Numer. Math. 52, 119–127 (1988)

Numerische Mathematik

A New Method for Computing Polynomial Greatest Common Divisors and Polynomial Remainder Sequences*

Alkiviadis G. Akritas
University of Kansas, Department of Computer Science, Lawrence, KS 66045, USA

Summary. A new method is presented for the computation of a greatest common divisor (gcd) of two polynomials, along with their polynomial remainder sequence (prs). This method is based on our generalization of a theorem by Van Vleck [12] and uniformly treats both normal and abnormal prs's, making use of Bareiss's [3] integer-preserving transformation algorithm for Gaussian elimination. Moreover, for the polynomials of the prs's, this method provides the smallest coefficients that can be expected without coefficient gcd computations (as in Bareiss [3]) and it clearly demonstrates the divisibility properties; hence, it combines the best of both the reduced and the subresultant prs algorithms.

Subject Classifications: AMS(MOS): 68C20, 68C25, 68-03, 01A55; CR: I.1.2.

1. Introduction

In this note we restrict our discussion to univariate polynomials with integer coefficients and to computations in $\mathbf{Z}[x]$, a unique factorization domain. Given the polynomial $p(x)=c_n x^n+c_{n-1}x^{n-1}+\ldots+c_0$, its degree is denoted by $\deg(p(x))$ and c_n, its leading coefficient, by $\mathrm{lc}(p)$; moreover, $p(x)$ is called *primitive* if its coefficients are relatively prime.

Consider now $p_1(x)$ and $p_2(x)$, two primitive, nonzero polynomials in $\mathbf{Z}[x]$, $\deg(p_1(x))=n$ and $\deg(p_2(x))=m$, $n\geqq m$. Clearly, the polynomial division (with remainder) algorithm, call it **PD**, that works over a field, cannot be used in $\mathbf{Z}[x]$ since it requires exact divisibility by $\mathrm{lc}(p_2)$. So we use *pseudo-division*, which always yields a pseudo-quotient and pseudo-remainder; in this process we have to premultiply $p_1(x)$ by $\mathrm{lc}(p_2)^{n-m+1}$ and then apply algorithm **PD**. Therefore we have:

$$\mathrm{lc}(p_2)^{n-m+1}\,p_1(x)=q(x)\,p_2(x)+p_3(x), \qquad \deg(p_3(x))<\deg(p_2(x)). \tag{1}$$

Applying the same process to $p_2(x)$ and $p_3(x)$, and then to $p_3(x)$ and $p_4(x)$, etc. (Euclid's algorithm), we obtain a *polynomial remainder sequence* (prs)

* This paper is affectionately dedicated to the memory of my father

$$p_1(x), p_2(x), p_3(x), \ldots, p_h(x), p_{h+1}(x) = 0,$$

where $p_h(x) \neq 0$ is a greatest common divisor of $p_1(x)$ and $p_2(x)$, $\gcd(p_1(x), p_2(x))$. If $n_i = \deg(p_i(x))$ and we have $n_i - n_{i+1} = 1$, for all i, the prs is called *normal*, otherwise, it is called *abnormal*. The problem with the above approach is that the coefficients of the polynomials in the prs grow exponentially and hence slow down the computations. We wish to control this coefficient growth. We observe that equation (1) can also be written more generally as

$$\begin{aligned} \mathrm{lc}(p_{i+1})^{n_i - n_{i+1}+1}\, p_i(x) &= q_i(x)\, p_{i+1}(x) + \beta_i\, p_{i+2}(x), \\ \deg(p_{i+2}(x)) &< \deg(p_{i+1}(x)), \end{aligned} \tag{2}$$

$i = 1, 2, \ldots, h-1$. That is, if a method for choosing β_i is given, the above equation provides an algorithm for constructing a prs. The obvious choice $\beta_i = 1$, for all i, is called the *Euclidean prs*; it was described above and leads to exponential growth of coefficients. Choosing β_i to be the greatest common divisor of the coefficients of $p_{i+2}(x)$ results in the *primitive prs*, and it is the best that can be done to control the coefficient growth. (Notice that here we are dividing $p_{i+2}(x)$ by the greatest common divisor of its coefficients before we use it again.) However, computing the greatest common divisor of the coefficients for each member of the prs (after the first two, of course) is an expensive operation and should be avoided. So far, in order both to control the coefficient growth and to avoid the coefficient gcd computations, either the *reduced* or the (improved) *subresultant* prs have been used. In the reduced prs we choose

$$\beta_1 = 1 \quad \text{and} \quad \beta_i = \mathrm{lc}(p_i)^{n_i - n_{i+1}+1}, \qquad i = 2, 3, \ldots, h-1, \tag{3}$$

whereas, in the subresultant prs we have

$$\beta_1 = (-1)^{n_1 - n_2 + 1} \quad \text{and} \quad \beta_i = (-1)^{n_i - n_{i+1}+1}\, \mathrm{lc}(p_i)\, H_i^{n_i - n_{i+1}}, \qquad i = 2, 3, \ldots, h-1, \tag{4}$$

where

$$H_2 = \mathrm{lc}(p_2)^{n_1 - n_2} \quad \text{and} \quad H_i = \mathrm{lc}(p_i)^{n_{i-1} - n_i} H_{i-1}^{1-(n_{i-1} - n_i)}, \qquad i = 3, 4, \ldots, h-1.$$

That is, in both cases above we divide $p_{i+2}(x)$ by the corresponding β_i before we use it again. The reduced prs algorithm is recommended if the prs is normal, whereas if the prs is abnormal the subresultant prs algorithm is to be preferred. The proofs that the β_i's shown in (3) and (4) exactly divide $p_{i+2}(x)$ are very complicated [6] and have up to now obscured simple divisibility properties [10], (see also [4] and [5]). For a simple proof of the validity of the reduced prs see [2]; analogous proof for the subresultant prs can be found in [8].

In what follows we present a method which uniformly treats both normal and abnormal prs's and provides the smallest coefficients in absolute value that can be expected without coefficient greatest common divisor computations [3]; moreover, this method clearly demonstrates the existing divisibility properties. We also present a theorem which is a generalization of a theorem by Van Vleck. (We have failed to detect prior use of Van Vleck's theorem in the literature.)

2. Gaussian Elimination and Sylvester's Form of the Resultant

Consider the two polynomials in $\mathbf{Z}[x]$, $p_1(x)=c_n x^n+c_{n-1}x^{n-1}+\ldots+c_0$ and $p_2(x)=d_m x^m+d_{m-1}x^{m-1}+\ldots+d_0$, $c_n\neq 0$, $d_m\neq 0$, $n\geqq m$. In the literature the most common encountered forms of the resultant of $p_1(x)$ and $p_2(x)$ are

$$\mathrm{res}_B(p_1,p_2)=\begin{vmatrix} c_n & c_{n-1} & \ldots & & c_0 & 0 & \ldots & 0 \\ 0 & c_n & c_{n-1} & \ldots & & c_0 & \ldots & 0 \\ & & & & & \vdots & & \\ 0 & 0 & \ldots & & c_n & c_{n-1} & \ldots & c_0 \\ d_m & d_{m-1} & \ldots & d_0 & 0 & 0 & \ldots & 0 \\ 0 & d_m & d_{m-1} & \ldots & d_0 & 0 & \ldots & 0 \\ & & & & \vdots & & & \\ 0 & 0 & \ldots & d_m & d_{m-1} & & \ldots & d_0 \end{vmatrix}$$

or

$$\mathrm{res}_T(p_1,p_2)=\begin{vmatrix} c_n & c_{n-1} & \ldots & & c_0 & 0 & \ldots & 0 \\ 0 & c_n & c_{n-1} & \ldots & & c_0 & \ldots & 0 \\ & & & & & \vdots & & \\ 0 & 0 & \ldots & & c_n & c_{n-1} & \ldots & c_0 \\ 0 & 0 & \ldots & d_m & d_{m-1} & & \ldots & d_0 \\ & & & & \vdots & & & \\ 0 & d_m & d_{m-1} & \ldots & d_0 & 0 & \ldots & 0 \\ d_m & d_{m-1} & \ldots & d_0 & 0 & 0 & \ldots & 0 \end{vmatrix}$$

where for both cases we have m rows of c's and n rows of d's; that is, the determinant is of order $m+n$. Contrary to established practice, we call the first Bruno's and the second Trudi's form of the resultant. (Actually, in the literature, Bruno's form is referred to as Sylvester's.) Notice that $\mathrm{res}_B(p_1,p_2)=(-1)^{n(n-1)/2}\,\mathrm{res}_T(p_1,p_2)$. However, we choose to call Sylvester's form the one described below; this form was "buried" in Sylvester's 1853 paper [11] and is only once mentioned in the literature in a paper by Van Vleck [12]. Sylvester indicates ([11], p. 426) that he had produced this form in 1839 or 1840 and some years later Cayley unconsciously reproduced it as well. It is Sylvester's form of the resultant that forms the foundation of our new method for computing polynomial remainder sequences; however, we first present the following theorem concerning Bruno's form of the resultant:

Theorem 1. (Laidacker [9]) *If we transform the matrix corresponding to* $\mathrm{res}_B(p_1,p_2)$ *into its upper triangular form* $T_B(R)$, *using row transformations only, then the last nonzero row of* $T_B(R)$ *gives the coefficients of a greatest common divisor of* $p_1(x)$ *and* $p_2(x)$.

The above theorem indicates that we can obtain only a greatest common divisor of $p_1(x)$ and $p_2(x)$ but none of the remainder polynomials. In order to compute both a $\gcd(p_1(x),p_2(x))$ and all the polynomial remainders we have

to use Sylvester's form of the resultant; this is of order $2n$ and of the following form ($p_2(x)$ has been transformed into a polynomial of degree n by introducing zero coefficients. Below $p_1(x)$ and $p_2(x)$ are replaced by $p(x)$ and $q(x)$, respectively):

$$\mathrm{res}_S(p,q)=\begin{vmatrix} c_n & c_{n-1} \ldots c_0 & 0 & 0 \ldots 0 \\ d_n & d_{n-1} \ldots d_0 & 0 & 0 \ldots 0 \\ 0 & c_n \ldots & c_0 & 0 \ldots 0 \\ 0 & d_n \ldots & d_0 & 0 \ldots 0 \\ & \ldots & & \\ 0 \ldots 0 & c_n & c_{n-1} & \ldots c_0 \\ 0 \ldots 0 & d_n & d_{n-1} & \ldots d_0 \end{vmatrix} \tag{S}$$

Sylvester obtains this form from the system of equations ([11], pp. 427–428)

$$\begin{aligned} p(x)&=0 \\ q(x)&=0 \\ x\cdot p(x)&=0 \\ x\cdot q(x)&=0 \\ x^2\cdot p(x)&=0 \\ x^2\cdot q(x)&=0 \\ &\ldots\ldots\ldots \\ x^{n-1}\cdot p(x)&=0 \\ x^{n-1}\cdot q(x)&=0 \end{aligned}$$

and he indicates that if we take k pairs of the above equations, the highest power of x appearing in any of them will be x^{n+k-1}. Therefore, we shall be able to eliminate so many powers of x, that x^{n-k} will be the highest power uneliminated and $n-k$ will be the degree of a member of the Sturmian polynomial remainder sequence generated by $p(x)$ and $q(x)$. Moreover, Sylvester showed that the polynomial remainders thus obtained are what he terms *simplified residues*; that is, the coefficients are the smallest possible obtained without integer gcd computations and without introducing rationals. Stated in other words, the polynomial remainders have been freed from their corresponding *allotrious factors.*

Example. Consider $p(x)=x^3-7x+7$ and $q(x)=3x^2-7$. Then

$$\mathrm{res}_S(p,q)=\begin{vmatrix} 1 & 0 & -7 & 7 & 0 & 0 \\ 0 & 3 & 0 & -7 & 0 & 0 \\ 0 & 1 & 0 & -7 & 7 & 0 \\ 0 & 0 & 3 & 0 & -7 & 0 \\ 0 & 0 & 1 & 0 & -7 & 7 \\ 0 & 0 & 0 & 3 & 0 & -7 \end{vmatrix}$$

and we can compute the negated coefficients of the first polynomial remainder (which is of degree $n-k=1$) if we take $k=n-1=2$ pairs of rows. So, the leading coefficient is

$$\begin{vmatrix} 1 & 0 & -7 & 7 \\ 0 & 3 & 0 & -7 \\ 0 & 1 & 0 & -7 \\ 0 & 0 & 3 & 0 \end{vmatrix} = 3 \cdot (21) - 1 \cdot 21 = 42$$

and the second coefficient is

$$\begin{vmatrix} 1 & 0 & -7 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 1 & 0 & 7 \\ 0 & 0 & 3 & -7 \end{vmatrix} = 3 \cdot (-21) = -63;$$

that is, the first polynomial remainder is $42x-63=(-1)\,p_3(x)$, where $p_3(x)$ was obtained from the Euclidean prs algorithm.

In general, if we have the polynomial remainder sequence $p_1(x)$, $p_2(x)$, $p_3(x)$, ..., $p_h(x)$, $\deg(p_1(x))=n$, $\deg(p_2(x))=m$, $n \geqq m$, we can obtain the (negated) coefficients of the $(i+1)$th member of the prs, $i=0, 1, 2, \ldots, h-1$, as minors formed from the first $2i$ rows of (S) by successively associating with the first $2i-1$ columns (of the $(2i)$ by $(2n)$ matrix) each succeeding column in turn.

Theorem 2. (Van Vleck [12]) *Given the polynomials in* $\mathbf{Z}[x]$ $p_1(x)=c_n x^n + c_{n-1} x^{n-1} + \ldots + c_0$ *and* $p_2(x)=d_m x^m + d_{m-1} x^{m-1} + \ldots + d_0$, $c_n \neq 0$, $d_m \neq 0$, $n \geqq m$ *then the successive polynomials which are formed from the first* $2i$ *rows of* (S) $i=1, 2, \ldots, n$ *constitute a Sturm sequence.*

From the above we see that Sylvester's form of the resultant can give us the Sturmian sequence of two polynomials (which is a normal polynomial remainder sequence). Moreover, and this is the most important fact, one does not have to compute determinants in order to find the coefficients. This is due to the fact that in the original determinant (S) the members of any two consecutive rows are the same as those of the two preceeding rows. So, if in any row the values of the members are changed by adding a multiple of the preceeding row, exactly the same change can be made in the members of each alternate row thereafter without altering the value of any minor which appears as a coefficient in one of our Sturm's polynomials. Therefore, we can bring the corresponding matrix into its upper triangular form without disturbing the repetitive character of the determinant. We therefore have:

Theorem 3. (Van Vleck [12]) *If we bring the matrix corresponding to Sylvester's form of the resultant, into its upper triangular form* $T_S(R)$, *then the even rows of* $T_S(R)$ *furnish the coefficients of the successive Sturm polynomial remainders. The coefficients taken from a given row are multiplied by* $(-1)^k$, *where k is the number of negative "constituents" in the principal diagonal above the row under consideration.*

Van Vleck demonstrated this theorem with an example [12]. However, the matrix corresponding to the resultant is transformed into its upper triangular form by performing elementary row operations and removing at each step the greatest common divisor of the coefficients, a computation which we want to avoid.

On the other hand, we transform the matrix corresponding to the resultant (S) into its upper triangular form using Bareiss's integer-preserving transformation algorithm [3]. That is: let $r_{00}^{(-1)}=1$, and $r_{ij}^{(0)}=r_{ij}$, $i,j=1,\ldots,n$; then for $k<i,j\leqq n$,

$$r_{ij}^{(k)}:=(1/r_{k-1,k-1}^{(k-2)})\cdot\begin{vmatrix} r_{kk}^{(k-1)} & r_{kj}^{(k-1)} \\ r_{ik}^{(k-1)} & r_{ij}^{(k-1)} \end{vmatrix} \tag{5}$$

Of particular importance in Bareiss's algorithm is the fact that the determinant of order 2 is divided *exactly* by $r_{k-1,k-1}^{(k-2)}$ (the proof is very short and clear and is described in Bareiss's paper [3]) and that the resulting coefficients are the smallest that can be expected without coefficient gcd computations and without introducing rationals. Notice how all the complicated expressions for β_i in the reduced and subresultant prs algorithms are mapped to the simple factor $r_{k-1,k-1}^{(k-2)}$ of this method.

It should be pointed out that using Bareiss's algorithm we will have to perform pivots (interchange two rows) which will result in a change of signs; see the example below. Therefore, care should be excercised in using Theorem 3. We also define the term *bubble* pivot as follows: if the diagonal element in row i is zero and the next nonzero element down the column is in row $i+j$, $j>1$, then row $i+j$ will become row i after pairwise interchanging it with the rows above it. Bubble pivot preserves the symmetry of the determinant.

Example. Using $p_1(x)=x^3-7x+7$ and $p_2(x)=3x^2-7$ we have

$$\begin{bmatrix} 1 & 0 & -7 & 7 & 0 & 0 \\ 0 & 3 & 0 & -7 & 0 & 0 \\ 0 & 1 & 0 & -7 & 7 & 0 \\ 0 & 0 & 3 & 0 & -7 & 0 \\ 0 & 0 & 1 & 0 & -7 & 7 \\ 0 & 0 & 0 & 3 & 0 & -7 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 & 0 & -7 & 7 & 0 & 0 \\ 0 & 3 & 0 & -7 & 0 & 0 \\ 0 & 0 & 9 & 0 & -21 & 0 \\ 0 & 0 & 0 & -42 & 63 & 0 \\ 0 & 0 & 0 & 0 & 196 & -294 \\ 0 & 0 & 0 & 0 & 0 & -49 \end{bmatrix} \quad *$$

The $*$-ed row indicates that a pivot was performed between the 3rd and 4th rows and this means that the Sturmian remainders are $42x-63$ and 49.

Note. If we consider the rows of $T_S(R)$ in the above example, we see that each corresponds to a given polynomial whose degree is one less than the number of elements *enclosed* between the leading and trailing zeros. The case might arise where one or more coefficients of the lower powers of x are zero; in that case the degree of the polynomial can be easily determined by examining the degrees of all the rows of the upper triangular form.

What we have said so far is valid for normal polynomial remainder sequences. In order to be able to deal with abnormal prs's we need the following theorem

which is our generalization of Theorem 3 (its proof is along the same lines as those of Theorem 3).

Theorem 4. [1] *Let $p_1(x)$ and $p_2(x)$ be two polynomials of degrees n and m respectively, $n \geqq m$. Using Bareiss's algorithm transform the matrix corresponding to $\text{res}_S(p_1, p_2)$ into its upper triangular form $T_S(R)$; let n_i be the degree of the polynomial corresponding to the* ith *row of $T_S(R)$, $i=1, 2, \ldots, 2n$, and let $p_k(x)$, $k \geqq 2$, be the* kth *member of the (normal or abnormal) polynomial remainder sequence of $p_1(x)$ and $p_2(x)$. Then if $p_k(x)$ is in row i of $T_S(R)$, the coefficients of $p_{k+1}(x)$ (within sign) are obtained from row $i+j$ of $T_S(R)$, where j is the smallest integer such that $n_{i+j} < n_i$. (If $n=m$ associate both $p_1(x)$ and $p_2(x)$ with the first row of $T_S(R)$.)*

Notice that as a special case of the above theorem we obtain Theorem 3 for normal prs's. We see, therefore, that based on Theorem 4, we have a new method to compute the polynomial remainder sequence and a greatest common divisor of two polynomials. This new method uniformly treats both normal and abnormal prs's and provides the smallest coefficients that can be expected without coefficient gcd computation.

3. Our Method

The inputs are two (primitive) polynomials in $\mathbf{Z}[x]$, $p_1(x)=c_n x^n + c_{n-1} x^{n-1} + \ldots + c_0$ and $p_2(x)=d_m x^m + d_{m-1} x^{m-1} + \ldots + d_0$, $c_n \neq 0$, $d_m \neq 0$, $n \geqq m$.

Step 1. Form the resultant (*S*), $\text{res}_S(p_1, p_2)$, of the two polynomials $p_1(x)$ and $p_2(x)$.

Step 2. Using Bareiss's algorithm (described above) transform the resultant (*S*) into its upper triangular form $T_S(R)$; then the coefficients of all the members of the polynomial remainder sequence of $p_1(x)$ and $p_2(x)$ are obtained from the rows of $T_S(R)$ with the help of Theorem 4.

Example. If we consider the polynomials $p_1(x)=x^5+5x^4+10x^3+5x^2+5x+2$ and $p_2(x)=x^4+4x^3+6x^2+2x+1$ the upper triangular form of the matrix corresponding to $\text{res}_S(p_1, p_2)$ is

$$\begin{bmatrix}
1 & 5 & 10 & 5 & 5 & 2 & 0 & 0 & 0 & 0 \\
0 & 1 & 4 & 6 & 2 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 4 & 3 & 4 & 2 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 7 & 1 & 3 & 2 & 0 & 0 \\
0 & 0 & 0 & 0 & 3 & -2 & -1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 9 & -6 & -3 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 58 & 50 & 18 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -266 & -112 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -756 & -532 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -980
\end{bmatrix} \quad *$$

The $_*$-ed row indicates that a pivot took place. Therefore, the members of the prs generated by $p_1(x)$ and $p_2(x)$ are $3x^2-2x-1$, $-266x-112$ and -980.

Theorem 5. *Let* $p_1(x)=c_n x^n+c_{n-1}x^{n-1}+\ldots+c_0$ *and* $p_2(x)=d_m x^m+d_{m-1}x^{m-1}+\ldots+d_0$, $c_n\neq 0$, $d_m\neq 0$, $n\geqq m$ *be two (primitive) polynomials in* $\mathbf{Z}[x]$ *and for some polynomial* $P(x)$ *in* $\mathbf{Z}[x]$ *let* $|P|_\infty$ *represent its maximum coefficient in absolute value. Then the method described above computes a greatest common divisor of* $p_1(x)$ *and* $p_2(x)$ *along with all the polynomial remainders in time*

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

where $|p|_\infty=\max(|p_1|_\infty, |p_2|_\infty)$.

Proof. Since we use exact integer arithmetic the cost of an operation on two integers depends not only on the operation itself but on the length (number of bits) of the operants as well. If A is an integer, we define $L(A)$, its length, by

$$L(A)=\begin{cases}1 & A=0\\ \lfloor \log_b |A|+1\rfloor & A\neq 0\end{cases}$$

where b indicates the base of the number system in which the operant A is represented when an operation is being performed. (Notice that $A\cdot B$ is computed in time $O(L(A)\cdot L(B))$.)

We know that if n is the highest degree of the two polynomials $p_1(x)$ and $p_2(x)$, then Sylvester's matrix will be $2n$ by $2n$. It is also known that, without taking advantage of the band form of this matrix, we can bring it into its upper triangular form (using Bareiss's method), performing $O(n^3)$ multiplications. In the worst case we assume that each integer multiplication is performed among the largest integers that will appear. These largest integers can be as large as $\mathrm{res}_S(p_1, p_2)$. Using Hadamard's inequality we have

$$|\mathrm{res}_S(p_1,p_2)|\leqq \prod_{1\leqq i\leqq 2n}\Big(\sum_{1\leqq j\leqq 2n} r_{ij}^2\Big)^{1/2}\leqq (2n)^n(|p|_\infty)^{2n}$$

where $|p|_\infty=\max(|p_1|_\infty, |p_2|_\infty)$.

Thus, the time for each multiplication (i.e. $(2n)^n(|p|_\infty)^{2n}$ by itself) is $L((2n)^n(|p|_\infty)^{2n})^2=[nL(2n)+2nL(|p|_\infty)]^2=O(n^2L(|p|_\infty)^2)$ from which follows the theorem.

4. Historical Remarks

1. According to Van Vleck [12], Sylvester used the above form (S) of the resultant to obtain from its minors the coefficients of all the polynomials of the prs of $p_1(x)$ and $p_2(x)$. That is, the coefficients of the $(i+1)$th polynomial of the prs, $i=0, 1, 2, \ldots h-1$, can be obtained as minors formed from the first $2i$ rows of (S) "by associating those constituents which are contained in the first $2i-1$ columns with those of each succeeding column in turn" ([12], pp. 3–4). A polynomial so constructed is called a *subresultant*. However, Van Vleck indicated that this approach is far more laborious than computing the corresponding polynomial by the usual process of (pseudo)division.

2. Brown, in both of his papers ([4], p. 485, [5], p. 238) attributes to Collins the discovery that every polynomial of a prs is proportional to some subresultant of the first two. This fact, which is known in the literature as the *fundamental theorem of subresultants*, was first proved by Sylvester in his 1853 paper [11] and was rediscovered by Freyer in 1959 [7].

References

1. Akritas, A.G.: A new method for computing polynomial greatest common divisors. TR-86-9, University of Kansas, Department of Computer Science, Lawrence, Ks 66045, 1986
2. Akritas, A.G.: A simple validity proof of the reduced prs algorithm. Computing **38**, 369–372 (1987)
3. Bareiss, E.H.: Sylvester's identity and multistep integer-preserving Gaussian elimination. Math. Comput. **22**, 565–578 (1968)
4. Brown, W.S.: On Euclid's algorithm and the computation of polynomial greatest common divisors. J ACM **18**, 476–504 (1971)
5. Brown, W.S.: The subresultant prs algorithm. ACM Trans. Math. Software **4**, 237–249 (1978)
6. Collins, G.E.: Subresultants and reduced polynomial remainder sequences. J ACM **14**, 128–142 (1967)
7. Fryer, W.D.: Applications of Routh's algorithm to network theory problems. IEEE Trans. Circuit Theo. **CT-6**, 144–149 (1959)
8. Habicht, W.: Eine Verallgemeinerung des Sturmschen Wurzelzählverfahrens. Comment. Math. Helv. **21**, 99–116 (1948)
9. Laidacker, M.A.: Another theorem relating Sylvester's matrix and the greatest common divisor. Math. Mag. **42**, 126–128 (1969)
10. Loos, R.: Generalized polynomial remainder sequences. In: Computer algebra symbolic and algebraic computations. (Computing Supplement) Buchberger, B., Collins, G.E., Loos, R. (eds.), Vol. 4, pp. 115–137. Wien, New York: Springer 1982
11. 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 algebraical common measure. Philos. Trans. **143**, 407–548 (1853)
12. Van Vleck, E.B.: On the determination of a series of Sturm's functions by the calculation of a single determinant. Ann. Math. (Second Series) **1**, 1–13 (1899–1900)

Received November 8, 1986/September 20, 1987

Note Added in Proof.

A. Normal/abnormal *prs*'s are also called complete/incomplete *prs*'s.

B. Historical remark 3. Like Brown, D.E. Knuth attributes to Collins the fundamental theorem of subresultants; see p. 410. The art of computer programming, Vol. 2: Seminumerical algorithms, Second edition. Addison-Wesley, Reading, Massachusetts, 1981.