EXTRACTA MATHEMATICAE 5, n.3, 150-152 (1990)

A Subresultant Theory for Multivariate Polynomials

Laureano González Vega[1]
Dpto. Matemáticas, Estadística y Computación
Universidad de Cantabria, Santander 39071, Spain

1990 A.M.S. Classification 13P10

In Computer Algebra, Subresultant Theory provides a powerful method to construct algorithms solving problems for polynomials in one variable in an optimal way. So, using this method we can compute the greatest common divisor of two polynomials in one variable with integer coefficients avoiding the exponential growth of the coefficients that will appear if we use the Euclidean Algorithm.

In this note, generalizing a forgotten construction appearing in [Hab], we extend the Subresultant Theory to the multivariate case. In order to achieve this, first of all, we introduce the definition of subresultant sequence asociated to two polynomials in one variable with coefficients in an integral domain and the properties of this sequence that we would like to extend to the multivariate case.

Let $\mathbb{D}$ be an integral domain, $\mathbb{F}$ its quotient field and $\mathbb{K}$ the algebraic clousure of $\mathbb{F}$. We consider two polynomials P and Q in $\mathbb{D}[x]$ and two positive integers p and q verifying $\deg(P) \leq p$ and $\deg(Q) \leq q$. The subresultant sequence associated to P, p, Q and q is a list of polynomials in $\mathbb{D}[x]$:

$$\{\mathbf{Sres}_i(P,p,Q,q)\}_{i\in\{1,\ldots,\inf(p,q)-1\}}$$

where each polynomial $\mathbf{Sres}_i(P,p,Q,q)$ is defined as follows:

$$\mathbf{Sres}_i(P,q,Q,q) = \textstyle\sum_{j=0}^{i} M_j^i(P,Q)x^j = M_i^i(P,Q)x^i + \cdots + M_1^i(P,Q)x + M_0^i(P,Q)$$

with every $M_j^i(P,Q)$ the determinant of the matrix built with the columns $1,2,\ldots,p+q-2i-1,p+q-i-j$ in the matrix:

$$m_i(P,p,Q,q) = \overbrace{\begin{pmatrix} a_p & \dots & a_0 & & \\ & \ddots & & \ddots & \\ & & a_p & \dots & a_0 \\ b_q & \dots & b_0 & & \\ & \ddots & & \ddots & \\ & & b_q & \dots & b_0 \end{pmatrix}}^{p+q-i} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} q-i \\ \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} p-i \end{matrix}$$

For each i in $\{1,\ldots,\inf(p,q)-1\}$ we shall note:

$$S_i(P,Q) = \mathbf{Sres}_i(P,\deg(P),Q,\deg(Q)) \qquad s_i(P,Q) = M_i^i(P,Q)$$

and if $s_i(P,Q)$ is different from 0 we shall say that $S_i(P,Q)$ is regular, otherwise defective.

The most important properties of the subresultant sequence associated to two polynomials P and Q in $\mathbb{D}[x]$ that we shall try to generalize to the multivariate case are the following:

Property I

For each i in $\{1,\ldots,\inf(p,q)-1\}$ the polynomial $S_i(P,Q)$ is in the ideal of $\mathbb{D}[x]$ generated by P and Q and it is posible to construct polynomials U_i and V_i in $\mathbb{D}[x]$ such that $U_iP + V_iQ = S_i(P,Q)$.

Property II

In the following situation:

$$s_0(P,Q) = \ldots = s_{k-1}(P,Q) = 0 \qquad \text{and} \qquad s_k(P,Q) \neq 0$$

we conclude that $S_k(P,Q)$ is a greatest common divisor of P and Q in $\mathbb{F}[x]$.

Property III

$$s_0(P,Q) = 0 \qquad \Longleftrightarrow \qquad \exists x_0 \in \mathbb{K} \qquad P(x_0) = Q(x_0) = 0$$

[1] Partially supported by CICyT PA 86/471 and PB 62/86.

Property IV
A subresultant sequence associated to P and Q can be computed in an easy way (using only $O(\deg(P)\deg(Q))$ arithmetic operations in $\mathbb{D}$) without computing the determinants which appear in the subresultant polynomial definition. Moreover, if $\mathbb{D} = \mathbb{Z}$ then the size of every M_j^i (i.e. its $\log_2$) is bounded by:

$$\deg(P)\log_2(N(Q)) + \deg(Q)\log_2(N(P))$$

where $N(P)$ (resp. N(Q)) is the euclidean norm of the vector formed with the coefficients of P (resp. Q).

The proof of these properties and another ones related with subresultant theory can be found in [GLRR]. Next we generalize the subresultant construction for n polynomials $F_1,\ldots,F_n$ in $\mathbb{D}[x_1,\ldots,x_{n-1}]$ where $\mathbb{D}$ is an integral domain. If d_i is the degree of each F_i then we shall note:

- $D = 1 + \sum_{i=1}^{n}(d_i - 1)$, $L = \binom{n+D-1}{D}$,
- $\alpha = (\alpha_1,\ldots,\alpha_{n-1})$, $\quad x^\alpha = x_1^{\alpha_1}\cdots x_{n-1}^{\alpha_{n-1}}$, $\quad \mathbb{B}_{n-1}^D = \{x^\alpha / \sum_{i=1}^{n-1}\alpha_i \leq D\}$.

The set $\mathbb{B}_{n-1}^D$ of the monomials in $x_1,\ldots,x_{n-1}$ with degree smaller than D has cardinal equal to L and we shall consider in this set the partition given by:

-. for each j in $\{1,\ldots,n-1\}$:

$$\mathbb{B}_j = \{x^\alpha/\alpha_k < d_k \quad k = 1,\ldots,j-1 \quad , \quad \alpha_j \geq d_j\} = \{H_j^{(k)}/k = 1,\ldots,s_j\} = \{x_j^{d_j}H_{j,k}/k = 1,\ldots,s_j\},$$

-. for the index n:

$$\mathbb{B}_n = \{x^\alpha/\alpha_k < d_k \quad k = 1,\ldots,n-1\} = \{H_n^{(k)}/k = 1,\ldots,s_n\} = \{H_{n,k}/k = 1,\ldots,s_n\}.$$

Clearly the sets $\{\mathbb{B}_j\}_{j=1,\ldots,n}$ are a partition of $\mathbb{B}_{n-1}^D$ and we suppose that the monomials in $\mathbb{B}_{n-1}^D$ and in every $\mathbb{B}_j$ are ordered using first the total degree and after the lexicographical order with $x_1 > \ldots > x_{n-1}$. The next definition introduces in this situation the analogous for the Sylvester matrix of two polynomials in one variable, that is $m_0(P,\deg(P),Q,\deg(Q))$.

Definition 1
The matrix $m_0(F_1,\ldots,F_n)$ is defined as follows:

> for each j in $\{1,\ldots,n\}$ and for each i verifying $\sum_{u=0}^{j-1}s_u < i \leq \sum_{u=0}^{j}s_u$ (with $s_0 = 0$) the elements in the row i-th are the coefficients of the polynomial $H_{i-\sum_{u=0}^{j-1}s_u,j}F_j$ written respect to the monomials in $\mathbb{B}_{n-1}^D$.

In the following picture it is found, in a clearer way, how to construct the matrix $m_0(F_1,\ldots,F_n)$ using the coefficients of the F_i's:

$$\begin{array}{rc} & x^{\alpha_1} \quad \ldots\ldots \quad x^{\alpha_L} \\ \begin{matrix} H_{1,j}F_1\{ \\ \vdots \\ H_{n,j}F_n\{ \end{matrix} & \left(\begin{matrix} \qquad\qquad & & \qquad\qquad \\ & & \\ & & \end{matrix}\right) \end{array}$$

Next we define the analogous in this situation for the notion of subresultant polynomial for two polynomials in one variable:

Definition 2
Let k be a non-negative integer. We define the matrix $m_k(F_1,\ldots,F_n)$ as the submatrix of $m_0(F_1,\ldots,F_n)$ constructed with the coefficients of the polynomials $H_{i,j}F_i$ of degree smaller or equal than $D-k$ and written their coefficients respect to the monomials in $\mathbb{B}_{n-1}^D$ of degree smaller or equal than $D-k$. Denoting by a_k the number of polynomials $H_{i,j}F_i$ of degree smaller or equal than $D-k$ then the matrix $m_k(F_1,\ldots,F_n)$ has a_k rows and $\binom{n+D-k-1}{D-k}$ columns. If $a_k \geq \binom{n+D-k-1}{D-k} - \binom{n+k-2}{k-1}$ then for every monomial x^α with degree equal to k we define:

$$S_k^{x^\alpha}[F_1,\ldots,F_n] = \tau_k x^\alpha + \sum_{\deg(x^\beta)<k} \tau_k^{[x^\alpha,x^\beta]}x^\beta$$

where:

- τ_k is the determinant of the matrix T_k formed with the first a_k rows and columns of the matrix $m_k(F_1, \ldots, F_n)$,
- $\tau_k^{[x^\alpha, x^\beta]}$ is 0 if the index of the monomial x^β is smaller than a_k, otherwise the determinant of the matrix got replacing in the matrix T_k the column corresponding to x^α by the column in $m_k(F_1, \ldots, F_n)$ corresponding to x^β.

For $n = 2$ the definition 2 specializes to the construction of the subresultant polynomials associated to two polynomials in one variable as showed before. In [GV$_2$], using the subresultants of index 1, is constructed a determinantal formulae for the systems of n polynomial equations with n variables. The next theorem shows that the property I still remains true for this definition in the multivariable case.

Theorem 3
Let $F_1, \ldots, F_n$ be polynomials in $\mathbb{D}[x_1, \ldots, x_{n-1}]$. Every polynomial $S_k^{x^\alpha}[F_1, \ldots, F_n]$ is in the ideal generated by $F_1, \ldots, F_n$ in $\mathbb{D}[x_1, \ldots, x_{n-1}]$.

Proof:
It is enough to study carefully the determinants appearing in the definition of the coefficients for every polynomial $S_k^{x^\alpha}[F_1, \ldots, F_n]$. A more detailed proof can be found in [GV$_1$]. ∎

Definition 4
Let $F_1, \ldots, F_n$ be polynomials in $\mathbb{D}[x_1, \ldots, x_{n-1}]$. The subresultant sequence associated to $F_1, \ldots, F_n$ is the list of polynomials in $\mathbb{D}[x_1, \ldots, x_{n-1}]$, $\{\{S_k^{x^\alpha}[F_1, \ldots, F_n]\}_{\deg(x^\alpha)=k}\}_{k=1,\ldots,k_0}$, where k_0 is the first non-negative integer not verifying $a_k \geq \binom{n+D-k-1}{D-k} - \binom{n+k-2}{k-1}$.

Example 5
In the particular case of $n = 4$ and $k = 2$ the structure of the subresultant sequence is the following:

$$S_2^{x^2} = a_2x^2 + c_{1,1}x + c_{1,2}y + c_{1,3}z + c_{1,4}$$
$$S_2^{y^2} = a_2y^2 + c_{2,1}x + c_{2,2}y + c_{1,3}z + c_{2,4} \quad S_2^{z^2} = a_2z^2 + c_{3,1}x + c_{3,2}y + c_{3,3}z + c_{3,4}$$
$$S_2^{xy} = a_2xy + c_{4,1}x + c_{4,2}y + c_{4,3}z + c_{4,4} \quad S_2^{xz} = a_2xz + c_{5,1}x + c_{5,2}y + c_{5,3}z + c_{5,4}$$

The proof of the following theorems is based on Definition 2 and Theorem 3. A more detailed proof can be found in [GV$_1$].

Theorem 6
Let $F_1, \ldots, F_n$ be polynomials in $\mathbb{D}[x_1, \ldots, x_{n-1}]$. Then:
i-. if $\tau_0 = S_0^1[F_1, \ldots, F_n] \neq 0$ then the system $F_1 = 0$, $F_2 = 0$, ..., $F_n = 0$ has no solutions in $\mathbb{K}^{n-1}$,
ii-. the size of the coefficients of the polynomials in the subresultant sequence associated to $F_1, \ldots, F_n$ is bounded by $\binom{n+D-1}{D}\log_2(N(F))$ where $N(F)$ is the maximun of the euclidean norms of the F_i's vector coefficients.

Theorem 7
Let $F_1, \ldots, F_n$ be polynomials in $\mathbb{D}[x_1, \ldots, x_{n-1}]$ and H a greatest common divisor of the F_i's. If k is the total degree of H then:
i-. H divides every $S_k^{x^\alpha}[F_1, \ldots, F_n]$ and $\tau_0 = \ldots = \tau_k = 0$,
ii-. if there exists $S_{k+1}^{x^\alpha}[F_1, \ldots, F_n]$ non identically 0 the H agrees with $S_{k+1}^{x^\alpha}[F_1, \ldots, F_n]$ or such polynomial factorizes as the product of H and a polynomial of degree 1.

References.

[GV$_1$] L. González Vega: *Une théorie des sous-résultants pour les polynômes en plusieurs variables.* To appear in C. R. de la Academie des Sciences (1990).

[GV$_2$] L. González Vega: *A Determinantal Formulae for the Solution Set of Zero-Dimensional Ideals.* Submitted to the J. of Pure and Applied Algebra (1990).

[GLRR] L. González Vega, H. Lombardi, T. Recio, M.-F. Roy: *Specialisation de la suite de Sturm et sous-resultants (I and II).* To appear in Revue de Informatique Theorique -RAIRO- (1989).

[Hab] V. W. Habicht: *Zur inhomogenen eliminationstheorie.* Comm. Math. Helvetici 21, 79-98 (1948).