

## ***D*-RESULTANT AND SUBRESULTANTS**

M'HAMMED EL KAHOUI

(Communicated by Bernd Ulrich)

ABSTRACT. We establish a connection between the  $D$ -resultant of two polynomials  $f(t)$  and  $g(t)$  and the subresultant sequence of  $f(t) - x$  and  $g(t) - y$ . This connection is used to decide in a more explicit way whether  $\mathcal{K}(f(t), g(t)) = \mathcal{K}(t)$  or  $\mathcal{K}[f(t), g(t)] = \mathcal{K}[t]$ . We also show how to extract a faithful parametrization from a given one.

### 1. INTRODUCTION

Let  $\mathcal{A}$  be a commutative domain with fractions field  $\mathcal{K}$ . The  $D$ -resultant of two nonlinear polynomials  $f(t), g(t) \in \mathcal{A}[t]$  is defined as the resultant with respect to  $t$  of the two polynomials

$$f_1(s, t) = \frac{f(t) - f(s)}{t - s}, \quad g_1(s, t) = \frac{g(t) - g(s)}{t - s}$$

where  $s$  is an indeterminate over  $\mathcal{A}[t]$ . Such a concept is introduced in [7] as an extension, to the nonzero characteristic case, of the so-called Taylor resultant defined in lecture 19 of [1]. The main motivation which led the authors to introduce such concepts was to find out algorithmic solutions to the following questions: How can one decide whether  $\mathcal{K}(t) = \mathcal{K}(f, g)$  or whether  $\mathcal{K}[t] = \mathcal{K}[f, g]$ , and how can one find the singularities, in the affine plane, of the curve defined by the parametrization  $x = f(t), y = g(t)$ ?

By extending the notion of  $D$ -resultant to the case of rational functions these same questions, among others, are solved in [9].

In this paper we address the same questions, but we seek more explicit information. For instance, to the question of deciding whether  $\mathcal{K}(t) = \mathcal{K}(f, g)$ , we substitute the more explicit question of finding a rational function  $r(x, y) \in \mathcal{K}(x, y)$  such that  $r(f, g) = t$ . In the case  $\mathcal{K}[t] = \mathcal{K}[f(t), g(t)]$ , the computation of a polynomial  $p(x, y)$  such that  $p(f(t), g(t)) = t$  is required. Let us point out here that in [1, 7, 9] the additional information, namely finding  $r(x, y)$  or  $p(x, y)$ , cannot obviously be extracted from the  $D$ -resultant.

The price we pay to get this more precise information is the computation of the subresultant sequence of  $f(t) - x$  and  $g(t) - y$  in  $\mathcal{A}[x, y][t]$  instead of the  $D$ -resultant. But in fact, the computation of the  $D$ -resultant has the same cost as the computation of the subresultant sequence. Indeed, the best actual algorithms for computing the resultant of two polynomials  $f(t)$  and  $g(t)$ , of maximal degree

---

Received by the editors June 24, 2003.

2000 *Mathematics Subject Classification*. Primary 13P05.

*Key words and phrases*.  $D$ -resultant, subresultant sequence.

$d$ , are those which compute the whole subresultant sequence of  $f(t)$  and  $g(t)$  (see [5, 11, 12]), and their cost is  $O(d^2)$  arithmetic operations in the ground ring. In the case of the  $D$ -resultant, one needs to perform  $O(d^2)$  arithmetic operations in the ring  $\mathcal{A}[s]$ , and the involved polynomials are of degree  $O(d^2)$  with respect to  $s$ . Since the multiplication of two univariate polynomials of degree  $O(n)$  requires  $O(n^2)$  arithmetic operations in  $\mathcal{A}$ , the total cost for the computation of the  $D$ -resultant is  $O(d^6)$  arithmetic operations. On the other hand, the computation of the subresultant sequence of  $f(t) - x$  and  $g(t) - y$  requires  $O(d^2)$  arithmetic operations involving polynomials in  $\mathcal{A}[x, y]$  of degree  $O(d)$ . Since the number of coefficients of a degree  $n$  polynomial in  $\mathcal{A}[x, y]$  is  $O(n^2)$ , the total cost of the subresultant sequence computation is  $O(d^6)$  arithmetic operations as well.

## 2. REVIEW OF SUBRESULTANTS

In this section we recall how subresultants are defined and give some of their main properties. For more details on subresultants theory we refer to [8, 4, 12, 13, 3, 11, 6], but the list is nowhere near exhaustive.

Throughout this paper all considered rings are commutative with unit. Given two positive integers  $m$  and  $n$  we denote by  $\mathcal{M}_{m,n}(\mathcal{A})$  the  $\mathcal{A}$ -module of  $m \times n$  matrices with coefficients in  $\mathcal{A}$ . Consider the free  $\mathcal{A}$ -module  $\mathcal{P}_n$  of univariate polynomials with coefficients in  $\mathcal{A}$  of degree at most  $n-1$  equipped with the basis  $\mathcal{B}_n = [t^{n-1}, \dots, t, 1]$ .

A sequence of polynomials  $[f_1, \dots, f_m]$  in  $\mathcal{P}_n$  will be identified with the  $m \times n$  matrix whose row's coefficients are the coordinates of the  $f_i$ 's in  $\mathcal{B}_n$ . Given positive integers  $p, q$  we let  $\delta(p, q) = q - 1$  if  $p = q$ , and  $\delta(p, q) = \min(p, q)$  if  $p \neq q$ .

**Definition 2.1.** Let  $\mathcal{A}$  be a ring and let  $p, q$  be positive integers. Let  $f, g \in \mathcal{A}[t]$  be two polynomials with  $\deg(f) = p$  and  $\deg(g) = q$ . For any  $i \leq \delta(p, q)$  we define the  $i$ -th subresultant polynomial associated to  $f$  and  $g$  as follows:

$$\text{Sr}_i(f, g) = \sum_{j=0}^i \text{sr}_{i,j}(f, g)t^j$$

where  $\text{sr}_{i,j}(f, g)$  is the determinant of the matrix built with the columns  $1, 2, \dots, p+q-2i-1$  and  $p+q-i-j$  in the matrix

$$\text{Sylv}_i(f, g) = [t^{q-i-1}f, \dots, f, t^{p-i-1}g, \dots, g].$$

The determinant  $\text{sr}_{i,i}(f, g)$  is called the  $i$ -th principal subresultant coefficient of  $f$  and  $g$  and is denoted by  $\text{sr}_i(f, g)$ .

Recall that the polynomials  $\text{Sr}_i(f(t), g(t))$  belong to the ideal  $\mathcal{I}(f, g)$  generated by  $f$  and  $g$  in  $\mathcal{A}[t]$ , and that  $\deg(\text{Sr}_i(f, g)) \leq i$ . Moreover,  $\text{Sr}_0(f(t), g(t))$  is nothing but the resultant  $\text{Res}(f, g)$  of  $f$  and  $g$  with respect to  $t$ .

If no risk of confusion arises, we write  $\text{Sr}_i$  and  $\text{sr}_{i,j}$  instead of  $\text{Sr}_i(f, g)$  and  $\text{sr}_{i,j}(f, g)$ . In the sequel we give some fundamental properties of subresultants. The first one is the most fundamental, and it answers the well-known problem of finding algebraic conditions on the coefficients of  $f$  and  $g$  in order that they have a gcd of given degree.

**Theorem 2.2.** *Let  $\mathcal{A}$  be a ring and let  $f, g, h \in \mathcal{A}[t]$  be polynomials with  $\deg(f) = p$ ,  $\deg(g) = q$  and  $\deg(h) = r$ , and assume that  $h$  has 1 as the leading coefficient.*

Then:

$$\text{Sr}_i(hf, hg) = \begin{cases} h\text{Sr}_{i-r} & \text{if } i \geq r, \\ 0 & \text{otherwise.} \end{cases}$$

In particular, if  $\mathcal{A}$  is a domain with fractions field  $\mathcal{K}$ , then the gcd of  $f$  and  $g$  over  $\mathcal{K}$  is of degree  $k$  if and only if

$$\begin{aligned} \text{sr}_i &= 0, \quad i = 0, 1, \dots, k - 1, \\ \text{sr}_k &\neq 0. \end{aligned}$$

Another fundamental property subresultants satisfy is the so-called specialization property. A systematic study of this property can be found in [8].

**Theorem 2.3.** *Let  $\mathcal{A}$  and  $\mathcal{B}$  be two rings, let  $\phi : \mathcal{A} \rightarrow \mathcal{B}$  be a ring homomorphism and let  $f, g \in \mathcal{A}[t]$  be two polynomials with  $\deg(f) = p$  and  $\deg(g) = q$ . If  $\deg(\phi(f)) = p$  and  $\deg(\phi(g)) = q$ , then for any  $i = 0, \dots, \delta(p, q)$  we have:*

$$\text{Sr}_i(\phi(f), \phi(g)) = \phi(\text{Sr}_i).$$

The next result we give concerns the behavior of subresultants under composition. This is an important result for our purpose insofar as it allows us to deal in an explicit and efficient way with the question of computing a faithful parametrization from a nonnecessarily faithful one. The version we give here addresses the case of composition by a polynomial  $\tau(t)$  with 1 as leading coefficient, which is enough for our need. For the general version and its proof we refer to [10].

**Theorem 2.4.** *Let  $\mathcal{A}$  be a ring and let  $f, g, h \in \mathcal{A}[t]$  be polynomials with  $\deg(f) = p$ ,  $\deg(g) = q$  and  $\deg(h) = r$ , and assume that  $h$  has 1 as the leading coefficient. Then:*

$$\text{Sr}_i(f \circ h, g \circ h) = \begin{cases} c_k^{r-1} \text{Sr}_k \circ h & \text{if } i = kr, \\ \sigma_k d_k^{r-1} \text{Sr}_{k-1} \circ h & \text{if } i = kr - 1, \\ 0 & \text{otherwise,} \end{cases}$$

where  $\sigma_k = (-1)^{(p-k)(r-1)}$ ,  $c_k = \text{sr}_k$ , and  $d_k = \text{sr}_{k-1}$ .

Let us point out that the results given in this section are elementary insofar as they are mainly due to the basic properties of polynomials and nice behavior of determinants under row and column operations (see e.g [6] for more details).

### 3. SUBRESULTANTS AND D-RESULTANT

In this section we show that the  $D$ -resultant of two nonlinear polynomials  $f$  and  $g$  in  $\mathcal{A}[t]$  is closely related to the first subresultant coefficient of  $f(t) - x$  and  $g(t) - y$  in  $\mathcal{A}[x, y][t]$ . In the rest of this paper we will write  $\text{Sr}_i(x, y)$  and  $\text{sr}_{i,j}(x, y)$  instead of  $\text{Sr}_i(f(t) - x, g(t) - y)$  and  $\text{sr}_{i,j}(f(t) - x, g(t) - y)$ .

We start with the following lemma which gives bounds on the degrees of the polynomials  $\text{sr}_{i,j}(x, y)$ .

**Lemma 3.1.** *Let  $\mathcal{A}$  be a domain and let  $f, g \in \mathcal{A}[t]$  be two nonlinear polynomials with  $\deg(f) = p$ ,  $\deg(g) = q$ . Then the following hold:*

- i)  $\text{sr}_0(x, y) = ay^p + bx^q + r(x, y)$ , where  $a$  and  $b$  are nonzero elements of  $\mathcal{A}$ ,  $\deg_y(r) < p$  and  $\deg_x(r) < q$ .
- ii) For any  $i \leq \delta(p, q)$  and any  $j \leq i$  we have  $\deg_x(\text{sr}_{i,j}(x, y)) \leq q - i$  and  $\deg_y(\text{sr}_{i,j}(x, y)) \leq p - i$ .

*Proof.* Let us write  $f = c_p t^p + \dots + c_0$  and  $g = d_q t^q + \dots + d_0$ , with  $c_p \neq 0$  and  $d_q \neq 0$ . The coefficients of the Sylvester matrix  $\text{Sylv}_i(f(t) - x, g(t) - y) = (a_{j,k}^{(i)})$  are either constants in  $\mathcal{A}$  or  $c_0 - x$  or  $d_0 - y$ . Moreover, the number of times  $c_0 - x$  (resp.  $d_0 - y$ ) appears in  $\text{Sylv}_i(f(t) - x, g(t) - y)$  is  $q - i$  (resp.  $p - i$ ). Since on the other hand  $\text{sr}_{i,j}(x, y)$  is a minor of this matrix, we have the bounds claimed in ii).

To prove the sharpness of these bounds in the case  $i = 0$  we need to be a little bit more precise, and give the exact subscripts  $j, k$  whose corresponding coefficient is  $c_0 - x$  (resp.  $d_0 - y$ ). In fact we have  $a_{j,k}^{(0)} = d_0 - y$  if and only if  $j \geq q + 1$  and  $k = j$ . Let us write

$$\text{sr}_0(x, y) = \sum_{\sigma \in \mathcal{S}_{p+q}} \varepsilon(\sigma) a_{1, \sigma(1)}^{(0)} \cdots a_{p+q, \sigma(p+q)}^{(0)}.$$

In order that a given  $\sigma$  generates a term of the type  $c(d_0 - y)^p$  it should satisfy  $\sigma(j) = j$  for any  $j \geq q + 1$ . This means in particular that  $\sigma(j) \leq q$  for any  $j \leq q$ . Therefore, the coefficient of the monomial  $(d_0 - y)^p$  in  $\text{sr}_0(x, y)$  is  $\det(A_{q,q})$ , where  $A_{q,q}$  is the  $q \times q$  principal submatrix of  $\text{Sylv}_0(f(t) - x, g(t) - y)$ . Clearly,  $A_{q,q}$  is upper triangular and its diagonal entries are equal to  $c_p$ . Thus, we have  $\text{sr}_0(x, y) = c_p^q (d_0 - y)^p + r_1(x, y)$  with  $\deg_y(r_1) < p$ . Similar arguments show that  $\text{sr}_0(x, y)$  can also be written as  $\text{sr}_0(x, y) = b(c_0 - x)^q + r_2(x, y)$ , where  $b$  is a nonzero element of  $\mathcal{A}$  and  $\deg_x(r_2) < q$ . Combining these two decompositions we get the one claimed in i).  $\square$

**Theorem 3.2.** *Let  $\mathcal{K}$  be a commutative field and let  $\overline{\mathcal{K}}$  be its algebraic closure. Let  $f$  and  $g$  be two nonlinear polynomials in  $\mathcal{K}[t]$  and let  $D(s)$  be their  $D$ -resultant. Then the following properties hold:*

- i)  $D(s) = \text{sr}_1(f(s), g(s))$ .
- ii)  $\mathcal{K}(f, g) = \mathcal{K}(t)$  if and only if  $D(s) \neq 0$ . In this case the rational function  $r(x, y) = -\text{sr}_1^{-1} \text{sr}_{1,0}(x, y)$  satisfies  $r(f(t), g(t)) = t$ .
- iii)  $\mathcal{K}[f, g] = \mathcal{K}[t]$  if and only if  $D(s)$  is a nonzero constant. In this case  $\text{sr}_1(x, y) = D(s)$ ,  $r(x, y)$  is a polynomial and  $r(f(t), g(t)) = t$ .

*Proof.* i) To simplify we let  $f_1(s, t) = \frac{f(t) - f(s)}{t - s}$  and  $g_1(s, t) = \frac{g(t) - g(s)}{t - s}$ . We also let  $\phi : \mathcal{A}[x, y] \rightarrow \mathcal{A}[s]$  be the  $\mathcal{A}$ -homomorphism defined by  $\phi(x) = f(s)$  and  $\phi(y) = g(s)$ . Since  $\phi(f(t) - x) = f(t) - f(s)$  and  $\phi(g(t) - y) = g(t) - g(s)$  we have by Theorem 2.3 the relation  $\text{Sr}_i(f(t) - f(s), g(t) - g(s)) = \text{Sr}_i(f(s), g(s))$ . On the other hand, we have  $f(t) - f(s) = f_1(s, t)(t - s)$  and  $g(t) - g(s) = g_1(s, t)(t - s)$ , which gives according to Theorem 2.2 the relation

$$\text{Sr}_1(f(t) - f(s), g(t) - g(s)) = (t - s) \text{Sr}_0(f_1(s, t), g_1(s, t)) = (t - s) D(s).$$

By comparing the leading coefficients with respect to  $t$  we get the claimed relation.

ii) Assume that  $D(s) \neq 0$ . Then by property i) we have  $\text{sr}_1(x, y) \neq 0$  and so the rational function  $r(x, y)$  is well defined. On the other hand, since  $\text{Sr}_1(x, y) \in \mathcal{I}(f(t) - x, g(t) - y)$  we have  $\text{Sr}_1(f(t), g(t)) = \text{sr}_1(f(t), g(t))t + \text{sr}_{1,0}(f(t), g(t)) = 0$ , and this proves that  $r(f(t), g(t)) = t$ . Conversely, assume that  $\mathcal{K}(f, g) = \mathcal{K}(t)$  and let  $u(x, y) = \frac{a(x, y)}{b(x, y)}$  be a rational function such that  $u(f(t), g(t)) = t$ . Let  $\mathcal{V}$  be the finite subset of  $\overline{\mathcal{K}}$  consisting of the roots of  $b(f(t), g(t))$ . Then the map  $\gamma : t \in \overline{\mathcal{K}} \setminus \mathcal{V} \rightarrow (f(t), g(t)) \in \overline{\mathcal{K}}^2$  is injective according to the fact that  $u(\gamma(t)) = t$ .

Moreover, by applying  $\partial_t$  to the relation  $u(f(t), g(t)) = t$  we get a relation of the type

$$v(t)f'(t) + w(t)g'(t) = b(f(t), g(t))^2,$$

where  $v(t)$  and  $w(t)$  are polynomials in  $\mathcal{K}[t]$ . This last relation proves in particular that the elements of  $\overline{\mathcal{K}} \setminus \mathcal{V}$  cannot be common roots of  $f'(t)$  and  $g'(t)$ .

Now let  $\alpha$  be an element of  $\overline{\mathcal{K}} \setminus \mathcal{V}$ . Since  $\gamma$  is injective, the system  $f(t) - f(\alpha) = g(t) - g(\alpha) = 0$  has only one solution, namely  $\alpha$ . Moreover, this solution is of multiplicity 1 according to the fact that it is not a common root of  $f'$  and  $g'$ . Thus, the gcd of  $f(t) - f(\alpha)$  and  $g(t) - g(\alpha)$  is  $t - \alpha$ , and by Theorem 2.2 we have  $D(\alpha) \neq 0$ .

iii) Assume that  $D(s)$  is a nonzero constant, say 1 to simplify. From the relation  $\text{Sr}_1(f(t), g(t)) = D(t)t + \text{sr}_{1,0}(f(t), g(t)) = 0$  we get  $-\text{sr}_{1,0}(f(t), g(t)) = t$  and hence  $\mathcal{K}[f, g] = \mathcal{K}[t]$ . Conversely, assume that  $\mathcal{K}[f, g] = \mathcal{K}[t]$  and let  $u(x, y) \in \mathcal{K}[x, y]$  be such that  $u(f(t), g(t)) = t$ . In this case, the subset  $\mathcal{V}$  defined above is empty and so  $D(\alpha) \neq 0$  for any  $\alpha \in \overline{\mathcal{K}}$ . This proves that  $D(s)$  is a nonzero constant.

Let us now prove that  $\text{sr}_1$  is constant. Since  $\mathcal{K}[f, g] = \mathcal{K}[t]$ , the parametrization  $(f(t), g(t))$  is faithful and so  $\text{sr}_0(x, y)$  is irreducible. Now if we let  $s_0 = D(s)$ , then  $\text{sr}_1(f(t), g(t)) - s_0 = 0$  and hence  $\text{sr}_1(x, y) - s_0$  is a multiple of  $\text{sr}_0(x, y)$ . By Lemma 3.1 we have

$$\deg_y(\text{sr}_1(x, y) - s_0) < \deg_y(\text{sr}_0(x, y)),$$

and so  $\text{sr}_1(x, y) - s_0 = 0$ . □

The previous theorem does not explain the case where  $D(s) = 0$ , i.e. the parametrization  $x = f(t)$ ,  $y = g(t)$  is unfaithful. In such a case it is natural to ask how one can extract a faithful parametrization from the given one by looking at the already computed subresultant sequence. The following result explains how one can read up on such information.

**Theorem 3.3.** *Let  $f$  and  $g$  be two nonlinear polynomials in  $\mathcal{A}[t]$  and let  $D(s)$  be their  $D$ -resultant. Assume that  $D(s) = 0$  and let  $r \geq 2$  be the smallest integer such that  $\text{Sr}_{r-1}(x, y) \neq 0$ . Then the following properties hold:*

i)  $\text{Sr}_r(x, y) = a(x, y)^{r-1}(a(x, y)\tau(t) + b(x, y))$ , where  $\tau(t)$  is of degree  $r$  and leading coefficient 1, and  $a(x, y), b(x, y) \in \mathcal{K}[x, y]$  with  $a(x, y) \neq 0$ .

ii) *There exist polynomials  $\tilde{f}, \tilde{g}$  in  $\mathcal{K}[t]$  such that  $f(t) = \tilde{f}(\tau(t))$ ,  $g(t) = \tilde{g}(\tau(t))$  and  $\mathcal{K}(\tilde{f}(t), \tilde{g}(t)) = \mathcal{K}(t)$ .*

*Proof.* The field  $\mathcal{K}(f, g)$  contains at least a nonconstant polynomial. Therefore, by the Noether-Schinzel theorem (see e.g. [14]) we have  $\mathcal{K}(f, g) = \mathcal{K}(\tau(t))$  for a polynomial  $\tau(t) \in \mathcal{K}[t]$  with 1 as the leading coefficient. The fact that  $\mathcal{K}[\tau(t)]$  is a principal ideal domain implies that  $\mathcal{K}(\tau(t)) \cap \mathcal{K}[t] = \mathcal{K}[\tau(t)]$ .

Let us write  $f(t) = \tilde{f}(\tau(t))$  and  $g(t) = \tilde{g}(\tau(t))$ , where  $\tilde{f}, \tilde{g} \in \mathcal{K}[t]$ , and let  $\ell = \deg(\tau(t))$ . Notice that  $\mathcal{K}(\tilde{f}(t), \tilde{g}(t)) = \mathcal{K}(t)$  and hence

$$\text{sr}_1(\tilde{f}(t) - x, \tilde{g}(t) - y) \neq 0.$$

On the other hand, by using Theorem 2.4 we deduce that

$$\begin{aligned} \text{Sr}_{\ell-1}(x, y) &= \varepsilon\sigma^\ell, \\ \text{Sr}_i(x, y) &= 0, \quad 1 \leq i \leq \ell - 2, \end{aligned}$$

where  $\varepsilon = \pm 1$  and  $\sigma = \text{sr}_0(\tilde{f}(t) - x, \tilde{g}(t) - y)$ . Since  $\sigma \neq 0$  we have  $r = \ell$ . Using Theorem 2.4 once again we get

$$\text{Sr}_r(x, y) = a(x, y)^{r-1}(a(x, y)\tau(t) + b(x, y)),$$

where  $a(x, y)t + b(x, y) = \text{Sr}_1(\tilde{f}(t) - x, \tilde{g}(t) - y)$ . □

**3.1. The Abhyankar-Moh theorem.** Let  $\mathcal{K}$  be a commutative field of characteristic zero and let  $\overline{\mathcal{K}}$  be its algebraic closure. The famous Abhyankar-Moh theorem [2] states that any algebraic embedding  $(f(t), g(t))$  of  $\overline{\mathcal{K}}$  in  $\overline{\mathcal{K}}^2$  is rectifiable. We show in the following theorem that an automorphism which rectifies  $(f, g)$  can be computed by using subresultants.

**Theorem 3.4.** *Let  $\mathcal{K}$  be a field of characteristic zero and let  $(f(t), g(t))$  be such that  $\mathcal{K}[f, g] = \mathcal{K}[t]$ . Then  $F = (\text{sr}_0(x, y), -\text{sr}_1^{-1}\text{sr}_{1,0}(x, y))$  is an automorphism of  $\mathcal{K}[x, y]$  which satisfies  $F(f(t), g(t)) = (0, t)$ .*

*Proof.* By the Abhyankar-Moh theorem there exists a  $\mathcal{K}$ -automorphism  $G = (p, q)$  of  $\mathcal{K}[x, y]$  such that  $G(f(t), g(t)) = (0, t)$ . Since  $\mathcal{K}$ -automorphisms of  $\mathcal{K}[x, y]$  are tame, we may assume, without loss of generality, that  $\deg(q) < \deg(p)$ .

The fact that  $p$  and  $\text{sr}_0$  are irreducible and satisfy  $p(f, g) = \text{sr}_0(f, g) = 0$  implies that  $p = \alpha \text{sr}_0$ , with  $\alpha \in \mathcal{K}^*$ . On the other hand, we have  $q(f, g) - \text{sr}_1^{-1}\text{sr}_{1,0}(f, g) = 0$  and so  $q(x, y) - \text{sr}_1^{-1}\text{sr}_{1,0}(x, y)$  is a multiple of  $\text{sr}_0(x, y)$ . Since  $\deg(q) < \deg(p)$  and by Lemma 3.1 we have  $\deg_y(\text{sr}_{1,0}) < \deg_y(\text{sr}_0)$ , we deduce that

$$\deg_y(q(x, y) - \text{sr}_1^{-1}\text{sr}_{1,0}(x, y)) < \deg_y(\text{sr}_0)$$

and so  $q(x, y) - \text{sr}_1^{-1}\text{sr}_{1,0}(x, y) = 0$ . □

#### REFERENCES

- [1] S. S. Abhyankar. *Algebraic geometry for scientists and engineers*, volume 35. Mathematical Surveys and Monographs, AMS, 1990. MR1075991 (92a:14001)
- [2] S. S. Abhyankar and T. T. Moh. Embeddings of the line in the plane. *J. Reine Angew. Math.*, 276:148–166, 1975. MR0379502 (52:407)
- [3] W. S. Brown and J. F. Traub. On Euclid’s algorithm and the theory of subresultants. *J. ACM*, 18(4):505–514, 1971. MR0303684 (46:2820)
- [4] G. E. Collins. Subresultants and reduced polynomial remainder sequences. *J. ACM*, 14:128–142, 1967. MR0215512 (35:6352)
- [5] L. Ducos. Optimization of the subresultant algorithm. *J. Pure and Applied Algebra*, 145:149–163, 2000. MR1733249 (2000m:68187)
- [6] M. El Kahoui. An elementary approach to subresultants theory. *J. Symbolic Computation*, 35(3):281–292, 2003. MR1962796 (2004b:68195)
- [7] A. van den Essen and J-T. Yu. The  $D$ -resultant, singularities and the degree of unfaithfulness. *Proc. Amer. Math. Soc.*, 125(3):689–695, 1997. MR1353403 (97e:13032)
- [8] L. González-Vega, H. Lombardi, T. Recio, and M-F. Roy. Spécialisation de la suite de Sturm et sous-résultants. *RAIRO Inform. Théor. Appl.*, 24(6):561–588, 1990. MR1082916 (92a:12016)
- [9] J Gutierrez, R. Rubio, and J-T. Yu.  $D$ -resultant for rational functions. *Proc. Amer. Math. Soc.*, 130(8):2237–2246, 2002. MR1896403 (2003c:13024)
- [10] H. Hong. Subresultants under composition. *J. Symbolic Computation*, 23(4):355–365, 1997. MR1445431 (98d:68112)
- [11] T. Lickteig and M-F. Roy. Sylvester-Habicht sequences and fast Cauchy index computation. *J. Symbolic Computation*, 31(3):315–341, 2001. MR1814336 (2002d:68120)
- [12] H. Lombardi, M-F. Roy, and M. Safey El Din. New structure theorem for subresultants. *J. Symbolic Computation*, 29:663–690, 2000. MR1769660 (2001m:13048)

- [13] R. Loos. Generalized polynomial remainder sequences. *Computer Algebra Symbolic and Algebraic Computation*, pages 115–138, 1982. Springer-Verlag. MR0728969
- [14] A. Schinzel. *Selected Topics on Polynomials*. Ann Arbor, MI: University of Michigan Press, 1982. MR0649775 (84k:12010)

DEPARTMENT OF MATHEMATICS, FACULTY OF SCIENCES SEMLALIA, CADI AYYAD UNIVERSITY,  
P.O BOX 2390, MARRAKECH, MOROCCO

*E-mail address:* `elkahoui@ucam.ac.ma`

*Current address:* Max-Planck Institute für Informatik, Stuhlsatzenhausweg 85, 66123 Saarbrücken, Germany

*E-mail address:* `elkahoui@mpi_sb.mpg.de`