Computer Algebra and Geometry — Some Interactions

Franz Winkler *
RISC-Linz, Johannes Kepler Universität Linz
Franz.Winkler@jku.at

Abstract

Algebraic curves and surfaces have been studied intensively in algebraic geometry for 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 rôle in computer aided geometric design, computer vision, computer aided manufacturing, coding theory, and cryptography, just to name a few application areas. Consequently, theoretical results need to be adapted to practical needs. We need efficient algorithms for generating, representing, manipulating, analyzing, rendering algebraic curves and surfaces. Exact computer algebraic methods can be employed effectively for dealing with these geometric problems.

1 Introduction

Algebraic curves and surfaces have been studied intensively in algebraic geometry for 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 rôle in computer aided geometric design, computer vision, computer aided manufacturing, coding theory, and cryptography, just to name a few application areas. Consequently, theoretical results need to be adapted to practical needs. We need efficient algorithms for generating, representing, manipulating, analyzing, rendering algebraic curves and surfaces. Exact computer algebraic methods can be employed effectively

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

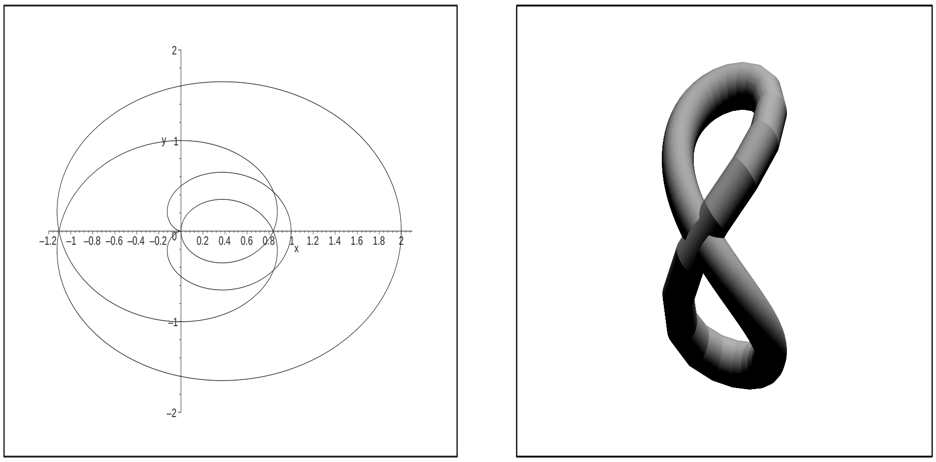

Figure 1: (a) cardioid curve and offset (b) Viviani pipe surface

for dealing with these geometric problems. So, for instance, we need to be able to factor over algebraically closed fields for determining whether a curve or surface is irreducible, we need to solve systems of algebraic equations for analyzing the singular locus of such objects, and we need to control algebraic extensions in computing rational parametrizations.

We describe some of the algorithms for computations with algebraic curves and surfaces which have been developed in the last few years. One interesting subproblem is the rational parametrization of curves and surfaces. Determining whether a curve or surface has a rational parametrization, and if so, computing such a parametrizaton, is a non-trivial task. But in the last few years there has been quite some progress in this area.

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 $\mathbb{Q}$. This is easy for a curve given parametrically. So it is highly desirable to have efficient algorithms for changing from implicit to parametric representation, and vice versa. We have described such parametrization algorithms for curves in [SeWi97], [SeWi99]. So, for instance, the cardioid curve and also its offset curve are both rational curves; compare Figure 1(a). Recently, in [LSWH00], we have developed a completely algebraic algorithm for parametrizing pipe and canal surfaces, such as the pipe around Viviani's temple, see Figure 1(b).

Sometimes algebraic curves and surfaces need to be visualized. Numerical approximation algorithms tend to have problems finding all the isolated components of these objects and also tracing them through singularities. On the other hand, symbolic algebraic algorithms might spend a lot of computation time on non-critical parts of these objects. We describe a hybrid symbolic-numerical algorithm for visualizing algebraic curves.

In the last section we mention some open problems in computational algebraic geometry. These open problems concern the "best" integer coefficients of a parametrization, optimal parametrization of surfaces, determining rational points on elliptic curves, decomposition of rational functions over the reals, and symbolic-numerical plotting of surfaces.

For a general background on computer algebra and on symbolic algebraic algorithms for algebraic curves and surfaces we refer to [Wink96] and [HSWi97].

2 Parametrization of algebraic curves

One interesting problem in computational algebraic geometry is the rational parametrization of curves and surfaces. Consider an affine plane algebraic curve $\mathcal{C}$ in $\mathbb{A}^2(\overline{K})$ defined by the bivariate polynomial $f(x,y) \in K[x,y]$ (here we denote by $\overline{K}$ the algebraic closure of the ground field K). I.e.

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

Of course, we could also view this curve in the projective plane $\mathbb{P}^2(\overline{K})$, defined by $F(x,y,z)$, the homogenization of $f(x,y)$.

A pair of rational functions $(x(t), y(t)) \in \overline{K}(t)^2$ is a *rational parametrization* of the curve $\mathcal{C}$, if and only if $f(x(t), y(t)) = 0$ and $x(t), y(t)$ are not both constant. Only irreducible curves, i.e. curves whose defining polynomial is 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. An algebraic curve having a rational parametrization is called a *rational curve.* A rational parametrization is called *proper* iff the corresponding rational map from K to $\mathcal{C}$ is invertible, i.e. iff the the affine line and the curve $\mathcal{C}$ are birationally equivalent. By Lüroth's theorem, every rational curve has a proper parametrization.

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 2.1: The curve defined in the affine or projective plane over $\mathbb{C}$ by the defining equation $f(x,y) = y^2 - x^3 - x^2 = 0$ is rationally parametrizable, and actually a parametrization is $x(t) = t^2 - 1$, $y(t) = t(t^2 - 1)$.

On the other hand, the elliptic curve defined by $f(x,y) = y^2 - x^3 + x = 0$ does not have a rational parametrization.

The tacnode curve defined by $f(x,y) = 2x^4 - 3x^2y + y^4 - 2y^3 + y^2 = 0$ 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. $\square$

A symbolic algebraic algorithm for rational parametrization of curves of genus 0 has been developed in [SeWi91], [SeWi97], [SeWi99]. Let us demonstrate the algorithm on a simple example.

Example 2.2: Let $\mathcal{C}$ be the curve in the complex plane defined by

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

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

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

$\mathcal{C}$ 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 3 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. $\tilde{\mathcal{H}}$ is called the *system of adjoint curves* of degree 2. 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 $\tilde{\mathcal{H}}$. 3 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 parametrization approach can be found in [Hoeij94].

In any case, computing such a parametrization essentially requires the solution of two major problems:
(1) a full analysis of singularities and determination of genus and adjoint curves (either by successive blow-ups, or by Puiseux expansion) and
(2) the determination of a regular point on the curve.
The fastest known method for (1) has been presented in [Stad00]. If $f(x, y) \in \mathbb{Q}[x, y]$ is the defining polynomial for the curve under consideration, then the problem can be solved in time $\mathcal{O}(d^5)$, where d is the degree of f.

Let us discuss the treatment of problem (2). 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. The treatment of this problem goes back to [HiHu90]. Its importance for the parametrization problem has been described in [HiWi98].

A rationally parametrizable curve always has infinitely many regular points over the algebraic closure $\overline{K}$ of the ground field K. Every one of these regular points is contained in an algebraic extension field of K of certain finite degree. The coordinates of the regular point determine directly the algebraic extension degree over K which is required for determining a parametrization based on this regular point. So the central issue is to find

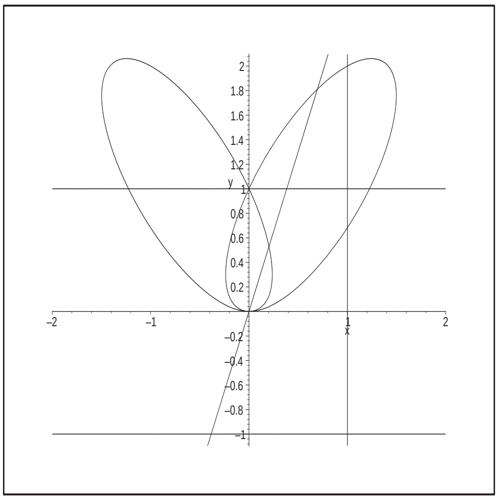

Figure 2: determining points on the tacnode curve

a regular point on the curve $\mathcal{C}$ of as low an algebraic extension degree as possible.

Example 2.3: Let us once more consider the tacnode curve $\mathcal{C}$ of Example 2.1, defined by

$$f(x,y) = 2x^4 - 3x^2y + y^4 - 2y^3 + y^2 = 0.$$

According to the approach described in Example 2.2 we need a regular point on the curve. We might determine such a point by intersecting $\mathcal{C}$ with a line. Such intersecting lines are shown in Figure 2.

Suppose we select the line $\mathcal{L}_1$ defined by $l_1(x,y) = y+1$. The 4 intersection points have the form $P = (\alpha, -1)$, where α is a root of the irreducible polynomial $2\alpha^4+3\alpha^2+4 = 0$. Using such a point leads to the parametrization $(x(t), y(t)) = (n_1(t)/d(t), n_2(t)/d(t))$, where

$$\begin{aligned} n_1(t) = & -\tfrac{\alpha}{4}(36t^4 + (60\alpha + 72\alpha^3)t^3 - (18 + 108\alpha^2)t^2 + (103\alpha + 42\alpha^3)t \\ & -20 - 24\alpha^2), \\ n_2(t) = & -9t^4 - (3\alpha + 18\alpha^3)t^3 + (2\alpha^2 - 33)t^2 - (2\alpha + 12\alpha^3)t - 4, \\ d(t) = & \ 9t^4 + 24\alpha t^3 - (16\alpha^2 + 60)t^2 - (20\alpha + 24\alpha^3)t + 6 + 12\alpha^2. \end{aligned}$$

This parametrization of $\mathcal{C}$ has complex coefficients of algebraic degree 4 over $\mathbb{Q}$.

Now suppose we select the line $\mathcal{L}_2$ defined by $l_2(x,y) = y - 1$. $\mathcal{L}_2$ intersects $\mathcal{C}$ in the double point $(0,1)$ and in the 2 intersection points having the form $P = (\beta : 1)$, where β is a root of the irreducible polynomial

$2\beta^2 - 3 = 0$. Using such a point leads to the parametrization $(x(t), y(t)) = (n_1(t)/d(t), n_2(t)/d(t))$, where

$$\begin{aligned} n_1(t) = &\quad 2\beta t^4 + 9t^3 - 27t - 18\beta, \\ n_2(t) = &\quad 2t^4 + 12\beta t^3 + 39t^2 + 36\beta t + 18, \\ d(t) = &\quad 11t^4 + 24\beta t^3 + 12t^2 + 18. \end{aligned}$$

This parametrization of $\mathcal{C}$ has real coefficients of algebraic degree 2 over $\mathbb{Q}$.

Next we select the line $\mathcal{L}_3$ defined by $l_3(x, y) = y - \frac{1792025}{687968}x = 0$. $\mathcal{L}_3$ intersects $\mathcal{C}$ in the double point $(0, 0)$ and in 2 other rational points, one of which has the coordinates

$$P = \left(\frac{1232888111650}{1772841609267}, \frac{3211353600625}{1772841609267}\right).$$

Using this point P leads to the parametrization $(x(t), y(t)) = (n_1(t)/d(t), n_2(t)/d(t))$, where

$$\begin{aligned} n_1(t) = &\quad -11095993004850t^4 - 12890994573912t^3 + 4296998191304t \\ &\quad +1232888111650, \\ n_2(t) = &\quad 28902182405625t^4 + 67155391392600t^3 + 58277689547446t^2 \\ &\quad +22385130464200t + 3211353600625, \\ d(t) = &\quad 15955574483403t^4 + 44963405382900t^3 + 54017766921682t^2 \\ &\quad +29782459134100t + 6069839800571. \end{aligned}$$

This parametrization of $\mathcal{C}$ has rational coefficients, but they are huge.

Finally we select the line $\mathcal{L}_4$ defined by $l_4(x, y) = x - 1$. $\mathcal{L}_4$ intersects $\mathcal{C}$ in 2 complex points and 2 real points, one of which has the coordinates $P = (1, 2)$. Using this point P leads to the parametrization $(x(t), y(t)) = (n_1(t)/d(t), n_2(t)/d(t))$, where

$$\begin{aligned} n_1(t) = &\quad 2t^4 + 7t^3 - 21t - 18, \\ n_2(t) = &\quad 4t^4 + 28t^3 + 73t^2 + 84t + 36, \\ d(t) = &\quad 9t^4 + 40t^3 + 64t^2 + 48t + 18. \end{aligned}$$

This parametrization of $\mathcal{C}$ has small rational coefficients. $\square$

In [SeWi97] we present an algorithm for determining the lowest algebraic extension degree $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ of a field $\mathbb{Q}(\alpha)$ which admits a rational parametrization of a curve defined over $\mathbb{Q}$. In fact, this algorithm also determines a parametrization over this optimal extension field. In [SeWi99] we describe a decision procedure for determining whether an algebraic curve with defining polynomial in $\mathbb{Q}[x, y]$ has a parametrization over the real numbers $\mathbb{R}$.

Once we are able to parametrize algebraic curves over the optimal extension field, we can also determine Diophantine solutions of the corresponding polynomial equations. We do not go into details here, but refer the reader to [PoVo00].

3 Parametrization of algebraic surfaces

The problem of rational parametrization can also be solved for algebraic surfaces. Also in this case, the analysis of singularities plays an essential rôle. Many different authors have been involved in the solution of this problem, we just mention [Hiro64] and [Vill91]. Based on the algorithmic solution of the singularity problem, Schicho has developed a general algorithm for determining the rational parametrizability of an algebraic surface, and, in the positive case, for actually computing such a parametrization. See [Schi98]. But whereas for the case of curves we know exactly the degrees of the rational functions and also the degree of the algebraic extension which might appear in the parametrization, these bounds are not known for surfaces, in general.

General parametrization algorithms for surfaces require considerable computation time. So it is natural to try to develop algorithms specifically taylored for classes of surfaces of practical importance. Such a class is, for instance, the one of pipe and canal surfaces. A *canal surface* $\mathcal{S}$, generated by a parametrized space curve $\mathcal{C} = (m_1(t), m_2(t), m_3(t))$ in $\mathbb{R}^3$, is the envelope of the set of spheres with rational radius function $r(t)$ centered at $\mathcal{C}$. The curve $\mathcal{C}$ is called the *spine curve* of $\mathcal{S}$. In a *pipe surface* $r(t)$ is constant. This concept generalizes the classical offsets (for constant $r(t)$) of plane curves. Pipe surfaces have numerous applications, such as shape reconstruction or robotic path planning. Canal surfaces with variable radius arise in the context of computer aided geometric design mainly as transition surfaces between pipes.

Whereas for curves it is crucial to determine a regular point with real coordinates, in the situation of pipe and canal surfaces we determine a rational curve with real coefficients on the surface, in the same parameter as the spine curve. Once we have determined such a rational curve on the canal surface $\mathcal{S}$, we can rotate this curve around the spine curve and in such a way compute a parametrization of $\mathcal{S}$.

So, for instance, Viviani's temple is defined as the intersection of a sphere of radius $2a$ and a circular cylinder of radius a:

$$\begin{aligned} x^2 + y^2 + z^2 &= 4a^2, \\ (x-a)^2 + y^2 &= a^2, \end{aligned}$$

see Figure 1(b). The pipe around Viviani's temple can be rationally parametrized.

In [PePo97] it is shown that canal surfaces with rational spine curve and rational radius function are in general rational. To be precise, they admit rational parametrizations of their real components. Recently we have developed a completely symbolic algebraic algorithm for computing rational parametrizations of pipe and canal surfaces over $\mathbb{Q}$, see [LSWH00].

4 Implicitization of curves and surfaces

The inverse problem to the problem of parametrization consists in starting from a (rational) parametrization and determining the implicit algebraic equation of the curve or surface. This is basically an elimination problem. Let us demonstrate the procedure for curves. We write the parametric representation of the curve $\mathcal{C}$,

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

as

$$h_1(t,x) = x \cdot r(t) - p(t) = 0, \quad h_2(t,y) = y \cdot r(t) - q(t) = 0.$$

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

$$I = \langle h_1(t,x), h_2(t,y) \rangle \ \cap \ K[x,y].$$

We can use any method in elimination theory, such as resultants of Gröbner bases, for determining this generator. For instance,

$$\text{resultant}_t(h_1(t,x), h_2(t,y))$$

will yield the polynomial defining the curve $\mathcal{C}$. Compare [Wink96] and [SeWi01] for details. In [SeWi01] we introduce the notion of the *tracing index* of a rational parametrization, i.e. the number of times a (possibly non-proper) parametrization "winds around, or traces, an algebraic curve". When we compute the resultant of h_1 and h_2 as above for an non-proper parametrization, then this tracing index will show up in the exponent of the generating polynomial.

Example 3.1: Let us do this for the cardioid curve of Figure 1(a). We start from the parametrization

$$x(t) = \frac{256t^4 - 16t^2}{256t^4 + 32t^2 + 1}, \quad y(t) = \frac{-128t^3}{256t^4 + 32t^2 + 1}.$$

So we have to eliminate the variable t from the equations

$$\begin{aligned} h_1(t,x) &= x \cdot (256t^4 + 32t^2 + 1) - 256t^4 + 16t^2, \\ h_2(t,y) &= y \cdot (256t^4 + 32t^2 + 1) + 128t^3. \end{aligned}$$

As the polynomial defining the cardioid curve we get

$$\text{resultant}_t(h_1(t,x), h_2(t,y)) = 17179869184 \cdot (4y^4 - y^2 + 8x^2y^2 - 4xy^2 + 4x^4 - 4x^3).$$

Similarly we could determine this defining polynomial by a Gröbner basis computation. □

5 Further topics in computational algebraic geometry

We have only described a few subproblems in computational algebraic geometry. For the algorithmic treatment of problems in computer aided geometric design, such as blending and offsetting, we refer the reader to [Hoff89]. A thorough analysis of the offset curves, in particular their genus, is given in [ASSe99]. If we need to decide problems on algebraic geometric objects involving not only equations but also inequalities, then the appropriate method is Collins' algorithm for cylindrical algebraic decomposition, see [CaJo98]. Further areas of investigation are desingularization of surfaces, determining rational points on elliptic curves, and fast algorithms for visualization of curves and surfaces. In general, it will be more and more important to bridge the gap between symbolic and numerical algorithms, combining the best features of both worlds.

6 Open problems

Integer coefficients in curve parametrization

As we have seen in Chapter 2, the quality of a rational parametrization of an algebraic curve crucially depends on the quality of a regular point which we can determine on this curve. For instance, starting from a defining polynomial $f(x, y)$ of $\mathcal{C}$ over the rational numbers $\mathbb{Q}$, we know that we will need an algebraic extension of degree 2, at most, for expressing such a point. But if we can actually find a regular point with coordinates in $\mathbb{Q}$, and therefore a parametrization with rational coefficients, the question is still how to find a parametrization with "smallest" rational coefficients. To our knowledge, this problem is unsolved.

Optimality of surface parametrization

For rational algebraic surfaces no algorithm is known, in general, for finding a parametrization with lowest possible degree of rational functions. The best we can currently do is to compute a parametrization having at most twice the optimal degree, see [Schi99].

Also the problem of determining the smallest algebraic field extension for expressing a rational parametrization of a rational algebraic surface is wide open. In general, we cannot decide whether there is a parametrization over the given field of definition. We also do not know whether a bound for the degree of the neccessary extension exists.

Decomposition of rational functions over $\mathbb{R}$

In the algorithm for rationally parametrizing pipe and canal surfaces, [LSWH00], the problem is finally reduced to finding a representation of a rational function as a sum of two squares. This is a special case of Hilbert's 17^{th} problem. Over the real algebraic numbers there exists a simple algorithm for solving this problem. Over $\mathbb{R}$ the problem is still open.

Determining rational points on elliptic curves

For curves of genus 0 we can decide the existence of rational points. If a curve of genus 0 over a field of characteristic 0 has one rational point then it must have infinitely many. In fact, we can determine these rational points. If the genus is greater or equal 2, then there are only finitely many rational points on the curve $\mathcal{C}$. This was conjectured by Mordell and proved by Faltings [Falt83]. For curves of genus 1, i.e. so-called *elliptic curves*, all possiblities can arise: no, finitely many, and infinitely many rational points. Elliptic curves play an important rôle in many areas of mathematics, and recently also in cryptography. Determining all, or at least one, rational point on an elliptic curve is an open problem. For a short introduction see [Drm00].

Symbolic-numerical plotting of surfaces

When we work with curves and surfaces, we do not only construct, transform, and analyze them, but sometimes we also want to visualize them on the screen. These geometrical objects might be quite complicated, having several real components, perhaps isolated singularities, and complicated branch points.

There are basically two approaches to the problem of plotting such curves or surfaces: numerical plotting and algebraic plotting. Whereas numerical plotting routines work well for simple objects and require relatively little computation time, they quickly become unreliable for more complicated objects: missing small components, getting the picture wrong around singularities. On the other hand, algebraic plotting routines can overcome these problems, but are notoriously slow.

Recently we have developed a hybrid symbolic-numerical routine in the program system CASA, [HHWi03], for reliable but relatively fast visualization of plane algebraic curves [MSWi00]. These methods need to be understood better and extended to surfaces.

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).

[ASSe99] E. Arrondo, J. Sendra, J.R. Sendra, “Genus Formula for Generalized Offset Curves”, *J. Pure and Applied Algebra* 136/3, 199–209 (1999).

[CaJo98] B.F. Caviness, J.R. Johnson, *Quantifier Elimination and Cylindrical Algebraic Decomposition*, Springer (1998).

[Drm00] M. Drmota, “Sieben Millenniums-Probleme. I.”, *Internat. Math. Nachrichten* 184, 29–36 (2000).

[Falt83] G. Faltings, “Endlichkeitssätze für abelsche Varietäten über Zahlenkörpern”, *Invent. Math.* 73, 549–576 (1983).

[HHWi03] R. Hemmecke, E. Hillgarter, F. Winkler, “CASA”, in: *Handbook of Computer Algebra: Foundations, Applications, Systems*, J. Grabmeier, E. Kaltofen, V. Weispfenning (eds.), 356–359, Springer-Verlag (2003).

[HiHu90] D. Hilbert, A. Hurwitz, “Über die Diophantischen Gleichungen vom Geschlecht Null”, *Acta math.* 14, 217–224 (1890).

[HiWi98] E. Hillgarter, F. Winkler, “Points on Algebraic Curves and the Parametrization Problem”, in *Automated Deduction in Geometry*, D. Wang (ed.), Springer-Verlag Berlin, LNAI 1360, 189–207 (1998).

[Hiro64] H. Hironaka, “Resolution of Singularities of an Algebraic Variety over a Field of Characteristic 0”, *Ann. Math.* 79, 109–326 (1964).

[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).

[Hoff89] C.M. Hoffmann, *Geometric & Solid Modeling*, Morgan Kaufmann Publ. (1989).

[HSWi97] C.M. Hoffmann, J.R. Sendra, F. Winkler, *Parametric Algebraic Curves and Applications*, Special issue of the *J. Symbolic Computation* 23/2&3 (1997).

[LSWH00] G. Landsmann, J. Schicho, F. Winkler, E. Hillgarter, "Symbolic Parametrization of Pipe and Canal Surfaces", in *Proc. Internat. Symposium on Symbolic and Algebraic Computation (ISSAC'2000)*, St.Andrews, Scotland, Aug. 2002, C. Traverso (ed.), 202–208, ACM Press (2000).

[MSWi00] C. Mittermaier, W. Schreiner, F. Winkler, "A Parallel Symbolic-Numerical Approach to Algebraic Curve Plotting", in *Computer Algebra in Scientific Computing, Proc. of CASC'2000*, 301–314, V.G. Ganzha, E.W. Mayr, E.V. Vorozhtsov (eds.), Springer-Verlag, Berlin (2000).

[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).

[Schi98] J. Schicho, "Rational Parametrization of Surfaces", *J. Symb. Computation* 26/1, 1–30 (1998).

[Schi99] J. Schicho, "A Degree Bound for the Parametrization of a Rational Surface", *J. Pure and Appl. Algebra* 145, 91–105 (1999).

[SeWi91] J.R. Sendra, F. Winkler, "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).

[SeWi01] J.R. Sendra, F. Winkler, “Tracing Index of Rational Parametrizations”, *RISC-Linz Report Series* 01-01, J.Kepler Univ., Linz, Austria (2001).

[Stad00] P. Stadelmeyer, *On the Computational Complexity of Resolving Curve Singularities and Related Problems*, Ph.D. thesis, RISC-Linz, J.Kepler Univ. Linz, Austria, Techn.Rep. RISC 00-31 (2000).

[Vill91] O. Villamayor, “Introduction to the Algorithm of Resolution”, in *Algebraic Geometry and Singularities, La Rabida 1991*, 123–154, A. Campillo Lopez et al. (eds.), Birkhäuser (1991).

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