Symbolic Parametrization of Curves *

J. RAFAEL SENDRA† and FRANZ WINKLER‡

† *Departamento de Matemáticas, Universidad de Alcalá de Henares, 28871 - Madrid, Spain*
‡ *Institut für Mathematik and RISC-LINZ, J. Kepler Universität, A-4040 Linz, Austria*

(*Received* 29 *January* 1990)

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. Various methods for computing a rational parametrization, if one exists, are described. As a new idea we introduce the concept of working with classes of conjugate (singular or simple) points on curves. All the necessary operations, like determining the multiplicity and the character of the singular points or passing a linear system of curves through these points, can be applied to such classes of conjugate points. Using this idea one can parametrize a curve if one knows only one simple point on it. We do not propose any new method for finding such a simple point. By classical methods a rational point on a rational curve can be computed, if such a point exists. Otherwise, one can express the coordinates of such a point in an algebraic extension of degree 2 over the ground field.

I. 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 finitely many 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

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

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

* This research was partially supported by the Austrian *Fonds zur Förderung der wissenschaftlichen Forschung* under Projekt Nr. P6763. The work described herein was carried out while the first author was visiting the Research Institute for Symbolic Computation (RISC-LINZ).

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 Arnon & Sederberg (1984) the problem of computing the implicit equations from a given parametric representation is investigated. The reverse problem, namely computing a rational parametrization from the given implicit equations, especially for plane curves, is a classical problem in algebraic geometry, see Walker (1950), Schafarewitsch (1972), van der Waerden (1953). 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 Walker (1950) also an algorithm is suggested for computing a rational parametrization. In Abhyankar & Bajaj (1988) basically this same algorithm is used for parametrization. Intuitively speaking, a curve is parametrizable if it has enough singularities. The method suggested in Walker (1950) and elaborated in Abhyankar & Bajaj (1988) proceeds by computing these singularities and sufficiently many simple points on the given curve of degree d. Through these points a pencil of curves of degree $d-2$ is passed, such that every element of the pencil intersects the given curve in exactly one additional point. A formula for this additional intersection point can be determined, yielding the desired parametrization of the curve.

We show that it is also possible to work with pencils of degree $d-1$ and d. In fact, these pencils are more attractive from a computational point of view. When exact computation is desired additional problems arise, which do not appear in numerical computation. In particular, 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. One of our new results is that a pencil can be passed through a set of points on the given curve without having to compute these points explicitly. This means that the necessary field extension for the parametrization can be kept small and any subsequent computations with the parametrization involve only algebraic numbers of low degree.

Let $\mathbb{K}$ be an algebraically closed field of characteristic 0. We will denote by $\mathbb{A}^2$ and $\mathbb{P}^2$ the affine and projective planes over $\mathbb{K}$, respectively. As usual the affine plane $\mathbb{A}^2$ is embedded into $\mathbb{P}^2$ by identifying the point $(a,b) \in \mathbb{A}^2$ with the point $(a:b:1) \in \mathbb{P}^2$. These points are sometimes called the points at finite distance of $\mathbb{P}^2$. In addition to the points at finite distance $\mathbb{P}^2$ contains points at infinity, namely the points with projective coordinates $(a:b:0)$.

An *affine algebraic (plane) curve* over $\mathbb{K}$ is the set

$$C = \{(a,b) \in \mathbb{A}^2 \mid f(a,b) = 0\}$$

for a nonzero polynomial $f(x,y) \in \mathbb{K}[x,y]$. The curve C is said to be *irreducible* iff it can be defined by means of an irreducible polynomial f. Unless explicitly stated otherwise, we will always work with irreducible polynomials defining our curves. In this case the polynomial f is uniquely defined up to a multiplicative constant in $\mathbb{K}$ and it is called the *polynomial defining* C. We will write f in the form

$$f(x,y) = f_d(x,y) + f_{d-1}(x,y) + \cdots + f_0(x,y),$$

where $f_k(x,y)$, $0 \le k \le d$, is a homogeneous polynomial of degree k, and $f_d(x,y)$ is nonzero. The polynomials f_k, $0 \le k \le d$, are called the *homogeneous components* of f, and d is called the *degree* of the curve C.

Associated with $f(x, y)$ there is a homogeneous polynomial $F(x, y, z)$ of degree d, the *homogenization* of f,

$$F(x, y, z) = f_d(x, y) + f_{d-1}(x, y) \cdot z + \cdots + f_0(x, y) \cdot z^d.$$

The *projective algebraic (plane) curve* corresponding to C is defined as the set

$$C^* = \{(a : b : c) \in \mathbb{P}^2 \mid F(a, b, c) = 0\}.$$

Every point (a, b) on C corresponds to a point $(a : b : 1)$ on C^* and every additional point on C^* is a point at infinity. In other words, the first two coordinates of the additional points are the nontrivial solutions of $f_d(x, y) = 0$. So the curve C^* has only finitely many points at infinity. By a suitable change of the coordinate system, i.e. an invertible linear homogeneous transformation, every point at infinity can be transformed to a point at finite distance.

Definition: *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). With this terminology we can state the problem of parametrization.

Parametrization problem:

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. □

In the sequel we exclude the cases where the degree of the polynomial f defining the curve C is less or equal 2, i.e. where C is a line or a conic. Obviously in these cases the parametrization does not present a problem.

We want to emphasize the fact that computing points with small algebraic degree on an algebraic curve is a costly operation. Our aim is to reduce the number of simple points needed in the parametrization algorithm. We show that if a pencil of curves of the same degree as C is used in the parametrization algorithm then only one simple point suffices. Of course, there are special cases in which a different approach might be preferable, e.g. when C is a quartic curve and a pencil of degree 2 is used. A practical implementation of a parametrization algorithm should take such special cases into account. Our aim, however, is not a treatment of these special cases, but a general algorithm.

II. Rational curves

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.

Since every point P at infinity can be transformed to a point at finite distance by a suitable change of coordinates, all these definitions also apply to points on a projective curve C^*.

An important result about singularities (see e.g. Walker (1950)) 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 particular, this inequality implies that an algebraic plane curve can have only finitely many singular points.

If $f(x,y)$ has no terms of degree less than r and has some terms of degree r, i.e.

$$f(x,y) = f_d(x,y) + \cdots + f_r(x,y),$$

then the origin is an r–fold point of the curve defined by f, and the curve defined by $f_r(x,y) = 0$ has as its components the tangents to f at the origin. If $r \geq 2$, then the origin is an ordinary singular point of C if and only if the discriminant of $f_r(x,1)$ is not zero.

An outline of the algorithm computing the singularities of an irreducible plane curve, defined by the irreducible polynomial $f(x,y)$, and their character can be given as follows: the singularities of the affine curve C given by $f(x,y)$ are the solutions of the system of algebraic equations

$$f(x,y) = 0, \quad \frac{\partial f}{\partial x}(x,y) = 0, \quad \frac{\partial f}{\partial y}(x,y) = 0.$$

Similarly the singularities of the projective curve C^* given by $F(x,y,z)$, the homogenization of $f(x,y)$, can be computed by setting one of the variables x,y,z to 1, thus getting affine curves C_x, C_y, C_z, and computing the singularities of these three affine curves. The corresponding systems of algebraic equations can be solved either by resultant computations or by the Gröbner basis method, as described in Buchberger (1985). Now successively each singular point P is moved to the origin and the multiplicity and character of P are determined by the preceding considerations.

The rationality problem for an affine curve is equivalent to the rationality problem for the associated projective curve.

Lemma 1: *Let C be an irreducible affine curve and C^* its corresponding projective curve. Then C is rational if and only if C^* is rational, and a parametrization of C can be computed from a parametrization of C^* and vice versa.*

Proof: Let $(x(t) = u_1(t)/u_2(t),\ y(t) = v_1(t)/v_2(t),\ z(t) = w_1(t)/w_2(t))$ with $u_i, v_i, w_i \in \mathbb{K}[t]$ be a rational parametrization of C^*. Observe that $w_1(t)$ cannot be identically equal to zero. Hence $(x(t) = u_1(t)w_2(t)/u_2(t)w_1(t),\ y(t) = v_1(t)w_2(t)/v_2(t)w_1(t))$ is a rational parametrization of C. The same argument also holds for u_1 and v_1.

Conversely, a rational parametrization of C can always be extended to a parametrization of C^* by setting the z–coordinate to 1. □

Observe that, as we have just proved, one can always assume that the rational functions giving the parametrization of a projective curve are not identically zero. Consequently, in the sequel we will always refer to a normalized parametrization of a projective curve, in the sense that the rational function giving the z–coordinate is the constant 1.

By Lemma 1 it is clear that deciding the rationality of an affine curve or a projective curve are equivalent problems. Moreover, their parametrizations are essentially the same. Therefore, we will work, without loss of generality, only with projective curves.

In the special case of an irreducible projective curve C^* 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 neighbouring points.

The tranformation of the projective plane $\mathbb{P}^2$ defined by $x' = yz,\ y' = xz,\ z' = xy$, where $(x : y : z)$ and $(x' : y' : z')$ are the coordinates of a point of $\mathbb{P}^2$ in two different coordinate systems, is called a *quadratic transformation*. For the special points $(1 : 0 : 0)$, $(0 : 1 : 0)$ and $(0 : 0 : 1)$ the quadratic transformation is not defined. These points are called the *fundamental points* of the transformation. Every point lying on one of the lines $x = 0$, $y = 0$ or $z = 0$ is sent to the point $(1 : 0 : 0)$, $(0 : 1 : 0)$ or $(0 : 0 : 1)$, respectively. These lines are called the *irregular lines* of the transformation. One can easily prove that this transformation defines a one to one correspondence between points of $\mathbb{P}^2$ not on irregular lines.

Now we study the action of a quadratic transformation on an irreducible projective curve C^*. Let C^* be defined by the homogeneous polynomial $F(x, y, z)$. Then the polynomial $G(x, y, z) = F(yz, xz, xy)$ is called the *algebraic transform* of F. However, although F is irreducible, G may have some irregular line as a factor. The *quadratic transform* of F is defined as the irreducible factor of G that is not an irregular line. We will denote it by F', and we will also say that the curve C'^* defined by F' is the quadratic transform of C^*.

The importance of quadratic transformations stems from the fact that by a finite sequence of quadratic transformations and changes of coordinates (i.e. moving certain points to the origin) the singularities of any irreducible plane curve can be resolved, i.e. the curve can be transformed into one having only ordinary singularities. Moreover, the rationality of the irreducible curve is invariant under these transformations. For future reference we quote a theorem from Walker (1950) which states how the singularities of a curve are effected by a quadratic transformation.

Theorem 1: *Let C^* be a curve of degree d defined by F and having $(1 : 0 : 0)$, $(0 : 1 : 0)$ and $(0 : 0 : 1)$ as points of multiplicity r_1, r_2 and r_3, respectively ($r_i \geq 0$). Let F' be the quadratic transform of F and C'^* the curve defined by F'. Then if no tangent at any of these points is an irregular line, the following holds:*

(1) The degree of F' is $2d - r_1 - r_2 - r_3$ and $F'(x, y, z) = F(yz, xz, xy)/x^{r_1}y^{r_2}z^{r_3}$. Furthermore, if $F(x, y, z) = f_d(x, y) + \cdots + f_{r_3}(x, y)z^{d-r_3}$, then

$$F' = x^{d-r_3-r_1}y^{d-r3-r2}f_{r_3} + \cdots + z^{d-r_3-1}x^{1-r_1}y^{1-r_2}f_{d-1} + z^{d-r_3}x^{-r_1}y^{-r_2}f_d.$$

(2) There is a one to one correspondence, preserving multiplicities, between the tangents to C^* at $(1:0:0),(0:1:0)$ and $(0:0:1)$ and the non–fundamental intersections of C'^* with the irregular lines $x=0,\ y=0$ and $z=0$, respectively.

(3) An r–fold point of C^* not on an irregular line is transformed into an r–fold point on C'^*, and the tangents at these two points correspond in multiplicity. In particular, the character of the r–fold point is preserved.

(4) C'^* has multiplicity $d-r_2-r_3, d-r_1-r_3, d-r_1-r_2$ at $(1:0:0),(0:1:0),(0:0:1)$, respectively, the tangents being distinct from the irregular lines and corresponding to the non–fundamental intersections of C^* with $x=0, y=0, z=0$, respectively. □

We describe an outline of a method for obtaining this sequence of quadratic transformations resolving the singularities of a given irreducible curve C^*:

(1) Choose a non–ordinary singularity of C^* and make a change of coordinates such that the singularity is moved to $(0:0:1)$, none of its tangents is an irregular line, and no other fundamental point is singular.

(2) Apply the quadratic transformation to C^*, getting the transform curve C'^*.

(3) Check whether there exists a non–fundamental intersection of C'^* and $z=0$, being a non–ordinary singular point. If this is the case, apply (1) and (2) to C'^* and this non–ordinary singular intersection point. Otherwise, choose any other non–ordinary singularity and repeat the process, until there are no non–ordinary singularities left.

This method selects a coordinate system, and also the order in which the non–ordinary singularities of the curve are moved to the fundamental points. One can prove that independent of these selections, the method always achieves an irreducible curve having only ordinary singularities in a finite number of steps. In the sequel, when we will speak about finite sequences of quadratic transformations reducing a given curve, we will assume that these sequences are obtained by the preceeding method.

Thus, theoretically, the rationality of a curve can be decided. However, the problem can be solved computationally in a more convenient way. For this purpose we introduce the concept of neighbouring points.

Let C^* be the irreducible curve of degree d defined by $F(x,y,z)$, and $\mathcal{T}=(T_1,\ldots,T_n)$ a finite sequence of quadratic transformations constructed as it has been described above and reducing C^* to a curve which has only ordinary singularities. We adopt the convention that T_i represents the composition of the quadratic transformation with a suitable change of the coordinate system that moves one of the singularities to a fundamental point. Let us also assume that $\mathcal{T}$ generates the sequence of irreducible curves

$$C^*=C_0^*\xrightarrow{T_1}C_1^*\xrightarrow{T_2}\cdots\xrightarrow{T_n}C_n^*,$$

where C_{i+1}^* is the quadratic transformation obtained from C_i^* by T_{i+1}, for $0\le i\le n-1$. Given an r–fold point P on C^*, suppose that during the process described by $\mathcal{T}$ the point P has not been translated to a fundamental point till the action of the i–th quadratic transformation. Then the *first neighbourhood* of P with respect to $\mathcal{T}$ is defined as the set of all the non–fundamental intersections of the curve C_{i+1}^* with the irregular line $z=0$, assuming that P was moved to $(0:0:1)$ by the according change of coordinates. Similarly, we take the non–fundamental intersections of C_{i+1}^* with $x=0$ or $y=0$ if P was translated to $(1:0:0)$ or $(0:1:0)$, respectively. The points in the first neighbourhood of P with respect to $\mathcal{T}$ are called the *neighbouring points of P at its first neighbourhood*. Using the fact that every neighbouring point P' of P at its first neighbourhood is a point on C^*_{i+1}, one defines the multiplicity and the character of P' as the multiplicity and character of P' as a point on C^*_{i+1}. Similarly, if $\{P'_1, \ldots, P'_s\}$ is the first neighbourhood of P with respect to $\mathcal{T}$, we get the second neighbourhood of P with respect to $\mathcal{T}$ as the union of the first neighbourhoods of P'_k, $k = 1, \ldots, s$. The points in the second neighbourhood of P with respect to $\mathcal{T}$ are called the *neighbouring points of* P *at its second neighbourhood.* The multiplicity and character of points at the second neighbourhood are defined in a way analogous to the one for points in the first neighbourhood. But, one must realize that now it may happen that not all the neighbouring points are lying on the same curve. These notions are easily extended to neighbourhoods of arbitrarily high order. In general, we will call any point in one of the neighbourhoods of P a *neighbouring point* of P. The neighbouring points of P with multiplicity higher than 1 will be called the *singular neighbouring points* of P.

Let P be a singular point of C^*, $\mathcal{T}$ the sequence of quadratic transformations as above. Then the *neighbourhood tree* of P w.r.t. C^* and $\mathcal{T}$ is the tree that has P as its root and the neighbourhood trees of the singular neighbouring points in the first neighbourhood of P as its subtrees. Finally, we define the *neighbourhood graph* of C^* w.r.t. $\mathcal{T}$ as the collection of all the neighbourhood trees of singular points w.r.t. C^* and $\mathcal{T}$.

If a fundamental point P, say $P = (0:0:1)$, is an r–fold point of the projective curve defined by $F(x,y,z) = f_d(x,y) + \cdots + f_0(x,y)z^d$ and if the polynomial $f_r(x,y)$ factors over $\mathbb{K}$ as

$$f_r(x,y) = (a_1x - b_1y)^{r_1} \cdots (a_sx - b_sy)^{r_s}$$

then the first neighbourhood of P is $\{P_i = (a_i : b_i : 0)\}_{i=1,\ldots,s}$. (I.e., the neighbouring points are determined by the tangents.) To prove this, let u and v be the multiplicities of $(0:1:0)$ and $(1:0:0)$, respectively, on the curve. The quadratic transform of F satisfies

$$F'(x,y,0) = x^{d-v-r}y^{d-u-r}f_r(y,x)$$

(see Theorem 1), and therefore the non–fundamental intersections are given by the factors of $f_r(x,y)$.

The neighbouring points of simple points are always simple points, and if P is an ordinary r–fold point its first neighbourhood contains exactly r simple points. Therefore, whenever a neighbourhood tree contains an ordinary singular point P, then the associated branch of the tree terminates in P. So the neighbourhood graph of any curve is finite.

Let us continue using the notation introduced above. That is, C^* is an irreducible projective curve, $\mathcal{T} = (T_1, \ldots, T_n)$ is a sequence of quadratic transformations reducing C^* and $C^* = C^*_0, \ldots, C^*_n$ is the sequence of projective curves generated by $\mathcal{T}$. Let d_i denote the degree of C^*_i, S_i the set of singularities of C^*_i and N_i the neighbourhood graph of C^*_i w.r.t. $\mathcal{T}$. Also, for simplicity, when we work with a point P in either S_i or N_i we will denote by r_P its multiplicity on the corresponding curve.

Theorem 2: *(1)* C^* *is rational if and only if* $(d_n-1)(d_n-2) = \sum_{P\in S_n} r_P(r_P-1)$.
(2) For every i, $0 \le i < n$,

$$(d_i-1)(d_i-2) - \sum_{P\in N_i} r_P(r_P-1) = (d_{i+1}-1)(d_{i+1}-2) - \sum_{P\in N_{i+1}} r_P(r_P-1).$$

(3) C^* *is rational if and only if* $(d-1)(d-2) = \sum_{P\in N_0} r_P(r_P-1)$.

Proof: (1) The rationality is invariant under the action of a quadratic transformation. Therefore, C^* is rational if and only if C_n^* is rational. But since all the singularities of C_n^* are ordinary, the curve C_n^* is rational if and only if $(d_n-1)(d_n-2) = \sum_{P\in S_n} r_P(r_P-1)$.

(2) Let $S_i = \{P_1, P_2, P_3, \ldots, P_s\}$, where $P_1 = (1:0:0), P_2 = (0:1:0), P_3 = (0:0:1)$. By abuse of notation we include all the fundamental points in S_i, even if they are not singular points of the curve C_i^*. That, however, does not affect the count in the equation. The points in S_{i+1} are the singular neighbouring points of P_1, P_2, P_3 at their first neighbourhood w.r.t. $\mathcal{T}$, the transformed points $T_{i+1}(P_k)$ of P_k, $4 \le k \le s$, and possibly three new ordinary singularities Q_1, Q_2, Q_3 (Theorem 1(4)). Again w.l.o.g. we include Q_j in S_{i+1}, even if it is a simple point. The quadratic transformation does not affect the character and multiplicity of P_k, $4 \le k \le s$, so we identify P_k and $T_{i+1}(P_k)$, $4 \le k \le s$. The points Q_i, $1 \le i \le 3$, do not have any neighbouring singularities. So the equation is equivalent to

$$(d_i-1)(d_i-2) - \sum_{j=1}^{3} r_{P_j}(r_{P_j}-1) = (d_{i+1}-1)(d_{i+1}-2) - \sum_{j=1}^{3} r_{Q_j}(r_{Q_j}-1)$$

(compare Fig. 1). But this follows immediately from the relations

$$d_{i+1} = 2d_i - \sum_{j=1}^{3} r_{P_j}, \qquad r_{Q_j} = d_i - \sum_{\substack{k=1\\k\neq j}}^{3} r_{P_k}, \quad 1 \le j \le 3.$$

(3) The statement follows immediately from (1) and (2). $\square$

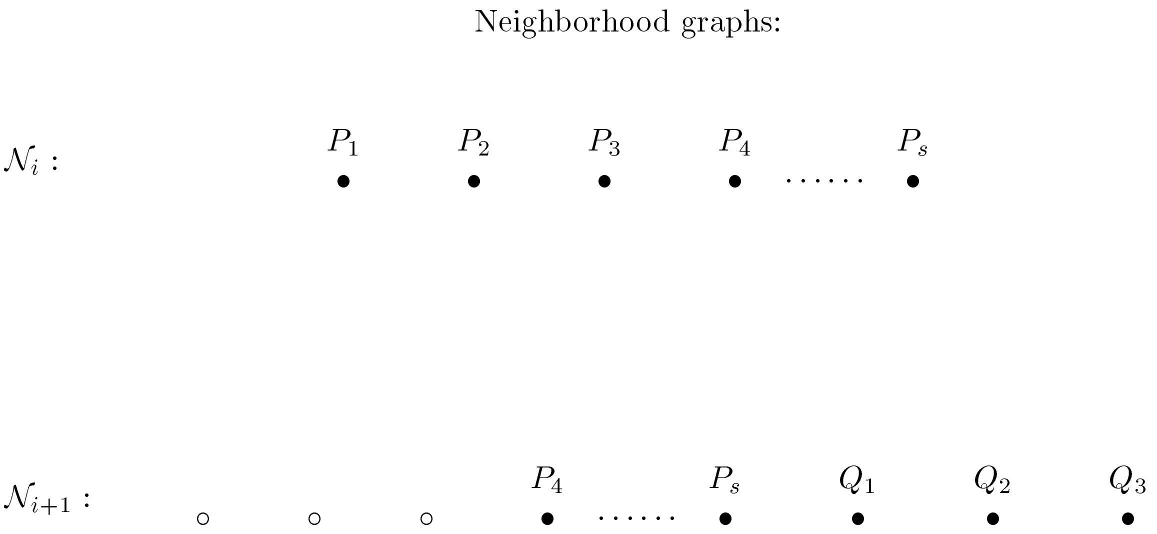

Fig. 1

In general, we will not compute the whole sequence of transform curves of the given curve C^*. Instead, we will act in an equivalent way: Let $\{P_1, \ldots, P_s\}$ be the set of all the non–ordinary singular points of the curve C^* of degree d. It is clear that for every P_k there always exists a sequence of quadratic transformations $\mathcal{T}(P_k) = (T_{1,k}, \ldots, T_{n_k,k})$ reducing C^* to a curve having only ordinary singularities and such that P_k is moved to a fundamental point by the action of $T_{1,k}$. Then, for every P_k, we only compute the sequence $\mathcal{T}(P_k)$ till all the neighbouring points of P_k w.r.t. $\mathcal{T}(P_k)$ have been determined, that is till another $P_{k'}$ is moved to a fundamental point. Let us say that this sequence is $\mathcal{T}^*(P_k) = \{T_{1,k}, \ldots, T_{r_k,k}\}$, $r_k \leq n_k$, and it generates the sequence of curves

$$C^* \xrightarrow{T_{1,k}} C_1^*(P_k) \xrightarrow{T_{2,k}} \cdots \xrightarrow{T_{r_k,k}} C_{r_k}^*(P_k),$$

where in general $C_{r_k}^*(P_k)$ can have non–ordinary singularities, but these are not singular neighbouring points of P_k. Then at the end of this process we have

$$\begin{array}{c} C^* \longrightarrow C_1^*(P_1) \longrightarrow \cdots \longrightarrow C_{r_1}^*(P_1), \\ \cdots\cdots\cdots \\ C^* \longrightarrow C_s^*(P_s) \longrightarrow \cdots \longrightarrow C_{r_s}^*(P_s). \end{array}$$

Lemma 2: *Let $P_1, \ldots, P_s$ be the singularities of the projective curve C^*. Let $S = \{P_1, \ldots, P_s\} \cup N(P_1) \cup \ldots \cup N(P_s)$, where $N(P_k)$ is the set of all the neighbouring singularities of P_k w.r.t. $\mathcal{T}^*(P_k)$ as above. For every $P \in S$ let r_P denote the multiplicity of P. Then C^* is rational if and only if $(d-1)(d-2) = \sum_{P \in S} r_P(r_P - 1)$.*

Proof: Taking into account the result stated in the third statement of Theorem 2, it is enough to note that the multiplicity of a neighbouring point does not depend on the reduction process of other singularities. □

Thus, the rationality of an irreducible affine algebraic plane curve C can be determined computationally by analyzing the multiplicities of the singularities and neighbouring singularites of its associated projective curve C^*.

<u>Algorithm</u> RATIONALITY
The input is an irreducible algebraic plane curve C of degree d, defined by the irreducible polynomial $f(x, y)$, and the output is the decision of the rationality of C.

(1) Compute the homogeneous polynomial $F(x, y, z)$ corresponding to f.
(2) Determine, using the quadratic transformation techniques explained above, the neighbourhood graph $\mathcal{N}$ of the projective curve C^* defined by F, computing also the multiplicity r_P of every point P in $\mathcal{N}$.
(3) Set $g = (d-1)(d-2) - \sum_{P \in \mathcal{N}} r_P(r_P - 1)$.
(4) If $g = 0$, then return "C is rational", otherwise return "C is not rational". □

III. Parametrization methods

In this chapter let us assume that the irreducible curve C^* of degree d defined by $F(x, y, z) = 0$ is rational. We describe methods for actually computing a rational parametrization.

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.

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

(1) every r–fold singular point on C^* is an $(r-1)$–fold point on D^*,
(2) every s–fold singular neighbouring point of C^* is an $(s-1)$–fold neighbouring point of D^* w.r.t. the same sequence of transformations,
(3) there exist $ad-(d-1)(d-2)-1$ simple points on C^* that are also simple points on D^*,
(4) 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 neighbouring 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 (3) we fix just so many simple intersection points of C^* and D^* as to leave at most one intersection point undetermined. This approach of course works only if the formula in (3) is nonnegative, i.e. if $a \geq d-2$.

<u>Pencil of degree $d-2$ or $d-1$</u>

Since C^* is irreducible and the degree of D^* is less than d, condition (4) is obviously satisfied for any pencil of degree $d-2$ or $d-1$. One can prove as follows that almost every curve in a pencil satisfying the requirements (1) – (3) has exactly $da-1$ intersections with C^* at the fixed common points, and therefore (by Bezout's theorem) almost every curve in the pencil meets C^* in one additional point.

Lemma 3: *The pencil of curves D^* of degree $a \in \{d-2, d-1\}$ satisfying (1) – (4) 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 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.*

Proof: By S let us denote the set of singularities of C^*, including the neighbouring singularities. By r_P we denote the multiplicity of a point P in S (on either C^* or the corresponding quadratic transformation of C^*). Then if N is the number of intersections of C^* and D^* at the fixed common points, N is bounded from below by

$$N \geq \sum_{P \in S} r_P(r_P-1) + ad - (d-1)(d-2) - 1.$$

Since C^* is rational we may substitute $(d-1)(d-2)$ for the sum in the formula, thus getting $N \geq ad-1$. On the other hand D^* satisfies (4). Therefore, according to Bezout's theorem,

$$da - 1 \leq N \leq da.$$

Now let us deal with the actual construction of the pencil. In order to describe the process for obtaining the pencil of degree a we suppose that Q is a fixed simple point on C^*, that P is an r–fold point of C^* $(r > 1)$, and that P' is an s–fold neighbouring point of P $(s > 1)$, lying on some transform of C^*. (Observe that condition (4) is always satisfied.)

Note that a curve of degree a has $m = (a+1)(a+2)/2$ coefficients. Let $u_1, \ldots, u_m$ be the power products of degree a in the variables x, y, z. Then, if H denotes the homogeneous polynomial defining a generic curve D^* in the pencil, H may be written as

$$H(x, y, z) = a_1 u_1 + \cdots + a_m u_m,$$

where the a_i are undetermined coefficients.

First we force Q to be a point on D^* by setting $H(Q) = 0$. We force P to have multiplicity at least $r - 1$ on D^*, and P' to be a neighbouring point of P of multiplicity at least $s - 1$ on D^*. This is achieved by setting the appropriate derivatives of H or its transform at P or P', respectively, equal to zero. All these conditions lead to exactly $m-2$ linear equations in the coefficients of H.

On the other hand, the number of independent coefficients defining D^* is $m-1$ (one of the coefficients in the homogeneous polynomial H can be chosen to be 1). Consequently, if we prove that the obtained linear system of $m - 2$ equations has maximum rank, a solution of it by means of a parameter t will achieve the expression of the pencil depending polynomially only on t. To justify that the $m-2$ equations are independent, let us assume that the rank of the system is $m - \epsilon$, with $\epsilon > 2$. Then $\epsilon - 2$ equations can be deleted from the system. Solving the new system, we obtain a pencil depending on $\epsilon - 1$ parameters. So if we take two new simple points lying on C^*, and since the pencil depends on at least two parameters, we can force the pencil to pass through these two new simple points. But then any curve in the pencil cuts C^* at least $da + 1$ times, which is impossible according to Bezout's theorem.

Now we see that the linear conditions derived from the fixed common points imply that Q is a point of multiplicity 1 on D^*, that P is an $(r-1)$–fold point on D^*, and that P' is an $(s-1)$–fold neighbouring point of P on D^*. Suppose that one of the fixed common points has a higher multiplicity than the desired one. This implies that although we have the same number of independent equations, C^* and D^* meet on the fixed common points at least da times. Thus, we can apply the same argument as above, taking a new simple point on C^* and forcing D^* to pass through it. Therefore, all the fixed common points have exactly the desired multiplicity on D^*.

Finally, if for a given curve D^* in the pencil $N = da$, C^* and D^* must have a common tangent at some fixed common point. But this situation can occur only in finitely many cases, because we have fixed only finitely many common points and the coefficients of D^* are polynomials in one parameter t. Therefore, almost every curve in the pencil intersects C^* in one additional point.

Since D^* depends on one parameter t, we can force D^* to pass through any simple point P on C^* which is not a fixed common point. □

<u>Pencil of degree d</u>

We show that it is also possible to work with a pencil of curves of degree d.

LEMMA 4: *The pencil of curves D^* of degree d satisfying (1) – (4) 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 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.*

Proof: Let H be the homogeneous polynomial defining D^*. Then the number of coefficients of H is $m = (d+1)(d+2)/2$. From the conditions forcing all the simple, singular, and neighbouring fixed common points to have at least the required multiplicities on D^* we obtain a linear system E in the coefficients of H with $m-3$ equations.

So now let us see how the condition (4) can be fulfilled. We assume that $\mathcal{P}$ is the subvectorspace of $\mathbb{K}^m$ defined by the solutions of the linear system E. It is clear that the dimension of $\mathcal{P}$ is at least three and that the vector c formed with the coefficients of C^* belongs to $\mathcal{P}$. In order to see that $\dim(\mathcal{P}) = 3$, let $\mathcal{V} = \{v_1, \ldots, v_k\}$ be a basis of $\mathcal{P}$. There exist $\lambda_1, \ldots, \lambda_k \in \mathbb{K}$, not all zero (say $\lambda_1 \neq 0$), such that $c = \lambda_1 v_1 + \cdots + \lambda_k v_k$. Now if $k > 3$, consider the vector $c' = t_2 v_2 + \cdots + t_k v_k$, with t_i some parameters. Since $\lambda_1 \neq 0$ and $\mathcal{V}$ is linearly independent, for no set of values for the parameters $t_2, \ldots, t_k$ does there exist a $\mu \in \mathbb{K}$ such that $c = \mu c'$. Therefore, since C^* is irreducible, for no values of the parameters do the curves C^* and $C^{*\prime}$ have a common component, where $C^{*\prime}$ is the curve defined by c'. Thus, according to Bezout's theorem, C^* and $C^{*\prime}$ have d^2 intersections. But this is impossible, because they already have $(d-1)(d-2) + 3(d-1) = d^2 - 1$ fixed intersections and $C^{*\prime}$ depends on at least two independent parameters. Therefore, $\dim(\mathcal{P}) = 3$ and $\mathcal{V} = \{v_1, v_2, v_3\}$. Now we let D^* be the pencil of curves of degree d whose coefficient vectors belong to the subvectorspace of $\mathbb{K}^m$ generated by $\mathcal{V}' = \{v_2, v_3\}$, where $c = \lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3$ and $\lambda_1 \neq 0$. In this way, every curve of D^* depends on two parameters. Since we are working with homogeneous polynomials, we can always consider that one of those parameters (e.g. the one associated with v_s) is 1. Therefore, D^* depends on only one independent parameter t. In this way we have forced the pencil D^* to satisfy the condition (4), because C^* cannot be a curve in the pencil.

To prove that D^* is exactly the required pencil, it only remains to show that the simple, singular, and neighbouring fixed common points have exactly the required multiplicities on D^*. The argument is the same as the one for the pencil of degree $d-1$ or $d-2$ and it is left to the reader.

Again by the same argument as in the previous section, one proves that for almost every curve in the pencil its number of intersections with C^* at the fixed common points is exactly $d^2 - 1$. Finally, we remark that since D^* depends on one parameter t, for every point P on C^* but the fixed common ones, there exists a curve in the pencil passing also through P. $\square$

In the sequel, when we will refer to a pencil D^* of curves of degree a, where a is $d, d-1$ or $d-2$, we will assume that such a pencil has been constructed in the way described above.

<u>Determination of intersection points</u>

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. First we quote some results giving information on how a common point of two curves affects the resultant of the polynomials defining the curves. Later we will apply these results to give a complete factorization of the resultant of F and H, where F defines the curve C^* and H defines the pencil D^*. In the sequel we denote by $\mathrm{Res}_v(A, B)$ the resultant of the polynomials A and B w.r.t. the variable v. For future reference we quote a statement from Walker (1950).

Lemma 5: *Let $f(x,y)$ and $h(x,y)$ be the polynomials defining the affine curves C_1 and C_2, respectively. Then if C_1 and C_2 have no intersection point on the x–axis except possibly at the origin, the resultant of f and h with respect to x has 0 as a root of multiplicity equal to the number of intersections of C_1 and C_2 at the origin.* □

For technical reasons we need the following lemma.

Lemma 6: *Let $F(x,y,z)$ and $H(x,y,z)$ be polynomials over $\mathbb{K}$ having no common factor. Then the resultant w.r.t x of $F(x+\lambda y+\mu z, y, z)$ and $H(x+\lambda y+\mu z, y, z)$ is independent of λ and μ.*

Proof: Let $R(y,z,\lambda,\mu)$ be the resultant of $F(x+\lambda y+\mu z, y, z)$ and $H(x+\lambda y+\mu z, y, z)$ w.r.t. x. F and H have no common factor, so $\mathrm{Res}_x(F,H)(y,z)$ does not vanish and hence is a polynomial over $\mathbb{K}$. Thus, since $R(y,z,0,0)=\mathrm{Res}_x(F,H)(y,z)$, R can be written as

$$R(y,z,\lambda,\mu) = U(y,z) + R'(y,z,\lambda,\mu) \quad \in \mathbb{K}[y,z][\lambda,\mu],$$

where $U(y,z)\neq 0$ and $R'(y,z,0,0)=0$. (Note that $U(y,z)=\mathrm{Res}_x(F,H)(y,z)$.) Now let us assume that R' is not identically zero. Then R' depends on at least one of the variables λ and μ, say μ. Thus, R' is a univariate polynomial of positive degree in μ, with coefficients in $\mathbb{K}[y,z,\lambda]$. Therefore, there exist $y_0, z_0, \lambda_0 \in \mathbb{K}$ such that

$$U(y_0,z_0)\cdot R'(y_0,z_0,\lambda_0,\mu)\neq 0.$$

$R(y_0,z_0,\lambda_0,\mu)\in\mathbb{K}[\mu]$ and $\deg_\mu(R(y_0,z_0,\lambda_0,\mu))\geq 1$. Since $\mathbb{K}$ is algebraically closed, there exists $\mu_0\in\mathbb{K}$ such that $R(y_0,z_0,\lambda_0,\mu_0)=0$. Thus, the polynomials $F(x+\lambda_0 y_0+\mu_0 z_0, y_0, z_0)$ and $H(x+\lambda_0 y_0+\mu_0 z_0, y_0, z_0)$ have a common root, and hence $F(x,y_0,z_0)$ and $H(x,y_0,z_0)$ also have a common root. This, however, is impossible since $\mathrm{Res}_x(F,H)(y_0,z_0)=U(y_0,z_0)\neq 0$. □

Now, returning to our problem, let C^* be an irreducible projective rational curve of degree d with defining polynomial F and let D^* be the generic representative of the pencil of a–degree curves with defining polynomial H, where $a\in\{d-2, d-1, d\}$. Let t be the independent parameter of D^*. Let us also suppose that

$$P_i = (\lambda_i, \mu_i, \rho_i), \quad 1\leq i\leq n,$$

are the singular points of C^*, where P_i is a point of multiplicity r_i on C^*, and that

$$Q_i = (\bar\lambda_i, \bar\mu_i, \bar\rho_i), \quad 1\leq i\leq ad-(d-1)(d-2)-1 =: M(a)$$

are the fixed common simple points of C^* and D^*. Let

$$\bar r_i := r_i(r_i-1) + \sum_{P\in N(P_i)} r_P(r_P-1), \quad 1\leq i\leq n,$$

where $N(P_i)$ is the set of neighbouring points of P_i w.r.t. C^* and some sequence of quadratic transformations and where r_P is the multiplicity of the neighbouring point P. With this notation we can formulate the theorem giving the complete factorization of the resultants of F and H.

Theorem 3: *With the notation introduced above, there exist polynomials $m_i(t), n_i(t)$, $1\leq i\leq 3$, in $\mathbb{K}[t]$, such that for almost all $t\in\mathbb{K}$ the following holds:*

(1) If $(1:0:0)$ is not on C^*, then

$$\mathrm{Res}_x(F,H) = \prod_{i=1}^{n}(\rho_i y - \mu_i z)^{\bar r_i}\cdot \prod_{i=1}^{M(a)}(\bar\rho_i y - \bar\mu_i z)\cdot(m_1(t)y - n_1(t)z).$$

(2) If $(0:1:0)$ is not on C^*, then

$$\mathrm{Res}_y(F,H) = \prod_{i=1}^{n}(\rho_i x - \lambda_i z)^{\bar r_i}\cdot \prod_{i=1}^{M(a)}(\bar\rho_i x - \bar\lambda_i z)\cdot(m_2(t)x - n_2(t)z).$$

(3) If $(0:0:1)$ *is not on* C^*, *then*

$$\mathrm{Res}_z(F,H) = \prod_{i=1}^{n}(\mu_i x - \lambda_i y)^{\bar{r}_i} \cdot \prod_{i=1}^{M(a)}(\bar{\mu}_i x - \bar{\lambda}_i y) \cdot (m_3(t)x - n_3(t)y).$$

Proof: We will only prove the first part of the theorem, parts (2) and (3) can be obtained analogously.

Almost every curve in the pencil D^* intersects C^* in the fixed common points exactly $da-1$ times. So for almost every $t \in \mathbb{K}$ there exists exactly one new common point of C^* and D^*. Let us assume that $w^t = (w_1^t : w_2^t : w_3^t)$ is the expression of this new point, where w_i^t are some functions depending on t.

Since C^* and D^* have no common components, the resultant of F and H w.r.t. x is not identically zero, and hence $\mathrm{Res}_x(F,H)$ is a homogeneous polynomial of degree da. $\mathrm{Res}_x(F,H)$ factors into linear factors over $\mathbb{K}$.

If $\mathrm{Res}_x(F,H)(b_1,b_2) = 0$ for some $b_1, b_2 \in \mathbb{K}$, with b_1 and b_2 not simultaneously zero, then $F(x,b_1,b_2)$ and $H(x,b_1,b_2)$ have a common factor. But $\mathbb{K}$ is algebraically closed, so this common factor has a root $b_0 \in \mathbb{K}$, and $(b_0 : b_1 : b_2)$ is a common point of C^* and D^*. Conversely, if $(b_0 : b_1 : b_2)$ is a common point of C^* and D^*, $\mathrm{Res}_x(F,H)(b_1,b_2) = 0$ with (b_1,b_2) a non–trivial solution, because it has been assumed that $(1:0:0)$ is not on C^*. Consequently, the resultant can be factorized as

$$\mathrm{Res}_x(F,H) = \prod_{i=1}^{n}(\rho_i y - \mu_i z)^{\epsilon_i} \cdot \prod_{i=1}^{M(a)}(\bar{\rho}_i y - \bar{\mu}_i z)^{\delta_i} \cdot (w_3^t y - w_2^t z)^{\gamma},$$

where ϵ_i, δ_i and γ are some positive integers.

Now, let us consider a factor $(b_2 y - b_1 z)$ of $\mathrm{Res}_x(F,H)$. W.l.o.g. we suppose that $b_2 \neq 0$. There exists at least one fixed common point $P = (b_0 : b_1 : b_2)$ generating this factor. Furthermore, there exists a line $L:\ c_0x + c_1y + c_2z = 0,\ c_0 \neq 0$, such that P is on L and L does not pass through any other common point. By the change of coordinates

$$x' = c_0x + c_1y + c_2z,\ y' = y - (b_1/b_2)z,\ z' = (1/b_2)z$$

the point P is sent to the origin and L is sent to the x–axis, i.e. the image of no other common point has the x–coordinate 0. On the other hand, by Lemma 6, the resultant w.r.t. x' of the transformed polynomials is $\mathrm{Res}_x(F,H)(y'+b_1z', b_2z')$, which has the factor y' to the same multiplicity as $\mathrm{Res}_x(F,H)(y,z)$ has the factor $(b_2y - b_1z)$. Let us assume that $f(x',y')$ and $h(x',y')$ are the polynomials obtained when z' is evaluated to 1 in the transformations of F and H, respectively. Thus, the affine curves defined by $f(x',y')$ and $h(x',y')$ have no common point on the x'–axis, with the exception of the origin. Therefore, according to Lemma 5, these affine curves meet at the origin as many times as the multiplicity of y' in $\mathrm{Res}_{x'}(f,h)(y') = \mathrm{Res}_x(F,H)(y'+b_1,b_2)$. Thus, the number of intersections of these affine curves at the origin is the multiplicity of the factor $(b_2y - b_1z)$ in $\mathrm{Res}_x(F,H)(y,z)$. Finally, since the number of intersections at P for almost every curve in the pencil and C^* is either $\bar{r}_i$ or 1, depending on whether P is a singular or a simple common point, it follows that the multiplicity of $(b_2y - b_1z)$ is the claimed one.

What remains to be seen is that the functions w_i^t are polynomials. But this follows from the fact that $F, H \in \mathbb{K}[t][x,y,z]$, and hence $\mathrm{Res}_x(F,H) \in \mathbb{K}[t][y,z]$. $\square$

COROLLARY: *Let $f(x,y)=F(x,y,1)$, $h(x,y)=H(x,y,1)$. Then*

$$\mathrm{Res}_x(f,h)=\prod_{i=1}^{n}(\rho_i y-\mu_i)^{\bar{r}_i}\cdot\prod_{i=1}^{M(a)}(\bar{\rho}_i y-\bar{\mu}_i)\cdot(m_1(t)y-n_1(t)),$$

$$\mathrm{Res}_y(f,h)=\prod_{i=1}^{n}(\rho_i x-\lambda_i)^{\bar{r}_i}\cdot\prod_{i=1}^{M(a)}(\bar{\rho}_i x-\bar{\lambda}_i)\cdot(m_2(t)x-n_2(t)).$$

$m_1(t), m_2(t)$ are not identically equal to zero.

Proof: The factorization of the resultants follows immediately from Theorem 3 and the evaluation homomorphism $z=1$, which can be applied before or after the resultant computation. $m_1(t)$ cannot be identically equal to zero, for otherwise at the roots of $n_1(t)$ one could choose any value for y to get an intersection point of C and $D(t)$. □

THEOREM 4: *Let C^* and D^* be as above, and $f(x,y)=F(x,y,1), h(x,y)=H(x,y,1)$. 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^*.*

Proof: As can be seen from the Corollary to Theorem 3, the factors $(u(t)x-v(t))$ and $(\bar{u}(t)y-\bar{v}(t))$ of $\mathrm{Res}_y(f,h)$ and $\mathrm{Res}_x(f,h)$, respectively, correspond to a common point of C^* and D^* for almost every value of t. Therefore, there exist functions $A(t), B(t)$ such that for almost every $t\in\mathbb{K}$, the point $(v(t):B(t):u(t))=(A(t):\bar{v}(t):\bar{u}(t))$ is on the curve C^*. So for almost every $t\in\mathbb{K}$ there exists a non–zero constant ρ such that $(v(t),B(t),u(t))=\rho\cdot(A(t),\bar{v}(t),\bar{u}(t))$. This leads to $B(t)=\rho\cdot\bar{v}(t)=\frac{u(t)}{\bar{u}(t)}\cdot\bar{v}(t)$. Thus, for almost every $t\in\mathbb{K}$, the point

$$u(t)\cdot(\frac{v(t)}{u(t)}:\frac{\bar{v}(t)}{\bar{u}(t)}:1)=(\frac{v(t)}{u(t)}:\frac{\bar{v}(t)}{\bar{u}(t)}:1)$$

is on C^*.

On the other hand, for every point P on C^* distinct from the fixed common points one can obtain a curve in the pencil D^* such that P is the new intersection point between C^* and the chosen curve in the pencil. To achieve that, one just has to evaluate the polynomial H defining D^* at the point P and determine a root t_0 of the result. Then the point P is

$$(\frac{v(t_0)}{u(t_0)}:\frac{\bar{v}(t_0)}{\bar{u}(t_0)}:1).$$ □

To finish this chapter, we give an outline of an 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) Compute the homogeneous polynomial $F(x,y,z)$ corresponding to $f(x,y)$.
(2) Determine the singularities of the projective curve C^* defined by F, including the neighbouring ones, and their multiplicities. (Note that if the rationality of C has been decided using the algorithm RATIONALITY, this information has already been obtained.)

(3) Choose a in $\{d-2, d-1, d\}$, and determine $ad-(d-1)(d-2)-1$ simple points on C^*.

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

(5) Let $S_1(y)$ be the primitive part of $\text{Res}_x(f,h)$ with respect to t, i.e. view $\text{Res}_x(f,h)$ as a univariate polynomial in t and eliminate the common factors of the coefficients; let $S_2(x)$ be the primitive part of $\text{Res}_y(f,h)$ with respect to t. By the Corollary to Theorem 3 $S_1(y)$ is linear in y and $S_2(x)$ is linear in x.

(6) 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.

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

The algorithm PARAMETRIZE always returns a proper parametrization in the sense of Sederberg (1986). Let the curve C be defined by the polynomial f. If $\mathcal{P}=(x(t)=\frac{u_1(t)}{v_1(t)},\ y(t)=\frac{u_2(t)}{v_2(t)})$ is the parametrization of C computed by PARAMETRIZE, then u_1, v_1 are relatively prime, u_2, v_2 are relatively prime, $\max\{\deg_t(u_1), \deg_t(v_1)\}=\deg_y(f)$ and $\max\{\deg_t(u_2), \deg_t(v_2)\}=\deg_x(f)$.

IV. Symbolic treatment of the rationality problem

In this chapter and also in the subsequent ones we start with an irreducible curve C given by a polynomial $f(x,y)\in\mathbb{F}[x,y]$, where $\mathbb{F}$ is a computable field of characteristic 0, i.e. all the field operations are computable. We do not assume that $\mathbb{F}$ is algebraically closed.

The algorithm RATIONALITY computes the neighbourhood graph of a curve and decides its rationality depending on the multiplicities of the points in the neighbourhood graph. Therefore, one only needs to compute the singular points of the curve, including the neighbouring ones, their multiplicities and characters.

For symbolically treating the rationality problem we decompose the set of singularities of the given curve as a union of special families of points such that the neighbourhood graph, and therefore the genus, can be computed without introducing algebraic numbers. We call such a decomposition a "standard decomposition". The basic idea of this approach is to work simultaneoulsy with all the points in the same family, determining a symbolic neighbourhood graph for each family.

Standard decomposition of the set of singularities

We deal with the affine singularities of the curve C^* (for singularities at infinity one just has to dehomogenize the defining polynomial F suitably). So in fact we consider the singular points of C. For this purpose let us assume w.l.o.g. that the defining polynomial f satisfies the conditions

- the coefficient of y^d in f is nonzero,
- if $f(x_0,y_i)=\frac{\partial f}{\partial x}(x_0,y_i)=0$ for $i=0,1$ then $y_0=y_1$.

This situation can be achieved algorithmically by a suitable change of coordinates, see for instance Sakkalis & Farouki (1990).

Now for $i \geq 1$ let us consider the polynomials

$$\begin{aligned}
\bar{B}_i &= \gcd(\mathrm{Res}_y(f, \frac{\partial f}{\partial x^i}), \mathrm{Res}_y(f, \frac{\partial f}{\partial x^{i-1} y}), \ldots, \mathrm{Res}_y(f, \frac{\partial f}{\partial y^i})), \\
B_i &= \frac{\bar{B}_i}{\gcd(\bar{B}_i, \bar{B}_i')}, \\
\bar{A}_i &= \frac{B_i}{B_{i+1}}.
\end{aligned}$$

Note that since C has finitely many singularities there can only exist finitely many non–constant polynomials $\bar{A}_i$. The x–coordinates of the $(i+1)$–fold affine points of C are exactly the roots of $\bar{A}_i$. Finally, we factorize the polynomials $\bar{A}_i$ to detect the rational singular points of the curve. In fact, all the subsequent operations can be carried out without this requirement, but we do not want to investigate this here.

The next step consists of applying the Gröbner basis algorithm or polynomial remainder sequences, Kalkbrener (1990), to the systems

$$\{f = 0,\ \frac{\partial f}{\partial x} = 0,\ \bar{A}_i = 0\}$$

to express the affine singularities of C as

$$\bigcup_{i \in I} \{(\alpha, \frac{m_i(\alpha)}{n_i(\alpha)})\}_{p_i(\alpha)=0}\ ,$$

where $m_i, m_i, p_i \in \mathbb{F}[x]$, p_i is irreducible, and each family of points contains only affine singularities of the same multiplicity. Repeating this process for singular points at infinity, we finally get a decomposition of the set of singularities of the projective curve C^* as

$$\bigcup_{i \in I} \{(m_i^{(1)}(\alpha) : m_i^{(2)}(\alpha) : m_i^{(3)}(\alpha))\}_{A_i(\alpha)=0}\ , \qquad (*)$$

where $m_i^{(1)}, m_i^{(2)}, m_i^{(3)}, A_i \in \mathbb{F}[x]$, A_i is irreducible, and each family of points contains only singularities of the same multiplicity. We will then say that the set of singularities *is decomposed in standard form*, $(*)$ is a *standard decomposition* of the set of singularities of C^*, and the families of points in $(*)$ are *standard families.*

Character of standard families

In order to compute the neighbourhood graph of C^* we still need to know the character of the singularities. However, this can be achieved easily because each standard family can only contain singularities of the same character. More precisely, we give the following algorithmic criterium: Take a generic representative P_α of the family $\mathcal{F}_i$ of r–fold points defined by $A_i(\alpha)$, and move P_α to the origin (we assume for simplicity that the points of $\mathcal{F}_i$ are not at infinity). Let $F_1(x, y, z, \alpha)$ be the transformation of $F(x, y, z)$ after this change of coordinates, and let $T(x, y, \alpha)$ be the coefficient of z^{d-r} in F_1. Compute $D_T(\alpha) = \mathrm{discriminant}_x(T(x, 1, \alpha))$. Now, since A_i is irreducible, the family $\mathcal{F}_i$ contains only points of the same character. Furthermore, $\mathcal{F}_i$ is a family of ordinary singularities if and only if $D_T(\alpha) \neq 0 \pmod{A_i}$.

Expansion of the neighbourhood graph

Finally, we deal with the computation of the neighbourhood graph. Given a family $\mathcal{F}$ of singular points of C^*, the idea consists of computing the neighbourhood graph of $\mathcal{F}$, that is a generic representative of the families of graphs derived from the points of $\mathcal{F}$.

To be more precise, let $\mathcal{F} = \{(m^{(1)}(\alpha) : m^{(2)}(\alpha) : m^{(3)}(\alpha))\}_{A(\alpha)=0}$ be a family of r–fold non–ordinary points in the standard decomposition of the set of singularities of C^*. We take a generic representative $P_\alpha = (m^{(1)}(\alpha) : m^{(2)}(\alpha) : m^{(3)}(\alpha))$ of $\mathcal{F}$ and apply a change of coordinates such that P_α is moved to the origin, no irregular line is a tangent to C^* at P_α, and the irregular points $(0:1:0), (1:0:0)$ are not points of C^*. Let us denote by $F_1(x, y, z, \alpha)$ the polynomial defining the transformed curve, and by $T(x, y, \alpha)$ the coefficient of z^{d-r} in F_1. Then the first neighbourhood of P_α can be expressed as

$$\{(\beta : 1 : 0)\}_{A_1(\beta,\alpha)=0} \ ,$$

where

$$A_1(x, \alpha) = \frac{T(1, x, \alpha)}{\gcd(T(1, x, \alpha), \frac{\partial T(1,x,\alpha)}{\partial x})}.$$

Hence, the set of all the singularities in the first neighbourhood of every point in $\mathcal{F}$ can be written as

$$\mathcal{F}_1 = \left\{\{(\beta : 1 : 0)\}_{A_1(\beta,\alpha)=0}\right\}_{A(\alpha)=0} \ .$$

We say that $\mathcal{F}_1$ is the first neighbourhood of $\mathcal{F}$.

In order to compute the second neighbourhood of $\mathcal{F}$ we need to obtain the standard decomposition of $\mathcal{F}_1$ as well as the character of the corresponding families. To achieve this, one can apply the previous argument to the quadratic transform of C^*. However, since $\mathcal{F}_1$ has a very special structure, one can achieve these results more efficiently by taking into account that a polynomial $G \in \mathbb{F}[x, y, z]$ vanishes on all the points of $\mathcal{F}_1$ if and only if the remainder w.r.t. s of dividing $G(s, 1, 0)$ by $A_1(s, \alpha)$ is zero modulo $A(\alpha)$.

Analogously, one can determine the neighbourhoods of $\mathcal{F}$ of higher order. Finally, the i–th neighbourhood of the family $\mathcal{F}$ will be decomposed as a union of families of the form

$$\{\cdots\{\{(\alpha_i : 1 : 0)\}_{A_i(\alpha_1,\ldots,\alpha_i)=0}\}\cdots\}_{A_1(\alpha_1)=0} \ ,$$

where $A_i \in \mathbb{F}[x_1, \ldots, x_i]$, A_i is irreducible, and all the singularities in the family are of the same multiplicity.

V. Symbolic treatment of the parametrization problem

The input of PARAMETRIZE is an irreducible rational affine curve C of degree d, defined by the irreducible polynomial $f(x, y)$. Let C^* be the projective curve associated with C and $F \in \mathbb{F}[x, y, z]$ its defining homogeneous polynomial. We assume that the singular points of C^*, including the neighbouring ones, and their multiplicities and characters have already been determined by an application of the algorithm RATIONALITY.

The difficulties appear in the construction of the pencil used in the parametrization algorithm. More precisely, difficulties can appear in:

(1) the selection of the fixed simple points on C^*,

(2) passing the pencil through the fixed simple points on C^*,
(3) passing the pencil through the singularities of C^*, including the neighbouring ones.

Let us start with the selection of the fixed simple points on C^*. In the study of this situation, let us assume that D_a^* is the pencil of curves of degree a, $a \in \{d-2, d-1, d\}$, that we have to construct, and that H is its definining homogeneous polynomial. In determining H, we must guarantee that C^* and D_a^* have exactly $M(a) = (a-d+2)d + (d-3)$ fixed common simple points in addition to the common singular points. A very first approach to compute the $M(a)$ simple points may be the following process:

(1) Take a line $L = (a_1 + b_1 t : a_2 + b_2 t : a_3 + b_3 t)$ not cutting C^* only at singular points.
(2) Cut C^* with the line L, that is compute $p(t) = F(a_1 + b_1 t, a_2 + b_2 t, a_3 + b_3 t)$.
(3) Compute an irreducible monic factor $q(t)$ of $p(t)$ such that none of the values of t corresponding to a singular point is a root of $q(t)$. Then $(a_1+b_1\beta : a_2+b_2\beta : a_3+b_3\beta)$, where $q(\beta) = 0$, is a simple point on C^*.

Repeating this process $M(a)$ times, one obtains all the necessary simple points, each one of them depending on a different algebraic number β of degree at most d.

On the other hand, one can also apply the classical method of Hilbert & Hurwitz (1890) and Poincaré (1901), based on birational transformations, to compute the $M(a)$ fixed points. Using this approach one only introduces algebraic numbers of degree at most 2. However, both methods can be very expensive. In the following we describe a process based on the idea of working with whole classes of conjugate points. Thereby the problem of constructing the common simple points is reduced to the determination of only one simple point on the curve C^*. This point may be computed by means of the methods mentioned above.

Until now we have been speaking about a pencil D_a^* of degree a, where a could be $d-2, d-1$ or d, but we have made no remark about the advantages of using one or the other degree. Moreover, we have presented the algorithm PARAMETRIZE for an arbitrary a in $\{d-2, d-1, d\}$. If we are working numerically, we obviously choose $a = d-2$, since $d-2$ is the smallest degree of the pencil and the number of simple points that have to be determined is the lowest for this choice of a. If we work symbolically and use any of the methods above for determining the simple points, we also want to choose $a = d-2$, since this leads to the lowest number of points. However, we will show that although $a = d$ forces us to work with curves of higher degree and although the number $M(a)$ of common simple points is higher, only one simple point on C^* has to be computed explicitly. In the case $a = d-1$ one needs two simple points, and in the case $a = d-2$ three simple points have to be determined, as shown in Sendra & Winkler (1989).

In the sequel we focus on the selection of a pencil of degree d (for pencils of degree $d-1$ and $d-2$ the problem can be dealt with analogously). Since $a = d$, we have to determine $M(d) = 3(d-1)$ simple points on C^*. Three different whole classes of conjugate simple points are constructed, each one of cardinality $d-1$. First we explain how to construct these classes of simple points, and afterwards we will show how to deal with these classes of points in the parametrization problem. The algorithm constructing the classes of conjugate points works as follows.

Algorithm SIMPLE
The input to SIMPLE is an irreducible rational curve C^* defined by the polynomial $F(x,y,z) \in \mathbb{F}[x,y,z]$ of degree d. The output consists of three distinct whole classes of conjugate simple points on C^* of the form $\{(\lambda_i\gamma_i + b_1 : \mu_i\gamma_i + b_2 : \nu_i\gamma_i + b_3)\}_{q_i(\gamma_i)=0}$, $i = 1, 2, 3$, where $q_i \in \mathbb{F}(\beta)[x]$. Each class contains $d-1$ points. By classical methods the

degree of β can be bounded by 2.
(1) Let S be the set of singularities of C^* (not neighbouring ones).
(2) Let $P = (b_1 : b_2 : b_3)$ be a simple point on C^*. The coordinates of P might be in an algebraic extension $\mathbb{F}(\beta)$ of $\mathbb{F}$.
(3) Choose $\lambda_1, \lambda_2, \lambda_3, \mu_1, \mu_2, \mu_3, \nu_1, \nu_2, \nu_3 \in \mathbb{F}$, such that
  (a) $P + (\lambda_i, \mu_i, \nu_i)s$, $i = 1, 2, 3$, are three different lines,
  (b) $\mathrm{Res}_s(\bar{q}_i(s), \bar{q}_i'(s)) \neq 0$ for $i = 1, 2, 3$, where $\bar{q}_i(s) = F(\lambda_i s + b_1, \mu_i s + b_2, \nu_i s + b_3)$ and $\bar{q}_i'$ denotes the derivative of $\bar{q}_i$ w.r.t. s.
(4) For $i = 1, 2, 3$ set $q_i(s) := \bar{q}_i(s)/s$.
(5) Now

$$\{(\lambda_i\gamma_i + b_1 : \mu_i\gamma_i + b_2 : \nu_i\gamma_i + b_3)\}_{q_i(\gamma_i)=0}, \qquad i = 1, 2, 3$$

are three distinct whole classes of $(d-1)$ simple points each on C^*. □

In order to prove the correctness of the algorithm SIMPLE, we first need the following technical lemma.

LEMMA 7: *Let P be a simple point on C^*. There exist at most $d(d-1)$ tangents to C^* at a simple point and passing through P.*

Proof: Since the property is geometric, we assume w.l.o.g. that P is the origin $(0 : 0 : 1)$. If a tangent to C^* at the simple point $Q = (a_1 : a_2 : a_3)$ passes through P, the coordinates a_1, a_2, a_3 have to satisfy

$$\frac{\partial F}{\partial z}(a_1, a_2, a_3) = 0, \quad F(a_1, a_2, a_3) = 0.$$

Since $F(x, y, z)$ is irreducible and since $\partial F/\partial z$ has total degree $d-1$, according to Bezout's theorem there are at most $d(d-1)$ different solutions. □

LEMMA 8: *The algorithm SIMPLE is correct.*

Proof: Steps (1) and (2) are obviously correct.
Step (3): (b) guarantees that the line $L_i = P + (\lambda_i, \mu_i, \nu_i)s$, $1 \leq i \leq 3$, is not a tangent to C^* and does not pass through a singular point of C^*. Step (3) can be carried out effectively if there exist only finitely many elements λ_i, μ_i such that $\bar{q}_i(s)$ has multiple roots. If $\bar{q}_i(s)$ has multiple roots, the line L_i intersects C^* on a simple point with multiplicity of intersection higher than 1. Therefore, this can only happen if the line L_i is tangent to C^* at the simple point. Now we apply Lemma 7 and we see that this can happen only $d(d-1)$ times.
Step(4): Note that P is one of the d intersection points of C^* and L_i. In q the parameter value corresponding to P is eliminated.
Step (5): We show that in total the classes of points $\{(\lambda_i\gamma_i+b_1 : \mu_i\gamma_i+b_2 : \nu_i\gamma_i+b_3)\}_{q_i(\gamma_i)=0}$ contain exactly $3(d-1)$ different points. For this purpose we observe first that no singular point belongs to these families. $\deg_s(q_i) = \deg_s(\bar{q}_i) - 1 = d - 1$, so in every class there are at most $d-1$ different points. But $\bar{q}_i(s)$ has no multiple root (by (3b)), and therefore also $q_i(s)$ has no multiple root. Thus, every class contains exactly $d-1$ different simple points. Finally, since the three lines L_1, L_2, L_3 only intersect at P, all these $3(d-1)$ simple points are different.
Hence, the algorithm SIMPLE is correct. □

In the previous section we have seen how to express the neighbourhood graph of C^* by means of classes of conjugate points. Now, also the set of the common fixed simple points is expressed in terms of classes of conjugate points by the algorithm SIMPLE. Therefore, in order to make algorithm PARAMETRIZE work efficiently, we have to be able to pass the pencil H through any class of conjugate points of C^*, with any multiplicity. The following theorems deal with this problem.

THEOREM 5: *Let* $\mathcal{F} = \{(m^{(1)}(\alpha_1) : m^{(2)}(\alpha_1) : m^{(3)}(\alpha_1))\}_{A(\alpha_1)=0}$, $m^{(1)}, m^{(2)}, m^{(3)}$, $A \in \mathbb{F}[x]$, *be a class of conjugate points, and* $G \in \mathbb{F}[x,y,z]$. *Then* G *vanishes on all the points of* $\mathcal{F}$ *if and only if* $A(s)$ *divides* $G(m^{(1)}(s), m^{(2)}(s), m^{(3)}(s))$.

Proof: For every root s_0 of A, let $P_{s_0} = (m^{(1)}(s_0) : m^{(2)}(s_0) : m^{(3)}(s_0))$ be a point of $\mathcal{F}$. Then G vanishes on P_{s_0} if and only if $s - s_0$ divides $G(m^{(1)}(s), m^{(2)}(s), m^{(3)}(s))$. Hence, G vanishes on the whole family $\mathcal{F}$ if and only if $A(s)$ divides $G(m^{(1)}(s), m^{(2)}(s), m^{(3)}(s))$. $\square$

THEOREM 6: *Let* $\mathcal{F} = \{\cdots\{\{(\alpha_i : 1 : 0)\}_{A_i(\alpha_1,\ldots,\alpha_i)=0}\}\cdots\}_{A_1(\alpha_1)=0}$, $A_j \in \mathbb{F}[x_1,\ldots,x_j]$ *for* $1 \le j \le i$, $i > 1$, *be a family in the standard decomposition of some* $(i-1)$*–st neighbourhood of* C^*, *and* $G \in \mathbb{F}[x,y,z]$.

(i) *ideal*$(A_1,\ldots,A_i) \cap \mathbb{F}[x_i]$ *is generated by a single nonzero element of* $\mathbb{F}[x_i]$.

(ii) *Let* $H(x_i)$ *be a generating element of ideal*$(A_1,\ldots,A_i) \cap \mathbb{F}[x_i]$. *Then* $G \in \mathbb{F}[x,y,z]$ *vanishes on all the points of* $\mathcal{F}$ *if and only if* H *divides* $G(x_i,1,0)$.

Proof: (1) Since $\mathcal{F}$ is 0–dimensional, there must be a nonzero polynomial in x_i vanishing on $\mathcal{F}$. In $\mathbb{F}[x_i]$ every ideal is a principal ideal.
(2) Since $A_1,\ldots,A_i$ are irreducible and determine a 0–dimensional variety V, *ideal*$(A_1,\ldots,A_i)$ is radical. So $g(x_i) = G(x_i,1,0)$ vanishes on every point in V if and only if $g(x_1) \in$ *ideal*$(A_1,\ldots,A_i) =$ *ideal*(H). $\square$

Remark: For $i = 2$ a resultant computation yields the polynomial H generating *ideal*$(A_1,A_2) \cap \mathbb{F}[x_2]$. However, if $i > 2$ there might be extraneous solutions in the resultant

$$\mathrm{Res}_{x_1}(\mathrm{Res}_{x_2}(\ldots\mathrm{Res}_{x_{i-2}}(\mathrm{Res}_{x_{i-1}}(A_i, A_{i-1}), A_{i-2}), \ldots), A_i).$$

In this case, a Gröbner basis calculation of $A_1,\ldots,A_i$ with respect to the lexicographic ordering with $x_1 > x_2 > \cdots > x_i$ yields the generating polynomial H.

From Theorems 5 and 6 it is clear that one can pass a pencil through the singularities, including the neighbouring ones, and through the simple points, without introducing algebraic numbers. Furthermore, the obtained relations among the undetermined coefficients of the generic representative of the pencil are linear.

Now let us present a new version of the algorithm PARAMETRIZE, where all the symbolic considerations are incorporated. We consider a d–degree pencil in the process. For degree $d-1$ or $d-2$ the algorithm can be designed analogously.

Algorithm PARAMETRIZE-1
The input is an irreducible affine rational curve C of degree d, defined by the irreducible polynomial $f(x,y) \in \mathbb{F}[x,y]$. The output is a rational parametrization of C.

(1) Compute the homogeneous polynomial $F(x,y,z)$ corresponding to $f(x,y)$.
(2) Determine the standard decomposition of the set of singularities of C^*, representatives for the neighbourhood graphs of the standard families, and the multiplicities of the standard families. (With this information the genus of the curve can be determined.)

(3) Let D_d^* be a linear system of curves of degree d, with undetermined coefficients.

(4) (4.1) Using algorithm SIMPLE, compute three different classes of simple points on C^*, each class containing $d-1$ points:

$$\{(\lambda_j\gamma_j + b_1 : \mu_j\gamma_j + b_2 : \nu_j\gamma_j + b_3)\}_{q_j(\gamma_j)=0}, \quad j = 1, 2, 3.$$

(4.2) Determine the linear relations between the coefficients of H (H is the defining polynomial of the d–degree pencil D_d^*) derived from the fixed common singular and neighbouring points of C^* and D_d^*. (Use Theorems 5,6.)

(4.3) Determine the linear relations between the coefficients of H derived from the fixed common simple points of C^* and D_d^* by equating

$$\text{remainder}_s(H(\lambda_j s + b_1, \mu_j s + b_2, \nu_j s + b_3),\ q_j(s)), \quad j = 1, 2, 3$$

to 0.

(4.4) From the system of linear equations obtained in (4.2) and (4.3) construct the pencil D_d^* as is has been described in Chapter III.

(5) Let $S_1(y)$ be the primitive part of $\text{Res}_x(f, h)$ w.r.t. t and $S_2(x)$ the primitive part of $\text{Res}_y(f, h)$ w.r.t. t, where $h(x, y) = H(x, y, 1)$.

(6) Solve the linear system of equations

$$S_1(y) = 0, \quad S_2(x) = 0,$$

where x, y are the unknowns. Let $(R_1(t), R_2(t))$ be the solution.

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

Remark: (a) Note that whenever we deal with a family of (singular or simple) points on the curve C^*, we do not really compute any algebraic numbers, so no algebraic number will be introduced in the pencil and therefore in the parametrization.
(b) The elimination of the factors corresponding to the fixed common points of the curve and the pencil can be done as in step (5) or by explicitly dividing by these factors, which are known in advance. We do not go into the details here, but refer to Sendra & Winkler (1990).

VI. Examples

In this chapter we illustrate the previous theoretical results by some examples. As the field of coefficients $\mathbb{F}$ we choose the field of rational numbers $\mathbb{Q}$. The purpose of these examples is to demonstrate the algorithms RATIONALITY, PARAMETRIZE-1, and SIMPLE. However, we want to emphasize that by using additional knowledge about the algebraic curves one can achieve parametrizations with smaller integer coefficients. For additional examples we refer to Sendra & Winkler (1989, 1990).

Example 1:

Let C^* be the irreducible curve defined by

$$yz^4 + xz^4 + 2y^3z^2 + \frac{13}{4}xy^2z^2 + \frac{13}{3}x^2yz^2 + 6x^3z^2 + y^5 + \frac{9}{4}xy^4 + 4x^2y^3 + 9x^3y^2 + 4x^4y + 9x^5.$$

The standard decomposition of the set of singularities of C^* is

$$\{(0:\alpha:-1)\}_{\alpha^2+1} \cup \{(\alpha:2:0)\}_{\alpha^2+2} \cup \{(-1:0:\alpha)\}_{\alpha^2+3},$$

where all the singular points are of multiplicity 2. So the genus of C^* is 0 and we proceed to parametrize the curve.

Let H_5 be the generic representative of a 5–degree pencil. We force H_5 to pass through the singularities of C^* with multiplicity 1. Hence,

$$\begin{aligned}
\text{remainder}(H_5(0,s,-1), s^2+1) &= 0,\\
\text{remainder}(H_5(s,2,0), s^2+2) &= 0,\\
\text{remainder}(H_5(-1,0,s), s^2+3) &= 0.
\end{aligned}$$

From this system we obtain 6 linear equations for the undetermined coefficients of H_5. As a rational point on C^* we take $P=(0:0:1)$. We consider the following 3 families of 4 simple points each:

$$\begin{aligned}
\mathcal{F}_1 &= \{(\alpha:\alpha:1+\alpha)\}_{p_1(\alpha)=562\alpha^4+470\alpha^3+331\alpha^2+96\alpha+24=0},\\
\mathcal{F}_2 &= \{(2\alpha:\alpha:1+\alpha)\}_{p_2(\alpha)=3134\alpha^4+958\alpha^3+551\alpha^2+72\alpha+18=0},\\
\mathcal{F}_3 &= \{(\alpha:2\alpha:1+\alpha)\}_{p_3(\alpha)=599\alpha^4+298\alpha^3+185\alpha^2+36\alpha+9=0}.
\end{aligned}$$

We force H_5 to pass through these three families by setting

$$\begin{aligned}
\text{remainder}(H_5(t,t,1+t), p_1(t)) &= 0,\\
\text{remainder}(H_5(2t,t,1+t), p_2(t)) &= 0,\\
\text{remainder}(H_5(t,2t,1+t), p_3(t)) &= 0.
\end{aligned}$$

Equating the coefficients of these remainders to 0 we obtain 12 new linear equation. Finally, we take a point not on C^*, e.g. $(1:0:0)$, and we force H_5 to pass through it. In this way we ensure that H_5 has no common component with C^*. Solving the system of 19 linear equations we obtain the expression of the pencil

$$\begin{aligned}
&H_5(x,y,z) =\\
&226152tz^5 + 260832yz^4 - 17160xz^4 + 525594ty^2z^3 - 47115txyz^3 + 1283622tx^2z^3\\
&+ 560274y^3z^2 + 66495xy^2z^2 + 1323322x^2yz^2 - 51480x^3z^2 + 299442ty^4z - 36645txy^3z\\
&+ 1380993tx^2y^2z - 151815tx^3yz + 1815498tx^4z + 299442y^5 + 57915xy^4 + 1429428x^2y^3\\
&+ 115830x^3y^2 + 1661088x^4y.
\end{aligned}$$

Finally, computing the primitive parts of the resultants one obtains the parametrization

$$\begin{aligned}
x(t) &= \frac{1396\,t\,(4287454760689\,t^4 + 4774688480133\,t^2 + 1219359228516)}{429\,(28498963997521\,t^4 + 23133701931912\,t^2 + 4877436914064)},\\
y(t) &= -\frac{1047\,t\,(4287454760689\,t^4 + 3168181401528\,t^2 + 541937434896)}{143\,(28498963997521\,t^4 + 23133701931912\,t^2 + 4877436914064)}.
\end{aligned}$$

Example 2:

Let C^* be the irreducible curve defined by

$$\frac{1251}{115}y^4z^3+\frac{5184}{115}xy^3z^3+\frac{5354}{115}x^2y^2z^3+x^4z^3-\frac{9552}{115}xy^4z^2-\frac{22496}{115}x^2y^3z^2$$
$$-\frac{5424}{115}x^3y^2z^2-\frac{32}{23}x^4yz^2+192x^2y^4z+\frac{17472}{115}x^3y^3z-\frac{13824}{115}x^3y^4.$$

The standard decomposition of the set of singularities of C^* is

$$\{\underbrace{(0:0:1)}_{P_1}\}\cup\{\underbrace{(0:1:0)}_{P_2}\}\cup\{\underbrace{(1:0:0)}_{P_3}\}\cup\{\underbrace{(1:1:1)}_{P_4}\}\cup\{\underbrace{(3:1:2)}_{P_5}\}\cup\{\underbrace{(-1:1:3)}_{P_6}\},$$

where P_1 is a 4–fold point, P_2 and P_3 are triple points, and P_4, P_5, P_6 are double points. Therefore the genus of C^* is 0 and we proceed to parametrize the curve by means of a 7–degree pencil.

As a rational point of C^* we take $P=(1:-1:1)$ and we consider the 3 families of 6 simple points each, obtained by intersecting C^* with the lines

$$L_1=P+(1:1:0)t, \quad L_2=P+(1:-2:0)t, \quad L_3=P+(1:2:0)t.$$

Finally, in order to guarantee that the pencil has no component in common with C^*, we let it pass through the point $(1:0:1)$ not on C^*. With these settings the algorithm PARAMETRIZE-1 yields the parametrization

$$x(t)=\frac{10917271\,t^4+38752614\,t^3+51665040\,t^2+30513024\,t+6718464}{270\,t^3\,(419\,t+288)},$$
$$y(t)=-\frac{10917271\,t^4+38752614\,t^3+51665040\,t^2+30513024\,t+6718464}{18\,t\,(682489\,t^3+1686888\,t^2+1378944\,t+373248)}.$$

Conclusion

Although it has been known theoretically for quite some time how the rationality of an algebraic plane curve can be decided and a rational parametrization can be computed if one exists, the development of a symbolic algorithm leads to interesting new problems. For some of these problems, like the selection of different kinds of pencils or the passing of a pencil through a family of points on a curve without having to compute these points, we have been able to find new algorithmic ideas. This is one more indication for our opinion that the development of symbolic algorithms needs an even closer analysis of the problem at hand.

There are still several open questions in connection with the parametrization of plane curves. Further research may focus on finding an efficient method for the detection of rational simple points on curves. The coefficients of a parametrization computed by PARAMETRIZE-1 can be extremely large. Is it possible to remedy this deficiency by a reparametrization?

Acknowledgement

We want to thank J. Schicho for interesting discussions on the subject of parametrization. We are indebted to the anonymous referees for some valuable suggestions.

References

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.

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.).

Buchberger, B. (1985). Gröbner bases: An algorithmic method in polynomial ideal theory. In: *Multidimensional Systems Theory*, N.K. Bose (ed.), Reidel Publ. Comp., Dordrecht.

Hilbert, D., Hurwitz, A. (1890). Über die Diophantischen Gleichungen vom Geschlecht Null, *Acta math.* **14**, 217-224.

Kalkbrener, M. (1990). Solving systems of bivariate algebraic equations by using primitive polynomial remainder sequences. Techn. Rep. RISC 90-21.0, Research Inst. Symb. Comp., Univ. Linz.

Poincaré, M.H. (1901). Sur les propriétés arithmétiques des courbes algébriques. *Journ. de Math.* (5^e série), tome VII, 161-233.

Sakkalis, T., Farouki, R. (1990). Singular points of algebraic curves. *J. of Symbolic Computation* **9/4**, 405-421.

Schafarewitsch, I.R. (1972). *Grundzüge der algebraischen Geometrie.* Vieweg, Braunschweig.

Sederberg, T.W. (1986). Improperly parametrized rational curves. *Computer Aided Geometric Design* **3**, 67-75.

Sendra, J.R., Winkler, F. (1989). A symbolic algorithm for the rational parametrization of algebraic plane curves. Techn. Rep. RISC 89-41.1, Research Inst. Symb. Comp., Univ. Linz.

Sendra, J.R., Winkler, F. (1990). Computer algebra methods in the parametrization of curves. Techn. Rep. RISC 90-45.0, Research Inst. Symb. Comp., Univ. Linz.

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.