Fundamenta Informaticae 34 (1999) 1–18

IOS Press

Algorithms for Rational Real Algebraic Curves*

J. Rafael Sendra†
Dpto de Matemáticas,
Universidad de Alcalá,
E-28871 Madrid, Spain
mtsendra@alcala.es

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

Abstract. In this paper, we study fundamental properties of real curves, especially of rational real curves, and we derive several algorithms to decide the reality and rationality of curves in the complex plane. Furthermore, if the curve is real and rational, we determine a real parametrization. More precisely, we present a reality test algorithm for plane curves, and three different types of real parametrization algorithms that we call: direct parametrization algorithms (they compute a rational real parametrization, if it exists), algebraically optimal parametrization algorithms (they compute a rational real parametrization over the smallest possible real field extension, if the curve is rational and real), and hybrid parametrization algorithms (they combine parametrization and reparametrization techniques to derive algebraically optimal rational real parametrizations).

*The first author was supported by DGICYT PB 95/0563. The second author was supported by the Austrian *Fonds zur Förderung der wissenschaftlichen Forschung* under Proj. HySaX, P11160-TEC and SFB F013, Project 1304. Both authors were supported by the Austrian-Spanish exchange program Acción Integrada HU1997-0006.

†Address for correspondence: Dpto de Matemáticas, Universidad de Alcalá, E-28871 Madrid, Spain

‡Address for correspondence: RISC-Linz, J. Kepler Universität Linz, A-4040 Linz, Austria

1. Introduction

Rational curves are curves that can be parametrized by means of rational functions. If one is working over an algebraically closed field of characteristic zero, the rationality of the curve can be decided effectively, and if so, rational parametrizations can be computed. In [SW91], [SW97] we have described a symbolic parametrization algorithm. This algorithm is implemented in the system CASA [MW96]. Approaches to the parametrization problem for algebraic curves are also described in [AB88] or [vH97].

However, if one is not working over an algebraically closed field of characteristic zero, some of the most important results in algebraic geometry cannot be applied and therefore new difficulties arise. In particular, this is the case when working over the real numbers.

In this paper, we study fundamental properties of real curves, especially of rational real curves, and we derive several algorithms (direct algorithms, algebraically optimal algorithms, and hybrid algorithms) to decide the reality and rationality of curves in the complex plane. Furthermore, if the curve is real and rational, we determine a real parametrization.

The paper is structured as follows. In Section 2, the basic notions and results on rational algebraic plane curves are briefly summarized. In Section 3 the notion of a real curve is introduced and basic properties are presented. Section 4 is devoted to the analysis of the reality of a given plane curve. We present a constructive characterization for any plane curve defined by a real polynomial and without multiple components, that allows to decide the reality and, in the affirmative case, shows how real simple points on the curve can be computed. In Section 5 we present two diferent direct approaches to the real parametrization problem. In Section 6 we analyze the problem of computing algebraically optimal real parametrizations; i.e. rational parametrizations with coefficients in the smallest possible real field extension of the ground field. In this context, we show how the main ideas and results in [SW97] can be adapted and applied to the real case. Finally, in Section 7, we briefly show how the reparametrization algorithms presented in [ARS97] and [RS97a] can be combined with the algorithms given in the previous sections to derive hybrid parametrization algorithms, i.e. algorithms that first parametrize over the complex numbers, and afterwards reparametrize, if possible, over an optimal real algebraic field.

A preliminary version of this paper was presented at the conference AISC'98 and appeared in the proceedings [SW98].

We introduce some notation. Throughout this paper $\mathbb{K}$ is a field of characteristic 0, $\mathcal{K}$ is the algebraic closure of $\mathbb{K}$, $\mathbb{C}, \mathbb{R}$, and $\mathbb{Q}$ are the fields of complex, real, and rational numbers, respectively, $\mathbb{L}$ is a computable subfield of $\mathbb{C}$, and $\mathbb{F}$ is a computable subfield of $\mathbb{R}$. In addition, for any field Σ of characteristic zero, $\mathbb{A}^2(\Sigma)$ is the affine plane over Σ, and $\mathbb{P}^2(\Sigma)$ is the projective plane over Σ. Points in the projective plane will be written as $(a : b : c)$. Furthermore, if $f \in \not\prec[x, y]$ defines an affine plane curve $\mathcal{C}$ in $\mathbb{A}^2(\Omega)$, where Ω is the algebraic closure of Σ, i.e.

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

whenever useful or necessary, we will consider the projective plane curve $\mathcal{C}^*$ associated with $\mathcal{C}$

in $\mathbb{P}^2(\Omega)$, i.e.

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

where $F(x,y,z)$ denotes the homogenization of $f(x,y)$.

For the sake of simplicity we consider only algebraic curves with ordinary singularities. All the results presented here can be extended to curves with non-ordinary singularities (compare [SW91]).

2. Preliminaries on Rational Algebraic Curves

In this section we briefly introduce some of the basic notions and results on algebraic curves, and more precisely on rational algebraic plane curves. For further details and proofs we refer to classical text books on algebraic curves, such as [BK86], [Fu89] or [Wa50].

Definition 2.1. Let $\mathcal{K}(t)$ be the field of rational functions of $\mathcal{C}$ over $\mathcal{K}$. Then, we say that $x(t), y(t) \in \mathcal{K}(t)$ constitute a *rational parametrization* of a plane curve $\mathcal{C}$ over $\mathcal{K}$, if and only if, except for finitely many exceptions, every evaluation $(x(t_0), y(t_0))$ 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 $\mathcal{K}$. In this case, $\mathcal{C}$ is called *parametrizable* or *rational.*

Equivalently, $\mathcal{P}(t) = (x(t), y(t))$ is a rational parametrization of $\mathcal{C}$ if the mapping $\mathcal{P} : \mathcal{K} \longrightarrow \mathcal{C}$ is rational and not both $x(t)$ and $y(t)$ are constant. Furthermore, if $\mathcal{P}$ is birational we say that $\mathcal{P}(t)$ is a *proper parametrization.*

Only irreducible curves can be rational. Furthermore, the parametrization problem (i.e. the problem of dediсing whether an implicitly given plane curve is rational, and if so finding a rational parametrization) for affine curves is equivalent to the parametrization problem for the associated projective curves. Indeed, a parametrization of $\mathcal{C}$ can be computed from a parametrization of $\mathcal{C}^*$ and vice versa (see, e.g. [SW91]).

Some useful characterizations of the rationality of plane algebraic curves are summarized in the following theorem.

Theorem 2.1. *Let $\mathcal{C}$ be an irreducible plane curve over $\mathcal{K}$, and $f(x,y) \in \mathbb{K}[x,y]$ its defining polynomial. The following statements are equivalent:*

(1) *$\mathcal{C}$ is rational.*

(2) *There exist rational functions $x(t), y(t) \in \mathcal{K}(t)$, not both constant, such that $f(x(t), y(t)) = 0$.*

(3) *The field of rational functions on $\mathcal{C}$, i.e. $\mathcal{K}(\mathcal{C})$, is isomorphic to $\mathcal{K}(t)$.*

(4) *$\mathcal{C}$ is birationally equivalent to $\mathcal{K}$ (i.e. the affine line $\mathbb{A}^1(\mathcal{K})$).*

(5) $\text{genus}(\mathcal{C}) = 0$.

The genus of a plane curve $\mathcal{C}$ is a birational invariant that can be characterized by means of the multiplicities of the singular points of the curve. More precisely, let $\mathcal{C}$ be an irreducible curve in $\mathbb{A}^2(\mathcal{K})$, of degree d. If $\mathcal{C}$ has only ordinary singularities $P_1, \ldots, P_n$ of multiplicities $r_1, \ldots, r_n$, respectively (i.e. if for each P_i there are r_i different tangents to $\mathcal{C}$ at P_i), then

$$\text{genus}(\mathcal{C}) = \frac{1}{2}[(d-1)(d-2) - \sum_{i=1}^{n} r_i(r_i - 1)].$$

As a consequence of this fact, genus, and hence rationality, can be decided, for instance, using blowing up techniques (see [SW91]) or Puiseux expansions (see [BK86], [Wa50]).

Once the rationality of the plane curve has been decided, we want to compute a rational parametrization. The classical geometric parametrization algorithm (see [Wa50], [Wi96]) is based on the notion of linear systems of adjoint curves of some fixed degree. Let $T_1, \ldots, T_n$ be a fixed ordering of the set of monomials in x, y, z of degree r, where $n = \frac{1}{2}(r+1)(r+2)$. Then, for every projective curve $\mathcal{C}$ of degree r there exists $(a_1 : \cdots : a_n) \in \mathbb{P}^{n-1}(\mathcal{K})$, such that $F = a_1T_1 + \cdots + a_nT_n$ defines $\mathcal{C}$, and vice versa. Thus, the set of all projective curves of degree r is identified with $\mathbb{P}^{n-1}(\mathcal{K})$. Now, any linear variety of $\mathbb{P}^{n-1}(\mathcal{K})$ is called a *linear system of curves*, and the *dimension* of the linear system is defined as the dimension of the corresponding linear variety.

An interesting type of linear systems arises when requiring that the curves pass through given points with given multiplicities. Let $P_1, \ldots, P_m \in \mathbb{P}^2(\mathcal{K})$, and $r_1, \ldots, r_m$ be non-negative integers. Then, we consider the set of projective curves $\mathcal{C}$ of degree r such that $P_i \in \mathcal{C}$ with multiplicity at least r_i, for $i = 1, \ldots, m$. Clearly, these conditions are linear, and therefore one gets a linear system of curves. The points P_i are called *base points* of multiplicity r_i of the system. If $r_j = 1$ we say that P_j is a *simple base point*.

Definition 2.2. Let $\mathcal{C}$ be a projective plane curve of degree d, and let $P_1, \ldots, P_m$ be the singularities of $\mathcal{C}$, with multiplicities $r_1, \ldots, r_m$, respectively. Then, for every $d' \in \mathbb{N}$, such that $d' \geq d-2$, *the linear system of adjoint curves of degree d' to $\mathcal{C}$* is defined as the linear system of curves of degree d' having every point $P_i, 1 \leq i \leq m$, as a base point of multiplicity $r_i - 1$.

This leads immediately to the following classical parametrization algorithm.

<u>Algorithm</u> CLASSICAL-PARAMETRIZATION(f)

- **Input:** $f \in \mathbb{K}[x, y]$ irreducible and defining a curve $\mathcal{C}$ in $\mathbb{A}^2(\mathcal{K})$ of degree d.
- **Output:** the message "$\mathcal{C}$ `is not rational`" or a rational parametrization of $\mathcal{C}$ over $\mathcal{K}$.

(1) If $d = 1$ then $\mathcal{C}$ is a line, and obviously it can be parametrized over $\mathbb{K}$. EXIT.
(2) If $d = 2$, then

(2.1) take one point $P \in \mathcal{C}^*$ and compute the defining equation H of the pencil of lines passing through P,

(2.2) output the rational parametrization of $\mathcal{C}$ obtained by computing the free intersection point of F (F is the homogenization of f) and H. EXIT.

(3) Compute $g = \text{genus}(\mathcal{C})$. If $g \neq 0$ report "$\mathcal{C}$ `is not rational`" and EXIT.
(4) Compute the linear system $\mathcal{H}$ of adjoint curves of degree $d-2$ to $\mathcal{C}^*$.
(5) Take $(d-3)$ simple points on $\mathcal{C}^*$ and compute the equation H' of the linear subsystem of $\mathcal{H}$ having all these simple points as simple base points.
(6) Output the rational parametrization of $\mathcal{C}$ obtained by computing the free intersection point of F (F is the homogenization of f) and H'. □

Remark 2.1. In steps (2.2) and (6), there can be only one intersection point depending on the parameter, because of Bézout's Theorem on the number of intersection points. This intersection point can be computed as the only linear factor of the resultant of the two forms w.r.t. x or y, respectively, depending on the parameter.

Algorithm CLASSICAL-PARAMETRIZATION always determines a proper parametrization. Furthermore, this parametrization has coefficients in a subfield of $\mathcal{K}$ that contains the coefficients of the defining polynomial of the curve, and the coordinates of the simple points used in the algorithmic process. An example illustrating this algorithm can be found in [Wi96], Example 11.2.2, where the Cardiod is parametrized.

In [SW91], using linear systems of adjoints of higher degree, we show how to carry out this parametrization process with only one simple point on the curve. Hence, from [SW91], we get the following theorem.

Theorem 2.2. *Let $\mathcal{C}$ be a rational affine plane curve in $\mathbb{A}^2(\mathcal{K})$, and $f(x,y) \in \mathbb{K}[x,y]$ its defining polynomial. The following statements are equivalent:*

(1) There exists a rational parametrization of $\mathcal{C}$ with coefficients in a field extension Σ of $\mathbb{K}$.
(2) $\mathcal{C}$ has infinitely many points with coordinates in Σ.
(3) $\mathcal{C}$ has one simple point with coordinates in Σ.

In [HH90] the following theorem is proved.

Theorem 2.3. *Any rational affine curve in $\mathbb{A}^2(\mathcal{K})$, with defining polynomial over $\mathbb{K}$, can be parametrized over a field extension of $\mathbb{K}$ of degree at most two. Furthermore, if the degree of the curve is odd, then it can be parametrized over $\mathbb{K}$.*

In [SW97] we show how to actually determine this optimal field extension efficiently.

3. Real Algebraic Curves

In this section we introduce the notion of a real algebraic curve, and we present some of the most relevant facts on such curves.

Definition 3.1. Let $f \in \mathbb{L}[x,y]$ define a plane curve $\mathcal{C}$ in the complex plane. Then the curve $\mathcal{C}$ is called a *real algebraic curve* if and only if $\mathcal{C}$ has infinitely many points in the real plane.

Real curves are not necessarely defined by real polynomials. For instance, x^2+y^2-1 defines a real curve, but $x^2+i\,xy$ also defines a real curve, since all real points $(0,b)$, with $b \in \mathbb{R}$, are on the curve. Furthermore, a real polynomial may not define a real curve, like for instance x^2+y^2+1. However, if the real curve is irreducible, then it always has a defining polynomial over the reals. A proof of the following lemma is given in [RS95].

Lemma 3.1. *Any irreducible real plane curve can be defined by a real polynomial.*

Clearly, from Bezout's Theorem, we get that a plane curve in the complex plane is real if and only if at least one component of the curve is real. Therefore, since one can always decompose any curve into irreducible components over $\mathbb{C}$, and taking into account Lemma 1, in the sequel we can assume that a *real plane curve* is a curve in the complex plane defined by a real square-free polynomial, and having infinitely many real points.

Also the irreducibility of real curves does not depend on whether we view it in $\mathbb{A}^2(\mathbb{R})$ or in $\mathbb{A}^2(\mathbb{C})$. A proof of the following lemma is given in [Wi96], Theorem 5.5.3.

Lemma 3.2. *Let $\mathcal{C}$ be a real curve defined by $f \in \mathbb{F}[x,y]$. $\mathcal{C}$ is irreducible over $\mathbb{R}$ if and only if $\mathcal{C}$ is irreducible over $\mathbb{C}$.*

As a consequence of Theorem 2 and Lemma 1, one can deduce that every parametrizable real curve can actually be parametrized with coefficients in the reals. This is of vital importance for practical applications, since in areas like computer aided geometric design we are usually interested in curves and surfaces over the reals. This result is also known as the algebraic version of Real Lüroth's Theorem [RS97b].

Theorem 3.1. *Every rational real algebraic curve can be parametrized over the reals.*

Applying Theorem?? and Lemma??, one also deduces that a parametrizable plane curve is real if and only if it has at least one real simple point. However, since we are working over $\mathbb{R}$, this last statement can be established more generally.

Theorem 3.2. *An affine plane curve $\mathcal{C}$ in $\mathbb{A}^2(\mathbb{C})$, defined by a square-free polynomial over $\mathbb{R}$, is real if and only if $\mathcal{C}$ has at least one simple point with real coordinates.*

Proof:
The left-to-right implication follows from the definition of a real curve, and from the fact that curves without multiple components only have finitely many singularities. Conversely, let $f \in \mathbb{R}[x,y]$ define the curve $\mathcal{C}$, and let $P \in \mathbb{A}^2(\mathbb{R})$ be a simple point on $\mathcal{C}$. Hence, not both partial derivatives of f vanish at P. Therefore, since f is real, we can apply the Implicit Function Theorem and deduce that $\mathcal{C}$ has infinitely many points in $\mathbb{A}^2(\mathbb{R})$. Thus, $\mathcal{C}$ is a real curve. $\square$

Note that Theorem?? is not true without the assumption of square-freeness; for instance, the curve of equation x^2 has infinitely many real points, but all of them are singular. However, we will always have square-free defining polynomials if we consider only curves without multiple components.

4. Reality Test for Algebraic Curves

In Section 3, Theorem 5, we have seen how the reality of a plane curve without multiple components is characterized by means of the existence of simple points with real coordinates. Moreover, the particular case of lines and conics can be treated specially: a line is real if and only if its monic defining polynomial is real, and reality of conics can be decided by means of the signature and rank of the corresponding quadratic form.

However, in this section, we present a constructive characterization for any plane curve defined by a real polynomial and without multiple components, that allows to decide the reality and, in the affirmative case, shows how real simple points on the curve can be computed. As a consequence of this result an algorithmic method is presented.

We start with a well known result in Real Algebra that can be directly deduced from the theory of Cylindrical Algebraic Decomposition (see, e.g., [Co75] or Section 9.2. in [Wi96]).

Lemma 4.1. *Let $f \in \mathbb{R}[x,y]$ be a square-free polynomial, let $D(x)$ be the discriminant of f with respect to the variable y, and let $I \subseteq \mathbb{R}$ be non-empty and connected. If $D(x)$ does not vanish on any element of I, then for every $a \in I$ the number of real roots of the univariate polynomial $f(a,y)$ is constant.*

Theorem 4.1. *Let $f \in \mathbb{R}[x,y]$ be a square-free polynomial, not having a linear factor independent of y. Let $\mathcal{C}$ be the affine plane curve defined by f in the complex plane, and let $D(x)$ be the discriminant of f with respect to the variable y. Then, it holds that:*

(1) If $D(x)$ has no real root, then $\mathcal{C}$ is a real plane curve if and only if the univariate polynomial $f(0,y)$ has real roots. Furthermore, if α is a real root of $f(0,y)$, then $(0,\alpha)$ is a real simple point of $\mathcal{C}$.

(2) If $D(x)$ has real roots, let $b_0,\ldots,b_r \in \mathbb{R}$ be such that

$$-\infty = a_0 < b_0 < a_1 < b_1 < a_2 < \cdots < b_{r-1} < a_r < b_r < a_{r+1} = +\infty,$$

where $a_1,\ldots,a_r$ are the real roots of $D(x)$. Then, $\mathcal{C}$ is a real plane curve if and only if there exists $i \in \{0,\ldots,r\}$ such that the univariate polynomial $f(b_i,y)$ has real roots. Furthermore, if α is a real root of $f(b_i,y)$, then (b_i,α) is a real simple point of $\mathcal{C}$.

Proof:
(1) Let $\mathcal{C}$ be a real plane curve. Since f is square-free, $\mathcal{C}$ has infinitely many real simple points. Let (a,b) be a real simple point on $\mathcal{C}$. Then, the polynomial $f(a,y)$ has real roots. Thus, if we take $I = \mathbb{R}$ in Lemma 3, since $D(x)$ does not vanish over the reals, for every $\lambda \in \mathbb{R}$ the polynomial $f(\lambda,y)$ has real roots; in particular $f(0,y)$ has real roots. Furthermore, if α is a real root of $f(0,y)$, then $(0,\alpha)$ is a point on the curve. Moreover, since $D(x)$ has no real root, the point $(0,\alpha)$ is simple.

Conversely, if $f(0,y)$ has real roots, we can apply Lemma 3 with $I = \mathbb{R}$ and deduce that any vertical line $x = a$, with $a \in \mathbb{R}$, intersects the curve at a real point. Thus, $\mathcal{C}$ has infinitely many real points and, therefore, is a real curve.

(2) The proof is similar to the proof of (1), but instead of $I = \mathbb{R}$ we consider the intervals $I = (a_i, a_{i+1})$, where $i = 0, \ldots, r$. Observe, that we excluded linear factors independent of y from f, so there can be only finitely many curve points of the form (a_i, λ). □

Remark 4.1. The proof of Theorem 6 is constructive, and we can derive a method for computing any number of real simple points. More precisely, if $D(x)$ has no real roots, then for every $a \in \mathbb{R}$ the polynomial $f(a,y)$ has real roots. Therefore, for every $a \in \mathbb{R}$ and for every real root α of $f(a,y)$, the point (a,α) is simple. On the other hand, if $D(x)$ has real roots, and $f(b_j,y)$ has real roots, then for every $a \in (a_j, a_{j+1})$ the polynomial $f(a,y)$ has real roots. Hence, for every $a \in (a_j, a_{j+1})$ and for every real root α of $f(a,y)$, the point (a,α) is simple.

We outline an algorithm for testing the reality of an algebraic curve. For this purpose, we use subalgorithms to decide the existence of real roots of univariate polynomials, and to "*compute*" them (see, e.g., [CR88], [Jo98], or [Mis93]). Clearly, the meaning of "*computing*" a real root depends on whether we want to manipulate the root numerically or symbolically. In our case, we work symbolically with the roots, by means of their minimal polynomials and approximating intervals, if necessary.

Algorithm REALITY-TEST(f, N)

- **Input:** $f \in \mathbb{F}[x,y]$ square-free and defining a curve $\mathcal{C}$ in $\mathbb{A}^2(\mathbb{C})$; $N \in \mathbb{N}$.
- **Output:** the message "$\mathcal{C}$ `is a real curve`" and N real simple points of $\mathcal{C}$, or the message "$\mathcal{C}$ `is not real`".

(1) If f has a real factor of the form $x - a$, then report "$\mathcal{C}$ `is a real curve`" and return N simple points on the line $x = a$. EXIT.
(2) Compute the discriminant $D(x)$ of the polynomial $f(x,y)$ with respect to y.
(3) Decide whether $D(x)$ has real roots.
(4) If $D(x)$ has no real root, decide whether $f(0,y)$ has real roots.

  (4.1) If $f(0,y)$ has no real roots, report "$\mathcal{C}$ `is not a real curve`".

  (4.2) If $f(0,y)$ has real roots, report "$\mathcal{C}$ `is a real curve`". For every $a \in \mathbb{Q}$ there are real simple points of the form (a,λ). "*Compute*" N of them, and return them.

(5) If $D(x)$ has real roots, isolate them with rational numbers $b_0, \ldots, b_r$:

$$-\infty = a_0 < b_0 < a_1 < b_1 < a_2 < \cdots < b_{r-1} < a_r < b_r < a_{r+1} = +\infty,$$

where $a_1, \ldots, a_r$ are the real roots of $D(x)$.

  (5.1) Check whether, at least, one polynomial $f(b_i,y)$, $i = 0, \ldots, r$, has real roots. If no polynomial $f(b_i,y)$, $i = 0, \ldots r$, has real roots, report "$\mathcal{C}$ `is not a real curve`".

  (5.2) If there exists b_j such that $f(b_j,y)$ has real roots, report "$\mathcal{C}$ `is a real curve`". For every rational $a \in (a_j, a_{j+1})$ there are real simple points of the form (a,λ). "*Compute*" N of them, and return them. □

Example 4.1. Let $\mathcal{C}$ be the plane curve of degree 5 in $\mathbb{A}^2(\mathbb{C})$ defined by:

$$f(x,y) = 3\,y^3 - 3\,xy^2 - 2\,xy^3 + x^2y^3 + x^3.$$

We apply the algorithm Reality-Test to decide whether $\mathcal{C}$ is real, and if so to compute one real simple point. For this purpose, we compute the discriminant $D(x)$ of f with respect to y:

$$D(x) = 27\,x^6\left(3 - 2\,x + x^2\right)\left(x^2 - 2\,x + 5\right)(x-1)^2.$$

$D(x)$ has two different real roots, $a_1 = 0$ and $a_2 = 1$, that can be isolated as:

$$b_0 = -1 < a_1 = 0 < b_1 = \frac{1}{2} < a_2 = 1 < b_2 = 2.$$

Now, we analyze the existence of real roots of the polynomials $f(b_j, y)$. The polynomial $f(b_0, y) = 6y^3 + 3y^2 - 1$ has only the real root

$$\alpha = \frac{\sqrt[3]{17 + 12\sqrt{2}}}{6} + \frac{1}{6\cdot\sqrt[3]{17+12\sqrt{2}}} - \frac{1}{6}.$$

Hence, $\mathcal{C}$ is a real curve, and $P = (-1, \alpha)$ is a real simple point of $\mathcal{C}$.

Now, we apply the algorithm to the curve $\mathcal{C}'$ defined by the polynomial $g(x,y) = 2y^2 + x^2 + 2x^2y^2$ (see [RS97a]). We first compute the discriminant $D(x)$ of g with respect to y: $D(x) = 16(1+x^2)^2x^2$. Therefore, since $D(x)$ has real roots, we isolate them. We take $b_0 = -1 < a_1 = 0 < b_1 = 1$. $g(b_0, y) = 4y^2 + 1 = g(b_1, y)$. Hence, applying the algorithm we conclude that $\mathcal{C}'$ is not a real curve.

5. Direct Real Parametrization Algorithms

In this section we present two different direct approaches to the real parametrization problem. The first approach is based on the Classical-Parametrization algorithm, while the second one applies the techniques introduced in [SW91].

Algorithm Direct-Real-Parametrization-I(f)

- **Input:** $f \in \mathbb{F}[x,y]$ irreducible and defining a curve $\mathcal{C}$ of degree d in $\mathbb{A}^2(\mathbb{C})$.
- **Output:** the message "$\mathcal{C}$ `is not rational`", or the message "$\mathcal{C}$ `is not real`", or a real rational parametrization of $\mathcal{C}$.

(1) If $d = 1$ then $\mathcal{C}$ is a line. Output a real parametrization and Exit.

(2) If $d = 2$ perform Reality-Test($f, 1$). If the output is the message "$\mathcal{C}$ `is not real`", report "$\mathcal{C}$ `is not real`" and Exit. Otherwise, proceed as in step (2) of Classical-Parametrization, using the point P returned by Reality-Test. Exit.

(3) Perform REALITY-TEST($f, d-3$). If the output is the message "$\mathcal{C}$ `is not real`", report "$\mathcal{C}$ `is not real`" and EXIT. Otherwise, say that $P_1, \ldots, P_{d-3}$ are the $d-3$ real simple points returned by REALITY-TEST.
(4) Compute $g = \text{genus}(\mathcal{C})$. If $g \neq 0$ report "$\mathcal{C}$ `is not rational`" and EXIT.
(5) Compute the linear system $\mathcal{H}$ of adjoint curves of degree $d-2$ to $\mathcal{C}^*$.
(6) Compute the equation H' of the linear subsystem of $\mathcal{H}$, having $P_1, \ldots, P_{d-3}$ as simple base points.
(7) Output the rational parametrization of $\mathcal{C}$ obtained by computing the free intersection point of F and H'. □

In general, the parametrization determined by this algorithm is given over a field extension $\mathbb{F}(\alpha_1, \ldots, \alpha_{d-3})$ of $\mathbb{F}$, where α_i, for $i = 1, \ldots, d-3$, are real algebraic numbers of degree at most d. The field extensions are introduced in steps (2) or (3), when computing the simple points on $\mathcal{C}$. Hence, in general, one needs to introduce a very high algebraic extension of the ground field $\mathbb{F}$.

But, as demonstrated in [SW91], a single simple point is sufficient in the parametrization process. This leads to a second direct parametrization approach, which requires only a real algebraic extension of $\mathbb{F}$ of degree at most d. For this purpose, we introduce the following definition.

Definition 5.1. Let $F \in \mathbb{F}[x, y, z]$ be an irreducible homogeneous polynomial defining a projective plane curve $\mathcal{C}$. Let $p_1, p_2, p_3, m \in \mathbb{F}[t]$. The set of projective points

$$\mathcal{F} = \{(p_1(\alpha) : p_2(\alpha) : p_3(\alpha)) \mid m(\alpha) = 0\} \subset \mathbb{P}^2(\mathbb{C})$$

is called a *family of s conjugate simple points on $\mathcal{C}$ over $\mathbb{F}$* if and only if the following conditions are satisfied: $m(t)$ is a square-free polynomial of degree s, $\deg(p_i) < \deg(m)$ for $i = 1, 2, 3$, $\gcd(p_1, p_2, p_3) = 1$, $\mathcal{F}$ contains exactly s points of $\mathbb{P}^2(\mathbb{C})$, $F(p_1(t), p_2(t), p_3(t)) = 0 \bmod m(t)$, and there exists $v \in \{x, y, z\}$ such that $\frac{\partial F}{\partial v}(p_1(t), p_2(t), p_3(t)) \bmod m(t) \neq 0$. □

Let $F(x, y, z) \in \mathbb{F}[x, y, z]$ be the defining homegeneous polynomial of a rational projective curve $\mathcal{C}$, and let $P \in \mathcal{C} \cap \mathbb{P}^2(\mathbb{F}(\alpha))$ be a simple point. If we choose all the points in a family of conjugate points over $\mathbb{F}(\alpha)$ as additional base points in the system of adjoint curves, then the defining polynomial of the corresponding subsystem will have coefficients in $\mathbb{F}(\alpha)$. Therefore, one can proceed as follows:

<u>Sub-algorithm-I</u>

(1) Take 3 different families $\mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_3$ of $(d-1)$ conjugate simple points each on $\mathcal{C}$ over $\mathbb{F}(\alpha)$, by intersecting $\mathcal{C}$ with lines passing through P and defining polynomials over $\mathbb{F}(\alpha)$.
(2) Compute the equation of the system $\mathcal{H}$ of adjoint curves to $\mathcal{C}$ of degree d.
(3) Take a point $Q \in \mathbb{P}^2(\mathbb{F}) \setminus \mathcal{C}$.
(4) Determine the equation H' of the linear subsystem $\mathcal{H}'$ of $\mathcal{H}$ obtained by introducing the new simple base points $\mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_3$ and Q. □

Observe that $H' \in \mathbb{F}(\alpha)[x,y,z]$ and that $\dim(\mathcal{H}') = 1$. $\mathcal{C}$ is not in $\mathcal{H}'$, because $Q \notin \mathcal{C}$. Hence, computing the free intersection point of F and H', we get a real parametrization of $\mathcal{C}$ over $\mathbb{F}(\alpha)$. These ideas are summarized in the following algorithm.

Algorithm DIRECT-REAL-PARAMETRIZATION-II(f)

- **Input:** $f \in \mathbb{F}[x,y]$ irreducible and defining a curve $\mathcal{C}$ of degree d in $\mathbb{A}^2(\mathbb{C})$.
- **Output:** the message "$\mathcal{C}$ `is not rational`", or the message "$\mathcal{C}$ `is not real`", or a real rational parametrization of $\mathcal{C}$.

(1) If $d \leq 4$ perform DIRECT-REAL-PARAMETRIZATION-I(f) and EXIT.
(2) Perform REALITY-TEST(f, 1). If the output is the message "$\mathcal{C}$ `is not real`", report "$\mathcal{C}$ `is not real`" and EXIT. Otherwise, let $P \in \mathcal{C} \cap \mathbb{R}^2$ be the real simple point returned by REALITY-TEST.
(3) Compute $g = \text{genus}(\mathcal{C})$. If $g \neq 0$ report "$\mathcal{C}$ `is not rational`" and EXIT.
(4) Apply Sub-algorithm-I to $\mathcal{C}^*$ and P, to get the polynomial H'.
(5) Output the rational parametrization of $\mathcal{C}$ obtained by computing the free intersection point of F and H'. □

Example 5.1. Let $\mathcal{C}$ be the affine plane curve of degree 5 introduced in Example 1. We already know that $\mathcal{C}$ is a real curve, and that $P = (-1 : \alpha : 1)$ is a real simple point of $\mathcal{C}^*$. Now we compute the genus of $\mathcal{C}$. The singularities of $\mathcal{C}^*$ are $Q_1 = (0:0:1), Q_2 = (0:1:0), Q_3 = (1:0:0), Q_4 = (1:1:1)$, where Q_1 is of multiplicity 3, and Q_2, Q_3, Q_4 are double points. Thus, $\text{genus}(\mathcal{C}) = 0$, and therefore $\mathcal{C}$ is rational. In order to compute a real rational parametrization, we first determine the defining polynomial H of the linear system $\mathcal{H}$ of adjoint curves to $\mathcal{C}^*$ of degree 5. Afterwards, we take a point $Q \notin \mathcal{C}^*$, for instance $Q = (1 : -1 : 1)$, and 3 families of 4 conjugate points on lines through P. More precisely, we take the following families over $\mathbb{Q}(\alpha)$:

$$\mathcal{F}_1 = \{(-1+\beta : \alpha+\beta : 1) \mid q_1(\beta) = 0\}$$

$$\mathcal{F}_2 = \{(-1+2\beta : \alpha+\beta : 1) \mid q_2(\beta) = 0\}$$

$$\mathcal{F}_2 = \{(-1+\beta : \alpha+2\beta : 1) \mid q_3(\beta) = 0\}$$

where

$$q_1(t) = 14 + 24\,t^2 - 24\,t^3 + 6\,t^4 + 36\,\alpha + 102\,\alpha^2 + 72\,\alpha t - 75\,\alpha^2 t - 72\,\alpha t^2 + t + 18\,\alpha^2 t^2 + 18\,\alpha t^3,$$
$$q_2(t) = -78\,\alpha^2 t - 25\,t + 14 + 48\,\alpha^2 + 24\,t^2 - 24\,t^3 + 12\,t^4 + 18\,\alpha + 18\,\alpha t - 72\,\alpha t^2 + 36\,\alpha^2 t^2 + 36\,\alpha t^3,$$
$$q_3(t) = -147\,\alpha^2 t + 55\,t + 14 + 210\,\alpha^2 + 222\,t^2 - 192\,t^3 + 48\,t^4 + 72\,\alpha + 360\,\alpha t - 288\,\alpha t^2 + 36\,\alpha^2 t^2 + 72\,\alpha t^3.$$

Now we determine the equation H' of the subsystem of $\mathcal{H}$ that has Q and the points of the families $\mathcal{F}_i$, for $i = 1,2,3$, as simple base points. This implies to solve the linear system of equations, in the undetermined coefficients of H, given by the conditions:

$$H(Q) = 0, \;\; H(-1+t, t+\alpha, 1) = 0 \bmod q_1(t),$$

$$H(-1+2t, t+\alpha, 1) = 0 \bmod q_2(t), \quad H(-1+t, 2t+\alpha, 1) = 0 \bmod q_3(t).$$

Finally, we compute the resultants of $f(x,y)$ and $H'(x,y,1)$, w.r.t. x and y, respectively. From the primitive parts of these resultants w.r.t. the parameter t we get the following parametrization over the real extension $\mathbb{Q}(\alpha)$ of $\mathbb{Q}$:

$$\mathcal{P}(t) = \left(\frac{-m_1(t)}{30187403656778\, t^3}, \frac{m_2(t)}{m_3(t)}\right)$$

where

$m_1(t) = -24793190 - 58397220\,\alpha - 63160272\,\alpha^2 - 57469827\,t - 135310473\,\alpha t - 146409246\,\alpha^2 t - 13688774\,t^3 - 33436584\,\alpha t^3 - 33983280\,t^3\alpha^2 - 47810298\,t^2 - 112758282\,\alpha t^2 - 121478652\,\alpha^2 t^2$

$m_2(t) = 14503164\alpha^2 + 5692324 + 13408542\alpha + 13208451t + 31052925\alpha + 10900410t^2 + 33579270\alpha^2 t + 26009478\alpha t^2 + 2733151t^3 + 8222472\alpha t^3 + 8792187t^3\alpha^2 + 28038096\alpha^2 t^2$

$m_3(t) = 134t(2104 + 4896\alpha + 5337\alpha^2)(3t^2 - 54\alpha^2 t + 5t + 27\alpha t + 3\alpha + 6\alpha^2 + 2).$

6. Algebraically Optimal Real Parametrization Algorithm

Since linear systems of adjoint curves of any degree to a rational plane curve $\mathcal{C}$ have defining polynomial over $\mathbb{F}$, and can be computed in a finite number of ground field operations [SW91], the problem of algebraically optimal real parametrization is reduced to the problem of determining one algebraically optimal real simple point on the curve (i.e. a simple point on the curve with coordinates in the smallest possible real extension of $\mathbb{F}$).

In this section we deal with the problem of finding such a simple point. To solve the problem we transform $\mathcal{C}$ birationally to a conic $\mathcal{D}$. The real simple points on $\mathcal{C}$ and on $\mathcal{D}$ correspond uniquely to each other, except for finitely many exceptions. So there is a real simple point on $\mathcal{C}$ if and only if there is a real simple point on $\mathcal{D}$. This question can be decided. If the answer is yes, a real point on $\mathcal{D}$ can be computed, transformed to a real point on $\mathcal{C}$, and from this point we can derive a parametrization of $\mathcal{C}$ over $\mathbb{R}$.

In [SW97] we proved the following generalization of a theorem by Hilbert and Hurwitz [HH90].

Theorem 6.1. *Let $\mathcal{C}$ be a rational plane curve of degree d defined by a polynomial over $\mathbb{F}$, let $\mathcal{H}_a$ be the linear system of adjoint curves to $\mathcal{C}$ of degree $a \in \{d, d-1, d-2\}$, and let $\tilde{\mathcal{H}}_a^s$ be a linear subsystem of $\mathcal{H}_a$ of dimension s obtained from $\mathcal{H}_a$ by fixing additional 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

$$\mathcal{T} = \{x' : y' : z' = \Phi_1 : \Phi_2 : \Phi_3\}$$

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.

In order to apply Theorem 7, we need to select a linear subsystem of low dimension in the system of adjoint curves by fixing additional base points. The same effect can be achieved by suitably increasing the multiplicities at the existing base points. These additional base points will introduce algebraic coefficients into the system, unless we can find rational ones or whole conjugate families of such points.

Definition 6.1. Let $\mathcal{C}$ be a projective plane curve defined by a polynomial over $\mathbb{F}$, let $\mathcal{H}$ be a linear system of adjoint curves to $\mathcal{C}$, let $\tilde{H}$ be 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 and only if the following conditions are satisfied: $\tilde{H} \in \mathbb{F}[x, y, z]$, and for almost every curve $\Phi \in \mathcal{H}$, and $\tilde{\Phi} \in \tilde{\mathcal{H}}$

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

where $\mathrm{mult}_P(\mathcal{C}_1, \mathcal{C}_2)$ 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 $\mathcal{C}$ is used to generate a subsystem $\tilde{\mathcal{H}}$ of $\mathcal{H}$ (by introducing some points on $\mathcal{C}$ as new base point on $\mathcal{H}$ with specific multiplicities) the linear system of equations containing the contraints is over $\mathbb{F}$, and its rank equals to the number of new known intersection points between $\mathcal{C}$ and a generic representative of the subsystem. In the next lemma some special cases of rational linear subsystems are analyzed. Lemma 4 and Theorem 8 are proved in [SW97].

Lemma 6.1. *Let $\mathcal{C}$ be a rational plane curve of degree d defined by a polynomial over $\mathbb{F}$, let $\mathcal{H}_a$ be the linear system of adjoint curves to $\mathcal{C}$ of degree $a \in \{d, d-1, d-2\}$, and let $\mathcal{F} = \{(p_1(\alpha) : p_2(\alpha) : p_3(\alpha)) \mid A(\alpha) = 0\}$ be a family of k conjugate points on $\mathcal{C}$ over $\mathbb{F}$. 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 $\dim(\tilde{\mathcal{H}}_a) = \dim(\mathcal{H}_a) - r\,k$.

Theorem 6.2. *Let $\mathcal{C}$ be a rational plane curve of degree d defined by a polynomial over $\mathbb{F}$, and let $\mathcal{H}_a$ be 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, derived from $\mathcal{H}_a$ by fixing additional base points on $\mathcal{C}$, provides curves that generate families of s conjugate simple points over $\mathbb{F}$ by intersection with $\mathcal{C}$.*

The proof of Theorem 8, given in [SW97], is constructive and we can derive the following algorithm from it.

Sub-algorithm-II

(1) Take $\Phi \in \tilde{\mathcal{H}}_a$ with no common tangents with $\mathcal{C}$, and such that all the x-coordinates of all the intersection points of Φ and F, that are not base points of $\tilde{\mathcal{H}}_a$, are different.
(2) Compute the resultant $\tilde{R}_1(x)$ of $\Phi(x,y,1)$ and $f(x,y)$ w.r.t. y, and the resultant $\tilde{R}_2(y)$ of $\Phi(x,y,1)$ and $f(x,y)$ w.r.t. x. Cross out in $\tilde{R}_1$ and in $\tilde{R}_2$ the factors that determine the x-coordinates of the intersection points of $\mathcal{C}$ and $\tilde{\mathcal{H}}_a$ that are not base points: say that R_1 and R_2 are the factors left in $\tilde{R}_1$ and $\tilde{R}_2$, respectively.
(3) Compute $S(x,y) = f(x,y) \bmod R_1(x)$, and determine the first subresultant $M(x,y) = ax + by + c$ w.r.t. y of $S(x,y)$ and $R_2(y)$ modulo $R_1(x)$.
(4) Output $\{(\alpha : \frac{-c-a\alpha}{b} : 1) \mid R_1(\alpha) = 0\}$. □

As a consequence of Lemma 4 and Theorem 8 we get the following algorithmically important facts.

Theorem 6.3. *Let $\mathcal{C}$ be a rational plane curve of degree d defined by a polynomial $f(x,y) \in \mathbb{F}[x,y]$.*

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

Proof:
(i) Let $P_1, \ldots, P_n$ be the singular points on $\mathcal{C}$, having multiplicities $r_1, \ldots, r_n$, respectively. Since $\mathcal{C}$ is rational, by Lemma 4 and genus formula, one has that $\dim(\mathcal{H}_{d-2}) = d-2$. Now we can apply Theorem 8 for $s = d-2$ (i.e. choosing the whole system) and we get that $\mathcal{C}$ has families of $d-2$ conjugate simple points. Similarly, by using systems of adjoint curves of degrees $d-1$ and d, respectively, we get that $\mathcal{C}$ has families of $2d-2$ and $3d-2$ conjugate simple points.
(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 Lemma 4 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 2. Thus, applying Theorem 8 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 Lemma 4 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 8 one concludes that $\mathcal{C}$ has simple points over $\mathbb{L}$.
(iv) This is an inmediate consequence of statement (ii). □

Summarizing, we get the following algorithm for deciding the parametrizability over $\mathbb{R}$ and, in the positive case, computing such a parametrization. Note that the proof of Theorem 9 is constructive. Thus, in the design of the next algorithm we will refer to Theorem 9. We also assume that we have an algorithm for deciding whether an irreducible conic, with defining polynomial over $\mathbb{F}$, has rational points (i.e. points with coordinates in $\mathbb{F}$), and if so determining one of them. For details see [IR82] and [HW98].

Algorithm ALGEBRAICALLY-OPTIMAL-REAL-PARAMETRIZATION(f)

- **Input:** $f \in \mathbb{F}[x,y]$ irreducible and defining a curve $\mathcal{C}$ of degree d.
- **Output:** the message "$\mathcal{C}$ `is not rational`", or the message "$\mathcal{C}$ `is not real`", or an algebraically optimal real rational parametrization of $\mathcal{C}$.

(1) If $d=1$ then $\mathcal{C}$ is a line. Output a real rational parametrization and EXIT.

(2) Perform REALITY-TEST($f, 1$). If the output is the message "$\mathcal{C}$ `is not real`", report "$\mathcal{C}$ `is not real`" and EXIT. Otherwise, say that $P \in \mathcal{C} \cap \mathbb{R}^2$ is the real simple point returned by REALITY-TEST.

(3) If $d=2$ decide whether $\mathcal{C}$ has rational points. If so, replace P by one of them (if no rational point exists, P is optimal). Compute the defining equation H of the pencil of lines passing through P. Output the rational parametrization of $\mathcal{C}$ obtained by computing the free intersection point of F and H. EXIT.

(4) Compute $g = \text{genus}(\mathcal{C})$. If $g \neq 0$ report "$\mathcal{C}$ `is not rational`" and EXIT.

(5) Compute the equation H of the linear system $\mathcal{H}$ of adjoint curves of degree $d-2$ to $\mathcal{C}^*$.

(6) If d is odd, apply Theorem 9 (ii) to find $\frac{d-3}{2}$ families of two simple conjugate points of $\mathcal{C}$ over $\mathbb{F}$. Determine the equation $H' \in \mathbb{F}[x,y,z]$ of the rational subsystem of $\mathcal{H}$, obtained by forcing these families to be simple base points. Output the rational parametrization of $\mathcal{C}$ obtained by computing the free intersection point of F and H'. EXIT.

(7) If d is even, apply Theorem 9 (ii) to find $\frac{d-4}{2}$ families of two simple conjugate points of $\mathcal{C}$ over $\mathbb{F}$. Determine the rational subsystem $\tilde{\mathcal{H}}$ of $\mathcal{H}$, obtained by forcing these families to be simple base points.

(8) Take $\Phi_1, \Phi_2, \Phi_3 \in \tilde{\mathcal{H}}$ such that the common intersections of the three curves Φ_i and F are the set of base points of $\tilde{\mathcal{H}}$, and such that $\mathcal{T} = \{x' : y' : z' = \Phi_1 : \Phi_2 : \Phi_3\}$ is a birational transformation (Theorem 7).

(9) Determine $\mathcal{D} = \mathcal{T}(\mathcal{C})$. $\mathcal{D}$ is a conic, and it can be efficiently computed by mapping 5 points of $\mathcal{C}$ and interpolating.

(10) Determine a point Q on $\mathcal{D}$ with coordinates in an extension field Σ of $\mathbb{F}$ of lowest degree, and such that $\mathcal{T}^{-1}(Q)$ is defined. Replace P by $\mathcal{T}^{-1}(Q)$.

(11) Compute the defining equation $H' \in \Sigma[x,y,z]$ of the rational subsystem of $\tilde{\mathcal{H}}$ obtained by forcing P to be a simple base point. Output the rational parametrization of $\mathcal{C}$ obtained by computing the free intersection point of F and H'. EXIT. □

Example 6.1. Let $\mathcal{C}$ be the affine plane curve of degree 5 introduced in Example 1 and 2. We already know that $\mathcal{C}$ is a real rational curve. Now, we want to obtain an algebraically optimal real parametrization of $\mathcal{C}$. Since degree of $\mathcal{C}$ is odd, we compute $\frac{d-3}{2} = 1$ family $\mathcal{F}$ of two conjugate points over $\mathbb{Q}$. For this purpose, we follow the proof of Theorem 9 (ii): we compute the defining equation H_3 of the system of adjoints of degree 3; we obtain, by means of H_3 (Sub-algorithm-II) two families $\mathcal{F}_1$, $\mathcal{F}_2$ of $d-2=3$ conjugate points; we determine the defining equation of the system H_4 of adjoints of degree 4, and the subsystem $\tilde{H}_4$ of H_4, obtained by forcing $\mathcal{F}_1$, $\mathcal{F}_2$ to be simple base points of H_4; applying Sub-algorithm-II to $\tilde{H}_4$ we compute $\mathcal{F}$. More precisely, $H_3(x,y,z,a_{1,1},a_{1,2},a_{2,0},a_{2,1}) = -y^2z\, a_{1,1} - a_{1,2}\, y^2 z - y^2 z\, a_{2,0} - y^2 z\, a_{2,1} + a_{1,1}\, x\, y\, z + a_{1,2}\, x\, y^2 + a_{2,0}\, x^2 z + a_{2,1}\, x^2 y$.

To compute $\mathcal{F}_1$ (resp. $\mathcal{F}_2$), we take $\phi_1 = H_3(x,y,z,0,0,0,1) = -y^2z + x^2y$ and $\phi_2 = H_3(x,y,z,1,0,0,1) = -2\,y^2z + xyz + x^2y$. Following Sub-algorithm-II one gets:

$$\mathcal{F}_1 = \{(\alpha : \alpha^2 : 1) \mid \alpha^3 + 2\alpha + 1 = 0\}$$

$$\mathcal{F}_2 = \{(\alpha : \frac{1}{2} + \frac{1}{2}\alpha^2 : 1) \mid \alpha^3 + 3\alpha^2 + 5\alpha + 5 = 0\}.$$

Then, $\tilde{H}_4$ is computed by solving the linear system of equations derived from the constraints: $H_4(t,t^2,1) \bmod t^3+2t+1 = 0$ and $H_4(t, \frac{1}{2}+\frac{1}{2}t^2, 1) \bmod t^3+3t^2+5t+5 = 0$. Now, applying Sub-algorithm-II to $\tilde{H}_4$ we get the family of two conjugate points over $\mathbb{Q}$:

$$\mathcal{F} = \{(\alpha : -\frac{41}{26} - \frac{8}{39}\alpha : 1) \mid 8\alpha^2 - 7\alpha + 123 = 0\}.$$

Once $\mathcal{F}$ is computed, we determine the equation H' of the linear subsystem of dimension one of H_3 obtained by forcing the points in $\mathcal{F}$ to be base simple points on H_3; i.e. by solving the linear system of equations derived from the constraint: $H_3(t, -\frac{41}{26} - \frac{8}{39}t, 1) \bmod 8t^2 - 7t + 123 = 0$.

Finally, we compute the resultants of $f(x,y)$ and $H'(x,y,1)$, w.r.t. x and y respectively. Taking the primitive part of these resultants w.r.t the parameter, we get the following optimal real parametrization of $\mathcal{C}$:

$$\left(-\frac{-78\,t^2 + 55\,t^3 - 8 + 36\,t}{8t^3}, \frac{-78\,t^2 + 55\,t^3 - 8 + 36\,t}{2t\,(-12\,t + 17\,t^2 + 4)}\right).$$

7. Hybrid Real Parametrization Algorithm

Let Σ be a finite algebraic extension of $\mathbb{L}$, and let $\mathcal{P}(t)$ be a rational proper parametrization of an irreducible plane curve in the complex plane. In [ARS97] an algorithmic method, based on canonical divisors, is given for reparametrizing $\mathcal{P}(t)$ over an optimal field extension of $\mathbb{L}$. In addition, in [RS97a], if $\mathcal{P}(t)$ is complex, the reality of $\mathcal{C}$ is decided by computing a gcd of two real bivariate polynomonials, and if the curve is real, a linear parameter change is determined to transform the original parametrization into a real one.

Therefore, one may also consider the following alternative approach to the real parametrization problem, combining parametrization and reparametrization algorithms.

Algorithm HYBRID-REAL-PARAMETRIZATION(f)

- **Input:** $f \in \mathbb{F}[x, y]$ irreducible and defining a curve $\mathcal{C}$ of degree d.
- **Output:** the message "$\mathcal{C}$ `is not rational`" , or the message "$\mathcal{C}$ `is not real`", or a real rational parametrization of $\mathcal{C}$.

(1) Perform REALITY-TEST(f, 1). If the output is the message "$\mathcal{C}$ `is not real`", report "$\mathcal{C}$ `is not real`" and EXIT.

(2) Apply DIRECT-REAL-PARAMETRIZATION-II to f. If $\mathcal{C}$ is rational, let $\mathcal{P}(t)$ be the parametrization returned by DIRECT-REAL-PARAMETRIZATION-II; in general it will be defined over a high degree extension field of $\mathbb{F}$.

(3) Apply the reparatrization algorithm in [ARS97] to $\mathcal{P}(t)$ to get a new parametrization $\mathcal{Q}(t)$ over a extension field of degree two of $\mathbb{F}$.

(4) Apply the reparametrization algorithm in [RS97a] to $\mathcal{Q}(t)$ to get a new parametrization $\mathcal{R}(t)$ over a real extension field of degree two of $\mathbb{F}$.

(5) Apply the reparametrization algorithm in [ARS97] to $\mathcal{R}(t)$ to get a new parametrization $\mathcal{S}(t)$ over an optimal real extension field of $\mathbb{F}$. □

Acknowledgments

We thank Laureano Gonzalez–Vega for his comments and suggestions on the reality test analysis. The first author also wants to thank the traffic jams in Madrid, since they offer a daily opportunity for quiet thinking.

References

[AB88] Abhyankar S.S, Bajaj C.L., (1988), *Automatic Parametrization of Rational Curves and Surfaces III: Algebraic Plane Curves.* Computer Aided Geometric Design **5**, 309-321.

[ARS97] Andradas C., Recio T., Sendra J.R., (1997), *A relatively Optimal Rational Space Curves Reparametrization Algorithm through Canonical Divisors.* Proc. ISSAC97 pp. 349-356, ACM Press

[BK86] Brieskorn E., Knörrer H. (1986), *Plane Algebraic Curves.* Birkhäuser Verlag.

[Co75] Collins G., (1975), *Quantifier Elimination for Real Closed Fields by Cylindrical Algebraic Decomposition*, Volume 33 of the Second GI Conference on Automata Theory and Formal Languages, Lectures Notes on Computer Science pp. 134-183. Springer Verlag.

[CR88] Coste M., Roy M.F., (1988), *Thom's Lemma, the Coding of Real Algebraic Numbers and the Computation of the Topology of Semialgebraic Sets.* J. of Symbolic Computation, 5 (1-2), pp. 589-597.

[Fu89] Fulton W., (1989), *Algebraic Curves, An Introduction to Algebraic Geometry.* Addison-Wesley Publ. Co., Inc.

[HH90] Hilbert D., Hurwitz A. (1890), *Über die Diophantischen Gleichungen vom Geschlecht Null.* Acta math. **14**, 217-224.

[HW98] Hillgarter E., Winkler F. (1998), *Points on Algebraic Curves and the Parametrization Problem.* In: D. Wang (ed.), Automated Deduction in Geometry, 185–203, Lecture Notes in Artif. Intell. 1360, Springer Verlag Berlin Heidelberg.

[vH97] van Hoeij M. (1997), *Rational Parametrizations of Algebraic Curves using a Canonical Divisor.* J. Symbolic Computation **23/2&3**, 209–227.

[Jo98] Johnson J.R. (1998), *Algorithms for Real Root Isolation.* Quantifier Elimination and Cylindrical Algebraic Decomposition, Text and Monograhs in Symbolic Computation, pp. 269-289. Springer Verlag.

[IR82] Ireland K., Rosen R. (1982), *A Classical Introduction to Modern Number Theory.* Springer Verlag, Graduate Texts in Mathematics, New York.

[Mis93] Mishra B. (1993), *Algorithmic Algebra.* Springer Verlag.

[MW96] Mňuk M., Winkler F. (1996), *CASA — A System for Computer Aided Constructive Algebraic Geometry.* In: J. Calmet and C. Limongelli (eds.), Proc. Internat. Symp. on Design and Implementation of Symbolic Computation Systems (DISCO'96), 297–307, LNCS 1128, Springer Verlag Berlin Heidelberg New York.

[RS95] Recio T., Sendra J.R. (1995), *Reparametrización Real de Curvas Reales Paramétricas.* Proc. EACA'95, 159-168, Univ. de Cantabria, Santander, Spain.

[RS97a] Recio T., Sendra J.R. (1997), *Real Reparametrizations of Real Curves.* J. Symbolic Computation **23/2&3**, 241–254.

[RS97b] Recio T., Sendra J.R. (1997), *A Really Elementary Proof of Real Lüroth's Theorem.* Revista Matemática de la Universidad Complutense de Madrid **10**, 283–291.

[SW91] Sendra J.R., Winkler F. (1991), *Symbolic Parametrization of Curves.* J. Symbolic Computation **12/6**, 607-631.

[SW97] Sendra J.R., Winkler F. (1997), *Parametrization of Algebraic Curves over Optimal Field Extensions.* J. Symbolic Computation **23/2&3**, 191–207.

[SW98] Sendra J.R., Winkler F. (1998), *Real Parametrization of Algebraic Curves.* In: J. Calmet and J. Plaza (eds.), Artificial Intelligence and Symbolic Computation (Proc. AISC'98), 284–295, Lecture Notes in Artif. Intell. 1476, Springer Verlag Berlin Heidelberg.

[Wa50] Walker R.J. (1950), *Algebraic Curves.* Princeton Unversity Press.

[Wi96] Winkler F. (1996), *Polynomial Algorithms in Computer Algebra.* Springer-Verlag Wien New York.