Subresultants in multiple roots: an extremal case

Alin Bostan, Carlos d'Andrea, Teresa Krick, Agnès Szanto, Marcelo Valdettaro

HAL Id: hal-01588546

https://hal.archives-ouvertes.fr/hal-01588546

Submitted on 15 Sep 2017

Subresultants in multiple roots: an extremal case

A. Bostan

Inria, Université Paris-Saclay, 1 rue Honoré d'Estienne d'Orves, 91120 Palaiseau, France.

C. D'Andrea

Departament de Matemàtiques i Informàtica, Universitat de Barcelona (UB), Gran Via de les Corts Catalanes 585, 08007 Barcelona, Spain

T. Krick

Departamento de Matemática, Facultad de Ciencias Exactas y Naturales and IMAS, CONICET, Universidad de Buenos Aires, Argentina

A. Szanto

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

M. Valdettaro

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

Abstract

We provide explicit formulae for the coefficients of the order-d polynomial subresultant of $(x - \alpha)^m$ and $(x - \beta)^n$ with respect to the set of Bernstein polynomials $\{(x - \alpha)^j (x - \beta)^{d-j}, 0 \le j \le d\}$. They are given by hypergeometric expressions arising from determinants of binomial Hankel matrices.

Keywords: Subresultants, Hankel matrices, Ostrowski's determinant,

Email addresses: `alin.bostan@inria.fr` (A. Bostan), `cdandrea@ub.edu` (C. D'Andrea), `krick@dm.uba.ar` (T. Krick), `aszanto@ncsu.edu` (A. Szanto), `mvaldettaro@gmail.com` (M. Valdettaro)
  URL: `http://specfun.inria.fr/bostan` (A. Bostan), `http://atlas.mat.ub.es/personals/dandrea` (C. D'Andrea), `http://mate.dm.uba.ar/~krick` (T. Krick), `www4.ncsu.edu/~aszanto` (A. Szanto)

Pfaff-Saalschütz identity.

2010 MSC: 13P15, 15B05, 33C05

---

1. Introduction

Let $\mathbb{K}$ be a field, and $f = f_m x^m + \cdots + f_0$ and $g = g_n x^n + \cdots + g_0$ be two polynomials in $\mathbb{K}[x]$ with $f_m \neq 0$ and $g_n \neq 0$. Set $0 \leq d < \min\{m, n\}$. The *order-d subresultant* $\mathrm{Sres}_d(f, g)$ is the polynomial in $\mathbb{K}[x]$ defined as

$$
\mathrm{Sres}_d(f, g) := \det \left. \begin{array}{|cccccc|}
\hline
f_m & \cdots & & \cdots & f_{d+1-(n-d-1)} & x^{n-d-1}f \\
& \ddots & & & \vdots & \vdots \\
& & f_m & \cdots & f_{d+1} & f \\
g_n & \cdots & & \cdots & g_{d+1-(m-d-1)} & x^{m-d-1}g \\
& \ddots & & & \vdots & \vdots \\
& & g_n & \cdots & g_{d+1} & g \\
\hline
\end{array} \right\}
\begin{array}{l} \\ n-d \\ \\ \\ m-d \end{array}
, \quad (1)
$$

where, by convention, $f_\ell = g_\ell = 0$ for $\ell < 0$.

Although it is not immediately transparent from the definition, $\mathrm{Sres}_d(f, g)$ is a polynomial of degree at most d, whose coefficients are equal to some minors of the Sylvester matrix of f and g. Subresultants were implicitly introduced by Jacobi [Jac1836] and explicitly by Sylvester [Syl1839, Syl1840], see [GL2003] for a comprehensive historical account[1].

For any finite subsets $A = \{\alpha_1, \ldots, \alpha_m\}$ and $B = \{\beta_1, \ldots, \beta_n\}$ of $\mathbb{K}$, and for $0 \leq p \leq m$, $0 \leq q \leq n$, one can define after Sylvester [Syl1840b] the *double sum* expression:

$$
\mathrm{Syl}_{p,q}(A, B)(x) := \sum_{\substack{A' \subset A, \, B' \subset B \\ |A'| = p, |B'| = q}} \frac{\mathcal{R}(A', B') \, \mathcal{R}(A \backslash A', B \backslash B')}{\mathcal{R}(A', A \backslash A') \, \mathcal{R}(B', B \backslash B')} \, \mathcal{R}(x, A') \, \mathcal{R}(x, B'),
$$

where $\mathcal{R}(Y, Z) := \prod_{y \in Y} \prod_{z \in Z}(y - z)$.

---

[1]The Sylvester matrix was defined in [Syl1840], and the order-d subresultant was introduced in [Syl1839, Syl1840] under the name of "prime derivative of the d-degree".

Sylvester stated in [Syl1840b], then proved in [Syl1853, Section II], the following connection between subresultants and double sums: assume that $d = p + q$, and suppose that f and g are the square-free polynomials

$$f = (x - \alpha_1) \cdots (x - \alpha_m) \quad \text{and} \quad g = (x - \beta_1) \cdots (x - \beta_n).$$

Then,

$$\binom{d}{p} \mathrm{Sres}_d(f, g) = (-1)^{p(m-d)} \mathrm{Syl}_{p,q}(f, g).$$

This identity can be regarded as a generalization to subresultants of the famous Poisson formula [Poi1802] for the resultant of f and g:

$$\mathrm{Res}(f, g) = \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j). \tag{2}$$

We note however that the Poisson formula also holds when f or g have multiple roots, since it does not involve denominators in terms of differences of roots in subsets of A or in subsets of B. To demonstrate the challenges in finding closed formulae for subresultants in the most general case, consider the instance when $f = (x - \alpha_1)^{m_1} \cdots (x - \alpha_r)^{m_r}$, $g = (x - \beta_1)^{n_1} \cdots (x - \beta_s)^{n_s}$ with $\alpha_i \neq \alpha_j$, $\beta_k \neq \beta_\ell$ and $d = 1$. A (quite intricate) closed formula for $\mathrm{Sres}_1(f, g)$ appears in [DKS2013, Th.2.7] and has the form:

$$\mathrm{Sres}_1(f, g) = \sum_{i=1}^{r} (-1)^{m-m_i} \Big(\prod_{\substack{1 \le j \le r \\ j \neq i}} \frac{g(\alpha_j)^{m_j}}{(\alpha_i - \alpha_j)^{m_j}} \Big) g(\alpha_i)^{m_i - 1} \Big((x - \alpha_i) \cdot$$

$$\sum_{\substack{k_1 + \cdots + \widehat{k}_i + \cdots \\ \cdots + k_{r+s} = m_i - 1}} \prod_{\substack{1 \le j \le r \\ j \neq i}} \frac{\binom{m_j - 1 + k_j}{k_j}}{(\alpha_i - \alpha_j)^{k_j}} \prod_{1 \le \ell \le s} \frac{\binom{n_\ell - 1 + k_{r+\ell}}{k_{r+\ell}}}{(\alpha_i - \beta_\ell)^{k_{r+\ell}}}$$

$$+ \min\{1, m_i - 1\} \sum_{\substack{k_1 + \cdots + \widehat{k}_i + \cdots \\ \cdots + k_{r+s} = m_i - 2}} \prod_{\substack{1 \le j \le r \\ j \neq i}} \frac{\binom{m_j - 1 + k_j}{k_j}}{(\alpha_i - \alpha_j)^{k_j}} \prod_{1 \le \ell \le s} \frac{\binom{n_\ell - 1 + k_{r+\ell}}{k_{r+\ell}}}{(\alpha_i - \beta_\ell)^{k_{r+\ell}}} \Big).$$

This is a nontrivial expression, and nothing similar has been found yet for subresultants of general orders. It is worth noticing, however, that determinantal formulations for subresultants of square-free polynomials readily generalize to the case of polynomials with multiple roots (see [DKS2013, Th.2.5]), so that the difficulty seems to lie in finding expanded expressions.

In this article we take a completely different approach and focus on an extremal case, which is when both f and g have only one multiple root each: we get explicit expressions for $\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n)$ for all $d < \min\{m, n\}$.

To do this, we set $0 < d < \min\{m, n\}$ or $d = \min\{m, n\}$ when $m \neq n$ and $c = c(m, n, d) := m + n - 2d - 1$. We introduce the $d \times (d+1)$ integer Hankel matrix with binomial entries by

$$
\begin{aligned}
H(m, n, d) &:= \left(\binom{c}{m-i-j} \right)_{\substack{1 \leq i \leq d \\ 0 \leq j \leq d}} \\
&= \begin{pmatrix}
\binom{c}{m-1} & \binom{c}{m-2} & \cdots & \cdots & \binom{c}{m-d-1} \\
\binom{c}{m-2} & & \cdot^{\cdot^{\cdot}} & \cdot^{\cdot^{\cdot}} & \binom{c}{m-d-2} \\
\vdots & \cdot^{\cdot^{\cdot}} & \cdot^{\cdot^{\cdot}} & & \vdots \\
\binom{c}{m-d} & \binom{c}{m-d-1} & \cdots & \cdots & \binom{c}{m-2d}
\end{pmatrix},
\end{aligned}
$$

where, by convention, $\binom{c}{k} = 0$ for $k < 0$ and for $k > c$.

Denote with $q_j(m, n, d)$ the j-th maximal minor of $H(m, n, d)$ defined as the determinant of the square submatrix $H_j(m, n, d)$ of $H(m, n, d)$ obtained by deleting its $(j+1)$-th column, for $0 \leq j \leq d$. By convention, $q_0(m, n, 0)$, the determinant of an empty matrix, equals 1.

Clearly, all $q_j(m, n, d)$ are integer numbers. To regard them as elements of the field $\mathbb{K}$, we consider their class via the natural ring homomorphism $\mathbb{Z} \to \mathbb{K}$ which maps the integer 1 to the unit $1_{\mathbb{K}}$ of $\mathbb{K}$.

We now describe our main result, which provides a closed-form expression for the coefficients of the subresultant $\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n)$ when expressed in the set of Bernstein polynomials $\left\{ (x-\alpha)^j(x-\beta)^{d-j}, \, 0 \leq j \leq d \right\}$.

Theorem 1.1. *Let* $m, n, d \in \mathbb{N}$ *with* $0 \leq d < \min\{m, n\}$, *and* $\alpha, \beta \in \mathbb{K}$. *Then,*

$$
\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n) = (-1)^{\binom{d}{2}} (\alpha-\beta)^{(m-d)(n-d)} \sum_{j=0}^{d} q_j(m, n, d)(x-\alpha)^j(x-\beta)^{d-j}.
$$

Note that Theorem 1.1 is consistent with the Poisson formula (2) for $d = 0$.

Our second result completes the first one by providing explicit expressions for the values of the minors $q_j(m, n, d)$, $0 \leq j \leq d$, as products of quotients of explicit factorials.

4

Theorem 1.2. *Let $m, n, d \in \mathbb{N}$ with $0 < d < \min\{m, n\}$, and $c = m + n - 2d - 1$. Then,*

$$q_0(m, n, d) = (-1)^{\binom{d}{2}} \prod_{i=1}^{d} \frac{(i-1)!\,(c+i-1)!}{(m-i-1)!(n-i)!},$$

and for $1 \leq j \leq d$ the following identities hold in $\mathbb{Q}$:

$$q_j(m, n, d) = \frac{\binom{d}{j}\binom{n-d+j-1}{j}}{\binom{m-1}{j}}\, q_0(m, n, d).$$

The proof of Theorem 1.1 yields as a byproduct (see Proposition 3.3) a nice description of the d-th principal subresultant $\mathrm{PSres}_d((x-\alpha)^m, (x-\beta)^n)$, that is, of the coefficient of x^d in $\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n)$:

$$\mathrm{PSres}_d((x-\alpha)^m, (x-\beta)^n) = (\alpha-\beta)^{(m-d)(n-d)} \prod_{i=1}^{d} \frac{(i-1)!\,(c+i)!}{(m-i)!(n-i)!}. \quad (3)$$

The product in (3) is an integer number whose prime factors are less than $m+n-d$. Thus, if $\alpha \neq \beta$ and if the characteristic of $\mathbb{K}$ is either zero or at least equal to $m+n-d$, the subresultant $\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n)$ is a polynomial of degree exactly d. When $\mathrm{char}(\mathbb{K})$ is positive but smaller than $m+n-d$, this is generally not true (though exceptions exist, e.g., for $m = 5, n = 3, d = 2$ and $\mathrm{char}(\mathbb{K}) = 3$). The change of behavior might be very radical. For instance, there exist triples (m, n, d) for which the degree of $\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n)$ is less than d for any positive characteristic $p < m+n-d$. Such an example is $(m, n, d) = (6, 8, 2)$. Another interesting example is when $p = m+n-d-1$: in that case, $\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n)$ reduces to a constant in characteristic p. In general, the degree of $\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n)$ can be determined using Theorem 1.2. For example, in characteristic 5, the order-8 subresultant of $(x-\alpha)^{11}$ and $(x-\beta)^9$ is a polynomial of degree 6 for all $\alpha \neq \beta$.

We briefly sketch our proof strategy for these results. We start from the basic fact that if $\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n)$ has degree exactly d, then any linear combination $\mathcal{F} \cdot (x-\alpha)^m + \mathcal{G} \cdot (x-\beta)^n$, of degree bounded by d with $\deg(\mathcal{F}) < n-d$ and $\deg(\mathcal{G}) < m-d$, is a scalar multiple of the subresultant (Lemma 3.1). In Proposition 3.4 we show that $\sum_{j=0}^{d} q_j(m, n, d)(x-\alpha)^j(x-\beta)^{d-j}$ can be expressed as such a linear combination, and determine the scalar multiple which is the ratio between this expression and the subresultant. Theorem 1.1

then follows by specializing the "generic case" (in characteristic zero) to fields of positive characteristic.

To prove Theorem 1.2, we proceed in two main steps. We first evaluate $q_0(m, n, d)$ in Lemma 2.3 by using a result due to Ostrowski (Lemma 2.1) for the determinant evaluation of a Hankel matrix involving binomial coefficients. Then, in Lemma 2.4 we reduce the computation of the remaining $q_j(m, n, d)$, $1 \leq j \leq d$, to a hypergeometric identity due to Pfaff and Saalschütz (Lemma 2.2).

Sylvester's original motivation for deriving expressions in roots for subresultants was to understand how Sturm's method for computing the number of real roots of a polynomial in a given interval works formally; see [Syl1853], where Sylvester applies the theory of subresultants developed there to the case when $g = f'$, with f having simple roots. Furthermore, Sylvester's formulae opened the door to have great flexibility in the evaluation of resultants and subresultants (see the book of Jouanolou and Apéry [AJ2006] for several ingenious formulae for the simple roots case). The search of explicit expressions for subresultants of polynomials having multiple roots is an active area of research; see for instance [Hon1999, LP2003, DHKS2007, DHKS2009, RS2011, DKS2013]. The quest for such formulae has uncovered some interesting connections of subresultants to other well-known objects and thus several new applications were discovered.

One of these applications are closed expressions for various rational interpolation problems, including the Cauchy interpolation or the osculatory rational interpolation problem [BL2000, DKS2015]. The search for formulae in multiple roots also uncovered the close connection of subresultants to multivariate symmetric Lagrange interpolation [KSV2017]; generalizations to symmetric Hermite interpolation are the topic of ongoing research. These formulae in roots may be used to analyze the vanishing of the coefficients of the subresultants (see the discussion after Theorem 1.2), a question related to the understanding of the performance of the Euclidean Algorithm for polynomials over finite fields [MG1990]. Our closed formulae also led us think about accelerating the computation of the subresultants in our particular extremal case; this will be explained in detail in a forthcoming paper.

The paper is organized as follows: We first derive Theorem 1.2 in Section 2 thanks to Lemmas 2.3 and 2.4. Section 3 then introduces the aforementioned multiple of the subresultant and proves Theorem 1.1.

2. Proof of Theorem 1.2

All along this section, we work over the rational numbers to compute the coefficients $q_j(m, n, d)$ which appear in the expression of the subresultant given in Theorem 1.1 over a field $\mathbb{K}$ of characteristic zero. As these numbers are integers, we can regard them as elements of any field $\mathbb{K}$ via the natural ring homomorphism $\mathbb{Z} \to \mathbb{K}$ which maps $1_\mathbb{Z} \mapsto 1_\mathbb{K}$.

We start by recalling Ostrowski's determinant evaluation (Lemma 2.1) for Hankel matrices with binomial coefficients entries, and the Pfaff-Saalschütz identity (Lemma 2.2) for the evaluation at the point 1 of a special family of $_3F_2$ hypergeometric functions.

Lemma 2.1 ([Ost1964]). *For $\ell, k \in \mathbb{N}$ and $a_0, a_1, \ldots, a_k \in \mathbb{N}$,*

$$\det\left(\binom{\ell}{a_i - j}\right)_{0 \leq i, j \leq k} = \ell!^{k+1} \frac{\prod_{i=1}^k (\ell + i)^{k+1-i} \prod_{0 \leq i < i' \leq k} (a_{i'} - a_i)}{\prod_{i=0}^k a_i! \prod_{i=0}^k (\ell + k - a_i)!}.$$

Lemma 2.2 ([Pfa1797, Saa1890, And1996, And1997], [Sla1966, §2.3.1]). *Let x, y, z be indeterminates over $\mathbb{Q}$. Then, for any $k \in \mathbb{N}$, the following identity holds in $\mathbb{Q}(x, y, z)$:*

$$\sum_{j=0}^k \frac{(x)_j (y)_j (-k)_j}{(z)_j (1 + x + y - z - k)_j \, j!} = \frac{(z - x)_k (z - y)_k}{(z)_k (z - x - y)_k}.$$

Here $(x)_0 := 1$ and $(x)_j := x(x+1) \cdots (x + j - 1)$ for $j \geq 1$ denotes the $j-$th Pochhammer symbol of x.

By applying these two results, Theorem 1.2 follows straightforwardly from Lemmas 2.3 and 2.4 below. Lemma 2.3 computes $q_0(m, n, d)$ as a direct consequence of Ostrowski's determinant evaluation. Lemma 2.4 computes all $q_j(m, n, d)$ for $j > 0$, and is a consequence of a binomial identity (given in (6)) which is, in fact, the Pfaff-Saalschütz identity in disguise. Recall that we have set $c = m + n - 2d - 1$.

Lemma 2.3. *Let $d, m, n \in \mathbb{N}$ with $0 < d < \min\{m, n\}$. Then,*

$$q_0(m, n, d) = (-1)^{\binom{d}{2}} \prod_{i=1}^{d} \frac{(i-1)!(c+i-1)!}{(m-i-1)!(n-i)!}.$$

Proof. Using Lemma 2.1 with $k = d-1$ and $a_i = m - i - 2$ for $0 \leq i \leq d-1$, and $\ell = c$ we get

$$\begin{aligned}
q_0(m, n, d) &= \det\left(\binom{c}{m-i-j}\right)_{1 \leq i,j \leq d} = \det\left(\binom{c}{m-i-j-2}\right)_{0 \leq i,j \leq d-1} \\
&= c!^d \frac{\prod_{i=1}^{d-1}(c+i)^{d-i} \prod_{0 \leq i < i' \leq d-1}(i-i')}{\prod_{i=0}^{d-1}(m-i-2)! \prod_{i=0}^{d-1}(c+d-1-(m-i-2))!} \\
&= \frac{\prod_{i=1}^{d}\left(c! \prod_{j=1}^{i-1}(c+j)\right) \cdot (-1)^{\binom{d}{2}} \prod_{i=1}^{d}(i-1)!}{\prod_{i=1}^{d}(m-i-1)! \prod_{i=1}^{d}(n-d+i-1)!}.
\end{aligned}$$

The statement follows by rearranging terms. $\qquad\square$

Lemma 2.4. *Let $j, d, m, n \in \mathbb{N}$ with $0 < j \leq d < \min\{m, n\}$. Then,*

$$q_j(m, n, d) = \frac{\binom{d}{j}\binom{n-d+j-1}{j}}{\binom{m-1}{j}} q_0(m, n, d).$$

Proof. Observe that the matrix H has full rank d since by Lemma 2.3, its minor $q_0(m, n, d)$ is non-zero. Therefore, an elementary linear algebra argument shows that the kernel of the induced linear map $H\colon \mathbb{Q}^{d+1} \to \mathbb{Q}^d$ has dimension 1, and is generated by the (non-zero) vector

$$\mathbf{q}(m, n, d) := (q_0(m, n, d), -q_1(m, n, d), \ldots, (-1)^d q_d(m, n, d)).$$

Set $k_j(m, n, d) := \dfrac{\binom{d}{j}\binom{n-d+j-1}{j}}{\binom{m-1}{j}}$ for $0 \leq j \leq d$. It suffices then to show that

$$\mathbf{k}(m, n, d) := (k_0(m, n, d), -k_1(m, n, d), \ldots, (-1)^d k_d(m, n, d)) \in \ker H, \quad (4)$$

so then we would have $\mathbf{k}(m, n, d) = \lambda \, \mathbf{q}(m, n, d)$ with $\lambda = 1/q_0(m, n, d)$, as $k_0(m, n, d) = 1$.

Therefore, to prove (4) it is enough to check the following identities

$$\sum_{j=0}^{d} \binom{m + n - 2d - 1}{m - j - i}(-1)^j k_j(m, n, d) = 0 \quad \text{for } 1 \leq i \leq d. \quad (5)$$

We actually prove that a more general identity holds for any $i \in \mathbb{N}$:

$$\sum_{j=0}^{d} \binom{m + n - 2d - 1}{m - j - i}(-1)^j \frac{\binom{d}{j}\binom{n-d+j-1}{j}}{\binom{m-1}{j}} = \frac{\binom{i-1}{d}\binom{m+n-d-1}{m-i}}{\binom{m-1}{d}}, \quad (6)$$

The expressions in (5) are then recovered by specializing i to $1, \ldots, d$.

The equalities in (6) follow from the Pfaff-Saalschütz identity described in Lemma 2.2. Since both sides of (6) are polynomials in n (of degree at most $m - i$) it is enough to verify them for an infinite number of values n. We will show that they hold for $n \geq 2d$.

By observing that $(a + j - 1)! = (a - 1)!(a)_j$, $\binom{a+j-1}{j} = \frac{(a)_j}{j!}$, $(a - j)! = (-1)^j \frac{a!}{(-a)_j}$ and $\binom{a}{j} = (-1)^j \frac{(-a)_j}{j!}$, we deduce that the left-hand side of (6) is equal, for $n \geq 2d$, to

$$\frac{(m + n - 2d - 1)!}{(m - i)!(n - 2d + i - 1)!} \cdot \sum_{j=0}^{d} \frac{(n - d)_j(-(m - i))_j(-d)_j}{(n - 2d + i)_j(-(m - 1))_j j!}.$$

To simplify the latter sum, we now apply Lemma 2.2 for $k = d$, and for x, y, z specialized respectively to $n - d, -(m - i), n - 2d + i$, and get

$$\sum_{j=0}^{d} \frac{(n - d)_j(-(m - i))_j(-d)_j}{(n - 2d + i)_j(-(m - 1))_j \, j!} = \frac{(i - d)_d(m + n - 2d)_d}{(n - 2d + i)_d(m - d)_d}$$

$$= \frac{\binom{i-1}{d}(m + n - 2d) \cdots (m + n - d - 1)}{\binom{m-1}{d}(n - 2d + i) \cdots (n - d + i - 1)},$$

from which (6) follows immediately. $\qquad \square$

3. Proof of Theorem 1.1

To prove Theorem 1.1, we make use of the following well-known result, which follows for instance from Lemmas 7.7.4 and 7.7.6 in [Mis1993].

Lemma 3.1. *Let $m, n, d \in \mathbb{N}$ with $0 \leq d < \min\{m, n\}$, and $f, g \in \mathbb{K}[x]$ have degrees m and n respectively. Assume $\mathrm{PSres}_d(f, g) \neq 0$. If $\mathcal{F}, \mathcal{G} \in \mathbb{K}[x]$ are such that $\deg(\mathcal{F}) < n - d$, $\deg(\mathcal{G}) < m - d$ and $h = \mathcal{F} f + \mathcal{G} g$ is a non-zero polynomial in $\mathbb{K}[x]$ of degree at most d, then there exists $\lambda \in \mathbb{K}\backslash\{0\}$ satisfying*

$$h = \lambda \cdot \mathrm{Sres}_d(f, g).$$

Following Lemma 3.1, we first prove that $\mathrm{Sres}_d((x - \alpha)^m, (x - \beta)^n)$ has indeed degree d when $\alpha \neq \beta$ and $\mathrm{char}(\mathbb{K}) = 0$ or $\mathrm{char}(\mathbb{K}) \geq m + n - d$, in other words, that its principal subresultant $\mathrm{PSres}_d((x - \alpha)^m, (x - \beta)^n)$ is non-zero. We start by recalling a well-known result, which is used in the proof.

Lemma 3.2 (Proposition 8.6(i) in [AJ2006]). *Let $f, g \in \mathbb{K}[x]$. Then, for any $\alpha \in \mathbb{K}$,*

$$\mathrm{Sres}_d(f, g)(x + \alpha) = \mathrm{Sres}_d(f(x + \alpha), g(x + \alpha))(x).$$

Proposition 3.3. *Let $d, m, n \in \mathbb{N}$ with $0 < d < \min\{m, n\}$, and $\alpha, \beta \in \mathbb{K}$. Then,*

$$\mathrm{PSres}_d\left((x - \alpha)^m, (x - \beta)^n\right) = (\alpha - \beta)^{(m-d)(n-d)} \prod_{i=1}^{d} \frac{(i-1)!\,(c+i)!}{(m-i)!(n-i)!}.$$

In particular, if $\alpha \neq \beta$ and $\mathrm{char}(\mathbb{K}) = 0$ or $\mathrm{char}(\mathbb{K}) \geq m + n - d$, then

$$\deg\left(\mathrm{Sres}_d((x - \alpha)^m, (x - \beta)^n)\right) = d.$$

Proof.

$$\mathrm{PSres}_d((x - \alpha)^m, (x - \beta)^n) = \mathrm{PSres}_d(x^m, (x + \alpha - \beta)^n)$$

$$= \mathrm{PSres}_d(x^m, \sum_{j=0}^{n} \binom{n}{j}(\alpha - \beta)^{n-j} x^j).$$

10

Therefore, by the definition of the principal subresultant,

$\mathrm{PSres}_d((x-\alpha)^m, (x-\beta)^n) =$

$$= \det \begin{bmatrix} \overset{\overbrace{\hspace{6cm}}^{m+n-2d}}{} \\ \left. \begin{array}{cccccc} 1 & \cdots & 0 & \cdots & 0 \\ \ddots & & \vdots & & \vdots \\ & \ddots & \vdots & & \vdots \\ & & 1 & 0 & \cdots & 0 \\ 1 & \cdots & \binom{n}{d}(\alpha-\beta)^{n-d} & \cdots & \binom{n}{m-1}(\alpha-\beta)^{n-(m-1)} \\ \ddots & & \vdots & & \vdots \\ & 1 & \cdots & \binom{n}{2d-m+1}(\alpha-\beta)^{n-(2d-m+1)} & \cdots & \binom{n}{d}(\alpha-\beta)^{n-d} \end{array}\right. \end{bmatrix} \begin{array}{l} n-d \\ \\ \\ \\ m-d \end{array}$$

$$= \det \begin{bmatrix} \overset{\overbrace{\hspace{5cm}}^{m-d}}{} \\ \begin{array}{ccc} \binom{n}{d}(\alpha-\beta)^{n-d} & \cdots & \binom{n}{m-1}(\alpha-\beta)^{n-(m-1)} \\ \binom{n}{d-1}(\alpha-\beta)^{n-(d-1)} & \cdots & \binom{n}{m-2}(\alpha-\beta)^{n-(m-2)} \\ \vdots & & \vdots \\ \binom{n}{2d-m+1}(\alpha-\beta)^{n-(2d-m+1)} & \cdots & \binom{n}{d}(\alpha-\beta)^{n-d} \end{array} \end{bmatrix} m-d$$

$$= (\alpha-\beta)^{(m-d)(n-d)} \det \left(\binom{n}{d-i+j} \right)_{1 \le i,j \le m-d}$$

$$= (\alpha-\beta)^{(m-d)(n-d)} \prod_{i=1}^{d} \frac{(i-1)!\,(c+i)!}{(m-i)!(n-i)!}.$$

The third equality above follows from the "weighted" homogeneities of the determinant. Indeed, by multiplying the i-th row in the second matrix above by $(\alpha-\beta)^{i-1}$, $1 \le i \le m-d$, the whole determinant gets multiplied by $(\alpha-\beta)^{1+\cdots+(m-d-1)} = (\alpha-\beta)^{\binom{m-d}{2}}$, but now for each $j = 1, \ldots, m-d$, column j has the same term $(\alpha-\beta)^{n-d+j-1}$ that can be factored out, obtaining $(\alpha-\beta)^{(n-d+m-d-1)+\cdots+(n-d+0)} = (\alpha-\beta)^{(m-d)(n-d)+\binom{m-d}{2}}$ and one can then clear out the spurious $(\alpha-\beta)^{\binom{m-d}{2}}$), and the equality can be derived from Lemma 2.1 with $\ell = n$, $k = m-d-1$ and $a_j = d+j+1$ for $0 \le i \le m-d-1$. $\qquad \square$

We now show how to express a scalar multiple of the polynomial expression $\sum_{j=0}^{d} q_j(m,n,d)(x-\alpha)^j(x-\beta)^{d-j}$ as a polynomial combination $\mathcal{F} \cdot (x-\alpha)^m + \mathcal{G} \cdot (x-\beta)^n$, with $\mathcal{F}$ and $\mathcal{G}$ satisfying the hypothesis of

11

Lemma 3.1. For this, we define for $0 \le d < \min\{m, n\}$,

$$h_d(\alpha, \beta, m, n) := (\alpha - \beta)^c \Big(\sum_{j=0}^{d} q_j(m, n, d)(x - \alpha)^j (x - \beta)^{d-j} \Big). \qquad (7)$$

Note that $h_d(\alpha, \beta, m, n) \in \mathbb{K}[x]$ has degree bounded by d.

Proposition 3.4. *Let $d, m, n \in \mathbb{N}$ with $0 \le d < \min\{m, n\}$, and $\alpha, \beta \in \mathbb{K}$. There exist $\mathcal{F}, \mathcal{G} \in \mathbb{K}[x]$ with $\deg(\mathcal{F}) < n - d$, $\deg(\mathcal{G}) < m - d$ such that*

$$h_d(\alpha, \beta, m, n) = \mathcal{F} \cdot (x - \alpha)^m + \mathcal{G} \cdot (x - \beta)^n.$$

Proof. Set $f := (x - \alpha)^m$ and $g := (x - \beta)^n$, and write

$$(\alpha - \beta)^c = (\alpha - x + x - \beta)^c = \sum_{k=0}^{c} (-1)^k \binom{c}{k} (x - \alpha)^k (x - \beta)^{c-k}.$$

Fix $0 \le j \le d$. Then,

$$(\alpha - \beta)^c (x - \alpha)^j (x - \beta)^{d-j} = \sum_{k=0}^{c} (-1)^k \binom{c}{k} (x - \alpha)^{k+j} (x - \beta)^{c-k+d-j}.$$

For $k + j \ge m$ the corresponding terms in the right-hand side are polynomial multiples of f, with coefficient $\mathcal{F}_j$ of degree bounded by $(k + j) + (c - k + d - j) - m = n - d - 1$. Similarly, for $c - k + d - j \ge n$, the corresponding terms are multiples of g, with coefficient $\mathcal{G}_j$ of degree bounded by $(k + j) + (c - k + d - j) - n = m - d - 1$. The remaining terms satisfy $k + j < m$, i.e. $k < m - j$ and $c - k + d - j < n$, i.e. $k > m - j - d - 1$.

Therefore

$$(\alpha - \beta)^c (x - \alpha)^j (x - \beta)^{d-j}$$

$$= \mathcal{F}_j f + \mathcal{G}_j g + \sum_{k=m-j-d}^{m-j-1} (-1)^k \binom{c}{k} (x - \alpha)^{k+j} (x - \beta)^{c-k+d-j}$$

$$= \mathcal{F}_j f + \mathcal{G}_j g + \sum_{i=1}^{d} (-1)^{m-i-j} \binom{c}{m-i-j} (x - \alpha)^{m-i} (x - \beta)^{n-d+i-1}.$$

12

Multiplying each of these equations by $q_j(m, n, d)$ for $0 \leq j \leq d$ and adding them up, we get

$$h_d(\alpha, \beta, m, n) = (\alpha - \beta)^c \Big(\sum_{j=0}^{d} q_j(m, n, d)(x - \alpha)^j (x - \beta)^{d-j} \Big)$$

$$= \mathcal{F} f + \mathcal{G} g +$$

$$\sum_{j=0}^{d} \Big(\sum_{i=1}^{d} (-1)^{m-i-j} \binom{c}{m-i-j} q_j(m, n, d)(x - \alpha)^{m-i}(x - \beta)^{n-d+i-1} \Big),$$

with $\mathcal{F} := \sum_{j=0}^{d} q_j(m, n, d)\mathcal{F}_j$ and $\mathcal{G} := \sum_{j=0}^{d} q_j(m, n, d)\mathcal{G}_j$. It turns out that

$$\sum_{j=0}^{d} \Big(\sum_{i=1}^{d} (-1)^{m-i-j} \binom{c}{m-i-j} q_j(m, n, d) \, (x - \alpha)^{m-i}(x - \beta)^{n-d+i-1} \Big)$$

$$= \sum_{i=1}^{d} (-1)^{m-i}(x - \alpha)^{m-i}(x - \beta)^{n-d+i-1} \Big(\sum_{j=0}^{d} (-1)^j \binom{c}{m-i-j} q_j(m, n, d) \Big)$$

$$= 0,$$

since, as observed in the proof of Lemma 2.4, $(q_0(m, n, d), -q_1(m, n, d), \ldots,$ $(-1)^d q_d(m, n, d))$ generates $\ker H$.
Therefore $h_d(\alpha, \beta, m, n) = \mathcal{F} \cdot (x - \alpha)^m + \mathcal{G} \cdot (x - \beta)^n$ with $\deg(\mathcal{F}) < n - d$ and $\deg(\mathcal{G}) < m - d$. $\qquad \square$

We now compute explicitly the d-th coefficient of $h_d(\alpha, \beta, m, n)$, which also implies in particular that it has degree exactly d when $\alpha \neq \beta$ and $\mathrm{char}(\mathbb{K}) = 0$ or $\mathrm{char}(\mathbb{K}) \geq m + n - d$.

Proposition 3.5. *Let $d, m, n \in \mathbb{N}$ with $0 < d < \min\{m, n\}$, and $\alpha, \beta \in \mathbb{K}$. Then,*

$$\mathrm{coeff}_{x^d}\big(h_d(\alpha, \beta, m, n) \big) = (-1)^{\binom{d}{2}}(\alpha - \beta)^c \prod_{i=1}^{d} \frac{(i-1)! \, (c+i)!}{(m-i)!(n-i)!}.$$

For $d = 0$ we have $h_0(\alpha, \beta, m, n) = (\alpha - \beta)^c$.

Proof. It is clear that $\mathrm{coeff}_{x^d}(h_d(\alpha, \beta, m, n)) = (\alpha - \beta)^c \sum_{j=0}^d q_j(m, n, d)$. The $d = 0$ case follows from our convention that $q_0(m, n, 0) = 1$.

We now show that $\sum_{j=1}^d q_j(m, n, d) = q_0(m+1, n, d)$, which proves the statement by Lemma 2.3.

Observe that

$$\sum_{j=0}^d q_j(m, n, d) = \det \overbrace{\begin{bmatrix} 1 & \cdots & (-1)^d \\ \binom{c}{m-1} & \cdots & \binom{c}{m-d-1} \\ \vdots & & \vdots \\ \binom{c}{m-d} & \cdots & \binom{c}{m-2d} \end{bmatrix}}^{d+1} \Big\} d+1 \; .$$

For $0 \le j \le d$ let $\mathbf{C}(j)$ denote the $(j+1)$-th column of the matrix above. We perform the following operations: $\mathbf{C}(j) + \mathbf{C}(j-1) \to \mathbf{C}(j)$ for $j = d, \ldots, 0$. By using the identity $\binom{c}{k-1} + \binom{c}{k} = \binom{c+1}{k}$, we get

$$\det \overbrace{\begin{bmatrix} 1 & \cdots & (-1)^d \\ \binom{c}{m-1} & \cdots & \binom{c}{m-d-1} \\ \vdots & & \vdots \\ \binom{c}{m-d} & \cdots & \binom{c}{m-2d} \end{bmatrix}}^{d+1} \Big\} d+1 = \det \begin{array}{|c|ccc|c} \multicolumn{1}{c}{\overbrace{}^{1}} & \multicolumn{3}{c}{\overbrace{}^{d}} & \\ \hline 1 & 0 & \cdots & 0 & \} 1 \\ \binom{c}{m-1} & \binom{c+1}{m-1} & \cdots & \binom{c+1}{m-d} & \\ \vdots & \vdots & & \vdots & \} d \\ \binom{c}{m-d-1} & \binom{c+1}{m-d} & \cdots & \binom{c+1}{m-2d+1} & \end{array}$$

$$= q_0(m+1, n, d).$$

$\square$

We are now ready to prove Theorem 1.1.

Proof of Theorem 1.1. When $\alpha = \beta$, both sides of the expression in Theorem 1.1 vanish.

Assume now that $\alpha \neq \beta$, and that $\mathrm{char}(\mathbb{K}) = 0$, or $\mathrm{char}(\mathbb{K}) \ge m + n - d$. Thanks to Propositions 3.3 and 3.5, both $\mathrm{Sres}_d((x - \alpha)^m, (x - \beta)^n)$ and $h_d(\alpha, \beta, m, n)$ are non-zero polynomials of degree exactly d. Recall that we have set $c = m + n - 2d - 1$. Proposition 3.4 and Lemma 3.1 with $\mu = 1/\lambda$ then imply that

$$\mathrm{Sres}_d((x - \alpha)^m, (x - \beta)^n) = \mu \cdot h_d(\alpha, \beta, m, n) \tag{8}$$

14

with

$$\mu = \frac{\text{PSres}_d((x-\alpha)^m, (x-\beta)^n)}{\text{coeff}_{x^d}(h_d(\alpha, \beta, m, n))}$$

$$= \frac{(\alpha - \beta)^{(m-d)(n-d)} \prod_{i=1}^{d} \frac{(i-1)! \, (c+i)!}{(m-i)!(n-i)!}}{(-1)^{\binom{d}{2}} (\alpha - \beta)^c \prod_{i=1}^{d} \frac{(i-1)! \, (c+i)!}{(m-i)!(n-i)!}}$$

$$= (-1)^{\binom{d}{2}} (\alpha - \beta)^{(m-d)(n-d)-c}.$$

To prove these equalities, we use the identities shown in Propositions 3.3 and 3.5. The final identity for μ also holds when $d = 0$. Plugging the expression of h_d given in (7) in the identity (8), we deduce Theorem 1.1 in this case.

In the general case, we use the fact that Theorem 1.1 holds for $(x - u_\alpha)^m$ and $(x - u_\beta)^n$ in $\mathbb{K} \supset \mathbb{Q}(u_\alpha, u_\beta)$, where u_α, u_β are indeterminates over $\mathbb{Q}$. As subresultants are defined via the determinant (1), and in this case they actually belong to $\mathbb{Z}[u_\alpha, u_\beta][x]$, the expression (1.1) holds after specializing $u_\alpha \mapsto \alpha$, $u_\beta \mapsto \beta$, and the standard ring homomorphism $\mathbb{Z} \to \mathbb{K}$. This concludes the proof of Theorem 1.1.

$\square$

[And1996] George E. Andrews. *Pfaff's method. II. Diverse applications.* J. Comput. Appl. Math. 68 (2009), no. 1–2, 15–23.
http://dx.doi.org/10.1016/0377-0427(95)00258-8

[And1997] George E. Andrews. *Pfaff's method. III. Comparison with the WZ method.* Electron. J. Combin. 3 (1996), no. 2, 18 pp.
http://www.combinatorics.org/ojs/index.php/eljc/article/view/v3i2r21

[AJ2006] François Apéry, Jean-Pierre Jouanolou *Résultant et sous-résultant: le cas d'une variable avec exercices corrigés.* Hermann, Paris (2006).
http://catalogue.bnf.fr/ark:/12148/cb409455562

[BL2000] Bernard Beckermann, George Labahn. *Fraction-free computation of matrix rational interpolants and matrix GCDs.* SIAM J. Matrix Anal. Appl. 22 (2000), no. 1, 114–144.
http://dx.doi.org/10.1137/S0895479897326912

[DHKS2007] Carlos D'Andrea, Hoon Hong, Teresa Krick, Agnes Szanto. *An elementary proof of Sylvester's double sums for subresultants.* J. Symbolic Comput. 42 (2007), no. 3, 290–297.
http://dx.doi.org/10.1016/j.jsc.2006.09.003

[DHKS2009] Carlos D'Andrea, Hoon Hong, Teresa Krick, Agnes Szanto. *Sylvester's double sums: the general case.* J. Symbolic Comput. 44 (2009), no. 9, 1164–1175.
http://dx.doi.org/10.1016/j.jsc.2008.02.011

[DKS2013] Carlos D'Andrea, Teresa Krick, Agnes Szanto. *Subresultants in multiple roots.* Linear Algebra Appl. 438 (2013), no. 5, 1969–1989.
http://dx.doi.org/10.1016/j.laa.2012.11.004

[DKS2015] Carlos D'Andrea, Teresa Krick, Agnes Szanto. *Subresultants, Sylvester sums and the rational interpolation problem.* J. Symbolic Comput. 68 (2015), P.1, 72–83.
http://dx.doi.org/10.1016/j.jsc.2014.08.008

[GL2003] Joachim von zur Gathen, Thomas Lücking. *Subresultants revisited.* Theoret. Comput. Sci. 297 (2003), no. 1–3, 199–239.
http://dx.doi.org/10.1016/S0304-3975(02)00639-4

[Hon1999] Hoon Hong. *Subresultants in roots.* Technical report, Department of Mathematics, North Carolina State University, 1999.

[Jac1836] C. G. J. Jacobi. *De eliminatione variabilis e duabus aequationibus algebraicis.* J. Reine Angew. Math. 15 (1836), 101–124.
http://doi.org/10.1515/crll.1836.15.101

[KSV2017] Teresa Krick, Agnes Szanto, Marcelo Valdettaro. *Symmetric interpolation, exchange lemma and Sylvester sums,* Communications in Algebra, **45**, 8, pp 3231–3250, (2017).
http://dx.doi.org/10.1080/00927872.2016.1236121

[LP2003] Alain Lascoux, Piotr Pragacz. *Double Sylvester sums for subresultants and multi-Schur functions.* J. Symbolic Comput. 35 (2003), no. 6, 689–710.
http://dx.doi.org/10.1016/S0747-7171(03)00038-5

[MG1990] Keju Ma; Joachim von zur Gathen. *Analysis of Euclidean algorithms for polynomials over finite fields.* J. Symbolic Comput. 9 (1990), no. 4, 429–455.
https://doi.org/10.1016/S0747-7171(08)80021-1

[Mis1993] Bhubaneswar Mishra. *Algorithmic algebra.* Texts and Monographs in Computer Science. Springer-Verlag, New York, 1993. xii+416 pp.
http://dx.doi.org/10.1007/978-1-4612-4344-1

[Ost1964] A. M. Ostrowski. *On some determinants with combinatorial numbers.* J. Reine Angew. Math 216 (1964) 25–30.
http://dx.doi.org/10.1515/crll.1964.216.25

[Pfa1797] J. F. Pfaff. *Observationes analyticae ad L. Euleri Institutiones Calculi Integralis, Vol. IV, Supplem. II et IV.* Histoire de l'Académie Impériale des Sciences, 1793. In: Nova Acta Academiae Scientiarum Imperialis Petropolitanae XI (1797), 37–57. (Note that the history section is paged separately from the scientific section of this journal.)

[Poi1802] S.-D. Poisson. *Mémoire sur l'élimination dans les équations algébriques.* Journal de l'École polytechnique, tome IV, 11e cahier (1802), 199–203.
http://gallica.bnf.fr/ark:/12148/bpt6k4336689/f209

[RS2011] Marie-Françoise Roy, Aviva Szpirglas. *Sylvester double sums and subresultants.* J. Symbolic Comput. 46 (2011), no. 4, 385–395.
http://dx.doi.org/10.1016/j.jsc.2010.10.012

[Saa1890] L. Saalschütz. *Eine Summationsformel.* Zeitschr. für Math. u. Phys. 35 (1890) 186–188.

[Sla1966] Lucy Joan Slater. *Generalized hypergeometric functions.* Cambridge University Press, 1966.
http://www.cambridge.org/9780521090612

[Syl1839] J. J. Sylvester. *On rational derivation from equations of coexistence, that is to say, a new and extended theory of elimination.*

Philos. Mag. 15 (1839), 428–435. Also appears in the Collected Mathematical Papers of James Joseph Sylvester, Vol. **1**, Chelsea Publishing Co. (1973), 40-46.
http://dx.doi.org/10.1080/14786443908649916

[Syl1840] J. J. Sylvester. *A method of determining by mere inspection the derivatives from two equations of any degree.* Philos. Mag. 16 (1840), 132–135. Also appears in the Collected Mathematical Papers of James Joseph Sylvester, Vol. **1**, Chelsea Publishing Co. (1973), 54-57.
http://dx.doi.org/10.1080/14786444008649995

[Syl1840b] J. J. Sylvester. *Note on elimination.* Philos. Mag. 17 (1840), no. 11, 379–380. Also appears in the Collected Mathematical Papers of James Joseph Sylvester, Vol. **1**, Chelsea Publishing Co. (1973), p. 58.
http://dx.doi.org/10.1080/14786444008650196

[Syl1853] J. J. Sylvester. *On a theory of the syzygetic relations of two rational integral functions, comprising an application to the theory of Sturm's functions and that of the greatest algebraical common measure.* Philosophical Transactions of the Royal Society of London, Part III (1853), 407–548. Also appears in the Collected Mathematical Papers of James Joseph Sylvester, Vol. **1**, Chelsea Publishing Co. (1973), 429–586.
http://dx.doi.org/10.1098/rstl.1853.0018