ELSEVIER

Journal of Symbolic Computation 36 (2003) 699–716

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Revisiting the μ-basis of a rational ruled surface

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

[a] *Department of Mathematics, University of Science and Technology of China, JinZhai Road 96, 230026 Hefei, Anhui, China*

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

Received 2 September 2002; accepted 23 March 2003

Abstract

The μ-basis of a rational ruled surface $\mathbf{P}(s,t) = \mathbf{P}_0(s)+t\mathbf{P}_1(s)$ is defined in Chen et al. (Comput. Aided Geom. Design 18 (2001) 61) to consist of two polynomials $p(x,y,z,s)$ and $q(x,y,z,s)$ that are linear in x, y, z. It is shown there that the resultant of p and q with respect to s gives the implicit equation of the rational ruled surface; however, the parametric equation $\mathbf{P}(s,t)$ of the rational ruled surface cannot be recovered from p and q. Furthermore, the μ-basis thus defined for a rational ruled surface does not possess many nice properties that hold for the μ-basis of a rational planar curve (Comput. Aided Geom. Design 18 (1998) 803). In this paper, we introduce another polynomial $r(x,y,z,s,t)$ that is linear in x, y, z and t such that p, q, r can be used to recover the parametric equation $\mathbf{P}(s,t)$ of the rational ruled surface; hence, we redefine the μ-basis to consist of the three polynomials p, q, r. We present an efficient algorithm for computing the newly-defined μ-basis, and derive some of its properties. In particular, we show that the new μ-basis serves as a basis for both the moving plane module and the moving plane ideal corresponding to the rational ruled surface.

Keywords: μ-Basis; Moving plane; Implicitization; Module; Rational ruled surface

1. Introduction

A rational ruled surface of degree n in homogeneous form is defined as

$$\mathbf{P}(s,t) = \mathbf{P}_0(s) + t\mathbf{P}_1(s) := (a(s,t), b(s,t), c(s,t), d(s,t)) \tag{1}$$

where

$$\mathbf{P}_i(s) = (a_i(s), b_i(s), c_i(s), d_i(s)), \qquad i = 0, 1 \tag{2}$$

* Corresponding author. Tel.: +86-55-13607537; fax: +86-55-13601005.
E-mail addresses: chenfl@ustc.edu.cn (F. Chen), wenping@csis.hku.hk (W. Wang).

0747-7171/03/$ - see front matter © 2003 Elsevier Ltd. All rights reserved.
doi:10.1016/S0747-7171(03)00064-6

and the maximum degree of $a_i(s)$, $b_i(s)$, $c_i(s), d_i(s)$, $i = 0, 1$, is n. To avoid the degenerate case where $\mathbf{P}(s,t)$ parameterizes a line, we assume that $\mathbf{P}_0(s)$ and $\mathbf{P}_1(s)$ are $\mathbb{R}[s]$-linearly independent. Furthermore, we assume that the rational ruled surface (1) is properly parameterized by $\mathbf{P}(s,t)$.

In a previous paper (Chen et al., 2001), we studied the μ-basis of a rational ruled surface, and based on the μ-basis, derived a closed-form representation of the implicit equation of a rational ruled surface. The μ-basis is defined to be two polynomials $p = p(x,y,z,s)$ and $q = q(x,y,z,s)$ that are linear in x, y, z and of degree $\mu (\mu \leq [m/2])$ and $m - \mu$ in s respectively, where m is the degree of the implicit equation. The implicit equation of the surface is then obtained merely by taking the resultant of p and q with respect to s. The idea of a μ-basis was originated in a series of papers by Sederberg and his collaborators where a novel technique called *moving curves and moving surfaces* was proposed to implicitize rational curves and surfaces (Sederberg et al., 1994; Sederberg and Chen, 1995; Sederberg and Saito, 1995). Cox et al. (1998b) applied tools from commutative algebra such as modules to study *moving lines* and define the μ-basis of a planar rational curve. The μ-basis of a planar rational curve can be used not only to generate a closed-form representation of the implicit equation, but also to recover the parametric equation of the rational curve. Thus, 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 μ-basis of a rational curve is subsequently generalized to rational ruled surfaces in Chen et al. (2001). However, unlike the case of a planar rational curve, the parametric equation $\mathbf{P}(s,t)$ of a rational ruled surface cannot be recovered from the μ-basis thus defined, since p and q do not involve the variable t. Furthermore, the μ-basis of a rational ruled surface does not possess many nice properties that hold for the μ-basis of a planar rational curve. To make the μ-basis of a rational ruled surface complete, in this paper we introduce another polynomial $r(x,y,z,s,t)$ that is linear in x, y, z and t so that p, q, r can be used to recover the parametric equation $\mathbf{P}(s,t)$ of the rational ruled surface; hence, we redefine the μ-basis to consist of the three polynomials p, q, r.

The remainder of the paper is organized as follows. In Section 2, we provide some preliminaries and recall some basic results from Chen et al. (2001). In Section 3, we redefine the μ-basis of a rational ruled surface, prove its existence, and present an efficient algorithm for computing this newly-defined μ-basis. In Section 4, we give some properties of the μ-basis; in particular, we show that the μ-basis is a basis for both the moving plane module and the moving plane ideal corresponding to the rational ruled surface. Finally, we conclude the paper in Section 5.

2. Preliminaries

Let R denote the polynomial ring $\mathbb{R}[s]$ or $\mathbb{R}[s,t]$ over the field of real numbers. Let R^m denote the set of m-dimensional row vectors with entries R. Similarly, let $R^{m\times n}$ denote the set of $m \times n$ matrices with entries in R.

For any $\mathbf{f}(s) = (f_1(s), f_2(s), f_3(s), f_4(s)) \in \mathbb{R}[s]^4$, the *degree* of $\mathbf{f}(s)$ is the maximum degree of $f_i(s)$, $i = 1, 2, 3, 4$, i.e., $\deg(\mathbf{f}) = \max_{1\le i\le 4} \deg(f_i(s))$. Write

$$\mathbf{f}(s) = \sum_{i=0}^{n} (f_{i1}, f_{i2}, f_{i3}, f_{i4}) s^i$$

where $n = \deg(\mathbf{f})$. The *leading coefficient vector* of $\mathbf{f}(s)$ is defined to be $LCV(\mathbf{f}) = (f_{n1}, f_{n2}, f_{n3}, f_{n4})$. For example, for $\mathbf{f}(s) = (2s - 1, s^2 + 3s + 1, 2s^2 - 1, s + 2)$, we have $\deg(\mathbf{f}) = 2$ and $LCV(\mathbf{f}) = (0, 1, 2, 0)$.

A set $M \subset R^m$ is called a *submodule* of R^m if $h_1\mathbf{f}_1 + h_2\mathbf{f}_2 \in M$ for any $\mathbf{f}_1, \mathbf{f}_2 \in M$ and $h_1, h_2 \in R$. A submodule $M \subset R^m$ is *finitely generated* if there exists a finite set of elements $\mathbf{f}_i \in M$, $i = 1, \ldots, k$, such that any $\mathbf{m} \in M$ can be expressed by

$$\mathbf{m} = h_1\mathbf{f}_1 + \cdots + h_k\mathbf{f}_k, \tag{3}$$

where $h_i \in R$, $i = 1, \ldots, k$; and in this case the set of the $\mathbf{f}_i$ is called a *generating set* of M. If the above express (3) is unique for any $\mathbf{m} \in M$, then $\mathbf{f}_1, \ldots, \mathbf{f}_k$ are called a *basis* of the module M. A module having a basis is called a *free module*. For any $(f_1, \ldots, f_k) \in R^k$, the set

$$syz(f_1, \ldots, f_k) := \{(h_1, \ldots, h_k) \in R^k \mid h_1 f_1 + \cdots + h_k f_k \equiv 0\} \tag{4}$$

is a module over R, called a *syzygy* module (Cox et al., 1998a). Syzygy modules play an important role in studying moving lines and moving planes.

A *moving plane*, denoted by $\mathbf{L}(s, t) := (A(s, t), B(s, t), C(s, t), D(s, t))$, is a family of planes $A(s, t)x + B(s, t)y + C(s, t)z + D(s, t) = 0$ with parameters (s, t). A moving plane is said to *follow* the rational ruled surface $\mathbf{P}(s, t)$ (1) if

$$\begin{aligned}\mathbf{L}(s, t) \cdot \mathbf{P}(s, t) = {} & A(s, t)a(s, t) + B(s, t)b(s, t) + C(s, t)c(s, t) \\ & + D(s, t)d(s, t) \equiv 0.\end{aligned} \tag{5}$$

Similarly, a *moving surface* of degree m in x, y, z and order l in s, t is a family of surfaces

$$F(x, y, z, s, t) := \sum_{0\le i+j\le l} f_{ij}(x, y, z) s^i t^j, \tag{6}$$

where $f_{ij}(x, y, z) \in \mathbb{R}[x, y, z]$ are polynomials of degree m. The moving surface $F(x, y, z, s, t)$ is said to *follow* $\mathbf{P}(s, t)$ if

$$d^m F(a/d, b/d, c/d, s, t) \equiv 0. \tag{7}$$

Let $\mathbf{L}_{s,t}$ be the set of all moving planes that follow the rational ruled surface $\mathbf{P}(s, t)$. Then $\mathbf{L}_{s,t}$ is a syzygy module over $\mathbb{R}[s, t]$.

Let $\mathbf{L}_s$ denote the set of all moving planes that involve only the parameter s; such a moving plane is denoted by $\mathbf{L}(s) := (A(s), B(s), C(s), D(s))$ with $\mathbf{L}(s) \cdot \mathbf{P}(s, t) \equiv 0$. Then $\mathbf{L}_s$ is a free module over $\mathbb{R}[s]$, as shown in Chen et al. (2001). Some of the main results in Chen et al. (2001) are stated in the following propositions.

Proposition 1. *Let* $g(s) = GCD([a, b], [a, c], [a, d], [b, c], [b, d], [c, d])$ *and* λ *be the maximum degree of* $[a, b], [a, c], [a, d], [b, c], [b, d], [c, d]$, *where* $[a, b] = a_0(s)b_1(s) - a_1(s)b_0(s)$ *and* $[a, c]$,$[a, d]$, $[b, c]$, $[b, d]$ *and* $[c, d]$ *are defined similarly. Then the implicit*

degree of the rational ruled surface $\mathbf{P}(s,t)$ *is* $m = \lambda - \deg(g)$. *Furthermore,* $\mathbf{P}(s,t)$ *does not have s-finite base points if and only if* $g(s) = 1$. *(A base point* (s_0, t_0) *of* $\mathbf{P}(s,t)$ *is called s-finite if* s_0 *is finite.)*

Proposition 2. *Let* $g(s)$ *be as defined in Proposition 1. Then the module* $\mathbf{L}_s$ *is generated by the rows of the following matrix:*

$$\mathbf{M} := \frac{1}{g(s)} \begin{pmatrix} 0 & [c,d] & [d,b] & [b,c] \\ [d,c] & 0 & [a,d] & [c,a] \\ [b,d] & [d,a] & 0 & [a,b] \\ [c,b] & [a,c] & [b,a] & 0 \end{pmatrix} \tag{8}$$

and $\operatorname{rank}(\mathbf{M}) = 2$ *for any parameter value s.*

Proposition 3. *There exist two elements* $\mathbf{p} = (p_1(s), p_2(s), p_3(s), p_4(s)) \in \mathbf{L}_s$ *and* $\mathbf{q} = (q_1(s), q_2(s), q_3(s), q_4(s)) \in \mathbf{L}_s$ *of degree* $\mu (\mu \le [m/2])$ *and* $m - \mu$, *respectively, such that* $\mathbf{p}$ *and* $\mathbf{q}$ *form a basis of* $\mathbf{L}_s$. *Here m is the implicit degree of the rational ruled surface (1). Furthermore,* $\mathbf{p}(s)$ *and* $\mathbf{q}(s)$ *are linearly independent for any parameter value s. In particular,* $LCV(\mathbf{p})$ *and* $LCV(\mathbf{q})$ *are linearly independent.*

Proposition 4. *Let* $\mathbf{p}$ *and* $\mathbf{q}$ *be as defined in Proposition 3. Denote* $p(x,y,z,s) = \mathbf{p} \cdot \mathbf{X}$ *and* $q(x,y,z,s) = \mathbf{q} \cdot \mathbf{X}$, *where* $\mathbf{X} = (x,y,z,1)$. *Then the implicit equation of* $\mathbf{P}(s,t)$ *is given by the resultant of p and q with respect to s.*

The polynomials p and q, or equivalently, the vector polynomials $\mathbf{p}$ and $\mathbf{q}$, are defined in Chen et al. (2001) to be a μ-basis of the rational ruled surface $\mathbf{P}(s,t)$. An efficient algorithm is presented in Chen et al. (2001) for computing p and q. Note that p and q cannot be used to recover the parametric equation of $\mathbf{P}(s,t)$ of the rational ruled surface, since p and q do not involve the parameter t.

3. Redefine the μ-basis of a rational ruled surface

In this section we introduce a polynomial $r(x,y,z,s,t)$ that is linear in x, y, z and t, and redefine the μ-basis of the rational ruled surface $\mathbf{P}(s,t)$ to consist of the three polynomials p, q and r. We first prove the existence of such a polynomial r and then present an algorithm for computing the newly defined μ-basis p, q and r.

We intend to find a vector valued polynomial

$$\mathbf{r}(s,t) := \mathbf{u}(s) + t\mathbf{v}(s) := (r_1(s,t), r_2(s,t), r_3(s,t), r_4(s,t)) \in \mathbf{L}_{s,t} \tag{9}$$

where

$$\mathbf{u}(s) = (u_1(s), u_2(s), u_3(s), u_4(s)) \in \mathbb{R}[s]^4,$$
$$\mathbf{v}(s) = (v_1(s), v_2(s), v_3(s), v_4(s)) \in \mathbb{R}[s]^4$$

and

$$r_i(s,t) = u_i(s) + v_i(s)t, \qquad i = 1,2,3,4$$

such that the parametric equation $\mathbf{P}(s,t)$ can be recovered from $\mathbf{p}$, $\mathbf{q}$ and $\mathbf{r}$; that is,

$$[\mathbf{p},\mathbf{q},\mathbf{r}] = \kappa\mathbf{P}(s,t) \tag{10}$$

for some nonzero constant κ. Here $[\mathbf{p},\mathbf{q},\mathbf{r}]$ is the *outer product* of $\mathbf{p}$, $\mathbf{q}$ and $\mathbf{r}$, which is defined by

$$[\mathbf{p},\mathbf{q},\mathbf{r}] = \left(\begin{vmatrix} p_2 & p_3 & p_4 \\ q_2 & q_3 & q_4 \\ r_2 & r_3 & r_4 \end{vmatrix}, -\begin{vmatrix} p_1 & p_3 & p_4 \\ q_1 & q_3 & q_4 \\ r_1 & r_3 & r_4 \end{vmatrix}, \begin{vmatrix} p_1 & p_2 & p_4 \\ q_1 & q_2 & q_4 \\ r_1 & r_2 & r_4 \end{vmatrix}, -\begin{vmatrix} p_1 & p_2 & p_3 \\ q_1 & q_2 & q_3 \\ r_1 & r_2 & r_3 \end{vmatrix} \right). \tag{11}$$

In the following, we show that such a polynomial $\mathbf{r}$ always exists, and we devise an efficient algorithm for computing the polynomial $\mathbf{r}$ with the lowest degree in s. We redefine the μ-basis of the rational ruled surface (1) to be the three polynomials $p = \mathbf{p}\cdot\mathbf{X}$, $q = \mathbf{q}\cdot\mathbf{X}$, $r = \mathbf{r}\cdot\mathbf{X}$, where $\mathbf{X} = (x, y, z, 1)$, or directly to be the three vector valued polynomials $\mathbf{p}$, $\mathbf{q}$ and $\mathbf{r}$. Some properties of the newly defined μ-basis will be presented in the next section.

Theorem 1. *There exists a vector valued polynomial* $\mathbf{r}(s,t) \in \mathbf{L}_{s,t}$ *as defined in* (9) *such that* (10) *holds.*

Proof. Take u_i and v_i, $i = 1, 2, 3, 4$, as unknowns and rewrite (10) in matrix form

$$\bar{\mathbf{M}}(\mathbf{u}(s)^{\mathrm{T}}, \mathbf{v}(s)^{\mathrm{T}}) = \kappa(\mathbf{P}_0(s)^{\mathrm{T}}, \mathbf{P}_1(s)^{\mathrm{T}}) \tag{12}$$

where

$$\bar{\mathbf{M}} = \begin{pmatrix} 0 & [3,4] & [4,2] & [2,3] \\ [4,3] & 0 & [1,4] & [3,1] \\ [2,4] & [4,1] & 0 & [1,2] \\ [3,2] & [1,3] & [2,1] & 0 \end{pmatrix} \tag{13}$$

and $[i, j] = p_i q_j - p_j q_i$.

We are going to prove that the system of equations (12) has a solution $\mathbf{r}(s,t)$. To this end, consider a rational ruled surface defined by

$$\bar{\mathbf{P}}(s,t) = \mathbf{p}(s) + t\mathbf{q}(s). \tag{14}$$

By Proposition 3, $\mathbf{p}(s)$ and $\mathbf{q}(s)$ are linearly independent for any parameter s. Therefore, $\bar{\mathbf{P}}(s,t)$ does not have any s-finite base point; for otherwise, there exist some t_0 and s_0 such that $\mathbf{p}(s_0) + t_0\mathbf{q}(s_0) = 0$, which implies that $\mathbf{p}(s_0)$ and $\mathbf{q}(s_0)$ are linearly dependent. It follows, by Proposition 1, that $GCD([1,2],[1,3],[1,4],[2,3],[2,4],[3,4]) = 1$. Since $\mathbf{p}\cdot\mathbf{P}_i(s) = 0$ and $\mathbf{q}\cdot\mathbf{P}_i(s) = 0$, $i = 0, 1$, $\mathbf{P}_0(s)$ and $\mathbf{P}_1(s)$ are moving planes that follow $\bar{\mathbf{P}}(s,t)$. By Proposition 2, $\mathbf{P}_0(s)$ and $\mathbf{P}_1(s)$ can be generated by the rows of the matrix $\bar{\mathbf{M}}$. Hence, there exists a polynomial $\mathbf{r}(s,t)$ satisfying (10).

Furthermore, since

$$\mathbf{P}(s,t)\cdot\mathbf{r}(s,t)=\begin{vmatrix} r_1 & r_2 & r_3 & r_4\\ p_1 & p_2 & p_3 & p_4\\ q_1 & q_2 & q_3 & q_4\\ r_1 & r_2 & r_3 & r_4 \end{vmatrix}\equiv 0$$

$r := \mathbf{r}(s,t)\cdot\mathbf{X}=0$ is a moving plane that follows $\mathbf{P}(s,t)$; that is, $\mathbf{r}(s,t)\in\mathbf{L}_{s,t}$. □

Below we present an algorithm for computing the newly defined μ-basis p,q,r, based on the proof of Theorem 1 and the algorithm developed in Chen et al. (2001) for computing the two elements $\mathbf{p},\mathbf{q}$. Before that, we first need to modify the algorithm in Chen et al. (2001) so as to use it to compute, besides $\mathbf{p}$ and $\mathbf{q}$, the matrix for transforming the rows of the matrix $\mathbf{M}$ to $\mathbf{p}$ and $\mathbf{q}$, i.e., a matrix $\mathbf{T}\in\mathbb{R}[s]^{2\times 4}$ such that

$$\mathbf{TM}=\begin{pmatrix}\mathbf{p}\\ \mathbf{q}\end{pmatrix}. \tag{15}$$

We begin with some notation, following Chen et al. (2001). Let $\mathbf{E}_i = (0,\ldots,0,1,0,\ldots,0)\in\mathbb{R}[s]^m$ be the standard basis vectors, $i=1,2,\ldots,m$, where 1 is in the ith position in the vector. Any $\mathbf{f}(s)\in\mathbb{R}[s]^m$ can be written as

$$\mathbf{f}(s)=\sum_{i=0}^{n}\sum_{j=1}^{m} f_{ij}s^i\mathbf{E}_j$$

where $n=\deg(\mathbf{f})$ and therefore at least one of the coefficients f_{nj}, $j=1,2,\ldots,m$, is nonzero. Let j be the smallest index such that f_{nj} is nonzero. Then we say that $\mathbf{f}$ contains the *basis vector* $\mathbf{E}_j$; and f_{nj}, $s^n\mathbf{E}_j$ and $f_{nj}s^n\mathbf{E}_j$ are called the *leading coefficient, leading monomial* and *leading term* of $\mathbf{f}$ (denoted by $LC(\mathbf{f})$, $LM(\mathbf{f})$ and $LT(\mathbf{f})$), respectively. For example, for $\mathbf{f}(s)=(2s-2,3s^2+1,s^2-3s+2,2s^2+s)\in\mathbb{R}[s]^4$, the basis vector is $\mathbf{E}_2$, $LC(\mathbf{f})=3$, $LM(\mathbf{f})=s^2\mathbf{E}_2$ and $LT(\mathbf{f})=3s^2\mathbf{E}_2$.

Now we outline the algorithm for computing $\mathbf{p},\mathbf{q}$ and the transformation matrix $\mathbf{T}$ between $\mathbf{p},\mathbf{q}$ and $\mathbf{M}$ as defined in (8). For convenience of description, we assume that the coefficients are integers.

Algorithm: *PMU-BASIS*

Input: A parametric equation $\mathbf{P}(s,t)$ of the rational ruled surface (1).

Output: Two elements $\mathbf{p},\mathbf{q}\in\mathbb{R}[s]^4$ of the μ-basis, and the transformation matrix $\mathbf{T}$ between the generating matrix $\mathbf{M}$ and $\mathbf{p},\mathbf{q}$.

Step 1. Set

$$\mathbf{v}_1=(0,[c,d],[d,b],[b,c])/g,\qquad \mathbf{v}_2=([d,c],0,[a,d],[c,a])/g,$$
$$\mathbf{v}_3=([b,d],[d,a],0,[a,b])/g,\qquad \mathbf{v}_4=([c,b],[a,c],[b,a],0)/g,$$

and $S=\{\mathbf{v}_1,\mathbf{v}_2,\mathbf{v}_3,\mathbf{v}_4\}$. Furthermore, set $\mathbf{T}=\mathbf{I}\in\mathbb{R}[s]^{4\times 4}$, where $\mathbf{I}$ is the identity matrix.

Step 2. Choose $\mathbf{v}_i$ and $\mathbf{v}_j$ from S such that $LT(\mathbf{v}_i)$ and $LT(\mathbf{v}_j)$ contain the same basis vector. Assume $\deg(\mathbf{v}_i)\geq\deg(\mathbf{v}_j)$.

Step 3. Replace $\mathbf{v}_i$ by

$$\mathbf{v}_i := \frac{LCM(LC(\mathbf{v}_i), LC(\mathbf{v}_j))}{LC(\mathbf{v}_i)}\mathbf{v}_i - \frac{LCM(LC(\mathbf{v}_i), LC(\mathbf{v}_j))}{LC(\mathbf{v}_j)}s^{\deg(\mathbf{v}_i)-\deg(\mathbf{v}_j)}\mathbf{v}_j$$

where $LCM(k, l)$ is the least common multiple of k and l. Update $\mathbf{T}$ by replacing the ith row $\mathbf{T}_i$ of $\mathbf{T}$ by

$$\mathbf{T}_i := \frac{LCM(LC(\mathbf{v}_i), LC(\mathbf{v}_j))}{LC(\mathbf{v}_i)}\mathbf{T}_i - \frac{LCM(LC(\mathbf{v}_i), LC(\mathbf{v}_j))}{LC(\mathbf{v}_j)}s^{\deg(\mathbf{v}_i)-\deg(\mathbf{v}_j)}\mathbf{T}_j.$$

Step 4. If $\mathbf{v}_i = 0$, remove $\mathbf{v}_i$ from S, and delete the ith row of $\mathbf{T}$.

Step 5. If the leading term of each element in S has a different basis vector, then stop; else go to Step 2.

The correctness of the above algorithm can be shown along the same line as in Chen et al. (2001).

Next we describe the main algorithm for computing the new element $\mathbf{r}$ of the μ-basis. Note that Step 3 of this algorithm is based on the observation that $\mathbf{P}_0(s)$ and $\mathbf{P}_1(s)$ are two moving planes following the rational ruled surface $\bar{\mathbf{P}}(s, t) = \mathbf{p}(s) + t\mathbf{q}(s)$.

Algorithm: *MU-BASIS*

Input: A parametric equation $\mathbf{P}(s, t)$ of the rational ruled surface (1).

Output: Three elements $\mathbf{p}$, $\mathbf{q}$, $\mathbf{r}$ of the μ-basis of $\mathbf{P}(s, t)$.

Step 1. Compute $\mathbf{p}$ and $\mathbf{q}$ using the algorithm developed in Chen et al. (2001).

Step 2. Compute the μ-basis $\bar{\mathbf{p}}$ and $\bar{\mathbf{q}}$ of the rational ruled surface $\bar{\mathbf{P}}(s, t)$ defined in (14) and the transformation matrix $\mathbf{T}$ between $\bar{\mathbf{p}}$, $\bar{\mathbf{q}}$ and $\bar{\mathbf{M}}^{\mathrm{T}}$ defined in (13), using the algorithm *PMU-BASIS*. Let $\bar{\mathbf{M}}_i$, $i = 1, 2, 3, 4$, be the rows of $\bar{\mathbf{M}}^{\mathrm{T}}$ and let $\mathbf{T} = (t_{ij})_{2\times 4}$. Then

$$\bar{\mathbf{p}} = \sum_{i=1}^{4} t_{1i}\bar{\mathbf{M}}_i, \qquad \bar{\mathbf{q}} = \sum_{i=1}^{4} t_{2i}\bar{\mathbf{M}}_i. \tag{16}$$

Step 3. Express $\mathbf{P}_0(s)$ and $\mathbf{P}_1(s)$ as $\mathbb{R}[s]$-linear combinations of $\bar{\mathbf{p}}, \bar{\mathbf{q}}$; that is, find polynomials $h_{ij}(s)$, $i, j = 0, 1$, and a nonzero constant κ, such that

$$\kappa\mathbf{P}_0(s) = h_{00}(s)\bar{\mathbf{p}} + h_{01}(s)\bar{\mathbf{q}}, \qquad \kappa\mathbf{P}_1(s) = h_{10}(s)\bar{\mathbf{p}} + h_{11}(s)\bar{\mathbf{q}} \tag{17}$$

where $\deg(h_{i0}\bar{\mathbf{p}}) \le \deg(\mathbf{P}_i)$, $\deg(h_{i1}\bar{\mathbf{q}}) \le \deg(\mathbf{P}_i)$, $i = 0, 1$. To express $\mathbf{P}_0(s)$ as an $\mathbb{R}[s]$-linear combination of $\bar{\mathbf{p}}$ and $\bar{\mathbf{q}}$, we first set $h_{00}(s) := 0$ and $h_{01}(s) := 0$. Suppose $\kappa LCV(\mathbf{P}_0) = \alpha LCV(\bar{\mathbf{p}}) + \beta LCV(\bar{\mathbf{q}})$. Update $\mathbf{P}_0(s)$ by

$$\mathbf{P}_0(s) := k\mathbf{P}_0(s) - \alpha s^{(\deg(\mathbf{P}_0)-\deg(\bar{\mathbf{p}}))}\bar{\mathbf{p}} - \beta s^{(\deg(\mathbf{P}_0)-\deg(\bar{\mathbf{q}}))}\bar{\mathbf{q}}$$

and update $h_{00}(s)$ and $h_{01}(s)$ by

$$h_{00}(s) := h_{00}(s) + \alpha s^{(\deg(\mathbf{P}_0)-\deg(\bar{\mathbf{p}}))}, \qquad h_{01}(s) := h_{01}(s) + \beta s^{(\deg(\mathbf{P}_0)-\deg(\bar{\mathbf{q}}))}.$$

Continue the above replacement until $\mathbf{P}_0(s) = 0$. Note that the constant κ in the two equations of (17) must be the same. Similarly, express $\mathbf{P}_1(s)$ in an $\mathbb{R}[s]$-linear combination of $\bar{\mathbf{p}}$ and $\bar{\mathbf{q}}$.

Step 4. Set

$$u_i(s) = t_{1i}(s)h_{00}(s) + t_{2i}(s)h_{01}(s), \qquad v_i(s) = t_{1i}(s)h_{10}(s) + t_{2i}(s)h_{11}(s)$$

$i = 1, 2, 3, 4$, $\mathbf{u} = (u_1, u_2, u_3, u_4)$ and $\mathbf{v} = (v_1, v_2, v_3, v_4)$.

Step 5. If $LCV(\mathbf{p})$, $LCV(\mathbf{q})$ and $LCV(\mathbf{u})$ are linearly dependent and $\deg(\mathbf{u}) \geq \deg(\mathbf{q})$, then there exist constants α, β and κ such that

$$\kappa LCV(\mathbf{u}) = \alpha LCV(\mathbf{p}) + \beta LCV(\mathbf{q}).$$

Replace $\mathbf{u}$ by

$$\mathbf{u} := \kappa\mathbf{u} - \alpha s^{(\deg(\mathbf{u})-\deg(\mathbf{p}))}\mathbf{p} - \beta s^{(\deg(\mathbf{u})-\deg(\mathbf{q}))}\mathbf{q}.$$

Repeat the above process until the conditions are no longer satisfied.

Step 6. If $LCV(\mathbf{p})$, $LCV(\mathbf{q})$ and $LCV(\mathbf{v})$ are linearly dependent and $\deg(\mathbf{v}) \geq \deg(\mathbf{q})$, then there exist constants α, β and κ such that

$$\kappa LCV(\mathbf{v}) = \alpha LCV(\mathbf{p}) + \beta LCV(\mathbf{q}).$$

Replace $\mathbf{v}$ by

$$\mathbf{v} := \kappa\mathbf{v} - \alpha s^{(\deg(\mathbf{v})-\deg(\mathbf{p}))}\mathbf{p} - \beta s^{(\deg(\mathbf{v})-\deg(\mathbf{q}))}\mathbf{q}.$$

Repeat the above process until the conditions are no longer satisfied.

Step 7. Make equal the constants κ multiplied to $\mathbf{u}$ and $\mathbf{v}$ in Steps 5 and 6. Set $\mathbf{r} = \mathbf{u} + t\mathbf{v}$ and output $\mathbf{p}$, $\mathbf{q}$ and $\mathbf{r}$.

Theorem 2. *The algorithm MU-BASIS correctly computes the newly defined μ-basis of the rational ruled surface $\mathbf{P}(s, t)$.*

Proof. From Steps 2–4, one has

$$\kappa\mathbf{P}_0(s) = h_{00}\bar{\mathbf{p}} + h_{01}\bar{\mathbf{q}} = \sum_{i=1}^{4}(t_{1i}h_{00} + t_{2i}h_{01})\mathbf{M}_i = \mathbf{u}\bar{\mathbf{M}}^{\mathrm{T}}.$$

Similarly,

$$\kappa\mathbf{P}_1(s) = \mathbf{v}\bar{\mathbf{M}}^{\mathrm{T}}.$$

Thus $\mathbf{u}$ and $\mathbf{v}$ are the solutions of the system of equations (12); that is, $\mathbf{r} = \mathbf{u} + t\mathbf{v}$ satisfies (10). Steps 3 can be done since $\mathbf{P}_0(s)$ and $\mathbf{P}_1(s)$ are moving planes following $\bar{\mathbf{P}}(s, t)$ and thus can be expressed as $\mathbb{R}[s]$-linear combinations of $\bar{\mathbf{p}}$ and $\bar{\mathbf{q}}$.

To show $\mathbf{r}$ has the lowest degree in s, we note that all solutions of the equation

$$\bar{\mathbf{M}}\mathbf{u}^{\mathrm{T}} = \mathbf{0}$$

are generated by $\mathbf{p}$ and $\mathbf{q}$. Therefore the solution of the equation

$$\bar{\mathbf{M}}\mathbf{u}^{\mathrm{T}} = \mathbf{P}_0(s)^{\mathrm{T}}$$

takes the form $\mathbf{u} = h_1\mathbf{p} + h_2\mathbf{q} + \mathbf{u}_0$, where $h_1, h_2 \in \mathbb{R}[s]$ and $\mathbf{u}_0$ is a particular solution of the above equation. Hence, Steps 5 and 6 reduce the degree of $\mathbf{r}$ and guarantee that $\mathbf{r}$ has the lowest degree in s. □

We end this section with an example from Chen et al. (2001) to demonstrate the algorithm *MU-BASIS*.

Let a rational ruled surface $\mathbf{P}(s,t) = \mathbf{P}_0(s) + t\mathbf{P}_1(s)$ be given by

$$\mathbf{P}_0(s) = (s^3 + 2s^2 - s + 3, -3s + 3, -2s^2 - 2s + 3, 2s^2 + s + 2)$$

and

$$\mathbf{P}_1(s) = (2s^3 + 2s^2 - 3s + 7, 2s^2 - 5s + 5, -6s^2 - 8s + 4, 5s^2 + 4s + 5).$$

Using the algorithm in Chen et al. (2001), $\mathbf{p}$ and $\mathbf{q}$ are found to be

$$\mathbf{p} = (22s + 31, 15s^2 + 39s + 33, 19s^2 - 11s - 28, 8s^2 - 11s - 54)$$
$$\mathbf{q} = (62s - 154, 4s^2 - 39s - 259, -23s^2 - 189s + 207, -54s^2 - 164s + 309).$$

Next we obtain the μ-basis $\bar{\mathbf{p}}$ and $\bar{\mathbf{q}}$ of $\bar{\mathbf{P}}(s,t) = \mathbf{p} + t\mathbf{q}$

$$\bar{\mathbf{p}} = 2526(1 - 2s, 2s - 1, -2s - 2, s + 1)$$
$$\bar{\mathbf{q}} = (746s^2 - 73s, 48s^3 - 650s^2 - 119s + 288, -48s^3 + 482s^2 + 818s + 432, 24s^3 - 193s^2 - 409s - 48)$$

and the transformation matrix

$$\mathbf{T} = \begin{pmatrix} 454s + 421 & 233s^2 + 687s + 421 & 239s^2 - 315s & 12s^2 - 397s \\ -140s - 48 & -70s^2 - 178s & -70s^2 + 123s & 112s \end{pmatrix}$$

between $\bar{\mathbf{M}}$ and $\bar{\mathbf{p}}$, $\bar{\mathbf{q}}$. Now express $\mathbf{P}_i(s)$, $i = 0, 1$, in (17), where

$$h_{00} = 24s^2 - 313s - 144, \qquad h_{01} = -2526, \qquad h_{10} = 48s^2 - 674s - 336,$$
$$h_{11} = -5052, \qquad \kappa = -121\,248$$

and obtain

$$\mathbf{u} = (60\,624 + 156\,491s - 131\,998s^2 + 10\,896s^3, 218\,927s - 61\,659s^2 - 60\,624 - 56\,441s^3 + 5592s^4, -265\,338s + 240\,999s^2 - 82\,367s^3 + 5736s^4, -225\,744s - 13\,284s^3 + 122\,533s^2 + 288s^4)$$
$$\mathbf{v} = 2(50\,520 + 135\,491s - 142\,894s^2 + 10\,896s^3, 192\,335s - 83\,739s^2 - 70\,728 - 62\,033s^3 + 5592s^4, -25\,7778s + 242\,823s^2 - 88\,103s^3 + 5736s^4, -216\,216s - 13\,572s^3 + 131\,773s^2 + 288s^4).$$

Reducing the degrees of $\mathbf{u}$ and $\mathbf{v}$ by Steps 5 and 6, we finally obtain $\mathbf{r} = \mathbf{u} + t\mathbf{v}$, where

$$\mathbf{u} = (882, 410s + 871, 379s - 1109, -62s - 966)$$
$$\mathbf{v} = (1818, 742s + 1718, 575s - 2389, -334s - 2352).$$

4. Properties of the newly defined μ-basis

In this section we will explore some properties of the μ-basis consisting of the three polynomials p, q and r. In particular, we show that the μ-basis serves as the basis for both the module $\mathbf{L}_{s,t}$ and the ideal corresponding to the rational ruled surface $\mathbf{P}(s,t)$.

Theorem 3. *The three elements* $\mathbf{p}, \mathbf{q}$ *and* $\mathbf{r} = \mathbf{u} + t\mathbf{v}$ *of the* μ*-basis are* $\mathbb{R}[s,t]$*-linearly independent. In particular,* $\mathbf{p}, \mathbf{q}, \mathbf{u}$ *are* $\mathbb{R}[s]$*-linearly independent and* $\mathbf{p}, \mathbf{q}, \mathbf{v}$ *are* $\mathbb{R}[s]$*-linearly independent. Furthermore, for a specific parameter pair* (s_0, t_0)*,*

1. $\mathbf{p}(s_0,t_0)$, $\mathbf{q}(s_0,t_0)$, $\mathbf{r}(s_0,t_0)$ *are linearly dependent if and only if* (s_0,t_0) *is a base point of* $\mathbf{P}(s,t)$*;*
2. $\mathbf{p}(s_0)$, $\mathbf{q}(s_0)$ *and* $\mathbf{u}(s_0)$ *are linearly dependent if and only if* s_0 *is a common zero of* $a_0(s)$, $b_0(s)$, $c_0(s)$ *and* $d_0(s)$*;*
3. $\mathbf{p}(s_0)$, $\mathbf{q}(s_0)$ *and* $\mathbf{v}(s_0)$ *are linearly dependent if and only if* s_0 *is a common zero of* $a_1(s)$, $b_1(s)$, $c_1(s)$ *and* $d_1(s)$.

Proof. If $\mathbf{p}, \mathbf{q}, \mathbf{r}$ are $\mathbb{R}[s,t]$-linearly dependent, then one can verify that the outer product of $\mathbf{p}, \mathbf{q}, \mathbf{r}$ is the zero vector identically, which contradicts (10). Therefore $\mathbf{p}, \mathbf{q}, \mathbf{r}$ are $\mathbb{R}[s,t]$-linearly independent. Similarly, $[\mathbf{p}, \mathbf{q}, \mathbf{u}] = \kappa\mathbf{P}_0(s)$ and $[\mathbf{p}, \mathbf{q}, \mathbf{v}] = \kappa\mathbf{P}_1(s)$ implies that $\mathbf{p}, \mathbf{q}, \mathbf{u}$ and $\mathbf{p}, \mathbf{q}, \mathbf{v}$ are $\mathbb{R}[s]$-linearly independent.

For a specific parameter pair (s_0,t_0), $\mathbf{p}(s_0,t_0)$, $\mathbf{q}(s_0,t_0)$, $\mathbf{r}(s_0,t_0)$ are linearly dependent if and only if $[\mathbf{p}(s_0,t_0), \mathbf{q}(s_0,t_0), \mathbf{r}(s_0,t_0)] = \mathbf{0}$, or if and only if $\mathbf{P}(s_0,t_0) = \mathbf{0}$ by (10), i.e., (s_0,t_0) is a base point of $\mathbf{P}(s,t)$. Similarly, $\mathbf{p}(s_0)$, $\mathbf{q}(s_0)$ and $\mathbf{u}(s_0)$ are linearly dependent if and only if $\mathbf{P}_0(s_0) = 0$; furthermore, $\mathbf{p}(s_0)$, $\mathbf{q}(s_0)$ and $\mathbf{v}(s_0)$ are linearly dependent if and only if $\mathbf{P}_1(s_0) = 0$. □

Theorem 4. $\mathbf{p}, \mathbf{q}$ *and* $\mathbf{r}$ *form a basis for the module* $\mathbf{L}_{s,t}$*; that is, for any* $\mathbf{l}(s,t) \in \mathbf{L}_{s,t}$*, there exist polynomials* $h_i(s,t)$, $i = 1,2,3$*, such that*

$$\mathbf{l}(s,t) = h_1\mathbf{p} + h_2\mathbf{q} + h_3\mathbf{r} \tag{18}$$

and the above expression is unique (thus $\mathbf{L}_{s,t}$ *is a free module). Furthermore,* $\deg_t(h_1\mathbf{p}) \le \deg_t(\mathbf{l})$, $\deg_t(h_2\mathbf{q}) \le \deg_t(\mathbf{l})$, $\deg_t(h_3\mathbf{r}) \le \deg_t(\mathbf{l})$*; and* $\deg_s(h_1\mathbf{p}) \le \deg_s(\mathbf{l})$, $\deg_s(h_2\mathbf{q}) \le \deg_s(\mathbf{l})$, $\deg_s(h_3\mathbf{r}) \le \deg_s(\mathbf{l})$ *if* $LCV(\mathbf{p})$, $LCV(\mathbf{q})$ *and* $LCV_s(\mathbf{r})$ *are* $\mathbb{R}[t]$*-linearly independent, else* $\deg_s(h_1\mathbf{p})$, $\deg_s(h_2\mathbf{q})$ *and* $\deg_s(h_3\mathbf{r})$ *are bounded by* $\deg_s(\mathbf{l}) + m + \deg_s(\mathbf{r}) - n$.

Remark 1. Note the following facts.

1. It is easy to see that $LCV(\mathbf{p})$, $LCV(\mathbf{q})$ and $LCV_s(\mathbf{r})$ are $\mathbb{R}[t]$-linearly independent, if one of the following holds: (i) $\deg(\mathbf{u}) > \deg(\mathbf{v})$ and $LCV(\mathbf{p})$, $LCV(\mathbf{q})$ and $LCV(\mathbf{u})$ are linearly independent; (ii) $\deg(\mathbf{v}) > \deg(\mathbf{u})$ and $LCV(\mathbf{p})$, $LCV(\mathbf{q})$ and $LCV(\mathbf{v})$ are linearly independent; (iii) $\deg(\mathbf{u}) = \deg(\mathbf{v})$ and $LCV(\mathbf{p})$, $LCV(\mathbf{q})$, $LCV(\mathbf{u})$ are linearly independent; (iv) $\deg(\mathbf{u}) = \deg(\mathbf{v})$ and $LCV(\mathbf{p})$, $LCV(\mathbf{q})$, $LCV(\mathbf{v})$ are linearly independent.
2. Since one always has $\deg_s(\mathbf{r}) < \deg(\mathbf{q}) = m - \mu$, when $LCV(\mathbf{p})$, $LCV(\mathbf{q})$ and $LCV_s(\mathbf{r})$ are $\mathbb{R}[t]$-linearly dependent, $\deg_s(h_1\mathbf{p})$, $\deg_s(h_2\mathbf{q})$ and $\deg_s(h_3\mathbf{r})$ are generally bounded by $\deg_s(\mathbf{l}) + m + (m - \mu - 1) - n = \deg_s(\mathbf{l}) + 2m - n - \mu - 1$ in this case.

Before proving the theorem, we need several lemmas.

Lemma 1. *Let $g(s)$ be the polynomial defined in Proposition 1. Then $g(s) \in \langle a, b, c, d\rangle \subset \mathbb{R}[s, t]$.*

Proof. Since $g(s) = GCD([a, b], [a, c], [a, d], [b, c], [b, d], [c, d])$, there exist polynomials $h_i(s) \in \mathbb{R}[s]$, $i = 1, \ldots, 6$, such that

$$g = h_1[a, b] + h_2[a, c] + h_3[a, d] + h_4[b, c] + h_5[b, d] + h_6[c, d].$$

Obviously, $[a, b] = b_1 a - a_1 b \in \langle a, b, c, d\rangle$. Similarly, $[a, c]$, $[a, d]$, $[b, c]$, $[b, d]$ and $[c, d]$ all belong to $\langle a, b, c, d\rangle$. Hence, $g \in \langle a, b, c, d\rangle$. □

Lemma 2. *For any moving plane $Ax + By + cz + D \in \mathbf{L}_{s,t}$, there exist polynomials $h_i(s, t) \in \mathbb{R}[s, t]$, $i = 1, \ldots, 6$, such that*

$$\begin{aligned} g * (Ax + By + Cz + D) = {} & h_1(dx - a) + h_2(dy - b) + h_3(dz - c) \\ & + h_4(bx - ay) + h_5(cy - bz) + h_6(cx - az). \end{aligned}$$

Here $g(s)$ is as defined in Proposition 1.

Proof. By Lemma 1, there exist polynomials $k_i(s) \in \mathbb{R}[s]$ such that $g = k_1 a + k_2 b + k_3 c + k_4 d$. Hence

$$g * (Ax + By + Cz + D) = (k_1 a + k_2 b + k_3 c + k_4 d)(Ax + By + Cz + D).$$

Since $Ax + By + Cz + D = 0$ follows $\mathbf{P}(s, t)$, one has

$$Aa + Bb + Cc + Dd \equiv 0.$$

Thus

$$\begin{aligned} a(Ax + By + Cz + D) &= (-Bb - Cc - Dd)x + aBy + aCz + aD \\ &= B(ay - bx) + C(az - cx) + D(a - dx). \end{aligned}$$

Similarly, one can show that $b(Ax + By + Cz + D)$, $c(Ax + By + Cz + D)$ and $d(Ax + By + Cz + D)$ are all $\mathbb{R}[s, t]$-linear combinations of $dx - a$, $dy - b$, $dz - c$, $bx - ay$, $cy - bz$ and $cx - az$; hence, so is $g * (Ax + By + Cz + D)$. □

Lemma 3. *$dx - a$, $dy - b$, $dz - c$, $bx - ay$, $cy - bz$ and $cx - az$ are all $\mathbb{R}[s, t]$-linear combinations of p, q, r, where p, q, r are the μ-basis.*

Proof. By (10), one can directly verify that

$$\kappa(dx - a) = (q_3 r_2 - q_2 r_3)p + (r_3 p_2 - r_2 p_3)q + (p_3 q_2 - p_2 q_3)r$$

where κ is a nonzero constant, so $dx - a$ is an $\mathbb{R}[s, t]$-linear combination of p, q, r. Similarly, $dy - b$, $dz - c$, $bx - ay$, $cy - bz$ and $cx - az$ are all $\mathbb{R}[s, t]$-linear combinations of p, q, r. □

Lemma 4. *Any moving plane $Ax + By + Cz + D \in \mathbf{L}_{s,t}$ is an $\mathbb{R}[s, t]$-linear combination of p, q, r.*

Proof. From Lemmas 2 and 3, there exist polynomials $\bar{h}_i \in \mathbb{R}[s,t]$, $i = 1,2,3$, such that

$$g * (Ax + By + Cz + D) = \bar{h}_1 p + \bar{h}_2 q + \bar{h}_3 r$$

or equivalently

$$g(A,B,C,D) = \bar{h}_1 \mathbf{p} + \bar{h}_2 \mathbf{q} + \bar{h}_3 \mathbf{r}.$$

In the following, we want to show $g \mid \bar{h}_i$, $i = 1,2,3$.

Forming the outer product on both sides of the above equation with $\mathbf{q}, \mathbf{r}$, we get

$$g[(A,B,C,D), \mathbf{q}, \mathbf{r}] = \bar{h}_1[\mathbf{p}, \mathbf{q}, \mathbf{r}] = \kappa \bar{h}_1 (a,b,c,d).$$

Since $GCD(a,b,c,d) = 1$, $g \mid \bar{h}_1$. Similarly, $g \mid \bar{h}_2$ and $g \mid \bar{h}_3$. Thus we conclude that

$$Ax + By + Cz + D = h_1 p + h_2 q + h_3 r$$

for some $h_i \in \mathbb{R}[s,t]$, $i = 1,2,3$. □

Now we are ready to prove Theorem 4.

By Lemma 4, $\mathbf{p}, \mathbf{q}$ and $\mathbf{r}$ are a generating set of the module $\mathbf{L}_{s,t}$. On the other hand, since $\mathbf{p}, \mathbf{q}$ and $\mathbf{r}$ are linearly independent by Theorem 3, the expression (18) is unique. That is, $\mathbf{p}, \mathbf{q}$ and $\mathbf{r}$ form a basis of $\mathbf{L}_{s,t}$. The first part of the theorem is proved.

For the next part, we first prove the bounds on the degrees of h_i, $i = 1,2,3$, with respect to t. Assume that the maximum degree of $h_1\mathbf{p}$, $h_2\mathbf{q}$ and $h_3\mathbf{r}$ in t is l. Write

$$h_i = \sum_{j=0}^{l} h_{ij}(s) t^j, \qquad i = 1,2, \qquad h_3 = \sum_{j=0}^{l-1} h_{3j}(s) t^j.$$

If $\deg_t(\mathbf{l}) < l$, then the leading term in t on the right-hand side of equation (18) must vanish, that is,

$$h_{1l}\mathbf{p} + h_{2l}\mathbf{q} + h_{3,l-1}\mathbf{v} \equiv \mathbf{0}$$

which implies $\mathbf{p}, \mathbf{q}, \mathbf{v}$ are $\mathbb{R}[s]$-linearly dependent, a contradiction with Theorem 3. Thus we must have $\deg_t(\mathbf{l}) \geq l$.

Next we prove the bounds on the degrees of h_i, $i = 1,2,3$, with respect to s. From (18), we have $[\mathbf{p}, \mathbf{q}, \mathbf{l}] = h_3[\mathbf{p}, \mathbf{q}, \mathbf{r}] = \kappa h_3 \mathbf{P}(s,t)$, so $\deg_s(h_3) \leq \deg_s(\mathbf{l}) + m - n$, where m is the implicit degree of the rational ruled surface $\mathbf{P}(s,t)$. Hence, $\deg_s(h_3\mathbf{r}) \leq \deg_s(\mathbf{l}) + m + \deg_s(\mathbf{r}) - n$.

If $LCV(\mathbf{p})$, $LCV(\mathbf{q})$ and $LCV_s(\mathbf{r})$ are $\mathbb{R}[t]$-linearly independent, then from $[\mathbf{p}, \mathbf{q}, \mathbf{r}] = \kappa \mathbf{P}(s,t)$, one has $\deg(\mathbf{p}) + \deg(\mathbf{q}) + \deg_s(\mathbf{r}) = \deg_s(\mathbf{P})$, so $\deg_s(\mathbf{r}) = n - m$. Hence $\deg_s(h_3\mathbf{r}) \leq \deg_s(\mathbf{l})$ in this case. The bounds on the degrees of $h_1\mathbf{p}$ and $h_2\mathbf{q}$ follow similarly. □

Next we discuss the relationship of the μ-basis p, q, r and the ideal corresponding to $\mathbf{P}(s,t)$.

Theorem 5. *Let $f(x,y,z) = 0$ be the implicit equation of rational ruled surface $\mathbf{P}(s,t)$. Then $f(x,y,z) \in \langle p, q, r \rangle$.*

Proof. By Proposition 4, $f(x,y,z) \in \langle p, q \rangle \subset \langle p, q, r \rangle$. □

Theorem 6. *Let*

$$I := \langle dx - a, dy - b, dz - c\rangle \subset \mathbb{R}[x, y, z, s, t] \tag{19}$$

be the ideal corresponding to rational ruled surface (1) *and* $g(s)$ *be the polynomial as defined in Proposition* 1. *Then*

$$g\langle p, q, r\rangle \subset I \subset \langle p, q, r\rangle. \tag{20}$$

In particular, if a rational ruled surface $\mathbf{P}(s, t)$ *does not have* s*-finite base points, then* $I = \langle p, q, r\rangle$.

Proof. By Lemma 3, $dx - a$, $dy - b$, $dz - c \in \langle p, q, r\rangle$. Hence $I \subset \langle p, q, r\rangle$. Next we show $g\langle p, q, r\rangle \subset I$. Let

$$\tilde{\mathbf{M}} = \begin{pmatrix} 0 & [c,d] & [d,b] & [b,c] \\ [d,c] & 0 & [a,d] & [c,a] \\ [b,d] & [d,a] & 0 & [a,b] \\ [c,b] & [a,c] & [b,a] & 0 \end{pmatrix}.$$

By Proposition 2, to prove $gp, gq \in I$, we only have to prove that, for each row $\mathbf{v}$ of the matrix $\tilde{\mathbf{M}}$, $\mathbf{v}\cdot\mathbf{X} \in I$. Since $[c, d]y + [d, b]z + [b, c] = (d_1z - c_1)(dy - b) - (d_1y - b_1) \times (dz - c) \in I$, for the first row $\mathbf{v}$ of matrix $\tilde{\mathbf{M}}$, $\mathbf{v}\cdot\mathbf{X} \in I$. Similarly, one can show that, for the other three rows of $\tilde{\mathbf{M}}$, $\mathbf{v}\cdot\mathbf{X} \in I$ also holds. Thus $gp, gq \in I$.

Next we want to prove $gr \in I$. By Lemma 2, there exist polynomials $h_i[s, t] \in \mathbb{R}[s, t]$, $i = 1, \ldots, 6$, such that

$$\begin{aligned} gr &= h_1(bx - ay) + h_2(cx - az) + h_3(dx - a) + h_4(cy - bz) + h_5(dy - b) \\ &\quad + h_6(dz - c) \\ &= (h_1y + h_2z + h_3)(dx - a) + (-h_1x + h_4z + h_5)(dy - b) \\ &\quad + (-h_2x - h_4y + h_6)(dz - c) \in I. \end{aligned}$$

The second part of the theorem is proved.

By Proposition 1, when $\mathbf{P}(s, t)$ does not have s-finite base points, $g(s) = 1$ and hence $I = \langle p, q, r\rangle$. □

Remark 2. When the rational ruled surface $\mathbf{P}(s, t)$ has base points, in general $I \neq g\langle p, q, r\rangle$ and $I \neq \langle p, q, r\rangle$. However, if $GCD(a_1, b_1, c_1, d_1) = 1$, then one can show that

$$g\langle p, q\rangle = I \cap \mathbb{R}[x, y, z, s]. \tag{21}$$

From Theorem 6 and the above Remark 2, we see that the μ-basis p, q, r generally does not serve as a basis of the ideal I and that the implicit equation of $\mathbf{P}(s, t)$ does not belong to the ideal I. However, in the following we will show that p, q, r serve as a basis for the ideal

$$I' := \langle dx - a, dy - b, dz - c, dw - 1\rangle \cap \mathbb{R}[x, y, z, s, t] \tag{22}$$

which is the "proper" ideal corresponding to the rational ruled surface $\mathbf{P}(s, t)$.

Lemma 5. *Let I' be the ideal defined in* (22)*, and $g(s)$ be the polynomial defined in Proposition* 1*. Then I' is a prime ideal, and $g(s) \notin I'$.*

Proof. It is enough to prove that the ideal

$$I'' := \langle dx - a, dy - b, dz - c, dw - 1\rangle \subset \mathbb{R}[x, y, z, w, s, t]$$

is prime.

Consider the ring homomorphism: $\phi : \mathbb{R}[x, y, z, w, s, t] \to \mathbb{R}[w, s, t]$ that sends x, y, z, w, s, t to aw, bw, cw, w, s, t respectively. Since $d \in \mathbb{R}[s, t]$, one easily sees that $dw-1$ is irreducible in $\mathbb{R}[w, s, t]$. Thus $\langle dw-1\rangle$ is a prime ideal, which means that $\phi^{-1}(\langle dw-1\rangle)$ is also prime. Now we show that $I'' = \phi^{-1}(\langle dw - 1\rangle)$, which implies I'' is prime.

It is easy to see that $f \in \phi^{-1}(\langle dw - 1\rangle)$ if and only if $f(aw, bw, cw, w, s, t) = h(w, s, t) \times (dw - 1)$ for some polynomial h. Since $dx - a|_{x=aw} = a(dw - 1)$, $dx - a \in \phi^{-1}(\langle dw - 1\rangle)$. Similarly, $dy - b, dz - c, dw - 1$ all belong to $\phi^{-1}(\langle dw - 1\rangle)$. Hence $I'' \subset \phi^{-1}(\langle dw - 1\rangle)$. Conversely, suppose $f \in \phi^{-1}(\langle dw - 1\rangle)$. By the binomial theorem, one has

$$\begin{aligned} f(x, y, z, w, s, t) &= f(x - aw + aw, y - bw + bw, z - cw + cw, w, s, t) \\ &= \text{element of } \langle x - aw, y - bw, z - cw\rangle \\ &\quad + f(aw, bw, cw, w, s, t). \end{aligned}$$

Notice that $x - aw = w(dx - a) - x(dw - 1)$, so $x - aw \in I''$. Similarly, $y - bw, z - cw \in I''$. Hence $f \in I''$. Therefore, $I'' = \phi^{-1}(\langle dw - 1\rangle)$ is prime. Furthermore, it is easy to see that $g \notin \phi^{-1}(\langle dw - 1\rangle) \cap \mathbb{R}[x, y, z, s, t] = I'$. This completes the proof. □

The ideal I' is closely related with the moving surfaces of $\mathbf{P}(s, t)$.

Theorem 7. *Let $F(x, y, z, s, t)$ be a moving surface as defined in* (6)*. Then $F(x, y, z, s, t)$ follows $\mathbf{P}(s, t)$ if and only if $F \in I'$.*

Proof. For sufficiency, suppose $F(x, y, z, s, t) \in I'$, then there exist polynomials $A, B, C, D \in \mathbb{R}[x, y, z, w, s, t]$ such that

$$F = A(dx - a) + B(dy - b) + C(dz - c) + D(dw - 1).$$

Setting $x = a/d, y = b/d, z = c/d$ and $w = 1/d$ in the above equation immediately gives

$$F(a/d, b/d, c/d, s, t) \equiv 0.$$

Hence $F(x, y, z, s, t)$ is a moving surface following $\mathbf{P}(s, t)$.

For necessity, let $F(x, y, z, s, t)$ be a moving surface following $\mathbf{P}(s, t)$. Divide F by $dx - a, dy - b, dz - c$ and $dw - 1$ (using x, y, z and w as the main variables) respectively, then there exist polynomials $h_i \in \mathbb{R}[x, y, z, w, s, t]$, $i = 1, 2, 3, 4$ and $h_5 \in \mathbb{R}[s, t]$ such that

$$d^k F = h_1(dx - a) + h_2(dy - b) + h_3(dz - c) + h_4(dw - 1) + h_5,$$

where k is a nonnegative integer. Substituting $x = a/d, y = b/d, z = c/d$ and $w = 1/d$ into the above equation, one gets $h_5 \equiv 0$. Thus $d^k F \in I'$. By Lemma 5, I' is prime and $d \notin I'$, so $F \in I'$. The theorem is thus proved. □

Lemma 6. *Let* $p_0 = p(x, y, z, s_0)$, $q_0 = q(x, y, z, s_0)$ *and* $r_0 = r(x, y, z, s_0, t)$. *Then* $syz(p_0, q_0, r_0) \subset \mathbb{R}[x, y, z, t]^3$ *is generated by* $\mathbf{v}_1 = (q_0, -p_0, 0)$, $\mathbf{v}_2 = (-r_0, 0, p_0)$ *and* $\mathbf{v}_3 = (0, r_0, -q_0)$.

Proof. Let

$$\mathbf{B} = \begin{pmatrix} p_1(s_0) & p_2(s_0) & p_3(s_0) & p_4(s_0) \\ q_1(s_0) & q_2(s_0) & q_3(s_0) & q_4(s_0) \end{pmatrix}.$$

By Proposition 3, the rank of the matrix **B** is 2. We prove the lemma for the following two cases.

Case 1. The first three columns of the matrix **B** have rank 1. In this case, there exist constants α, β (at least one of them is nonzero) such that

$$\alpha(p_1(s_0), p_2(s_0), p_3(s_0)) + \beta(q_1(s_0), q_2(s_0), q_3(s_0)) = \mathbf{0}.$$

Then $\alpha p_0 + \beta q_0 = \alpha p_4(s_0) + \beta q_4(s_0)$ is a nonzero constant since rank(**B**) $= 2$. Thus $\langle p_0, q_0 \rangle = \mathbb{R}[x, y, z, t]$, which in turn implies that $\langle p_0, q_0, r_0 \rangle = \mathbb{R}[x, y, z, t]$. Now the argument of Lemma 1 of Cox et al. (1998b) (see also Exercise 15 on page 285 of Cox et al., 1998a) implies that $syz(p_0, q_0, r_0)$ is generated by $\mathbf{v}_1$, $\mathbf{v}_2$ and $\mathbf{v}_3$.

Case 2. The first three columns of the matrix **B** have rank 2. We will show in this case that p_0, q_0, r_0 form a regular sequence, that is, p_0, q_0, r_0 have the following properties:

- p_0 is not a zero divisor in $\mathbb{R}[x, y, z, t]$.
- q_0 is not a zero divisor in $\mathbb{R}[x, y, z, t]/\langle p_0 \rangle$.
- r_0 is not a zero divisor in $\mathbb{R}[x, y, z, t]/\langle p_0, q_0 \rangle$.

Then a standard result in commutative algebra guarantees that the syzygies on p_0, q_0, r_0 have the desired form.

Since the first three columns of the matrix **B** have rank 2, we can make an affine change of coordinates so that $p_0 = x$ and $q_0 = y$. Then

$$r_0 = (u_1(s_0) + v_1(s_0)t)x + (u_2(s_0) + v_2(s_0)t)y + (u_3(s_0) + v_3(s_0)t)z + u_4(s_0) + v_4(s_0)t.$$

It is obvious that $p_0 = x$ is not a zero divisor in $\mathbb{R}[x, y, z, t]$ and that $q_0 = y$ is not a zero divisor in $\mathbb{R}[x, y, z, t]/\langle p_0 \rangle = \mathbb{R}[y, z, t]$. Furthermore, since $\mathbb{R}[x, y, z, t]/\langle p_0, q_0 \rangle = \mathbb{R}[z, t]$, it follows that r_0 gives a nonzero divisor in $\mathbb{R}[x, y, z, t]/\langle p_0, q_0 \rangle$ if and only if

$$(u_3(s_0) + v_3(s_0)t)z + u_4(s_0) + v_4(s_0)t \neq 0 \qquad \text{in } \mathbb{R}[z, t] \qquad (*).$$

If $\mathbf{p}(s_0) = (1, 0, 0, 0)$, $\mathbf{q}(s_0) = (0, 1, 0, 0)$ and $\mathbf{u}(s_0)$ are linearly independent, then $u_3(s_0) \neq 0$ or $u_4(s_0) \neq 0$; otherwise, $\mathbf{p}(s_0)$, $\mathbf{q}(s_0)$, $\mathbf{v}(s_0)$ must be linearly independent by Theorem 3, so $v_3(s_0) \neq 0$ or $v_4(s_0) \neq 0$. In either case, equation $(*)$ holds. Thus r_0 is not a zero divisor in $\mathbb{R}[x, y, z, t]/\langle p_0, q_0 \rangle$. Therefore p_0, q_0, r_0 form a regular sequence. This completes the proof of the lemma. □

Lemma 7. *Suppose* $hf \in \langle p, q, r \rangle \subset \mathbb{R}[x, y, z, s, t]$, *where* $h \in \mathbb{R}[s]$. *Then* $f \in \langle p, q, r \rangle$.

Proof. We will first show that if $(s - s_0) f \in \langle p, q, r\rangle$, then $f \in \langle p, q, r\rangle$. Without loss of generality, we assume $s_0 = 0$. Since $sf \in \langle p, q, r\rangle$, there exist polynomials $h_i \in \mathbb{R}[x, y, z, s, t]$, $i = 1, 2, 3$ such that

$$sf = h_1 p + h_2 q + h_3 r.$$

Write $h_i = \sum_{j=0}^{n_i} h_{ij} s^j$, $i = 1, 2, 3$, where $h_{ij} \in \mathbb{R}[x, y, z, t]$. Since $s | h_1 p + h_2 q + h_3 r$, one gets

$$h_{10} p_0 + h_{20} q_0 + h_{30} r_0 \equiv 0$$

where $p_0 = p(x, y, z, 0)$, $q_0 = q(x, y, z, 0)$ and $r_0 = r(x, y, z, 0, t)$. By Lemma 6, there exist polynomials $H_i \in \mathbb{R}[x, y, z, t]$, $i = 1, 2, 3$ such that

$$h_{10} = H_1 q_0 - H_2 r_0, \qquad h_{20} = H_3 r_0 - H_1 p_0, \qquad h_{30} = H_2 p_0 - H_3 q_0$$

so

$$h_{10} p + h_{20} q + h_{30} r = H_1(q_0 p - p_0 q) + H_2(p_0 r - r_0 p) + H_3(r_0 q - q_0 r).$$

Since

$$\begin{aligned} q_0 p - p_0 q &= \left(q - \sum_{i=1}^{m-\mu} q_i s^i\right) p - \left(p - \sum_{i=1}^{\mu} p_i s^i\right) q \\ &= s\left(q \sum_{i=1}^{\mu} p_i s^{i-1} - p \sum_{i=1}^{m-\mu} q_i s^{i-1}\right) \end{aligned}$$

$q_0 p - p_0 s \in s\langle p, q, r\rangle$. Similarly, $p_0 r - r_0 p, r_0 q - q_0 r \in s\langle p, q, r\rangle$. Hence $h_{10} p + h_{20} q + h_{30} r \in s\langle p, q, r\rangle$. But

$$sf = s\left(p \sum_{j=1}^{n_1} h_{1j} s^{j-1} + q \sum_{j=1}^{n_2} h_{2j} s^{j-1} + r \sum_{j=1}^{n_1} h_{3j} s^{j-1}\right) + h_{10} p + h_{20} q + h_{30} r.$$

Thus $sf \in s\langle p, q, r\rangle$, i.e., $f \in \langle p, q, r\rangle$.

Now let s_0 be a zero of $h(s)$, and $h' = h/(s - s_0)$. By the above result, $h' f \in \langle p, q, r\rangle$. The general result holds by mathematical induction on the degree of h. □

Lemma 8. *Let $f \in I' \subset \mathbb{R}[x, y, z, s, t]$. Then*

$$g^N f \in \langle p, q, r\rangle$$

for some positive integer N. Here g is the polynomial defined in Proposition 1.

Proof. From $f \in I'$, we know that

$$f = A(dx - a) + B(dy - b) + C(dz - c) + D(dw - 1)$$

for some polynomials $A, B, C, D \in \mathbb{R}[x, y, z, w, s, t]$. Since w does not appear in f, setting $w = 1/d$ gives

$$\begin{aligned} f = {} & A(x, y, z, 1/d, s, t)(dx - a) + B(x, y, z, 1/d, s, t)(dy - b) \\ & + C(x, y, z, 1/d, s, t)(dz - c). \end{aligned}$$

Multiplying both sides of the above equation by d^M for M sufficiently large shows that $d^M f \in I$, where I is the ideal defined in (19). Next from

$$a^M f = (dx - (dx - a))^M f$$

and the binomial theorem, we obtain $a^M f \in I$, and $b^M f, c^M f \in I$ follow similarly. Now setting $N = 4M$, one can easily show that

$$\langle a, b, c, d\rangle^N f \subset I.$$

Then $g^N f \in I \subset \langle p, q, r\rangle$ follows immediately since $g \in \langle a, b, c, d\rangle$ by Lemma 1. □

Theorem 8. *Let I' be the ideal defined in* (22)*. Then*

$$I' = \langle p, q, r\rangle. \tag{23}$$

Proof. From Theorem 6, we have $g\langle p, q, r\rangle \subset I \subset I'$. Since by Lemma 5 I' is prime and $g \notin I'$, $\langle p, q, r\rangle \subset I'$.

Conversely, suppose $f \in I'$, then by Lemma 8, $g^N f \in \langle p, q, r\rangle$ for some positive integer N, and so $f \in \langle p, q, r\rangle$ by Lemma 7. Hence $I' \subset \langle p, q, r\rangle$. The theorem is thus confirmed. □

Remark 3. Theorem 5 is a corollary of Theorems 7 and 8.

Remark 4. In Cox (2001), Cox introduces the notion of a *strong μ-basis* for a general rational surface. The strong μ-basis is defined as a basis of the syzygy module of the rational surface. At this point, the μ-basis defined in this paper for a rational ruled surface resembles the strong μ-basis. However, the strong μ-basis is defined for triangular surfaces in projective space, and, in general, the strong μ-basis does not exist. In contrast, the μ-basis defined in this paper for a rational ruled surface always exists.

5. Conclusion

By introducing a polynomial $r(x, y, z, s, t)$ that is linear in x, y, z and t, we have redefined the μ-basis of a rational ruled surface to be three polynomials p, q and r such that the implicit equation of the surface is given by the resultant of p and q with respect to s and the parametric equation of the surface can be recovered from p, q and r. We also presented an efficient algorithm for computing p, q and r, and discussed some properties of the newly defined μ-basis. In particular, we show that the new μ-basis serves a basis for both the moving plane module and the moving plane ideal corresponding to the rational ruled surface. These results are helpful for understanding the construction of the μ-basis for a general rational surface—a problem worthy of further study.

Acknowledgements

The authors are grateful for the referees' careful reading and invaluable remarks which have greatly improved the presentation of the paper. One of the referees suggested the current proofs of Lemmas 5, 6 and 8, which simplify the proofs in the earlier manuscript. Falai Chen is supported by the Outstanding Youth Grant of NSF of China (No. 60225002),

NKBRSF on Mathematical Mechanics (No. G1998030600), the TRAPOYT and the Doctoral Program (No. 20010358003) of MOE of China. Wenping Wang is supported partially by the grants HKU 7032/99E and HKU 7031/01E from Research Grant Council of Hong Kong.

References

Chen, F., Zheng, J., Sederberg, T.W., 2001. The μ-basis of a rational ruled surface. Comput. Aided Geom. Design 18, 61–72.

Cox, D., 2001. Equations of parametric curves and surfaces via syzygies. In: Symbolic Computation: Solving Equations in Algebra, Geometry and Engineering, Contemporary Mathematics, vol. 286. AMS, Providence, RI, pp. 1–20.

Cox, D., Little, J., O'Shea, D., 1998a. Using Algebraic Geometry. Springer-Verlag, New York.

Cox, D., Sederberg, T.W., Chen, F., 1998b. The moving line ideal basis of planar rational curves. Comput. Aided Geom. Design 15, 803–827.

Sederberg, T.W., Chen, F., 1995. Implicitization using moving curves and surfaces. In: SIGGRAPH'95, Annual Conference Series. pp. 301–308.

Sederberg, T.W., Saito, T., 1995. Rational ruled surfaces: implicitization and section curves. CVGIP: Graphical Models and Image Processing 57, 334–342.

Sederberg, T.W., Saito, T., Qi, D., Klimaszewski, K.S., 1994. Curve implicitization using moving lines. Comput. Aided Geom. Design 11, 687–706.