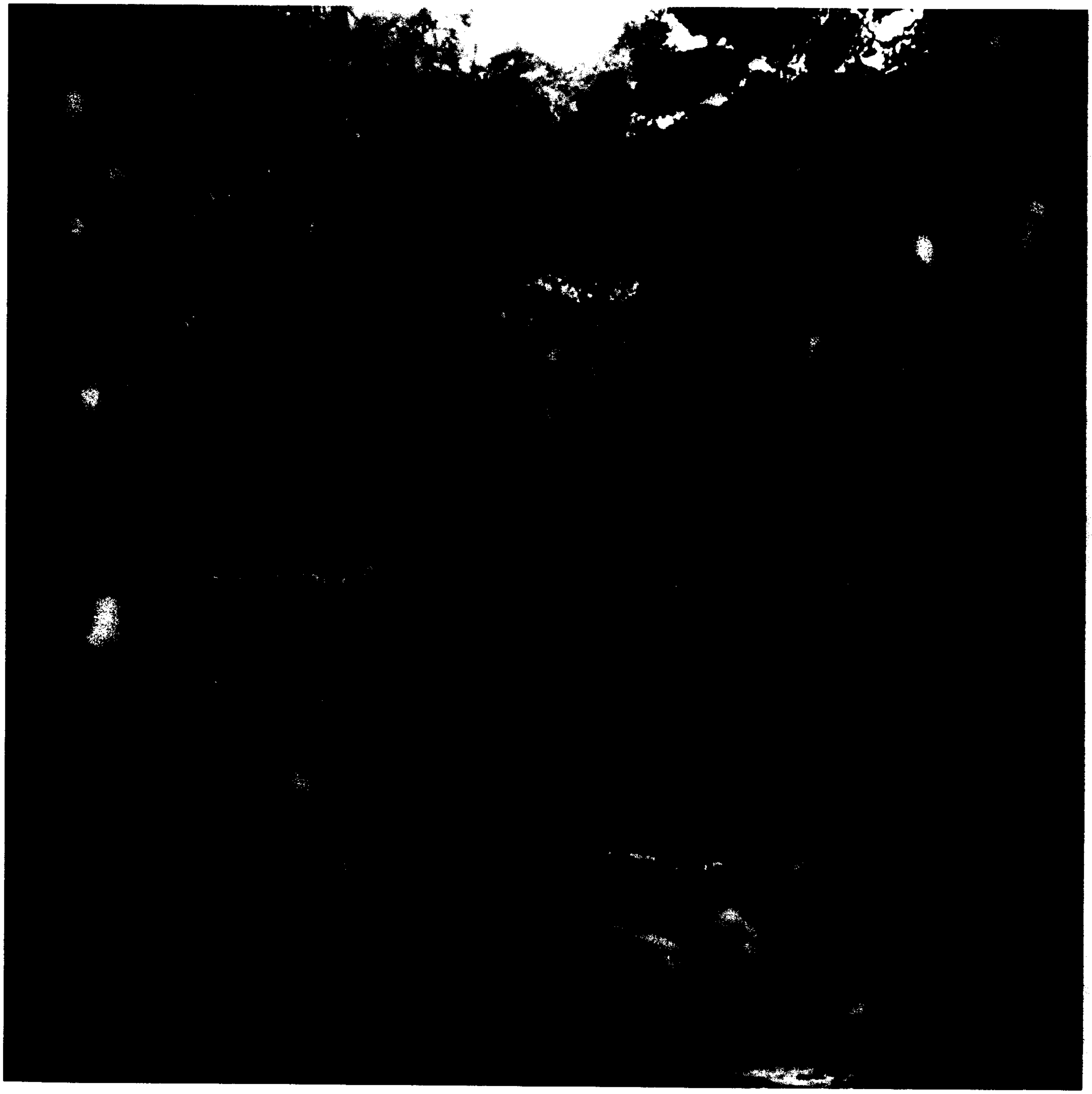
ISSAC 97

July 21–23, 1997 • Maui, Hawaii, USA



Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation

PRESS

Table of Contents

Algorithms I *Monday, July 21, 8:00-9:30*
(Session Chair: Richard Fateman, U. California at Berkeley, USA)

Algorithm Analysis & Complexity I *Monday, July 21, 9:45-11:15*
(Session Chair: George Labahn, U. Waterloo, Canada)

Applications I *Monday, July 21, 14:00-15:00*
(Session Chair: Todd Torgersen, Wake Forest U., USA)

Polynomial Algorithms I *Monday, July 21, 16:00-17:00*
(Session Chair: Liu Zhuojun, Academia Sinica, PRC)

Algorithms II *Tuesday, July 22, 8:00-9:30*
(Session Chair: Eugene V. Zima, Moscow U., Russia)

Systems of Equations *Tuesday, July 22, 10:15-11:45*
(Session Chair: Bruno Buchberger, RISC/Linz, Austria)

Differential Equations I *Tuesday, July 22, 10:15-11:45*
(Session Chair: Jacques Calmet, U. Karlsruhe, Germany)

Algorithm Analysis & Complexity II *Tuesday, July 22, 14:00-15:00*
(Session Chair: Y.N. Lakshman, Drexel U., USA)

Applications II *Tuesday, July 22, 14:00-15:00*
(Session Chair: Kazuhiro Yokoyama, Fujitsu Labs, Japan)

Polynomial Algorithms II *Tuesday, July 22, 16:00-17:00*
(Session Chair: Keith Geddes, U. Waterloo, Canada)

Systems I *Tuesday, July 22, 16:00-17:00*
(Session Chair: Matu-Tarow Noda, Ehime U., Japan)

Polynomial Algorithms III *Wednesday, July 23, 8:00-9:30*
(Session Chair: George Collins, U. Delaware, USA)

Differential Equations II *Wednesday, July 23, 8:00-9:30*
(Session Chair: Bob Caviness, U. Delaware, USA)

Algorithms III *Wednesday, July 23, 10:00-11:30*
(Session Chair: Robert Corless, U. Western Ontario, Canada)

Geometry *Wednesday, July 23, 10:00-11:30*
(Session Chair: Vilmar Trevisan, UFRGS, Brazil)

Systems II *Wednesday, July 23, 15:00-16:00*
(Session Chair: Michael Monagan, Simon Fraser U., Canada)

Applications III *Wednesday, July 23, 15:00-16:00*
(Session Chair: Arjeh M. Cohen, RIACA, The Netherlands)

A Relatively Optimal Rational Space Curve Reparametrization Algorithm Through Canonical Divisors *

Carlos Andradas
Departamento de Algebra
Universidad Complutense
E-28080 Madrid, Spain
andradas@matss2.mat.ucm.es

Tomás Recio
Departamento de Matemáticas
Universidad de Cantabria
E-39071 Santander, Spain
recio@matesco.unican.es

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

Abstract

Let $\mathbb{K}$ be a given computable field of characteristic zero and let $\mathbb{L}$ be a finite field extension of $\mathbb{K}$, with algebraic closure $\mathbb{F}$. Assume a rational parametrization $\mathcal{P}(t) \in \mathbb{L}(t)^n$ of some irreducible curve $\mathcal{C}$ in the affine n-space over $\mathbf{F}$ is also given. In this paper we will show, first, how to decide -without implicitization algorithms- whether the given curve $\mathcal{C}$ is definable (by a set of equations with coefficients) over $\mathbf{K}$; and, if this is the case, we will determine -without computing the implicit equation set and then using parametrization techniques- a reparametrization of $\mathcal{P}(t)$ over the smallest possible field extension of $\mathbb{K}$; that is, over a field extension of $\mathbb{K}$ of degree at most two.

1 Introduction

Rational curves play an important role in the field of Computer Aided Geometric Design. They arise in practical applications such as computer graphics, geometric modeling or in the manipulation of offset varieties. As a consequence, in the past years different algorithms have been developed in order to perform various computations over parametric varieties; we refer the reader, for instance, to a recent special issue of the Journal of Symbolic Computation [4].

In particular, several authors have addressed the problem of computing *good* parametrizations of rational curves. In some of these works *good* is interpreted as a quality of the maximum degree (that of being the smallest possible one) of the polynomials involved in a collection of rational functions parametrizing the variety; while, in some other papers, *good* means that the coefficients of such functions lie on a small algebraic extension of some given field. For instance, (t^2, t^4) would be an example of a bad -in the first sense- parametrization of parabola $y - x^2 = 0$, but it is good in the other sense, since it involves just rational coefficients; and $(it, -t^2)$) is a case of a bad (in the second sense) parametrization of the same variety, but also of a good one in the first sense, since it is of maximum degree two.

A further dichotomy appears between authors that achieve good parametrizations by taking as starting point a set of implicit equations for the parametric variety, and those that consider any given parametrization as their basic input. For example, *proper* parametrizations (i.e. parametrizations with optimal degree) are directly output in most parametrization algorithms (i.e. algorithms that yield a set of parametric equations from the implicit ones); see [5],[11]. Moreover, *reparametrization* methods (i.e. the conversion of a given parametrization into a better one by means of an algorithm entirely performing inside some subfield of $\mathbf{F}(t)$ and avoiding implicitization) that yield proper parametrizations for improperly parametrized curves are also available, for instance, in [2],[10].

In [12],[6] algorithmic solutions (via adjoint curves and canonical divisors, respectively) to the so called *"optimal parametrization problem"* (i.e. procedures determining parametrizations over the smallest possible field extension of the ground field) are presented for plane curves, but in both cases involving manipulation of the implicit equations, since their primary goal is to parametrize and, just as an extra, to do it in an optimal way. Also in both methods, a birational map over the ground field (i.e. an "a priori" determined field containing the coefficients of a defining monic polynomial of the plane curve) that maps the original curve onto a conic is found. In this way the parametrization problem is reduced to curves of degree two. Therefore, a parametrization of the given curve over a ground field extension of degree at most two is finally obtained.

As remarked above, both approaches assume that the curve is given implicitly: in fact, even the formulation of the problem they deal with appeals to a certain ground field of coefficients of the implicit equations. Apparently there is no way in these works to take advantage of knowing in advance some set of parametric equations of the curve. However, in many applications, algebraic varieties are directly presented in parametric form, although not necessarily in an optimal one. Furthermore, parametrization procedures of implicitly given varieties are quite expensive in terms of complexity (see [8]). Hence, if a parametrization is already known, finding an optimal one (or merely testing if the given one is already optimal) by implicitizing and then parametrizing again by the methods in [12] and [6] seems not an effi-

*All three authors supported by HCM:"SAC"; first author supported by DGES PB 95-0354 and EC contract CHRX-CT94-0506; second author supported by ESPRIT-IV:"FRISCO" and HCM:"SAC"; third author supported by HCM"SAC" and DGICYT PB 95-0563: "Sistemas de Ecuaciones Algebraicas: Resolución y Aplicaciones" and UAH-Proy. E010/97:"Algoritmos y aplicaciones de las variedades paramétricas en diseño geométrico".

cient solution; and, in any case, not an aesthetically pleasant one. Thus we feel that this issue needs to be reconsidered once more, but this time entirely within the parametric point of view, i.e. considering an optimal (*reparametrization*) method. An algorithmic solution to a version of this problem, for the particular case when a parametrization is given over $\mathbf{Q}(i)$, is presented in [9]: first, by computing some *gcd* it is checked whether the curve admits a parametrization over $\mathbf{R}$, and in that case, a parametrization over $\mathbf{Q}$ or over a degree two extension of $\mathbf{Q} \subset \mathbf{R}$ is found, in time quadratic on the degree of the given parametrization.

More precisely, the *relatively optimal reparametrization problem* can be stated as follows: Let $\mathbb{K}$ be a computable field of characteristic zero, $\mathbf{L}$ a finite field extension of $\mathbf{K}$, $\mathbb{F}$ its algebraic clousure (therefore also the closure of $\mathbf{K}$), and let $\mathcal{C}$ be the rational space curve over $\mathbf{F}$ given by the parametrization $\mathcal{P}(t) \in \mathbb{L}(t)^n$. In this setting we want, first, to decide whether $\mathbb{K} \subset \mathbb{K}(\mathcal{P}(t))$ is a regular field extension [13]. This is an indirect way to check (see section 2, Theorem 2), whether the given curve is implicitly defined by a set of equations with coefficients in $\mathbb{K}$; otherwise, it is clear that the curve has not a parametrization over $\mathbf{K}$. Then, in the affirmative case, we want to determine -without implicitizing and parametrizing again- a reparametrization of $\mathcal{P}(t)$ over the smallest possible field extension of $\mathbb{K}$; that is, over a field extension of $\mathbb{K}$ of degree at most two. Having found a good, in this sense, parametrization, it is straight-forward to see that it can be guaranteed, also, to be a proper one. Since, as mentioned above, the proper reparametrization problem is well solved over any characteristic zero field, we do not include any further comments on this aspect; moreover, we can assume the given parametrization verifies this property (section 2, Corollary 3).

Such are the goals of this paper. We call this approach *relatively optimal* since it depends on the field $\mathbf{K}$ that has been "a priori" specified. We present, in section 2, a method to test regularity (Theorem 3 and following comments), and we give, in section 3, an algorithmic solution to the reparametrization question, based on canonical divisors as in [6], but without implicitizitization. The idea of the reparametrization process is to compute a birational map over $\mathbb{K}$ that sends the original curve onto a conic. We observe that knowing a parametrization of the curve allows a simple description of the field of rational function on the curve. Thus, we analyze the method described in [6], and we show how it can be adapted to our situation. In addition, we also present a specially simple approach to the same problem, when the degree of the extension $\mathbb{K} \subset \mathbb{L}$ is two.

At this stage it is hard to compare our method with the previous ones that assume as input data a set of implicit equations. As Theorem 1 shows, it is easy, from this input, to determine *the* smallest field of definition for the curve and thus, to achieve an *absolute* version of the optimal parametrization problem. Starting with a parametrization does not allow to find it (unless we implicitize). On the other hand, if by some external information it happens that we are given both the ground field of the curve *and* a parametrization over an algebraic extension, it seems that reparametrizing is computationally simpler than implicitizing and finding -a new- a good parametrization, althought the precise computation and comparison of complexities has not been done.

2 Regular Field Extensions and Parametric Curves

As above, let $\mathbf{K}$ be a computable field of characteristic zero, $\mathbf{L}$ a finite field extension of $\mathbf{K}$, $\mathbf{F}$ its algebraic clousure. Let $\mathcal{C}$ be the irreducible curve defined over $\mathbf{F}$ by

$$\mathcal{P}(t) = (\frac{p_1(t)}{q(t)}, \ldots, \frac{p_n(t)}{q(t)}) \in \mathbf{L}(t)^n,$$

where $\gcd(p_1, \ldots, p_n, q) = 1$ (this situation is always reachable from any rational parametrization). Moreover, we will use the following notation: $\bar{x} = (x_1, \ldots, x_n)$; if $\mathcal{K}$ is a subfield of $\mathbf{F}$, then $\mathcal{I}_{\mathcal{K}}(\mathcal{C})$ denotes the ideal of the set of points of the curve that lie in $\mathcal{K}^n$, i.e. $\mathcal{I}_{\mathcal{K}}(\mathcal{C}) = \mathcal{I}(\mathcal{C} \cap \mathcal{K}^n)$; and for every ideal $\mathcal{J}$ in $\mathcal{K}[\bar{x}]$, $\mathcal{J}\mathbf{F}[\bar{x}]$ denotes the extension of $\mathcal{J}$ to $\mathbf{F}[\bar{x}]$.

In this section, we study the regularity of the field extension $\mathbb{K} \subset \mathbb{K}(\mathcal{P}(t))$ (see Theorem 2). We recall that a field extension Ω of a field Σ is said regular if the extension is separable and Σ is maximally algebraic in Ω; i.e. every element of Ω that is algebraic over Σ belongs to Σ. In particular, (see [13], Theorem 39, Ch. VII, 11, Vol. II), if $\mathcal{I}$ is a prime ideal over a polynomial ring $\mathcal{K}[\bar{x}]$, it holds that the quotient field of $\mathcal{K}[\bar{x}]/\mathcal{I}$ is a regular field extension of $\mathcal{K}$ if and only if $\mathcal{I}$ is absolutely prime. Requiring that the extension is regular amounts to say (in the classical terminology of algebraic function fields, see, for instance [3]) that $\mathbf{K}$ is the exact constant field of the rational function field of $\mathbf{K}(\mathcal{P}(t))$.

For our problem, we consider the homomorphism

$$\Psi : \mathbf{K}[\bar{x}] \longrightarrow \mathbf{F}(t)$$

such that $\Psi(x_i) = \frac{p_i(t)}{q(t)}$ for $i = 1, \ldots, n$. Then, since $ker(\Psi)$ is a prime ideal, in order to analyze the regularity of the extension $\mathbb{K} \subset \mathbb{K}(\mathcal{P}(t))$ one has to study when $ker(\Psi)$ is absolutely prime. For this purpose, we start with the following lemmas.

LEMMA 1. $ker(\Psi) = \mathcal{I}_{\mathbb{F}}(\mathcal{C}) \cap \mathbb{K}[\bar{x}]$

PROOF: Let $g \in ker(\Psi)$. Then $g \in \mathbb{K}[\bar{x}]$ and $g(\mathcal{P}(t)) = 0$. Thus, since $\mathcal{C}$ is irreducible, g vanishes on all the points of $\mathcal{C}$. Hence, $g \in \mathcal{I}_{\mathbb{F}}(\mathcal{C}) \cap \mathbb{K}[\bar{x}]$. Conversely, let $g \in \mathcal{I}_{\mathbb{F}}(\mathcal{C}) \cap \mathbb{K}[\bar{x}]$, then clearly $g(\mathcal{P}(t)) = 0$, and $g \in \mathbf{K}[\bar{x}]$. Therefore $g \in \ker(\Psi)$ □.

LEMMA 2. Let $\mathcal{D}$ be an algebraic curve over a characteristic zero algebraically closed field $\mathbb{F}$, and let $\mathbb{K} \subset \mathbb{L}$ be subfields of $\mathbb{F}$ (without requiring that the extension is algebraic or that $\mathbb{F}$ is the algebraic closure of $\mathbb{K}$ or of $\mathbb{L}$). Then it holds that:

(1) $\mathcal{D} \cap \mathbb{K}^n$ is an algebraic set in the affine space $\mathbf{A}^n(\mathbb{K})$ over $\mathbb{K}$.

(2) If $\mathcal{D}$ is an irreducible curve, then $card(\mathcal{D} \cap \mathbb{K}^n) = \infty$ if and only if $\mathcal{I}_{\mathbb{F}}(\mathcal{D}) \cap \mathbb{K}[\bar{x}] = \mathcal{I}_{\mathbb{K}}(\mathcal{D})$.

(3) If $\mathcal{D}$ is an irreducible curve and $card(\mathcal{D} \cap \mathbb{K}^n) = \infty$, then $\mathcal{D} \cap \mathbb{K}^n$ is a curve, and $\mathcal{I}_{\mathbb{F}}(\mathcal{D})$ is generated by polynomials in $\mathbb{K}[\bar{x}]$, namely, by $\mathcal{I}_{\mathbb{K}}(\mathcal{D})$.

(4) If $\mathcal{D}$ is a rational curve, then $card(\mathcal{D} \cap \mathbb{K}^n) = \infty$ if and only if $\mathcal{D}$ can be parametrized over $\mathbb{K}$.

(5) If $\mathcal{D}$ is a rational curve, and $\mathcal{P}(t)$ a parametrization of $\mathcal{D}$ over $\mathbb{L}$. Then $card(\mathcal{D} \cap \mathbb{K}^n) = \infty$ if and only if there exists a parametrization $\mathcal{Q}(t)$ of $\mathcal{D}$ over $\mathbb{K}$ such that $\mathbb{K}(\mathcal{P}(t))$ is isomorphic to $\mathbb{K}(\mathcal{Q}(t))$.

PROOF. (1) Let $f_1, \ldots, f_s \in \mathbf{F}[\bar{x}]$ be the generators of $\mathcal{I}_{\mathbb{F}}(\mathcal{D})$, and let $\{e_1, \ldots, e_r\}$ be a basis of the $\mathbf{K}$-vector space generated by the coefficients of the f_j's. Then, for every generator f_j there exist $M_{i,j} \in \mathbf{K}[\bar{x}]$ such that $f_j = \sum_{i=1}^{r} M_{i,j} e_i$, and clearly $\mathcal{D} \cap \mathbf{K}^n$ is the algebraic set in $\mathbf{A}^n(\mathbf{K})$ defined by $\{M_{i,j}\}_{\{1 \le i \le r, 1 \le j \le s\}}$.
(2) Let $\mathcal{D}$ have infinitely many points in $\mathbf{K}^n$. Clearly,

$$\mathcal{I}_{\mathbb{F}}(\mathcal{D}) \cap \mathbf{K}[\bar{x}] \subset \mathcal{I}_{\mathbf{K}}(\mathcal{D}).$$

Let $g \in \mathcal{I}_{\mathbf{K}}(\mathcal{D})$. Then $g \in \mathbf{K}[\bar{x}]$, and g vanishes on infinitely points of the curve. Thus, since $\mathcal{D}$ is irreducible one deduces that g vanishes on all the points of $\mathcal{D}$; that is $g \in \mathcal{I}_{\mathbb{F}}(\mathcal{D}) \cap \mathbf{K}[\bar{x}]$. Therefore, the two ideals are equal.
Conversely, from the proof of statement (1) it follows that:

$$\mathcal{I}_{\mathbb{F}}(\mathcal{D}) \subset (M_{i,j})\mathbf{F}[\bar{x}] \subset \mathcal{I}_{\mathbf{K}}(\mathcal{D})\mathbf{F}[\bar{x}]$$

Therefore, if $\mathcal{I}_{\mathbb{F}}(\mathcal{D}) \cap \mathbb{K}[\bar{x}] = \mathcal{I}_{\mathbb{K}}(\mathcal{D})$, then

$$\mathcal{I}_{\mathbb{K}}(\mathcal{D})\mathbb{F}[\bar{x}] = (\mathcal{I}_{\mathbb{F}}(\mathcal{D}) \cap \mathbb{K}[\bar{x}])\mathbb{F}[\bar{x}] = \mathcal{I}_{\mathbb{F}}(\mathcal{D})$$

Furthermore, since $\mathcal{I}_{\mathbb{K}}(\mathcal{D})$ is prime (it is the contraction of a prime ideal), and since the dimension of a prime ideal is preseved when extending (see [13]),one has that:

$$dim(\mathcal{I}_{\mathbb{K}}(\mathcal{D})) = dim(\mathcal{I}_{\mathbb{F}}(\mathcal{D})) = 1$$

Hence, $card(\mathcal{D} \cap \mathbb{K}^n) = \infty$
(3) If $card(\mathcal{D} \cap \mathbb{K}^n) = \infty$, following the proof of statement (2), one deduces that $\mathcal{D} \cap \mathbb{K}^n$ is a curve, and that $\mathcal{I}_{\mathbb{K}}(\mathcal{D})\mathbb{F}[\bar{x}] = \mathcal{I}_{\mathbb{F}}(\mathcal{D})$. Thus, $\mathcal{I}_{\mathbb{F}}(\mathcal{D})$ is generated by the basis of $\mathcal{I}_{\mathbb{K}}(\mathcal{D})$.
(4) The right-left implication is trivial, and the other implication follows, for instance, from the parametrization algorithm in [11].
(5) follows trivially from (4). □

Applying Lemma 2 one may prove that there exists an optimal "*candidate*" subfield Σ of $\mathbb{F}$, that we call the *ground field* of the curve, for parametrizing. More precisely, one has the following result.

THEOREM 1. Let $\mathcal{D}$ be a rational curve over $\mathbb{F}$. Then, it holds that:

(1) There is a smallest subfield Σ of $\mathbb{F}$ (or a smallest subfield Σ containing a given subfield $\mathbb{K}$, if we wish to fix a base field; the general case is equivalent to taking $\mathbb{K} = \mathbb{Q}$) such that $\mathcal{I}_{\mathbb{F}}(\mathcal{D})$ is generated by polynomials in $\Sigma[\bar{x}]$.

(2) If Ω is a subfield of $\mathbb{F}$ (respectively, a subfield containing $\mathbb{K}$) and $\mathcal{Q}(t) \in \Omega(t)^n$ parametrizes $\mathcal{D}$, then $\Sigma \subset \Omega$.

(3) There always exists a parametrization of $\mathcal{D}$ over an algebraic extension of Σ of degree at most two.

(4) There are subfields Ω of $\mathbb{F}$ (respectively, subfields containing $\mathbb{K}$) which are minimal with respect to the property: $\mathcal{D}$ can be parametrized over Ω.

(5) There are subfields Ω of $\mathbb{F}$ (respectively, subfields containing $\mathbb{K}$) which are minimal with respect to the property: $card(\mathcal{D} \cap \Omega^n) = \infty$.

PROOF. (1) Compute the unique reduced Gröbner bases of $\mathcal{I}_{\mathbb{F}}(\mathcal{D})$ and consider the field Σ generated (over $\mathbb{Q}$ or $\mathbb{K}$) by the coefficients of the polynomials in the basis. Next supose that this ideal is also generated by a different collection of polynomials over some other field Ω. ¿From this collection we can compute again a reduced Gröbner bases, which will have coefficients all in Ω. But reduced bases are unique, so $\Sigma \subset \Omega$.
(2) If $\mathcal{Q}(t) \in \Omega(t)^n$ parametrizes $\mathcal{D}$, then $card(\mathcal{D} \cap \Omega^n) = \infty$, and therefore, by Lemma 2 statement (3), one has that $\mathcal{I}_{\mathbb{F}}(\mathcal{D})$ is generated by polynomials in $\Omega[\bar{x}]$. Thus, $\Sigma \subset \Omega$.
(3) A constructive proof follows from [12].
(4) Given a curve, if it can be parametrized over the smallest field of definition Σ, it trivially holds, by (2), that this field is also the smallest one with respect to the parametrization property. Otherwise, by (3), there are degree two extensions Σ' of Σ where the curve is parametrizable, and we claim that any such is a minimal field for the parametrization property. In fact, suppose there is a subfield Σ'' of Σ' where the curve has also a parametrization. Then, by (2), $\Sigma \subset \Sigma''$. From $\Sigma \subset \Sigma'' \subset \Sigma'$ it follows, by degree considerations, that $\Sigma'' = \Sigma'$.
(5) it is just a version of (4) considering Lemma 2 (4). □

REMARK. Note that these results do not imply that there is a smallest subfield of $\mathbf{F}$ where we can find parametric equations of a given variety. In fact, a simple example (such as $x^2 + y^2 = 6$) shows a curve that can be parametrized over two different fields ($\mathbf{Q}(\sqrt(2))$, $\mathbf{Q}(\sqrt(5))$ in this case) but not over any common subfield. According to (4), both fields are just minimal fields with the parametrization property. On the other hand, the usual Zorn's lemma argument fails to show that (5) holds for non-parametric varieties, and we guess it is not true in general. In fact, for the elliptic cubic $\mathcal{D} \equiv x^3 + y^3 = 1$, one can find a strictly decreasing chain of fields $\mathbb{K}_i$, such that for all i, $card(\mathcal{D} \cap \mathbb{K}_i^n) = \infty$, but $\mathbf{Q}$ will be the only lower bound for the chain and the cubic has just a finite number of rational points. Take an infinite number of indeterminates over $\mathbf{Q}$, $\{x_1, \ldots, x_n, \ldots\}$ and define the fields $\mathbb{K}_i = \mathbb{Q}(x_i, x_{i+1}, \ldots.)[\sqrt[3]{1 - x_i^3}), \sqrt[3]{1 - x_{i+1}^3}, \ldots]$. [1] □

For the following theorem, we assume again that the parametrization is given with coefficients in a field $\mathbf{L}$ which is a finite field extension of $\mathbb{K}$, and where $\mathbb{L} \subset \mathbf{F}$ is its algebraic clousure. The next result characterizes the regularity of the field extension $\mathbb{K} \subset \mathbb{K}(\mathcal{P})$ by means of the implicit representation of the curve.

THEOREM 2. $\mathbb{K} \subset \mathbb{K}(p_1(t), p_2(t))$ is regular if and only if $\mathcal{I}_{\mathbb{F}}(\mathcal{C})$ is generated by elements in $\mathbb{K}[\bar{x}]$.

PROOF. Let $\mathcal{I}_{\mathbb{F}}(\mathcal{C})$ be generated by elements in $\mathbb{K}[\bar{x}]$. Then

$$(\mathcal{I}_{\mathbb{F}}(\mathcal{C}) \cap \mathbb{K}[\bar{x}])\mathbb{F}[\bar{x}] = \mathcal{I}_{\mathbb{F}}(\mathcal{C})$$

Thus, by Lemma 1, one has that $ker(\Psi)$ is absolutely prime, and therefore the extension is regular.
Conversely, let $\mathbb{K} \subset \mathbb{K}(p_1(t), p_2(t))$ be a regular extension. Then, $ker(\Psi)\mathbb{F}[\bar{x}]$ is prime, and by Lemma 1

$$ker(\Psi)\mathbb{F}[\bar{x}] = (\mathcal{I}_{\mathbb{F}}(\mathcal{C}) \cap \mathbb{K}[\bar{x}])\mathbb{F}[\bar{x}] \subset \mathcal{I}_{\mathbb{F}}(\mathcal{C}).$$

On the other hand, $dim(ker(\Psi)) = 1$, since it is equal to the transcendence degree of $\mathbb{K}(\mathcal{P}(t))$ over $\mathbb{K}$, and this agrees with the transcendence degree of the function field of the curve $\mathbb{F}(\mathcal{P}(t))$ over $\mathbb{F}$, because $\mathbb{F}$ is an algebraic extension of $\mathbb{K}$. Therefore $ker(\Psi)\mathbb{F}[\bar{x}]$ is also of dimension 1 and prime, hence, $ker(\Psi)\mathbb{F}[\bar{x}] = \mathcal{I}_{\mathbb{F}}(\mathcal{C})$. Thus, $\mathcal{I}_{\mathbb{F}}(\mathcal{C})$ is generated by

[1] we thank A. Prestel for this example

elements in $\mathbf{K}[\bar{x}]$. □

REMARK. Note that if $\mathbf{L}$ is not algebraic over $\mathbf{K}$, the right-left implication in Theorem 2 remains true. However, the left-right implication does not hold. For instance, given the parametrization (π, t), the extension $\mathbf{Q} \subset \mathbf{Q}(\pi, t)$ is regular, but the implicit equation of the curve is not in $\mathbf{Q}[x, y]$. □

COROLLARY 1. Without the restriction of algebraicity of $\mathbf{K} \subset \mathbf{L}$, if $\mathbf{K} \subset \mathbf{K}(p_1(t), p_2(t))$ is regular, then $\mathcal{C}$ can be parametrized over a extension of $\mathbf{K}$ of degree at most two.

PROOF. A classical result states that a function field of genus zero is the function field of a conic over the exact constant field ([3], see the comments at the beginning of this section) and the corollary follows from it. For a constructive proof, let $\mathbf{K} \subset \mathbf{K}(p_1(t), p_2(t))$ be regular. Then, by Theorem 2, one has that the ground field Σ of the curve is contained in $\mathbf{K}$. Thus, by Theorem 1, $\mathcal{C}$ is parametrizable over $\Sigma(\beta)$, with β algebraic over Σ of degree at most two. Thus, $\mathcal{C}$ is parametrizable over $\mathbf{K}(\beta)$ and β is also algebraic over $\mathbb{K}$ of degree at most two. □

COROLLARY 2. Let Ω be any subfield of $\mathbf{F}$ (not necessarily algebraic over $\mathbf{K}$) and $\mathcal{Q}(t) \in \Omega(t)^n$ a parametrization of $\mathcal{C}$. Then, if $card(\mathcal{C} \cap \mathbf{K}^n) = \infty$ it holds that $\mathbf{K} \subset \mathbf{K}(\mathcal{Q}(t))$ is regular.

PROOF. It follows from Lemma 2, statement (3), and Theorem 2. □.

On the other hand, Theorem 2 implies that the regularity of the extension depends only on the curve and not on the parametrization (provided they have coefficients algebraic over $\mathbb{K}$). More precisely:

COROLLARY 3. Let $\mathcal{P}_1(t)$ and $\mathcal{P}_2(t)$ be rational parametrizations of $\mathcal{C}$ over and algebraic extension $\mathbb{K} \subset \mathbb{L}$. Then, $\mathbb{K} \subset \mathbb{K}(\mathcal{P}_1(t))$ is regular if and only if $\mathbb{K} \subset \mathbb{K}(\mathcal{P}_2(t))$ is regular.

Thus, in order to analyze the regularity one may assume properness of the given parametrization. Furthermore, it is obvious that the regularity can be tested by implicitizing. In the following we give an alternative algorithmic characterization of the regularity that does not require this elimination procedure.

THEOREM 3. Let $\mathbf{L} = \mathbf{K}(\alpha)$, $[\mathbb{L} : \mathbb{K}] = d$, $\bar{t} = (t_0, \ldots, t_{d-1})$, $\tilde{t} = t_0 + t_1\alpha + \cdots + t_{d-1}\alpha^{d-1}$, and let:

$$\frac{p_1(\tilde{t})}{q(\tilde{t})} = \frac{v_{0,1}(\bar{t})}{u(\bar{t})} + \frac{v_{1,1}(\bar{t})}{u(\bar{t})}\alpha + \cdots + \frac{v_{d-1,1}(\bar{t})}{u(\bar{t})}\alpha^{d-1},$$

$$\vdots$$

$$\frac{p_n(\tilde{t})}{q(\tilde{t})} = \frac{v_{0,n}(\bar{t})}{u(\bar{t})} + \frac{v_{1,n}(\bar{t})}{u(\bar{t})}\alpha + \cdots + \frac{v_{d-1,n}(\bar{t})}{u(\bar{t})}\alpha^{d-1},$$

where $u, v_{i,j} \in \mathbb{K}[\bar{t}]$. Then, $\mathbb{K} \subset \mathbb{K}(\frac{p_1(t)}{q(t)}, \ldots, \frac{p_n(t)}{q(t)})$ is regular if and only if the dimension of the variety

$$\mathcal{W} = \mathcal{V}(v_{1,1}, \ldots, v_{d-1,1}, \ldots, v_{1,n}, \ldots, v_{d-1,n})$$

over $\mathbb{F}$ is one.

PROOF. Let $\mathcal{P}(t) = (\frac{p_1(t)}{q(t)}, \ldots, \frac{p_n(t)}{q(t)})$, and let $\mathcal{C}$ be the rational curve that $\mathcal{P}(t)$ defines over $\mathbb{F}$. Also, let $T(\bar{x}) \in \mathbb{L}[\bar{x}]$ be the inverse of the parametrization $\mathcal{P}(t)$; that is, $T(\mathcal{P}(t)) = t$ and $\mathcal{P}(T(\bar{x})) = \bar{x}$ modulo $\mathcal{I}_{\mathbf{F}}(\mathcal{C})$. Then, we express T as

$$T(\bar{x}) = T_0(\bar{x}) + T_1(\bar{x})\alpha + \cdots + T_{d-1}(\bar{x})\alpha^{d-1}.$$

with $T_i \in \mathbf{K}(\bar{x})$. Let $\varphi : \mathbf{F}[\bar{t}] \longrightarrow \mathbf{F}(\mathcal{C})$ be the homomorphism such that $\varphi(t_i) = T_i$ modulo $\mathcal{I}_{\mathbf{F}}(\mathcal{C})$, for $i = 0, \ldots, d-1$. In this situation, we prove that it always holds that, up to finitely many points, $\mathcal{W}$ is contained in the variety $\mathcal{V}(ker(\varphi))$ generated by $ker(\varphi)$, and that $dim(ker(\varphi)) = 1$. For this purpose, we observe that, since T is the inversion of $\mathcal{P}(t)$, one has that:

$$\tilde{t} = T(\mathcal{P}(\tilde{t})) = T_0(\mathcal{P}(\tilde{t})) + T_1(\mathcal{P}(\tilde{t}))\alpha + \cdots + T_{d-1}(\mathcal{P}(\tilde{t}))\alpha^{d-1}.$$

Hence, modulo the ideal generated by the polynomials $v_{i,j}$, $1 \leq i \leq d-1, j \leq j \leq n$, it holds that:

$$t_i = T_i(\frac{v_{0,1}(\bar{t})}{u(\bar{t})}, \ldots, \frac{v_{0,n}(\bar{t})}{u(\bar{t})}) \quad i = 0, \ldots, d-1.$$

Therefore, if $\bar{t}' \in \mathcal{W}$ such that $u(\bar{t}') \neq 0$, (note that only finitely many points of $\mathcal{W}$ vanish u) and $G \in Ker(\varphi)$, one has that:

$$G(\bar{t}') = G(T_0(\bar{x}'), \ldots, T_{d-1}(\bar{x}')) = \varphi(G) = 0.$$

where $\bar{x}' = (\frac{v_{0,1}(\bar{t}')}{u(\bar{t}')}, \ldots, \frac{v_{0,n}(\bar{t}')}{u(\bar{t}')})$. Thus, up to finitely many points, $\mathcal{W} \subset \mathcal{V}(ker(\varphi))$. On the other hand, since $\mathcal{P}(T(\bar{x})) = \bar{x}$ modulo $\mathcal{I}_{\mathbf{F}}(\mathcal{C})$, one deduces that

$$\varphi(\mathcal{P}(\tilde{t})) = \mathcal{P}(T(\bar{x})) = \bar{x}.$$

Therefore, φ is suprajective, and hence $dim(ker(\varphi)) = 1$.

Let now assume that $\mathbf{K} \subset \mathbf{K}(\mathcal{P}(t))$ is regular. Then, by Theorem 2, $\mathcal{I}_{\mathbf{F}}(\mathcal{C})$ is generated by a set $H \subset \mathbf{K}[\bar{x}]$. Thus, since $\mathcal{P}(T(\bar{x})) = \bar{x}$ modulo $\mathcal{I}_{\mathbf{F}}(\mathcal{C})$, one deduces that:

$$\varphi(v_{i,j}(\bar{t})) = 0 \text{ for } 1 \leq i \leq d-1, 1 \leq j \leq n$$

Therefore, $\mathcal{V}(ker(\varphi)) \subset \mathcal{W}$. Hence, $dim(\mathcal{W}) = 1$

Conversely, let $dim(\mathcal{W}) = 1$. Then, since $ker(\varphi)$ is irreducible of dimension one, and since $\mathcal{W}$ is included -up to finitely many exceptions- in $\mathcal{V}(ker(\varphi))$, one deduces that $\mathcal{W}$ decomposes as the union of $\mathcal{V}(ker(\varphi))$ and of a zero dimensional variety. Then, it follows that $ker(\varphi)$ is generated by polynomials over $\mathbb{K}$ (note that since $\mathcal{W}$ is the zero set of an ideal $\mathcal{J}$ generated by polynomials over $\mathbb{K}$, then -see [13],Ch. VII, Vol. II- its only prime component of dimension one of the radical over $\mathbf{F}$ of $\mathcal{J}$ is also generated by polynomials over $\mathbb{K}$). On the other hand, if φ' is the resctriction of φ to $\mathbb{K}[\bar{t}]$, it is clear that the quotient field of $\mathbb{K}[\bar{t}]/ker(\varphi')$ is isomorphic to $\mathbb{K}(\mathcal{P}(t))$. Furthermore, $ker(\varphi') = ker(\varphi) \cap \mathbb{K}[\bar{t}]$. Hence, $ker(\varphi')$ is absolutely prime, and therefore one concludes that $\mathbb{K} \subset \mathbb{K}(\mathcal{P}(t))$ is regular. □

This test is particularly simple for the case of degree two extensions:

COROLLARY 4. Let $[\mathbb{L} : \mathbb{K}] = 2$. Then, with the notation of Theorem 3, one has that $\mathbb{K} \subset \mathbb{K}(\frac{p_1(t)}{q(t)}, \ldots, \frac{p_n(t)}{q(t)})$ is regular if and only if $\gcd(v_{1,1}, \ldots, v_{1,n}) \notin \mathbb{F}$.

PROOF. It follows directly from Theorem 3, considering the intersection of the plane curves $v_{1,1=0}, \ldots, v_{1,n} = 0$. □

REMARK. Let $\mathcal{C}$ be a rational space curve given by a parametrization $\mathcal{P}(t) \in \mathbb{L}(t)$. Then, since $\mathcal{C}$ is $\mathbb{K}$-birationally equivalent to a plane curve $\mathcal{D}$, and since the regularity is kept under birational morphims, the regularity of $\mathbf{K} \subset \mathbb{K}(\mathcal{P}(t))$ is equivalent to the regularity of $\mathbf{K} \subset \mathbb{K}(\mathcal{Q}(t))$, where $\mathcal{Q}(t)$ is the image of $\mathcal{P}(t)$ under the morphism. Thus, one simply has to apply methods described above to plane curves. Furthermore, note that if $\mathcal{P}(t)$ is proper, then $\mathcal{Q}(t)$ is also proper, and therefore implicitizing $\mathcal{Q}(t)$ basically involves a resultant computation. □

3 Relatively Optimal Reparametrizations

In this section we present an algorithm, based on canonical divisors, that solves the relatively optimal reparametrization problem for space curves. Let $\mathbb{K}$, $\mathbb{L}$, and $\mathbb{F}$, be as in section 1. Then, given a rational parametrization $\mathcal{P}(t)$ over $\mathbb{L}$ of an irreducible space curve $\mathcal{C}$ over $\mathbb{F}$, and assuming that the extension $\mathbb{K} \subset \mathbb{K}(\mathcal{P}(t))$ is regular, we want to reparametrize the curve over a field extension of $\mathbb{K}$ of degree at most two (see Corollary 1 of the previous section). Obviously, since $\mathbb{L}$ is finite over $\mathbb{K}$, the regularity of the extension can be decided either by implicitization or by Theorem 3 and following remarks. If the extension is not regular, then we know that there is no parametrization over $\mathbb{K}$ (Lemma 2, and Theorem 2), and we must reconsider another field $\mathbb{K}$.

Assuming the regularity has been established, the idea consists, first, in birationally projecting, over $\mathbb{K}$, the given parametrization onto a parametrization of a plane curve which is also defined over $\mathbb{K}$. Then, we will compute a birational transformation, again over $\mathbb{K}$, that sends the plane curve onto a $\mathbb{K}$-conic. Therefore, the problem is reduced to analyzing a conic and this can be done as in [6]. The second birational map is obtained by means of canonical divisors, again following [6], but instead of using the implicit equation the basic idea here is to observe that knowing a parametrization of the curve, the field of rational functions on the curve is much simply described. Thus, we show here how Hoeij's method can be adapted to our case. As a consequence, one gets an apparently computationally simpler process (if one starts with parametric data: for instance, implicitization and integral basis computation are not required).

We start with the reduction of the problem to plane curves. Afterwards, the general case for plane curves is analyzed.

Reduction to Plane Curves

Let $\mathcal{C}$ be an irreducible space curve over $\mathbb{F}$ given by the parametrization $\mathcal{P}(t) = (\frac{p_1(t)}{q(t)}, \ldots, \frac{p_n(t)}{q(t)}) \in \mathbb{L}(t)^n$. Then, it is well known that $\mathcal{C}$ is birationally equivalent to a plane curve. Algorithmic versions of this fact, for implicitly represented curves, can be found in the literature, via the primitive element algorithm [7]. In our case, since the curve is given parametrically, one basically has to analyze the field $\mathbb{K}(\mathcal{C})$ of $\mathbb{K}$-rational functions on the curve, which is isomorphic to $\mathbb{K}(\mathcal{P}(t))$. Then, since the transcendence degree of $\mathbb{K}(\mathcal{C})$ over $\mathbb{K}$ is one, $\mathbb{K}(\mathcal{C}) = \mathbb{K}(M, N)$, where $M \in \mathbb{K}(\mathcal{C})$ is trancendental over $\mathbb{K}$, and N is the primitive element of the algebraic extension $\mathbb{K}(\mathcal{C})$ over $\mathbb{K}(M)$. Furthermore, one may take M as any nonconstant rational function in $\mathcal{P}(t)$, say $M = \frac{p_1}{q}$, and N as a $\mathbb{K}$ linear combination of the remaining rational functions, say $N = a_2\frac{p_2}{q} + \cdots + a_n\frac{p_n}{q}$.

Thus, again, $M, N \in \mathbb{L}(t)^n$ and the extension $\mathbb{K} \subset \mathbb{K}(M(t), N(t))$ is also regular, since this last field is $\mathbb{K}$-birationally isomorphic to $\mathbb{K}(\mathcal{P}(t))$ and regularity is kept under birational morphisms (see the definition in the introduction to Section 2). Notice that also $\mathbf{L}(\mathcal{C}) = \mathbf{L}(M, N)$ and $\mathbf{F}(\mathcal{C}) = \mathbf{F}(M, N)$. Therefore, in the following, we might assume that we are given an irreducible plane curve.

The General Method

Let $\mathcal{C}$ be a rational plane curve over $\mathbb{F}$ and let $\mathbf{F}(\mathcal{C})$ be the field of rational functions on $\mathcal{C}$. Then, if $D = \sum n_p P$ is a divisor on $\mathcal{C}$, we denote by $\mathcal{L}_{\mathbb{F}}(D)$ the $\mathbb{F}$-vector space

$$\mathcal{L}_{\mathbb{F}}(D) = \{h \in \mathbb{F}(\mathcal{C}) / ord_P(h) \geq -n_p \text{ for all places } P \in \mathbb{F}(\mathcal{C})\}$$

Similar definitions apply to the other fields $\mathbb{K}$, $\mathbb{L}$ under consideration. The method presented in [6] (basically a computational version of the classic procedure [3]) consists in considering a rational divisor D of $\mathbb{F}(\mathcal{C})$ of degree two and dimension 3, where rational means being invariant under the action of the Galois group $Gal(\mathbb{F}/\Sigma)$, and Σ is the ground field of the curve. In particular, $-D$ is taken as the divisor of the differential dx. Thus, since the genus of $\mathcal{C}$ is zero, by Riemann-Roch Theorem one has that $deg(D) = 2$, and $dim(\mathcal{L}_{\mathbb{F}}(D)) = 3$. Then, by means of integral basis computation, a basis $g_1, g_2, g_3 \in \Sigma(\mathcal{C})$ of $\mathcal{L}_{\mathbb{F}}(D)$ is determined. In this situation, $(\frac{g_1}{g_3}, \frac{g_2}{g_3})$ defines a birational map over Σ from $\mathcal{C}$ onto a conic. Therfore, the initial problem is reduced to analyzing this conic and to inverting the parametrization of this conic via the birational map.

Here, we show that these ideas can be adapted to solve our problem. For this purpose, we assume that we are given a proper parametrization $\mathcal{P}(t) = (\frac{p_1}{q}, \frac{p_2}{q}) \in \mathbb{L}(t)^2$, and we want to compute, from $\mathcal{P}(t)$, the canonical divisor $div(dx)$ of the function field $\mathbb{K}(\mathcal{C})$, and to determine a basis over $\mathbb{K}$ of $\mathcal{L}_{\mathbb{K}}(-div(dx))$.

To compute $div(dx)$, we proceed over $\mathbb{F}(\mathcal{C}) = \mathbb{F}(t)$. Here the places of $\mathcal{C}$ are easy to determine, since it is clear that

$$\{\mathcal{P}(t + t_0) \,/\, t_0 \in \mathbb{F}\}$$

plus $\mathcal{P}(\frac{1}{t})$ generates the set of all places of $\mathbb{F}(\mathcal{C})$. Moreover, let P_{t_0} (respectively $P_{\frac{1}{t}}$) be the place defined by $\mathcal{P}(t + t_0)$ (respectively, $\mathcal{P}(\frac{1}{t})$) and let n_{t_0} (or $n_{\frac{1}{t}}$) be the corresponding coefficient of P_{t_0} (or $P_{\frac{1}{t}}$) in $div(dx)$. Then, since

$$dx = g(t)\,dt \quad \text{where} \quad g(t) = (\frac{p_1}{q})',$$

one has that $n_{t_0} = ord_t(g(t + t_0))$. Therefore, $n_{t_0} \neq 0$ if and only if t_0 vanishes either the numerator or the denominator of $g(t)$. For $n_{\frac{1}{t}}$ one has to compute, $ord_t(-\frac{1}{t^2}g(\frac{1}{t}))$.

Although the canonical divisor is determined over $\mathbb{F}$, since we know it is rational, the corresponding expressions over $\mathbb{L}$ or over $\mathbb{K}$ could be obtained. Next a basis over $\mathbb{K}$ of $\mathcal{L}_{\mathbb{K}}(-div(dx))$ has to be obtained. We know that in the separable case, under extension of the coefficient field both the dimension and degree of divisors remain invariant. Thus, first a basis over $\mathbb{L}$ is computed, taking advantage of the fact that $\mathbb{L}(\mathcal{P}(t)) = \mathbb{L}(t)$. Therefore, since the dimension of $\mathcal{L}_{\mathbb{L}}(-div(dx))$ is known in advance, it is easy to find three elements $h_1, h_2, h_3 \in \mathbb{L}(t)$ satisfying the conditions imposed by $\mathcal{L}_{\mathbb{L}}(-div(dx))$ and being linearly independent. Now a basis over $\mathbb{K}$ must be derived.

First we observe that the map:

$$\begin{array}{llll} \varphi: & \mathbb{L}(\mathcal{C}) & \longrightarrow & \mathbb{L}(\frac{p_1}{q}, \frac{p_2}{q}) = \mathbb{L}(t) \\ & u(x, y) & \longrightarrow & u(\frac{p_1}{q}, \frac{p_2}{q}) \end{array}$$

is an isomorphism and it is computationally simple to invert. Then, we consider the elements $u_i(x,y) = \varphi^{-1}(h_i), i = 1,2,3$.

In order to derive from $\{u_1, u_2, u_3\}$ a basis over $\mathbf{K}$ of $\mathcal{L}_{\mathbf{K}}(-div(dx))$, we observe that the extension $\mathbf{K} \subset \mathbf{K}(\mathcal{P}(t))$ is regular. Therefore, by Theorem 2, one deduces that the ground field Σ of $\mathcal{C}$ is contained in $\mathbf{K}$. Thus, results in [6] implies that there exists a basis $\{v_1, v_2, v_3\}$ of $\mathcal{L}_{\mathbf{K}}(-div(dx))$ over $\mathbb{K}$. To compute such a basis, we apply that $[\mathbf{L} : \mathbb{K}] = d < \infty$. Let $\mathbb{L} = \mathbb{K}(\alpha)$. Then, each v_i can be expressed as a linear combination over $\mathbf{L}$ of the basis $\{u_1, u_2, u_3\}$. Thus, introducing undetermined coefficients we find algebraic conditions for $v \in \mathcal{L}_{\mathbf{L}}(-div(dx)) \cap \mathbf{K}(\mathcal{C})$. More preceisely, v can be expressed in the form:

$$v = (\sum_{j=0}^{d-1} a_j\alpha^j)u_1 + (\sum_{j=0}^{d-1} b_j\alpha^j)u_2 + (\sum_{j=0}^{d-1} c_j\alpha^j)u_3$$

where $a_j, b_j, c_j \in \mathbb{K}$. Hence, writing also u_i in terms of the powers of α, v is expressed as:

$$v = \frac{R_0}{S_0} + \frac{R_1}{S_1}\alpha + \cdots + \frac{R_{d-1}}{S_{d-1}}\alpha^{d-1}$$

where $R_j \in \mathbb{K}[a_0, \ldots, a_{d-1}, b_0, \ldots, b_{d-1}, c_0, \ldots, c_{d-1}][x,y]$, and $S_j \in \mathbb{K}[x,y]$. Now, note that the coefficients of the R_j depend linearly on the a_j, b_j, c_j. Therefore, solving the linear system of equations derived from the conditions $R_i = 0$, $i = 1, \ldots, d-1$, one may find $\{v_1, v_2, v_3\}$.

Summarizing, we have computed a birational map $(\frac{v_1}{v_3}, \frac{v_2}{v_3})$ over K that sends the original curve $\mathcal{C}$ over the conic $\mathcal{D}$ parametrized projectively over $\mathbb{L}$ as $(v_1(\mathcal{P}), v_2(\mathcal{P}), v_3(\mathcal{P}))$. Furthermore, since regularity is kept under birational morphisms, the defining polynomial of $\mathcal{D}$ is over $\mathbf{K}$. Being a conic, $\mathcal{D}$ can be parametrized over a field extesion of $\mathbf{K}$ of degree at most two. Thus, inverting such a parametrization one achieves a solution to our problem.

We finish this section with an example that illustrates the ideas described before.

Example. We consider the rational space curve $\mathcal{C}$ given by the rational parametrization

$$\mathcal{P}(t) = (p_1, p_2, p_3) = (\frac{t^2 + 2t\alpha^2 - 3 - t - \alpha^2}{t^3 + 3t^2\alpha^2 + t^2 - 7t + 2t\alpha^2 - 3\alpha^2 - 3},$$

$$\frac{t^2 + 2t\alpha^2 - 2 + t + \alpha^2}{t + \alpha^2 - 1}, -\frac{2t + 2\alpha^2 - 1}{t + \alpha^2 - 1})$$

over $\mathbf{Q}(\alpha)$, where $\alpha^4 + 2 = 0$. Then, we project $\mathcal{C}$ birationally onto the plane curve $\mathcal{D}$ parametrized as $\mathcal{Q}(t) = (p_1, p_2 + p_3)$:

$$\mathcal{Q}(t) = (\frac{t^2 + 2t\alpha^2 - 3 - t - \alpha^2}{t^3 + 3t^2\alpha^2 + t^2 - 7t + 2t\alpha^2 - 3\alpha^2 - 3},$$

$$\frac{t^2 + 2t\alpha^2 - 1 - t - \alpha^2}{t + \alpha^2 - 1}).$$

Now, the regularity of the extension $\mathbf{Q} \subset \mathbf{Q}(\mathcal{Q}(t))$, and therefore the regularity of the extension $\mathbf{Q} \subset \mathbf{Q}(\mathcal{P}(t))$, can be checked using the results in section 2. For instance, we compute the defining polynomial

$$f(x,y) = -4 + 12x - 9x^2 + y^2 - xy^3 + 11xy - 4x^2y^2 - 2y - 12x^2y$$

of the curve $\mathcal{D}$. Thus, since $f \in \mathbb{Q}[x,y]$, we conclude that $\mathbf{Q} \subset \mathbf{Q}(\mathcal{P}(t))$ is regular.

In order to compute the canonical divisor $div(dx)$, we determine

$$g(t) = p_1(t)' = -\frac{(t - 3 + \alpha^2)(t + \alpha^2)^2}{(t + 1 + \alpha^2)^3(t + \alpha^2 - 1)^2}.$$

Furthermore, $ord_t(g(t + 3 - \alpha^2)) = 1, ord_t(g(t - \alpha^2)) = 2, ord_t(g(t - 1 - \alpha^2)) = -3, ord_t(g(t + 1 - \alpha^2) = -2$, and $ord_t(-\frac{1}{t^2}g(\frac{1}{t})) = 0$. Hence:

$$div(dx) = P_{t_1} + 2\,P_{t_2} - 3\,P_{t_3} - 2\,P_{t_4},$$

where $t_1 = 3 - \alpha^2, t_2 = -\alpha^2, t_3 = -1 - \alpha^2$, and $t_4 = 1 - \alpha^2$. Therefore,

$$h1 = \frac{(t + 1 + \alpha^2)^3(t + \alpha^2 - 1)^2}{t - 3 + \alpha^2}$$

$$h2 = \frac{(t + 1 + \alpha^2)^3(t + \alpha^2 - 1)^2}{(t + \alpha^2)^2}$$

$$h3 = \frac{(t + 1 + \alpha^2)^3(t + \alpha^2 - 1)^2}{(t - 3 + \alpha^2)(t + \alpha^2)^2}$$

is a basis of $\mathcal{L}_{\mathbf{Q}(\alpha)}(-div(dx))$ over $\mathbb{Q}(\alpha)$. Now, we compute the inverse $M(x,y)$ of $\mathcal{Q}(t)$

$$M(x,y) = -\frac{2y - 4xy - 2\alpha^2 + 3x\alpha^2 + 2 - 3x + y\alpha^2 - y^2}{3x - 2 + y},$$

that applied to $\{h_1, h_2, h_3\}$ provides the basis $\{u_1, u_2, u_3\}$, $u_i = h_i(M(x,y))$:

$$u_1 = \frac{(-3 + 4x + y)^2y^2(-y + 4xy - 4 + 6x + y^2)^3}{(-5y + 4xy + 4 - 6x + y^2)(3x - 2 + y)^4}$$

$$u_2 = \frac{(-3 + 4x + y)^2y^2(-y + 4xy - 4 + 6x + y^2)^3}{(-2y + 4xy - 2 + 3x + y^2)^2(3x - 2 + y)^3}$$

$$u_3 = \frac{(-3 + 4x + y)^2y^2(-y + 4xy - 4 + 6x + y^2)^3}{a(t)}$$

where $a(t)$ is the polynomial

$$(-2y + 4xy - 2 + 3x + y^2)^2(-5y + 4xy + 4 - 6x + y^2)(3x - 2 + y)^2,$$

that is already a basis over $\mathbb{Q}$. Thus,

$$\psi(t) = (\frac{u_1}{u_3}, \frac{u_2}{u_3}) =$$

$$(\frac{(-2y + 4xy - 2 + 3x + y^2)^2}{(3x - 2 + y)^2}, \frac{-5y + 4xy + 4 - 6x + y^2}{3x - 2 + y})$$

defines a birational map from $\mathcal{D}$ onto a conic $\mathcal{E}$, that is parametrized by

$$\psi(\mathcal{Q}) = (t^2 + 2t\alpha^2 - 2, t - 3 + \alpha^2).$$

Therefore, $\mathcal{E}$ is the parabola $x - 9 - y^2 - 6y$, that can be parametrized over $\mathbf{Q}$ as $\mathcal{M}(t) = (9 + t^2 + 6t, t)$. Hence, inverting $\mathcal{M}(t)$ by ψ^{-1}, one gets the parametrization of $\mathcal{D}$ over $\mathbf{Q}$

$$\mathcal{Q}^*(t) = (\frac{5t + t^2 + 5}{(t^2 + 8t + 16)(2 + t)}, \frac{7 + t^2 + 5t}{2 + t}).$$

Finally, inverting the plane parametrization over $\mathbb{Q}$, one deduces an optimal parametrization of the space curve $\mathcal{C}$

$$\mathcal{P}^*(t) = (\frac{5t + t^2 + 5}{(t^2 + 8t + 16)(2 + t)}, \frac{12 + 7t + t^2}{2 + t}, -\frac{2t + 5}{2 + t})$$

4 Alternative Approach to the Two Degree Case

In this last section, we present an alternative approach to the case where $[\mathbb{L} : \mathbb{K}] = 2$. Note that this particular situation appears, for instance, when working in real geometry. The following theorem shows how to proceedTheorem 4. Let $\mathcal{C}$ be the rational curve over $\mathbf{F}$ parametrized by $\mathcal{P}(t) = (\frac{p_1}{q}, \ldots, \frac{p_n}{q}) \in \mathbb{K}(\alpha)(t)^n$, where $[\mathbf{K}(\alpha) : \mathbf{K}] = 2$. Then, if $\bar{t} = t_0 + t_1\alpha$, and

$$\frac{p_1(\bar{t})}{q(\bar{t})} = \frac{v_{0,1}(t_0,t_1)}{u(t_0,t_1)} + \frac{v_{1,1}(t_0,t_1)}{u(t_0,t_1)}\alpha,$$

$$\vdots$$

$$\frac{p_n(\bar{t})}{q(\bar{t})} = \frac{v_{0,n}(t_0,t_1)}{u(t_0,t_1)} + \frac{v_{1,n}(t_0,t_1)}{u(t_0,t_1)}\alpha,$$

where $u, v_{i,j} \in \mathbb{K}[t_0, t_1]$, it holds that:

(1) $deg(gcd(v_{1,1}, v_{1,2})) \leq 2$

(2) $\mathcal{C}$ is parametrizable over $\mathbf{K}$ if and only if the curve defined by $gcd(v_{1,1}, v_{1,2})$ is parametrizable over $\mathbb{K}$. Furthermore, if $\mathcal{M}(t) = (m_1, m_2)$ is a parametrization of $gcd(v_{1,1}, v_{1,2})$ over $\mathbb{K}$, then $\mathcal{P}(m_1(t) + \alpha m_2(t))$ is a parametrization of $\mathcal{C}$ over $\mathbf{K}$.

(3) If $\mathbf{K}$ is the prime subfield of $\mathbf{F}$, and $gcd(v_{1,1}, v_{1,2}) \in \mathbb{F}$, then $\mathbb{K}(\alpha)$ is the ground field of $\mathcal{C}$, and $\mathcal{P}(t)$ is an optimal parametrization of $\mathcal{C}$.

(4) If $\mathbf{K}$ is the prime subfield of $\mathbf{F}$, $gcd(v_{1,1}, v_{1,2}) \notin \mathbf{F}$. but $gcd(v_{1,1}, v_{2,1})$ can not be parametrized over $\mathbb{K}$, then $\mathbb{K}$ is the ground field of $\mathcal{C}$, and $\mathcal{P}(t)$ is an optimal parametrization of $\mathcal{C}$.

Proof. (1) and (2) follow from a direct generalization of the results in [9].
(3) Let Σ be the ground field of $\mathcal{C}$. By Corollary 4, one has that $\mathbb{K} \subset \mathbb{K}(\mathcal{P}(t))$ is not regular. Thus, applying Theorem 2, one deduces that $\mathbb{K}$ is a proper subfield of Σ. On the other hand, Theorem 1 implies that $\Sigma \subset \mathbf{K}(\alpha)$. Hence, $\Sigma = \mathbf{K}(\alpha)$.
(4) Let Σ be the ground field of $\mathcal{C}$. By Corollary 4, one has that $\mathbb{K} \subset \mathbf{K}(\mathcal{P}(t))$ is regular. Applying Theorem 2, one deduces that $\Sigma \subset \mathbb{K}$. Thus, since $\mathbf{K}$ is prime, one deduces that $\Sigma = \mathbb{K}$. On the other hand, by statement (2), $\mathcal{C}$ can not be parametrized over $\mathbb{K}$. Hence, $\mathcal{P}(t)$ is optimal. □

Remark. The natural question after this result is to analyze whether the theorem can be generalized to algebraic extensions of higher degree. The problem is that the curve that the polynomials $v_{i,j}$ define in the general case is of degree equal to the degree of the field extension, and therefore, it is not a conic anymmore.

5 Acknowledgement

The authors want to thank M. Hoeij for the useful lectures on his ideas, given at University of Cantabria in the fall of 1996.

References

[1] Abhyankar S., (1990), *Algebraic Geometry for scientists and engineers.* Mathematical surveys and monographs, 35. A.M.S. 1990.

[2] Alonso C., Gutiérrez J., Recio T., (1995) *A rational function decomposition algorithm by near separated polynomials.* Journal of Symbolic Computation 11.

[3] Eichler M. (1966), *Introduction to the theory of Algebraic Numbers and Functions.* Academic Press.

[4] Hoffmann C., Sendra J.R., Winkler F. (eds) (1997). Journal of Symbolic Computation vol. 23, Special Issue on "Parametric Algebraic Curves and Applications".

[5] van Hoeij M. (1994), *Computing parametrizations of rational algebraic curves.* In J. von zur Gathen (ed.), Proc. ISSAC94 187-190, ACM Press.

[6] van Hoeij M. (1997). *Rational Parametrization of curves using Canonical Divisors.* J. Symbolic Computation vol. 23.

[7] Loos R. (1982)*Generalized Polynomial Remainder Sequences.* In:"Computer Algebra". Ed. Buchberger-Collins-Loos. Computing Supplementum 4. Springer-Verlag.

[8] Mñuk M., Sendra J.R., Winkler F. (1993), *On the Complexity of Parametrizing Curves.* To appear in Beiträge zur Algebra und Geometrie.

[9] Recio T., Sendra J.R., (1997). *Real Reparametrizations of Real Curves.* J. Symbolic Computation vol. 23.

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

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

[12] Sendra J.R., Winkler F. (1997). *Parametrization of Algebraic Curves over Optimal Field Extensions.* J. Symbolic Computation vol. 23.

[13] Zariski O., Samuel P. (1960). *Commutative Algebra, Vol II.* Springer Verlag.