Advances in Algebraic Geometric Computation

Franz Winkler *
RISC-Linz, J. Kepler University Linz, A-4040 Austria
Franz.Winkler@risc.uni-linz.ac.at

Keywords: computer algebra, algebraic curves and surfaces, computer aided geometric design

Mathematics Subject Classification: 14H25, 14J20, 14J26, 68Q40

Abstract

Algebraic curves and surfaces play an important and ever increasing role in computer aided geometric design, computer vision, and computer aided manufacturing. Consequently, theoretical results need to be adapted to practical needs. We need efficient algorithms for generating, representing, manipulating, analyzing, rendering algebraic curves and surfaces. In the last years there has been dramatic progress in all areas of algebraic computation. In particular, the application of computer algebra to the design and analysis of algebraic curves and surfaces has been extremely successful. In this lecture we report on some of these developments.

One interesting subproblem in algebraic geometric computation is the rational parametrization of curves and surfaces. The tacnode curve defined by $f(x,y) = 2x^4 - 3x^2y + y^4 - 2y^3 + y^2$ in the real plane has the rational parametrization

$$x(t) = \frac{t^3 - 6t^2 + 9t - 2}{2t^4 - 16t^3 + 40t^2 - 32t + 9}, \quad y(t) = \frac{t^2 - 4t + 4}{2t^4 - 16t^3 + 40t^2 - 32t + 9}$$

over $\mathbb{Q}$. The criterion for parametrizability is the genus. Only curves of genus 0 have a rational parametrization, and only surfaces of arithmetic genus 0 and second plurigenus 0 have a rational parametrization. Conversely, given a parametric representation of a curve or surface, we might ask for the implicit algebraic equation defining it.

Computing parametrizations essentially requires the full analysis of singularities (either by successive blow-ups, or by Puiseux expansion) and the determination of regular points on the curve or surface. We can control the quality of the resulting parametrization by controlling the field over which we choose this regular point. Thus, finding a regular curve point over a minimal field extension on a curve of genus 0 is one of the central problems in rational parametrization of curves, compare [SeWi97]. Similarly, finding rational curves on surfaces leads to parametrizations,

*The author wants to acknowledge support from the Austrian *Fonds zur Förderung der wissenschaftlichen Forschung (FWF)* under project SFB F013/1304.

compare [LSWH00]. The quality of parametrizations can be measured by the necessary field extension and also by the number of times the variety is traced by the parametrization. We will analyze the relation of the tracing index of a curve to the degrees of the implicit equation and the degree of the parametrization, compare [SeWi01].

1 Parametrization of Algebraic Curves

Algebraic curves and surfaces have been studied intensively in algebraic geometry for decades and even centuries. Thus, there exists a huge amount of theoretical knowledge about these geometric objects. Recently, algebraic curves and surfaces play an important and ever increasing role in computer aided geometric design, computer vision, and computer aided manufacturing. Consequently, theoretical results need to be adapted to practical needs. We need efficient algorithms for generating, representing, manipulating, analyzing, rendering algebraic curves and surfaces. Such efficient symbolic algorithms can be constructed based on method of computer algebra as described, for instance, in [Wink96].

One interesting subproblem is the rational parametrization of curves and surfaces.

Definition 1.1. Let $\mathbb{K}$ be an algebraically closed field of characteristic 0. Consider an affine plane algebraic curve $\mathcal{C}$ in $\mathbb{A}^2(\mathbb{K})$ defined by the bivariate polynomial $f(x, y) \in \mathbb{K}[x, y]$, i.e.

$$\mathcal{C} = \{(a, b) \mid (a, b) \in \mathbb{A}^2(\mathbb{K}) \text{ and } f(a, b) = 0\}.$$

Of course, we could also view this curve in the projective plane $\mathbb{P}^2(\mathbb{K})$, defined by $F(x, y, z)$, the homogenization of $f(x, y)$. We denote the field of rational function over $\mathcal{C}$ by $\mathbb{K}(\mathcal{C})$.

A pair of rational functions $\mathcal{P} = (x(t), y(t)) \in \mathbb{K}(t)$ is a *rational parametrization* of the curve $\mathcal{C}$, if and only if $f(x(t), y(t)) = 0$ and for almost every point $(x_0, y_0) \in \mathcal{C}$ (i.e. up to finitely many exceptions) there is a parameter value $t_0 \in \overline{K}$ such that $(x_0, y_0) = (x(t_0), y(t_0))$.

Only irreducible curves, i.e. curves whose defining polynomials are absolutely irreducible, can have a rational parametrization. Almost any rational transformation of a rational parametrization is again a rational parametrization, so such parametrizations are not unique.

Implicit representations (by defining polynomial) and parametric representations (by rational parametrization) both have their particular advantages and disadvantages. Given an implicit representation of a curve and a point in the plane, it is easy to check whether the point is on the curve. But it is hard to generate "good" points on the curve, i.e. for instance points with rational coordinates if the defining field is $\mathbb{Q}$. On the other hand, generating good points is easy for a curve given parametrically, but deciding whether a point is on the curve requires the solution of a system of algebraic equations. So it is highly desirable to have efficient algorithms for changing from implicit to parametric representation, and vice versa.

Example 1.1: Let us consider curves in the plane (affine or projective) over $\mathbb{C}$. The curve defined by $f(x,y) = y^2 - x^3 - x^2$ (see Fig. 1.1) is rationally parametrizable, and actually a parametrization is $(t^2-1, t(t^2-1))$.

On the other hand, the elliptic curve defined by $f(x,y) = y^2 - x^3 + x$ (see Fig 1.2) does not have a rational parametrization.

The tacnode curve (see Fig. 1.3) defined by $f(x,y) = 2x^4 - 3x^2y + y^4 - 2y^3 + y^2$ has the parametrization

$$x(t) = \frac{t^3 - 6t^2 + 9t - 2}{2t^4 - 16t^3 + 40t^2 - 32t + 9}, \quad y(t) = \frac{t^2 - 4t + 4}{2t^4 - 16t^3 + 40t^2 - 32t + 9}.$$

The criterion for parametrizability of a curve is its genus. Only curves of genus 0, i.e. curves having as many singularities as their degree permits, have a rational parametrization.

Also the cardioid curve (see Fig. 1.4) can be rationally parametrized over $\mathcal{Q}$. $\square$

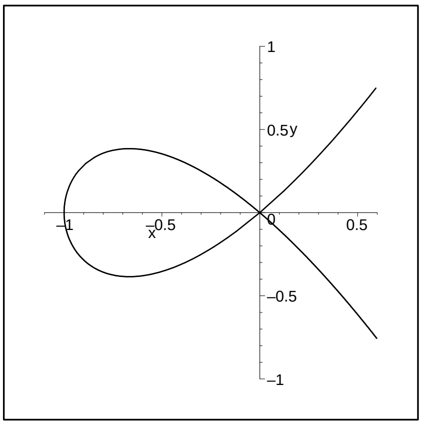

Fig. 1.1

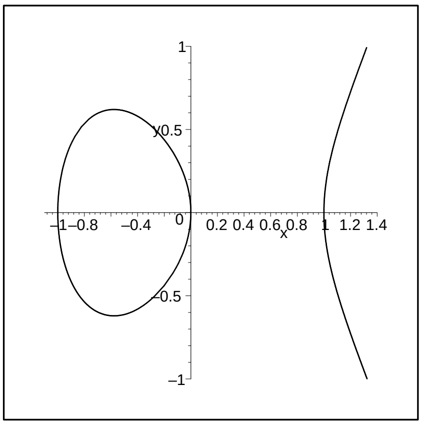

Fig. 1.2

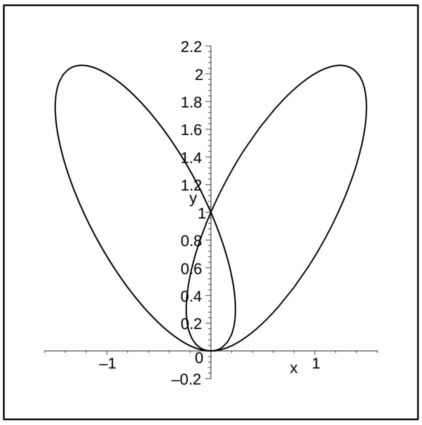

Fig. 1.3

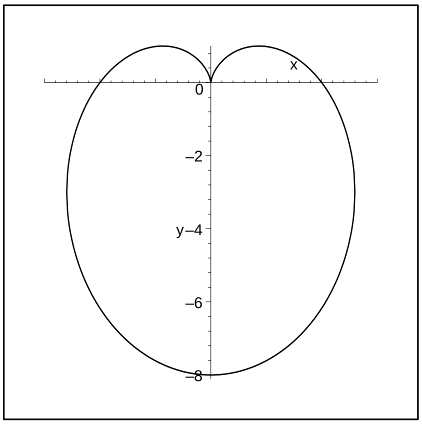

Fig. 1.4

In [SeWi91] Sendra and Winkler have developed a fully symbolic algorithm for solving the parametrization problem of algebraic curves. Computing such a parametrization essentially requires the full analysis of singularities (either by successive blow-ups, or by Puiseux expansion) and the determination of a regular point on the curve. We can control the quality of the resulting parametrization by controlling the field over which we choose this regular point. Thus, finding a regular curve point over a minimal field extension on a curve of genus 0 is one of the central problems in rational parametrization, compare [SeWi97], [SeWi99]. The determination of rational points on algebraic curves can be an extremely complicated problem. But for curves of genus 0 the situation can actually be controlled very well. For a curve over $\mathbb{Q}$ or $\mathbb{R}$ we can determine whether the curve has a regular point over this field, or otherwise find a quadratic field extension which admits such a regular point.

Example 1.2: Let $\mathcal{C}$ be the cardioid curve in the complex plane defined by

$$f(x,y) = (x^2 + 4y + y^2)^2 - 16(x^2 + y^2) = 0.$$

For a picture of this curve in the real affine plane see Fig. 1.4.

The curve $\mathcal{C}$ has the following rational parametrization:

$$\begin{aligned} x(t) &= -32 \cdot \frac{-1024i + 128t - 144it^2 - 22t^3 + it^4}{2304 - 3072it - 736t^2 - 192it^3 + 9t^4}, \\ y(t) &= -40 \cdot \frac{1024 - 256it - 80t^2 + 16it^3 + t^4}{2304 - 3072it - 736t^2 - 192it^3 + 9t^4}. \end{aligned}$$

As we see in Fig. 1.4, $\mathcal{C}$ has infinitely many real points. But generating any one of these real points from the above parametrization is not obvious. Does this real curve $\mathcal{C}$ also have a parametrization over $\mathbb{R}$? Indeed it does, let's see how we can get one.

In the projective plane over $\mathbb{C}$, $\mathcal{C}$ has three double points, namely $(0:0:1)$ and $(1:\pm i:0)$. Let $\tilde{\mathcal{H}}$ be the linear system of conics passing through all these double points. The system $\tilde{\mathcal{H}}$ has dimension 2 and is defined by

$$h(x,y,z,s,t) = x^2 + sxz + y^2 + tyz = 0,$$

i.e., for any particular values of s and t we get a conic in $\tilde{\mathcal{H}}$. Three elements of this linear system define a birational transformation

$$\begin{aligned} \mathcal{T} &= (h(x,y,z,0,1) : h(x,y,z,1,0) : h(x,y,z,1,1)) \\ &= (x^2 + y^2 + yz : x^2 + xz + y^2 : x^2 + xz + y^2 + yz) \end{aligned}$$

which transforms $\mathcal{C}$ to the conic $\mathcal{D}$ defined by

$$15x^2 + 7y^2 + 6xy - 38x - 14y + 23 = 0.$$

For a conic defined over $\mathbb{Q}$ we can decide whether it has a point over $\mathbb{Q}$ or $\mathbb{R}$. In particular, we determine the point $(1, 8/7)$ on $\mathcal{D}$, which, by $\mathcal{T}^{-1}$, corresponds to the regular point $P = (0, -8)$ on $\mathcal{C}$. Now, by restricting $\tilde{\mathcal{H}}$ to conics through P and intersecting $\tilde{\mathcal{H}}$ with $\mathcal{C}$ (for details see [SeWi97]), we get the parametrization

$$x(t) = \frac{-1024t^3}{256t^4 + 32t^2 + 1}, \quad y(t) = \frac{-2048t^4 + 128t^2}{256t^4 + 32t^2 + 1}.$$

over the reals. $\square$

An alternative approach to the problem of parametrization of curves can be found in [Hoeij94].

Now that we have seen some examples of the parametrization problem treated by symbolic algebraic computation, let us just briefly discuss the inverse problem, namely the problem of implicitization. If we are given, for instance, a rational parametrization in $K(t)$ of a plane curve, i.e.

$$x(t) = p(t)/r(t), \quad y(t) = q(t)/r(t),$$

we essentially want to eliminate the parameter t from these relations, and get a relation just between x and y. We also want to make sure that we do not consider components for which the denominator $r(t)$ vanishes. This leads to the system of algebraic equations

$$\begin{aligned} x \cdot r(t) - p(t) &= 0, \\ y \cdot r(t) - q(t) &= 0, \\ r(t) \cdot z - 1 &= 0. \end{aligned}$$

The implicit equation of the curve must be the generator of the ideal

$$I = \langle x \cdot r(t) - p(t), y \cdot r(t) - q(t), r(t) \cdot z - 1 \rangle \;\cap\; K[x, y].$$

Using the elimination property of Gröbner bases, we can compute this generator by a Gröbner basis computation w.r.t. the lexicographic ordering based on $x < y < z < t$.

Example 1.3: Let us do this for the curve of Example 1.2. We start from the parametrization

$$x(t) = \frac{-1024t^3}{256t^4 + 32t^2 + 1}\,, \quad y(t) = \frac{-2048t^4 + 128t^2}{256t^4 + 32t^2 + 1}\,.$$

So we have to solve the equations

$$\begin{aligned} x \cdot (256t^4 + 32t^2 + 1) + 1024t^3 &= 0, \\ y \cdot (256t^4 + 32t^2 + 1) + 2048t^4 - 128t^2 &= 0, \\ (256t^4 + 32t^2 + 1) \cdot z - 1 &= 0. \end{aligned}$$

The Gröbner basis of this system w.r.t. the lexicographic ordering based on $x < y < z < t$ is

$$G = \{........, x^4 + y^4 + 8x^2y + 2x^2y^2 + 8y^3 - 16x^2\}.$$

So we have found the implicit equation of the curve. $\square$

2 Parametrization of Algebraic Surfaces

Many of these ideas which work for curves can actually be generalized to higher dimensional geometric objects. For instance, one subproblem in computer aided geometric design is the manipulation of offset curves, offset surfaces, pipe and canal surfaces. These are geometric objects keeping certain distances from a generating object. Let us just consider the case of a pipe surface in an example.

Example 2.1: We consider the space curve $\mathcal{C}$ in $\mathbb{A}^2(\mathbb{R})$ given parametrically by $(x(t), y(t), z(t)) = (t, t^2, t^3)$. We want to construct a parametric representation of the pipe surface $\mathcal{S}$ (at distance 1) along $\mathcal{C}$, i.e. the locus of points having normal distance 1 from $\mathcal{C}$. This pipe surface $\mathcal{S}$ is the envelope of spheres of radius 1 moving along $\mathcal{C}$, i.e. every point on $\mathcal{S}$ lies on a circle in a hypersurface perpendicular to the curve $\mathcal{C}$. If we can find a parametric representation of a curve $\tilde{\mathcal{C}}$ on $\mathcal{S}$, which meets every one of these circles, then by a pencil of lines in the corresponding hypersurface we can generate a rational representation for all the points on this circle, and thus finally a rational parametrization of the pipe surface.

Such a curve can by determined by algebraic computation, giving for instance the parametrization $(\tilde{c}_1(t), \tilde{c}_2(t), \tilde{c}_3(t))$ with

$$\begin{pmatrix} \tilde{c}_1(t) \\ \tilde{c}_2(t) \\ \tilde{c}_3(t) \end{pmatrix} = \begin{pmatrix} t + \frac{3(36t^4 - 13t^2 - 4\sqrt{5}t - 5)t^2}{(1+4t^2)(21t^2+2\sqrt{5}t+5+27t^4)} \\ t^2 - \frac{3(60t^3+14t-\sqrt{5}+4\sqrt{5}t^2)t^2}{(1+4t^2)(21t^2+2\sqrt{5}t+5+27t^4)} \\ t^3 + \frac{21t^2+2\sqrt{5}t+5}{21t^2+2\sqrt{5}t+5+27t^4} \end{pmatrix}.$$

From this parametric representation of $\tilde{\mathcal{C}}$ we can compute a parametric representation of the pipe surface. □

For a geometric approach to parametrization of pipe and canal surfaces see [PePo97], an algebraic approach can be found in [LSWH00].

In [PeSe01] Pérez-Díaz and Sendra have developed symbolic algorithms for the computation of parametric blending surfaces. There are various special kinds of surfaces such as pipe and canal surfaces or blending surfaces, which are of particular importance in computer aided geometric design. Special techniques for these important types of surfaces are available.

But there is also the general problem of rational parametrization of surfaces, i.e. of deciding whether an algebraic surface $\mathcal{S}$ can be rationally parametrized and if so computing a parametrization. This problem is more or less solved, we refer to the excellent description by Schicho in [Schi98]. The theorem by Enriques and Manin states that a rational surface either contains a pencil of rational curves or is equivalent to a Del Pezzo surface. In the first case, a rational parametrization over $\mathbb{C}$ or $\mathbb{R}$ can be computed from the pencil of rational curves. In the second case, parametrization algorithms are known over the ground field $\mathbb{C}$, but the problem is still open over $\mathbb{R}$ or $\mathbb{Q}$. By the method of adjoints the theorem of Enriques and Manin can be turned into a constructive algorithm. This requires a full resolution of the singularities of the surface $\mathcal{S}$. The existence of resolution has been demonstrated by Walker and Zariski for surfaces, and by Hironaka for general hypersurfaces. But Hironaka's proof is inconstructive. A first constructive proof has been given by Villamayor in [Villa89]. Schicho has turned this into a recursive algorithm and implemented it in the computer algebra system Maple, see [BoSc00].

Example 2.2. (From [Schi98]) The algebraic surface $\mathcal{S}$ defined by

$$f(x, y, z) = x^4 + z^4 + (xy + z^2)^3 = 0$$

can be parametrized as

$$\mathcal{P}(s, t) = \frac{1}{s^5 + s} \cdot \left(-s^2t^3,\ t^3 + s^4t + t,\ -st^3\right).$$

On the other hand, if we start from the parametrization $\mathcal{P}$ and compute the Gröbner basis for

$$\{x \cdot (s^5 + s) + s^2t^3,\ y \cdot (s^5 + s) - t^3 - s^4t - t,\ z \cdot (s^5 + s) + st^3,\ (s^5 + s) \cdot w - 1\}$$

w.r.t. the lexicographic ordering based on $x < y < z < w < s < t$, we get

$$\{......., \ x^4 + z^4 + (xy + z^2)^3\}.$$

So we have found the implicit equation of the surface $\mathcal{S}$.

3 Tracing Index of Curve Parametrizations

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 [AnRS97], [AnRS99], [Hoeij97], [Schi92], [SeWi97]). 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, e.g. [AbBa88], [Hoeij94], [SeWi91], provide proper parametrizations. Furthermore, improperness can be detected algorithmically, and the given parametrization can be reparametrized into a proper one [Sede86]. Proper parametrizations play an important role in many practical applications in computer aided geometric design, such as in visualization or rational parametrization of offsets.

For a parametrization $\mathcal{P}(t)$ of a curve $\mathcal{C}$ over $\mathbb{K}$ we write its components as

$$\mathcal{P}(t) = (x(t), y(t)) = \left(\frac{x_1(t)}{x_2(t)}, \frac{y_1(t)}{y_2(t)}\right).$$

We will assume in the sequel that rational parametrizations are given in reduced form, that is $\gcd(x_1(t), x_2(t)) = \gcd(y_1(t), y_2(t)) = 1$. Furthermore, for a given parametrization $\mathcal{P}(t)$ we consider the polynomials

$$G_1(s,t) = x_1(s)x_2(t) - x_2(s)x_1(t), \quad G_2(s,t) = y_1(s)y_2(t) - y_2(s)y_1(t),$$

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

$$H_1(t,x) = xx_2(t) - x_1(t), \quad H_2(t,y) = yy_2(t) - y_1(t).$$

We start by recalling some basic results on proper parametrizations. A parametrization $\mathcal{P}(t)$ of the curve $\mathcal{C}$ 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.

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.

Theorem 3.1 *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 $\mathcal{Q}(t) = \mathcal{P}(L(t))$.

In [SeWi01a] we have investigated computational problems for such rational maps between algebraic curves. In [SeWi01b] we have introduced the notion of the tracing index of a rational parametrization. Here we summarize the essential facts.

Theorem 3.2. *Let $\mathcal{P}(t) = (x(t), y(t))$ be a parametrization with non-constant components in reduced form. Then*

(1) *for $\alpha \in \mathbb{K}$ such that $x_2(\alpha)y_2(\alpha) \neq 0$, and such that $G_1(\alpha, t)$, $G_2(\alpha, t)$ do not have multiple roots,*
$\mathrm{Card}(\mathcal{P}^{-1}(\mathcal{P}(\alpha))) = \deg_t(\gcd(G_1(\alpha, t), G_2(\alpha, t)))$;

(2) *for all but finitely many values α of s we have*
$\deg_t(G(s, t)) = \deg_t(\gcd(G_1(\alpha, t), G_2(\alpha, t)))$;

(3) *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 3.1. 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 $\mathrm{index}(\mathcal{P}(t))$, if all but finitely many points on $\mathcal{C}$ are generated, via $\mathcal{P}(t)$, by k parameter values; i.e. $\mathrm{index}(\mathcal{P}(t))$ represents the number of times that $\mathcal{P}(t)$ traces $\mathcal{C}$.

Note that by Theorem 3.2(3) $\mathrm{index}(\mathcal{P}(t)) = \deg_t(G(s, t))$. Also, the tracing index can be computed by Theorem 3.2(1).

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, $\mathrm{index}(\mathcal{P}(t))$ 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; i.e. $\mathrm{index}(\mathcal{P}(t)) = [\mathbb{K}(t) : \varphi_{\mathcal{P}}(\mathbb{K}(\mathcal{C}))]$.

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 3.3. *A rational parametrization is proper if and only if its tracing index is 1; i.e. if and only if $\deg_t(G(s, t)) = 1$.*

Example 3.1. 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 this case we have

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

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

Let $\mathcal{P}(t) = \left(\frac{x_1(t)}{x_2(t)}, \frac{y_1(t)}{y_2(t)} \right)$ be a rational parametrization. Then we define the *degree of* $\mathcal{P}(t)$, denoted by $\deg(\mathcal{P}(t))$, as

$$\deg(\mathcal{P}(t)) = \max \left\{ \deg_t \left(\frac{x_1(t)}{x_2(t)} \right), \deg_t \left(\frac{y_1(t)}{y_2(t)} \right) \right\}.$$

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 remark after Def. 3.1). For instance, any proper rational parametrization of a circle has degree 2 but its index is 1 because it is proper. 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.

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 [SeWi01b] the following theorem is proved.

Theorem 3.4. *Let $\mathcal{C}$ be a rational affine curve defined over $\mathbb{K}$ by the polynomial $f(x,y) \in \mathbb{K}[x,y]$, let $\mathcal{P}(t) = \left(\frac{x_1(t)}{x_2(t)}, \frac{y_1(t)}{y_2(t)}\right)$ be a rational parametrization of $\mathcal{C}$, and let $n = \max\{\deg_x(f), \deg_y(f)\}$. Then*

(1) $\mathcal{P}(t)$ is proper if and only if $\deg(\mathcal{P}(t)) = n$. Furthermore, if $\mathcal{P}(t)$ is proper, then $\deg(\frac{x_1}{x_2}) = \deg_y(f)$, and $\deg(\frac{y_1}{y_2}) = \deg_x(f)$;

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

(3) $Res_t(H_1(t,x), H_2(t,y)) = c \cdot (f(x,y))^{\mathrm{index}(\mathcal{P})}$, for some non-zero constant c.

Example 3.2. 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 3.4(1) 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 $\mathrm{index}(\mathcal{P}(t)) = 1$.

On the other hand, we consider the parametrization

$$\mathcal{P}'(t) = \left(\frac{(t^{10}+1)^5}{t^{20}+2\,t^{10}+2}, \frac{(t^{10}+1)^2}{t^{20}+2\,t^{10}+2}\right)$$

of the quintic $\mathcal{C}$. This new parametrization $\mathcal{C}'$ of $\mathcal{C}$ is obtained by reparametrizing the proper parametrization $\mathcal{P}$ with the rational function $t^{10}+1$, i.e. $\mathcal{P}' = \mathcal{P}(t^{10}+1)$. 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

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

Conclusion

In this paper we have considered the problem of rational parametrization of algebraic curves and surfaces over an algebraically closed field of characteristic 0, and also the inverse problem of implicitizing a rational parametrization. We have seen that in the last decade many efficient algorithms have been developed for treating these problems in a symbolic algebraic way. Such rational parametrizations are of importance in computer aided geometric design, e.g. for determining surface-to-surface intersections or offsets and blendings, but also for solving diophantine problems and determining rational points on curves and surfaces, see [PoVo00]. For fields of positive characteristic the situation is much less satisfactory, and efficient algorithms need to be developed.

References

[AbBa88] S.S. Abhyankar, C.L. Bajaj, "Automatic Parametrization of Rational Curves and Surfaces III: Algebraic Plane Curves", *Computer Aided Geometric Design* 5, 309-321 (1988).

[AnRS97] C. Andradas, T. Recio, J.R. Sendra, "A Relatively Optimal Reparametrization Algorithm", in *Proc. ISSAC'97*, W.W. Küchlin (ed.), 349-356, ACM Press (1997).

[AnRS99] C. Andradas, T. Recio, J.R. Sendra, "Base Field Restriction Techniques for Parametric Curves", in *Proc. ISSAC'99*, S. Dooley (ed.), 17-22, ACM Press (1999).

[BoSc00] G. Bodnár, J. Schicho, "A Computer Program for the Resolution of Singularities", *Progress in Math.* 181, 231–238 (2000).

[Hoeij94] M. van Hoeij, "Computing Parametrizations of Rational Algebraic Curves", in *Proc. ISSAC'94*, J. von zur Gathen and M. Giesbrecht (eds.), ACM Press, 187–190 (1994).

[Hoeij97] M. van Hoeij M., "Rational Parametrizations of Curves Using Canonical Divisors", *J. of Symbolic Computation* 23, 209-227 (1997).

[LSWH00] G. Landsmann, J. Schicho, F. Winkler, E. Hillgarter, "Symbolic Parametrization of Pipe and Canal Surfaces", *Proc. ISSAC'00*, 202–208, C. Traverso (ed.), ACM Press (2000).

[LaSW01] G. Landsmann, J. Schicho, F. Winkler, "The Parametrization of Canal Surfaces and the Decomposition of Polynomials into a Sum of Two Squares", *J. Symbolic Computation* 32/1&2, 119–132 (2001).

[PeSe01] S. Pérez-Díaz, R. Sendra, "Parametric G^1–Blending of Several Surfaces", *Computer Algebra in Scientific Computing – CASC'2001*, V.G. Ganzha, E.W. Mayr, E.V. Vorozhtsov (eds.), 445–459, Springer-Verlag (2001).

[PePo97] M. Peternell, H. Pottmann, “Computing Rational Parametrizations of Canal Surfaces”, *J. Symbolic Computation* 23/2&3, 255–266 (1997).

[PoVo00] D. Poulakis, E. Voskos, “On the Practical Solution of Genus Zero Diophantine Equations”, *J. Symbolic Computation* 30/5, 573–582 (2000).

[Schi92] J. Schicho, “On the Choice of Pencils in the Parametrization of Curves”, *J. of Symbolic Computation* 14, 557-576 (1992).

[Schi98] J. Schicho, “Rational Parametrization of Surfaces”, *J. Symbolic Computation* 26/1, 1–29 (1998).

[Sede86] T.W. Sederberg, “Improperly Parametrized Rational Curves”, *Computer Aided Geometric Design* 3, 67–75 (1986).

[SeGH97] T.W. Sederberg, R. Goldman, H. Du, “Impliciting Rational Curves by the Method of Moving Algebraic Curves”, *J. Symbolic Computation* 23, 153-176 (1997).

[SeWi91] J.R. Sendra, F. Winkler F., “Symbolic Parametrization of Curves“, *J. Symbolic Computation* 12/6, 607-631 (1991).

[SeWi97] J.R. Sendra, F. Winkler, “Parametrization of Algebraic Curves over Optimal Field Extensions”, *J. Symbolic Computation* 23/2&3, 191–207 (1997).

[SeWi99] J.R. Sendra, F. Winkler, ”Algorithms for Rational Real Algebraic Curves”, *Fundamenta Informaticae* 39/1-2, 211–228 (1999).

[SeWi01a] J.R. Sendra, F. Winkler, “Computation of the Degree of a Rational Map between Curves”, in *Proc. ISSAC'01*, B. Mourrain (ed.), 317–322 (2001).

[SeWi01b] J.R. Sendra, F. Winkler, ”Tracing Index of Rational Curve Parametrizations”, *Computer Aided Geometric Design* 18, 771–795 (2001).

[Villa89] O. Villamayor, “Constructiveness of Hironaka's resolution”, *Ann. Scient. Ecole Norm. Sup. 4*, vol.22, 1–32 (1989).

[Wink96] F. Winkler, *Polynomial Algorithms in Computer Algebra*, Springer-Verlag, Wien New York (1996).