http://dx.doi.org/10.1016/j.laa.2009.08.012

Linear Algebra and its Applications xxx (2009) xxx–xxx

Contents lists available at ScienceDirect

Linear Algebra and its Applications

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

Bounds for resultants of univariate and bivariate polynomials

Yuval Bistritz*, Alexander Lifshitz

Department of Electrical Engineering, Tel Aviv University, Tel Aviv 69978, Israel

ARTICLE INFO

Article history:
Received 23 August 2008
Accepted 3 August 2009
Available online xxxx

Submitted by V. Olshevsky

AMS classification:
11C20
11S05
15A60
13F20

Keywords:
Resultant
Sylvester matrix
Bezoutian
Hadamard bound

ABSTRACT

The paper considers bounds on the size of the resultant for univariate and bivariate polynomials. For univariate polynomials we also extend the traditional representation of the resultant by the zeros of the argument polynomials to formal resultants, defined as the determinants of the Sylvester matrix for a pair of polynomials whose actual degree may be lower than their formal degree due to vanishing leading coefficients. For bivariate polynomials, the resultant is a univariate polynomial resulting by the elimination of one of the variables, and our main result is a bound on the largest coefficient of this univariate polynomial. We bring a simple example that shows that our bound is attainable and that a previous sharper bound is not correct.

1. Introduction

The resultant is an algebraic tool used for analysis and derivation of various algorithms associated with the greatest common divisor (gcd) problem. It is a classical concept that has been formulated originally for a pair of polynomials by Euler and Bezout in the 18th century. Even with this respectable age the resultant is a young addendum to the gcd problem that has been traced back to an algorithm for finding common factor of integers in Euclid's book *Elements* c. 300 BC. The resultant made a wide impact on many algebraic algorithms and today it has generalizations to more than two polynomials, to matrix and to multivariate polynomials. A revived interest in it stems from the instrumental role it was found to play in adjusting gcd related algorithms to modern symbolic computation environments.

* Corresponding author.
E-mail addresses: bistritz@eng.tau.ac.il (Y. Bistritz), alex_lif@yahoo.com (A. Lifshitz).

0024-3795/$ - see front matter © 2009 Elsevier Inc. All rights reserved.
doi:10.1016/j.laa.2009.08.012

Let $\mathbb{F}$ be an arbitrary field, and let

$$\begin{aligned} a(z) &= a_m z^m + a_{m-1} z^{m-1} + \cdots + a_0 \\ b(z) &= b_n z^n + b_{n-1} z^{n-1} + \cdots + b_0 \end{aligned} \tag{1}$$

be two (univariate) polynomials of degree m and n in $\mathbb{F}[z]$.

Definition 1. The resultant of $a(z)$ and $b(z)$, denoted by $\mathcal{R}(a,b)$, is the smallest degree polynomial of the variables $\{a_i,\ i = 0,\ldots,m\}$ and $\{b_i,\ i = 0,\ldots,n\}$ that vanishes if, and only if, $a(z)$ and $b(z)$ have a common zero.

It is possible to obtain expressions for the resultant in terms of the zeros of one of the polynomials or both. Let the factorization of the polynomials in (1) be

$$\begin{aligned} a(z) &= a_m \prod_{i=1}^{m} (z - \alpha_i) \\ b(z) &= b_n \prod_{i=1}^{n} (z - \beta_i) \end{aligned} \tag{2}$$

where $\{\alpha_i\}_{i=1}^m,\ \{\beta_i\}_{i=1}^n \in \mathbb{K} \supseteq \mathbb{F}$ are the zeros of $a(z)$ and $b(z)$, respectively.

Theorem 1. *The resultant for the two polynomials $a(z)$ and $b(z)$ (1) with zeros as in (2) may be expressed by any of the following three expressions*:

$$\mathcal{R}(a,b) = a_m^n \prod_{i=1}^{m} b(\alpha_i) \tag{3}$$

$$\mathcal{R}(a,b) = (-1)^{mn} b_n^m \prod_{i=1}^{n} a(\beta_i) \tag{4}$$

$$\mathcal{R}(a,b) = a_m^n b_n^m \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j) \tag{5}$$

A simple derivation of (3) and (4) from Definition 1 is given in [1]. The third expression (5) follows by substitution of (2) into (3).

There are other expressions for the resultant that do not involve the value of the zeros of its argument polynomials and thus emphasize better its purely algebraic entity. They present the resultant by determinants of certain matrices that are easily formed from the coefficients of the polynomials. They can be classified into two types: one that has become associated with the name of Sylvester and another that was devised by Bézout. In his celebrated paper of 1764 [2] (whose title is apparently the source for the term resultant), Bézout considered two ways to construct $\mathcal{R}(a,b)$. The first, that follows a paper that Euler published earlier (in 1748), expresses $\mathcal{R}(a,b)$ by the determinant of a matrix of size $n+m$. The second expresses $\mathcal{R}(a,b)$ by the determinant of an abridged matrix whose size is only $max(m,n)$ known today as the Bézoutian matrix, a name given to it already by Sylvester [3].

Euler constructed for the pair of polynomials $a(z)$ and $b(z)$ (1) the following matrix of size $(n+m)$,

$$\mathrm{Syl}(a,b) = \begin{pmatrix} a_m a_{m-1} \ldots a_0 & & \\ & a_m a_{m-1} \ldots a_0 & \\ & \ldots & \\ & & a_m a_{m-1} \ldots a_0 \\ b_n b_{n-1} \ldots b_0 & & \\ & b_n b_{n-1} \ldots b_0 & \\ & \ldots & \\ & & b_n b_{n-1} \ldots b_0 \end{pmatrix} \begin{matrix} \left.\begin{matrix} \\ \\ \\ \\ \end{matrix}\right\} n \text{ rows} \\ \left.\begin{matrix} \\ \\ \\ \\ \end{matrix}\right\} m \text{ rows} \end{matrix} \tag{6}$$

Please cite this article in press as: Y. Bistritz, A. Lifshitz, Bounds for resultants of univariate and bivariate polynomials, Linear Algebra Appl. (2009), doi:10.1016/j.laa.2009.08.012

(regard blank spaces as filled with zeros) whose determinant is equal to the resultant,

$$\mathcal{R}(a,b)=\det \mathrm{Syl}(a,b) \tag{7}$$

The matrix (6) is called today the Sylvester matrix. For a simple proof that the presentation of $\mathcal{R}(a,b)$ by (7) is commensurate with Definition 1, see [1]. The above expression makes apparent that $\mathcal{R}(a,b)$ is a polynomial whose variables are the coefficients a_i and b_i of the two polynomials but, by comparison with the expressions in Theorem 1, obscures its common zero detection property. It is possible, as some texts do, to take Eqs. (6) and (7) as *definition* for the resultant and then proceed from there to show equivalence with Definition 1, with the expressions in Theorem 1, or to show just the corollary "$\mathcal{R}(a,b)=0$ if and only if the two polynomials have a common zero", see [4,5] for proofs of some of these direction.

The three expressions in Theorem 1 are the most transparent demonstration of the ability of the resultant to detect common zeros of the two polynomials. But they do not offer a convenient expression to derive the resultant when the zeros are not known. Most applications of the resultant use the determinant of the Sylvester or the Bezout matrix. Nevertheless, the expressions in Theorem 1 do play a constructive role in the derivation of new algorithms associated with resultants. In fact, the extension presented in this paper of expressions for Theorem 1 to resultant of polynomials that occasionally may have vanishing leading coefficients stems from a need for these generalized expressions that we encountered during a certain study (more on that in a moment) that we could not find in the literature.

The paper will also consider resultants for bivariate polynomials. Given two bivariate polynomials $P(s,z), Q(s,z)\in\mathbb{F}[s,z]$,

$$\begin{aligned} P(s,z) &= \sum_{i=0}^{m_s}\sum_{j=0}^{m_z} p_{i,j}s^iz^j \\ Q(s,z) &= \sum_{i=0}^{n_s}\sum_{j=0}^{n_z} p_{i,j}s^iz^j \end{aligned} \tag{8}$$

their resultant is defined by the determinant of a corresponding Sylvester matrix, by regarding the each bivariate polynomial as univariate polynomial in one of the variables (the 'primary' variable) with coefficients that are univariate polynomials of the other ('secondary') variable. This means that it is possible to form for the pair of polynomials (8) two different resultants, $\mathcal{R}_z(P,Q)$ that takes z as the primary variable and is a (univariate) polynomial in s, and $\mathcal{R}_s(P,Q)$ that takes s as the primary variable and is a polynomial in z.

It is noticed that the expressions in Theorem 1 require polynomials with non-vanishing leading coefficients. In difference, the expression of the resultant by the Sylvester matrix is more tolerant to vanishing leading coefficients. Consequently, it is possible to use the Sylvester formulation to define the resultant for also polynomials that are degree deficient (i.e. polynomials with actual degree lower than their formally assumed degree). The resulting extension, to which we refer as *formal resultant*, is useful in automated evaluation of resultants because it allows a same procedure to proceed also when occasionally one of the input polynomials has a vanishing leading coefficients. The paper will extend the expressions in Theorem 1 and some more properties of the resultant to formal resultants.

Often algorithms associated with the resultant require a known-in-advance bound on the maximal size of the resultant. Such a requirement arises when devising of a procedure to compute the resultants (or an algorithm related to it) with modular arithmetics (in order to speed it up, to increase computation accuracy or to carry it out on a restricted platform). The paper will derive predeterminable bounds on the magnitude of univariate and bivariate resultants.

This paper will use only Sylvester formulation. Since the Bezoutian and Sylvester matrix provide equivalent ways to express the resultant, it is in order to point out differences between the Sylvester and the Bezout matrices that affect their relative suitability for certain tasks. It is usually more convenient to express stability conditions for discrete-time or continuous-time linear systems by positive definiteness of corresponding Bezout matrices than stating it on a sequence of determinants of corresponding submatrices of the Sylvester matrix. Algorithms to test stability can also be nicely related to triangular factorization of a corresponding Bezout matrices [6]. However, the process of reducing the size from the Sylvester matrix to the Bezout matrix creates a matrix whose entries are no longer a simple layout of the polynomial coefficients. The simple exhibition of the polynomial coefficients is often a desirable asset. The Sylvester formulation has been proved useful in establishing efficient gcd algorithm over integral domains [7–9]. It was also used successfully in [10] to show that a modified form of the Schur unit-circle stability test, known as the modified Jury test, is integer preserving and subsequently to implement it with modular arithmetics.

The content of this paper stems from needs that we encountered during work on the implementation in modular arithmetics of the stability (and unit-circle zero location) test for one-dimensional discrete-time system in [11] and the stability test for two-dimensional discrete-time systems in [12]. The goal of that study (yet to be published) is to enhance these procedures (already recognized as the most efficient procedures for their tasks in terms of conventional counts of arithmetical operations) by versions that are immune to numerical inaccuracy and hardware limitations. Formal resultants arise in the analysis of the zero location procedure [11] because it admits degree-deficient polynomial. Bivariate resultants occur in the corresponding two-dimensional stability test [12] because it follows the interpolation of a scheme that acts like a stability test of a univariate polynomial with coefficients that are polynomials in the second variable. However, the scope of presentation in this paper is not restricted to the immediate needs that motivated it. We bring a fairly general setting that should render the content useful for more applications. Needless to say that even tough we use only the Sylvester formulation, the bounds and other results, once established, apply also for expressing the resultants by matching Bezoutians.

The paper is constructed as follows. The next section considers resultant of univariate polynomials and brings bound and other properties for a formal resultant. The third section considers resultants for bivariate polynomials. It first obtains a bound on the determinant of an arbitrary (univariate) polynomial matrix and then derives a max-norm bound for the polynomial resultant of two bivariate polynomials.

2. Univariate polynomials

Let $\mathbb{F}$ be an arbitrary field, and let

$$a(z) = a_m z^m + a_{m-1} z^{m-1} + \cdots + a_0$$

be a polynomial in $\mathbb{F}[z]$, where we want *not* to exclude the possibility that $a_m = 0$. For a polynomial $a(z)$ written in the above form, m is called the *formal degree* of $a(z)$ and a_m is its *formal leading coefficient*. If the formal leading coefficient is different from zero, then the polynomial is said to be of *full degree*. If, on the other hand, $a_m = a_{m-1} = \cdots = a_{m-\lambda_a+1} = 0$ and $a_{m-\lambda_a} \neq 0$, then $a(z)$ is said to be *degree-deficient* and λ_a is the degree deficiency of $a(z)$. Clearly, $\lambda_a = \operatorname{fdeg} a - \deg a$, where $\operatorname{fdeg} a$ is the formal degree and $\deg a$ is the actual degree of $a(z)$.

Theorem 1 provides relationship between the resultant and zeros of $a(z)$ and $b(z)$ with restriction to full-degree polynomials. In difference, the expression of the resultant by Eqs. (6) and (7) has a larger capacity to evaluate the resultant because it does not involve the zeros of the polynomial. In automated evaluation of the resultant one wants to have a same routine to evaluate the resultant of any pair of polynomials $a(z)$ and $b(z)$ of degrees m and n, irrespective of whether the formal leading coefficient vanishes or not. We cover this extension by the term *formal resultant*.

Let $a(z)$ and $b(z)$ be two polynomials in $\mathbb{F}[z]$ with formal degree m and n and degree deficiency of $\lambda_a \geqslant 0$ and $\lambda_b \geqslant 0$ respectively, and let $\mathbb{K}$ be a field ($\mathbb{K} \supseteq \mathbb{F}$) such that $a(z)$ and $b(z)$ can be factored into linear terms over $\mathbb{K}$

$$\begin{aligned} a(z) &= a_{m-\lambda_a} \prod_{i=1}^{m-\lambda_a} (z - \alpha_i) \\ b(z) &= b_{n-\lambda_b} \prod_{i=1}^{n-\lambda_b} (z - \beta_i) \end{aligned} \tag{9}$$

where $\{\alpha_i\}_{i=1}^{m-\lambda_a} \in \mathbb{K}$ and $\{\beta_i\}_{i=1}^{n-\lambda_b} \in \mathbb{K}$ are zeros of $a(z)$ and $b(z)$ respectively.

Definition 2. We call $\mathcal{R}(a, b)$, defined for polynomials (9) by Eqs. (6) and (7), a formal resultant when the two polynomials are not declared as full-degree polynomials.

We next obtain extension of the expressions in Theorem 1 to a formal resultant.

Theorem 2. *The formal resultant* $\mathcal{R}(a,b)$ *for the polynomials* (9) *may be expressed by any of the following three expressions (to be read with* $0^0=1$*).*

$$\mathcal{R}(a,b)=(-1)^{n\lambda_a}a_m^{\lambda_b}b_n^{\lambda_a}a_{m-\lambda_a}^{n-\lambda_b}\prod_{i=1}^{m-\lambda_a}b(\alpha_i) \tag{10}$$

$$\mathcal{R}(a,b)=(-1)^{n\lambda_a+(m-\lambda_a)(n-\lambda_b)}a_m^{\lambda_b}b_n^{\lambda_a}b_{n-\lambda_b}^{m-\lambda_a}\prod_{i=1}^{n-\lambda_b}a(\beta_i) \tag{11}$$

$$\mathcal{R}(a,b)=(-1)^{n\lambda_a}a_m^{\lambda_b}b_n^{\lambda_a}a_{m-\lambda_a}^{n-\lambda_b}b_{n-\lambda_b}^{m-\lambda_a}\prod_{i=1}^{m-\lambda_a}\prod_{j=1}^{n-\lambda_b}(\alpha_i-\beta_j) \tag{12}$$

Proof. Denote by $\hat{a}(z)$ and $\hat{b}(z)$ the polynomials $a(z)$ and $b(z)$ with respect to their nominal degrees. The resultant $\mathcal{R}(\hat{a},\hat{b})$ is equal to the determinant of the corresponding Sylvester matrix of size $m-\lambda_a+n-\lambda_b$

$$\mathrm{Syl}(\hat{a},\hat{b})=\begin{pmatrix} a_{m-\lambda_a}a_{m-\lambda_a-1}\dots a_0 & & & \\ & a_{m-\lambda_a}a_{m-\lambda_a-1}\dots a_0 & & \\ & \dots & & \\ & & a_{m-\lambda_a}a_{m-\lambda_a-1}\dots a_0 & \\ b_{n-\lambda_b}b_{n-\lambda_b-1}\dots b_0 & & & \\ & b_{n-\lambda_b}b_{n-\lambda_b-1}\dots b_0 & & \\ & \dots & & \\ & & b_{n-\lambda_b}b_{n-\lambda_b-1}\dots b_0 & \end{pmatrix}\begin{array}{l}\left.\vphantom{\begin{matrix}1\\1\\1\\1\end{matrix}}\right\}\quad n-\lambda_b\text{ rows}\\ \left.\vphantom{\begin{matrix}1\\1\\1\\1\end{matrix}}\right\}\quad m-\lambda_a\text{ rows}\end{array} \tag{13}$$

By applying Theorem 1 to $\hat{a}(z)$ and $\hat{b}(z)$ we have

$$\mathcal{R}\left(\hat{a},\right)\hat{b}=a_{m-\lambda_a}^{n-\lambda_b}\prod_{i=1}^{m-\lambda_a}b(\alpha_i)$$

$$\mathcal{R}\left(\hat{a},\right)\hat{b}=(-1)^{(m-\lambda_a)(n-\lambda_b)}b_{n-\lambda_b}^{m-\lambda_a}\prod_{i=1}^{n-\lambda_b}a(\beta_i)$$

Thus, by comparing these equations to Eqs. (10) and (11), we must show that

$$\det\mathrm{Syl}(a,b)=(-1)^{n\lambda_a}a_m^{\lambda_b}b_n^{\lambda_a}\det\mathrm{Syl}(\hat{a},\hat{b}) \tag{14}$$

For simplicity of the following, we specify submatrices of $\mathrm{Syl}(a,b)$ by participating columns and rows. For example, in terms of this convention,

$$\mathrm{Syl}(a,b)\equiv S_{a,b}(1:m+n,1:m+n)$$

For the proof of (10) and (11) we consider in the following four cases.

<u>*Case 1*</u>: $\lambda_a=0,\lambda_b>0$.

In this case we must show that $\det\mathrm{Syl}(a,b)=a_m^{\lambda_b}\det\mathrm{Syl}(\hat{a},\hat{b})$. Since each submatrix $S_{a,b}(k:m+n,k:m+n)$ for $1\leqslant k\leqslant\lambda_b$ has only one non-zero element in the first column ($S_{a,b}(k,k)=a_m$), then by successive expansion of the determinant $\det\mathrm{Syl}(a,b)$ along the first column of each submatrix we obtain

$$\begin{aligned}&\det S_{a,b}(1:m+n,1:m+n)\\ &\quad=a_m\det S_{a,b}(2:m+n,2:m+n)\\ &\quad\dots\end{aligned}$$

ARTICLE IN PRESS
http://dx.doi.org/10.1016/j.laa.2009.08.012

$$\begin{aligned}
&= a_m^{\lambda_b} \det S_{a,b}(\lambda_b + 1 : m + n, \lambda_b + 1 : m + n) \\
&= a_m^{\lambda_b} \det \mathrm{Syl}(\hat{a}, \hat{b})
\end{aligned}$$

<u>Case 2</u>: $\lambda_a > 0, \lambda_b = 0$.

In this case we must show that $\det \mathrm{Syl}(a, b) = (-1)^{n\lambda_a} b_n^{\lambda_a} \det \mathrm{Syl}(\hat{a}, \hat{b})$. Since each submatrix $S_{a,b}([1 : n, n + k : m + n], k : m + n)$ for $1 \leqslant k \leqslant \lambda_b$ has only one non-zero element in the first column ($S_{a,b}(n + k, k) = b_n$), then by successive expansion of the determinant $\det \mathrm{Syl}(a, b)$ along the first column of each submatrix we obtain

$$\begin{aligned}
&\det S_{a,b}(1 : m + n, 1 : m + n) \\
&\quad = (-1)^{n+2} b_n \det S_{a,b}([1 : n, n + 2 : m + n], 2 : m + n) \\
&\quad \ldots \\
&\quad = [(-1)^{n+2} b_n]^{\lambda_a} \det S_{a,b}([1 : n, n + 1 + \lambda_a : m + n], \lambda_a + 1 : m + n) \\
&\quad = (-1)^{n\lambda_a} b_n^{\lambda_a} \det \mathrm{Syl}(\hat{a}, \hat{b})
\end{aligned}$$

<u>Case 3</u>: $\lambda_a > 0, \lambda_b > 0$.

Since $a_m = b_n = 0$, the resultant must be zero.

$$\det \mathrm{Syl}(a, b) = (-1)^{n\lambda_a} 0^{\lambda_b} 0^{\lambda_a} \det \mathrm{Syl}(\hat{a}, \hat{b}) = 0$$

<u>Case 4</u>: $\lambda_a = 0, \lambda_b = 0$.

Since $\hat{a}(z) = a(z)$ and $\hat{b}(z) = b(z)$, we must have $\mathrm{Syl}(a, b) = \mathrm{Syl}(\hat{a}, \hat{b})$

$$\det \mathrm{Syl}(a, b) = (-1)^{n\lambda_a} a_m^0 b_n^0 \det \mathrm{Syl}(\hat{a}, \hat{b}) = \det \mathrm{Syl}(\hat{a}, \hat{b})$$

This completes the proofs for (10) and (11). Finally, evaluating $b(z)$ in (9) at $z = \alpha_i$ we obtain

$$b(\alpha_i) = b_{n-\lambda_b} \prod_{j=1}^{n-\lambda_b} (\alpha_i - \beta_j)$$

Substituting $b(\alpha_i)$ into (10) gives

$$\begin{aligned}
\mathcal{R}(a, b) &= (-1)^{n\lambda_a} a_m^{\lambda_b} b_n^{\lambda_a} a_{m-\lambda_a}^{n-\lambda_b} \prod_{i=1}^{m-\lambda_a} b_{n-\lambda_b} \prod_{j=1}^{n-\lambda_b} (\alpha_i - \beta_j) \\
&= (-1)^{n\lambda_a} a_m^{\lambda_b} b_n^{\lambda_a} a_{m-\lambda_a}^{n-\lambda_b} b_{n-\lambda_b}^{m-\lambda_a} \prod_{i=1}^{m-\lambda_a} \prod_{j=1}^{n-\lambda_b} (\alpha_i - \beta_j)
\end{aligned}$$

This proves (12). □

The expressions (10)–(12) form the extension to degree-deficient polynomials of the expressions (3)–(5), respectively.

Theorem 2 implies readily the next conclusion.

Theorem 3. *Let $a(z)$ and $b(z)$ be polynomials in $\mathbb{F}[z]$ of formal degrees m and n and degree deficiency of $\lambda_a \geqslant 0$ and $\lambda_b \geqslant 0$, respectively. Their formal resultant $\mathcal{R}(a, b) = 0$ if, and only if, $a(z)$ and $b(z)$ have at least one common (finite) zero or are both degree-deficient polynomials ("have at least one common zero at infinity").*

We bring two more useful properties of the formal resultant.

Theorem 4. *Let $a(z), b(z) \in \mathbb{F}[z]$ with* fdeg $a = m$, fdeg $b = n$, *then*

$$\mathcal{R}(b,a) = (-1)^{mn}\mathcal{R}(a,b)$$

Proof. Evaluating (12) with a and b reversed gives

$$\begin{aligned}\mathcal{R}\,(b,a) &= (-1)^{m\lambda_b} a_m^{\lambda_b} b_n^{\lambda_a} a_{m-\lambda_a}^{n-\lambda_b} b_{n-\lambda_b}^{m-\lambda_a} \prod_{i=1}^{m-\lambda_a}\prod_{j=1}^{n-\lambda_b}(\beta_j - \alpha_i)\\ &= (-1)^{m\lambda_b+(n-\lambda_b)(m-\lambda_a)} a_m^{\lambda_b} b_n^{\lambda_a} a_{m-\lambda_a}^{n-\lambda_b} b_{n-\lambda_b}^{m-\lambda_a} \prod_{i=1}^{m-\lambda_a}\prod_{j=1}^{n-\lambda_b}(\alpha_i - \beta_j)\\ &= (-1)^{n\lambda_a+mn} a_m^{\lambda_b} b_n^{\lambda_a} a_{m-\lambda_a}^{n-\lambda_b} b_{n-\lambda_b}^{m-\lambda_a} \prod_{i=1}^{m-\lambda_a}\prod_{j=1}^{n-\lambda_b}(\alpha_i - \beta_j)\\ &= (-1)^{mn}\mathcal{R}(a,b) \qquad \square\end{aligned}$$

Theorem 5. *Let $K_1, K_2 \in \mathbb{F}$ and $a(z), b(z) \in \mathbb{F}[z]$ with* fdeg $a = m$, fdeg $b = n$, *then*

$$\mathcal{R}\,(K_1 a, K_2 b) = K_1^n K_2^m \mathcal{R}(a,b)$$

Proof. Follows immediately by direct substitution into (6) and taking K_1 and K_2 out of determinant or by a straightforward evaluation of (10). □

Note that the last couple of properties bear for formal resultants the same appearance as for normal (i.e. full-degree polynomials) resultants.

In the remaining of this section we want to derive bounds on the size of a formal resultant. To this end, we shall assume polynomials that are defined over $\mathbb{C}$, the field of complex numbers. The bound will be on the absolute value of $\mathcal{R}(a,b)$ as function of the Euclidean norm (2-norm) or the max-norm of its argument polynomials.

Definition 3. The *2-norm* (or Euclidean norm) $\|\cdot\|_2$ of a polynomial $d(s) = \sum_{k=0}^{N} d_k s^k \in \mathbb{C}[s]$ is defined as the scalar $\|d\|_2 = \left(\sum_{k=0}^{N} |d_k|^2\right)^{1/2}$.

Definition 4. The *max-norm* (or ∞-norm) $\|\cdot\|_\infty$ of a polynomial $d(s) = \sum_{k=0}^{N} d_k s^k \in \mathbb{C}[s]$ is defined as the scalar $\|d\|_\infty = \max\{|d_k| : 0 \leqslant k \leqslant N\}$.

Theorem 6 (Hadamard's bound). *Let S be a square matrix of size N. Then the absolute value of its determinant is bounded by*

$$|\det(S)| \leqslant \prod_{i=1}^{N}\left(\sum_{j=1}^{N}|s_{ij}|^2\right)^{1/2} = \prod_{i=1}^{N}\|s_i\|_2 \tag{15}$$

where s_i is the ith row of S.

Proof. The following proof is due to Knuth [13]. Consider the matrix $C = SS^H$. Clearly, $\det(C) = |\det(S)|^2$. Each element of the matrix C is given by $c_{ij} = \sum_{k=1}^{N} s_{ik}s_{jk}^*$. In particular, $c_{ii} = \sum_{k=1}^{N}|s_{ik}|^2$. Thus, in terms of elements of C we must show that

$$|\det(S)|^2 = \det(C) \leqslant \prod_{i=1}^{N} c_{ii}$$

We may assume that $c_{ii} > 0$ for all i. If $c_{ij} \neq 0$ for some $i \neq j$, we can replace row i of matrix S by $(s_{i1} - \gamma s_{j1} \cdots s_{iN} - \gamma s_{jN})$, where $\gamma = c_{ij}/c_{jj}$. This operation has the effect of Gauss elimination on matrix C and does not change the value of the determinant of S. It can be readily shown that it acts to replace the value of c_{ii} by the smaller value $c_{ii} - |c_{ij}|^2/c_{jj}$ so it tends to sharpen the bound. These replacements can be performed in a systematic way for increasing i and for $j < i$ until the matrix C is diagonal and its determinant is given by the product of its elements on the main diagonal. □

Theorem 7 (Bound for univariate polynomials resultant). *Let $a = \sum_{j=0}^{m} a_j z^j$ and $b = \sum_{j=0}^{n} q_j z^j$ be two polynomials in $\mathbb{C}[z]$, $\operatorname{fdeg} a = m$, $\operatorname{fdeg} b = n$. An upper bound on the absolute value of the resultant $\mathcal{R}(a,b)$ is given by*

$$|\mathcal{R}(a,b)| \leqslant \|a\|_2^n \|b\|_2^m \leqslant (m+1)^{n/2}(n+1)^{m/2}\|a\|_\infty^n \|b\|_\infty^m \tag{16}$$

Proof. The first inequality follows from applying Eq. (15) to $S = \mathrm{Syl}(a,b)$, the Sylvester matrix for the polynomials $a(z)$ and $b(z)$ of the form (6) and the fact that $\mathcal{R}(a,b) = \det \mathrm{Syl}(a,b)$. The second inequality uses the inequality $\|a\|_2 \leqslant (m+1)^{1/2}\|a\|_\infty$ that holds for any polynomial a of degree m. □

3. Bivariate polynomials

The resultant for a pair of bivariate polynomials (8), can be defined in two different ways, depending on the variable that is eliminated. To be specific, we shall consider the resultant $\mathcal{R}_z(P,Q)$ of $P(s,z)$ and $Q(s,z)$ that represents the elimination of the variables z. This resultant is defined as follows. First, the two polynomials are written as univariate polynomials in z with coefficients that are polynomials in s, vis.

$$P(s,z) = \sum_{j=0}^{m_z} p_j(s) z^j$$

$$Q(s,z) = \sum_{j=0}^{n_z} q_j(s) z^j$$

where $\deg p_j(s) \leqslant m_s, 0 \leqslant j \leqslant m_z$ and $\deg q_j(s) \leqslant n_s, 0 \leqslant j \leqslant n_z$. Then, the Sylvester matrix (6) becomes

$$\mathrm{Syl}(P,Q) = \left(\begin{array}{l} p_{m_z}(s)p_{m_z-1}(s)\ldots p_0(s) \\ \quad p_{m_z}(s)p_{m_z-1}(s)\ldots p_0(s) \\ \qquad \ldots \\ \qquad\quad p_{m_z}(s)p_{m_z-1}(s)\ldots p_0(s) \\ q_{n_z}(s)q_{n_z-1}(s)\ldots q_0(s) \\ \quad q_{n_z}(s)q_{n_z-1}(s)\ldots q_0(s) \\ \qquad \ldots \\ \qquad\quad q_{n_z}(s)q_{n_z-1}(s)\ldots q_0(s) \end{array}\right) \begin{array}{l} \left.\begin{array}{l} \\ \\ \\ \\ \end{array}\right\} \quad n_z \text{ rows} \\ \left.\begin{array}{l} \\ \\ \\ \\ \end{array}\right\} \quad m_z \text{ rows} \end{array} \tag{17}$$

The resultant $\mathcal{R}_z(P,Q)$ is defined by

$$\mathcal{R}_z(P,Q) = \det \mathrm{Syl}(P,Q) \tag{18}$$

Since the (non-vanishing) entries of the Sylvester matrix are now polynomials of s, the resultant $\mathcal{R}_z(P,Q)$ is a polynomial in $\mathbb{F}[s]$ that, when convenient, we shall also denote by

$$r(s) = \mathcal{R}_z(P,Q) \tag{19}$$

Theorem 8. *Let $P(s,z), Q(s,z) \in \mathbb{C}[s,z]$ with $\deg_z P = m_z$, $deg_z Q = n_z$ and $\deg_s P = m_s$, $deg_s Q = n_s$ and let $r(s)$ be the resultant of P and Q with respect to z, then*

$$\operatorname{fdeg} r(s) = (m_z + n_z)\max(m_s, n_s) \tag{20}$$

Please cite this article in press as: Y. Bistritz, A. Lifshitz, Bounds for resultants of univariate and bivariate polynomials, Linear Algebra Appl. (2009), doi:10.1016/j.laa.2009.08.012

Proof. This follows from definition (17) noticing that the determinant is formed as sum of entries that each is at most the product of $m_z + n_z$ polynomials from the set of polynomials $p_k(s), 0 \leqslant k \leqslant m_z$ and $q_k(s), 0 \leqslant k \leqslant n_z$ of degree not higher then $\max(m_s, n_s)$. □

The following theorem presents an upper bound on the determinant of an arbitrary polynomial matrix. A bound on the size of the resultant for bivariate polynomials will follow from it as a special case.

Theorem 9 (Bound for the determinant of a polynomial matrix). *Let D be a square matrix of size N with elements in $\mathbb{C}[s]$ given by*

$$D_{i,j}(s) = \sum_{k=0}^{n_s} d_k^{(i,j)} s^k, \quad 1 \leqslant i,j \leqslant N \tag{21}$$

Then the determinant of D is a polynomial $\Delta^{(N)}(s)$ of formal degree $n_s N$, and the maximum absolute value of its coefficients $\|\Delta^{(N)}\|_\infty$ is bounded by

$$\|\Delta^{(N)}\|_\infty \leqslant N!(n_s + 1)^{N-1} \|D\|_\infty^N \tag{22}$$

where $\|D\|_\infty = \max_{i,j,k} |d_k^{(i,j)}|$.

Proof. It is easy to realize that the formal degree of $\Delta^{(N)}(s)$ is $n_s N$. To simplify the proof for (22), we define for an arbitrary polynomial $d(s) = \sum_{k=0}^N d_k s^k$ an operator $\langle | \cdot | \rangle$ as follows

$$\langle |d(s)| \rangle = \sum_{k=0}^{N} |d_k| s^k$$

Expanding the determinant $\Delta^{(N)}(s)$ of formal degree $n_s N$ along the first column of D we obtain

$$\Delta^{(N)}(s) = \sum_{i=1}^{N} (-1)^{i+1} D_{i,1}(s) \Delta_i^{(N-1)}(s)$$

Then,

$$\begin{aligned}
\left\| \left\langle \left| \Delta^{(N)}(s) \right| \right\rangle \right\|_\infty &\leqslant \left\| \sum_{i=1}^{N} \left\langle \left| D_{i,1}(s) \right| \right\rangle \left\langle \left| \Delta_i^{(N-1)}(s) \right| \right\rangle \right\|_\infty \\
&\leqslant N \|D\|_\infty \left\| \left(\sum_{k=0}^{n_s} s^k \right) \max_i \left\langle \left| \Delta_i^{(N-1)}(s) \right| \right\rangle \right\|_\infty \\
&\leqslant N(N-1) \|D\|_\infty^2 \left\| \left(\sum_{k=0}^{n_s} s^k \right)^2 \max_i \left\langle \left| \Delta_i^{(N-2)}(s) \right| \right\rangle \right\|_\infty \\
&\vdots \\
&\leqslant N! \|D\|_\infty^N \left\| \left(\sum_{k=0}^{n_s} s^k \right)^N \right\|_\infty
\end{aligned}$$

where in the above, each line involves expansion of the remaining determinant along its first column. Therefore,

$$\|\Delta^{(N)}\|_\infty = \left\| \left\langle \left| \Delta^{(N)}(s) \right| \right\rangle \right\|_\infty \leqslant N! \left\| \left(\sum_{k=0}^{n_s} s^k \right)^N \right\|_\infty \|D\|_\infty^N$$

Note that $I(n_s,N) := \left\| \left(\sum_{k=0}^{n_s} s^k \right)^N \right\|_\infty$ is a well defined integer function of n_s and N only and consequently the above is already a predeterminable legitimate (and sharper) bound for the determinant of a polynomial matrix. The inequality in (22) follows because $I(n_s,N) \leqslant (n_s+1)^{N-1}$ (strictly for $N > 1$). □

The upper bound on the size of $\mathcal{R}_z(P,Q)$ will be expressed by the max-norm of its bivariate polynomials defined as follows.

Definition 5. The *max-norm* $\|\cdot\|_\infty$ of a bivariate polynomial $T(s,z) = \sum_{i=0}^{M}\sum_{j=0}^{N} t_{i,j}s^i z^j,\ t_{i,j} \in \mathbb{C}$ is defined as the scalar $\|T\|_\infty = \max\{|t_{i,j}| : 0 \leqslant i \leqslant M, 0 \leqslant j \leqslant N\}$.

Theorem 10 (Bound for bivariate polynomials resultant). *Let $P(s,z), Q(s,z) \in \mathbb{C}[s,z]$ with $\deg_z P = m_z, \deg_z Q = n_z$ and $\deg_s P = m_s, \deg_s Q = n_s$. Denote the resultant of P and Q with respect to z as defined in* (17) *and* (18), *by $r(s) = \mathcal{R}_z(P,Q)$. Then*

$$\|r\|_\infty \leqslant (m_z+n_z)!(\max(m_s,n_s)+1)^{m_z+n_z-1}\|P\|_\infty^{n_z}\|Q\|_\infty^{m_z} \tag{23}$$

Proof. By applying the max-norm bound in Theorem 9 to the special case of the determinant of the matrix $\mathrm{Syl}(P,Q)$ with size m_z+n_z and polynomial entries of maximal degree $\max(m_s,n_s)$, we obtain at once the bound

$$\|r\|_\infty \leqslant (m_z+n_z)!(\max(m_s,n_s)+1)^{m_z+n_z-1}\|D\|_\infty^{m_z+n_z} \tag{24}$$

where $\|D\|_\infty = \max(\|P\|_\infty, \|Q\|_\infty)$. The bound (23), that is sharper when $\|P\|_\infty \neq \|Q\|_\infty$, is obtained by adjusting the proof outlined for Theorem 9 to the specifics of the Sylvester matrix (17). In the first n_z inequalities (presenting evaluation of determinants along the first n_z rows) we collect powers of $\|P\|_\infty \left(\sum_{k=0}^{n_s} s^k\right)$ and in the subsequent m_z inequalities (evaluation along the remaining m_z rows) we collect powers of $\|Q\|_\infty \left(\sum_{k=0}^{n_s} s^k\right)$. This gives

$$\|r\|_\infty \leqslant (m_z+n_z)!\|P\|_\infty^{n_z}\|Q\|_\infty^{m_z} \left\| \left(\sum_{k=0}^{m_s} s^k\right)^{n_z} \left(\sum_{k=0}^{n_s} s^k\right)^{m_z} \right\|_\infty \tag{25}$$

Next, use

$$\left\| \left(\sum_{k=0}^{m_s} s^k\right)^{n_z} \left(\sum_{k=0}^{n_s} s^k\right)^{m_z} \right\|_\infty \leqslant I(\max(m_s,n_s), m_z+n_z) \leqslant (\max(m_s,n_s)+1)^{m_z+n_z-1}$$

to obtain (23). □

It is notable that during the above proof we obtained a legitimate predeterminable bound (25) that is usually a strictly sharper bound than (23). However, the simpler looking bound (23) might be good enough for most of its anticipated applications. Usually, the tightness of the bound is not too crucial as long as the bound is valid. For example, suppose one wants to compute the resultant of a pair of integer polynomials using modular arithmetics. A tighter bound may admit the choice of a smaller prime (or relative primes run in parallel) and hence smaller residue numbers. But the smallness of the numbers can also be controlled by increasing the number of modular parallel channels. On the other hand, if these primes are chosen based on an assumed bound that is not true, the recovery of the true numbers from the residues will fail when the computation contains an integer that exceeds the single prime or the product of relative primes.

Numerical example. Consider the following polynomials

$$\begin{aligned} P(s,z) &= 1+s+s^2+(1-s+s^2)z \\ Q(s,z) &= 1-s+s^2-(1+s+s^2)z \end{aligned}$$

For $m_z = n_z = 1, m_s = n_s = 2, \|P\|_\infty = \|Q\|_\infty = 1$ here, (23) predicts for $r(s) = \mathcal{R}_z(P, Q)$ the bound $\|r\|_\infty \leqslant (1+1)!(2+1)^1 \cdot 1 \cdot 1 = 6$. (The two other expressions, (24) and (25), produce the same bound.) Zippel in [1, Proposition 78] proposed the sharper bound $\|r\|_\infty \leqslant (m_z + n_z)!\|P\|_\infty^{n_z}\|Q\|_\infty^{m_z}$ that predicts for this example that $\|r\|_\infty \leqslant 2$. The resultant can be calculated easily for this simple example,

$$r(s) = \det\begin{pmatrix} (1 - s + s^2) & (1 + s + s^2) \\ -(1 + s + s^2) & (1 - s + s^2) \end{pmatrix} = 2 + 6s^2 + 2s^4$$

Thus the currently derived bound is attainable and the previously proposed bound is not correct.

4. Conclusion

We extended the traditional representation of the resultant from full degree polynomials to formal resultants that incorporate the case where the formal leading coefficients of the polynomials may be equal to zero. Expressions for the formal resultant of a pair of univariate polynomials in terms of zeros of the polynomials as well as some more properties were obtained. We also derived bounds on the size of univariate and bivariate resultants that are determinable in advance from the size of their argument polynomials. In the process, we also obtained a bound on the determinant of an arbitrary polynomial matrix. We shall show elsewhere a use of the results in this paper to carry out the unit-circle zero location method in [11] and the stability test for two-dimensional discrete-time systems [12] with modular arithmetics. The present results should prove similarly useful for also other algorithms associated with resultants.

References

[1] R. Zippel, Effective Polynomial Computation, Cornell University, 1994.
[2] É. Bézout, Recherchez sur le degré des équations résultantes de l'évanouissement des inconnues et sur le moyens qu'il convient d'employer pour trouver ces équations, Mem. Acad, Paris (1764) 288–338.
[3] J. Sylvester, On a theory of Syzygetic relations of two rational integral functions, comprising an application to the theory of Sturm functions, and that of the greatest Algebraical Common Measure, Phil. Trans. Roy. Soc. London 143 (1853) 407–548.
[4] M. Mignotte, Mathematics for Computer Algebra, Springer-Verlag, 1992.
[5] S. Basu, R. Pollack, M.-F. Roy, Algorithms in Real Algebraic Geometry, Springer, 2003.
[6] H. Lev-Ari, Y. Bistritz, T. Kailath, Generalized Bézoutians and families of efficient zero-location procedures, IEEE Trans. Circuits Syst. 38 (February) (1991) 170–186.
[7] G.E. Collins, Subresultants and reduced polynomial remainder sequences, J. ACM 14 (January) (1967).
[8] W.S. Brown, On Euclid's algorithm and the computation of polynomial greatest common divisors, J. ACM 18 (October) (1971).
[9] W.S. Brown, J.F. Traub, On Euclid's algorithm and the theory of subresultants, J. ACM 18 (1971).
[10] P.G. Anderson, M.R. Garey, L.E. Heindel, Combinational aspects of deciding if all roots of a polynomial lie within the unit circle, Computing 16 (1976) 293–304.
[11] Y. Bistritz, Zero location of polynomials with respect to the unit-circle unhampered by nonessential singularities, IEEE Trans. Circuits Systems, I: Fundam. Theory Appl. 49 (3) (2002) 305–314.
[12] Y. Bistritz, On testing stability of 2-D discrete systems by a finite collection of 1-D stability tests, IEEE Trans. Circuits Systems, I: Fundam. Theory Appl. 49 (2002) 1634–1638.
[13] D.E. Knuth, The Art of Computer Programming, Seminumerical Algorithms, vol. 2, third ed., Addison-Wesley, 1998.