J. Symbolic Computation (2001) **11**, 1–000

Parametrization of Algebraic Curves over Optimal Field Extensions

J. RAFAEL SENDRA[†] AND FRANZ WINKLER[‡]

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

(Received 23 April 2001)

In this paper we investigate the problem of determining rational parametrizations of plane algebraic curves over an algebraic extension of least degree over the field of definition. This problem reduces to the problem of finding simple points with coordinates in the field of definition on algebraic curves of genus 0. Consequently we are also able to decide parametrizability over the reals. We generalize a classical theorem of Hilbert and Hurwitz about birational transformations. An efficient algorithm for computing such optimal parametrizations is presented.

1. Introduction

In Sendra and Winkler (1991) we have described a symbolic algorithm for computing a rational parametrization $\varphi(t), \chi(t), \psi(t)$ of a plane algebraic curve $\mathcal{C}$ of genus 0. Exactly these plane algebraic curves have a rational parametrization. So we call a curve of genus 0 a rational curve.

If the irreducible projective curve $\mathcal{C}$ is defined as the set of solutions in the projective plane $\mathbb{P}^2(\mathcal{K})$ of the homogeneous polynomial equation

$$F(x_1, x_2, x_3) = 0$$

over the field of characteristic zero $\mathbb{K}$, i.e. $F \in \mathbb{K}[x_1, x_2, x_3]$ and $\mathcal{K}$ is the algebraic closure of $\mathbb{K}$, then $\varphi(t), \chi(t), \psi(t) \in \mathcal{K}(t)$, the field of rational functions over $\mathcal{K}$, constitute a rational parametrization of $\mathcal{C}$ iff, except for finitely many exceptions, every evaluation $(\varphi(t_0) : \chi(t_0) : \psi(t_0))$ at $t_0 \in \mathcal{K}$ is a point on $\mathcal{C}$, and conversely almost every point on $\mathcal{C}$ is the result of evaluating the parametrization at some element of $\mathcal{K}$. The parametrization problem for algebraic curves consists in first deciding whether the given curve $\mathcal{C}$ has such a rational parametrization, and if so finding one.

If $\mathcal{C}$ has a rational parametrization, then in fact it has lots of them. So the issue is to keep the degrees in the parametrization small and also to keep the coefficients in the parametrization simple. The algorithms given by van Hoeij (1994), Schicho (1992),

[†] Partially supported by Univ. Alcalá Proj. 030/95 and DGICYT PB 95/0563-A: Sistemas de ecuaciones algebraicas: resolución y applicaciones
[‡] Partially supported by the Austrian *Fonds zur Förderung der wissenschaftlichen Forschung* under Proj. SGC, No. 8573, and Proj. POSSO, No. 9181 (ESPRIT BRA No. 6846)

0747–7171/90/000000 + 00 \$03.00/0

Sendra and Winkler (1991) compute parametrizations with optimal degrees. In this paper we concentrate on the coefficients in such a parametrization. In fact, we show how to compute in an efficient way a parametrization with optimal coefficients, i.e. coefficients in the field of definition $\mathbb{K}$ or at most in a quadratic algebraic extension of $\mathbb{K}$. The basic ideas and results in this paper have been available since 1993 (see the technical reports Sendra and Winkler, 1993, and Sendra and Winkler, 1994). Similar results can be achieved using the algebraic approach in van Hoeij (1996).

Let us demonstrate this problem by an example. Consider the curve $\mathcal{C}$ defined by the homogeneous polynomial

$$\begin{aligned} F(x_1,x_2,x_3) \;=\;& x_3^5\,x_1\,x_2^4 + x_3^4\,x_1\,x_2^5 + x_3^5\,x_1^2\,x_2^3 + x_3^3\,x_1^5\,x_2^2 - 19\,x_3^3\,x_1^2\,x_2^5 - 53\,x_3^3\,x_1^3\,x_2^4 \\ &+x_3^4\,x_1^5\,x_2 + x_1^5\,x_2^5 + x_3^5\,x_1^5 + 43\,x_3^4\,x_1^3\,x_2^3 + x_3^3\,x_1^4\,x_2^3 + 12\,x_3^2\,x_1^4\,x_2^4 \\ &+57\,x_3^2\,x_1^3\,x_2^5 - 19\,x_3^2\,x_1^5\,x_2^3 - 36\,x_3\,x_1^4\,x_2^5 + x_3^5\,x_2^5 + 21\,x_3\,x_1^5\,x_2^4 \\ &-15\,x_3^5\,x_1^3\,x_2^2 \end{aligned}$$

in the projective plane over $\mathbb{C}$. This curve is reconsidered as F_9 in Section 4. $\mathcal{C}$ has singularities at $P_1=(1:0:0), P_2=(0:1:0), P_3=(0:0:1), P_4=(1:1:1)$, where P_1,P_2,P_3 are 5-fold points and P_4 is a 4-fold point. So the genus of $\mathcal{C}$ is 0, i.e. $\mathcal{C}$ has a rational parametrization.

The problem of determining a parametrization with optimal coefficients, i.e. coefficients expressible in a least degree algebraic extension of $\mathbb{Q}$, reduces to finding a few simple points of $\mathcal{C}$ with coordinates in a least degree extension of the ground field $\mathbb{Q}$. So we have to try to solve over $\mathbb{P}^2(\mathbb{Q})$ the diophantine equation

$$F(x_1,x_2,x_3)=0.$$

Indeed this equation has solutions in $\mathbb{P}^2(\mathbb{Q})$, e.g. $(-\frac{239}{149}:-\frac{239}{731}:1)$. Using this rational point on $\mathcal{C}$, we can get the following optimal parametrization of $\mathcal{C}$:

$$\begin{cases} \varphi(t) = \frac{400t^2-712t^3+350t^4+80t-32-83t^5}{-306t^4-944t^2+1048t^3+272t+185t^5-32} \\ \chi(t) = \frac{-400t^2+712t^3-350t^4-80t+32+83t^5}{-946t^4+2248t^3+1360t-2832t^2+217t^5-160} \\ \psi(t)=1. \end{cases}$$

In this particular example it is not difficult to get a point on $\mathcal{C}$ with rational coordinates, since the line through P_1 and P_4 must intersect $\mathcal{C}$ in a simple point with rational coordinates. However, in general the situation will be less favourable.

2. Solving Diophantine Equations of Genus Zero.

Since the adjoint curves to a rational plane curve can be computed in a finite number of ground field operations (see e.g. Sendra and Winkler, 1991), the problem of parametrizing over an optimal field extension of the ground field is reduced to the problem of determining rational simple points on the curve, or equivalently to diophantine equations of genus zero.

The problem of solving diophantine equations of genus zero can be stated as follows: let $\mathbb{K}$ be a computable field of characteristic zero, then one wants to determine the nonzero rational solutions (solutions over $\mathbb{K}$) of

$$F(x_1,x_2,x_3)=0$$

where $F \in \mathbb{K}[x_1, x_2, x_3]$ is an irreducible homogeneous polynomial of degree d, and the plane curve defined by F is rational.

In 1890, Hilbert and Hurwitz introduced a method for dealing with this problem. Basically, their main result states that there exist adjoint curves $\Phi_1, \Phi_2, \Phi_3 \in \mathbb{K}[x_1, x_2, x_3]$ of degree $d-2$ to F such that the rational transformation $\{y_1 : y_2 : y_3 = \Phi_1 : \Phi_2 : \Phi_3\}$ is birational, and the transformed curve of F is of degree $d-2$. Furthermore, those adjoint curves not providing birational transformations satisfy certain algebraic conditions. Thus, the method consists in applying a birational transformation, defined by adjoint curves to F of degree $d-2$, to map F onto a curve G of degree $d-2$. Then, since the transformation is birational, almost every rational point on $\mathcal{C}$ corresponds to a rational point on the curve defined by G and viceversa. Hence, the original problem is reduced to a diophantine equation of genus zero and degree $d-2$. This process is continued until one arrives at a curve of degree three or two, depending on whether the degree of the original curve is odd or even, respectively. For rational cubics the problem is trivial, and for conics over many interesting fields there are complete decision procedures. Once the rational points on the birationally equivalent cubic or conic have been determined, one can express all the rational points on $\mathcal{C}$ by inverting the birational map.

The main difficulty of this approach is that, in general, $\mathcal{O}(d)$ birational transformations are required in order to reach a cubic, or a conic. This renders the method all but impossible in practical applications to curves whose degree is not extremely small.

In this section we generalize the result of Hilbert and Hurwitz to linear subsystems of adjoint curves. As a consequence, by controlling the dimension of a system of adjoint curves one can solve the problem without executing any birational transformation (if the degree of the equation is odd) or applying one birational transfomation (if the degree of the equation is even). Moreover, in the next section it is shown how to use interpolation to execute the birational transformation. More precisely, Hilbert-Hurwitz's result can be generalized as follows:

Theorem 2.1. *Let $\mathcal{C}$ be a rational plane curve of degree d, $\mathcal{H}_a$ the linear system of adjoint curves to $\mathcal{C}$ of degree $a \in \{d, d-1, d-2\}$, and $\tilde{\mathcal{H}}_a^s$ a linear subsystem of $\mathcal{H}_a$ of dimension s with all its base points on $\mathcal{C}$. Then we have the following:*

(i) If $\Phi_1, \Phi_2, \Phi_3 \in \tilde{\mathcal{H}}_a^s$ are such that the common intersections of the three curves Φ_i and $\mathcal{C}$ are the set of base points of $\tilde{\mathcal{H}}_a^s$, and such that

$$\mathcal{T} = \{y_1 : y_2 : y_3 = \Phi_1 : \Phi_2 : \Phi_3\}$$

is a birational transformation, then the birationally equivalent curve to $\mathcal{C}$, obtained by $\mathcal{T}$, is irreducible of degree s.

(ii) Those values of the parameters for which the rational transformation $\mathcal{T}$ is not birational satisfy some algebraic conditions.

Proof. (i) Let $\mathcal{D}$ be the birationally equivalent curve to $\mathcal{C}$. $\mathcal{T}$ determines a one-to-one relation between the points of $\mathcal{C}$ and $\mathcal{D}$, except for finitely many points on these curves. We call these points the exception points. Since $\mathcal{T}$ is a birational transformation, $\mathcal{D}$ is an irreducible rational curve; and therefore, one just has to prove that the degree of $\mathcal{D}$ is s. Let $n = deg(\mathcal{D})$ and let $b \in \mathbb{K}$ such that $\Phi_1 - b\Phi_3$ intersects $\mathcal{C}$ at the base points with minimal multiplity. We take a line $\mathcal{L} = \{(b : t : 1)\}_{t \in \mathcal{K}}$ ($\mathcal{K}$ the algebraic closure of $\mathbb{K}$) intersecting $\mathcal{D}$ in n different simple points $\{(b : \lambda_i : 1)\}_{i=1,\ldots,n}$ and such that none of them is an exception point on $\mathcal{D}$. Now, applying the inverse of $\mathcal{T}$ we obtain n different points $\{P_1, \ldots, P_n\}$ on $\mathcal{C}$ and on the curve $\mathcal{M}$ defined by $M = \Phi_1 - b\,\Phi_3$, that are not base points of $\tilde{\mathcal{H}}_a^s$. Hence, since the number of free intersections of $\mathcal{C}$ and $\mathcal{M}$ is at most s, it follows that $n \leq s$. On the other hand, let us assume that $n < s$. Then, we take an additional common point P_{n+1} of $\mathcal{C}$ and $\mathcal{M}$, not being a base point of $\tilde{\mathcal{H}}_a^s$ or an exception point for $\mathcal{T}$ (note that this is always possible since the common intersection points of the three curves Φ_i and $\mathcal{C}$ are the set of base points of $\tilde{\mathcal{H}}_a^s$, and since $\mathcal{M}$ and $\mathcal{C}$ intersect at the base points with minimal multiplicity). If we now apply the birational transformation $\mathcal{T}$ to $\{P_1, \ldots, P_{n+1}\}$, we obtain the $(n+1)$ different simple points on $\mathcal{D}$:

$$\{\,(b : \lambda_i : 1)\}_{i=1,\ldots,n} \cup \{(b : \mu : 1)\} \text{ for some } \mu \in \mathcal{K}$$

Therefore $\mathcal{L}$ cuts $\mathcal{D}$ in $(n+1)$ points, which is impossible. Hence $n = s$.

(ii) We consider three elements $\Phi_i(x_1, x_2, x_3, \Lambda_i) \in \tilde{\mathcal{H}}_a^s$, $i = 1, 2, 3$, depending on three different evaluations $\Lambda_1, \Lambda_2, \Lambda_3$ of the undetermined parameters in the family $\tilde{\mathcal{H}}_a^s$. Let G be the defining polynomial of the transformed curve of $\mathcal{C}$ under the rational transformation

$$y_1 : y_2 : y_3 = \Phi_1(x_1, x_2, x_3, \Lambda_1) : \Phi_2(x_1, x_2, x_3, \Lambda_2) : \Phi_3(x_1, x_2, x_3, \Lambda_3).$$

Then, we first show that $G \in \mathbb{K}[\Lambda_1, \Lambda_2, \Lambda_3][y_1, y_2, y_3]$, with some exceptions that correspond to some values of the parameters that satisfy certain algebraic conditions $\mathcal{A}_1$. Indeed, G can be interpolated by sending, with the rational transformation, points on $\mathcal{C}$ to points on G; this can be done for all values of the parameters that do not make the determinant of the corresponding interpolating linear system vanish. This determinant belongs to $\mathbb{K}[\Lambda_1, \Lambda_2, \Lambda_3]$. In addition, because of technical reasons, we also include in $\mathcal{A}_1$ those algebraic conditions on the parameters that decrease the formal degree of G. Furthermore, we observe that those values of the parameters that transform $\mathcal{C}$ into a reducible curve G include values of the parameters that do not generate a birational transformation; and therefore it is enough to look for algebraic conditions on these values of the parameters.

Let $(p_1(t), p_2(t), p_3(t))$ be a proper rational parametrization of $\mathcal{C}$. Then

$$\left\{\begin{array}{l} y_1 = q_1(t, \Lambda_1) = \Phi_1(p_1, p_2, p_3, \Lambda_1) \\ y_2 = q_2(t, \Lambda_2) = \Phi_2(p_1, p_2, p_3, \Lambda_2) \\ y_3 = q_3(t, \Lambda_3) = \Phi_3(p_1, p_2, p_3, \Lambda_3) \end{array}\right.$$

is a parametrization of some component of the curve G. In fact, one can assume that the parametrization is proper, since the algorithm given by Sederberg (1986) for reparametrizing can always be applied, with the exceptions of those values of the parameters that satisfy certain algebraic conditions $\mathcal{A}_2$ corresponding to some determinants.

Now, we want to formally implicitize the parametrization (q_1, q_2, q_3). We take $\mathcal{A}_3$ as the set of the leading coefficients w.r.t. t in q_1, q_2, q_3. Then, since the parametrization is proper, for all the values of the parameters that do not satisfy conditions $\mathcal{A}_2 \cup \mathcal{A}_3$, the implicitized curve $M(y_1, y_2, y_3)$ is – also under evaluations – the resultant w.r.t. t of $q_3 y_1 - q_1 y_3$ and $q_3 y_2 - q_2 y_3$.

On the other hand, M is a factor of G. Hence, for all the values of the parameters that do not statisfy conditions $\mathcal{A}_1 \cup \mathcal{A}_2 \cup \mathcal{A}_3$, it holds that G is reducible if and only if the degree of the formal curve M is smaller than the degree of the formal curve G. Thus, if $\mathcal{A}_4$ contains the algebraic conditions on the parameters that force M to decrease its degree, we may conclude that those values of the parameters that do not satisfy conditions $\bigcup_{i=1}^{4} \mathcal{A}_i$ generate irreducible transform curves, and thus birational tranformations. □

REMARK 2.1. Note that statement (ii) in Theorem 2.1 guarantees that birational transformations in statement (i) can always be obtained.

In order to apply efficiently the previous theorem to the diophantine problem one needs to compute, using only ground field operations, linear systems of low dimension. For this purpose, we introduce the notion of families of conjugate simple points and the concept of rational linear subsystems.

DEFINITION 2.1. Let $F \in \mathbb{K}[x_1, x_2, x_3]$ be a homogeneous polynomial defining a rational projective curve $\mathcal{C}$ over the algebraic closure $\mathcal{K}$ of $\mathbb{K}$, and $p_1, p_2, p_3, m \in \mathbb{K}[t]$. The set of projective points $\mathcal{F} = \{(p_1(\alpha) : p_2(\alpha) : p_3(\alpha)) \ / \ m(\alpha) = 0\} \subset \mathbb{P}^2(\mathcal{K})$ is a *family of s conjugate simple points on $\mathcal{C}$ over* $\mathbb{K}$ if the following conditions are satisfied:

(1) m is squarefree and $deg(m) = s$,
(2) $deg(p_i) < deg(m)$ for $i = 1, 2, 3$, and $gcd(p_1, p_2, p_3) = 1$,
(3) $\mathcal{F}$ contains exactly s different points of $\mathbb{P}^2(\mathcal{K})$,
(4) $F(p_1(t), p_2(t), p_3(t)) = 0 \mod m(t)$,
(5) there exists $i \in \{1, 2, 3\}$ such that $\frac{\partial F}{\partial x_i}(p_1(t), p_2(t), p_3(t)) \mod m(t) \neq 0$. □

We denote such a family by $\{\, (p_1(t) : p_2(t) : p_3(t)) \,\}_{m(t)}$, and we refer to it as a family of conjugate simple points. Analogously, one can introduce the notion of family of conjugate singular points. For the symbolic manipulation of these families see Sendra and Winkler (1991).

DEFINITION 2.2. Let $\mathcal{C}$ be a plane curve, $\mathcal{H}$ a linear system of curves in which all the elements are of the same degree, $\tilde{H}$ the defining polynomial of a linear subsystem $\tilde{\mathcal{H}}$ of $\mathcal{H}$, and let $\tilde{\mathcal{S}}$ be the set of base points of $\tilde{\mathcal{H}}$ that are not base points of $\mathcal{H}$. Then, we say that $\tilde{\mathcal{H}}$ is a *rational subsystem* of $\mathcal{H}$ if the following conditions are satified:

(1) $\tilde{H}$ is defined over $\mathbb{K}$.
(2) For almost every curve $\Phi \in \mathcal{H}$, and $\tilde{\Phi} \in \tilde{\mathcal{H}}$ it holds that

$$dim(\mathcal{H}) - dim(\tilde{\mathcal{H}}) = \sum_{P \in \tilde{\mathcal{S}}} (mult_P(\tilde{\Phi}, \mathcal{C}) - mult_P(\Phi, \mathcal{C})),$$

where $mult_P(\mathcal{C}_1, \mathcal{C}_2)$ denotes the multiplicity of intersection of the curves $\mathcal{C}_1$, $\mathcal{C}_2$ at the point P. □

Essentially, this notion requires that when a point or a family of points on $\mathcal{C}$ are used to generate a subsystem $\tilde{\mathcal{H}}$ of $\mathcal{H}$ (by introducing some points on $\mathcal{C}$ as new base points on $\mathcal{H}$ with specific multiplicities) the linear system of equations containing the contraints is over $\mathbb{K}$, and its rank equals the number of new known intersection points between $\mathcal{C}$ and a generic representative of the subsystem. In the next proposition some special cases of rational linear subsystems are analyzed.

PROPOSITION 2.1. *Let $\mathcal{C}$ be a rational plane curve of degree d, $\mathcal{H}_a$ the linear system of adjoint curves to $\mathcal{C}$ of degree $a \in \{d, d-1, d-2\}$, and $\mathcal{F} = \{(p_1(t) : p_2(t) : p_3(t))\}_{A(t)}$ a family of k conjugate points on $\mathcal{C}$ over $\mathbb{K}$. Then we have the following:*

(i) If $\mathcal{F}$ is a family of simple points, $k \leq dim(\mathcal{H}_a)$, and $\tilde{\mathcal{H}}_a$ is the subsystem of $\mathcal{H}_a$ obtained by forcing every point in $\mathcal{F}$ to be a simple base point of $\tilde{\mathcal{H}}_a$, then $\tilde{\mathcal{H}}_a$ is rational, and $dim(\tilde{\mathcal{H}}_a) = dim(\mathcal{H}_a) - k$.

(ii) If $\mathcal{F}$ is a family of r-fold points, $r \cdot k \leq dim(\mathcal{H}_a)$, and $\tilde{\mathcal{H}}_a$ is the subsystem of $\mathcal{H}_a$ obtained by forcing every point in $\mathcal{F}$ to be a base point of $\tilde{\mathcal{H}}_a$ of multiplicity r, then $\tilde{\mathcal{H}}_a$ is rational, and $dim(\tilde{\mathcal{H}}_a) = dim(\mathcal{H}_a) - r \cdot k$.

PROOF. Let H_a and $\tilde{H}_a$ be the defining polynomials of $\mathcal{H}_a$ and $\tilde{\mathcal{H}}_a$, respectively.
(i) First, we observe that the rank of the system of equations given by the condition $H_a(p_1, p_2, p_3) = 0 \mod A(t)$ is k: let us assume that the rank is $k - \epsilon$, with $\epsilon > 0$. Then, $dim(\tilde{\mathcal{H}}_a) = dim(\mathcal{H}_a) - k + \epsilon > 0$. Thus, one may take a new simple point P on $\mathcal{C}$, and force $\tilde{\mathcal{H}}_a$ to have P as simple base point (this can always be achived since $\tilde{H}_a(P)$ is identically zero for finitely many simple points P on $\mathcal{C}$; otherwise it would imply that $\tilde{\mathcal{H}}_a$ and $\mathcal{C}$ have a common component, which is impossible according to the irreducibility of $\mathcal{C}$ if $a \in \{d-1, d-2\}$ and to the construction of the $\mathcal{H}_a$ if $a = d$ (see Sendra and Winkler, 1991). Repeating this process $dim(\mathcal{H}_a) - k + \epsilon$ times one obtains a curve in $\mathcal{H}_a$ such that its number of intersections with $\mathcal{C}$ is at least $(d-1)\,(d-2) + dim(\mathcal{H}_a) + \epsilon = a\,d + \epsilon > a\,d$, which is impossible according to Bezout's Theorem.

Thus, $\tilde{H}_a$ is defined over $\mathbb{K}$ and $dim(\tilde{\mathcal{H}}_a) = dim(\mathcal{H}_a) - k$. Furthermore, since k new additional simple base points have been introduced, for every $P \in \mathcal{F}$ it follows that $mult_P(\tilde{\Phi}, \mathcal{C}) = mult_P(\Phi, \mathcal{C}) + 1$, for almost all $\tilde{\Phi} \in \tilde{\mathcal{H}}_a, \Phi \in \mathcal{H}_a$.
(ii) $\tilde{\mathcal{H}}_a$ is obtained solving the system of equations given by the conditions

$$\frac{\partial H_a}{\partial x^i \partial y^j}(p_1, p_2, p_3) = 0 \mod A(t) \quad for \quad i + j = r - 1$$

(note that the points in $\mathcal{F}$ are already base points of $\mathcal{H}_a$ of multiplicity $r-1$). Since the equations are over $\mathbb{K}$, and the rank of the system is $r \cdot k$ (this can be proved as above), it follows that $dim(\tilde{\mathcal{H}}_a) = dim(\mathcal{H}_a) - kr$, and that $\tilde{H}_a$ is defined over $\mathbb{K}$. Moreover, for every $P \in \mathcal{F}$, and for almost all $\Phi \in \mathcal{H}_a, \tilde{\Phi} \in \tilde{\mathcal{H}}_a$ one has that $mult_P(\Phi, \mathcal{C}) = (r-1)r$ and $mult_P(\tilde{\Phi}, \mathcal{C}) = r^2$. $\square$

The next theorem shows how adjoint curves can be applied to compute families of conjugate points.

THEOREM 2.2. *Let $\mathcal{C}$ be a rational plane curve of degree d, and $\mathcal{H}_a$ the linear system of adjoint curves to $\mathcal{C}$ of degree $a \in \{d, d-1, d-2\}$. Then every rational linear subsystem of $\mathcal{H}_a$ of dimension s with all its base points on $\mathcal{C}$ provides curves that generate families of s conjugate simple points over $\mathbb{K}$ by intersection with $\mathcal{C}$.*

PROOF. Let $\tilde{\mathcal{H}}_a$ be a rational linear subsystem of $\mathcal{H}_a$ of dimension s with all its base points on $\mathcal{C}$. Let Φ be a curve in $\tilde{\mathcal{H}}_a$ with no common tangents with F (F is the defining polynomial of $\mathcal{C}$) at the base points of the subsystem (i.e. Φ and F intersect with the expected multiplicities at the base points), and such that all the x_1-coordinates of all the intersection points of Φ and F, that are not base points of $\tilde{\mathcal{H}}_a$, are different. Then, we consider $\phi(x_1, x_2) = \Phi(x_1, x_2, 1)$, $f(x_1, x_2) = F(x_1, x_2, 1)$ and $\tilde{R}_1(x_1) = resultant_{x_2}(\phi, f)$,

$\tilde{R}_2(x_2) = resultant_{x_1}(\phi, f)$. Now, since Φ and F have no common tangents at the base points, there exist $\bar{R}_1, R_1 \in \mathbb{K}[x_1]$ and $\bar{R}_2, R_2 \in \mathbb{K}[x_2]$ such that $\tilde{R}_1 = \bar{R}_1 R_1$, $\tilde{R}_2 = \bar{R}_2 R_2$, $\gcd(\bar{R}_1, R_1) = 1$, $\gcd(\bar{R}_2, R_2) = 1$ and $deg(R_1) = deg(R_2) = s$ (the factor $\bar{R}_i$ basically determines the x_i-coordinates of the intersection points of $\mathcal{C}$ and $\tilde{H}_a$ that are not base points. For further details see Sendra and Winkler (1991)). Furthermore, since all the x_1-coordinates of the intersections are different, R_1 is squarefree. Thus, for every root α of R_1 there exists a unique root β_α of R_2 such that $(\alpha, \beta_\alpha, 1)$ is a simple point on $\mathcal{C}$. Moreover, β_α can be expressed as a polynomial in α: $(y - p(\alpha)) = (y - \beta_\alpha)$ is the gcd of $S(\alpha, x_2)$ and $R_2(x_2)$ in $\mathbb{K}(\alpha)[x_2]$, where $S(x_1, x_2) \equiv f(x_1, x_2) \ mod \ R_1(x_1)$. In general, R_1 may be reducible, but the gcd can be obtained either by dynamic evaluation (see Duval, 1987) or determining the first subresultant w.r.t. x_2 of $S(x_1, x_2)$ and $R_2(x_2)$ modulo $R_1(x_1)$. Therefore, $\{(t, p(t), 1)\}_{R_1(t)}$ is a family of s simple points on $\mathcal{C}$.

Let $\tilde{H}_a(x_1, x_2, x_3, \lambda_1, \ldots, \lambda_{s+1})$ be the defining polynomial of $\tilde{\mathcal{H}}_a$. We observe that curves Φ satisfying the above assumptions can be obtained because those values of parameters, for which the curves $\tilde{H}_a(x_1, x_2, x_3, \lambda_1, \ldots, \lambda_{s+1})$ violate the conditions, satisfy certain algebraic constraints (basically, this can be reached by computing formally the resultant of $\tilde{H}_a$ and F w.r.t. x_1, crossing out the known factors to get $R_1(x_1, \lambda_1, \ldots, \lambda_{s+1})$, and forcing R_1 to vanish at $x_1 = a_1$ for every affine base point $(a_1, a_2, 1)$ of $\tilde{\mathcal{H}}_a$ and that $discrim_{x_1}(R_1) = 0$). $\square$

The next corollary states that there always exist families of conjugate simple points of certain cardinality. D. Lazard in a personal communication has pointed out to us that Theorem 2.2 may be applied to find families of two conjugate simple points on $\mathcal{C}$ (statement (ii) of the corollary).

Corollary 2.1. *Let $\mathcal{C}$ be a rational plane curve with defining polynomial over $\mathbb{K}$ and degree d. Then it holds that:*

(i) $\mathcal{C}$ has families of $(d-2)$, $(2d-2)$, and $(3d-2)$ conjugate simple points over $\mathbb{K}$.
(ii) $\mathcal{C}$ has families of two conjugate simple points over $\mathbb{K}$.
(iii) If d is odd, then $\mathcal{C}$ has simple points over $\mathbb{K}$.
(iv) If d is even then $\mathcal{C}$ has simple points on an algebraic extension of $\mathbb{K}$ of degree two.
(v) If d is even and $\mathcal{C}$ has a singularity over $\mathbb{K}$ of odd multiplicity, then $\mathcal{C}$ has simple points over $\mathbb{K}$.

Proof. For (i) apply Theorem 2.2 to $a = d-2$, $a = d-1$, and $a = d$.
(ii) We first apply statement (i) to obtain two different families of $(d-2)$ simple points. Let $\mathcal{H}_{d-1}$ be the system of adjoint curves of degree $(d-1)$. Applying Proposition 2.1 one has that the linear subsystem $\tilde{\mathcal{H}}_{d-1}$ obtained by forcing all the points in these two families to be simple base points of $\mathcal{H}_{d-1}$ is rational of dimension two. Thus, applying Theorem 2.2 to $\tilde{\mathcal{H}}_{d-1}$ one obtains families of two simple points.
(iii) Applying statement (ii) one can determine $\frac{d-3}{2}$ different families of two simple points on $\mathcal{C}$. Let $\mathcal{H}_{d-2}$ be the system of adjoint curves of degree $(d-2)$. Applying Proposition 2.1 one has that the linear subsystem $\tilde{\mathcal{H}}_{d-2}$ obtained by forcing all the points in these families to be simple base points of $\mathcal{H}_{d-2}$ is rational of dimension one. Thus, applying Theorem 2.2 one concludes that $\mathcal{C}$ has simple points over $\mathbb{K}$.
(iv) This an inmediate consequence of statement (ii).
(v) Let P be a r-fold point of $\mathcal{C}$ over $\mathbb{K}$, with r odd. Let $\mathcal{H}_{d-1}$ be the system of adjoint

curves of degree $(d-1)$. Applying Proposition 2.1 one has that the linear subsystem $\tilde{\mathcal{H}}_{d-1}$ obtained by forcing P to be a base point of multiplicity r of $\mathcal{H}_{d-1}$ is rational of dimension $k = 2d-2-r$. Now, since k is odd, one can compute $\frac{k-1}{2}$ families of two simple points, that generate a rational subsystem of $\mathcal{H}_{d-1}$ of dimension 1. □

Since the previous proofs are constructive, one can apply them to present an improved version of Hilbert-Hurwitz's method for solving diophantine equations of genus zero. We finish this section with an outline of this method.

Algorithm DIOPHANTINE-SOLVER(F)

Input: $F(x_1, x_2, x_3) \in \mathbb{K}[x_1, x_2, x_3]$ is an irreducible homogeneous polynomial of degree d, that defines a rational plane curve.
Output: The solution over $\mathbb{K}$ of the diophantine equation of genus zero $F(x_1, x_2, x_3) = 0$.

(1) Determine the singularities of the curve defined by F. Let $\mathcal{A}$ be the set of all the singularities over $\mathbb{K}$.
(2) Compute the linear system H of adjoint curves to F of degree $(d-2)$.
(3) If d is odd, apply Corollary 2.1 (iii) to find $(d-3)$ simple points of F over $\mathbb{K}$.
(4) If d is even, apply Corollary 2.1 (ii) to find $\frac{d-3}{2}$ families of two simple points of F over $\mathbb{K}$.
(5) Determine the linear rational subsystem $\tilde{H}$ obtained by forcing the points computed in steps (3) or (4), respectively, to be simple base points on H.
(6) Take $\tilde{\Phi}_1, \tilde{\Phi}_2, \tilde{\Phi}_3 \in \tilde{H}$ such that the common intersections of the three curves $\tilde{\Phi}_i$ and F are the set of base points of $\tilde{H}$, and such that $\mathcal{T} = \{y_1 : y_2 : y_3 = \tilde{\Phi}_1 : \tilde{\Phi}_2 : \tilde{\Phi}_3\}$ is a birational transformation (Theorem 2.1).
(7) Determine the transformed curve G to F obtained by $\mathcal{T}$ (note that applying Theorem 2.1 one has that G is either a conic or a line depending on whether d is even or odd, respectively).
(8) If d is odd parametrize the line G over $\mathbb{K}$. Apply the inverse transformation $\mathcal{T}^{-1}$ to find a parametric expression $\mathcal{S}(t)$ of the solutions over $\mathbb{K}$ of $F = 0$. Return $\mathcal{S}(t) \cup \mathcal{A}$.
(9) If d is even decide whether the conic G can be parametrized over $\mathbb{K}$. If so, parametrize G over $\mathbb{K}$ and applying $\mathcal{T}^{-1}$ find a parametric expression $\mathcal{S}(t)$ of the solutions over $\mathbb{K}$ of $F = 0$. Return $\mathcal{S}(t) \cup \mathcal{A}$. Otherwise return $\mathcal{A}$.

Clearly this algorithm can be applied to the problem of computing optimal parametrizations. In fact, if the curve defined by F can be parametrized over the ground field then DIOPHANTINE-SOLVER returns an optimal parametrization. However, if the curve can not be parametrized over the groung field then DIOPHANTINE-SOLVER returns the finitely many rational singularities of the curve. In order to reach an optimal parametrization in this case, one can adapt the algorithm to find one non singular solution of the equation over a two degree extension of $\mathbb{K}$, and use it as simple point in a parametrization algorithm. In the next section we collect all these ideas to construct an optimal parametrization algorithm.

3. Optimal Parametrizations.

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. Furthermore, in Sendra and Winkler (1991) a symbolic parametrization algorithm is presented. However, achieving the theoretically optimal form of parametrizations (an optimal parametrization is expressed in an algebraic extension of the ground field $\mathbb{K}$ as small as possible) has been a serious problem for practical algorithms such as presented in van Hoeij (1994), or Sendra and Winkler (1991). In this section, we show how the results in Section 2 can be applied to compute optimal parametrizations of rational plane curves, and how this can be achieved without excessive demands on computing time.

Every rational plane curve is parametrizable over an algebraic extension of the ground field of degree at most two. Furthermore, if the curve is of odd degree, then parametrizations over the ground field exist. However, when the curve is of even degree a decision problem appears, and the existence of parametrizations over the ground field depends directly on the existence of simple points on the curve over the ground field. More precisely, one has the following classical theorem:

THEOREM 3.1. *Let $\mathcal{C}$ be a rational plane curve with defining polynomial over $\mathbb{K}$ and degree d. Then it holds that:*

(i) If d is odd, then $\mathcal{C}$ is parametrizable over $\mathbb{K}$.
(ii) If d is even, then $\mathcal{C}$ is parametrizable over an algebraic extension of $\mathbb{K}$ of degree at most two.

PROOF. See Hilbert and Hurwitz (1890), or simply apply Corollary 2.1. □

Algorithms for computing such parametrizations can be found in the literature. In Hilbert and Hurwitz (1890) the problem is solved by means of the recursive application of $\mathcal{O}(d)$ birational transformations (d is the degree of the curve), mapping the original curve into a cubic or a conic, depending on whether d is odd or even. Thus, this approach involves in general $\mathcal{O}(d)$ resolutions of systems of algebraic equations in four variables. An alternative approach is presented in Schicho (1992) for the case of curves without neighboring singularities, that deals with linear systems of curves of $\mathcal{O}(d^2)$ degree; but Mňuk et al. (1993) shows that the degree of the linear system drastically affects the complexity of our process, Sendra and Winkler (1991), and we have good reasons to expect that this will be similar in Schicho's approach.

In this section, we present an algorithm that uses linear systems of curves of degree $\mathcal{O}(d)$ and that only needs one birational tranformation to obtain an optimal parametrization in the even case, and no one in the odd case. Moreover, when the birational transformation is required, then the image curve is computed by simply solving a linear system of five equations over $\mathbb{K}$.

To be more precise, let $F \in \mathbb{K}[x_1, x_2, x_3]$ be a homogeneous polynomial of degree d defining a rational plane curve $\mathcal{C}$. Let $\mathcal{H}_{d-2}$ be the linear system of adjoint curves to $\mathcal{C}$ of degree $(d-2)$. By Theorem 2.1, one has that the problem of computing optimal parametrizations of $\mathcal{C}$ is reduced to the problem of computing a rational linear subsystem of $\mathcal{H}_{d-2}$ of dimension 1 or 2. If d is odd, applying Corollary 2.1, one can compute $\frac{d-3}{2}$ families of two points over $\mathbb{K}$ that can be used to construct a rational linear subsystem of $\mathcal{H}_{d-2}$ of dimension 1 (see Proposition 2.1). Therefore, a parametrization over the ground field can be determined. If d is even, applying Corollary 2.1, one can compute $\frac{d-4}{2}$ families of two points over $\mathbb{K}$ that can be used to construct a rational linear subsystem of $\mathcal{H}_{d-2}$ of dimension 2 (see Proposition 2.1). However, applying Theorem 2.1 to this subsystem one can always find a birational transformation, defined by elements of the linear subsystem, that maps $\mathcal{C}$ onto a conic. Hence, the optimality question is reduced to the existence and computation of optimal parametrizations of the corresponding conic. Indeed, since one has a subsystem of dimension 2, one only needs to lift a point on the conic with coordinates over an optimal field extension to obtain a new subsystem of dimension 1, and therefore to parametrize $\mathcal{C}$ over an optimal extension. Thus, the question now is how to compute the birationally equivalent conic, and how to invert a rational point, when it exists.

3.1. Computation of the Conic

Let $\mathcal{C}$ and $\mathcal{H}_{d-2}$ be as above (d is even) and let $\tilde{\mathcal{H}}_{d-2}$ be the linear subsystem of $\mathcal{H}_{d-2}$ obtained by forcing all the points in $\frac{d-4}{2}$ families of two conjugates simple points on $\mathcal{C}$ over $\mathbb{K}$ to be simple base points on $\tilde{\mathcal{H}}_{d-2}$. Now, by Theorem 2.1, we know that if $\Phi_1, \Phi_2, \Phi_3 \in \tilde{\mathcal{H}}_{d-2}$ are such that the common intersections of the three curves Φ_i and $\mathcal{C}$ are the set of base points of $\tilde{\mathcal{H}}_{d-2}$, and such that $\{y_1 : y_2 : y_3 = \Phi_1 : \Phi_2 : \Phi_3\}$ is a birational transformation, then the birationally equivalent curve $G(y_1, y_2, y_3)$ to $F(x_1, x_2, x_3)$ is a conic.

The basic idea for the computation of the conic is to interpolate it. For this purpose, we consider a generic expression $G(y_1, y_2, y_3, \mu_1, \ldots, \mu_6)$ of the conic depending on undetermined coefficients. We take a line $\mathcal{L} = \{(a_1t + a_0 : b_1t + b_0 : c_1t + c_0)\}_{t \in \mathcal{K}}$, $a_i, b_i, c_i \in \mathbb{K}$ such that no base point of $\tilde{\mathcal{H}}_{d-2}$ is on $\mathcal{L}$. Then, we consider the family $\mathcal{F} = \{(a_1t + a_0 : b_1t + b_0 : c_1t + c_0)\}_{m(t)}$ of d conjugate simple points on $\mathcal{C}$ over $\mathbb{K}$ where $m(t) = F(a_1t + a_0, b_1t + b_0, c_1t + c_0) \in \mathbb{K}[t]$ (if $d = 4$, we determine two families of four points on $\mathcal{C}$, cutting with lines). Now, applying the birational transformation to $\mathcal{F}$ one gets a family $\mathcal{G}$ of d simple points over $\mathbb{K}$ on the conic

$$\mathcal{G} = \{(p_1(t) : p_2(t) : p_3(t))\}_{m(t)}$$

where $p_i(t) \equiv \Phi_i(a_1t + a_0, b_1t + b_0, c_1t + c_0) \mod m(t)$. Therefore, we have detected more than five points on the conic and by forcing G to pass through them, the birationally equivalent conic is determined. Moreover, in order to effectively guarantee that the curves Φ_i, taken in the linear subsystem $\tilde{\mathcal{H}}_{d-2}$, define a birational transformation, we test the irreducibility of the conic by checking the rank of the corresponding quadratic form. It is clear that the method can also be applied to odd degree curves, but this is not interesting for our purposes.

Finally, we outline the algorithm that computes a birationally equivalent conic to any even degree rational curve. We detone this algorithm by CONIC. In designing CONIC we assume that the linear subsystem $\tilde{\mathcal{H}}_{d-2}$ has already been computed.

Algorithm CONIC$(F, \tilde{H}_{d-2})$

Input: $F \in \mathbb{K}[x_1, x_2, x_3]$ is a homogeneous polynomial of even degree d defining a rational plane curve, and $\tilde{H}_{d-2}$ is a rational linear subsystem of dimension two of the linear system of adjoint curves to F of degree $(d-2)$.

Output: A birationally equivalent conic to F over $\mathbb{K}$, and the corresponding birational transformation.

(1) Take a generic conic $G(y_1, y_2, y_3, \mu_1, \ldots, \mu_6)$ depending on undetermined coefficients.

(2) Take three different elements Φ_1, Φ_2, Φ_3 in $\tilde{H}_{d-2}$.
(3) If $d > 4$ then

(3.1) Take a line (with defining polynomial over $\mathbb{K}$) not passing through any base point of $\tilde{H}_{d-2}$, and generate a family $\mathcal{F} = \{(\ell_1(t) : \ell_2(t) : \ell_3(t))\}_{m(t)}$ with d simple points on F over $\mathbb{K}$.
(3.2) Compute $p_i(t) \equiv \Phi_i(\ell_1, \ell_2, \ell_3) \mod m(t)$, for $i = 1, 2, 3$.
(3.3) Determine the linear system of equations $\mathcal{S}$ generated by the condition

$$G(p_1(t), p_2(t), p_3(t)) \equiv 0 \mod m(t).$$

(3.4) If $rank(\mathcal{S}) \neq 5$ go to step (2) and take three new curves in $\tilde{H}_{d-2}$. Otherwise solve $\mathcal{S}$ and substitute the solution in G.
(3.5) If the determinant of the associated matrix to G is zero go to step (2), and take three new curves in the $\tilde{H}_{d-2}$.

(4) If $d = 4$ then compute two families, of four different simple points each, as in step (3.1), and proceed analogously to steps (3.2) to (3.5).
(5) Return G.

Now let us consider the problem of inverting points on the conic, i.e. mapping them back to the original curve. First of all, we observe that we are only interested in inverting rational points on the conic, because, if no rational point on the conic exists then we take a point on the original curve over an algebraic extension of degree two as described in Corollary 2.1. Let us then assume that $Q = (q_1 : q_2 : 1)$ is an invertible rational point on a conic $G(y_1, y_2, y_3)$ by means of the birational transformation $\{y_1 : y_2 : y_3 = \Phi_1(x_1, x_2, x_3) : \Phi_2(x_1, x_2, x_3) : \Phi_3(x_1, x_2, x_3)\}$. Then, we want to compute the inverse rational point P on F. Thus, one has to solve the system

$$\left\{ \begin{array}{l} F(x_1, x_2, x_3) = 0 \\ M_1(x_1, x_2, x_3) := \Phi_3(x_1, x_2, x_3)\, q_1 - \Phi_1(x_1, x_2, x_3) = 0 \\ M_2(x_1, x_2, x_3) := \Phi_3(x_1, x_2, x_3)\, q_2 - \Phi_2(x_1, x_2, x_3) = 0 \end{array} \right.$$

We know that the system has a unique solution. Therefore, we can solve the system by computing resultants and rational roots of univariate polynomials over $\mathbb{K}$.

3.2. Optimal Parametrization Algorithm

The previous ideas can be summarized in an algorithm that always outputs an optimal parametrization, in the sense described above. We denote this algorithm by OPTIMAL-PARAMETRIZATION. In the design of the algorithm we do not consider the trivial case of rational curves that can be parametrized by lines. Furthermore, we assume that a method for deciding the existence and computation of rational points on conics is provided (see Ireland and Rosen, 1982), and we refer to Sendra and Winkler (1991) for determining the standard singularity decomposition of the curve.

Algorithm OPTIMAL-PARAMETRIZATION(F, G)

Input: $F \in \mathbb{K}[x_1, x_2, x_3]$ is a homogeneous polynomial of degree d defining a rational plane curve.
Output: An optimal rational parametrization of F.

(1) Determine the standard singularity decomposition $\mathcal{S}$ of F, and compute the linear system H of adjoint curves to F of degree $(d-2)$.
(2) $free := d-3$.
(3) For every family $\mathcal{G} \in \mathcal{S}$ containing s points do
   (3.1) If the points in $\mathcal{G}$ are r-fold points (possibly neighboring singularities), and $free - s\,r \geq 0$ and $free - s\,r$ is even then force the points in $\mathcal{G}$ to be base points of multiplicity r of H, and set $free := free - s\,r$.
(4) If $free$ is even apply Corollary 2.1 (ii) to produce $\frac{free}{2}$ different families of two simple points over $\mathbb{K}$, and force all of them to be simple base points of H.
(5) If $free$ is odd then do
   (5.1) Apply Corollary 2.1 (ii) to produce $\frac{free-1}{2}$ different families of two simple points over $\mathbb{K}$, and force all of them to be base simple points of H.
   (5.2) Apply algorithm CONIC to obtain a conic G birationally equivalent to F.
   (5.3) Decide whether there exist rational points on G.
   (5.4) If there exist rational points on G then compute one, map it back to obtain a rational point P on F, and force P to be a simple base point on H.
   (5.5) If there do not exist rational points on G then
      (5.5.1) Apply Corollary 2.1 (ii) to generate a new different family of two simple points $\mathcal{F} = \{(a_1t + a_0 : b_1t + b_0 : c_1t + c_0)\}_{m(t)}$ over $\mathbb{K}$ (note that m is a quadratic polynomial).
      (5.5.2) Force the points in $\mathcal{F}$ to be simple base points of H (now $\mathbb{K}$ has been extended to $\mathbb{K}(\alpha)$ with minimal polynomial $m(t)$).
(6) $R_i :=\text{resultant}_{x_i}(F(x_1, x_2, 1), H(x_1, x_2, 1, t))$ for $i = 1, 2$.
(7) Set R_1 and R_2 to their primitive part w.r.t. t, respectively.
(8) Solve the linear system $\{R_1 = 0, R_2 = 0\}$ in the variables $\{x_1, x_2\}$ and return the solution.

In general the coefficients of the conic birationally equivalent to the original curve can be large, and therefore the computation of rational points can be extremely time consuming. To avoid this problem, and for practical implementations, we also consider an algorithm that provides parametrizations (that we call nearly optimal parametrizations) over the ground field for odd degree curves, and over an algebraic extension of degree two of $\mathbb{K}$ for even degree curves. Thus, the existence of rational simple points on even degree curves without singularities with special multiplicities is not considered. More precisely, one simply has to partially eliminate Step 6 in the previous algorithm. We illustrate the algorithm by carrying out the parametrization process for the curve defined in the introduction.

EXAMPLE. Let $\mathcal{C}$ be the 10 degree curve given in the introduction. The singularities of $\mathcal{C}$ are the points $P_1 = (1:0:0)$, $P_2 = (0:1:0)$, $P_3 = (0:0:1)$ and $P_4 = (1:1:1)$; where P_i, for $i = 1, 2, 3$ are 5-fold points, and P_4 is a 4-fold point. Thus, $\mathcal{C}$ is rational. Furthermore, in this special example, taking a line through P_4 and any of the 5-fold points, one obtains a rational simple point on $\bar{\mathcal{C}}$. Thus, the algorithm described in Sendra and Winkler (1991) can be directly applied to get an optimal parametrization. However, we want to illustrate how the adjoints map birationally $\mathcal{C}$ onto a conic. Thus, we compute the defining polynomial H_8 of the linear system $\mathcal{H}_8$ of adjoint curves to $\mathcal{C}$ of degree

$d-2=8$:

$$\begin{aligned}
H_8 \;=\;& t_8 x_3^4 x_2^4 + 4\,x_3^2 x_1^3 x_2^3 + t_2 x_3^4 x_1^4 + x_3^2 x_2^2 x_1^4 + t_3 x_1^4 x_2^4 - x_3^4 x_1^2 x_2^2 - 16\,t_2 x_3 x_1^4 x_2^3 - \\
& 6\,t_5 x_3 x_1^4 x_2^3 - 4\,x_3 x_1^4 x_2^3 - 9\,t_1 x_3 x_1^4 x_2^3 - t_7 x_3 x_1^3 x_2^4 - 2\,t_7 x_3^2 x_1^3 x_2^3 - 2\,t_6 x_3 x_1^4 x_2^3 + \\
& t_7 x_3 x_1^4 x_2^3 + 3\,t_6 x_3 x_1^3 x_2^4 + 24\,t_2 x_3^2 x_1^3 x_2^3 + 21\,t_2 x_3 x_1^3 x_2^4 + 2\,t_4 x_3 x_1^4 x_2^3 - 3\,t_3 x_3 x_1^3 x_2^4 + \\
& 12\,t_1 x_3 x_1^3 x_2^4 + 5\,x_3 x_1^3 x_2^4 + 12\,t_1 x_3^2 x_1^3 x_2^3 + t_1 x_3^3 x_1^4 x_2 + 2\,t_6 x_3^2 x_1^3 x_2^3 + 8\,t_5 x_3 x_1^3 x_2^4 - \\
& 3\,t_4 x_3^2 x_1^3 x_2^3 - 21\,t_1 x_3^2 x_1^2 x_2^4 - 5\,t_6 x_3^2 x_1^2 x_2^4 + 8\,t_1 x_3^3 x_1 x_2^4 + 2\,t_6 x_3^3 x_1 x_2^4 + 2\,t_7 x_3^2 x_1^2 x_2^4 - \\
& 3\,t_4 x_3 x_1^3 x_2^4 - 15\,t_5 x_3^2 x_1^2 x_2^4 + 6\,t_4 x_3^2 x_1^2 x_2^4 + t_7 x_3^3 x_1^2 x_2^3 - t_8 x_3 x_1^3 x_2^4 + 9\,t_5 x_3^2 x_1^3 x_2^3 - \\
& 39\,t_2 x_3^2 x_1^2 x_2^4 + 3\,t_3 x_3^2 x_1^2 x_2^4 - 3\,t_1 x_3^4 x_1^2 x_2^2 - t_3 x_3^3 x_1 x_2^4 - t_7 x_3^3 x_1 x_2^4 + 15\,t_2 x_3^3 x_1 x_2^4 + \\
& 3\,x_3^3 x_1 x_2^4 + 3\,t_8 x_3^2 x_1^2 x_2^4 + t_6 x_3^3 x_1^3 x_2^2 - 8\,x_3^2 x_1^2 x_2^4 + 6\,t_5 x_3^3 x_1 x_2^4 - 3\,t_4 x_3^3 x_1 x_2^4 - \\
& 3\,t_8 x_3^3 x_1 x_2^4 + t_5 x_3^4 x_1^3 x_2 - 6\,t_2 x_3^4 x_1^2 x_2^2 - t_6 x_3^4 x_1^2 x_2^2 - 3\,t_5 x_3^4 x_1^2 x_2^2 + t_4 x_3^4 x_1 x_2^3
\end{aligned}$$

In this situation, one has to compute 7 simple points. For this purpose, one gets 3 families of two points, as described above, and maps $\mathcal{C}$ onto a conic to find the remaining simple point. Nevertheless, since P_4 is a 4-fold point, we can find a family with six different simple points on $\mathcal{C}$. More precisely, we take the family $\mathcal{F} = \{\,(1-2t, 1+2t, 1+4t)\,\}_{A(t)=0}$, where $A(t) = 327 + 2965\,t + 8762\,t^2 + 7240\,t^3 - 7808\,t^4 - 13936\,t^5 - 5984\,t^6$. Then, by forcing the system $\mathcal{H}_8$ to pass through $\mathcal{F}$, one obtains the defining polynomial $\tilde{H}$ of the linear subsystem $\mathcal{H}_8^2$ of dimension 2:

$$\begin{aligned}
\tilde{H} \;=\;& -x_3 x_1^4 x_2^3 + x_3^2 x_2^2 x_1^4 - 4\,x_3^2 x_1^3 x_2^3 - 2\,x_3^4 x_1^2 x_2^2 - t_1\, x_3 x_1^4 x_2^3 + \frac{1}{2}\, t_4\, x_3 x_1^4 x_2^3 + \\
& 3\,t_1\, x_3 x_1^3 x_2^4 + 3\,x_3 x_1^3 x_2^4 - \frac{3}{2}\, t_4\, x_3 x_1^3 x_2^4 - 6\,t_1\, x_3^2 x_1^2 x_2^4 + t_1\, x_3^3 x_1^4 x_2 - 4\,t_1\, x_3^4 x_1^2 x_2^2 + \\
& 3\,t_4\, x_3^2 x_1^2 x_2^4 - 3\,x_3^2 x_1^2 x_2^4 - \frac{3}{2}\, t_4\, x_3^3 x_1 x_2^4 + t_4\, x_3^4 x_1 x_2^3 - 5\,t_1\, x_3^3 x_1^3 x_2^2 + 2\,t_1\, x_3^4 x_1^3 x_2 + \\
& 5\,x_3^3 x_1^2 x_2^3 + 10\,t_1\, x_3^3 x_1^2 x_2^3 - \frac{3}{2}\, t_4\, x_3^3 x_1^2 x_2^3 + x_3^3 x_1^3 x_2^2
\end{aligned}$$

that only depends on two parameters t_1, t_4. We now take three curves $\tilde{\Phi}_1$, $\tilde{\Phi}_2$, $\tilde{\Phi}_3$ in $\bar{\mathcal{H}}_8^2$ ($\tilde{\Phi}_1 = -\tilde{H}(t_1 = 0, t_4 = 1), \tilde{\Phi}_2 = -\tilde{H}(1,0), \tilde{\Phi}_3 = -\tilde{H}(1,1)$), and we consider the birational transformation $(y_1 : y_2 : y_3) = (\tilde{\Phi}_1(x_1,x_2,x_3) : \tilde{\Phi}_2(x_1,x_2,x_3) : \tilde{\Phi}_3(x_1,x_2,x_3))$. Applying this transformation to $\mathcal{C}$ we get the birationally equivalent conic $\mathcal{D}$ defined by

$$G(y_1,y_2,y_3) = -3y_2^2 + 8y_2y_3 - 5y_3^2 - 4y_2y_1 + y_1^2 + 4y_1y_3$$

In this situation, inverting the transformation, one can lift finitely many simple points on $\mathcal{D}$, or even a parametrization. For instance, the simple point $Q = (\frac{8}{3} : \frac{5}{3} : 1)$ on $\mathcal{D}$ corresponds to the simple rational point $P = (-\frac{239}{149} : -\frac{239}{731} : 1)$ on $\mathcal{C}$. Now, forcing $\bar{\mathcal{H}}_8^2$ to pass through P one gets a linear subsystem of dimension 1, and computing the free intersection point with the orginal curve one obtains the optimal parametrization

$$\left\{\begin{array}{l}
x_1 = \frac{400t^2-712t^3+350t^4+80t-32-83t^5}{-306t^4-944t^2+1048t^3+272t+185t^5-32} \\[2ex]
x_2 = \frac{-400t^2+712t^3-350t^4-80t+32+83t^5}{-946t^4+2248t^3+1360t-2832t^2+217t^5-160} \\[2ex]
x_3 = 1.
\end{array}\right.$$

3.3. Parametrizing over the reals

As an application of the previous results, an algorithm for analyzing the existence of real parametrizations, and for computing one if they exist, of rational plane curves with defining polynomial over $\mathbb{Q}$ is presented (in fact, the following is also true for any rational plane curve with defining polynomial over any computable subfield of the reals). If the curve is given parametrically, techniques presented in Recio and Sendra (1996) can also be applied.

For this purpose, we now assume that the rational plane curve $\mathcal{C}$ is defined by a homogeneous polynomial $F(x_1, x_2, x_3)$ over $\mathbb{Q}$, and we want to parametrize over $\mathbb{R}$. For odd degree curves this can always be achieved. In fact, parametrizations over $\mathbb{Q}$ can be computed. However, for even degree curves, the existence of parametrizations over $\mathbb{Q}$ or over $\mathbb{R}$ depends on the existence of rational points or real points on a conic birationally equivalent to $\mathcal{C}$, respectively.

The following theorem characterizes the existence of parametrizations over the reals of rational plane curves over the rationals by means of the non-existence of birational transformations over the reals (i.e. the rational functions defining the transfomations are over the reals) mapping the original curve into a certain conic.

Theorem 3.2. *A rational algebraic plane curve over $\mathbb{Q}$ is parametrizable over $\mathbb{R}$ if and only if it is not birationally equivalent over $\mathbb{R}$ to the conic $x_1^2 + x_2^2 + x_3^2$.*

Proof. Applying the paper by Hilbert and Hurwitz (1890), or the ideas in the previous sections, it is clear that there always exists a birational transformation over the rationals that maps the given curve into a conic. Furthermore, there exists a birational transformation over the reals that maps the original curve into an irreducible conic G of the form $x_1^2 + \delta_1 x_2^2 + \delta_2 x_3^2$, where $\delta_i \in \{1, -1\}$. Thus, there exist real simple points on the original curve (and therefore parametrizations over the reals) if and only if there exist real points on G; i.e. if and only if $G(x_1, x_2, x_3)$ is not the conic $x_1^2 + x_2^2 + x_3^2$. □

Therefore, applying algorithm conic the problem is computationally reduced to the well known problem of deciding the existence of rational or real points on conics. Nevertheless, inverting a real point on a conic can be expensive, since resultants and root computations over a real algebraic extension of degree two (possibly with large integers in the minimal polynomial) of the rationals are performed. In the following, a direct approach to compute real points on the original curve is described, that does not invert real points. Let $F \in \mathbb{Q}[x_1, x_2, x_2]$ be an irreducible homogeneous polyomial of even degree d, and let $\tilde{H}_{d-2}(x_1, x_2, x_3, \lambda_1, \lambda_2, \lambda_3)$ be a rational linear subsystem of dimension 2 of the system of adjoint curves to F of degree $(d-2)$. We compute the resultant

$$\tilde{R}_1(x_1, \lambda_1, \lambda_2, \lambda_3) = resultant_{x_2}(F(x_1, x_2, 1), \tilde{H}_{d-2}(x_1, x_2, 1, \lambda_1, \lambda_2, \lambda_3))$$

and we consider the polynomial $R_1(x_1, \lambda_1, \lambda_2, \lambda_3)$ obtained by crossing out in $\tilde{R}_1$ the factors generated by the base points. Now, for every set of rational values of parameters $\lambda_1, \lambda_2, \lambda_3$ for which the leading coefficient of R_1 does not vanish, R_1 is the minimal polynomial of a family of two simple points on F. Therefore those rational values of parameters, that make the discriminant of R_1 w.r.t. x_1 non-negative, generate minimal polynomials with real roots; and hence, real simple points on F. Observe, that taking rational points out of a curve is computationally simpler than taking rational points on a curve. Thus one can obtain a linear subsystem of $\tilde{H}_{d-2}$ of dimension 1 over a real algebraic extension of $\mathbb{Q}$ of degree 2. Hence real optimal parametrizations can be computed.

4. Complexity Analysis and Practical Implementation.

This section is devoted to the theoretical and experimental computing times of the previous algorithms. First, we briefly comment on the theoretical complexity of the parametrization algorithm, and then the section focuses on the implementation of a prototype of the algorithm and actual computing times.

In Mňuk et al. (1993) a detailed theoretical complexity analysis of the parametrization algorithm in Sendra and Winkler (1991) is given. Basically, the conclusion in Mňuk et al. (1993) is that the worst case computing time functions of the standard singularity decomposition and parametrization algorithms are polynomial, if no neighboring expansion is required and rational simple points are freely available. In general, curves with very deep neighboring graphs, containing neighboring points in high algebraic extensions, may appear. This might lead to exponential behaviour of the algorithm. Many problems relating to complexity are still open, and a complete analysis is lacking. However, practical examples suggest that the overall worst case complexity analysis is too pessimistic. In the sequel, the experimental computing times of two different main procedures implemented in Maple V.2. are analyzed.

The first one is called PARAMETRIZE and deals with the computation of nearly optimal parametrizations of algebraic plane curves over the rationals. First, the standard singularity decomposition is determined, and therefore the rationality of the curve is decided (if the curve is not in regular position, see Sakkalis and Farouki (1990), a random change of coordinates is applied). Then, a nearly optimal parametrization is obtained. The output is a parametrization over $\mathbb{K}$ for odd degree curves, and over a finite extension of $\mathbb{K}$ of degree at most two, for even degree curves. Nevertheless, the procedure analyzes the existence of rational intersections from the singularities. Heuristics such as those mentioned in Section 2 or Step 4.1. in algorithm OPTIMAL-PARAMETRIZATION are used for trying to find rational simple points. In many cases, though the curve is of even degree, the algorithm either does not need to find rational simple points or it changes to need an even number of them. In both cases, it parametrizes over the rationals. We have observed that these heuristics do not lead to a relevant increase of the length of the coefficients of the linear system, and therefore of the output parametrization.

The second implementation is called REAL-PARAMETRIZE. Basically, it works as PARAMETRIZE, but it takes care of parametrizing over the reals when this is possible. Thus, REAL-PARAMETRIZE parametrizes over $\mathbb{Q}$ for odd degree curves, and over an algebraic extension of $\mathbb{Q}$ of degree at most two for even degree curves. Furthermore, the procedure analyzes the existence of simple real points on the curve, and in the affirmative case, it introduces a real algebraic number of degree at most two.

For demonstrating the performance of these implementations, let us consider the following example curve

$$F_1(x_1, x_2, x_3) := (x_1^2 + 4\,x_2\,x_3 + x_2^2)^2 - 16\,(x_1^2 + x_2^2)\,x_3^2$$

$$F_2(x_1, x_2, x_3) := x_2\,x_3^4 - \frac{29088}{2287}\,x_1^3\,x_2^2 + \frac{4352}{6861}\,x_1^5 + 4\frac{832}{48027}\,x_1^3\,x_3^2 - \frac{17264}{16009}\,x_1^3\,x_2\,x_3 + \frac{6976}{48027}\,x_1^4\,x_3$$
$$+\frac{2624}{2287}\,x_1^4\,x_2 + \frac{118908}{16009}\,x_1^2\,x_2\,x_3^2 - \frac{46248}{16009}\,x_1^2\,x_2^2\,x_3 + \frac{29360}{48027}\,x_1^2\,x_3^3 + \frac{26600}{2287}\,x_1^2\,x_2^3 - \frac{15252}{2287}\,x_1\,x_2^2\,x_3^2$$
$$+\frac{10468}{16009}\,x_1\,x_2^3\,x_3 - \frac{9372}{2287}\,x_1\,x_2^4 + \frac{22124}{16009}\,x_1\,x_2\,x_3^3 - \frac{49160}{48027}\,x_1\,x_3^4 + \frac{1035}{2287}\,x_2^5 + \frac{22454}{16009}\,x_2^3\,x_3^2 - \frac{208}{6861}\,x_3^5$$

$F_3(x_1,x_2,x_3) := 1805\,x_2^5+(3610\,x_1+3610\,x_3)\,x_2^4+(-2703\,x_1^2-12626\,x_1\,x_3-13533\,x_3^2)\,x_2^3+(5406\,x_1^2\,x_3+16218\,x_1\,x_3^2+10812\,x_3^3)\,x_2^2+(-4508\,x_1^2\,x_3^2-18032\,x_1\,x_3^3-16227\,x_3^4)\,x_2+3610\,x_1^2\,x_3^3+14440\,x_1\,x_3^4+14440\,x_3^5$

$F_4(x_1,x_2,x_3) := \frac{29493}{322}x_1^4x_2^2-\frac{14409}{70}x_1^3x_2^3-\frac{18691}{920}x_3x_1^4x_2+\frac{1561249}{6440}x_3x_1^3x_2^2+\frac{4757}{140}x_3x_1^2x_2^3 -\frac{320539}{3220}\,x_1^4\,x_3^2-\frac{4129}{6440}\,x_3^2\,x_1^3\,x_2-\frac{452397}{6440}\,x_3^2\,x_1^2\,x_2^2+x_3^2\,x_1\,x_2^3+\frac{3443}{140}\,x_3^3\,x_1^3+x_3^3\,x_1^2\,x_2+x_3^3x_1\,x_2^2 +x_3^3\,x_2^3$

$F_5(x_1,x_2,x_3) := \frac{1251}{115}\,x_2^4\,x_3^3+\frac{5184}{115}\,x_1\,x_2^3\,x_3^3+\frac{5354}{115}\,x_1^2\,x_2^2\,x_3^3+x_1^4\,x_3^3-\frac{9552}{115}\,x_1\,x_2^4\,x_3^2 -\frac{22496}{115}\,x_1^2\,x_2^3\,x_3^2-\frac{5424}{115}\,x_1^3\,x_2^2\,x_3^2-\frac{32}{23}\,x_1^4\,x_2\,x_3^2+192\,x_1^2\,x_2^4\,x_3+\frac{17472}{115}\,x_1^3\,x_2^3\,x_3-\frac{13824}{115}\,x_1^3\,x_2^4$

$F_6(x_1,x_2,x_3) := -\frac{155139}{400}\,x_1\,x_2^4\,x_3^2+\frac{40963}{200}\,x_1\,x_2^3\,x_3^3-\frac{19637}{25}\,x_1^3\,x_2^4+x_1^4\,x_3^3+\frac{17421}{400}\,x_2^4\,x_3^3 +x_1^4\,x_2^3+\frac{104727}{400}\,x_1^2\,x_2^2\,x_3^3+\frac{28477}{600}\,x_1^3\,x_2\,x_3^3-\frac{160421}{150}x_1^2x_2^3x_3^2-\frac{177781}{400}x_1^3x_2^2x_3^2+\frac{313519}{300}x_1^2x_2^4x_3 +\frac{324763}{300}\,x_1^3\,x_2^3\,x_3$

$F_7(x_1,x_2,x_3) := -\frac{64}{3}\,x_1^2\,x_2^5\,x_3-\frac{8873052}{5929}\,x_1^3\,x_2^3\,x_3^2-\frac{511740}{5929}\,x_1^5\,x_2\,x_3^2+\frac{336722448}{41503}\,x_1^3\,x_2^2\,x_3^3 +\frac{37077888}{41503}\,x_1x_2^4x_3^3+\frac{3718656}{5929}x_1^4x_2^2x_3^2-\frac{1479360}{5929}x_1x_2^5x_3^2+\frac{23765344}{17787}x_1^2x_2^4x_3^2-\frac{25912800}{5929}x_1^4x_2x_3^3 -\frac{65314160}{11319}\,x_1^2\,x_2^3\,x_3^3+\frac{34153200}{41503}\,x_1^5\,x_3^3+\frac{2794752}{41503}\,x_2^5\,x_3^3+x_1^5\,x_2^3$

$F_8(x_1,x_2,x_3) := -2\,x_1\,x_2^4\,x_3^4+x_1^4\,x_2^5+12\,x_1^4\,x_2^3\,x_3^2+12\,x_1^2\,x_2^4\,x_3^3-x_1^3\,x_2\,x_3^5+11\,x_1^3\,x_2^2\,x_3^4-21\,x_1^3\,x_2^3\,x_3^3-4\,x_1^4\,x_2\,x_3^4+2\,x_1^4\,x_2^2\,x_3^3-6\,x_1^4\,x_2^4\,x_3+x_1^5\,x_3^4-3\,x_1^5\,x_2^2\,x_3^2+x_1^5\,x_2^3\,x_3-3\,x_1\,x_2^5\,x_3^3-2\,x_1^2\,x_2^3\,x_3^4+x_1^3\,x_2^4\,x_3^2+x_2^5\,x_3^4$

$F_9(x_1,x_2,x_3) := x_3^5\,x_1\,x_2^4+x_3^4\,x_1\,x_2^5+x_3^5\,x_1^2\,x_2^3+x_3^3\,x_1^5\,x_2^2-19\,x_3^3\,x_1^2\,x_2^5-53\,x_3^3\,x_1^3\,x_2^4+x_3^4\,x_1^5\,x_2+x_1^5\,x_2^5+x_3^5\,x_1^5+43\,x_3^4\,x_1^3\,x_2^3+x_3^3\,x_1^4\,x_2^3+12\,x_3^2\,x_1^4\,x_2^4+57\,x_3^2\,x_1^3\,x_2^5-19\,x_3^2\,x_1^5\,x_2^3-36\,x_3\,x_1^4\,x_2^5+x_3^5\,x_2^5+21\,x_3\,x_1^5\,x_2^4-15\,x_3^5\,x_1^3\,x_2^2$

Table 1. shows the computing times for these curves. Times are measured on a DECSTATION 5240, and given in seconds of CPU time.

Table 1. Computing times

Curve	Degree of the curve	Degree of the field extension	Time
F_1	4	2 and real	21
F_2	5	1	72
F_3	5	1	17
F_4	6	1	4
F_5	7	1	5
F_6	7	1	7
F_7	8	1	28
F_8	9	1	252
F_9	10	1	461

References

Duval D. (1987). *Diverses questions relatives au calcul formel avec des nombres algébriques.* Ph.D. thesis, Institut Fourier, France.

Gebauer R., Kalkbrener M., Wall B. and Winkler F. (1991). *CASA: A computer algebra package for constructive algebraic geometry*. In: S.M. Watt (ed.) Proc. ISSAC'91, 403-410, ACM Press.

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

van Hoeij M. (1994). *Computing parametrizations of rational algebraic curves*. In: J. von zur Gathen (ed.), Proc. ISSAC'94, 187-190, ACM Press.

van Hoeij M. (1996). *Rational Parametrization of curves using Canonical Divisors*. J. Symbolic Computation, this special issue.

Ireland K., Rosen R. (1982). *A classical introduction to modern number theory*. Springer Verlag, Graduate Texts in Mathematics, New York.

Mňuk M., Sendra J.R., Winkler F. (1993). *On the complexity of parametrizing curves*. Techn. Rep. RISC 93-51, Research Inst. Symb. Comp., Univ. Linz. To appear in Beiträge zur Algebra und Geometrie.

Recio T., Sendra J.R., (1996). *Real Reparametrizations of Real Curves*. J. Symbolic Computation, this special issue.

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

Schicho J. (1992). *On the choice of pencils in the parametrization of curves*. J. Symbolic Computation **14,** 557-576.

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

Sendra J.R., Winkler F. (1991). *Symbolic parametrization of curves*. J. Symbolic Computation **12/ 6,** 607-631.

Sendra J.R., Winkler F. (1993). *Determining simple points on rational algebraic curves*. Techn. Rep. RISC 93-23, Research Inst. Symb. Comp., Univ. Linz.

Sendra J.R., Winkler F. (1994). *Optimal parametrization of algebraic curves*. Tech. Rep. RISC 94-65, Research Inst. Symb. Comp., Univ. Linz.