Tracing Index of Rational Parametrizations*

J. Rafael Sendra
Dpto de Matemáticas
Universidad de Alcalá
E-28871 Madrid, Spain
Rafael.Sendra@uah.es

Franz Winkler
RISC-LINZ
Johannes Kepler Universität
A-4040 Linz, Austria
Franz.Winkler@risc.uni-linz.ac.at

Abstract

A rational parametrization of an algebraic curve establishes a rational equivalence of this curve with the affine or projective line, that is birational if the parametrization is proper. So, intuitively speaking, a rational parametrization determines a linear tracing of the curve. Such a parametrization might trace the curve once or several times. We formally introduce the concept of the tracing index of a parametrization, we show how to compute it, and we relate it to the degree of rational reparametrizations as well as to the degree of the curve.

1 Introduction

Plane algebraic curves can be uniquely represented, up to multiplication by constants, by their defining implicit equations. However rational curves, i.e. algebraic curves parametrizable by means of rational functions, may be expressed by infinitely many different such parametrizations. One may introduce different criteria of optimality in order to choose the best parametric representation. For instance, if one is interested in the coefficients of the rational functions, one may analyze the smallest possible field where the curve can be parametrized (see [2],[3],[9],[13],[17]). Another possibility is to optimize the degree of the rational functions involved in the parametrization. This leads to the notion of proper parametrization. Intuitively speaking, proper parametrizations are parametrizations tracing the curve once when giving values to the parameter. More rigorously speaking proper parametrizations correspond to bijective mappings from the field of parameter values onto the curve.

*First author partially supported by DGES PB98-0713-C02-01 and DGES HU1999-0029. Second author partially supported by the Austrian Science Fund (FWF) under Project SFB F1304, and by ÖAD Acc.Int. Proj.Nr. 19/2000.

Most parametrization algorithms provide proper parametrizations (see [1],[8],[16]). Furthermore, improperness can be detected algorithmically, and the given parametrization can be reparametrized into a proper one (see [14]). An alternative approach based on rational function decomposition can be found in [21]. Proper parametrizations play an important role in many practical applications in computer aided geometric design, such as in visualization (see [10],[11],[12]) or rational parametrization of offsets (see [4]). Also, they provide an implicitization approach based on resultants (see Theorem 7).

In this paper, we study the relation of improper parametrization to proper ones. As a consequence of this analysis, the intuitive statements on the tracing properties of a parametrization are formally established. For this purpose, we introduce the notion of tracing index of a parametrization of a plane algebraic curve. Essentially it is the cardinality of a generic fibre of the parametrization. Thus, intuitivelly speaking, it meassures the number of times that a parametrization traces a curve. The theorem on the dimension of fibres (see [18], pp.76) states that for almost all points on the curve the dimension of the fibre is zero. However, in order to formally define the concept of index, the cardinality of the fibres must be, in fact, invariant for all points in a non–empty Zariski open subset of the curve. This follows from the properties of the degree of a regular map between irreducible varieties of the same dimension (see [18], Section 6.3.). In fact, the cardinality of a generic fibre is the degree of the mapping (see [7], Proposition 7.16). However, the treatment given to this problem in classical algebraic geometry is not computational. In this paper, we give a computational approach that shows how to compute the degree of the mapping and that characterizes those points where the cardinality of the fibre equals the degree of the mapping (see Theorem 1); i.e. those points where the mapping is unramified. This result provides the theoretical requirements to introduce formally the notion of index, and shows that the tracing index really represents the number of times that the parametrization traces the curve. Furthermore, we give an algorithmic approach based on gcds to compute the index (see Theorem 2), that fits perfectly with Sederberg's criterion for properness (see Theorem 3).

Once the basic properties of the index have been established, we deal with the problem of analyzing the behaviour of the index under reparametrizations (Theorem 4), and we relate it to the degree of the curve. For this purpose, we first prove how the degree of a proper parametrization (i.e. the maximum degree w.r.t. the parameter of the rational function components of the parametrization) and the degree of the curve are related (see Theorem 5). This result is specially usefull in approaching the implicitization problem by means of interpolation techniques. Next, we show how the index of the parametrization, the degree of the parametrization and the degree of the curve are related (see Theorem 6). In the last part of the paper, we relate the problem of implicitizing rational parametrizations with the tracing index, proving that the resultant w.r.t. the parameter of the polynomials obtained by clearing the denominators in the parametrization is the defining polynomial of the curve to the power of the index (see Theorems 7 and 8).

In this paper, we only deal with the tracing index for rational plane parametrizations. Nevertheless the notion of tracing index, as well as most of the results presented here, can be easily generalized to space curve parametrizations. For this purpose, one just has to introduce the tracing index as the degree of the rational mapping defined by the parametrization. Furthermore, taking into account that every space curve is birationally equivalent to a plane curve (see e.g. [20] Theorem 6.5.), the tracing index of an space parametrization is directly related to the tracing index of a plane parametrization.

In the sequel, we use the following **notation**. $\mathbb{K}$ is an algebraically closed field of characteristic zero. If $\mathcal{C}$ is an algebraic curve over $\mathbb{K}$, we denote the field of rational functions over $\mathcal{C}$ by $\mathbb{K}(\mathcal{C})$. For a parametrization $\mathcal{P}(t)$ of a curve $\mathcal{C}$ over $\mathbb{K}$ we write its components as

$$\mathcal{P}(t) = \left(\frac{\chi_1(t)}{\chi_{3,1}(t)}, \frac{\chi_2(t)}{\chi_{3,2}(t)} \right).$$

Furthermore, for given parametrization $\mathcal{P}(t)$ we consider the polynomials

$$G_1(s,t) = \chi_1(s)\chi_{3,1}(t) - \chi_{3,1}(s)\chi_1(t), \;\; G_2(s,t) = \chi_2(s)\chi_{3,2}(t) - \chi_{3,2}(s)\chi_2(t).$$

as well as the polynomials

$$H_1(t,x) = x\chi_{3,1}(t) - \chi_1(t), \;\; H_2(t,y) = y\chi_{3,2}(t) - \chi_2(t).$$

2 Proper Parametrizations

We start recalling some basic results on proper parametrizations. Let $\mathbb{K}$ be an algebraically closed field of characteristic zero, and $\mathcal{C}$ be a rational plane algebraic curve over $\mathbb{K}$. Then, a parametrization $\mathcal{P}(t)$ of $\mathcal{C}$ is *proper* if and only if the map

$$\begin{array}{rccc} \mathcal{P}: & \mathbb{K} & \longrightarrow & \mathcal{C} \\ & t & \longmapsto & \mathcal{P}(t) \end{array}$$

is birational, or equivalently, if for almost every point on $\mathcal{C}$ and for almost all values of the parameter in $\mathbb{K}$ the mapping $\mathcal{P}$ is rationally bijective.

The notion of properness can also be stated algebraically in terms of fields of rational functions. In fact, a rational parametrization $\mathcal{P}(t)$ is proper if and only if the induced monomorphism $\varphi_{\mathcal{P}}$ on the fields of rational functions

$$\begin{array}{rccc} \varphi_{\mathcal{P}}: & \mathbb{K}(\mathcal{C}) & \longrightarrow & \mathbb{K}(t) \\ & R(x,y) & \longmapsto & R(\mathcal{P}(t)). \end{array}$$

is an isomorphism. Therefore, $\mathcal{P}(t)$ is proper if and only if the mapping $\varphi_{\mathcal{P}}$ is surjective, that is, if and only if $\varphi_{\mathcal{P}}(\mathbb{K}(\mathcal{C})) = \mathbb{K}(\mathcal{P}(t)) = \mathbb{K}(t)$. Thus, Lüroth's Theorem implies that any rational curve over $\mathbb{K}$ can be properly parametrized. Most of the parametrization algorithms always output proper parametrizations (see [1],[8],[16]). Furthermore, given an improper parametrization, in [14] it is shown how to compute a new parametrizatrion of the same curve being proper.

An important fact on proper parametrizations is that any other rational parametrization of the same curve can be obtained from a proper one by a rational change of parameter. More precisely, the following lemma holds.

Lemma 1. *Let $\mathcal{P}(t)$ be a proper parametrization of a plane curve $\mathcal{C}$, and let $\mathcal{Q}(t)$ be any other rational parametrization of $\mathcal{C}$. Then, it holds that:*

(1) There exists a non–constant rational function $R(t) \in \mathbb{K}(t)$ such that $\mathcal{Q}(t) = \mathcal{P}(R(t))$.

(2) $\mathcal{Q}(t)$ is proper if and only if there exists a linear rational function $L(t) \in \mathbb{K}(t)$ such that $\mathcal{Q}(t) = \mathcal{P}(L(t))$.

Proof: (1) Since $\mathcal{P}$ is a birational mapping, it is clear that $R(t) = \mathcal{P}^{-1}(\mathcal{Q}(t)) \in \mathbb{K}(t)$, and that $\mathcal{Q}(t) = \mathcal{P}(R(t))$.
(2) If $\mathcal{Q}(t)$ is proper, one has that $L(t) = \mathcal{P}^{-1}(\mathcal{Q}(t))$ is a birational mapping from $\mathbb{K}$ onto $\mathbb{K}$. Hence, $L(t)$ induces an automorphism $L = \mathcal{P}^{-1} \circ \mathcal{Q}$ of $\mathbb{K}(t)$ defined as:

$$\begin{array}{rccc} L: & \mathbb{K}(t) & \longrightarrow & \mathbb{K}(t) \\ & t & \longmapsto & \varphi(t). \end{array}$$

Therefore, since $\mathbb{K}$-automorphisms of $\mathbb{K}(t)$ are the invertible rational functions (see e.g. [19]), one has that $L(t)$ is a linear rational function, and clearly $\mathcal{Q}(t) = \mathcal{P}(L(t))$.

Conversely, let L is the birational mapping from $\mathbb{K}$ onto $\mathbb{K}$ defined by the linear rational function $L(t) \in \mathbb{K}(t)$. Then, $\mathcal{Q} = \mathcal{P} \circ L : \mathbb{K} \to \mathcal{C}$ is a birational mapping, and therefore $\mathcal{Q}(t)$ is proper. □

3 Tracing Index

In this section, we introduce the notion of tracing index of a parametrization of a plane algebraic curve and we show how to determine it. For this purpose, we first prove the following technical lemma.

Lemma 2. *Let $p(x), q(x) \in \mathbb{K}[x]^\star$ be relatively prime such that at least one of them is non-constant, and let $E = \{(a, b) \in \mathbb{K}^2 \mid p(a) - bq(a) = 0,\ p'(a) - bq'(a) = 0\}$. Then,* $\mathrm{Card}(E) < \infty$*, and $p(x) - bq(x)$ has multiple roots if and only if b is the y–coordinate of a point in E.*

Proof: Let us consider the polynomials $f(x,y) = p(x) - yq(x), g(x,y) = p'(x) - yq'(x)$. Clearly, $p(x) - bq(x)$ has multiple roots if and only if b is a root of the discriminant of f w.r.t. y. That is, if and only if b is the y–coordinate of a point in E. Since $\gcd(p,q) = 1$ and p, q are non-zero, one has that f is irreducible. Furthermore, g is non-zero, since at least one of the two polynomials p and q is non-constant. If g is a constant it follows that E is the empty set. Moreover, if g is not constant, since f is irreducible and $\deg(g) \leq \deg(f)$, applying Bézout's Theorem one concludes that the curves defined over $\mathbb{K}$ by f and g have finitely many intersection points. Hence $\mathrm{Card}(E) < \infty$. □

Corollary. *Let $p(x), q(x) \in \mathbb{K}[x]^\star$ be relatively prime such that at least one of them is non-constant, and let $R(y)$ be the resultant*

$$R(y) = Res_x(p(x) - yq(x), p'(x) - yq'(x)).$$

Then, for all $b \in \mathbb{K}$ such that $R(b) \neq 0$, the polynomial $p(x) - bq(x)$ is squarefree.

Remark. If $\deg(p) > \deg(q)$ then the roots of the resultant are exactly the values of b for which $p(x) - bq(x)$ has multiple roots. However, if $\deg(p) \leq \deg(q)$ the leading coefficients, w.r.t. x, of the polynomials involved in the resultant have a common root, and this root may generate extraneous factors in the resultant. For instance, take $p(x) = x^2, q(x) = 2x^2 + 1$. Then $R(y) = -4y(2y-1)^2$, but $p(x) - 1/2q(x) = -1/2$.

Theorem 1. *Let $\mathcal{P}(t)$ be a parametrization with non-constant components in reduced form (i.e. $\gcd(\chi_1, \chi_{3,1}) = \gcd(\chi_2, \chi_{3,2}) = 1$). Then, for $\alpha \in \mathbb{K}$ such that $\chi_{3,1}(\alpha)\chi_{3,2}(\alpha) \neq 0$, and such that $G_1(\alpha,t)$, $G_2(\alpha,t)$ do not have multiple roots, it holds that*

$$\mathrm{Card}(\mathcal{P}^{-1}(\mathcal{P}(\alpha))) = \deg_t(\gcd(G_1(\alpha,t), G_2(\alpha,t))).$$

Proof: Let S be the set of all $\alpha \in \mathbb{K}$ such that $P_\alpha = \mathcal{P}(\alpha)$ is defined, and such that $G_1(\alpha,t)$ and $G_2(\alpha,t)$ do not have multiple roots. First, we see that S is an infinite set. Indeed: $\mathcal{P}(t)$ is not defined only for the common roots of the denominators. Furthermore, if α is such that $\chi_{3,1}(\alpha)\chi_{3,2}(\alpha) \neq 0$, and $G_1(\alpha,t)$ has multiple roots, then the polynomial $\chi_1(t) - \frac{\chi_1(\alpha)}{\chi_{3,1}(\alpha)}\chi_{3,1}(t)$ also has multiple roots. But, by Lemma 2, this can only happen for finitely many values of α (note that $\chi_1, \chi_{3,1}$ are non-zero relatively prime polynomials). Similarly for $G_2(\alpha,t)$. Therefore, S is infinite.

Now, observe that every element of the fibre $\mathcal{P}^{-1}(P_\alpha)$ is a common root of $G_1(\alpha,t)$ and $G_2(\alpha,t)$. On the other hand, let β be a root of $\gcd(G_1(\alpha,t), G_2(\alpha,t))$. Note that $\gcd(G_1(\alpha,t), G_2(\alpha,t))$ is defined since no component of $\mathcal{P}$ is constant, and therefore none of the polynomials $G_i(\alpha,t)$ is zero. So $\chi_{3,1}(\beta) \neq 0$, since otherwise it would imply that $\chi_{3,1}(\alpha)\chi_1(\beta) = 0$, but $\chi_{3,1}(\alpha) \neq 0$ and hence $\chi_1(\beta) = 0$, which is impossible because $\gcd(\chi_1, \chi_{3,1}) = 1$. Similarly, $\chi_{3,2}(\beta) \neq 0$. Thus, $\beta \in \mathcal{P}^{-1}(P_\alpha)$. Therefore, since $G_1(\alpha,t)$ and $G_2(\alpha,t)$ do not have multiple roots, the cardinality of the fibre is the degree of the gcd. □

Corollary. *Let $\mathcal{P}(t)$ be a parametrization and let*

$$R_1(s) = Res_t(G_1, \frac{\partial G_1}{\partial t}), \;\; R_2(s) = Res_t(G_2, \frac{\partial G_2}{\partial t})$$

Then, for $\alpha \in \mathbb{K}$ such that $\chi_{3,1}(\alpha)\chi_{3,2}(\alpha)R_1(\alpha)R_2(\alpha) \neq 0$, it holds that

$$\mathrm{Card}(\mathcal{P}^{-1}(\mathcal{P}(\alpha))) = \deg_t(\gcd(G_1(\alpha,t), G_2(\alpha,t))).$$

Theorem 1 implies that a point $(x_\alpha, y_\alpha) = \mathcal{P}(\alpha) \in \mathcal{C}$ is generated more than once if and only if $\deg_t(\gcd(G_1(\alpha,t), G_2(\alpha,t))) > 1$. In Lemma 4 we will see that the degree of this gcd is preserved under almost all specializations of the variable s. First we state the following result on gcds. Let φ_a denote the natural evaluation homomorphism of $\mathbb{K}[x,y]$ into $\mathbb{K}[y]$, i.e. for $a \in \mathbb{K}$,

$$\begin{array}{rccc} \varphi_a : & \mathbb{K}[x,y] & \rightarrow & \mathbb{K}[y] \\ & f(x,y) & \mapsto & f(a,y). \end{array}$$

Lemma 3. *Let $f, g \in \mathbb{K}[x,y]^*$, $f = \bar{f} \cdot \gcd(f,g)$, $g = \bar{g} \cdot \gcd(f,g)$. Let $a \in \mathbb{K}$ be such that not both leading coefficients of f and g vanish at a.*

(1) $\deg_y(\gcd(\varphi_a(f), \varphi_a(g))) \geq \deg_y(\gcd(f,g))$

(2) If the resultant w.r.t. y of $\bar{f}$ and $\bar{g}$ does not vanish at a, then

$$\varphi_a(\gcd(f,g)) = \gcd(\varphi_a(f), \varphi_a(g)).$$

Proof: Let $h = gcd(f,g)$. Since not both leading coefficients (w.r.t. y) of f and g vanish under φ_a, also the leading coefficient of h cannot vanish under φ_a. So $\deg(\varphi_a(h)) = \deg_y(h)$. Furthermore, $\varphi_a(f) = \varphi_a(\bar{f})\varphi_a(h)$ and $\varphi_a(g) = \varphi_a(\bar{g})\varphi_a(h)$.
(1) $\varphi_a(h)$ divides $gcd(\varphi_a(f), \varphi_a(g))$, so

$$\deg(\gcd(\varphi_a(f), \varphi_a(g))) \geq \deg(\varphi_a(\gcd(f,g))) = \deg_y(\gcd(f,g)).$$

(2) We have

$$\gcd(\varphi_a(f), \varphi_a(g)) = \gcd(\varphi_a(\bar{f}), \varphi_a(\bar{g})) \cdot \varphi_a(h).$$

If $\gcd(\varphi_a(f), \varphi_a(g)) \neq \varphi_a(h)$, then $\gcd(\varphi_a(\bar{f}), \varphi_a(\bar{g})) \neq 1$. Hence, the resultant w.r.t. y of $\varphi_a(\bar{f}), \varphi_a(\bar{g})$ is zero. Therefore, since φ_a is a ring homomorphism one obtains that

$$0 = Res_y(\varphi_a(\bar{f}), \varphi_a(\bar{g})) = \varphi_a(Res_y(\bar{f}, \bar{g})).$$

This, however, is excluded by the assumptions. □

Lemma 4. *Let $\mathcal{P}(t)$ be a rational parametrization in reduced form with non–constant components. Then for all but finitely many values α of s we have*

$$\deg_t(\gcd(G_1(s,t), G_2(s,t))) = \deg_t(\gcd(G_1(\alpha,t), G_2(\alpha,t))).$$

Proof: Since no component of $\mathcal{P}(t)$ is constant, one has that $G_1(s,t)$ and $G_2(s,t)$ are non-zero. Thus, if $H = \gcd(G_1, G_2)$ and $G_1 = \bar{G}_1 \cdot H, G_2 = \bar{G}_2 \cdot H$, it holds that $T(s) = Res_t(\bar{G}_1, \bar{G}_2) \in \mathbb{K}[s]$ is not identically zero. Therefore, $T(s)$ and the leading coefficients of G_1 and G_2, w.r.t. t, can only vanish at finitely many values. Thus, by Lemma 3(2), for almost all $\alpha \in \mathbb{K}$, $\varphi_\alpha(\gcd(G_1, G_2)) = \gcd(\varphi_\alpha(G_1), \varphi_\alpha(G_2))$. In particular, for almost all $\alpha \in \mathbb{K}$,

$$\deg_t(\gcd(\varphi_\alpha(G_1), \varphi_\alpha(G_2))) = \deg_t(\varphi_\alpha(\gcd(G_1, G_2))) \leq \deg_t(\gcd(G_1, G_2)).$$

On the other hand, by Lemma 3(1), for almost all $\alpha \in \mathbb{K}$,

$$\deg_t(\gcd(\varphi_\alpha(G_1), \varphi_\alpha(G_2))) \geq \deg_t(\gcd(G_1, G_2)).$$

Thus, for almost all $\alpha \in \mathbb{K}$,

$$\deg_t(\gcd(\varphi_\alpha(G_1), \varphi_\alpha(G_2))) = \deg_t(\gcd(G_1, G_2)).$$

□

Theorem 2. *Let $\mathcal{P}(t)$ be a parametrization in reduced form of a plane curve $\mathcal{C}$. Then all but finitely many points in $\mathcal{C}$ are generated, via $\mathcal{P}(t)$, by exactly m parameter values, where $m = \deg_t(\gcd(G_1(s,t), G_2(s,t))$.*

Proof: If $\mathcal{P}(t)$ does not have constant components, the result follows from Theorem 1 and Lemma 4.
Now assume that $\mathcal{P}(t)$ has a constant component. W.l.o.g. let the first component be constant. Then $\gcd(G_1(s,t), G_2(s,t)) = G_2(s,t)$. Now consider the set Ω of all points $a \in \mathbb{K}$ such that $\mathcal{P}(a)$ is defined, $G_2(a,t)$ is squarefree and $\deg_t(G_2(s,t)) = \deg_t(G_2(a,t))$. Note that since the denominators in $\mathcal{P}$ as well as the leading coefficient w.r.t. t of G_1 are univariate polynomials. Applying Lemma 2, one deduces that Ω is a non-empty open subset of $\mathbb{K}$. Moreover, $\mathcal{C} \setminus \mathcal{P}(\Omega)$ is finite, and for all points in $\mathcal{C} \setminus \mathcal{P}(\Omega)$ the theorem holds. □

With these preparations we can now introduce the notion of tracing index of a parametrization.

Definition. Let $\mathcal{C}$ be a rational affine plane curve, and let $\mathcal{P}(t)$ be a rational parametrization of $\mathcal{C}$. Then, we say that $k \in \mathbb{N}$ is the *tracing index* of $\mathcal{P}(t)$, and we denote it by $\text{index}(\mathcal{P}(t))$, if all but finitely many points on $\mathcal{C}$ are generated, via $\mathcal{P}(t)$, by k parameter values; i.e. $\text{index}(\mathcal{P}(t))$ represents the number of times that $\mathcal{P}(t)$ traces $\mathcal{C}$. □

Remark.

(1) Note that by Theorem 2

$$\text{index}(\mathcal{P}(t)) = \deg_t(\gcd(G_1(s,t), G_2(s,t)).$$

Also, the tracing index can be computed by the corollary to Theorem 1.

(2) If we consider the map $\mathcal{P} : \mathbb{K} \to \mathcal{C}$ induced by the parametrization $\mathcal{P}(t)$, it holds that the tracing index of the parametrization $\mathcal{P}(t)$ is the degree of the rational map $\mathcal{P}$. Therefore, index$(\mathcal{P}(t))$ is the degree of the finite field extension $\varphi_{\mathcal{P}}(\mathbb{K}(\mathcal{C})) \subset \mathbb{K}(t)$, where $\varphi_{\mathcal{P}}$ is the monomorphism induced by $\mathcal{P}$ on the fields of rational functions (see [7],[18]); that is

$$\text{index}(\mathcal{P}(t)) = [\mathbb{K}(t) : \varphi_{\mathcal{P}}(\mathbb{K}(\mathcal{C}))].$$

Since properness of a parametrization $\mathcal{P}$ is defined by requiring $\mathcal{P}$ to be a birationality, properness is characterized by a tracing index 1.

Theorem 3. *A rational parametrization is proper if and only if its tracing index is 1; i.e. if and only if* $\deg_t(\gcd(G_1, G_2)) = 1$.

4 Tracing Index and Curve Degree

In this section we analyze how the tracing index of a parametrization behavies under reparametrizations and how it is related to the degree of the curve. For this purpose, we use the notion of degree of a rational parametrization $\mathcal{P}(t)$, that it is defined as

$$\deg(\mathcal{P}(t)) = \max\left\{\deg_t\left(\frac{\chi_1(t)}{\chi_{3,1}(t)}\right), \deg_t\left(\frac{\chi_2(t)}{\chi_{3,2}(t)}\right)\right\}.$$

Note that the degree, $\deg(\mathcal{P}(t))$, of $\mathcal{P}(t)$ is in general different to the degree, index$(\mathcal{P}(t))$, of the rational mapping $\mathcal{P}$ induced by $\mathcal{P}(t)$ (see Theorem 6). For instance, any rational proper parametrization of a circle has degree 2 but its index is 1 because it is proper. In the sequel, in order to avoid possible ambiguities, we will use the notation $\deg(\mathcal{P}(t))$ for the degree w.r.t. the parameter, and index$(\mathcal{P}(t))$ for the degree as rational map.

In order to study the behaviour of the index under reparametrizations we first prove a technical lemma where we show that, in the case of a single non-constant rational function $R(t)$, the degree w.r.t. t of $R(t)$ is the degree of the rational map, from $\mathbb{K}$ on $\mathbb{K}$, that $R(t)$ defines.

Lemma 5. *Let $R(t) \in \mathbb{K}(t)$ be a non-constant rational function, and let $R : \mathbb{K} \to \mathbb{K}$ be the rational map induced by $R(t)$. Then, for allmost all $a \in \mathbb{K}$ it holds that* $\text{Card}(R^{-1}(a)) = \deg_t(R(t))$; *i.e. the degree of the rational map R is $deg_t(R(t))$.*

Proof: Let $R(t) = p(t)/q(t)$ be in reduced form. Let W_0 be the non–empty open subset of $\mathbb{K}$ where R is defined, and let V_0 be the subset of points $a \in \mathbb{K}$ such that $p(t) - aq(t)$ is square-free, and such that $\deg(p(t) - aq(t)) = \deg(R(t))$. Note that from Lemma 2 one has that V_0 is open and non–empty. Furthermore, since R is non-constant, one has that $R(W_0)$ is also a non–empty open set. We consider the set $U = V_0 \cap R(W_0)$. Since $\mathbb{K}$ is irreducible, one has that $V_0 \cap R(W_0)$ is a non–empty open set. Let us see that for all $a \in U$ it holds that $\mathrm{Card}(R^{-1}(a)) = \deg(R(t))$. Indeed: take $a \in U$, since $a \in R(W_0)$ one has that $R^{-1}(a)$ is non–empty. Moreover, since $a \in V_0$, it holds that $p(t) - aq(t)$ is square-free, and that $\deg(p(t) - aq(t)) = \deg(R(t))$. Therefore, $\mathrm{Card}(R^{-1}(a)) = \deg(R(t))$ □

Theorem 4. *Let $\mathcal{P}(t)$ be a rational parametrization, and $R(t) \in \mathbb{K}(t) \setminus \mathbb{K}$, then*

$$\mathrm{index}(\mathcal{P}(R(t))) = \deg_t(R(t)) \cdot \mathrm{index}(\mathcal{P}(t)).$$

Proof: Let $\mathcal{Q}(t) = \mathcal{P}(R(t))$, then in terms of mappings we have:

$$\mathcal{Q} : \mathbb{K} \xrightarrow{R} \mathbb{K} \xrightarrow{\mathcal{P}} \mathcal{C}.$$

Taking into account that $\mathrm{index}(\mathcal{Q}(t)) = [\mathbb{K}(t) : \varphi_{\mathcal{Q}}(\mathbb{K}(\mathcal{C}))]$, where $\varphi_{\mathcal{Q}}$ is the monomorphism induced by $\mathcal{Q}$ on the fields of rational functions, and using that the degree of finite field extensions is multiplicative (see e.g. [19]), one has that the degree of a composition of maps is the product of the degrees. Thus, applying Lemma 5, one concludes that $\mathrm{index}(\mathcal{Q}(t)) = \deg_t(R(t)) \cdot \mathrm{index}(\mathcal{P}(t))$. □

In Theorem 5, we prove how the degree of a proper parametrization and the degree of the curve are related.

Theorem 5. *Let $\mathcal{C}$ be a rational affine curve defined over $\mathbb{K}$ by the polynomial $f(x, y) \in \mathbb{K}[x, y]$, and let $\mathcal{P}(t)$ be a rational parametrization of $\mathcal{C}$. Then it holds that $\mathcal{P}(t)$ is proper if and only if*

$$\deg(\mathcal{P}(t)) = \max\{\deg_x(f), \deg_y(f)\}.$$

Furthermore, if $\mathcal{P}(t)$ is proper, then $\deg(\frac{\chi_1}{\chi_{3,1}}) = \deg_y(f)$, and $\deg(\frac{\chi_2}{\chi_{3,2}}) = \deg_x(f)$.

Proof: We first prove the result for the special case of parametrizations having a constant component; i.e. for lines. Afterwards, we consider the general case. Let $\mathcal{P}(t)$ be a parametrization such that one of its two components is constant, say $\mathcal{P}(t) = (\chi_1(t), \lambda)$ where $\lambda \in \mathbb{K}$. Then the curve $\mathcal{C}$ is the line of equation $y = \lambda$. Hence, (t, λ) is a proper parametrization of $\mathcal{C}$. So, by Lemma 1(1) every proper parametrization of $\mathcal{C}$ is of the form $(\frac{at+b}{ct+d}, \lambda)$, where $a, b, c, d, \in \mathbb{K}$ and $ad - bc \neq 0$. Therefore, $\deg(\chi_1) = 1$, and the theorem clearly holds.

In order to prove the general case, let $\mathcal{P}(t)$ be proper, in reduced form, and such that none of its components is constant. Then we prove that $\max\{\deg(\chi_2), \deg(\chi_{3,2})\} = \deg_x(f)$, and analogously one can prove that $\max\{\deg(\chi_1), \deg(\chi_{3,1})\} = \deg_y(f)$. ¿From these relations, we inmediately get that $\deg(\mathcal{P}(t)) = \max\{\deg_x(f), \deg_y(f)\}$. For this purpose, we define $\mathcal{S}$ as the subset of $\mathbb{K}$ containing:

(a) all the second coordinates of those points on $\mathcal{C}$ that are not generated by $\mathcal{P}(t)$,

(b) those $b \in \mathbb{K}$ such that the polynomial $\chi_2(t) - b\chi_{3,2}(t)$ has multiple roots,

(c) $lc(\chi_2)/lc(\chi_{3,2})$, where " lc" denotes the leading coefficient,

(d) those $b \in \mathbb{K}$ such that the polynomial $f(x, b)$ has multiple roots,

(e) the roots of the leading coefficient, with respect to x, of $f(x, y)$.

$\mathcal{S}$ is finite. Indeed: $\mathcal{P}(t)$ is a parametrization, so only finitely many points on the curve are not generated by $\mathcal{P}(t)$, and therefore only finitely many field elements satisfy (a). According to Lemma 2 there are only finitely many field elements satisfying (b). The argument for (c) is trivial. An element $b \in \mathbb{K}$ satisfies (d) iff b is the second coordinate of a singular point of $\mathcal{C}$ or the line $y = b$ is tangent to the curve at some simple point. Since $\mathcal{C}$ is irreducible, it has only finitely many singular points. Moreover, $y = b$ is tangent to $\mathcal{C}$ at some point (a, b) if (a, b) is a solution of the system $\{f = 0, \frac{\partial f}{\partial x} = 0\}$. However, by Bézout's Theorem, this system has only finitely many solutions; note that f is not a line. So only finitely many field elements satisfy (d). Since the leading coefficient, with respect to x, of $f(x, y)$ is a non-zero univariate polynomial (note that, since $\mathcal{C}$ is not a line, f is a non-linear irreducible bivariate polynomial), only finitely many field elements satisfy (e). Therefore, $\mathcal{S}$ is finite.

Now we take an element $b \in \mathbb{K} \setminus \mathcal{S}$ and we consider the intersection of $\mathcal{C}$ and the line of equation $y = b$. Since $b \notin \mathcal{S}$, by (e), one has that the degree of $f(x, b)$ is exactly $\deg_x(f(x, y))$, say $m := \deg_x(f(x, y))$. Furthermore, by (d), $f(x, b)$ has m different roots, say $\{r_1, \ldots, r_m\}$. So, there are m different points on $\mathcal{C}$ having b as a second coordinate (i.e. $\{(r_i, b)\}_{i=1,\ldots,m}$), and they can be generated by $\mathcal{P}(t)$, becasuse of (a).

On the other hand, we consider the polynomial $M(t) = \chi_2(t) - b\chi_{3,2}(t)$. We note that, since every point (r_i, b) is generated by some value of the parameter t, $\deg_t(M) \geq m$. But, since $\mathcal{P}(t)$ is proper, and since M cannot have multiple roots, we get that $\deg_t(M) = m = \deg_x(f(x, y))$. Now, since b is not the quotient of the leading coefficients of χ_2 and $\chi_{3,2}$, one has that $\deg_x(f(x, y)) = \deg(M) = \max\{\deg(\chi_2), \deg(\chi_{3,2})\}$.

Conversely, let $\mathcal{P}(t)$ be a parametrization of $\mathcal{C}$ such that $\deg(\mathcal{P}(t)) = \max\{\deg_x(f), \deg_y(f)\}$, and let $\mathcal{Q}(t)$ be any proper parametrization of $\mathcal{C}$. Then, by Lemma 1 statement (1), one has that there exists $R(t) \in \mathbb{K}(t)$ such that $\mathcal{Q}(R(t)) = \mathcal{P}(t)$. Now, since $\mathcal{Q}(t)$ is proper, one deduces that $\deg(\mathcal{Q}(t)) = \max\{\deg_x(f), \deg_y(f)\} = \deg(\mathcal{P}(t))$. Therefore, since the degree is multiplicative with respect to composition, one deduces that $R(t)$ is of degree one, and hence invertible. Thus, by Lemma 1(2), $\mathcal{P}(t)$ is proper. $\square$

Applying Theorem 5 and Lemma 1 one deduces the following corollary.

Corollary. *Let $\mathcal{C}$ be a rational affine plane curve defined by $f(x,y) \in \mathbb{K}[x,y]$, then the degree of any rational parametrization of $\mathcal{C}$ is a multiple of* $\max\{\deg_x(f), \deg_y(f)\}$.

In Theorem 6 we apply Theorem 5 to show the relation between the index of a parametrization, the degree of a parametrization and the degree of the curve.

Theorem 6. *Let $\mathcal{C}$ be a rational affine plane curve defined by $f(x,y) \in \mathbb{K}[x,y]$, let $n = \max\{\deg_x(f), \deg_y(f)\}$, and let $\mathcal{P}(t)$ be a rational parametrization of $\mathcal{C}$. Then,*

$$\mathrm{index}(\mathcal{P}(t)) = \frac{\deg(\mathcal{P}(t))}{n}.$$

Proof: By Lüroth's theorem it follows that there exists a proper parametrization $\mathcal{P}'(t)$ of $\mathcal{C}$, and by Lemma 1 there exists $R(t) \in \mathbb{K}(t) \setminus \mathbb{K}$ such that $\mathcal{P}(t) = \mathcal{P}'(R(t))$. Applying Theorem 4 and that $\mathcal{P}'(t)$ is proper, one has that

$$\mathrm{index}(\mathcal{P}(t)) = \deg_t(R(t)) \cdot \mathrm{index}(\mathcal{P}'(t)) = \deg_t(R(t)).$$

Furthermore, since the degree of rational functions is multiplicative, it also holds that $\deg(\mathcal{P}(t)) = \deg_t(R(t)) \cdot \deg(\mathcal{P}'(t))$. Thus,

$$\mathrm{index}(\mathcal{P}(t)) = \frac{\deg(\mathcal{P}(t))}{\deg(\mathcal{P}'(t))}$$

Moreover, taking into account that $\mathcal{P}'(t)$ is proper, by Theorem 5 one has that $\deg(\mathcal{P}'(t)) = n$, and therefore

$$\mathrm{index}(\mathcal{P}(t)) = \frac{\deg(\mathcal{P}(t))}{n}.$$

□

5 Tracing Index and Implicitization

The problem of implicitization consists of finding the defining equations for the smallest algebraic set containing a given set of points S. The problem can be solved by elimination techniques (see [5]). This approach is specially usefull for parametric varieties in $\mathbb{K}^n$. Also, for surfaces, different approaches can be found in [6], [15]. However, for the case of plane curves, the implicit equation can be found by means of gcd's and resultants. For instance, applying Lemma 6, the defining polynomials of the curve defined by $\mathcal{P}(t)$ can be obtained by computing the square-free part of a resultant. Moreover, if properness is guaranteed, Theorem 7 shows that the implicit equation can be computed by a single resultant. In addition to these results, in Theorem 8 we see that when computing the resultant the implicit equation appears to the power of the tracing index.

Lemma 6. *Let $\mathcal{P}(t)$ be a parametrization in reduced form with non-constant components of a curve $\mathcal{C}$. If $f(x,y)$ is the defining polynomial of $\mathcal{C}$, there exists $r \in \mathbb{N}$ such that, up to multiplication by constants,*

$$Res_t(H_1(t,x), H_2(t,y)) = (f(x,y))^r.$$

Proof: We see H_1, H_2 as polynomials in $\mathbb{K}[t,x,y]$. Let $h(x,y) = Res_t(H_1, H_2)$. First, we observe that H_1, H_2 are irreducible because $\gcd(\chi_1, \chi_{3,1}) = \gcd(\chi_2, \chi_{3,2}) = 1$. Hence H_1, H_2 do not have common factors. Therefore, $h(x,y)$ is not the zero polynomial. Furthermore, let us see that h is neither a constant polynomial. Indeed: let $t_0 \in \mathbb{K}$ be such that $\chi_{3,1}(t_0)\chi_{3,2}(t_0) \neq 0$. Then $H_1(t_0, \mathcal{P}(t_0)) = H_2(t_0, \mathcal{P}(t_0)) = 0$. This implies that $h(\mathcal{P}(t_0)) = 0$. Thus, since h is not the zero polynomial it can not be constant.

Now, we consider the square–free part $h'(x,y)$ of $h(x,y)$ and the plane curve $\mathcal{C}'$ defined by $h'(x,y)$ over $\mathbb{K}$. Let us see that $\mathcal{P}(t)$ parametrizes the curve $\mathcal{C}'$. For this purpose, we check that for almost all values of the parameter t, $\mathcal{P}(t) \in \mathcal{C}'$, and that almost all points on $\mathcal{C}'$ are generated by $\mathcal{P}(t)$.

1. Let $t_0 \in \mathbb{K}$ be such that $\chi_{3,1}(t_0)\chi_{3,2}(t_0) \neq 0$. By the previous argument one has that $h(\mathcal{P}(t_0)) = 0$. Thus $h(\mathcal{P}(t_0)) = 0$, and hence $\mathcal{P}(t_0)$ is on $\mathcal{C}'$.

2. Let L_1, L_2 be the leading coefficients of H_1, H_2, w.r.t. t, respectively. Note that $L_1 \in \mathbb{K}[x], L_2 \in \mathbb{K}[y]$ are of degree at most 1. Let $(x_0, y_0) \in \mathcal{C}'$ be such that $L_1(x_0) \neq 0$ or $L_2(y_0) \neq 0$ (note that at most one point in $\mathbb{K}^2$ may vanish both L_1 and L_2). Then, $h'(x_0, y_0) = 0$ and thus $h(x_0, y_0) = 0$. Therefore, since h is a resultant, there exists $t_0 \in \mathbb{K}$ such that $H_1(t_0, x_0, y_0) = H_2(t_0, x_0, y_0) = 0$. Also, observe that $\chi_{3,1}(t_0) \neq 0$ since otherwise it would imply that $\chi_{3,1}(t_0) = \chi_1(t_0) = 0$, which is impossible since $\gcd(\chi_1, \chi_{3,1}) = 1$. Similarly, $\chi_{3,2}(t_0) \neq 0$. Thus, $(x_0, y_0) = \mathcal{P}(t_0)$. Therefore, almost all points on $\mathcal{C}'$ are generated by $\mathcal{P}(t)$.

Therefore, $\mathcal{C} = \mathcal{C}'$, and $f = h'$ up multiplication by constants. Thus, since f irreducible there exists $r \in \mathbb{N}$ such that $h(x,y) = (h'(x,y))^r$. □

Theorem 7. *Let $\mathcal{P}(t)$ be a proper parametrization in reduced form of a curve $\mathcal{C}$. Then, the defining polynomial of $\mathcal{C}$ is the resultant*

$$Res_t(H_1(t,x), H_2(t,y)).$$

Proof: We know from Theorem 5 that, if $f(x,y)$ is the implicit equation of $\mathcal{C}$ then $\deg_y(f) = \max\{\deg_t(\chi_1), \deg_t(\chi_{3,1})\}$, and $\deg_x(f) = \max\{\deg_t(\chi_2), \deg_t(\chi_{3,2})\}$. The polynomials H_1, H_2 can be written as

$$\begin{aligned} H_1(t,x) &= a_m(x)t^m + \cdots + a_0(x), \qquad &\text{where } m = \deg_y(f), \\ H_2(t,y) &= b_n(y)t^n + \cdots + b_0(y), \qquad &\text{where } n = \deg_x(f), \end{aligned}$$

where $\deg_x(a_i) \leq 1$ and $\deg_y(b_i) \leq 1$.

Let $R(x,y)$ be the resultant of H_1 and H_2 with respect to t, and let A be the Sylvester matrix of $H_1, H_2 \in \mathbb{K}(x,y)[t]$ as univariate polynomials in t:

$$A = \begin{pmatrix} a_m(x) & \cdots & \cdots & \cdots & a_0(x) & & \\ & \ddots & & & & \ddots & \\ & & a_m(x) & \cdots & \cdots & \cdots & a_0(x) \\ b_n(y) & \cdots & \cdots & \cdots & b_0(y) & & \\ & \ddots & & & & \ddots & \\ & & b_n(y) & \cdots & \cdots & \cdots & b_0(y) \end{pmatrix}.$$

Therefore, since only the entries in the first n rows depend on x, and this dependence on x is linear, $\deg_x(R) \leq n$. Analogously, $\deg_y(R) \leq m$. On the other hand, from Lemma 6 one has that $f(x,y)$ is a factor of $R(x,y)$. Thus, $\deg_x(f) = \deg_x(R)$ and $\deg_y(f) = \deg_y(R)$. Therefore, up to a constant, $f(x,y) = R(x,y)$. □

We finish this section showing how Lemma 6, Theorem 7 and the notion of tracing index of a parametrization are related. Basically, the result follows from the next lemma on resultants.

Lemma 7. *Let $A, B \in \mathbb{L}[t]$ be non–constant polynomials over a field $\mathbb{L}$:*

$$A(t) = a_m t^m + \cdots + a_0, \quad B(t) = b_n t^n + \cdots + b_0,$$

and let $R(t) = \frac{M(t)}{N(t)} \in \mathbb{L}(t)$ be a non–constant rational function in reduced form, such that for every root β of $A(t)B(t)$ it holds that $\deg(M - \beta N) = \deg(R)$. Let $A'(t)$ and $B'(t)$ be the polynomials

$$A'(t) = a_m M(t)^m + a_{m-1} M(t)^{m-1} N(t) + \cdots + a_0 N(t)^m$$

$$B'(t) = b_n M(t)^n + a_{n-1} M(t)^{n-1} N(t) + \cdots + b_0 N(t)^n$$

Then, if b is the leading coefficient of B and b' is the leading coefficient of B'

$$Res_t(A', B') = \frac{(b')^{m(\deg(R)-\deg(N))}}{b^{\deg(R)m}} Res_t(A,B)^{\deg(R)} \cdot Res_t(B', N)^m.$$

Proof: Let B decompose over the algebraic closure of $\mathbb{L}$ as

$$B(t) = b_n \prod_{i=1}^{n} (t - b_i).$$

Since $B'(t) = N^n \cdot B(R)$ one has that

$$B'(t) = b_n \prod_{i=1}^{n} (M(t) - b_i N(t)).$$

Therefore, since for every $i \in \{1, \dots, n\}$ it holds that $\deg(M - b_i N) = \deg(R)$, one has that $\deg(B') = n \cdot \deg(R)$. In particular, since R is non–constant, one gets that B' is not a constant polynomial. Similarly one gets that $\deg(A') = m \cdot \deg(R)$, and that A' is also a non–constant polynomial.

Now, observe that if $r = \deg(R)$, every root b_i of B generates r roots $\{b_{i,1}, \dots, b_{i,r}\}$ of $B'(t)$, namely the roots of $M(t) - b_i N(t)$. Morevoer, if α is a root of B' then $N(\alpha) \neq 0$, since otherwise one gets that $M(\alpha) = 0$, which is impossible since $\gcd(M, N) = 1$. Therefore, one deduces that

$$b_i = \frac{M(b_{i,j})}{N(b_{i,j})} = R(b_{i,j}), \quad j = 1, \dots, r$$

Let $S = Res_t(A, B)$, $S' = Res_t(A', B')$ and $S'' = Res_t(B', N)$. Then, using that $A' = N^m \cdot A(R)$ one gets

$$S' = (b')^{mr} \prod_{B'(\alpha)=0} A'(\alpha) = (b')^{mr} \prod_{i=1}^{n} \prod_{j=1}^{r} A'(b_{i,j}) = (b')^{mr} \prod_{i=1}^{n} A(b_i)^r \prod_{i=1}^{n} \prod_{j=1}^{r} N(b_{i,j})^m$$

Furthermore, if $k = \deg(N)$, one has that

$$S = b^m \prod_{i=1}^{n} A(b_i), \quad S'' = (b')^k \prod_{i=1}^{n} \prod_{j=1}^{r} N(b_{i,j})$$

Thus,

$$S' = \frac{(b')^{mr}}{b^{rm}} S^r \prod_{i=1}^{n} \prod_{j=1}^{r} N(b_{i,j})^m = \frac{(b')^{mr-km}}{b^{rm}} S^r (S'')^m.$$

□

Theorem 8. *Let $\mathcal{P}(t)$ be a parametrization in reduced form of curve $\mathcal{C}$. If $f(x, y)$ is the defining polynomial of $\mathcal{C}$, then we have, up to multiplication by constants,*

$$Res_t(H_1(t, x), H_2(t, y)) = (f(x, y))^{\mathrm{index}(\mathcal{P})}.$$

Proof: We distinguish two cases depending on whether $\mathcal{C}$ is a vertical or a horizontal line or not. If $\mathcal{C}$ is one these lines, let us say $y = a$, then $\mathcal{P}(t) = (\frac{\chi_1(t)}{\chi_{3,1}(t)}, a)$. Therefore,

$$Res_t(\chi_{3,1}(t)x - \chi_1(t), y - a) = (y - a)^{\deg(\mathcal{P})},$$

and the theorem follows from Theorem 6.

Let us now assume that $\mathcal{C}$ is neither a vertical nor a horizontal line; i.e. its defining polynomial depends on both variables x, y. By Lüroth's theorem, we know that there exist proper rational parametrizations of $\mathcal{C}$. Let us see that there always exists a proper parametrization of $\mathcal{C}$ such that the degrees of the numerator and denominator of each parametrization component, in reduced form, are the same. In order to prove this, we remark that, by Lemma 1, any linear reparametrization of a proper parametrization is again proper. Let $\mathcal{P}'$ be any proper parametrization of $\mathcal{C}$. If zero is a root of none of the numerators and denominators in $\mathcal{P}'$, then $\mathcal{P}'(\frac{1}{t})$ is still proper and the requirement on the degree is fullfilled. If zero is a root of any of the numerators or denominators, we consider the proper parametrization $\mathcal{P}'(t+a)$, where a is not a root of any of the numerators and denomintors. This a always exists since we have excluded vertical and horizontal lines, and therefore no component of the parametrization can be identically zero. Now, observe that no numerator or denominator in $\mathcal{P}'(t+a)$ vanishes at zero. Therefore, one can always reparametrize the initial proper parametrization into a proper one, where degrees of numerator and denominator at each component agree.

Let

$$\mathcal{P}'(t) = \left(\frac{\xi_1(t)}{\xi_{3,1}(t)}, \frac{\xi_2(t)}{\xi_{3,2}(t)} \right)$$

be a proper parametrization, in reduced form, of $\mathcal{C}$ where $\deg(\xi_i) = \deg(\xi_{3,i})$. By Lemma 1 there exists a non-constant rational function $R(t)$ such that $\mathcal{P}(t) = \mathcal{P}'(R(t))$. Let $R(t) = \frac{M(t)}{N(t)}$ be in reduced form. We consider the polynomials

$$H_1^{\mathcal{P}} = \chi_{3,1}(t)x - \chi_1(t), \;\; H_2^{\mathcal{P}} = \chi_{3,2}(t)y - \chi_2(t)$$
$$H_1^{\mathcal{P}'} = \xi_{3,1}(t)x - \xi_1(t), \;\; H_2^{\mathcal{P}'} = \xi_{3,2}(t)y - \xi_2(t)$$

and let

$$\xi_i(t) = \sum_{j=1}^{n_i} a_{i,j}t^j, \;\; \xi_{3,i}(t) = \sum_{j=1}^{n_i} b_{i,j}t^j, \;\; H_i^{\mathcal{P}'}(t) = \sum_{j=1}^{m_i} h_{i,j}t^j, \quad i = 1, 2$$

Observe that $m_i = n_i$. For $i = 1, 2$, we introduce the polynomials

$$\bar{\xi}_i(t) = \sum_{j=1}^{n_i} a_{i,j}M(t)^j N(t)^{n_i - j}, \;\; \bar{\xi}_{3,i}(t) = \sum_{j=1}^{n_i} b_{i,j}M(t)^j N(t)^{n_i-j},$$

$$\bar{H}_i^{\mathcal{P}'}(t) = \sum_{j=1}^{m_i} h_{i,j}M(t)^j N(t)^{m_i-j},$$

which result from $\xi_i, \xi_{3,i}, H_i^{\mathcal{P}'}$ by substituting $R(t)$ for t and clearing denominators. In order to apply Lemma 7 to the polynomials $H_1^{\mathcal{P}'}(t), H_2^{\mathcal{P}'}(t)$ and the rational function $R(t)$, let us see that for every root β of $H_1^{\mathcal{P}'}(t) \cdot H_2^{\mathcal{P}'}(t)$ it holds that $\deg(M(t) - \beta N(t)) = \deg(R)$. Indeed, if β is such that the $\deg(M(t) - \beta N(t)) < \deg(R)$ one has that $\beta \in \mathbb{K}$. Therefore, either $H_1^{\mathcal{P}'}(\beta) = 0$ or $H_2^{\mathcal{P}'}(\beta) = 0$ and $\beta \in \mathbb{K}$. This implies that either $\gcd(\xi_1, \xi_{3,1}) \neq 1$ or $\gcd(\xi_2, \xi_{3,2}) \neq 1$, which is impossible. The application of Lemma 7 leads to

$$Res_t(\bar{H}_1^{\mathcal{P}'}, \bar{H}_2^{\mathcal{P}'}) = \frac{(b')^{n_1(\deg(R)-\deg(N))}}{h_{2,n_2}^{\deg(R)n_1}} \cdot Res_t(H_1^{\mathcal{P}'}, H_2^{\mathcal{P}'})^{\deg(R)} \cdot Res_t(\bar{H}_2^{\mathcal{P}'}, N)^{n_1},$$

where b' is the leading coefficient of $\bar{H}_2^{\mathcal{P}'}$.
In addition, since $\mathcal{P}(t) = \mathcal{P}'(R(t))$, it holds that

$$\xi_j(R(t)) \cdot \chi_{3,j}(t) = \chi_j(t) \cdot \xi_{3,j}(R(t)), \quad j = 1, 2.$$

Thus,

$$\chi_j(t) \cdot H_j^{\mathcal{P}'}(R(t)) = \xi_j(R(t)) \cdot H_j^{\mathcal{P}}(t), \quad j = 1, 2,$$

and (note that $m_j = n_j = k_j$)

$$\chi_j(t)\bar{H}_j^{\mathcal{P}'}(t) = \bar{\xi}_j(t)H_j^{\mathcal{P}}(t), \quad j = 1, 2.$$

$$\chi_j(t)\bar{\xi}_{3,j}(t) = \bar{\xi}_j(t)\chi_{3,j}(t), \quad j = 1, 2.$$

Now, we prove $\gcd(\chi_1, \chi_2) = \gcd(\bar{\xi}_1, \bar{\xi}_2)$. Indeed: $\gcd(\chi_1, \chi_2)$ divides $\bar{\xi}_j \cdot \chi_{3,j}$, and since $\gcd(\chi_j, \chi_{3,j}) = 1$ one has that $\gcd(\chi_1, \chi_2)$ divides $\bar{\xi}_j$. Thus $\gcd(\chi_1, \chi_2)$ divides $\gcd(\bar{\xi}_1, \bar{\xi}_2)$. In order to prove that $\gcd(\bar{\xi}_1, \bar{\xi}_2)$ divides $\gcd(\chi_1, \chi_2)$, we first see that $\gcd(\bar{\xi}_j, \bar{\xi}_{3,j}) = 1$. Let a be a common root of $\bar{\xi}_j$ and $\bar{\xi}_{3,j}$. Note that by definition of $\bar{\xi}_j$ it follows that $N(a) \neq 0$, since otherwise it would imply that $M(a) = 0$, which is impossible since $gcd(M, N) = 1$. Therefore, taking into account that $\bar{\xi}_j = N^{n_j}\xi_j(R)$, $\bar{\xi}_{3,j} = N^{k_j}\xi_{3,j}(R)$, one deduces that $\xi_j(R(a)) = \xi_{3,j}(R(a)) = 0$ which is impossible since $\gcd(\xi_j, \xi_{3,j}) = 1$. Now, since $\gcd(\bar{\xi}_1, \bar{\xi}_2)$ divides $\chi_j \cdot \bar{\xi}_{3,j}$, using that $\gcd(\bar{\xi}_j, \bar{\xi}_{3,j}) = 1$, one deduces that $\gcd(\bar{\xi}_1, \bar{\xi}_2)$ divides $\gcd(\chi_1, \chi_2)$.

As a consequence of this remark the equalities above can be expressed as:

$$\chi_j^*(t)\bar{H}_j^{\mathcal{P}'}(t) = \bar{\xi}_j^*(t)H_j^{\mathcal{P}}(t), \quad j = 1, 2.$$

$$\chi_j^*(t)\bar{\xi}_{3,j}(t) = \bar{\xi}_j^*(t)\chi_{3,j}(t), \quad j = 1, 2.$$

where $\gcd(\chi_1^*, \chi_2^*) = \gcd(\bar{\xi}_1^*, \bar{\xi}_2^*) = 1$. Therefore,

$$Res_t(\chi_1^*\bar{H}_1^{\mathcal{P}'}, \chi_2^*\bar{H}_2^{\mathcal{P}'}) = Res_t(\bar{\xi}_1^*H_1^{\mathcal{P}}, \bar{\xi}_2^*H_2^{\mathcal{P}}).$$

So,

$$Res_t(\chi_1^*, \chi_2^*) \cdot Res_t(\chi_1^*, \bar{H}_2^{\mathcal{P}'}) \cdot Res_t(\bar{H}_1^{\mathcal{P}'}, \chi_2^*) \cdot Res_t(\bar{H}_1^{\mathcal{P}'}, \bar{H}_2^{\mathcal{P}'}) =$$
$$= Res_t(\bar{\xi}_1^*, \bar{\xi}_2^*) \cdot Res_t(\bar{\xi}_1^*, H_2^{\mathcal{P}}) \cdot Res_t(H_1^{\mathcal{P}}, \bar{\xi}_2^*(t)) \cdot Res_t(H_1^{\mathcal{P}}, H_2^{\mathcal{P}}).$$

We prove that if $L(t) \in \mathbb{K}[t]$ then $\gcd(L, H_i^{\mathcal{P}}) = \gcd(L, \bar{H}_i^{\mathcal{P}'}(t)) = 1$. Indeed: if the gcd is not trivial there exists $a \in \mathbb{K}$ such that, for instance, $H_i^{\mathcal{P}}(a)$ but this implies that $\gcd(\chi_i, \chi_{3,i}) \neq 1$, which is impossible. Also, if $\bar{H}_i^{\mathcal{P}'}(a) = 0$, from its definition it follows that $N(a) \neq 0$. Therefore, since $\bar{H}_i^{\mathcal{P}'}(t) = N^{m_i}H_i^{\mathcal{P}'}(R(t))$, one would deduce that $H_i^{\mathcal{P}'}(R(a)) = 0$, and hence $\gcd(\xi_i, \xi_{3,i}) \neq 1$ which is impossible.

Taking into account this fact and that $\gcd(\chi_1^*, \chi_2^*) = \gcd(\bar{\xi}_1^*, \bar{\xi}_2^*) = 1$, the previous equality on resultants can be written as

$$T_1(y)T_2(x)Res_t(\bar{H}_1^{\mathcal{P}'}, \bar{H}_2^{\mathcal{P}'}) = T_1^{'}(y)T_2^{'}(x)Res_t(H_1^{\mathcal{P}}, H_2^{\mathcal{P}})$$

where $T_i, T_i^{'}$ are univariate non–zero polynomials over $\mathbb{K}$. Now, combining this last equality and the one on resultants deduced from Lemma 7 one gets that:

$$T_1(y)T_2(x)\left(\frac{(b')^{n_1(\deg(R)-\deg(N))}}{h_{2,n_2}^{\deg(R)n_1}}Res_t(H_1^{\mathcal{P}'}, H_2^{\mathcal{P}'})^{\deg(R)}\cdot Res_t(\bar{H}_2^{\mathcal{P}'}, N)^{n_1}\right)=$$

$$=T_1^{'}(y)T_2^{'}(x)Res_t(H_1^{\mathcal{P}}, H_2^{\mathcal{P}}).$$

Furthermore, if $f(x,y)$ is the implicit equation of $\mathcal{C}$, by Lemma 6 and Theorem 7 one obtains that there exists $\ell \in \mathbb{N}$ such that

$$T_1(y)T_2(x)\left(\frac{(b')^{n_1(\deg(R)-\deg(N))}}{h_{2,n_2}^{\deg(R)n_1}}f(x,y)^{\deg(R)}\cdot Res_t(\bar{H}_2^{\mathcal{P}'}, N)^{n_1}\right)=T_1^{'}(y)T_2^{'}(x)f(x,y)^{\ell}$$

Moreover, since $b', h_{2,n_2} \in \mathbb{K}[y]^*$ and $Res_t(\bar{H}_2^{\mathcal{P}'}, N)^{n_1} \in \mathbb{K}[y]^*$ (note that we have already proved that the gcd of $\bar{H}_2^{\mathcal{P}'}$ and a polynomial depending only on t is trivial) the above equaliy can be written as

$$K_1(y)K_2(x)f(x,y)^{\deg(R)} = K_1^{'}(y)K_2^{'}(x)f(x,y)^{\ell}$$

for some non-zero polynomials $K_i, K_i^{'}$. Therefore, since $f(x,y)$ is irreducible and it depends on both variables x, y, one concludes that there exits $\ell \in \mathbb{K}$ such that

$$f(x,y)^{\deg(R)} = f(x,y)^{\ell}.$$

Thus, $\deg(R) = \ell$. Furthermore, from Theorem 4 one has that

$$\mathrm{index}(\mathcal{P}(t)) = \mathrm{index}(\mathcal{P}'(R(t)) = \deg(R)\cdot \mathrm{index}(\mathcal{P}'(t)) = \deg(R).$$

□

References

[1] Abhyankar S.S., Bajaj C.L. (1988), *Automatic Parametrization of Rational Curves and Surfaces III: Algebraic Plane Curves.* Computer Aided Geometric Design **5**, 309-321.

[2] Andradas C., Recio T., Sendra J.R. (1997), *A Relatively Optimal Reparametrization Algorithm.* Proc.ISSAC97, pp. 349-356, ACM Press.

[3] Andradas C., Recio T., Sendra J.R. (1999), *Base field restriction techniques for parametric curves.* Proc. ISSAC 99, pp.17-22, ACM Press.

[4] Arrondo E., Sendra J., Sendra J.R. (1997), *Parametric Generalized Offsets to Hypersurfaces.* J. of Symbolic Computation **23**, 267-285.

[5] Cox D., Little J., O'Shea D. (1997), *Ideals, Varieties, and Algorithms (2nd ed.).* Springer-Verlag, New York.

[6] González-Vega L. (1997), *Implicitization of Parametric Curves and Surfaces by using Multidimensional Newton Formulae.* J. Symbolic Computation vol. 23, pp. 137-152.

[7] Harris J. (1995), *Algebraic Geometry. A first Course.* Springer-Verlag.

[8] van Hoeij M. (1994), *Computing Parametrizations of Rational Algebraic Curves.* Proc. ISSAC'94, ACM Press, 187-190.

[9] van Hoeij M. (1997), *Rational Parametrizations of Curves Using Canonical Divisors.* J. of Symbolic Computation **23**, 209-227.

[10] Hoffmann C. M. (1993), *Geometric and Solid Modeling.* Morgan Kaufmann Publ., Inc.

[11] Hoffmann C.M., Sendra J.R., Winkler F. (1997), *Parametric Algebraic Curves and Applications.* J.of Symbolic Computation 23.

[12] Hoschek J., Lasser D. (1993), *Fundamentals of Computer Aided Geometric Design.* A.K. Peters Wellesley MA., Ltd.

[13] Schicho J. (1992), *On the Choice of Pencils in the Parametrization of Curves.* J. of Symbolic Computation **14**, 557-576.

[14] Sederberg T.W. (1986), *Improperly Parametrized Rational Curves.* Computer Aided Geometric Design **3**, 67-75.

[15] Sederberg T.W., Goldman R., Du H., (1997). *Impliciting Rational Curves by the method of moving algebraic curves.* J. Symbolic Computation vol. 23, pp. 153-176.

[16] Sendra J.R., Winkler F. (1991), *Symbolic Parametrization of Curves.* J. Symbolic Computation **12/ 6,** 607-631.

[17] Sendra J.R., Winkler F. (1997). *Parametrization of Algebraic Curves over Optimal Field Extensions.* J. Symbolic Computation vol. 23, pp. 191-207.

[18] Shafarevich, I.R. (1994). *Basic Algebraic Geometry 1; Varieties in Projective Space.* Springer-Verlag, Berlin New York.

[19] van der Waerden, B.L. (1953). *Modern Algebra, vol. 1.* Frederick Ungar Publ.Co., New York.

[20] Walker, R.J. (1950). *Algebraic Curves.* Princeton University Press.

[21] Zippel R., *Rational Function Decomposition.* Proc. of ISSAC91 pp. 1-6 ACM Press.