Subresultants of $(x-\alpha)^m$ and $(x-\beta)^n$, Jacobi polynomials and complexity

Alin Bostan, T Krick, A Szanto, M Valdettaro

Subresultants of $(x-\alpha)^m$ and $(x-\beta)^n$, Jacobi polynomials and complexity

A. Bostan

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

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

In an earlier article [BDKSV2017], explicit expressions were described for the coefficients of the order-d polynomial subresultant of $(x-\alpha)^m$ and $(x-\beta)^n$ with respect to Bernstein's set of polynomials $\{(x-\alpha)^j(x-\beta)^{d-j},\ 0 \le j \le d\}$, for $0 \le d < \min\{m,n\}$. The current paper further develops the study of these structured polynomials and shows that the coefficients of the subresultants of $(x-\alpha)^m$ and $(x-\beta)^n$ with respect to the monomial basis can be computed in *linear* arithmetic complexity, which is faster than for arbitrary polynomials. The result is obtained as a consequence of the amazing though seemingly unnoticed fact that these subresultants are scalar multiples

Email addresses: alin.bostan@inria.fr (A. Bostan), krick@dm.uba.ar (T. Krick), aszanto@ncsu.edu (A. Szanto), mvaldett@dm.uba.ar (M. Valdettaro)

URL: http://specfun.inria.fr/bostan (A. Bostan), http://mate.dm.uba.ar/~krick (T. Krick), http://aszanto.math.ncsu.edu (A. Szanto), http://cms.dm.uba.ar/Members/mvaldettaro/ (M. Valdettaro)

of Jacobi polynomials up to an affine change of variables.

Keywords: Subresultants, algorithms, complexity, Jacobi polynomials.

2010 MSC: 13P15, 15B05, 33C05, 33C45, 33F10, 68W30

---

1. Introduction

Let $\mathbb{K}$ be a field, and let $f = f_m x^m + \cdots + f_0$ 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

$$\mathrm{Sres}_d(f,g) := \det \begin{array}{|cccccc|} \multicolumn{6}{c}{\overbrace{}^{m+n-2d}} \\ \hline f_m & \cdots & & \cdots & f_{d+1-(n-d-1)} & x^{n-d-1}f \\ & \ddots & & & \vdots & \vdots \\ & & f_m & \cdots & f_{d+1} & f \\ \hline g_n & \cdots & & \cdots & g_{d+1-(m-d-1)} & x^{m-d-1}g \\ & \ddots & & & \vdots & \vdots \\ & & g_n & \cdots & g_{d+1} & g \\ \hline \end{array} \begin{array}{l} \\ \\ n-d \\ \\ \\ m-d \end{array}, \quad (1)$$

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

The polynomial $\mathrm{Sres}_d(f, g)$ has degree at most d, and each of its coefficients is equal to a minor of the Sylvester matrix of f and g. In particular the coefficient of x^d, called the *principal subresultant* of f and g, is given by

$$\mathrm{PSres}_d(f,g) := \det \begin{array}{|cccccc|} \multicolumn{6}{c}{\overbrace{}^{m+n-2d}} \\ \hline f_m & \cdots & & \cdots & f_{d-(n-d-1)} \\ & \ddots & & & \vdots \\ & & f_m & \cdots & f_d \\ \hline g_n & \cdots & & \cdots & g_{d-(m-d-1)} \\ & \ddots & & & \vdots \\ & & g_n & \cdots & g_d \\ \hline \end{array} \begin{array}{l} \\ \\ n-d \\ \\ \\ m-d \end{array}.$$

Subresultants were introduced implicitly by Jacobi [Jac1836] and explicitly by Sylvester [Syl1839, Syl1840]; we refer to [GL2003] for a detailed historical account[1].

Let $\mathsf{M}(n)$ denote the arithmetic complexity of degree-n polynomial multiplication. Precisely, $\mathsf{M}(n)$ is an upper bound for the total number of additions/subtractions and products/divisions in the base field $\mathbb{K}$ that are sufficient to compute the product of any two polynomials in $\mathbb{K}[x]$ of degree at most n. It is classical, see e.g. [GG2013, Ch. 8], that $\mathsf{M}(n) = O(n \log n \log\log n)$ by using FFT-based algorithms. For arbitrary polynomials $f, g \in \mathbb{K}[x]$ of degree n, the fastest known algorithms are able to compute in $O(\mathsf{M}(n) \log n)$ arithmetic operations in $\mathbb{K}$ either one selected polynomial subresultant $\mathrm{Sres}_d(f, g)$ [Rei1997, Lec2018], or all their principal subresultants $\mathrm{PSres}_d(f, g)$ for $0 \leq d < n$ [GG2013, Cor. 11.18]. It is an open question whether this can be improved to $O(\mathsf{M}(n))$, even for the classical resultant (the case $d = 0$).

In this paper we present *linear* complexity results for these two questions for a special family of polynomials, namely $f = (x - \alpha)^m$ and $g = (x - \beta)^n$, with $\alpha, \beta \in \mathbb{K}$. To our knowledge, we are exhibiting the first family of "structured polynomials" for which subresultants (and all principal subresultants) can be computed in optimal arithmetic complexity. We also thoroughly discuss the (characteristic of the) fields for which our complexity results hold.

We now describe the main complexity result of the current article.

Theorem 1. *Let $\mathbb{K}$ be a field and $\alpha, \beta \in \mathbb{K}$. Set $d, m, n \in \mathbb{N}$ with $0 \leq d < \min\{m, n\}$, and write*

$$\mathrm{Sres}_d((x - \alpha)^m, (x - \beta)^n) = \sum_{k=0}^{d} s_k \, x^k.$$

Then, when $\mathrm{char}(\mathbb{K}) = 0$ or $\mathrm{char}(\mathbb{K}) \geq \max\{m, n\}$, all the coefficients s_k

[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". The term "polynomial subresultant" was seemingly coined by Collins [Col1967], and probably inspired to him by Bôcher's textbook [Boc1907, §69] who had used the word "subresultants" to refer to determinants of certain submatrices of the Sylvester matrix. Almost simultaneously, Householder and Stewart [HS1967, Hou1968] employed the term "polynomial bigradients".

for $0 \leq k \leq d$ *can be computed using* $O(\min\{m,n\} + \log(mn))$ *arithmetic operations in* $\mathbb{K}$.

This result is obtained via an amazing (and seemingly previously unobserved) close connection of the subresultants $\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n)$ with the classical family of orthogonal polynomials known as the *Jacobi polynomials*, introduced and studied by Jacobi in his posthumous article [Jac1859]. This allows us to produce a recurrence for the coefficients of the subresultant in the monomial basis that is derived from the differential equation satisfied by the Jacobi polynomial, and hence, by the subresultant.

To express the polynomial subresultants $\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n)$ as Jacobi polynomials, let us recall [Sze1975, Chapter 4] that for any $k, \ell, r \in \mathbb{Z}$ with $r \geq 0$, the Jacobi polynomial $P_r^{(k,\ell)}(x)$ can be defined in $\frac{1}{2}\mathbb{Z}[x]$, and thus also in $\mathbb{K}[x]$ for any abstract field $\mathbb{K}$ with $\mathrm{char}(\mathbb{K}) \neq 2$, in two equivalent ways:

- by Rodrigues' formula

$$P_r^{(k,\ell)}(x) := \frac{(-1)^r}{2^r\, r!}(1-x)^{-k}(1+x)^{-\ell}\frac{\partial^r}{\partial x^r}\left[(1-x)^{k+r}(1+x)^{\ell+r}\right],$$

- as a hypergeometric sum:

$$P_r^{(k,\ell)}(x) := \sum_{j=0}^{r} \frac{(k+r-j+1)_j}{j!}\frac{(\ell+j+1)_{r-j}}{(r-j)!}\left(\frac{x-1}{2}\right)^{r-j}\left(\frac{x+1}{2}\right)^{j},$$

  where for any $a \in \mathbb{Z}$, $(a)_0 := 1$ and $(a)_j := a(a+1)\cdots(a+j-1)$ for $j \geq 1$ denotes the jth Pochhammer symbol, or, rising factorial, of a.

We then have the following result, which asserts that the d-th subresultant of $(x-\alpha)^m$ and $(x-\beta)^n$ coincides, up to an explicit multiplicative constant and up to an affine change of variables, with the Jacobi polynomial $P_d^{(-n,-m)}(x)$.

Theorem 2. *Let* $\mathbb{K}$ *be a field,* $m, n \in \mathbb{N}$ *and assume* $\mathrm{char}(\mathbb{K}) = 0$ *or* $\mathrm{char}(\mathbb{K}) \geq \max\{m,n\}$. *Let* $\alpha, \beta \in \mathbb{K}$ *with* $\alpha \neq \beta$. *Set* $d \in \mathbb{N}$ *with* $0 \leq d < \min\{m,n\}$. *Then*

$$\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n) \tag{2}$$
$$= \prod_{i=1}^{d} \frac{i!(m+n-d-i-1)!}{(m-i)!(n-i)!} \cdot (\alpha-\beta)^{(m-d)(n-d)+d} \cdot P_d^{(-n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right).$$

A comment is in order here: Although the Jacobi polynomials are only defined in characteristic different from 2 and although the rational coefficient

$$\prod_{i=1}^{d} \frac{i!(m+n-d-i-1)!}{(m-i)!(n-i)!}$$

is not in general an integer number, Theorem 2 *does hold* in any characteristic in the following sense: The theorem holds over the field $\mathbb{Q}(u_\alpha, u_\beta)$ to give an expression for $\mathrm{Sres}_d((x-u_\alpha)^m, (x-u_\beta)^n)$, where u_α, u_β are indeterminates. Since $\mathrm{Sres}_d((x-u_\alpha)^m, (x-u_\beta)^n) \in \mathbb{Z}[u_\alpha, u_\beta, x]$ by the definition of subresultants, the right-hand side of equality (2) also has integer coefficients when expanded in the monomial basis. Then we can interpret the theorem for arbitrary fields $\mathbb{K}$ by applying a classical specialization argument, via the ring homomorphism $\mathbb{Z}[u_\alpha, u_\beta] \to \mathbb{K}$ which maps $1 \mapsto 1_\mathbb{K}, u_\alpha \mapsto \alpha, u_\beta \mapsto \beta$.

As mentioned above, we derive from Theorem 2 a second-order recurrence satisfied by the coefficients of $\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n)$ in the usual monomial basis, which is the key ingredient in the proof of our complexity result in Theorem 1.

Corollary 3. *Let $\mathbb{K}$ be a field and $\alpha, \beta \in \mathbb{K}$. Set $d, m, n \in \mathbb{N}$ with $0 \le d < \min\{m, n\}$, and write*

$$\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n) = \sum_{k=0}^{d} s_k\, x^k.$$

Then, when $\mathrm{char}(\mathbb{K}) = 0$ or $\mathrm{char}(\mathbb{K}) \ge m+n-d$, the following second-order linear recurrence is satisfied by the coefficients s_k, for $0 \le k \le d$:

$$\begin{aligned} s_d &= \mathrm{PSres}_d((x-\alpha)^m, (x-\beta)^n), \\ s_{d-1} &= \frac{-d((n-d)\alpha + (m-d)\beta)}{m+n-2d}\, \mathrm{PSres}_d((x-\alpha)^m, (x-\beta)^n), \end{aligned}$$

and for $k = d-2, \ldots, 0$,

$$s_k = \frac{-(k+1)\Big(\big((n-k-1)\alpha + (m-k-1)\beta\big)s_{k+1} + (k+2)\alpha\beta s_{k+2}\Big)}{(d-k)(m+n-d-k-1)}.$$

Concerning the characteristic of the field $\mathbb{K}$, in Section 2.4 below, Corollary 7 shows how the recurrence in Corollary 3 can be refined in such a way that another slightly different second-order recurrence holds if $\mathrm{char}(\mathbb{K}) \geq \max\{m,n\}$. This explains why the assumption $\mathrm{char}(\mathbb{K}) \geq m+n-d$ in Corollary 3 can be relaxed to $\mathrm{char}(\mathbb{K}) \geq \max\{m,n\}$ in Theorem 1.

Our next complexity result concerns the computation of all principal subresultants $\mathrm{PSres}_d(f,g)$ for $0 \leq d < \min\{m,n\}$.

Theorem 4. *Let $\mathbb{K}$ be a field, let $m,n \in \mathbb{N}$ and assume $\mathrm{char}(\mathbb{K}) = 0$ or $\mathrm{char}(\mathbb{K}) \geq m+n$. Let $\alpha,\beta \in \mathbb{K}$. Then one can compute all the principal subresultants $\mathrm{PSres}_d((x-\alpha)^m,(x-\beta)^n) \in \mathbb{K}$ for $0 \leq d < \min\{m,n\}$ using $O(\min\{m,n\}+\log(mn))$ operations in $\mathbb{K}$.*

This is again obtained thanks to a recurrence that is derived from the description of $\mathrm{PSres}_d((x-\alpha)^m,(x-\beta)^n)$ from [BDKSV2017, Proposition 3.3]:

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

where the product in the right-hand side belongs to $\mathbb{Z}$ if $\mathrm{char}(\mathbb{K}) = 0$ and to $\mathbb{Z}/p\mathbb{Z}$ if $\mathrm{char}(\mathbb{K}) = p$. This description implies in particular that if $\alpha \neq \beta$, and $\mathrm{char}(\mathbb{K}) = 0$ or $\mathrm{char}(\mathbb{K}) \geq m+n$, the principal subresultant $\mathrm{PSres}_d((x-\alpha)^m,(x-\beta)^n)$ is non-zero, that is, $\mathrm{Sres}_d((x-\alpha)^m,(x-\beta)^n)$ has degree exactly d for all $0 \leq d < \min\{m,n\}$.

In the current article, we repeatedly use the crucial fact that improved complexity results are obtained using recurrence relations that algebraic objects obey, rather than just computing independently a collection of these objects. This is one of the strength of our results: not only they provide nice formulae for the subresultants, but they also exploit their particular structure for designing efficient algorithms.

This work has an interesting story. While working on paper [BDKSV2017], we first realized that [BDKSV2017, Theorems 1.1 and 1.2] (see Theorem 9 below) implies the linear recurrence on the coefficients of $\mathrm{Sres}_d((x-\alpha)^m,(x-\beta)^n)$ in the usual monomial basis described in Corollary 3. This recurrence was initially found using a computer-driven "guess-and-prove" approach, where the guessing part relied on algorithmic *Hermite-Padé approximation* [SZ94], and where the proving part relied on Zeilberger's *creative*

telescoping algorithm [Zei90, WZ1992]. From this we derived a first proof of our complexity result (Theorem 1). Shortly after that, by studying the differential equation attached to this recurrence, we realized that it has a basis of solutions of hypergeometric polynomials, which appeared to be Jacobi polynomials. We have then obtained an indirect and quite involved proof of Theorem 2 and of Corollary 3 based on manipulations of hypergeometric functions, notably on the Chu-Vandermonde identity, much inspired by an experimental mathematics approach. The proof that we choose to present in this article is the shortest and the simplest that we could find. It is chronologically the latest proof of our results, and the one which provides the deepest structural insight. This proof was obtained by applying some classical results and the fact that any polynomial that can be written as a polynomial combination of f and g in $\mathbb{K}[x]$ with given degree bounds is in fact a constant multiple of the subresultant of f and g: we prove that the Jacobi polynomial can indeed be expressed as such a combination of $(x-\alpha)^m$ and $(x-\beta)^n$, and we determine the scalar multiple that gives the subresultant. In conclusion, we want to stress here the importance of the interaction between computer science and classical mathematics, which allowed us to guess and prove all our statements using the computer, before finding a short and elegant human proof.

The paper is organized as follows: We first derive Theorem 2 in Section 2. Section 3 is dedicated to the proof of Theorem 1, while in Section 4 we prove Theorem 4. Section 5 explains the connection of our results with previous work, notably the relationship with classical results on Padé approximation. We conclude the paper with various remarks and perspectives in Section 6.

Acknowledgements. We thank Christian Krattenthaler for precious help with hypergeometric identities during an early stage of this work. T. Krick and M. Valdettaro were partially supported by ANPCyT PICT-2013-0294, CONICET PIP-11220130100073CO and UBACyT 2014-2017-20020130100143BA. A. Szanto was partially supported by the NSF grants CCF-1813340 and CCF-1217557.

2. Proof of Theorem 2 and beyond

As explained in the introduction, the proof of Theorem 1 crucially relies on the description of the subresultant as a Jacobi polynomial, as stated in Theorem 2, so we first give the proof of Theorem 2. In the second half

of Section 2, we give similar expressions for the coefficients in the *Bézout identity* (14), and also prove Corollary 3.

2.1. Proof of Theorem 2.

We will need the next classical lemma, which follows e.g. from [Mis1993, Lemmas 7.7.4 and 7.7.6], and which is also a key ingredient in [BDKSV2017].

Lemma 5. *Let $m, n \in \mathbb{N}$ and f, $g \in \mathbb{K}[x]$ of degrees m and n respectively. Set $0 \leq d < \min\{m, n\}$ and assume $\mathrm{PSres}_d(f, g) \neq 0$. If $\mathcal{F}, \mathcal{G} \in \mathbb{K}[x]$ with $\deg(\mathcal{F}) < n - d$, $\deg(\mathcal{G}) < m - d$ are such that $h = \mathcal{F}\, f + \mathcal{G}\, g$ is a non-zero polynomial in $\mathbb{K}[x]$ of degree at most d, then there exists $\lambda \in \mathbb{K} \setminus \{0\}$ satisfying*

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

□

For the convenience of the reader, we recall that Theorem 2 claims that

$$\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n) = (\alpha-\beta)^{(m-d)(n-d)+d} C(m,n,d) P_d^{(-n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right),$$

where

$$C(m,n,d) := \prod_{i=1}^{d} \frac{i!(m+n-d-i-1)!}{(m-i)!(n-i)!}. \tag{4}$$

We first assume that $\mathbb{K}$ has characteristic 0. One can check (or refer to [Sze1975, Theorem 4.23.1] to verify) that the polynomials

$$P_d^{(-n,-m)}(z),\ (1+z)^m P_{n-d-1}^{(-n,m)}(z) \text{ and } (1-z)^n P_{m-d-1}^{(n,-m)}(z)$$

all solve the linear differential equation

$$(1-z^2)y''(z) + \big((m+n-2)z - m + n\big)y'(z) + d(d+1-m-n)y(z) = 0.$$

Substituting $z = \dfrac{2x-\alpha-\beta}{\beta-\alpha}$ in this differential equation shows that the polynomials

$$\begin{aligned}
y_1(x) &:= P_d^{(-n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right),\\
y_2(x) &:= \left(\frac{2}{\beta-\alpha}\right)^m (x-\alpha)^m P_{n-d-1}^{(-n,m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right) \quad \text{and}\\
y_3(x) &:= \left(\frac{2}{\alpha-\beta}\right)^n (x-\beta)^n P_{m-d-1}^{(n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right)
\end{aligned}$$

all solve the linear differential equation

$$(x-\alpha)(x-\beta)y''(x)+\big(\alpha(n-1)+\beta(m-1)-(m+n-2)x\big)y'(x) \\ +d(m+n-d-1)y(x)=0. \tag{5}$$

Since the dimension of the solution space of this second-order linear differential equation is 2, the three polynomials y_1, y_2, y_3 must be linearly dependent over $\mathbb{K}$. Now, it is well-known that the Jacobi polynomials satisfy

$$P_r^{(k,\ell)}(1)=\frac{(k+1)_r}{r!} \quad \text{and} \quad P_r^{(k,\ell)}(-1)=(-1)^r\frac{(\ell+1)_r}{r!}. \tag{6}$$

This implies that y_2 and y_3 are not linearly dependent over $\mathbb{K}$ since

$$y_2(\beta)=2^m P_{n-d-1}^{(-n,m)}(1)=(-1)^{n-d-1}2^m\binom{n-1}{d}\neq 0 \ \text{ and } \ y_2(\alpha)=0 \tag{7}$$

while

$$y_3(\beta)=0 \ \text{ and } \ y_3(\alpha)=2^n P_{m-d-1}^{(n,-m)}(-1)=2^n\binom{m-1}{d}\neq 0. \tag{8}$$

Thus, there exist $A, B\in\mathbb{K}$ such that $y_1(x)=A\,y_2(x)+B\,y_3(x)$, that is,

$$P_d^{(-n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right)=A\left(\frac{2}{\beta-\alpha}\right)^m P_{n-d-1}^{(-n,m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right)(x-\alpha)^m \\ +B\left(\frac{2}{\alpha-\beta}\right)^n P_{m-d-1}^{(n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right)(x-\beta)^n. \tag{9}$$

In addition $P_d^{(-n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right)\neq 0$, since

$$P_d^{(-n,-m)}(1)=(-1)^d\binom{n-1}{d} \quad \text{and} \quad P_d^{(-n,-m)}(-1)=\binom{m-1}{d}. \tag{10}$$

Moreover, $\deg P_d^{(-n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right)\leq d$, $\deg P_{n-d-1}^{(-n,m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right)<n-d$ and $\deg P_{m-d-1}^{(n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right)<m-d$. Therefore, since $\mathrm{PSres}_d(f,g)\neq 0$ by (3), Lemma 5 implies that there exists $\mu:=1/\lambda\in\mathbb{K}$ such that

$$\mathrm{Sres}_d((x-\alpha)^m,(x-\beta)^n)=\mu\,P_d^{(-n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right). \tag{11}$$

We compute μ by comparing the leading coefficients of both sides of (11). The leading coefficient of $P_d^{(-n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right)$ equals by definition

$$\begin{aligned}\frac{1}{(\beta-\alpha)^d}\sum_{j=0}^{d}\frac{(-n+d-j+1)_j}{j!}\frac{(-m+j+1)_{d-j}}{(d-j)!}\\ =\frac{(-1)^d}{(\beta-\alpha)^d}\sum_{j=0}^{d}\binom{n-d+j-1}{j}\binom{m-j-1}{d-j}\\ =\frac{1}{(\alpha-\beta)^d}\binom{m+n-d-1}{d}.\end{aligned}$$

The last equality can be easily checked by thinking of a d-combination with repetition from a set of size $m+n-2d$, written as a disjoint union of a subset with $n-d$ elements and its complement with $m-d$ elements, computed by adding, for $0\leq j\leq d$, the j-combination with repetition from the first subset of size $n-d$ combined with the $(d-j)$-combination with repetition from the second subset of size $m-d$.
Therefore

$$\mu=\frac{(\alpha-\beta)^d}{\binom{m+n-d-1}{d}}\mathrm{PSres}_d((x-\alpha)^m,(x-\beta)^n)$$

where we know by (3) that

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

This implies

$$\begin{aligned}\mu&=(\alpha-\beta)^{(m-d)(n-d)+d}\frac{\prod_{i=1}^{d}\frac{(i-1)!\,(m+n-d-i)!}{(m-i)!(n-i)!}}{\binom{m+n-d-1}{d}}\\ &=(\alpha-\beta)^{(m-d)(n-d)+d}\prod_{i=1}^{d}\frac{i!(m+n-d-i-1)!}{(m-i)!(n-i)!}\\ &=(\alpha-\beta)^{(m-d)(n-d)+d}\,C(m,n,d),\end{aligned}\tag{12}$$

for $C(m,n,d)$ defined in (4), and proves Theorem 2 when $\mathrm{char}(\mathbb{K})=0$.

Since the denominator of $C(m,n,d)$ is a product of integers smaller than m and n, and since by the second definition of the Jacobi polynomials,

$$P_d^{(-n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right)=\sum_{j=0}^{d}\binom{n-d+j-1}{j}\binom{m-j-1}{d-j}\frac{(x-\alpha)^j(x-\beta)^{d-j}}{(\alpha-\beta)^d}, \tag{13}$$

is well defined in any characteristic, the claim is also true when $\mathrm{char}(\mathbb{K})\geq\max\{m,n\}$.

2.2. Beyond Theorem 2

An advantage of our proof of Theorem 2 is that it also shows that the unique polynomials F_d and G_d in $\mathbb{K}[x]$ of degrees respectively less than $n-d$ and $m-d$ that are the coefficients of the *Bézout identity*

$$\mathrm{Sres}_d((x-\alpha)^m,(x-\beta)^n)=F_d\cdot(x-\alpha)^m+G_d\cdot(x-\beta)^n \tag{14}$$

are also (scalar multiples of) Jacobi polynomials, up to the same affine change of variables. More precisely, we have:

Corollary 6. *Let $\mathbb{K}$ be a field, $\alpha,\beta\in\mathbb{K}$ with $\alpha\neq\beta$ and assume that $\mathrm{char}(\mathbb{K})=0$ or $\mathrm{char}(\mathbb{K})\geq\max\{m,n\}$. Let $d,m,n\in\mathbb{N}$ with $0\leq d<\min\{m,n\}$. Then, the polynomials F_d and G_d defined in (14) satisfy*

$$\begin{aligned}
F_d&=\frac{(-1)^{n-1}\mu}{(\beta-\alpha)^m}P_{n-d-1}^{(-n,m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right)\\
&=(-1)^{m-d}(\alpha-\beta)^{(m-d)(n-d)-(m+n-2d-1)}\,C(m,n,d)\cdot\\
&\quad\cdot\sum_{j=0}^{n-d-1}(-1)^j\binom{d+j}{d}\binom{m+n-d-1}{m+j}(x-\alpha)^j(x-\beta)^{n-d-1-j},\\
G_d&=\frac{(-1)^{n}\mu}{(\beta-\alpha)^n}P_{m-d-1}^{(n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right)\\
&=(\alpha-\beta)^{(m-d)(n-d)-(m+n-2d-1)}\,C(m,n,d)\cdot\\
&\quad\cdot\sum_{j=0}^{m-d-1}(-1)^j\binom{m+n-d-1}{j}\binom{m-j-1}{d}(x-\alpha)^j(x-\beta)^{m-d-1-j},
\end{aligned}$$

where μ is defined in (12) and $C(m,n,d)$ in (4).

Proof. We first assume that $\mathbb{K}$ is a field of characteristic 0.
By Identities (14), (11) and (9), one has

$$F_d = \mu\, A \left(\frac{2}{\beta-\alpha}\right)^m P_{n-d-1}^{(-n,m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right) \text{ and}$$
$$G_d = \mu\, B \left(\frac{2}{\alpha-\beta}\right)^n P_{m-d-1}^{(n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right).$$

We now determine the values of A and B. By Identities (10), (6), (8) and (7), we get

$$\begin{aligned}\binom{m-1}{d} = P_d^{(-n,-m)}(-1) &= B\left(\frac{2}{\alpha-\beta}\right)^n P_{m-d-1}^{(n,-m)}(-1)(\alpha-\beta)^n \\ &= 2^n\binom{m-1}{d}B,\\ (-1)^d\binom{n-1}{d} = P_d^{(-n,-m)}(1) &= A\left(\frac{2}{\beta-\alpha}\right)^m P_{n-d-1}^{(-n,m)}(1)(\beta-\alpha)^m \\ &= (-1)^{n-d-1}2^m\binom{n-1}{d}A.\end{aligned}$$

Therefore $A = \dfrac{(-1)^{n-1}}{2^m}$ and $B = \dfrac{1}{2^n}$. The statement follows when $\mathrm{char}(\mathbb{K}) = 0$. Since the denominator of $C(m,n,d)$ is a product of integers smaller than m and n, the claim is also true if $\mathrm{char}(\mathbb{K}) \geq \max\{m,n\}$. □

2.3. Proof of Corollary 3

We now prove Corollary 3, which gives a recurrence satisfied by the coefficients (in the monomial basis) of $\mathrm{Sres}_d((x-\alpha)^m,(x-\beta)^n)$. The recurrence is inherited from the differential equation (5) satisfied by this subresultant. Clearly, $s_d = \mathrm{PSres}_d((x-\alpha)^m,(x-\beta)^n)$. Note that by Identity (11), the differential equation (5) satisfied by the Jacobi polynomial is also satisfied by $s(x) := \mathrm{Sres}_d((x-\alpha)^m,(x-\beta)^n)$. We now show that this fact implies the expression for s_{d-1}, and the recurrence. We start with

$$s(x) = \sum_{k=0}^{d} s_k x^k, \quad s'(x) = \sum_{k=1}^{d} k s_k x^{k-1} \text{ and } s''(x) = \sum_{k=2}^{d} k(k-1)s_k x^{k-2}.$$

We then have

$$\begin{aligned}(x-\alpha)(x-\beta)s''(x) &= \sum_{k=2}^{d} k(k-1)s_k x^k - (\alpha+\beta)\sum_{k=2}^{d} k(k-1)s_k x^{k-1} \\ &\quad + \alpha\beta \sum_{k=2}^{d} k(k-1)s_k x^{k-2} \\ &= \sum_{k=0}^{d} k(k-1)s_k x^k - (\alpha+\beta)\sum_{k=0}^{d-1}(k+1)ks_{k+1}x^k \\ &\quad + \alpha\beta\sum_{k=0}^{d-2}(k+2)(k+1)s_{k+2}x^k,\end{aligned}$$

$$\begin{aligned}\big(\alpha(n-1)+\beta(m-1)-(m+n-2)x\big)\,s'(x) &= -(m+n-2)\sum_{k=1}^{d} ks_k x^k \\ &\quad + (\alpha(n-1)+\beta(m-1))\sum_{k=1}^{d} ks_k x^{k-1} \\ &= -(m+n-2)\sum_{k=0}^{d} ks_k x^k + (\alpha(n-1)+\beta(m-1))\sum_{k=0}^{d-1}(k+1)s_{k+1}x^k,\end{aligned}$$

and

$$d(m+n-d-1)s(x) = d(m+n-d-1)\sum_{k=0}^{d} s_k x^k.$$

Then, comparing the coefficients of degree $d-1$ in (5), we get

$$\begin{aligned}&(d-1)(d-2)s_{d-1} - (\alpha+\beta)d(d-1)s_d - (m+n-2)(d-1)s_{d-1} \\ &\quad + \big(\alpha(n-1)+\beta(m-1)\big)ds_d + d(m+n-d-1)s_{d-1} = 0.\end{aligned}$$

This implies

$$s_{d-1} = \frac{-d((n-d)\alpha+(m-d)\beta)}{m+n-2d}\,s_d.$$

We then compare the degree-k coefficient in (5) for $k = 0,\dots,d-2$:

$$\begin{aligned}&\big(k(k-1)-(m+n-2)k+d(m+n-d-1)\big)s_k + \big(-(\alpha+\beta)(k+1)k \\ &\quad + (\alpha(n-1)+\beta(m-1))(k+1)\big)s_{k+1} + \alpha\beta(k+2)(k+1)s_{k+2} = 0.\end{aligned}$$

Therefore,

$$s_k = \frac{-(k+1)\Big(\big((n-k-1)\alpha + (m-k-1)\beta\big)s_{k+1} + (k+2)\alpha\beta s_{k+2}\Big)}{(d-k)(m+n-d-k-1)}.$$

We observe that these recurrence expressions hold for fields $\mathbb{K}$ of characteristic 0 or $\geq m+n-d$ since we are dividing only by natural numbers less than $m+n-d$. □

2.4. Refining Corollary 3

We now refine the expressions in Corollary 3 in order to avoid dividing by numbers as big as $m+n-d-1$. To do so, we exhibit a slightly different recurrence that holds for fields $\mathbb{K}$ of finite characteristic $\geq \max\{m,n\}$.

Corollary 7. *Let $m,n,d \in \mathbb{N}$ with $d < \min\{m,n\}$ and let $\mathbb{K}$ be a field with $\operatorname{char}(\mathbb{K}) = 0$ or $\operatorname{char}(\mathbb{K}) \geq \max\{m,n\}$. Let $\alpha,\beta \in \mathbb{K}$ with $\alpha \neq \beta$, and write*

$$\operatorname{Sres}_d((x-\alpha)^m,(x-\beta)^n) = \sum_{k=0}^{d} s_k x^k.$$

Define recursively

$$t_d := (\alpha-\beta)^{(m-d)(n-d)} \prod_{i=1}^{d} \frac{(i-1)!\,(m+n-d-i-1)!}{(m-i)!(n-i)!},$$
$$t_{d-1} = -d\big((n-d)\alpha + (m-d)\beta\big)\, t_d,$$

and for $k = d-2,\ldots,0$,

$$t_k = -(k+1)\Big(\frac{(n-k-1)\alpha + (m-k-1)\beta}{d-k} t_{k+1} + \frac{(k+2)(m+n-d-k-2)\alpha\beta}{d-k} t_{k+2}\Big).$$

Then for $k = d,\ldots,0$ one has

$$s_k = \left(\prod_{i=d+1}^{d+k} (m+n-i)\right) t_k.$$

Proof. It suffices to show that the terms we just recursively defined also satisfy the recurrence proposed in Corollary 3 in a field of characteristic 0, and then use the specialization $\mathbb{Z} \to \mathbb{K}, 1 \mapsto 1_{\mathbb{K}}$, noting that the only divisions that occur are by natural numbers less than $\max\{m, n\}$.
Clearly $s_d = \big(\prod_{i=d+1}^{2d}(m+n-i)\big)t_d = \mathrm{PSres}_d((x-\alpha)^m, (x-\beta)^n)$ by (3), since

$$\prod_{i=d+1}^{2d}(m+n-i) = \prod_{i=1}^{d}(m+n-d-i).$$

Now,

$$\begin{aligned}
s_{d-1} &= \left(\prod_{i=d+1}^{2d-1}(m+n-i)\right)t_{d-1} \\
&= \left(\prod_{i=d+1}^{2d-1}(m+n-i)\right)\big(-d((n-d)\alpha+(m-d)\beta)t_d\big) \\
&= \frac{-d((n-d)\alpha+(m-d)\beta)}{m+n-2d}\left(\prod_{i=d+1}^{2d}(m+n-i)\right)t_d \\
&= \frac{-d((n-d)\alpha+(m-d)\beta)}{m+n-2d}s_d
\end{aligned}$$

also agrees with the expression in Corollary 3.
Finally, for $k = d-2, \ldots, 0$, we get that

$$\begin{aligned}
s_k &= \left(\prod_{i=d+1}^{d+k}(m+n-i)\right)t_k \\
&= -(k+1)\left(\prod_{i=d+1}^{d+k}(m+n-i)\right)\left(\frac{(n-k-1)\alpha+(m-k-1)\beta}{d-k}t_{k+1}\right. \\
&\qquad \left.+\frac{(k+2)(m+n-d-k-2)\alpha\beta}{d-k}t_{k+2}\right),
\end{aligned}$$

which implies

$$s_k = -(k+1)\left(\frac{(n-k-1)\alpha+(m-k-1)\beta}{(d-k)(m+n-d-k-1)}\left(\prod_{i=d+1}^{d+k+1}(m+n-i)\right)t_{k+1}\right.$$
$$\left.+\frac{(k+2)\alpha\beta}{(d-k)(m+n-d-k-1)}\left(\prod_{i=d+1}^{d+k+2}(m+n-i)\right)t_{k+2}\right)$$
$$=\frac{-(k+1)\Big(\big((n-k-1)\alpha+(m-k-1)\beta\big)s_{k+1}+(k+2)\alpha\beta s_{k+2}\Big)}{(d-k)(m+n-d-k-1)}.$$

This agrees with the desired expression. □

3. Proof of Theorem 1.

We start with the following simple observation.

Observation 8. *For any integers $k,\ell\geq 0$, the binomial coefficient $\binom{k+\ell}{k}$ can be computed in $O(\min\{k,\ell\})$ operations in $\mathbb{K}$.*

Proof. It is enough to use the most economic of the writings $(k+\ell)\cdots(k+1)/\ell!$ and $(k+\ell)\cdots(\ell+1)/k!$. □

The second-order recurrence of Corollary 3 immediately implies that one can compute all coefficients of the d-th subresultant using $O(\min\{m,n\}+\log(mn))$ operations in $\mathbb{K}$ as follows:
First, $s_d=\mathrm{PSres}_d((x-\alpha)^m,(x-\beta)^n)$ can be computed thanks to (3) using $O(\min\{m,n\}+\log(mn))$ arithmetic operations in $\mathbb{K}$: We set

$$r(i):=\frac{(i-1)!(m+n-d-i)!}{(m-i)!(n-i)!},\quad 1\leq i\leq d$$

so that $\mathrm{PSres}_d((x-\alpha)^m,(x-\beta)^n)=(\alpha-\beta)^{(m-d)(n-d)}\prod_{i=1}^d r(i)$.
First $r(d)=(d-1)!\binom{m+n-2d}{m-d}$ can be computed in $O(\min\{m,n\})$ arithmetic operations by applying Lemma 8. Then we deduce $r(d-1),\ldots,r(1)$ thanks to the recurrence

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

and the product $r(1)\cdots r(d)$, adding $O(d)$ operations. The term $(\alpha-\beta)^{(m-d)(n-d)}$ can be computed by binary powering with $O(\log((m-d)(n-d)) \leq \log(O(mn))$ operations. This computes s_d using $O(\min\{m,n\}+\log(mn))$ arithmetic operations in $\mathbb{K}$.
Then one computes s_{d-1} adding $O(1)$ operations, and from these one keeps computing s_{d-2} to s_0 adding $O(1)$ operations in $\mathbb{K}$ for each of these $d-1$ terms. This shows that all s_k can be computed using $O(\min\{m,n\}+\log(mn))$ operations in $\mathbb{K}$. The same holds for the terms t_k in Corollary 7.
Remark that during the whole procedure only divisions by integers at most $\max\{m,n\}-1$ occur. □

4. Proof of Theorem 4

By (3),

$$\mathrm{PSres}_d((x-\alpha)^m,(x-\beta)^n) = c(d)(\alpha-\beta)^{(m-d)(n-d)}, \tag{15}$$

where

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

is an integer number, as already mentioned in the introduction. When $\alpha=\beta$ all the principal subresultants vanish, so we can assume w.l.o.g. that $\alpha\neq\beta$. We set

$$u(0) := c(0) = 1$$

and for $1 \leq d < \min\{m,n\}$,

$$u(d) := \frac{c(d)}{c(d-1)}.$$

We observe that $u(k+1)$ for all $k>0$ can be computed thanks to the equality

$$u(k+1) = v(1)\cdot v(2)\cdots v(k), \tag{16}$$

where

$$v(1) = u(1) = c(1) = \binom{m+n-2}{m-1} \tag{17}$$

and, by (15), for $1 \leq k < \min\{m,n\}-1$,

$$v(k) = \frac{u(k+1)}{u(k)} = \frac{c(k+1)c(k-1)}{c(k)^2}$$
$$= \frac{k(m-k)(n-k)(m+n-k)}{(m+n-2k-1)(m+n-2k)^2(m+n-2k+1)}. \quad (18)$$

We note that the only numbers that appear in the denominators of $u(1)$ and of the previous fractions are products of integers of absolute value less than $m+n$, which are invertible in $\mathbb{K}$ by the assumption that $\mathrm{char}(\mathbb{K}) \geq m+n$.

Based on these considerations, we now design an algorithm that computes all principal subresultants $\mathrm{PSres}_d((x-\alpha)^m, (x-\beta)^n)$ with $1 \leq d < \min\{m,n\}$ in $O(\min\{m,n\}+\log(mn))$ arithmetic operations in $\mathbb{K}$, thus proving Theorem 4.
First, $v(1)$ is computed by (17), using $O(\min\{m,n\})$ arithmetic operations in $\mathbb{K}$ using Observation 8.
Then, $v(2)$ to $v(\min\{m,n\}-1)$ are computed using (18) from the previous one using $O(1)$ arithmetic operations each.
Next, Identity (16) allows us to compute all $u(d)$ for $2 \leq d < \min\{m,n\}$ in $O(\min\{m,n\})$ operations in $\mathbb{K}$. Then, the elements $c(d) = u(0)\cdot u(1)\cdots u(d)$, with $0 \leq d < \min\{m,n\}$, are computed in $O(\min\{m,n\})$ operations in $\mathbb{K}$.
It remains to compute all the powers $p(d) := (\alpha-\beta)^{(m-d)(n-d)}$, and finally to output $\mathrm{PSres}_d((x-\alpha)^m, (x-\beta)^n) = c(d)\cdot p(d)$, for $0 \leq d < \min\{m,n\}$:
We first compute the elements $\gamma(d) := (\alpha-\beta)^{2d+1-m-n}$ for $d < \min\{m,n\}$, using $O(\log(m+n) + \min\{m,n\})$ operations in $\mathbb{K}$. This can be done by computing $\gamma(0) = (\alpha-\beta)^{1-m-n}$ by binary powering, then unrolling the recurrence $\gamma(d+1) = (\alpha-\beta)^2 \cdot \gamma(d)$ for $d < \min\{m,n\}-1$.
Next we compute $p(0) = (\alpha-\beta)^{mn}$ by binary powering, and then all $p(d)$, for $1 \leq d < \min\{m,n\}$, by repeated products using $p(d+1) = \gamma(d)\cdot p(d)$, for a total cost of $O(\log(mn) + \min\{m,n\})$ operations in $\mathbb{K}$.
We conclude the proof by Identity (15) without changing the order of the arithmetic operations we used. □

5. Connections to previous results

Theorem 2 is closely connected to some previous results. First we discuss the connection to the work [BDKSV2017] (some of the co-authors are the authors of the current paper). Second, we explain the relationship of the present work to classical results on *Padé approximation*.

5.1. Connection with [BDKSV2017]

We show that the expression for the subresultant obtained in [BDKSV2017], though not expressed in terms of Jacobi polynomials, is equivalent to the one in Theorem 2. First, let us recall the main results of [BDKSV2017].

Theorem 9. *[BDKSV2017, Theorems 1.1 and 1.2]*
Let $\mathbb{K}$ be a field and $\alpha, \beta \in \mathbb{K}$. Set $d, m, n \in \mathbb{N}$ with $0 \leq d < \min\{m, n\}$. Then,

$$\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n) = (\alpha-\beta)^{(m-d)(n-d)} \sum_{j=0}^{d} c_j(m,n,d)(x-\alpha)^j(x-\beta)^{d-j},$$

where the coefficients $c_0(m,n,d), \ldots, c_d(m,n,d)$ are defined by

$$c_0(m,n,d) = \prod_{i=1}^{d} \frac{(i-1)!\,(m+n-d-i-1)!}{(m-i-1)!(n-i)!},$$

and

$$c_j(m,n,d) = \frac{\binom{d}{j}\binom{n-d+j-1}{j}}{\binom{m-1}{j}}\, c_0(m,n,d), \quad \text{for} \quad 1 \leq j \leq d.$$

(Here $c_0(m,n,0) = 1$, following the convention that an empty product equals 1.) Moreover, for $0 \leq j \leq d$, $c_j(m,n,d) \in \mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z}$ if $\mathrm{char}(\mathbb{K}) = 0$ or $\mathrm{char}(\mathbb{K}) = p$, respectively.

Theorem 9 describes the coefficients of $\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n)$ with respect to the set of Bernstein polynomials $\{(x-\alpha)^j(x-\beta)^{d-j},\ 0 \leq j \leq d\}$, which we remark here is a basis for the $\mathbb{K}$-vector space of polynomials in $\mathbb{K}[x]$ of degree bounded by d in the non-trivial case when $\alpha \neq \beta$ (note that all subresultants vanish in the trivial case when $\alpha = \beta$).

Proof that Theorems 9 and 2 are equivalent. Set $c := m + n - d - 1$. We want to prove that

$$\begin{aligned}
&\sum_{j=0}^{d} c_j(m,n,d)(x-\alpha)^j(x-\beta)^{d-j} \\
&\qquad = \ (\alpha-\beta)^d \prod_{i=1}^{d} \frac{i!(c-i)!}{(m-i)!(n-i)!}\, P_d^{(-n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right),
\end{aligned}$$

where

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

By (13),

$$(\alpha-\beta)^d P_d^{(-n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right) = \sum_{j=0}^{d} \binom{n-d+j-1}{j}\binom{m-j-1}{d-j}(x-\alpha)^j(x-\beta)^{d-j}.$$

Thus, we only need to verify that

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

i.e. after simplification, that

$$\frac{(m-1)!}{(m-d-1)!}\prod_{i=1}^{d}\frac{i!}{(m-i)!} = d!\prod_{i=1}^{d}\frac{(i-1)!}{(m-i-1)!},$$

which trivially holds.

It remains to show that the coefficients $c_j(m,n,d)$ belong to $\mathbb{Z}$ for $0 \le j \le d$ when $\mathrm{char}(\mathbb{K}) = 0$ (and therefore belong to the prime ring $\mathbb{Z}/p\mathbb{Z}$ when $\mathrm{char}(\mathbb{K}) = p$). In [BDKSV2017] it is shown that they are integer numbers by showing they coincide (up to a sign) with the determinants of some combinatorial matrices. We give here an independent proof of this fact: For $\alpha = 0$ and $\beta = -1$, one has on the one hand

$$\mathrm{Sres}_d(x^m,(x+1)^n) = \sum_{j=0}^{d} c_j(m,n,d)x^j(x+1)^{d-j}$$

with $c_j(m,n,d) \in \mathbb{Q}$ because of their expression, while on another hand $\mathrm{Sres}_d(x^m,(x+1)^n) \in \mathbb{Z}[x]$ by the determinantal definition (1) of the subresultant. This means that

$$\sum_{j=0}^{d} c_j(m,n,d)x^j(x+1)^{d-j} = \sum_{k=0}^{d} a_k x^k$$

with $a_k \in \mathbb{Z}$ for $0 \le k \le d$. Comparing coefficients, we observe that

$$a_k = \sum_{j=0}^{k} \binom{d}{k-j} c_j(m,n,d), \quad 0 \le k \le d,$$

i.e., that

$$\begin{pmatrix} a_0 \\ \vdots \\ a_d \end{pmatrix} = \begin{pmatrix} 1 & & & \\ \binom{d}{1} & 1 & & \\ \vdots & \vdots & \ddots & \\ \binom{d}{d} & \binom{d}{d-1} & \dots & 1 \end{pmatrix} \begin{pmatrix} c_0(m,n,d) \\ \vdots \\ c_d(m,n,d) \end{pmatrix}.$$

We conclude that $c_j(m,n,d) \in \mathbb{Z}$ for $0 \le j \le d$ since the a_k's are integer numbers and the transition matrix is an invertible integer matrix. □

5.2. Connection with Padé approximation

In this subsection we show that Theorem 2 and Corollary 6 are also equivalent to classical descriptions of some Padé approximants via Gauss hypergeometric functions.

The starting point is a theorem due to Padé [Pad1901], stating that the $[m/n]$ Padé approximation in $\mathbb{C}(x)$ to $(1-x)^k$ is the ratio of hypergeometric functions

$$\frac{{}_2F_1(-m,-k-n;-m-n;x)}{{}_2F_1(-n,k-m;-m-n;x)}. \tag{19}$$

That result had been previously obtained, by different methods and under several additional assumptions, by Laguerre [Lag1885] and Jacobi [Jac1859]. See also [Per1913, Eq. (Padé 5), p. 252], [Bak1975, p. 65], [Ise1979] and Theorem 4.1 in [GGZ2012].

There is also a well-known connection between subresultants and Padé approximants (c.f. [GG2013, Corollary 5.21]): the $[m/n]$ Padé approximation in $\mathbb{C}(x)$ to $(1-x)^k$, for integer $k \ge m$, equals

$$\frac{\mathrm{Sres}_m(x^{m+n+1},(1-x)^k)}{G_m(x^{m+n+1},(1-x)^k)} = (-1)^k \frac{\mathrm{Sres}_m(x^{m+n+1},(x-1)^k)}{G_m(x^{m+n+1},(x-1)^k)}, \tag{20}$$

where $G_m := G_m(x^{m+n+1},(x-1)^k)$ is the polynomial coefficient of degree $\le n$ in the Bézout expression

$$\mathrm{Sres}_m(x^{m+n+1},(x-1)^k) = F_m \cdot x^{m+n+1} + G_m \cdot (x-1)^k.$$

Identity (19) implies that

$$\frac{{}_2F_1(-m,-n-k;-m-n;x)}{{}_2F_1(-n,k-m;-m-n;x)} = (-1)^k \frac{\mathrm{Sres}_m(x^{m+n+1},(x-1)^k)}{G_m(x^{m+n+1},(x-1)^k)}.$$

We showed earlier that the fact that x^{m+n+1} and $(x-1)^k$ are coprime polynomals implies that $\deg(\mathrm{Sres}_m(x^{m+n+1},(x-1)^k)) = m$, and it is also immediate to verify that $\mathrm{Sres}_m(x^{m+n+1},(x-1)^k)$ and $G_m(x^{m+n+1},(x-1)^k)$ are coprime. Therefore, since the degree of

$${}_2F_1(-m,-k-n;-m-n;x) = \sum_{i=0}^{m}(-1)^i \binom{m}{i} \frac{(-k-n)_i}{(-m-n)_i} x^i$$

equals m, one derives that there exists a non-zero $\lambda \in \mathbb{C}$ such that

$$\begin{aligned}
\mathrm{Sres}_m(x^{m+n+1},(x-1)^k) &= \lambda \cdot {}_2F_1(-m,-k-n;-m-n;x),\\
G_m(x^{m+n+1},(x-1)^k) &= (-1)^k\lambda \cdot {}_2F_1(-n,k-m;-m-n;x).
\end{aligned}$$

Here, λ can be computed by comparing the leading coefficients of $\mathrm{Sres}_m(x^{m+n+1},(x-1)^k)$ and ${}_2F_1(-m,-k-n;-m-n;x)$:

$$\begin{aligned}
\lambda &= (-1)^m \frac{(k+n-m)!(m+n)!}{(k+n)!n!}\,\mathrm{PSres}_m(x^{m+n+1},(x-1)^k)\\
&= (-1)^{(n+1)(k-m)+m} \prod_{i=1}^{m} \frac{(i-1)!(k+n-i)!}{(k-i)!(m+n-i)!},
\end{aligned}$$

by Identity (3).

Now, according to [EMOT1953, (1.6)], see also [Koo1984, (1.5)]:

$$\begin{aligned}
{}_2F_1(-m,-k-n;-m-n;x) &= \frac{1}{\binom{m+n}{m}} P_m^{(-k,-m-n-1)}(2x-1),\\
{}_2F_1(-n,k-m;-m-n;x) &= \frac{1}{\binom{m+n}{m}} P_n^{(k,-m-n-1)}(2x-1),
\end{aligned}$$

while, according to our Theorem 2 and Corollary 6,

$$\begin{aligned}
\mathrm{Sres}_m(x^{m+n+1},(x-1)^k) &= \mu\, P_m^{(-k,-m-n-1)}(2x-1),\\
G_m(x^{m+n+1},(x-1)^k) &= (-1)^k\overline{\mu}\, P_n^{(k,-m-n-1)}(2x-1),
\end{aligned}$$

for

$$\overline{\mu} := (-1)^{(n+1)(k-m)+m} \prod_{i=1}^{m} \frac{i!(k+n-i)!}{(k-i)!(m+n+1-i)!}.$$

This shows the equivalence of the results for $\alpha = 0, \beta = 1$, since $\lambda = \binom{m+n}{m}\overline{\mu}$.

In order to deduce Theorem 2 and Corollary 6 for any α, β we apply the usual changes of variables formulas that can be found in the now classical book [ApJo2006]:

$$\begin{aligned}
&\mathrm{Sres}_d(f(x-\alpha), g(x-\alpha)) = \mathrm{Sres}_d(f,g)(x-\alpha),\\
&\mathrm{Sres}_d(f(\gamma x), g(\gamma x)) = \gamma^{mn-d(d+1)}\mathrm{Sres}_d(f,g)(\gamma x).
\end{aligned}$$

Therefore,

$$\begin{aligned}
\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n) &= \mathrm{Sres}_d(x^m, (x-(\beta-\alpha))^n)(x-\alpha),\\
\mathrm{Sres}_d(x^m, (x-\gamma)^n)(\gamma x) &= \frac{1}{\gamma^{mn-d(d+1)}}\,\mathrm{Sres}_d((\gamma x)^m, (\gamma x-\gamma)^n)\\
&= \frac{1}{\gamma^{mn-d(d+1)}}\,\mathrm{Sres}_d(\gamma^m x^m, \gamma^n (x-1)^n)\\
&= \frac{\gamma^{m(n-d)+n(m-d)}}{\gamma^{mn-d(d+1)}}\,\mathrm{Sres}_d(x^m, (x-1)^n)\\
&= \gamma^{(m-d)(n-d)+d}\,\mathrm{Sres}_d(x^m, (x-1)^n).
\end{aligned}$$

Hence, since we have just proven that $\mathrm{Sres}_d(x^m, (x-1)^n) = \tilde{\mu}\, P_d^{-n,-m}(2x-1)$ for $\tilde{\mu} = \prod_{i=1}^{d} \frac{i!(m+n-d-i-1)!}{(m-i)!(n-i)!}$, we deduce that

$$\mathrm{Sres}_d(x^m, (x-(\beta-\alpha))^n)((\beta-\alpha)x) = \tilde{\mu}\,(\beta-\alpha)^{(m-d)(n-d)+d} P_d^{-n,-m}(2x-1)$$

which implies that

$$\mathrm{Sres}_d(x^m, (x-(\beta-\alpha))^n)(x) = \tilde{\mu}\,(\beta-\alpha)^{(m-d)(n-d)+d} P_d^{-n,-m}\left(2\left(\frac{x}{\beta-\alpha}\right)-1\right).$$

We conclude with

$$\begin{aligned}
\mathrm{Sres}_d((x-\alpha)^m, g(x-\beta)^n) &= \mathrm{Sres}_d(x^m, (x-(\beta-\alpha))^n)(x-\alpha)\\
&= \tilde{\mu}\,(\beta-\alpha)^{(m-d)(n-d)+d} P_d^{-n,-m}\left(2\left(\frac{x-\alpha}{\beta-\alpha}\right)-1\right)\\
&= \tilde{\mu}\,(\beta-\alpha)^{(m-d)(n-d)+d} P_d^{-n,-m}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right),
\end{aligned}$$

as stated in Theorem 2.
Note that similar arguments allow to deduce $G_d((x-\alpha)^m,(x-\beta)^n)$ from $G_d(x^m,(x-1)^n)$.

6. Final remarks

6.1. Algorithmic optimality

The complexity result $O(\min\{m,n\}+\log(mn))$ is quasi-optimal for Theorem 4, since the size of the output is $\min\{m,n\}$. On the other hand, the complexity result $O(\min\{m,n\}+\log(mn))$ for Theorem 1 is not optimal when d is small compared to m and n. A natural question is whether an algorithm of arithmetic complexity $O(d+\log(mn))$ may exist. We argue that this is unlikely; moreover, no algorithm of complexity $\mathrm{polylog}(d,\log(mn))$ would probably exist. Else, we could in particular compute the leading coefficient of $\mathrm{Sres}_1((x-\alpha)^m,(x-\beta)^n)$, which is readily checked to be equal to $(\alpha-\beta)^{(m-1)(n-1)}\cdot\binom{m+n-2}{m-1}$, in arithmetic complexity $\mathrm{polylog}(\log(mn))$. This does not seem plausible, since it would imply in particular that the central binomial coefficient $\binom{2N}{N}$ could be computed using an arithmetic complexity polynomial in $\log N$. Although no proof exists, this is generally believed to be false.

6.2. Fast computation of cofactors

One can use similar ideas as in the proof of Theorem 1 in order to compute the cofactors $F_d(x)$ and $G_d(x)$ in Corollary 6 using $O(\min\{m,n\}+\log(mn))$ arithmetic operations in $\mathbb{K}$.

6.3. Fast factorials

It is possible to further improve some of our complexity results by using Strassen's algorithm [Str1976] for the computation of $N!$ in arithmetic complexity $O(\mathsf{M}(\sqrt{N})\log N)$, which becomes quasi-linear in $\sqrt{N}$ when FFT-based algorithms are used for polynomial multiplication. For instance, for fixed d, the principal subresultant $\mathrm{PSres}_d((x-\alpha)^m,(x-\beta)^n)$ can be computed using fast factorials in

$$O(d+\log(mn)+\mathsf{M}(\sqrt{\min\{m-d,n-d\}})\log\min\{m-d,n-d\})$$

operations in $\mathbb{K}$. The same cost can be also achieved for the computation of the whole polynomial subresultant $\mathrm{Sres}_d((x-\alpha)^m,(x-\beta)^n)$ in Theorem 1.

6.4. Bit complexity

We have only discussed arithmetic complexity. When $\mathbb{K}$ is a finite field, this is perfectly realistic, since arithmetic complexity reflects quite well the running time of the algorithms. When $\mathbb{K}$ is infinite, for instance when $\mathbb{K} = \mathbb{Q}$, assuming operations in $\mathbb{K}$ at unit cost is not realistic anymore, so studying bit complexity becomes a much more pertinent model.

6.5. Subresultants for other structured polynomials

The question addressed in this article is a particular case of a much broader topic, the design of efficient algorithms for *structured polynomials*. Preliminary results let us hope that for polynomials whose coefficients satisfy linear recurrences, the computation of subresultants can be performed in linear time. This generalization of Theorems 1 and 4 will be the subject of a forthcoming work.

References

[ApJo2006] F. Apéry, J.-P. Jouanolou. *Résultant et sous-résultant: le cas d'une variable avec exercices corrigés.* Hermann, Paris (2006).

[Bak1975] G. A. Baker Jr. *The Essentials of Padé Approximants.* Academic Press, New York, 1975. xi+306 pp.
https://doi.org/10.1017/CBO9780511530074

[Boc1907] M. Bôcher. *Introduction to Higher Algebra.* The MacMillan Company, 1907. xi+321 pp.
http://archive.org/details/cu31924002936536

[BDKSV2017] A. Bostan, C. D'Andrea, T. Krick, A. Szanto, M. Valdettaro. *Subresultants in multiple roots: an extremal case.* Linear Algebra Appl. 529 (2017), no. 3, 185–198.
http://dx.doi.org/10.1016/j.laa.2017.04.019

[Col1967] G. E. Collins. *Subresultants and reduced polynomial remainder sequences.* J. ACM 14 (1967), no. 1, 128–142.
http://dx.doi.org/10.1145/321371.321381

[EMOT1953] A. Erdélyi, W. Magnus, F. Oberhettinger and F. G. Tricomi. *Higher transcendental functions, Vol. II.* McGraw-Hill, 1953. xviii+396 pp. Based, in part, on notes left by Harry Bateman, and compiled by the Staff of the Bateman Manuscript Project. http://authors.library.caltech.edu/43491/

[Eul1778] L. Euler. *Specimen transformationis singularis serierum.* Nova Acta Academiae Scientarum Imperialis Petropolitinae 12, 1794, pp. 58–70. Reprinted in Opera Omnia Series 1, Volume 16, 2, pp. 41–55, Enestrm-Number E710. http://eulerarchive.maa.org

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

[GG2013] J. von zur Gathen, J. Gerhard. *Modern Computer Algebra, 3rd Edition.* Cambridge University Press, 2013. http://dx.doi.org/10.1017/CBO9781139856065

[GGZ2012] O. Gomilko, F. Greco, K. Ziętak. *A Padé family of iterations for the matrix sign function and related problems.* Numer. Linear Algebra Appl. 19 (2012), no. 3, 585–605. http://doi.org/10.1002/nla.786

[HS1967] A. S. Householder, G. W. Stewart. *Bigradients, Hankel determinants, and the Padé table.* In *Constructive aspects of the fundamental theorem of algebra*, 131–150 (Proc. Sympos., Zürich-Rüschlikon, 1967, edited by B. Dejon and P. Henrici). Wiley-Interscience, New York, 1969.

[Hou1968] A. S. Householder. *Bigradients and the problem of Routh and Hurwitz.* SIAM Rev. 10 (1968), no. 1, 56–66. http://doi.org/10.1137/1010003

[Ise1979] A. Iserles. *A note on Padé approximations and generalized hypergeometric functions.* BIT 19 (1979), no. 4, 543–545. http://doi.org/10.1007/BF01931272

[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

[Jac1859] C. G. J. Jacobi. Untersuchungen über die Differentialgleichung der hypergeometrischen Reihe. J. Reine Angew. Math. 56 (1859), 149–165.
https://eudml.org/doc/147752

[Koo1984] T.H. Koornwinder *Orthogonal polynomials with weight function* $(1-x)^\alpha(1+x)^\beta + M\delta(x+1) + N\delta(x-1)$. Canad. Math. Bull. 27 (1984), no.2, 205–214.
http://doi.org/10.4153/CMB-1984-030-7

[Lag1885] E. Laguerre. *Sur la réduction en fractions continues d'une fraction qui satisfait à une équation différentielle linéaire du premier ordre dont les coefficients sont rationnels.* Journal de mathématiques pures et appliquées 4e série, tome 1, (1885), 135–166.
http://sites.mathdoc.fr/JMPA/PDF/JMPA_1885_4_1_A5_0.pdf

[Lec2018] G. Lecerf. *On the complexity of the Lickteig-Roy subresultant algorithm.* J. Symbolic Comput. (2018), in press.
http://doi.org/10.1016/j.jsc.2018.04.017

[Mis1993] B. 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

[Pad1901] H. Padé. *Sur l'expression générale de la fraction rationnelle approchée de* $(1+x)^m$. C.R. Acad. Sci. Paris, 132 (1901), 754–756.
http://www.numdam.org/article/ASENS_1892_3_9__S3_0.pdf

[Per1913] O. Perron. *Die Lehre von den Kettenbrüchen.* Druck und Verlag von B.G. Teubner, Leipzig & Berlin, 1913. viii+520 pp.
https://archive.org/details/dielehrevondenk00perrgoog/

[Rei1997] D. Reischert. *Asymptotically fast computation of subresultants.* Proceedings ISSAC'97, 233–240, ACM, New York, 1997.
http://dx.doi.org/10.1145/258726.258792

[SZ94] B. Salvy, P. Zimmermann. *GFUN: a Maple package for the manipulation of generating and holonomic functions in one variable.* ACM Transactions on Mathematical Software 20 (1994), no. 2, 163–177.
http://dl.acm.org/citation.cfm?id=178368

[Str1976] V. Strassen. *Einige Resultate über Berechnungskomplexität.* Jber. Deutsch. Math.-Verein 78 (1976), no. 1, 1–8.
https://eudml.org/doc/146659

[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

[Sze1975] G. Szegö. *Orthogonal Polynomials*, Providence, RI: Amer. Math. Soc., originally published 1939, 4th ed. 1975.
https://people.math.osu.edu/nevai.1/SZEGO/szego=szego1975=ops=OCR.pdf

[WZ1992] H.S. Wilf, D. Zeilberger. *An algorithmic proof theory for hypergeometric (ordinary and "q") multisum/integral identities.* Invent. Math. 108 (1992), no. 3, 575–633.
http://dx.doi.org/10.1007/BF02100618

[Zei90] D. Zeilberger. *The method of creative telescoping.* J. Symbolic Comput. 11 (1991), no. 3, 195–204.
http://dx.doi.org/10.1016/S0747-7171(08)80044-2