On the Subresultant PRS Algorithm

W. S. Brown

Bell Laboratories,
Murray Hill, New Jersey 07974

ABSTRACT

This paper is a sequel to two earlier papers [1, 2] on the generalization of Euclid's algorithm to domains of polynomials.

In attempting such a generalization one easily arrives at the concept of a *polynomial remainder sequence* (PRS), and then quickly discovers the phenomenon of explosive coefficient growth.

Fortunately, this explosive growth is not inherent in the problem, but is only an artifact of various naive solutions. If one removes the *content* (that is, the greatest common divisor of the coefficients) from each polynomial in a PRS, the coefficient growth in the resulting *primitive PRS* is relatively modest. However, the cost of computing the content (by applying Euclid's algorithm in the coefficient domain) may be unacceptably or even prohibitively high, especially if the coefficients are themselves polynomials in one or more additional variables.

The key to controlling coefficient growth without the costly computation of greatest common divisors (GCD's) of coefficients is the discovery by Collins [3] that every polynomial in a PRS is proportional to some subresultant of the first two. By arranging for the constants of proportionality to be unity, Collins developed the *subresultant PRS algorithm,* which is the subject of this paper. Unfortunately, Collins' formulation of the algorithm was too complicated for convenient application, and he therefore recommended the simpler *reduced PRS algorithm* as a practical compromise.

Later, Brown and Traub [1] discovered the *fundamental theorem of subresultants,* and used it to derive a much simpler formulation of the subresultant PRS algorithm. Also, Brown [2] derived essentially linear bounds on the coefficient growth in a subresultant PRS, while showing that the coefficient growth in a reduced PRS can be exponential if the sequence involves degree differences greater than unity. Although such *abnormal* sequences are a set of measure zero in the space of all PRS's, they are not uncommon in practice, and it is important to deal sensibly with them when they arise.

A few months after [1] and [2] were published, I discovered a corollary of the fundamental theorem, which led to a simpler derivation and deeper understanding of the subresultant PRS algorithm. The new approach, which is presented in this paper, reveals the subresultant PRS algorithm as a simple generalization of the reduced PRS algorithm, and converts the conjecture that was mentioned in [1] and [2] into an elementary remark.

Although I cannot assert with confidence that the subresultant PRS algorithm is optimal for any important class of problems, it is clearly the best of its kind and deserves to be thoroughly understood. Among its competitors are the *modular GCD algorithm,* which is shown in [2] to be superior if the given polynomials are sufficiently large and sufficiently dense, and the *EZ-GCD algorithm* of Moses and Yun [4], which is also modular, but has the advantage of benefiting from sparseness. On the other hand, if one desires only the resultant of the given polynomials, and their degrees are not too large, it may be advantageous to evaluate Sylvester's determinant, or the equivalent but lower-order Bezout's determinant, via expansion by minors. The merits of this approach are explored empirically by Ku and Adler [5], and their important but overstated conclusions are challenged by Collins [6].

In this paper the subresultant PRS algorithm is presented from the new viewpoint, and the outstanding conjecture is proved. The algorithm is then analyzed, and its practical importance is assessed.

[1] W. S. Brown and J. F. Traub, "On Euclid's Algorithm and the Theory of Subresultants", *J. ACM* **18,** pp. 505-514 (October 1971).

[2] W. S. Brown, "On Euclid's Algorithm and the Computation of Polynomial Greatest Common Divisors", *J. ACM* **18,** pp. 478-504 (October 1971).

[3] G. E. Collins, "Subresultants and Reduced Polynomial Remainder Sequences", *J. ACM* **14,** pp. 128-142 (1967).

[4] Joel Moses and David Y. Y. Yun, "The EZ GCD Algorithm", *Proc. of the ACM National Conference,* pp. 159-166 (August 1973).

[5] S. Y. Yu and R. J. Adler, "Computing Polynomial Resultants: Bezout's Determinant vs. Collins' Reduced PRS Algorithm", *Comm. ACM* **12,** pp. 23-30 (January 1969).

[6] G. E. Collins, "Comment on a Paper by Ku and Adler", Letter to the Editor, *Comm. ACM* **12,** pp. 302-303 (June 1969).