Journal of Symbolic Computation 101 (2020) 330–351

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

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

A. Bostan [a], T. Krick [b], A. Szanto [c], M. Valdettaro [d]

[a] Inria, Université Paris-Saclay, 1 rue Honoré d'Estienne d'Orves, 91120 Palaiseau, France
[b] Departamento de Matemática, Facultad de Ciencias Exactas y Naturales and IMAS, CONICET, Universidad de Buenos Aires, Argentina
[c] Department of Mathematics, North Carolina State University, Raleigh, NC 27695, USA
[d] Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Argentina

ARTICLE INFO

Article history:
Received 29 December 2018
Accepted 2 October 2019
Available online 10 October 2019

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

Keywords:
Subresultants
Algorithms
Complexity
Jacobi polynomials

ABSTRACT

In an earlier article (Bostan et al., 2017), with Carlos D'Andrea, we described explicit expressions 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 of Jacobi polynomials up to an affine change of variables.

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

URLs: 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).

https://doi.org/10.1016/j.jsc.2019.10.003

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

$$\mathrm{Sres}_d(f,g) := \det \overbrace{\left|\begin{array}{ccccc} f_m & \cdots & \cdots & f_{d+1-(n-d-1)} & x^{n-d-1} f \\ & \ddots & & \vdots & \vdots \\ & & f_m \;\cdots & f_{d+1} & f \\ \hline g_n & \cdots & \cdots & g_{d+1-(m-d-1)} & x^{m-d-1} g \\ & \ddots & & \vdots & \vdots \\ & & g_n \;\cdots & g_{d+1} & g \end{array}\right|}^{m+n-2d} \begin{array}{l} \\ n-d \\ \\ \\ m-d \\ \\ \end{array}, \tag{1}$$

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

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

Subresultants were introduced implicitly by Jacobi (1836) and explicitly by Sylvester (1839, 1840); we refer to Loos (1983) and von zur Gathen and Lücking (2003) for detailed historical accounts[1].

Let $\mathsf{M}(n)$ denote the arithmetic complexity of degree-n polynomial multiplication in $\mathbb{K}[x]$. 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. (von zur Gathen and Gerhard, 2013, 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 $\mathrm{Sres}_d(f, g)$ (Reischert, 1997; Lickteig and Roy, 2001; Lecerf, 2019), or all their principal subresultants $\mathrm{PSres}_d(f, g)$ for $0 \leq d < n$ (von zur Gathen and Gerhard, 2013, 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 algorithms with *linear* complexity for these two tasks for the special family of polynomials considered in (Bostan et al., 2017), namely $f = (x - \alpha)^m$ and $g = (x - \beta)^n$ in $\mathbb{K}[x]$, when $\mathrm{char}(\mathbb{K}) = 0$ or $\mathrm{char}(\mathbb{K}) \geq \max\{m, n\}$, and $\alpha \neq \beta \in \mathbb{K}$ (note that when $\alpha = \beta$ there is nothing to compute since all subresultants vanish). To our knowledge, we are exhibiting the first

[1] The Sylvester matrix was defined in (Sylvester, 1840), and the order-d subresultant was introduced by Sylvester (1839, 1840) under the name of "prime derivative of the d-degree". The term "polynomial subresultant" was seemingly coined by Collins (1967), and probably inspired to him by Bôcher's textbook (Bôcher, 1907, §69) who had used the word "subresultants" to refer to determinants of certain submatrices of the Sylvester matrix. Almost simultaneously, Householder and Stewart (1969) and Householder (1968) employed the term "polynomial bigradients". The principal subresultants were named "Nebenresultanten" (minor resultants) by Habicht (1948). The current terminology *principal subresultants* seems to appear for the first time in Collins' paper (Collins, 1974).

family of "structured polynomials" for which subresultants (and all principal subresultants) can be computed in optimal arithmetic complexity.

Let us first observe that the resultant $\mathrm{Sres}_0((x-\alpha)^m, (x-\beta)^n) = (\alpha-\beta)^{mn}$, which corresponds to the case $d=0$, can be computed by binary powering in $O(\log(mn))$ arithmetic operations in $\mathbb{K}$. The general case is not so simple: for example the particular case $d=1$ of Theorems 1.1 and 1.2 in (Bostan et al., 2017) (see also Theorem 2 below) shows that, for $1 < \min\{m,n\}$,

$$\mathrm{Sres}_1((x-\alpha)^m, (x-\beta)^n) = (\alpha-\beta)^{(m-1)(n-1)}\left(\binom{m+n-2}{m-1}x - \binom{m+n-3}{m-1}\alpha - \binom{m+n-3}{n-1}\beta\right).$$

This identity implies that, from a computational perspective, there is already a striking difference between the cases $d=0$ and $d=1$. Indeed, although the term $(\alpha-\beta)^{(m-1)(n-1)}$ can be computed in $O(\log(mn))$ operations in $\mathbb{K}$, no algorithm with arithmetic complexity polynomial in $\log(mn)$ is known for computing binomial coefficients such as $\binom{m+n-2}{m-1}$. However, the right-hand side of the previous identity can be computed in $O(\min\{m,n\})$ operations (see Lemma 8 below), provided the characteristic of the base field $\mathbb{K}$ is zero or large enough. The main result of the current article extends this complexity observation to arbitrary $1 \le d < \min\{m,n\}$.

Theorem 1. *Let $d,m,n \in \mathbb{N}$ with $1 \le d < \min\{m,n\}$ and let $\mathbb{K}$ be a field with $\mathrm{char}(\mathbb{K}) = 0$ or $\mathrm{char}(\mathbb{K}) \ge \max\{m,n\}$, and $\alpha,\beta \in \mathbb{K}$ with $\alpha \ne \beta$. Set*

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

Then,

(a) *if $\mathrm{char}(\mathbb{K}) = 0$ or $\mathrm{char}(\mathbb{K}) \ge m+n-d$, then $s_d \ne 0$ and all the coefficients s_k for $0 \le k \le d$ can be computed using $O(\min\{m,n\} + \log(mn))$ arithmetic operations in $\mathbb{K}$,*

(b) *when $\mathrm{char}(\mathbb{K}) = m+n-d-1$, the following equality holds in $\mathbb{K}$:*

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

and $\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n)$ can be computed using $O(\log(mn))$ arithmetic operations in $\mathbb{K}$,

(c) *if $m+n-d-1 > \mathrm{char}(\mathbb{K}) \ge \max\{m,n\}$, then*

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

We prove Theorem 1 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 (Jacobi, 1859). This allows us to produce a recurrence for the coefficients of the subresultant, which 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 (Szegő, 1939, Chapter 4) that for any $k,\ell,r \in \mathbb{Z}$ with $r \ge 0$, 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 $\mathrm{char}(\mathbb{K}) \ne 2$, 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 the rising factorial, of a.

Our next result 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 $P_d^{(-n,-m)}(x)$. More precisely, for $\alpha \neq \beta$, we consider the following change of variables in the Jacobi polynomial

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

and note that it belongs to $\frac{1}{(\alpha-\beta)^d}\mathbb{Z}[x-\alpha, x-\beta]$ when we consider α and β as distinct indeterminates over $\mathbb{Z}$. We denote by p_d its coefficient of x^d, for which we show in (15) below that

$$p_d = \frac{1}{(\alpha-\beta)^d}\binom{m+n-d-1}{d}. \tag{3}$$

We also recall that, following the notation in Theorem 1, the principal subresultant $s_d := \mathrm{PSres}_d((x-\alpha)^m, (x-\beta)^n)$ is the coefficient of x^d in $\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n)$, which by Proposition 3.3 in (Bostan et al., 2017) satisfies

$$s_d = (\alpha-\beta)^{(m-d)(n-d)} \prod_{i=1}^{d} r(i), \quad \text{with } r(i) := \frac{(i-1)!(m+n-d-i)!}{(m-i)!(n-i)!}. \tag{4}$$

As a consequence, s_d belongs to $\mathbb{Q}[\alpha-\beta] \cap \mathbb{Z}[\alpha,\beta] = \mathbb{Z}[\alpha-\beta]$. In fact it is shown in Theorem 1.1 of (Bostan et al., 2017) that the whole polynomial $\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n)$ belongs to $\mathbb{Z}[x-\alpha, x-\beta]$ (see also Lemma 6 below for an independent proof). Denote by $Q_d^{(-n,-m)}$ the following polynomial

$$Q_d^{(-n,-m)}(\alpha,\beta,x) := \frac{s_d \cdot P_d^{(-n,-m)}\left(\frac{(x-\alpha)+(x-\beta)}{\beta-\alpha}\right)}{p_d}. \tag{5}$$

Since $\alpha-\beta = (x-\beta)-(x-\alpha)$, the polynomial $Q_d^{(-n,-m)}(\alpha,\beta,x)$ belongs a priori to $\mathbb{Q}[x-\alpha, x-\beta]$. We will show that $Q_d^{(-n,-m)}(\alpha,\beta,x)$ actually coincides with $\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n)$ in $\mathbb{Z}[x-\alpha, x-\beta]$ and we then obtain, via the map $1_{\mathbb{Z}} \to 1_{\mathbb{K}}$, the following result:

Theorem 2. *Let $\mathbb{K}$ be a field and $\alpha, \beta \in \mathbb{K}$ with $\alpha \neq \beta$. Set $d, m, n \in \mathbb{N}$ with $0 \leq d < \min\{m, n\}$. Then, with the notation in (5),*

$$\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n) = Q_d^{(-n,-m)}(\alpha,\beta,x). \tag{6}$$

The key ingredient to prove Theorem 1 will be to derive from Theorem 2 a second-order recurrence satisfied by the coefficients of $\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n)$ in the monomial basis, as follows:

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

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

Then, when $\mathrm{char}(\mathbb{K}) = 0$ or $\mathrm{char}(\mathbb{K}) \ge m + n - d$, for $s_{d+1} := 0$ and for s_d as defined in (4), the following second-order linear recurrence is satisfied by the coefficients s_k, for $k = d-1, \dots, 0$:

$$s_k = \frac{-(k+1)\Big(\big((n-k-1)\alpha + (m-k-1)\beta\big)s_{k+1} + (k+2)\alpha\beta s_{k+2}\Big)}{(d-k)(m+n-d-k-1)}. \tag{7}$$

Our next result concerns the complexity of the computation of all principal subresultants $\mathrm{PSres}_d((x-\alpha)^m, (x-\beta)^n)$ for $0 \le d < \min\{m, n\}$. We note that the proof of this result is independent from our previous results, as it is a consequence of a recurrence that is derived directly from (4). We give it here for sake of completeness of our complexity results.

Theorem 4. *Let $\mathbb{K}$ be a field, let $m, n \in \mathbb{N}$ and assume $\mathrm{char}(\mathbb{K}) = 0$ or $\mathrm{char}(\mathbb{K}) \ge m + n$. 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 $0 \le d < \min\{m, n\}$ using $O(\min\{m, n\} + \log(mn))$ operations in $\mathbb{K}$.*

In the current article, we repeatedly use the crucial fact that, for *structured* algebraic objects, one can obtain improved complexity results by using recurrence relations that these objects obey, rather than just computing them independently. This is one of the strengths of our results: not only they provide nice formulae for the subresultants, but they also exploit their particular structure in order to design efficient algorithms.

This work has an interesting story. While working on the paper (Bostan et al., 2017), we first realized that Theorems 1.1 and 1.2 in (Bostan et al., 2017) (see Theorem 12 below) imply the linear recurrence on the coefficients of $\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n)$ in the usual monomial basis described in Theorem 3. This recurrence was initially found using a computer-driven "guess-and-prove" approach, where the guessing part relied on algorithmic *Hermite-Padé approximation* (Salvy and Zimmermann, 1994), and where the proving part relied on Zeilberger's *creative telescoping* algorithm (Zeilberger, 1991; Wilf and Zeilberger, 1992). 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 Theorem 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. To conclude this introduction, 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 Theorems 2 and 3 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, experimental results and perspectives in Section 6.

A preliminary version of this work is part of the doctoral thesis of Marcelo Valdettaro (2017).

Acknowledgements. We thank Christian Krattenthaler for precious help with hypergeometric identities during an early stage of this work, and Mohab Safey El Din for generously sharing his subresultants implementations with us. We are also grateful to the referees for helping us substantially improve the presentation of our results. 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. Proofs of Theorem 2 and Theorem 3

2.1. Proof of Theorem 2

The proof of Theorem 2 proceeds in 3 steps: (1) We prove the theorem in the case when $\mathbb{K}$ has characteristic 0. (2) We show, independently from Bostan et al. (2017), that $\mathrm{Sres}_d((x-\alpha)^m,(x-\beta)^n)$ belongs to $\mathbb{Z}[x-\alpha,x-\beta]$ when we consider both polynomials $(x-\alpha)^m$ and $(x-\beta)^n$ in $\mathbb{Z}[\alpha,\beta,x]$ for α,β new indeterminates over $\mathbb{Z}$, which implies that $(\alpha-\beta)^d\,p_d$ divides

$$s_d\cdot(\alpha-\beta)^d P_d^{(-n,-m)}\left(\frac{(x-\alpha)+(x-\beta)}{\beta-\alpha}\right) \text{ in } \mathbb{Z}[x-\alpha,x-\beta].$$

(Here we multiply both terms by $(\alpha-\beta)^d$ to guarantee that they are both polynomials in $\mathbb{Z}[x-\alpha,x-\beta]$.) (3) We finally conclude that the identity stated in Theorem 2 holds in any characteristic via the map $1_{\mathbb{Z}}\to 1_{\mathbb{K}}$.

We will need the next classical lemma, which follows e.g. from Mishra (1993, Lemmas 7.7.4 and 7.7.6) and was also a key ingredient in (Bostan et al., 2017).

Lemma 5. *Let $m,n\in\mathbb{N}$ and $f,\ g\in\mathbb{K}[x]$ of degrees m and n respectively. Set $0\le d<\min\{m,n\}$ and assume $\mathrm{Sres}_d(f,g)\neq 0$ has degree exactly d. 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*

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

2.1.1. Proof of Theorem 2 when $\mathrm{char}(\mathbb{K})=0$

In this case $\mathrm{Sres}_d((x-\alpha)^m,(x-\beta)^n)$ has degree exactly d by Identity (4) since $\alpha\neq\beta$. We will then show that $h=P_d^{(-n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right)$ satisfies the conditions of Lemma 5 applied to $f=(x-\alpha)^m$ and $g=(x-\beta)^n$.

One can check (or refer to Szegő, 1939, 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

$$y_1(x):=P_d^{(-n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right),$$

$$y_2(x):=\left(\frac{2}{\beta-\alpha}\right)^m(x-\alpha)^m P_{n-d-1}^{(-n,m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right) \text{ and}$$

$$y_3(x):=\left(\frac{2}{\alpha-\beta}\right)^n(x-\beta)^n P_{m-d-1}^{(n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right),$$

all solve the linear differential equation

$$(x-\alpha)(x-\beta)y''(x)+\big(\alpha(n-1)+\beta(m-1)-(m+n-2)x\big)y'(x) \\ +d(m+n-d-1)y(x)=0. \tag{8}$$

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

$$P_r^{(k,\ell)}(1)=\frac{(k+1)_r}{r!} \quad \text{and} \quad P_r^{(k,\ell)}(-1)=(-1)^r\frac{(\ell+1)_r}{r!}. \tag{9}$$

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

$$y_2(\beta)=2^m P_{n-d-1}^{(-n,m)}(1)=(-1)^{n-d-1}2^m\binom{n-1}{d}\neq 0 \text{ and } y_2(\alpha)=0, \tag{10}$$

while

$$y_3(\beta)=0 \text{ and } y_3(\alpha)=2^n P_{m-d-1}^{(n,-m)}(-1)=2^n\binom{m-1}{d}\neq 0. \tag{11}$$

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

$$P_d^{(-n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right)=A\left(\frac{2}{\beta-\alpha}\right)^m P_{n-d-1}^{(-n,m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right)(x-\alpha)^m \\ +B\left(\frac{2}{\alpha-\beta}\right)^n P_{m-d-1}^{(n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right)(x-\beta)^n. \tag{12}$$

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

$$P_d^{(-n,-m)}(1)=(-1)^d\binom{n-1}{d} \quad \text{and} \quad P_d^{(-n,-m)}(-1)=\binom{m-1}{d}. \tag{13}$$

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 Lemma 5 implies that there exists $\lambda\in\mathbb{K}$ such that

$$P_d^{(-n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right)=\lambda\cdot \mathrm{Sres}_d((x-\alpha)^m,(x-\beta)^n). \tag{14}$$

Thus, the left-hand side and right-hand side of this equality have the same coefficient of x^d, which implies that $\lambda=p_d/s_d$. We now determine p_d.

By Identity (2),

$$p_d=\frac{1}{(\alpha-\beta)^d}\sum_{j=0}^{d}\binom{n-d+j-1}{j}\binom{m-j-1}{d-j}=\frac{1}{(\alpha-\beta)^d}\binom{m+n-d-1}{d}, \tag{15}$$

where the second identity can be 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 $m-d$.

Passing $\lambda^{-1}=s_d/p_d$ to the left-hand side in Identity (14) proves Theorem 2 when $\mathrm{char}(\mathbb{K})=0$. □

2.1.2. Proof that $\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n)$ *belongs to* $\mathbb{Z}[x-\alpha, x-\beta]$

This result is already proved by Bostan et al. (2017), but we give here an independent proof because in Section 5.1 we will show that the result in (Bostan et al., 2017), recalled in Theorem 12 below, and our Theorem 2 are equivalent.

Lemma 6. *Set* $d, m, n \in \mathbb{N}$ *with* $0 \le d < \min\{m, n\}$*, and let* $(x-\alpha)^m, (x-\beta)^n \in \mathbb{Z}[\alpha, \beta, x]$*. Then*

$$\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n) \in \mathbb{Z}[x-\alpha, x-\beta].$$

Proof. It is well-known from the matrix formulation of the subresultant that $\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n) \in \mathbb{Z}[\alpha, \beta, x]$. Theorem 2 gives us a way of writing

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

where $c_j \in \mathbb{Q}$.

In particular, for $\alpha = 0$ and $\beta = -1$, one has on the one hand

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

with $c_j \in \mathbb{Q}$ while on the other hand $\mathrm{Sres}_d(x^m, (x+1)^n) = \sum_{k=0}^{d} a_k x^k$ with $a_k \in \mathbb{Z}$, $0 \le k \le d$. This means that

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

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

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

i.e., that

$$\begin{pmatrix} a_0 \\ \vdots \\ a_d \end{pmatrix} = \begin{pmatrix} 1 & & & \\ \binom{d}{1} & 1 & & \\ \vdots & \vdots & \ddots & \\ \binom{d}{d} & \binom{d}{d-1} & \cdots & 1 \end{pmatrix} \begin{pmatrix} c_0 \\ \vdots \\ c_d \end{pmatrix}.$$

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

2.1.3. Concluding the proof of Theorem 2

We assume that α and β are distinct indeterminates over $\mathbb{Q}$. The theorem holds over the field $\mathbb{Q}(\alpha, \beta)$, with both sides of equality (6) belonging to $\mathbb{Z}[x-\alpha, x-\beta]$. To prove the theorem for an arbitrary field $\mathbb{K}$, and for distinct values $\tilde{\alpha}$ and $\tilde{\beta}$ in $\mathbb{K}$, we apply a classical specialization argument, using the ring homomorphism $\mathbb{Z}[x-\alpha, x-\beta] \to \mathbb{K}[x]$ which maps $1_{\mathbb{Z}} \mapsto 1_{\mathbb{K}}, \alpha \mapsto \tilde{\alpha}, \beta \mapsto \tilde{\beta}$.

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*

$$\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n) = F_d \cdot (x-\alpha)^m + G_d \cdot (x-\beta)^n, \tag{16}$$

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

Corollary 7. *Let $\mathbb{K}$ be a field and $\alpha, \beta \in \mathbb{K}$ with $\alpha \neq \beta$. Set $d, m, n \in \mathbb{N}$ with $0 \le d < \min\{m, n\}$. Then, the polynomials F_d and G_d defined in (16) satisfy*

$$F_d = \frac{(-1)^{n-1} s_d\, P_{n-d-1}^{(-n,m)}\left(\frac{(x-\alpha)+(x-\beta)}{\beta-\alpha}\right)}{(\beta-\alpha)^m\, p_d}, \quad G_d = \frac{(-1)^{n} s_d\, P_{m-d-1}^{(n,-m)}\left(\frac{(x-\alpha)+(x-\beta)}{\beta-\alpha}\right)}{(\beta-\alpha)^n\, p_d}.$$

Proof. As in the proof of Theorem 2 we first assume that $\mathbb{K}$ is a field of characteristic 0. By this theorem, Identities (16) and (12), one has

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

We now determine the values of A and B. By Identities (10), (11), (12) and (13), we get

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

Therefore $A = \dfrac{(-1)^{n-1}}{2^m}$ and $B = \dfrac{1}{2^n}$. This proves the statement when $\mathrm{char}(\mathbb{K}) = 0$. Finally, both sides in the equalities of Corollary 7 belong to $\frac{1}{(\alpha-\beta)^{m+n-d-1}}\mathbb{Z}[\alpha, \beta, x]$ and so they specialize well to a field of any characteristic via the map $1 \mapsto 1_{\mathbb{K}}$. □

2.3. Proof of Theorem 3

We now prove Theorem 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 (8) satisfied by $P_d^{(-n,-m)}\left(\dfrac{(x-\alpha)+(x-\beta)}{\beta-\alpha}\right)$ in characteristic 0.

By Theorem 2,

$$\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n) = Q_d^{(-n,-m)}(\alpha, \beta, x)$$
$$= \frac{s_d}{p_d} \cdot P_d^{(-n,-m)}\left(\frac{(x-\alpha)+(x-\beta)}{\beta-\alpha}\right), \tag{17}$$

where $P_d^{(-n,-m)}\left(\dfrac{(x-\alpha)+(x-\beta)}{\beta-\alpha}\right)$ is the integer Jacobi polynomial described in Identity (2), and

$$\begin{aligned}\frac{s_d}{p_d} &= (\alpha-\beta)^{(m-d)(n-d)+d}\,\frac{\prod_{i=1}^{d} r(i)}{\binom{m+n-d-1}{d}}\\ &= (\alpha-\beta)^{(m-d)(n-d)+d}\prod_{i=1}^{d}\frac{i!(m+n-d-i-1)!}{(m-i)!(n-i)!}.\end{aligned} \tag{18}$$

Therefore, the differential equation (8) 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 statement. 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

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

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

and

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

Now we compare the degree-k coefficient in (8) for $k=0,\ldots,d-1$:

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

Therefore,

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

This proves the recurrence when $\mathrm{char}(\mathbb{K})=0$. It is clear that the same recurrence also holds for fields $\mathbb{K}$ of characteristic $\geq m+n-d$ via the map $1_{\mathbb{Z}}\to 1_{\mathbb{K}}$ since in all the steps we are dividing only by natural numbers less than $m+n-d$. $\square$

3. Proof of Theorem 1

3.1. Proof of Theorem 1 (a)

We start with the following simple observation.

Lemma 8. *Let $\mathbb{K}$ be a field, let $k, \ell \geq 0$ be integers and assume* $\mathrm{char}(\mathbb{K}) = 0$ *or* $\mathrm{char}(\mathbb{K}) > \min\{k, \ell\}$. *Then the (image in $\mathbb{K}$ of the) binomial coefficient $\binom{k+\ell}{k}$ can be computed in $O(\min\{k, \ell\})$ arithmetic operations in $\mathbb{K}$.*

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

The proof that one can compute all coefficients of the d-th subresultant of $(x-\alpha)^m$ and $(x-\beta)^n$ in $O(\min\{m,n\} + \log(mn))$ operations in $\mathbb{K}$ when $\mathrm{char}(\mathbb{K})$ is either zero or larger than $m+n-d$ will be derived from the recurrence (7) described in Theorem 3. The proof is algorithmic and proceeds in several steps.

We start with $s_d = (\alpha-\beta)^{(m-d)(n-d)} \prod_{i=1}^{d} r(i)$, with $r(i)$ defined in (4), and observe that for the mentioned characteristics, $s_d \neq 0$ since $\alpha \neq \beta$.

- The term $(\alpha-\beta)^{(m-d)(n-d)}$ can be computed in $O(\log(mn))$ arithmetic operations, by using binary powering.
- The element $r(d) = (d-1)!\binom{m+n-2d}{m-d}$ can be computed in $O(\min\{m,n\})$ arithmetic operations by applying Lemma 8, and using that $d < \min\{m,n\}$.
- Thanks to the recurrence
$$r(i) = \frac{(m+n-d-i)}{i(m-i)(n-i)} r(i+1),$$
all $r(d-1), \ldots, r(1)$ can be deduced from $r(d)$ in $O(d)$ additional operations; then, computing $r(1)\cdots r(d)$ also takes $O(d)$ operations.
Note that during the unrolling of the recurrence, the only divisions that occur are by positive integers less than $\max\{m,n\}$, legitimate in $\mathbb{K}$ by the assumption on its characteristic.

This shows that s_d can be computed using $O(\min\{m,n\} + \log(mn))$ arithmetic operations in $\mathbb{K}$.

- Starting from $s_{d+1} = 0$ and s_d, we use the recurrence (7) to compute $s_{d-1}, s_{d-2}, \ldots, s_0$ in $O(d)$ operations, by adding $O(1)$ operations in $\mathbb{K}$ for each of these d terms.
Note that in this step only divisions by integers less than $m+n-d-1$ may occur, and all these elements are invertible in $\mathbb{K}$, by assumption.

In conclusion, all the coefficients $s_0, \ldots, s_d$ of $\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n)$ can be computed in $O(\min\{m,n\} + \log(mn))$ operations in $\mathbb{K}$, when $\mathrm{char}(\mathbb{K}) = 0$ or $\mathrm{char}(\mathbb{K}) \geq m+n-d$. □

3.2. Proof of Theorem 1 (b)

We apply again the recurrence given by Theorem 3, in the characteristic 0 case, to show that when $\mathrm{char}(\mathbb{K}) = m+n-d-1$, the polynomial subresultant $\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n))$ is actually a (non-zero) constant in $\mathbb{K}$.

Lemma 9. *Set $d, m, n \in \mathbb{N}$ with $1 \leq d < \min\{m,n\}$ and let*

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

Assume that $m+n-d-1$ equals a prime number p. Then $p \mid s_k$ in $\mathbb{Z}[\alpha,\beta]$ for $1 \leq k \leq d$.

Proof. By applying Identity (4), we first show that $p \mid s_d$: clearly p does not divide the denominator but p divides $(m+n-d-1)!$ which is in the numerator of $r(1)$. Therefore $p \mid \prod_{i=1}^{d} r(i)$ and $p \mid s_d$ (since $d \geq 1$). Observe that for $1 \leq k \leq d-1$, the denominators that appear in the recurrence defining the sequence s_k in Theorem 3 range from $(d-1)(m+n-d-2)$ to $(m+n-2d)$, and thus none of them is divisible by $p = m+n-d-1$. Therefore, since $p \mid s_{d+1}$ and $p \mid s_d$, we inductively conclude that $p \mid s_k$ for $1 \leq k \leq d$. □

Via the map $1_{\mathbb{Z}} \to 1_{\mathbb{K}}$, we immediately deduce that $s_d = \cdots = s_1 = 0$ in $\mathbb{K}$, and therefore $\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n) \in \mathbb{K}$. We compute its value by specializing Identity (17) at $x = \alpha$, and thanks to (13) and (18). Set $p := m+n-d-1 = \mathrm{char}(\mathbb{K})$, then $\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n)$ is equal to

$$
\begin{aligned}
&(\alpha-\beta)^{(m-d)(n-d)+d} \prod_{i=1}^{d} \frac{i!(m+n-d-i-1)!}{(m-i)!(n-i)!} P_d^{(-n,-m)}(-1) \\
&= (\alpha-\beta)^{(m-d)(n-d)+d} \prod_{i=1}^{d} \frac{i!(p-i)!}{(m-i)!(n-i)!} \binom{m-1}{d} \\
&= (\alpha-\beta)^{(m-d)(n-d)+d} \prod_{i=1}^{d} \frac{(i-1)!(p-i)!}{(m-i-1)!(n+i-d-1)!} \\
&= (\alpha-\beta)^{(m-d)(n-d)+d} \prod_{i=1}^{d} \frac{\binom{p-1}{m-i-1}}{\binom{p-1}{i-1}}.
\end{aligned}
$$

It remains to show that the last product is equal to $(-1)^{md}$ in $\mathbb{K}$. This is an immediate consequence of the following elementary lemma.

Lemma 10. $\binom{p-1}{\ell} = (-1)^{\ell}$ *in* $\mathbb{K}$, *for any* $0 \leq \ell < p = \mathrm{char}(\mathbb{K})$.

Proof. By Fermat's little theorem we have $(x-1)^{p-1} = (x-1)^p/(x-1) = (x^p-1)/(x-1) = x^{p-1} + \cdots + 1$ in $\mathbb{K}[x]$. Thus, the coefficient $(-1)^{\ell}\binom{p-1}{\ell}$ of x^{ℓ} in $(x-1)^{p-1}$ is equal to 1 in $\mathbb{K}$. □

Finally, by the previous lemma, the following equalities hold in $\mathbb{K}$:

$$
\prod_{i=1}^{d} \frac{\binom{p-1}{m-i-1}}{\binom{p-1}{i-1}} = \prod_{i=1}^{d} \frac{(-1)^{m-i-1}}{(-1)^{i-1}} = (-1)^{md}.
$$

This concludes the proof of Theorem 1 (b). □

3.3. *Proof of Theorem 1* (c)

This non-obvious fact follows for instance from Theorem 2. We know by Identity (17) in the characteristic 0 case that

$$
\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n) = \frac{s_d}{p_d} \cdot P_d^{(-n,-m)}\left(\frac{(x-\alpha)+(x-\beta)}{\beta-\alpha}\right)
$$

where $P_d^{(-n,-m)}\left(\frac{(x-\alpha)+(x-\beta)}{\beta-\alpha}\right)$ is the integer polynomial described in Identity (2), and

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

We note that the denominator in this last term does not vanish in the mentioned characteristics while the numerator equals 0, since it is a multiple of $(m+n-d-2)!$ for $d \geq 1$. We conclude the proof of Theorem 1(c) via the map $1_{\mathbb{Z}} \to 1_{\mathbb{K}}$. □

Remark. Notice that Theorem 1(c) also follows from Theorem 1(b) and from Collins' fundamental theorem of subresultants (Collins, 1973, §4, see also Habicht, 1948, §2 and Collins, 1967, Theorem 1) which states that for an arbitrary field $\mathbb{K}$ and arbitrary $f, g \in \mathbb{K}[x]$, the subresultants and the Euclidean remainder sequence of f and g are closely related: if $A_1 := f, A_2 := g, A_3, \ldots, A_\ell$ is an Euclidean polynomial remainder sequence of f and g with $\deg(A_k) = n_k$ for $1 \leq k \leq \ell$, then there exist $c_1, \ldots, c_\ell, d_1, \ldots, d_\ell \in \mathbb{K}^\times$ such that

$$\begin{aligned}&\mathrm{Sres}_{n_k}(f,g) = c_k \cdot A_k, \ \ \mathrm{Sres}_{n_{k-1}-1}(f,g) = d_k \cdot A_k, \ \text{and}\\ &\mathrm{Sres}_d(f,g) = 0 \text{ for } n_k < d < n_{k-1} - 1,\end{aligned}$$

for all $1 \leq k \leq \ell$. In particular, if two nonzero subresultants $\mathrm{Sres}_e(f,g)$ and $\mathrm{Sres}_{e'}(f,g)$ have the same degree for some $e' < e$, then they are constant multiples of each other, and all the intermediate subresultants $\mathrm{Sres}_d(f,g)$ are zero for $e' < d < e$. In our situation, with $\max\{m,n\} \leq p := \mathrm{char}(\mathbb{K}) < m+n-d-1$, and $f = (x-\alpha)^m, g = (x-\beta)^n$ in $\mathbb{K}[x]$ with $\alpha \neq \beta$, we have that $\mathrm{Sres}_0(f,g) \in \mathbb{K}^\times$ and also, by Theorem 1(b), that $\mathrm{Sres}_{m+n-p-1}(f,g) \in \mathbb{K}^\times$. Therefore, $\mathrm{Sres}_d(f,g) = 0$ for $1 \leq d < m+n-1-p$, which reproves part (c) of Theorem 1.

4. Proof of Theorem 4

With the notation $r(i) := \dfrac{(i-1)!(m+n-d-i)!}{(m-i)!(n-i)!}$ introduced in (4), we have:

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

While in previous sections d was considered as a fixed value, in this section we view it as variable. Therefore, in order to avoid confusion, we write $r_d(i) := r(i)$, to emphasize also its dependence on d. For all integers $d \geq 1$, we define

$$c(d) := \prod_{i=1}^{d} r_d(i)$$

and note that it is an integer number, as mentioned in the introduction, although the terms $r_d(i)$ are not all integers. We also set $c(0) := 1$.

The key observation for what follows is contained in the next lemma.

Lemma 11. *Let $\mathbb{K}$ be a field with $\mathrm{char}(\mathbb{K}) = 0$ or $\mathrm{char}(\mathbb{K}) \geq m+n$. Set $u(d) := c(d)/c(d-1)$ for $1 \leq d < \min\{m,n\}$ and $v(d) := u(d+1)/u(d)$ for $1 \leq d \leq \min\{m,n\} - 2$. Then, for $1 \leq d \leq \min\{m,n\} - 2$,*

$$v(d) = \frac{d(m-d)(n-d)(m+n-d)}{(m+n-2d-1)(m+n-2d)^2(m+n-2d+1)}. \tag{19}$$

Proof. We have that $u(1) = c(1) = \binom{m+n-2}{m-1}$ and for $d \geq 2$,

$$\frac{r_d(i)}{r_{d-1}(i)} = \frac{1}{(m+n-d-i+1)}.$$

Therefore

$$u(d) = \frac{c(d)}{c(d-1)} = \frac{\prod_{i=1}^{d} r_d(i)}{\prod_{i=1}^{d-1} r_{d-1}(i)} = r_d(d) \cdot \prod_{i=1}^{d-1} \frac{r_d(i)}{r_{d-1}(i)}$$

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

Hence

$$v(d) = \frac{u(d+1)}{u(d)} = d \frac{(m-d)(n-d)}{(m+n-2d-1)(m+n-2d)} \cdot \frac{(m+n-d)}{(m+n-2d)(m+n-2d+1)},$$

which is the desired expression.

Note that the only numbers that appear in the denominators of $u(d)$ and of $v(d)$ are products of integers of absolute value less than $m+n$, which are invertible in $\mathbb{K}$ by the assumption on the characteristic of $\mathbb{K}$. □

Based on Lemma 11, we now design an algorithm that computes all principal subresultants $\mathrm{PSres}_d((x-\alpha)^m, (x-\beta)^n)$ with $1 \le d < \min\{m,n\}$ in $O(\min\{m,n\} + \log(mn))$ operations in $\mathbb{K}$, thus proving Theorem 4.

- First, $v(1), \ldots, v(\min\{m,n\}-2)$ are computed by using (19) in $O(1)$ arithmetic operations each, for a total of $O(\min\{m,n\})$ operations in $\mathbb{K}$.
- Then, $u(1), \ldots, u(\min\{m,n\}-1)$ are determined, by computing $u(1) := \binom{m+n-2}{m-1}$ using Lemma 8, in $O(\min\{m,n\})$ arithmetic operations in $\mathbb{K}$, and by computing iteratively $u(d) = u(d-1) \cdot v(d-1)$, for $2 \le d < \min\{m,n\}$, in $O(\min\{m,n\})$ operations in $\mathbb{K}$.
- Next we compute the elements $c(1), \ldots, c(\min\{m,n\}-1)$ iteratively by $c(d) = u(d) \cdot c(d-1)$ for $1 \le d < \min\{m,n\}$, in $O(\min\{m,n\})$ operations in $\mathbb{K}$.

At this stage, it remains to compute all the powers $h(d) := (\alpha-\beta)^{(m-d)(n-d)}$ for $0 \le d < \min\{m,n\}$, and finally to output $\mathrm{PSres}_d((x-\alpha)^m, (x-\beta)^n) = c(d) \cdot h(d)$, for $0 \le d < \min\{m,n\}$. This is done as follows.

- First, all the elements $\gamma(d) := (\alpha-\beta)^{2d+1-m-n}$, for $d < \min\{m,n\}$, are computed 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, $h(0) := (\alpha-\beta)^{mn}$ is computed by binary powering, and then all $h(d)$, for $1 \le d < \min\{m,n\}$, by repeated products using $h(d+1) := \gamma(d) \cdot h(d)$, for a total cost of $O(\log(mn) + \min\{m,n\})$ operations in $\mathbb{K}$.
- Finally, we compute and return the values $\mathrm{PSres}_d((x-\alpha)^m, (x-\beta)^n) = c(d) \cdot h(d)$, for $0 \le d < \min\{m,n\}$, using $O(\min\{m,n\})$ operations in $\mathbb{K}$.

Adding up the various arithmetic costs proves Theorem 4. □

5. Connections to previous results

Theorem 2 is closely connected to some previous results. First we discuss the connection to the work (Bostan et al., 2017). Second, we explain the relationship of the present work to classical results on *Padé approximation.*

5.1. Connection with (Bostan et al., 2017)

We show that the expression for the subresultant obtained in Bostan et al. (2017), though not expressed in terms of Jacobi polynomials, is equivalent to the one in Theorem 2. First, let us recall the main results of Bostan et al. (2017).

Theorem 12. *(Bostan et al., 2017, 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 $0 \le d < \min\{m, n\}$. 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

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

(*Here $c_0(m,n,0) = 1$, following the convention that an empty product equals 1.*)

Moreover, for $0 \le j \le d$, $c_j(m,n,d) \in \mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z}$ if $\mathrm{char}(\mathbb{K}) = 0$ or $\mathrm{char}(\mathbb{K}) = p$, respectively.

Proof that Theorems 12 and 2 are equivalent We want to prove that

$$(\alpha-\beta)^{(m-d)(n-d)} \sum_{j=0}^{d} c_j(m,n,d)(x-\alpha)^j (x-\beta)^{d-j} = \frac{s_d\, P_d^{(-n,-m)}\left(\frac{2x-\alpha-\beta}{\beta-\alpha}\right)}{p_d}, \tag{20}$$

where

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

for $c := m+n-d-1$.

By (18) the right-hand side of (20) equals

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

where by (2),

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

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. □

5.2. Connection with Padé approximation

In this subsection we show that Theorem 2 and Corollary 7 are also equivalent to classical descriptions of some Padé approximants via Gauss hypergeometric functions.

The starting point is a theorem due to Padé (1901), stating that the $[m/n]$ Padé approximation in $\mathbb{C}(x)$ to $(1-x)^k$ is the ratio of hypergeometric functions

$$\frac{{}_2F_1(-m,-k-n;-m-n;x)}{{}_2F_1(-n,k-m;-m-n;x)}. \tag{21}$$

That result had been previously obtained, using different methods and under several additional assumptions, by Euler (1778), Laguerre (1885) and Jacobi (1859). See also (Perron, 1913, Eq. (Padé 5), p. 252), (Baker, 1975, p. 65), (Iserles, 1979) and Theorem 4.1 in Gomilko et al. (2012).

There is also a well-known connection between subresultants and Padé approximants (cf. von zur Gathen and Gerhard, 2013, Corollary 5.21): the $[m/n]$ Padé approximation in $\mathbb{C}(x)$ to $(1-x)^k$, for integer $k \geq m$, equals

$$\frac{\mathrm{Sres}_m(x^{m+n+1},(1-x)^k)}{G_m(x^{m+n+1},(1-x)^k)} = (-1)^k \frac{\mathrm{Sres}_m(x^{m+n+1},(x-1)^k)}{G_m(x^{m+n+1},(x-1)^k)}, \tag{22}$$

where $G_m := G_m(x^{m+n+1},(x-1)^k)$ is the polynomial coefficient of degree $\leq n$ 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 (21) 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 polynomials 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

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

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

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

by Identity (4).

Now, according to (Erdélyi et al., 1953, (1.6)), see also (Koornwinder, 1984, (1.5)):

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

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

while, according to our Theorem 2 and Corollary 7,

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

for

$$\mu := (\alpha-\beta)^{(m-d)(n-d)+d} \prod_{i=1}^{d} \frac{i!(m+n-d-i-1)!}{(m-i)!(n-i)!} \quad \text{and}$$
$$\overline{\mu} := (-1)^{(n+1)(k-m)+m} \prod_{i=1}^{m} \frac{i!(k+n-i)!}{(k-i)!(m+n+1-i)!}.$$

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 7 for any α, β we apply the usual changes of variables formulas that can be found in the now classical book (Apéry and Jouanolou, 2006):

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

Therefore,

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

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

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

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. 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 7 using $O(\max\{m,n\}+\log(mn))$ arithmetic operations in $\mathbb{K}$, when $\mathrm{char}(\mathbb{K})=0$ or $\mathrm{char}(\mathbb{K})\geq\max\{m,n\}$. More precisely, we have the following result, whose proof is omitted:

Theorem 13. *Let $d,m,n\in\mathbb{N}$ with $1\leq d<\min\{m,n\}$ and let $\mathbb{K}$ be a field with $\mathrm{char}(\mathbb{K})=0$ or $\mathrm{char}(\mathbb{K})\geq\max\{m,n\}$, and $\alpha,\beta\in\mathbb{K}$ with $\alpha\neq\beta$. Let F_d and G_d be as defined in (16). Then,*

(a) if $\mathrm{char}(\mathbb{K})=0$ or $\mathrm{char}(\mathbb{K})\geq m+n-d$, then all the coefficients of F_d and G_d can be computed using $O(\max\{m,n\}+\log(mn))$ arithmetic operations in $\mathbb{K}$,
(b) when $\mathrm{char}(\mathbb{K})=m+n-d-1$, the following equalities hold in $\mathbb{K}$

$$F_d=(-1)^{dm+1}(\alpha-\beta)^{(m-d-1)(n-d-1)}(x-\alpha)^{n-d-1},$$
$$G_d=(-1)^{dm}(\alpha-\beta)^{(m-d-1)(n-d-1)}(x-\beta)^{m-d-1},$$

and the coefficients of F_d and G_d can be computed using $O(\max\{m,n\}+\log(mn))$ arithmetic operations in $\mathbb{K}$,
(c) if $m+n-d-1>\mathrm{char}(\mathbb{K})\geq\max\{m,n\}$ then

$$F_d=G_d=0.$$

6.2. Comparison with generic algorithms

As mentioned in the introduction, the fastest algorithms for subresultants of polynomials of degree at most n have arithmetic complexity $O(\mathsf{M}(n)\log n)$, where $\mathsf{M}(n)$ denotes the arithmetic complexity of degree-n polynomial multiplication (Reischert, 1997; Lickteig and Roy, 2001; Lecerf, 2019). These algorithms can compute either one selected polynomial subresultant, or all principal subresultants. Using FFT-based algorithms for polynomial multiplication (von zur Gathen and Gerhard, 2013, Ch. 8), their complexity $O(\mathsf{M}(n)\log n)$ becomes $O(n\log^2 n\log\log n)$, which is quasi-linear up to polylogarithmic factors. These algorithms are generic in the sense that they apply to arbitrary polynomials, and they work in any characteristic.

The algorithms described in the current article are specific to very structured polynomials, namely powers of linear polynomials, and they achieve linear arithmetic complexity in their maximum degree n. They also compute either one selected polynomial subresultant, or all principal subresultants, but they are restricted to characteristic zero or large enough. The reason is that they require divisions, which is the price to pay for optimality. We leave as an open question whether linear arithmetic complexity can be also achieved in arbitrary characteristic.

Another interesting difference is that, while classical algorithms for the order-d subresultant spend more time when d is small (typically, the resultant computation, corresponding to $d=0$, is the most expensive), our algorithms spend less time when d is small. For more on practical comparisons, see §6.6.

6.3. 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. While this is true for $d=0$, we believe that this is unlikely for $d\geq1$, and moreover we suspect that there is no algorithm for Theorem 1 with arithmetic complexity polynomial in both d and $\log(mn)$. Otherwise, we could in particular compute the first principal subresultant

$$\mathrm{PSres}_1((x-\alpha)^m, (x-\beta)^n) = (\alpha-\beta)^{(m-1)(n-1)} \binom{m+n-2}{m-1},$$

in arithmetic complexity *polynomial in* $\log(mn)$. 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 impossible.

6.4. Fast factorials

It is possible to further improve some of our complexity results by using Strassen's algorithm (Strassen, 1976) 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 also be achieved for the computation of the whole polynomial subresultant $\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n)$ in Theorem 1.

6.5. 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. Over $\mathbb{K} = \mathbb{Q}$, our algorithms in Sections 3 and 4 have very good complexity behaviors in this model too. Indeed, they only involve binary powering, computation of factorials and binomials, unrolling of recurrences, which can be computed in quasi-optimal bit complexity. This is confirmed by the timings in Tables 1 and 2, which appear to be indeed quasi-linear in the output size.

6.6. Practical issues

The algorithms described in this article have not only a good theoretical complexity, but also a good practical efficiency. We performed some experimental comparisons in Maple, between an implementation of our specialized algorithm in Section 3 and a generic subresultant algorithm available in the package RegularChains.[2] As expected, our algorithm is much faster, since it exploits the special structure of the input polynomials.

Table 1 displays some timings for computing $\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n)$, for various random choices of α, β, m, n and d. Even for moderate degrees m, n, the specialized algorithm is about thousands of times faster. For higher degrees, the generic algorithm becomes quite slow, while the specialized algorithm has a very satisfactory speed.

We also implemented in Maple the algorithm in Section 4, and this time we compared it, on the same examples as in Table 1, with an algorithm written in C by Mohab Safey El Din. The experimental results are displayed in Table 2. Once again, the specialized algorithm is faster than the generic algorithm.

[2] http://www.regularchains.org/index.html.

Table 1
Comparative timings (in seconds) for the computation of the polynomial subresultants $\mathrm{Sres}_d((x-\alpha)^m, (x-\beta)^n)$, on several instances of $(\alpha, \beta) \in \mathbb{Q}^2$ and $(m, n, d) \in \mathbb{N}^3$, using a generic subresultant algorithm implemented in the RegularChains package (column Generic 1), versus the specialized algorithm described in Section 3 (column New 1). All examples were run on the same machine, with the latest version of Maple. For entries marked with a –, the computations were aborted after more than 17 hours, with all available memory (150 Gb of RAM) consumed. The last column displays the bit size of the output.

#	(α, β)	(m, n, d)	Generic 1	New 1	Output size
T1	(10, 11)	(121, 92, 32)	0.164	0.001	112 125
T2	(13, 17)	(196, 169, 84)	5.439	0.002	2 463 994
T3	(12, 19)	(227, 245, 87)	23.543	0.006	6 996 907
T4	(12, 14)	(483, 295, 203)	71.613	0.011	11 869 930
T5	(10, 7)	(715, 694, 290)	2112.891	0.092	123 580 220
T6	(8, 4)	(1917, 1532, 805)	–	1.227	1 982 541 397
T7	(8, 4)	(2409, 3833, 1261)	–	7.847	10 745 238 510
T8	(3, 2)	(7840, 6133, 3510)	–	40.983	45 784 567 320

Table 2
Comparative timings (in seconds) for the computation of the principal subresultants $\mathrm{PSres}_d((x-\alpha)^m, (x-\beta)^n)$, on the instances T1–T8 from Table 1, using a generic subresultant algorithm implemented in C (column Generic 2), versus the specialized algorithm described in Section 4 implemented in Maple (column New 2). Column Output size G2 displays the bit size of the integer $\mathrm{PSres}_d((x-\alpha)^m, (x-\beta)^n)$ computed by Generic 2. Timings displayed in column New 2 correspond to the computation of all $\mathrm{PSres}_d((x-\alpha)^m, (x-\beta)^n)$ for $0 \le d < \min\{m, n\} - 1$. Column Output size N2 displays the bit size of the $\min\{m, n\}$ integers computed by New 2.

#	Generic 2	Output size G2	New 2	Output size N2
T1	0.011	3 297	0.001	201 764
T2	0.071	28 739	0.005	5 113 012
T3	0.281	79 253	0.030	14 744 328
T4	0.306	57 633	0.034	24 875 833
T5	8.921	423 993	0.905	249 854 978
T6	211.895	2 458 114	12.578	4 187 207 983
T7	1992.231	8 511 770	83.145	21 885 019 390
T8	15627.306	13 035 552	237.423	57 964 587 220

6.7. 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 indicate that, for many polynomials whose coefficients satisfy linear recurrences, their subresultants have coefficients that also obey such recurrences; this leaves hope that their computation can be performed in linear time. We plan to study such generalizations in a future work.

For the time being, we performed promising experiments for subresultants of generalized Laguerre polynomials (Szegő, 1939, §5.1), defined by

$$L_n^{(\alpha)}(x) = \sum_{i=0}^{n} \binom{n+\alpha}{n-i} \frac{(-x)^i}{i!},$$

and on classical Hermite polynomials (Szegő, 1939, §5.5), defined by

$$H_{2n}(x) = (2n)! \sum_{m=0}^{n} \frac{(-1)^m}{m!(2n-2m)!} (2x)^{2n-2m}.$$

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

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

Baker Jr., G.A., 1975. The Essentials of Padé Approximants. Academic Press, New York. xi+306 pp.

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

Bostan, A., D'Andrea, C., Krick, T., Szanto, A., Valdettaro, M., 2017. Subresultants in multiple roots: an extremal case. Linear Algebra Appl. 529 (3), 185–198. https://doi.org/10.1016/j.laa.2017.04.019.

Collins, G.E., 1967. Subresultants and reduced polynomial remainder sequences. J. ACM 14 (1), 128–142. https://doi.org/10.1145/321371.321381.

Collins, G.E., 1973. Computer algebra of polynomials and rational functions. Am. Math. Mon. 80, 725–755. https://doi.org/10.2307/2318161.

Collins, G.E., 1974. Quantifier elimination for real closed fields by cylindrical algebraic decomposition–preliminary report. SIGSAM Bull. 8 (3), 80–90. https://doi.org/10.1145/1086837.1086852.

Erdélyi, A., Magnus, W., Oberhettinger, F., Tricomi, F.G., 1953. Higher Transcendental Functions, vol. II. McGraw-Hill. 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/.

Euler, L., 1778. Specimen transformationis singularis serierum. Nova Acta Academiae Scientiarum Imperialis Petropolitinae 12, 58–70. Written in 1778, published in 1794. Reprinted in Opera Omnia Series 1, vol 16, part 2, pp. 41–55, B. G. Teubner, Berlin, 1935. Eneström number E710. http://eulerarchive.maa.org/tour/tour_08.html.

von zur Gathen, J., Lücking, T., 2003. Subresultants revisited. Theor. Comput. Sci. 297 (1–3), 199–239. https://doi.org/10.1016/S0304-3975(02)00639-4.

von zur Gathen, J., Gerhard, J., 2013. Modern Computer Algebra, 3rd Edition. Cambridge University Press.

Gomilko, O., Greco, F., Ziętak, K., 2012. A Padé family of iterations for the matrix sign function and related problems. Numer. Linear Algebra Appl. 19 (3), 585–605. https://doi.org/10.1002/nla.786.

Habicht, W., 1948. Eine Verallgemeinerung des Sturmschen Wurzelzählverfahrens. Comment. Math. Helv. 21, 99–116. https://link.springer.com/article/10.1007/BF02568028.

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

Householder, A.S., 1968. Bigradients and the problem of Routh and Hurwitz. SIAM Rev. 10 (1), 56–66. https://doi.org/10.1137/1010003.

Iserles, A., 1979. A note on Padé approximations and generalized hypergeometric functions. BIT Numer. Math. 19 (4), 543–545. https://doi.org/10.1007/BF01931272.

Jacobi, C.G.J., 1836. De eliminatione variabilis e duabus aequationibus algebraicis. J. Reine Angew. Math. 15, 101–124. https://doi.org/10.1515/crll.1836.15.101.

Jacobi, C.G.J., 1859. Untersuchungen über die Differentialgleichung der hypergeometrischen Reihe. J. Reine Angew. Math. 56, 149–165. http://eudml.org/doc/147752.

Koornwinder, T.H., 1984. Orthogonal polynomials with weight function $(1-x)^\alpha(1+x)^\beta + M\delta(x+1) + N\delta(x-1)$. Can. Math. Bull. 27 (2), 205–214. https://doi.org/10.4153/CMB-1984-030-7.

Laguerre, E., 1885. Sur la réduction en fractions continues d'une fraction qui satisfait à une équation différentielle linéaire du premier ordre dont les coefficients sont rationnels. J. Math. Pures Appl. 4e sér. 1, 135–166. http://sites.mathdoc.fr/JMPA/PDF/JMPA_1885_4_1_A5_0.pdf.

Lecerf, G., 2019. On the complexity of the Lickteig-Roy subresultant algorithm. J. Symb. Comput. 92, 243–268. https://doi.org/10.1016/j.jsc.2018.04.017.

Loos, R., 1983. Generalized polynomial remainder sequences. In: Computer Algebra. In: Part of the Computing Supplementa Book Series, vol. 4, pp. 115–137.

Lickteig, T., Roy, M.-F., 2001. Sylvester-Habicht sequences and fast Cauchy index computation. J. Symb. Comput. 31 (3), 315–341. https://doi.org/10.1006/jsco.2000.0427.

Mishra, B., 1993. Algorithmic Algebra. Texts and Monographs in Computer Science. Springer-Verlag, New York. xii+416 pp.

Padé, H., 1901. Sur l'expression générale de la fraction rationnelle approchée de $(1+x)^m$. C. R. Acad. Sci. Paris 132, 754–756. http://gallica.bnf.fr/ark:/12148/bpt6k30888/f802.item.

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

Reischert, D., 1997. Asymptotically fast computation of subresultants. In: Proceedings ISSAC'97. ACM, New York, pp. 233–240.

Salvy, B., Zimmermann, P., 1994. GFUN: a Maple package for the manipulation of generating and holonomic functions in one variable. ACM Trans. Math. Softw. 20 (2), 163–177. http://dl.acm.org/citation.cfm?id=178368.

Strassen, V., 1976. Einige Resultate über Berechnungskomplexität. Jber. Deutsch. Math.-Verein 78 (1), 1–8. http://eudml.org/doc/146659.

Sylvester, J.J., 1839. Memoir on rational derivation from equations of coexistence, that is to say, a new and extended theory of elimination. Philos. Mag. 15, 428–435. Also appears in the Collected Mathematical Papers of James Joseph Sylvester, vol. 1, Chelsea Publishing Co., 1973, pp. 40–46. http://doi.org/10.1080/14786443908649916.

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

Szegő, G., 1939. Orthogonal Polynomials, 4th ed. Amer. Math. Soc., Providence, RI. https://bookstore.ams.org/coll-23, 1975.
Valdettaro, Marcelo A., 2017. Fórmulas en raíces para las subresultantes. Tesis Doctoral. Universidad de Buenos Aires, Facultad de Ciencias Exactas y Naturales. http://cms.dm.uba.ar/academico/carreras/doctorado/tesis-Valdettaro.pdf.
Wilf, H.S., Zeilberger, D., 1992. An algorithmic proof theory for hypergeometric (ordinary and “q”) multisum/integral identities. Invent. Math. 108 (3), 575–633. https://doi.org/10.1007/BF02100618.
Zeilberger, D., 1991. The method of creative telescoping. J. Symb. Comput. 11 (3), 195–204. https://doi.org/10.1016/S0747-7171(08)80044-2.