REPRESENTATION OF ALGEBRAIC CURVES *)

F. Winkler
RISC-LINZ, J. Kepler Universität, Linz, Austria

Abstract

If algebraic varieties like curves or surfaces are to be manipulated by computers, it is essential to be able to represent these geometric objects in an appropriate way. For some applications an implicit representation by algebraic equations is desirable, whereas for others an explicit or parametric representation is more suitable. Therefore, transformation algorithms from one representation to the other are of utmost importance.

We investigate the transformation of an implicit representation of a plane algebraic curve into a parametric representation. In the course of the transformation algorithm the coefficient field has to be extended algebraically. If the known parametrization algorithms are used uncritically, the algebraic extensions get so high that any computation becomes practically impossible. Our goal is to keep the degree of the necessary algebraic extension as small as possible.

Introduction

An algebraic variety V, the main object of study in algebraic geometry, can be represented in various different ways, for instance as the set of zeros of polynomial equations

$$V = \{(x,y) \mid 2x^4 - 3x^2y + y^2 - 2y^3 + y^4 = 0,\ x,y \in \mathbb{C}\},$$

or as the set of values of rational functions

$$\begin{aligned} V = \{(\phi(t),\chi(t)) \mid \phi(t) &= -\frac{18t^4+21t^3-7t-2}{18t^4+48t^3+64t^2+40t+9}, \\ \chi(t) &= \frac{36t^4+84t^3+73t^2+28t+4}{18t^4+48t^3+64t^2+40t+9}, \quad t \in \mathbb{C}\}. \end{aligned}$$

We call the first representation *implicit* and the second *explicit* or *parametric.*

The representation of choice is of course determined by the operations one wants to perform with the variety. For determining whether a given point is a point of the variety, or for computing singular points of the variety, the implicit representation is more desirable than the parametric one. On the other hand, the parametric representation lends itself very easily to the determination of the curvature, to tracing of varieties, and in particular to visualizing them on a computer screen. The intersection of varieties can be determined rather easily if one of the varieties is given implicitely and the other one explicitely. For this reason it is essential to be able to switch between different representations.

In /3/ the problem of computing the implicit equations from a given parametric representation is treated. Recently the application of the Gröbner basis method to the implicitization problem has been further investigated in /5/. The reverse problem, namely computing a rational parametrization from the given implicit equations, is a classical problem in algebraic geometry, see for instance /8/. In /2/,/4/ the problem of parametrization for space curves is reduced to the problem of parametrization of plane curves. In this paper we will deal only with the problem of parametrizing plane curves.

*) This research was supported by the Austrian *Fonds zur Förderung der wissenschaftlichen Forschung* under Projekt Nr. P6763.

Theoretically the problem of parametrization of plane curves is solved, and it is known that the parametrizable curves are exactly the curves of genus 0. In /8/ also an algorithm is suggested for computing a rational parametrization. Instead of a pencil of degree $d-2$, as in /1/, one could also use pencils of degree $d-1$ and d in the parametrization algorithm. In fact, these pencils are more attractive from a computational point of view. The determination of simple points on the curve introduces a lot of algebraic numbers. If they are not controlled, the computation soon becomes too inefficient. We show that a pencil can be passed through a set of points on the given curve without having to compute these points explicitly. It turns out that if $\mathbb{F}$ is a field in which the coordinates of the singular points of the curve C can be represented, then a rational parametrization of C can be found in an extension field of degree $\deg(C)$ over $\mathbb{F}$. Our conjecture, however, is that for a curve of odd degree we need no algebraic extension of $\mathbb{F}$. In this paper we can only state the results of our work. For details on the methods and proofs we refer to /7/.

Let $\mathbb{K}$ be an algebraically closed field of characteristic 0. We will consider curves in the affine and projective planes over $\mathbb{K}$. If the curve C is defined by $f(x,y)=0$ then the associated projective curve C^* is defined by $F(x,y,z)=0$, where F is the homogenization of f.

The irreducible affine curve C defined by the irreducible polynomial $f(x,y) \in \mathbb{K}[x,y]$ is *rational* iff there exist rational functions $\phi(t), \chi(t) \in \mathbb{K}(t)$ such that

(1) for almost all (i.e. for all but a finite number of exceptions) $t_0 \in \mathbb{K}$, $(\phi(t_0), \chi(t_0))$ is a point on C, and

(2) for almost every point (x_0, y_0) on C there is a $t_0 \in \mathbb{K}$ such that $(x_0, y_0) = (\phi(t_0), \chi(t_0))$.

If ϕ, χ satisfy the conditions (1) and (2), (ϕ, χ) is a *rational parametrization* of C.

The notion of rationality for affine curves can be extended in a natural way to a notion of rationality for projective curves. This is achieved by introducing a third rational function $\psi(t)$ and postulating the conditions (1),(2). In fact, a parametrization of C can be immediately obtained from a parametrization of the associated curve C^* in the projective plane and vice versa.

With this terminology we can state the problem of parametrization.

<u>Parametrization problem</u>:

given: an irreducible polynomial $f(x,y) \in \mathbb{K}[x,y]$ defining an irreducible affine algebraic plane curve C

decide: the rationality of C

find: (if C is rational) rational functions $\phi(t), \chi(t) \in \mathbb{K}(t)$ such that (ϕ, χ) is a rational parametrization of C. $\square$

In the sequel we exclude the case where the degree of the polynomial f defining the curve C is 1, i.e. where C is a line. Obviously the parametrization of lines does not present a problem.

A singular point P of multiplicity r on the affine curve C defined by $f(x,y)$ is an *ordinary* singular point iff the r tangents to C at P are distinct. Otherwise P is called *non–ordinary*. The property of a singular point P of being ordinary or non–ordinary is called the *character* of P. An important result about singularities is the fact that if C is an irreducible projective or affine curve of degree d having multiplicities r_P at points P, then $(d-1)(d-2) \geq \sum_{P \in C} r_P(r_P - 1)$. In the special case of an irreducible projective curve C^*, defined by $F(x,y,z)=0$, having only ordinary singularities one can characterize the rationality as follows. If $r_1, \ldots, r_n$ are the multiplicities of the singular points of C^*, C^* is rational if and only if $(d-1)(d-2) = \sum_{i=1}^{n} r_i(r_i - 1)$. In the general case, for characterizing the rationality of a plane curve one usually introduces the concept of neighboring points. If we include also the neighboring singular points, then the above equation is a criterion for the rationality of a curve C.

A parametrization algorithm

Let us assume that the irreducible projective curve C^* of degree d defined by $F(x,y,z)=0$ is rational. If C^* has a $(d-1)$–fold point, then it is rational and a parametrization can be determined by cutting C^* with lines passing through this $(d-1)$–fold point. By Bezout's theorem there will be exactly one additional intersection point depending on the slope of the line, yielding the desired parametrization. This idea may be generalized. In the general situation one can also construct a pencil of curves such that for almost every curve in the pencil all its intersection points with C^*, except one, are predetermined. Moreover, all the predetermined intersection points are the same for every curve in the pencil. Thus, if one computes the intersection points of a generic element of the pencil with C^*, the expression of the unknown intersection point gives the parametrization of the curve by means of the parameter defining the pencil. Here we discuss only pencils of degree d.

Let us assume that D^* is a generic representative of a pencil of curves of degree d. Then in general D^* has d^2 intersections with C^*. We postulate that D^* satisfies the properties:

(1) every r–fold singular point (including the neighboring ones) on C^* is an $(r-1)$–fold point on D^*,

(2) there exist $3d-3$ simple points on C^* that are also simple points on D^*,

(3) C^* and D^* do not have a common component.

In this way, we force D^* to have some specific common points with C^*. In the sequel, we will refer to these points as the *fixed common points* of C^* and the pencil. The intersection multiplicity of C^* and D^* at the singular points P of C^* (including the neighboring ones) is at least $\sum r_P(r_P-1) = (d-1)(d-2)$, where r_P is the multiplicity of P on C^*. So by condition (2) we fix just so many simple intersection points of C^* and D^* as to leave at most one intersection point undetermined.

LEMMA 1: *The pencil of curves D^* of degree d satisfying (1) – (3) can be effectively computed and the coefficients of the pencil are polynomials in one free parameter. Almost every curve in the pencil intersects C^* in one additional point and for almost every simple point Q on C^* which is not one of the fixed common points there exists a curve in the pencil intersecting C^* at Q.* □

Having determined the pencil D^*, we want to compute a formula for the unknown intersection point of an arbitrary curve in the pencil with the given rational curve C^*. By resultant computations we will derive the rational parametrization from this formula. In the sequel we denote by $\mathrm{Res}_v(p,q)$ the resultant of the polynomials p and q w.r.t. the variable v.

Let t be the independent parameter of D^*. Let us also suppose that $P_i = (\lambda_i, \mu_i, \rho_i)$, $1 \le i \le n$, are the singular points of C^*, where P_i is a point of multiplicity r_i on C^*, and that $Q_i = (\bar{\lambda}_i, \bar{\mu}_i, \bar{\rho}_i)$, $1 \le i \le 3d-3$, are the fixed common simple points of C^* and D^*. Let $\bar{r}_i := r_i(r_i-1) + \sum_{P\in N(P_i)} r_P(r_P-1)$, $1 \le i \le n$, where $N(P_i)$ is the set of neighboring points of P_i w.r.t. C^*. Let C be the affine curve associated with C^*, i.e. C is defined by $f(x,y) = F(x,y,1)$. Let $h(x,y) = H(x,y,1)$ be the dehomogenization of the defining polynomial of the pencil D^*.

THEOREM 2: *With the notation introduced above there exist nonzero polynomials $m_1(t), m_2(t), n_1(t), n_2(t) \in \mathbb{K}[t]$ such that*

$$\mathrm{Res}_x(f,h) = \prod_{i=1}^{n}(\rho_i y - \mu_i)^{\bar{r}_i} \cdot \prod_{i=1}^{3d-3}(\bar{\rho}_i y - \bar{\mu}_i) \cdot (m_1(t)y - n_1(t)),$$
$$\mathrm{Res}_y(f,h) = \prod_{i=1}^{n}(\rho_i x - \lambda_i)^{\bar{r}_i} \cdot \prod_{i=1}^{3d-3}(\bar{\rho}_i x - \bar{\lambda}_i) \cdot (m_2(t)x - n_2(t)).$$
□

THEOREM 3: *Let C, C^*, D^*, F, H, f, h be as above. If $(u(t)x - v(t))$ and $(\bar{u}(t)y - \bar{v}(t))$ are the factors of $\mathrm{Res}_y(f,h)$ and $\mathrm{Res}_x(f,h)$ depending on t, respectively, then $\big(x(t) = v(t)/u(t),\ y(t) = \bar{v}(t)/\bar{u}(t),\ z(t) = 1\big)$ is a parametrization of C^* and $\big(x(t) = v(t)/u(t),\ y(t) = \bar{v}(t)/\bar{u}(t)\big)$ is a parametrization of C.* □

So we arrive at the following algorithm for computing a rational parametrization of an irreducible affine rational curve.

Algorithm PARAMETRIZE

The input is an irreducible affine rational curve C of degree d, defined by the irreducible polynomial $f(x,y)$. The output is a rational parametrization of C.

(1) Determine the singularities of the projective curve C^* associated with C, including the neighboring ones, and their multiplicities. Determine $3d-3$ simple points on C^*. Determine the

pencil D^* as it has been described above. Let $H(x,y,z)$ be the polynomial defining the pencil, $h(x,y) = H(x,y,1)$.

(2) Compute $S_1(y) = \mathrm{Res}_x(f,h)$ and $S_2(x) = \mathrm{Res}_y(f,h)$.

(3) Remove the factors corresponding to the common points of C^* and D^* from $S_1(y)$ and $S_2(x)$, as described in Theorem 2.

(4) Solve the linear system of equations $S_1(y) = 0,\ S_2(x) = 0$, where x, y are the unknowns. Let $(R_1(t), R_2(t))$ be the solution.

(5) Return the parametrization $(R_1(t), R_2(t))$. □

Of course we are interested in parametrizations which need only few, if any, algebraic numbers. Let $\mathbb{F}$ be a field of characteristic zero in which all the field operations can be carried out effectively and in which the singularities of the curve C can be represented. The remaining problem then is the selection of the simple common points of the curve C^* and the pencil D^*. We propose to use whole conjugacy classes of simple points in order to keep the necessary algebraic extension as low as possible.

Lemma 4: *Let $q \in \mathbb{F}[s]$ with $\deg(q) = n \le a$, $\{\beta_1, \ldots, \beta_n\}$ the roots of q, and $a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{F}$.*

(a) The points $\{(a_1 + b_1\beta_i : a_2 + b_2\beta_i : a_3 + b_3\beta_i)\}_{i=1,\ldots,n}$ are on D^* if and only if $q(s)$ divides $H(a_1 + b_1 s, a_2 + b_2 s, a_3 + b_3 s)$.

(b) If $\{(a_1+b_1\beta_i : a_2+b_2\beta_i : a_3+b_3\beta_i)\}_{i=1,\ldots,n}$ are common points of C^* and D^*, then $q(\frac{a_2-a_3y}{b_3y-b_2}) \cdot (b_3y - b_2)^n$ divides $\mathrm{Res}_x(f,h)$ and $q(\frac{a_1-a_3x}{b_3x-b_1}) \cdot (b_3x - b_1)^n$ divides $\mathrm{Res}_y(f,h)$. □

The algorithm constructing the classes of conjugate common simple points works as follows.

<u>Algorithm</u> SIMPLE

The input to SIMPLE is an irreducible rational curve C^* defined by the polynomial $F(x,y,z)$. The output consists of three distinct whole classes of conjugate simple points on C^*, each class containing $d-1$ points. One algebraic number β of degree at most d has to be introduced.

(1) Choose $b_1, b_2 \in \mathbb{F}$ such that for every singular point $(\rho_1 : \rho_2 : \rho_3)$ of C^* we have $b_2\rho_1 - b_1\rho_2 \neq 0$ (i.e. b_1, b_2 cannot be the first two coordinates of a singular point of C^*). Compute an irreducible monic factor of the univariate polynomial $F(b_1, b_2, s)$, say $q(s)$. Now, since b_1, b_2 are not the first two coordinates of a singular point of C^*, $P = (b_1 : b_2 : \beta)$, with $q(\beta) = 0$, is a simple point on C^*.

(2) Choose $\lambda_1, \lambda_2, \lambda_3, \mu_1, \mu_2, \mu_3 \in \mathbb{F}$, such that
   - (a) $\lambda_i\mu_j - \lambda_j\mu_i \neq 0$ for $i \neq j$,
   - (b) $\mathrm{Res}_s(\bar{q}_i(s), \bar{q}_i'(s)) \neq 0$ for $i = 1,2,3$, where $\bar{q}_i(s) = F(\lambda_i s + b_1, \mu_i s + b_2, s + \beta)$ and $\bar{q}_i'$ denotes the derivative of q_i w.r.t. s.

(3) For $i = 1,2,3$ set $q_i(s) := \bar{q}_i(s)/s \in \mathbb{F}(\beta)[s]$.

(4) Now $\{(\lambda_i\beta_i + b_1 : \mu_i\beta_i + b_2 : \beta_i + \beta)\}_{q_i(\beta_i)=0}$, $i = 1,2,3$, are three distinct whole classes of $(d-1)$ simple points each on C^*. □

Theorem 5: *A parametrization of a curve of degree d can be found in an extension of degree d over $\mathbb{F}$.*

Proof: Use algorithms PARAMETRIZE and SIMPLE. □

Example: Applying the algorithms PARAMETRIZE and SIMPLE to the implicitely given curve at the beginning of this paper and choosing $(2/9, 4/9)$ as the simple point in step (1) of SIMPLE, we get the associated parametrization. □

A number theoretical problem

These considerations allow to keep the algebraic extension of the field small. But even the bound given in Theorem 5 might be far to pessimistic. J. Schicho, a Ph.D. student at RISC-LINZ, has given the following reduction of the problem of finding a parametrization with few algebraic numbers to a number theoretical problem.

Let C be an affine rational curve of degree d. Let it have k singularities $P_1, \ldots, P_k$, including the neighboring ones, with multiplicities $s_1, \ldots, s_k$, respectively. Since the genus of C is 0, we have

$$\sum_{i=1}^{k} s_i(s_i - 1) = (d-1)(d-2). \tag{1}$$

Let S be the linear system of curves of degree a ($\leq d$) that have P_i, $1 \leq i \leq k$, as an r_i–fold point. The dimension of the system S is

$$\dim(S) = t = \tfrac{a(a+3)}{2} - \sum_{i=1}^{k} \tfrac{r_i(r_i+1)}{2}. \tag{2}$$

S has $\sum_{i=1}^{k} r_i s_i$ intersections with C. Thus,

$$t \leq ad - \sum_{i=1}^{k} r_i s_i, \tag{3}$$

because there is a curve in S with at least $t + \sum_{i=1}^{k} r_i s_i$ intersections with C, and the number of intersections cannot be greater than ad by Bezout's theorem. We are particularly interested in the case where equality holds in (3). Suppose

$$t = ad - \sum_{i=1}^{k} r_i s_i \geq 1. \tag{4}$$

Then we define a subsystem R of S intersecting C at $t-1$ simple points. R has dimension 1. All the intersection points of R and C, except one, are fixed. The pencil R can now be used to parametrize the curve C along the lines described in the previous chapter. In order to avoid algebraic field extensions, t should be as small as possible. So we arrive at the following number theoretical problem:

<u>Pencil selection problem</u>:
given: nonnegative integers $d, k, s_1, \ldots, s_k$ satisfying the condition (1),
find: $t, a (1 \leq a \leq d), r_1, \ldots, r_k$ that solve (2) and (4), where t is as small as possible. □

If d is odd and the curve C has at least $l = (d-3)/2$ double points, say $P_1, \ldots, P_l$, then there exists a solution to the pencil selection problem with $t = 1$, namely $a = d-2, t = 1, r_1 = \ldots = r_l = 2, r_i = s_i - 1$ for $l+1 \leq i \leq k$. So for curves of this type no algebraic extension is needed. If d is even and the curve C has at least $l = (d/2) - 2$ double points, say $P_1, \ldots, P_l$, then there exists a solution to the pencil selection problem with $t = 2$, namely $a = d-2, t = 1, r_1 = \ldots = r_l = 2, r_i = s_i - 1$ for $l+1 \leq i \leq k$. So for curves of this type only an algebraic extension of degree d is needed. This bound on the field extension coincides with Theorem 5.

The conjecture, based on computer aided searches for solutions to the pencil selection problem, is that for every curve of odd degree a solution with $t = 1$ can be found, and for every curve of even degree a solution with $t = 2$ can be found.

References

1. Abhyankar, S.S., Bajaj, C.L. (1988). Automatic parameterization of rational curves and surfaces III: Algebraic plane curves. *Computer Aided Geometric Design* **5**, 309-321.
2. Abhyankar, S.S., Bajaj, C.L. (1990). Automatic rational parametrization of curves and surfaces IV: Algebraic space curves. To appear in *ACM Trans. on Graphics*.
3. Arnon, D.S., Sederberg, T.W. (1984). Implicit equation for a parametric surface by Groebner basis. *Proc. 1984 MACSYMA User's Conference*, V.E. Golden (ed.).
4. Garrity T., Warren J. (1989). On computing the intersection of a pair of algebraic surfaces. *Computer Aided Geometric Design* **6**, 137-153.
5. Kalkbrener, M. (1990). Implicitization of rational parametric curves and surfaces. Submitted to *AAECC-8*.
6. Sederberg, T.W. (1986). Improperly parametrized rational curves. *Computer Aided Geometric Design* **3**, 67-75.
7. Sendra, J.R., Winkler, F. (1989) *A Symbolic Algorithm for the Rational Parametrization of Algebraic Plane Curves.* Techn. Rep. RISC 89-41.0, RISC-LINZ, J.Kepler Univ., Linz, Austria.
8. Walker, R.J. (1978). *Algebraic Curves.* Springer-Verlag, New York-Heidelberg-Berlin.