Singular factors of rational plane curves

Laurent Busé, Carlos d'Andrea

SINGULAR FACTORS OF RATIONAL PLANE CURVES

LAURENT BUSÉ AND CARLOS D'ANDREA

Abstract. We give a complete factorization of the invariant factors of resultant matrices built from birational parameterizations of rational plane curves in terms of the singular points of the curve and their multiplicity graph. This allows us to prove the validity of some conjectures about these invariants stated by Chen, Wang and Liu. As a byproduct, we also give a complete factorization of the D-resultant for rational functions in terms of the similar data extracted from the multiplicities.

1. Introduction

Curves in Computer Aided Geometric Design and in Visualization are often given in parametric form. Their singularities are usually points where the shape of the graphic gets more complicated. Hence, understanding the nature and character of these singular points has been an active area of research in the last years, see for instance [6, 11, 15, 12, 5, 4, 9] and the references therein.

In this article, we will focus on parametric plane curves defined over the complex numbers, although our results are valid for any field of characteristic zero, and the computational aspects can be performed also on any field containing the coefficients of the input polynomials. Let $a, b, c \in \mathbb{C}[s, v]$ be homogeneous polynomials of the same degree $n \geq 3$ with $\gcd(a, b, c) = 1$, such that the map

$$\begin{array}{rccc} \phi: & \mathbb{P}^1_{\mathbb{C}} & \to & \mathbb{P}^2_{\mathbb{C}} \\ & (s_0 : v_0) & \mapsto & (a(s_0, v_0) : b(s_0, v_0) : c(s_0, v_0)) \end{array} \tag{1}$$

parameterizes a plane rational algebraic curve $\mathcal{C}$ birationally onto its image (which is equivalent to say that the degree of $\mathcal{C}$ is n). As it was shown by Abhyankar in [1] for $c = v^n$, and later in general by Sendra and Winkler in [14], Gutierrez, Rubio and Yie in [8], and Pérez-Diaz in [12] among others, the parameterization ϕ can be used to detect the singular points of $\mathcal{C}$, which are those $P \in \mathcal{C}$ such that their multiplicity $m_P(\mathcal{C})$ is strictly greater than 1. As ϕ is generically one-to-one, $m_P(\mathcal{C})$ is actually the number of points in the preimage of $\phi^{-1}(P)$ counted with multiplicities (for a proper "parameterization-free" definition of $m_P(\mathcal{C})$ as well as its properties, see [1, 18]). This explains why from a computational point of view, the parameterization ϕ provides a lot of information about the singularities of $\mathcal{C}$. The purpose of this paper is to shed some light in this area.

We will use the notation and definitions given in [3] (see also [16]). Let $\{P_1, \ldots, P_r\}$ be the proper singular points of $\mathcal{C}$, and for all $i = 1, \ldots, r$ denote by

- $\mathfrak{z}^i_j$, $j \in I_i$, the irreducible branch-curves of $\mathcal{C}$ at P_i,
- $(t_{i,j} : u_{i,j})$, $j \in I_i$, the point of $\mathbb{P}^1_{\mathbb{C}}$ such that $\mathfrak{z}^i_j(t_{i,j} : u_{i,j}) = P_i$,

Date: February 20, 2012.

2010 *Mathematics Subject Classification.* Primary 14Q05; Secondary 13P15,68W30.

Key words and phrases. Rational plane curves, rational parameterizations, μ-bases, D-resultants, subresultants, invariant factors.

Both authors were partially supported by the bilateral (French-Spanish) collaboration PAI Picasso HF 2006–0220 . The second author was also partially supported by the research project MTM2007–67493 (Spain).

- $(P^i_{j,h})_{0\leq h}$ the neighboring point sequence of $\mathfrak{z}^i_j$ at P_i,
- $(m^i_{j,h})_{0\leq h}$ the multiplicity sequence of $\mathfrak{z}^i_j$ at P_i,
- $(\sim_h)_{o\leq h}$ the equivalence relations of the multiplicity graph of $\mathcal{C}$.

For a virtual point $P^i_{j,h}$ of $\mathcal{C}$, we define its multiplicity as $m_{P^i_{j,h}}(\mathcal{C}) := \sum_{j'\sim_h j} m^i_{j',h}$. Set

$$\begin{array}{rcl} F(s,v;t,u) & := & a(s,v)c(t,u) - a(t,u)c(s,v) \\ G(s,v;t,u) & := & b(s,v)c(t,u) - b(t,u)c(s,v), \end{array} \tag{2}$$

and let $\mathrm{Res}_{(s,v)}(-,-)$ be the Sylvester resultant operator which eliminates the homogeneous variables s and v . If $c = v^n$, then it is shown in [1] that there exists $0 \neq \gamma \in \mathbb{C}$ such that

$$\mathrm{Res}_{(s,v)}\left(\frac{F(s,v;t,u)}{su-tv}, \frac{G(s,v;t,u)}{su-tv}\right) = \gamma \prod_{\substack{i=1,\ldots,r \\ j\in I_i}} (u_{i,j}t - t_{i,j}u)^{\epsilon_{i,j}} \tag{3}$$

where for all $i = 1,\ldots,r$ and $j \in I_i$

$$\epsilon_{i,j} = \sum_{h\geq 0} m^i_{j,h}(m_{P^h_{j,h}}(\mathcal{C}) - 1).$$

From now on we will most of the time omit the nonzero constants. Hence, all identities involving polynomials should be understood up to a nonzero $\gamma \in \mathbb{C}$.

Let $B_{F,G}(t,u) \in \mathbb{C}[t,u]^{n\times n}$ be the square Bézout matrix built from $F(s,v;t,u)$, $G(s,v,t;u)$ regarded as polynomials in the variables (s,v) (see Section 5 for its precise definition and construction). Clearly, $B_{F,G}(t,u)$ does not have maximal rank as $su-tv$ is a common factor of both F and G. In [6], Chiohn and Sederberg showed that by analyzing the maximal minors of this matrix, one can obtain all the singular points of $\mathcal{C}$ in a very direct way. This approach was improved and refined by Chen, Wang and Liu in [5], where (2) is replaced with

$$\begin{array}{rcl} p_\phi(s,v;t,u) & = & p_1(s,v)a(t,u) + p_2(s,v)b(t,u) + p_3(s,v)c(t,u) \\ q_\phi(s,v;t,u) & = & q_1(s,v)a(t,u) + q_2(s,v)b(t,u) + q_3(s,v)c(t,u), \end{array} \tag{4}$$

with $\{p,q\} := \{(p_1,p_2,p_3), (q_1,q_2,q_3)\}$ being a basis of the free $\mathbb{C}[s,v]$-module of syzygies of (a,b,c). Suppose w.l.o.g. that $\deg(p) \leq \deg(q)$ and set $\mu := \deg(p)$. We then easily have $\mu \leq n-\mu = \deg(q)$. In the Computer Aided Geometric Design community, the set $\{p,q\}$ is called a μ-basis of the parameterization ϕ.

Let now $B_{p_\phi,q_\phi}(t,u) \in \mathbb{C}[t,u]^{(n-\mu)\times(n-\mu)}$ be the hybrid Bézout matrix associated to $p_\phi(s,v;t,u)$, $q_\phi(s,v;t,u)$ (for a definition of hybrid Bézout matrices, se also Section 5). It is shown in [5] that by computing the invariant factors of this matrix, one gets some kind of stratification of the singularities of $\mathcal{C}$ with respect to their multiplicities (Theorem 4 in [5]). This stratification is well understood when all the singularities of $\mathcal{C}$ are *ordinary* (i.e. when there are no virtual points $P^i_{j,h}$ with $h > 0$) and one can get an explicit description of the invariant factors of this matrix in terms of the singular points of $\mathcal{C}$ and their multiplicities (Theorems 5 and 6 in [5]).

In the case where $\mathcal{C}$ has singularities that are not ordinary, Chen, Wang and Liu stated a couple of conjectures (Conjectures 1 and 2 in [5]) relating the invariant factors with the multiplicity of the virtual points appearing in the process of desingularization of the curve. The main result of this paper is a complete factorization of the singular factors of $B_{p_\phi,q_\phi}(t,u)$ and as a consequence a complete proof and clarification of both conjectures.

To be more precise, let $S_{p_\phi,q_\phi}(t,u)$ be the Sylvester matrix of (4). It is simply the square $(n\times n)$-matrix of the $\mathbb{C}[t,u]$-linear map

$$\begin{array}{rcl}\mathbb{C}[t,u]\otimes_{\mathbb{C}}\mathbb{C}[s,v]_{n-\mu-1}\oplus\mathbb{C}[t,u]\otimes_{\mathbb{C}}\mathbb{C}[s,v]_{\mu-1} & \to & \mathbb{C}[t,u]\otimes_{\mathbb{C}}\mathbb{C}[s,v]_{n-1}\\ \alpha\oplus\beta & \mapsto & \alpha p_\phi+\beta q_\phi\end{array}\tag{5}$$

in the canonical monomial bases (the notation $\mathbb{C}[s,v]_d$, $d\in\mathbb{N}$, stands for the $\mathbb{C}$-vector space of homogeneous polynomials of degree d in $\mathbb{C}[s,v]$). A collection of homogeneous polynomials $d_1(t,u),d_2(t,u),\ldots,d_n(t,u)$ in $\mathbb{C}[t,u]$ such that, for $i=1,\ldots,n$ the product

$$d_n(t,u)^{n-i+1}d_{n-1}(t,u)^{n-i}\cdots d_{i+1}(t,u)^2d_i(t,u)\in\mathbb{C}[t,u]$$

is equal to the greatest common divisor of the $(n+1-i)$-minors of $S_{p_\phi,q_\phi}(t,u)$, is called a collection of *singular factors* of the parameterization ϕ. The existence of these polynomials is guaranteed by homogenizing with some care the invariant factors of $S_{p_\phi,q_\phi}(t,1)$.

The terminology of *singular factors* is taken from [5]. Note also that if $a,b,c\in k[s,v]$ with k a subfield of $\mathbb{C}$, then the singular factors will have their coefficients in k. This observation is of importance for computational purposes.

Now we are ready to present the main result of this paper.

Theorem 1.1. *With the notation established above, we have*

$$d_{n-\mu+1}(t,u)=\cdots=d_n(t,u)=1,$$

and for $k=2,\ldots,n-\mu$

$$d_k(t,u)=\prod_{i=1,\ldots,r,\ j\in I_i}(u_{i,j}t-t_{i,j}u)^{\epsilon^k_{i,j}}$$

where

$$\epsilon^k_{i,j}=\sum_{h\text{ such that }m_{P^i_{j,h}}(\mathcal{C})=k}m^i_{j,h}$$

We will see how this theorem implies Conjectures 1 and 2 in [5] in Section 2 and prove it in Section 4. We also point out that the factorization of invariant factors of matrices related to this problem is also considered in [9].

The reader may have already noticed that we just claimed above that the conjectures posted in [5] where made over the matrix $B_{p_\phi,q_\phi}(t,u)$ instead of $S_{p_\phi,q_\phi}(t,u)$. We will show in Section 5 that the cokernels of these two matrices plus a whole family of hybrid resultant matrices are isomorphic, thus Theorem 1.1 can also be formulated over the invariant factors of any of them. Our results in Section 5 can be regarded as an extension of those shown already by Apéry and Jouanolou in [2, Proposition 18].

We will also see in Section 6 that there is an explicit connection between $B_{p_\phi,q_\phi}(t,u)$ and $B_{F,G}(t,u)$, which will allow us to get a complete description of the invariant factors of the latter. As a direct consequence of this, we get a complete factorization into irreducible factors of D-resultants. These are a natural generalization of Abhyankar's formula (3) for $c=v^n$. Indeed, in [8], it is shown that if we take

$$\tilde{\Delta}(t,u):=\operatorname{Res}_{(s,v)}\left(\frac{F(s,v;t,u)}{su-tv},\frac{G(s,v;t,u)}{su-tv}\right),\tag{6}$$

for a general rational parameterization, it turns out that if $\phi(t_0:u_0)$ is a singularity of $\mathcal{C}$, then $\tilde{\Delta}(t_0,u_0)=0$, but there may be other roots coming from curves being parameterized by permutations of (a,b,c) see [8, Theorem 3.1], and there was no known analogue of a factorization like (3) for $\tilde{\Delta}(t,u)$.

In [4], the first author shows that by replacing (2) with (4) in the definition of $\tilde{\Delta}(t,u)$, one gets a polynomial $\Delta(t,u)$ which factorizes like (3). We will review the properties of $\Delta(t,u)$ in Section 2.

However, there was still missing a complete factorization of $\tilde{\Delta}(t,u)$. In Theorems 6.3 and 6.4 we give a precise description of the factors of the D-resultant, completing the information given in [8, Theorem 3.1].

Understanding the algebraic structure of these matrices may lead to new algorithms for studying the geometry of singular points of rational curves. We will see for instance in Example 2.1 that in some non trivial cases one can reconstruct the whole multiplicity graph of $\mathcal{C}$ from the invariant factors of these matrices, with operations only over the ground field of the parameterization. From a symbolic point of view, this problem has already been studied in [13, 16, 12].

Organization of the paper. In Section 2 we introduce some basic definitions and results, and also show how Theorem 1.1 implies Conjectures 1 and 2 in [5]. In Section 3 we prove the main theorem for curves having only ordinary singularities. The proof of the general case is given in Section 4. Section 5 is devoted to show that any resultant matrix can be used in Theorem 5. In Section 6, we describe all the invariant factors of $B_{F,G}(t,u)$ and show the complete factorization of D-resultants.

Acknowledgements. We would like to thank José Ignacio Burgos, Eduardo Casas-Alvero and Teresa Cortadellas for very interesting comments, suggestions and clarifications on topics about singularities of curves and commutative algebra. The second author would also like to thank the Fields Institute in Toronto, where part of this work was done.

2. Preliminary results and the singular factors conjectures

Throughout this paper, we will work over the field of complex numbers $\mathbb{C}$. However, it should be noted that all the statements and proofs work over any algebraically closed field of characteristic zero. We recall here again that every identity involving polynomials should be understood up to a nonzero constant.

Let $(x_1 : x_2 : x_3)$ be the homogeneous coordinates of $\mathbb{P}^2_{\mathbb{C}}$. By Hilbert-Burch's theorem, the first syzygy module of the sequence $a(s,v), b(s,v), c(s,v)$ is a free $\mathbb{C}[s,v]$-module of rank 2. Moreover, if μ denotes the smallest degree of a nonzero syzygy, then this syzygy module is generated in degrees μ and $n-\mu$. A μ-basis of the parameterization ϕ is then a choice of a basis of this syzygy module. Identifying any syzygy (g_1,g_2,g_3) with the bi-homogeneous form $g_1x_1+g_2x_2+g_3x_3$, a μ-basis corresponds to a couple of bi-homogeneous forms $p,q \in \mathbb{C}[s,v] \otimes_{\mathbb{C}} \mathbb{C}[x_1,x_2,x_3]$ of bi-degree $(\mu,1)$ and $(n-\mu,1)$ respectively, such that $1 \leq \mu \leq n-\mu$.

As $\mathcal{C}$ is a rational projective curve, we have that its number of singular points, counted properly, is given by the well known *genus formula*:

$$(n-1)(n-2) = \sum_{P \in \mathrm{Sing}(\mathcal{C})} m_P(\mathcal{C})(m_P(\mathcal{C})-1)$$

where $\mathrm{Sing}(\mathcal{C})$ stands for the singular points, proper as well as infinitely near, of the curve $\mathcal{C}$ and $m_P(\mathcal{C})$ stands for the multiplicity of the singular point P on $\mathcal{C}$. Notice that in our case we know that there exists at least one (proper) singular point on $\mathcal{C}$, since $n \geq 3$.

It is a well known fact that $\mathrm{Res}_{(s,v)}(p,q) \in \mathbb{C}[x_1,x_2,x_3]$ is an implicit equation of the curve $\mathcal{C}$, meaning that it is an irreducible and homogeneous degree n polynomial whose zero locus is exactly the curve $\mathcal{C}$ (recall that the parametrization ϕ is assumed

to be birational onto $\mathcal{C}$). Another interesting property is the following (see also [5, Lemma 2]):

Proposition 2.1. *Let $Q = (\alpha_1 : \alpha_2 : \alpha_3)$ be a point in $\mathbb{P}^2_{\mathbb{C}}$ and denote by $H_Q(s,v)$ a greatest common divisor of the two forms $\sum_{i=1}^3 \alpha_i p_i(s,v)$ and $\sum_{i=1}^3 \alpha_i q_i(s,v)$ in $\mathbb{C}[s,v]$. Then $H_Q(s,v)$ is a homogeneous polynomial of degree $m_Q(\mathcal{C})$ and if $m_Q(\mathcal{C}) \geq 1$ we have*

$$H_Q(s,v) = \prod_{i=1}^{N} (v_i s - s_i v)^{m_i}$$

where N is the number of irreducible branch-curves of $\mathcal{C}$ centered at Q and m_i denotes the multiplicity of Q with respect to the irreducible branch-curve $\mathfrak{z}$ such that $\mathfrak{z}(s_i : v_i) = Q$.

Proof. By a linear change of coordinates in $\mathbb{P}^2_{\mathbb{C}}$, one can assume that $Q = (0:0:1)$, because μ-bases have the expected property under linear changes of coordinates. By Hilbert Burch's theorem we have that, up to a constant,

$$a(s,v) = \begin{vmatrix} p_2(s,v) & p_3(s,v) \\ q_2(s,v) & q_3(s,v) \end{vmatrix} \text{ and } b(s,v) = \begin{vmatrix} p_3(s,v) & p_1(s,v) \\ q_3(s,v) & q_1(s,v) \end{vmatrix}.$$

If $h(s,v)$ is a divisor of $p_3(s,v)$ and $q_3(s,v)$, then it follows that $h(s,v)$ divides both $a(s,v)$ and $b(s,v)$. Reciprocally, suppose that $h(s,v)$ is a nontrivial divisor of $a(s,v)$ and $b(s,v)$. Then, as

$$p_1(s,v)a(s,v) + p_2(s,v)b(s,v) + p_3(s,v)c(s,v) = 0$$

and $c(s,v)$ does not share any nontrivial common factor with neither $a(s,v)$ nor $b(s,v)$, then $h(s,v)$ must divide $p_3(s,v)$. The same argument works for $q_3(s,v)$ and we deduce that $\gcd(p_3(s,v), q_3(s,v)) = \gcd(a(s,v), b(s,v))$. From here, the claimed equality follows from the definition of the multiplicity of a point on an irreducible branch-curve. □

Remark 1. As an easy consequence of Proposition 2.1, we have that if Q is a proper singular point on $\mathcal{C}$ then either $2 \leq m_Q(\mathcal{C}) \leq \mu$ or $m_Q(\mathcal{C}) = n - \mu$, a fact that has already been noticed in [15].

Proposition 2.1 shows that a μ-basis of ϕ provides nontrivial information on the proper singularities of $\mathcal{C}$. It turns out that it also carries informations on the infinitely near singularities of $\mathcal{C}$. Recall that we have the following property:

$$m_{P^i_{j,h}}(\mathcal{C}) = \sum_{j' \sim_h j} m^i_{j',h} \geq m^i_{j,h}.$$

Also, denote with $\mathrm{SRes}(p,q) \in \mathbb{C}[x_1, x_2, x_3]$ the first principal subresultant of p and q with respect to the couple of homogeneous variables (s,v). It is simply a certain minor of the Sylvester matrix of p and q with respect to (s,v) (see e.g. [2, 7, 4] for a precise definition). The following result is a slight refinement of [4, Section 4].

Theorem 2.2. *We have*

$$\Delta(t,u) = \mathrm{SRes}(p,q)(a(t,u), b(t,u), c(t,u)) = \gamma \prod_{\substack{i=1,\dots,r \\ j \in I_i}} (u_{i,j}t - t_{i,j}u)^{\epsilon_{i,j}} \tag{7}$$

where $0 \neq \gamma \in \mathbb{C}$ and for all $i = 1, \dots, r$ and $j \in I_i$

$$\epsilon_{i,j} = \sum_{h \geq 0} m^i_{j,h}(m_{P^h_{j,h}}(\mathcal{C}) - 1).$$

In particular,

$$\deg(\Delta(t,u)) = (\deg(\mathcal{C})-1)(\deg(\mathcal{C})-2) = \sum_{P\in \mathrm{Sing}(\mathcal{C})} m_P(\mathcal{C})(m_P(\mathcal{C})-1).$$

Proof. Although not stated explicitly under this form, this theorem follows from the results contained in [4, Section 4]. Indeed, the proof of Theorem 4.8 in loc. cit. shows that all the inequalities given in Proposition 4.6, always in loc. cit., are actually equalities for the first principal subresultant of p and q. Since these equalities occur at the level of irreducible branch-curves, they imply the above theorem which requires the use of the multiplicity graph of $\mathcal{C}$. In fact, the properties (P1), (P2) and (P3) in loc. cit. are consequences of this theorem but they constitute the finer result one can state without introducing the multiplicity graph of $\mathcal{C}$. □

Notice that Theorem 1.1 can be regarded as a refinement of the above theorem, since it provides non trivial factors of (7) that are in relation with the multiplicities of the singular points of the curve $\mathcal{C}$.

Let us now show how Theorem 1.1 implies the two conjectures stated in [5]. For each proper singular point $P_i \in \mathcal{C}$, $i = 1,\dots,r$, we have

$$H_{P_i}(t,u) = \prod_{j\in I_i} (u_{i,j}t - t_{i,j}u)^{m_{P_i}(\mathfrak{z}^i_j)} = \prod_{j\in I_i} (u_{i,j}t - t_{i,j}u)^{m^i_{j,0}}.$$

For all $2 \le k \le n-\mu$, set

$$h_k(t,u) = \prod_{P_i \text{ such that } m_{P_i}(\mathcal{C})=k} H_{P_i}(t,u).$$

From Theorem 1.1, it is clear that $h_k(t,u)$ divides $d_k(t,u)$. Actually, we have:

$$d_k(t,u) = h_k(t,u) \prod_{\substack{i=1,\dots,r\\ j\in I_i}} (u_{i,j}t - t_{i,j}u)^{\bar{\epsilon}^k_{i,j}},$$

where

$$\bar{\epsilon}^k_{i,j} = \sum_{h>0 \text{ such that } m_{P^i_{j,h}}(\mathcal{C})=k} m^i_{j,h} = \epsilon^k_{i,j} - \begin{cases} m^i_{j,0} & \text{if } m_{P_i}(\mathcal{C}) = k \\ 0 & \text{otherwise.}\end{cases}$$

Therefore, following the notation in [5, Conjecture 1], we can establish the validity of the first conjecture:

$$d_k(t,u) = h_k(t,u) \prod_{s=k}^{n-\mu} \Psi^s_k(t,u),$$

where for all pair $2 \le k, s \le n-\mu$,

$$\Psi^s_k(t,u) = \prod_{\substack{i=1,\dots,r\\ j\in I_i\\ m_{P_i}(\mathcal{C})=s}} (u_{i,j}t - t_{i,j}u)^{\bar{\epsilon}^k_{i,j}}.$$

Obviously $\Psi^s_k(t,u) = 0$ if $s < k$ (for multiplicities cannot increase through blowing up). Moreover, it is not hard to check that $\deg(\Psi^s_k(t,u))$ is k times the number of infinitely near and non-proper singularities of multiplicity r above a proper singular point of multiplicity s, which proves and makes more precise [5, Conjecture 1].

Now, define for all $k = 2,\dots,n-\mu$ the *reduced singular factor* $\tilde{d_k}(t,u)$ by the following procedure:

- Set $\tilde{d_k}(t,u) := d_k(t,u)$.
- Then, for all $l = n-\mu$ down to $k+1$ do $\tilde{d_k}(t,u) := \frac{\tilde{d_k}(t,u)}{\gcd(\tilde{d_k}(t,u), d_l(t,u))}$.

Theorem 1.1 then implies that

$$\tilde{d_k}(t,u) = \prod_{i=1,\dots,r,\ j\in I_i} (u_{i,j}t - t_{i,j}u)^{\tilde{\epsilon}^k_{i,j}},$$

where

$$\tilde{\epsilon}^k_{i,j} = \max\{\epsilon^k_{i,j} - \sum_{s=k+1}^{n-\mu} \epsilon^s_{i,j}, 0\}.$$

Therefore $\tilde{\epsilon}^k_{i,j} \neq 0$ if and only if $m_{P_i}(\mathcal{C}) = k$ and in this case it is equal to $\epsilon^k_{i,j}$. It follows that

$$\tilde{d_k}(t,u) = \prod_{\substack{i=1,\dots,r\\ j\in I_i\\ m_{P_i}(\mathcal{C})=k}} (u_{i,j}t - t_{i,j}u)^{\epsilon^k_{i,j}} = \prod_{P_i \text{ such that } m_{P_i}=k} H_{P_i}(t,u)^{l_i},$$

where l_i is the number of infinitely near points of multiplicity k above P_i, including P_i. This proves [5, Conjecture 2].

Before moving on to the next section, from a computational as well as theoretical point of view, it is interesting to point out that $\mathbb{C}[t]$ is a principal ideal domain, and hence one can use the theory of invariant factors over principal domains in order to get that the matrix $S_{p_\phi,q_\phi}(t,1)$ is equivalent to a diagonal matrix whose nonzero elements are

$$d_n(t,1), d_n(t,1)d_{n-1}(t,1), \cdots, d_n(t,1)d_{n-1}(t,1)\dots d_3(t,1)d_2(t,1), 0.$$

We will recall and use this property for proving Theorem 1.1. Notice also that a *single* Smith normal form computation of $S_{p_\phi,q_\phi}(t,1)$ yields *all* the singular factors of ϕ, after a linear change of coordinates of $\mathbb{P}^1$ if necessary – see Lemma 3.3. Let us conclude this section with an illustrative example.

Example 2.1. Take the following parameterization of a rational algebraic plane curve of degree $n = 10$:

$$\begin{cases} a &= s^2\,(2\,s+v)^2\,(s+v)^6 \\ b &= s^3\,(2\,s+v)^5\,\left(3\,s^2+2\,sv+v^2\right) \\ c &= -\,(s+v)^{10} \end{cases}$$

The computation of the μ-basis gives $\mu = 4$ and

$$p = (s+v)^4 x_1 + s^2\,(2\,s+v)^2\,x_3$$

$$q = s\left(3\,s^2+2\,sv+v^2\right)(2\,s+v)^3\,x_1 - (s+v)^6\,x_2$$

The associated Bézout matrix is then a 6×6-matrix from which we get, after dehomogenization $u = 1$ and a single Smith form computation, the following singular factors

$$d_6(t) = (t+1)^6,\ d_5(t) = 1,\ d_4(t) = \frac{1}{4}\,(2\,t+1)^2\,(t+1)^4\,t^2,\ d_3(t) = \frac{1}{4}\,(2\,t+1)^2\,t,$$

$$d_2(t) = \frac{1}{43}\left(43\,t^6+74\,t^5+71\,t^4+48\,t^3+21\,t^2+6\,t+1\right)(t+1)^6$$

and reduced singular factors

$$\tilde{d_6}(t) = d_6(t),\ \tilde{d_5}(t) = d_5(t) = 1, \tilde{d_4}(t) = \frac{1}{4}\,(2\,t+1)^2\,t^2, \tilde{d_3}(t) = 1,$$

$$\tilde{d_2}(t) = \frac{1}{43}\left(43\,t^6+74\,t^5+71\,t^4+48\,t^3+21\,t^2+6\,t+1\right)$$

Although it is not always possible in general, we can recover here the multiplicity graph of the curve by using Theorem 1.1. For that purpose, we start by inspecting d_6, the non-trivial singular factor with the highest index. We deduce that there

is an irreducible singularity of multiplicity 6 corresponding to the parameter value $t = -1$. Looking at the other singular factors, we obtain that this singular point has a multiplicity 4 singular point in its first neighborhood and then has singular points of multiplicity 2 in its third, fourth and fifth neighborhood. So we obtain the first branch of the multiplicity graph, see Fig. 1.

Now, by inspecting d_4, we deduce that there is a singular point of multiplicity 4 which is formed by two irreducible branch-curves, one, say $\mathfrak{z}_1$ centered at $t = -1/2$ and another one, say $\mathfrak{z}_2$ centered at $t = 0$. The singular factor d_3 then shows that these two irreducible branches split up at the third neighborhood and have the multiplicities given in Fig. 1 in the second neighborhood (the horizontal bar stands for the equivalence relation of the multiplicity graph). Then, since d_2 does not vanish at $t = -1/2$ or $t = 0$ the mutliplicity graph at this multiplicity 4 point is known; see Fig. 1.

Finally, a simple additional computation shows that the discriminant of $d_2/(t+1)^6$ is nonzero. Therefore, it only remains to add 3 ordinary double points to the multiplicity graph to complete it.

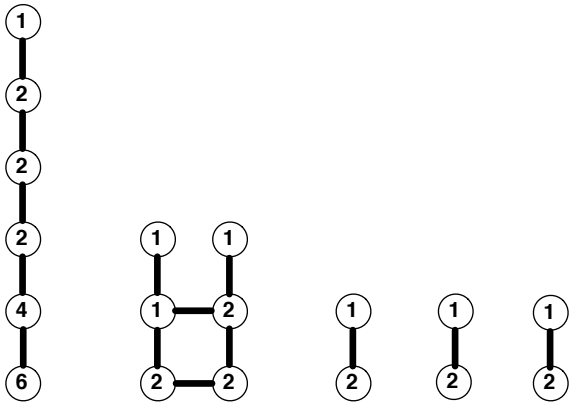

FIGURE 1. Multiplicity graph of the degree 10 rational plane curve given in Example 2.1

3. The case of ordinary curves

To prove Theorem 1.1, we will proceed by induction on the minimal length of a resolution of singularities of $\mathcal{C}$. The initial step would then correspond to the case where $\mathcal{C}$ is an ordinary curve, i.e. $\mathcal{C}$ has only ordinary singularities. Although a proof of this result already appeared in [5, Theorem 5], we provide in this section an alternative proof for the sake of completeness and also as the preparation for the proof of Theorem 1.1.

We start by recalling very briefly some results of invariant factors and Fitting ideals theory we will need in the sequel. The reader may consult any book on Algebra like [10, Chapter III, §7 and Chapter XIX, §2] for proofs of these statements.

Let R be a principal ideal domain and M a finitely generated R-module. There exists a sequence of non invertible elements $(\alpha_1, \ldots, \alpha_\ell)$ such that

i) For all $i = 1, \ldots, \ell - 1$, α_i divides α_{i+1}.
ii) M is isomorphic to $\frac{R}{(\alpha_1)} \oplus \frac{R}{(\alpha_2)} \oplus \cdots \oplus \frac{R}{(\alpha_\ell)}$.

The elements $\alpha_1, \ldots, \alpha_\ell$ are unique up to multiplication by a unit and are called the *invariant factors* of the R-module M. They can be recovered from the Fitting ideals of M, denoted $\mathfrak{F}_i(M)$, since

$$\mathfrak{F}_0(M) = (\alpha_1 \ldots \alpha_\ell) \subset \mathfrak{F}_1(M) = (\alpha_1 \ldots \alpha_{\ell-1}) \subset \ldots \subset \mathfrak{F}_{\ell-1}(M) = (\alpha_1) \subset \mathfrak{F}_\ell(M) = \mathfrak{F}_{\ell+1}(M) = \cdots = R$$

The smallest integer r such that $\mathfrak{F}_r(M) \neq 0$ is called the *rank* of M.

It is important to notice for further use that the Fitting invariants of M commute with localization: if S is a multiplicatively closed subset of R not containing the zero element, then for every integer $\nu \geq 0$ we have

$$\mathfrak{F}_\nu(M)R_S = \mathfrak{F}_\nu(M_S) \tag{8}$$

Also, the Fitting invariants of M can be computed from any finite R-presentation of M. Such a presentation corresponds to a matrix, say A, with entries in R. The above results mean that this matrix is equivalent to a diagonal matrix, sometimes called the Smith normal form of A, whose nonzero elements are the invariant factors of $M = \operatorname{coker}(A)$.

We will also use later in the text the following result which is due to Thompson [17].

Theorem 3.1. *Let A, B, C be three square matrices with entries in R such that $AB = C$. If $\alpha_1|\alpha_2|\ldots|\alpha_n$, $\beta_1|\beta_2|\ldots|\beta_n$, $\gamma_1|\gamma_2|\ldots|\gamma_n$ are the invariant factors of A, B, and C respectively, then*

$$\alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_m}\beta_{j_1}\beta_{j_2}\cdots\beta_{j_m} | \gamma_{i_1+j_1-1}\gamma_{i_2+j_2-2}\cdots\gamma_{i_m+j_m-m}$$

whenever the integer subscripts satisfy

$$1 \leq i_1 < i_2 < \cdots < i_m,\ 1 \leq j_1 < j_2 < \cdots < j_m,\quad i_m + j_m \leq m + n.$$

Now, we examine the behavior of the singular factors under linear change of coordinates, it will also be very useful in the sequel.

Lemma 3.2. *The singular factors of a proper parameterization do not depend neither on the choices of the μ-basis nor the coordinates of $\mathbb{P}^2$.*

Proof. Indeed, a change of μ-bases or a change of coordinates of $\mathbb{P}^2$ correspond to elementary transformation of the Sylvester matrix $S_{p_\phi, q_\phi}(t, u)$. Therefore, its Fitting invariants remains unchanged so that the same holds for their codimension one part. □

Recall that a linear change of coordinates of $\mathbb{P}^1$, that is to say an isomorphism

$$\psi : \mathbb{P}^1 \xrightarrow{\sim} \mathbb{P}^1 : (t' : u') \mapsto (\alpha t' + \beta u' : \delta t' + \gamma u')$$

where $\alpha, \beta, \delta, \gamma \in \mathbb{C}$ and $\alpha\gamma - \beta\delta \neq 0$, corresponds to the isomorphism of graded rings ("base change" map)

$$\begin{array}{rcl} \psi^\sharp : \mathbb{C}[t, u] & \xrightarrow{\sim} & \mathbb{C}[t', u'] \\ t & \mapsto & (\gamma t' - \beta u')/(\alpha\gamma - \beta\delta) \\ u & \mapsto & (\delta t' - \alpha u')/(\alpha\gamma - \beta\delta). \end{array}$$

The following lemma shows that computing singular factors "commutes" with linear changes of coordinates of $\mathbb{P}^1$.

Lemma 3.3. *Let $d_1(t, u), d_2(t, u), \ldots, d_n(t, u)$ be the singular factors of the parameterization ϕ of $\mathcal{C}$ and let ψ be a linear change of coordinates in $\mathbb{P}^1$. Then, the homogeneous polynomials in $\mathbb{C}[t', u']$*

$$\psi^\sharp(d_1(t, u)), \psi^\sharp(d_2(t, u)), \ldots, \psi^\sharp(d_n(t, u))$$

are the singular factors of the parameterization $\phi \circ \psi : \mathbb{P}^1 \to \mathbb{P}^2$ *of* $\mathcal{C}$.

Proof. It is not hard to check that if $\{p, q\}$ is a μ-basis of ϕ then $\psi^\sharp(p), \psi^\sharp(q)$ is a μ-basis of $\phi \circ \psi$. Now, the map $\psi^\sharp$ gives a $\mathbb{C}[t,u]$-module structure to $\mathbb{C}[t',u']$ so that the Sylvester matrix obtained by the change of coordinates ψ is nothing but $S_{p_\phi,q_\phi}(t,u) \otimes_{\mathbb{C}[t,u]} \mathbb{C}[t',u']$. Therefore, by the right-exactness of tensor product we deduce that the Fitting ideals of the cokernel of $S_{p_\phi,q_\phi}(t,u) \otimes_{\mathbb{C}[t,u]} \mathbb{C}[t',u']$ are equal to the Fitting ideals of $S_{p_\phi,q_\phi}(t,u)$ tensored with $\mathbb{C}[t',u']$ over $\mathbb{C}[t,u]$. It follows that the same property holds for the codimension one part of these Fitting ideals. Hence, the lemma is proved. □

Let M stand for the cokernel of the Sylvester matrix $S_{p_\phi,q_\phi}(t,1)$ defined in (5). Note that M is a $\mathbb{C}[t]$-module.

Proposition 3.4. *With above notation, we have* $\mathfrak{F}_0(M) = 0$ *and* $\mathfrak{F}_1(M) = (\Delta(t,1))$*; in particular,* M *has rank 1. Moreover,* $\mathfrak{F}_\ell(M) = R$ *for all* $\ell > n - \mu$.

Proof. Since (5) provides a finite presentation of M, one can compute the Fitting invariants of M as the determinantal ideals of (5), namely the Sylvester matrix of p_ϕ and q_ϕ. Thus, $\mathfrak{F}_0(M)$ is generated by the determinant of this Sylvester matrix, which is equal to zero.

Recall the following classic property of the Sylvester matrix: the corank of the Sylvester matrix of two given polynomials is equal to the degree of the gcd of these two polynomials. So, by using Proposition 2.1 and Remark 1, we have that the Fitting invariants of M are supported on the singular locus of $\mathcal{C}$ and $\mathfrak{F}_\ell(M) = A$ for all $\ell > n - \mu$ since there are no singular points on $\mathcal{C}$ of multiplicity $> n - \mu$.

To prove that $\mathfrak{F}_1(M) = (\Delta(t,1))$, we proceed as follows: let

$$\begin{array}{rcl} P(s,v;t) & = & \frac{p_\phi(s,v;t,1)}{s-t\,v} \\ Q(s,v;t) & = & \frac{q_\phi(s,v;t,1)}{s-t\,v}. \end{array}$$

Applying the results given in [7, Theorem 2.2], we get that

$$\mathrm{S}_1(p_\phi, q_\phi; s, v) = Res_{(s,v)}(P(s,v;t), Q(s,v;t))\,(s - t\,v)v^{n-3}, \tag{9}$$

where S_1 denotes the first subresultant polynomial operator applied to the sequence p_ϕ, q_ϕ with respect to the homogeneous variables (s,v). By taking leading coefficients with respect to s in both sides of the latter equality, we get

$$\Delta(t,1) = \mathrm{SRes}(p,q)(a(t,1), b(t,1), c(t,1)) = \mathrm{Res}_{(s,v)}(P(s,v;t), Q(s,v;t)),$$

the first equality is given by Theorem 2.2.

Now, we can decompose the map (5) as the composition between:

$$\begin{array}{ccc} \mathbb{C}[t] \otimes_{\mathbb{C}} \mathbb{C}[s,v]_{n-\mu-1} \oplus \mathbb{C}[t] \otimes_{\mathbb{C}} \mathbb{C}[s,v]_{\mu-1} & \stackrel{\psi_1}{\to} & \mathbb{C}[t] \otimes_{\mathbb{C}} \mathbb{C}[s,v]_{n-2} \\ \alpha \oplus \beta & \mapsto & \alpha \frac{p_\phi(s,v;t,1)}{s-tv} + \beta \frac{q_\phi(s,v;t,1)}{s-tv} \end{array}$$

and

$$\begin{array}{ccc} \mathbb{C}[t] \otimes_{\mathbb{C}} \mathbb{C}[s,v]_{n-2} & \stackrel{\times(s-tv)}{\to} & \mathbb{C}[t] \otimes_{\mathbb{C}} \mathbb{C}[s,v]_{n-1} \\ \gamma & \mapsto & (s-tv)\gamma. \end{array}$$

By setting $v = 1$, it is now clear that all the minors of size $(n-1)$ in the matrix $S(a(t,1), b(t,1), c(t,1))$ are linear combinations of maximal minors of ψ_1 times maximal minors of the multiplication map in the right. If we build the matrices of these morphisms using the basis $\{(s-tv)^j s^{n-1-j}\}$ instead of $\{s^j v^{n-1-j}\}$ and compute the matrices of these linear transformations, then the morphism of

multiplication by $s - tv$ would have an $n \times (n-1)$ matrix of the form

$$\begin{pmatrix} 0 & 0 & \dots & 0 \\ 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}.$$

This essentially implies that in these bases there is only one nonzero minor of ψ_1 to be considered, and due to (9), it is easy to see that this minor is actually $\mathrm{SRes}(p,q)(a(t,1),b(t,1),c(t,1)) = \mathrm{Res}_{(s,v)}(P(s,v;t),Q(s,v;t))$. The proof follows straightforwardly from here. □

Corollary 3.5. *With the above notation, up to multiplicition by a nonzero constant in $\mathbb{C}$ we have $d_k(t,u) = 1$ for all $k > n - \mu$ and*

$$\Delta(t,u) = d_{n-\mu}(t,u)^{n-\mu-1} d_{n-\mu-1}(t,u)^{n-\mu-2} \cdots d_2(t,u)$$

Proof. Perform a sufficiently general linear change of coordinates in $\mathbb{P}^2$ in such a way that there are no singularities of $\mathcal{C}$ at $\{x_3 = 0\}$, and then apply Proposition 3.4 and Lemma 3.3. □

Remark 2. If instead of $P(s,v;t)$, $Q(s,v;t)$ we used in the proof of Proposition 3.4 $\frac{F(s,v;t,1)}{s-tv}$, $\frac{G(s,v;t,1)}{s-tv}$ then we would not have $\Delta(t,1)$ equals to the resultant of these two polynomials anymore, as we may loose some kind of uniqueness by allowing this symmetry (see for instance the statement of Theorem 3.1 in [8]). We will give a proper factorization of this polynomial in Section 6.

Proposition 3.6. *For any proper singularity Q on $\mathcal{C}$, the polynomial $H_Q(t,u)$ defined in Proposition 2.1 divides $d_{m_Q(\mathcal{C})}(t,u)$. Also, we have that $H_Q(t,u)$ and $d_k(t,u)$ are coprime for all $k > m_Q(\mathcal{C}) = \deg\big(H_Q(t,u)\big)$.*

Proof. Let $S_{p,q}(x_1,x_2,x_3)$ be the Sylvester matrix of the polynomials $\sum_{i=1}^3 x_i p_i(s,v)$ and $\sum_{i=1}^3 x_i q_i(s,v)$ with respect to the homogeneous variables (s,v). Its entries are linear forms in $\mathbb{C}[x_1,x_2,x_3]$. Therefore, its determinantal ideals, denoted $I_k(-)$, $k = 1,\dots,n$, are homogeneous ideals in $\mathbb{C}[x_1,x_2,x_3]$.

Then, by using Proposition 2.1 we deduce that

$$V(I_k(S_{p,q}(x_1,x_2,x_3))) = \emptyset \subset \mathbb{P}^2_{\mathbb{C}}$$

for all $k = 1,\dots,\mu$, as there cannot be any common factor of degree more than $n-\mu$ of these two forms after specializing the x_i (see Remark 1). It follows then that

$$V(I_k(S_{p,q}(a(t,u),b(t,u),c(t,u)))) = \emptyset \subset \mathbb{P}^1_{\mathbb{C}}$$

for all $k = 1,\dots,\mu$, and this implies $d_k(t,u) = 1$ for all $k > n - \mu$.

Now, assume for simplicity that $Q = (0:0:1)$ as both $H_Q(t,u)$ and $d_{m_Q(\mathcal{C})}(t,u)$ are invariant under linear changes of coordinates in $\mathbb{P}^2_{\mathbb{C}}$, and set $m := \deg(H_Q(t,u))$. As we did above, we have $Q \notin V(I_k(S_{p,q}(x_1,x_2,x_3)))$ for all $k = 1,\dots,n-m$ which implies that $H_Q(t,u)$ and $d_k(t,u)$ are relatively prime polynomials for all $k > m$. On the other hand, $Q \in V(I_{n-m+1}(S_{p,q}(x_1,x_2,x_3)))$, that is $I_{n-m+1}(S_{p,q}(x_1,x_2,x_3)) \subset (x_1,x_2)$, and hence

$$I_{n-m+1}(S_{p,q}(a(t,u),b(t,u),c(t,u))) \subset (a(t,u),b(t,u)) \subset (H_Q(t,u)) \subset \mathbb{C}[t,u]$$

It follows that $H_Q(t,u)$ divides $d_{n-1}(t,u)^{n-m} \cdots d_{m+1}(t,u)^2 d_m(t,u)$. As it is coprime with $d_{n-1}(t,u)^{n-m} \cdots d_{m+1}(t,u)^2$, we conclude that $H_Q(t,u)$ divides $d_m(t,u)$. □

As a corollary we recover Theorem 5 in [5].

Corollary 3.7. *The curve $\mathcal{C}$ has no infinitely near singularities if and only if for all $k = 2, \ldots, n-1$*

$$d_k(t,u) = \prod_{Q \in \mathrm{Sing_p}(\mathcal{C}) \text{ such that } m_Q(\mathcal{C})=k} H_Q(t,u)$$

where $\mathrm{Sing_p}(\mathcal{C})$ denotes the subset of $\mathrm{Sing}(\mathcal{C})$ consisting exclusively of the proper singularities of the curve $\mathcal{C}$.

In particular, if the curve $\mathcal{C}$ has only ordinary singularities then Theorem 1.1 holds.

Proof. By Proposition 3.6, $H_Q(t,u)$ divides $d_{m_Q}(t,u)$. Note that if $Q \neq Q'$, then the polynomials $H_Q(t,u)$ and $H_{Q'}(t,u)$ are coprime as each of them provides an inversion formula for the parameterization around two different points. We deduce from here that $\prod_{Q \in \mathrm{Sing_p}(\mathcal{C}):\, m_Q=k} H_Q(t,u)$ divides $d_k(t,u)$, and hence that $\prod_{Q \in \mathrm{Sing_p}(\mathcal{C}):\, m_Q=k} H_Q(t,u)^{m_Q-1}$ divides $d_k(t,u)^{k-1}$. Finally, this implies that

$$\prod_{Q \in \mathrm{Sing_p}(\mathcal{C})} H_Q(t,u)^{m_Q(\mathcal{C})-1} \text{ divides } d_{n-\mu}(t,u)^{n-\mu-1} d_{n-\mu-1}(t,u)^{n-\mu-2} \cdots d_2(t,u)$$

and that these two polynomials are equal (up to a nonzero multiplicative constant) if and only if for all $k = 2, \ldots, n-\mu$

$$d_k(t,u) = \prod_{Q \in \mathrm{Sing_p}(\mathcal{C}) \text{ such that } m_Q(\mathcal{C})=k} H_Q(t,u).$$

As the polynomial $H_Q(t,u)$ has degree $m_Q(\mathcal{C})$, we deduce that

$$\deg\left(\prod_{Q \in \mathrm{Sing_p}(\mathcal{C})} H_Q(t,u)^{m_Q(\mathcal{C})-1}\right) = \sum_{Q \in \mathrm{Sing_p}(\mathcal{C})} m_Q(\mathcal{C})(m_Q(\mathcal{C}) - 1). \tag{10}$$

But by Corollary 3.5

$$d_{n-\mu}(t,u)^{n-\mu-1} d_{n-\mu-1}(t,u)^{n-\mu-2} \cdots d_2(t,u) = \Delta(t,u),$$

and by Theorem 2.2, $\Delta(t,u)$ has degree equal to (10) if and only if $\mathrm{Sing_p}(\mathcal{C}) = \mathrm{Sing}(\mathcal{C})$, i.e. if and only if all the singularities are ordinary. □

4. Proof of the main theorem

To prove Theorem 1.1 we will proceed by induction on the minimal length of a resolution of $\mathcal{C}$. Define the following property for any integer $N \geq 0$:

(H_N) : *Theorem 1.1 holds for any rational projective plane curve $\mathcal{C}$ whose singularities can be resolved after a sequence of N blow-ups, assuming that (5) is built from a μ-basis of a proper parameterization of $\mathcal{C}$.*

Corollary 3.7 implies that the property (H_0) holds. Now, assume that $\mathcal{C}$ can be resolved by a sequence of N blow-ups and that (H_{N-1}) holds. By hypothesis, there exists a sequence of rational projective plane curves

$$\mathcal{C} = \mathcal{C}_0 \leftarrow \tilde{\mathcal{C}} = \mathcal{C}_1 \leftarrow \mathcal{C}_2 \leftarrow \cdots \leftarrow \mathcal{C}_{N-1} \leftarrow \mathcal{C}_N$$

such that each arrow corresponds to a blow-up (quadratic transformation) at a singular point and $\mathcal{C}_N$ has only ordinary singularities. It is clear that $\tilde{\mathcal{C}}$ can be resolved by a sequence of $N-1$ blow-ups, so Theorem 1.1 holds for $\tilde{\mathcal{C}}$ by our inductive hypothesis.

The curve $\tilde{\mathcal{C}}$ is obtained by blowing-up $\mathcal{C}$ at a singular point P of $\mathcal{C}$. To simplify the notation, we will hereafter denote by $m \geq 2$ the multiplicity of P on $\mathcal{C}$, by $\mathfrak{z}_i$ the

irreducible branch-curve of $\mathcal{C}$ such that $\mathfrak{z}_i(t_i) = P$, $i = 1, \dots, i_P$ and by $1 \leq \nu_i \leq m$ the multiplicity of P on $\mathfrak{z}_i$. We will also denote by

- $(P = P_0^i, P_1^i, \dots)$ the sequence of points infinitely near to P in the blow-up sequence of $\mathfrak{z}_i$,
- $(m = m_0^i, m_1^i, \dots)$ the sequence of the corresponding multiplicities of the P_j^i as points on $\mathcal{C}$,
- and by $(\nu_i = \nu_0^i, \nu_1^i, \dots)$ the sequence of the corresponding multiplicities as points on $\mathfrak{z}_i$.

Given $f(t) \in \mathbb{C}[t]$ and $a \in \mathbb{C}$, the notation $\mathrm{val}_a\big(f(t)\big)$ stands for the valuation of $f(t)$ at a, that is to say the largest integer k such that $(t-a)^k$ divides $f(t)$.

For $i \in \{1, \dots, i_P\}$, let $\mathfrak{p}_i$ be the principal ideal in $\mathbb{C}[t]$ generated by $t - t_i$. Consider the $R_{\mathfrak{p}_i}$-module $M_{\mathfrak{p}_i}$. It satisfies $\mathfrak{F}_\nu(M)R_{\mathfrak{p}_i} = \mathfrak{F}_\nu(M_{\mathfrak{p}_i})$ for all $\nu \in \mathbb{N}$. From the proof of Proposition 3.6, we already know that $\mathfrak{F}_0(M_{\mathfrak{p}_i}) = 0$ and that $\mathfrak{F}_j(M_{\mathfrak{p}_i}) = R_{\mathfrak{p}_i}$ for all $j \geq m$, so that

$$\mathrm{val}_{t_i}(d_{n-1}(t)) = \mathrm{val}_{t_i}(d_{n-2}(t)) = \cdots = \mathrm{val}_{t_i}(d_{m+1}(t)) = 0$$

Moreover, from Proposition 3.4 and Theorem 2.2 we obtain that $\mathfrak{F}_1(M_{\mathfrak{p}_i})$ is generated by $d_m(t)^{m-1}d_{m-1}(t)^{m-2}\dots d_3(t)^2 d_2(t)$ and

$$\mathrm{val}_{t_i}\left(d_m(t)^{m-1}d_{m-1}(t)^{m-2}\dots d_3(t)^2 d_2(t)\right) = \sum_{k=2}^{m}\left((k-1)\sum_{m_j^i = k}\nu_j^i\right). \tag{11}$$

Recall that $\tilde{\mathcal{C}}$ is obtained after blowing up a point in $\mathcal{C}$. We want to assume w.l.o.g. that the point being blown up is $(0:0:1)$, and that the quadratic transformation is $X = X'$ and $Y = X'Y'$. In order to do this correctly, we will perform a general change of coordinates of $\mathbb{P}^1$ and of $\mathbb{P}^2$ that will simplify the blow-up computations. Recall that the R-module M is not affected by a change of coordinates of $\mathbb{P}^2$ thanks to Lemma 3.2, and Lemma 3.3 shows that Theorem 1.1 can be proved w.l.o.g. in any choice of coordinates of $\mathbb{P}^1$.

After then a general change of coordinates in both spaces, we can assume w.l.o.g. that

(i) our singular point above is $P = (0:0:1)$,
(ii) the only singularity of $\mathcal{C}$ on the line $\{x_1 = 0\}$ is P,
(iii) the line $\{x_1 = 0\}$ is not tangent to $\mathcal{C}$ at P,
(iv) $\phi(1:0)$ is not a singular point of $\mathcal{C}$,
(v) $(0:1:0) \notin \mathcal{C}$ and $(1:0:0) \notin \mathcal{C}$, i.e. $\gcd(a,c) = \gcd(b,c) = 1$,
(vi) $\phi(1:0) \in \{x_3 = 0\}$, which essentially means that $\deg_t(c(t,u)) < n$,
(vii) there are no singularities of $\mathcal{C}$ on the line $\{x_3 = 0\}$.

Now, since we assumed (i)-(iii), we apply the quadratic transformation $X = X'$ and $Y = X'Y'$ so that the exceptional divisor corresponds to the line $X' = 0$. The curve $\mathcal{C}$ is then properly parameterized on affine coordinates as follows:

$$\mathbb{A}^1_{\mathbb{C}} \xrightarrow{\phi} \mathbb{A}^2_{\mathbb{C}} : s_0 \mapsto \left(\frac{a(s_0,1)}{c(s_0,1)}, \frac{b(s_0,1)}{c(s_0,1)}\right).$$

We write

$$\begin{aligned} a(s,1) &= h(s)\tilde{a}(s), \\ b(s,1) &= h(s)\tilde{b}(s), \end{aligned}$$

with $\gcd(\tilde{a}, \tilde{b}) = 1$. Note that with the notation of Proposition 2.1, we have

$$h(s) = H_P(s,1) = \lambda^* \prod_{i=1}^{i_P}(t - t_i)^{\nu_i} \tag{12}$$

with λ^* a nonzero constant in $\mathbb{C}$. By (iv), we have $m = \sum_{i=1}^{i_P} \nu_i$, and by (v), $\tilde{\mathcal{C}}$ has degree $2n-\nu$ and is properly parameterized by

$$\mathbb{A}^1_{\mathbb{C}} \xrightarrow{\tilde{\phi}} \mathbb{A}^2_{\mathbb{C}} : s_0 \mapsto \left(\frac{a(s_0,1)}{c(s_0,1)}, \frac{\tilde{b}(s_0)}{\tilde{a}(s_0)}\right) = \left(\frac{a(s_0,1)\tilde{a}(s_0)}{\tilde{a}(s_0)c(s_0,1)}, \frac{c(s_0,1)\tilde{b}(s_0)}{\tilde{a}(s_0)c(s_0,1)}\right).$$

From here, it is not hard to see that a μ-basis associated to $\tilde{\phi}$ is given by

$$\begin{array}{rcl} \tilde{p} & = & \tilde{a}^h(s,v)x_2 - \tilde{b}^h(s,v)x_3, \\ \tilde{q} & = & c(s,v)x_1 - a(s,v)x_3, \end{array}$$

with $\tilde{a}^h$ and $\tilde{b}^h$ being the homogenizations of $\tilde{a}$ and $\tilde{b}$ respectively up to degree $n-\nu$.

Now, let $\tilde{M}$ be the R-module built from this μ-basis, i.e.

$$\tilde{M} := \operatorname{coker} \operatorname{Sylv}_{(s,v)} \Big(\tilde{a}^h(s,v)c(t,1)\tilde{b}(t) - \tilde{b}^h(s,v)\tilde{a}(t)c(t,1), \\ c(s,v)a(t,1)\tilde{a}(t) - a(s,v)\tilde{a}(t)c(t,1)\Big).$$

Recall from (12) that $H_P(s,v)$ is the homogenization of $h(s)$. As we have

$$\begin{aligned} \tilde{a}(t)^2\left(b(s,v)c(t,1) - c(s,v)b(t,1)\right) &= -\tilde{b}(t)\left(c(s,v)a(t,1)\tilde{a}(t) - a(s,v)\tilde{a}(t)c(t,1)\right) \\ &\quad + \tilde{a}(t)H_P(s,v)\left(\tilde{b}^h(s,v)c(t,1)\tilde{a}(t) - \tilde{a}^h(s,v)c(t,1)\tilde{b}(t)\right), \end{aligned}$$

we deduce, after setting $v=1$, that for any prime $\mathfrak{p}$ of $\mathbb{C}[t]$ such that $\tilde{a}(t) \notin \mathfrak{p}$, the multiplication by $b(s,1)c(t,1) - b(t,1)c(s,1)$ in the quotient ring

$$R_{\mathfrak{p}}[s]/\big(c(s,1)a(t,1)\tilde{a}(t) - a(s,1)\tilde{a}(t)c(t,1)\big) = R_{\mathfrak{p}}[s]/\big(c(s,1)a(t,1) - a(s,1)c(t,1)\big)$$

decomposes as the multiplication by $h(s)$ times the multiplication by

$$\Big(\tilde{b}(s)c(t,1)\tilde{a}(t) - \tilde{a}(s)c(t,1)\tilde{b}(t)\Big)$$

(notice that since $\tilde{a}(t) \notin \mathfrak{p}$, one can here cancel it out without changing the valuations of the above quantities). The leading coefficient of $a(s,1)c(t,1) - a(t,1)c(s,1)$ as a polynomial in s is equal to $a_n c(t,1)$ by (vi), and we have $c(t_i,1) \neq 0$ as otherwise we will have a singularity of $\mathcal{C}$ at $\{x_3 = 0\}$, a contradiction with (vii). So, we can use the following

Lemma 4.1 ([2, §3.3])**.** *Given a commutative ring A and two polynomials $f(X), g(X)$ in $A[X]$ such that the leading coefficient of f is a unit in A, then the cokernel of the Sylvester matrix of $f(X)$ and $g(X)$ is isomorphic, as an A-module, to the cokernel of the multiplication by $g(X)$ in the quotient ring $A[X]/(f(X))$.*

We deduce that for every prime $\mathfrak{p}_i = (t-t_i)$, the cokernel of the localized Sylvester matrix $\tilde{M}$ is isomorphic to the cokernel of the product of the matrices associated to the multiplication by $h(s)$ times the multiplication by $\Big(\tilde{b}(s)c(t,1)\tilde{a}(t) - \tilde{a}(s)c(t,1)\tilde{b}(t)\Big)$ in $R_{\mathfrak{p}_i}[s]/\big(c(s,1)a(t,1) - a(s,1)c(t,1)\big)$.

Lemma 4.2. *Let $\mathfrak{p}_i = (t-t_i)$ with $\phi(t_i:1)$ a singular point of $\mathcal{C}$. The invariant factors of the multiplication map by $h(s)$ in the quotient ring $R_{\mathfrak{p}_i}[s]/(a(s,1)c(t,1) - a(t,1)c(s,1))$ are*

$$\alpha_1 = 1, \ldots, \alpha_{n-m} = 1, \alpha_{n-m+1} = a(t,1), \alpha_{n-m_i+2} = a(t,1), \ldots, \alpha_n = a(t,1).$$

In particular, we have

$$\operatorname{val}_{t_i}(\alpha_k) = 0,\ 1 \leq k \leq n-m, \quad \operatorname{val}_{t_i}(\alpha_k) = \nu_i,\ n-m+1 \leq k \leq n.$$

Proof. As the leading coefficient of $a(s,1)c(t,1)-a(t,1)c(s,1)$ as a polynomial in s is invertible $R_{\mathfrak{p}_i}[t]$, then by using Lemma 4.1, it turns out that the cokernel of the multiplication map is actually isomorphic to the cokernel of the following Sylvester matrix:

$$\operatorname{coker}\operatorname{Sylv}_s\left(a(s,1)c(t,1)-a(t,1)c(s,1),h(s)\right)\otimes R_{\mathfrak{p}_i}[t] \\ \simeq \operatorname{coker}\operatorname{Sylv}_s\left(a(t,1)c(s,1),h(s)\right)\otimes R_{\mathfrak{p}_i}[t].$$

The matrix $\operatorname{Sylv}_s\left(a(t,1)c(s,1),h(s)\right)$ has $m=\deg(h)$ rows multiplied by $a(t,1)$, and also has maximal rank as $\operatorname{Res}_s(c(s,1),h(s))\neq 0$. This means that all the Fitting ideals of this matrix are not zero, and moreover from $i=n+1$ to $n+h$ they are multiples of $a(t,1)^{i-1}$. From here, the claim follows straightforwardly. □

Now we are ready for dealing with the inductive step and complete the proof of the main Theorem. As we already know that the singular factors of M are supported in the singularities of ϕ by Proposition 3.4, it is enough to prove the claim for localizations of the type $M_{\mathfrak{p}_0}$ with $\mathfrak{p}_0=(t-t_0)$, $\phi(t_0:1)$ being a singular point of $\mathcal{C}$.

Let us pick then $t_0\in\mathbb{C}$ with this property. As $c(t_0,1)\neq 0$ due to (vii) then, as we already used above, we have

$$\operatorname{coker}\operatorname{Sylv}_s(a(s,1)c(t,1)-c(s,1)a(t,1),b(s,1)c(t,1)-c(s,1)b(t,1))\otimes R_{\mathfrak{p}_0} \\ \simeq \operatorname{coker}\left(M_h\, M_{\tilde{b}(s)c(t,1)\tilde{a}(t)-\tilde{a}(s)c(t,1)\tilde{b}(t)}\right),$$

where M_* is a matrix of the multiplication map in $R_{\mathfrak{p}_0}[s]/(a(s,1)c(t,1)-c(s,1)a(t,1))$.

If $h(t_0)\neq 0$, then the character of $\phi(t_0:1)$ does not change before and after the blow up. In addition, M_h is an isomorphism and hence

$$\operatorname{coker}\left(M_h\, M_{\tilde{b}(s)c(t,1)\tilde{a}(t)-\tilde{a}(s)c(t,1)\tilde{b}(t)}\right)\simeq \operatorname{coker}\left(M_{\tilde{b}(s)c(t,1)\tilde{a}(t)-\tilde{a}(s)c(t,1)\tilde{b}(t)}\right) \\ \simeq \operatorname{coker}\left(\tilde{M}_{\mathfrak{p}_0}\right),$$

$\tilde{M}$ being the matrix of the syzygies of $\tilde{\phi}$. Here, we apply the inductive hypothesis and conclude.

Suppose now that $h(t_0)=0$. This means that $t_0\in\{t_1,\dots,t_{i_P}\}$. Suppose w.l.o.g. that $t_0=t_1$.

After localization, we denote the invariant factors of the matrix corresponding to the blow-up curve $\tilde{\mathcal{C}}$ with

$$\beta_1=1,\dots,\beta_{d-m}=1,\beta_{d-m+1}=\tilde{d}_m,\beta_{d-m+2}=\tilde{d}_m\tilde{d}_{m-1},\dots, \\ \beta_{d-1}=\tilde{d}_m\tilde{d}_{m-1}\dots\tilde{d}_2,\beta_d=0$$

and those of the matrix corresponding to $\mathcal{C}$ are set as

$$\gamma_1=1,\dots,\gamma_{d-m}=1,\gamma_{d-m+1}=d_m,\gamma_{d-m+2}=d_md_{m-1},\dots, \\ \gamma_{d-1}=d_md_{m-1}\dots d_2,\gamma_d=0$$

Applying Thompson's Theorem (Theorem 3.1), we deduce that, for all $1\leq i\leq m-1$

$$\alpha_1\dots\alpha_{d-m+1}\beta_1\dots\beta_{d-m}\beta_{d-m+i}\,|\,\gamma_1\dots\gamma_{d-m}\gamma_{d-m+i},$$

that is to say

$$(t-t_1)^{\nu_1}\tilde{d}_m\dots\tilde{d}_{m-i+1}\,|\,d_m\dots d_{m-i+1}$$

It follows that there exist non-negative integers $\epsilon_2,\dots,\epsilon_{m-1}$ such that, for all $i=1,\dots,m-1$, we have

$$\operatorname{val}_{t_1}(d_m\dots d_{m-i+1})=\nu_1+\epsilon_{m-i+1}+\operatorname{val}_{t_1}(\tilde{d}_m\dots\tilde{d}_{m-i+1})$$

Therefore, we deduce that

$$\mathrm{val}_{t_1}(d_m(t)^{m-1}d_{m-1}(t)^{m-2}\dots d_3(t)^2d_2(t)) = \sum_{i=1}^{m-1}\mathrm{val}_{t_1}(d_m\dots d_{m-i+1}) =$$

$$(m-1)\nu_1 + \sum_{i=2}^{m}\epsilon_i + \mathrm{val}_{t_1}(\tilde{d}_m(t)^{m-1}\tilde{d}_{m-1}(t)^{m-2}\dots\tilde{d}_3(t)^2\tilde{d}_2(t)).$$

By (11) we know that the left hand side of this equality is equal to

$$\sum_{k=2}^{m}\left((k-1)\sum_{m_i^1=k}\nu_i^1\right).$$

On the other hand, using our inductive hypothesis, the right hand side of this equality must be equal to

$$\sum_{k=2}^{m}\left((k-1)\sum_{m_i^1=k}\nu_i^1\right)+\sum_i\epsilon_{m-i+d}.$$

Comparing the two above quantities, we deduce that $\sum_i\epsilon_{m-i+d}=0$ and therefore that all $\epsilon_i=0$ for all $i=2,\dots,m$. It follows that $d_m(t)=(t-t_1)^{\nu_1}\tilde{d_m}(t)$ and that $d_i(t)=\tilde{d}_i(t)$ for all $i=2,\dots,m-1$. Therefore, we deduce that (H_N) holds.

5. Cokernels of resultant matrices

In this section, we show that the singular factors can be computed not only from the Sylvester matrix of the μ-basis, but from a collection of matrices of smaller matrix known as the hybrid Bézout matrices.

Let R be a commutative ring, $m,n\in\mathbb{N}$ with $n\geq m\geq 1$, and

$$\begin{array}{rcl} f(t) & = & a_0+a_1t+\ldots+a_nt^n,\\ g(t) & = & b_0+b_1t+\ldots+b_mt^m \end{array}$$

polynomials in $R[t]$.

For $k=0,\dots,m-1$, set

$$\begin{array}{rcl} f_k(t) & := & a_nt^{n-m+k}+a_{n-1}t^{n-m+k-1}+\ldots+a_{m-k},\\ g_k(t) & := & b_mt^k+b_{m-1}t^{k-1}+\ldots+b_{m-k}, \end{array}$$

and define

$$p_k(t) := g_k(t)f(t)-f_k(t)g(t).$$

Note that as

$$\begin{array}{rcl} f(t) & = & f_k(t)t^{m-k}+a_{m-k-1}t^{m-k-1}+\ldots+a_1t+a_0\\ \\ g(t) & = & g_k(t)t^{m-k}+b_{m-k-1}t^{m-k-1}+\ldots+b_1t+b_0, \end{array}$$

then it turns out that $\deg(p_k(t))\leq n-1\ \forall\, k=0,\dots m-1$.

For $j\in\{0,1,\dots,m\}$, we consider the following map of R-modules of finite rank:

$$\begin{array}{rcl} \psi_j : R^j\oplus R[t]_{\leq m-j-1}\oplus R[t]_{\leq n-j-1} & \to & R[t]_{\leq m+n-j-1}\\ \big(e_i,a(t),b(t)\big) & \mapsto & p_{m-j+i-1}(t)+a(t)f(t)+b(t)g(t) \end{array}$$

It is easy to see that ψ_0 is the Sylvester map of (f,g). We will call ψ_m the *hybrid Bézout* map of these polynomials, and its matrix in the monomial bases is what we have referred to as the *hybrid Bézout* matrix all along the text. If $n=m$, we just call them Bézout map and Bézout matrix respectively. For $1\leq j\leq m-1$, ψ_j it is also a *hybrid* type map in the sense that it has a piece of Sylvester type and a piece of Bézout.

In [2, Proposition 18] it is shown that if the leading coefficients of f and g generate R, then the cokernels of ψ_0 and ψ_m are isomorphic. The following result is a generalization of this fact.

Theorem 5.1. *Suppose that there exists a nonzero divisor $d \in R$, $d \neq 0$ such that $\langle a_n, b_m\rangle = \langle d\rangle$. Then the following sequence is exact*

$$R/\langle d\rangle \to \mathit{coker}(\psi_{j+1}) \to \mathit{coker}(\psi_j) \to R/\langle d\rangle \to 0 \ \forall j = 0, \dots m-1. \tag{13}$$

In particular, if $d = 1$ we then have $\mathit{coker}(\psi_j) \cong \mathit{coker}(\psi_k)$ for all j, k.

Remark 3. Note that as $d \neq 0$, then at least one between a_n and b_m must be different from zero.

Proof. Fix $j \in \{1, \dots m-1\}$ and consider the following commutative diagram of R-modules:

$$\begin{array}{ccc} & & 0 \\ & & \downarrow \\ R^{j+1} \oplus R[t]_{\leq m-j-2} \oplus R[t]_{\leq n-j-2} & \xrightarrow{\psi_{j+1}} & R[t]_{\leq m+n-j-2} \\ \downarrow \alpha & & \downarrow \mathbf{i} \\ R^{j} \oplus R[t]_{\leq m-j-1} \oplus R[t]_{\leq n-j-1} & \xrightarrow{\psi_{j}} & R[t]_{\leq m+n-j-1} \\ \downarrow & & \downarrow \\ \operatorname{coker}(\alpha) & \xrightarrow{\beta} & \operatorname{coker}(\mathbf{i}) \\ \downarrow & & \downarrow \\ 0 & & 0 \end{array} \tag{14}$$

where β is the induced morphism of cokernels, $\mathbf{i}$ the canonical injection, and α is defined as

$$\begin{array}{lcll} \alpha(0, a(t), b(t)) & = & (0, a(t), b(t)) & \\ \alpha(e_1, 0, 0) & = & (0, g_{m-j-1}(t), -f_{m-j-1}(t)) & \\ \alpha(e_{i+1}, 0, 0) & = & (e_i, 0, 0) & \text{for } i > 1. \end{array} \tag{15}$$

Clearly, we have $\operatorname{coker}(\mathbf{i}) \cong t^{m+n-j-1}\, R$. On the other hand, it is easy to see that

$$\operatorname{im}(\alpha) \cong R^j \oplus R[t]_{\leq m-j-2} \oplus R[t]_{\leq n-j-2} \oplus (b_m t^{m-j-1}, -a_n t^{n-j-1})R. \tag{16}$$

Let $u, v, w, z \in R$ such that $ua_n + vb_m = d$, $wd = a_n$, $zd = b_m$. As d is not a zero divisor in R, then we have $uw + vz = 1$, and hence we have an isomorphism

$$(t^{m-j-1}, 0)R \oplus (0, t^{n-j-1})R \cong (ut^{m-j-1}, vt^{n-j-1})R \oplus (zt^{m-j-1}, -wt^{n-j-1})R,$$

and from here, using (16), we then get

$$\operatorname{coker}(\alpha) \cong (ut^{m-j-1}, vt^{n-j-1})R \oplus \big(zt^{m-j-1}, -wt^{n-j-1}\big)R/\langle d\rangle.$$

With these identifications, it is straightforward to compute β explicitly:

$$\beta\left(r_1(ut^{m-j-1}, vt^{n-j-1}) + [r_2]\big(zt^{m-j-1}, -wt^{n-j-1}\big)\right) = dr_1 t^{m+n-j-1}$$

for $r_1 \in R$, $[r_2] \in R/\langle d\rangle$. We deduce, then

$$\begin{array}{rcl} \ker(\beta) & \cong & R/\langle d\rangle, \\ \operatorname{coker}(\beta) & \cong & R/\langle d\rangle. \end{array} \tag{17}$$

The claim now follows straightforwardly by applying the Snake Lemma to (14). □

The following lemma will imply that the cokernels of all the hybrid matrices of μ-bases are isomorphic and hence that the Fitting invariants of all type of resultant matrices are the same.

Lemma 5.2. *Let $p_\phi(s,1;t)$, $q_\phi(s,1;t) \in \mathbb{C}[s,t]$ be the specialization in $v=1$ of the polynomials defined in (4). If $\phi(1:0)$ is not a singular point on $\mathcal{C}$, then the leading coefficients of these two polynomials with respect to s are coprime in $\mathbb{C}[t]$.*

Proof. Note that the leading coefficients of $\sum_{i=1}^3 p_i(s,1)x_i$ and $\sum_{i=1}^3 q_i(s,1)x_i$ are two linear forms, say $L_p(x_1,x_2,x_3)$ and $L_q(x_1,x_2,x_3)$ in $\mathbb{C}[x_1,x_2,x_3]$ that are $\mathbb{C}$-linearly independent, otherwise by making a reversible linear combination of these elements, one could replace the μ-basis (p_ϕ, q_ϕ) with (p_ϕ, q'_ϕ) with $\deg(q'_\phi) < n-\mu$, a contradiction.

Now, it is easy to see that these two linear forms intersect at $\phi(1:0)$, and as they are linearly independent, this is their only point of intersection in $\mathbb{P}^2$. From here it follows that $L_p(a(t,1),b(t,1),c(t,1))$ and $L_q(a(t,1),b(t,1),c(t,1))$ are necessarily coprime in $\mathbb{C}[t]$, otherwise they will have a common factor $h(t)$ of positive degree, and we would have that

$$\phi(t_0:1) = \big(a(t_0,1) : b(t_0,1) : c(t_0:1)\big) = \phi(1:0)$$

for every t_0 such that $h(t_0)=0$, contradicting the fact that $\phi(1:0)$ is not a singularity of $\mathcal{C}$. □

Corollary 5.3. *The singular factors of all the matrices $\psi_j\big(p_\phi(s,v;t,u), q_\phi(s,v;t,u)\big)$ in $\mathbb{C}[t,u]$ are the same for any $j=0,\dots,m$, and for any $\{p,q\}$ μ-basis of ϕ.*

Proof. If $\phi(1:0)$ is not a singular point on $\mathcal{C}$, then the result follows from Theorem 5.1 and Lemma 5.2. If this is not the case, by applying a linear change of coordinates in $\mathbb{P}^1$, we may assume that $\phi(1:0)$ is not a singular point on $\mathcal{C}$ and the result then follows from Lemma 3.3 which holds not only for the Sylvester matrix ψ_0, but also for all the matrices ψ_j, $j=0,\dots,m$ (the same proof works verbatim). □

6. On the invariant factors of the D-resultant matrix

In this section, we will describe the invariant factors of a matrix closely related to $S_{p_\phi,q_\phi}(t,u)$ that was originally studied in [6] in order to compute the singularities of $\mathcal{C}$. As a consequence we obtain a complete factorization of the D-resultant for rational polynomials, introduced in [8].

Let $B(x_1,x_2,x_3) \in \mathbb{C}[x_1,x_2,x_3]^{n\times n}$ be the Bézout matrix associated to the polynomials $a(s,v)x_3 - c(s,v)x_1$ and $b(s,v)x_2 - c(s,v)x_3$ with respect to the homogeneous variables (s,v), and $S(x_1,x_2,x_3) \in \mathbb{C}[x_1,x_2,x_3]^{n\times n}$ be the Sylvester matrix associated to $p(s,v)=\sum_{i=1}^3 x_i p_i(s,v)$ and $q(s,v)=\sum_{i=1}^3 x_i q_i(s,1)$ with respect to (s,v). Here, as usual, $\{p,q\}$ is a μ-basis of (a,b,c).

Proposition 6.1. *There exists an invertible $N \in \mathbb{C}^{n\times n}$ such that*

$$B(x_1,x_2,x_3) = x_3\, N\, S(x_1,x_2,x_3). \tag{18}$$

Proof. Set $B = \big(B_{i,j}(x_1,x_2,x_3)\big)_{0\le i,j\le n-1}$. We then have

$$\begin{array}{rcl}\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} B_{i,j}(x_1,x_2,x_3)s^i t^j & = & \frac{1}{s-t}\big(\big(a(s,1)x_3 - c(s,1)x_1\big)\big(b(t,1)x_3 - c(t,1)x_2\big) \\ & & -\big(a(t,1)x_3 - c(t,1)x_1\big)\big(b(s,1)x_3 - c(s,1)x_2\big)\big).\end{array}$$

By setting $x_3=0$ above, it is easy to see that the right hand side vanishes, and hence we have $B_{i,j}(x_1,x_2,0)=0$ for all i,j. This shows that

$$B_{i,j}(x_1,x_2,x_3) = x_3 A_{i,j}(x_1,x_2,x_3)\ i,j=0,\dots,n-1$$

with $A_{i,j}(x_1,x_2,x_3)$ a homogeneous linear form. If now we substitute

$$x_1 \mapsto a(s,1),\ x_2 \mapsto b(s,1),\ x_3 \mapsto c(s,1)$$

we again have that the whole Bezoutian polynomial vanishes. So we conclude that

$$c(s,1)\sum_{i=0}^{n-1}\left(\sum_{j=0}^{n-1}A_{i,j}(a(s,1),b(s,1),c(s,1))s^i\right)t^j=0.$$

As $c(s,1)\neq 0$, this shows that for all $i=0,\dots,n-1$,

$$L_i(s,v;x_1,x_2,x_3):=\sum_{j=0}^{n-1}A_{i,j}(x_1,x_2,x_3)s^iv^{n-1-i}$$

is a syzygy of (a,b,c) of degree $n-1$. Moreover, the fact that $\det(B)\neq 0$ (as we have assumed $\gcd(a,b,c)=1$) shows then that $\det(A_{ij}(x_1,x_2,x_3))\neq 0$ and this implies that the family $\{L_0,\dots,L_{n-1}\}$ is a basis of the $\mathbb{C}$-vector space of syzygies of (a,b,c) of degree $n-1$.

On the other hand, it is easy to check that the family

$$\{v^{n-\mu-1}p, v^{n-\mu-2}sp,\dots,s^{n-\mu-1}p, v^{\mu-1}q, v^{\mu-2}sq,\dots,s^{\mu-1}q\}$$

is another basis of the same $\mathbb{C}$-vector space. This is due to the fact that the matrix of coefficients of this family with respect to the monomial basis is actually $S(x_1,x_2,x_3)$, whose determinant gives the implicit equation.

So, as both sets are bases of the same space, we then get that there exists an invertible $N\in\mathbb{C}^{n\times n}$ such that

$$\big(A_{i,j}(x,y,z)\big)=N\,S.$$

From here, the proof follows straightforwardly. □

As a direct application of Proposition 6.1 we get the explicit description of the invariant factors of the matrix $B_{F,G}(t,u)$ stated in the introduction. Denote with $D_i(B_{F,G})$ the gcd of the $(n-i)$-minors of $B_{F,G}(t,u)$.

Theorem 6.2. *$D_0(B_{F,G})=0$ and for $i=1,\dots,n-1$,*

$$D_i(B_{F,G})=c(t,u)^{n-i}\,d_n(t,u)^{n-i}d_{n-1}(t,u)^{n-i-1}\dots d_{i+1}(t,u).$$

Proof. Set $x_1\mapsto a(t,u)$, $x_2\mapsto b(t,u)$, $x_3\mapsto c(t,u)$ in (18) and compute the invariant factors on both sides. □

As an immediate consequence, we also get the following

Theorem 6.3 (Factorization of the D-resultant, case of same denominator)**.**

$$\tilde{\Delta}(t,u)=c(t,u)^{n-1}\,d_n(t,u)^{n-1}d_{n-1}(t,u)^{n-2}\dots d_2(t,u). \tag{19}$$

Proof. Recall that $\mathrm{Res}_{(s,v)}\left(\frac{F(s,v;t,u)}{su-tv},\frac{G(s,v;t,u)}{su-tv}\right)$ is equal to the first subresultant of the pair $F(s,v;t,u)$, $G(s,v;t,u)$. Set $i=1$ in Theorem 6.2 and use Proposition 3.4. □

Actually, the D-resultant in [8] was defined for an affine parameterization of the form $\left(\frac{A(t)}{C(t)},\frac{B(t)}{D(t)}\right)$ with $\gcd(A,C)=\gcd(B,D)=1$. In order to tackle this situation, set

$$n_1:=\max\{\deg(A),\deg(C)\},\ \ n_2:=\max\{\deg(B),\deg(D)\}.$$

Let $\tilde{A}(s,v)$, $\tilde{C}(s,v)$ (resp. $\tilde{B}(s,v)$, $\tilde{D}(s,v)$) be the homogenizations of A and C (resp. B and D) to degree n_1 (resp. n_2). The D-resultant of the curve given by

this parameterization is defined in [8] as

$$\tilde{\Delta}_{\tilde{A},\tilde{C},\tilde{B},\tilde{D}}(t,u) := \tag{20}$$
$$\mathrm{Res}_{(s,v)}\left(\frac{\tilde{A}(s,v)\tilde{C}(t,u)-\tilde{A}(t,u)\tilde{C}(s,v)}{su-tv}, \frac{\tilde{B}(s,v)\tilde{D}(t,u)-\tilde{B}(t,u)\tilde{D}(s,v)}{su-tv}\right).$$

Denote with $\tilde{\mathcal{C}} \subset \mathbb{P}^2$ the curve defined by the closure of the image of the parameterization given by $\big(\frac{A(t_0)}{C(t_0)}, \frac{B(t_0)}{D(t_0)}\big)$, with $t_0 \in \mathbb{C}$. We assume that this parameterization is proper, and hence $\tilde{\mathcal{C}}$ is birationally parametrized by

$$\begin{array}{rccc} \nu: & \mathbb{P}^1 & \to & \mathbb{P}^2 \\ & (s_0:v_0) & \mapsto & \big(\tilde{a}(s_0:v_0):\tilde{b}(s_0:v_0):\tilde{c}(s_0:v_0)\big), \end{array}$$

with $\tilde{c}(s,v)$ being the least common multiple of $\tilde{C}(s,v)$ and $\tilde{D}(s,v)$; $\tilde{a}(s,v) := \frac{\tilde{A}(s,v)\tilde{c}(s,v)}{\tilde{C}(s,v)}$ and $\tilde{b}(s,v) := \frac{\tilde{B}(s,v)\tilde{c}(s,v)}{\tilde{D}(s,v)}$. The polynomials $\tilde{a}$, $\tilde{b}$, $\tilde{c}$ have then the same degree $n \geq \max\{n_1,n_2\}$, and no common factors. Hence, the degree of $\tilde{\mathcal{C}}$ is then n and we have

$$\tilde{c}(t,u) = h(t,u)\tilde{C}(t,u) = q(t,u)\tilde{D}(t,u),$$

with $h(t,u)$ and $q(t,u)$ coprimes. We also get $\tilde{a}(t,u) = h(t,u)\tilde{A}(t,u)$ and $\tilde{b}(t,u) = q(t,u)\tilde{B}(t,u)$, and $\gcd(\tilde{a}(t,u),\tilde{b}(t,u),\tilde{c}(t,u)) = 1$.

We will denote with $\Delta_\nu(t,v)$ the polynomial defined in (7) associated with the parameterization ν. A complete factorization of this polynomial in terms of the singularities of $\tilde{\mathcal{C}}$ and its multiplicity graph is given in Corollary 3.5.

Finally, let $\delta(t,u) := \gcd(B(t,u),D(t,u))$. Note that we have

$$\tilde{C}(t,u) = q(t,u)\delta(t,u), \quad \tilde{D}(t,u) = h(t,u)\delta(t,u).$$

Theorem 6.4 (Factorization of the D-resultant, case of different denominators)**.** *If the parameterization defined by $\big(\frac{A(t)}{C(t)}, \frac{B(t)}{D(t)}\big)$ is proper, then with the notation established above, we have*

$$h(t,u)^{\deg(h)-1} q(t,u)^{\deg(q)-1} \tilde{\Delta}_{\tilde{A},\tilde{C},\tilde{B},\tilde{D}}(t,u) = \delta(t,u)^{\deg(\delta)-1}\Delta_\nu(t,u). \tag{21}$$

Remark 4. Note that (21) generalizes (19), as in the case of common denominators we have $h(t,u) = q(t,u) = 1$ and $\delta(t,u) = \tilde{c}(t,u)$.

Proof. We apply Theorem 6.3 to the parameterization given by $(\tilde{a}:\tilde{b}:\tilde{c})$ and have

$$\tilde{\Delta}_{\tilde{a},\tilde{b},\tilde{c}}(t,u) = \tilde{c}(t,u)^{n-1}\Delta_\nu(t,u), \tag{22}$$

where $\tilde{\Delta}_{\tilde{a},\tilde{b},\tilde{c}}(t,u) := \mathrm{Res}_{(s,v)}\left(\frac{\tilde{a}(s,v)\tilde{c}(t,u)-\tilde{a}(t,u)\tilde{c}(s,v)}{su-tv}, \frac{\tilde{b}(s,v)\tilde{c}(t,u)-\tilde{b}(t,u)\tilde{c}(s,v)}{su-tv}\right)$, which actually factorizes as

$$\begin{aligned} &\mathrm{Res}_{(s,v)}\left(h(s,v)h(t,u)\tfrac{\tilde{A}(s,v)\tilde{C}(t,u)-\tilde{A}(t,u)\tilde{C}(s,v)}{su-tv}, q(s,v)q(t,u)\tfrac{\tilde{B}(s,v)\tilde{D}(t,u)-\tilde{B}(t,u)\tilde{D}(s,v)}{su-tv}\right) \\ = \;& \lambda_0\, h(t,u)^{n-1}q(t,u)^{n-1}\mathrm{Res}_{(s,v)}\left(h(s,v), \tfrac{\tilde{B}(s,v)\tilde{D}(t,u)-\tilde{B}(t,u)\tilde{D}(s,v)}{su-tv}\right)\times \\ & \qquad \mathrm{Res}_{(s,v)}\left(\tfrac{\tilde{A}(s,v)\tilde{C}(t,u)-\tilde{A}(t,u)\tilde{C}(s,v)}{su-tv}, q(s,v)\right)\tilde{\Delta}_{\tilde{A},\tilde{C},\tilde{B},\tilde{D}}(t,u), \end{aligned}$$

with $\lambda_0 := \mathrm{Res}_{(s,v)}\big(h(s,v),q(s,v)\big) \neq 0$. As $\frac{\tilde{B}(s,v)h(t,u)\delta(t,u)-\tilde{B}(t,u)h(s,v)\delta(s,v)}{su-tv}$ can be written as

$$\delta(t,u)\tilde{B}(s,v)\frac{h(t,u)-h(s,v)}{su-tv} + h(s,v)\frac{\tilde{B}(s,v)\delta(t,u)-\tilde{B}(t,u)\delta(s,v)}{su-tv},$$

and using the fact that $D(t,u) = h(t,u)\delta(t,v)$ we get that

$$\mathrm{Res}_{(s,v)}\left(h(s,v), \frac{\tilde{B}(s,v)\tilde{D}(t,u) - \tilde{B}(t,u)\tilde{D}(s,v)}{su-tv}\right) = \mathrm{Res}_{(s,v)}\left(h(s,v), \delta(t,u)\tilde{B}(s,v)\frac{h(t,u)-h(s,v)}{su-tv}\right).$$

Note that $(\frac{\tilde{A}h}{\tilde{C}h}, \frac{\tilde{B}q}{\tilde{D}q})$ is the minimal expression that makes the denominators $\tilde{C}h = \tilde{D}q$, hence h must be coprime with $\tilde{B}$ otherwise the second fraction would simplify. So, we have $\mathrm{Res}_{(s,v)}(h(s,v), \tilde{B}(s,v)) = \lambda^* \neq 0$, and then

$$\mathrm{Res}_{(s,v)}\left(h(s,v), \frac{\tilde{B}(s,v)\tilde{D}(t,u) - \tilde{B}(t,u)\tilde{D}(s,v)}{su-tv}\right) = \lambda^*\delta(t,u)^{\deg(h)}\mathrm{Res}_{(s,v)}\left(h(s,v), \frac{h(t,u)-h(s,v)}{su-tv}\right).$$

By using the Poisson formula for the resultant, we have that -up to a nonzero constant-

$$\mathrm{Res}_{(s,v)}\left(h(s,v), \frac{h(t,u)-h(s,v)}{su-tv}\right) = \prod_{h(\xi_0:\xi_1)=0} \frac{h(t,u)}{\xi_0 u - \xi_1 t} = h(t,u)^{\deg(h)-1}.$$

So, we get

$$\mathrm{Res}_{(s,v)}\left(h(s,v), \frac{\tilde{B}(s,v)\tilde{D}(t,u) - \tilde{B}(t,u)\tilde{D}(s,v)}{su-tv}\right) = \lambda_1\,\delta(t,u)^{\deg(h)}h(t,u)^{\deg(h)-1},$$

with $\lambda_1 \in \mathbb{C}_{\neq 0}$.

The computation of $\mathrm{Res}_{(s,v)}\left(\frac{\tilde{A}(s,v)\tilde{C}(t,u)-\tilde{A}(t,u)\tilde{C}(s,v)}{su-tv}, q(s,v)\right)$ follows the same line: one has that -up to a nonzero constant- $\tilde{C}(t,u) = q(t,u)\delta(t,u)$ and then

$$\mathrm{Res}_{(s,v)}\left(\frac{\tilde{A}(s,v)\tilde{C}(t,u) - \tilde{A}(t,u)\tilde{C}(s,v)}{su-tv}, q(s,v)\right) = \lambda_2\,\delta(t,u)^{\deg(q)}q(t,u)^{\deg(q)-1},$$

for $\lambda_2 \neq 0$. Collecting all this information, we get

$$\tilde{\Delta}_{\tilde{a},\tilde{b},\tilde{c}}(t,u) = \lambda\;\tilde{c}(t,u)^{n-\deg(\delta)}h(t,u)^{n-\deg(q)-2}q(t,u)^{n-\deg(h)-2}\tilde{\Delta}_{\tilde{A},\tilde{C},\tilde{B},\tilde{D}}(t,u)$$

with $\lambda \neq 0$. And now we use (22) to get that -up to a constant-

$$\begin{aligned} h(t,u)^{n-\deg(q)-2}q(t,u)^{n-\deg(h)-2}\tilde{\Delta}_{\tilde{A},\tilde{C},\tilde{B},\tilde{D}}(t,u) &= \tilde{c}(t,u)^{\deg(\delta)-1}\Delta_\nu(t,u) \\ &= \big(h(t,u)q(t,u)\delta(t,u)\big)^{\deg(\delta)-1}\Delta_\nu(t,u). \end{aligned}$$

From here, we deduce

$$h(t,u)^{\deg(h)-1}q(t,u)^{\deg(q)-1}\tilde{\Delta}_{\tilde{A},\tilde{C},\tilde{B},\tilde{D}}(t,u) = \delta(t,u)^{\deg(\delta)-1}\Delta_\nu(t,u),$$

which is the claim we wanted to prove. □

References

[1] Shreeram S. Abhyankar. *Algebraic geometry for scientists and engineers*, volume 35 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1990.

[2] Francois Apéry, and Jean-Pierre Jouanolou. *Élimination: le cas d'une variable*. Collection Méthodes. Hermann Paris, 2006.

[3] Egbert Brieskorn, and Horst Knörrer. *Plane algebraic curves.* Translated from the German by John Stillwell. Birkhäuser Verlag, Basel, 1986.

[4] Laurent Busé. On the equations of the moving curve ideal of a rational algebraic plane curve. *J. Algebra*, 321(8):2317–2344, 2009.

[5] Falai Chen, Wenping Wang, and Yang Liu. Computing singular points of plane rational curves. *J. Symbolic Comput.*, 43(2):92–117, 2008.

[6] Eng-Wee Chionh and Thomas W. Sederberg. On the minors of the implicitization Bézout matrix for a rational plane curve. *Comput. Aided Geom. Design*, 18(1):21–36, 2001.

[7] M'Hammed El Kahoui. *D*-resultant and subresultants. *Proc. Amer. Math. Soc.*, 133(8):2193–2199 (electronic), 2005.

[8] Jaime Gutierrez, Rosario Rubio, and Jie-Tai Yu. *D*-resultant for rational functions. *Proc. Amer. Math. Soc.*, 130(8):2237–2246 (electronic), 2002.

[9] Xiaohong Jia, and Ron Goldman. Using Smith forms and μ-bases to compute all the singularities of rational planar curves. Preprint, 2009.
[10] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.
[11] Hyungju Park. Effective computation of singularities of parametric affine curves. *J. Pure Appl. Algebra*, 173(1):49–58, 2002.
[12] Sonia Pérez-Díaz. Computation of the singularities of parametric plane curves. *J. Symbolic Comput.*, 42(8):835–857, 2007.
[13] J. Rafael Sendra, and Franz Winkler. Symbolic parametrization of curves. *J. Symbolic Comput.* 12 (1991), no. 6, 607–631.
[14] J. Rafael Sendra, and Franz Winkler. Tracing index of rational curve parametrizations. *Comput. Aided Geom. Design* 18(8): 771–795, 2001.
[15] Ning Song, Falai Chen, and Ron Goldman. Axial moving lines and singularities of rational planar curves. *Comput. Aided Geom. Design*, 24(4):200–209, 2007.
[16] Peter Stadelmeyer. *On the computational complexity of resolving curve singularities and related problems.* PhD thesis, Research Institute for Symbolic Computation & Johannes Kepler Universität, Linz, Austria. 2000
[17] Robert C. Thompson. An inequality for invariant factors. *Proc. Amer. Math. Soc.*, 86(1):9–11, 1982.
[18] Robert J. Walker. *Algebraic Curves*. Princeton Mathematical Series, vol. 13. Princeton University Press, Princeton, N. J., 1950.

INRIA Sophia Antipolis - Méditerranée. 2004 route des Lucioles, B.P. 93 06902 Sophia Antipolis, France
E-mail address: Laurent.Buse@inria.fr
URL: http://www-sop.inria.fr/members/Laurent.Buse/

Departament d'Àlgebra i Geometria, Universitat de Barcelona. Gran Via 585, 08007 Barcelona, Spain
E-mail address: cdandrea@ub.edu
URL: http://atlas.mat.ub.es/personals/dandrea