Matrix Computation of Subresultant Polynomial Remainder Sequences in Integral Domains

Alkiviadis G. Akritas and Evgenia K. Akritas
University of Kansas, Lawrence, USA
and
Genadii I. Malaschonok
Kiev University, Kiev, Ukraine

February 7, 2002

Abstract

We present an improved variant of the matrix-triangularization subresultant prs method [2] for the computation of a greatest common divisor of two polynomials A and B (of degrees m and n, respectively) along with their polynomial remainder sequence. It is improved in the sense that we obtain complete theoretical results, independent of Van Vleck's theorem [13] (which is not always true [1], [6]), and, instead of transforming a matrix of order $2\cdot\max(m,n)$ [2], we are now transforming a matrix of order $m+n$. An example is also included to clarify the concepts.

1 Introduction

Let I be an integral domain, and let

$$A_i = \sum_{j=1}^{m} c_{ij}x^{m-j},$$

where $c_{ij} \in I$, $i = 1, 2, \ldots, n$; then

$$mat(A_1, A_2, \ldots, A_n)$$

denotes the matrix (c_{ij}) of order $n \times m$. Moreover, let $A, B \in I[x], \deg A = m, \deg B = n$ and let

$$\begin{aligned} M_k &= mat(x^{n-k-1}A, x^{n-k-2}A, \ldots, A, x^{m-k-1}B, x^{m-k-2}B, \ldots, B), \\ &\quad 0 \le k < \min(m,n) \end{aligned}$$

be the matrix of order $(m+n-2k) \times (m+n-k)$, where M_0 is the well-known Sylvester's matrix. Then, kth subresultant polynomial of A and B is called the polynomial

$$S_k = \sum_{i=0}^{k} M_k^i x^i,$$

of degree $\leq k$, where M_k^i is a minor of the matrix M_k of order $m+n-2k$, formed by the elements of columns $1, 2, \ldots, m+n-2k-1$ and column $m+n-k-i$. Habicht's known theorem [7] establishes a relation between the subresultant polynomials $S_0, S_1, \ldots, S_{\min(m,n)-1}$ and the polynomial remainder sequence(prs) of A and B, and also demonstrates the so-called *gap* structure. (For a surprisingly simple proof of Habicht's theorem see González et al [6].)

According to the matrix-triangularization subresultant prs method (see for example Akritas' book [1] or papers [2], [3]) all the subresultant polynomials of A and B can be computed *within sign* by transforming the matrix (suggested by Sylvester [12])

$$mat(x^{\max(m,n)-1}A, x^{\max(m,n)-1}B, x^{\max(m,n)-2}A, x^{\max(m,n)-2}B, \ldots, A, B),$$

of order $2 \cdot \max(m,n)$, into its upper triangular form with the help of Dodgson's integer preserving transformations [5]; they are then located using an extension of a theorem by Van Vleck [2], [13]. (We depart from established practice and we give credit to Dodgson, and not to Bareiss [4], for the integer preserving transformations; see also the work of Waugh and Dwyer [14] where they use the same method as Bareiss, but 23 years earlier, and they name Dodgson as their source–differing from him only in the choice of the pivot element ([14], page 266). Charles Lutwidge Dodgson (1832–1898) is the same person widely known for his writing *Alice in Wonderland* under the pseudonym Lewis Carroll.)

Below we propose a matrix-triangularization subresultant prs method allowing us to *exactly* compute and locate the members of the prs (*without* using Van Vleck's theorem [13]) by applying Dodgson's integer preserving transformations to a matrix of order $m+n$.

2 Our Method and Its Theoretical Justification

We assume that $\deg A = m \geq \deg B = n$ and we denote by M the following matrix

$$M = mat(x^{m-1}B, x^{m-2}B, \ldots, x^{n-1}B, x^{n-1}A, x^{n-2}B, x^{n-2}A, \ldots, B, A)$$

of order $m+n$ with elements $a_{ij}\,(j, i = 1, 2, \ldots, m+n)$. (This matrix can be obtained from Sylvester's matrix M_0 after a rearrangement of its rows.)

Dodgson's integer preserving transformations (which can be easily proved using Sylvester's identity (S) below)

$$a_{ij}^{k+1} = \frac{(a_{ij}^k a_{kk}^k - a_{ik}^k a_{kj}^k)}{a_{k-1,k-1}^{k-1}} \qquad \text{(D)}$$

(see [4], [5], [9] or [14]) where we set $a_{00}^0 = 1$ and it is assumed that $a_{kk}^k \neq 0, k = 1, 2, \ldots, m+n$, are applied to the matrix $M = (a_{ij})$ and transform it to the upper-triangular matrix $M_D = (b_{ij}), (i, j = 1, 2, \ldots, m+n)$, where

$$b_{ij} = \begin{cases} 0 & \text{for } i > j \\ a_{ij}^i & \text{for } i \leq j \end{cases}$$

and, in general,

$$a_{ij}^k = \begin{vmatrix} a_{11} & \ldots & a_{1,k-1} & a_{1j} \\ \vdots & \ddots & \vdots & \vdots \\ a_{k-1,1} & \ldots & a_{k-1,k-1} & a_{k-1,j} \\ a_{i1} & \ldots & a_{i,k-1} & a_{ij} \end{vmatrix}$$

with $1 \leq k \leq m+n$, and $k \leq i, j \leq m+n$.

The following two theorems can be used to locate the members of the prs in the rows of M_D. The *correct* sign is computed.

> **Case 1:** If none of the diagonal minors of the matrix M is equal to zero, then we have:

Theorem 1. Dodgson's integer preserving transformation will transform matrix M to the upper triangular matrix M_D, which contains all n subresultants (located in rows $m+n-2k, k = 0, 1, 2, \ldots, n-1$)

$$S_k = \sum_{i=0}^{k} M_k^i x^i,$$

where

$$M_k^i = (-1)^{\sigma(k)} a_{m+n-2k, m+n-k-i}^{m+n-2k}$$

and

$$\begin{aligned} \sigma(k) &= (m-n+1) + \cdots + (m-k) \\ &= \frac{(n-k)(2m-n-k+1)}{2}, \\ k &= 0, 1, \ldots, n-1. \end{aligned}$$

Proof: It is easy to see that the submatrix located in the upper left corner of the matrix M (where the matrix M was defined in the beginning of *this section*) and having $m+n-2k$ rows and $m+n-k$ columns ($k = 0, 1, \ldots, n-1$) will be

$$M_k' = mat(x^{m-k-1}B, \ldots, x^{n-k-1}B, x^{n-k-1}A, x^{n-k-2}B, x^{n-k-2}A, \ldots, B, A).$$

M_k' differs from matrix M_k (mentioned above) only in the arrangement of the rows. That is, in order to obtain M_k from M_k' it is necessary to rearrange

$$\begin{aligned} \sigma(k) &= (m-n+1) + \cdots + (m-k) \\ &= \frac{(n-k)(2m-n-k+1)}{2}, \end{aligned}$$

adjacent rows.

Therefore we have

$$M_k^i = (-1)^{\sigma(k)} a^{m+n-2k}_{m+n-2k,m+n-k-i}$$

where $i = 0, 1, \ldots, k$, and $k = 0, 1, \ldots, n-1$. $\square$

Before we proceed further, we state Sylvester's determinant identity [11] which is needed in the proof. If we set $\beta^0_{00} = 1$, Sylvester's identity can be expressed as

$$detD_p(B) = (detB) \cdot (\beta^{p-1}_{p-1,p-1})^{r-p}, \quad 1 \leq p \leq r, \tag{S}$$

where $B = (b_{ij})$, $(i, j = 1, 2, \ldots, r)$,

$$D_p(B) = \begin{vmatrix} \beta^p_{p,p} & \beta^p_{p,p+1} & \cdots & \beta^p_{p,r} \\ \beta^p_{p+1,p} & \beta^p_{p+1,p+1} & \cdots & \beta^p_{p+1,r} \\ \vdots & \vdots & \ddots & \vdots \\ \beta^p_{r,p} & \beta^p_{r,p+1} & \cdots & \beta^p_{r,r} \end{vmatrix}$$

of order $r-p+1$, and $\beta^p_{i,j}$ $(p, i, j = 1, 2, \ldots, r)$ are minors (just like a^k_{ij} defined above) obtained from matrix B by adding row i and column j to the (upper left) corner minor of order $p-1$ (see for example Malaschonok's work [9], ([10], pages 30–35), [4], or [8]).

> **Case 2:** If *not* all diagonal minors of the matrix M are nonzero, then we have the following theorem (the term *bubble pivot*, used below, means that, after pivoting, row i_p is *immediately* below row j_p):

Theorem 2. Dodgson's integer preserving transformations with *bubble pivot* and choice of the pivot element by column, will transform matrix M to the upper triangular matrix M_D, and at the same time will compute all subresultants S_k; if, in the process, s row replacements take place, namely row j_1 replaces row i_1, j_2 replaces $i_2, \ldots, j_s$ replaces i_s, (and after each replacement row i_p is immediately below row j_p, $p = 1, 2, \ldots, s$), then **(a)** $S_k = 0$, for all k such that $\frac{(m+n-i_p)}{2} > k > \frac{(m+n-j_p)}{2}$ and for all $p = 1, 2, \ldots, s$. **(b)** for all $p = 1, 2, \ldots, s$, if $k = \frac{(m+n-i_p)}{2}$ is an integer number not in (a), S_k is located in row i_p *before* it is replaced by row j_p. **(c)** for the remaining k, ($k = 0, 1, \ldots, n-1$ and those not in (a) or (b)) S_k is located in row $j = m+n-2k$.

Moreover, in (b) and (c) the subresultant $S_k = \sum_{i=0}^{k} M_k^i x^i$, is located in row j in such a way that

$$M_k^i = (-1)^{\sigma(k)+\sigma(j)} a^j_{j,j+k-i}$$

where

$$\begin{aligned} \sigma(k) &= \frac{(n-k)(2m-n-k+1)}{2}, \\ \sigma(j) &= \sum_{p=1}^{s} j_p - \sum_{p=1}^{s} i_p, \ j_p \leq j, i_p \leq j. \end{aligned}$$

Proof: It is clear that the first $m-n+1$ diagonal minors are not equal to zero because a_{ss}, for $s=1,2,\ldots,m-n+1$, is the leading coefficient of B; therefore

$$a_{ss}^s=(a_{11})^s\neq 0,\ (s=1,2,\ldots,m-n+1).$$

Suppose now that for some $s>m-n+1$ we have $a_{ss}^s=0$, with $a_{s-1,s-1}^{s-1}\neq 0$. In this case we have the following two subcases :

$$\textbf{I}\quad a_{is}^s=0,\ \text{for all } i=s,s+1,\ldots,m+n.$$

Here, making the correspondence $a_{ij}^s\leftrightarrow\beta_{i,j}^p$, $a_{ij}^k\leftrightarrow detB$, and $a_{s-1,s-1}^{s-1}\leftrightarrow\beta_{p-1,p-1}^{p-1}$ in Sylvester's identity, we see that $a_{is}^s=0$ for $i=s,s+1,\ldots,m+n$ if and only if the first column of $D_p(B)$ is 0, and hence detB =0; that is all minors of the form a_{ij}^k $(k>s,\ i>s,\ j>s)$ are equal to zero, and therefore $S_k=0$ for all $k\leq\frac{(m+n-s)}{2}$.

$$\textbf{II}\quad a_{is}^s=0,\ \text{for all } i=s,s+1,\ldots,p-1;\ a_{ps}^s\neq 0.$$

In this subcase, using again Sylvester's identity, we see that all minors $a_{ij}^k=0$ $(s<k\leq p-1,\ i>s,\ j>s)$. Therefore, $S_k=0$ for all k such that $\frac{(m+n-s-1)}{2}\geq k\geq\frac{(m+n-p+1)}{2}$. However it is necessary to continue the computation of the remaining subresultants S_k, $k\leq\frac{(m+n-p)}{2}$; in order to do this we use *bubble-pivot* to replace row s by row p, where $a_{ps}^s\neq 0$ plays the role of the corner mirror, and we now can continue Dodgson's integer preserving transformations. Such an interchange of rows results in all minors a_{ij}^k $(k>p)$ being multiplied by $(-1)^{(p-s)}$, that is, all subresultants $S_k, k=0,1,\ldots,k_1(k_1\leq\frac{(m+n-p)}{2})$ are being multiplied by $(-1)^{(p-s)}$.

Dodgson's transformations may be continued further, as long as situations **I** or **II** are not encountered. □

Note that in cases (b) and (c) Theorem 2 reduces to Theorem 1 in the case of a complete prs, and due to the fact that rows above row j change places, the sign changes by a factor $(-1)^{\sigma(j)}$.

3 Example

As in [2], it should be noted that if $|P|_\infty$ represents the maximum coefficient in absolute value of a polynomial P over the integers, then the theoretical computing time of this method is

$$O(n^5L(|p|_\infty)^2)$$

where $|p|_\infty=max(|A|_\infty,|B|_\infty)$. Below, we present an example that helps clarify the method introduced above.

Example: If we triangularize the matrix M, of order 7, corresponding to the polynomials [1, Example 2, p. 270]

$$\begin{aligned} A= &\ 2x^4+5x^3+5x^2-2x+1 \text{ and}\\ B= &\ 3x^3+3x^2+3x-4\end{aligned}$$

we obtain the following matrix:

$$\begin{pmatrix} 3 & 3 & 3 & -4 & 0 & 0 & 0 \\ 0 & 9 & 9 & 9 & -12 & 0 & 0 \\ 0 & 0 & 27 & 27 & 27 & -36 & 0 \\ 0 & 0 & 0 & -63 & 135 & 0 & 0 \\ 0 & 0 & 0 & 0 & 147 & -315 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3411 & -588 \\ 0 & 0 & 0 & 0 & 0 & 0 & 15683 \end{pmatrix}$$

along with the information that one pivot took place and row 3 was replaced by row 4.

The obtained polynomial remainder sequence is incomplete, and we only have the remainders $-63x + 135$ and 15683, of degree 1 and 0 respectively. However, we still have to determine the signs of these remainders; since pivoting took place, we are going to use Theorem 2 above.

In Theorem 2 we see have that we have to compute the quantity $(-1)^{\sigma(k)+\sigma(j)}$ for $k = 0$, and 2, and $j = 4$, by which the two remainders are going to be multiplied. By the formula stated in the theorem, and given that the degrees are $m = 4$ and $n = 3$, we see that

- $\sigma(0) = (3-0)(2 \cdot 4 - 3 - 0 + 1)/2 = 9$,
- $\sigma(2) = (3-2)(2 \cdot 4 - 3 - 2 + 1)/2 = 2$,
- $\sigma(4) = 4 - 3 = 1$

Therefore, 15683, the remainder of degree 0, is multiplied times $(-1)^{9+1} = 1$ whereas, $S_2 = -63x + 135$, the remainder of degree 1, is multiplied times $(-1)^{2+1} = -1$.

References

[1] Akritas, A. G. *Elements of Computer Algebra with Applications.* J. Wiley Interscience, New York, 1989.

[2] Akritas, A. G. A new method for computing polynomial greatest common divisors and polynomial remainder sequences. Numerische Mathematik **52**, 119–127, 1988.

[3] Akritas, A. G. Exact algorithms for the matrix-triangularization subresultant prs method. Proceedings of the Conference on Computers and Mathematics, Boston, Massachusetts, 145–155, June 1989.

[4] Bareiss, E. H. Sylvester's identity and multistep integer-preserving Gaussian elimination. Mathematics of Computation **22**, 565–578, 1968.

[5] Dodgson, C. L. Condensation of determinants. Proceedings of the Royal Society of London **15**. 150–155, 1866.

[6] González, L., Lombardi, H., Recio, T., and Roy, M-F. Spécialization de la suite de Sturm et sous–résultants. University of Cantabria, Department of Mathematics, Statistics and Computation, Technical Report 8–1990, S-39071 Santander, Spain.

[7] Habicht, W. Eine Verallgemeinerung des Sturmschen Wurzelzaelverfahrens. Commentarii Mathematici Helvetici **21**, 99–116, 1948.

[8] Kowalewski, G. *Einfürung in die Determinantentheorie*. Chelsea, New York, 1948.

[9] Malaschonok, G. I. Solution of a system of linear equations in an integral domain. USSR Journal of Computational Mathematics and Mathematical Physics **23**, 1497–1500, 1983 (in Russian).

[10] Malaschonok, G. I. *System of Linear Equations over a Commutative Ring.* Academy of Sciences of Ukraine. Lvov, 1986 (in Russian).

[11] Sylvester, J. J. On the relation between the minor determinants of linearly equivalent quadratic functions. Philosophical Magazine **1** (Fourth Series), 259–305, 1851.

[12] Sylvester, J. J. On a theory of the syzygetic relations of two rational integral functions, comprising an application to the theory of Sturm's functions, and that of the greatest common measure. Philoshophical Transactions **143**, 407–548, 1853.

[13] Van Vleck, E. B. On the determination of a series of Sturm's functions by the calculation of a single determinant. Annals of Mathematics **1**, Second Series, 1–13, 1899–1900.

[14] Waugh, F. V. and P. S. Dwyer Compact computation of the inverse of a matrix. Annals of Mathematical Statistics **16**, 259–271, 1945.