ACADEMIC PRESS

Available at www.ComputerScienceWeb.com
POWERED BY SCIENCE DIRECT®

Graphical Models 64 (2003) 368–381

Graphical Models

www.elsevier.com/locate/gmod

The μ-basis of a planar rational curve—properties and computation

Falai Chen[a,*] and Wenping Wang[b]

[a] *Department of Mathematics, University of Science and Technology of China, Hefei, Anhui 230026, PR China*

[b] *Department of Computer Science and Information Systems, University of Hong Kong, Hong Kong, PR China*

Received 29 October 2001 received in revised form 19 November 2002 accepted 3 December 2002

Abstract

A moving line $L(x,y;t)=0$ is a family of lines with one parameter t in a plane. A moving line $L(x,y;t)=0$ is said to follow a rational curve $\mathbf{P}(t)$ if the point $\mathbf{P}(t_0)$ is on the line $L(x,y;t_0)=0$ for any parameter value t_0. A μ-basis of a rational curve $\mathbf{P}(t)$ is a pair of lowest degree moving lines that constitute a basis of the module formed by all the moving lines following $\mathbf{P}(t)$, which is the syzygy module of $\mathbf{P}(t)$. The study of moving lines, especially the μ-basis, has recently led to an efficient method, called the *moving line method*, for computing the implicit equation of a rational curve [3,6]. In this paper, we present properties and equivalent definitions of a μ-basis of a planar rational curve. Several of these properties and definitions are new, and they help to clarify an earlier definition of the μ-basis [3]. Furthermore, based on some of these newly established properties, an efficient algorithm is presented to compute a μ-basis of a planar rational curve. This algorithm applies vector elimination to the moving line module of $\mathbf{P}(t)$, and has $O(n^2)$ time complexity, where n is the degree of $\mathbf{P}(t)$. We show that the new algorithm is more efficient than the fastest previous algorithm [7].

Keywords: Rational curve; Implicitization; Moving line; μ-Basis; Syzygy module

* Corresponding author.
E-mail addresses: chenfl@ustc.edu.cn (F. Chen), wenping@csis.hku.hk (W. Wang).

1524-0703/03/$ - see front matter
doi:10.1016/S1524-0703(02)00017-5

1. Introduction

A moving line is a family of lines with one parameter t in the plane, and can thus be represented by $L(x,y;t) \equiv A(t)x + B(t)y + C(t) = 0$, where $A(t), B(t), C(t)$ are polynomials. A moving line $L(x,y;t)$ is said to follow a rational curve $\mathbf{P}(t) = (a(t), b(t), c(t))$ if the point $\mathbf{P}(t_0)$ is on the line $L(x,y;t_0) = 0$ for any parameter value t_0. As a convention, we call a moving line that follows the curve $\mathbf{P}(t)$ a moving line of $\mathbf{P}(t)$. A μ-basis of a rational curve $\mathbf{P}(t)$ is a pair of lowest degree moving lines that constitute a basis of the module formed by all the moving lines of $\mathbf{P}(t)$.

The μ-basis of a planar rational curve has been proposed for computing the implicit equation of a planar rational curve [3]. Applying a variant of Bezout's resultant to the μ-basis, we can write the implicit equation of $\mathbf{P}(t)$ as an $(n-\mu) \times (n-\mu)$ determinant, where $0 < \mu \leqslant \lfloor n/2 \rfloor$; in contrast, with other resultant based methods, the implicit equation must be written either as an $n \times n$ determinant (using the Bezout resultant) or as a $2n \times 2n$ determinant (using the Sylvester resultant). In the generic case where $\mu = \lfloor n/2 \rfloor$, the implicit equation can be written as an $\lceil n/2 \rceil \times \lceil n/2 \rceil$ determinant. Thus, the μ-basis provides a compact solution to the implicitization of a planar rational curve.

Recent studies also show that the μ-basis can be used to derive inversion formulas or study the singular points of a planar rational curve [2]; besides, the rational parametric equation of the curve can easily be obtained from the μ-basis. Hence, the μ-basis serves as a compact and useful representation of a planar rational curve—connecting its implicit equation and parametric equation, and facilitating the study of many properties of the curve.

The definition and some properties of the μ-basis of a planar rational curve have been studied in [3]. However, the definition of the μ-basis has not been given consistently, and the properties, especially those characterizing properties, of the μ-basis have not been presented completely or systematically in the literature. In light of this, we present in Section 2 a list of properties and equivalent definitions of the μ-basis of a planar rational curve. Several of these properties and definitions are new and provide insight into efficient computation of the μ-basis. These results have recently been used in studying the reparameterization of rational ruled surfaces [1]. As an application, in Sections 3 we describe a new algorithm for computing the μ-basis of a planar rational curve, and show that, besides being conceptually simpler, this algorithm is more efficient than the previous known fastest algorithm for computing the μ-basis [7]. We conclude the paper in Section 4 with some open problems.

2. Definition and properties of μ-basis

We begin with some preliminary knowledge about modules. Let $\mathcal{R}[t]$ and $\mathcal{R}[x,y,t]$ be the polynomial rings over the field of real numbers, $\mathcal{R}$, and $\mathcal{R}[t]^d$ denote the set of d-dimensional row vectors with entries in $\mathcal{R}[t]$. A set of vector polynomials $\mathbf{M} \subset \mathcal{R}[t]^d$ is called a *module* over $\mathcal{R}[t]$ if $h_1\mathbf{f}_1 + h_2\mathbf{f}_2 \in \mathbf{M}$ for any $\mathbf{f}_1, \mathbf{f}_2 \in \mathbf{M}$ and $h_1, h_2 \in \mathcal{R}[t]$.

Suppose that $\mathbf{M} \subset \mathcal{R}[t]^d$ is a module. If there exists a finite set of elements $\mathbf{f}_i \in \mathbf{M}$, $i = 1, \ldots, m$, such that any $\mathbf{f} \in \mathbf{M}$ can be expressed by

$$\mathbf{f} = h_1\mathbf{f}_1 + \cdots + h_m\mathbf{f}_m, \tag{1}$$

with $h_i \in R[t]$, $i = 1, \ldots, m$, then $\mathbf{M}$ is said to be *finitely generated*, $\{\mathbf{f}_1, \ldots, \mathbf{f}_m\}$ is called a *generating set* of $\mathbf{M}$, and we write $\mathbf{M} = \langle \mathbf{f}_1, \ldots, \mathbf{f}_m \rangle$. If expression (1) is unique for any $\mathbf{f} \in \mathbf{M}$, then the generating set $\{\mathbf{f}_1, \ldots, \mathbf{f}_m\}$ is called a *basis* of the module $\mathbf{M}$. A finitely generated module over $\mathcal{R}[t]$ always has a basis and is called a free module [4].

Vector polynomials $\mathbf{g}_i(t)$ in $\mathcal{R}[t]^3$, $i = 1, 2, \ldots, m$, are said to be $\mathcal{R}[t]$-linearly independent if $\sum_{i=1}^{m} h_i(t)\mathbf{g}_i(t) = 0$, with $h_i(t) \in \mathcal{R}[t]$, implies $h_i(t) = 0$ for $i = 1, 2, \ldots, m$.

Let a planar rational curve be given by

$$\mathbf{P}(t) = (a(t), b(t), c(t)) \tag{2}$$

in homogeneous form, where $a(t)$, $b(t)$, $c(t) \in \mathcal{R}[t]$ are relatively prime. The degree of $\mathbf{P}(t)$ is defined to be $n \equiv \max\{\deg(a(t)), \deg(b(t)), \deg(c(t))\}$. For brevity, we will often denote $a(t), b(t)$, and $c(t)$ by a, b, and c, respectively, where there is no danger of confusion.

A *moving line* is a family of lines with one parameter t, defined by [5]

$$L(x, y; t) := A(t)x + B(t)y + C(t) = 0, \tag{3}$$

where $A(t), B(t), C(t) \in \mathcal{R}[t]$. The degree of $L(x, y; t)$ is defined to be

$$\deg(L(x, y; t)) \equiv \max\{\deg(A(t)), \deg(B(t)), \deg(C(t))\}.$$

For convenience, we also denote a moving line by $\mathbf{L}(t) \equiv (A(t), B(t), C(t))$.

The moving line (3) follows the rational curve $\mathbf{P}(t) = (a(t), b(t), c(t))$ if and only if

$$\mathbf{L}(t) \cdot \mathbf{P}(t) = A(t)a(t) + B(t)b(t) + C(t)c(t) \equiv 0. \tag{4}$$

A moving line $L(x, y; t) = 0$ follows the curve $\mathbf{P}(t)$ if the point $\mathbf{P}(t_0)$ is on the line $L(x, y; t_0) = 0$ for any parameter value t_0. So one may say that an arbitrary point $\mathbf{P}(t_0)$ of the curve $\mathbf{P}(t)$ is at the intersection of two different moving lines of $\mathbf{P}(t)$ with the same parameter value t_0.

The *moving line ideal* of a rational curve $\mathbf{P}(t)$ is defined to be

$$I_P = \{h_1(cx - a) + h_2(cy - b) \,|\, h_1, h_2 \in R[x, y, t]\} \subset R[x, y, t]. \tag{5}$$

Let J_1 denote the set of all polynomials of degree one in x and y but some finite degree in t. Then $M_P \equiv I_P \cap J_1$ consists of all moving lines in I_P and is a module over $\mathcal{R}[t]$ [3]. It is proved in [3] that a moving line $L(x, y; t)$ is a moving line of $\mathbf{P}(t)$ if and only if $L(x, y; t) \in M_P$. Thus M_P is called the *moving line module* of $\mathbf{P}(t)$.

The moving line module M_P of the rational curve $\mathbf{P}(t)$ is isomorphic to the module

$$\mathbf{M}_P = \{(A(t), B(t), C(t)) \mid A(t)a(t) + B(t)b(t) + C(t)c(t) \equiv 0\} \subset \mathcal{R}[t]^3$$

under the isomorphism $A(t)x + B(t)y + C(t) \to (A(t), B(t), C(t))$. So we will use M_P and $\mathbf{M}_P$ interchangeably to represent the moving line module of $\mathbf{P}(t)$.

Let a vector polynomial $\mathbf{p}(t) \in \mathcal{R}[t]^3$ be written as

$$\mathbf{p} = (p_1(t), p_2(t), p_3(t)) = \sum_{i=0}^{m} (p_{i1}, p_{i2}, p_{i3}) t^i,$$

with the leading coefficient vector $(p_{m1}, p_{m2}, p_{m3}) \neq \mathbf{0}$. We denote (p_{m1}, p_{m2}, p_{m3}) by $\mathrm{LV}(\mathbf{p})$ and the degree of $\mathbf{p}$ by $\deg(\mathbf{p}) = m$. For example, for

$$\mathbf{p} = (2t^2 + 3t + 1, t + 4, t^2 + 2t + 3),$$

$\mathrm{LV}(\mathbf{p}) = (2, 0, 1)$ and $\deg(\mathbf{p}) = 2$.

Definition 1. Two moving lines $p = p_1(t)x + p_2(t)y + p_3(t)$ and $q = q_1(t)x + q_2(t)y + q_3(t)$ are called a μ-basis of a rational curve $\mathbf{P}(t)$, or equivalently, a μ-basis of $\mathbf{M}_P$, if
1. $\mathbf{p}$ and $\mathbf{q}$ are a basis of $\mathbf{M}_P$, i.e., any moving line $\mathbf{L} \in \mathbf{M}_P$ can be expressed by

$$\mathbf{L} = h_1\mathbf{p} + h_2\mathbf{q}, \tag{6}$$

with $h_1, h_2 \in \mathcal{R}[t]$; and
2. $\mathbf{p}$ and $\mathbf{q}$ have the lowest degrees among all bases of $\mathbf{M}_P$; that is, assuming $\deg(\mathbf{p}) \leqslant \deg(\mathbf{q})$, then there does not exist another basis $\tilde{\mathbf{p}}$ and $\tilde{\mathbf{q}}$ of $\mathbf{M}_P$, with $\deg(\tilde{\mathbf{p}}) \leqslant \deg(\tilde{\mathbf{q}})$, such that $\deg(\tilde{\mathbf{p}}) < \deg(\mathbf{p})$ or $\deg(\tilde{\mathbf{q}}) < \deg(\mathbf{q})$.

The above definition of a μ-basis appears to be different from a definition given in [3] for the μ-basis for a rational curve in R^d, $d \geqslant 2$. Actually, two definitions for the μ-basis are given in [3]; the first one on page 809 is for a planar rational curve and the second one on page 824 for a rational curve in R^d. The first definition is one of the equivalent definitions for the μ-basis to be given in the present paper; however, the second condition, which covers the case of a planar rational curve, though equivalent to the first one, contains a redundant condition.

The following is proved in [3]:

Proposition 1. *Any planar rational curve $\mathbf{P}(t)$ has a μ-basis.*

2.1. Properties

The existence of a μ-basis of a planar rational curve, along with some of its properties, are proved in [3]. In the following we will present a more complete list of properties of the μ-basis, including some from [3], and then give several equivalent definitions of the μ-basis.

Theorem 1. *Let $p = p_1(t)x + p_2(t)y + p_3(t)$ and $q = q_1(t)x + q_2(t)y + q_3(t)$ be a μ-basis of a planar rational curve $\mathbf{P}(t)$, where $\deg(p) \leqslant \deg(q)$. Denote $\mathbf{p} = (p_1, p_2, p_3)$ and $\mathbf{q} = (q_1, q_2, q_3)$. Then the following properties hold:*
1. *$\mathbf{p}$ and $\mathbf{q}$ are $\mathcal{R}[t]$-linearly independent.*
2. *$\mathbf{p}(t_0) \neq \mathbf{0}$ and $\mathbf{q}(t_0) \neq \mathbf{0}$ for any parameter value t_0.*
3. *$\mathbf{p}(t_0)$ and $\mathbf{q}(t_0)$ are linearly independent for any parameter value t_0.*
4. *$\mathrm{LV}(\mathbf{p})$ and $\mathrm{LV}(\mathbf{q})$ are linearly independent.*

5. *Expression* (6) *is unique for any moving line* $\mathbf{L}$ *of* $\mathbf{P}(t)$.
6. *Any moving line* $\mathbf{L}$ *of* $\mathbf{P}(t)$ *can be expressed in* (6) *with* $\deg(h_1\mathbf{p}) \leqslant \deg(\mathbf{L})$ *and* $\deg(h_2\mathbf{q}) \leqslant \deg(\mathbf{L})$.
7. $\mathbf{p} \times \mathbf{q} = k\mathbf{P}(t)$ *for some non-zero constant* k.
8. $\deg(\mathbf{p}) + \deg(\mathbf{q}) = n$. *Denote* $\deg(p) = \mu$ *and* $\deg(q) = n - \mu$ *in* t, *where* $0 \leqslant \mu \leqslant \lfloor n/2 \rfloor$. *Then* μ *is unique for a given curve* $\mathbf{P}(t)$; *furthermore*, μ *is the lowest degree of any moving line of the curve* $\mathbf{P}(t)$.
9. $I_P = \langle p, q \rangle$.
10. *The implicit equation of* $\mathbf{P}(t)$ *is given by* $\mathrm{Res}(p, q, t)$, *i.e., the resultant of* p *and* q *with respect to* t.

Proof. (1) Consider the two moving lines of $\mathbf{P}(t) = (a(t), b(t), c(t))$: $\mathbf{u} = (c, 0, -a)$ and $\mathbf{v} = (0, c, -b)$, which are clearly $\mathcal{R}[t]$-linearly independent. Then $\mathbf{u} = h_{11}\mathbf{p} + h_{12}\mathbf{q}$ and $\mathbf{v} = h_{21}\mathbf{p} + h_{22}\mathbf{q}$ for some polynomials $h_{ij} \in R[t]$, $i, j = 1, 2$. Hence

$$c(a, b, c) = \mathbf{u} \times \mathbf{v} = h\mathbf{p} \times \mathbf{q},$$

where $h = h_{11}h_{22} - h_{12}h_{21} \neq 0$. Thus $\mathbf{p} \times \mathbf{q} \neq \mathbf{0}$ except for possibly finitely many values, and it follows that $\mathbf{p}$ and $\mathbf{q}$ are $\mathcal{R}[t]$-linearly independent.

(2) Suppose $\mathbf{p}(t_0) = \mathbf{0}$ for some t_0, then $(t - t_0)|\mathbf{p}(t)$. Let $\tilde{\mathbf{p}}(t) = \mathbf{p}(t)/(t - t_0)$. Then $\tilde{\mathbf{p}}(t)$ and $\mathbf{q}(t)$ are also a basis of $\mathbf{M}_P$. But $\deg(\tilde{\mathbf{p}}(t)) < \deg(\mathbf{p}(t))$, a contradiction to that $\mathbf{p}(t)$ and $\mathbf{q}(t)$ are a μ-basis. Similarly, one can show that $\mathbf{q}(t_0) \neq \mathbf{0}$.

(3) Suppose that $\mathbf{p}(t_0)$ and $\mathbf{q}(t_0)$ are linearly dependent for some t_0. Then there exist constants α and β, both of them are nonzero, such that $\alpha\mathbf{p}(t_0) + \beta\mathbf{q}(t_0) = 0$. Let $\mathbf{L} = \alpha\mathbf{p} + \beta\mathbf{q}$. Then $\mathbf{L} \in \mathbf{M}_P$, and $\mathbf{L}$ is not identically zero, since, by Property (1), $\mathbf{p}$ and $\mathbf{q}$ are $\mathcal{R}[t]$-linearly independent. Since $\mathbf{L}(t_0) = 0$, $(t - t_0)|\mathbf{L}$. Let $\tilde{\mathbf{q}} = \mathbf{L}/(t - t_0)$. Then it is easy to verify that $\mathbf{p}$ and $\tilde{\mathbf{q}}$ also form a basis of the module $\mathbf{M}_P$. But $\deg(\tilde{\mathbf{q}}) < \deg(\mathbf{q})$, contradicting that $\mathbf{p}$ and $\mathbf{q}$ are a μ-basis. Hence, $\mathbf{p}(t_0)$ and $\mathbf{q}(t_0)$ are linearly independent for any t_0.

(4) Suppose that $\mathrm{LV}(\mathbf{p})$ and $\mathrm{LV}(\mathbf{q})$ are linearly dependent. Then $\alpha\mathrm{LV}(\mathbf{p}) + \beta\mathrm{LV}(\mathbf{q}) = 0$ for some constants α and β, both are nonzero. Let $\tilde{\mathbf{q}} = \alpha\mathbf{p}t^d + \beta\mathbf{q}$, where $d = \deg(\mathbf{q}) - \deg(\mathbf{p})$. Then $\mathbf{p}$ and $\tilde{\mathbf{q}}$ also form a basis of $\mathbf{M}_P$. However, since the leading coefficient vectors of $\alpha\mathbf{p}t^d$ and $\beta\mathbf{q}$ cancel each other, $\deg(\tilde{\mathbf{q}}) < \deg(\mathbf{q})$, contradicting that $\mathbf{q}$ has the lowest degree among all the bases of $\mathbf{P}(t)$. Hence, $\mathrm{LV}(\mathbf{p})$ and $\mathrm{LV}(\mathbf{q})$ are linearly independent.

(5) For any moving line $\mathbf{L}$ of $\mathbf{P}$, suppose $\mathbf{L} = h_1\mathbf{p} + h_2\mathbf{q}$ and $\mathbf{L} = g_1\mathbf{p} + g_2\mathbf{q}$. Then $(h_1 - g_1)\mathbf{p} + (h_2 - g_2)\mathbf{q} = 0$. It follows that $h_1 = g_1$ and $h_2 = g_2$, since, by Property (1) above, $\mathbf{p}$ and $\mathbf{q}$ are $\mathcal{R}[t]$-linearly independent. Hence expression (6) is unique.

(6) Suppose $\mathbf{L} = h_1\mathbf{p} + h_2\mathbf{q}$. If $\deg(h_1\mathbf{p}) > \deg(\mathbf{L})$, then $\mathrm{LV}(h_1\mathbf{p}) + \mathrm{LV}(h_2\mathbf{q}) = \mathbf{0}$, thus $\mathrm{LV}(\mathbf{p})$ and $\mathrm{LV}(\mathbf{q})$ are linearly dependent, contradicting Property (4) above. Hence, $\deg(h_1\mathbf{p}) \leqslant \deg(\mathbf{L})$. Similarly, $\deg(h_2\mathbf{q}) \leqslant \deg(\mathbf{L})$.

(7) Since $\mathbf{p} \cdot \mathbf{P}(t) = \mathbf{q} \cdot \mathbf{P}(t) = 0$, and $\mathbf{p}$ and $\mathbf{q}$ are $\mathcal{R}[t]$-linearly independent, we have $\mathbf{p} \times \mathbf{q} = (g(t)/h(t))\mathbf{P}(t)$ for $g(t), h(t) \in \mathcal{R}[t]$, where g and h are relatively prime. Since $a(t)$, $b(t)$, and $c(t)$ are relatively prime, $h(t)$ must be a constant. If $g(t)$ is not a constant, letting t_0 be a zero of $g(t)$ over the complex field, then $\mathbf{p}(t_0) \times \mathbf{q}(t_0) = 0$, i.e.

$\mathbf{p}(t_0)$ and $\mathbf{q}(t_0)$ are linearly dependent; but this contradicts Property (3) above. So $g(t)$ is also a constant, and plainly, $g \neq 0$. Hence, $\mathbf{p} \times \mathbf{q} = k\mathbf{P}(t)$ for some nonzero constant k.

(8) From Property (7), $\deg(\mathbf{p} \times \mathbf{q}) = \deg(\mathbf{P}) = n$. Let $\mathbf{p} = \mathbf{p}_\mu t^\mu + \mathbf{p}_{\mu-1} t^{\mu-1} + \cdots + \mathbf{p}_0$ and $\mathbf{q} = \mathbf{q}_v t^v + \mathbf{q}_{v-1} t^{v-1} + \cdots + \mathbf{q}_0$. Then $\mathbf{p} \times \mathbf{q} = (\mathbf{p}_\mu \times \mathbf{q}_v) t^{\mu+v} + \cdots + \mathbf{p}_0 \times \mathbf{q}_0$. By Property (4), $\mathrm{LV}(\mathbf{p}) = \mathbf{p}_\mu$ and $\mathrm{LV}(\mathbf{q}) = \mathbf{q}_v$ are linearly independent, so $\mathbf{p}_\mu \times \mathbf{q}_v \neq 0$. It follows that

$$\deg(\mathbf{p}) + \deg(\mathbf{q}) = \mu + v = \deg(\mathbf{p} \times \mathbf{q}) = \deg(\mathbf{P}) = n.$$

The uniqueness of μ is implied by the minimality of the degrees of $\mathbf{p}$ and $\mathbf{q}$.

On the other hand, let $\mathbf{L} \in \mathbf{M}_P$ be any moving line of $\mathbf{P}(t)$, then $\mathbf{L} = h_1\mathbf{p} + h_2\mathbf{q}$ for some $h_1, h_2 \in R[t]$. If $\deg(\mathbf{L}) < \mu$, then $\mathrm{LV}(h_1\mathbf{p})$ and $\mathrm{LV}(h_2\mathbf{q})$ cancel with each other. Hence $\mathrm{LV}(\mathbf{p})$ and $\mathrm{LV}(\mathbf{q})$ are linearly dependent, a contradiction to Property 4 above. Thus μ is the lowest degree of any moving line of $\mathbf{P}(t)$.

(9) First recall that the moving line ideal I_P is generated by $cx - a$ and $cy - b$. Since $cx - a, cy - b \in M_P$, and p and q are a basis of M_P, $cx - a, cy - b$ can be expressed by linear combinations of p and q over $\mathcal{R}[t]$. Hence, I_P can be generated by p and q.

(10) See [3].

This completes of the proof of Theorem 1. □

The relationship between different μ-bases of a rational curve $\mathbf{P}(t)$ is given by the following theorem.

Theorem 2. *Let* $\mathbf{p}, \mathbf{q}$, *and* $\tilde{\mathbf{p}}, \tilde{\mathbf{q}}$ *be two* μ*-bases of a rational curve* $\mathbf{P}(t)$, *with* $\deg(\mathbf{p}) \leqslant \deg(\mathbf{q})$ *and* $\deg(\tilde{\mathbf{p}}) \leqslant \deg(\tilde{\mathbf{q}})$. *Then* $\deg(\mathbf{p}) = \deg(\tilde{\mathbf{p}})$ *and* $\deg(\mathbf{q}) = \deg(\tilde{\mathbf{q}})$. *Furthermore, if* $\deg(\mathbf{p}) = \deg(\mathbf{q})$, *then*

$$\tilde{\mathbf{p}} = \alpha_1\mathbf{p} + \beta_1\mathbf{q}, \quad \tilde{\mathbf{q}} = \alpha_2\mathbf{p} + \beta_2\mathbf{q}$$

for some constants α_1, α_2, β_1, *and* β_2 *with* $\alpha_1\beta_2 - \alpha_2\beta_1 \neq 0$; *if* $\deg(\mathbf{p}) < \deg(\mathbf{q})$, *then*

$$\tilde{\mathbf{p}} = \alpha\mathbf{p}, \quad \tilde{\mathbf{q}} = h\mathbf{p} + \beta\mathbf{q}$$

for some nonzero constants α *and* β, *and* $h \in \mathcal{R}[t]$ *with* $\deg(h) \leqslant \deg(\mathbf{q}) - \deg(\mathbf{p})$.

Proof. By the definition of the μ-basis, it is straightforward to see that $\deg(\mathbf{p}) = \deg(\tilde{\mathbf{p}})$ and $\deg(\mathbf{q}) = \deg(\tilde{\mathbf{q}})$. This is also Property (8) of Theorem 1.

Since $\tilde{\mathbf{p}}, \tilde{\mathbf{q}} \in \mathbf{M}_P$, and $\mathbf{p}, \mathbf{q}$ are a basis of $\mathbf{M}_P$,

$$\tilde{\mathbf{p}} = \alpha_1\mathbf{p} + \beta_1\mathbf{q}, \quad \tilde{\mathbf{q}} = \alpha_2\mathbf{p} + \beta_2\mathbf{q},$$

with $\alpha_i, \beta_i \in \mathcal{R}[t]$, $i = 1, 2$. If $\deg(\mathbf{p}) = \deg(\mathbf{q})$, then $\deg(\tilde{\mathbf{p}}) = \deg(\tilde{\mathbf{q}}) = \deg(\mathbf{p}) = \deg(\mathbf{q})$. It then follows from by Property (6) of Theorem 1 that α_1, α_2, β_1, and β_2 are constants. We have $\alpha_1\beta_2 - \alpha_2\beta_1 \neq 0$ since $\tilde{\mathbf{p}}$ and $\tilde{\mathbf{q}}$ are $\mathcal{R}[t]$-linearly independent.

If $\deg(\mathbf{p}) < \deg(\mathbf{q})$, then $\deg(\tilde{\mathbf{p}}) = \deg(\mathbf{p}) < \deg(\mathbf{q})$. Again by Property (6) of Theorem 1, $\beta_1 = 0$ and α_1 is a nonzero constant. Similarly, from $\deg(\tilde{\mathbf{q}}) = \deg(\mathbf{q}) > \deg(\mathbf{p})$, one has β_2 is a nonzero constant and $\deg(\alpha_2) \leqslant \deg(\mathbf{q}) - \deg(\mathbf{p})$. □

2.2. Equivalent definitions

Next we provide some equivalent definitions of a μ-basis of a planar rational curve.

Theorem 3. *Let $\mathbf{p}, \mathbf{q} \in \mathbf{M}_P$ be two moving lines of a planar rational curve $\mathbf{P}(t)$ of degree n. Assume $\deg(\mathbf{p}) \leqslant \deg(\mathbf{q})$. Then $\mathbf{p}$ and $\mathbf{q}$ form a μ-basis of $\mathbf{P}(t)$ if and only if one of the following conditions holds*

1. *Any moving line $\mathbf{L}$ can be expressed in* (6) *with $\deg(h_1\mathbf{p}) \leqslant \deg(\mathbf{L})$ and $\deg(h_2\mathbf{q}) \leqslant \deg(\mathbf{L})$.*
2. *Any moving line $\mathbf{L}$ can be expressed in* (6)*, and $\mathrm{LV}(\mathbf{p})$ and $\mathrm{LV}(\mathbf{q})$ are linearly independent.*
3. *Any moving line $\mathbf{L}$ can be expressed in* (6) *and $\deg(\mathbf{p}) + \deg(\mathbf{q}) = n$.*
4. *$\mathbf{p} \times \mathbf{q} = k\mathbf{P}$ for some non-zero constant k and $\deg(\mathbf{p}) + \deg(\mathbf{q}) = n$.*
5. *$\mathbf{p} \times \mathbf{q} = k\mathbf{P}$ for some non-zero constant k, and $\mathrm{LV}(\mathbf{p})$ and $\mathrm{LV}(\mathbf{q})$ are linearly independent.*
6. *$\deg(\mathbf{p}) + \deg(\mathbf{q}) = n$, and $\mathbf{p}$ and $\mathbf{q}$ are $\mathcal{R}[t]$-linearly independent.*
7. *$\deg(\mathbf{p}) + \deg(\mathbf{q}) = n$, and $\mathrm{LV}(\mathbf{p})$ and $\mathrm{LV}(\mathbf{q})$ are linearly independent.*
8. *$\deg(\mathbf{p}) + \deg(\mathbf{q}) = n$ and $I_P = \langle p, q \rangle$. Here $p = \mathbf{p} \cdot (x, y, 1)$ and $q = \mathbf{q} \cdot (x, y, 1)$.*

Proof. The necessity of all the above conditions has been proved in Theorem 1. So in the following we consider only their sufficiency.

(1) We just need to show that $\mathbf{p}$ and $\mathbf{q}$ have the lowest possible degree among all the bases of $\mathbf{M}_P$. Let $\tilde{\mathbf{p}}$ and $\tilde{\mathbf{q}}$ be any basis of $\mathbf{M}_P$ with $\deg(\tilde{\mathbf{p}}) \leqslant \deg(\tilde{\mathbf{q}})$. We first show $\deg(\mathbf{p}) \leqslant \deg(\tilde{\mathbf{p}})$. Clearly,

$$\tilde{\mathbf{p}} = h_{11}\mathbf{p} + h_{12}\mathbf{q}, \quad \tilde{\mathbf{q}} = h_{21}\mathbf{p} + h_{22}\mathbf{q}$$

for some $h_{ij} \in \mathcal{R}[t]$, $i, j = 1, 2$. If $h_{11} \neq 0$, since $\deg(h_{11}\mathbf{p}) \leqslant \deg(\tilde{\mathbf{p}})$, it follows that $\deg(\mathbf{p}) \leqslant \deg(\tilde{\mathbf{p}})$; if $h_{11} = 0$ and $h_{12} \neq 0$, then $\deg(\mathbf{p}) \leqslant \deg(\mathbf{q}) \leqslant \deg(\tilde{\mathbf{p}})$. So there is always $\deg(\mathbf{p}) \leqslant \deg(\tilde{\mathbf{p}})$.

Next we show $\deg(\mathbf{q}) \leqslant \deg(\tilde{\mathbf{q}})$. If $h_{22} \neq 0$, since $\deg(h_{22}\mathbf{q}) \leqslant \deg(\tilde{\mathbf{q}})$, we have $\deg(\mathbf{q}) \leqslant \deg(\tilde{\mathbf{q}})$. If $h_{22} = 0$, then $h_{12} \neq 0$, for otherwise $\tilde{\mathbf{p}}$ and $\tilde{\mathbf{q}}$ cannot be a basis of $\mathbf{P}$. In this case, since $\deg(h_{12}\mathbf{q}) \leqslant \deg(\tilde{\mathbf{p}})$, we have $\deg(\mathbf{q}) \leqslant \deg(\tilde{\mathbf{p}}) \leqslant \deg(\tilde{\mathbf{q}})$. So there is always $\deg(\mathbf{q}) \leqslant \deg(\tilde{\mathbf{q}})$.

We have shown that $\mathbf{p}$ and $\mathbf{q}$ are a basis of $\mathbf{M}_P$ with the lowest degrees. Hence, $\mathbf{p}$ and $\mathbf{q}$ form a μ-basis of $\mathbf{M}_P$.

(2) Given a moving line $\mathbf{L}$ of $\mathbf{P}$, suppose $\mathbf{L} = h_1\mathbf{p} + h_2\mathbf{q}$. Since $\mathrm{LV}(\mathbf{p})$ and $\mathrm{LV}(\mathbf{q})$ are linearly independent, $\mathrm{LV}(h_1\mathbf{p})$ and $\mathrm{LV}(h_2\mathbf{q})$ do not cancel each other; hence, $\deg(h_1\mathbf{p}) \leqslant \deg(\mathbf{L})$ and $\deg(h_2\mathbf{q}) \leqslant \deg(\mathbf{L})$. Then, by condition (1), $\mathbf{p}$ and $\mathbf{q}$ form a μ-basis of $\mathbf{M}_P$.

(3) Again, we just need to show that $\mathbf{p}$ and $\mathbf{q}$ have the lowest degrees possible. First note that $\mathbf{p}$ and $\mathbf{q}$ form a basis of $\mathbf{M}_P$ since, by assumption, any moving line in $\mathbf{M}_P$ is expressible in (6). Let $\tilde{\mathbf{p}}$ and $\tilde{\mathbf{q}}$ be a μ-basis of $\mathbf{M}_P$ with $\deg(\tilde{\mathbf{p}}) = \mu$ and $\deg(\tilde{\mathbf{q}}) = n - \mu$, where $0 < \mu \leqslant \lfloor n/2 \rfloor$. Because of the minimality of the degrees of

the μ-basis, we have $\deg(\mathbf{p}) \geqslant \mu$. If $\deg(\mathbf{p}) > \mu$, then $\deg(\mathbf{p}) \leqslant \deg(\mathbf{q}) < n - \mu$ since $\deg(\mathbf{p}) + \deg(\mathbf{q}) = n$. By Property (6) of the μ-basis in Theorem 1, $\mathbf{p} = h_1\tilde{\mathbf{p}}$ and $\mathbf{q} = h_2\tilde{\mathbf{p}}$ for some $h_1, h_2 \in R[t]$. Thus $h_2\mathbf{p} - h_1\mathbf{q} = 0$, that is, $\mathbf{p}$ and $\mathbf{q}$ are $\mathcal{R}[t]$-linearly dependent. This contradicts that $\mathbf{p}$ and $\mathbf{q}$ form a basis of $\mathbf{M}_P$. Thus $\deg(\mathbf{p}) = \mu$ and $\deg(\mathbf{q}) = n - \mu$, and hence, $\mathbf{p}$ and $\mathbf{q}$ are a μ-basis of $\mathbf{M}_P$.

(4) Since $\mathbf{p} \times \mathbf{q} = k\mathbf{P}$ for some nonzero constant k, for any moving line $\mathbf{L}$ of $\mathbf{P}(t)$, $\mathbf{L} \cdot \mathbf{p} \times \mathbf{q} = \mathbf{L} \cdot \mathbf{P} \equiv 0$. Hence $g\mathbf{L} = h_1\mathbf{p} + h_2\mathbf{q}$ for some $g, h_1, h_2 \in R[t]$, where $\mathrm{GCD}(g, h_1, h_2) = 1$. Further, if g is not a constant, letting t_0 be a zero of g over the complex field, then $h_1(t_0)\mathbf{p}(t_0) + h_2(t_0)\mathbf{q}(t_0) = 0$, but this contradicts Property (3) of Theorem 1 stating that $\mathbf{p}(t_0)$ and $\mathbf{q}(t_0)$ are linearly independent for any parameter value t_0. Hence g is a nonzero constant. So we may write $\mathbf{L} = h_1\mathbf{p} + h_2\mathbf{q}$ for some $h_1, h_2 \in \mathcal{R}[t]$. Then, by condition (3) above, $\mathbf{p}$ and $\mathbf{q}$ form a μ-basis of $\mathbf{M}_P$.

(5) Similar to the argument in the proof above for condition (4), it can be shown that any moving lines $\mathbf{L}$ of $\mathbf{P}(t)$ can be expressed by $\mathbf{L} = h_1\mathbf{p} + h_2\mathbf{q}$ with $h_1, h_2 \in \mathcal{R}[t]$. Then, by condition (2), the proof is completed.

(6) Since $\mathbf{p}$ and $\mathbf{q}$ are $\mathcal{R}[t]$-linearly independent moving lines of $\mathbf{P}$, $g(\mathbf{p} \times \mathbf{q}) = h\mathbf{P}$ for $g, h \in \mathcal{R}[t]$, where g, h are relatively prime. Since the components $a, b, c \in \mathcal{R}[t]$ of $\mathbf{P}$ are relatively prime, g must be a nonzero constant. Thus

$$n = \deg(\mathbf{p}) + \deg(\mathbf{q}) \geqslant \deg(\mathbf{p} \times \mathbf{q}) = \deg(h) + \deg(\mathbf{P}) = \deg(h) + n.$$

It follows that $\deg(h) = 0$. Hence, we may write $\mathbf{p} \times \mathbf{q} = k\mathbf{P}$ for some nonzero constant k. Now, by condition (4), $\mathbf{p}$ and $\mathbf{q}$ are a μ-basis of $\mathbf{M}_P$.

(7) Since $\mathrm{LV}(\mathbf{p})$ and $\mathrm{LV}(\mathbf{q})$ are linearly independent, $\mathrm{LV}(\mathbf{p} \times \mathbf{q}) = \mathrm{LV}(\mathbf{p}) \times \mathrm{LV}(\mathbf{q}) \neq 0$. It follows that $\mathbf{p} \times \mathbf{q} \neq 0$; thus $\mathbf{p}$ and $\mathbf{q}$ are $\mathcal{R}[t]$-linearly independent. Now, by condition (6), $\mathbf{p}$ and $\mathbf{q}$ form a μ-basis of $\mathbf{M}_P$.

(8) Since $cx - a, cy - b \in I = \langle p, q \rangle$, similar to the proof of Property (1) of Theorem 1, one can show that $\mathbf{p}$ and $\mathbf{q}$ are $\mathcal{R}[t]$-linearly independent. By condition (6), $\mathbf{p}$ and $\mathbf{q}$ are a μ-basis of $\mathbf{P}(t)$.

The proof of Theorem 3 is completed. □

Two definitions for the μ-basis are given in [3]. The first definition is for planar rational curves and equivalent to condition (6) in Theorem 3 above. The second definition is for the general case of a rational curve in R^d, $d \geqslant 2$. This second definition, when $d = 2$, is equivalent to the first one but contains a redundant condition $\deg(\mathbf{p}) + \deg(\mathbf{q}) = n$.

3. Computation of μ-basis

We present in this section a new method for computing a μ-basis of a planar rational curve. The conditions (2) and (3) in Theorem 3 will play a key role in developing this algorithm. We begin with the review of some existing methods.

The first method for computing a μ-basis of a rational curve $\mathbf{P}(t)$ using undetermined coefficients is described by Sederberg et al. [6]. This algorithm needs $O(n^3)$ arithmetic operations, where n is the degree of $\mathbf{P}(t)$.

A more efficient algorithm for computing the μ-basis has recently been developed by Zheng and Sederberg [7]; we will call it the *ZS algorithm*. Given a set of three generating vector polynomials of the moving line module $\mathbf{M}_P$, the ZS algorithm sorts all the terms of the vector polynomials in the order of their degrees and component indices, and exploits the observation that the leading coefficients of at least two generating vector polynomials have the same basis vector; this observation enables one to reduce the degree of one component of one vector polynomial in each reduction step, until a μ-basis is reached. The ZS algorithm is similar to Buchberger's algorithm for computing the Gröebner basis of a module, and its efficiency lies in that no more than three generators of the module $\mathbf{M}_P$ are maintained at any moment. The complexity of the ZS algorithm is $O(n^2)$ [7].

We will present, in this paper, an improved algorithm for computing the μ-basis of a planar rational curve. Our algorithm is similar to the ZS algorithm in that it also operates in the moving line module. However, based on the linear dependency of the leading coefficient vectors of the generating vector polynomials of $\mathbf{M}_P$, we are able to eliminate simultaneously the highest degree terms of *all* components of a vector polynomial in each reduction step, thus reducing the degrees of the polynomials more quickly than the ZS algorithm does. Moreover, our approach is conceptually simpler since it skips the need of sorting all the terms of the generating vector polynomials. In addition, the effective vector elimination scheme used makes the new algorithm easily extendable to computing the μ-basis of a rational curve in higher dimensions.

Based on operation count, the new algorithm also has the time complexity $O(n^2)$, but with the proportional constant about twice as small as that of the ZS algorithm. In the following we present the algorithm and analyze its time complexity. Before going on, we provide two lemmas.

3.1. Lemmas

Lemma 1. *The moving line module* $\mathbf{M}_P$ *of a planar rational curve* $P(t) = (a(t), b(t), c(t))$ *is generated by the three vector polynomials* $\mathbf{v}_1, \mathbf{v}_2$, *and* $\mathbf{v}_3$, *where* $\mathbf{v}_1 = (-b, a, 0)$, $\mathbf{v}_2 = (-c, 0, a)$, *and* $\mathbf{v}_3 = (0, c, -b)$.

Proof. The proof will be given by adapting the proof of Lemma 1 in [3]. See also [7]. For completeness, we sketch the proof in the following.

Since a, b, and c are relatively prime, there exist $u, v, w \in \mathcal{R}[t]$ such that $ua + vb + wc = 1$. Suppose that $A(t)x + B(t)y + C(t) = 0$ is a moving line in $\mathbf{M}_P$. For brevity, $A(t)$, $B(t)$, and $C(t)$ will be denoted by A, B, and C, respectively, in the following. Since $aA + bB + cC = 0$, it follows that

$$\begin{aligned} A &= uaA + vbA + wcA = u(-bB - cC) + vbA + wcA \\ &= -b(uB - vA) - c(uC - wA). \end{aligned}$$

Similarly,

$$B = a(uB - vA) + c(-vC + wB)$$

and

$$C = a(uC - wA) - b(-vC + wB).$$

Then

$$(A, B, C) = h_1\mathbf{v}_1 + h_2\mathbf{v}_2 + h_3\mathbf{v}_3,$$

where $h_1 = uB - vA$, $h_2 = uC - wA$, $h_3 = -vC + wB$. Hence, $\mathbf{M}_P \subset \langle \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3 \rangle$. On the other hand, it is easy to see that $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3 \in \mathbf{M}_P$. Hence, $\mathbf{M}_P = \langle \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3 \rangle$. □

Lemma 2. *Let* $\mathbf{v}_1$, $\mathbf{v}_2$, *and* $\mathbf{v}_3$ *be as defined in Lemma* 1. *Then*
1. $\mathrm{rank}(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) = 2$
2. $\mathrm{rank}(\mathrm{LV}(\mathbf{v}_1), \mathrm{LV}(\mathbf{v}_2), \mathrm{LV}(\mathbf{v}_3)) = 2$.

Proof. Since $c\mathbf{v}_1 - b\mathbf{v}_2 + a\mathbf{v}_3 = 0$, $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ are $\mathcal{R}[t]$-linearly dependent, thus $\mathrm{rank}(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) \leqslant 2$. On the other hand, $\mathbf{v}_1$ and $\mathbf{v}_2$ are $\mathcal{R}[t]$-linearly independent. Hence $\mathrm{rank}(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) = 2$.

To prove (2), suppose

$$a = \sum_{i=0}^{\deg(a)} a_i t^i, \quad b = \sum_{i=0}^{\deg(b)} b_i t^i, \quad c = \sum_{i=0}^{\deg(c)} c_i t^i.$$

Wlog, assume $n = \deg(a) \geqslant \deg(b) \geqslant \deg(c)$. Then $a_n \neq 0$. It follows that $\mathrm{LV}(\mathbf{v}_1) = (-b_n, a_n, 0)$ and $\mathrm{LV}(\mathbf{v}_2) = (-c_n, 0, a_n)$ are linearly independent. But $\mathrm{LV}(\mathbf{v}_1)$, $\mathrm{LV}(\mathbf{v}_2)$, and $\mathrm{LV}(\mathbf{v}_3)$ are linearly dependent, since $c_n\mathrm{LV}(\mathbf{v}_1) - b_n\mathrm{LV}(\mathbf{v}_2) + a_n\mathrm{LV}(\mathbf{v}_3) = 0$. Hence, $\mathrm{rank}(\mathrm{LV}(\mathbf{v}_1), \mathrm{LV}(\mathbf{v}_2), \mathrm{LV}(\mathbf{v}_3)) = 2$. □

3.2. Algorithm

Now we are ready to describe the new algorithm for computing a μ-basis of a planar rational curve.

Algorithm for computing a μ-basis

Input: $\mathbf{P}(t) = (a(t), b(t), c(t)) \in \mathcal{R}[t]^3$.

Output: Two polynomials forming a μ-basis of $\mathbf{P}(t)$.

Variables: $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3$ are program variables for vector polynomials, and $\mathbf{m}_1, \mathbf{m}_2, \mathbf{m}_3$ are program variables for numerical vectors.

Step 1 Set $\mathbf{u}_1 := \mathbf{v}_1 \equiv (-b, a, 0)$, $\mathbf{u}_2 := \mathbf{v}_2 \equiv (-c, 0, a)$, and $\mathbf{u}_3 := \mathbf{v}_3 \equiv (0, c, -b)$. Set $\mathbf{m}_1 := \mathrm{LV}(\mathbf{u}_1)$, $\mathbf{m}_2 := \mathrm{LV}(\mathbf{u}_2)$, and $\mathbf{m}_3 := \mathrm{LV}(\mathbf{u}_3)$.

Step 2 Set $n_i := \deg(\mathbf{u}_i)$, $i = 1, 2, 3$. Without loss of generality, assume $n_1 \geqslant n_2 \geqslant n_3$, by renumbering the $\mathbf{u}_i$, $i = 1, 2, 3$, if necessary. Find real numbers $\alpha_1, \alpha_2, \alpha_3$ (at least two of them are non-zero) such that

$$\alpha_1\mathbf{m}_1 + \alpha_2\mathbf{m}_2 + \alpha_3\mathbf{m}_3 = \mathbf{0}. \tag{7}$$

If $\alpha_1 \neq 0$, update $\mathbf{u}_1$ by

$$\mathbf{u}_1 := \alpha_1\mathbf{u}_1 + \alpha_2 t^{n_1 - n_2}\mathbf{u}_2 + \alpha_3 t^{n_1 - n_3}\mathbf{u}_3$$

and set $\mathbf{m}_1 := \mathrm{LV}(\mathbf{u}_1)$ and $n_1 := \deg(\mathbf{u}_1)$. If $\alpha_1 = 0$ (then both α_2 and α_3 are non-zero), update $\mathbf{u}_2$ by

$$\mathbf{u}_2 := \alpha_2\mathbf{u}_2 + \alpha_3 t^{n_2-n_3}\mathbf{u}_3$$

and set $\mathbf{m}_2 := \mathrm{LV}(\mathbf{u}_2)$ and $n_2 := \deg(\mathbf{u}_2)$.

Step 3 If one of $\mathbf{u}_1$, $\mathbf{u}_2$, and $\mathbf{u}_3$ is zero, say $\mathbf{u}_1 = 0$, then output $\mathbf{u}_2$ and $\mathbf{u}_3$, and stop; else, go to **Step 2**.

Theorem 4. *Let* $\mathbf{p}$ *and* $\mathbf{q}$ *denote the two vector polynomials output by the above algorithm. Then*
1. *The algorithm terminates in a finite number of steps.*
2. $\mathbf{p}$ *and* $\mathbf{q}$ *are a* μ*-basis of* $\mathbf{M}_P$.

Proof. Upon initialization, by Lemma 2, $\mathrm{rank}(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3) = 2$ and $\mathrm{rank}\{\mathbf{m}_1, \mathbf{m}_2, \mathbf{m}_3\} = \mathrm{rank}(\mathrm{LV}(\mathbf{u}_1), \mathrm{LV}(\mathbf{u}_2), \mathrm{LV}(\mathbf{u}_3)) = 2$. Note that the basic iteration step in the algorithm is the replacement in **Step 2**. Since each replacement is an invertible elementary row reduction applied to matrix $(\mathbf{u}_1^{\mathrm{T}}, \mathbf{u}_2^{\mathrm{T}}, \mathbf{u}_3^{\mathrm{T}})^{\mathrm{T}}$ as well as $(\mathbf{m}_1^{\mathrm{T}}, \mathbf{m}_2^{\mathrm{T}}, \mathbf{m}_3^{\mathrm{T}})^{\mathrm{T}}$, $\mathrm{rank}(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$ and $\mathrm{rank}(\mathbf{m}_1, \mathbf{m}_2, \mathbf{m}_3)$ are not altered, i.e., they are always 2. Since $\mathrm{rank}(\mathbf{m}_1, \mathbf{m}_2, \mathbf{m}_3) = 2$, there exist real numbers α_1, α_2, and α_3, at least two of which are nonzero, such that (7) holds. Hence, **Step 2** can be carried out properly. Because each replacement in **Step 2** lowers at least by one the degree of one of the $\mathbf{u}_i$, $i = 1, 2, 3$, one of the $\mathbf{u}_i$ must become zero vector in a finite number of steps. Hence, the algorithm terminates in a finite number of steps. This proves (1).

When the algorithm terminates, suppose we have $\mathbf{u}_1 = 0$. Since $\mathrm{rank}\{\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3\} = 2$, $\mathbf{u}_2$ and $\mathbf{u}_3$, which are output as $\mathbf{p}$ and $\mathbf{q}$, are $\mathcal{R}[t]$-linearly independent. Furthermore, since each replacement in **Step 2** is an invertible row reduction, $\{\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3\}$ is the generating set of module $\mathbf{M}_P$ after each replacement. Hence, $\mathbf{p}$ and $\mathbf{q}$ generate $\mathbf{M}_P$, i.e., any moving line $\mathbf{L} \in \mathbf{M}_P$ can be expressed by $\mathbf{L} = h_1\mathbf{p} + h_2\mathbf{q}$ with $h_1, h_2 \in \mathbf{M}_P$.

Next we show that $\mathrm{LV}(\mathbf{p})$ and $\mathrm{LV}(\mathbf{q})$ are linearly independent. Since $\mathrm{rank}(\mathbf{m}_1, \mathbf{m}_2, \mathbf{m}_3) = 2$ always holds, upon the termination of the algorithm, $\mathrm{rank}(0, \mathrm{LV}(\mathbf{p}), \mathrm{LV}(\mathbf{q})) = 2$; that is, $\mathrm{LV}(\mathbf{p})$ and $\mathrm{LV}(\mathbf{q})$ are linearly independent. Then, by condition (2) of Theorem 3, $\mathbf{p}$ and $\mathbf{q}$ form a μ-basis of $\mathbf{M}_P$. □

By condition (7) of Theorem 3, which is an equivalent definition of the μ-basis, we may use, as an alternative, the following termination condition: The algorithm terminates when there exist two vector polynomials among $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3$, say $\mathbf{u}_2$ and $\mathbf{u}_3$, such that $\deg(\mathbf{u}_2) + \deg(\mathbf{u}_3) = n$ and $\mathrm{LV}(\mathbf{u}_2)$ and $\mathrm{LV}(\mathbf{u}_3)$ are linearly independent.

Remark. Our algorithm is based on the linear dependency of the leading coefficient vectors of the three non-zero generators, and its correctness is implied by a newly established property that a μ-basis of $\mathbf{M}_P$ is a basis of $\mathbf{M}_P$ with linearly independent leading coefficient vectors, i.e., condition (2) of Theorem 3. In comparison, the ZS algorithm is based on the observation that the leading terms of two of the three

generating vector polynomials have the same standard basis vector [7], and therefore all monomial terms in a vector polynomial have to be sorted by their degrees and then by positions, component-wise, in order to carry on the algorithm. As a consequence, we are able to devise a conceptually simpler and computationally more efficient algorithm for computing the μ-basis than the ZS algorithm, saving the trouble to sort all the terms of a vector polynomial component-wise.

The example below illustrates how our algorithm works.

Example 1. Consider a quadratic curve

$$\mathbf{P}(t) = (2t^2 + 4t + 5, 3t^2 + t + 4, t^2 + 2t + 3).$$

Then

$$\begin{aligned}
\mathbf{u}_1 &:= (3t^2 + t + 4, -2t^2 - 4t - 5, 0),\\
\mathbf{u}_2 &:= (t^2 + 2t + 3, 0, -2t^2 - 4t - 5),\\
\mathbf{u}_3 &:= (0, t^2 + 2t + 3, -3t^2 - t - 4).
\end{aligned}$$

The leading vectors of $\mathbf{u}_i$, $i = 1, 2, 3$, are $\mathbf{m}_1 = (3, -2, 0)$, $\mathbf{m}_2 = (1, 0, -2)$ and $\mathbf{m}_3 = (0, 1, -3)$. Since $\mathbf{m}_1 - 3\mathbf{m}_2 + 2\mathbf{m}_3 = \mathbf{0}$, we update $\mathbf{u}_3$ by

$$\mathbf{u}_3 := \mathbf{u}_1 - 3\mathbf{u}_2 + 2\mathbf{u}_3 = (-5t - 5, 1, 10t + 7)$$

and $\mathbf{m}_3$ by $(-5, 0, 10)$.

For the next step, since $5\mathbf{m}_2 + \mathbf{m}_3 = \mathbf{0}$, we update $\mathbf{u}_2$ by

$$\mathbf{u}_2 := 5\mathbf{u}_2 + t\mathbf{u}_3 = (5t + 15, t, -13t - 25)$$

and $\mathbf{m}_2$ by $(5, 1, -13)$. Now, since $\deg(\mathbf{u}_2) + \deg(\mathbf{u}_3) = 2 = \deg(\mathbf{P}(t))$, and $\mathbf{m}_2$ and $\mathbf{m}_3$ are $\mathcal{R}[t]$-linearly independent, the algorithm terminates and we obtain the μ-basis

$$p = (5t + 15)x + ty - 13t - 25, \qquad q = (-5t - 5)x + y + 10t + 7.$$

3.3. Computational complexity

Now we analyze in this section the computational complexity of the new algorithm and compare it with the ZS algorithm.

When the termination condition $\deg(\mathbf{p}) + \deg(\mathbf{q}) = n$ is satisfied, the degrees of the polynomials $\mathbf{u}_i$, $i = 1, 2, 3$, are $n - \mu$, μ, and $v > \mu$, respectively, with $\mu \leqslant [n/2]$. Thus, totally, at most $\mu + (n - \mu) + (n - \mu - 1) = 2n - \mu - 1$ replacements are performed. To update a degree i ($i > n - \mu$) vector polynomial, $9i + 6$ multiplications and $6i + 3$ additions are required, including computing the constants α, β, and γ. Similarly, to update a degree i ($\mu < i \leqslant n - \mu$) vector polynomial, $6i$ multiplications and $3i$ additions are needed. Thus, totally, at most $3\sum_{i=n-\mu+1}^{n}(9i + 6) + 2\sum_{i=\mu+1}^{n-\mu} 6i = 27\mu(2n - \mu + 1)/2 + 6(n - 1)(n - 2\mu) + 18\mu$ multiplications and $3\sum_{i=n-\mu+1}^{n}(6i + 3) + 2\sum_{i=\mu+1}^{n-\mu} 3i = 9\mu(2n - \mu + 1) + 3(n - 1)(n - 2\mu) + 9\mu$ additions are required.

In the generic case where $\mu = n/2$, the costs are about $(81/8)n^2 + (63/4)n$ multiplications and $(27/4)n^2 + 9n$ additions. In comparison, the cost of the ZS algorithm is $(81/4)n^2 + (63/2)n$ multiplications and $(81/8)n^2 + (63/4)n$ additions. So our algorithm is about twice as fast as the ZS algorithm in the generic case. As $\mu < n/2$ gets smaller, the improvement of our algorithm over the ZS algorithm is even better; for example, if $\mu = n/3$, the number of multiplications used in our algorithm and the number of multiplications in the ZS algorithm are about $(19/2)n^2$ and $21n^2$, respectively.

4. Conclusion

We have presented some properties and equivalent definitions of the μ-basis of a planar rational curve. Several of these properties and definitions are new, and help us gain a better understanding of the μ-basis. These results have recently been used in the study of the reparameterization of a rational ruled surface [1]. Furthermore, based on these results, we presented in the present paper an improved algorithm for computing a μ-basis of a planar rational curve. The idea of the algorithm is to apply vector elimination efficiently to the moving line module of a rational curve. We have shown that the new algorithm is faster than the ZS algorithm [7], which is the fastest previous algorithm for computing the μ-basis of a planar rational curve. The two algorithms have the same order of operation counts, $O(n^2)$, but the proportional constant of our algorithm is about twice as small as that of the ZS algorithm; this difference further widens for rational curves in higher dimensions.

Acknowledgments

Falai Chen is supported by the Outstanding Youth Grant of NSF of China (No. 60225002), NSF of China (No. 19971087), NKBRSF on Mathematical Mechanics (No. G1998030600), the TRAPOYT in Higher Education Institute of MOE of China and the Doctoral Program of MOE of China (No. 20010358003). Wenping Wang is supported by RGC grants from Hong Kong Research Grant Council. Thanks go to the referees whose comments helped improved the presentation of the paper.

References

[1] F.L. Chen, Reparameterization of a rational ruled surface by μ-basis, Comput. Aided Geom. Design (2003), to appear.
[2] F.L. Chen, W.P. Wang, Computing the singular points of a planar rational curve using the μ-basis, preprint 2002.
[3] D. Cox, T. Sederberg, F. Chen, The moving line ideal basis of planar rational curves, Comput. Aided Geom. Design 15 (1998) 803–827.
[4] D. Cox, J. Little, D. O'Shea, Using Algebraic Geometry, Springer-Verlag, Berlin, 1998.

[5] T. Sederberg, T. Saito, D. Qi, K. Klimaszewski, Curve implicitization using moving lines, Comput Aided Geom. Design 11 (1994) 687–706.
[6] T. Sederberg, F. Chen, Implicitization using moving curves and surfaces, Computer Graphics Proceedings, Annual Conference Series 2 (1995) 301–308.
[7] J. Zheng, T.W. Sederberg, A direct approach to computing the μ-basis of planar rational curves, J. Symbolic Comput. 31 (2001) 619–629.