#36

THE TWO CLASSICAL SUBRESULTANT PRS METHODS

(*Extended Abstract*).

Alkiviadis G. Akritas*
Moscow State University
Department of Mathematics and Mechanics
Moscow 119899, USSR

---

*On a Fulbright grant for the Spring Semester 1990. Permanent address: University of Kansas, Department of Computer Science, Lawrence, KS 66045-2192.

Abstract. We present in some detail the two classical subresultant prs methods that exist in the literature for computing polynomial remainder sequences (prs) and greatest common divisors (gcd) of polynomials over the integers. Both methods are based on Sylvester's paper of 1853 [12]; the first method makes use of pseudodivisions whereas the second one triangularizes a matrix corresponding to the resultant of the two polynomials under consideration. The following figure demonstrates the relation of these two methods [3]

<-------- Sylvester's paper of 1853 -------->

↓ pseudodivisions

↓ matrix-triangularization

The two methods. We restrict our discussion to univariate polynomials with integer coefficients and to computations in $\mathbb{Z}[x]$, which is *not* a Euclidean 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 $\mathrm{lc}(p(x))$; 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 $\mathbb{Z}[x]$, $\deg(p_1(x)) = n$ and $\deg(p_2(x)) = m$, $n \geq m$.

The Pseudodivisions Subresultant PRS Method. We know that the polynomial division algorithm (with remainder), call it PD, that works over a field, cannot be used in $\mathbb{Z}[x]$ since it requires exact divisibility by $lc(p_2(x))$. So we use *pseudodivision*, which always yields a pseudoquotient and pseudoremainder; in this process we have to premultiply $p_1(x)$ by $lc(p_2(x))^{n-m+1}$ and then apply algorithm **PD**. That is, we have:

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

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)

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

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

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

$i = 1, 2, \ldots , h-1$. That is, if a method for choosing β_i is given, the above equation provides an algorithm for constructing a prs.

In Sylvester's approach of 1853 we have [12]

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

which is ideally suited for complete prs's; for incomplete prs's we can easily modify (3) to obtain

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

It should be noted that using (3′) we obtain smaller coefficients than those obtained by (3), but still, we do not obtain the smallest possible coefficients. This was achieved by Habicht in 1948 [8].

In Habicht's approach we have

$$\beta_1 = (-1)^{n_1 - n_2 + 1} \quad \text{and} \quad \beta_i = (-1)^{n_i - n_{i+1} + 1} \, lc(p_i(x)) H_i^{n_i - n_{i+1}},$$

$$i = 2, 3, \ldots, h-1, \qquad (4)$$

where

$$H_2 = lc(p_2(x))^{n_1 - n_2} \quad \text{and} \quad H_i = lc(p_i(x))^{n_{i-1} - n_i} H_{i-1}^{1-(n_{i-1} - n_i)}$$

$$i = 3, 4, \ldots, h-1.$$

In the case of incomplete prs's using (4) we obtain the smallest possible coefficients without coefficient gcd calculations. (Also note that in the case of complete prs's using (3), (3′) and (4) we obtain the same coefficients.)

In both cases above what we did was to divide $p_{i+2}(x)$ by the corresponding β_i before we use it again. The proofs that the β_i's shown in (3) and (4) exactly divide $p_{i+2}(x)$ have been presented in a very complicated fashion in [5], [6], and [7] and have up to now obscured simple divisibility properties [10]; see also [1].

The Matrix Triangularization Subresultant PRS Method. In this case we make use of Sylvester's form of the resultant (for the two polynomials $p_1(x)$ and $p_2(x)$ mentioned above)which can be expressed in the following form [2]:

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

Note that $p_2(x)$ has been transformed into a polynomial of degree n by introducing zero coefficients and that this is a matrix of order 2n (as opposed to n+m for the forms of the resultant encountered in the literature). This form of the resultant appears in Sylvester's paper of 1853 [12] and is only once mentioned in the literature by Van Vleck [13].

Van Vleck showed that, if we have the polynomial remainder sequence $p_1(x), p_2(x), \dots, p_h(x)$ we can obtain the (negated) coefficients of the $(i+1)$th member of the prs, $i = 0, 1, 2, \dots, h-1$, 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 successive column in turn. Moreover, it has been proved by Habicht [8] that the coefficients obtained in this way are the *smallest* possible without coefficient gcd computations; see also [9].

Using Bareiss's integer-preserving transformation algorithm [4] (see also Malashonok's preprint [11]) and *bubble pivot* we have shown the following:

Theorem. Let $p_1(x)$ and $p_2(x)$ be two polynomials of degree n and m respectively, $n \geq m$. Using Bareiss's algorithm transform the matrix $\mathbf{M}_S$ corresponding to $res_S(p_1(x), p_2(x))$ into its upper triangular form $T(\mathbf{M}_S)$; let n_i be the degree of the polynomial corresponding to the ith row of $T(\mathbf{M}_S)$, $i = 1, 2, \dots, 2n$, and let $p_k(x)$, $k \geq 2$, be the kth 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 $T(\mathbf{M}_S)$, the coefficients of $p_{k+1}(x)$ (within sign) are obtained from row $i+j$ of $T(\mathbf{M}_S)$, 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 $T(\mathbf{M}_S)$.)

For a proof and examples see [3].

References

[1] Akritas, A.G.: A simple proof of the reduced prs algorithm. Computing 38, 369–372, 1987.

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

[3] Akritas, A.G.: *Elements of Computer Algebra with Applications.* John Wiley, New York, 1989.

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

[5] Brown, W.S.: On Euclid's algorithm and the computation of polynomial greatest common divisors. Journal of ACM **18**, 476–504, 1971.

[6] Brown, W.S.: The subresultant prs algorithm. ACM Transactions On Mathematical Software **4**, 237–249, 1978.

[7] Collins, G.E.: Subresultants and reduced polynomial remainder sequences. Journal of ACM **14**, 128–142, 1967.

[8] Habicht, W.: Eine Verallgemeinung des Sturmschen Wurzelzälverfahrens. Commentarii Mathematici Helvetici **21**, 99–116, 1948.

[9] Laidacker, M.A.: Another theorem relating Sylvester's matrix and the greatest common divisor. Mathematics Magazine **42**, 126–128, 1969.

[10] Loos, R.: Generalized polynomial remainder sequences. In: Computer Algebra Symbolic and Algebraic Computations. Ed. by B. Buchberger, G.E. Collins and R. Loos, Springer Verlag, Wien, New York, 1982, Computing Supplement 4, 115–137.

[11] Malashonok, G.I.: Solution of a system of linear equations in a commutative ring. (In Russian.) Preprint FMI AS UkrSSR, Lvov 1986.

[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 algebraical 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, Second Series, Vol **1**, 1–13, 1899–1900.