Resultants and Subresultants: Univariate vs. Multivariate Case

Carlos D'Andrea
Departament d'Àlgebra i Geometria
Facultat de Matemàtiques
Universitat de Barcelona
cdandrea@ub.edu

1 Univariate resultants and subresultants

1.1 Univariate Resultants

Consider the following homogeneous system of two linear equations in two unknowns:

$$\left\{\begin{array}{rcl} A\mathbf{x}_1 + B\mathbf{x}_2 & = & 0 \\ C\mathbf{x}_1 + D\mathbf{x}_2 & = & 0 \end{array}\right. . \tag{1}$$

It is very well-known that this system has a non-trivial solution if and only if $AD - BC$ equals to zero.

One can generalize the previous situation in two different directions. The most classical one is the notion of *determinant*, which is the condition under which a system of n homogeneous equations in n unknowns

$$\left\{\begin{array}{rcl} A_{11}\mathbf{x}_1 + A_{12}\mathbf{x}_2 + \ldots + A_{1n}\mathbf{x}_n & = & 0 \\ A_{21}\mathbf{x}_1 + A_{22}\mathbf{x}_2 + \ldots + A_{2n}\mathbf{x}_n & = & 0 \\ \vdots & \vdots & \vdots \\ A_{n1}\mathbf{x}_1 + A_{n2}\mathbf{x}_2 + \ldots + A_{nn}\mathbf{x}_n & = & 0 \end{array}\right.$$

has a non-trivial solution. The other generalization is to consider two homogeneous forms of higher degrees:

$$\left\{\begin{array}{rclcl} f(\mathbf{x}_1, \mathbf{x}_2) & := & A_0\mathbf{x}_1^n + A_1\mathbf{x}_1^{n-1}\mathbf{x}_2 + \ldots + A_n\mathbf{x}_2^n & = & 0 \\ g(\mathbf{x}_1, \mathbf{x}_2) & := & B_0\mathbf{x}_1^m + B_1\mathbf{x}_1^{m-1}\mathbf{x}_2 + \ldots + B_m\mathbf{x}_2^m & = & 0 \end{array}\right. . \tag{2}$$

```
Which is the condition under which (2) has a non-trivial solution?
```

Note that in this case, the answer to this question depends on where we allow the solutions to live. Let us assume for a while that the A_i, B_j's live in an algebraically closed field $\mathbb{K}$. Then

Proposition 1.1. *The following are equivalent*

1. *There exists* $(x_0 : y_0) \in \mathbb{P}^1_{\mathbb{K}}$ *such that* $f(x_0, y_0) = g(x_0, y_0) = 0$.
2. *There exists* $h(\mathbf{x}_1, \mathbf{x}_2) \in \mathbb{K}[\mathbf{x}_1, \mathbf{x}_2]_{\geq 1}$ *such that* $h(\mathbf{x}_1, \mathbf{x}_2)$ *divides* $f(\mathbf{x}_1, \mathbf{x}_2)$ *and* $g(\mathbf{x}_1, \mathbf{x}_2)$.
3. *Let* K *be any field that contains the coefficients of* $f(\mathbf{x}_1, \mathbf{x}_2)$ *and* $g(\mathbf{x}_1, \mathbf{x}_2)$. *There exists* $h(\mathbf{x}_1, \mathbf{x}_2) \in K[\mathbf{x}_1, \mathbf{x}_2]_{\geq 1}$ *such that* $h(\mathbf{x}_1, \mathbf{x}_2)$ *divides* $f(\mathbf{x}_1, \mathbf{x}_2)$ *and* $g(\mathbf{x}_1, \mathbf{x}_2)$ *in* $K[\mathbf{x}_1, \mathbf{x}_2]$.

Note that the last condition can be translated into linear algebra in the coefficient field. The existence of such and $h(\mathbf{x}_1, \mathbf{x}_2)$ can be checked by testing if the linear map

$$\begin{array}{cccc} \phi & : & K[\mathbf{x}_1, \mathbf{x}_2]_{m-1} \oplus K[\mathbf{x}_1, \mathbf{x}_2]_{n-1} & \to & K[\mathbf{x}_1, \mathbf{x}_2]_{m+n-1} \\ & & (a(\mathbf{x}_1, \mathbf{x}_2), b(\mathbf{x}_1, \mathbf{x}_2)) & \mapsto & a(\mathbf{x}_1, \mathbf{x}_2)f(\mathbf{x}_1, \mathbf{x}_2) + b(\mathbf{x}_1, \mathbf{x}_2)g(\mathbf{x}_1, \mathbf{x}_2) \end{array} \tag{3}$$

is bijective or not. Indeed, if we have

$$\begin{array}{rcl} f(\mathbf{x}_1, \mathbf{x}_2) & = & l(\mathbf{x}_1, \mathbf{x}_2)\, F(\mathbf{x}_1, \mathbf{x}_2) \\ g(\mathbf{x}_1, \mathbf{x}_2) & = & l(\mathbf{x}_1, \mathbf{x}_2)\, G(\mathbf{x}_1, \mathbf{x}_2) \end{array}$$

for a linear form $l(\mathbf{x}_1, \mathbf{x}_2)$ then the vector $(G(\mathbf{x}_1, \mathbf{x}_2), -F(\mathbf{x}_1, \mathbf{x}_2))$ lies in the kernel of ϕ. Reciprocally, one can show that if there is a non-trivial element in the kernel of ϕ, then the gcd of $f(\mathbf{x}_1, \mathbf{x}_2)$ and $g(\mathbf{x}_1, \mathbf{x}_2)$ has positive degree.

Definition 1.2. The *resultant* of $f(\mathbf{x}_1, \mathbf{x}_2)$ and $g(\mathbf{x}_1, \mathbf{x}_2)$ is the determinant of the matrix of ϕ in the monomial bases.

Ordering conveniently the monomial bases, we have that the resultant of $f(\mathbf{x}_1, \mathbf{x}_2)$ and $g(\mathbf{x}_1, \mathbf{x}_2)$ (Res(f, g) for short) equals

$$\mathrm{Res}(f, g) := \det \begin{array}{c} m+n \\ \left|\begin{array}{cccccc} A_n & \cdots & A_0 & & & \\ & \ddots & & \ddots & & \\ & & A_n & \cdots & A_0 & \\ \hline B_m & \cdots & B_0 & & & \\ & \ddots & & \ddots & & \\ & & B_m & \cdots & B_0 & \end{array}\right| \end{array} \begin{array}{c} m \\ \\ n \end{array} \tag{4}$$

Corollary 1.3.

$$\deg\left(\gcd(f(\mathbf{x}_1, \mathbf{x}_2), g(\mathbf{x}_1, \mathbf{x}_2))\right) = 0 \iff \mathrm{Res}(f, g) \neq 0.$$

1.2 Univariate Subresultants

Now we will focus in a more general problem. Let $k \leq \min\{m, n\}$. We want to answer the following question:

$$\boxed{\deg \gcd\left(f(\mathbf{x}_1, \mathbf{x}_2), g(\mathbf{x}_1, \mathbf{x}_2)\right) = k \iff ????}$$

The solution is related with the rank of the matrix of ϕ above. Also, one can study simpler linear transformations like the following:

$$\begin{array}{cccc} \phi_k & : & K[\mathbf{x}_1, \mathbf{x}_2]_{m-1-k} \oplus K[\mathbf{x}_1, \mathbf{x}_2]_{n-1-k} & \to & K[\mathbf{x}_1, \mathbf{x}_2]_{m+n-1-k} \\ & & (a(\mathbf{x}_1, \mathbf{x}_2), b(\mathbf{x}_1, \mathbf{x}_2)) & \mapsto & a(\mathbf{x}_1, \mathbf{x}_2) f(\mathbf{x}_1, \mathbf{x}_2) + b(\mathbf{x}_1, \mathbf{x}_2) g(\mathbf{x}_1, \mathbf{x}_2) \end{array} \tag{5}$$

The *scalar subresultant* $S_k^{(j)}$ of $f(\mathbf{x}_1, \mathbf{x}_2)$ and $g(\mathbf{x}_1, \mathbf{x}_2)$ is defined for $0 \leq j \leq k \leq \min\{m, n\}$ as the following determinant:

$$S_k^{(j)} := \det \begin{array}{c} m+n-2k \\ \left|\begin{array}{cccccc} A_n & \cdots & & \cdots & A_{k+1-(m-k-1)} & A_{j-(m-k-1)} \\ & \ddots & & & \vdots & \vdots \\ & & A_n & \cdots & A_{k+1} & A_j \\ \hline B_m & \cdots & & \cdots & B_{k+1-(n-k-1)} & B_{j-(n-k-1)} \\ & \ddots & & & \vdots & \vdots \\ & & B_m & \cdots & B_{k+1} & B_j \end{array}\right| \end{array} \begin{array}{c} \\ m-k \\ \\ \\ n-k \\ \end{array} \tag{6}$$

where $A_\ell = B_\ell = 0$ for $\ell < 0$.

The *subresultant polynomial* $\mathrm{Sres}_k(f, g)$ is defined for $0 \leq k \leq \min\{m, n\}$ as

$$\mathrm{Sres}_k(f, g) := \sum_{j=0}^{k} S_k^{(j)} \mathbf{x}_1^j \mathbf{x}_2^{k-j}.$$

When $k = 0$, $Sres_0(f, g) = S_0^{(0)}$ coincides with $\mathrm{Res}(f, g)$.

Scalar subresultants satisfy the following property:

Proposition 1.4.

$$\boxed{\deg \gcd(f, g) = k \iff S_\ell^{(\ell)} = 0 \textit{ for } 0 \leq \ell < k \textit{ and } S_k^{(k)} \neq 0.}$$

Moreover, the polynomial subresultants $\mathrm{Sres}_k(f, g)$ are determinant expressions for modified remainders in the Euclidean algorithm. In particular, for the first k such that $S_k^{(k)} \neq 0$,

$$\gcd(f, g) = \mathrm{Sres}_k(f, g).$$

The theory of resultants and subresultants of two univariate polynomials go back to Leibniz, Euler, Bézout and Jacobi. In their modern form, subresultants were introduced by Sylvester in [27]. They have been used to give an efficient and parallelable algorithm for computing the greatest common divisor of two polynomials [4, 3, 12, 8, 16, 17, 26]. More recently they were also applied in symbolic-numeric computation [9, 31, 23, 30].

2 Multivariate Resultants

Now we would like to generalize the case of two homogeneous polynomials in two homogeneous variables to a more general setting. We will also generalize the situation of the $n \times n$ determinant.

Let $d_1, \ldots, d_n$ be a set of positive integers. Consider the following system of homogeneous equations:

$$\left\{ \begin{array}{lcl} \sum_{|\alpha|=d_1} A_{1\alpha}\mathbf{X}^\alpha & = & 0 \\ \sum_{|\alpha|=d_2} A_{2\alpha}\mathbf{X}^\alpha & = & 0 \\ \vdots & \vdots & \vdots \\ \sum_{|\alpha|=d_n} A_{n\alpha}\mathbf{X}^\alpha & = & 0 \end{array} \right. \tag{7}$$

where $\alpha \in \mathbb{N}^n$, $\mathbf{X}^\alpha = \mathbf{x_1}^{\alpha_1}\mathbf{x_2}^{\alpha_2}\ldots\mathbf{x}_n{}^{\alpha_n}$. We want to answer the following question:

`Which is the condition under which (7) has a non-trivial solution?`

Denote with

$$\left\{ \begin{array}{lcl} f_1(\mathbf{X}) & := & \sum_{|\alpha|=d_1} A_{1\alpha}\mathbf{X}^\alpha \\ f_2(\mathbf{X}) & := & \sum_{|\alpha|=d_2} A_{2\alpha}\mathbf{X}^\alpha \\ \vdots & \vdots & \vdots \\ f_3(\mathbf{X}) & := & \sum_{|\alpha|=d_n} A_{n\alpha}\mathbf{X}^\alpha \end{array} \right. \tag{8}$$

We have the following

Theorem 2.1. *There exists an irreducible polynomial* Res *in* $\mathbb{Z}[A_{i,\alpha}]$ *such that it vanishes after a specialization of the* $A_{i\alpha}$*'s in a field* $\mathcal{K}$ *if and only if the specialized system (7) has a solution in* $\mathbb{P}^{n-1}_{\overline{\mathcal{K}}}$.

The polynomial Res is called the *multivariate resultant* of $f_1, \ldots, f_n$. Multivariate resultants were mainly introduced by Macaulay in [25], after earlier work by Euler, Sylvester and Cayley. The can be computed by manipulating the maximal minors of the following map which should be regarded as a generalization of (2):

$$\begin{array}{ccc} \oplus_{i=1}^n K[\mathbf{X}]_{t-d_i} & \mapsto & K[\mathbf{X}]_t \\ (A_1(\mathbf{X}), \ldots, A_n(\mathbf{X})) & \mapsto & \sum_{i=1}^n A_i(\mathbf{X}) f_i(\mathbf{X}) \end{array} \tag{9}$$

for t big enough, namely for $t > (d_1 - 1) + \ldots + (d_n - 1)$. Here, K is any field that contains all the coefficients of the f_i's.

3 Multivariate Subresultants

What do we get if we check the maximal minors of the map (9) for small values of t? The answer will be given by *multivariate subresultants*, which we will see generalize very well the $S_k^{(j)}$ defined before. First we have the following

Proposition 3.1. *If the A_i, B_j have been specialized in a field $\mathcal{K}$ then $S_k^{(j)} = 0$ if and only if the set of monomials*

$$\{\mathbf{x}_1^{m+n-k-1}, \mathbf{x}_1^{m+n-k-2}\mathbf{x}_2, \ldots, \mathbf{x}_1^{m+n-k-j}\mathbf{x}_2^{j-1}, \mathbf{x}_1^{m+n-k-j-2}\mathbf{x}_2^{j+1}, \ldots, \mathbf{x}_1^{m+n-2k-1}\mathbf{x}_2^{k}\}$$

is linearly dependent in $\mathcal{K}[\mathbf{x}_1, \mathbf{x}_2]/\langle f(\mathbf{x}_1, \mathbf{x}_2), g(\mathbf{x}_1, \mathbf{x}_2)\rangle$.

We will generalize this as follows: let $s \leq n$ and set

$$S(T) := \frac{\prod_{i=1}^{s}(1 - T^{d_i})}{(1 - T)^n} = s_0 + s_1 T + \ldots$$

and $\mathcal{S} = \{\mathbf{X}^{\alpha_1}, \ldots, \mathbf{X}^{\alpha_{s_t}}\}$ be a set of s_t monomials in n variables of degree t.

Theorem 3.2. *There exists a polynomial $\Delta_{\mathcal{S}}$ in $\mathbb{Z}[A_{i,\alpha}]$ such that it vanishes after a specialization of the $A_{i\alpha}$'s in a field $\mathcal{K}$ if and only if the set $\mathcal{S}$ fails to be a linearly independent in $\mathcal{K}[\mathbf{X}]/\langle f_1(\mathbf{X}), \ldots, f_s(\mathbf{X})\rangle$.*

The polynomial $\Delta_{\mathcal{S}}$ is called the $\mathcal{S}$-*subresultant* associated to the system $(f_1, \ldots, f_s)$. Subresultants can also be computed by manipulations on the maximal minors of the matrix of (9). They were first defined by Gonzalez-Vega in [10, 11], generalizing Habicht's method [13].

4 General framework

From a more algebraic point of view, resultants and subresultants are elements of what is called an *Elimination Ideal* of a system of homogeneous polynomials. The following formalism is borrowed from the foundational work of Jouanolou [20, 21, 22] (see also [1]).

Let A be a commutative ring. For us, A is going to be the ring of coefficients of the input polynomials. Consider the graded polynomial ring $A[\mathbf{x}_1, \ldots, \mathbf{x}_n]$ with $\deg(\mathbf{x}_i) = 1$. Let $\mathcal{M}$ be its irrelevant homogeneous ideal $\mathcal{M} := \langle \mathbf{x}_1, \ldots, \mathbf{x}_n\rangle$.

Given a finitely generated homogeneous ideal $I := \langle f_1, \ldots, f_s\rangle \subset \mathcal{M}$, we set $B := A[\mathbf{X}]/I$ which is naturally a graded $A[\mathbf{X}]$-module (the grading is with respect to the variables $\mathbf{x}_1, \ldots, \mathbf{x}_n$).

We consider the incidence scheme

$$Proj(B) \subset \mathbb{P}_A^{n-1} := Proj\,(A[\mathbf{X}])$$

(this A-schemes inclusion is induced by the surjective map $A[\mathbf{X}] \to B$) and want to "compute" the image of its canonical projection on $Spec(A)$. This corresponds to *eliminating* the variables $\mathbf{x}_1, \ldots, \mathbf{x}_n$. It turns out that this image is closed and has a natural scheme structure. Its definition ideal is

$$\begin{aligned}\mathcal{U} \quad := \quad & Ker\left(A = \Gamma\left(Spec(A), \mathcal{O}_{Spec(A)}\right) \stackrel{can}{\to} \Gamma\left(Proj(B), \mathcal{O}_{Proj(B)}\right)\right) \subset A \\ & (I :_{A[\mathbf{x}]} \mathcal{M}^\infty) = H^0_{\mathcal{M}}(B)_0.\end{aligned}$$

Recall that

$$H^0_{\mathcal{M}}(B) := \bigcup_{k \in \mathbb{N}} \left(0 :_B \mathcal{M}^k\right) = \{p \in B : \exists k \in \mathbb{N} \,\text{such that}\, \mathcal{M}^k p = 0\}.$$

In a more algebraic language, we have the following well-known *Elimination Theorem*

Theorem 4.1. *Let K be any field, and suppose that we have a morphism $\rho : A \to \mathcal{K}$ (a specialization map). Then the following are equivalent:*

1. $\rho(\mathcal{U}) = 0$.
2. *There exists an extension L of $\mathcal{K}$ and a non-trivial zero of I in L^n.*
3. *I has a non-trivial zero in $\overline{\mathcal{K}}^n$.*

This is a very classical result. For a modern proof of it, see for instance [14, 15].

One can regard resultants and subresultants as elements of this elimination ideal $\mathcal{U}$. There are standard techniques for computing these elements that generalize the determinant $\operatorname{Res}(f, g)$ (see [1] for a detailed exposition of this topic).

5 Some Recent and ongoing work in the area

This section reports some active areas of research that involve subresultants. Recall that resultants are particular cases of subresultants.

5.1 Complexity aspects Euclid's algorithm

As mentioned before, univariate subresultants were applied for computing the gcd of two univariate polynomials. The formalism of subresultants allows to treat this subject in a somehow "general" framework. As explained in Proposition 1.4, by testing if some determinats are zero one can compute the degree of the gcd of two polynomials. Moreover, one can get the gcd without performing the whole polynomial remainder sequence. This allows to perform a parallelable Euclid's algorithm, and also one bound the size of the output in a nice way. For more details, see [4, 3, 12, 8, 16, 17, 26].

5.2 Formal integration of rational functions

Resultants and subresultants can be used for solving the following problem: how to solve "formally" (i.e. without having to compute roots) the following formal integral $\int \frac{P(t)}{Q(t)}dt$,where $P(t)$ and $Q(t)$ are polynomials in $K[t]$ (K any field). In [24], the following is proven:

Theorem 5.1. *Let $P(t), Q(t)$ as before, with $\gcd(P,Q) = 1$ and $Q(t)$ square-free. Then*

$$\int \frac{P(t)}{Q(t)}dt = \sum_{b:\, S(b)=0} b \log(R_i(t,b))$$

- $S(y) := Res_t(P(t) - yQ'(t), Q(t))$
- $R_i(x,t)$:=*the i-th subresultant polynomial.*

5.3 Resolution of over-determined systems

"In general", n polynomials in $n-1$ variables do not have common zeroes, and when they have a common solution, their resultant vanishes so will not give us any useful information. This is the so called over-determined case.

Even when the resultant vanishes, subresultants can still be used for recovering information about the solutions. By using relations of the form

$$\Delta_{\{\mathbf{X}^\beta\}}\mathbf{X}^\alpha \pm \Delta_{\{\mathbf{X}^\alpha\}}\mathbf{X}^\beta \in \langle f_1, \ldots, f_n\rangle$$

One can deal with this case. This approach has been explored in [10, 11, 29]

5.4 Computation of residues

Let $\mathbf{f} := (f_1, \ldots, f_n)$ be a sequence of polynomials with finite zeroes in $\mathbb{C}^n$. The residue associated to $\mathbf{f}$ of the monomial $\mathbf{X}^\alpha$ is by definition

$$\mathrm{Residue}_{\mathbf{f}}(\mathbf{X}^\alpha) := \left(\frac{1}{2\pi i}\right)^n \int_{|f_1(\mathbf{X})|=\epsilon} \cdots \int_{|f_n(\mathbf{X})|=\epsilon} \frac{\mathbf{X}^\alpha}{f_1(\mathbf{X})\ldots f_n(\mathbf{X})} d\mathbf{x}_1 \wedge \ldots \wedge d\mathbf{x}_n$$

This integral is actually a rational expression on the coefficients of the f_i's. We can explicit the residue by means of resultants and subresultants.

Theorem 5.2. *[19, 6]*

$$\mathit{Residue}_{\mathbf{f}}(\mathbf{X}^\alpha) = \frac{\Delta_{\{\mathbf{X}^\alpha\}}}{\mathrm{Res}(f_1, \ldots, f_n)}.$$

5.5 Singularities of the Resultant

The irreducible hypersurface $\{\mathrm{Res} = 0\}$ has a lot of interesting properties. For instance, we saw before that the points in this surface correspond to overdetermined systems, and by manipulating subresultants (or partial derivatives of the resultant, see [18, 28]) one can get information about them. It is of natural interest then to study the geometry of this hypersurface. In [19], Jouanolou made a precise description of the locus of rational singularities of the resultant hypersurface. This turns out to be the zero locus of all subresultants in *critical degree*:

$$\text{Rational Singularities of}\,\{\mathrm{Res} = 0\} = \{\Delta_{\{\mathbf{X}^\alpha\}} = 0, |\alpha| = d_1 + \ldots + d_n - n\}.$$

5.6 Formulas in roots

In the bivariate case, if we set

$$\begin{cases} f(\mathbf{x}_1, 1) & = & A_0\mathbf{x}_1^n + A_1\mathbf{x}_1^{n-1} + \ldots + A_n & = & A_0 \prod_{i=1}^n (\mathbf{x}_1 - \alpha_i) \\ g(\mathbf{x}_1, 1) & = & B_0\mathbf{x}_1^m + B_1\mathbf{x}_1^{m-1} + \ldots + B_m & = & B_0 \prod_{j=1}^m (\mathbf{x}_1 - \beta_j), \end{cases}$$

then it is well-known that

$$\mathrm{Res}(f, g) = {A_0}^m \prod_{i=1}^n g(\alpha_i, 1) = {A_0}^m {B_0}^n \prod_{i,j} (\alpha_i - \beta_j), \tag{10}$$

and similar results hold for subresultants. In the multivariate case, there is an analogue of the first equality of (10) for resultants (formulas "a la Poison", see [20]), and we recently extended this kind of formulas for subresultants (see [7]). Currently, we are working in a generalization of the symmetric formula given in the second equality of (10) for the multivariate case. This is an ongoing work with Teresa Krick, Hoon Hong and Agnes Szanto.

6 Some open questions

So far we have introduced multivariate resultants and subresultants, and show some of their properties and applications. The theory is an active and interesting area of research. There are lots of things that are still to be found about subresultants. For instance, it would be interesting to have a more geometrical explanation of them: in contrast with resultants which are the equation of an irreducible hypersurface (hence they are irreducible), subresultants do factorize, and sometimes they are identically zero.

We present here a list of problems related to that. All of them combine Algebra with Geometry and Combinatorics.

- Characterize all $\mathcal{S}$ such that $\Delta_{\mathcal{S}}$ is identically zero.

For instance, if $n = 4$ and f_1, f_2, f_3 are generic homogenous polynomials of degree two. Then it is easy to check that the set

$$\mathcal{S} := \{\mathbf{x}_4^3, \mathbf{x}_1\mathbf{x}_4^2, \mathbf{x}_2\mathbf{x}_4^2, \mathbf{x}_3\mathbf{x}_4^2, \mathbf{x}_1^2\mathbf{x}_4, \mathbf{x}_2^2\mathbf{x}_4, \mathbf{x}_3^2\mathbf{x}_4, \mathbf{x}_1\mathbf{x}_2\mathbf{x}_4\}$$

satisfies $\Delta_{\mathcal{S}} = 0$. An explanation for this particular case can be found in [5]. It would be interesting to have a characterization of all the sets that have this condition.

- Which $\Delta_{\mathcal{S}}$'s are irreducible in $\mathbb{Q}[A_{ij}]$? Which in $\mathbb{Z}[A_{ij}]$?

  Some partial answers were given [2], but a whole characterization is still open. For instance, if $n = 2$ and $f_1 = a\mathbf{x}_1 + b\mathbf{x}_2 + c\mathbf{x}_2$, then for $\mathcal{S} := \{\mathbf{x}_1^2, \mathbf{x}_2^2, \mathbf{x}_3^2\}$ we have that $\Delta_{\mathcal{S}} = \pm 2abc$. The explanation is given by the fact that f_1^2 equals a linear combination of elements of $\mathcal{S}$ times 2 times a combination of $\mathbf{x}_1\mathbf{x}_2$, $\mathbf{x}_1\mathbf{x}_3$, $\mathbf{x}_2\mathbf{x}_3$.

- If $\Delta_{\mathcal{S}}$ factorizes, is it true that it factors as a product of subresultants? How does the factorization work and how are these factors related with $\mathcal{S}$?

References

[1] Busé Laurent. *Elimination theory in codimension one and applications.* Lecture Notes for the CIMPA-UNESCO-IRAN school in Zanjan, Iran, July 9–22 2005.

[2] Busé, Laurent; D'Andrea, Carlos. *On the irreducibility of multivariate subresultants.* C. R. Math. Acad. Sci. Paris 338 (2004), no. 4, 287–290.

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

[4] Collins, George E. *Subresultants and reduced polynomial remainder sequences.* J. Assoc. Comput. Mach. 14 1967 128–142.

[5] D'Andrea, Carlos; Jeronimo, Gabriela. *Subresultants and generic monomial bases*. J. Symbolic Comput. 39 (2005), no. 3–4, 259–277.

[6] D'Andrea, Carlos; Khetan, Amit. *Macaulay style formulas for the toric residue.* Compositio Math. 141 (2005) 713-728.

[7] D'Andrea, Carlos; Krick, Teresa; Szanto, Agnes. *Multivariate subresultants in roots.* Journal of Algebra, to appear.

[8] Ducos, Lionel. *Algorithme de Bareiss, algorithme des sous-résultants.* RAIRO Inform. Théor. Appl. 30 (1996), no. 4, 319–347.

[9] Emiris, Ioannis Z.; Galligo, André; Lombardi, Henri. *Certified approximate univariate GCDs.* Algorithms for algebra (Eindhoven, 1996). J. Pure Appl. Algebra 117/118 (1997), 229–251.

[10] González-Vega, Laureano. *A subresultant theory for multivariate polynomials.* Extracta Math. 5 (1990), no. 3, 150–152.

[11] González-Vega, Laureano. *Determinantal formulae for the solution set of zero-dimensional ideals.* J. Pure Appl. Algebra 76 (1991), no. 1, 57–80.

[12] González-Vega, L.; Lombardi, H.; Recio, T.; Roy, M.-F. *Spécialisation de la suite de Sturm et sous-résultants.* RAIRO Inform. Thor. Appl. 24 (1990), no. 6, 561–588.

[13] Habicht, Walter. *Zur inhomogenen Eliminationstheorie.* Comment. Math. Helv. 21 (1948). 79–98.

[14] Harris, Joe. *Algebraic geometry. A first course.* Graduate Texts in Mathematics, vol. 133, Springer-Verlag, New York, 1992.

[15] Hartshorne, Robin. *Algebraic Geometry.* Graduate Texts in Mathematics, vol. 52, Springer-Verlag, New York, 1977.

[16] Hou, Xiaorong; Wang, Dongming. *Subresultants with the Bézout matrix.* Computer mathematics (Chiang Mai, 2000), 19–28, Lecture Notes Ser. Comput., 8, World Sci. Publishing, River Edge, NJ, 2000.

[17] Ho, Chung-Jen; Yap, Chee Keng. *The Habicht approach to subresultants.* J. Symbolic Comput. 21 (1996), no. 1, 1–14.

[18] Jeronimo, G.; Krick, T.; Sabia, J.; Sombra, M. *The computational complexity of the Chow form.* Foundations of Computational Mathematics, Vol. 4 (2004), No. 1, pp. 41-117.

[19] Jouanolou, J. P. *Singularités rationelles du résultant.* in *Algebraic geometry (Proc. Summer Meeting, Univ. Copenhagen, Copenhagen, 1978)*, volume 732 of *Lecture Notes in Math.*, 183–213. Springer, Berlin, 1979.

[20] Jouanolou, J. P. *Le formalisme du résultant.* Adv. Math. 90 (1991), no. 2, 117–263.

[21] Jouanolou, J. P. *Aspects invariants de l'élimination.* Adv. Math. 114 (1995), no. 1, 1–174.

[22] Jouanolou, J. P. *Formes d'inertie et résultant: un formulaire.* Adv. Math. 126 (1997), no. 2, 119–250.

[23] Kaltofen, Erich; May, John. *On approximate irreducibility of polynomials in several variables.* Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, 161–168, ACM, New York, 2003.

[24] Lazard, D.; Rioboo, R. *Integration of rational functions: rational computation of the logarithmic part.* J. Symbolic Comput. 9 (1990), no. 2, 113–115.

[25] Macaulay, F. *Some formulae in elimination.* Proc. London. Math. Soc., 33(1):3–27, 1902.

[26] Reischert, Daniel. *Asymptotically fast computation of subresultants.* Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation (Kihei, HI), 233–240, ACM, New York, 1997.

[27] Sylvester, J. *A theory of syzygetic relations of two rational integral functions, comprising an application to the theory of sturm's functions, and that of the greatest algebraic common measure.* Philosophical Trans., 1853.

[28] Szanto, Agnes. *Multivariate subresultants using Jouanolou's resultant matrices.* To appear in the Journal of Pure and Applied Algebra.

[29] Szanto, Agnes. *Solving over-determined systems by subresultant methods.* Submitted for publication, 2001.

[30] Zeng, Zhonggang; Dayton, Barry. *The approximate gcd of inexact polynomials.* Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation, 320–327, ACM Press, 2004.

[31] Zeng, Zhonggang. *A method computing multiple roots of inexact polynomials.* Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, 266–272, ACM, New York, 2003.