SYLVESTER'S FORGOTTEN FORM OF THE RESULTANT

Alkiviadis G. Akritas
Department of Computer Science, University of Kansas, Lawrence, KS 66045-2192
(Submitted November 1991)

1. INTRODUCTION

It is well known that Euclid's algorithm for computing the greatest common divisor (gcd) of two integer numbers is more than two thousand years old and, as it turns out, it is the oldest known algorithm. Interest in computing a gcd of two polynomials first appeared only in the sixteenth century and the problem was solved by Simon Stevin [13] simply by applying Euclid's algorithm (for integers) to polynomials with integer coefficients. However, from the computational point of view, Euclid's algorithm applied to polynomials with integer coefficients is very inefficient because of the growth of coefficients that takes place and the eventual slowdown of computations. This growth of coefficients is due to the fact that the ring $\mathbf{Z}[x]$ is not a Euclidean domain, and hence, divisions (as we know them) cannot always be performed.

For example, take the two polynomials $p_1(x) = x^3 - 7x + 7$ and $p_2(x) = 3x^2 - 7$ which have very small coefficients. Observe that, *over the integers*, we cannot divide $p_1(x)$ by $p_2(x)$ (since 3 does not divide 1) and, hence, we have to introduce the concept of *pseudo-division*, which always yields a pseudo-quotient and pseudo-remainder. According to this process, we have to premultiply $p_1(x)$ by the leading coefficient of $p_2(x)$ raised to the power 2 [that is, we premultiply $p_1(x)$ by $9 = 3^2$] and then apply our usual polynomial division algorithm. [Below we denote the leading coefficient (lc) of a polynomial $p(x)$ by $\mathrm{lc}(p(x))$ and its degree by $\deg(p(x))$.]

In the general case where $\deg(p_1(x)) = n$, and $\deg(p_2(x)) = m$, we premultiply $p_1(x)$ by $\mathrm{lc}(p_2(x))^{n-m+1}$. In this was we know for sure that all the polynomial divisions involved in the process of computing a greatest common divisor of $p_1(x)$ and $p_2(x)$ will be carried out in $\mathbf{Z}[x]$. That is, in general, we start with

$$\mathrm{lc}(p_2(x))^{n-m+1} p_1(x) = q_1(x)p_2(x) + p_3(x), \quad \deg(p_3(x)) < \deg(p_2(x)) \tag{1}$$

and applying the same process $p_2(x)$ 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)

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

where $p_h(x) \neq 0$ is a greatest common divisor of $p_1(x)$ and $p_2(x)$, denoted by $\gcd(p_1(x), p_2(x))$. The reader should compute the prs of the above example and verify that the coefficients grow rather rapidly (even when we start with such very small coefficients!!) **Answer:** $q_1(x) = 3x$, $p_3(x) = -42x + 63$, $q_2(x) = -126x - 189$, $p_4(x) = -441$, $q_3(x) = 18522x - 27783$, and $p_5(x) = 0$.

Note that we are dealing with exact integer computations and, for reasons that cannot be discussed here, the length of the integers involved is taken into consideration when we analyze the complexity of an algorithm. (Generally speaking, the complexity of an algorithm refers to the

according to this number that the various algorithms are being compared for efficiency.) For an introduction to Computer Algebra, the area that deals with exact integer computations, see [3].

Therefore, 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 without having to compute gcd's of coefficients (because that in itself can be time consuming). In what follows, we use the following conventions: if $n_i = \deg(p_i(x))$ and we have $n_i - n_{i+1} = 1$, for all i, the prs is called *complete*, otherwise, it is called *incomplete*; moreover, a polynomial $p(x)$ is called *primitive* if its coefficients are relatively prime.

As we will see immediately below, using pseudo-divisions, the problem of controlling the coefficient growth was originally solved (at least partially) by Sylvester in his 1853 paper and fully by Habicht in 1948. Equivalently, as we will see in §2, the problem can be solved by triangularizing the matrix corresponding to what we call Sylvester's form of the resultant (and which form is different from the one people are used to), thus avoiding explicit polynomial pseudo-divisions. It turns out that Sylvester's paper of 1853 is the basis for both classical methods to restrict the coefficient growth (see Figure 1 below) and, thus, we have one more case indicating the importance of mathematics of the last century, and its connection with computational mathematics as done today.

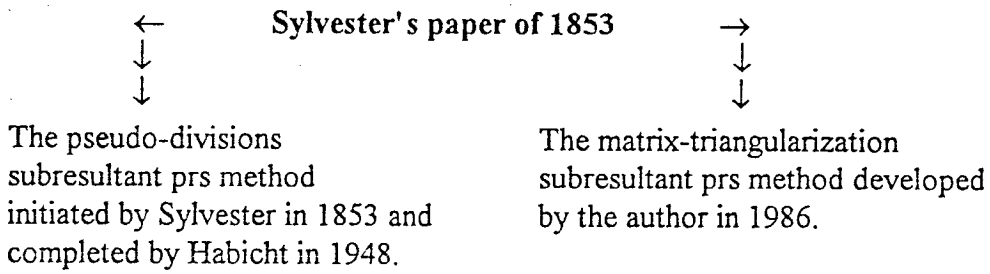

FIGURE 1.

Overview of the historical development of the two classical subresultant prs methods for restricting the growth of coefficients. The method developed by Sylvester should be used only when the prs is complete, whereas the one by Habicht should be used when the prs is incomplete, something which we do not know apriori. (Actually, Habicht's method also can be used when the prs is complete, at additional computational cost.) The matrix-triangularization method can be identically used for both kinds of prs's.

To see how Sylvester's results can be applied in the pseudo-divisions method, observe that (1) can also be written, for any two successive polynomials $p_i(x)$ and $p_{i+1}(x)$ of the prs, as

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

$i = 1, 2, \ldots, h-1$, where β_i is the integer which we want to divide out of the coefficients of $p_{i+2}(x)$. 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, as we saw, it leads to exponential growth of coefficients. Next, choosing β_i to be the greatest common divisor of the coefficients $p_{i+2}(x)$ 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, as

we indicated above, computing the gcd 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 (developed by Sylvester) we choose

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

whereas, in the subresultant prs (developed by Habicht) we have

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

where

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

That is, in both cases above, we divide $p_{i+2}(x)$ by the corresponding β_i before we use it again.

Consider again the above-stated example where we are dealing with a complete prs and, hence, (3) and (4) yield exactly the same results [note that, using (4), we have to perform some extra computations]; the reader should verify that, in both cases, we obtain $\beta_1 = 1$ and, hence, $p_3(x) = -42x + 63$ whereas $\beta_2 = 9$ and, hence, $p_4(x) = -49\ (= 441/9)$ instead of $p_4(x) = -441$ obtained before. Note that, with this approach, we were able to reduce the coefficients of $p_4(x)$, but there is no way to reduce the coefficients of $p_3(x)$!

The reduced prs algorithm is recommended if the prs is complete, whereas if the prs is incomplete the subresultant prs algorithm is to be preferred. The proofs that the β_i's shown in (3) and (4) exactly divide $p_{i+2}(x)$ *were* very complicated [7] and have up to now obscured simple divisibility properties [13] (see also [5] and [6]). For a simple proof of the validity of the reduced prs, see [1]; analogous proof for the subresultant prs can be found in [10] and [3]. A very simple proof of Habicht's theorem can be found in the recent work of Gonzalez et al. [9]. For some interesting comments regarding priority rights for the development of these prs algorithms see [11] and Historical Notes to Chapter 5 in [3, p. 282].

In contrast to the above prs algorithms, the matrix-triangularization subresultant prs method avoids explicit polynomial divisions. In what follows, we present this method and show how to solve the example mentioned above.

2. SYLVESTER'S FORGOTTEN FORM OF THE RESULTANT

Consider the two polynomials in $\mathbf{Z}[x]$, $p_1(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_0$ and $p_2(x) = d_m x^m + d_{m-1}x^{m-1} + \cdots + d_0, c_n \neq 0, d_m \neq 0, n \geq m$. In the literature, the most commonly encountered forms of the resultant of $p_1(x)$ and $p_2(x)$ (both known as "Sylvester's" forms) are:

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

and

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

where in 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 di Bruno's and the second Trudi's form of the resultant [3] (di Bruno was sanctified by the Roman Catholic Church in the 1980s). Notice that $\mathrm{res}_B(p_1(x), p_2(x)) = (-1)^{n(n-1)/2}\,\mathrm{res}_T(p_1(x), p_2(x))$. For these two forms of the resultant, the following theorem holds.

Theorem 1 (Laidacker [12]): If we transform the matrix corresponding to $\mathrm{res}_B(p_1(x), p_2(x))$ 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 off $p_1(x)$ and $p_2(x)$.

Theorem 1 indicates that using these forms of the resultant we can obtain only a greatest common divisor of $p_1(x)$ and $p_2(x)$ but, in general, 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. We choose to call Sylvester's form the one described below; this form was "buried" in Sylvester's 1853 paper [14] and is only once mentioned in the literature in a paper by Van Vleck [15]. Sylvester indicates [14, p. 426] that he had produced this form in 1839 or 1840 and some years later Cayley unconsciously reproduced it as well. This form is of order $2n$ (as opposed to $n + m$ for the other two forms) and can be written as follows [$p_2(x)$ has now been transformed into a polynomial of degree n by introducing zero coefficients]:

$$\operatorname{res}_S(p_1(x), p_2(x)) = \begin{vmatrix} c_n & c_{n-1} & \cdots & c_0 & 0 & 0 & \cdots & 0 \\ d_n & d_{n-1} & \cdots & d_0 & 0 & 0 & \cdots & 0 \\ 0 & c_n & \cdots & & c_0 & 0 & \cdots & 0 \\ 0 & d_n & \cdots & & d_0 & 0 & \cdots & 0 \\ & & \vdots & & & & & \\ 0 & \cdots & 0 & c_n & c_{n-1} & \cdots & & c_0 \\ 0 & \cdots & 0 & d_n & d_{n-1} & \cdots & & d_0 \end{vmatrix} \qquad \text{(S)}$$

Sylvester obtained this form from the system of equations [14, pp. 427-28]

$$\begin{aligned} p_1(x) &= 0 \\ p_2(x) &= 0 \\ x \cdot p_1(x) &= 0 \\ x \cdot p_2(x) &= 0 \\ x^2 \cdot p_1(x) &= 0 \\ x^2 \cdot p_2(x) &= 0 \\ &\cdots \\ x^{n-1} \cdot p_1(x) &= 0 \\ x^{n-1} \cdot p_2(x) &= 0 \end{aligned}$$

and he indicated 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 $p_1(x)$ and $p_2(x)$. 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 Sylvester's words, the polynomial remainders have been freed from their corresponding *allotrious factors.*

It has been proved [15] that if we want to compute the *complete* polynomial remainder sequence $p_1(x), p_2(x), p_3(x), \ldots, p_h(x)$, $\deg(p_1(x)) = n$, $\deg(p_2(x)) = m$, $n \geq m$, we can obtain the (negated) coefficients of the $(i+1)^{\text{th}}$ 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.

However, instead of proceeding as in [15], and in order to handle incomplete prs's as well, we transform the matrix corresponding to the resultant (S) into its upper triangular form and obtain the members of the prs with the help of Theorem 2 below. We also use Dodgson's integer-preserving transformation algorithm [8], which works as follows: Suppose that

$$r_{ij}^{(0)} = r_{ij}, \qquad i, j = 1, \ldots, n$$

are the matrix elements at the beginning of the algorithm (0^{th} iteration). There are n iterations performed, and in the k^{th} one (indicated here) the following actions are taken: (a) the elements of the k^{th} column located below the k^{th} (diagonal) element are being turned to zero, (b) all the elements located in rows *and* columns greater than k get updated as shown below, and (c) all the

other elements of the matrix remain unchanged. In this way, at the end of the process, all the elements of the matrix located below the diagonal are zero. That is, we have: let

$$r_{00}^{(-1)} = 1, \quad \text{and} \quad r_{ij}^{(0)} = r_{ij}, \quad i, j = 1, \ldots, n;$$

then for $k < i, j \le n$,

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

Of particular importance in Dodgson's algorithm is the fact that the determinant of order 2 is divided *exactly* by $r_{k-1,k-1}^{(k-2)}$ (a very short and clear proof of (D) is described in Bareiss's paper [4]—see also the Historical note at the end of this paper) 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 Dodgson's algorithm (D) we will have to perform pivots (interchange two rows) which will result in a change of signs. We 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 beccome row i after pairwise interchanging it with the rows above it. (Note that, after a bubble pivot, ex-row i becomes row $i + 1$, whereas with regular pivot it would have become row $i + j$.) Bubble pivot preserves the symmetry of the determinant.

The following theorem helps us locate the members of the (complete or incomplete) prs in the final, triangularized, matrix.

Theorem 2 ([2]): Let $p_1(x)$ and $p_2(x)$ be two polynomials of degrees n and m, respectively, $n \ge m$. Then, using Dodgson's algorithm (D), transform the matrix corresponding to $\mathrm{res}_S(p_1(x), p_2(x))$ into its upper triangular form $T_S(R)$; let n_i be the degree of the polynomial corresponding to the i^{th} row of $T_S(R)$, $i = 1, 2, \ldots, 2n$, and let $p_k(x)$, $k \ge 2$, be the k^{th} member of the (*complete or incomplete*) 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 $T_S(R)$.]

Therefore, we see that, based on Theorem 2, we have a new method for computing the polynomial remainder sequence and a greatest common divisor of two polynomials. This new method uniformly treats both complete and incomplete prs's and provides the smallest coefficients that can be expected without coefficient gcd computation.

3. THE MATRIX-TRIANGULARIZATION SUBRESULTANT PRS METHOD

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

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

Step 2: Using Dodgson's algorithm (D) (and bubble pivot), transform the matrix corresponding to 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 2.

The computing time of this method is given by the following theorem (see [2]).

Theorem 3: Let $p_1(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_0$ and $p_2(x) = d_m x^m + d_{m-1}x^{m-1} + \cdots + d_0$, $c_n \neq 0$, $d_m \neq 0, n \geq m$, 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 $0(n^5 L(|p|_\infty)^2)$ where $|p|_\infty = \max(|p_1|_\infty, |p_2|_\infty)$ and $L(|p|_\infty)$ is the length, in bits (or even the logarithm) of the maximum coefficient (of the two polynomials) in absolute value.

Proof: The result follows by combining (a) the well-known result that in the matrix-triangularization procedure there are performed $0(n^3)$ multiplications and (b) the fact that we are now using exact integer arithmetic and, hence, each multiplication is executed in time $0(n^2 L(|p|_\infty)^2)$ (see [2] and [3]). □

Below, we present the example stated in the introduction solved using this new approach; the reader should observe that the coefficients obtained for $p_3(x)$ are smaller than those obtained using the reduced (or the improved, for that matter) subresultant prs algorithm.

Example: Let us find the polynomial remainder sequence of the polynomials $p_1(x) = x^3 - 7x + 7$ and $p_2(x) = 3x^2 - 7$ using the matrix-triangularization procedure described above. Below, the matrix on the left side is the starting one, and the one on the right side is the final (transformed) one, obtained after application of Dodgson's method (D).

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

The *-ed row indicates that a (normal) pivot was performed between the third and fourth rows. With the help of Theorem 2 we see, from the transformed matrix, that the polynomial remainders (within sign) are $p_3(x) = -42x + 63$ and $p_4(x) = -49$ (as obtained before); also note that, using

this approach, there is no way for us to obtain the quotients. The smaller coefficients for $p_3(x)$ are obtained if we save the row before picot; in our example, the row before pivot was $p_3(x) = -14x + 21$, which was then changed to $p_3(x) = -42x + 63$. Thus, the remainder polynomials are $p_3(x) = -14x + 21$ and $p_4(x) = -49$ and, in this case, we did manage to reduce the coefficients of $p_3(x)$!

REFERENCES

1. Alkiviadis G. Akritas. "A Simple Validity Proof of the Reduced prs Algorithm." *Computing* **38** (1987):369-72.
2. Alkiviadis G. Akritas. "A New Method for Computing Greatest Common Divisors and Polynomial Remainder Sequences." *Numerische Mathematik* **52** (1988):119-27.
3. Alkiviadis G. Akritas. *Elements of Computer Algebra with Applications.* New York: Wiley Interscience, 1989.
4. E. H. Bareiss. "Sylvester's Identity and Multistep Integer-Preserving Gaussian Elimination." *Math. Comp.* **22** (1968):565-78.
5. W. S. Brown. "On Euclid's Algorithm and the Computation of Polynomial Greatest Common Divisors." *J. Assoc. Comput. Machinery* **18** (1971):476-504.
6. W. S. Brown. "The Subresultant prs Algorithm. *ACM Transactions on Mathematical Software* **4** (1978):237-49.
7. G. E. Collins. "Subresultants and Reduced Polynomial Remainder Sequences." *J. Assoc. Comput. Machinery* **14** (1967):128-42.
8. C. L. Dodgson. "Condensation of Determinants." *Proc. Royal Soc. London* **15** (1866):150-55.
9. L. H. Gonzalez, T. Recio Lombardi, & M.-F. Roy. "Specialization de la suite de Sturm et sous-resultants." Preprint No. 8-1990, Department of Mathematics, Statistics and Computation, University of Cantabria, 39071 Santander, Spain.
10. W. Habicht. "Eine Verallgemeinerung des Sturmschen Wurzelzaehlverfahrens." *Commentarii Mathematici Helvetici* **21** (1948):99-116.
11. Donald E. Knuth. *The Art of Computer Programming.* Vol. II, 2nd ed.: *Seminumerical Algorithms.* Reading, Mass.: Addison-Wesley, 1981.
12. M. A. Laidacker. "Another Theorem Relating Sylvester's Matrix and the Greatest Common Divisor." *Math. Magazine* **42** (1969):126-28.
13. R. Loos. "Generalized Polynomial Remainder Seqiemces." In *Computer Algebra Symbolic and Algebraic Computations*, Computing Supplement **4**:115-37. Ed. B. Buchberger, G. E. Collins, and R. Loos. New York: Springer Verlag, 1982.
14. J. J. Sylvester. "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." *Philosophical Trans.* **143** (1853):407-548.
15. E. B. Van Vleck. "On the Determination of a Series of Sturm's Functions by the Calculation of a Single Determinant." *Ann. Math. Second Series* **1** (1899-1900):1-13.
16. F. V. Waugh & P. S. Dwyer. "Compact Computation of the Inverse of a Matrix." *Ann. Math. Statis.* **16** (1945):259-71.

Historical Note: Note that we depart from established practice and give credit to Dodgson—and not to Bareiss [4]—for the integer-preserving transformations; see also the work of Waugh and Dwyer [16] 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 [16, p. 266]. Charles Lutwidge Dodgson (1832-1898) is the same person widely known for his writing *Alice in Wonderland* under the pseydonym Lewis Carroll.

AMS numbers: 68C20; 68C25; 01A55

❖❖❖