MATHEMATICS OF COMPUTATION
Volume 86, Number 308, November 2017, Pages 3001–3018
http://dx.doi.org/10.1090/mcom/3202
Article electronically published on April 7, 2017

A PARAMETRIC VERSION OF THE HILBERT-HURWITZ THEOREM USING HYPERCIRCLES

LUIS FELIPE TABERA

Abstract. Let $\mathbb{K}$ be a characteristic zero field, let α be an algebraic element over $\mathbb{K}$ and $\mathcal{C}$ a rational curve defined over $\mathbb{K}$ given by a parametrization ψ with coefficients in $\mathbb{K}(\alpha)$. We propose an algorithm to solve the following problem, that is, a parametric version of Hilbert-Hurwitz: To compute a linear fraction $u = \frac{at+b}{ct+d}$ such that $\psi(u)$ has coefficients over an algebraic extension of $\mathbb{K}$ of degree at most two and a conic $\mathbb{K}$-birational to $\mathcal{C}$. Moreover, if the degree of $\mathcal{C}$ is odd or α is of odd degree over $\mathbb{K}$, we can compute a parametrization of $\mathcal{C}$ with coefficients over $\mathbb{K}$. The problem is solved without implicitization methods nor analyzing the singularities of $\mathcal{C}$.

1. Introduction

Let $\mathbb{K}$ be a characteristic zero field, $\mathbb{F}$ its algebraic closure. Let $\mathcal{C} \subseteq \mathbb{P}(\mathbb{F})^N$ be a rational curve in a space of dimension N. We say that $\mathbb{K}$ is a *field of definition* of $\mathcal{C}$ if $\mathcal{C}$ can be described as the zero set of a system of polynomials with coefficients in $\mathbb{K}$. Analogously, we say that $\mathcal{C}$ is *parametrizable* over $\mathbb{K}$ if there is a parametrization of $\mathcal{C}$ defined by rational functions in $\mathbb{K}(t)$. If $\mathcal{C}$ is parametrizable over $\mathbb{K}$, then it is trivially defined over $\mathbb{K}$. However, if $\mathcal{C}$ is not parametrizable over $\mathbb{K}$, the best we can say is that there are minimal fields of parametrization that are quadratic algebraic extensions of $\mathbb{K}$ ([4], [8], [16], [24]).

Suppose that we are given a curve $\mathcal{C}$ defined by an (affine) birational parametrization $\psi(t)$ with coefficients over $\mathbb{K}(\alpha)$, where α is algebraic of degree n over $\mathbb{K}$. This curve $\mathcal{C}$ could be the outcome of some geometric transformations in the context of CAGD, computing offsets or bisector curves may naturally add square roots in the resulting parametrization (see for instance Example 5.1). The problems of deciding if $\mathcal{C}$ can be parametrized over $\mathbb{K}$ and computing such a parametrization have been studied (among others) in [1], [2], [3], [15], [16], [17], [24]. Any birational parametrization of $\mathcal{C}$ with coefficients in $\mathbb{K}$ is of the form $\psi\left(\frac{at+b}{ct+d}\right)$, where $\frac{at+b}{ct+d} \in \mathbb{K}(\alpha)(t)$. Computing a valid linear fraction $\frac{at+b}{ct+d}$ that reparametrizes ψ over $\mathbb{K}$ is at least as hard as computing a point in $\mathcal{C} \cap \mathbb{K}^N$. To compute a rational point on $\mathcal{C}$, one usually computes a plane conic or a line $\mathbb{K}$-birational to the given curve using the methods in [8], [16], [24] and then applies algorithms to find rational points in

Received by the editor August 1, 2011 and, in revised form, February 19, 2014 and July 26, 2016.

2010 *Mathematics Subject Classification.* Primary 14Q05, 68W30, 14M20.

Key words and phrases. Hypercircles, rational curves, rational points.

The author is supported by the Spanish "Ministerio de Ciencia e Innovación" projects MTM2008-04699-C03-03 and MTM2011-25816-C02-02 and "Ministerio de Economa y Competitividad" and by the European Regional Development Fund (ERDF) project MTM2014-54141-P.

conics, for example, the methods in [5] or [18]. For a self-contained reference that develops the method above and a full algorithm we refer to Chapter 5 in [17].

A parametric version of Weil's descent method was proposed in [2] to attack this problem. Following this approach, the curve $\mathcal{C}$ is substituted by a *witness curve*, $\mathcal{U}$, where the problem is thought to be easier. During the last twelve years there has been an effort to systematically study this transformation and its application to the reparametrization problem [2], [9], [10], [11], [12], [13], [14], [15], [22], [20], [25]. It is known [2], [3] that $\mathcal{C}$ is parametrizable over $\mathbb{K}$ if and only if $\mathcal{U}$ is a special curve called α-hypercircle. Algorithms to compute a reparametrization of $\mathcal{C}$ using α-hypercircles are found in [12, 13].

If we already know a smooth point of $\mathcal{C} \cap \mathbb{K}^N$, then we are able to compute a unit $u(t) = \frac{at+b}{ct+d}$ such that $\psi(u(t))$ has coefficients over $\mathbb{K}$; see [12]. However, it was an open problem how to deal with the general case in which we do not know any rational point on the curve without using adjoint curves *à la Hilbert-Hurwitz*. In [9], it was proposed to study specific algorithms to compute points on hypercircles with coefficients over $\mathbb{K}$.

In this article we present how to attack algorithmically this problem, as well as some ideas for an efficient implementation. Given the curve $\mathcal{C}$ represented by a parametrization ψ with coefficients in $\mathbb{K}(\alpha)$ and defined over $\mathbb{K}$, we compute a linear fraction $u(t)$ such that $\psi(u(t))$ has coefficients over an extension of $\mathbb{K}$ of degree at most 2. As a corollary, we can also compute a conic or a line that is $\mathbb{K}$-birational to $\mathcal{C}$ without using implicitization methods. Moreover, if we are given an odd divisor on the curve defined over $\mathbb{K}$ (that can always be obtained if the geometric degree of $\mathcal{C}$ is odd or α is of odd degree over $\mathbb{K}$), then we can compute a rational point $p \in \mathcal{C} \cap \mathbb{K}^N$ and a parametrization over $\mathbb{K}$.

In the implicit case, the Hilbert-Hurwitz method uses adjoint curves on a curve of degree r to compute a curve of degree $r-2$ that is $\mathbb{K}$-birational to $\mathcal{C}$. Applying this method $\mathcal{O}(r)$ times, we get a line or a conic that is birational to $\mathcal{C}$. This method can be improved (cf. [16]) to compute directly the line or the conic using only one birational transformation.

Our method is as follows: Given the parametrization ψ of a curve $\mathcal{C}$, we compute its associated hypercircle $\mathcal{U}$. This will be a spatial curve of degree r. Then, we can easily compute a divisor of degree $2r-2$ on $\mathcal{U}$ defined over $\mathbb{K}$. Intersecting the hypercircle with a quadric hypersurface that passes through the $2r-2$ points in the divisor, we can compute a point $p \in \mathcal{U}$ defined over a quadratic extension of $\mathbb{K}$. From p, we compute the birational line or conic to $\mathcal{C}$ as well as a linear fraction $u(t)$ such that $\psi(u)$ has coefficients on the field of definition of p. One big advantage of this method is that, since we are working with a parametrization, we do not have to analyze the singularities of the curve.

The presentation is structured as follows: In Section 2 we present the basic properties of hypercircles that are relevant for the reparametrization problem. In Section 3 we present how to effectively compute a point in the hypercircle defined over a quadratic extension of $\mathbb{K}$ and a birational conic. In Section 4 we discuss some strategies to implement the method described in Section 3. Finally, we present in Section 5 some examples and experimental results.

2. Background on hypercircles

In this section, we present the main properties of hypercircles needed to develop our method.

Let $\mathbb{K}$ be a characteristic zero field, $\mathbb{F}$ its algebraic closure and $\alpha \in \mathbb{F}$ be algebraic of degree n over $\mathbb{K}$. Let $\psi(t) = (\psi_1(t), \ldots, \psi_N(t))$ be a proper parametrization of a curve $\mathcal{C} \subseteq \mathbb{P}(\mathbb{F})^N$, where $\psi_i(t) \in \mathbb{K}(\alpha)(t)$, $1 \leq i \leq N$. Write the rational functions with a common denominator g, $\psi_i(t) = f_i/g$, $1 \leq i \leq N$, $\gcd(f_1, \ldots, f_N, g) = 1$.

We show the parametric Weil descent version as presented in [2] and substitute $t = \sum_{i=0}^{n-1} \alpha^i t_i$, where t_i are new variables. We rewrite:

$$\psi_j\left(\sum_{i=0}^{n-1} \alpha^i t_i\right) = \sum_{i=0}^{n-1} \alpha^i \lambda_{ij}(t_0, \ldots, t_{n-1}), \lambda_{ij} = \frac{F_{ij}}{D} \in \mathbb{K}(t_0, \ldots, t_{n-1}).$$

In this context we have the following definition:

Definition 2.1. Let $\mathcal{Z}$ be the Zariski closure of

$$\{F_{ij} = 0 \mid 1 \leq i \leq n-1,\ 1 \leq j \leq N\} \setminus \{D = 0\} \subseteq \mathbb{F}^n.$$

$\mathcal{Z}$ is called the *witness variety* or *the parametric variety of Weil* (cf. [2]) of the parametrization ψ.

Theorem 2.2 ([2], [3])**.** *With the previous notation:*

- $\dim \mathcal{Z} \leq 1$.
- $\mathcal{Z}$ *has at most one 1-dimensional component* $\mathcal{U}$.
- $\mathbb{K}$ *is a field of definition of* $\mathcal{C}$ *if and only if* $\dim \mathcal{Z} = 1$.
- $\mathcal{C}$ *is parametrizable over* $\mathbb{K}$ *if and only if* $\mathcal{U}$ *is parametrizable over* $\mathbb{K}$.

In the case that $\mathcal{C}$ is not defined over $\mathbb{K}$, we showed in [22] how to compute the minimum field of definition $\mathbb{L}$ of $\mathcal{C}$ satisfying $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{K}(\alpha)$. So, we will assume, without loss of generality, that $\mathcal{C}$ is defined over $\mathbb{K}$. Thus, the problem of parametrizing $\mathcal{C}$ over $\mathbb{K}$ can be translated to the problem of parametrizing the curve $\mathcal{U} \subseteq \mathcal{Z}$. The interest of this construction is that the result is related with the study of hypercircles:

Definition 2.3. Let $\frac{at+b}{ct+d} \in \mathbb{K}(\alpha)(t)$ represent a $\mathbb{K}(\alpha)$-isomorphism of $\mathbb{K}(\alpha)(t)$, where $a, b, c, d \in \mathbb{K}(\alpha)$ and $ad - bc \neq 0$. Write

$$\frac{at+b}{ct+d} = \lambda_0(t) + \lambda_1(t)\alpha + \cdots + \lambda_{n-1}(t)\alpha^{n-1},$$

where $\lambda_i(t) \in \mathbb{K}(t)$. The *$\alpha$-hypercircle* $\mathcal{U}$ associated with $\frac{at+b}{ct+d}$ for the extension $\mathbb{K} \subseteq \mathbb{K}(\alpha)$ is the parametric curve in $\mathbb{P}(\mathbb{F})^n$ given by the (affine) parametrization $(\lambda_0, \ldots, \lambda_{n-1})$.

If $\mathcal{U}$ is an α-hypercircle, any linear fraction $u(t) = \frac{at+b}{ct+d}$ such that $\mathcal{U}$ is the α-hypercircle associated with u is called an *associated unit*. If u is an associated unit, then every other associated unit is of the form $u \circ k$ with $k \in \mathbb{K}(t)$ a linear fraction with coefficients in $\mathbb{K}$. If the algebraic extension $\mathbb{K} \subseteq \mathbb{K}(\alpha)$ is clear from the context, we will call $\mathcal{U}$ the hypercircle associated with $u(t)$.

Recall that, in the semigroup $(\mathbb{K}(\alpha)(t), \circ)$ of rational functions with the composition operation, the set of units is exactly the set of linear fractions $\frac{at+b}{ct+d}$, $ad-bc \neq 0$. When referring to units, we refer to units under the composition operation, that is, linear fractions. We refer to [9] for a study of the main properties of hypercircles using this approach.

The main result that relates hypercircles with the reparametrization problem is the following.

Theorem 2.4 ([2], [3]). *In the previous conditions, $\mathbb{K}$ is a field of parametrization of $\mathcal{C}$ and $\psi(\frac{at+b}{ct+d})$ is a parametrization of $\mathcal{C}$ over $\mathbb{K}$ if and only if the curve $\mathcal{U} \subseteq \mathcal{Z}$ in Weil's descent construction is an α-hypercircle associated with $\frac{at+b}{ct+d}$ for the extension $\mathbb{K} \subseteq \mathbb{K}(\alpha)$.*

One problem with this approach is that we can only assume that we are working with hypercircles if $\mathcal{C}$ can be parametrizable over $\mathbb{K}$. Hence we lose all the rich geometric structure to manipulate these curves. We now show that this is not really the case, since the curve $\mathcal{U}$ can be interpreted as a hypercircle, but possibly with respect to a different algebraic extension.

Theorem 2.5 ([22]). *Let $\mathcal{C}$ be a curve $\mathbb{K}$-definable, that is not $\mathbb{K}$-parametrizable, where $\mathbb{K}$ is finitely generated over $\mathbb{Q}$ (as a field). Let φ be an α-parametrization for $\mathcal{C}$. Let $\mathcal{U}$ be the 1-dimensional component of the parametric Weil variety of $\mathcal{C}$ for the extension $\mathbb{K} \subseteq \mathbb{K}(\alpha)$. Then, there exists an η, quadratic over $\mathbb{K}$ such that $\mathcal{U}$ is an α-hypercircle for the extension $\mathbb{K}(\eta) \subseteq \mathbb{K}(\eta, \alpha)$.*

This result allows us to work with hypercircles even in the case that there is no parametrization of $\mathcal{C}$ over the ground field $\mathbb{K}$. All the computations throughout the text will be done over a field of the form $\mathbb{K}(\alpha, \beta)$. But the curve $\mathcal{C}$ will always have points with coefficients over a field $\mathbb{L} = \mathbb{K}(\eta)$ with $\mathbb{K}(\eta) \cap \overline{\mathbb{K}(\alpha, \beta)} = \mathbb{K}$, where $\overline{\mathbb{K}(\alpha, \beta)}$ is the normal closure of $\mathbb{K}(\alpha, \beta)$ over $\mathbb{K}$. Even if all the computations are done in $\mathbb{K}(\alpha, \beta)$, the correctness of the results and computations are really proven in $\mathbb{L}(\alpha, \beta)$. Hence, without loss of generality, we may always assume that the curve $\mathcal{C}$ has points with coefficients in $\mathbb{K}$. We refer to [22] for the technical details.

Let $\mathcal{U}$ be a hypercircle. There is a canonical way of describing $\mathcal{U}$ by a distinguished parametrization.

Definition 2.6 ([12]). The *standard parametrization* of a hypercircle $\mathcal{U}$ is the unique parametrization $\varphi = (\varphi_0, \varphi_1, \ldots, \varphi_{n-1}) \in \mathbb{K}(\alpha)(t)^n$ of $\mathcal{U}$ such that $\sum_{i=0}^{n-1} \varphi_i(t)\alpha^i = t$.

To any hypercircle $\mathcal{U}$, we can always take an associated unit $u = \frac{at+b}{ct+d}$ with $c \neq 0$. Write the standard parametrization $\varphi(t)$ of $\mathcal{U}$ with a common denominator

$$\varphi(t) = (\frac{q_0}{Q}, \ldots, \frac{q_{n-1}}{Q}),$$

$\gcd(q_0, \ldots, q_{n-1}, Q) = 1$.

We describe now some properties of $\mathcal{U}$ and φ that will be useful throughout the text.

Theorem 2.7 ([9], [12], [22], [23]). *Let $\mathcal{U}$ be a hypercircle, $u = \frac{at+b}{ct+d}$, $c \neq 0$ an associated unit. Let $r = [\mathbb{K}(d/c) : \mathbb{K}]$ and let φ be the standard parametrization of $\mathcal{U}$. Then*

1. *$\mathcal{U}$ is a rational normal curve of degree r in $\mathbb{P}(\mathbb{F})^n$ defined over $\mathbb{K}$.*
2. *$u(t)$ is an associated unit if and only if $\varphi(u)$ has coefficients in $\mathbb{K}$.*
3. *If φ_i is any nonconstant component of φ, then $\varphi_i = \frac{q_i(t)}{Q(t)}$, $\gcd(q_i, Q) = 1$, $\deg(q_i) = r$ and $\deg(Q(t)) = r - 1$.*
4. *$\mathcal{U}$ has exactly r different points in the hyperplane at infinity. the field of definition (over $\mathbb{K}$) of any of these points is ($\mathbb{K}$-isomorphic to) $\mathbb{K}(d/c)$.*
5. *The points at infinity are attained by the $r-1$ roots of $Q(t)$ and by $t = \infty$.*

(6) $\gcd(Q(t), Q'(t)) = 1$, *the denominator has no multiple root.*
(7) *If* $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ *are the conjugates of* α *in* $\mathbb{F}$. *Write* $\psi(\alpha_j, t)$ *as the* j*-th conjugate parametrization of* ψ, *then the standard parametrization verifies* $\sum_{i=0}^{n-1} \varphi_i(\alpha, t)\alpha_j^i = \psi(\alpha_j, t)^{-1} \circ \psi(\alpha, t)$.

The standard parametrization of $\mathcal{U}$ can be computed from the parametrization ψ of $\mathcal{C}$ without computing the variety $\mathcal{Z}$.

Theorem 2.8 ([23])**.** *Let* $\mathbb{K}$ *be a computable field with factorization of characteristic zero. Let* α *be algebraic of degree* n *over* $\mathbb{K}$ *of minimal polynomial* $M(x)$. *Let* $\psi(t) = (\psi_1, \ldots, \psi_N)$ *be a proper parametrization of a spatial curve* $\mathcal{C}$ *of degree* d *in dimension* N *with coefficients in* $\mathbb{K}(\alpha)$. *Then it can be decided if* $\mathcal{C}$ *is defined over* $\mathbb{K}$ *and, in the affirmative case, compute the standard parametrization of the associated hypercircle* $\mathcal{U}$ *in* $K + \mathcal{O}(Nd^5n^8)$ *operations over* $\mathbb{K}$, *where* K *is the time needed to factor* $M(x)$ *in* $\mathbb{K}(\alpha)[x]$.

In order to define a hypercircle, we need the parametrization ψ, but we also need the algebraic extension $\mathbb{K} \subseteq \mathbb{K}(\alpha)$ and the primitive element α. We now show how the hypercircle is modified under some changes of field extensions.

Theorem 2.9 ([22])**.** *Let* $\mathcal{C}$ *be a rational curve defined over* $\mathbb{K}$ *and given by a parametrization* ψ *with coefficients in* $\mathbb{K}(\alpha)$. *Let* β *be such that* $\mathbb{K} \subsetneq \mathbb{K}(\beta) \subsetneq \mathbb{K}(\alpha)$. *Let* n *be the degree of* α *over* $\mathbb{K}$ *and* m *the degree of* α *over* $\mathbb{K}(\beta)$. *Let* $M \in \mathcal{M}_{m\times n}(\mathbb{K}(\beta))$ *such that the* i*-th column contains the coordinates of* α^{i-1} *in the base* $\{1, \alpha, \ldots, \alpha^{m-1}\}$ *over* $\mathbb{K}(\beta)$. *Let* φ *be the standard parametrization of the* α*-hypercircle associated with* ψ *for the extension* $\mathbb{K} \subseteq \mathbb{K}(\alpha)$. *Then,* $M(\varphi) = (\varphi'_0, \ldots, \varphi'_{m-1}) \in \mathbb{K}(\alpha)^m$ *is the standard parametrization of the* α*-hypercircle associated with* ψ *for the extension* $\mathbb{K}(\beta) \subseteq \mathbb{K}(\alpha)$.

Another property that characterizes the standard parametrization is that it is invariant under the Weil descent method.

Theorem 2.10. *Let* ψ *be a proper parametrization of a spatial curve* $\mathcal{C}$ *with coefficients in* $\mathbb{K}(\alpha)$. *Let* φ *be the standard parametrization of the hypercircle* $\mathcal{U}$ *associated with* ψ *for the extension* $\mathbb{K} \subseteq \mathbb{K}(\alpha)$. *Then* ψ *is the standard parametrization of a hypercircle for the extension* $\mathbb{K} \subseteq \mathbb{K}(\alpha)$ *if and only if* $\psi = \varphi$.

Proof. If $\psi = \varphi$, then $\mathcal{U} = \mathcal{C}$ and ψ is the standard parametrization of a hypercircle. Assume now that $\mathcal{C}$ is a hypercircle and ψ is its standard parametrization. Let u be an associated unit to $\mathcal{C}$ as hypercircle. By Theorem 2.7, $\psi(u)$ has coefficients in $\mathbb{K}$ and u is a reparametrization unit of ψ. It follows from Theorem 2.4, that u also an associated unit to $\mathcal{U}$ for the same extension $\mathbb{K} \subseteq \mathbb{K}(\alpha)$. Then $\mathcal{C} = \mathcal{U}$ and ψ, φ are parametrizations of $\mathcal{C}$. Now, since both are standard parametrizations $\sum_{i=0}^{n-1} \psi_i\alpha^i = \sum_{i=0}^{n-1} \varphi_i\alpha^i = t$, it must happen that $\psi = \varphi$. □

3. Rational canonical divisor on hypercircles

Our aim is to compute a rational parametrization of the original curve $\mathcal{C}$ over an extension $\mathbb{K}(\beta)$ quadratic over $\mathbb{K}$ and a $\mathbb{K}$-birational conic to $\mathcal{C}$. It turns out that this problem can be reduced to compute a point in $\mathcal{U}$ with coefficients in $\mathbb{K}(\beta)$. This section shows how to compute such a point. We start computing an appropriate divisor on $\mathcal{U}$.

Theorem 3.1. *Let $\varphi = (\varphi_0, \ldots, \varphi_{n-1})$ be the standard parametrization of an α-hypercircle $\mathcal{U}$ of degree r. Let φ_i be nonconstant components of φ and write $\varphi_i(t)' = \frac{A(t)}{B(t)}$, $\gcd(A(t), B(t)) = 1$. Let $t_1, \ldots, t_\ell$ be the roots of $A(t)$ counted with multiplicity. Then $\ell = 2r-2$ and $[\varphi(t_1)] + \ldots + [\varphi(t_{2r-2})]$ is a divisor of $\mathcal{U}$ defined over $\mathbb{K}$ of degree $2r-2$ consisting of points not in the hyperplane at infinity.*

Proof. Let $\mathcal{U}^*$ be the affine part of $\mathcal{U}$, since $\mathcal{U}$ is a curve defined over $\mathbb{K}$, the i-th projection: $x_i : \mathbb{F}^n \to \mathbb{F}$ restricted to $\mathcal{U}^*$ is a rational map defined over $\mathbb{K}$, so the divisor associated with the differential dx_i is a canonical divisor defined over $\mathbb{K}$. Hence, both the divisor of zeros and the divisor of poles of dx_i are defined over $\mathbb{K}$. Since $\mathcal{U}$ is a rational curve, the degree of the divisor of dx_i is -2.

From the parametrization, $x_i = \varphi_i(t) = \frac{q_i}{Q}$, so $dx_i = \frac{q_i'(t)Q(t) - q_i(t)Q'(t)}{Q^2(t)} dt$ and the divisor of dx_i, in the space of parameters $\mathbb{P}^1(\mathbb{F})$, is $\operatorname{div}(\frac{q_i'(t)Q(t) - q_i(t)Q'(t)}{Q^2(t)}) - 2[\infty]$.

Now, $\frac{A}{B} = \frac{q_i'Q - q_iQ'}{Q^2}$. Let us prove that this fraction is already reduced. If we had an irreducible common factor f of the numerator and denominator, then it must be a factor of $Q(t)$, so f divides q_iQ'. But f cannot be a factor of q_i since $\gcd(q_i, Q) = 1$ and cannot be a factor of Q' since all the roots of Q are distinct by Theorem 2.7. So, the fraction is reduced, $A = q_i'Q - q_iQ'$ and $B = Q^2$, write $q_i = a_it^r + \ldots$, $Q = t^{r-1} + \ldots$, then $A = a_it^{2r-2} + \ldots$ is a polynomial of degree $2r-2$ and $\frac{A}{B}$ is the quotient of two polynomials of degree $2r-2$. Thus, there is no zero nor a pole of $\frac{A}{B}$ at $t = \infty$. Hence $\operatorname{div}(dx_i)$ corresponds, via the parametrization φ with

$$\operatorname{div}_0(q_i'Q - q_iQ') - \operatorname{div}_0(Q^2) - 2[\infty] \xrightarrow{\varphi} \operatorname{div}(dx_i)$$

The divisor of poles $\operatorname{div}_0(Q^2) + 2[\infty]$ corresponds, via the parametrization, with twice the points at infinity of $\mathcal{U}$, $2[o_1] + 2[o_2] + \ldots + 2[o_r]$. Let $t_1, \ldots, t_\ell$ be the roots of A (in $\mathbb{F}$) counted with multiplicities, $\ell = 2r-2$. By the parametrization, the divisor $[t_1] + \ldots + [t_{2r-2}]$ corresponds to the set of zeros of dx_i, that is, a divisor of degree $2r-2$ defined over $\mathbb{K}$. □

Example 3.2. Let $\mathbb{K} = \mathbb{Q}(\alpha)$ where α is a primitive 5-th root of unity. Let $\mathcal{U}$ be the hypercircle associated with the unit $u = \frac{1}{t-\alpha}$. Let $\varphi = (\varphi_0, \varphi_1, \varphi_2, \varphi_3)$ be the standard parametrization of $\mathcal{U}$. The numerators of $\varphi_i'(t)$ are:

- $numerator(\varphi_0')$: $\frac{1}{5}(t+\alpha^4)^3 \cdot (5t^3 - (3\alpha^3 + \alpha^2 - \alpha - 3)t^2 - (3\alpha^2 - \alpha - 2)t - \alpha + 1)$,
- $numerator(\varphi_1')$: $\frac{1}{5}t \cdot (t + \alpha^4)^2 \cdot (5t^3 - (8\alpha^3 + 6\alpha^2 + 4\alpha + 2)t^2 + (4\alpha^3 - 2\alpha + 8)t - 4\alpha^3 - 4\alpha - 2)$,
- $numerator(\varphi_2')$: $\frac{1}{5}(t + \alpha^4) \cdot t^2 \cdot (5t^3 - (13\alpha^3 + 11\alpha^2 + 9\alpha + 7)t^2 + (3\alpha^3 - 12\alpha^2 - 6)t + 6\alpha^3 + 3\alpha^2 + 6)$,
- $numerator(\varphi_3')$: $\frac{1}{5}t^3 \cdot (5t^3 - (18\alpha^3 + 16\alpha^2 + 14\alpha + 12)t^2 + (12\alpha^3 - 9\alpha^2 - 3\alpha)t + 4\alpha^2 - 4\alpha)$.

This example shows that it can happen that, for every projection along the coordinate directions, the divisor we obtain by Theorem 3.1 can have points with multiplicity greater than one. In the method we propose to compute a parametrization of $\mathcal{C}$ over $\mathbb{K}(\beta)$, we will need to compute the divisor of φ_i. If it were the case that we want to work with divisors such that the multiplicity at each point is 0 or 1 only, we could do the following: If a point p in the canonical divisor defined by dx_i has multiplicity greater than one, then the field of definition of p has degree less than r over $\mathbb{K}$. We could use slight variations of the algorithms in [12], [13] to

reparameterize the original curve over the field of definition of p and, then, compute another hypercircle for the new extension. The problem with this approach is that there may be cases such that the number of iterations is not better than the classical Hilbert-Hurwitz approach. Still, a point p with multiplicity greater than one has chances to be a point over $\mathbb{K}$. It may then be worth checking the field of the definition of p.

Another standard approach is to take more generic projections

$$d(a_1x_0 + \ldots + a_{n-1}x_{n-1}), \qquad a_i \in \mathbb{K}.$$

The problem with this approach is that, in practice, the coefficients grow too much. Instead, we will just assume that the divisor may have higher multiplicities and take care that our results hold in this situation too.

Let $D = a_1[p_1] + \ldots + a_s[p_s]$ be a $\mathbb{K}$-defined effective divisor on $\mathcal{U}$ of degree $2r-2$. Let W be any quadric not containing $\mathcal{U}$, then the number of intersection points of W and $\mathcal{U}$ is $2r$ counted with multiplicity. We are now studying the space of quadrics W such that the intersection multiplicity of W and $\mathcal{U}$ along p_i is at least a_i.

Definition 3.3. Let $\mathcal{U}$ be a hypercircle of degree $r > 2$. Let D be a degree $2r-2$ effective divisor of $\mathcal{U}$ defined over $\mathbb{K}$ that contains no point in the hyperplane at infinity, we define W_D as the set of (projective) quadrics such that either $\mathcal{U} \subseteq W$ or $|\mathcal{U} \cap W| < \infty$ and $\mathcal{U} \cap W \succeq D$.

Since the space of quadrics is of dimension $\binom{n+2}{2} - 1$ and we are adding at most $2r-2$ independent linear conditions, then $\dim(W_D) \geq \binom{n+2}{2} - 2r + 1$. Moreover, since $\mathcal{U}$ and D are defined over $\mathbb{K}$, W_D is also defined over $\mathbb{K}$. On the other hand, $\mathcal{U}$ is a rational normal curve of degree r. Thus, the space of quadrics containing $\mathcal{U}$ is (projective) linear, of dimension $\binom{n+2}{2} - 2r - r$. Hence, the space of quadrics containing $\mathcal{U}$ is of codimension at least three on W_D. We can take a random quadric in W_D and it will not contain the curve with high probability. More precisely, if we have a basis of W_D defined over $\mathbb{K}$, then one of the elements of the basis is guaranteed to work. We now show how to check if a quadric is in W_D.

Lemma 3.4. *Let $F = \sum_{i\in I} a_i x_0^{i_0} \cdot \ldots \cdot x_n^{i_n}$, $I = \{(i_0, \ldots, i_n) | \sum_j i_j = 2\}$ be a quadratic homogeneous polynomial in $n+1$ variables defining a quadric W not containing $\mathcal{U}$. $F(\varphi) = \sum_{i\in I} a_i q_0^{i_0} \cdot \ldots \cdot q_{n-1}^{i_{n-1}} Q^{i_n} \in \mathbb{F}[t]$. Let $p \in \mathcal{U} \cap \mathbb{F}^n$ be an affine point of $\mathcal{U}$, $p = \varphi(t_0)$. Then the intersection multiplicity of W and $\mathcal{U}$ along p is the algebraic multiplicity of t_0 as a root of $F(\varphi)$.*

Proof. We follow [7, I, §7]. Let $S = \mathbb{F}[x_0, \ldots, x_n]$, let $I_{\mathcal{U}}$ be the homogeneous ideal of $\mathcal{U}$, and let $\mathfrak{p}$ be the prime ideal of p. Then the intersection multiplicity is the length of the $S_{\mathfrak{p}}$-module $(S/(F \cdot S + I_{\mathcal{U}}))_{\mathfrak{p}}$. The birational map φ induces an isomorphism between $(S/I_{\mathcal{U}})_{\mathfrak{p}}$ and $\mathbb{F}[t,s]_{(t-t_0 s)}$. Under this isomorphism, $F(x_0, \ldots, x_n)$ corresponds to G, the homogenization of $F(Q, q_1, \ldots, q_n)$, where $\varphi_i = q_i/Q$. The length ℓ of the module $M = (\mathbb{F}[t,s]/(G))_{(t-t_0 s)}$ is the multiplicity of $(t - t_0 s)$ as a factor of G. We have the maximal chain of submodules $0 = (t-t_0 s)^\ell \subset (t-t_0 s)^{\ell-1} \subset \ldots \subset (t-t_0 s) \subset (1) = M$. This multiplicity equals the algebraic multiplicity of t_0 as a root of $F(\varphi)$. Note that, if $(t - t_0 s)$ is not a factor of G, then $M = 0$. □

Corollary 3.5. *Let $D = a_1[\varphi(t_1)] + \ldots + a_s[\varphi(t_s)]$ be a divisor of degree $2r-2$ and defined over $\mathbb{K}$ of $\mathcal{U}$ with affine support. Let $A(t) = (t-t_1)^{a_1} \cdots (t-t_s)^{a_s}$ and let F be the implicit equation of a quadric. Then $F \in W_D$ if and only if $F(\varphi)$ is a multiple of $A(t)$.*

Proof. $\mathcal{U} \subseteq W$ if and only if $F(\varphi) = 0$. The other case follows inmediately from Lemma 3.4. □

We are now able to compute points in $\mathcal{U}$ defined on a quadratic extension of $\mathbb{K}$.

Theorem 3.6. *Let $\mathcal{U}$ be a hypercircle of degree $r > 2$. Let $W \in W_D$ be a quadric not containing $\mathcal{U}$, intersecting $\mathcal{U}$ along D and defined over $\mathbb{K}$. Then $W \cap \mathcal{U} = D + [p_1] + [p_2]$ where p_1, p_2 are affine points of $\mathcal{U}$ defined on an extension of $\mathbb{K}$ of degree at most 2.*

Proof. Since W does not contain $\mathcal{U}$, we have by Bezout that $W \cap \mathcal{U}$ is a divisor of degree $2r$ that is defined over $\mathbb{K}$. By construction, this divisor has the form $D + [p_1] + [p_2]$. Now, since W, $\mathcal{U}$ and D are defined over $\mathbb{K}$, then $[p_1] + [p_2]$ is a divisor defined over $\mathbb{K}$. It follows that p_1, p_2 are points defined on an extension of degree at most 2 of $\mathbb{K}$. By Theorem 2.7, the points at infinity of $\mathcal{U}$ are defined over an extension of degree $r > 2$ over $\mathbb{K}$. So p_1 and p_2 are both affine points. □

Hence, we can always compute a point in $\mathcal{U}$ defined over an extension of $\mathbb{K}$ of degree at most 2. If $r = 2$, then $\mathcal{U}$ is a conic and we can compute those points intersecting $\mathcal{U}$ with any hyperplane defined over $\mathbb{K}$ not containing $\mathcal{U}$. If $r > 2$, then compute D from dx_i and a base of W_D defined over $\mathbb{K}$. Next, at least one of the elements W of the base will not contain $\mathcal{U}$. The desired point is one of the intersection points of W and $\mathcal{U}$. In order to continue the journey towards the computation of a birational conic, we have to distinguish two cases. If $\mathbb{K}(\beta)$ is a quadratic extension defining the point p_1, we have to distinguish if $\beta \in \mathbb{K}(\alpha)$ or not. In the case that $\beta \in \mathbb{K}(\alpha)$ we can transform the hypercircle $\mathcal{U}$ into the hypercircle associated with ψ for the extension $\mathbb{K}(\beta) \subseteq \mathbb{K}(\alpha)$ using Theorem 2.9.

Theorem 3.7. *Let $\mathcal{U}$ be a hypercircle with standard parametrization φ. Then, we can compute a unit v such that $\varphi(v)$ has coefficients on an extension of $\mathbb{K}$ of degree at most 2.*

Proof. First, if $r = 1$, then we can easily compute a point p_1 defined over $\mathbb{K}$. If $r = 2$, then $\mathcal{U}$ is a conic. Intersecting $\mathcal{U}$ with a hyperplane defined over $\mathbb{K}$ not containing $\mathcal{U}$ provides an intersection point p_1 defined over an extension of degree at most 2. Let p_1 be one of such intersection points. If $r > 2$, apply Theorem 3.6 to compute a point p_1 on $\mathcal{U}$ defined on an extension of degree at most 2.

If p_1 is defined over $\mathbb{K}$, then we can apply the algorithms in [12] to compute an associated unit v of $\mathcal{U}$. In this case $\varphi(v)$ has coefficients over $\mathbb{K}$.

If p_1 is not defined over $\mathbb{K}$, let $\mathbb{K}(\beta)$ be the field of definition of p_1. This is a degree two extension of $\mathbb{K}$. We distinguish two cases. If $\beta \notin \mathbb{K}(\alpha)$, then $[\mathbb{K}(\alpha,\beta) : \mathbb{K}(\alpha)] = 2$ and $[\mathbb{K}(\alpha,\beta) : \mathbb{K}(\beta)] = n$. It follows that the minimum polynomial of α over $\mathbb{K}(\beta)$ equals the minimum polynomial of α over $\mathbb{K}$. If we compute the α-hypercircle associated with the parametrization φ of $\mathcal{U}$ with respect the extension $\mathbb{K}(\beta) \subseteq \mathbb{K}(\beta,\alpha)$, we obtain, by Theorem 2.10, the very same curve $\mathcal{U}$. But in this case, we have a point p_1 with coefficients in $\mathbb{K}(\beta)$. So, using the algorithms in [12], we can compute a unit v that parametrizes $\mathcal{U}$ over $\mathbb{K}(\beta)$.

Finally, if $\beta \in \mathbb{K}(\alpha)$, apply Theorem 2.9 to compute the standard parameterization φ' of the hypercircle $\mathcal{U}'$ associated with the parametrization φ with respect to the extension $\mathbb{K}(\beta) \subseteq \mathbb{K}(\alpha)$. The image of p_1 by the linear transformation relating φ and φ' is a point $p_1' \in \mathcal{U}'$ with coefficients in $\mathbb{K}(\beta)$. Now, apply the algorithms in [12] to compute a unit v such that $\varphi'(v)$ has coefficients in $\mathbb{K}(\beta)$. By Theorem 2.4, $\varphi(v)$ has coefficients in $\mathbb{K}(\beta)$, as desired. □

Corollary 3.8. *Let $\mathcal{C}$ be a curve defined over $\mathbb{K}$ given by a proper parametrization ψ over $\mathbb{K}(\alpha)$. We can compute a unit v such that $\psi(v)$ has coefficients over an extension $\mathbb{K}(\beta)$ of $\mathbb{K}$ of degree at most 2 and a planar line or conic $\mathbb{K}$-birational to $\mathcal{C}$. We compute at most two birational transformations of $\mathcal{C}$. One mandatory transformation is computing the hypercircle $\mathcal{U}$ and the other, only needed in case $\beta \in \mathbb{K}(\alpha)$, is computing the hypercircle of $\mathcal{C}$ for the extension $\mathbb{K}(\beta) \subseteq \mathbb{K}(\alpha)$, that is, the image of $\mathcal{U}$ under a linear map $\mathbb{P}(\mathbb{F})^n \to \mathbb{P}(\mathbb{F})^{n/2}$ defined over $\mathbb{K}(\beta)$.*

Proof. Let $\mathcal{U}$ be the hypercircle associated with ψ with respect to the extension $\mathbb{K} \subseteq \mathbb{K}(\alpha)$. Let v be the unit computed in Theorem 3.7. Note that, if $\beta \in \mathbb{K}(\alpha)$, in Theorem 3.7 we need to compute the hypercircle of $\mathcal{C}$ for the extension $\mathbb{K}(\beta) \subseteq \mathbb{K}(\alpha)$. v is an associated unit of $\mathcal{U}$, so $\psi(v)$ has coefficients over an extension of degree at most 2 over $\mathbb{K}$.

If $\psi(v)$ has coefficients over $\mathbb{K}$, then we are done. The planar birational curve is $\{y = 0\}$ and the birational morphism is given by $(t, 0) \mapsto \psi(v(t))$. If this is not the case, then $\psi(v)$ will have coefficients over an extension of $\mathbb{K}$ of degree 2. The planar birational conic is the hypercircle associated with the parametrization $\psi(v(t))$ with respect to the extension $\mathbb{K} \subseteq \mathbb{K}(\beta)$. To sum up, given ψ, we can either compute a reparameterization over $\mathbb{K}$ or we can compute the standard parametrization of a $\mathbb{K}$-birational conic. □

Remark 3.9. Assume that $D = a_1[p_1] + \ldots + a_s[p_s]$ is an odd divisor of degree $m > 1$ of the conic $\mathcal{F}$. We can compute S_D to be the set of degree $a = (m + 1)/2$ curves intersecting $\mathcal{F}$ along D in the same way as W_D. S_D is a linear space in $\mathbb{F}^{\binom{a+2}{2}}$. If $C \in S_D$ not containing $\mathcal{F}$, by Bezout, $C \cap \mathcal{F} = D + [q]$. $[q]$ must be a point with coordinates in $\mathbb{K}$. Using this point we can compute a parametrization of $\mathcal{F}$ and an associated unit w. Then $\psi(v(w))$ will be a parametrization of $\mathcal{C}$ with coefficients in $\mathbb{K}$. See [24] for a similar approach to this fact. In particular, we can compute easily an odd divisor if one of the degrees of $\mathcal{C}$, $\mathcal{U}$, or α is odd. Note that, if α is of odd degree over $\mathbb{K}$, then $\mathcal{U}$ is always of odd degree and there is always a computable point with coefficients over $\mathbb{K}$. Using this rational point, we can compute a parametrization of the conic with coefficients over $\mathbb{K}$ and hence a parametrization of $\mathcal{C}$ with coefficients over $\mathbb{K}$.

To sum up, the algorithm used to solve the reparametrization problem we propose is the following:
input: A proper parametrization ψ of a curve $\mathcal{C}$ with coefficients in $\mathbb{K}(\alpha)$.
output: Decide if $\mathcal{C}$ is defined over $\mathbb{K}$. In the affirmative case, return also:

- A linear fraction v such that $\psi(v)$ has coefficients in $\mathbb{K}(\beta)$ with β of degree 1 or 2 over $\mathbb{K}$.
- The standard parametrization of the hypercircle associated with $\psi(v)$ for the extension $\mathbb{K} \subseteq \mathbb{K}(\beta)$, that is, a line or a conic $\mathbb{K}$-birational to $\mathcal{C}$.

If α is of odd degree or $\deg(\mathcal{C})$ is odd, we can guarantee that $\psi(v)$ has coefficients over $\mathbb{K}$ and the $\mathbb{K}$-birational planar curve is a line. Also, if we can decide if a conic has $\mathbb{K}$-rational points, we can compute a reparametrization unit over $\mathbb{K}$.

The steps of the algorithm are:

(1) Compute φ the standard parametrization of the hypercircle $\mathcal{U}$ associated with ψ using the algorithm in [23]. If $\mathcal{C}$ is not defined over $\mathbb{K}$, **return** $\mathcal{C}$ *is not defined over* $\mathbb{K}$.
(2) Take φ_i to be a nonconstant component of φ.
(3) Compute the divisor of zeros D of $dx_i = \varphi_i' dt$.
(4) Compute a basis $\mathcal{B}$ of W_D over $\mathbb{K}$.
(5) Take $W \in \mathcal{B}$ not containing $\mathcal{U}$.
(6) Compute $W \cap \mathcal{U} = D + [p_1] + [p_2]$.
(7) Let $\mathbb{K}(\beta)$ be the field of definition of p_1.
(8) **If** $\beta \in \mathbb{K}$, we have a rational point:
    (a) Compute an associated unit v of $\mathcal{U}$ from p_1 using the algorithms in [12].
    (b) **Return** v and the parametrization $(t, 0)$.
(9) **Else If** $\beta \notin \mathbb{K}(\alpha)$:
    (a) Compute the associated unit v of $\mathcal{U}$ from p_1 using the algorithms in [12].
    (b) Let $\mathcal{F}$ the hypercircle associated with the parametrization $\psi(v)$ for the extension $\mathbb{K}(\alpha) \subseteq \mathbb{K}(\alpha)(\beta)$.
(10) **Else**
    (a) Compute $\mathcal{U}_1$ the hypercircle associated with ψ for the extension $\mathbb{K}(\beta) \subseteq \mathbb{K}(\alpha)$ and its standard parametrization φ' using Theorem 2.9.
    (b) Compute an associated unit v of $\mathcal{U}_1$ and p_1 using the algorithm in [12].
    (c) Compute $\mathcal{F}$ to be the hypercircle associated with $\psi(v)$ for the extension $\mathbb{K} \subseteq \mathbb{K}(\beta)$.
(11) **If** we have an odd divisor D on $\mathcal{F}$ of degree ℓ, or we can decide and compute a point $p \in \mathcal{F} \cap \mathbb{K}^2$:
    (a) Compute the space of curves S_D.
    (b) Take $W \in S_D$ not containing $\mathcal{F}$.
    (c) Compute $W \cap \mathcal{F} = D + [p]$.
    (d) Compute a unit w associated with $\mathcal{F}$ using p.
    (e) **Return** $v \circ w$ and the standard parametrization of $\mathcal{F}$.
(12) **Else** Return v and the standard parametrization of $\mathcal{F}$.

4. Implementation and computational issues

In this section, we detail some computational steps of the method outlined. The main problem in practice is that we are dealing with parametrizations with huge coefficients, so we have to try to keep the coefficients as small as possible. We assume that $\mathbb{K} = \mathbb{Q}$ for the rest of the text. Note that, in this case, we can always decide if the birational conic has rational points or not and compute one [17], [5], [18]. So in this case the result is optimal. If $\mathcal{C}$ can be parametrized over $\mathbb{Q}$ we can always compute such a parametrization. If not, we can compute a parametrization over a quadratic extension $\mathbb{Q}(\beta)$.

4.1. **Computing W_D and a degree 2 rational divisor.** In Section 3 we described the space of quadrics W_D. We show how to compute W_D and an appropriate quadric in W_D. Let $D = a_1[\varphi(t_1)] + \ldots + a_s[\varphi(t_s)]$ be a divisor of degree $2r-2$ and $A(t) = (t-t_1)^{a_1}\cdots(t-t_s)^{a_s}$ as in Corollary 3.5. Let $F = \sum_{i\in I} b_i x_0^{i_0}\cdots x_n^{i_n}$, $I = \{(i_0,\ldots,i_n) | \sum_j i_j = 2\}$ be a quadratic homogeneous polynomial in $n+1$ variables with indeterminate coefficients and $F(\varphi) = \sum_{i\in I} b_i q_0^{i_0}\cdots q_{n-1}^{i_{n-1}} Q^{i_n} \in \mathbb{K}(\alpha)[t]$.

Let $R(t) \in \mathbb{K}(\alpha)[b_i | i \in I][t]$ be the remainder of the division of $F(\varphi)$ by A. Write $R(t) = \sum_{j=0}^{2r-3} l_j t^j$, $l_j \in \mathbb{K}(\alpha)[b_i | i \in I]$, $0 \le j \le 2r-3$. Now, a quadric W is in W_D if and only if the coefficients of its implicit equation are a solution of the linear system $\{l_0,\ldots,l_{2r-3}\}$. Moreover, if $l_j = \sum_{k=0}^{n-1} m_{jk}\alpha^k$, $m_{jk} \in \mathbb{K}[b_i | i \in I]$. Since we know that W_D is defined over $\mathbb{K}$, a quadric W defined over $\mathbb{K}$ is in W_D if and only if the coefficients of its implicit equation are the solution of the set of equations $\{m_{jk} = 0 \mid 0 \le j \le 2r-3, 0 \le k \le n-1\}$. That is,

$$W_D = \{m_{jk} = 0 \mid 0 \le j \le 2r-3, 0 \le k \le n-1\}.$$

Note that there are $n(2r-2)$ polynomials m_{jk}, so they are not linearly independent. In practice, we compute the polynomials m_{jk} from $F(\varphi)$ and A, then we compute a basis of W_D as a vector space in $\mathbb{Q}^{\binom{n+2}{2}}$. We already know that one of the elements of the base will be a quadric not containing $\mathcal{U}$. However, if we take an element of the basis computed, we cannot go much further in our computations due to coefficient explosion. We try in this step to keep the coefficients of the quadric as small as possible. Thus, we compute a basis of the (saturated) lattice $\mathbb{Z}^{\binom{n+2}{2}} \cap W_D$ and, from this basis, an LLL reduced basis. In our experiments there is a big difference between the original basis and the reduced one. In this reduced basis, we will take the smallest vector representing a quadric W not containing $\mathcal{U}$.

Remark 4.1. It is worth noting that, experimentally, for the generic case $r = n$, the LLL basis consists of $\binom{n+2}{2} - 2n + 2$ generators, the first $\binom{n+2}{2} - 2n - 1$ vectors form precisely a basis of the bad space of quadrics containing $\mathcal{U}$ and the last three vectors do not contain $\mathcal{U}$. Hence if we take a quadric passing through D defined over $\mathbb{Q}$ with very small coefficients, it will likely contain the whole hypercircle. So we cannot go too far in our optimization of the size of the coefficients of W.

Let $W \in W_D$ be any quadric not containing $\mathcal{U}$ defined by a polynomial F. This means that $F(\varphi)$ is not identically zero and divisible by the polynomial A defined in Theorem 3.1. Hence the divisor of degree 2, $[p_1] + [p_2]$, defined over $\mathbb{Q}$ in Theorem 3.6 is attained by the roots of $R(t) = F(\varphi)/A$, which is a polynomial of degree 2. The polynomial $f(x) = \mathrm{res}_t(\mathrm{numerator}(\varphi_i(t) - x), R(t))$ is a polynomial of degree 2 whose roots are the i-th coordinates of the pair of points $[p_1] + [p_2]$. We use this information to compute a generator β of the field of the definition of p_1, p_2. If for an index i the coordinates of the divisor are not in $\mathbb{Q}$, then $f(x)$ will be an irreducible polynomial of degree 2 over $\mathbb{Q}$ defining the extension $\mathbb{Q}(\beta)$. We can take β to be the root of the discriminant of f. But usually, it is advisable to take a β that is a squarefree integer. Passing to the square root of an integer is easy, since $\mathbb{Q}(\sqrt{a/b}) = \mathbb{Q}(\sqrt{ab})$. Passing to a squarefree integer is costly, so in practice we will look to partial factorizations of ab, eliminating easy to find square factors, $\mathbb{Q}(\sqrt{ab})$, with ab integer without small square factors.

4.2. **Computing the birational conic.** We saw that we can compute a unit v such that $\psi(v)$ or $\varphi(v)$ is a proper parametrization with coefficients in $\mathbb{K}(\beta)$.

Hence, we can compute a $\mathbb{K}$-birational conic that is just the hypercircle of $\psi(v)$ for the extension $\mathbb{K} \subseteq \mathbb{K}(\beta)$. However, computing the composition $\psi(v)$ can be hard if we have big coefficients. Let us check how can we compute the conic without computing $\psi(v)$, at least if $\beta \notin \mathbb{K}(\alpha)$.

Theorem 4.2. *Let ψ be a proper parametrization of a curve $\mathcal{C}$ with coefficients in $\mathbb{K}(\alpha)$ and $v \in \mathbb{K}(\alpha,\beta)(t)$ a linear fraction such that $\psi(v)$ has coefficients in $\mathbb{K}(\beta)$, β quadratic over $\mathbb{K}$. Assume also that $\beta \notin \mathbb{K}(\alpha)$. Let $\mathcal{F}$ be the conic that is the β-hypercircle of the parametrization $\psi(v)$ for the extension $\mathbb{K} \subseteq \mathbb{K}(\beta)$. Then $\mathcal{F}$ is also the β-hypercircle of the parametrization $v : \mathbb{F} \to \mathbb{F}$ for the extension $\mathbb{K}(\alpha) \subseteq \mathbb{K}(\alpha,\beta)$.*

Proof. Recall from Theorem 2.4 that v is a unit associated with a hypercircle if and only if $\psi(v)$ has coefficients over the ground field. Let w be a unit associated with $\mathcal{F}$. That is, $w \in \mathbb{K}(\beta)(t)$ and $\psi(v(w))$ has coefficients in $\mathbb{K}$. Let $u \in \mathbb{K}(\alpha)(t)$ be a unit such that $\psi(u)$ also has coefficients in $\mathbb{K}$. Then, there is a linear fraction $k \in \mathbb{K}(t)$ such that $v \circ w = u \circ k$. Hence $v \circ w = u \circ k \in \mathbb{K}(\alpha)(t)$. To sum up, w is a unit with coefficients in $\mathbb{K}(\beta) \subsetneq \mathbb{K}(\alpha,\beta)$ and such that $v \circ w$ has coefficients in $\mathbb{K}(\alpha)$. Since β is also quadratic over $\mathbb{K}(\alpha)$, w is a unit associated with the β-hypercircle of $v : \mathbb{F} \to \mathbb{F}$ for the extension $\mathbb{K}(\alpha) \subseteq \mathbb{K}(\alpha,\beta)$. We conclude that $\mathcal{F}$ is the β-hypercircle of the parametrization v for the extension $\mathbb{K}(\alpha) \subseteq \mathbb{K}(\alpha,\beta)$. □

Corollary 4.3. *With the same hypothesis as Theorem 4.2, the β-hypercircle associated with the parametrization $v : \mathbb{F} \to \mathbb{F}$ for the extension $\mathbb{K}(\alpha) \subseteq \mathbb{K}(\alpha,\beta)$ is a line or a conic. Its standard parametrization is defined over $\mathbb{K}(\beta)$. If w is any unit in $\mathbb{K}(\beta)(t)$ such that $v \circ w \in \mathbb{K}(\alpha)(t)$, then $\psi \circ v \circ w$ is a parametrization of $\mathcal{C}$ over $\mathbb{K}$.*

Proof. From Theorem 4.2, we may consider $\mathcal{F}$ either as the β-hypercircle of $\psi \circ v$ for the extension $\mathbb{K} \subseteq \mathbb{K}(\beta)$, or of the parametrization v for the extension $\mathbb{K}(\alpha) \subseteq \mathbb{K}(\alpha)(\beta)$. The standard parametrization ξ of $\mathcal{F}$ is the same in both cases (as it only depends on β), so it has coefficients in $\mathbb{K}(\alpha,\beta) \cap \mathbb{K}(\beta) = \mathbb{K}(\beta)$. Let $w \in \mathbb{K}(\beta)(t)$ be any unit such that $v \circ w \in \mathbb{K}(\alpha)(t)$. Then w is an associated unit of $\mathcal{F}$ interpreted as the β-hypercircle of the parametrization v. Hence, by Theorem 2.7, $\xi \circ w \in \mathbb{K}(\alpha)(t)$. But, both ξ and w are defined over $\mathbb{K}(\beta)$, so $\xi \circ w$ has coefficients in $\mathbb{K}(\alpha) \cap \mathbb{K}(\beta) = \mathbb{K}$. Again, from Theorem 2.7, this means that w is an associated unit of $\mathcal{F}$ intepreted as the β-hypercircle of $\psi \circ v$. Thus, $\psi \circ v \circ w$ have coefficients in $\mathbb{K}$. □

Remark 4.4. The main problem if $\beta \in \mathbb{K}(\alpha)$ is that it may not be possible to write $\mathbb{K}(\alpha) = \mathbb{K}(\alpha,\beta)$ as a field $\mathbb{K}(\alpha) = \mathbb{K}(\gamma)(\beta)$ with β quadratic over $\mathbb{K}(\gamma)$. So we cannot make sense of $\mathcal{F}$ as a hypercircle for an alternative extension. If $\beta \in \mathbb{K}(\alpha)$, we have to compute $\psi(v)$ and then the conic. For instance, let α be a root of $t^6 - 2t^3 - 17$. $\mathbb{Q}(\alpha)$ has only one intermediate field defined by $t^2 - 2t - 17$, this polynomial has discriminant 72. Hence, the intermediate field is $\mathbb{Q}(\sqrt{2})$. Since there are no more nontrivial subfields in $\mathbb{Q}(\alpha)$, we cannot express $\mathbb{Q}(\alpha)$ as $\mathbb{Q}(\gamma)(\sqrt{2})$ with $\sqrt{2} \notin \mathbb{Q}(\gamma)$.

Remark 4.5. Note that computing the hypercircle associated with v for the extension $\mathbb{K}(\alpha) \subseteq \mathbb{K}(\alpha,\beta)$ is fairly easy following Theorem 2.7.7. By our computations, we always choose a β of the form $\sqrt{d}$, so its conjugate is $\overline{\beta} = -\beta$. Let $v(\beta)$ be the input linear fraction and $v(-\beta)$ its conjugate. Let $u(t) = v(-\beta)^{-1} \circ v(\beta)$. Then,

the standard parametrization ξ_0, ξ_1 of $\mathcal{F}$ verifies that $\xi_0 + \beta\xi_1 = t$, $\xi_0 - \beta\xi_1 = u(t)$. Thus,

$$\xi(t) = \left(\frac{t + u(t)}{2}, \frac{t - u(t)}{2\beta}\right).$$

4.3. **Computing the rational point in the conic.** If $\mathcal{C}$ is of odd degree or α is of odd degree, we can define an odd divisor in the conic as follows. Let $\xi = (\xi_0, \xi_1)$ be the standard parametrization of $\mathcal{F}$. For almost all $t \in \mathbb{K}$, $\psi(t)$ has coefficients in $\mathbb{K}(\alpha)$ and define an odd divisor of $\mathcal{C}$ of degree n. Write $t = v(s)$ for a generic t, $s = v^{-1}(t)$ is such that $\psi(v(s))$ defines a point with coefficients in $\mathbb{K}(\alpha)$. Passing to the conic, $\xi(s) = \xi(v^{-1})(t)$ will have coefficients in $\mathbb{K}(\alpha)$ for almost all $t \in \mathbb{K}$. If $\mathcal{C}$ is of odd degree and α is even, cut $\mathcal{C}$ with a random hyperplane defined over $\mathbb{K}$. This intersection will define an odd divisor defined over $\mathbb{K}$. Compute the parameters $t_1, \ldots, t_m$ such that $\prod_{i=1}^{m}(t - t_i) \in \mathbb{K}(\alpha)[t]$ corresponds with this odd divisor via ψ. Then $v^{-1}(t_1), \ldots, v^{-1}(t_m)$ defines an odd divisor, via ξ, in $\mathcal{F}$, defined over $\mathbb{K}$. Note that $\prod_{i=1}^{m}(t - v^{-1}(t_i))$ can be computed using resultants.

4.4. **Simplifying the solution.** Assume now that we have performed all the computations as outlined and we have obtained a linear fraction $u(t)$ such that $\psi(u(t))$ has coefficients over $\mathbb{Q}$. The problem we may face is that, if u has big coefficients and ψ has high degree, then $\psi(u)$ will most likely have huge coefficients. It is an interesting open problem to provide algorithms to compute a linear fraction u_1 such that $\psi(u_1(t))$ has small, rational coefficients. We know that u_1 must be of the form $u \circ k$, with $k \in \mathbb{Q}(t)$. In this subsection we present a strategy to compute a linear fraction k such that $u(k)$ has small coefficients. This will not solve the original problem, but, heuristically, if the coefficients of u are not too big, there should not be a coefficient explosion in $\psi(u)$. Let $u = \frac{at+b}{ct+d} \in \mathbb{Q}(\alpha)(t)$, $a = \sum_{i=0}^{n-1} a_i\alpha^i$, $b = \sum_{i=0}^{n-1} b_i\alpha^i$, $c = \sum_{i=0}^{n-1} c_i\alpha^i$, $d = \sum_{i=0}^{n-1} d_i\alpha^i$. By multiplying and dividing by suitable integers, we may assume that $a_i, b_i, c_i, d_i \in \mathbb{Z}$, $0 \le i \le n-1$, and $\gcd(a_0, \ldots, a_{n-1}, b_0, \ldots, d_{n-1}) = 1$. Let $k = \frac{k_1t+k_2}{k_3t+k_4}$. Let $v = u \circ k = \frac{et+f}{gt+h}$, $e = \sum_{i=0}^{n-1} e_i\alpha^i$, $f = \sum_{i=0}^{n-1} f_i\alpha^i$, $g = \sum_{i=0}^{n-1} g_i\alpha^i$, $h = \sum_{i=0}^{n-1} h_i\alpha^i$. Then

$$\begin{pmatrix} e_0 & \ldots & e_{n-1} & f_0 & \ldots & f_{n-1} \\ g_0 & \ldots & g_{n-1} & h_0 & \ldots & h_{n-1} \end{pmatrix} = \begin{pmatrix} a_0 & \ldots & a_{n-1} & b_0 & \ldots & b_{n-1} \\ c_0 & \ldots & c_{n-1} & d_0 & \ldots & d_{n-1} \end{pmatrix} \cdot \begin{pmatrix} k_1 & k_2 \\ k_3 & k_4 \end{pmatrix},$$

$(e, g) = k_1(a, c) + k_3(b, d)$, $(f, g) = k_2(a, c) + k_4(b, d)$. One possibility to compute a linear fraction of the form $u \circ k$ is to take the two-dimensional lattice $\langle (a_0, \ldots, a_{n-1}, c_0, \ldots, c_{n-1}), (b_0, \ldots, b_{n-1}, d_0, \ldots, d_{n-1}) \rangle \subset \mathbb{Z}^{2n}$ and compute a reduced basis, $\{(e_0, \ldots, e_{n-1}, g_0, \ldots, g_{n-1}), (f_0, \ldots, f_{n-1}, h_0, \ldots, h_{n-1})\}$. From this basis we recover an associated unit u_1 with small coefficients. In our experiments, computing $\psi(u)$ may be infeasible, while computing $\psi(u_1)$ is reasonable.

5. Examples

Example 5.1. Consider the following simple example with a flavor of Computer Aided Geometric Design. Take the parabola $y = x^2$. A usual construction in CAGD is computing the offset of a given curve. The offset of the parabola at distance d is the envelope of circles or radius d centered on the parabola. Which is also the set of points at normal distance d from the parabola. The nonproper parametrization

$$\left(\frac{t^2 - 16}{16t}, \frac{(t^2 - 16)^2}{256t^2}\right)$$

of the parabola has a rational normal unit vector $n = \left(\frac{-t^2+16}{t^2+16}, \frac{8t}{t^2+16}\right)$.

A proper parametrization of the offset of the parabola at distance d is:

$$\psi_d = \left(\frac{t^2-16}{16t} + d\frac{-t^2+16}{t^2+16}, \frac{t^4-32t^2+256}{256t^2} + d\frac{8t}{t^2+16}\right).$$

Now let $\mathcal{C}$ be the offset of the parabola passing through the point $(0,3)$. The closest point in the parabola to $(0,3)$ is the point $(1,1)$ and the distance is $\sqrt{5}$. A proper parametrization of $\mathcal{C}$ is

$$\psi = \left(\frac{t^2-16}{16t} + \sqrt{5}\frac{-t^2+16}{t^2+16}, \frac{t^4-32t^2+256}{256t^2} + \sqrt{5}\frac{8t}{t^2+16}\right).$$

We now apply the hypercircle method and get that the standard parametrization of the hypercircle associated with ψ is $\varphi = \left(\frac{\frac{1}{2}t^2-8}{t}, \frac{\frac{1}{10}\sqrt{5}t^2+\frac{8}{5}\sqrt{5}}{t}\right)$, which is the conic of the implicit equation $x^2 - 5y^2 + 16 = 0$.

So $\mathcal{C}$ is defined over $\mathbb{Q}$. Moreover, note that, by construction, $(0,3) \in \mathcal{C}$. We can use this point as odd divisor and obtain the associated unit of the hypercircle. The computation gives $u(t) = \frac{(4\sqrt{5}+8)t-4\sqrt{5}-12}{t+\sqrt{5}+1}$.

Finally,

$$\psi(u) = \left(\frac{-t^4-3t^3+27t^2-36t+10}{t^4-6t^2+12t-8}, \frac{(t^2-1)(2t^4-2t^3+27t^2-82t+62)}{t^6+2t^5-10t^4+40t^2-64t+32}\right)$$

is a parametrization over $\mathbb{Q}$ of $\mathcal{C}$.

Example 5.2. Here, we present a randomly generated example. We take the algebraic element α to be a root of $x^3 - 2x + 3$.

Let $\mathcal{C}$ be the curve with rational parametrization

$$\psi_{\mathbb{Q}} = \left(\frac{\frac{2}{171}x^{10} - x^8 - \frac{1}{6}x^7 + \frac{1}{4}x^5 - \frac{1}{6}x^4 + x^3 + x^2 + \frac{1}{3}x - 2}{-x^{10} + 2x^8 + \frac{1}{5}x^7 - x^6 - x^5 - 3x^4 + 107x}, \right.$$
$$\left. \frac{-x^{10} + \frac{5}{13}x^7 - 490x^5 + 16x^4 + \frac{6}{37}x^2 + 5}{-x^{10} + 2x^8 + \frac{1}{5}x^7 - x^6 - x^5 - 3x^4 + 107x}\right).$$

We start with the parametrization $\psi = \psi_{\mathbb{Q}}(u)$, where

$$u = \frac{(13\alpha^2 + 41\alpha + 35)t + 59\alpha^2 + 88\alpha + 39}{t + 47\alpha^2 + 17\alpha + 79}.$$

ψ is a birational parametrization with coefficients in $\mathbb{Q}(\alpha)$ that we do not reproduce here due to space constraints, ψ is the parametrization of a curve of degree 10 in the plane whose coefficients are of the form $c_0+c_1\alpha+c_2\alpha^2$, with $c_i \sim 2^{75}$. So we are dealing with an example that has no small coefficients. We compute the standard parametrization φ of the associated hypercircle $\mathcal{U}$ using the method of moving hyperplanes in [23]. φ has the standard parametrization: $(61654(16\alpha^2+36\alpha+49)t^3 + (650780235\alpha^2 + 199608197\alpha - 867706980)t^2 + (-11698757039\alpha^2 - 56561111034\alpha + 56981476123)t - 120067895802\alpha^2 + 107542043663\alpha - 36385848735)/D$,
$((-1664658\alpha^2-493232\alpha+2219544)t^3+(-67094856\alpha^2+575620560\alpha+89459808)t^2+ (12412548180\alpha^2+62664529350\alpha-64337524434)t+6426002048\alpha^2+130251703893\alpha- 170095553155)/D$,
$((-739848\alpha^2 - 1664658\alpha + 986464)t^3 + (66492657\alpha^2 - 266027709\alpha - 88656876)t^2 + (-6956873685\alpha^2-33137522622\alpha+34086297597)t-28936913994\alpha^2-18554618293\alpha+ 47690019897)/D$, where $D = t^2+(1270729233/13008994\alpha^2-288327548/6504497\alpha+$

131660715/13008994)t+35569161269/6504497α^2−141477963297/13008994α+1191 56399449/13008994. $\mathcal{U}$ is a curve of degree 3 in $\mathbb{F}^3$.

The divisor of zeros of dx_0 corresponds, via the standard parameterization, to the parameters that are roots of the polynomial: 2406169548228t^4+(470073240788292α^2−213318559732704α+48704458335660)t^3+ (95935700146598127α^2−157107893974743062α+83526919601681007)t^2+(1263978 6813312905308α^2−239047739574437528 46α+204455858524139404 62)t+742291603 049776565874α^2−139810335039351326 3890α+115534681781390640 2052. Now, we compute the space of quadrics in three space that passes to these points in the hypercircle. An LLL-reduced basis of this space of quadrics is:

$$\begin{pmatrix} 110 & 102 & -102 & 225 & 322 & 330 & 702 & -338 & 543 & 374 \\ 179 & 152 & -165 & 1130 & 523 & 537 & 183 & -590 & -2258 & 725 \\ 330 & 319 & -347 & -1031 & 1007 & 990 & -5 & -1057 & 557 & -2011 \\ 1348 & 1376 & -1596 & 3440 & -890 & -5592 & 2100 & -3515 & 625 & -3830 \\ 1280 & 1320 & -1604 & -5893 & 844 & -2256 & -3998 & -3701 & 1143 & 5605 \\ 697 & 951 & -379 & 10061 & 3660 & 3996 & -12931 & -2070 & 7185 & 384 \end{pmatrix}.$$

Regarding this basis, the first three generators form a basis of the space of quadrics that contain the hypercircle, so we take the fourth equation. This corresponds with the quadric in three space with the projective implicit equation: $1348W_0^2 + 1376W_0W_1 - 1596W_0W_2 + 3440W_0W_3 - 890W_1W_1 - 5592W_1W_2 + 2100W_1W_3 - 3515W_2^2 + 625W_2W_3 - 3830W_3^2$. If we intersect this quadric with the hypercircle, we get our four points from the divisor plus two other points that correspond with the parameters that are the roots of $5289963t^2 + (15252170\alpha^2 - 21222015\alpha + 38892330)t - 471156309\alpha^2 + 907148780\alpha - 743730576$. These parameters correspond to the points:

$$\left(\frac{4059}{1763321}\beta - \frac{6482055}{1763321}, -\frac{25183}{10579926}\beta + \frac{7074005}{3526642}, \frac{321}{251903}\beta - \frac{7626085}{5289963}\right)$$

and its conjugate, where $\beta = \sqrt{7296701}$. It happens that $\beta \notin \mathbb{K}(\alpha)$ which is the generic case. Now, we use the method in [12] to compute a unit that reparametrizes $\mathcal{C}$ and the hypercircle over $\mathbb{K}(\beta)$. The unit obtained is: v = (((321/251903β − 7626085/5289963)α^2+(−25183/10579926β+7074005/3526642)α+4059/1763321β− 6482055/1763321)t + (32368498208832185119/10579926β + 15129427928014217047 9/10579926)α^2 + (−60500076187993431799/10579926β − 26747281652102646049 1/1511418)α + 2765293860090586323/503806β − 95154528307068425296 23/352664 2)/(t+(147176658712632/251903β−3870833163155746065/251903)α^2+(−3871292 82397317/251903β+8462057680983061884/251903)α–196235544950176/251903β+ 627512849909690167082/251903).

We now compute the birational conic, that in this case is the hypercircle associated with the parametrization $v : \mathbb{F} \to \mathbb{F}$. This conic is the conic $\mathcal{F} = Y_0^2 - 7296701Y_1^2 + 1202903341306750426927/251903Y_0Y_2 - 6874188924189704841236 21/251903Y_1Y_2 + 1433115394536581115533926889597706022/251903Y_2^2$, that is, a β-hypercircle with standard parametrization: ((1/2t^2+6874188924189704841236 21/3676121744006βt−7165576972682905577669 6344479885 3011/251903)/(t + 6874188924189704841236 21/3676121744006β + 120 2903341306750426927/503806), (1/14593402βt^2+1202903341306750426927/367612 1744006βt+7165576972682905577669634447988530 11/1838060872003β)/(t+68741 889241897048412362 1/3676121744006β + 120290334130675042692 7/503806)).

Since α is of odd degree over $\mathbb{Q}$, we can use this information to compute odd degree divisors on the conic defined over $\mathbb{Q}$. The standard parametrization of $\mathcal{F}$ applied to $v^{-1}(0)$ gives the point:
$(-92717241963296367543963426555525/70792854026359559 8\alpha^2 + 85782720638536526613210223622769/70792854026359598\alpha - 77840381063674000943949119468289595/353964270131797799, -43292690061037624628891501283/70792854026359598\alpha^2+65527786400859002371365755163/70792854026359598\alpha-19591512156121218838380642686/353964270131797799)$, that is, a point in the conic of degree 3 over $\mathbb{Q}$. So, we look for curves of degree $(3+1)/2 = 2$ that pass through this point and its conjugates over $\mathbb{Q}$.

The space of conics that pass through the previous point and its conjugates has an LLL reduced basis composed by three conics. In this case, we take the first vector in the reduced basis, that is, the conic:
$1285236343279687612 3Y_0^2 - 64797499881226258696832Y_0Y_1 + 290823925399272555908607931Y_1^2 + 28403727338255796921549681969143424Y_0Y_2 + 51124766122063827278107816973336 7Y_1Y_2 + 31492510276432154508753366362588484Y_2^2$.

If we intersect this conic with $\mathcal{F}$, we get that the fourth intersection point is attained by the parameter $-10763040570013453663551088/22873858705399\beta - 41215750871253947543245714978/22873858705399$. If we plug this parameter into the standard parametrization, we get the rational point in the conic $\mathcal{F}$:

$$(-41215750871253947543245714978/22873858705399,$$
$$-10763040570013453663551088/22873858705399).$$

From this point, we compute an associated unit of the conic:
$w = ((19468474498232646247379/112745485225\beta - 3635522916773478233169631 96/112745485225)t + 356837163448559925859/9019638818\beta - 6497551861500133832515435/9019638818)/(t-1/1790300\beta+401199/1790300)$. We know that the linear fraction $v \circ w$ reparametrizes $\mathcal{C}$ over $\mathbb{Q}$. But if we write $v \circ w$ with monic denominator, then the coefficients involve numbers of the form $c_0+\alpha c_1+\alpha^2 c_2$, where $c_i = a/b$ and $a, b > 2^{140}$. If we simplify this unit using again LLL as in subsection 4.4, we get the reparametrization unit:
$u_1 = ((3243332478959\alpha^2-69617833234861\alpha-87203854258100)t-4493615445562\alpha^2 -35007060177512\alpha-71547744855792)/(942610188815 78t+28333704896\alpha^2-61084110185\alpha + 64478276179717)$ where the integers involved are bounded by 2^{38}.

Note that the unit u_1 is different from u^{-1}, which is also an associated unit. What we know is that we will obtain a unit of the form $u^{-1} \circ k$ with $k \in \mathbb{Q}(t)$. But it is impossible to develop an algorithm that returns u^{-1}, since the input is $\psi_{\mathbb{Q}} \circ u$. In this example $k = (3620968t+2379081)/(9063369t+6193880)$, which is relatively small compared to the coefficients we are dealing with in ψ.

These computations have been performed with a specific library devoted to hypercircles [21] implemented on a modified version of the SAGE CAS [19]. See Table 1 for the running time in several examples of odd degree extensions, the input is the parametrization ψ of a planar curve $\mathcal{C}$ of degree $\deg(\mathcal{C})$ and a random extension $\mathbb{Q}(\alpha)$, α of degree n. Then we compute, φ the standard parametrization of the associated hypercircle, $[p_1] + [p_2]$ a degree two divisor of $\mathcal{U}$ defined over $\mathbb{Q}$. A unit v such that $\psi(v)$ has coefficients over a quadratic extension $\mathbb{Q}(\sqrt{d})$, the birational conic $\mathcal{F}$, a unit w associated with $\mathcal{F}$ and a simplification of $v \circ w$ in the sense of Subsection 4.4. To make a comparison with other approaches, in the last

TABLE 1. Running time of different components of the algorithm

$\deg(\mathcal{C}), n$	φ	$[p]$, v, $\mathcal{F}$	w, u	total	implicit.+param.
5,3	0.28	0.54	0.20	1.01	0.94
10,3	0.59	0.53	0.20	1.33	>600
5,5	1.32	2.59	1.44	5.35	2.66
10,5	3.61	3.43	2.12	9.16	>600
5,7	26.49	34.62	157.17	218.27	10.77
10,7	35.74	29.92	123.17	188.83	> 600

column, we show the time taken by Singular [6] over the same input to compute the implicit equation of $\mathcal{C}$ using resultants and compute a parametrization of $\mathcal{C}$ using the library *paraplanecurves.lib*. The computations are done on an intel 64bits processor, 2.6GHz (in seconds). We can appreciate that the method presented here is especially useful for high degree curves with a relatively small algebraic extension.

ACKNOWLEDGEMENTS

The author wants to thank Tomas Recio, Rafael Sendra and Carlos Villarino for useful discussions. The author also thanks the anonymous referee for many suggestions on improving the text.

REFERENCES

[1] C. Andradas, T. Recio, and J. R. Sendra, *A relatively optimal rational space curve reparametrization algorithm through canonical divisors*, Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation (Kihei, HI) (New York), ACM, 1997, pp. 349–355. MR1810004

[2] C. Andradas, T. Recio, and J. R. Sendra, *Base field restriction techniques for parametric curves*, Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation (Vancouver, BC), ACM, New York, 1999, pp. 17–22, DOI 10.1145/309831.309845. MR1802062

[3] C. Andradas, T. Recio, J. R. Sendra, and L. F. Tabera, *On the simplification of the coefficients of a parametrization*, J. Symbolic Comput. **44** (2009), no. 2, 192–210, DOI 10.1016/j.jsc.2008.09.001. MR2479298

[4] C. Chevalley, *Introduction to the Theory of Algebraic Functions of One Variable*, Mathematical Surveys, No. VI, American Mathematical Society, New York, NY, 1951. MR0042164

[5] J. E. Cremona and D. Rusin, *Efficient solution of rational conics*, Math. Comp. **72** (2003), no. 243, 1417–1441, DOI 10.1090/S0025-5718-02-01480-1. MR1972744

[6] W. Decker, G.-M. Greuel, G. Pfister, and H. Schönemann, SINGULAR *3-1-5 – A computer algebra system for polynomial computations*, (2012), http://www.singular.uni-kl.de.

[7] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52. MR0463157

[8] D. Hilbert and A. Hurwitz, *Über die diophantischen Gleichungen vom Geschlecht Null* (German), Acta Math. **14** (1890), no. 1, 217–224, DOI 10.1007/BF02413323. MR1554798

[9] T. Recio, J. R. Sendra, L. F. Tabera, and C. Villarino, *Generalizing circles over algebraic extensions*, Math. Comp. **79** (2010), no. 270, 1067–1089, DOI 10.1090/S0025-5718-09-02284-4. MR2600556

[10] T. Recio and J. R. Sendra, *Real reparametrizations of real curves*, J. Symbolic Comput. **23** (1997), no. 2-3, 241–254, DOI 10.1006/jsco.1996.0086. MR1448697

[11] T. Recio, J. R. Sendra, L. F. Tabera, and C. Villarino, *Fast computation of the implicit ideal of a hypercircle*, Actas de AGGM 2006, 2006, pp. 258–265.

[12] T. Recio, J. R. Sendra, L. F. Tabera, and C. Villarino, *Algorithmic detection of hypercircles*, Math. Comput. Simulation **82** (2011), no. 1, 54–67, DOI 10.1016/j.matcom.2010.07.017. MR2846415

[13] T. Recio, J. R. Sendra, and C. Villarino, *From hypercircles to units*, ISSAC 2004, ACM, New York, 2004, pp. 258–265, DOI 10.1145/1005285.1005323. MR2126952

[14] J. R. Sendra and C. Villarino, *Optimal reparametrization of polynomial algebraic curves*, Internat. J. Comput. Geom. Appl. **11** (2001), no. 4, 439–453, DOI 10.1142/S0218195901000572. MR1852578

[15] J. R. Sendra and C. Villarino, *Algebraically optimal parametrizations of quasi-polynomial algebraic curves*, J. Algebra Appl. **1** (2002), no. 1, 51–74, DOI 10.1142/S0219498802000045. MR1907738

[16] J. R. Sendra and F. Winkler, *Parametrization of algebraic curves over optimal field extensions*, J. Symbolic Comput. **23** (1997), no. 2-3, 191–207, DOI 10.1006/jsco.1996.0083. Parametric algebraic curves and applications (Albuquerque, NM, 1995). MR1448694

[17] J. R. Sendra, F. Winkler, and S. Pérez-Díaz, *Rational Algebraic Curves*: *A Computer Algebra Approach*, Algorithms and Computation in Mathematics, vol. 22, Springer, Berlin, 2008. MR2361646

[18] D. Simon, *Solving quadratic equations using reduced unimodular quadratic forms*, Math. Comp. **74** (2005), no. 251, 1531–1543, DOI 10.1090/S0025-5718-05-01729-1. MR2137016

[19] W. A. Stein et al., *Sage Mathematics Software (Version 6.1.1)*, The Sage Development Team, 2011, `http://www.sagemath.org`.

[20] L. F. Tabera, *Two tools in algebraic geometry: Construction of configurations in tropical geometry and hypercircles for the simplification of parametric curves*, Ph.D. thesis, Universidad de Cantabria, Université de Rennes I, 2007.

[21] L. F. Tabera, *Implementation of a hypercircle library in the sage cas*, (2011), `http://personales.unican.es/taberalf/hypercircles`.

[22] L. F. Tabera, *Optimal affine reparametrization of rational curves*, J. Symbolic Comput. **46** (2011), no. 8, 967–976, DOI 10.1016/j.jsc.2011.04.001. MR2811050

[23] L. F. Tabera, *Computing hypercircles by moving hyperplanes*, J. Symbolic Comput. **50** (2013), 450–464, DOI 10.1016/j.jsc.2012.09.001. MR2996890

[24] M. van Hoeij, *Rational parametrizations of algebraic curves using a canonical divisor*, J. Symbolic Comput. **23** (1997), no. 2-3, 209–227, DOI 10.1006/jsco.1996.0084. MR1448695

[25] C. Villarino, *Algoritmos de optimalidad algebraica y de cuasi-polinomialidad para curvas racionales*, Ph.D. thesis, Universidad de Alcalá, 2007.

Departamento de Matemáticas Estadística y Computación, Universidad de Cantabria, 39071, Santander, Spain

E-mail address: `taberalf@unican.es`