PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 130, Number 8, Pages 2237–2246
S 0002-9939(02)06331-1
Article electronically published on January 23, 2002

D-RESULTANT FOR RATIONAL FUNCTIONS

JAIME GUTIERREZ, ROSARIO RUBIO, AND JIE-TAI YU

(Communicated by Wolmer V. Vasconcelos)

ABSTRACT. In this paper we introduce the D-resultant of two rational functions $f(t), g(t) \in \mathbb{K}(t)$ and show how it can be used to decide if $\mathbb{K}(f(t), g(t)) = \mathbb{K}(t)$ or if $\mathbb{K}[t] \subset \mathbb{K}[f(t), g(t)]$ and to find the singularities of the parametric algebraic curve define by $X = f(t), Y = g(t)$. In the course of our work we extend a result about implicitization of polynomial parametric curves to the rational case, which has its own interest.

INTRODUCTION

Let R be an integral domain, $\mathbb{K}$ its quotient field and $R[s,t]$ the polynomial ring in two variables over R. The D-resultant of two non-constant polynomials $f(t)$ and $g(t)$ in $R[t]$ is defined as the resultant, with respect to the variable t, of the polynomials (cf. [EY])

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

This concept coincides with the Taylor resultant of two non-constant polynomials, over a field of characteristic zero, defined in lecture 19 of [Abh]. In [EY], the authors introduce this concept to solve the following questions: how can we decide if $\mathbb{K}(t) = \mathbb{K}(f(t), g(t))$ or if $\mathbb{K}[t] = \mathbb{K}[f(t), g(t)]$ and how can we compute the singularities of the curve defined by $X = f(t)$, $Y = g(t)$?

In this paper we introduce the so-called D-resultant (see Section 2) of rational functions $f(t), g(t) \in \mathbb{K}(t)$ over an arbitrary field $\mathbb{K}$. Furthermore we show that the following three questions can be very easily solved by the D-resultant: a test to decide if $\mathbb{K}(f(t), g(t)) = \mathbb{K}(t)$ or if $\mathbb{K}[t] \subset \mathbb{K}[f(t), g(t)]$ and a method to compute the singularities of the parametric algebraic curve defined by $X = f(t), Y = g(t)$ (Theorem 3.1).

To prove our main result, we need a generalization of a result in [MW], which has its own interest.

Concerning applications, the D-resultant provides a faster algorithm to test whether two rational function fields $\mathbb{K}(f_1(t), \ldots, f_r(t))$ and $\mathbb{K}(t)$ are the same or not; see [Swe]. Corollary 3.2 states a necessary and sufficient condition to decide when a parametric curve has no singularities in the affine plane. Besides, the D-resultant gives an algorithm to compute the singularities of a plane parametric

Received by the editors May 24, 2000 and, in revised form, March 7, 2001.
1991 *Mathematics Subject Classification.* Primary 13P05; Secondary 14E05.
Key words and phrases. Resultant, implicitization, parametric algebraic curve.

curve given by a parametrization (see Corollary 3.2). Finally, we remark that the formulas obtained in Proposition 2.4 also turn out to be useful for applications.

The paper is divided into three sections. In Section 1 we introduce our notations and definitions. We also prove in this section the result on the implicitization of two rational functions and some basic results on parametric curves. These results will be used throughout the subsequent sections. Section 2 is dedicated to introducing the notion of D-resultant for rational functions over arbitrary domains, including useful results for later use. Then (Section 3) we state and prove our main result.

1. Preliminaries

1.1. **Rational functions.** Let $\mathbb{K}$ be an arbitrary field. As usual, we denote by $\mathbb{K}(t)$ the field of rational functions in the variable t. The only $\mathbb{K}$-automorphisms of the field $\mathbb{K}(t)$ are the linear transformations $(at+b)/(ct+d)$, such that $ad-bc \neq 0$.

If f is a non-constant rational function, then there exist polynomials f_n, f_d such that $\gcd(f_n, f_d) = 1$ and $f = f_n/f_d$; we say that f_n/f_d is a *reduced* representation of the rational function f. In this paper f is always given by a reduced representation. So, we can define the *degree* of f as the maximum of the degrees of f_n and f_d, $\deg f = \max(\deg f_n, \deg f_d)$. In this case $\mathbb{K}(f) \subset \mathbb{K}(t)$ is an algebraic extension of degree $\deg f$, i.e., $\deg f = [\mathbb{K}(t) : \mathbb{K}(f)]$.

We say that a non-constant rational function f is *decomposable* if there exist $g, h \in \mathbb{K}(t)$, such that $f = g \circ h = g(h)$ and $\deg g, \deg h > 1$. If $f, h \in \mathbb{K}(t)$ are such that $\mathbb{K}(f) \subset \mathbb{K}(h) \subset \mathbb{K}(t)$, then there exists $g \in \mathbb{K}(t)$ with $f = g(h)$ and $\deg f = \deg g \times \deg h$. By Lüroth's Theorem we have that f is decomposable if and only if $\mathbb{K}(f) \subset \mathbb{K}(t)$ is an algebraic extension with proper subfields. We are interested in the following characterization of decomposable rational functions (cf. [AGR]):

Proposition 1.1. *Let $\mathbb{K}$ be an arbitrary field and let $f = f_n/f_d, h = h_n/h_d$ be two non-constant rational functions in $\mathbb{K}(t)$. Then the bivariate polynomial $h_n(y)h_d(x) - h_n(x)h_d(y)$ divides $f_n(y)f_d(x) - f_n(x)f_d(y)$ if and only if $f = g(h)$, for some rational function $g \in \mathbb{K}(t)$.*

1.2. **Resultants.** We denote by $\overline{\mathbb{K}}$ the algebraic closure of $\mathbb{K}$ and by $\mathbb{K}^\times = \mathbb{K}\backslash\{0\}$. Given two non-zero polynomials $p, q \in R[t]$, the *resultant* of p and q with respect to t is denoted by $Res_t(p, q)$. The next proposition summarises some of its properties:

Proposition 1.2. *Let $p, q, r \in R[t]$ be non-constant polynomials, with $u = \deg p$, $v = \deg q, w = \deg r$. Then:*

1. $Res_t(p, q) = (-1)^{uv} Res_t(q, p)$.
2. $Res_t(pq, r) = Res_t(p, r) \cdot Res_t(q, r)$.
3. *If a is a non-zero element of R, then $Res_t(a, p) = a^u$.*
4. *If $p(t) = a \prod_{i=1}^{u} (t - \alpha_i)$ and $q(t) = b \prod_{i=1}^{v} (t - \beta_i)$ where $\alpha_i, \beta_i \in \overline{\mathbb{K}}$ and $a, b \in \mathbb{K}^\times$, then*

$$\mathrm{Res}_t(p, q) \quad = a^v b^u \prod_{i=1}^{u} \prod_{j=1}^{v} (\alpha_i - \beta_j) = (-1)^{uv} b^u \prod_{i=1}^{v} p(\beta_i) = a^v \prod_{i=1}^{v} q(\alpha_i).$$

5. *There exist $\hat{p}, \hat{q} \in R[t]$ such that $Res_t(p, q) = p\hat{p} + q\hat{q}$. In particular p and q have a common zero in $\overline{\mathbb{K}}$ if and only if $Res_t(p, q) = 0$.*
6. $Res_t(p \circ r, q \circ r) = c Res_t(p, q)^w$, *for some $c \in \mathbb{K}^\times$.*

1.3. **Minimal polynomials and normal parametrizations.** Let $f = f_n/f_d$, $g = g_n/g_d$ be two elements of $\mathbb{K}(t)$, not both constants. Then $f(t)$ and $g(t)$ are algebraically dependent over $\mathbb{K}$, so there exists an irreducible polynomial $m(X,Y) \in \mathbb{K}[X,Y]$, such that $m(f(t),g(t)) = 0$. It is well known that m is unique up to a non-zero constant factor. We call such polynomial m a *minimal polynomial* of f and g.

Let $h(X,Y)$ be a polynomial in $\mathbb{K}[X,Y]$ and $V(h(X,Y))$ the zero set of the polynomial $h(X,Y)$, i.e., $V(h(X,Y)) = \{(x_0,y_0) \in \overline{\mathbb{K}}^2, h(x_0,y_0) = 0\}$. We say that $V(m(X,Y))$ is the parametric curve defined by the parametrization (f,g).

Now, the implicitization problem is: given $f(t), g(t)$ we want to find a minimal polynomial $m(X,Y) \in \mathbb{K}[X,Y]$ of f and g (cf. [CLO]). We will see that it can be computed using resultants.

The polynomial case of the following interesting result is in [MW].

Theorem 1.3. *Let m be a minimal polynomial of the rational functions f, g. Then there exists $c \in \mathbb{K}^\times$ such that*

$$Res_t(f_n(t) - Xf_d(t), g_n(t) - Yg_d(t)) = cm(X,Y)^w,$$

where $w = [\mathbb{K}(t) : \mathbb{K}(f,g)]$.

Proof. The theorem is clearly true if one of the rational functions is constant.

By Gauss' lemma the polynomial $F(X,t) = f_n(t) - Xf_d(t)$ (respectively $G(Y,t) = g_n(t) - Yg_d(t)$) is irreducible in $\mathbb{K}(X)[t]$ (respectively in $\mathbb{K}(Y)[t]$).

We distinguish two possibilities:

(a) $F(X,t)$ or $G(Y,t)$ is a separable polynomial. We can suppose, without loss of generality, that $F(X,t)$ is separable. Then the splitting field $\mathbb{E}$ of $F(X,t)$ over $\mathbb{K}(X)$ is separable and we get the following factorization:

$$F(X,t) = a(t-\theta_1)\cdots(t-\theta_u),$$

where $u = \deg f$, $a \in \mathbb{K}(X)$ and $\theta_i \in \mathbb{E}$ for $1 \le i \le u$. We note that $g(\theta_i)$ is a non-zero element of $\mathbb{E}$. Moreover, from Galois Theory, we know that $\mathbb{E}$ is a Galois extension of $\mathbb{K}(X)$, and its Galois group H acts transitively on $\{\theta_1,\dots,\theta_u\}$. By the properties of Proposition 1.2,

$$\begin{aligned} R(X,Y) &= Res_t(F(X,t),G(Y,t)) = Res_t(f_n(t) - Xf_d(t), g_n(t) - Yg_d(t)) \\ &= a^v \prod_{i=1}^{u} (g_n(\theta_i) - Yg_d(\theta_i)) = b\prod_{i=1}^{u}(Y - g(\theta_i)), \end{aligned}$$

for some $b \in \mathbb{K}[X]$. This gives a complete factorization of $R(X,Y) \in \mathbb{E}[Y]$. It follows that any monic irreducible factor of $R(X,Y)$ in $\mathbb{K}(X)[Y]$ must have $g(\theta_i)$ as a root for some i, $1 \le i \le u$, hence it must be the minimal polynomial of $g(\theta_i)$ over $\mathbb{K}(X)$ for some i.

Now, let $h(Y)$ be the minimal polynomial of $g(\theta_1)$ over $\mathbb{K}(X)$. Then for all $\sigma \in H$, $h(g(\sigma\theta_1)) = \sigma h(g(\theta_1)) = 0$. By the transitivity of H, $h(g(\theta_i)) = 0$ for all i. This shows that $g(\theta_i)$ $(i = 1,\dots,u)$ all have the same minimal polynomial over $\mathbb{K}(X)$.

Since $R(f(t),g(t)) = 0$, we can write $R(X,Y) = bm(X,Y)^w$ for some divisor w of u. In order to show that w is the degree of the field extension of $\mathbb{K}(t)$ over

$\mathbb{K}(f(t), g(t))$, note

$$\begin{aligned} \deg_Y R(X,Y) = u &= [\mathbb{K}(t) : \mathbb{K}(f)], \\ \deg_Y m(X,Y) = \deg h(Y) &= [\mathbb{K}(f,g) : \mathbb{K}(f)]. \end{aligned}$$

Hence,

$$w = \frac{[\mathbb{K}(t) : \mathbb{K}(f)]}{[\mathbb{K}(f,g) : \mathbb{K}(f)]} = [\mathbb{K}(t) : \mathbb{K}(f,g)].$$

Comparing the degrees with respect to the variable X,

$$R(X,Y) = cm(X,Y)^w,$$

for some non-zero constant c.

(b) Suppose that $F(X,t)$ and $G(Y,t)$ are not separable polynomials and let p be the characteristic of the field $\mathbb{K}$. So, their partial derivatives with respect to t are zero, and

$$f_n'(t) = f_d'(t) = 0 \ \text{ and } \ g_n'(t) = g_d'(t) = 0.$$

Then we can write $f = \hat{f}(t^{rp})$ and $g = \hat{g}(t^{rp})$, where $\hat{f} = \hat{f}_n/\hat{f}_d, \hat{g} = \hat{g}_n/\hat{g}_d \in \mathbb{K}(t)$ and r is a positive natural number, such that $\hat{F}(X,t) = \hat{f}_n(t) - X\hat{f}_d(t)$ or $\hat{G}(Y,t) = \hat{g}_n(t) - Y\hat{g}_d(t)$ is separable. Note that $m(X,Y)$ is also a minimal polynomial of $\hat{f}$ and $\hat{g}$. By Proposition 1.2 and separability properties, we have

$$\begin{aligned} R(X,Y) &= Res_t(F(X,t), G(X,t)) = Res_t(\hat{f}_n(t^{rp}) - X\hat{f}_d(t^{rp}), \hat{g}_n(t^{rp}) - Y\hat{g}_d(t^{rp})) \\ &= Res_t(\hat{F}(X,t), \hat{G}(Y,t))^{rp} = \hat{c}^{rp} m(X,Y)^{\hat{w}rp}, \end{aligned}$$

where $\hat{w} = [\mathbb{K}(t) : \mathbb{K}(\hat{f}(t), \hat{g}(t))]$ and $\hat{c} \in \mathbb{K}^\times$. Therefore,

$$\begin{aligned} [\mathbb{K}(t) : \mathbb{K}(f(t), g(t))] &= [\mathbb{K}(t) : \mathbb{K}(\hat{f}(t^{rp}), \hat{g}(t^{rp}))] \\ &= [\mathbb{K}(t) : \mathbb{K}(t^{rp})] \cdot [\mathbb{K}(t^{rp}) : \mathbb{K}(\hat{f}(t^{rp}), \hat{g}(t^{rp}))] = rp\hat{w}. \end{aligned}$$

□

Now, we state a basic result on parametric curves, for later use.

Definition 1.4. Given a parametrization (f,g) of the plane curve $C = V(m)$:

– We say that (f,g) is a *normal* parametrization if $C = \{(f(t_0), g(t_0)) \mid t_0 \in \overline{\mathbb{K}}\}$; that is, every point $(x_0, y_0) \in C$ can be written as $(x_0, y_0) = (f(t_0), g(t_0))$ for some $t_0 \in \overline{\mathbb{K}}$.

– We say that (f,g) is a *faithful* parametrization if there exists a one-to-one map from points $(x_0, y_0) \in C$ to values of the parameters $t_0 \in \overline{\mathbb{K}}$, such that $(x_0, y_0) = (f(t_0), g(t_0))$, except a finite number of them.

Proposition 1.5. *Let (f,g) be a parametrization of the parametric curve C. Then:*

1. *(f,g) is a faithful parametrization if and only if $\overline{\mathbb{K}}(f,g) = \overline{\mathbb{K}}(t)$.*
2. *If $\deg f > \deg f_d$ or $\deg g > \deg g_d$, then (f,g) is a normal parametrization of C. If $\deg f = \deg f_d$ and $\deg g = \deg g_d$, then there exists at most one point of the curve C that cannot be written as $(f(t_0), g(t_0))$ for any $t_0 \in \overline{\mathbb{K}}$.*

Proof. The first part is a well-known fact (cf. [Sha]).

For the second part, by the Extension Theorem (cf. [CLO]), given $(x_0, y_0) \in C$, there exists $t_0 \in \overline{\mathbb{K}}$ such that $(x_0, y_0) = (f(t_0), g(t_0))$ if $\deg_t(f_n(t) - Xf_d(t)) = \deg(f_n(t) - x_0 f_d(t))$ or $\deg_t(g_n(t) - Yg_d(t)) = \deg(g_n(t) - y_0 g_d(t))$. So, we immediately get both claims. □

Remark 1.6. Given a parametrization (f, g) of C, there are methods to check if it is faithful or not, and in the negative case to compute a faithful one (cf. [AGR]).

On the other hand, it is easy to check if (f, g) is a normal parametrization: depending on the degree of the numerator and denominator, at most, you have to compute a $\gcd(f_n(t) - x_0 f_d(t), g_n(t) - y_0 g_d(t))$ for one point (x_0, y_0).

To conclude this section we give a simple fact which will be used below: let $f(t) = f_n/f_d \in \mathbb{K}(t)$ and $a \in \mathbb{K}$, such that $f(a)$ is defined, that is, $f_d(a) \neq 0$. Instead of $f(a)$ we sometimes write $f(t)|_{t=a}$.

Lemma 1.7. $\frac{f(t)-f(a)}{t-a}\big|_{t=a} = f'(a)$, *provided* $f(a)$ *is defined.*

Proof. We have

$$\frac{f(t) - f(a)}{t - a} = \frac{\frac{f_n(t)}{f_d(t)} - \frac{f_n(a)}{f_d(a)}}{t - a} = \frac{\frac{f_n(t)f_d(a) - f_n(a)f_d(t)}{t-a}}{f_d(t)f_d(a)}.$$

Then,

$$\frac{f(t) - f(a)}{t - a}\Big|_{t=a} = \frac{f_n'(a)f_d(a) - f_n(a)f_d'(a)}{f_d(a)f_d(a)} = f'(a).$$

□

2. The D-resultant of two rational functions

In [EY], the authors define the *D-resultant* of two polynomials $p(t), q(t) \in \mathbb{K}[t]$ as the resultant, with respect to the variable t, of the polynomials $\frac{p(t)-p(s)}{t-s}, \frac{q(t)-q(s)}{t-s}$. This definition can be extended to rational functions. First, we need this technical result:

Lemma 2.1. *Let* h_n, h_d *be non-constant polynomials in* $\mathbb{K}[t]$ *such that* $\gcd(h_n, h_d) = 1$. *Then the bivariate polynomial* $h_n(t)h_d(s) - h_d(t)h_n(s) \in \mathbb{K}[s, t]$ *does not have univariate factors. Moreover, if* $h_d'(t) \neq 0$, *then it has not the factor* $(t - s)^2$.

Proof. The proof of the first claim is straightforward (cf. [AGR]).

On the other hand, if $(t - s)^2$ divides $h_n(t)h_d(s) - h_d(t)h_n(s)$, then u^2 divides $h_n(t)h_d(t + u) - h_d(t)h_n(t + u)$. So $u = 0$ would be a common double root of the above polynomial and after derivation with respect to the variable u and setting $u = 0$, we would obtain

$$\frac{h_n(t)}{h_d(t)} = \frac{h_n'(t)}{h_d'(t)}.$$

But this is a contradiction since $\gcd(h_n, h_d) = 1$. □

Definition 2.2. Given a non-constant rational function $h(t) = h_n/h_d$ such that $\gcd(h_n, h_d) = 1$, the associated bivariate polynomial $h(s, t) \in \mathbb{K}[s, t]$ of h is

$$h(s, t) = \frac{h_n(t)h_d(s) - h_d(t)h_n(s)}{t - s}.$$

Now, given two non-constant rational functions $f(t) = f_n/f_d, g(t) = g_n/g_d$, we define the D-resultant of $f(t), g(t)$ by

$$DRes_t(f(t), g(t)) := Res_t(f(s, t), g(s, t)).$$

The D stands for Divided difference. Obviously this resultant is an element of $\mathbb{K}[s]$. If there is not confusion, we write $D(s)$ instead of $DRes_t(f(t), g(t))$. We observe that the D-resultant has a good behaviour under linear transformations:

Proposition 2.3. *Let (f, g) be two non-constant rational functions and $\lambda = \dfrac{at+b}{ct+d}$ a linear transformation. Then:*

1. *(f, g) and $(f(\lambda), g(\lambda))$ have the same minimal polynomial and their $R(X, Y)$'s coincide up to multiplication by a non-zero constant.*
2. *(f, g) and $(\lambda(f), \lambda(g))$ have the same D-resultant up to multiplication by a non-zero constant.*

The next useful proposition relates $D(s)$ to

$$R(X, Y) := Res_t(f_n(t) - Xf_d(t), g_n(t) - Yg_d(t)).$$

Proposition 2.4.

$$f'(s)D(s) = (-1)^{\deg f} g_d(s)^{\deg f-2} f_d(s)^{\deg g-2} R_Y(f(s), g(s))$$

and

$$g'(s)D(s) = (-1)^{\deg f+1} g_d(s)^{\deg f-2} f_d(s)^{\deg g-2} R_X(f(s), g(s)),$$

where R_X, R_Y are, respectively, the partial derivatives of R with respect to X, Y.

Proof. Let $r(s) := Res_t\left(f(s,t), g_n(t)g_d(s) - g_d(t)g_n(s)\right)$. If we write $g_n(t)g_d(s) - g_d(t)g_n(s) = (t-s)g(s,t)$, then by Proposition 1.2 we obtain

$$\begin{aligned} r(s) &= Res_t\left(f(s,t), t-s\right) D(s) = (-1)^{\deg f-1} f(s,s)D(s) \\ &= (-1)^{\deg f-1}\big(f_d(s)f_d(t)\frac{f(t)-f(s)}{t-s}\big)\big|_{t=s} D(s). \end{aligned}$$

By Lemma 1.7, we have

$$r(s) = (-1)^{\deg f-1} f_d(s)^2 f'(s)D(s). \tag{1}$$

Define $\tilde{R}(s, Y) := Res_t(f(s,t), g_n(t) - Yg_d(t))$. By Proposition 1.2

$$r(s) \quad = \tilde{R}(s, Y)|_{Y=g(s)} Res_t(g_d(s), f(s,t)) = \tilde{R}(s, Y)|_{Y=g(s)} g_d(s)^{\deg f-1}.$$

Also, writing $f_n(t)f_d(s) - f_d(t)f_n(s) = (t-s)f(s,t)$ we have

$$\begin{aligned} \tilde{R}(s, Y) &= \frac{Res_t(f_n(t)f_d(s) - f_d(t)f_n(s), g_n(t) - Yg_d(t))}{Res_t(t-s, g_n(t) - Yg_d(t))} \\ &= \frac{Res_t(f_n(t)f_d(s) - f_d(t)f_n(s), g_n(t) - Yg_d(t))}{g_n(s) - Yg_d(s)} \\ &= \frac{R(f(s), Y)f_d(s)^{\deg g}}{g_n(s) - Yg_d(s)}. \end{aligned}$$

Consequently, using $R(f(s), g(s)) = 0$ we obtain

$$\begin{aligned} r(s) \quad &= \quad g_d(s)^{\deg f-1} f_d(s)^{\deg g} \frac{R(f(s), Y) - R(f(s), g(s))}{g_n(s) - Yg_d(s)}\Big|_{Y=g(s)} \\ &= \quad -g_d(s)^{\deg f-2} f_d(s)^{\deg g} R_Y(f(s), g(s)) \quad \text{(by Lemma 1.7).} \end{aligned}$$

So together with (1) this gives

$$(-1)^{\deg f-1} f_d(s)^2 f'(s)D(s) = -g_d(s)^{\deg f-2} f_d(s)^{\deg g} R_Y(f(s), g(s)).$$

Therefore,

$$f'(s)D(s) = (-1)^{\deg f} g_d(s)^{\deg f-2} f_d(s)^{\deg g-2} R_Y(f(s), g(s)).$$

Analogously, we prove the second formula. □

3. The main theorem

Now we are able to state and prove the main result of this paper.

Theorem 3.1. *Let $f(t) = \frac{f_n(t)}{f_d(t)}$ and $g(t) = \frac{g_n(t)}{g_d(t)}$ in $\mathbb{K}(t)$ be non-constant rational functions and let $m \in \mathbb{K}[X, Y]$ be a minimal polynomial of (f, g) and $C = V(m)$ the associated parametric curve. We have:*

1. *$\mathbb{K}(f(t), g(t)) = \mathbb{K}(t)$ if and only if $D(s) \neq 0$.*
2. *$\mathbb{K}[t] \subset \mathbb{K}[f(t), g(t)]$ if and only if (f, g) is normal and $D(s) = c\prod_{i=1}^{r}(s - s_i)^{e_i}$ where each e_i is a positive integer and s_i is a root of f_d or g_d.*
3. *If $D(s) \neq 0$, say $D(s) = c\prod_{i=1}^{r}(s - s_i)^{e_i}$, where each e_i is a positive integer and all $s_i \in \overline{\mathbb{K}}$ are distinct, then:*
   (a) *If $(f(s_i), g(s_i))$ is defined, then it is a singularity of the curve C.*
   (b) *If $(f(s_0), g(s_0))$ is a singularity of C, then $s_0 = s_i$ for some $i \in \{1, \ldots, r\}$.*
   (c) *If $(f(s_i), g(s_i))$ is not defined, then s_i produces a singularity in one of the parametric curves defined by the parametrizations $(1/f, g)$, $(f, 1/g)$ or $(1/f, 1/g)$.*

Proof. 1. For zero characteristic fields, it has been proved in [AGR]. We are proving the theorem for an arbitrary field $\mathbb{K}$ adapting the mentioned proof.

Suppose that $\mathbb{K}(f(t), g(t)) = \mathbb{K}(h(t))$, with $\deg h > 1$; then $\mathbb{K}(f), \mathbb{K}(g) \subset \mathbb{K}(h)$. Then by Proposition 1.1, $h_n(t)h_d(s) - h_d(t)h_n(s)$ divides both $f_n(t)f_d(s) - f_d(t)f_n(s)$ and $g_n(t)g_d(s) - g_d(t)g_n(s)$. Hence, $f(s, t), g(s, t)$ have the common factor $h(s, t)$ and $D(s) = 0$.

Conversely, if $D(s) = 0$, we will prove that $\mathbb{K}(f(t), g(t)) = \mathbb{K}(h(t))$, with $\deg h > 1$.

We are going to divide this part of the proof into two different cases. The first case is when $f'_d(t)$ or $g'_d(t) \neq 0$ and the second one is when $f'_d(t) = g'_d(t) = 0$.

Case 1. We suppose that $D(s) = 0$; then $f(s, t), g(s, t)$ have a common factor, namely $H(s, t)$. Thus,

$$f_n(t)f_d(s) - f_d(t)f_n(s) = H(s, t)N(s, t)(t - s)$$

and

$$g_n(t)g_d(s) - g_d(t)g_n(s) = H(s, t)M(s, t)(t - s)$$

for some $N, M \in \mathbb{K}[s, t]$.

Next, we consider the algebraic set T defined by the polynomial $H(s, t)$, that is, $T = V(H(s, t)) \subset \overline{\mathbb{K}}^2$, which contains an infinite number of points. Moreover, since $H(s, t)$ has no univariate factors and it does not have $(t - s)$ as a factor (see Lemma 2.1), there exists an infinite number of points $(a, b) \in T$, with $a \neq b$ such that $f_d(a), g_d(a), f_d(b)$ and $g_d(b)$ are not zero. Then we find for these points that

$$\frac{f_n(a)}{f_d(a)} = \frac{f_n(b)}{f_d(b)} \quad \text{and} \quad \frac{g_n(a)}{g_d(a)} = \frac{g_n(b)}{g_d(b)}.$$

Moreover, note that $\mathbb{K}(f,g) = \mathbb{K}(t)$ implies $\overline{\mathbb{K}}(f,g) = \overline{\mathbb{K}}(t)$. This is a contradiction, because by Proposition 1.5, over an algebraically closed field, there cannot be an infinite number of images of $(f(t), g(t))$ in which the mapping is not injective.

Case 2. Let $p > 0$ be the characteristic of the field $\mathbb{K}$, and $f_d'(t) = g_d'(t) = 0$. If $f_n'(t)$ or $g_n'(t) \neq 0$, then we are in Case 1 for $1/f, 1/g$ and both have the same D-resultant; see Proposition 2.3 for $\lambda = 1/t$.

Otherwise, there exist $\hat{f}, \hat{g} \in \mathbb{K}(t)$ such that $f(t) = \hat{f}(t^p)$ and $g(t) = \hat{g}(t^p)$; then $\mathbb{K}(f,g) \subset \mathbb{K}(t^p)$.

3. Since $D(s) \neq 0$, we have $\mathbb{K}(f,g) = \mathbb{K}(t)$.

3(a) Suppose that $D(s_i) = 0$ and $f_d(s_i)g_d(s_i) \neq 0$. From Proposition 2.4 we have $f_d(s_i)^\alpha g_d(s_i)^\beta R_Z(f(s_i), g(s_i)) = 0$ for $Z \in \{X, Y\}$ and $\alpha, \beta \geq 0$. By Theorem 1.3 we get $m_X(f(s_i), g(s_i)) = m_Y(f(s_i), g(s_i)) = 0$. So $(f(s_i), g(s_i))$ is a singular point of the curve C.

3(b) Let $(f(s_0), g(s_0))$ be a singularity of C. If either $f'(s_0) \neq 0$ or $g'(s_0) \neq 0$, by Proposition 2.4 $D(s_0) = 0$.

Suppose that $f'(s_0) = g'(s_0) = 0$. Then $f(s_0, s_0) = g(s_0, s_0) = 0$. Since $D(s)$ is the resultant of $f(s,t), g(s,t)$ we can write (Proposition 1.2)

$$D(s) = f(s,t)h_1(s,t) + g(s,t)h_2(s,t)$$

for some polynomials $h_1(s,t), h_2(s,t)$. Substituting s and t by s_0 we get that $D(s_0) = 0$.

3(c) We have just seen that the zeroes of D can be either singularities of C or roots of $f_d(s)g_d(s)$. We claim that if $f_d(s_i) = 0$ or $g_d(s_i) = 0$, then s_i is a singular point of one of the curves defined by $X = 1/f(t), Y = g(t)$; $X = f(t), Y = 1/g(t)$; or $X = 1/f(t), Y = 1/g(t)$. By Proposition 2.3, the D-resultant of f, g is the D-resultant of the mentioned curves up to multiplication by a non-zero constant. So, we immediately get this claim.

2. Suppose $\mathbb{K}[t] \subset \mathbb{K}[f(t), g(t)]$. Then there exists a non-zero polynomial $p \in \mathbb{K}[X, Y]$ such that $t = p(f(t), g(t))$.

We claim that $\deg f > \deg f_d$ or $\deg g > \deg g_d$. If $\deg f \leq \deg f_d$ and $\deg g \leq \deg g_d$, then the degree of the denominator of $p(f,g)$ is greater than or equal to the degree of the numerator of $p(f,g)$, since the property is invariant with respect to the multiplication or sum of such rational functions. But this is a contradiction. By Proposition 1.5, we have that (f,g) is a normal parametrization.

On one hand, we have $\frac{p(f(t),g(t))-p(f(s),g(s)))}{t-s} = 1$. There exits a natural number r such that $e^r p(f(t), g(t)), e^r p(f(s), g(t))$ and $e^r p(f(s), g(s))$ are polynomials, where $e = f_d(t)f_d(s)g_d(t)g_d(s)$. Hence,

$$\frac{e^r p(f(t), g(t)) - e^r p(f(s), g(t))}{t - s} + \frac{e^r p(f(s), g(t)) - e^r p(f(s), g(s))}{t - s} = e^r. \tag{2}$$

Observe that $e^r(p(X, g(t)) - p(a, g(t)))$ is divisible by $X - a$ (for all a in $\mathbb{K}[s]$). So substituting $X = f(t)$ and $a = f(s)$ we obtain that for some $h_1, h_2 \in \mathbb{K}[s,t]$ and for some $r' \in \mathbb{N}$

$$e^{r'}(p(f(t), g(t)) - p(f(s), g(t))) \quad = (f(t) - f(s))h_1 = f(s,t)\tfrac{-h_1}{f_d(t)f_d(s)}$$

and

$$e^{r'}(p(f(s), g(t)) - p(f(s), g(s))) \quad = (g(t) - g(s))h_2 = g(s,t)\tfrac{-h_2}{g_d(t)g_d(s)}.$$

So by (2), we get that there exist polynomials $\hat{h}_1, \hat{h}_2 \in \mathbb{K}[s,t]$ such that

$$\hat{h}_1(s,t)f(s,t) + \hat{h}_2(s,t)g(s,t) = e^{r'}.$$

Let $s_0 \in \overline{\mathbb{K}}$ such that $f_d(s_0)g_d(s_0) \neq 0$. Then $f(s_0,t)$ and $g(s_0,t)$ have no common zero: If $f(s_0,t)$ and $g(s_0,t)$ have common zero t_0, then $g_d(t_0) = 0$. Since $g(s_0,t_0) = 0$, $g_d(s_0)g_n(t_0) = g_n(s_0)g_d(t_0) = 0$ and we get that $g_n(t_0) = 0$ or $g_d(s_0) = 0$. Contradiction.

On the other hand, we have that either $\deg f_n > \deg f_d$ or $\deg g_n > \deg g_d$. We can suppose, without loss of generality, that $\deg f_n > \deg f_d$. If $\deg g_n > \deg g_d$, we get $D(s_0) \neq 0$ since $\gcd(f(s_0,t), g(s_0,t)) = 1$.

For $\deg g_n < \deg g_d$, we have that $D(s_0) \neq 0$, if $g(s_0) \neq 0$. Suppose, $g(s_0) = 0$ and $D(s_0) = 0$. Then there exists θ in some algebraic extension of $\mathbb{K}(t)$ such that $f(s,\theta) = 0$ and $g(s,\theta) = 0$. Observe that $\theta \notin \overline{\mathbb{K}}$, otherwise we will get that $f(s) = f(\theta) \in \overline{\mathbb{K}}$. In particular, $\theta \neq s_0$ and $g_n(\theta)g_d(s_0) = 0$. This implies that $g_n(\theta) = 0$, which is not possible. So if $\deg g_n < \deg g_d$, we also get that $D(s_0) \neq 0$.

Finally, for $\deg g_n = \deg g_d$, we can take $\hat{g} = g + a$ such that $\deg \hat{g}_n < \deg \hat{g}_d$. Then we are in the same situation as before. Moreover, (f,g) and $(\hat{f},\hat{g})$ have the same D-resultant, up to multiplication by a non-zero constant.

To prove the converse, we can assume that $\mathbb{K}$ is algebraically closed, since $\overline{\mathbb{K}}[t] \subset \overline{\mathbb{K}}[f(t), g(t)]$ implies $\mathbb{K}[t] \subset \mathbb{K}[f(t), g(t)]$. Now suppose that $D(s) = \prod_{i=1}^{r}(s - s_i)^{e_i}$ where $f_d(s_i)g_d(s_i) = 0$.

Since $D(s) \neq 0$, $\mathbb{K}(f(t), g(t)) = \mathbb{K}(t)$. By hypothesis, (f,g) is normal; then each singularity can be written as $(f(s_0), g(s_0))$. By 3. we get that the irreducible plane curve $m(X,Y) = 0$ has no singularities. So for each maximal ideal η of the ring $A = \mathbb{K}[X,Y]/(m) (\simeq \mathbb{K}[f,g])$, A_η is a discrete valuation ring. Hence by [AMc, Theorem 9.3], A is integrally closed. So $\mathbb{K}[f,g]$ is integrally closed in $\mathbb{K}(t)$. Since t is obviously integral over $\mathbb{K}[f,g]$ it follows that $t \in \mathbb{K}[f,g]$, whence $\mathbb{K}[t] \subset \mathbb{K}[f,g]$ as desired. □

Corollary 3.2. *Let $f(t) = \frac{f_n(t)}{f_d(t)}$ and $g(t) = \frac{g_n(t)}{g_d(t)}$ in $\mathbb{K}(t)$ be non-constant rational functions and let $m \in \mathbb{K}[X,Y]$ be a minimal polynomial of (f,g) and $C = V(m)$ the associated parametric curve. We have:*

1. *If (f,g) is a faithful parametrization, then $\mathbb{K}[t] \subset \mathbb{K}[f,g]$ if and only if C has no singularities and (f,g) is normal.*
2. *We can find the singularities of the parametric curve C by computing the D-resultant.*

Proof. Via the D-resultant of f, g, we can decide if the parametrization is faithful and in the negative case we can compute a faithful one (see Remark 1.6).

By Theorem 3.1 we can compute every singularity of the form $(f(s_0), g(s_0))$. By Proposition 1.5 there exists at most one singularity that cannot be written as above. Moreover, we know exactly which one it is. □

Finally, we present some examples which show that in Theorem 3.1 we cannot omit any hypothesis. The first example shows that in part 3(b) we cannot avoid (f,g) to be normal:

Example 3.3. $f = \frac{-5t-28}{t^2}$ and $g = \frac{t^2}{-11t^2+38}$ is a parametrization of $m = 444X^2Y^2 + 2128XY + 23408XY^2 + 784 + 16298Y + 84414Y^2$. It is not normal since $(0, -1/11)$

is a point of the curve, but cannot be written as $(f(t_0), g(t_0))$. Moreover, $D(s) = 190s^2$ and $f_d(0) = 0$, but $\mathbb{K}[t] \not\subset \mathbb{K}[f, g]$.

In the next example, we will first see that there exist parametric curves with a singularity which cannot be produced via D-resultant, and secondly that the behaviour of the roots of $D(s)$ is unpredictable.

Example 3.4. Let $f = \frac{-50t^3-12t^2-18t+31}{-62t^5+77t^4+66t^3}, g = \frac{t^3-47}{-61t^5+41t^4-58t^2-90t}$. Their minimal polynomial m has a singularity in $(0, 0)$, but $\gcd(f_n, g_n) = 1$. The D-resultant of $f = t^2/(1 + t)$ and $g = t^3$ is $d = s^2(1 + s + s^2)$. $s_1 = 0$ gives the singularity $(0, 0)$; the other roots s_2, s_3 give the same singularity $(-1, 1)$.

Acknowledgements

This research is partially supported by Spanish DGES Grant Project PB97-0346 and by Hong Kong RGC Grant Project HKU 7126/98P.

References

[Abh] S. Abhyankar, *Algebraic Geometry for Scientists and Engineers*, Mathematical Surveys and Monographs **35**, American Mathematical Society, 1990. MR **92a:**14001

[AGR] C. Alonso, J. Gutierrez, T. Recio, *A rational function decomposition algorithm by near-separated polynomials*, J. Symbolic Computation **19** (1995), 527-544. MR **96j:**13025

[AMc] M. F. Atiyah, I. G. Macdonald, *Introduction to Commutative Algebra*, Addison Wesley, 1969. MR **39:**4129

[CLO] D. Cox, J. Little, D. O'Shea, *Ideals, Varieties and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Undergraduate Texts in Mathematics, Springer-Verlag, 1997. MR **97h:**13024

[EY] A. van den Essen, J.-T. Yu, *The D-resultant, singularities and the degree of unfaithfulness*, Proc. of the American Mathematical Society **125** (1997), 689-695. MR **97e:**13032

[MW] J. McKay, S. Wang, *An inversion formula for two polynomials in two variables*, J. Pure Applied Algebra **40** (1986), 245-257. MR **87j:**12003

[Swe] M. Sweedler, *Using Groebner bases to determine the algebraic and transcendental nature of field extensions: return of the killer tag variables*, pp. 66-75, Lectures Notes Computer Science **678**, Springer-Verlag, 1993. MR **94k:**13036

[Sha] I. R. Shafarevich, *Basic Algebraic Geometry*, Springer Study Edition, Springer-Verlag, 1977. MR **56:**5538

Departamento de Matemáticas, Estadística y Computación, Universidad de Cantabria, Avda. Los Castros, s/n 39005 Santander, Spain

E-mail address: jaime@matesco.unican.es

Departamento de Matemáticas, Estadística y Computación, Universidad de Cantabria, Avda. Los Castros, s/n 39005 Santander, Spain

E-mail address: sarito@matesco.unican.es

Department of Mathematics, The University of Hong Kong, Pokfulam Road, Hong Kong, China

E-mail address: yujt@hkusua.hku.hk