J. Symbolic Computation (1997) **23**, 241–254

Real Reparametrizations of Real Curves

TOMAS RECIO† AND J. RAFAEL SENDRA‡

† *Departamento de Matemáticas, Universidad de Cantabria, E-39071 Santander, Spain*
‡ *Departamento de Matemáticas, Universidad de Alcalá, E-28871 Madrid, Spain*

(Received 8 January 1996)

In this paper we study the following two problems: first, given a rational parametrization $\mathcal{P}(z) = (p_1(z), p_2(z)) \in \mathbb{C}(z)^2$ of a complex curve $\mathcal{C}$ in $\mathbb{C}^2$, to determine algorithmically, if $\mathcal{C}$ has an infinite number of real points (i.e. if the trace of $\mathcal{C}$ in $\mathbb{R}^2$ is a real curve). If this is the case, then we would like to find another parametrization mapping of the same curve, but this time with real rational functions. The solution to both problems is given here by a simple algorithm, requiring essentially just a gcd computation and a parametrization of a real line or circle. On the other hand, the theoretical foundation for the algorithm seems more involved, relying on factorization properties of conjugate harmonic polynomials. The case of space curves or curves over a higher dimensional space follows by a direct generalization of our results or by considering the primitive element theorem.

1. Introduction

In this paper we study the following two problems: first, given a rational parametrization $\mathcal{P}(z) = (p_1(z), p_2(z)) \in \mathbb{C}(z)^2$ of a complex curve $\mathcal{C}$ in $\mathbb{C}^2$, to determine algorithmically, if $\mathcal{C}$ has an infinite number of real points (i.e. points in $\mathbb{R}^2$). If this is the case, then we would like to find another parametrization mapping of the same curve, but this time with real rational functions. The case of space curves or curves over a higher dimensional space follows by a direct generalization of our results or by considering the primitive element theorem.

From a purely mathematical point of view, the solution is simple: let us consider the imaginary parts $Im(p_1(x+i\,y)), Im(p_2(x+i\,y))$ of the given parametrization components. Then $\mathcal{C}$ has an infinite number of real points if and only if there is an infinite number of real points in common for the curves $Im(p_1(x+i\,y)) = 0, Im(p_2(x+i\,y)) = 0$, and therefore, according to Bezout's theorem, if and only if the numerators of $Im(p_1(x+i\,y))$ and $Im(p_2(x+i\,y))$ have a common factor which vanishes at an infinite number of real points. From the algorithmic point of view, this approach is not satisfactory for several

† E-mail: `recio@matsun1.unican.es`. Partially supported by PB 92/0498/C02/01: Geometría Real y Algorítmos.

‡ E-mail: `mtsendra@alcala.es`. Partially supported by Univ. Alcalá Proj. 030/95 and DGICYT PB 95/0563-A: Sistemas de ecuaciones algebraicas: resolución y aplicaciones.

0747–7171/97/020241 + 14 $25.00/0 sy960086

reasons: it is not so trivial to factorize over the reals a given two-variate polynomial; it is also non-trivial to determine which factors vanish over an infinite number of real points.

Again, from a non-algorithmic viewpoint, the solution to the second problem (reparametrizing with real coefficients) is quite straightforward: if $\mathcal{C}$ has an infinite number of real points, then its implicit equation can be taken with real coefficients and it yields a real curve (in the sense of having an infinite number of real points). Now, according to the real version of Luroth's theorem [see Recio and Sendra (1995)], a real curve that has a parametrization over $\mathbb{C}(z)^2$, has also a real parametrization. If the given parametrization is proper (also called faithful in the literature: i.e. a parametrization such that $\mathbb{C}(p_1(z), p_2(z)) = \mathbb{C}(z)$), then we know that any other desired parametrization can be obtained via a simple change of variables of the form $\frac{az+b}{cz+d}$ in the given one. We could then perform formally such substitution depending on the complex coefficients a, b, c, d as parameters, on the given rational functions, and then we could search for complex values of a, b, c, d such that the resulting expression is a real parametrization. But this implies solving a non-linear system of equations and it is not feasible in practice. The case of non-proper parametrizations can be reduced to this one by finding the greatest common component of $\{p_1(z), p_2(z)\}$ [see Alonso *et al.* (1995a); Sederberg (1986)]. There is another possibility (in theory): to obtain, first, the implicit equation of the curve $\mathcal{C}$ (using implicitization algorithms, rather costly); to check, then, if it has an infinite number of real points and to re-start a suitable parametrization process [such as in Sendra and Winkler (1997)] that outputs a real parametrization mapping when the given curve is real. But this procedure has, again, high time complexity.

As a counterpoint, the algorithms presented in this paper are very simple, involving essentially trivial operations such as finding a greatest common factor of two bivariate real polynomials and deciding if this gcd is non-constant and of degree less than two. Otherwise we will show the curve is non-real. In the affirmative case the curve must be real and the reparametrization mapping will be obtained just by composing the given parametrization with any real parametrization of the line or circle defined by the vanishing of the gcd. After the idea is explained, one is tempted to think that the proof must be quite obvious. In fact, it is so from a geometric point of view. If the curve given by the parametrization $\mathcal{P}(z) = (p_1(z), p_2(z))$ is real, it is quite easy to show that the zeroes of the gcd of the imaginary parts $Im(p_1(x+i\,y))$, $Im(p_2(x+i\,y))$ must be a real line or circle, since the image of a real line by a conformal mapping is a line or a circle. The problem is that, from an algebraic point of view (hence from an algorithmic point of view), the equation of the line or of the circle could be just one factor among many others of the gcd, these ones having no real zeroes. Therefore one should, in principle, have got to factor the gcd in order to check if the curve is real or not. But a finer algebraic analysis of the situation implies that this step can be always avoided and the elimination of such factorization requirement is an important goal of this paper.

The tools we use to guarantee that the algebraic behaviour of this gcd agrees with the geometric expectative are some basic, but apparently new, properties of analytic polynomials (ie. conjugate harmonic polynomial functions) and analytic rational functions, concerning real factors (see Section 2). The main result is that the gcd of conjugate harmonic polynomials is always 1 (see Lemma 2.1). This Section 2 could be thought of independent interest, as harmonic functions appear in many different mathematical contexts. For instance, from an algorithmic point of view, Section 2 establishes some simplification properties for various standard manipulations with rational functions of complex variables, such as the irreducibilty of the real and imaginary parts of an irre-

ducible rational function (see Lemma 2.2). Section 3 is devoted to prove the main result, the criterion for reality of a curve given by a complex parametrization mapping (see Theorem 3.1) and the real reparametrization procedure (see Theorem 3.2). Section 4 ends with the description of algorithms, a few computed examples of their performance, and the computing time analysis that shows that the complexity of our algorithm is low degree polynomial.

The interest of the problems we deal with in this paper is twofold. It is clear that the analysis of the conversion of geometric objects from implicit to parametric representation and viceversa is an important aspect of Computer Aided Geometric Design [see Hoffmann (1989); Buchberger (1987); Sederberg (1987)]. On the other hand, with few exceptions [see Sendra and Winkler (1997); Bajaj and Royappa (1993); Alonso *et al.* (1995b)], algebraic algorithms for dealing with these problems are usually done assuming an algebraically closed field (such as the complex number field) as framework, since real algebraic geometry is less comfortable to work with. But since the objects of interest in CAGD are, most commonly, subsets of the real plane or space, some analysis of the reality of the output of such algorithms is finally required. On a second motivation, we can say that this paper is just a step towards the more general (and difficult) goal of obtaining optimal parametrizations of given curves, that is, parametrizations with "best" coefficients and degrees. Here in our work, by "best" we have understood, when the given curve has one real parametrization but a complex one is given as input data (coming, maybe, from a conversion algorithm from an implicit equation), the parametrization that has coefficients belonging to the real field as opposed to one with complex coefficients.

2. Analytic Rational Functions

Analytic rational functions are bivariate rational functions with complex coefficients that are generated by univariate complex rational functions when the complex variable is formally replaced by its expansion as a real plus a purely imaginary variable.

DEFINITION 2.1. A polynomial $p(x,y) \in \mathbb{C}[x,y]$ is called *analytic* if there exists a polynomial $f(z) \in \mathbb{C}[z]$ such that $f(x+i\,y) = p(x,y)$. Similarly, a rational function $r(x,y) \in \mathbb{C}(x,y)$ is called *analytic* if there exist a rational function $h(z) \in \mathbb{C}(z)$ such that $h(x+i\,y) = r(x,y)$.

Equivalent definitions and basic properties of analytic polynomials can be found in complex analysis textbooks in the context of harmonic functions [e.g., Bak and Newman (1982)]; for instance, it can be proved that $p \in \mathbb{C}[x,y]$ is analytic if and only if $\frac{\partial p}{\partial y} = i\,\frac{\partial p}{\partial x}$; if and only if $\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y}$ and $\frac{\partial u}{\partial y} = -\frac{\partial v}{\partial x}$ (where $u(x,y)$ and $v(x,y)$ are the real and imaginary parts of $p(x,y)$); if and only if $p(x,y) = p(x+i\,y,0)$; if and only if $p(x,y) = p(0,-i\,x+y)$.

For our purposes, we are mainly interested in the real and imaginary parts of analytic polynomials. These polynomials are very special. For instance, the number of real intersections, counted with multiplicity, of the complex plane curves that they define, is always the degree of the complex univariate polynomial that generates the analytic polynomial. We start with the following lemma, stating that analytic polynomials do not have real factors.

LEMMA 2.1. *Let $p(x,y)$ be a non-constant analytic polynomial, and $u(x,y), v(x,y)$ the real and imaginary part of $p(x,y)$. Then it holds that* $\gcd(u,v) = 1$

PROOF. $f(z) \in \mathbb{C}[z]$ such that $p(x,y) = f(x+iy)$. We consider $g(z) \in \mathbb{C}[z]$ monic, and $\lambda \in \mathbb{C}$ such that $f(z) = \lambda g(z)$, and let $u'(x,y)$ and $v'(x,y)$ be the real and imaginary parts of $g(x+iy)$. Then, if $\lambda = \lambda_1 + i\lambda_2$, with $\lambda_1, \lambda_2 \in \mathbb{R}$, one has that $u = \lambda_1 u' - \lambda_2 v'$, $v = \lambda_2 u' + \lambda_1 v'$; and since $\lambda \neq 0$, one also has that $u' = \frac{\lambda_1}{|\lambda|^2}u + \frac{\lambda_2}{|\lambda|^2}v$, $v' = -\frac{\lambda_2}{|\lambda|^2}u + \frac{\lambda_1}{|\lambda|^2}v$. Thus $\gcd(u,v) = \gcd(u',v')$. Now since g is not constant, g can be expressed as:

$$g(z) = \prod_{j=1}^{j=n}(z - \xi_j)$$

where n is the degree of $g(z)$ and $\{\xi_1, \ldots, \xi_n\}$ are its roots. Hence, if $\xi_j = \xi_j^1 + i\,\xi_j^2$, with $\xi_j^1, \xi_j^2 \in \mathbb{R}$, one has that:

$$g(x+iy) = u'(x,y) + i\,v'(x,y) = \prod_{j=1}^{j=n}((x - \xi_j^1) + i\,(y - \xi_j^2))$$

Let $q(x,y) = \gcd(u'(x,y), v'(x,y))$ and let us suppose that $q(x,y) \neq 1$. As q divides $g(x+iy)$, there exist $s \neq 0$ and $k_1, \ldots, k_s \in \{1, \ldots, n\}$ such that $q = \prod_{j=1}^{s}((x - \xi_{k_j}^1) + i\,(y - \xi_{k_j}^2))$. But this implies that $q(x,y) \notin \mathbb{R}[x,y]$ (consider $q = \bar{q}$ and use the unique factorization property over $\mathbb{C}[x,y]$), which is impossible since the gcd of real polynomials is always real. Therefore, one concludes that q is constant. □

The next lemma analyses analytic rational functions. If one normalizes a rational function (i.e. transforming it into a rational function with real denominator) such that the new denominator is the square of the norm of the initial complex denominator, then it is clear that the new numerator is not analytic anymore; hence Lemma 2.1 cannot be applied to study its real factors. However, it can be shown that the real factors of the numerator are directly related to the gcd of the univariate complex polynomials that define the analytic rational function. More precisely:

LEMMA 2.2. *Let $f, g \in \mathbb{C}[z]$ be non-constant polynomials, $h(z) = \gcd(f,g)$, and $f_1, f_2 \in \mathbb{R}[x,y]$, $g_1, g_2 \in \mathbb{R}[x,y]$, and $h_1, h_2 \in \mathbb{R}[x,y]$ be the real and imaginary parts of $f(x+iy)$,$g(x+iy)$, and $h(x+iy)$, respectively. Then, if*

$$\frac{f(x+iy)}{g(x+iy)} = \frac{(f_1(x,y) + i\,f_2(x,y))(g_1(x,y) - i\,g_2(x,y))}{g_1(x,y)^2 + g_2(x,y)^2} = \frac{u(x,y) + i\,v(x,y)}{g_1(x,y)^2 + g_2(x,y)^2}$$

where u, v are the real and imaginary parts of $f(x+iy) \cdot \bar{g}(x-iy)$, it holds that:

(1) $\gcd(u,v)$ *and* $h_1^2 + h_2^2$ *are associated (i.e. equal except for a real constant).*
(2) $\gcd(u, v, g_1^2 + g_2^2)$ *and* $h_1^2 + h_2^2$ *are associated.*
(3) $\gcd(u, g_1^2 + g_2^2)$ *and* $h_1^2 + h_2^2$ *are associated.*
(4) $\gcd(v, g_1^2 + g_2^2)$ *and* $h_1^2 + h_2^2$ *are associated.*

PROOF. (1) We first observe that one can assume that f and g are monic: Let $f(z) = \lambda f^\star(z)$ and $g(z) = \mu g^\star(z)$, where $\lambda, \mu \in \mathbb{C}$ and $f^\star, g^\star \in \mathbb{C}[z]$, and let $u^\star, v^\star$ be the real and imaginary part of $f^\star(x+iy)\bar{g}^\star(x-iy)$. Then, if $\alpha = \lambda\bar{\mu} = \alpha_1 + i\,\alpha_2$, with $\alpha_1, \alpha_2 \in \mathbb{R}$, it holds that $u = \alpha_1 u^\star - \alpha_2 v^\star$, $v = \alpha_2 u^\star + \alpha_1 v^\star$, and $u^\star = \frac{\alpha_1}{\alpha\bar{\alpha}}u + \frac{\alpha_2}{\alpha\bar{\alpha}}v$, $v^\star = -\frac{\alpha_2}{\alpha\bar{\alpha}}u + \frac{\alpha_1}{\alpha\bar{\alpha}}v$. Therefore, $\gcd(u,v) = \gcd(u^\star, v^\star)$.

Let then $f(z), g(z)$ be monic. We factor them as:

$$f(z) = \prod_{j=1}^{j=n} (z - \xi_j), \qquad g(z) = \prod_{j=1}^{j=m} (z - \eta_j),$$

and let $q(x,y) = \gcd(u,v) \in \mathbb{R}[x,y]$. Then, since $q(x,y)$ divides $f(x+iy)\bar{g}(x-iy)$, there exist $k_1, \ldots, k_s \in \{1, \ldots, n\}$ and $t_1, \ldots, t_r \in \{1, \ldots, m\}$ such that:

$$q_1(x,y) = \prod_{j=1}^{j=s} ((x - \xi_{k_j}^1) + i\,(y - \xi_{k_j}^2)), \qquad q_2(x,y) = \prod_{j=1}^{j=r} ((x - \eta_{t_j}^1) - i\,(y - \eta_{t_j}^2))$$

and $q = q_1 q_2$, where $\xi_j = \xi_j^1 + i\xi_j^2$, $\eta_j = \eta_j^1 + i\eta_j^2$, with $\xi_j^1, \xi_j^2, \eta_j^1, \eta_j^2 \in \mathbb{R}$. Then, taking into account that $q = q_1\, q_2$ is real one deduces that for every k_j there exists $t_{j'}$ such that $\xi_{k_j} = \eta_{t_{j'}}$. Hence, $\bar{q}_1(x,y) = q_2(x,y)$. Then, $q_1(x,y)$ divides $f(x+iy)$ and $g(x+iy)$, and therefore q_1 divides $h(x+iy)$. Thus, one concludes that $q = q_1\, q_2$ divides $h(x+iy)\,\bar{h}(x-iy) = h_1^2 + h_2^2$.

On the other hand, let $f', g' \in \mathbb{C}[z]$ such that $f = h\,f'$ and $g = h\,g'$. Thus, $u + iv = (h_1^2 + h_2^2) f'(x+iy)\bar{g}'(x-iy)$, and taking into account that $h_1^2 + h_2^2$ is real one deduces that $h_1^2 + h_2^2$ divides $\gcd(u,v)$.

(2) Let $q = \gcd(u, v, g_1^2 + g_2^2)$. Then q divides $h_1^2 + h_2^2 = \gcd(u,v)$. On the other hand, by (1), $h_1^2 + h_2^2$ divides u, v, and since h divides g one also has that $h_1^2 + h_2^2$ divides $g_1^2 + g_2^2$.

(3) From (2) it follows that $h_1^2 + h_2^2$ divides u and $g_1^2 + g_2^2$. In order to see that $q(x,y) = \gcd(u, g_1^2 + g_2^2)$ divides $h_1^2 + h_2^2$, we first observe that after (2), one simply has to prove that $q(x,y)$ also divides v. Let $g(z)$ factor as:

$$g(z) = \prod_{j=1}^{j=m} (z - \eta_j),$$

and let $\eta_j = \eta_j^1 + i\,\eta_j^2$, with $\eta_j^1, \eta_j^2 \in \mathbb{R}$. Then, since $q \in \mathbb{R}[x,y]$ is a divisor of

$$g_1^2 + g_2^2 = g(x+iy)\bar{g}(x-iy) = \prod_{j=1}^{m} ((x - \eta_j^1)^2 + (y - \eta_j^2)^2)$$

there exist $k_1, \ldots, k_s \in \{1, \ldots, m\}$ such that

$$q(x,y) = \prod_{j=1}^{s} ((x - \eta_{k_j}^1)^2 + (y - \eta_{k_j}^2)^2).$$

Let $\Delta_{k_j} = (x - \eta_{k_j}^1) + i\,(y - \eta_{k_j}^2)$. Then, for $j = 1, \ldots, s$ it holds that $\bar{\Delta}_{k_j}$ divides u, and since $\bar{\Delta}_{k_j}$ divides $\bar{g}(x - iy)$ it follows that $\bar{\Delta}_{k_j}$ also divides $u + iv = f(x+iy)\bar{g}(x-iy)$. Therefore, $\bar{\Delta}_{k_j}$ divides v for $j = 1, \ldots, s$. Hence, since $v \in \mathbb{R}[x,y]$, one also deduces that Δ_{k_j} divides v for $j = 1, \ldots, s$. Therefore, $q = \prod_{j=1}^{s} \bar{\Delta}_{k_j} \Delta_{k_j}$ divides $v(x,y)$.

Analogously, one proves (4). □

COROLLARY 2.1. *Let $f, g, h \in \mathbb{C}[z]$ be non-constant polynomials such that $\gcd(f,g,h) = 1$, and let $f_1, f_2 \in \mathbb{R}[x,y]$, $g_1, g_2 \in \mathbb{R}[x,y]$, and $h_1, h_2 \in \mathbb{R}[x,y]$ be the real and imaginary*

parts of $f(x+i\,y)$, $g(x+i\,y)$, *and* $h(x+i\,y)$, *respectively. Then, if*

$$\frac{f(x+i\,y)}{h(x+i\,y)} = \frac{u_1(x,y)+i\,v_1(x,y)}{h_1(x,y)^2+h_2(x,y)^2}, \qquad \frac{g(x+i\,y)}{h(x+i\,y)} = \frac{u_2(x,y)+i\,v_2(x,y)}{h_1(x,y)^2+h_2(x,y)^2}$$

where u_1, v_1 *and* u_2, v_2 *are the real and imaginary parts of* $f(x+i\,y)\cdot\bar{h}(x-i\,y)$ *and* $g(x+i\,y)\cdot\bar{h}(x-i\,y)$, *respectively, it holds that* $\gcd(v_1, v_2, h_1^2+h_2^2) = 1$.

PROOF. Let $p = \gcd(f,h)$, $q = \gcd(g,h)$ and $A = \gcd(v_1, v_2, h_1^2+h_2^2)$. Then $A = \gcd(\gcd(v_1, h_1^2+h_2^2), \gcd(v_2, h_1^2+h_2^2))$. Thus, if $p_1(x,y), p_2(x,y)$ and $q_1(x,y), q_2(x,y)$ are the real and imaginary parts of $p(x+i\,y)$ and $q(x+i\,y)$, respectively, applying Lemma 2.2, one deduces that $A = \gcd(p_1^2+p_2^2, q_1^2+q_2^2)$.

Let now $B \in \mathbb{R}[x,y]$ be a non-trivial common factor of $p_1^2+p_2^2$ and $q_1^2+q_2^2$, and let $p(z) = \prod_{j=1}^{j=n}(z-\xi_j), q(z) = \prod_{j=1}^{m}(z-\eta_j)$. Then, there exist $k_1,\ldots,k_s \in \{1,\ldots,n\}$ and $t_1,\ldots,t_s \in \{1,\ldots,m\}$ such that

$$B(x,y) = \prod_{j=1}^{j=s}((x-\xi_{k_j}^1)^2+(y-\xi_{k_j}^2)^2) = \prod_{j=1}^{j=r}((x-\eta_{t_j}^1)^2+(y-\eta_{t_j}^2)^2)$$

where $\xi_j = \xi_j^1 + i\,\xi_j^2, \eta_j = \eta_j^1 + i\,\eta_j^2$ and $\xi_j^1, \xi_j^2, \eta_j^1, \eta_j^2 \in \mathbb{R}$. Therefore, for every k_j there exists $t_{j'}$ such that $\xi_{k_j} = \eta_{t_{j'}}$. This implies that $\gcd(p,q) \neq 1$, which is impossible since $\gcd(p,q) = \gcd(f,g,h) = 1$. □

Linear invertible rational functions play an important role in the parametrization of curves. For the particular case of these rational functions, Lemma 2.2 can be sharpened as follows

LEMMA 2.3. *Let* $f(z) = a\,z+b, g(z) = c\,z+d \in \mathbb{C}[z]$ *such that* $\frac{f(z)}{g(z)}$ *is invertible (i.e.* $ad-bc \neq 0$*), and let* $f_1, f_2 \in \mathbb{R}[x,y]$ *and* $g_1, g_2 \in \mathbb{R}[x,y]$ *be the real and imaginary parts of* $f(x+i\,y)$ *and* $g(x+i\,y)$, *respectively. Then, if*

$$\frac{f(x+i\,y)}{g(x+i\,y)} = \frac{u(x,y)+i\,v(x,y)}{g_1(x,y)^2+g_2(x,y)^2}$$

where u, v *are the real and imaginary parts of* $f(x+i\,y)\cdot\bar{g}(x-i\,y)$, *it holds that* $g_1^2+g_2^2$ *is a constant or irreducible in* $\mathbb{R}[x,y]$, *and* u, v *are constants or irreducible in* $\mathbb{C}[x,y]$. *Moreover, if* u *or* v *are not constants, then they are either real lines or real circles.*

PROOF. Let $a = a_1+i\,a_2$, $b = b_1+i\,b_2$, $c = c_1+i\,c_2$, and $d = d_1+i\,d_2$, with $a_j, b_j, c_j, d_j \in \mathbb{R}$, and let

$$\begin{aligned} A_1 &= a_2\,c_2 + a_1\,c_1 & B_1 &= c_1a_2 - c_2a_1 \\ A_2 &= a_2\,d_2 + b_2\,c_2 + a_1\,d_1 + b_1\,c_1 & B_2 &= a_2d_1 + b_2c_1 - a_1d_2 - b_1c_2 \\ A_3 &= b_2\,c_1 + a_1\,d_2 - a_2\,d_1 - b_1\,c_2 & B_3 &= a_1d_1 + a_2d_2 - b_1c_1 - b_2c_2 \\ A_4 &= b_2\,d_2 + b_1\,d_1 & B_4 &= d_1b_2 - d_2b_1. \end{aligned}$$

Then, after some computations one shows that:

$$\begin{aligned} u(x,y) &= A_1\,(x^2+y^2) + A_2x + A_3y + A_4 \\ v(x,y) &= B_1\,(x^2+y^2) + B_2x + B_3y + B_4 \\ g_1^2+g_2^2 &= (c_1x - c_2y + d_1)^2 + (c_2x + c_1y + d_2)^2. \end{aligned}$$

Let us suppose that $g_1^2 + g_2^2$ is not a constant. Then, neither g_1 nor g_2 are constants. Now, $g_1^2 + g_2^2$ factors over $\mathbb{C}[x, y]$ as $(g_1 + ig_2)(g_1 - ig_2)$, and each factor, being of degree one, is irreducible. It follows that if $g_1^2 + g_2^2$ factors in $\mathbb{R}[x, y]$, it must have two factors, one associated with $g_1 + i\,g_2$, the other with $g_1 - i\,g_2$. But $g_1 + i\,g_2$ does not have, by Lemma 2.1, real factors. Then, $g_1^2 + g_2^2$ is irreducible over the reals.

In order to analyse the polynomial u, we distinguish two cases. If $A_1 = 0$ then u is a real line and therefore irreducible over $\mathbb{C}$, or a constant. Let $A_1 \neq 0$, then we express u as sum of squares as follows:

$$u = A_1\left(x + \frac{A_2}{2A_1}\right)^2 + A_1\left(y + \frac{A_3}{2A_1}\right)^2 + \frac{4A_4A_1 - A_2^2 - A_3^2}{4A_1}.$$

Moreover, since $4A_4A_1 - A_2^2 - A_4^2 = -A^2 - B^2$, one deduces that u can also be written as:

$$u = A_1\left(x + \frac{A_2}{2A_1}\right)^2 + A_1\left(y + \frac{A_3}{2A_1}\right)^2 - \frac{A^2 + B^2}{4A_1}$$

where $A = a_2\,d_2 - b_2\,c_2 + b_1\,c_1 - a_1\,d_1$, and $B = b_2\,c_1 - a_1\,d_2 + b_1\,c_2 - a_2\,d_1$. In this situation it is clear that u is irreducible over $\mathbb{C}$ if and only if $A^2 + B^2 \neq 0$. Thus, taking into account that $ad - bc = 1$ (since we have by hypothesis that $ad - bc \neq 0$, one can always assume that the value of this determinant is 1), the irreducibility of u over $\mathbb{C}$ for any values of a, b, c, d verifying this relation can be deduced by computing the Gröbner basis of the ideal generated by the involved equations:

$$\begin{aligned}(a_2\,d_2 - b_2\,c_2 + b_1\,c_1 - a_1\,d_1)^2 + (b_2\,c_1 - a_1\,d_2 + b_1\,c_2 - a_2\,d_1)^2 &= 0\\ a_1\,d_1 - b_1\,c_1 - a_2\,d_2 + b_2\,c_2 - b_2\,c_1 + a_1\,d_2 + a_2\,d_1 - b_1\,c_2 &= 1\\ a_1\,d_2 + a_2\,d_1 - b_1\,c_2 - b_2\,c_1 &= 0,\end{aligned}$$

where the last two ones express the condition $ad - bc = 1$. Performing such computation with a symbolic computation package, it turns that the basis is $\{1\}$. Thus there is no solution for this system of equations and, therefore, it always holds that $A^2 + B^2 \neq 0$. Furthermore, the signature of the quadratic form defined by u is either two (if $A_1 > 0$) or one (if $A_1 < 0$). In any case, the conic is the real circle of radius $\frac{\sqrt{A^2+B^2}}{2A_1}$ centered at $(-\frac{A_2}{2A_1}, -\frac{A_3}{2A_1})$.

Similarly, if $B_1 = 0$, then v defines a real line or a constant. Let $B_1 \neq 0$, then we express v as sum of squares as follows:

$$\begin{aligned}v &= B_1\left(x + \frac{B_2}{2B_1}\right)^2 + B_1\left(y + \frac{B_3}{2B_1}\right)^2 + \frac{4B_4B_1 - B_2^2 - B_3^2}{4B_1}\\ &= B_1\left(x + \frac{B_2}{2B_1}\right)^2 + B_1\left(y + \frac{B_3}{2B_1}\right)^2 - \frac{A^2 + B^2}{4B_1}\end{aligned}$$

where A and B are as above. In this situation, a similar reasoning concludes that v is the real circle of radius $\frac{\sqrt{A^2+B^2}}{2B_1}$ centered at $(-\frac{B_2}{2B_1}, -\frac{B_3}{2B_1})$. □

3. Real Reparametrization of Real Curves

In this section we present our main result (Theorem 3.1) that gives a necessary and sufficient condition, easy to test algorithmically, on the existence of real simple points on a complex rational plane curve. By the real Lüroth's theorem [see Recio and Sendra

(1995); Chevalley (1951)], this is equivalent to the existence of a rational parametrization over the reals for the given curve. We assume that the input data is a complex rational curve, properly parametrized by $p_1(z) = \frac{f(z)}{h(z)}$, $p_2(z) = \frac{g(z)}{h(z)} \in \mathbb{C}[z]$, both non-constants and such that $\gcd(f, g, h) = 1$. Let us remark that it is quite easy to get to convert any given parametrization into one having these properties (see the introduction); the case of some constant component is trivial to handle directly. The theoretical basis for a reparametrizing algorithm is given in Theorem 3.2: it is a simple consequence of the condition given in Theorem 3.1.

Our main result states that this curve is real if and only if the imaginary parts of the two analytic rational functions $p_1(z), p_2(z)$, the coordinate functions in the parametrization mapping, intersect exactly in one real line or one real circle. More precisely, one has the following theorem.

THEOREM 3.1. *Let* $p_1(z) = \frac{f(z)}{h(z)}, p_2(z) = \frac{g(z)}{h(z)} \in \mathbb{C}[z]$, *both non-constants, such that* $\gcd(f, g, h) = 1$ *and* $\mathbb{C}(p_1(z), p_2(z)) = \mathbb{C}(z)$, *and let*

$$p_1(x + i\,y) = \frac{u_1(x, y) + i\,v_1(x, y)}{h_1(x, y)^2 + h_2(x, y)^2}, \qquad p_2(x + i\,y) = \frac{u_2(x, y) + i\,v_2(x, y)}{h_1(x, y)^2 + h_2(x, y)^2}$$

where $h_1, h_2 \in \mathbb{R}[x, y]$, $u_1, v_1 \in \mathbb{R}[x, y]$ *and* $u_2, v_2 \in \mathbb{R}[x, y]$ *are the real and imaginary parts of* $h(x + i\,y)$, $f(x + i\,y) \cdot \bar{h}(x - i\,y)$ *and* $g(x + i\,y) \cdot \bar{h}(x - i\,y)$, *respectively. Then, the plane curve* $\mathcal{C}$ *that* $(p_1(z), p_2(z))$ *defines over* $\mathbb{C}$, *i.e.* $\mathcal{C} = \{(p_1(z), p_2(z)) \in \mathbb{C}^2 \,/\, z \in \mathbb{C}\}$, *has infinitely many real points if and only if* $\gcd(v_1, v_2)$ *is either a real line or a real circle.*

PROOF. Let $\gcd(v_1, v_2)$ be a real line or a real circle. From Corollary 2.1, one has that $\gcd(v_1, v_2, h_1^2 + h_2^2) = 1$. Thus, there exists an infinite set $\mathcal{M} \subset \mathbb{R}^2$ such that for every $(x, y) \in \mathcal{M}$ it holds that $v_1(x, y) = v_2(x, y) = 0$, and $h_1(x, y)^2 + h_2(x, y)^2 \neq 0$. Furthermore, $\mathcal{N} = \{(p_1(x+i\,y), p_2(x+i\,y))/(x, y) \in \mathcal{M}\} \subset \mathcal{C} \cap \mathbb{R}^2$ and $\text{cardinal}(\mathcal{N}) = \infty$; indeed, since (p_1, p_2) is proper, it is injective over $\mathcal{M}$.

Conversely, let $\text{cardinal}(\mathcal{C} \cap \mathbb{R}^2) = \infty$, and let $F(x, y) = F_1(x, y) + i\,F_2(x, y) \in \mathbb{C}[x, y]$, with $F_1, F_2 \in \mathbb{R}[x, y]$, be the primitive irreducible polynomial that defines $\mathcal{C}$. Then, there exist infinitely many $(x, y) \in \mathbb{R}^2$ such that $F_1(x, y) = F_2(x, y) = 0$. Therefore, since $\gcd(F_1, F_2) = 1$, it follows that either $F_1 = 0$ or $F_2 = 0$. This implies that F is associated with a real polynomial, and hence we can assume that F is real. Now, since $F \in \mathbb{R}[x, y]$, and $\text{cardinal}(\mathcal{C} \cap \mathbb{R}^2) = \infty$, applying real Lüroth's theorem, one deduces that $\mathcal{C}$ can be parametrized over $\mathbb{R}$. Let $(q_1(z), q_2(z))$ be a real proper rational parametrization of $\mathcal{C}$. Then, there exists an invertible rational function $\varphi(z) = \frac{a\,z+b}{c\,z+b} \in \mathbb{C}(z)$, $a, b, c, d \in \mathbb{C}$, such that $(p_1(z), p_2(z)) = (q_1(\varphi(z)), q_2(\varphi(z)))$. Also, let $M(x, y) = \frac{M_1(x,y)}{M_2(x,y)} \in \mathbb{R}(x, y)$ be a rational inversion of (q_1, q_2); i.e. $M(q_1(z), q_2(z)) = z$ (note, that since by assumption $\mathbb{R}(q_1, q_2) = \mathbb{R}(z)$, we can take $M(x, y) \in \mathbb{R}(x, y)$). Therefore, $M(p_1(z), p_2(z)) = \varphi(z)$.

In this situation, we consider the homogenization of the polynomials $M_1, M_2 \in \mathbb{R}[x, y]$. That is, $M_1^h(x, y, z) = z^{\alpha_1} M_1(\frac{x}{z}, \frac{y}{z})$, and $M_2^h(x, y, z) = z^{\alpha_2} M_2(\frac{x}{z}, \frac{y}{z})$, where $\alpha_1 = \deg(M_1)$ and $\alpha_2 = \deg(M_2)$. Then, one has that:

$$M_j(p_1(x + i\,y), p_2(x + i\,y)) = \frac{M_j^h(f(x + i\,y), g(x + i\,y), h(x + i\,y))}{h(x + i\,y)^{\alpha_j}}$$

$$= \frac{M_j^h(f(x+iy), g(x+iy), h(x+iy)) \cdot \bar{h}(x-iy)^{\alpha_j}}{(h_1^2+h_2^2)^{\alpha_j}}$$

$$= \frac{M_j^h(f(x+iy)\bar{h}(x-iy), g(x+iy)\bar{h}(x-iy), h(x+iy)\bar{h}(x-iy))}{(h_1^2+h_2^2)^{\alpha_j}}$$

$$= \frac{M_j^h(u_1+iv_1, u_2+iv_2, h_1^2+h_2^2)}{(h_1^2+h_2^2)^{\alpha_j}} = \frac{A_j(x,y)+iB_j(x,y)}{(h_1^2+h_2^2)^{\alpha_j}}$$

where $A_j, B_j \in \mathbb{R}[x,y]$ are the real and imaginary parts of $M_j^h(u_1+iv_1, u_2+iv_2, h_1^2+h_2^2)$. Therefore,

$$M(p_1(x+iy), p_2(x+iy)) = \frac{A_1(x,y)+iB_1(x,y)}{A_2(x,y)+iB_2(x,y)} \cdot (h_1^2+h_2^2)^{\alpha_2-\alpha_1} = \varphi(x+iy).$$

Thus, applying Lemma 2.3, one has that

$$\frac{A_1(x,y)+iB_1(x,y)}{A_2(x,y)+iB_2(x,y)} \cdot (h_1^2+h_2^2)^{\alpha_2} = \frac{u(x,y)+iv(x,y)}{w(x,y)} \cdot (h_1^2+h_2^2)^{\alpha_1}$$

where $w \in \mathbb{R}[x,y]$ is irreducible, and u, v define either real lines or real circles. Normalizing the left-hand side of the equality one obtains:

$$w \cdot (h_1^2+h_2^2)^{\alpha_2} \cdot (A_1A_2 + B_1B_2 + i(A_2B_1 - A_1B_2)) = (A_2^2+B_2^2) \cdot (h_1^2+h_2^2)^{\alpha_1} \cdot (u+iv)$$

and taking the imaginary parts one deduces that

$$w \cdot (h_1^2+h_2^2)^{\alpha_2} \cdot (A_2B_1 - A_1B_2) = (A_2^2+B_2^2) \cdot (h_1^2+h_2^2)^{\alpha_1} \cdot v.$$

Now, let $G = \gcd(v_1, v_2)$. Then $G \neq 0$, since $v_1, v_2 \neq 0$. In fact it is easy to prove that the imaginary part of a non-constant analytic polynomial cannot be zero, using Cauchy-Riemann conditions. Assume $p_1 = \frac{f(z)}{h(z)}$ is not constant. Then v_1 is not zero, since, if $f = f_1 + if_2, h = h_1 + ih_2$, then $0 = v_1 = f_2h_1 - h_2f_1$ implies, by Lemma 2.1, that every real factor of f_2 divides h_2 and conversely; and the same applies to f_1 and h_1; thus f and h are associated and p_1 is a constant. Furthermore we observe that G is not a non-zero constant since cardinal$(\mathcal{C} \cap \mathbb{R}^2) = \infty$. We have to prove that G is either a real line or a real circle. We first note that, since $M_j^h(x,y,z) \in \mathbb{R}[x,y,z]$, and since G divides v_1, v_2, one has that G divides B_1, B_2. Thus, G divides $(A_2^2+B_2^2) \cdot (h_1^2+h_2^2)^{\alpha_1} \cdot v$. On the other hand, taking into account Corollary 2.1, one knows that $\gcd(v_1, v_2, h_1^2+h_2^2) = 1$. Hence G divides $(A_2^2+B_2^2) \cdot v$. Let us see that $\gcd(G, A_2^2+B_2^2) = 1$. If so, since v is irreducible, then G and v are associated, and therefore, G defines either a real line or a real circle. Let H be an irreducible real common factor of G and $A_2^2+B_2^2$. Then, since H divides B_2, it follows that H divides also A_2. Therefore, since

$$\frac{M_2^h(f(x+iy), g(x+iy), h(x+iy))}{h(x+iy)^{\alpha_2}} = \frac{A_2(x,y)+iB_2(x,y)}{(h_1^2+h_2^2)^{\alpha_2}},$$

applying Lemma 2.2, one deduces that H divides C^2+D^2, where $C, D \in \mathbb{R}[x,y]$ are the real and imaginary part of $N(x+iy)$ and $N(z) = \gcd(M_2^h(f(z), g(z), h(z)), h(z)^{\alpha_2})$. Moreover, since $N \cdot \bar{N}$ divides $h^{\alpha_2} \cdot \bar{h}^{\alpha_2}$, one has that H divides $(h_1^2+h_2^2)^{\alpha_2}$. However, since H is irreducible, one deduces that H divides $(h_1^2+h_2^2)$. Therefore H divides $\gcd(v_1, v_2, h_1^2+h_2^2)$. Thus, by Corollary 2.1, one concludes that $H = 1$. □

The next theorem shows how to reparametrize, over $\mathbb{R}$, real curves given by complex rational parametrizations.

THEOREM 3.2. *Let* $p_1(z) = \frac{f(z)}{h(z)}$, $p_2(z) = \frac{g(z)}{h(z)} \in \mathbb{C}[z]$, *both non-constants, such that* $\gcd(f, g, h) = 1$ *and* $\mathbb{C}(p_1(z), p_2(z)) = \mathbb{C}(z)$, *and let*

$$p_1(x + i\,y) = \frac{u_1(x, y) + i\,v_1(x, y)}{h_1(x, y)^2 + h_2(x, y)^2}, \qquad p_2(x + i\,y) = \frac{u_2(x, y) + i\,v_2(x, y)}{h_1(x, y)^2 + h_2(x, y)^2}$$

where $h_1, h_2 \in \mathbb{R}[x, y]$, $u_1, v_1 \in \mathbb{R}[x, y]$ *and* $u_2, v_2 \in \mathbb{R}[x, y]$ *are the real and imaginary parts of* $h(x + i\,y)$, $f(x + i\,y) \cdot \bar{h}(x - i\,y)$ *and* $g(x + i\,y) \cdot \bar{h}(x - i\,y)$, *respectively. Then, if the plane curve* $\mathcal{C}$, *that the proper rational parametrization* $\mathcal{P}(z) = (p_1(z), p_2(z))$ *defines over* $\mathbb{C}$, *has infinitely many real points and* $(m_1(z), m_2(z))$ *is a real proper rational parametrization of* $\gcd(v_1, v_2)$, *it holds that* $\mathcal{P}(m_1(z) + i\,m_2(z))$ *is now a real proper rational parametrization of* $\mathcal{C}$.

PROOF. If $\text{cardinal}(\mathcal{C} \cap \mathbb{R}^2) = \infty$, one has by Theorem 3.1 that $G = \gcd(v_1, v_2)$ is either a real line or a real circle. If G is a real line, since $(m_1(z), m_2(z))$ is proper, it holds that $m_1(z) + i\,m(z)$ is a complex linear invertible rational function. On the other hand, let G be a real circle of the form $(x - a)^2 + (y - b)^2 = c^2$, with $a, b, c \in \mathbb{R}$. Then,

$$\mathcal{N}(z) = \left(a + c\frac{z^2 - 1}{z^2 + 1}, b + c\frac{2\,z}{z^2 + 1}\right)$$

is a real parametrization of the circle. Therefore, since $(m_1(z), m_2(z))$ is another proper parametrization of the same circle, there exists an invertible rational function $\phi \in \mathbb{C}(z)$ such that $(m_1(z), m_2(z)) = \mathcal{N}(\phi(z))$. Thus, after doing some computations,

$$m_1(z) + i\,m_2(z) = \frac{b\,i\,\phi(z) + c\phi(z) + i\,c + b + a\phi(z) - i\,a}{\phi(z) - i}$$

which is a complex linear rational function. In both situations one deduces that $\mathcal{P}(m_1(z) + i\,m_2(z))$ is again a proper rational parametrization of $\mathcal{C}$. Furthermore, by Corollary 2.1 one has that $\gcd(v_1, v_2, h_1^2 + h_2^2) = 1$, and hence $h_1(m_1, m_2)^2 + h_2(m_1, m_2)^2 \neq 0$. Therefore, since $(m_1(z), m_2(z))$ parametrizes G, one has that

$$\mathcal{P}(m_1(z) + i\,m_2(z)) = \left(\frac{u_1(m_1(z), m_2(z))}{h_1(m_1, m_2)^2 + h_2(m_1, m_2)^2}, \frac{u_2(m_1(z), m_2(z))}{h_1(m_1, m_2)^2 + h_2(m_1, m_2)^2}\right) \in \mathbb{R}(z)^2.$$

□

4. Real Reparametrization Algorithm

This section is devoted to the detailed description of the real reparametrization algorithm, as well as to the computing time analysis. In the following algorithm REAL-REPARAMETRIZATION is outlined. Given a proper rational parametrization whose rational functions have the same denominator (note that this situation can always be achieved from any proper rational parametrization), it decides whether the curve can be parametrized over the reals and, if this is the case, exhibits a reparametrizing linear rational function that transforms the input parametrization onto a real one.

Algorithm REALREPARAMETRIZATION

GIVEN: a computable subfield $\mathbb{L}$ of $\mathbb{C}$, and a proper rational parametrization $\mathcal{P}(z) = (\frac{f(z)}{h(z)}, \frac{g(z)}{h(z)}) \in \mathbb{L}(z)^2$, with $\gcd(f, g, h) = 1$, of an affine complex plane curve $\mathcal{C}$.

DECIDE: whether $\mathcal{C}$ can be parametrized over the reals.

DETERMINE: (in the affirmative case) a proper real parametrization of $\mathcal{C}$.

1. Compute $u_1 + i\,v_1 := f(x + i\,y)\bar{h}(x - i\,y)$, $u_2 + i\,v_2 := g(x + i\,y)\bar{h}(x - i\,y)$, and $w := h(x + i\,y)\bar{h}(x - i\,y)$, where $u_1, v_1, u_2, v_2, w \in \mathbb{R}[x, y]$.
2. Obtain $G(x, y) = \gcd(v_1, v_2)$.
3. IF $\deg(G) \notin \{1, 2\}$ THEN RETURN that $\mathcal{C}$ cannot be parametrized over $\mathbb{R}$.
4. IF $\deg(G) = 1$ THEN
   4.1. Compute a real proper rational parametrization $(m_1(z), m_2(z))$ of the real line that G defines.
   4.2. RETURN $(\frac{u_1(m_1,m_2)}{w(m_1,m_2)}, \frac{u_2(m_1,m_2)}{w(m_1,m_2)})$.
5. IF $\deg(G) = 2$ THEN
   5.1. Check whether G defines a real circle.
   5.2. IF G is a real circle THEN
      5.2.1. Compute a real proper rational parametrization $(m_1(z), m_2(z))$ of G.
      5.2.2. RETURN $(\frac{u_1(m_1,m_2)}{w(m_1,m_2)}, \frac{u_2(m_1,m_2)}{w(m_1,m_2)})$.
      ELSE
      5.2.3. RETURN that $\mathcal{C}$ cannot be parametrized over the reals.

The following examples illustrate the algorithm. The first example corresponds to a real reparametrization of a real curve defined by a complex parametrization. However, the second example takes a complex parametrization and detects that the corresponding curve cannot be parametrized over the reals.

EXAMPLE. Let $\mathcal{P}(z)$ be the proper complex parametrization

$$\left(\frac{52\,z-24\,z\,i-20\,i+16-30\,z^5-24\,z^5\,i-8\,z^4-154\,z^4\,i-148\,z^3-184\,z^3\,i-128\,z^2-4\,z^2\,i}{82\,z^5+240\,z^4+110\,z^4\,i-60\,z^3+280\,z^3\,i+300\,z^2\,i-240\,z^2+50\,z\,i-40\,z-18\,i-2},\right.$$
$$\left.\frac{-36\,z^5+4\,z^5\,i+108\,z^4-176\,z^4\,i-296\,z^3-368\,z^3\,i+248\,z^2\,i-264\,z^2+230\,z+20\,z\,i+20-66\,i}{82\,z^5+240\,z^4+110\,z^4\,i-60\,z^3+280\,z^3\,i+300\,z^2\,i-240\,z^2+50\,z\,i-40\,z-18\,i-2}\right),$$

and let $\mathcal{C}$ be the affine plane curve defined by $\mathcal{P}(z)$. Then, the gcd computed in step 2 of the algorithm is the real circle:

$$G(x, y) = -1 - x + x^2 + y^2$$

that can be parametrized over the reals as:

$$\mathcal{M}(z) = (m_1(z), m_2(z)) = \left(-\frac{-1 + 2\,z}{z^2 + 1}, \frac{z^2 - 1 - z}{z^2 + 1}\right).$$

Thus, $\mathcal{C}$ has infinitely many real points, and a real parametrization of $\mathcal{C}$ is

$$\mathcal{P}(m_1(z) + i\,m_2(z)) = \left(\frac{z^4 - 4\,z^3 + 6\,z^2 - 4\,z + 2}{z(z^4 - 5\,z^3 + 10\,z^2 - 10\,z + 5)}, \frac{z^4 - 4\,z^3 + 6\,z^2 - 2\,z + 3}{z(z^4 - 5\,z^3 + 10\,z^2 - 10\,z + 5}\right).$$

We finish the example giving the implicit equation $f(x, y)$ of the curve $\mathcal{C}$

$$f(x, y) = -97\,x - 278\,x^3 + 574\,x^2\,y - 1713\,x^5 + 2585\,x^4\,y - 1370\,x^3\,y^2 - 94\,x\,y^3 + 636\,x^2\,y^2 - 1064\,x^3\,y + 332\,x^4 - 4\,y^4 + 320\,x^2\,y^3 - 35\,x\,y^4 + 2\,y^5 - 36\,x^2 - 374\,x\,y^2 + 112\,x\,y + 78\,y^3 - 76\,y^2 + 97\,y.\ \square$$

EXAMPLE Let $\mathcal{C}$ be the affine plane curve defined by the proper complex parametrization

$$\mathcal{P}(z) = \left(\frac{-4\,z - 4\,z^3 + 2 - 2\,z^4}{-2 - 4\,z - 4\,z^3 + 2\,z^4}, \frac{-6\,z^2\,i + i + z^4\,i}{-2 - 4\,z - 4\,z^3 + 2\,z^4} \right).$$

Then, the gcd computed in step 2 of the algorithm is:

$$G(x, y) = x^2 + y^2 + 1.$$

Thus, since $\deg(G) = 2$ and it does not define a real circle, it follows that $\mathcal{C}$ cannot be parametrized over the reals, or equivalently, $\mathcal{C}$ does not have infinitely many real points. Indeed, since $\mathcal{C}$ is not real, one has that $\mathcal{C}$ has no real simple point. In fact, $\mathcal{C}$ is the curve

$$f(x, y) = 2\,y^2 + x^2 + 2\,x^2\,y^2$$

that corresponds to a 4-degree curve with all its singularities real. More precisely, the curve has three double points at each affine origin $(1 : 0 : 0), (0 : 1 : 0), (0 : 0 : 1)$. □

We finish this section with the computing time analysis of the given algorithm. Note that the output is given in simplified form, i.e. as a composition of rational functions. This seems to be more suitable, in practice, than to expand the result of the computation. In deriving bounds we shall assume that all arithmetic operations on integers and polynomials are preformed by classical algorithms. Then it holds that the complexity of the algorithm is quadratic in the maximum degree of the rational functions of the parametrization. More precisely, one has the following result:

THEOREM 4.1. *Let $\mathbb{L}$ be a computable subfield of $\mathbb{C}$, $\mathcal{P}(z) = (\frac{f(z)}{h(z)}, \frac{f(z)}{h(z)}) \in \mathbb{L}(z)^2$, with $\gcd(f, g, h) = 1$, and let $n = \max\{\deg_z(f), \deg_z(g), \deg_z(h)\}$. Then algorithm* REAL-REPARAMETRIZATION *requires at most $\mathcal{O}(n^2)$ field operations.*

PROOF. The polynomials $f(x + i\,y), g(x + i\,y), h(x + i\,y)$ and $\bar{h}(x - i\,y)$ can be computed in $\mathcal{O}(n^2)$ (note that it basically implies to determine recursively $\mathcal{O}(n^2)$ combinatorial numbers). Futhermore, since the degree of $f(x + i\,y), g(x + i\,y), h(x + i\,y), \bar{h}(x - i\,y)$ is bounded by n, the polynomials u_j, v_j, w can be determined in $\mathcal{O}(n^2)$ field operations. Therefore, step 1 requires at most $\mathcal{O}(n^2)$ field operations. Also, since the degree of v_1, v_2 is bounded by $2n$, one has that step 2 also is dominated by n^2.

To analyse step 4 we observe that, since G is a line, step 4 is dominated by $\mathcal{O}(1)$ (we assume that step 4.2 and step 5.2.2 return the formal solution, and hence no substitution and no rational function reduction are performed).

Step 5 basicaly involves the decision on the reality of G and its parametrization. In order to check whether the quadratic polynomial G defines a real circle it is enough to check whether G defines a real conic (observe that if G defines a real conic then by Theorem 3.2 it has to be a circle). Thus, step 5.1 can be perfomed analysing the signature and rank of the corresponding quadratic form. Hence, it requires $\mathcal{O}(1)$ field operations. On the other hand, to parametrize G over the reals one can compute the center and the radius of the circle, and that can be done applying linear algebra. Thus step 5 is dominated by 1. Therefore, algorithm REALREPARAMETRIZATION requires at most $\mathcal{O}(n^2)$ field operations. □

Now, we analyse the bit-complexity of the real reparametrization algorithm when $\mathbb{L} = \mathbb{Q}(i)$. For this purpose, let $\mathcal{P}(z) = (\frac{f(z)}{h(z)}, \frac{f(z)}{h(z)}) \in \mathbb{Q}(i)(z)^2$, with $\gcd(f, g, h) = 1$, be

a proper parametrization of an affine complex curve $\mathcal{C}$, let L be the maximum of the max-lengths [see Buchberger *et al.* (1982)] of the polynomials $f(z), g(z), h(z)$, and let $n = \max\{\deg_z(f), \deg_z(g), \deg_z(h)\}$. Then, we prove the following technical lemma.

LEMMA 4.1. *Let $G \in \mathbb{Z}[x,y]$ be a quadratic polynomial of max-length L. Then it holds that:*

(1) *The worst case complexity for deciding whether G is a real circle is $\mathcal{O}(L^2)$.*
(2) *Let G define a real circle, then G can be parametrized over $\mathbb{Q}(\alpha)$, where α is an algebraic real number whose minimal polymonial has length $\mathcal{O}(L)$. Furthermore, the worst case complexity for computing such parametrization is $\mathcal{O}(L^2)$*

PROOF. (1) Let $G = a_{11}x^2 + a_{22}y^2 + a_{12}xy + a_{13}x + a_{23}y + a_{33} \in \mathbb{Z}[x,y]$. Then, G defines a real circle if and only if $a_{11} = a_{22} \neq 0$, $a_{12} = 0$, and $4a_{11}a_{33} < a_{13}^2 + a_{23}^2$. Thus, the worst case complexity for deciding whether G is a real circle is $\mathcal{O}(L^2)$.

(2) Let G define a real circle. Then G is of the form $G(x,y) = a_{11}x^2 + a_{11}y^2 + a_{13}x + a_{23}y + a_{33}$, with $a_{11} \neq 0$, $a_{12} = 0$, and $4a_{11}a_{33} < a_{13}^2 + a_{23}^2$. Then, the center of G is $(-\frac{a_{12}}{2a_{11}}, -\frac{a_{23}}{2a_{11}})$ and the radius is $\frac{\sqrt{a_{13}^2+a_{23}^2-4a_{11}a_{33}}}{2a_{11}}$. Thus, if α is the algebraic number defined by any real irreducible factor of the polynomial $p_\alpha(x) = x^2 - (a_{13}^2 + a_{23}^2 - 4a_{11}a_{33})$, one has that G can be parametrized over $\mathbb{Q}(\alpha)$ as:

$$\mathcal{P}(z) = \left(-\frac{a_{12}}{2a_{11}} + \frac{\alpha}{2a_{11}} \frac{z^2-1}{z^2+1}, -\frac{a_{23}}{2a_{11}} + \frac{\alpha}{2a_{11}} \frac{2z}{z^2+1} \right).$$

Now, we observe that the length of any real irreducible factor of $p_\alpha(z)$ is $\mathcal{O}(L)$. Furthermore, it is clear that $\mathcal{P}(z)$ can be computed in $\mathcal{O}(L^2)$. □

We finish this section with the following theorem that analyses the bit-complexity of our algorithm.

THEOREM 4.2. *The worst case complexity for algorithm* REALREPARAMETRIZATION, *working over $\mathbb{L} = \mathbb{Q}(i)$, is $\mathcal{O}(n^5(L + n\log n)^2)$*

PROOF. Let T_i be the time of execution of step i of algorithm REALREPARAMETRIZATION. In step 1, first $f(x+iy), g(x+iy), h(x+iy)$ and $\bar{h}(x-iy)$ have to be determined. This essentially implies to compute the integers $a \cdot \binom{j}{k}$ for $0 \leq k \leq j \leq n$, and $a \in \mathbb{Z}$ being the real part or the imaginary part of any coefficient of $f(z), g(z), h(z), \bar{h}(\bar{z})$. Thus, since the combinatorial numbers can be obtained recursively as the sum of other already computed combinatorial numbers, one has that the computing time for determining the combinatorial numbers is $\mathcal{O}(n^3 \log n)$ (observe that the length of $\binom{j}{k}$ is dominated by $k \log j$). Therefore, $f(x+iy), g(x+iy), h(x+iy)$ and $\bar{h}(x-iy)$ can be determined in $\mathcal{O}(L\, n^3 \log n)$. Furthermore, the length of $f(x+iy), g(x+iy), h(x+iy)$ and $\bar{h}(x-iy)$ is dominated by $L + n\log n$. In order to compute $u_j, v_j, w \in \mathbb{R}[x,y]$, we assume that the real and imaginary parts of $f(x+iy), g(x+iy), h(x+iy)$ and $\bar{h}(x-iy)$ have been already collected. This implies to read all the coefficients of the polynomials, hence it can be achieved in $\mathcal{O}(n^2(L + n\log n))$. In this situation, u_j, v_j, w can be computed in $\mathcal{O}(n^2(L + n\log n)^2)$. Therefore, $T_1 = \mathcal{O}(n^2(L + n\log n)^2)$, and the length of u_j, v_j, w is clearly $\mathcal{O}(L + n\log n)$.

In step 2, one has to compute the gcd of two polynomials in $\mathbb{Z}[x, y]$ of length $\mathcal{O}(L + n \log n)$ and degree $2n$. Thus, using Brown's modular algorithm [see Buchberger *et al.* (1982)] it follows that $T_2 = \mathcal{O}(n^5(L + n \log n)^2)$, and using Landau–Mignotte bound for the length of the factors of integer polynomials [see Buchberger *et al.* (1982)], one has that the length of G is $\mathcal{O}(L + n \log n)$.

Step 3 is clearly codominated by 1. To analyse step 4, we observe that if G is a line then it can trivially be parametrized over $\mathbb{Q}$, and $m_1(z), m_2(z)$ are bounded in length by the length of G. Thus, $T_4 = \mathcal{O}(n(L + n \log n))$ (we assume that step 4.2 and step 5.2.2 return the formal solution, and therefore no substitution or rational function reduction are performed).

Finally, applying Lemma 4.1 one has the $T_5 = \mathcal{O}((L + n \log n)^2)$. Thus, the worst case complexity for algorithm REALREPARAMETRIZATION is $\mathcal{O}(n^5(L + n \log n)^2)$. □

Acknowledgements

We want to acknowledge our thanks to several colleagues who have been consulted in relation with the analytic polynomial and rational function properties, specially to J. Vinuesa, J. Ruiz and R. Heersink.

References

Alonso, C., Gutiérrez, J., Recio, T. (1995a). A rational function decomposition algorithm by near-separated polynomials. *J. Symbolic Computation* **19**, 527–544.

Alonso, C., Gutiérrez, J., Recio, T. (1995b). Reconsidering algorithms for real parametric curves. *J. AAECC* **6**, 345–352.

Bajaj, C., Royappa, A.V. (1993). Finite representations of real parametric curves and surfaces. In Falcidiendo, B., Kunni, T., eds, Modeling in Computer Graphics. *Proc. IFIP TC 5/WC 5.10 II Conf. on Geom. Modeling in Computer Graphics*, Springer-Verlag pp. 347–358.

Bak, J., Newman, D.J. (1982). *Complex Analysis Undergraduate Texts in Mathematics.* Springer-Verlag, New York.

Buchberger, B. (1987). Applications of Groebner Bases in non-linear Computational Geometry. In Janssen, R., ed., *Trends in Computer Algebra. LNCS* **296**, 52–91.

Buchberger, B., Collins, G.E., Loos, R. (1982). *Computer Algebra; Symbolic and Algebraic Computation.* Springer Verlag.

Chevalley C. (1951). *Introduction to the theory of algebraic functions of one variable.* Mathematical Surveys, VI. A.M.S.

Hoffmann C. (1989). *Geometric and Solid Modeling: An Introduction.* Morgan Kaufmann, USA.

Recio, T., Sendra, J.R. (1995). *A really elementary proof of real Luroth's theorem.* To appear in Revista Matemática de la Universidad Complutense de Madrid.

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

Sederberg, T.W. (1987). Algebraic Geometry for Surface and Solid Modelling. In Farin, G.E., ed., *Proc. Geometric Modelling: Algorithms and new trends, SIAM Publ.*, pp. 29–42.

Sendra, J.R., Winkler, F. (1997). Parametrization of Algebraic Curves over Optimal Field Extensions. *J. Symbolic Computation* **23**, 191–207.