducing the notations we need.

Notations:

- For $n \in \mathbb{N}$ and $1 \leq i \leq n+1$,

$$f_i := \sum_{|\alpha| \leq d_i} a_{i\alpha} \mathbf{x}^\alpha \ \in \ K[\mathbf{x}],$$

  where $\alpha = (\alpha_1, \ldots, \alpha_n) \in (\mathbb{Z}_{\geq 0})^n$, $\mathbf{x}^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, $|\alpha| = \alpha_1 + \cdots + \alpha_n$, and $K := \mathbb{Q}(a_{i\alpha}, 1 \leq i \leq n+1, |\alpha| \leq d_i)$, with $a_{i\alpha}$ algebraically independent variables over $\mathbb{Q}$ (representing the indeterminate coefficients of $n+1$ generic polynomials in n variables f_i of degrees d_i respectively).
- For any $j \in \mathbb{Z}$, $K[\mathbf{x}]_j := K[x_1, \ldots, x_n]_j = \{0\} \cup \{f \in K[\mathbf{x}] : \deg f \leq j\}$.
- We set $t \in \mathbb{N}$, $\rho := (d_1 - 1) + \cdots + (d_n - 1)$ and $t^* := \max\{\rho, t\}$.
- $k := \mathcal{H}_{d_1 \ldots d_{n+1}}(t)$, 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.

$$k := \#\{\mathbf{x}^\alpha : |\alpha| \leq t, \alpha_i < d_i, 1 \leq i \leq n, \text{ and } t - |\alpha| < d_{n+1}\}.$$

- $\mathcal{S} := \{\mathbf{x}^{\gamma_1}, \ldots, \mathbf{x}^{\gamma_k}\} \subset K[\mathbf{x}]_t$ a set of k monomials of degree bounded by t.
- For $1 \leq i \leq n+1$,

$$\mathcal{R}_i := \{\mathbf{x}^\alpha, |\alpha| \leq t - d_i, \alpha_j < d_j \text{ for } j < i\}.$$

  We observe that for $1 \leq i \leq n$,

$$\#(\mathcal{R}_i) = \#\{\mathbf{x}^\alpha, |\alpha| \leq t, \alpha_j < d_j \text{ for } j < i \text{ and } \alpha_i \geq d_i\},$$

  and

$$\#(\mathcal{R}_{n+1}) = \#\{\mathbf{x}^\alpha, |\alpha| \leq t, \alpha_j < d_j \ \forall j \text{ and } t - |\alpha| \geq d_{n+1}\}.$$

  Therefore

$$N := \binom{t+n}{n} = \dim_K K[\mathbf{x}]_t = k + \#(\mathcal{R}_1) + \cdots + \#(\mathcal{R}_{n+1}). \qquad (8)$$

- In particular, we denote $\mathcal{R}_{n+1} =: \{\mathbf{x}^{\beta_1}, \ldots, \mathbf{x}^{\beta_r}\}$, where $r := \#(\mathcal{R}_{n+1})$ and we observe that

$$k + r = \#\{\mathbf{x}^\alpha, |\alpha| \leq t, \alpha_j < d_j \ \forall j\} = \dim K[\mathbf{x}]_t/(f_1, \ldots, f_n) \cap K[\mathbf{x}]_t. \quad (9)$$

- For $j \geq 0$, $\tau_j := \mathcal{H}_{d_1 \ldots d_n}(j)$, the Hilbert function at j of a regular sequence of n homogeneous polynomials in n variables of degrees $d_1, \ldots, d_n$, i.e.

$$\tau_j := \#\{\mathbf{x}^\alpha : \ |\alpha| = j, \alpha_i < d_i \text{ for } 1 \leq i \leq n\}.$$

We note that $\tau_j = 0$ if $j > \rho$.

- For $j \geq 0$,

$$\mathcal{T}_j := \begin{cases} \textit{any} \text{ set of } \tau_j \text{ monomials of degree } j & \text{for } j \geq \max\{0, t - d_{n+1} + 1\}, \\ \{\mathbf{x}^\alpha : |\alpha| = j, \alpha_i < d_i \text{ for } 1 \leq i \leq n\} & \text{for } 0 \leq j < t - d_{n+1} + 1. \end{cases} \tag{10}$$

See Remark 3.3 for a discussion on the definition of $\mathcal{T}_j$.

- $\mathcal{T} := \cup_{j \geq 0} \mathcal{T}_j$ and $\mathcal{T}^* := \cup_{j=t+1}^{t^*} \mathcal{T}_j$. We note that $\#\mathcal{T} = \mathbf{d}$, where $\mathbf{d} := d_1 \cdots d_n$ is the *Bézout number*, the number of common solutions of $f_1, \ldots, f_n$ in $\overline{K}^n$, and that $\mathcal{T}^* = \emptyset$ if $t^* = t$, i.e. if $t \geq \rho$.

  In particular, we denote $\mathcal{T} = \{\mathbf{x}^{\alpha_1}, \ldots, \mathbf{x}^{\alpha_\mathbf{d}}\}$, and we assume that $\mathcal{T}^* = \{\mathbf{x}^{\alpha_1}, \ldots, \mathbf{x}^{\alpha_s}\}$, the first $s := \#(\mathcal{T}^*)$ elements of $\mathcal{T}$.
- $K[\mathbf{x}]_{t,*}$ denotes the K-vector space generated by $K[\mathbf{x}]_t \cup \mathcal{T}^*$ and $N^* := \dim(K[\mathbf{x}]_{t,*})$.
- For $1 \leq i \leq n+1$, $M_{f_i} \in K^{\dim(\mathcal{R}_i) \times N^*}$ denotes the transpose of the matrix in the monomial bases of the composition between the Sylvester multiplication map and the inclusion $K[\mathbf{x}]_t \to K[\mathbf{x}]_{t,*}$:

$$\begin{array}{rcl} \mu_{f_i} : \langle \mathcal{R}_i \rangle & \to & K[\mathbf{x}]_{t,*} \\ \mathbf{x}^\alpha & \mapsto & \mathbf{x}^\alpha f_i \end{array}.$$

  For later convenience we order the monomial basis of $K[\mathbf{x}]_{t,*}$ in such a way that all monomials in $\mathcal{T}$ precede the monomials in $K[\mathbf{x}]_{t,*} \setminus \mathcal{T}$.
- $\widetilde{M}_\mathcal{S} \in K^{(N-k)\times(N-k)}$ denotes the Macaulay-Chardin matrix obtained from

$$\begin{bmatrix} M_{f_1} \\ \vdots \\ M_{f_{n+1}} \end{bmatrix} \tag{11}$$

  by deleting the columns indexed by the monomials in $\mathcal{S} \cup \mathcal{T}^*$.
- Following [24,5], we define *the extraneous factor* $\mathcal{E}(t)$ as the determinant of the square submatrix of (11) whose rows are indexed by all those monomials $\mathbf{x}^\alpha \in \mathcal{R}_i$, $1 \leq i \leq n$, such that $t - d_i - |\alpha| \geq d_{n+1}$ or there exists $j > i$ with $\alpha_j \geq d_j$, and whose columns are indexed by those $\mathbf{x}^\alpha$ such that $t - |\alpha| \geq d_{n+1}$ and for some index i, $\alpha_i \geq d_i$, or such that there exist at least two different indexes $1 \leq i, j \leq n$ with $\alpha_i \geq d_i, \ \alpha_j \geq d_j$. It is straightforward to verify that this is really a square matrix. An important property of $\mathcal{E}(t)$ is that it neither depends on the coefficients of f_{n+1} nor on $\mathcal{S}$.
- $\Delta_\mathcal{S} := \Delta_{\mathcal{S}^h}^{(t)}(f_1^h, \ldots, f_{n+1}^h)$ denotes the *order t subresultant of* $f_1^h, \ldots, f_{n+1}^h$ *with respect to* $\mathcal{S}^h := \{\mathbf{x}^{\gamma_1} x_{n+1}^{t-|\gamma_1|}, \ldots, \mathbf{x}^{\gamma_k} x_{n+1}^{t-|\gamma_k|}\}$. Here, f_i^h denotes the homogenization of f_i by the variable x_{n+1}. It turns out that by [4] we have

$$\Delta_{\mathcal{S}} = \pm \frac{|\widetilde{M}_{\mathcal{S}}|}{\mathcal{E}(t)}. \tag{12}$$

- For $1 \leq i \leq n$, $\overline{f}_i$ is the homogeneous component of degree d_i of f_i, and $\overline{\Delta}_{\mathcal{T}_j} := \Delta^{(j)}_{\mathcal{T}_j}(\overline{f}_1, \ldots, \overline{f}_n)$ is the order j subresultant of $\overline{f}_1, \ldots, \overline{f}_n$ with respect to $\mathcal{T}_j$.
- $\{\xi_1, \ldots, \xi_{\mathbf{d}}\}$ denotes the set of all common roots of $f_1, \ldots, f_n$ in $\overline{K}^n$, and $\mathcal{V}_{\mathcal{T}} := \det(\xi_j^{\alpha_i})_{1 \leq i,j \leq \mathbf{d}}$, the generalized Vandermonde determinant associated to $\mathcal{T}$.

Remark 3.1 The order t subresultant given in (12) generalizes both the univariate case and the usual multivariate projective resultant as defined for instance in [6, Th. 2.3].

(1) When $n = 1$ and $t \leq d_1 + d_2 - 1$, there are no rows and columns of (11) satisfying the condition that contributes to the extraneous factor $\mathcal{E}_t$, and thus $\mathcal{E}(t) = 1$. Therefore $\Delta_{\mathcal{S}}$ of (12) coincides with the univariate order t subresultant of f and g with respect to $\mathcal{S}$ defined in Section 2.

(2) When $t \geq \rho + d_{n+1}$, then $k = 0$ since $\alpha_1 < d_1, \ldots, \alpha_n < d_n$ imply $|\alpha| \leq \rho$, thus $t - |\alpha| \geq d_{n+1}$. Therefore $\mathcal{S} := \emptyset$. In that case we recover Macaulay's construction [24, Th. p.9 and Th. 4] and $\Delta_{\mathcal{S}} = \pm \mathrm{Res}(f_1^h, \ldots, f_{n+1}^h)$.

We are ready now to state the main result of the paper, the multivariate generalization of Theorem 2.2.

Theorem 3.2 *Let $f_1, \ldots, f_{n+1} \in K[\mathbf{x}]$ and $\{\xi_1, \ldots, \xi_{\mathbf{d}}\}$ be the set of common roots of $f_1, \ldots, f_n$ in $\overline{K}^n$. Then, under the previous notations, for any $t \in \mathbb{Z}_{\geq 0}$ and for any $\mathcal{S} = \{\mathbf{x}^{\gamma_1}, \ldots, \mathbf{x}^{\gamma_k}\} \subset K[\mathbf{x}]_t$ of cardinality $k = \mathcal{H}_{d_1 \ldots d_{n+1}}(t)$, the order t subresultant $\Delta_{\mathcal{S}}$ satisfies:*

$$\Delta_{\mathcal{S}} = \pm \left(\prod_{j=t-d_{n+1}+1}^{t} \overline{\Delta}_{\mathcal{T}_j} \right) \frac{|\mathcal{O}_{\mathcal{S}}|}{\mathcal{V}_{\mathcal{T}}}, \tag{13}$$

where

$$\mathcal{O}_{\mathcal{S}} = \left[\begin{array}{ccc} \xi_1^{\gamma_1} & \cdots & \xi_{\mathbf{d}}^{\gamma_1} \\ \vdots & & \vdots \\ \xi_1^{\gamma_k} & \cdots & \xi_{\mathbf{d}}^{\gamma_k} \\ \hline \xi_1^{\alpha_1} & \cdots & \xi_{\mathbf{d}}^{\alpha_1} \\ \vdots & & \vdots \\ \xi_1^{\alpha_s} & \cdots & \xi_{\mathbf{d}}^{\alpha_s} \\ \hline \xi_1^{\beta_1} f_{n+1}(\xi_1) & \cdots & \xi_{\mathbf{d}}^{\beta_1} f_{n+1}(\xi_{\mathbf{d}}) \\ \vdots & & \vdots \\ \xi_1^{\beta_r} f_{n+1}(\xi_1) & \cdots & \xi_{\mathbf{d}}^{\beta_r} f_{n+1}(\xi_{\mathbf{d}}) \end{array} \right] \in \overline{K}^{\mathbf{d} \times \mathbf{d}}.$$

Proof. First we check that $\mathcal{O}_{\mathcal{S}}$ is a square matrix, i.e. that $\mathbf{d} = k+s+r$. This is clear by Formula (9) since
$\mathbf{d} - s = \#(\mathcal{T}) - \#(\mathcal{T}^*) = \#(\mathcal{T} \setminus \mathcal{T}^*) = \#\{\mathbf{x}^\alpha, |\alpha| \le t, \alpha_j < d_j \ \forall j\} = k + r.$
In this proof the monomial basis $\{\mathbf{x}^{\delta_1}, \ldots, \mathbf{x}^{\delta_{N^*}}\}$ of $K[\mathbf{x}]_{t,*}$ is ordered such as was specified in the notations (monomials in $\mathcal{T}$ precede the rest of the monomials in $K[\mathbf{x}]_{t,*}$).

Like in the univariate case, we define $I_{\mathcal{S}} \in K^{(k+s)\times N^*}$ as the transpose of the matrix of the immersion of the K-vector space generated by $\mathcal{S} \cup \mathcal{T}^*$ into $K[\mathbf{x}]_{t,*}$ in the monomial bases. We set

$$M_{\mathcal{S}} := \left[\begin{array}{c} I_{\mathcal{S}} \\ \hline M_{f_1} \\ \vdots \\ M_{f_n} \\ \hline M_{f_{n+1}} \end{array}\right] \in K^{N^*\times N^*}.$$

($M_{\mathcal{S}}$ is a square matrix by (8) and since $N^* = N + \dim(\mathcal{T}^*)$.)

Furthermore, it is immediate to verify that $|M_{\mathcal{S}}| = \pm\,|\widetilde{M}_{\mathcal{S}}| = \pm\,\mathcal{E}(t)\,\Delta_{\mathcal{S}}$, where $\mathcal{E}(t)$ denotes the extraneous factor that has been introduced in (12).

We set

$$V_{N^*} = \begin{bmatrix} \xi_1^{\delta_1} & \ldots & \xi_{\mathbf{d}}^{\delta_1} \\ \vdots & & \vdots \\ \xi_1^{\delta_{N^*}} & \ldots & \xi_{\mathbf{d}}^{\delta_{N^*}} \end{bmatrix} \in \overline{K}^{N^*\times \mathbf{d}}, \text{ and } V_{\mathbf{d}} := \left[\begin{array}{c|c} & \mathbf{0} \\ V_{N^*} & \\ & Id \end{array}\right] \in \overline{K}^{N^*\times N^*}$$

and we observe that $\mathcal{V}_{\mathcal{T}} = |V_{\mathbf{d}}|$. We perform the product $M_{\mathcal{S}}\,V_{\mathbf{d}}$:

$$M_{\mathcal{S}}\,V_{\mathbf{d}} = \left[\begin{array}{c} I_{\mathcal{S}} \\ \hline M_{f_1} \\ \vdots \\ M_{f_n} \\ \hline M_{f_{n+1}} \end{array}\right] \cdot \left[\begin{array}{c|c} \xi_j^{\delta_i} & \begin{array}{c} \mathbf{0} \\ \\ Id \end{array} \end{array}\right] = \left[\begin{array}{c|c} \xi_j^{\gamma_i} & * \\ \hline \xi_j^{\alpha_i} & * \\ \hline \mathbf{0} & \begin{array}{c} M'_{f_1} \\ \vdots \\ M'_{f_n} \end{array} \\ \hline \xi_j^{\beta_i} f_{n+1}(\xi_j) & * \end{array}\right],$$

where $M' := \begin{bmatrix} M'_{f_1} \\ \vdots \\ M'_{f_n} \end{bmatrix}$ is the submatrix of $\begin{bmatrix} M_{f_1} \\ \vdots \\ M_{f_n} \end{bmatrix}$ with the same number of rows and whose columns are indexed by all monomials in $\mathbf{x}^\alpha \in K[\mathbf{x}]_{t,*} \smallsetminus \mathcal{T} = K[\mathbf{x}]_t \smallsetminus (\mathcal{T} \smallsetminus \mathcal{T}^*) = K[\mathbf{x}]_t \smallsetminus \mathcal{T}$. It is immediate to verify that M' is a square matrix since, again by (9), $\#(\mathcal{R}_1)+\cdots+\#(\mathcal{R}_n) = N-k-r = N-\#(\mathcal{T}\smallsetminus\mathcal{T}^*) = N^* - \mathbf{d}$.

We recall that $\#(\mathcal{T}\smallsetminus\mathcal{T}^*) = \#\{\mathbf{x}^\alpha, |\alpha| \le t, \alpha_i < d_i \ \forall i\}$, and therefore M' is the Macaulay-Chardin matrix associated to the computation of $\Delta^{(t)}_{\mathcal{T}\smallsetminus\mathcal{T}^*}(f_1, \dots, f_n)$, the order t subresultant of $f_1, \dots, f_n$ with respect to $\mathcal{T} \smallsetminus \mathcal{T}^*$.

To conclude the proof we are left to prove that

$$|M'| = \pm\mathcal{E}(t) \left(\prod_{j=t-d_{n+1}+1}^{t} \overline{\Delta}_{\mathcal{T}_j} \right).$$

This was proven in [24, p.14] (see also the proof of [4, Lem. 1] and [8, Thm. 5.2]). For the reader's convenience, we rewrite the proof here.

We reorganize the matrix M' as follows: we recall that the columns correspond to monomials $\mathbf{x}^\alpha \in K[\mathbf{x}]_t \smallsetminus \mathcal{T}$ and we index the columns by graded descending order, first all monomials of degree t in $K[\mathbf{x}]_t \smallsetminus \mathcal{T}$, then all monomials of degree $t-1$ in $K[\mathbf{x}]_t \smallsetminus \mathcal{T}$, and so on, up to all monomials of degree $t - d_{n+1} + 1$. Finally, we put in the last block all monomials of degree bounded by $t - d_{n+1}$. The rows correspond to $\mathcal{R}_i$ for $1 \le i \le n$. We also index them by graded descending order: first all monomials of degree $t - d_i$ in $\mathcal{R}_i$ for $1 \le i \le n$, then all monomials of degree $t - d_i - 1$ in $\mathcal{R}_i$, $1 \le i \le n$, and so on up to all monomials of degree $t - d_i - d_{n+1} + 1$ in $\mathcal{R}_i$, $1 \le i \le n$. In the last block we put all monomials of degree bounded by $t - d_i - d_{n+1}$ in $\mathcal{R}_i$, $1 \le i \le n$.

With this ordering M' has a block structure:

$$M' = \begin{bmatrix} M_t & * & * & * \\ & \ddots & * & * \\ & & M_{t-d_{n+1}+1} & * \\ \mathbf{0} & & & E \end{bmatrix}, \tag{14}$$

where the square matrix M_j corresponds to the coefficients of the terms of degree j of $\mathbf{x}^\alpha f_i$, where $|\alpha| = j - d_i$, that is, the coefficients of $\mathbf{x}^\alpha \overline{f}_i$ except those corresponding to terms in $\mathcal{T}_j$.

Hence M_j is the Macaulay-Chardin matrix associated to the j-subresultant $\overline{\Delta}_{\mathcal{T}_j}$ of $\overline{f}_1, \ldots, \overline{f}_n$ with respect to $\mathcal{T}_j$ ([5]) and it turns out that

$$|M_j| = \mathcal{E}_j \, \overline{\Delta}_{\mathcal{T}_j},$$

where $\mathcal{E}_j$ is the extraneous factor associated to this construction, that we recall only depends on j and not on the set $\mathcal{T}_j$.

But it turns out that the extraneous factor $\mathcal{E}(t)$ has a block structure similar to (14) (see [24,4,8]). We have, with our notation:

$$\mathcal{E}(t) = |E| \prod_{j=t-d_{n+1}+1}^{t} \mathcal{E}_j, \tag{15}$$

(see [24, Th. 6]). This concludes the proof of the Theorem. □

Remark 3.3 The reason why we cannot allow $\mathcal{T}_j$ to be *any* subset of monomials of degree j for $j \leq t - d_{n+1} + 1$ is the factorization formula on the right hand side of (15), where the $\mathcal{E}_j$'s involved in the product are only those corresponding to j satisfying $t - d_{n+1} + 1 \leq j \leq t$. This is not just a technical obstruction. If we could pick any $\mathcal{T}_j$ for every j, then setting $t := \rho + d_{n+1}$, the Poisson formula for the resultant $\operatorname{Res}(f_1^h, \ldots, f_{n+1}^h)$ would read as follows

$$\frac{\begin{vmatrix} \xi_1^{\beta_1} & \cdots & \xi_{\mathbf{d}}^{\beta_1} \\ \vdots & & \vdots \\ \xi_1^{\beta_r} & \cdots & \xi_{\mathbf{d}}^{\beta_r} \end{vmatrix}}{V_{\mathcal{T}}} \operatorname{Res}(\overline{f}_1, \ldots, \overline{f}_n)^{d_{n+1}} \prod_{\xi \in V_{\overline{K}^n}(f_1,\ldots,f_n)} f_{n+1}(\xi),$$

which is obviously false in general since the fraction does not cancel unless $\mathcal{T} = \mathcal{R}_{n+1}$, i.e. $\mathcal{T}_j$ is defined as in (10).

Like in the univariate case, we illustrate Theorem 3.2 with a specific example.

Example 3.4 Let $n = 2$, $d_1 = d_2 = d_3 = 2$ and $t = t^* = 2$.

Here $k = \#\{x_1, x_2, x_1x_2\} = 3$, $\mathcal{R}_1 = \mathcal{R}_2 = \mathcal{R}_3 = \{1\}$ and $\mathcal{T} = \{1, x_1, x_2, x_1x_2\}$.

We fix the ordered monomial basis $(1, x_1, x_2, x_1x_2, x_1^2, x_2^2)$ of $K[\mathbf{x}]_2$ and

$$\begin{aligned} f_1 &= a_0 + a_1x_1 + a_2\,x_2 + a_3x_1x_2 + a_4x_1^2 + a_5x_2^2 \\ f_2 &= b_0 + b_1x_1 + b_2\,x_2 + b_3x_1x_2 + b_4x_1^2 + b_5x_2^2 \\ f_3 &= c_0 + c_1x_1 + c_2\,x_2 + c_3x_1x_2 + c_4x_1^2 + c_5x_2^2. \end{aligned}$$

Then

$$\begin{bmatrix} M_{f_1} \\ M_{f_2} \\ M_{f_3} \end{bmatrix} = \begin{bmatrix} a_0 & a_1 & a_2 & a_3 & a_4 & a_5 \\ b_0 & b_1 & b_2 & b_3 & b_4 & b_5 \\ c_0 & c_1 & c_2 & c_3 & c_4 & c_5 \end{bmatrix}.$$

We choose $\mathcal{S} := \{x_1, x_1x_2, x_1^2\}$. Then

$$\Delta_{\mathcal{S}} = c_0(a_2b_5 - a_5b_2) - c_2(a_0b_5 - a_5b_0) + c_5(a_0b_2 - a_2b_0).$$

On the other hand, if $V_{\overline{K}}(f_1, f_2) = \{\xi_1, \xi_2, \xi_3, \xi_4\}$ with $\xi_j = (\xi_{j1}, \xi_{j2})$ for $1 \leq j \leq 4$, then

$$\mathcal{O}_{\mathcal{S}} = \begin{bmatrix} \xi_{11} & \xi_{21} & \xi_{31} & \xi_{41} \\ \xi_{11}\xi_{12} & \xi_{21}\xi_{22} & \xi_{31}\xi_{32} & \xi_{41}\xi_{42} \\ \xi_{11}^2 & \xi_{21}^2 & \xi_{31}^2 & \xi_{41}^2 \\ f_3(\xi_1) & f_3(\xi_2) & f_3(\xi_3) & f_3(\xi_4) \end{bmatrix}.$$

Therefore, if we set V for the generalized Vandermonde matrix on $\xi_1, \ldots, \xi_4$ corresponding to the sequence of monomials $1, x_1, x_2, x_1x_2, x_1^2, x_2^2$, i.e.

$$V := \begin{bmatrix} 1 & 1 & 1 & 1 \\ \xi_{11} & \xi_{21} & \xi_{31} & \xi_{41} \\ \xi_{12} & \xi_{22} & \xi_{32} & \xi_{42} \\ \xi_{11}\xi_{12} & \xi_{21}\xi_{22} & \xi_{31}\xi_{32} & \xi_{41}\xi_{42} \\ \xi_{11}^2 & \xi_{21}^2 & \xi_{31}^2 & \xi_{41}^2 \\ \xi_{12}^2 & \xi_{22}^2 & \xi_{321}^2 & \xi_{42}^2 \end{bmatrix} \in \overline{K}^{6\times 4},$$

and $V_{i,j}$, $0 \leq i < j \leq 5$, for the square submatrix obtained from V deleting the i-th and j-th rows (we adopt the convention of numbering the rows from 0 to 5 like the coefficients of the f_i's), we conclude that

$$|\mathcal{O}_{\mathcal{S}}| = -c_0\,|V_{2,5}| + c_2\,|V_{0,5}| + c_5\,|V_{0,2}|.$$

Also, with this notation $V_{4,5}$ is the Vandermonde matrix corresponding to $\mathcal{T}$.

Now, since the only non-trivial homogeneous subresultant $\overline{\Delta}_{\mathcal{T}_j}$ in (13) is for $\mathcal{T}_2 = \{x_1x_2\}$, and is equal to

$$\overline{\Delta}_{\mathcal{T}_2} = a_4b_5 - a_5b_4,$$

Theorem 3.2 states that

$$c_0(a_2b_5 - a_5b_2) - c_2(a_0b_5 - a_5b_0) + c_5(a_0b_2 - a_2b_0)$$
$$= \pm(a_4b_5 - a_5b_4)\left(-c_0\frac{|V_{2,5}|}{|V_{4,5}|} + c_2\frac{|V_{0,5}|}{|V_{4,5}|} + c_5\frac{|V_{0,2}|}{|V_{4,5}|}\right).$$

Indeed, we show below that this equality holds since for any $i < j$ and $k < l$:

$$(-1)^{i+j}\frac{|V_{i,j}|}{a_ib_j - a_jb_i} = (-1)^{k+l}\frac{|V_{k,l}|}{a_kb_l - a_lb_k}. \tag{16}$$

If for $0 \leq i, j \leq 5$, we set $I_{i,j} \in K^{4\times 6}$ a 4-identity matrix with added 0 columns for column i and column j, and $I^{i,j} \in K^{6\times 2}$ the matrix with 4 null rows and the identity matrix plugged in rows i and j, we observe that

$$\begin{array}{|c|}\hline I_{i,j} \\ \hline M_{f_1} \\ M_{f_2} \\ \hline \end{array} \cdot \begin{array}{|c|c|}\hline V & I^{k,l} \\ \hline \end{array} = \begin{array}{|c|cc|}\hline V_{i,j} & \multicolumn{2}{c|}{*} \\ \hline & a_k & a_l \\ \mathbf{0} & b_k & b_l \\ \hline \end{array}$$

since $f_1(\xi_j) = f_2(\xi_j) = 0$, $1 \leq j \leq 4$. Thus, taking determinants on both sides,

$$(-1)^{5-j+4-i}(a_ib_j - a_jb_i)\cdot(-1)^{k+l-1}|V_{k,l}| = |V_{i,j}|\cdot(a_kb_l - a_lb_k),$$

and we obtain (16).

Applying this to our case, we conclude that here

$$\Delta_{\mathcal{S}} = -\left(\prod_{j=t-d_{n+1}+1}^{t}\overline{\Delta}_{\mathcal{T}_j}\right)\frac{|\mathcal{O}_{\mathcal{S}}|}{\mathcal{V}_{\mathcal{T}}}.$$

□

Next, we recover Theorem 2.2 in the univariate case:

Observation 3.5 For $n = 1$, by setting $f_1 := g$ and $f_2 := f$, as $\overline{f_1} = b_{d_2}x^{d_2}$, it turns out that

$$\overline{\Delta}_{\mathcal{T}_j} = \begin{cases} b_{d_2} & \text{if } j \geq d_2 \\ 1 & \text{if } j < d_2. \end{cases}$$

So, if $t \geq d_2$, then $\prod_{j=t-d_1+1}^{t}\overline{\Delta}_{\mathcal{T}_j} = {b_{d_2}}^{t-d_2+1}$. If $t < d_2$, the product of subresultants equals 1. □

In the particular case $t = \rho + d_{n+1}$, Theorem 3.2 gives a new proof for the Poisson product formula for the multivariate resultant (see [6]):

Corollary 3.6 (Poisson product formula)

$$\mathrm{Res}(f_1^h, \ldots, f_{n+1}^h) = \pm \mathrm{Res}(\overline{f}_1, \ldots, \overline{f}_n)^{d_{n+1}} \prod_{\xi \in V_{\overline{K}^n}(f_1,\ldots,f_n)} f_{n+1}(\xi).$$

Proof. We apply Remark 3.1 (2) for $t := \rho + d_{n+1}$ to Theorem 3.2. We observe that by the same remark, for $j > \rho$, i.e. for $j \geq t - d_n + 1$, $\overline{\Delta}_{\mathcal{T}_j} = \mathrm{Res}(\overline{f}_1, \ldots, \overline{f}_n)$. We conclude that $\mathcal{O}_{\mathcal{S}}$ equals $\left(\prod_{\xi \in V_{\overline{K}^n}(f_1,\ldots,f_n)} f_{n+1}(\xi)\right)$ times the generalized Vandermonde matrix whose determinant equals $\mathcal{V}_{\mathcal{T}}$. □

We end this paper by giving the multivariate version of Corollary 2.7, i.e. a discrete Wrónskian type expression for the *generalized subresultant polynomial*:

$$s(\mathbf{x}) := \sum_{j=0}^{k} \Delta_{\mathcal{S}_j} \mathbf{x}^{\gamma_j}, \tag{17}$$

defined for a fixed $t \in \mathbb{N}$ and $k := \mathcal{H}_{d_1 \ldots d_{n+1}}(t)$, under the usual notations,

$\mathcal{S} := \{\mathbf{x}^{\gamma_j}, 0 \leq j \leq k\} \subset K[\mathbf{x}]_t$ and $\mathcal{S}_j := \mathcal{S} \setminus \{\mathbf{x}^{\gamma_j}\}$.

It turns out that $s(\mathbf{x})$ belongs to the ideal generated by the f_i's (see [5]), and the following result can be proved mutatis mutandis the proof of Corollary 2.6.

Corollary 3.7 *Let $f_1, \ldots, f_{n+1} \in K[\mathbf{x}]$ and $s(\mathbf{x})$ be the generalized subresultant polynomial defined in (17). Then, we have*

$$s(\mathbf{x}) = \pm {\mathcal{V}_{\mathcal{T}}}^{-1} \left(\prod_{j=t-d_{n+1}+1}^{t} \overline{\Delta}_{\mathcal{T}_j} \right) \begin{vmatrix} \mathbf{x}^{\gamma_0} & \xi_1^{\gamma_0} & \cdots & \xi_{\mathbf{d}}^{\gamma_0} \\ \mathbf{x}^{\gamma_1} & \xi_1^{\gamma_1} & \cdots & \xi_{\mathbf{d}}^{\gamma_1} \\ \vdots & \vdots & & \vdots \\ \mathbf{x}^{\gamma_k} & \xi_1^{\gamma_k} & \cdots & \xi_{\mathbf{d}}^{\gamma_k} \\ 0 & \xi_1^{\xi_1} f_{n+1}(\xi_1) & \cdots & \xi_{\mathbf{d}}^{\xi_1} f_{n+1}(\xi_{\mathbf{d}}) \\ \vdots & \vdots & & \vdots \\ 0 & \xi_1^{\xi_r} f_{n+1}(\xi_1) & \cdots & \xi_{\mathbf{d}}^{\xi_r} f_{n+1}(\xi_{\mathbf{d}}) \end{vmatrix}.$$

□

Remark 3.8 If $\gcd(\mathcal{S}) \in \mathcal{S}$, then one can reduce the previous determinant, as in Corollary 2.7.

References

[1] Busé, Laurent; D'Andrea, Carlos. *Inversion of parameterized hypersurfaces by means of subresultants.* Proceedings of the 2004 International Symposium on

Symbolic and Algebraic Computation, 65–71, ACM Press (2004).

[2] Busé, Laurent; D'Andrea, Carlos. *On the irreducibility of multivariate subresultants.* C. R. Math. Acad. Sci. Paris 338 (2004), no. 4, 287–290.

[3] Brown, W. S.; Traub, J. F. *On Euclid's algorithm and the theory of subresultants.* J. Assoc. Comput. Mach. 18 (1971), 505–514.

[4] Chardin, Marc. *Formules à la Macaulay pour les sous-résultants en plusieurs variables.* C. R. Acad. Sci. Paris Sr. I Math. 319 (1994), no. 5, 433–436.

[5] Chardin, Marc. *Multivariate subresultants.* J. Pure Appl. Algebra 101 (1995), no. 2, 129–138.

[6] Cox, David; Little, John; O'Shea, Donal. *Using algebraic geometry.* Graduate Texts in Mathematics, 185. Springer-Verlag, New York, 1998. xii+499 pp.

[7] Collins, George E. *Subresultants and reduced polynomial remainder sequences.* J. Assoc. Comput. Mach. 14 1967 128–142.

[8] D'Andrea, Carlos; Jeronimo, Gabriela. *Subresultants and generic monomial bases*. J. Symbolic Comput. 39 (2005), no. 3–4, 259–277.

[9] Diaz-Toca, Gema M.; González-Vega, Laureano. *Various new expressions for subresultants and their applications.* Appl. Algebra Engrg. Comm. Comput. 15 (2004), no. 3-4, 233–266.

[10] Ducos, Lionel. *Algorithme de Bareiss, algorithme des sous-résultants.* RAIRO Inform. Théor. Appl. 30 (1996), no. 4, 319–347.

[11] Emiris, Ioannis Z.; Galligo, André; Lombardi, Henri. *Certified approximate univariate GCDs.* Algorithms for algebra (Eindhoven, 1996). J. Pure Appl. Algebra 117/118 (1997), 229–251.

[12] von zur Gathen, Joachim; Gerhard, Jürgen. *Modern computer algebra.* Cambridge University Press, 1999.

[13] González-Vega, Laureano. *A subresultant theory for multivariate polynomials.* Extracta Math. 5 (1990), no. 3, 150–152.

[14] González-Vega, Laureano. *Determinantal formulae for the solution set of zero-dimensional ideals.* J. Pure Appl. Algebra 76 (1991), no. 1, 57–80.

[15] González-Vega, L.; Lombardi, H.; Recio, T.; Roy, M.-F. *Spécialisation de la suite de Sturm et sous-résultants.* RAIRO Inform. Thor. Appl. 24 (1990), no. 6, 561–588.

[16] Habicht, Walter. *Zur inhomogenen Eliminationstheorie.* Comment. Math. Helv. 21 (1948). 79–98.

[17] Hong, Hoon. *Subresultants in roots.* Technical report, Department of Mathematics. North Carolina State Unversity, 1999. Submitted for publication.

[18] Hong, Hoon. *Ore subresultants coefficients in solutions.* J. Applic. Algebra 12-5 (2001) 421-428.

[19] Hou, Xiaorong; Wang, Dongming. *Subresultants with the Bézout matrix.* Computer mathematics (Chiang Mai, 2000), 19–28, Lecture Notes Ser. Comput., 8, World Sci. Publishing, River Edge, NJ, 2000.

[20] Ho, Chung-Jen; Yap, Chee Keng. *The Habicht approach to subresultants.* J. Symbolic Comput. 21 (1996), no. 1, 1–14.

[21] Jouanolou, J.-P. *Le formalisme du résultant.* Adv. Math. 90 (1991), no. 2, 117–263.

[22] Kaltofen, Erich; May, John. *On approximate irreducibility of polynomials in several variables.* Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, 161–168, ACM, New York, 2003.

[23] Lascoux, Alain. *Symmetric functions and combinatorial operators on polynomials.* CBMS Regional Conference Series in Mathematics, 99. Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 2003.

[24] Macaulay, F. *Some formulae in elimination.* Proc. London. Math. Soc., 33(1):3–27, 1902.

[25] Reischert, Daniel. *Asymptotically fast computation of subresultants.* Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation (Kihei, HI), 233–240, ACM, New York, 1997.

[26] Sylvester, J. *A theory of syzygetic relations of two rational integral functions, comprising an application to the theory of sturm's functions, and that of the greatest algebraic common measure.* Philosophical Trans., 1853.

[27] Szanto, Agnes. *Multivariate subresultants using Jouanolou's resultant matrices.* To appear in the Journal of Pure and Applied Algebra.

[28] Szanto, Agnes. *Solving over-determined systems by subresultant methods.* Submitted for publication, 2001.

[29] Weber, Heinrich. *Lehrbuch der Algebra.* Braunschweig : F. Vieweg & Sohn, 1912.

[30] Zeng, Zhonggang; Dayton, Barry. *The approximate gcd of inexact polynomials.* Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation, 320–327, ACM Press, 2004.

[31] Zeng, Zhonggang. *A method computing multiple roots of inexact polynomials.* Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, 266–272, ACM, New York, 2003.