Computing 38, 369–372 (1987)

Computing

A Simple Proof of the Validity of the Reduced prs Algorithm

A. G. Akritas, Lawrence, Kansas

Received November 11, 1986; revised February 23, 1987

Abstract — Zusammenfassung

A Simple Proof of the Validity of the Reduced prs Algorithm. Given two univariate polynomials with integer coefficients, it has been *rediscovered* [2] that the reduced polynomial remainder sequence (prs) algorithm can be used mainly to compute over the integers the members of a *normal* prs, keeping under control the coefficient growth and avoiding greatest common divisor (gcd) computations of the coefficients. The validity proof of this algorithm as presented in the current literature [2] is very involved and has obscured simple divisibility properties. In this note, we present Sylvester's theorem of 1853 [4] which makes these simple divisibility properties clear for normal prs's. The proof presented here is a modification of Sylvester's original proof.

AMS Subject Classifications: 68A15, 68-03.

Key words: Polynomial greatest common divisor, polynomial remainder sequence, Sylvester's theorem (1853).

Ein einfacher Beweis der Gültigkeit des reduzierten Polynom-Rest-Sequenz-Algorithmus. Für zwei gegebene Polynome in einer Variablen und mit ganzzahligen Koeffizienten wurde *wiederentdeckt* [2], daß der reduzierte prs-Algorithmus hauptsächlich verwendet werden kann, um die Elemente einer *normalen* prs mit ganzzahligen Operationen zu berechnen, wobei das Anwachsen der Koeffizienten unter Kontrolle gehalten und vermieden wird, Berechnungen vom größten gemeinsamen Teiler der Koeffizienten durchzuführen. Der Beweis für diesen Algorithmus, wie er in der heutigen Literatur [2] präsentiert wird, ist sehr kompliziert und hat einfache Divisionseigenschaften verborgen. In dieser Mitteilung wird das Sylvestertheorem von 1853, welches diese einfache Divisionseigenschaften für normale prs klar macht, dargestellt. Der Beweis, der hier präsentiert wird, ist eine Modifikation von Sylvesters ursprünglichem Beweis.

Introduction

In this note we restrict our discussion to univariate polynomials with integer coefficients and to computations in $\boldsymbol{Z}[x]$ as a unique factorization domain; recall that $\boldsymbol{Z}[x]$ is the set of all univariate polynomials with integer coefficients. 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 $\boldsymbol{Z}[x]$, $\deg(p_1(x))=n$ and $\deg(p_2(x))=m, n\geq m$. Clearly, the polynomial division (with remainder) algorithm, call it PD, that works over a field, cannot be used in $\boldsymbol{Z}[x]$

since it requires exact divisibility by $\mathrm{lc}(p_2(x))$. 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 $\mathrm{lc}(p_2(x))^{n-m+1}$ and then apply algorithm PD. Therefore we have:

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

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*

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

where $p_h(x) \neq 0$ is a greatest common divisor of $p_1(x)$ and $p_2(x)$. 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

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

$i = 1, 2, \ldots, h-1$. 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. In order both to control the coefficient growth and to avoid the coefficient gcd computations, it was *rediscovered* [2] that, mainly for normal prs's, the reduced prs algorithm can be used. In the reduced prs algorithm we set

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

or, since we deal mainly with normal prs's

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

That is, we divide $p_{i+2}(x)$ by the corresponding β_i before we use it again. However, as presented in [2], the proof of the fact that the β_i's shown above in (3) and (3') *exactly* divide $p_{i+2}(x)$ is rather involved and has obscured simple divisibility properties; see also ([3], p. 372).

Below, we present a theorem by Sylvester from 1853 which indicates that the reduced prs algorithm, as used *only* for normal prs's, is at least 133 years old; see also [1]. The proof given by Sylvester is simple and clearly demonstrates the existing divisibility properties. Moreover, it is worth mentioning that we have modified Sylvester's proof since he was interested in obtaining Sturm's sequences, where the

negative of each remainder is used; so, the determinants in his proof are exactly like the ones used below except for the fact that they have the second and third rows interchanged.

Sylvester and the Reduced prs Algorithm

While computing the greatest common divisor of two polynomials with integer coefficients, Sylvester [1853] was interested in removing the *allotrious factors* in order to keep the coefficient growth of the *normal* polynomial remainder sequence under control. We have the following:

Theorem (*Sylvester* 1853): *Let* $p_1(x), p_2(x), p_3(x), \ldots, p_h(x)$ *be a normal polynomial remainder sequence,* $p_i(x) \in \boldsymbol{Z}[x]$, *for* $i = 1, 2, \ldots, h$. *Then* $\mathrm{lc}(p_i(x))^2 \mid p_{i+2}(x)$, $1 < i \leq h-2$; *that is, the square of the leading coefficient of* $p_i(x)$ *is a divisor of* $p_{i+2}(x)$.

Proof: Let $a, b, c, d, \ldots$ be the coefficients of any divident $p_{i-1}(x)$ and $\alpha, \beta, \gamma, \delta, \ldots$ of the divisor $p_i(x)$, where $a = \mathrm{lc}(p_{i-1}(x))$ and $\alpha = \mathrm{lc}(p_i(x))$. Then, it is easily seen that the coefficients of the remainder $p_{i+1}(x)$, forming the second divisor, are:

$$(1/a^2) \cdot \begin{vmatrix} a & b & c \\ \alpha & \beta & \gamma \\ 0 & \alpha & \beta \end{vmatrix}, \quad (1/a^2) \cdot \begin{vmatrix} a & b & d \\ \alpha & \beta & \delta \\ 0 & \alpha & \gamma \end{vmatrix}, \quad (1/a^2) \cdot \begin{vmatrix} a & b & e \\ \alpha & \beta & \varepsilon \\ 0 & \alpha & \delta \end{vmatrix}, \ldots$$

In the same way, the coefficients of the second remainder

$$\left(\text{setting } m := \begin{vmatrix} a & b & c \\ \alpha & \beta & \gamma \\ 0 & \alpha & \beta \end{vmatrix} \right)$$

will be each of the form of the compound determinant:

$$(1/m^2) \cdot \begin{vmatrix} & \alpha & & & \beta & & & \gamma & \\ a & b & c & a & b & d & a & b & e \\ \alpha & \beta & \gamma & \alpha & \beta & \delta & \alpha & \beta & \varepsilon \\ 0 & \alpha & \beta & 0 & \alpha & \gamma & 0 & \alpha & \delta \\ & & & a & b & c & a & b & d \\ & 0 & & \alpha & \beta & \gamma & \alpha & \beta & \delta \\ & & & 0 & \alpha & \beta & 0 & \alpha & \gamma \end{vmatrix}$$

where the above expression is $\mathrm{lc}(p_{i+2}(x))$. Omitting the common multiplier $(1/m^2)$ and expanding along the first column, the determinant above is equal to

$$\alpha \left\{ \begin{vmatrix} a & b & d \\ \alpha & \beta & \delta \\ 0 & \alpha & \gamma \end{vmatrix} \cdot \begin{vmatrix} a & b & d \\ \alpha & \beta & \delta \\ 0 & \alpha & \gamma \end{vmatrix} - \begin{vmatrix} a & b & c \\ \alpha & \beta & \gamma \\ 0 & \alpha & \beta \end{vmatrix} \cdot \begin{vmatrix} a & b & e \\ \alpha & \beta & \varepsilon \\ 0 & \alpha & \delta \end{vmatrix} \right\}$$

$$- \begin{vmatrix} \alpha & b & c \\ \alpha & \beta & \gamma \\ 0 & \alpha & \beta \end{vmatrix} \left\{ \beta \cdot \begin{vmatrix} a & b & d \\ \alpha & \beta & \delta \\ 0 & \alpha & \gamma \end{vmatrix} - \gamma \cdot \begin{vmatrix} a & b & c \\ \alpha & \beta & \gamma \\ 0 & \alpha & \beta \end{vmatrix} \right\}$$

Expanding again, we see that (for some expressions A, B) the first term is of the form

$$\alpha^2 A + \alpha(a\beta\gamma \cdot a\beta\gamma - \alpha\beta^2 \cdot a\beta\delta),$$

whereas the second term is of the form (expand and simplify the expression in the brackets first)

$$\alpha^2 B - \alpha(\gamma^2 - \beta\delta) a^2 \beta^2.$$

Hence, after cancellations, the entire determinant is of the form $\alpha^2 (A + B)$ and we see that α^2 will enter as a factor into this and every coefficient of $p_{i+2}(x)$.

Sylvester's theorem indicates a divisibility property that exists between *certain* members of normal prs's and as a result of which we easily see the validity of the reduced prs algorithm. Sylvester indicates that "the same explicit method might be applied to show, that if the first divisor were e degrees instead of being only one degree lower than the first divident, α^{e+1} would be contained in every term of the second residue; the difficulty, however, of the proof by this method augments with the value of e" ([4], p. 419).

References

[1] Akritas, A. G.: A new method for computing polynomial greatest common divisors. University of Kansas, TR-86-9, Lawrence, Kansas, 1986. Submitted for publication.

[2] Collins, G. E.: Subresultants and reduced polynomial remainder sequences. JACM *14*, 128–142 (1967).

[3] Knuth, D.: The art of computer programming. Vol. II: Seminumerical algorithms. Reading, Mass.: Addison-Wesley 1969.

[4] 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).

Alkiviadis G. Akritas
University of Kansas
Department of Computer Science
Lawrence, KS 66045
U.S.A.

Verleger: Springer-Verlag KG, Mölkerbastei 5, A-1010 Wien. — Herausgeber: Prof. Dr. Hans J. Stetter, Institut für Angewandte und Numerische Mathematik der Technischen Universität Wien, Wiedner Hauptstraße 6—10, A-1040 Wien. — Redaktion: Wiedner Hauptstraße 6—10, A-1040 Wien. — Hersteller: Satz Austro-Filmsatz Richard Gerin, Zirkusgasse 13, A-1020 Wien, Druck Paul Gerin, Zirkusgasse 13, A-1021 Wien. — Verlagsort: Wien. — Herstellungsort: Wien. — Printed in Austria.