ELSEVIER

Computer Aided Geometric Design 18 (2001) 61–72

COMPUTER AIDED GEOMETRIC DESIGN

www.elsevier.com/locate/comaid

The mu-basis of a rational ruled surface

Falai Chen [a,*], Jianmin Zheng [b], Thomas W. Sederberg [c]

[a] *Department of Mathematics, University of Science and Technology of China, Hefei, Anhui 230026, China*
[b] *Department of Mathematics, Zhejiang University, Hangzhou 310027, China*
[c] *Department of Computer Science, Brigham Young University, Provo, UT 84602, USA*

Received 5 May 2000; revised 11 November 2000

Abstract

The mu-basis of a planar rational curve is a polynomial ideal basis comprised of two polynomials that greatly facilitates computing the implicit equation of the curve. This paper defines a mu-basis for a rational ruled surface, and presents a simple algorithm for computing the mu-basis. The mu-basis consists of two polynomials $p(x, y, z, s)$ and $q(x, y, z, s)$ that are linear in x, y, z and degree μ and $m - \mu$ in s respectively, where m is the degree of the implicit equation. The implicit equation of the surface is then obtained by merely taking the resultant of p and q with respect to s. This implicitization algorithm is faster and/or more robust than previous methods. © 2001 Elsevier Science B.V. All rights reserved.

Keywords: Ruled surface; Implicitization; Moving plane; Mu-basis; Module; Syzygy

1. Introduction

A rational ruled surface is a bi-degree $(n, 1)$ tensor product rational surface which is defined in homogeneous form:

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

where

$$\boldsymbol{P}_i(s) := \bigl(a_i(s), b_i(s), c_i(s), d_i(s)\bigr), \quad i = 0, 1, \tag{2}$$

* Corresponding author.
E-mail addresses: chenfl@ustc.edu.cn (F. Chen), zjm@math.zju.edu.cn (J. Zheng), tom@byu.edu (T.W. Sederberg).

PII: S0167-8396(01)00012-7

and the maximum degree of $a_i(s)$, $b_i(s)$, $c_i(s)$ and $d_i(s)$ is n. To avoid the degenerate case where $\boldsymbol{P}(s,t)$ parameterizes a curve, $\boldsymbol{P}_0(s)$ and $\boldsymbol{P}_1(s)$ are always assumed to be linearly independent. In Cartesian coordinates, the rational ruled surface $\boldsymbol{P}(s,t)$ can be expressed

$$\widetilde{\boldsymbol{P}}(s,t)=\frac{(a_0(s),b_0(s),c_0(s))+t(a_1(s),b_1(s),c_1(s))}{d_0(s)+td_1(s)}. \tag{3}$$

Ruled surfaces have a long theoretical history (Edge, 1931) along with many applications in the design and manufacturing industries (Aumann, 1991; Lang and Roschel, 1992; Ravani and Chen, 1986). In this paper, we are interested in the problem of finding the *implicit equation* of a ruled surface. It has been known that there exists a homogeneous irreducible polynomial $f(x,y,z,w)$ such that $f(\boldsymbol{P}(s,t))\equiv 0$. This polynomial equation represents an algebraic surface of the ruled surface. By Bezout's theorem (van der Waerden, 1950), the degree of polynomial f—say, h—is equal to the number of intersections of the algebraic surface with a *generic* line. We now consider the intersection of the rational ruled surface with a generic line and denote the number of the intersection points by m. If the ruled surface is properly parameterized, then $m=h$. Otherwise, there is an integer $k>1$, called the number of correspondence, such that in general each point on the surface corresponds to k parameter values. Thus $m=kh$ (Chionh and Goldman, 1992). From the point of view of the parameterization, m reflects the multiplicity of the correspondence. So in the rest of the paper when we say the implicit degree of the rational ruled surface, it means m, rather than h.

The authors previously developed a technique called *moving planes* and *moving surfaces* to compute implicit representations of rational surfaces (Sederberg and Chen, 1995). This approach is much more efficient than traditional implicitizing techniques such as resultants and Groebner bases. Furthermore, base points cause resultant based methods to fail, whereas the method of moving surfaces actually simplifies if base points are present. However, the method of moving surfaces has two drawbacks. First, it involves solving a very large system of linear equations, and when there are more solutions than required, it is difficult to determine which of the solutions to select. Second, there is no rigorous proof that the method always succeeds in computing an implicit equation of any surface, such as in the case of complicated base points—though the method has never failed in practice.

A line of research that we hope will permit us to rigorously prove the method of moving surfaces and to make it much faster is the *mu-basis* method. The mu-basis method was devised for implicitizing planar curves (Cox et al., 1998). Zheng and Sederberg (2000) give an efficient algorithm to compute the mu-basis of a planar rational curve. In this paper, we extend the mu-basis method to ruled surfaces, thereby making the implicitization of ruled surfaces much faster than the fastest previous methods (Sederberg and Saito, 1995) and completely rigorous. Work is ongoing to extend the mu-basis method to surfaces in general.

We organize the paper as follows. In Section 2, we present an algorithmic approach for deriving the mu-basis of a ruled surface. Section 2.1 provides some terminology and defines a monomial order over a module. Section 2.2 presents some lemmas as background to Section 2.3, which describes the details of the algorithm and proves its correctness. In Section 3, the implicit equation of a rational ruled surface is formulated by taking the resultant of the two elements of the mu-basis, and an example is provided. Finally, we make some observations and point out further research problems.

2. Mu-basis of a rational ruled surface

A *moving plane* $\boldsymbol{L}(s,t) := (A(s,t), B(s,t), C(s,t), D(s,t))$ is a family of planes $A(s,t)x + B(s,t)y + C(s,t)z + D(s,t)w = 0$ with one plane corresponding to parameter pair (s,t). A moving plane $\boldsymbol{L}(s,t)$ is said to *follow* rational ruled surface $\boldsymbol{P}(s,t)$ if

$$\begin{aligned}\boldsymbol{L}(s,t)\cdot\boldsymbol{P}(s,t) &= A(s,t)a(s,t) + B(s,t)b(s,t) + C(s,t)c(s,t)\\ &\quad + D(s,t)d(s,t) \equiv 0.\end{aligned} \tag{4}$$

In this paper, we are interested in moving planes which only involve parameter value s—$\boldsymbol{L}(s) := (A(s), B(s), C(s), D(s))$ for which $\boldsymbol{L}(s)\cdot\boldsymbol{P}(s,t) \equiv 0$. The set of all such moving planes forms a module over polynomial ring $R[s]$ (the set of all polynomials in s with real coefficients) where the "R" denotes the field of real numbers (Cox et al., 1992, 1998), and we denote the module by $\boldsymbol{L}[s]$. A basis of the module $\boldsymbol{L}[s]$ is called a *mu-basis* of rational ruled surface (1). In the following, we will present a constructive proof that the mu-basis of ruled surface (1) has two elements, and the sum of the degrees of the two elements is the implicit degree of the rational ruled surface. These properties of the mu-basis lead to a closed form representation of the implicit equation of the rational ruled surface.

Before proceeding, we introduce some terminology.

2.1. Monomial orders over a module

Let $R[s]^r$ be the set of r-dimensional row vectors with entries in the polynomial ring $R[s]$. $R[s]^r$ is a module over $R[s]$ (Cox et al., 1998). A module can be thought of as a vector space whose elements belong to some ring (in a vector space, the elements belong to a field). Denote the standard basis vectors in $R[s]^r$ by $E_i = (0,\ldots,1,\ldots,0)$, $i = 1,2,\ldots,r$, where 1 is in the ith position in the vector. Any element $f = (f_1(s),\ldots,f_r(s)) \in R[s]^r$ can be written

$$f = \sum_{i=1}^{r}\sum_{j=0}^{\deg(f_i)} f_{ij}s^jE_i,$$

where $f_{i,j} \in R$ and $f_{i,\deg(f_i)} \neq 0$. Element s^jE_i is called a *monomial* in $R[s]^r$. Now we define an ordering relation $>_M$ on the monomials of $R[s]^r$: we say $s^iE_j >_M s^kE_l$ if $i > k$, or if $i = k$ and $j < l$. This order sorts the monomials first by degree, and then breaks ties using position within the vector in $R[s]^r$. As is well known, the monomial ordering relation $>_M$ has the following properties:

(1) $>_M$ is a total ordering relation, which means the terms appearing within $f \in R[s]^r$ can be uniquely listed in increasing or decreasing order under $>_M$.
(2) If $s^iE_j >_M s^kE_l$, then $s^{i+\alpha} >_M s^{k+\alpha}E_l$ for any nonnegative integer α.
(3) $>_M$ is a well ordering, that is, every nonempty collection of monomials has a smallest element under $>_M$.

We can express any $f \in R[s]^r$ uniquely in the form:

$$f = \sum_{i=1}^{l} f_ie_i$$

with $f_i \neq 0$ in R and monomials e_i ordered $e_1 >_M e_2 >_M \cdots >_M e_l$. $f_1 e_1$, f_1 and e_1 are called the *leading term*, *leading coefficient* and *leading monomial* (denoted by $LT(f)$, $LC(f)$ and $LM(f)$) respectively. If $e_1 = s^k E_l$, we say f has degree k and the leading term contains basis vector E_l. For example, let $f = (3s^2 + s + 4, -2s^2 - 4s - 5, 3s + 2)$, then $LT(f) = 3s^2 E_1$, $LC(f) = 3$, $LM(f) = s^2 E_1$.

2.2. Lemmas

In this section, we set up the strategy for describing the algorithm to compute the mu-basis of a rational ruled surface.

Lemma 1. *Let $g(s) = GCD([a,b],[a,c],[a,d],[b,c],[b,d],[c,d])$, and λ be the maximum degree of $[a,b]$, $[a,c]$,$[a,d]$, $[b,c]$, $[b,d]$ and $[c,d]$. Then the implicit degree of rational ruled surface $\boldsymbol{P}(s,t)$ is $m = \lambda - \deg(g)$. Here we use the notation $[a,b] = a_0(s)b_1(s) - a_1(s)b_0(s)$.*

Proof. The implicit degree of a surface is the number of intersections (counted properly) between a generic line and the surface. Let the line be defined as the intersection of two planes $A_0x + B_0y + C_0z + D_0w = 0$ and $A_1x + B_1y + C_1z + D_1w = 0$. Then the implicit degree of rational ruled surface $\boldsymbol{P}(s,t)$ is the number of intersections of the following two generic curves in the (s,t) plane:

$$\begin{aligned} &(A_0a_0 + B_0b_0 + C_0c_0 + D_0d_0) + t(A_0a_1 + B_0b_1 + C_0c_1 + D_0d_1) = 0, \\ &(A_1a_0 + B_1b_0 + C_1c_0 + D_1d_0) + t(A_1a_1 + B_1b_1 + C_1c_1 + D_1d_1) = 0. \end{aligned} \tag{5}$$

Eliminating t from the above equation, we have

$$\begin{aligned} &\begin{vmatrix} A_0a_0 + B_0b_0 + C_0c_0 + D_0d_0 & A_0a_1 + B_0b_1 + C_0c_1 + D_0d_1 \\ A_1a_0 + B_1b_0 + C_1c_0 + D_1d_0 & A_1a_1 + B_1b_1 + C_1c_1 + D_1d_1 \end{vmatrix} \\ &\quad = [A,B][a,b] + [A,C][a,c] + [A,D][a,d] + [B,C][b,c] \\ &\qquad + [B,D][b,d] + [C,D][c,d] = 0. \end{aligned} \tag{6}$$

Now all the solutions of Eq. (6) can be classified into two categories. The first category consists of the common zeros of $[a,b]$, $[a,c]$, $[a,d]$, $[b,c]$, $[b,d]$ and $[c,d]$, which correspond to the s-coordinates of the base points of $\boldsymbol{P}(s,t)$. The other category corresponds to the actual intersection points of the two curves in (5). Thus the implicit degree of $\boldsymbol{P}(s,t)$ is $m = \lambda - \deg(g)$. $\square$

Lemma 2. *Let*

$$\begin{aligned} g_1(s) &:= GCD\big([c,d],[d,b],[b,c]\big), \qquad g_2(s) := GCD\big([d,c],[a,d],[c,a]\big), \\ g_3(s) &:= GCD\big([b,d],[d,a],[a,b]\big), \qquad g_4(s) := GCD\big([c,b],[a,c],[b,a]\big). \end{aligned} \tag{7}$$

Then the module $\boldsymbol{L}(s)$ is generated by the rows of the following matrix:

$$M := \begin{pmatrix} 0 & [c,d]/g_1 & [d,b]/g_1 & [b,c]/g_1 \\ [d,c]/g_2 & 0 & [a,d]/g_2 & [c,a]/g_2 \\ [b,d]/g_3 & [d,a]/g_3 & 0 & [a,b]/g_3 \\ [c,b]/g_4 & [a,c]/g_4 & [b,a]/g_4 & 0 \end{pmatrix}. \tag{8}$$

Proof. Let $g(s)$ be the GCD of polynomials $[a,b]$, $[a,c]$, $[a,d]$, $[b,c]$, $[b,d]$ and $[c,d]$. In fact, we can prove $\boldsymbol{L}(s)$ is generated by the rows of matrix:

$$\widetilde{M} := \frac{1}{g} \begin{pmatrix} 0 & [c,d] & [d,b] & [b,c] \\ [d,c] & 0 & [a,d] & [c,a] \\ [b,d] & [d,a] & 0 & [a,b] \\ [c,b] & [a,c] & [b,a] & 0 \end{pmatrix}. \tag{9}$$

Let $\boldsymbol{L}(s) := (A(s), B(s), C(s), D(s))$ be a moving plane which follows the ruled surface (1), then

$$\begin{cases} A(s)a_0(s) + B(s)b_0(s) + C(s)c_0(s) + D(s)d_0(s) \equiv 0, \\ A(s)a_1(s) + B(s)b_1(s) + C(s)c_1(s) + D(s)d_1(s) \equiv 0. \end{cases} \tag{10}$$

Since $GCD([a,b],[a,c],[a,d],[b,c],[b,d],[c,d]) = g$, there exist polynomials $k_{ij} \in R[s]$, $1 \leqslant i < j \leqslant 4$ such that

$$k_{12}[a,b] + k_{13}[a,c] + k_{14}[a,d] + k_{23}[b,c] + k_{24}[b,d] + k_{34}[c,d] = g,$$

so

$$\begin{aligned} gA &= A\big(k_{12}[a,b] + k_{13}[a,c] + k_{14}[a,d] + k_{23}[b,c] + k_{24}[b,d] + k_{34}[c,d]\big) \\ &= (k_{12}b_1 + k_{13}c_1 + k_{14}d_1)Aa_0 - (k_{12}b_0 + k_{13}c_0 + k_{14}d_0)Aa_1 \\ &\quad + k_{23}A[b,c] + k_{24}A[b,d] + k_{34}A[c,d]. \end{aligned} \tag{11}$$

By (10), one has

$$Aa_0 = -(Bb_0 + Cc_0 + Dd_0), \qquad Aa_1 = -(Bb_1 + Cc_1 + Dd_1).$$

Substituting the above equation into (11), we get

$$\begin{aligned} gA &= -(k_{12}b_1 + k_{13}c_1 + k_{14}d_1)(Bb_0 + Cc_0 + Dd_0) \\ &\quad + (k_{12}b_0 + k_{13}c_0 + k_{14}d_0)(Bb_1 + Cc_1 + Dd_1) + k_{23}A[b,c] \\ &\quad + k_{24}A[b,d] + k_{34}A[c,d] \\ &= h_2[d,c] + h_3[b,d] + h_4[c,b] \end{aligned} \tag{12}$$

with $h_2 = -k_{34}A + k_{14}C - k_{13}D$, $h_3 = k_{24}A - k_{14}B + k_{12}D$ and $h_4 = -k_{23}A + k_{13}B - k_{12}C$. Similarly, we have

$$gB = h_1[c,d] + h_3[d,a] + h_4[a,c], \tag{13}$$

$$gC = h_1[d,b] + h_2[a,d] + h_4[b,a], \tag{14}$$

$$gD = h_1[b,c] + h_2[c,a] + h_3[a,b], \tag{15}$$

where $h_1 = k_{34}B - k_{24}C + k_{23}D$. Hence

$$(A, B, C, D) = h_1M_1 + h_2M_2 + h_3M_3 + h_4M_4, \tag{16}$$

where M_i is the ith row of matrix $\widetilde{M}$, $i = 1, 2, 3, 4$. The lemma is thus proven. □

It is an easy exercise to check that $\operatorname{rank}(M) = 2$, that is the rows of M are linearly dependent over $R[s]$. This dependency between the rows of M is the key property to make the algorithm to compute the mu-basis work.

Lemma 3. *Let $p_i = (p_{11}, \ldots, p_{1r}) \in R[s]^r$, $i = 1, 2, \ldots, k \leqslant r$, be linearly dependent vectors over $R[s]$. Then there are at least two of them whose leading terms contain the same basis vector.*

Proof. Suppose p_i, $i = 1, 2, \ldots, k$, have different basis vectors. Then for $i \neq j$, the S-vector $S(p_i, p_j)$ of p_i and p_j is 0 by definition (see §2 of Chapter 5 of (Cox et al., 1998)), and thus the Buchberger's Criterion for modules implies that $p_1, \ldots, p_k$ form a Gröbner basis for the module they generate. Furthermore, since $S(p_i, p_j) = 0\,p_i + \cdots + 0\,p_k$, the Syzygy Theorem (see Theorem 3.3 in p. 212 of (Cox et al., 1998)) implies the syzygy module $Syz(p_1, \ldots, p_k)$ is 0. This means $p_1, \ldots, p_k$ are linearly independent, and thus the lemma is proved. □

Above we used some basic facts about Gröbner bases for modules to prove the lemma. There is also an elementary argument along the lines of the proof in (Zheng and Sederberg, 2000).

2.3. Algorithm

Based on the main concepts developed in the last subsection, we would like to devise an algorithm to compute the mu-basis of a rational ruled surface from generating set matrix M. This algorithm is a direct extension of the algorithm to compute the mu-basis of a planar rational curve (Zheng and Sederberg, 2000). First, we outline the algorithm.

Input: (a, b, c, d)—the parametric equation of a rational ruled surface.
Output: Two elements of the mu-basis.
Procedure:
Step 1 Set

$$v_1 = (0, [c, d], [d, b], [b, c])/g_1, \qquad v_2 = ([d, c], 0, [a, d], [c, a])/g_2,$$
$$v_3 = ([b, d], [d, a], 0, [a, b])/g_3, \qquad v_4 = ([c, b], [a, c], [b, a], 0)/g_4,$$

and $S = \{v_1, v_2, v_3, v_4\}$.
Step 2 Choose v_i, v_j from S so that $LT(v_i)$ and $LT(v_j)$ contain the same basis vector. Assume $\deg(v_i) \geqslant \deg(v_j)$.
Step 3 Replace v_i by the S-vector of v_i and v_j:

$$v_i \leftarrow LC(v_j)v_i - LC(v_i)s^{\deg(v_i)-\deg(v_j)}v_j.$$

Step 4 If $v_i = 0$, remove v_i from S.
Step 5 If the leading term of each element in S has different basis vector, then stop; else go to Step 2.

Note that if all the coefficients of v_i are integers, then in forming the S-vector, we could remove common factors to simplify the computation.

Theorem 1. *The algorithm described above terminates in a finite number of steps, and the output contains two elements.*

Proof. Since each replacement of v_i in Step 3 lowers the degree of the leading term of v_i, the algorithm terminates in a finite number of steps.

On the other hand, after each replacement in Step 3, the elements in S still generate the module $\boldsymbol{L}[s]$ and they are linearly dependent over $R[s]$ before the final stage. Since $\operatorname{rank}(M) = 2$, at the final stage, S contains only two elements. $\square$

Obviously, S-vectors play an important role in the above algorithm. S-vectors have been used in the usual Buchberger's algorithm for finding a Gröbner basis. However, instead of adding remainders of S-vectors as the Buchberger's algorithm does, we here replace elements with S-vectors. This is the key to the efficiency of the algorithm.

The output of the above algorithm is two vectors $p(s), q(s) \in R[s]^4$ which are generators of the module $\boldsymbol{L}[s]$, and which are a *mu-basis* of rational ruled surface $\boldsymbol{P}(s,t)$. A mu-basis has the following nice property.

Theorem 2. *Let $p(s), q(s)$ be the two elements of the mu-basis generated by the algorithm described above, and $\deg(p) \leqslant \deg(q)$. Then $p(s)$ has the lowest degree in s of any element in $\boldsymbol{L}[s]$, and the sum of $\deg(p)$ and $\deg(q)$ is equal to the implicit degree of rational ruled surface $\boldsymbol{P}(s,t)$.*

Proof. Suppose there is an element $h \in \boldsymbol{L}[s]$ whose degree in s is smaller than $\deg(p)$. Then there exists polynomials $h_1(s)$ and $h_2(s)$ such that

$$h - h_1 p - h_2 q = 0.$$

By Theorem 1, at least two of h, p and q have the leading terms containing the same basis vector. Since $\deg(h) < \deg(p) \leqslant \deg(q)$, $LT(p)$ and $LT(q)$ must have the same basis vector. This contradicts the construction of p and q. Hence $p(s)$ has the lowest degree.

Next we prove that the sum of $\deg(p)$ and $\deg(q)$ is equal to the implicit degree of $\boldsymbol{P}(s,t)$. Let $\deg(p) = m_0$, $\deg(q) = m_1$ and the implicit degree of $\boldsymbol{P}(s,t)$ be m. We first show $m \geqslant m_0 + m_1$.

Since $p := (p_1, p_2, p_3, p_4)$ and $q := (q_1, q_2, q_3, q_4)$ are the generators of module $\boldsymbol{L}[s]$, there exist polynomials $h_{ij}(s)$, $i = 1, 2, 3, 4$, $j = 1, 2$, such that

$$\begin{aligned}
&\big(0, [c,d], [d,b], [b,c]\big) = g_1(h_{11}p + h_{12}q),\\
&\big([d,c], 0, [a,d], [c,a]\big) = g_2(h_{21}p + h_{22}q),\\
&\big([b,d], [d,a], 0, [a,b]\big) = g_3(h_{31}p + h_{32}q),\\
&\big([c,b], [a,c], [b,a], 0\big) = g_4(h_{41}p + h_{42}q).
\end{aligned}$$

Define

$$p \times q = \big([12], [13], [14], [23], [24], [34]\big),$$

and

$$p * q = \big([34], [42], [23], [14], [31], [12]\big),$$

where $[ij] = p_i q_j - p_j q_i$. From the first two of the above equations, we get

$$[c,d]\boldsymbol{P}_0(s) * \boldsymbol{P}_1(s) = (h_{11}h_{22} - h_{21}h_{12})g_1 g_2\, p \times q.$$

Similarly, we can get five other equations

$$\begin{aligned}
&[d,b]\boldsymbol{P}_0(s) * \boldsymbol{P}_1(s) = (h_{11}h_{32} - h_{31}h_{12})g_1 g_3\, p \times q,\\
&[b,c]\boldsymbol{P}_0(s) * \boldsymbol{P}_1(s) = (h_{11}h_{42} - h_{41}h_{12})g_1 g_4\, p \times q,\\
&[a,d]\boldsymbol{P}_0(s) * \boldsymbol{P}_1(s) = (h_{21}h_{32} - h_{31}h_{22})g_2 g_3\, p \times q,\\
&[c,a]\boldsymbol{P}_0(s) * \boldsymbol{P}_1(s) = (h_{21}h_{42} - h_{41}h_{22})g_2 g_4\, p \times q,\\
&[a,b]\boldsymbol{P}_0(s) * \boldsymbol{P}_1(s) = (h_{31}h_{42} - h_{41}h_{32})g_3 g_4\, p \times q.
\end{aligned}$$

Since $GCD([c,d],[d,b],[b,c],[a,d],[c,a],[a,b]) = GCD(g_1, g_2, g_3, g_4) = g$, there exist polynomials $k_i \in R[s]$, $i = 1, \ldots, 6$, such that

$$k_1[c,d] + k_2[d,b] + k_3[b,c] + k_4[a,d] + k_5[c,a] + k_6[a,b] = g,$$

so

$$g\big([c,d],[d,b],[b,c],[a,d],[c,a],[a,b]\big) = hg^2\, p \times q,$$

where $h \in R[s]$ is a nonzero polynomial. Since the leading terms of p and q do not have the same basis vector, $\deg(p \times q) = \deg(p) + \deg(q)$. Therefore $m \geqslant m_0 + m_1$ by considering the degrees of the polynomials in both sides of the above equation.

Next we need to show $m \leqslant m_0 + m_1$. To this end, we note the four rows M_i, $i = 1,2,3,4$, of the matrix M generate p and q, so there exist polynomials $\tilde{h}_{ij} \in R[s]$, $i = 1,2$, $j = 1,2,3,4$, such that

$$\begin{aligned}
p &= \tilde{h}_{11}M_1 + \tilde{h}_{12}M_2 + \tilde{h}_{13}M_3 + \tilde{h}_{14}M_4,\\
q &= \tilde{h}_{21}M_1 + \tilde{h}_{22}M_2 + \tilde{h}_{23}M_3 + \tilde{h}_{24}M_4.
\end{aligned}$$

It is easy to show

$$p \times q = \tilde{h}\big([c,d],[d,b],[b,c],[a,d],[c,a],[a,b]\big)/g$$

for some polynomials $\tilde{h} \in R[s]$. Thus $m_0 + m_1 \geqslant m$. The theorem is proven. □

Remark. It can be shown that the computational cost of the above algorithm is $O(n^2)$, where n is the maximum degree of polynomials a_i, b_i, c_i, d_i, $i = 1,2$, while the computational complexity by the moving planes method is $O(n^3)$. Thus the above algorithm is not only more robust but also more efficient than previous algorithms.

3. Implicitization of rational ruled surfaces

The mu-basis of a rational ruled surface leads to a closed form representation of the implicit equation of the rational ruled surface.

Theorem 3. *Let p, q be the mu-basis of the rational ruled surface* (1). *Then the implicit equation of $\boldsymbol{P}(s,t)$ is given by* $\operatorname{Res}(p \cdot X, q \cdot X, s) = 0$, *where* $X = (x, y, z, w)$.

Proof. We prove the assertion in the following four steps.

(1) For any point X_0 on the ruled surface $\boldsymbol{P}(s,t)$, the resultant $\operatorname{Res}(p \cdot X_0, q \cdot X_0, s) = 0$.
In fact, since p and q are moving planes which follow $\boldsymbol{P}(s,t)$, there exists parameter σ such that

$$p(\sigma) \cdot X_0 = q(\sigma) \cdot X_0 = 0,$$

so $p \cdot X_0$ and $q \cdot X_0$ have a common zero σ. Hence $\operatorname{Res}(p \cdot X_0, q \cdot X_0, s) = 0$.

(2) $p \cdot X$ is irreducible in $R[x, y, z, w, s]$.
Suppose $p \cdot X$ is reducible, then there exist polynomials $F, G \in R[x, y, z, w, s]$ such that $p \cdot X = FG$, where F is linear in x, y, z, w and G is a polynomial in s. Since $p \cdot X$ follows $\boldsymbol{P}(s,t)$, F is also a moving plane which follows $\boldsymbol{P}(s,t)$. But this contradicts the fact that p has the lowest degree.

(3) $\operatorname{Res}(p \cdot X, q \cdot X, s)$ is not identically zero.
If $\operatorname{Res}(p \cdot X, q \cdot X, s) \equiv 0$, then $p \cdot X$ and $q \cdot X$ must have a common factor. Since $p \cdot X$ is irreducible in $R[x, y, z, w, s]$, $p \cdot X$ is a factor of $q \cdot X$, which contradicts the construction of the mu-basis.

(4) If $\operatorname{Res}(p \cdot X_0, q \cdot X_0, s) = 0$, then X_0 is on the ruled surface $\boldsymbol{P}(s,t)$.
We represent $\operatorname{Res}(p \cdot X, q \cdot X, s)$ as the Sylvester resultant. For any point X_0 satisfying $\operatorname{Res}(p \cdot X_0, q \cdot X_0, s) = 0$, from standard properties of resultants, either $p(s) \cdot X_0 = 0$ and $q(s) \cdot X_0 = 0$ have a common solution $s = \sigma$, or the leading coefficients of $p(s) \cdot X_0$ and $q(s) \cdot X_0$ vanish, which corresponds to the common solution $\sigma = \infty$. From (10), we know that line $\boldsymbol{P}(\sigma, t)$ lies on the planes $p(\sigma) \cdot X = 0$ and $q(\sigma) \cdot X = 0$. Therefore, if X_0 is not on the line $\boldsymbol{P}(\sigma, t)$, $p(\sigma) \cdot X = 0$ defines a plane determined by point X_0 and line $\boldsymbol{P}(\sigma, t)$, so does $q(\sigma) \cdot X = 0$. This contradicts the construction of p and q.

In summary, we have shown that any point on the ruled surface makes the resultant to be zero, and the resultant vanishes only on the ruled surface. Thus the proof is completed. □

We should mention that if the rational ruled surface is improperly parameterized, $\operatorname{Res}(p \cdot X, q \cdot X, s)$ is actually a power of the irreducible polynomial which gives the implicit equation of the surface. But in terms of the parameterization, one can argue that $\operatorname{Res}(p \cdot X, q \cdot X, s) = 0$ is also the correct implicit equation because it reflects the fact that the rational ruled surface $\boldsymbol{P}(s,t)$ is multiply traced.

Based on the above theorem, we can construct two different determinant representations of the implicit equation of rational ruled surface $\boldsymbol{P}(s,t)$.

Let

$$p=\sum_{i=0}^{m_0} p_i(x,y,z,w)s^i, \qquad q=\sum_{i=0}^{m_1} q_i(x,y,z,w)s^i$$

be the mu-basis of $\boldsymbol{P}(s,t)$, where p_i and q_i are linear functions in x,y,z,w. Let the implicit degree of the rational ruled surface $\boldsymbol{P}(s,t)$ be m. Multiply p by $1,s,\ldots,s^{m-m_0-1}$ respectively, and multiply q by $1,s,\ldots,s^{m-m_1-1}$ respectively, we arrive at m moving planes whose degree in s is $m-1$. These m moving planes result in the Sylvester style resultant of p and q:

$$\operatorname{Res}(p\cdot X,q\cdot X,s)=\det\begin{pmatrix} p_0 & p_1 & \cdots & p_{m_0} & & \\ & \ddots & & & \ddots & \\ & & p_0 & & \cdots & p_{m_0} \\ q_0 & q_1 & \cdots & q_{m_0} & & \\ & \ddots & & & \ddots & \\ & & & q_0 & \cdots & q_{m_0} \end{pmatrix}. \tag{17}$$

We can also write the resultant $\operatorname{Res}(p\cdot X,q\cdot X,s)$ as a variant of the Bezout's resultant (Cox et al., 1998).

$$\operatorname{Res}(p\cdot X,q\cdot X,s)=\det\begin{pmatrix} R_{m_1-1,0} & \cdots & R_{m_1-1,m_1-1} \\ \vdots & \cdots & \vdots \\ R_{0,0} & \cdots & R_{0,m_1-1} \end{pmatrix}, \tag{18}$$

where

$$R_{ij}=\begin{cases} \displaystyle\sum_{\substack{k_1\leqslant\min(i,j)\\ k_1+k_2=i+j+1}} [k_1k_2], & 0\leqslant i\leqslant m_0-1,\ 0\leqslant j\leqslant m_1-1,\\ p_{i+j+1-m_1}, & m_0\leqslant i\leqslant m_1-1,\ 0\leqslant j\leqslant m_1-1, \end{cases}$$

and $[ij]=p_iq_j-p_jq_i$.

Note that, in the Bezout resultant, there are m_1-m_0 linear rows and m_0 quadratic rows. Thus the Bezout representations of implicit equations are more compact than the Sylvester forms.

We conclude with an example. Let

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

and

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

It is easy to compute the matrix $M=(C_1,C_2,C_3,C_4)$ with the columns

$$C_1=\begin{pmatrix} 0\\ -2s^3-2s^2-7s-7\\ -4s^3-3s^2-3s+5\\ -4s^3-8s^2+8s+3 \end{pmatrix}, \qquad C_2=\begin{pmatrix} 2s^3+2s^2+7s+7\\ 0\\ -s^4-7s^3-s^2-5s-1\\ -2s^4-10s^3-4s^2+4s-9 \end{pmatrix},$$

$$C_3 = \begin{pmatrix} 4s^3+3s^2+3s-5 \\ s^4+7s^3+s^2+5s+1 \\ 0 \\ -2s^4-3s^3+10s^2-16s+6 \end{pmatrix},$$

$$C_4 = \begin{pmatrix} 4s^3+8s^2-8s-3 \\ 2s^4+10s^3+4s^2-4s+9 \\ 2s^4+3s^3-10s^2+16s-6 \\ 0 \end{pmatrix}.$$

The algorithm described in Section 2.3 computes the following mu-basis of $\boldsymbol{P}(s,t)$:

$$\begin{aligned} p &= -5310xs + \bigl(-4797s+2947-2434s^2\bigr)y + \bigl(-2213s^2+7553s-2105\bigr)z \\ &\quad + \bigl(-1263+6778s+442s^2\bigr)w, \\ q &= (-842s+2434)x + (4017+741s)y + \bigl(-3217+421s^2+2791s\bigr)z \\ &\quad + \bigl(842s^2+2416s-4851\bigr)w, \end{aligned}$$

so we know the implicit degree of rational ruled surface $\boldsymbol{P}(s,t)$ is 4 (in fact, $\boldsymbol{P}(s,t)$ has three base points $(s,t)=(-1,-1/2)$, $t=\infty$ and $s=\infty$ with multiplicities 1, 9 and 2 respectively). The implicit equation can be obtained by taking the determinant of the Sylvester matrix or Bezout matrix:

$$\begin{aligned} \mathrm{Res} &= 1006268875426076xz^2w - 490774658180520x^2zw \\ &\quad + 768112098422340zyw^2 - 127376438447320xy^2w \\ &\quad - 310601970486032y^2zw + 8380357023360x^2yw \\ &\quad + 5367419141152xy^2z - 262113124982716xyz^2 \\ &\quad + 712552326680564z^2yw + 1068420695862120xzw^2 \\ &\quad + 36993290288832x^2yz - 163057803797376xyw^2 \\ &\quad + 74345738735808x^2y^2 + 104761945253628xy^3 \\ &\quad - 230018352906348x^2z^2 - 593566221872108xyzw \\ &\quad + 56904120680940y^4 - 137213381334264w^4 \\ &\quad - 108283690526540z^4 + 304521223336344xz^3 \\ &\quad - 227646412570272x^2w^2 + 311040941568208xw^3 \\ &\quad - 22080744264228y^3z - 169642370030016y^3w \\ &\quad + 5813872684956y^2w^2 - 134387504992756y^2z^2 \\ &\quad + 210913134216188z^3y + 136425228709448yw^3 \\ &\quad - 910982220747372z^2w^2 - 653800037977508zw^3 \\ &\quad - 525760154599172z^3w + 26487914163120x^3y \\ &\quad + 52975828326240x^3z + 52975828326240x^3w. \end{aligned}$$

4. Conclusion

This paper presents an algorithmic approach to derive the mu-basis of a rational ruled surface. The algorithm has two main advantages over previous implicitization methods. First, it is not necessary to eliminate the base points before computing the mu-basis, which is usually a cumbersome task. Second, the algorithm is rigorous in that it is totally automatic, and no trial and error is needed. The mu-basis leads directly to the closed form representation of the implicit equation of a rational ruled surface.

While ruled surfaces are important in their own right, we hope that ultimately our new approach may help with the more challenging problem of developing the mu-basis and closed form representation of the implicit equation of a general rational surface.

Acknowledgements

The authors wish to express their gratitude to the referee for his careful reading and invaluable remarks which have helped to improve the manuscript. The current proof of Lemma 3, suggested by the referee, simplified our original proof.

This work was supported by NSF grant number CCR-9712407. Falai Chen is partially supported by 973 Project on Mathematical Mechanics (no. G1998030600) and National Natural Science Foundation of China (19971087). Jianmin Zheng is partially supported by National Natural Science Foundation of China (69973042) and Foundation of State Key Basic Research 973 Development Programming Item (G1998030600).

References

Aumann, G., 1991. Interpolation with developable Bézier patches. Comput. Aided Geom. Design 8, 409–420.

Chionh, E.-W., Goldman, R., 1992. Degree, multiplicity, and inversion formulas for rational surfaces using u-resultants. Comput. Aided Geom. Design 9, 93–108.

Cox, D., Little, J., O'Shea, D., 1992. Ideals, Varieties and Algorithms. Springer-Verlag.

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

Cox, D., Sederberg, T., Chen, F., 1998. The moving line ideal basis of planar rational curves. Comput. Aided Geom. Design 15 (8), 803–827.

Edge, W.L., 1931. The Theory of Ruled Surfaces. Cambridge Univ. Press, Cambridge, UK.

Lang, J., Roschel, O., 1992. Developable $(1, n)$-Bézier surfaces. Comput. Aided Geom. Design 9, 291–298.

Ravani, B., Chen, Y.J., 1986. Computer-aided design and machining of composite ruled surfaces. J. Mech. Trans. Automat. Design 108, 217–223.

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 (4), 334–342.

van der Waerden, B.L., 1950. Modern Algebra, 2nd ed. Frederick Ungar, New York.

Zheng, J., Sederberg, T.W., 2000. A direct approach to the mu-basis of planar rational curves. To appear.