Tracing index of rational curve parametrizations ⋆

J. Rafael Sendra [a,*] Franz Winkler [b]

[a] *Dpto de Matemáticas, Universidad de Alcalá, E-28871 Madrid, Spain*

[b] *RISC-Linz, Johannes Kepler Universität, A-4040 Linz, Austria*

Abstract

A rational parametrization of an algebraic curve establishes a rational correspondence of this curve with the affine or projective line. This correspondence is a birational equivalence if the parametrization is proper. So, intuitively speaking, a rational parametrization determines a linear tracing of the curve, when the parameter takes values in the algebraic closure of the ground field. 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. In addition, we show how to apply these results to the case of real curves, where we introduce the notion of real tracing index.

Key words: tracing index, real tracing index, algebraic curves, parametrization.

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

⋆ 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.

* Corresponding Author

Email addresses: rafael.sendra@uah.es (J. Rafael Sendra), franz.winkler@risc.uni-linz.ac.at (Franz Winkler).

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 Andradas et al, 1997, 1999; van Hoeij, 1997; Schicho, 1992; Sendra and Winkler, 1997). 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 in the algebraic closure of the field containing the coefficients of the parametrization. More rigorously speaking proper parametrizations correspond to bijective mappings from the field of parameter values onto the curve.

Most parametrization algorithms provide proper parametrizations (see Abhyankar and Bajaj, 1988; van Hoeij, 1994; Sendra and Winkler, 1991). Furthermore, improperness can be detected algorithmically, and the given parametrization can be reparametrized into a proper one (see Sederberg, 1986). An alternative approach based on rational function decomposition can be found in Zippel (1991). Proper parametrizations play an important role in many practical applications in computer aided geometric design, such as in visualization (see Hoffmann, 1993; Hoffmann et al, 1997; Hoschek and Lasser, 1993) or rational parametrization of offsets (see Arrondo et al, 1997). Also, they provide an implicitization approach based on resultants (see Theorem 7); similar results on implicitization can be found in Chionh and Goldman (1992) and Cox et al (1998). For other related questions of proper parametrizations we refer to Gao and Chou (1992).

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 measures the number of times that a parametrization traces a curve over the algebraic closure of the ground field. The theorem on the dimension of fibres (see Shafarevich, 1994, pp. 76) states that for almost all points on the curve the dimension of the fibre, i.e. the set of parameter values mapped to this point, 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 Shafarevich, 1994, Section 6.3.). In fact, the cardinality of a generic fibre is the degree of the mapping (see Harris, 1995, Prop. 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 determine 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 preparation for formally introducing 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 greatest common divisors for computing the index (see Theorem 2), that agrees with Sederberg's criterion (see Sederberg, 1986) for properness (see Theorem 3).

As we have mentioned, the tracing index measures the number of times the curve is traced when the parameter takes values in an algebraically closed field. However, in practice, it might be interesting to know the tracing index when the parameter values are real. In Section 4 we deal with this problem, introducing the notion of real tracing index and showing how to compute it.

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). Similar results on implicitization can be found in Chionh and Goldman (1992) and Cox et al (1998).

In this paper, we only deal with the tracing index for plane curve 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. Walker, 1950, Theorem 6.5.), the tracing index of a space parametrization is directly related to the tracing index of a plane parametrization. Furthermore, a more general theoretical statement of the problem can be studied if the degree of rational maps between curves is considered. For further details on this related problem we refer to Sendra and Winkler (2001).

In the sequel, we use the following notations. $\mathbb{K}$ 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

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

We will assume in the paper that rational parametrizations are given in reduced form, that is $\gcd(\chi_{1,1}, \chi_{1,2}) = \gcd(\chi_{2,1}, \chi_{2,2}) = 1$. Furthermore, for given parametrization $\mathcal{P}(t)$ we consider the polynomials

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

and $G(s,t) = \gcd(G_1, G_2)$, as well as the polynomials

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

Proofs are collected in Appendix A.

2 Proper Parametrizations

We start recalling some basic results on proper parametrizations. Let $\mathbb{K}$ be an algebraically closed field of characteristic zero, and $\mathcal{C}$ 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

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

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

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

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 (Abhyankar and Bajaj, 1988; van Hoeij, 1994; Sendra and Winkler, 1991, see). Furthermore, given an improper parametrization, in Sederberg (1986) it is shown how to compute a new parametrization 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*

(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 $\mathcal{Q}(t) = \mathcal{P}(L(t))$.

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 state 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.*

From Lemma 2 we immediately get the following corollary.

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.

Note that, 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 may 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. Then, for $\alpha \in \mathbb{K}$ such that $\chi_{1,2}(\alpha)\chi_{2,2}(\alpha) \neq 0$, and such that $G_1(\alpha, t)$, $G_2(\alpha, t)$ do not have multiple roots,*

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

The following result follows from Theorem 1 and Corollary of Lemma 2.

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 $\chi_{1,2}(\alpha)\chi_{2,2}(\alpha)R_1(\alpha)R_2(\alpha) \neq 0$,

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

Theorem 1 implies that a point $(x_\alpha, y_\alpha) = \mathcal{P}(\alpha) \in \mathcal{C}$, with α satisfying the hypothesis of the theorem, 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 $a \in \mathbb{K}$,

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

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 w.r.t. y 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

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

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*

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

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 $m = \deg_t(G(s,t))$.

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 $\text{index}(\mathcal{P}(t)) = \deg_t(G(s,t))$. 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 $\mathcal{P}(t)$, then the tracing index of the parametrization $\mathcal{P}(t)$ is the degree of the rational map $\mathcal{P}$. Therefore, $\text{index}(\mathcal{P}(t))$ 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 Harris, 1995; Shafarevich, 1994); i.e. $\text{index}(\mathcal{P}(t)) = [\mathbb{K}(t) : \varphi_{\mathcal{P}}(\mathbb{K}(\mathcal{C}))]$. For the relation between the tracing index and the degree of a rational map see Sendra and Winkler (2001).

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* $\deg_t(G(s,t)) = 1$.

The previous results can be used to derive the following algorithm.

Algorithm INDEX. Given a rational parametrization $\mathcal{P}(t) = \left(\frac{\chi_{1,1}(t)}{\chi_{1,2}(t)}, \frac{\chi_{2,1}(t)}{\chi_{2,2}(t)}\right)$, in reduced form, the algorithm computes $\text{index}(\mathcal{P}(t))$, and decides whether the parametrization is proper.

1. Compute the polynomials $G_1(s,t) = \chi_{1,1}(s)\chi_{1,2}(t) - \chi_{1,2}(s)\chi_{1,1}(t)$, and $G_2(s,t) = \chi_{2,1}(s)\chi_{2,2}(t) - \chi_{2,2}(s)\chi_{2,1}(t)$.
2. Determine $G(s,t) = \gcd(G_1, G_2)$.
3. $t = \deg_t(G(s,t))$.
4. If $t = 1$ then return "$\mathcal{P}(t)$ `is proper`" else return "$\mathcal{P}(t)$ `is not proper and` $\text{index}(\mathcal{P}(t)) = t$".

We illustrate the algorithm INDEX by an example.

Example 1. Let $\mathcal{P}(t)$ be the rational parametrization

$$\mathcal{P}(t) = \left(\frac{(t^2-1)\,t}{t^4-t^2+1}, \frac{(t^2-1)\,t^2}{t^6-3\,t^4+3\,t^2-1-2\,t^3} \right).$$

In Step 1 the polynomials

$$\begin{aligned} G_1(s,t) &= s^3t^4 - s^3t^2 + s^3 - st^4 + st^2 - s - t^3s^4 + s^2t^3 - t^3 + ts^4 - ts^2 + t \\ G_2(s,t) &= s^4t^6 - s^4 - 2\,t^3s^4 - s^2t^6 + s^2 + 2\,s^2t^3 - t^4s^6 + t^4 + 2\,s^3t^4 + t^2s^6 \\ &\quad -t^2 - 2\,s^3t^2, \end{aligned}$$

are generated, and in Step 2 their gcd is determined as $G(s,t) = t-s+st^2-s^2t$. Thus, $\mathrm{index}(\mathcal{P}(t)) = 2$, and therefore the parametrization is not proper. □

Behavior of the cardinality of the fibre

The cardinality of the fibres of the mapping $\mathcal{P} : \mathbb{K} \longrightarrow \mathcal{C}$ is the same for almost all points on $\mathcal{C}$. Nevertheless, for finitely many expections, the cardinality may vary. ¿From the proofs of the previous results one deduces the following summary on the behavior of the cardinalty. Let $\alpha \in \mathbb{K}$, then $\mathcal{P}^{-1}(\mathcal{P}(\alpha)) = \{\beta \in \mathbb{K} \,|\, G_1(\alpha,\beta) = 0,\, G_2(\alpha,\beta) = 0\}$ if $\chi_{1,2}(\alpha)\chi_{2,2}(\alpha) \neq 0$, and $\mathcal{P}^{-1}(\mathcal{P}(\alpha)) = \emptyset$ otherwise. Now, let $\ell_i(t)$ be the leading coefficient of G_i w.r.t. t, let $T(s) = Res_t(G_1, G_2)$ and let $R_1(s)$ and $R_2(s)$ be as in the statement of Corollary to Theorem 1. Then, it holds that

(1) if $\ell_1(\alpha) = 0$ or $\ell_2(\alpha) = 0$ or $T(\alpha) = 0$ then $\mathrm{Card}(\mathcal{P}(\mathcal{P}^{-1}(\alpha))) \geq \mathrm{index}(\mathcal{P}(t))$;
(2) if $\ell_1(\alpha)\ell_2(\alpha)T(\alpha) \neq 0$ then $\mathrm{Card}(\mathcal{P}(\mathcal{P}^{-1}(\alpha))) \leq \mathrm{index}(\mathcal{P}(t))$;
(3) if $R_1(\alpha)\,R_2(\alpha) \neq 0$ then $\mathrm{Card}(\mathcal{P}(\mathcal{P}^{-1}(\alpha))) = \mathrm{index}(\mathcal{P}(t))$.

The explanation of this behavior is the following: in (1) it may happen that $\deg_t(\gcd(G_1(\alpha,t), G_2(\alpha,t))) > \deg_t(G(s,t)) = \mathrm{index}(\mathcal{P}(t))$ (see Lemma 3 (1)). In (2), by Lemma 3 (2), one has that $\deg_t(\gcd(G_1(\alpha,t), G_2(\alpha,t))) = \deg_t(G(s,t)) = \mathrm{index}(\mathcal{P}(t))$, but it may happen that $\gcd(G_1(\alpha,t), G_2(\alpha,t))$ is not squarefree, and therefore the cardinality of the fibre decreases. For (3) see Corollary to Theorem 1.

Example 2. Let $\mathcal{P}(t)$ be the rational parametrization in Example 1. $G(s,t) = t - s + st^2 - s^2t$. Thus, $\mathrm{index}(\mathcal{P}(t)) = 2$. On the other hand, the polynomials

$\ell_1(s), \ell_2(s), T(s), R_1(s)$, and $R_2(s)$ are

$$\ell_1(s,t) = (s^3 - s)$$
$$\ell_2(s,t) = (s^4 - s^2)$$
$$T(s) = s^2\,(s-1)^2\,(s+1)^2\,(s^2+s-1)^4$$
$$R_1(s) = s\,(s-1)\,(s+1)\,(4\,s^4 - 7\,s^2 + 4)\,(s^2+1)^2\,(s^2+s-1)^4\,(s^2-s-1)^4$$
$$R_2(s) = -64\,s^6\,(s-1)^3\,(s+1)^3\,(s^8 - 4\,s^5 - s^4 + 4\,s^3 + 1)\,(s^2+1)^2$$
$$(s^2-2\,s-1)^2\,(s^4+2\,s^3+2\,s^2-2\,s+1)^2\,(s^2+s-1)^4\,(s^4-s^3-s^2+s+1)^4$$

The roots of $\ell_1(s), \ell_2(s), T(s)$ may generate points whose fibre has cardinality greater than 2. In our example these roots are $\{0, 1, -1, -\frac{1}{2} \pm \frac{\sqrt{5}}{2}\}$, and

$$\mathcal{P}^{-1}(\mathcal{P}(0)) = \mathcal{P}^{-1}(\mathcal{P}(1)) = \mathcal{P}^{-1}(\mathcal{P}(-1)) = \mathcal{P}^{-1}((0,0)) = \{0, 1, -1\},$$
$$\mathcal{P}^{-1}(\mathcal{P}(-\tfrac{1}{2} \pm \tfrac{\sqrt{5}}{2})) = \{-\tfrac{1}{2} + \tfrac{\sqrt{5}}{2}, -\tfrac{1}{2} - \tfrac{\sqrt{5}}{2}\}.$$

The roots of $R_1(s)$ and $R_2(s)$ not being roots of $\ell_1(s), \ell_2(s), T(s)$ may generate points whose fibre has cardinality less that 2. In our example

$$\mathcal{P}^{-1}(\mathcal{P}(i)) = \{i\},\ \ \mathcal{P}^{-1}(\mathcal{P}(-i)) = \{-i\}.$$

Finally, the theory ensures that for any α not being a root of $R_1(s), R_2(s)$, $\chi_{1,2}(t)$, or $\chi_{2,2}(t)$, the fibre has cardinality 2. □

Geometric interpretation

Let α be such that $\chi_{1,2}(\alpha)\chi_{2,2}(\alpha) \neq 0$. Then, the fibre is expressed as

$$\mathcal{P}^{-1}(\mathcal{P}(\alpha)) = \{\beta \in \mathbb{K} \,|\, G_1(\alpha, \beta) = 0, G_2(\alpha, \beta) = 0\}.$$

Thus, $\mathcal{P}^{-1}(\mathcal{P}(\alpha))$ can be seen as the common affine intersection points of the curves defined by $G_1(s,t), G_2(s,t)$ and the line $s = \alpha$. Therefore, for all but finitely many exceptions, $\mathcal{P}^{-1}(\mathcal{P}(\alpha))$ can be seen as the common affine intersection points of the curve defined by $G(s,t)$ and the line $s = \alpha$ (case (3) of the behavior of the cardinality of the fibre). Thus, for all but finitely many exceptions, index$(\mathcal{P}(t))$ is the number of affine intersections, counted without multiplicity, of the curve defined by $G(s,t)$ and the line $s = \alpha$. Note that the line $s = t$ is always a component of $G(s,t)$.

However it may happen that, for finitely many values α of s, the number of intersection points of G_1, G_2, and $s = \alpha$, is greater than the number of

intersection points of G, and $s = \alpha$ (case (1) of the behavior of the cardinality of the fibre). Moreover, it may occur that, although the previous situation does not happen, the line $s = \alpha$ is tangent to the curve $G(s, t)$, in which case the cardinality of the fibre decreases (case (2) of the behavior of the cardinality of the fibre).

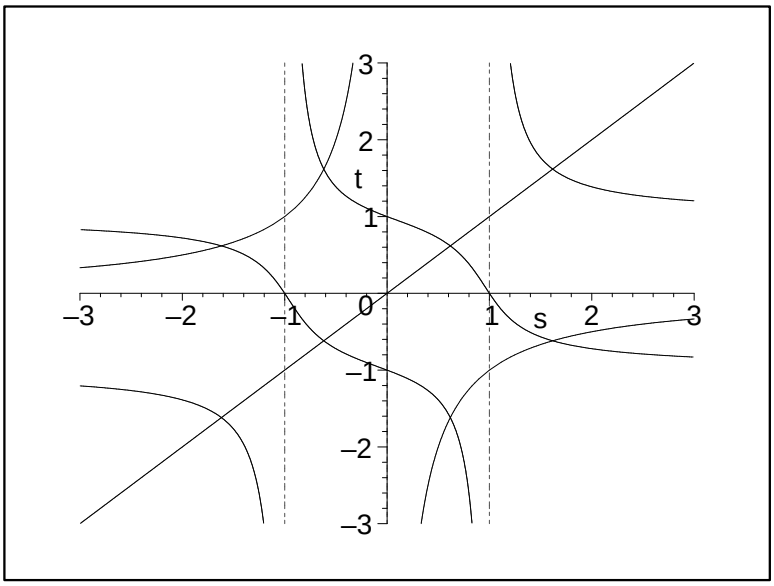

Fig. 1. Curve $G_1(s, t)$

We finish this section by an analysis of Example 1. In Figure 1, the real part of the curve $G_1(s, t)$ is plotted together with the vertical lines $s = 0$,$s = 1$, and $s = -1$.

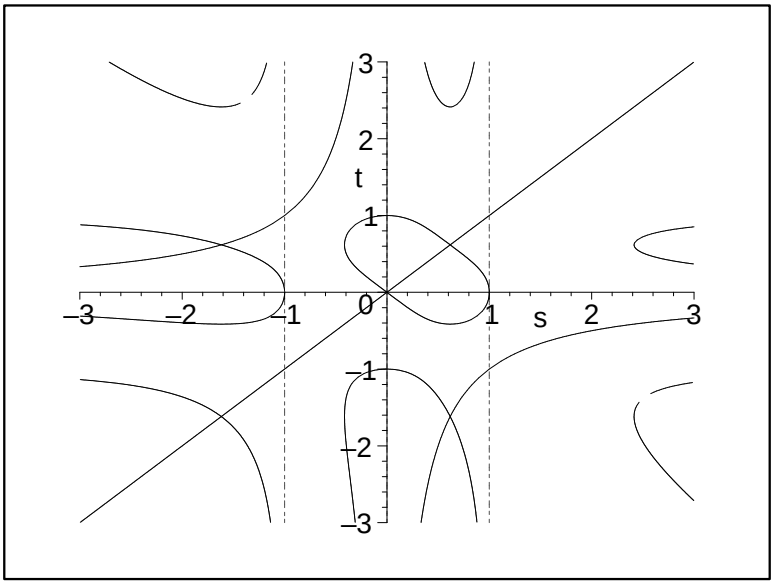

Fig. 2. Curve $G_2(s, t)$

In Figure 2 the real part of $G_2(s, t)$ together with these vertical lines is plotted,

and in Figure 3 the real part of $G(s,t)$ is plotted.

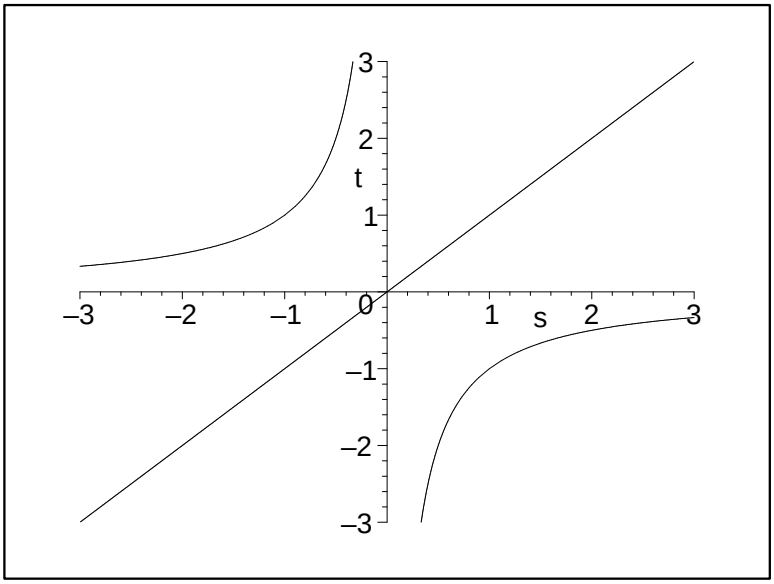

Fig. 3. Curve $G(s,t)$

Now observe that for all $\alpha \neq 0$ the intersection of $s = \alpha$ and $G(s,t)$ consists of two affine points. However, the intersections of $s = 0$ and $G_1(s,t), G_2(s,t)$ are three affine points; similarly for $s = 1$ and $s = -1$.

4 Real tracing index

The tracing index measures the number of times a parametrization traces the curve when the parameter takes values in the algebraically closed field $\mathbb{K}$. However, in pratice, one may be interested in computing the number of times the curve is traced when the parameter takes real values. This leads to the notion of real tracing index.

Let $\mathcal{C}$ be a real curve, i.e. a curve with infinitely many real points, defined by a rational parametrization $\mathcal{P}(t)$. In principle, it may happen that $\mathcal{P}(t)$ contains non–real complex coefficients. However, there exist algorithmic approaches that reparametrize $\mathcal{P}(t)$ into a new rational parametrization, defined over the reals, of the same real curve (see Recio and Sendra (1997)). Therefore, in the following, we assume that $\mathcal{P}(t)$ is a rational parametrization over $\mathbb{R}$ in reduced form. In this situation, we want to compute the cardinality of the fibres of the map

$$\mathcal{P}|_{\mathbb{R}} : \mathbb{R} \longrightarrow \mathcal{C}.$$

If $\alpha \in \mathbb{R}$ is such that $\chi_{1,2}(\alpha)\chi_{2,2}(\alpha) \neq 0$ we denote the fibre $\mathcal{P}|_{\mathbb{R}}^{-1}(\mathcal{P}|_{\mathbb{R}}(\alpha))$ by $\mathcal{F}_{\mathcal{P}}^{\mathbb{R}}(\alpha)$. That is,

$$\mathcal{F}_{\mathcal{P}}^{\mathbb{R}}(\alpha) = \mathcal{P}^{-1}(\mathcal{P}(\alpha)) \cap \mathbb{R} = \{\beta \in \mathbb{R} \mid \gcd(G_1(\alpha,t), G_2(\alpha,t))(\beta) = 0\}.$$

Thus, for a particular α, $\mathrm{Card}(\mathcal{F}_{\mathcal{P}}^{\mathbb{R}}(\alpha))$ can be computed by counting the number of different real roots of a univariate polynomial over the real numbers. There exist many algorithmic approaches to the problem of counting the number of different real roots of a univariate polynomial (see, e.g., Bini et al (2000)).

Before giving a geometric interpretation of the problem, we observe that the curve defined by $G(s,t)$ is real since it has at least one real component, namely the line $s - t = 0$. However, $G(s,t)$ may have non–real components. For instance, if $\mathcal{P}(t) = (\frac{1}{t^4}, \frac{1}{t^4})$, then $G(s,t) = (s-t)(s+t)(s^2+t^2)$.

For almost all $\alpha \in \mathbb{R}$, $\mathrm{Card}(\mathcal{P}^{-1}(\mathcal{P}(\alpha)))$ is the number of affine intersection points of the curve $G(s,t)$ and the line $s = \alpha$. Thus, since $\mathcal{F}_{\mathcal{P}}^{\mathbb{R}}(\alpha) = \mathcal{P}^{-1}(\mathcal{P}(\alpha)) \cap \mathbb{R}$, geometrically, the cardinality of $\mathcal{F}_{\mathcal{P}}^{\mathbb{R}}(\alpha)$ can be seen as the number of real affine intersections of the real curve $G(s,t)$ with the line $s = \alpha$. However, the cardinality of the fibre may be different for the values in two different intervals of $\mathbb{R}$. Nevertheless, under certain conditions of square–freeness the theory of Cylindrical Algebraic Decomposition (C.A.D.), see Collins (1975), ensures the existence of a finite partition of intervals $\{I_i\}_{0 \leq i \leq r}$ of $\mathbb{R}$ such that in the interior of each interval I_i the cardinality of the fibre is constant. Then, the idea is to define the real tracing index as the maximum of the cardinalities of the fibres in each of these finitely many intervals. For instance, if we consider the parametrization $\mathcal{P}(t) = (t^4 - t^2, t^4 - t^2)$ of the line $y = x$, then $G(s,t) = (t^2 - s^2)(t^2 + s^2 - 1)$, and hence $\mathrm{index}(\mathcal{P}(t)) = 4$. The C.A.D. of $G(s,t)$ generates the following partition (see Figure 4)

$$\mathbb{R} = (-\infty, -1] \cup (-1, -\frac{\sqrt{2}}{2}) \cup (-\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}) \cup (\frac{\sqrt{2}}{2}, 1) \cup [1, \infty)$$

and the cardinality of the fibre in the interior of each interval is

$$\begin{aligned}
&\text{if } \alpha \in (-\infty, -1) \text{ then } \mathrm{Card}(\mathcal{F}_{\mathcal{P}}^{\mathbb{R}}(\alpha)) = 2,\\
&\text{if } \alpha \in (-1, -\tfrac{\sqrt{2}}{2}) \text{ then } \mathrm{Card}(\mathcal{F}_{\mathcal{P}}^{\mathbb{R}}(\alpha)) = 4,\\
&\text{if } \alpha \in (-\tfrac{\sqrt{2}}{2}, \tfrac{\sqrt{2}}{2}) \text{ then } \mathrm{Card}(\mathcal{F}_{\mathcal{P}}^{\mathbb{R}}(\alpha)) = 4,\\
&\text{if } \alpha \in (\tfrac{\sqrt{2}}{2}, 1) \text{ then } \mathrm{Card}(\mathcal{F}_{\mathcal{P}}^{\mathbb{R}}(\alpha)) = 4,\\
&\text{if } \alpha \in (1, \infty) \text{ then } \mathrm{Card}(\mathcal{F}_{\mathcal{P}}^{\mathbb{R}}(\alpha)) = 2.
\end{aligned}$$

Furthermore, $\mathcal{F}_{\mathcal{P}}^{\mathbb{R}}(-1))$, and $\mathcal{F}_{\mathcal{P}}^{\mathbb{R}}(1))$ have cardinality 3, and $\mathcal{F}_{\mathcal{P}}^{\mathbb{R}}(-\frac{\sqrt{2}}{2}), \mathcal{F}_{\mathcal{P}}^{\mathbb{R}}(\frac{\sqrt{2}}{2})$ have cardinality 4.

In order to formally state these ideas, we start with a well known result in Real Algebra that can be directly deduced from the theory of Cylindrical Algebraic Decomposition (see, e.g., Collins (1975) or Section 9.2. in Winkler (1996)).

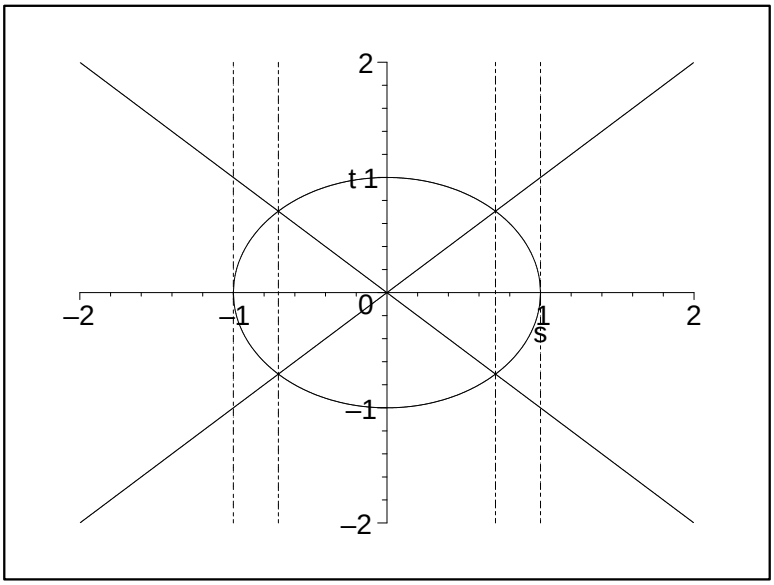

Fig. 4. C.A.D. generated by $G(s,t)$

Lemma 5. *Let $f \in \mathbb{R}[x,y]$ be a square-free polynomial, let $D(x)$ be the discriminant of f with respect to the variable y, and let $I \subseteq \mathbb{R}$ be non-empty and connected. If $D(x)$ does not vanish on any element of I, then for every $a \in I$ the polynomial $f(a,y)$ is square-free, and the number of real roots of $f(a,y)$ is constant.*

In the next lemma we show that the polynomial $G(s,t)$ satisfies the hypothesis of Lemma 5.

Lemma 6. *$G(s,t)$ is a square–free real polynomial.*

Lemma 7. *Let $D(t)$ be the discriminant of $G(s,t)$ w.r.t. t, and let $b_0, \ldots, b_r \in \mathbb{R}$ be such that*

$$-\infty = a_0 < b_0 < a_1 < b_1 < a_2 < \cdots < b_{r-1} < a_r < b_r < a_{r+1} = +\infty,$$

where $a_1, \ldots, a_r$ are the real roots of $D(x)$, and let ℓ_i denote the number of real roots of the polynomial $G(b_i,t)$. Then for almost all $\alpha \in (a_i, a_{i+1}), i = 0, \ldots, r$, we have

$$\mathrm{Card}(\mathcal{F}_{\mathcal{P}}^{\mathbb{R}}(\alpha)) = \ell_i.$$

Taking into account Lemma 7, we introduce the notion of real tracing index.

Definition. Let $D(t)$ be the discriminant of $G(s,t)$ w.r.t. t, and let $b_0,\ldots,b_r \in \mathbb{R}$ be such that

$$-\infty = a_0 < b_0 < a_1 < b_1 < a_2 < \cdots < b_{r-1} < a_r < b_r < a_{r+1} = +\infty,$$

where $a_1,\ldots,a_r$ are the real roots of $D(x)$, and let ℓ_i denote the number of real roots of the polynomial $G(b_i,t)$. Then, we define the *real tracing index* of $\mathcal{P}(t)$, denoted by $\text{index}_{\mathbb{R}}(\mathcal{P}(t))$, as

$$\text{index}_{\mathbb{R}}(\mathcal{P}(t)) = \max\{\ell_0,\ldots,\ell_r\}.$$

Remark.

(1) If $D(t)$ does not have real roots, then for all $\alpha \in \mathbb{R}$ the number of real roots of $G(\alpha,t)$ is invariant, and therefore the cardinaltiy of the fibre is the same for almost all real values. In particular, this is the case if the given parametrization is proper. Note that in this case $G(s,t) = s - t$, and its discriminant is $D(t) = 1$. The converse is not true, for instance the parametrization (t^5+t, t^5+t) is not proper ($\text{index}(\mathcal{P}(t)) = 5$), but the discriminat of $G(s,t)$ has no real roots.

(2) In some applications it may be interesting to know the real tracing index in a particular interval I of $\mathbb{R}$. In this case, one may proceed as follows:

$$\text{index}_I(\mathcal{P}(t)) = \max\{\ell_i \mid b_i \in I\}.$$

In the following, we outline the algorithm for computing the real tracing index of a rational parametrization.

Algorithm REAL-INDEX. Given a rational real parametrization $\mathcal{P}(t) = \left(\frac{\chi_{1,1}(t)}{\chi_{1,2}(t)}, \frac{\chi_{2,1}(t)}{\chi_{2,2}(t)}\right)$, in reduced form, the algorithm computes $\text{index}_{\mathbb{R}}(\mathcal{P}(t))$.

1. Compute the polynomials $G_1(s,t)$, and $G_2(s,t)$.
2. Determine $G(s,t) = \gcd(G_1, G_2)$.
3. Compute the discriminant $D(t)$ of $G(s,t)$ w.r.t. t.
4. Isolate the real roots of $D(t)$. Let $I_i = (b_i, b_{i+1}), i = 0,\ldots,r-1$ be such that each I_i contains exactly one real root of $D(t)$.
5. If $D(t)$ does not have real roots, then
   5.1. Compute the number of ℓ real roots of $G(0,t)$.
   5.2. Return ℓ.
6. For i from 0 to r determine the number ℓ_i of real roots of $G(b_i,t)$.
7. Return $\max\{\ell_0,\ldots,\ell_r\}$.

Example 3. We consider the real parametrization

$$\mathcal{P}(t) = \left(\frac{1}{t\,(t^2-1)}, \frac{t^9 - 3\,t^7 + 3\,t^5 - t^3 + 1}{t\,(t^2-1)} \right).$$

$G(s,t) = t^3 - t - s^3 + s$. Thus, $\mathrm{index}(\mathcal{P}(t)) = 3$. The discriminant of G w.r.t. is $D(t) = (3\,s^2-4)\,(3\,s^2-1)^2$, and the real roots of $D(t)$ are

$$\left\{ -\frac{2}{3}\sqrt{3}, -\frac{1}{3}\sqrt{3}, \frac{1}{3}\sqrt{3}, \frac{2}{3}\sqrt{3} \right\}.$$

Therefore, we may take $b_0 = -2, b_1 = -1, b_2 = 0, b_3 = 1, b_4 = 2$. In this situation, one has that $\ell_0 = 1, \ell_1 = 3, \ell_2 = 3, \ell_3 = 3, \ell_4 = 1$. So we see that $\mathrm{index}_{\mathbb{R}}(\mathcal{P}(t)) = 3$. □

5 Tracing Index and Curve Degree

In this section we analyze how the tracing index of a parametrization behaves 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 $\mathcal{P}(t)$.

Definition. Let $R(t) = \frac{p(t)}{q(t)} \in \mathbb{K}(t)$ be a rational function in reduced form (i.e. $\gcd(p,q) = 1$). Then we define the *degree of* $R(t)$, denoted by $\deg_t(R)$, as

$$\deg_t(R(t)) = \max\{\deg_t(p(t)), \deg_t(q(t))\}.$$

Definition. Let $\mathcal{P}(t) = \left(\frac{\chi_{1,1}(t)}{\chi_{1,2}(t)}, \frac{\chi_{2,1}(t)}{\chi_{2,2}(t)}\right)$ be a rational parametrization. Then we define the *degree of* $\mathcal{P}(t)$, denoted by $\deg(\mathcal{P}(t))$, as

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

Remark.

(1) Note that $\deg(\mathcal{P}(t))$, the degree of $\mathcal{P}(t)$, is in general different from $\mathrm{index}(\mathcal{P}(t))$, the degree of the rational mapping $\mathcal{P}$ induced by $\mathcal{P}(t)$ (see Theorem 6). For instance, any proper rational 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 $\mathrm{index}(\mathcal{P}(t))$ for the degree of the rational map.

(2) The degree of a plane curve is defined as the total degree of its implicit equation. Note that the degree of a rational parametrization of a curve $\mathcal{C}$ does not always agree with the degree of $\mathcal{C}$. For instance, the parametrization $\left(t, \frac{1}{t}\right)$ has degree 1 but it defines the hyperbola $yx = 1$, whose degree is 2.

In order to study the behavior 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 $\mathbb{K}$ to $\mathbb{K}$ defined by $R(t)$.

Lemma 8. *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 $\mathrm{Card}(R^{-1}(a)) = \deg_t(R(t))$ for almost all $a \in \mathbb{K}$.*

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

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

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 $\mathcal{P}(t)$ 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 $\deg(\frac{\chi_{1,1}}{\chi_{1,2}}) = \deg_y(f)$, and $\deg(\frac{\chi_{2,1}}{\chi_{2,2}}) = \deg_x(f)$.

Example 4. We consider the rational quintic $\mathcal{C}$ defined by the polynomial $f(x, y) = y^5 + x^2y^3 - 3\,x^2y^2 + 3\,x^2y - x^2$. Theorem 5 ensures that any rational proper parametrization of $\mathcal{C}$ must have a first component of degree 5, and a second component of degree 2. It is easy to check that

$$\mathcal{P}(t) = \left(\frac{t^5}{t^2+1}, \frac{t^2}{t^2+1}\right)$$

properly parametrizes $\mathcal{C}$. Note that $f(\mathcal{P}(t)) = 0$, and that $\mathrm{index}(\mathcal{P}(t)) = 1$. □

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

Corollary. *Let $\mathcal{C}$ be a rational affine plane curve defined by the polynomial $f(x,y) \in \mathbb{K}[x,y]$. 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*

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

6 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 Cox et al, 1997). This approach is specially usefull for parametric varieties in $\mathbb{K}^n$. Also, for surfaces, different approaches can be found in González-Vega (1997), Sederberg et al (1997). However, for the case of plane curves, the implicit equation can be found by means of gcd's and resultants. For instance, applying Lemma 9, the defining polynomial of the curve parametrized 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. This result can be found in Sederberg et al (1997), or can be easily deduced from Lemma 9. 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. Similar results on implicitization can be found in Chionh and Goldman (1992) and Cox et al (1998).

Lemma 9. *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,*

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

The next result can be found in Sederberg et al (1997), or can be easily deduced from Lemma 9.

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*

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

We finish this section showing how Lemma 9, Theorem 7 and the notion of tracing index of a parametrization are related. Basically, the result follows from the next lemma on resultants.

Lemma 10. *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* $\deg(M - \beta N) = \deg(R)$ *for every root* β *of* $A(t)B(t)$*. 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'

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

Theorem 8 relates Theorem 7 and the tracing index.

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

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

We finish this section with an example that illustrates Theorem 8.

Example 5. We consider the quintic $\mathcal{C}$ of Example 4 and its parametrization

$$\mathcal{P}(t) = \left(\frac{(t^{10}+1)^5}{t^{20} + 2\,t^{10} + 2}, \frac{(t^{10}+1)^2}{t^{20} + 2\,t^{10} + 2} \right).$$

This new parametrization of $\mathcal{C}$ is obtained by reparametrizing the proper parametrization in Example 4 with the rational function $t^{10} + 1$. Thus, the index of the parametrization should be 10. In fact, $G(s,t) = t^{10} - s^{10}$. On the

other hand, computing the resultant w.r.t. t of the polynomials H_1 and H_2 one gets

$$Res_t(H_1(t,x),H_2(t,y)) = \left(y^5 + x^2y^3 - 3\,x^2y^2 + 3\,x^2y - x^2\right)^{10}$$

Appendix A.

Proof of Lemma 1. (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:

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

Therefore, since $\mathbb{K}$-automorphisms of $\mathbb{K}(t)$ are the invertible rational functions (see e.g. van der Waerden, 1953), one has that $L(t)$ is a linear rational function, and clearly $\mathcal{Q}(t) = \mathcal{P}(L(t))$.
Conversely, let L be 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. □

Proof of Lemma 2. 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. x. 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 $\mathrm{Card}(E) < \infty$. □

Proof of Theorem 1. 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 $\chi_{1,2}(\alpha)\chi_{2,2}(\alpha) \neq 0$, and $G_1(\alpha,t)$ has multiple roots, then the polynomial $\chi_{1,1}(t) - \frac{\chi_{1,1}(\alpha)}{\chi_{1,2}(\alpha)}\chi_{1,2}(t)$ also has multiple roots. But, by Lemma 2, this can only happen for finitely many values of α (note that $\chi_{1,1}, \chi_{1,2}$ are non-zero relatively prime polynomials). Similarly for $G_2(\alpha,t)$. Therefore, S is infinite.
Now, let us see that $\mathcal{P}^{-1}(\mathcal{P}(\alpha)) = \{\beta \in \mathbb{K} \mid \gcd(G_1(\alpha,t), G_2(\alpha,t))(\beta) = 0\}$.

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 $G_\alpha(t)$. So $\chi_{1,2}(\beta)\neq 0$, since otherwise it would imply that $\chi_{1,2}(\alpha)\chi_{1,1}(\beta)=0$, but $\chi_{1,2}(\alpha)\neq 0$ and hence $\chi_{1,1}(\beta)=0$, which is impossible because $\gcd(\chi_{1,1},\chi_{1,2})=1$. Similarly, $\chi_{2,2}(\beta)\neq 0$. Thus, $\beta\in\mathcal{P}^{-1}(P_\alpha)$.
Finally, 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. □

Proof of Lemma 3. 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 $\gcd(\varphi_a(f),\varphi_a(g))$, thus one has that $\deg(\gcd(\varphi_a(f),\varphi_a(g)))\geq \deg(\varphi_a(\gcd(f,g)))=\deg_y(\gcd(f,g))$.

(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 $\varphi_a(\bar{f})$ and $\varphi_a(\bar{g})$ 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. □

Proof of Lemma 4. 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 $G_1=\bar{G}_1\cdot G$, $G_2=\bar{G}_2\cdot G$, 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 $\alpha\in\mathbb{K}$, $\varphi_\alpha(G)=\gcd(\varphi_\alpha(G_1),\varphi_\alpha(G_2))$. In particular, for almost all $\alpha\in\mathbb{K}$,

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

On the other hand, by Lemma 3(1), $\deg_t(\gcd(\varphi_\alpha(G_1),\varphi_\alpha(G_2)))\geq\deg_t(G)$ for almost all $\alpha\in\mathbb{K}$. Thus, for almost all $\alpha\in\mathbb{K}$, $\deg_t(\gcd(\varphi_\alpha(G_1),\varphi_\alpha(G_2)))=\deg_t(G)$. □

Proof of Theorem 2. 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 $G(s,t)=G_2(s,t)$. 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 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 all points in $\mathcal{C}\setminus\mathcal{P}(\Omega)$ are generated by m parameter values. □

Proof of Lemma 6. Clearly, $G(s,t)$ is real. Let us assume that $G(s,t)$ is not square–free. Then, $G_1(s,t)$ and $G_2(s,t)$ are not square–free. Let us assume w.l.o.g. that the first component of the parametrization is not constant. For almost all $\alpha \in \mathbb{C}$ the polynomial $G_1(\alpha,t)$ has multiple roots, and $\chi_{1,2}(t), \chi_{2,2}(t)$ vanish only for finitely many values of α. Thus, for almost all $\alpha \in \mathbb{C}$ the polynomial $x_1(t) - \frac{\chi_{1,1}(\alpha)}{\chi_{1,2}(\alpha)}\chi_{1,2}(t)$ has multiple roots, which is impossible because of Lemma 2. □

Proof of Lemma 7. For almost all $\alpha \in (a_i, a_{i+1})$ it holds that $\mathrm{Card}(\mathcal{F}_{\mathcal{P}}^{\mathbb{R}}(\alpha))$ is the number of real affine intersections of $G(s,t)$ and $s = \alpha$. Thus, it is the number of different real roots of $G(\alpha,t)$. Now, by Lemma 5 and Lemma 6, $G(\alpha,t)$ is squarefree and the number of real roots of $G(\alpha,t)$ is invariant for all $\alpha \in (a_i, a_{i+1})$. In particular for $\alpha = b_i$. □

Proof of Lemma 8. 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, $\mathrm{Card}(R^{-1}(a)) = \deg(R(t))$ □

Proof of Theorem 4. 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. van der Waerden, 1953), one has that the degree of a composition of maps is the product of the degrees. Thus, applying Lemma 8, one concludes that $\mathrm{index}(\mathcal{Q}(t)) = \deg_t(R(t)) \cdot \mathrm{index}(\mathcal{P}(t))$. □

Proof of Theorem 5. 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 $\mathcal{P}(t) = (\frac{\chi_{1,1}(t)}{\chi_{1,2}(t)}, \lambda)$ 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, $\deg_t\left(\frac{\chi_{1,1}}{\chi_{1,2}}\right) = 1$, 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. In this situation, we prove that $\max\{\deg(\chi_{2,1}), \deg(\chi_{2,2})\} = \deg_x(f)$, and analogously one can prove that

$\max\{\deg(\chi_{1,1}), \deg(\chi_{1,2})\} = \deg_y(f)$. From these relations, we immediately 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 $\chi_{2,1}(t) - b\chi_{2,2}(t)$ has multiple roots,
(c) $lc(\chi_{2,1})/lc(\chi_{2,2})$, 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 $f(x, y)$.

First we show that $\mathcal{S}$ 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 $M(t) = \chi_{2,1}(t) - b\chi_{2,2}(t)$. 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 $\chi_{2,1}$ and $\chi_{2,2}$, we get that $\deg_x(f(x, y)) = \deg(M) = \max\{\deg(\chi_{2,1}), \deg(\chi_{2,2})\}$.
Conversely, let $\mathcal{P}(t)$ be a parametrization of the curve $\mathcal{C}$ 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), there exists $R(t) \in \mathbb{K}(t)$ such that $\mathcal{Q}(R(t)) = \mathcal{P}(t)$. Now, since $\mathcal{Q}(t)$ is a proper parametrization, one has 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, $R(t)$ is of degree 1, and hence R is invertible. Thus, by Lemma 1(2), $\mathcal{P}(t)$ is proper. □

Proof of Theorem 6. Lüroth's theorem guarantees the existence of 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, $\text{index}(\mathcal{P}(t)) = \deg_t(R(t)) \cdot \text{index}(\mathcal{P}'(t)) = \deg_t(R(t))$. 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,

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

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

Proof of Lemma 9. 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, note that the polynomials H_1, H_2 are irreducible because $\gcd(\chi_{1,1}, \chi_{1,2}) = \gcd(\chi_{2,1}, \chi_{2,2}) = 1$. 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 $\chi_{1,2}(t_0)\chi_{2,2}(t_0) \neq 0$. 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 $\chi_{1,2}(t_0)\chi_{2,2}(t_0) \neq 0$. 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 $\chi_{1,2}(t_0) \neq 0$ since otherwise it would imply that $\chi_{1,2}(t_0) = \chi_{1,1}(t_0) = 0$, which is impossible since $\gcd(\chi_{1,1}, \chi_{1,2}) = 1$. Similarly, $\chi_{2,2}(t_0) \neq 0$. 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 $h(x, y) = (h'(x, y))^r$. □

Proof of Lemma 10. 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 $\deg(M - b_i N) = \deg(R)$ for every $i \in \{1, \ldots, n\}$, 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 $r = \deg(R)$, then every root b_i of B generates r roots $\{b_{i,1}, \ldots, b_{i,r}\}$ 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 $M(\alpha) = 0$. But this is impossible because M and N are relatively prime. Therefore, one deduces that

$$b_i = \frac{M(b_{i,j})}{N(b_{i,j})} = R(b_{i,j}) \quad \text{for} \quad j = 1, \ldots, r.$$

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

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

□

Proof of Theorem 8. 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 $\mathcal{P}(t) = (\frac{\chi_{1,1}(t)}{\chi_{1,2}(t)}, a)$. Therefore,

$$Res_t(\chi_{1,2}(t)x - \chi_{1,1}(t), y - a) = (y - a)^{\deg(\mathcal{P})},$$

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 0 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 0 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 0. Now, observe that no numerator or denominator in $\mathcal{P}'(t+a)$ vanishes at 0. Therefore, one can always reparametrize the initial proper parametrization into a proper one, where degrees of numerator and denominator at each component agree.
Now, let

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

be a proper parametrization, in reduced form, of $\mathcal{C}$ where $\deg(\xi_{i,1}) = \deg(\xi_{i,2})$. By Lemma 1 there exists a non-constant rational function $R(t)$ such that $\mathcal{P}(t) = \mathcal{P}'(R(t)) = (\frac{\chi_{1,1}}{\chi_{1,2}}, \frac{\chi_{2,1}}{\chi_{2,2}})$. Let $R(t) = \frac{M(t)}{N(t)}$ be in reduced form. We consider the polynomials

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

and let

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

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

$$\bar{\xi}_{i,1}(t) = \sum_{j=1}^{n_i} a_{i,j}M(t)^j N(t)^{n_i - j}, \quad , \bar{\xi}_{i,2}(t) = \sum_{j=1}^{n_i} b_{i,j}M(t)^j N(t)^{n_i - j},$$

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

which result from $\xi_{i,1}, \xi_{i,2}, H_i^{\mathcal{P}'}$ by substituting $R(t)$ for t and clearing denominators. In order to apply Lemma 10 to the polynomials $H_1^{\mathcal{P}'}(t), H_2^{\mathcal{P}'}(t)$ and the rational function $R(t)$, let us see that $\deg(M(t) - \beta N(t)) = \deg(R)$ for every root β of $H_1^{\mathcal{P}'}(t) \cdot H_2^{\mathcal{P}'}(t)$. 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 $\gcd(\xi_{1,1}, \xi_{1,2}) \neq 1$ or $\gcd(\xi_{2,1}, \xi_{2,2}) \neq 1$, which is impossible. The application of Lemma 10 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 $\mathcal{P}(t) = \mathcal{P}'(R(t))$, we get

$$\xi_{j,1}(R(t)) \cdot \chi_{j,2}(t) = \chi_{j,1}(t) \cdot \xi_{j,2}(R(t)) \quad \text{for} \quad j = 1, 2.$$

Thus,

$$\chi_{j,1}(t) \cdot H_j^{\mathcal{P}'}(R(t)) = \xi_{j,1}(R(t)) \cdot H_j^{\mathcal{P}}(t) \quad \text{for} \quad j = 1, 2,$$

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

$$\chi_{j,1}(t)\bar{H}_j^{\mathcal{P}'}(t) = \bar{\xi}_{j,1}(t)H_j^{\mathcal{P}}(t) \quad \text{for} \quad j = 1, 2,$$

$$\chi_{j,1}(t)\bar{\xi}_{j,2}(t) = \bar{\xi}_{j,1}(t)\chi_{j,2}(t) \quad \text{for} \quad j = 1, 2.$$

Now, we prove $\gcd(\chi_{1,1}, \chi_{2,1}) = \gcd(\bar{\xi}_{1,1}, \bar{\xi}_{2,1})$. Indeed: $\gcd(\chi_{1,1}, \chi_{2,1})$ divides $\bar{\xi}_{j,1} \cdot \chi_{j,2}$, and since $\gcd(\chi_{j,1}, \chi_{j,2}) = 1$ one has that $\gcd(\chi_{1,1}, \chi_{2,1})$ divides $\bar{\xi}_{j,1}$. Thus $\gcd(\chi_{1,1}, \chi_{2,1})$ divides $\gcd(\bar{\xi}_{1,1}, \bar{\xi}_{2,1})$. In order to prove that $\gcd(\bar{\xi}_{1,1}, \bar{\xi}_{2,1})$ divides $\gcd(\chi_{1,1}, \chi_{2,1})$, we first see that $\gcd(\bar{\xi}_{j,1}, \bar{\xi}_{j,2}) = 1$. Let a be a common root of $\bar{\xi}_{j,1}$ and $\bar{\xi}_{j,2}$. Note that by definition of $\bar{\xi}_{j,1}$ it follows that $N(a) \neq 0$, since otherwise we would have $M(a) = 0$. But this is impossible because M and N are relatively prime. Therefore, taking into account that $\bar{\xi}_{j,1} = N^{n_j}\xi_{j,1}(R)$, $\bar{\xi}_{j,2} = N^{k_j}\xi_{j,2}(R)$, one deduces that $\xi_{j,1}(R(a)) = \xi_{j,2}(R(a)) = 0$ which is impossible since $\gcd(\xi_{j,1}, \xi_{j,2}) = 1$. Now, since $\gcd(\bar{\xi}_{1,1}, \bar{\xi}_{2,1})$ divides $\chi_{j,1} \cdot \bar{\xi}_{j,2}$, from $\gcd(\bar{\xi}_{j,1}, \bar{\xi}_{j,2}) = 1$ we deduce that $\gcd(\bar{\xi}_{1,1}, \bar{\xi}_{2,1})$ divides $\gcd(\chi_{1,1}, \chi_{2,1})$.
As a consequence of this remark the equalities above can be expressed as:

$$\chi_{j,1}^*(t)\bar{H}_j^{\mathcal{P}'}(t) = \bar{\xi}_{j,1}^*(t)H_j^{\mathcal{P}}(t) \quad \text{for} \quad j = 1, 2,$$

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

where $\gcd(\chi^*_{1,1}, \chi^*_{2,1}) = \gcd(\bar{\xi}^*_{1,1}, \bar{\xi}^*_{2,1}) = 1$. Therefore,

$$Res_t(\chi^*_{1,1}\bar{H}_1^{\mathcal{P}'}, \chi^*_{2,1}\bar{H}_2^{\mathcal{P}'}) = Res_t(\bar{\xi}^*_{1,1}H_1^{\mathcal{P}}, \bar{\xi}^*_{2,1}H_2^{\mathcal{P}}).$$

So,

$$Res_t(\chi^*_{1,1}, \chi^*_{2,1}) \cdot Res_t(\chi^*_{1,1}, \bar{H}_2^{\mathcal{P}'}) \cdot Res_t(\bar{H}_1^{\mathcal{P}'}, \chi^*_{2,1}) \cdot Res_t(\bar{H}_1^{\mathcal{P}'}, \bar{H}_2^{\mathcal{P}'}) =$$

$$= Res_t(\bar{\xi}^*_{1,1}, \bar{\xi}^*_{2,1}) \cdot Res_t(\bar{\xi}^*_{1,1}, H_2^{\mathcal{P}}) \cdot Res_t(H_1^{\mathcal{P}}, \bar{\xi}^*_{2,1}(t)) \cdot Res_t(H_1^{\mathcal{P}}, H_2^{\mathcal{P}}).$$

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, $H_i^{\mathcal{P}}(a) = 0$ but this implies that $\gcd(\chi_{i,1}, \chi_{i,2}) \neq 1$, 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 $\gcd(\xi_{i,1}, \xi_{i,2}) \neq 1$ which is impossible.
Taking into account this fact and that $\gcd(\chi^*_{1,1}, \chi^*_{2,1}) = \gcd(\bar{\xi}^*_{1,1}, \bar{\xi}^*_{2,1}) = 1$, 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 10 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 9 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 we get

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

□

References

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.

Andradas C., Recio T., Sendra J.R., 1997. A Relatively Optimal Reparametrization Algorithm. In: W.W. Küchlin (ed.), Proc. ISSAC'97, 349-356, ACM Press.

Andradas C., Recio T., Sendra J.R., 1999. Base field restriction techniques for parametric curves. In: S. Dooley (ed.), Proc. ISSAC'99, 17-22, ACM Press.

Arrondo E., Sendra J., Sendra J.R., 1997. Parametric Generalized Offsets to Hypersurfaces. J. of Symbolic Computation vol. 23, 267-285.

Bini P., Dario A., Fiorentino G., 2000. Design, analysis, and implementation of a multiprecision polynomial rootfinder. Numer. Algorithms vol. 23 no. 2–3, pp. 127–173.

Chionh E.-W., Goldman R.N., 1992. Using multivariate resultants to find the implicit equation of a rational surface. The Visual Computer vol. 8, pp. 171–180.

Collins G., 1975. Quantifier Elimination for Real Closed Fields by Cylindrical Algebraic Decomposition, in: H. Brakhage (ed.), Automata Theory and Formal Languages, Lectures Notes in Computer Science, vol. 33, 134–183, Springer Verlag.

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

Cox D.A., Sederberg T.W., Chen F., 1998. The moving line ideal basis of planar rational curves. Computer Aided Geometric Design vol. 8, pp. 803–827.

Gao X.-S., Chou S.-C., 1992. Implicitization of Rational Parametric Equations. J. Symbolic Computation vol. 14, pp. 459–470.

González-Vega L. (1997), Implicitization of Parametric Curves and Surfaces

by using Multidimensional Newton Formulae. J. Symbolic Computation vol. 23, pp. 137-152.

Harris J., 1995. Algebraic Geometry. A First Course. Springer-Verlag.

van Hoeij M., 1994. Computing Parametrizations of Rational Algebraic Curves. In: J. von zur Gathen, M. Giesbrecht (eds.), Proc. ISSAC'94, ACM Press, 187-190.

van Hoeij M., 1997. Rational Parametrizations of Curves Using Canonical Divisors. J. of Symbolic Computation vol. 23, 209-227.

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

Hoffmann C.M., Sendra J.R., Winkler F., 1997. Parametric Algebraic Curves and Applications. Special issue, J. of Symbolic Computation 23/2& 3.

Hoschek J., Lasser D., 1993. Fundamentals of Computer Aided Geometric Design. A.K. Peters Wellesley MA., Ltd.

Recio T., Sendra J.R., 1997. Real Reparametrizations of Real Curves. J. Symbolic Computation vol. 23, 241–254.

Schicho J., 1992. On the Choice of Pencils in the Parametrization of Curves. J. of Symbolic Computation vol. 14, 557-576.

Sederberg T.W., 1986. Improperly Parametrized Rational Curves. Computer Aided Geometric Design 3, 67-75.

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.

Sendra J.R., Winkler F., 1991. Symbolic Parametrization of Curves. J. Symbolic Computation vol. 12/ 6, pp. 607-631.

Sendra J.R., Winkler F., 1997. Parametrization of Algebraic Curves over Optimal Field Extensions. J. Symbolic Computation vol. 23, 191-207.

Sendra J.R., Winkler F., 2001. Computing the degree of rational maps between curves. Proc. of ISSAC'2001, ACM Press (To appear).

Shafarevich, I.R., 1994. Basic Algebraic Geometry 1; Varieties in Projective Space. Springer-Verlag, Berlin New York.

van der Waerden, B.L., 1953. Modern Algebra, vol. 1. Frederick Ungar Publ.Co., New York.

Walker, R.J., 1950. Algebraic Curves. Princeton University Press.

Winkler F., 1996. Polynomial Algorithms in Computer Algebra. Springer-Verlag Wien New York.

Zippel R., 1991. Rational Function Decomposition. In: S.M. Watt (ed.), Proc. of ISSAC'91, 1-6, ACM Press.