New structure theorems for subresultants

Mohab Safey El Din
en collaboration avec
H. Lombardi et M.F Roy

February 8, 1999

La suite des sous-résultants est un outil fondamental de la Géométrie Algébrique Réelle et plus particulièrement du Calcul Formel. Dérivée de la suite des restes euclidiens, elle sert à calculer l'indice de Cauchy et permet ainsi le comptage et l'isolation des racines réelles d'un polynôme univarié par des méthodes formelles. Avec l'essort du Calcul Formel, et l'exploration de nouveaux domaines par celui-ci, le calcul de cette suite (quadratique en complexité théorique) a trouvé de nouvelles applications et est aujourd'hui une routine de base dans bon nombre d'algorithmes. En effet, elle est utilisée en théorie de Galois par certains algorithmes de calul des résolvantes, pour la résolution de systèmes d'équations polynomiales par les algorithmes de triangulation, ainsi que dans l'algorithme de construction d'une décomposition cylindrique algébrique.

Les progrès algorithmiques pour le calcul de cette suite constituent donc un enjeu majeur pour le calcul formel. Les travaux de D. Lazard [7], ainsi que ceux de T. Lickteig et M.F. Roy [8] ont permis de faire des progrès lorsque des sauts de degré apparaissent dans la suite des restes. En revanche, aucun progrès ne fut constaté dans les cas génériques. Le récent travail de L. Ducos [4] va dans ce sens. L'idée clé de tous ces travaux est de mieux comprendre la structure de la matrice de Sylvester, pour en déduire de nouveaux théorèmes de structure permettant de limiter la croissance des coefficients intermédiaires apparaissant au cours de l'algorithme de calcul.

En effet, les sous-résultants sont des polynômes ayant comme coefficients des mineurs extraits de la matrice de Sylvester. La difficulté repose dans le "dilemme" suivant. Si A et B sont deux polynômes univariés de degré $\leq d$ et dont la taille maximale en bits des coefficients est τ, la méthode de Jordan-Bareiss permet de calculer ces mineurs en produisant des résultats intermédiaires de taille 2τ. En revanche elle effectue $O(d^3)$ opérations arithmétiques.

L'algorithme classique des sous-résultants (qui utilise mieux les propriétés de cette matrice) n'effectue que $O(d^2)$ opérations arithmétiques mais il crée des coefficients intermédiaires de taille 3τ lorsqu'il n'y a pas de sauts de degré dans la suite des restes. Lorsque des sauts de degré apparaissent dans la suite des restes, la croissance des coefficients intermédiaires n'est plus en $O(\tau)$.

Nous proposons un algorithme en $O(d^2)$ opérations arithmétiques dont les coefficients intermédiaires sont de taille 2τ (l'algorithme de [4] a les mêmes caractéristiques). L'idée clé de cet algorithme est de préciser les relations entre les coefficients sous-résultants de A et B d'une part, et de A et XB d'autre part. Pour parvenir à ces résultats, nous introduisons la notion de G-reste (résultat de la division de deux polynômes en forçant le quotient à être unitaire : $\mathrm{GRem}(A,B) = -\frac{\mathrm{lc}(B)}{\mathrm{lc}(A)}\mathrm{Rem}(A,B)$). Nous étudions les propriétés de la suite des G-restes et définissons une *forme r-réduite* des mineurs de la matrice de Sylvester pour corréler la suite des sous-résultants avec la suite des G-restes en faisant de l'algèbre linéaire sur les polynômes. Nous redémontrons ainsi le théorème de structure dans [8]. Puis, en étudiant les passages des mineurs de la matrice de Sylvester associée au couple (A, B), aux mineurs de la matrice de Sylvester associée au couple (A, XB) et inversement (qui se font simplement par manipulation de lignes), nous mettons à profit le formalisme précédemment introduit pour déduire de nouvelles relations et donc un nouveau théorème de structure plus fin que ceux que l'on peut trouver dans la littérature.

Nous en déduisons un algorithme que nous avons implanté en langage Aldor. Nous procédons pour terminer à l'analyse des résultats expérimentaux que nous obtenons et constatons des progrès notables (comparativement à l'algorithme classique) en particulier dans le cas de polynômes à coefficients polynomiaux et dans les cas génériques. Les temps de calcul sont équivalents à ceux de [4].

Signalons pour terminer que dans le cas générique, notre algorithme est identique à celui de [10] que nous redémontrons dans le formalisme développé.

References

[1] Brown, W. S. *On Euclid's algorithm and the computation of polynomial greatest common divisors.* J. Assoc. Comput. Machin. 18, 478-504 (1971)

[2] Brown, W. S., Traub, J.F. *On Euclid's algorithm and the theory of subresultants.* J. Assoc. Comput. Machin. 18, 505-514 (1971)

[3] Collins, G. E. *Subresultants and reduced polynomial remainder sequences.* J. Assoc. Comput. Mach. 14, 128-142 (1967)

[4] Ducos L. *Optimizations of the subresultant algorithm*, to appear in Journal of Pure and Applied Algebra.

[5] L. Gonzalez, H. Lombardi, T. Recio, and M.-F. Roy, Spécialisation de la suite de Sturm et sous-résultants I, *Informatique théorique et applications* **24** (1990), 561- 588.

[6] W. Habicht, Eine Verallgemeinerung des Sturmschen Wurzelzählverfahrens, *Comm. Math. Helvetici* **21** (1948), 99-116.

[7] D. Lazard, Sous-résultants, Manuscrit non publié.

[8] Lickteig, T., Roy, M.-F. *Cauchy Index computation.* Calcolo, 33, 337-351 (1996)

[9] R. Loos, Generalized polynomial remainder sequences, in: *Computer algebra, symbolic and algebraic computation*, Springer-Verlag, Berlin (1982).

[10] C. Quitté, Une démonstration de l'algorithme de Bareiss par l'algèbre extérieure, Manuscrit non publié.

[11] L. González-Vega, F. Rouillier, M.-F. Roy, G. Trujillo Symbolic Recipes for Real Solutions, In: Some tapas of computer algebra, A. Cohen ed. Springer, to appear.