Journal of Computational and Applied Mathematics 416 (2022) 114571

Contents lists available at ScienceDirect

Journal of Computational and Applied Mathematics

journal homepage: www.elsevier.com/locate/cam

Using μ-bases to reduce the degree in the computation of projective equivalences between rational curves in n-space

Juan Gerardo Alcázar [a,1,2], Carlos Hermoso [a,1,2], Sonia Pérez Díaz [a,*,1,2], Li-Yong Shen [b,3]

[a] *Universidad de Alcalá, Departamento de Física y Matemáticas, E-28871 Madrid, Spain*
[b] *School of Mathematical Sciences, University of Chinese Academy of Sciences, 100049, Beijing, China*

ARTICLE INFO

Article history:
Received 24 February 2022
Received in revised form 26 May 2022

Keywords:
Projective equivalences
μ-bases
Rational curves

ABSTRACT

We study how projective equivalences between rational curves in $\mathbb{R}^n$ are transferred to the elements of smallest degree of the μ-bases of the curves. We show how to compute these elements of smallest degree without computing the whole μ-basis, and prove some results on the degrees of μ-bases of curves in $\mathbb{R}^n$. As a result, we provide a way to reduce the cost of computing the projective equivalences between rational curves in $\mathbb{R}^n$ by replacing the given curves for the curves represented by the elements of smallest degree of the μ-bases of the curves, which have a much smaller degree compared to the original degree of the curves.

1. Introduction

The notion of a μ-basis for rational curves was introduced in 1998 (see [1]) as a new technique to speed up the computation of the implicit form of a rational curve. Since then, much work has been done to improve the algorithms for finding μ-bases of curves [2–4] and for applying μ-bases not only to the implicitization problem, but also to other problems like computing singularities of curves [5], inversion and intersection [4], and, more recently, detection of properness and proper reparametrization of curves [6].

The notion of a μ-basis is usually introduced, in an algebraic fashion, as a basis of a free module related to a given rational curve. From a more geometric point of view, a μ-basis is a collection of curves derived from an original curve, which can replace the curve for certain tasks (e.g. implicitizing, properness detection, singularity computation, etc.) Although one might think that replacing one curve by a collection of several curves is not very clever, the great advantage is that the degrees of these curves are much smaller, which makes computations more efficient.

While algebraic aspects of μ-bases of curves have been extensively studied in, among others, the references in the first paragraph, geometric questions have not been explored so thoroughly. In this sense, one can wonder whether there are properties of the original curve that are somehow inherited by the curves in the μ-basis. The main contribution of this

[*] Corresponding author.
E-mail addresses: juange.alcazar@uah.es (J.G. Alcázar), carlos.hermoso@uah.e (C. Hermoso), sonia.perez@uah.es (S. Pérez Díaz), lyshen@ucas.ac.cn (L.-Y. Shen).

[1] Supported by the grant PID2020-113192GB-I00 (Mathematical Visualization: Foundations, Algorithms and Applications) from the Spanish MICINN.

[2] Member of the Research Group ASYNACS (Ref. CCEE2011/R34).

[3] Supported by the National Natural Science Foundation of China under Grant 61872332, 11731013.

https://doi.org/10.1016/j.cam.2022.114571

paper is to show that projective equivalences between rational curves, and therefore affine equivalences and symmetries, are inherited by the elements of smallest degree in the μ-bases.

Symmetries and similarities between rational curves were studied in a series of papers by Alcázar et al. (see the bibliographies of [7,8] and of the very recent paper, uploaded to ArXiv, [9]). In [7–9], the problem, with different approaches, was generalized to computing projective equivalences between rational curves. Although a thorough complexity analysis of the algorithms in [7–9] is still absent, it is clear that the cost of these algorithms depends strongly on the degrees of the curves whose projective equivalences one wants to compute. In this paper, we show that the computation of projective equivalences between two rational curves can be transferred to the curves of minimal degree belonging to the μ-bases of the given curves. Since the curves in the μ-bases have a much smaller degree compared with the original degrees, using μ-bases to study projective equivalences can be an advantage.

Additionally, we present a new algorithm for computing μ-bases of rational curves which allows us to compute the elements of the μ-basis by increasing degree. In particular, if we are only interested in computing the elements of minimal degree of the μ-basis, we do not need to compute the whole μ-basis. Some new results about the degrees of the elements in the μ-basis are also provided.

The structure of the paper is the following. The background on projective equivalences and μ-bases of rational curves is provided in Section 2. The main results about projective equivalences and μ-bases are provided in Section 3. In Section 4 we consider several aspects of the computation of μ-bases, and provide techniques to find only the elements of minimal degree. Additional questions on the computation of projective equivalences combining μ-bases and known algorithms are given in Section 5. We present our conclusion in Section 6.

2. Preliminaries on projective equivalences and μ-bases of rational curves

2.1. Projective equivalences

Let us denote by $\mathbf{x}$ the elements of the projective space $\mathbb{PR}^n$, i.e.

$$\mathbf{x} = [x_1 : \cdots : x_{n+1}].$$

The points $\mathbf{x} \in \mathbb{PR}^n$ where $x_{n+1} = 0$ are called *points at infinity*. A *projective transformation*, also called *projectivity*, is a mapping $f : \mathbb{PR}^n \to \mathbb{PR}^n$ where

$$f(\mathbf{x}) = \mathcal{A}\mathbf{x}, \tag{1}$$

with $\mathcal{A}$ an $(n+1) \times (n+1)$ nonsingular matrix. If $\mathcal{A}$ has the following block structure

$$\mathcal{A} = \begin{bmatrix} \mathbf{A} & \mathbf{b} \\ \mathbf{0} & 1 \end{bmatrix} \tag{2}$$

then $\mathcal{A}$ is an *affine transformation* or an *affinity*. Furthermore, if $\boldsymbol{A}$ is orthogonal, i.e. $\boldsymbol{A}^T\boldsymbol{A} = \text{Id}$, with Id being the $n \times n$ identity matrix, we say that f represents an *isometry*, also called a *rigid motion*; if $\boldsymbol{A} = \lambda\boldsymbol{Q}$ with $\boldsymbol{Q}$ orthogonal and $\lambda > 0$, f represents a *similarity*. In particular, isometries preserve angles and distances, while similarities only preserve angles and scale all distances by a same factor λ.

In order to avoid a cumbersome notation, whenever a vector is multiplied by a matrix, we will understand that the vector corresponds to a column matrix.

A rational curve $\mathcal{C} \subset \mathbb{R}^n$, rationally parametrized by

$$\mathcal{Q}(t) = \left(\frac{q_1(t)}{q_{n+1}(t)}, \ldots, \frac{q_n(t)}{q_{n+1}(t)}\right), \tag{3}$$

with $\gcd(q_1, \ldots, q_{n+1}) = 1$, can be embedded into $\mathbb{PR}^n$ as

$$\mathcal{Q}(t) = [q_1(t) : \cdots : q_{n+1}(t)]. \tag{4}$$

By an abuse of notation and since we will be working in $\mathbb{PR}^n$, we will also denote the projective parametrization as $\mathcal{Q}(t)$.

Given two rational curves $\mathcal{C}_1, \mathcal{C}_2 \subset \mathbb{R}^n$ rationally parametrized by projective parametrizations $\mathcal{Q}_1(t)$, $\mathcal{Q}_2(t)$, we will say that $\mathcal{C}_1, \mathcal{C}_2$ are *projectively equivalent* if there exists a projective transformation f mapping $\mathcal{C}_1$ onto $\mathcal{C}_2$; we say that f is a *projective equivalence* between $\mathcal{C}_1$ and $\mathcal{C}_2$. If f is an affine transformation (resp. an isometry or a similarity), we will say that $\mathcal{C}_1, \mathcal{C}_2$ are *affinely equivalent* (resp. *isometric* or *similar*), and that f is an *affine equivalence*. In Fig. 1, from left to right, we can see a deltoid and the curves resulting after applying an isometry, an affine transformation and a projective transformation, respectively, to the deltoid. Notice that the first three curves have the same topology; however, the last one has a different topology because the considered projective transformation maps some affine points of the deltoid to points at infinity.

In the following discussion we will assume that the parametrizations $\mathcal{Q}_1(t)$, $\mathcal{Q}_2(t)$ are *proper*, i.e. generically injective; one can always check whether or not a rational parametrization is proper, and properly reparametrize it in case it is not proper (see [10]).

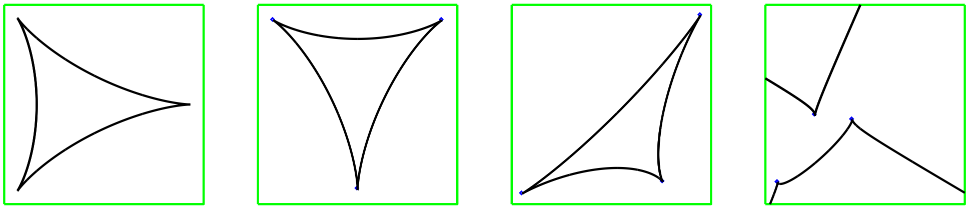

Fig. 1. From left to right: a deltoid, and its images under an isometry, an affine mapping and a projective transformation.

Suppose now that we are given two rational curves $\mathcal{C}_i$, properly parametrized by $\mathcal{Q}_i(t)$, $i = 1, 2$, and that f is a projective equivalence between $\mathcal{C}_i$. Since each $\mathcal{Q}_i(t)$ is proper by assumption, $\mathcal{Q}_i^{-1}$ exists for $i \in \{1, 2\}$. Thus, there exists a Möbius transformation φ,

$$\varphi(t) = \frac{at + b}{ct + d}, \; ad - bc \neq 0$$

making the following diagram commutative

$$\begin{tikzcd} \mathcal{C}_1 \arrow[r, "f"] & \mathcal{C}_2 \\ \mathbb{R} \arrow[u, dashed, "\mathcal{Q}_1"] \arrow[r, dashed, "\varphi"'] & \mathbb{R} \arrow[u, dashed, "\mathcal{Q}_2"'] \end{tikzcd} \tag{5}$$

Notice that the existence of φ follows from the fact that both $f \circ \mathcal{Q}_1$ and $\mathcal{Q}_2$ are proper parametrizations of $\mathcal{C}_2$; thus, they can differ only in a Möbius transformation (see [10]). We say that φ is *associated* with f. In particular,

$$f \circ \mathcal{Q}_1 = \mathcal{Q}_2 \circ \varphi. \tag{6}$$

2.2. μ-bases of rational curves

In this section we shall present the definition and properties of μ-bases for $(n + 1)$-polynomials in $\mathbb{R}[t]$, the ring of polynomials in one variable with real coefficients (see [4]).

In order to do this, let $\mathcal{C} \subset \mathbb{R}^n$ be a rational curve, not a line, and let $\mathcal{Q}(t)$ be a proper parametrization of $\mathcal{C}$ as in Eq. (4). Let $(q_1(t), \dots, q_{n+1}(t))$ be the vector which results from collecting the components in Eq. (4). Also, let $\text{syz}(q_1, \dots, q_{n+1})$ be the syzygy module consisting of all the vectors of polynomials

$$\boldsymbol{u}(t) = (p_1(t), \dots, p_{n+1}(t))$$

such that

$$\boldsymbol{u}(t) \cdot \mathcal{Q}(t) = p_1(t)q_1(t) + p_2(t)q_2(t) + \cdots + p_n(t)q_n(t) + p_{n+1}(t)q_{n+1}(t) = 0. \tag{7}$$

The set of these $(n+1)$-tuples has the structure of a free module $\text{syz}(\mathcal{Q}(t))$ over the ring $\mathbb{R}[t]$, with n generators (see [1]). This module is called the *syzygy module* of $\mathcal{Q}(t)$. Furthermore, each element in this module can be identified with a 1-parameter family of hyperplanes in $\mathbb{R}^n$

$$p_1(t)x_1 + \cdots + p_n(t)x_n + p_{n+1}(t)x_{n+1} = 0$$

with the property that for a fixed t, the corresponding hyperplane in the family has a common point with the curve $\mathcal{C}$, namely the point $\mathcal{Q}(t)$; this follows from Eq. (7). Such family is said to be *following* the curve $\mathcal{C}$, and is called a *moving hyperplane*.

We can write $\boldsymbol{u}(t) = (p_1(t), \dots, p_{n+1}(t))$ as

$$\boldsymbol{u}(t) = \sum_{i=0}^{k} (p_{i1}, \dots, p_{i(n+1)})t^i, \tag{8}$$

where the leading coefficient vector satisfies $(p_{k1}, \dots, p_{k(n+1)}) \neq 0$. In the following discussion, we define $\deg(\boldsymbol{u}) = \max\{\deg(p_1), \dots, \deg(p_{n+1})\}$, and we denote the vector defined by the leading coefficient of each component of the vector $(p_{k1}, \dots, p_{k(n+1)})$ by $\text{LV}(\boldsymbol{u})$.

In Definition 1, we introduce the notion of μ-basis. An equivalent definition is given in Definition 3.

Definition 1. A set of n vector polynomials $\{\boldsymbol{u}_1(t), \dots, \boldsymbol{u}_n(t)\}$, with each $\boldsymbol{u}_i(t)$ given as in Eq. (8), is called a *μ-basis* of the parametrization $\mathcal{Q}(t) = [q_1(t) : q_2(t) : \cdots : q_n(t) : q_{n+1}(t)]$ or equivalently, a μ-basis of the syzygy module *syz*$(q_1, \dots, q_{n+1})$, if

(1) $\{\boldsymbol{u}_1(t), \dots, \boldsymbol{u}_n(t)\}$ forms a basis of the syzygy module $syz(q_1, \dots, q_{n+1})$. That is, $\boldsymbol{u}_i(t) \in syz(q_1, \dots, q_{n+1})$ for $i = 1, \dots, n$, and any $\ell \in syz(q_1, \dots, q_{n+1})$ can be written uniquely as

$$\ell = h_1\boldsymbol{u}_1 + \cdots + h_n\boldsymbol{u}_n, \tag{9}$$

where h_i are polynomials in t.

(2) $LV(\boldsymbol{u}_1), \dots, LV(\boldsymbol{u}_n)$ are linearly independent.

We will assume that the elements $\boldsymbol{u}_1(t), \dots, \boldsymbol{u}_n(t)$ are ordered by increasing degree, i.e.

$$\deg(\boldsymbol{u}_1(t)) \le \cdots \le \deg(\boldsymbol{u}_n(t)), \tag{10}$$

and we will set $\mu = \deg(\boldsymbol{u}_1(t))$. The following theorem collects some properties of μ-bases (see [2,4]).

Theorem 2. *Let $\{\boldsymbol{u}_1(t), \dots, \boldsymbol{u}_n(t)\}$ be a μ-basis for $\mathcal{Q}(t)$ with $\deg(\boldsymbol{u}_1) \le \cdots \le \deg(\boldsymbol{u}_n)$. Then,*

(1) Every $\ell \in syz(q_1, \dots, q_{n+1})$ can be written as in Eq. (9) with $\deg(h_i\boldsymbol{u}_i) \le \deg(\ell)$, $i = 1, \dots, n$.
(2) If $\boldsymbol{v}_1(t), \dots, \boldsymbol{v}_n(t)$ is a set of polynomials in $syz(q_1, \dots, q_{n+1})$ that are linearly independent over the polynomial ring $\mathbb{R}[t]$ with $\deg(\boldsymbol{v}_1) \le \cdots \le \deg(\boldsymbol{v}_n)$, then $\deg(\boldsymbol{u}_i) \le \deg(\boldsymbol{v}_i)$, $i = 1, \dots, n$.
(3) If $\{\boldsymbol{v}_1(t), \dots, \boldsymbol{v}_n(t)\}$ is another μ-basis for $\mathcal{Q}(t)$ with $\deg(\boldsymbol{v}_1) \le \cdots \le \deg(\boldsymbol{v}_n)$, then $\deg(\boldsymbol{u}_i) = \deg(\boldsymbol{v}_i)$, $i = 1, \dots, n$.
(4) The outer product of $\boldsymbol{u}_1(t), \dots, \boldsymbol{u}_n(t)$ is equal to $c \cdot \mathcal{Q}(t)$ for some non-zero constant $c \in \mathbb{R} - \{0\}$.
(5) $\sum_{i=1}^{n} \deg(\boldsymbol{u}_i) = \deg(\mathcal{Q})$.

Remark 1. The generalized outer product operation $\boldsymbol{u}_1(t) \times \boldsymbol{u}_2(t) \times \cdots \times \boldsymbol{u}_n(t)$ referred to in statement (4) of Theorem 2 corresponds to the value of the determinant whose rows are the components of the $\boldsymbol{u}_i$.

Some of the properties stated in Theorem 2 are used in certain references (see for instance [4]) to give another, equivalent, definition of a μ-basis, which is provided here.

Definition 3. A set $\{\boldsymbol{u}_1(t), \dots, \boldsymbol{u}_n(t)\} \in syz(\mathcal{Q}(t))$ is called a *μ-basis* of $\mathcal{Q}(t)$ if

$$\boldsymbol{u}_1(t) \times \boldsymbol{u}_2(t) \times \cdots \times \boldsymbol{u}_n(t) = c \cdot \mathcal{Q}(t), \tag{11}$$

where $c \in \mathbb{R} - \{0\}$ and $\deg(\boldsymbol{u}_1) + \cdots + \deg(\boldsymbol{u}_n) = \deg(\mathcal{Q})$.

A μ-basis always exists, and algorithms to compute it have been provided in the literature [1,3,4]. Furthermore, μ-bases are not unique, but the sequence of degrees in any μ-basis is certainly unique (see statement (3) in Theorem 2). In particular, given $\mathcal{Q}(t)$ and a μ-basis $\{\boldsymbol{u}_1(t), \dots, \boldsymbol{u}_n(t)\}$, one can consider the subset $\{\boldsymbol{u}_1(t), \dots, \boldsymbol{u}_{i_0}(t)\}$ of elements of the μ-basis whose degree is equal to $\mu = \deg(\boldsymbol{u}_1(t))$: then, from statement (3) in Theorem 2, the number i_0 is an invariant for all μ-bases of $\mathcal{Q}(t)$. This observation is essential for the problem treated in this paper. Furthermore, from statement (1) in Theorem 2, for any other μ-basis of $\mathcal{Q}(t)$, and assuming that their elements are ordered by increasing degrees, the first i_0 elements of the new μ-basis must be linear combinations of $\boldsymbol{u}_1(t), \dots, \boldsymbol{u}_{i_0}(t)$. We express this property by saying that the elements $\{\boldsymbol{u}_1(t), \dots, \boldsymbol{u}_{i_0}(t)\}$ are *unique* up to linear combinations or just *unique*, for short. Additionally, if $i_0 = 1$ then $\boldsymbol{u}_1(t)$ is unique up to multiplication by a non-zero constant, i.e. any other μ-basis of $\mathcal{Q}(t)$ must have $\boldsymbol{u}_1(t)$ (or a multiple of $\boldsymbol{u}_1(t)$) as its first element. We refer to the elements of $\{\boldsymbol{u}_1(t), \dots, \boldsymbol{u}_{i_0}(t)\}$ as the elements of least degree, or smallest degree, or minimal degree of the μ-basis.

3. Projective equivalences and μ-bases (I): results

The goal of this section is to explore how the projective equivalences between two parametric curves in $\mathbb{R}^n$ are inherited by the elements of smallest degree in their μ-bases. In order to see this, let $\mathcal{C}_1, \mathcal{C}_2 \subset \mathbb{R}^n$ be two rational curves properly and rationally parametrized by $\mathcal{Q}_1(t)$, $\mathcal{Q}_2(t)$, and let $f(\mathbf{x}) = \mathcal{A}\mathbf{x}$, as in Eq. (1), be a projective equivalence between $\mathcal{C}_1, \mathcal{C}_2$. Furthermore, let $\mathcal{I} = \{1, \dots, n\}$, and let $\{\boldsymbol{u}_i(t)\}_{i\in\mathcal{I}}$, $\{\boldsymbol{v}_i(t)\}_{i\in\mathcal{I}}$ be μ-bases of $\mathcal{Q}_1(t)$, $\mathcal{Q}_2(t)$, where we assume that the $\boldsymbol{u}_i(t)$ and the $\boldsymbol{v}_i(t)$ are given by increasing degree. Furthermore, we set $\mu_1 = \deg(\boldsymbol{u}_1(t))$, $\mu_2 = \deg(\boldsymbol{v}_1(t))$, and we represent by $\mathcal{J}_1$ and $\mathcal{J}_2$ the subsets of $\{1, \dots, n\}$ corresponding to the elements of the μ-bases $\{\boldsymbol{u}_i(t)\}_{i\in\mathcal{I}}$, $\{\boldsymbol{v}_i(t)\}_{i\in\mathcal{I}}$ whose degrees are μ_1 and μ_2 respectively. Thus, if $\mathcal{J}_1 = \{1, \dots, i_0\}$ then $\deg(\boldsymbol{u}_i(t)) = \mu_1$ for every $i = 1, \dots, i_0$; analogously for $\mathcal{J}_2$.

We first need the following lemma, which is a reformulation of Lemma 2 in [11].

Lemma 4. *Let $\mathcal{C} \subset \mathbb{R}^n$ be a rational curve projectively parametrized by $\mathcal{Q}(t)$, and let $f(\mathbf{x}) = \mathcal{A}\mathbf{x}$ be a projective transformation. Let $\{\boldsymbol{u}_i(t)\}_{i\in\mathcal{I}}$ be a μ-basis of $\mathcal{Q}(t)$. Then $\{\mathcal{A}^{-T}\boldsymbol{u}_i(t)\}$ is a μ-basis of $(f \circ \mathcal{Q})(t)$.*

From Lemma 4, if

$$\{\boldsymbol{u}_1(t), \dots, \boldsymbol{u}_n(t)\} \tag{12}$$

is a μ-basis of $\mathcal{Q}_1(t)$, which parametrizes $\mathcal{C}_1$, then

$$\{\mathcal{A}^{-T}\boldsymbol{u}_1(t), \dots, \mathcal{A}^{-T}\boldsymbol{u}_n(t)\} \tag{13}$$

is a μ-basis of $(f \circ \mathcal{Q}_1)(t)$, which parametrizes $\mathcal{C}_2$ because f is a projective equivalence between $\mathcal{C}_1$ and $\mathcal{C}_2$. Since projective transformations preserve the degree, we have the following result.

Lemma 5. *If $\mathcal{C}_1$ and $\mathcal{C}_2$ are related by a projective equivalence, then $\mathcal{J}_1 = \mathcal{J}_2$. In particular, $\boldsymbol{u}_1(t)$ is unique if and only if $\boldsymbol{v}_1(t)$ is unique.*

Taking Lemma 5 into account, let us set $\mathcal{J}_1 = \mathcal{J}_2 = \mathcal{J}$. Now since f is a projective equivalence between $\mathcal{C}_1$ and $\mathcal{C}_2$, by Eq. (5) $f \circ \mathcal{Q}_1 = \mathcal{Q}_2 \circ \varphi$ where φ is the Möbius transformation associated with f. In particular, Eq. (13) is a μ-basis of $\mathcal{Q}_2 \circ \varphi$. Additionally, by Lemma 2 in [6]

$$\{(\boldsymbol{v}_1 \circ \varphi)(t), \dots, (\boldsymbol{v}_n \circ \varphi)(t)\} \tag{14}$$

is also a μ-basis of $\mathcal{Q}_2 \circ \varphi$. Since $f \circ \mathcal{Q}_1 = \mathcal{Q}_2 \circ \varphi$, Eqs. (13) and (14) are both μ-bases of $\mathcal{Q}_2 \circ \varphi$.

We distinguish now the cases when $\mathcal{J}$ consists of just one element or more than one element. In the first case, by Lemma 5 both $\boldsymbol{u}_1(t)$ and $\boldsymbol{v}_1(t)$ are unique.

If $\boldsymbol{v}_1(t)$ is unique up to multiplication by a non-zero constant, $(\boldsymbol{v}_1 \circ \varphi)(t)$, as an element of a μ-basis of $\mathcal{Q}_2 \circ \varphi$, is also unique up to multiplication by a non-zero constant. Recall that Eq. (13) is also a μ-basis of $\mathcal{Q}_2 \circ \varphi$. Furthermore, since projective transformations preserve the degree, we deduce that $\mathcal{A}^{-T}\boldsymbol{u}_1(t)$ is the element of smallest degree in Eq. (13). And by the uniqueness of the first element in the μ-basis, we get that

$$\mathcal{A}^{-T}\boldsymbol{u}_1(t) = \lambda(\boldsymbol{v}_1 \circ \varphi)(t) \tag{15}$$

for some nonzero constant λ. Calling $\gamma = \frac{1}{\lambda}$, we deduce that

$$\gamma\mathcal{A}^{-T}\boldsymbol{u}_1(t) = (\boldsymbol{v}_1 \circ \varphi)(t). \tag{16}$$

But this implies that the rational curves in $\mathbb{R}^n$ defined by $\boldsymbol{u}_1(t), \boldsymbol{v}_1(t)$ are projectively equivalent, and are related by the projective transformation $g(\mathbf{x}) = \mathcal{B}\mathbf{x}$, where $\mathcal{B} = \gamma\mathcal{A}^{-T}$. Moreover, since $\mathcal{B}$ represents the matrix of a projective transformation, we can safely make $\gamma = 1$. Thus, we have the following result, which summarizes these ideas.

Theorem 6. *Let $\mathcal{C}_1, \mathcal{C}_2 \subset \mathbb{R}^n$ be two rational curves properly and rationally parametrized by $\mathcal{Q}_1(t)$, $\mathcal{Q}_2(t)$, and let $f(\mathbf{x}) = \mathcal{A}\mathbf{x}$ as in Eq. (1) be a projective equivalence between $\mathcal{C}_1, \mathcal{C}_2$. Furthermore, let $\mathcal{I} = \{1, \dots, n\}$, and let $\{\boldsymbol{u}_i(t)\}_{i\in\mathcal{I}}$, $\{\boldsymbol{v}_i(t)\}_{i\in\mathcal{I}}$ be μ-bases of $\mathcal{Q}_1(t)$, $\mathcal{Q}_2(t)$. If $\boldsymbol{u}_1(t)$, $\boldsymbol{v}_1(t)$ are unique up to multiplication by a non-zero constant, then $g(\mathbf{x}) = \mathcal{A}^{-T}\mathbf{x}$ is a projective equivalence between the curves defined by $\boldsymbol{u}_1(t)$, $\boldsymbol{v}_1(t)$ in $\mathbb{R}^n$. Furthermore, if $\boldsymbol{u}_1(t)$ and $\boldsymbol{v}_1(t)$ are proper, then the Möbius function associated with g coincides with the Möbius function associated with f.*

Remark 2. Notice that $\boldsymbol{u}_1(t)$, $\boldsymbol{v}_1(t)$ need not be proper. Still, Eq. (16) implies that the curves in $\mathbb{R}^n$ defined by $\boldsymbol{u}_1(t)$, $\boldsymbol{v}_1(t)$ are projectively equivalent, and in fact are mapped to each other by $g(\mathbf{x}) = \mathcal{A}^{-T}\mathbf{x}$.

Theorem 6 provides the following corollary.

Corollary 7. *Suppose that the conditions in Theorem 6 hold. If $\mathcal{A}$ is orthogonal, then $f(\mathbf{x}) = \mathcal{A}\mathbf{x}$ is also a projective equivalence between the curves in $\mathbb{R}^n$ defined by $\boldsymbol{u}_1(t)$, $\boldsymbol{v}_1(t)$.*

In particular, Corollary 7 implies the following.

Corollary 8. *Suppose that the conditions in Theorem 6 hold.*

(1) If $\mathcal{A}$ represents an isometry f where $\mathbf{b} = \mathbf{0}$, then f is also an isometry between the curves in $\mathbb{R}^n$ defined by $\boldsymbol{u}_1(t)$, $\boldsymbol{v}_1(t)$.
(2) If $\mathcal{C}_1 = \mathcal{C}_2 = \mathcal{C}$ and $\mathcal{A}$ represents a symmetry f of $\mathcal{C}$ with a fixed point, then f is also a symmetry of the curve in $\mathbb{R}^n$ defined by $\boldsymbol{u}_1(t)$.

Now we consider the case when $\mathcal{J}$ consists of more than one element. In this case, $\{\boldsymbol{v}_1(t), \dots, \boldsymbol{v}_{i_0}(t)\}$, as elements of a μ-basis of $\mathcal{Q}_2(t)$, are unique up to linear combinations; similarly for $\{(\boldsymbol{v}_1 \circ \varphi)(t), \dots, (\boldsymbol{v}_{i_0} \circ \varphi)(t)\}$ as elements of a μ-basis of $(\mathcal{Q}_2 \circ \varphi)(t)$. Since projective transformations preserve the degree and Eq. (13) is also a μ-basis of $\mathcal{Q}_2(t)$, we get that each $\mathcal{A}^{-T}\boldsymbol{u}_j(t)$, with $j \in \{1, \dots, i_0\}$, must be a linear combination of $\{(\boldsymbol{v}_1 \circ \varphi)(t), \dots, (\boldsymbol{v}_{i_0} \circ \varphi)(t)\}$, i.e. for $j \in \{1, \dots, i_0\}$ there exist constants $\lambda_1^{(j)}, \dots, \lambda_{i_0}^{(j)}$ such that

$$\mathcal{A}^{-T}\boldsymbol{u}_j(t) = \lambda_1^{(j)}(\boldsymbol{v}_1 \circ \varphi)(t) + \cdots + \lambda_{i_0}^{(j)}(\boldsymbol{v}_{i_0} \circ \varphi)(t). \tag{17}$$

We summarize these ideas in the following result.

Theorem 9. *Let $\mathcal{C}_1, \mathcal{C}_2 \subset \mathbb{R}^n$ be two rational curves properly and rationally parametrized by $\mathcal{Q}_1(t)$, $\mathcal{Q}_2(t)$, and let $f(\mathbf{x}) = \mathcal{A}\mathbf{x}$ as in Eq. (1) be a projective equivalence between $\mathcal{C}_1, \mathcal{C}_2$. Furthermore, let $\mathcal{I} = \{1, \dots, n\}$, and let $\{\boldsymbol{u}_i(t)\}_{i\in\mathcal{I}}$, $\{\boldsymbol{v}_i(t)\}_{i\in\mathcal{I}}$ be μ-bases of $\mathcal{Q}_1(t)$, $\mathcal{Q}_2(t)$. If $\{\boldsymbol{u}_1(t), \dots, \boldsymbol{u}_{i_0}(t)\}$ and $\{\boldsymbol{v}_1(t), \dots, \boldsymbol{v}_{i_0}(t)\}$ are unique up to linear combinations, then for each $j \in \{1, \dots, i_0\}$ there exist constants $\lambda_1^{(j)}, \dots, \lambda_{i_0}^{(j)}$ such that $g(\mathbf{x}) = \mathcal{A}^{-T}\mathbf{x}$ is a projective equivalence between the curves in $\mathbb{R}^n$ defined by $\boldsymbol{u}_1(t)$*

and $\lambda_1^{(j)}\boldsymbol{v}_1(t)+\cdots+\lambda_{i_0}^{(j)}\boldsymbol{v}_{i_0}(t)$*. Furthermore, if* $\boldsymbol{u}_1(t)$ *and* $\lambda_1^{(j)}\boldsymbol{v}_1(t)+\cdots+\lambda_{i_0}^{(j)}\boldsymbol{v}_{i_0}(t)$ *are proper, then the Möbius function associated with* g *coincides with the Möbius function associated with* f*.*

Theorems 6 and 9 are useful because they allow to reduce the search of the projective equivalences between $\mathcal{C}_1$ and $\mathcal{C}_2$ to the projective equivalences between curves with smaller degrees. Nevertheless, notice that while each projective equivalence between the $\mathcal{C}_i$ gives rise to a projective equivalence between the curves corresponding to elements of minimal degree in the μ-bases, the converse is not true, i.e. not every projective equivalence between the μ-bases corresponds to a projective equivalence between the $\mathcal{C}_i$. In other words, we must test the projective equivalences computed between the elements of minimal degree of the μ-bases, to check which ones correspond to projective equivalences between $\mathcal{C}_1$ and $\mathcal{C}_2$.

Applying Theorems 6 and 9 requires knowing if $\boldsymbol{u}_1(t)$, $\boldsymbol{v}_1(t)$ are unique or not. In the next section we will characterize this situation, and we will provide an algorithm to find $\{\boldsymbol{u}_i(t)\}_{i\in\mathcal{J}}$, $\{\boldsymbol{v}_i(t)\}_{i\in\mathcal{J}}$ without computing the whole μ-basis. We end this section with the following two examples.

Example 1. Let $\mathcal{C}_1, \mathcal{C}_2 \subset \mathbb{R}^2$ be the two planar curves defined by

$$\mathcal{Q}_1(t) = [q_1(t) : q_2(t) : q_3(t)],\ \ \mathcal{Q}_2(t) = [r_1(t) : r_2(t) : r_3(t)],$$

where

$$\begin{array}{rcl} q_1(t) & = & -809t^7 - 2167t^6 - 1734t^5 + 490t^4 + 2035t^3 + 1539t^2 + 567t + 79, \\ q_2(t) & = & -7t^7 + 19t^6 + 8t^5 - 80t^4 + 105t^3 - 53t^2 + 6t + 2, \\ q_3(t) & = & 2187t^7 + 10206t^6 + 20412t^5 + 22680t^4 + 15120t^3 + 6048t^2 + 1344t + 128 \end{array}$$

and

$$\begin{array}{rcl} r_1(t) & = & 117t^7 - 537t^6 + 378t^5 - 1115t^4 - 480t^3 - 876t^2 - 434t - 49, \\ r_2(t) & = & 342t^7 - 1467t^6 + 1918t^5 - 1915t^4 + 470t^3 - 251t^2 + 6t + 81, \\ r_3(t) & = & 223t^7 - 958t^6 + 1372t^5 - 1360t^4 - 170t^3 - 719t^2 - 456t - 126. \end{array}$$

The first element in the μ-basis of $\mathcal{Q}_1(t)$ is the curve

$$\boldsymbol{u}_1(t) = [87t^3 + 154t^2 + 106t + 28, -57t^3 - 104t^2 - 71t - 18, 32t^3 - 6t^2 - 9t - 17],$$

and is unique. The first element in the μ-basis of $\mathcal{Q}_2(t)$ is the curve

$$\boldsymbol{v}_1(t) = [-29t^3 + 81t^2 - 3t + 63, 51t^3 - 29t^2 + 47t - 7, -63t^3 - 3t^2 - 81t - 29],$$

which is also unique. Furthermore, both $\boldsymbol{u}_1(t)$ and $\boldsymbol{v}_1(t)$ are proper parametrizations. The computation, following [8], to find the projective equivalences $g(\mathbf{x}) = \mathcal{A}\mathbf{x}$ between $\boldsymbol{u}_1(t)$ and $\boldsymbol{v}_1(t)$ provides two equivalences, which is expected since one can check that the curves have symmetries. These projective equivalences correspond to

$$\mathcal{A}_1 = \begin{bmatrix} 1 & -1 & -1 \\ 1 & 1 & 1 \\ -1 & 1 & -1 \end{bmatrix},\ \ \varphi_1(t) = \frac{t}{t+1},$$

and

$$\mathcal{A}_2 = \begin{bmatrix} 1 & -1 & 1 \\ 1 & 1 & -1 \\ -1 & 1 & 1 \end{bmatrix},\ \ \varphi_2(t) = \frac{t+4}{7t+3},$$

where we have also included the Möbius functions in Eq. (6). One can directly check that for $i = 1, 2$, $\{f_i, \varphi_i\}$, with $f_i(\mathbf{x}) = \mathcal{A}_i^{-T}\mathbf{x}$, satisfy Eq. (6), so for $i = 1, 2$, $f_i(\mathbf{x}) = \mathcal{A}_i^{-T}\mathbf{x}$ are projective equivalences between $\mathcal{C}_1$ and $\mathcal{C}_2$.

Example 2. Let $\mathcal{C}_1, \mathcal{C}_2 \subset \mathbb{R}^3$ be the two space curves defined by

$$\mathcal{Q}_1(t) = [q_1(t) : q_2(t) : q_3(t) : q_4(t)],\ \ \mathcal{Q}_2(t) = [r_1(t) : r_2(t) : r_3(t) : r_4(t)],$$

where

$$\begin{array}{rcl} q_1(t) & = & (t-1)^2(16t^6 - 124t^5 + 388t^4 - 568t^3 + 438t^2 - 178t + 30), \\ q_2(t) & = & (t-1)^2(-56t^7 + 396t^6 - 1148t^5 + 1722t^4 - 1485t^3 + 742t^2 - 197t + 21), \\ q_3(t) & = & -8t^8 + 62t^7 - 194t^6 + 299t^5 - 220t^4 + 35t^3 + 59t^2 - 40t + 8, \\ q_4(t) & = & (16t^6 - 74t^5 + 96t^4 + 15t^3 - 124t^2 + 101t - 27)(t-1)^2 \end{array}$$

and

$$\begin{array}{rcl} r_1(t) & = & -10t^7 + 3t^6 + 28t^5 - 10t^4 + 17t^3 - 28t^2 - 41t - 39, \\ r_2(t) & = & t^8 - 9t^7 + 4t^6 + 7t^5 + 5t^4 + 19t^3 - 22t^2 - 13t - 40, \\ r_3(t) & = & t^8 - 4t^7 - 7t^5 + 18t^4 + 7t^3 + 5t^2 - 22t - 22, \\ r_4(t) & = & t^8 - 9t^7 + 3t^6 + 27t^5 - 15t^4 + 4t^3 - 76t + 17. \end{array}$$

In this case, the elements of a μ-basis of $\mathcal{Q}_1(t)$ with minimal degree are the following two curves of degree two:

$$\begin{aligned} \boldsymbol{u}_1(t) &= [2t^2-2t+1, (t-1)t, (t-1)(3t-3), 3t^2-5t+2], \\ \boldsymbol{u}_2(t) &= [(t-1)t, -t^2+t+1, (t-1)(11t-6), (t-1)^2], \end{aligned}$$

and the elements of a μ-basis of $\mathcal{Q}_2(t)$ with minimal degree are the following two curves, also of degree two:

$$\begin{aligned} \boldsymbol{v}_1(t) &= [5t+17/2, -7t-27/2, t^2+4t+6, -t^2-2t-9/2], \\ \boldsymbol{v}_2(t) &= [t^2-11t-11, -t^2+13t+17, -8t-6, t^2+5t+7]. \end{aligned}$$

From Theorem 9 and since $\boldsymbol{u}_1(t), \boldsymbol{u}_2(t)$ are proper, for every projective equivalence $f(\mathbf{x}) = \mathcal{A}\mathbf{x}$ between $\mathcal{Q}_1(t)$ and $\mathcal{Q}_2(t)$, with associated Möbius function φ, we must have $\lambda_i, \mu_i \in \mathbb{R}$ such that

$$\mathcal{A}^{-T}\boldsymbol{u}_i(t) = \lambda_i(\boldsymbol{v}_1 \circ \varphi)(t) + \mu_i(\boldsymbol{v}_2 \circ \varphi)(t), \tag{18}$$

for $i = 1, 2$. Eq. (18) for $i = 1$ gives rise to a system whose unknowns are λ_1, μ_1, the parameters of φ and the entries of the matrix defining a projective transformation between $\boldsymbol{u}_1(t)$ and $\lambda_1\boldsymbol{v}_1(t) + \mu_1\boldsymbol{v}_2(t)$. However, the system has infinitely many solutions. But if additionally we consider Eq. (18) for $i = 2$ too, then the system consisting of all the equations (i.e. the equations obtained from Eq. (18) for $i = 1, 2$) has only one solution, which corresponds to

$$\lambda_1 = 2,\ \mu_1 = 1,\ \lambda_2 = -2,\ \mu_2 = -2,\ \varphi(t) = \frac{t}{t-1}, \tag{19}$$

and

$$\mathcal{A} = \begin{bmatrix} 1 & 2 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ -1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \end{bmatrix}. \tag{20}$$

One can directly check that $f(\mathbf{x}) = \mathcal{A}\mathbf{x}$, with $\mathcal{A}$ in Eq. (20), and the $\varphi(t)$ in Eq. (19), satisfy Eq. (6). Thus, $f(\mathbf{x}) = \mathcal{A}\mathbf{x}$ is a projective equivalence between $\mathcal{C}_1$ and $\mathcal{C}_2$.

4. Computing the elements of minimal degree of the μ-basis

In the previous section we saw that the projective equivalences of the curves are somehow captured when we determine the projective equivalences between the elements of smallest degree of the μ-bases. Furthermore, we saw that the most advantageous case is the case when there is just one element of smallest degree.

In this section we will study the situation when there is just one element of minimal degree. Furthermore, we will provide an algorithm to compute the elements of a μ-basis by increasing order. This algorithm allows us to compute only the elements of minimal degree without computing the whole μ-basis. The procedure provided here is inspired by the algorithm given in [3] to compute a μ-basis of the syzygy module of $n+1$ polynomials of maximum degree d, in one variable. The method in [3], whose theoretical computational complexity is $\mathcal{O}(d^2n + d^3 + n^2)$, is based on Linear Algebra, and differs from other algorithms for computing μ-bases, like [1] or [4]. Let us also mention that the notion of a μ-basis in [12] is extended to arbitrary univariate polynomial matrices. In [12] one can find an efficient algorithm to compute a μ-basis for a univariate polynomial matrix, based on polynomial matrix factorization; the computational complexity of the algorithm is $\mathcal{O}(dn^4 + d^2n^3)$.

In order to do this, we consider a projective parametrization $\mathcal{Q}(t)$ with degree $\deg(\mathcal{Q}) = m$ of a curve $\mathcal{C} \subset \mathbb{R}^n$. Furthermore, for simplicity we will consider first the case $n = 2$, and then we will generalize the results to $n \geq 3$.

4.1. The case of plane curves

Let us write $\deg(\mathcal{Q}) = m = 2\kappa + \ell$, $\ell \in \{0, 1\}$, and let $\{\boldsymbol{u}_1(t), \boldsymbol{u}_2(t)\}$ be a μ-basis of $\mathcal{Q}(t)$ where $\deg(\boldsymbol{u}_1(t)) = \mu \leq \deg(\boldsymbol{u}_2(t))$. Notice that

$$\kappa = \lfloor m/2 \rfloor. \tag{21}$$

Furthermore, from statement (5) of Theorem 2 we get that $0 < \mu \leq \kappa$ and $\deg(\boldsymbol{u}_2(t)) = m - \mu$. The following lemma is proved in [6].

Lemma 10. *Let $\{\boldsymbol{u}_1(t), \boldsymbol{u}_2(t)\}$ be a μ-basis of $\mathcal{Q}(t)$ with $\deg(\boldsymbol{u}_1(t)) \leq \deg(\boldsymbol{u}_2(t))$.*

(1) If $\deg(\boldsymbol{u}_1(t)) < \deg(\boldsymbol{u}_2(t))$, $\boldsymbol{u}_1(t)$ is unique up to a nonzero constant scalar.
(2) If $\deg(\boldsymbol{u}_1(t)) = \deg(\boldsymbol{u}_2(t))$, $\{\boldsymbol{u}_1(t), \boldsymbol{u}_2(t)\}$ is unique up to a linear combination.

Lemma 10 provides the following corollary, which follows from statement (5) of Theorem 2.

Corollary 11.

(1) If $m = 2\kappa + 1$ then $\boldsymbol{u}_1(t)$ is unique. Furthermore, $\deg(\boldsymbol{u}_1(t)) < \deg(\boldsymbol{u}_2(t))$ *and* $\deg(\boldsymbol{u}_1(t)) \le \kappa - 1$.
(2) If $m = 2\kappa$ then $\boldsymbol{u}_1(t)$ is unique if and only if $\deg(\boldsymbol{u}_1(t)) \ne \deg(\boldsymbol{u}_2(t))$*, i.e. if and only if* $\deg(\boldsymbol{u}_1(t)) < \kappa$*.*

Now let us see how to compute the elements in the μ-basis by increasing degree. In order to do this, we recall the notation $\mathcal{Q}(t) = [q_1(t) : q_2(t) : q_3(t)]$ and we consider a vector polynomial $\boldsymbol{u}(t) = (p_1(t), p_2(t), p_3(t))$ with $\deg(\boldsymbol{u}) = \mu$, where

$$p_i = a_{\mu i}t^{\mu} + \cdots + a_{0i},\ \ i = 1, 2, 3.$$

We impose the condition that $\boldsymbol{u}(t)$ belongs to the syzygy module $\mathrm{syz}(q_1, q_2, q)$,

$$\begin{aligned}
&0 = q_1p_1 + q_2p_2 + q_3p_3 = \\
&= t^{\mu}(q_1a_{\mu 1} + q_2a_{\mu 2} + qa_{\mu 3}) + t^{\mu-1}(q_1a_{(\mu-1)1} + q_2a_{(\mu-1)2} + q_3a_{(\mu-1)3}) + \cdots \\
&\cdots + (q_1a_{01} + q_2a_{02} + q_3a_{03})
\end{aligned}$$

(see Eq. (7)). Also, let us write

$$q_i = b_{mi}t^m + \cdots + b_{0i},\ \ i = 1, 2, \qquad q_3 = b_mt^m + \cdots + b_0.$$

Thus, we get a homogeneous system $\mathcal{S}_{\mu}$ with $(m+\mu+1)$ equations and $3(\mu+1)$ unknowns (the a_{ij}, with $i \in \{0, 1, \dots, \mu\}$, $j \in \{1, 2, 3\}$). We will write the system $\mathcal{S}_{\mu}$ as $(M_{\mu}|I) = \mathbf{0}$, with

$$I = \begin{pmatrix} a_{\mu 1} & a_{\mu 2} & a_{\mu 3} & a_{(\mu-1)1} & a_{(\mu-1)2} & a_{(\mu-1)3} & \cdots & a_{01} & a_{02} & a_{03} \end{pmatrix}^T,$$

and

$$M_{\mu} = \left(\begin{array}{ccccccccccccc}
 & & | & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\
 & C & | & & & | & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\
 & & | & & C & | & & & | & \dots & \vdots & \vdots & \vdots \\
 & & | & & & | & & C & | & \dots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & & & | & & & | & \dots & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & & & | & \dots & | & & \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \dots & | & C & \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & | & &
\end{array}\right), \tag{22}$$

which is an $(m + \mu + 1) \times 3(\mu + 1)$ matrix where C is the $(m + 1) \times 3$ matrix

$$C = \begin{pmatrix} b_{m1} & b_{m2} & b_m \\ b_{(m-1)1} & b_{(m-1)2} & b_{(m-1)} \\ \vdots & \vdots & \vdots \\ b_{01} & b_{02} & b_0 \end{pmatrix}. \tag{23}$$

Observe that C, as a box, appears $\mu + 1$ times in the matrix M_{μ}. If the system $(M_{\mu}|I) = \mathbf{0}$ has nontrivial solutions, these solutions provide the coefficients of the vector(s) polynomial(s) with degree equal to μ. In particular, the solution provides $\boldsymbol{u}_1(t)$, when $\boldsymbol{u}_1(t)$ is unique, or $\{\boldsymbol{u}_1(t), \boldsymbol{u}_2(t)\}$, when the degree of both elements in the μ-basis is the same. Certainly, a priori we do not know the value of μ: however, we can set $\mu := 1$, check if the system $(M_{\mu}|I) = \mathbf{0}$ has nontrivial solutions, and make $\mu := \mu + 1$ in case it does not. Then we recursively repeat this scheme.

Observe that one may consider different approaches for dealing with this recursive search. For instance, let us consider a planar curve of degree $2\kappa + 1$. In this case, generically the lowest degree element of the μ-basis has degree κ. Using the approach suggested above, one would need to test κ cases starting from degree 1. A binary search would start by testing degree $\kappa/2$. If no syzygy of degree $\kappa/2$ is found, then we try the value midway between $\kappa/2$ and κ. If a syzygy of degree $\kappa/2$ is found, then we try the value midway between 0 and $\kappa/2$, and so on. The speed of this binary search is worst case $\mathcal{O}(\ln(\kappa))$, whereas the speed of the linear search algorithm starting from degree 1 is worst cast $\mathcal{O}(\kappa)$.

4.2. The case of curves in $\mathbb{R}^n$

In this subsection we deal with the general case of a projective parametrization $\mathcal{Q}(t)$ of degree $m = \deg(\mathcal{Q})$ of a curve $\mathcal{C} \subset \mathbb{R}^n$. In order to do this, let $\{\boldsymbol{u}_1(t), \dots, \boldsymbol{u}_n(t)\}$, where $\deg(\boldsymbol{u}_1(t)) \le \cdots \le \deg(\boldsymbol{u}_n(t))$, be a μ-basis of $\mathcal{Q}(t)$. We denote $\mu_i = \deg(\boldsymbol{u}_i(t))$ for $i = 1, \dots, n$,

$$\kappa = \lfloor m/n \rfloor, \tag{24}$$

and we write $m = n\kappa + \ell$, where $0 \le \ell < n$. First we generalize Lemma 10.

Proposition 12. *Let $\{\boldsymbol{u}_1(t), \ldots, \boldsymbol{u}_n(t)\}$ be a μ-basis of $\mathcal{Q}(t)$ with $\mu_1 \leq \mu_2 \leq \cdots \leq \mu_n$, where $\deg(\boldsymbol{u}_i) = \mu_i,\ i = 1, \ldots, n$, and $\deg(\mathcal{Q}) = m = n\kappa + \ell,\ 0 \leq \ell < n$. The following statements are true.*

(1) The number μ_1 satisfies that $0 \leq \mu_1 \leq \kappa$.
(2) If $\mu_1 < \mu_2$ then $\boldsymbol{u}_1(t)$ is unique up to a nonzero constant scalar
(3) If $\mu_1 = \mu_2 < \mu_3$ then $\{\boldsymbol{u}_1(t), \boldsymbol{u}_2(t)\}$ is unique up to linear combinations.
(4) If $\mu_1 = \cdots = \mu_k < \mu_{k+1}$ for some $2 \leq k \leq n$ then $\{\boldsymbol{u}_1(t), \ldots, \boldsymbol{u}_k(t)\}$ is unique up to linear combinations.
(5) If $\mu_1 = m/n$, in which case $m = n\kappa$, then $\mu_1 = \mu_2 = \cdots = \mu_n$, and $\{\boldsymbol{u}_1(t), \ldots, \boldsymbol{u}_n(t)\}$ is unique up to linear combinations.

Proof.

(1) From Definition 3 we get that $\mu_1 + \cdots + \mu_n = m$. If $\mu_1 > \kappa$ then for $i = 1, \ldots, n$ we have $\mu_i \geq \kappa + 1$. Thus,

$$m = n\kappa + \ell = \sum_{i=1}^{n} \mu_i \geq n(\kappa + 1),$$

which is impossible since $\ell < n$.

(2) Assume that $\mu_1 < \mu_2$, and suppose that there exists $\tilde{\boldsymbol{u}}_1(t) \neq \boldsymbol{u}_1(t)$ belonging to a μ-basis of $\mathcal{Q}(t)$, with $\deg(\tilde{\boldsymbol{u}}_1(t)) = \mu_1$. Then from Definition 3, $\boldsymbol{u}_1(t) \cdot \mathcal{Q}(t) = 0$ and $\tilde{\boldsymbol{u}}_1(t) \cdot \mathcal{Q}(t) = 0$. But this cannot happen since $\deg(\tilde{\boldsymbol{u}}_1(t)) + \mu_1 + \mu_2 + \cdots + \mu_n < \deg(\mathcal{Q}(t))$.

(3) Assume that $\mu_1 = \mu_2$, and suppose that there exists another μ-basis different from the basis $\{\boldsymbol{u}_1(t), \boldsymbol{u}_2(t), \boldsymbol{u}_3(t), \ldots, \boldsymbol{u}_n(t)\}$ (although with the same degrees). Let us write this μ-basis as $\{\tilde{\boldsymbol{u}}_1(t), \tilde{\boldsymbol{u}}_2(t), \boldsymbol{u}_3(t), \ldots, \boldsymbol{u}_n(t)\}$. By the definition of a μ-basis, it holds that $\tilde{\boldsymbol{u}}_1(t) = \sum_{i=1}^{n} \alpha_i(t)\boldsymbol{u}_i(t)$ with $\mu_1 = \mu_2 < \mu_3$, and that the leading vectors $LV(\boldsymbol{u}_i)$ of $\boldsymbol{u}_i(t)$, $i = 1, \ldots, n$ linearly independent. Hence $\alpha_j = 0,\ j = 3, \ldots, n$, i.e. $\tilde{\boldsymbol{u}}_1(t) = \alpha_1(t)\boldsymbol{u}_1(t) + \alpha_2(t)\boldsymbol{u}_2(t)$. Similarly, one also has that $\tilde{\boldsymbol{u}}_2(t) = \beta_1(t)\boldsymbol{u}_1(t)+\beta_2(t)\boldsymbol{u}_2(t)$. According to the properties of a μ-basis, $\deg(\tilde{\boldsymbol{u}}_1(t))+\mu_2+\cdots+\mu_n = m$ and $\tilde{\boldsymbol{u}}_1(t) \times \boldsymbol{u}_2(t) \times \cdots \times \boldsymbol{u}_n(t) = (\alpha_1(t)\boldsymbol{u}_1(t)+\alpha_2(t)\boldsymbol{u}_2(t)) \times \boldsymbol{u}_2(t) \times \cdots \times \boldsymbol{u}_n(t) = \alpha_1(t)\boldsymbol{u}_1(t) \times \boldsymbol{u}_2(t) \times \cdots \times \boldsymbol{u}_n(t) = \alpha_1(t)\mathcal{Q}(t)$. Since $\deg(\tilde{\boldsymbol{u}}_1(t) \times \boldsymbol{u}_2(t) \times \cdots \times \boldsymbol{u}_n(t)) \leq m$ one gets that $\alpha_1(t) \in \mathbb{K}$. Analogously for the other coefficients. Thus $(\tilde{\boldsymbol{u}}_1(t) \quad \tilde{\boldsymbol{u}}_2(t))^T = \begin{pmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{pmatrix} (\boldsymbol{u}_1 \quad \boldsymbol{u}_2)^T$ where the coefficient matrix is a nonsingular constant matrix.

(4) We argue as in statement (3) for $\{\boldsymbol{u}_1(t), \ldots, \boldsymbol{u}_k(t)\}$.

(5) Let $\mu_1 = m/n$. We know that $\mu_2 \geq \mu_1$, so assume that $\mu_2 > \mu_1 = m/n$. Since $\mu_j \geq \mu_2$ for $j = 3, \ldots, n$, we get that

$$\mu_1 + \mu_2 + \cdots + \mu_n = \frac{m}{n} + \mu_2 + \cdots + \mu_n > n \cdot \frac{m}{n} = m,$$

which cannot happen because $\mu_1 + \cdots + \mu_n = m$. Arguing analogously for the other μ_j and using statement (4), the result follows. □

Proposition 12 provides the following corollary, equivalent to Corollary 11.

Corollary 13. *If $m = n\kappa + \ell$, $0 < \ell < n$, $\kappa \geq 0$, then there exists $i_0 \in \{1, \ldots, n-1\}$ such that $\mu_1 = \cdots = \mu_{i_0} < \mu_{i_0+1} \leq \cdots \leq \mu_n$ and $\mu_j \leq \kappa - 1$ for $j \in \{1, \ldots, i_0\}$. Furthermore, $\{\boldsymbol{u}_1(t), \ldots, \boldsymbol{u}_{i_0}(t)\}$ is unique up to a linear combination. In particular, if $i_0 = 1$ then $\boldsymbol{u}_1$ is unique up to a nonzero constant scalar.*

Now let us see how to compute the elements of a μ-basis by increasing order. We proceed as in Section 4.1, i.e. we consider an unknown polynomial vector $\boldsymbol{u}(t) = (p_1(t), \ldots, p_{n+1}(t))$ with $\deg(\boldsymbol{u}) = \mu$, where

$$p_i = a_{\mu i}t^{\mu} + \cdots + a_{0i},\ \ i = 1, \ldots, n+1,$$

and we impose the condition

$$0 = q_1p_1 + q_2p_2 + \cdots + q_{n+1}p_{n+1} =$$
$$= t^{\mu}(q_1a_{\mu 1} + q_2a_{\mu 2} + \cdots + q_{n+1}a_{\mu(n+1)}) + t^{\mu-1}(q_1a_{(\mu-1)1} + q_2a_{(\mu-1)2} + \cdots + q_{n+1}a_{(\mu-1)(n+1)}) + \cdots$$
$$\cdots + (q_1a_{01} + q_2a_{02} + \cdots + q_{n+1}a_{0(n+1)})$$

(see Eq. (7)), with

$$q_i = b_{mi}t^m + \cdots + b_{0i},\ \ i = 1, \ldots, n, \qquad q_{n+1} = b_mt^m + \cdots + b_0.$$

This way we get an homogeneous system $\mathcal{S}_{\mu}$ with $m + \mu + 1$ equations and $(n+1)(\mu+1)$ unknowns (a_{ij}), which can be written as $(M_{\mu}|I) = \mathbf{0}$, where

$$I = \begin{pmatrix} a_{\mu 1} & \cdots & a_{\mu(n+1)} & a_{(\mu-1)1} & \cdots & a_{(\mu-1)(n+1)} & \cdots & a_{01} & \cdots & a_{0(n+1)} \end{pmatrix}^T,$$

M_μ is an $(m+\mu+1)\times(n+1)(\mu+1)$ matrix with a structure analogous to Eq. (22), and C is the $(m+1)\times(n+1)$ matrix

$$C=\begin{pmatrix} b_{m1} & b_{m2} & \cdots & b_m \\ b_{(m-1)1} & b_{(m-1)2} & \cdots & b_{(m-1)} \\ \vdots & \vdots & \vdots & \\ b_{01} & b_{02} & \cdots & b_0 \end{pmatrix}.$$

Note that C appears $\mu+1$ times in the matrix M_μ.

As in Section 4.1, the nontrivial independent solutions of the linear system $(M_\mu|I)=\mathbf{0}$ with $\mu=\mu_1$ provide the coefficients of the vector polynomials in $\{\boldsymbol{u}_1(t),\dots,\boldsymbol{u}_{i_0}(t)\}$. Also as in Section 4.1, a priori we do not know the value of μ. Thus, we start fixing $\mu:=1$, and check whether or not $(M_\mu|I)=\mathbf{0}$ has nontrivial solutions. If it has trivial solutions, we set $\mu:=\mu+1$ and start again.

5. Projective equivalences and μ-bases (II): computation

In the previous sections we have not really provided a new approach, alternative to those in [7–9], to compute projective equivalences: rather, we have shown that in order to carry out the computation, we can replace the original curves by other curves of smaller degree. In this section we want to show how this replacement can benefit the computations when one uses the approaches in [7–9]. In order to do this, recall that we denote by m the degrees of the projective parametrizations $\mathcal{Q}_1(t)$, $\mathcal{Q}_2(t)$ of the curves $\mathcal{C}_1,\mathcal{C}_2\subset\mathbb{R}^n$ whose projective equivalences we want to find. The general idea is that in all the cases, computing the projective equivalences is carried out by solving a polynomial system whose degree is strongly related to the degree of the parametrizations involved [7,8] or by factoring a polynomial whose computation also depends on the degrees of the curve parametrizations [9].

5.1. Using the algorithm in [8]

In [8] one has a particularly detailed study of the degrees involved in the computations, which is useful to show how the results in this paper can help to simplify the process. The idea in [8] is essentially to use Eq. (6), which writing $f(\mathbf{x})=\mathcal{A}\mathbf{x}$ gives rise to

$$\mathcal{A}\mathcal{Q}_1(t)=\mathcal{Q}_2(\varphi(t)).$$

This equation leads to a system of polynomial equations which is linear in the entries of the matrix $\mathcal{A}$, and nonlinear in the coefficients of the Möbius transformation φ. By writing the entries of $\mathcal{A}$ in terms of φ, using the remaining equations in the system and exploiting the structure, we arrive (see Section 3.2 in [8]) to a polynomial system, which can be solved by using Gröbner bases, with the following features:

- Number of coefficients: 5 (the coefficients of the Möbius transformation plus one extra variable).
- The system contains 1 equation of degree $(m-n)(n+1)+1$.
- The system contains $(m-n)(n+1)$ equations of degree m.

In our case, using Theorems 6 and 9 in Section 3 we can transfer the problem to computing projective equivalences between the elements $\{\boldsymbol{u}_1(t),\dots,\boldsymbol{u}_{i_0}(t)\}$ and $\{\boldsymbol{v}_1(t),\dots,\boldsymbol{v}_{i_0}(t)\}$ of smallest degree of two μ-bases of $\mathcal{Q}_1(t)$ and $\mathcal{Q}_2(t)$. These elements can be computed by using the results in Section 4, which rely on elementary Linear Algebra, and are, therefore, computationally cheap.

The most advantageous case arises when $i_0=1$. In that case, the problem essentially reduces to computing the projective equivalences between the curves defined by $\boldsymbol{u}_1(t)$ and $\boldsymbol{v}_1(t)$. From statement (1) in Proposition 12, the degree of both $\boldsymbol{u}_1(t)$ and $\boldsymbol{u}_2(t)$ is bounded by $\kappa=\lfloor m/n\rfloor$, so when applying the algorithm in [8] we move from polynomials of degree m to polynomials of degrees bounded by m/n, resulting in a simpler polynomial system. In more detail, in this case, following [8], we need to solve a polynomial system with the following features:

- Number of coefficients: 5 (the coefficients of the Möbius transformation plus one extra variable).
- The system contains 1 equation of degree bounded by
  $$(\kappa-n)(n+1)+1.$$
- The system contains at most
  $$(\kappa-n)(n+1)$$
  equations of degree κ.

When $i_0\geq 2$, the problem can be transferred to the computation of the projective equivalences between, say, $\boldsymbol{u}_1(t)$, and an unknown linear combination of $\boldsymbol{v}_1(t),\dots,\boldsymbol{v}_{i_0}(t)$. Thus, again following [8], the coefficients of this linear combination, which are the coefficients $\lambda_1,\dots,\lambda_{i_0}$ on the right hand-side of Eq. (17) must also be included as unknowns of the polynomial system that we need to solve. Thus, the number of unknowns increases from 5 to $5 + i_0$, although the degree of the polynomials involved in the computation decreases due to the fact that the degree of $\boldsymbol{u}_1(t)$ and of $\boldsymbol{v}_1(t), \ldots, \boldsymbol{v}_{i_0}(t)$ is bounded by $\kappa = \lfloor m/n \rfloor$. So depending on the size of i_0, m, n we may or may not have an advantage. In more detail, in this case we have:

- Number of coefficients: 5+i_0
- The system contains 1 equation of degree bounded by
$$(\kappa + 1 - n)(n + 1) + 1.$$
- The system contains at most
$$(\kappa - n)(n + 1)$$
equations of degree $\kappa + 1$.

5.2. *Using the algorithms in [7,9]*

In [7] the projective equivalences between the curves are computed by first determining the projective equivalences between finite point sets corresponding to *stall points*, namely points in the curves where the osculating hyperplane has contact higher than expected. These stall points are captured as the roots of homogeneous forms of degrees $(m-n)(n+1)$. In [9], the authors address projective equivalences of space curves by means of differential invariants. In this case the projective equivalences are computed by factoring a gcd of two polynomials whose degrees are, roughly, linear functions in the degree m of the curves involved in the computations.

If there is a unique element of minimal degree in the μ-bases of the curves, in these two approaches we move from degree m to degree κ. The case when there is more than one element of minimal degree is still an advantage in the case of [7], since the polynomial system that needs to be solved has a smaller degree. In the case of [9] this is not so useful, since the algorithm in [9] requires to compute a gcd, which would be more complicated in the presence of the extra parameters $\lambda_1, \ldots, \lambda_{i_0}$.

5.3. *Further experiments*

In this subsection we report on experiments carried out in Maple with plane and space curves of higher degree. Some of the results of our experiments are shown in Table 1, where we provide the timings for seven plane curves, and seven space curves of various degrees. The description of the columns in Table 1 is as follows: "Deg". is the degree of the curves; N_μ is the number of curves of least degree in the μ-bases (notice that $N_\mu = 1$ implies that the element of least degree in the μ-basis of each curve is unique); D_μ is the smallest degree in the μ-basis; # is the number of computed equivalences; t_1 is the timing in seconds for computing projective equivalences *without* using μ-bases; t_μ is the timing in seconds for computing the curves of smallest degree in the μ-bases of the curves; t_2 is the timing in seconds of the computation of equivalences using μ-bases, i.e. applying our ideas. Finally, "Imp". is the percentage of improvement by applying our algorithm, which is computed in the following way: if $t_1 > 120$ we interrupt the computation, in which case we set Imp $= 100$; if $t_1 \leq 120$, we set
$$\text{Imp} = \frac{t_1 - (t_\mu + t_2)}{t_1} \cdot 100.$$

The parametrizations used in the examples can be found in the webpage of one of the authors [13]; furthermore, in the same webpage one can find Maple sheets corresponding to two of the examples in Table 1. For planar curves we implemented a simplified version of the algorithm in [8]; for space curves we used the implementation in [9], which is publicly available, except for Example 11, where we implemented the algorithm in [7], which is better suited for parameters. In all the cases we used the same algorithm for t_1 and t_2.

In Table 1 one can see that the benefit of using μ-bases is, in general, higher as the degree of the curves increases; in particular, the six examples shown in red correspond to examples whose execution we stopped after 120 s without using μ-bases, but that could be computed with the help of μ-bases. For curves of small degree, which do not appear in Table 1, existing algorithms for computing projective equivalences are fast and the benefit of using μ-bases is small or even non-existent, since we also need to compute the elements of minimal degree in the μ-bases.

Some facts worth mentioning that we observed in our experimentation were the following:

- When the element of smallest degree in the μ-basis is unique, using μ-bases is generally an advantage, an in some cases, as shown in Table 1, it allows us to perform a computation which is very costly to complete without this tool. Something that can happen, though, which we observed when picking random parametrizations, is that the coefficients of the μ-basis can be very big even for parametrizations of small coefficients. In several cases the advantage is kept despite of this, but in certain cases it can be lost.

Table 1
Experiments.

Ex.	Plane/Space	Deg.	N_μ	D_μ	#	t_1	t_μ	t_2	Imp.
1	Plane	18	2	9	1	11.109	2.875	7.000	11.11%
2	Plane	27	1	13	1	21.032	2.297	5.359	63.60%
3	Plane	32	2	16	0	16.750	2.641	7.328	40.48%
4	Plane	39	1	19	1	$>$ 120	5.734	16.969	100%
5	Plane	45	1	22	2	30.672	3.359	7.031	66.12%
6	Plane	59	1	19	1	$>$ 120	6.797	95.969	100%
7	Plane	64	2	32	2	$>$ 120	5.407	32.703	100%
8	Space	23	1	7	1	3.547	2.719	0.562	7.50%
9	Space	23	2	5	0	$>$ 120	4.156	1.120	100%
10	Space	40	1	12	1	18.813	3.782	5.781	49.17%
11	Space	41	1	8	2	7.000	2.672	1.875	35.04%
12	Space	54	1	18	1	24.250	4.719	8.797	44.26%
13	Space	64	1	22	1	$>$ 120	3.109	38.203	100%
14	Space	95	1	31	1	$>$ 120	5.781	90.468	100%

- When the element of smallest degree in the μ-basis is not unique, the polynomial system that we need to solve has more unknowns. If there are two elements of smallest degree the advantage can still be kept, but not always. For three or more elements the system is, in general, too complicated, and is better not to use μ-bases.
- One can use μ-bases repeatedly, i.e. one can transfer the computation of the projective equivalences to the elements of smallest degree, and in turn transfer the computation of the projective equivalences of the latter to their own μ-bases, etc. We did not take this into account in our experimentation, but that is certainly possible. Of course, the most advantageous case is the one when there is repeatedly a unique element of minimal degree in the μ-basis.
- Another limitation of the method is that if the elements of minimal degree in the μ-bases have very low degree (lines, for instance), then they have infinitely many projective equivalences, which is not really useful to compute the projective equivalences between the original curves.

6. Conclusion

We have shown that projective equivalences between two curves in $\mathbb{R}^n$ give rise to projective equivalences between the curves defining the elements of minimal degree of the μ-bases of the curves. If there exists just one element with minimal degree in the μ-bases, the projective transformations between the curves can be recovered from the projective transformations between the curves defined by these elements of minimal degree. Otherwise, the projective transformations between the curves can be recovered from the projective transformations between the curves defined by the elements of minimal degree of one of the curves, and linear combinations, with coefficients to be determined, of the elements of minimal degree of the other curve. On the computational side we have also shown how our results can help to seriously reduce the cost of computing projective equivalences between two curves in certain cases.

It is natural to wonder about the extension of these results to surfaces. Although μ-bases of rational surfaces do exist [14], the case of surfaces has not yet been completely well-understood. In particular, unlike curves, algorithms for computing μ-bases of surfaces are not simple except for some particular cases (ruled surfaces [15,16], quadric surfaces [17], surfaces of revolution [18], cyclides [19]). Also, the properties satisfied by the degrees of the elements of the μ-bases in the case of curves do not extend to the case of surfaces [14].

Although the extension of our results to surfaces is desirable, such an extension is not direct, and requires further research. On the one hand, it is still unclear whether the fact that certain properties of μ-bases of curves do not generalize to surfaces is an obstacle for generalizing our results. On the other hand, while in the case of curves we need to consider birational transformations of the line, for surfaces we need to consider birational transformations of the plane. These transformations are called *Cremona transformations*, and their structure is much more complicated than Möbius transformations. Additionally, it is not clear whether the notion of uniqueness that we have for μ-bases of curves can be extended to surfaces.

It should also be noted that the reduction approach of μ-bases could be loosely related to the reduction method in the recent paper [20], extending an earlier paper [21], for computing projective equivalences between rational surfaces.

References

[1] D.A. Cox, T.W. Sederberg, F. Chen, The moving line ideal basis of planar rational curves, Comput. Aided Geom. Design 15 (1998) 803–827.
[2] F. Chen, W. Wang, The μ-basis of a planar rational curve—properties and computation, Graph. Models 64 (2002) 368–381.
[3] H. Hong, Z. Hough, I.A. Kogan, Algorithm for computing μ-bases of univariate polynomials, J. Symbolic Comput. 80 (2017) 844–874.
[4] N. Song, R. Goldman, *mu*-Bases for polynomial systems in one variable, Comput. Aided Geom. Design 26 (2009) 217–230.
[5] F. Chen, W. Wang, Y. Liu, Computing singular points of plane rational curves, J. Symbolic Comput. 43 (2008) 92–117.
[6] S. Pérez-Díaz, L.-Y. Shen, Inversion, degree, reparametrization and implicitization of rational planar curves using μ-basis, Comput. Aided Geom. Design 84 (2021) 101957.

[7] M. Bizzarri, M. Lávička, J. Vršek, Computing projective equivalences of special algebraic varieties, J. Comput. Appl. Math. 367 (2020) 112438.
[8] M. Hauer, B. Jüttler, Projective and affine symmetries and equivalences of rational curves in arbitrary dimension, J. Symbolic Comput. 87 (2018) 68–86.
[9] U. Gözütok, H.A. Çoban, Y. Sağiroğlu, J.G. Alcázar, Using differential invariants to detect projective equivalences and symmetries of rational 3D curves, 2021, arXiv:2110.05436.
[10] J.R. Sendra, F. Winkler, S. Pérez-Díaz, Rational Algebraic Curves, Springer-Verlag, 2008.
[11] S. Pérez-Díaz, L.-Y. Shen, Computing the μ-bases of algebraic monoid curves and surfaces, Comput. Graph. 97 (2021) 78–87.
[12] H. Bingru, F. Chen, Computing μ-bases of univariate polynomial matrices using polynomial matrix factorization, J. Syst. Sci. Complex 34 (2021) 1189–1206.
[13] https://juange-alcazar.web.uah.es/Publications.htm.
[14] F. Chen, D. Cox, Y. Liu, The μ-basis and implicitization of a rational parametric surface, J. Symbolic Comput. 39 (2005) 689–706.
[15] F. Chen, W. Wang, Revisiting the μ-basis of a rational ruled surface, J. Symbolic Comput. 36 (2003) 699—716.
[16] L.-Y. Shen, Computing μ-bases from algebraic ruled surfaces, Comput. Aided Geom. Design 46 (2016) 125–130.
[17] F. Chen, L. Shen, J. Deng, Implicitization and parametrization of quadratic and cubic surfaces by μ-bases, Computing 79 (2007) 131—142.
[18] X. Shi, R. Goldman, Implicitizing rational surfaces of revolution using μ-bases, Comput. Aided Geom. Design 29 (2012) 348–362.
[19] X. Jia, Role of moving planes and moving spheres following dupin cyclides, Comput. Aided Geom. Design 31 (2014) 168–181.
[20] B. Jüttler, N. Lubbes, J. Schicho, Projective isomorphisms between rational surfaces, J. Algebra 594 (2022) 571–596.
[21] M. Hauer, B. Jüttler, J. Schicho, Projective and affine symmetries and equivalences of rational and polynomial surfaces, J. Comput. Appl. Math. 349 (2019) 424–437.