Available online at www.sciencedirect.com
SCIENCE DIRECT®

Journal of Symbolic Computation 39 (2005) 689–706

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

The μ-basis and implicitization of a rational parametric surface

Falai Chen[a,*], David Cox[b], Yang Liu[c]

[a]Department of Mathematics, University of Science and Technology of China, Hefei, Anhui 230026, PR China
[b]Department of Mathematics and Computer Science, Amherst College, Amherst, MA 01002, USA
[c]Department of Computer Science and Information System, University of Hong Kong, Hong Kong, China

Received 9 October 2003; accepted 13 January 2005
Available online 4 March 2005

Abstract

The concept of a μ-basis was introduced in the case of parametrized curves in 1998 and generalized to the case of rational ruled surfaces in 2001. The μ-basis can be used to recover the parametric equation as well as to derive the implicit equation of a rational curve or surface. Furthermore, it can be used for surface reparametrization and computation of singular points. In this paper, we generalize the notion of a μ-basis to an arbitrary rational parametric surface. We show that: (1) the μ-basis of a rational surface always exists, the geometric significance of which is that any rational surface can be expressed as the intersection of three moving planes without extraneous factors; (2) the μ-basis is in fact a basis of the moving plane module of the rational surface; and (3) the μ-basis is a basis of the corresponding moving surface ideal of the rational surface when the base points are local complete intersections. As a by-product, a new algorithm is presented for computing the implicit equation of a rational surface from the μ-basis. Examples provide evidence that the new algorithm is superior than the traditional algorithm based on direct computation of a Gröbner basis. Problems for further research are also discussed.

Keywords: μ-basis; Moving plane; Syzygy module; Rational surface; Implicitization; Base point

[*] Corresponding author. Tel.: +86 551 3607537; fax: +86 551 3601005.
E-mail address: chenfl@ustc.edu.cn (F. Chen).

0747-7171/$ - see front matter © 2005 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jsc.2005.01.003

1. Introduction

The concept of a μ-basis was first introduced in Cox et al. (1998b) to provide an implicitization algorithm for planar rational curves. The μ-basis of a rational curve consists of two polynomials $p(x, y, t)$ and $q(x, y, t)$ which are linear in x, y and have degree μ ($\mu \leq [n/2]$) and $n - \mu$ in t respectively, where n is the degree of the rational curve. The resultant of $p(x, y, t)$ and $q(x, y, t)$ with respect to t gives the implicit equation of the rational curve. Using a variant form of the Bézout resultant, the implicit equation of a rational curve can be written as the determinant of an $(n - \mu) \times (n - \mu)$ matrix, whereas the previous resultant technique writes the implicit equation as an $n \times n$ determinant. Later it was shown that the μ-basis can be used to derive a more compact representation for the implicit equation of a rational curve with high order of singularities (Chen and Sederberg, 2002), and to compute the singular points of a rational curve (Chen and Wang, 2003c). Efficient algorithms were also developed to compute the μ-basis of a rational curve (Zheng and Sederberg, 2001; Chen and Wang, 2003b).

The idea of a μ-basis originated in a series of papers by Sederberg and his colleagues, where a new 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; Sederberg et al., 1997; Zhang et al., 1999; Cox et al., 2000). This idea was subsequently generalized to rational ruled surfaces (Chen et al., 2001; Chen and Wang, 2003a). The μ-basis of a rational ruled surface is defined to be three polynomials $p(x, y, z, s)$, $q(x, y, z, s)$ and $r(x, y, z, s, t)$ which are linear in x, y, z, and the intersection of the three planes $p = 0$, $q = 0$ and $r = 0$ gives exactly the parametric equation of the rational surface $\mathbf{P}(s, t)$. The μ-basis can be used not only to recover the parametric equation but also to derive the implicit equation of the rational ruled surface by taking the resultant of p and q. It also gives a simple way to reparametrize a rational ruled surface (Chen, 2003). In this paper, we generalize the notion of a μ-basis to an arbitrary rational surface. The main contributions of the current paper are as follows. First, we show that the μ-basis of a rational surface always exists. Geometrically, this means that every rational surface can be expressed as the intersection of three moving planes without extraneous factors. This is an unexpected result, for after ten years of exploration, researchers in the geometric modelling community generally believed that this was not true. Second, we show that the μ-basis of a general rational surface has properties similar to those of the μ-basis of a rational ruled surface. In particular, the μ-basis serves as a basis of the moving plane module, and when the base points are local complete intersections, it generates the moving surface ideal corresponding to the rational surface. Though similar to the theory developed for rational ruled surfaces in Chen and Wang (2003a), our results here apply to arbitrary rational surfaces, and some of the proofs require techniques from commutative algebra. Finally, we use the properties of μ-bases to present a new algorithm for computing the implicit equation of a rational surface. Examples seem to show that the new algorithm is more efficient than the traditional method of computing a Gröbner basis of the moving surface ideal.

The paper is organized as follows. In the next section, we recall some basic facts about syzygy modules, moving planes, and base points, and then define the μ-basis for an arbitrary rational surface. In Section 3, we prove the existence of the μ-basis and derive some useful properties for the μ-basis. Similar to Busé et al. (2003) and Cox (2004), the nicest case is when the base points are local complete intersections. Based on these properties, we derive a new algorithm to compute the implicit equation of a rational surface in Section 4. Examples are provided to compare the new algorithm with traditional algorithms. Finally, in Section 5, we conclude the paper with some problems for further research.

2. Definition of the μ-basis

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

A *submodule* M of R^m is a subset of R^m for which the following condition holds: for any $\mathbf{f}_1, \mathbf{f}_2 \in M$ and $h_1, h_2 \in R$, we have $h_1\mathbf{f}_1 + h_2\mathbf{f}_2 \in M$. A set of elements $\mathbf{f}_i \in M$, $i = 1, \ldots, k$, is called a *generating set* of M if for any $\mathbf{m} \in M$, there exist $h_i \in R$, $i = 1, \ldots, k$ such that

$$\mathbf{m} = h_1\mathbf{f}_1 + \cdots + h_k\mathbf{f}_k. \tag{2.1}$$

The Hilbert Basis Theorem tells us that every submodule $M \subset R^m$ has a finite generating set. If for any $\mathbf{m} \in M$, the above expression is unique, then $\{\mathbf{f}_1, \ldots, \mathbf{f}_k\}$ is called a *basis* of the module M. If a module has a basis, then it is called a *free module*. For any $(f_1, \ldots, f_k) \in R^k$, the set

$$\operatorname{syz}(f_1, \ldots, f_k) := \{(h_1, \ldots, h_k) \in R^k \mid h_1 f_1 + \cdots + h_k f_k \equiv 0\} \tag{2.2}$$

is a module over R, called a *syzygy* module (Cox et al., 1998b). An important result about syzygy modules is the following.

Proposition 2.1. *Let $a, b, c, d \in \mathbb{R}[s,t]$ be four relatively prime polynomials. Then the syzygy module* $\operatorname{syz}(a,b,c,d)$ *is a free module of rank* 3.

Proof. The proof is rather technical and will be given in the Appendix. □

A rational surface in homogeneous form is defined by

$$\mathbf{P}(s,t) = (a(s,t), b(s,t), c(s,t), d(s,t)), \tag{2.3}$$

where $a, b, c, d \in \mathbb{R}[s,t]$ are bi-degree (m,n) polynomials and $\gcd(a,b,c,d) = 1$. We assume that $m \geq n$ and the rational surface (2.3) is properly parametrized, i.e., the map

$$(s,t) \to \left(\frac{a(s,t)}{d(s,t)}, \frac{b(s,t)}{d(s,t)}, \frac{c(s,t)}{d(s,t)}\right)$$

is birational.

A *moving surface* of degree l is a family of algebraic surfaces with parameter pairs (s,t):

$$S(x,y,z,s,t) = \sum_{i=1}^{\sigma} f_i(x,y,z) b_i(s,t) \tag{2.4}$$

where $f_i(x, y, z)$, $i = 1, \ldots, \sigma$ are degree l polynomials, and $b_i(s, t) \in \mathbb{R}[s, t]$, $i = 1, \ldots, \sigma$ are called *blending functions* which are linearly independent. A moving surface is said to *follow* the rational surface (2.3) if

$$d^l S(a/d, b/d, c/d, s, t) \equiv 0. \tag{2.5}$$

Note that the implicit equation of the rational surface $\mathbf{P}(s, t)$ is a moving surface of $\mathbf{P}(s, t)$.

A *moving plane* is a moving surface of degree 1. The moving plane

$$A(s, t)x + B(s, t)y + C(s, t)z + D(s, t)$$

will be denoted by $\mathbf{L}(s, t) := (A(s, t), B(s, t), C(s, t), D(s, t)) \in \mathbb{R}[s, t]^4$. Let $\mathbf{L}_{s,t}$ be the set of the moving planes which follow the rational surface $\mathbf{P}(s, t)$. Thus $\mathbf{L}_{s,t}$ is exactly the syzygy module $\operatorname{syz}(a, b, c, d)$.

In this paper, we work over the real numbers $\mathbb{R}$. The one exception is that when we consider base points, we need to work over the complex numbers $\mathbb{C}$. A *base point* of the rational surface $\mathbf{P}(s, t)$ is a parameter pair (s_0, t_0) such that $\mathbf{P}(s_0, t_0) = \mathbf{0}$. Base points are closely related with the implicit degree of a rational surface. Generally, a rational surface with total degree n has implicit degree $n^2 - r$, where r is the number of base points counted with multiplicities, complex ones and points at infinity Sederberg and Saito (1995). The following example illustrates why we should work over $\mathbb{C}$ instead of $\mathbb{R}$ when considering base points.

Example 2.1. One can check that the cubic triangular parametrization

$$\mathbf{P}(s, t) = (a, b, c, d) = (s(s^2 + 1), s^2 t, (s + 1)t^2, t^3)$$

has an implicit equation $x^2 - 4y^3 + 4xyz - yz^4 = 0$ of degree 5. Over $\mathbb{R}$, the only base point is $(s, t) = (0, 0)$ of multiplicity 2. This gives an implicit degree of $3^2 - 2 = 7$, which is wrong because we ignored the complex base points $(s, t) = (\pm \mathrm{i}, 0)$ of multiplicity 1. Using these, the implicit degree is the correct number $3^2 - 2 - 1 - 1 = 5$.

We say that a base point of (2.3) is a *local complete intersection* if in a neighborhood of the base point, the ideal generated by a, b, c, d can be generated by two polynomials. Local complete intersection base points are discussed in Cox (2004). The article Cox (2004) also discusses multiplicities.

Several of our results involve conditions on the *finite base points* of the parametrization. By the above convention, this refers to all real and complex base points which are finite, i.e., which correspond to parameter values s, t of a point in the affine plane $\mathbb{C}^2$.

Now we define the μ-basis of the rational surface (2.3).

Definition 2.1. Let $\mathbf{p}, \mathbf{q}, \mathbf{r} \in \mathbf{L}_{s,t}$ be three moving planes such that

$$[\mathbf{p}, \mathbf{q}, \mathbf{r}] = \kappa \mathbf{P}(s, t) \tag{2.6}$$

for some nonzero constant κ. Then $\mathbf{p}, \mathbf{q}, \mathbf{r}$ are said to form a **μ-basis** of the rational surface (2.3). Here $[\mathbf{p}, \mathbf{q}, \mathbf{r}]$ is the **outer product** of $\mathbf{p}$, $\mathbf{q}$, and $\mathbf{r}$ defined by

$$[\mathbf{p}, \mathbf{q}, \mathbf{r}] = \left(\begin{vmatrix} p_2 & p_3 & p_4 \\ q_2 & q_3 & q_4 \\ r_2 & r_3 & r_4 \end{vmatrix}, - \begin{vmatrix} p_1 & p_3 & p_4 \\ q_1 & q_3 & q_4 \\ r_1 & r_3 & r_4 \end{vmatrix}, \begin{vmatrix} p_1 & p_2 & p_4 \\ q_1 & q_2 & q_4 \\ r_1 & r_2 & r_4 \end{vmatrix}, - \begin{vmatrix} p_1 & p_2 & p_3 \\ q_1 & q_2 & q_3 \\ r_1 & r_2 & r_3 \end{vmatrix} \right). \tag{2.7}$$

Furthermore, $\mathbf{p}, \mathbf{q}, \mathbf{r}$ are said to form a **minimal μ-basis** of the rational surface (2.3) if

1. among all the triples of $\mathbf{p}, \mathbf{q}, \mathbf{r}$ satisfying (2.6), $\deg_t(\mathbf{p}) + \deg_t(\mathbf{q}) + \deg_t(\mathbf{r})$ is smallest, and
2. among all the triples of $\mathbf{p}, \mathbf{q}, \mathbf{r}$ satisfying (2.6) and item 1, $\deg_s(\mathbf{p}) + \deg_s(\mathbf{q}) + \deg_s(\mathbf{r})$ is smallest.

Here, $\deg_t(\mathbf{p}) = \max_{1\le i\le 4}(\deg_t(p_i))$ when $\mathbf{p} = (p_1, p_2, p_3, p_4)$, and $\deg_t(\mathbf{q})$, $\deg_t(\mathbf{r})$, $\deg_s(\mathbf{p})$, $\deg_s(\mathbf{q})$, $\deg_s(\mathbf{s})$ are defined similarly.

Sometimes we refer to the three polynomials

$$p = \mathbf{p} \cdot \mathbf{X}, \qquad q = \mathbf{q} \cdot \mathbf{X}, \qquad r = \mathbf{r} \cdot \mathbf{X}, \qquad \mathbf{X} = (x, y, z, 1),$$

as the μ-basis of the rational surface (2.3).

The above definition is a natural generalization of the definition of the μ-basis for a rational ruled surface. In the next section, we will prove the existence of the μ-basis and derive some properties which are similar to those for the μ-basis of a rational ruled surface.

Remark 2.1. Geometrically, Eq. (2.6) means that the rational surface $\mathbf{P}(s, t)$ can be represented as the intersection of three moving planes $\mathbf{p}$, q and $\mathbf{r}$ without extraneous factors. This generalizes the result in Sederberg et al. (1994), where it was shown that any rational curve is the intersection of two moving lines. While the result in the curve case was discovered ten years ago, the surface case has been a mystery for a long time, and many in the geometric modelling community doubted the existence of a general theory of μ-bases. However, we will show in the next section that the μ-basis always exists, that is, the generalization for the surface case is also true!

Remark 2.2. One can similarly define a μ-basis for a total degree rational surface. For a triangular surface of total degree n, if among all the triples of $\mathbf{p}, \mathbf{q}, \mathbf{r}$ satisfying (2.6), $\deg(\mathbf{p}) + \deg(\mathbf{q}) + \deg(\mathbf{r})$ is smallest, then $\mathbf{p}, \mathbf{q}, \mathbf{r}$ are called a *minimal μ-basis* of the triangular rational surface.

We illustrate an example of the above definition.

Example 2.2. Given the canonical Steiner surface

$$\mathbf{P}(s, t) = (a, b, c, d) = (2st, 2t, 2s, s^2 + t^2 + 1),$$

one can easily verify that

$$\mathbf{p} = (0, st, 1 + s^2, -2s), \quad \mathbf{q} = (0, 1 + t^2, st, -2t), \quad \mathbf{r} = (1, -s, 0, 0)$$

gives a μ-basis of the Steiner surface. Let us show that they form a minimal μ-basis.

To do so, we first notice that the two lowest degree moving planes are $\mathbf{r}_1 = (1, -s, 0, 0)$ and $\mathbf{r}_2 = (1, 0, -t, 0)$. We claim that for any $\mathbf{r}_3 = (r_{31}, r_{32}, r_{33}, r_{34}) \in \mathbb{R}[s, t]^4$, $\mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3$ cannot be a μ-basis. In fact, from

$$[\mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3](r_{34}st, r_{34}t, r_{34}s, -r_{31}st - r_{32}t - r_{33}s) = \kappa \mathbf{P}(s, t)$$

one has $\kappa = r_{34}$ and $-r_{31}st - r_{32}t - r_{33}s = \kappa(s^2 + t^2 + 1)$. The later equation cannot hold since setting $s = t = 0$ on both sides of the equation gives $0 = \kappa \neq 0$. This means that at most one of the μ-basis elements has degree 1, so the other elements have degree greater than or equal to 2. Thus $\mathbf{p}, \mathbf{q}, \mathbf{r}$ form a minimal μ-basis.

3. Existence and properties of μ-bases

In this section, we will first prove the existence of μ-bases, and then explore some properties of the μ-basis of a rational surface, especially the property that it serves as the basis of the moving plane module $\mathbf{L}_{s,t}$. We also explore the relation between the μ-basis and the moving surface ideal. This is where the results for general rational surfaces differ from the results for rational ruled surfaces and where local complete intersection base points become important. For some results in this section, the proofs are the same as for rational ruled surface case, and for these we refer the reader to Chen and Wang (2003a) for details. However, it must be emphasized that the results are all new for a general rational surface.

Theorem 3.1. *For any rational surface as defined in* (2.3), *there always exist three moving planes* $\mathbf{p}, \mathbf{q}, \mathbf{r}$ *such that* (2.6) *holds. In fact, any basis* $\mathbf{p}, \mathbf{q}, \mathbf{r}$ *of* $\mathrm{syz}(a, b, c, d)$ *satisfies* (2.6).

Proof. Since a, b, c, d are relatively prime, by Proposition 2.1, the syzygy module $\mathrm{syz}(a, b, c, d)$ is free. Let $\mathbf{p}, \mathbf{q}, \mathbf{r}$ be a basis of $\mathrm{syz}(a, b, c, d)$. Notice that $\mathbf{p}, \mathbf{q}, \mathbf{r}$ are moving planes following $\mathbf{P}(s, t)$, that is, as four dimensional vectors, $\mathbf{p}, \mathbf{q}, \mathbf{r}$ are all perpendicular to $\mathbf{P}(s, t)$. Hence $\mathbf{P}(s, t)$ is parallel to $[\mathbf{p}, \mathbf{q}, \mathbf{r}]$, that is, there exist polynomials $h, \bar{h} \in \mathbb{R}[s, t]$, where $\bar{h}$ and h are relatively prime, such that

$$\bar{h}\,[\mathbf{p}, \mathbf{q}, \mathbf{r}] = h\,\mathbf{P}(s, t).$$

Since $\gcd(\bar{h}, h) = 1$ and $\gcd(a, b, c, d) = 1$, $\bar{h}$ must be a nonzero constant, so that without loss of generality, we may assume $\bar{h} = 1$. Since $(-b, a, 0, 0)$, $(-c, 0, a, 0)$ and $(-d, 0, 0, a)$ all belong to $\mathbf{L}_{s,t}$, there exist polynomials $h_{ij} \in \mathbb{R}[s, t]$, $i, j = 1, 2, 3$ such that

$$\begin{aligned}
(-b, a, 0, 0) &= h_{11}\mathbf{p} + h_{12}\mathbf{q} + h_{13}\mathbf{r},\\
(-c, 0, a, 0) &= h_{21}\mathbf{p} + h_{22}\mathbf{q} + h_{23}\mathbf{r},\\
(-d, 0, 0, a) &= h_{31}\mathbf{p} + h_{32}\mathbf{q} + h_{33}\mathbf{r}.
\end{aligned}$$

Forming the outer product of the above three vector polynomials, one has

$$a^2\mathbf{P}(s, t) = \det(h_{ij})[\mathbf{p}, \mathbf{q}, \mathbf{r}] = \det(h_{ij})h\,\mathbf{P}(s, t),$$

where $\det(h_{ij})$ is the determinant of the matrix $(h_{ij})_{3\times 3}$. Thus $h|a^2$, and similarly we have $h|b^2$, $h|c^2$ and $h|d^2$. Therefore $h|\gcd(a^2, b^2, c^2, d^2) = 1$, i.e., h must be a nonzero constant. The theorem is thus proved. □

Now we explore some properties of μ-bases. We first study the relation between the μ-basis and the moving plane module $\mathbf{L}_{s,t}$.

Theorem 3.2. *Let* $\mathbf{p}, \mathbf{q}, \mathbf{r}$ *be a* μ*-basis of the rational surface* (2.3)*. Then* $\mathbf{p}$, $\mathbf{q}$ *and* $\mathbf{r}$ *give a basis for the module* $\mathbf{L}_{s,t}$ *(thus* $\mathbf{L}_{s,t}$ *is a free module), i.e., for any* $\mathbf{l}(s,t) \in \mathbf{L}_{s,t}$*, there exist polynomials* $h_i(s,t)$*,* $i = 1, 2, 3$*, such that*

$$\mathbf{l}(s,t) = h_1\mathbf{p} + h_2\mathbf{q} + h_3\mathbf{r} \tag{3.1}$$

and the above expression is unique. Furthermore, $\deg_t(h_1\mathbf{p}), \deg_t(h_2\mathbf{q}), \deg_t(h_3\mathbf{r})$ *are bounded by* $\deg_t(\mathbf{l})+\deg_t(\mathbf{p})+\deg_t(\mathbf{q})+\deg_t(\mathbf{r})-n$*, and* $\deg_s(h_1\mathbf{p}), \deg_s(h_2\mathbf{q}), \deg_s(h_3\mathbf{r})$ *are bounded by* $\deg_s(\mathbf{l}) + \deg_s(\mathbf{p}) + \deg_s(\mathbf{q}) + \deg_s(\mathbf{r}) - m$.

Proof. The proof is similar to the proof of Theorem 4 in Chen and Wang (2003a) and is based on a series of lemmas similar to Lemmas 2, 3 and 4 in Chen and Wang (2003a). The only difference is that here the polynomial $g(s) \in \mathbb{R}[s]$ is defined by $\langle a, b, c, d\rangle \cap \mathbb{R}[s] = \langle g\rangle$. □

Remark 3.1. For a triangular surface of total degree n, the μ-basis has the same property as above. Furthermore, $\deg(h_1\mathbf{p})$, $\deg(h_2\mathbf{q})$ and $\deg(h_3\mathbf{r})$ are bounded by $\deg(\mathbf{l})+\deg(\mathbf{p})+\deg(\mathbf{q}) + \deg(\mathbf{r}) - n$.

Remark 3.2. There is one important difference between μ-bases for curves and surfaces. For a curve parametrization, the μ-basis $\mathbf{p}, \mathbf{q}$ defined in Cox et al. (1998a) has the property that if a moving line $\mathbf{l}$ follows the parametrization, then there are unique polynomials $h_i(t)$, $i = 1, 2$ such that

$$\mathbf{l}(t) = h_1\mathbf{p} + h_2\mathbf{q}, \qquad \deg(h_1\mathbf{p}) \le \deg(\mathbf{l}) \qquad \text{and} \qquad \deg(h_2\mathbf{q}) \le \deg(\mathbf{l}).$$

These degree bounds are much stronger than those given in Theorem 3.2. The reason is that in the curve case, the μ-basis remains a basis of the syzygy module after homogenization. To see that this can fail in the surface case, recall from Example 2.2 that

$$\mathbf{p} = (0, st, 1 + s^2, -2s), \qquad \mathbf{q} = (0, 1 + t^2, st, -2t), \qquad \mathbf{r} = (1, -s, 0, 0)$$

is a minimal μ-basis of the Steiner surface

$$\mathbf{P}(s,t) = (2st, 2t, 2s, s^2 + t^2 + 1).$$

When we homogenize using the new variable u, the μ-basis becomes

$$\widetilde{\mathbf{p}} = (0, st, u^2 + s^2, -2su), \quad \widetilde{\mathbf{q}} = (0, u^2 + t^2, st, -2tu), \quad \widetilde{\mathbf{r}} = (u, -s, 0, 0).$$

It is easy to see that the moving plane $\mathbf{l} = (0, s, -t, 0)$ cannot be expressed as an $\mathbb{R}[s,t,u]$-linear combination of $\widetilde{\mathbf{p}}$, $\widetilde{\mathbf{q}}$ and $\widetilde{\mathbf{r}}$. In fact, the homogeneous syzygy module is not a free module, and this explains why we do not get the strong degree bounds as in the curve case. The moral is that in order to get a μ-basis of a surface, we must work with the affine variables s, t. (Actually, there are some special surfaces which have homogeneous μ-bases. These are called *special* μ*-bases* in Cox (2004, Section 5).)

An immediate consequence of Theorems 3.1 and 3.2 is:

Corollary 3.1. $\mathbf{p}, \mathbf{q}$ *and* $\mathbf{r}$ *form a* μ*-basis if and only if* $\mathbf{p}, \mathbf{q}$ *and* $\mathbf{r}$ *are a basis of* $\mathrm{syz}(a, b, c, d)$.

Remark 3.3. From the above corollary, a μ-basis can be obtained by computing a basis for the syzygy module $\mathrm{syz}(a, b, c, d)$. We also note that Theorems 3.1 and 3.2 are closely related to the Hilbert–Burch theorem, as discussed in Eisenbud (1995, Section 20.4).

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

Theorem 3.3. *Let*

$$I := \langle dx - a, dy - b, dz - c\rangle \subset \mathbb{R}[x, y, z, s, t] \tag{3.2}$$

be the ideal corresponding to rational surface (2.3)*, and $g(s) \in \mathbb{R}[s]$ be the polynomial defined by $\langle a, b, c, d\rangle \cap \mathbb{R}[s] = \langle g\rangle$. Then*

$$g\langle p, q, r\rangle \subset I \subset \langle p, q, r\rangle. \tag{3.3}$$

In particular, if the rational surface $\mathbf{P}(s, t)$ has no s-finite base points (i.e., the s-coordinates of the base points are finite), then $I = \langle p, q, r\rangle$.

Proof. The proof is similar to the proof of Theorem 6 in Chen and Wang (2003a). □

We now introduce the *moving surface ideal*:

$$I' := \langle dx - a, dy - b, dz - c, dw - 1\rangle \cap \mathbb{R}[x, y, z, s, t]. \tag{3.4}$$

This name is justified by the following:

Theorem 3.4. *Let I' be the moving surface ideal and $g(s)$ be the polynomial as defined in* Theorem 3.3*. Then I' is a prime ideal, and $g(s) \notin I'$. Furthermore, $f \in I'$ if and only if $f = 0$ is a moving surface following the rational surface $\mathbf{P}(s, t)$. In particular, if $f(x, y, z) = 0$ is the implicit equation of the rational surface $\mathbf{P}(s, t)$, then $f(x, y, z) \in I'$.*

Proof. Again, the proof is similar to the proof of Lemma 5 and Theorem 7 in Chen and Wang (2003a). □

The relationship of the ideal generated by the μ-basis and the moving surface ideal I' is characterized by the following theorem.

Theorem 3.5. *Let I' be the ideal defined in* (3.4) *and $g(s)$ be the polynomial defined in* Theorem 3.3*. Then*

$$\begin{aligned} I' = \langle p, q, r\rangle : g^{\infty} &= \bigcup_{N=0}^{\infty} \langle p, q, r\rangle : g^{N} \\ &= \{ f \mid g^{N} f \in \langle p, q, r\rangle \text{ for some } N \geq 0\}. \end{aligned} \tag{3.5}$$

In particular, if all finite base points of the rational surface $\mathbf{P}(s, t)$ are local complete intersections, then

$$I' = \langle p, q, r\rangle. \tag{3.6}$$

The proof of Theorem 3.5 follows the strategy used to prove Theorem 8 in Chen and Wang (2003a), which used Lemmas 6–8 in Chen and Wang (2003a). However, the key lemma—Lemma 6 in Chen and Wang (2003a)—should be replaced by the following lemma.

Lemma 3.1. *Fix a parameter value $s = s_0$. Suppose, for any parameter t, the matrix with columns $\mathbf{p}, \mathbf{q}, \mathbf{r}$ has rank at least two at (s_0, t). Let $p_0 = p(x, y, z, s_0, t)$, $q_0 = q(x, y, z, s_0, t)$ and $r_0 = r(x, y, z, s_0, t)$. Then $\operatorname{syz}(p_0, q_0, r_0) \subset \mathbb{R}[x, y, z, t]^3$ 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. We will study the Koszul complex of p_0, q_0, r_0 over the ring $R = \mathbb{R}[x, y, z, t]^3$. This consists of the maps

$$0 \longrightarrow R \xrightarrow{\begin{bmatrix} r_0 \\ -q_0 \\ p_0 \end{bmatrix}} R^3 \xrightarrow{\begin{bmatrix} q_0 & r_0 & 0 \\ -p_0 & 0 & r_0 \\ 0 & -p_0 & -q_0 \end{bmatrix}} R^3 \xrightarrow{\begin{bmatrix} p_0 & q_0 & r_0 \end{bmatrix}} \langle p_0, q_0, r_0 \rangle \longrightarrow 0.$$

We will show that this sequence is *exact*, meaning that, at each position, the image of the incoming map equals the nullspace of the outgoing map. Note that the lemma follows immediately once we prove exactness.

Our proof will use methods from commutative algebra. In particular, given a point $p = (x_0, y_0, z_0, t_0)$, we will use the local ring

$$R_p = \left\{ \frac{f}{g} \,\middle|\, f, g \in R, g(p) \neq 0 \right\}.$$

Then the *localized Koszul complex* is obtained from the above Koszul complex by replacing R with R_p. Standard results in commutative algebra show that the original Koszul complex is exact if and only if all of the localized Koszul complexes are exact.

First suppose that p_0, q_0, r_0 do not all vanish at p. Then in R_p, we have $\langle p_0, q_0, r_0 \rangle = R_p$. In this situation, Exercise 15 from Section 4 of Chapter 6 of Cox et al. (1998a) implies that the localized Koszul complex is exact.

Next suppose that p_0, q_0, r_0 all vanish at p. This means that p lies in the variety $\mathbf{V}(p_0, q_0, r_0) \subset \mathbb{C}^4$. We will show that $\mathbf{V}(p_0, q_0, r_0)$ has dimension ≤ 1. The key point is that the equations $p_0 = q_0 = r_0 = 0$ give a linear system in x, y, z whose matrix consists of the columns $\mathbf{p}, \mathbf{q}, \mathbf{r}$ evaluated at (s_0, t). We write this matrix as

$$M = \begin{pmatrix} A \\ B \end{pmatrix}$$

where A is a 3×3 matrix, B is a 1×3 matrix, and all entries lie in $\mathbb{R}[t]$. In this notation, the equations $p_0 = q_0 = r_0 = 0$ can be expressed as

$$(x\ y\ z)A = -B. \tag{3.7}$$

According to Definition 2.1, $\det(A) = -\kappa d(s_0, t)$, and the other 3×3 minors of M give $a(s_0, t)$, $b(s_0, t)$, $c(s_0, t)$ up to sign. Now fix a parameter value $t \in \mathbb{C}$ and consider the following cases:

1. (s_0, t) is not a base point of $\mathbf{P}$. If $d(s_0, t) \neq 0$, then $\det(A) \neq 0$ at t, so that (3.7) has a unique solution. On the other hand, if $d(s_0, t) = 0$, then one of $a(s_0, t)$, $b(s_0, t)$, $c(s_0, t)$ must be nonzero. This means that at t, M has rank 3 yet A has rank <3. It follows that (3.7) is inconsistent. Hence we have at most 1 solution when (s_0, t) is not a base point. Putting these solutions together as we vary t gives a solution set of dimension ≤ 1.

2. (s_0, t) is a base point of $\mathbf{P}$. This means that the above matrix M has rank <3 at t. Since M always has rank ≥ 2 by hypothesis, the rank is exactly 2 at t. If A also has rank 2 at t, then (3.7) has a 1-dimensional space of solutions, while if A has rank <2, the system is inconsistent. Thus each of these t's contributes a solution set of dimension ≤ 1.

Since there are only finitely many t's in the second case, it follows that all solutions form a variety of dimension ≤ 1, as claimed.

It follows that in the local ring R_p, the three elements p_0, q_0, r_0 generate an ideal whose variety has dimension at most 1. Since these polynomials vanish at p, the variety is nonempty and hence has dimension at least 1 since each equation drops the dimension by at most 1. It follows that the dimension is exactly 1. Then standard results in commutative algebra (specifically, Corollary 1.6.14(b), Theorem 2.1.2(c), and Theorem 2.1.9 of Bruns and Herzog (1993)) imply that the localized Koszul complex is exact. □

We can explain the rank condition appearing in Lemma 3.1 in terms of base points as follows.

Lemma 3.2. *The finite base points of* $\mathbf{P}(s, t)$ *are all local complete intersections if and only if the matrix with columns* $\mathbf{p}$, $\mathbf{q}$, $\mathbf{r}$ *has rank at least* 2 *for all finite values of* s, t.

Proof. This follows from the argument given in Case 2 of Remark 5.1 of Busé et al. (2003). □

Now we sketch the proof of Theorem 3.5.

For any $f \in I'$, there exists a nonnegative integer N such that $g^N f \in \langle p, q, r\rangle$ by a lemma similar to Lemma 8 in Chen and Wang (2003a). So $f \in \langle p, q, r\rangle : \langle g^N\rangle$ and hence $I' \subset \langle p, q, r\rangle : g^\infty$.

On the other hand, for any $f \in \langle p, q, r\rangle : g^\infty$, there exists a nonnegative integer N such that $f \in \langle p, q, r\rangle : \langle g^N\rangle$. So $g^N f \in \langle p, q, r\rangle \subset I'$. By Theorem 3.4, $f \in I'$. Thus $\langle p, q, r\rangle : g^\infty \subset I'$. Therefore the first equality in (3.5) holds.

The proof of (3.6) follows by an argument similar to the proof of Theorem 8 in Chen and Wang (2003a). □

Remark 3.4. The above theorems are also valid for the μ-basis of a triangular rational surface.

Remark 3.5. For a rational ruled surface, all base points are local complete intersections, and thus (3.6) always holds. While for a general rational surface, (3.6) may not be true.

4. Implicitization algorithm

From the theorems presented in the last section, we can devise a new algorithm to compute the implicit equation of the rational surface $\mathbf{P}(s, t)$.

Algorithm MU-BASIS-IMP

Input: The parametric equation of a rational surface, assumed to be proper.
Output: The implicit equation of the rational surface.

Step 1 Compute the implicit degree of the rational surface $\mathbf{P}(s,t) = (a(s,t), b(s,t), c(s,t), d(s,t))$ and let it be l. Thus l is the number of intersection points of a random line

$$\alpha_1 x + \beta_1 y + \gamma_1 z + \delta_1 = \alpha_2 x + \beta_2 y + \gamma_2 z + \delta_2 = 0$$

with the surface. The s values corresponding to intersection points are roots of the resultant

$$h(s) = \mathrm{Res}(\alpha_1 a + \beta_1 b + \gamma_1 c + \delta_1 d, \alpha_2 a + \beta_2 b + \gamma_2 c + \delta_2 d, t).$$

However, $h(s)$ has extraneous roots coming from the base points. To remove them, make a different random choice $\tilde{\alpha}_1, \ldots, \tilde{\delta}_2$. Using these in the above resultant formula, we get a polynomial $\tilde{h}(s)$ having the same extraneous roots as $h(s)$. Then it follows easily that

$$l = \deg(h(s)) - \deg(\gcd(h(s), \tilde{h}(s)))$$

since the parametrization is proper. Now go to the next step.

Step 2 For a tensor product surface of bi-degree (m,n), if $l = 2mn$ (or for a triangular surface of total degree n, if $l = n^2$), then $\mathbf{P}(s,t)$ does not have base points and the Dixon resultant (or the classical multivariate resultant for a triangular surface) gives the implicit equation of $\mathbf{P}(s,t)$. Let $F(x,y,z)$ be this resultant and go to **Step 7**. Otherwise, go to the next step.

Step 3 Compute a μ-basis $\mathbf{p}, \mathbf{q}, \mathbf{r}$ for the rational surface $\mathbf{P}(s,t)$ and the polynomial $g(s)$ defined in Theorem 3.3. Now set $J := \langle p, q, r \rangle$, where $p = \mathbf{p} \cdot \mathbf{X}$, $q = \mathbf{q} \cdot \mathbf{X}$, $r = \mathbf{r} \cdot \mathbf{X}$, for $\mathbf{X} = (x,y,z,1)$. Then go to the next step.

Step 4 Compute a Gröbner basis for J under a monomial order such that t is greater than any monomial in s,x,y,z and s is greater than any monomial in x,y,z. Let $F(x,y,z)$ be the polynomial in the Gröbner basis which involves only x,y,z (if any). If $\deg(F) = l$, then go to **Step 7**. Otherwise, relabel $J := \langle p, q, r \rangle \bigcap \mathbb{R}[x,y,z,s]$ and go to the next step.

Step 5 Compute a Gröbner basis for the ideal $J : g$ under a monomial order such that s is greater than any monomial in x,y,z. Then relabel $J := J : g$ and go to the next step.

Step 6 Let $F(x,y,z)$ be the polynomial in the Gröbner basis of J which involves only x,y,z (if any). If $\deg(F) = l$, then go to **Step 7**. Otherwise, go to **Step 5**.

Step 7 Output $F(x,y,z)$.

Remark 4.1. By Theorems 3.4 and 3.5, we know that the implicit equation F lies in the saturation $\langle p, q, r \rangle : g^\infty$. Thus $F \in \langle p, q, r \rangle : g^N$ for some integer $N \geq 0$. This proves termination and correctness of the algorithm.

The minimal N for which $F \in \langle p, q, r \rangle : g^N$ tells us how many times the loop in **Steps 5** and **6** is performed. We obtain the a priori bound $N \leq l$ as follows. Since l is the degree of F, we can divide $d^l F$ by $dx - a, dy - b, dz - c$ to obtain

$$d^l F \in \langle dx - a, dy - b, dz - c \rangle.$$

If $i + j + k \leq l$, then multiply by $x^i y^j z^k$ and use $dx(dx - a) + a$, etc., to obtain

$$a^i b^j c^k d^{l-i-j-k} F \in \langle dx - a, dy - b, dz - c\rangle.$$

It follows that $\langle a, b, c, d\rangle^l F \subset \langle dx - a, dy - b, dz - c\rangle$. Since $g \in \langle a, b, c, d\rangle$, we see that $g^l F \in \langle dx - a, dy - b, dz - c\rangle$, and then $F \in \langle p, q, r\rangle : g^l$ follows from Theorem 3.3.

However, $N \leq l$ might not the optimal bound. We have tested dozens of examples, and in every example, we found that $g^N F \in \langle p, q, r\rangle$ for some integer $N \leq m_b - 1$, where m_b is the highest multiplicity of the base points of the rational surface $\mathbf{P}(s, t)$. We conjecture that this is always true, though we have not been able to find a proof.

Another approach would be to replace the loop in **Steps 5** and **6** with a computation of the saturation of $\langle p, q, r\rangle \cap \mathbb{R}[x, y, z, s]$ with respect to g, say using the `sat` command from the `elim.lib` library of *Singular*. However, the minimal N that works for F may be strictly smaller than the saturation exponent of $\langle p, q, r\rangle \cap \mathbb{R}[x, y, z, s]$ with respect to g.

In the presence of base points, the examples we have tested indicate that the above algorithm may be more efficient than the traditional technique based on directly computing a Gröbner basis for the ideal I', especially for rational surfaces of low degree. The complexity of this algorithm is not easy to determine, given the many Gröbner basis computations involved. If we ignore the size of the coefficients, then we can informally explain the efficiency of the algorithm as follows. While computing the Gröbner basis of I' involves six variables x, y, z, w, s, t and four polynomials, computing the Gröbner basis for the ideal $\langle p, q, r\rangle$ involves only five variables x, y, z, s, t and three polynomials. Furthermore, computing $g(s)$ and $\mathrm{syz}(a, b, c, d)$ is relatively efficient since only two variables s, t are involved. For low degree rational surfaces, the examples seem to suggest that the degree of the μ-basis is also low. Thus computation costs decrease.

The computations were performed on a PC machine with Pentium 4 2.40 GHz CPU and 256 MB RAM using the symbolic computation software *Singular*.

Example 4.1. Consider the cubic parametric surface defined by

$$a = s^2t - t^2, \qquad b = -s + s^3 + st^2,$$
$$c = -t + st + s^2t - t^2, \qquad d = -t + s^2t + t^2.$$

It has four base points $(1, 0, 1)$, $(-1, 0, 1)$, $(0, 0, 1)$, and $(0, 1, 0)$, all simple, so that its implicit degree is $3^2 - 4 = 5$. A μ-basis is computed as

$$\begin{aligned}
\mathbf{p} &= [-2s^2 - s + 2, 0, 2s^2 - 1, -s + 1],\\
\mathbf{q} &= [-2ts - 3t + s + 1, 0, 2ts + 2t - s - 1, -t + 1],\\
\mathbf{r} &= [ts + 2t + 4s^4 + 6s^3 - 4s - 4,\\
&\qquad -2t, -2ts - t - 4s^4 - 4s^3 + 4s + 2, ts + t + 2s^3 - 2].
\end{aligned}$$

Since all the base points are local complete intersections, the implicit equation of the parametric surface can be obtained by computing the Gröbner basis of the ideal $\langle p, q, r\rangle$:

$$\begin{aligned}
F(x, y, z) = {} & 8x^5 - 5x^4y - 4x^3y^2 - 12x^4z + 10x^3yz + 4x^2y^2z - 2x^3z^2 + x^2yz^2\\
& + 4xy^2z^2 + 11x^2z^3 - 10xyz^3 - 4y^2z^3 - 6xz^4 + 4yz^4 + z^5 + 19x^3y\\
& + 4x^2y^2 - 22x^3z - 46x^2yz - 12xy^2z + 47x^2z^2 + 38xyz^2 + 8y^2z^2
\end{aligned}$$

$$
\begin{aligned}
&- 32xz^3 - 10yz^3 + 7z^4 + 2x^3 + 2x^2y + 4xy^2 - 12x^2z - 8xyz\\
&- 4y^2z + 14xz^2 + 5yz^2 - 5z^3 + 2x^2 - xy + 4xz\\
&- 5z^2 - 2x + y + 3z - 1 = 0.
\end{aligned}
$$

The computation time is negligible. If one computes the Gröbner basis of I', then the computation time is 31 ms (milliseconds).

Example 4.2. Consider the cubic parametric surface defined by

$$
\begin{aligned}
a &= t^2 - 3t^3 - 5st^2 - 3s^2t - s^3,\\
b &= -5t^2 + 2st^2 - 3s^2 - 5s^2t - 5s^3,\\
c &= t^2 + 5t^3 - 5st^2 + s^2 - 5s^2t + 3s^3,\\
d &= -4t^2 - 2t^3 + 4st^2 + 3s^2 - 4s^2t - 5s^3.
\end{aligned}
$$

The base point $(s, t) = (0, 0)$ has multiplicity 4, and the degree of the implicit equation is $3^2 - 4 = 5$. One can check that the base point is a local complete intersection, so the implicit equation can be obtained by computing the Gröbner basis of the ideal $\langle p, q, r\rangle$. The computation time was 31 ms. However, it took 5562 ms to compute the Gröbner basis of I'.

Example 4.3. Consider the biquadratic surface parametrized by

$$
\begin{aligned}
&a = 4 - 4t^2 - 4st + 4s^2t - 3s^2t^2, \qquad b = 1 - 2t^2 - 5st + 3s^2t - 3s^2t^2,\\
&c = -5 + st + 5s^2t - 5s^2t^2, \qquad d = 1 + 5t^2 - st + 2s^2t - 4s^2t^2.
\end{aligned}
$$

The only base point occurs at $s = \infty$, $t = 0$ and has multiplicity 2. Hence the implicit degree of the surface is $2 \times 2^2 - 2 = 6$. Again the base point is a local complete intersection. The μ-basis was computed in 125 ms and the Gröbner basis of $\langle p, q, r\rangle$ in 31 ms. However, it took 36 172 ms to compute the Gröbner basis of I'.

Example 4.4. In our final example, consider the biquadratic surface parameterized by

$$
\begin{aligned}
&a = t^2 + st + 2s^2 - 2s^2t, \qquad b = t^2 + 2st + st^2 + 2s^2 - s^2t + 2s^2t^2,\\
&c = -t^2 + st + 2st^2 + 2s^2 - s^2t - 2s^2t^2, \qquad d = 2st - 2st^2 - 2s^2t - s^2t^2.
\end{aligned}
$$

$\mathbf{P}(s, t)$ has a base point at $(s, t) = (0, 0)$ of multiplicity 4, and the implicit degree of $\mathbf{P}(s, t)$ is 4. One can compute a μ-basis as

$$
\begin{aligned}
\mathbf{p} &= [-8s^3 + 11s^2 - 4s + 4, 5s^3 - 6s^2 + 8s - 4, 3s^3 - 5s^2 - 4s, 4s^3 + s^2 + 2],\\
\mathbf{q} &= [-229530ts - 50278t + 139288s^2 - 174717s + 194136,\\
&\quad 131160ts + 155206t - 87055s^2 + 85766s - 194136,\\
&\quad 65580ts + 104928t - 52233s^2 + 88951s,\\
&\quad 131160ts + 100556t - 69644s^2 - 58603s + 97068],
\end{aligned}
$$

$$\begin{aligned}\mathbf{r} = [&-1344390ts^2 + 34075368ts - 22657890t - 5710808s^3 - 181563s^2\\&- 23392736s - 4984080, 1344390ts^2 - 25195836ts + 10711400t\\&+ 3569255s^3 + 1074194s^2 + 18408656s + 4984080,\\&1344390ts^2 - 17483628ts - 11946490t + 2141553s^3\\&- 892631s^2 + 4984080s, -11391246ts + 6590790t\\&+ 2855404s^3 + 6075203s^2 + 9704572s - 2492040].\end{aligned}$$

Since the 2×2 minors of the matrix with columns $\mathbf{p}$, $\mathbf{q}$ and $\mathbf{r}$ vanish simultaneously at $(0, 0)$, the base point $(0, 0)$ is not a local complete intersection. In fact, the generator $F(x, y, z)$ of $\langle p, q, r\rangle \bigcap \mathbb{R}[x, y, z]$ is not the implicit equation of $\mathbf{P}(s, t)$ (rather, it is the implicit equation multiplied by an extraneous factor). To get the exact implicit equation, we proceed with **Steps 5** and **6**. We compute a Gröbner basis for $J : g$ under a monomial order such that s is greater than any monomial in x, y, z. Then the polynomial in the Gröbner basis which involves only x, y, z is the implicit equation of $\mathbf{P}(s, t)$:

$$\begin{aligned}F(x, y, z) = {}&35836x^4 - 12848x^3y + 678x^2y^2 - 23036xy^3 + 11804y^4\\&- 58602x^3z + 41602x^2yz + 5280xy^2z - 5900y^3z + 26134x^2z^2\\&- 60272xyz^2 + 18146y^2z^2 + 3462xz^3 + 14158yz^3 + 3558z^4\\&+ 53371x^3 - 36329x^2y - 66840xy^2 + 44040y^3 - 49383x^2z\\&+ 84030xyz - 22648y^2z - 2855xz^2 + 10799yz^2 - 9813z^3\\&+ 6028x^2 - 85025xy + 60041y^2 + 23239xz - 13453yz + 18806z^2\\&- 27627x + 33238y - 7676z + 7028 = 0.\end{aligned}$$

The total computation time was 47 ms. However, it took 843 ms to compute the Gröbner basis of I'.

5. Conclusions and problems for further research

In this paper, we generalize the notion of a μ-basis to an arbitrary rational parametric surface. We show that the μ-basis of any rational surface always exists, the geometric significance of which is that any rational surface can be expressed as the intersection of three moving planes without extraneous factors! We also show that the μ-basis serves as a basis of the moving plane module of the rational surface. The relationship of the μ-basis and the moving surface ideal is also discussed. Based on the relationship, a new technique for computing the implicit equation of a rational surface is presented. Examples indicate that the new algorithm may be more efficient than the algorithm based on direct computation of a Gröbner basis of the moving surface ideal.

However, there are still some interesting problems worthy of further research. We list them below.

- Is there a more efficient method for computing μ-bases, especially minimal μ-bases? Currently, we rely on syzygy module computations.
- What can be said about the degrees of the polynomials in a minimal μ-basis?

- Is there a more efficient method for deriving the implicit equation from a minimal μ-basis? Right now, we have to compute a Gröbner basis of the ideal $\langle p, q, r\rangle$.
- We conjecture in Remark 4.1 that the minimal N such that $g^N F \in \langle p, q, r\rangle \cap \mathbb{R}[s]$ satisfies $N \le m_b - 1$. It would be nice to have a proof or counterexample.
- Do μ-bases have other applications? For example, can we use a minimal μ-basis to compute the singular locus of a rational surface?
- It is an interesting problem to analyze the complexity of the algorithm and compare it with a direct Gröbner basis computation.
- In the curve case, the resultant of a μ-basis gives the implicit equation. It this true in the surface case? In Example 2.2, we saw that the Steiner surface has a minimal μ-basis given by

  $$p = st\,y + (1+s^2)z - 2s, \qquad q = (1+t^2)y + st\,z - 2t, \qquad r = x - sy.$$

  Using the classical multivariate resultant, one can compute that

  $$\operatorname{Res}(p, q, r) = y^4 F(x, y, z),$$

  where $F(x, y, z) = 0$ is the implicit equation of the Steiner surface. The extraneous factor y^4 is mysterious but may be related to the failure of the μ-basis to be a basis of the homogenized syzygy module. More work is needed to understand this extraneous factor.
- In the surface case, the resultant $\operatorname{Res}(dx - a, dy - b, dz - c)$ vanishes identically when there are base points. However, the resultant $\operatorname{Res}(p, q, r)$ of a μ-basis need not vanish identically in this situation. A preliminary analysis suggests the following:

  (1) When a finite base point blows up to a line lying on the surface, the resultant of the μ-basis is unaffected. Furthermore, this case occurs if and only if the base point is a local complete intersection.

  (2) When a finite base point blows up to a plane curve lying on the surface (but on not a line), the resultant of the μ-basis acquires an extraneous factor consisting of the equation of the plane to some (currently unknown) power.

  (3) When a finite base point blows up to a space curve lying on the surface (but not on a plane), the resultant of the μ-basis vanishes identically.

  We do not yet understand how base points at infinity affect $\operatorname{Res}(p, q, r)$.

Acknowledgements

The first author is supported by the Outstanding Youth Grant of NSF of China (No. 60225002), 973 Program on Mathematical Mechanics and its Application in Information (No. 2004CB318006) and the TRAPOYT in Higher Education Institute of MOE of China. The second author would like to thank Winfried Bruns and Jürgen Herzog for help with the proof of Proposition 2.1. The authors are also grateful to the reviewers for their helpful comments.

Appendix

The proof of Proposition 2.1 uses standard results and techniques in commutative algebra. We include a proof for the convenience of readers in the geometric modeling community who wish to learn more commutative algebra.

Proof. Let F be a field. We will prove the more general result that given polynomials $f_1, \ldots, f_k \in R = F[s,t]$, the syzygy module $\mathrm{syz}(f_1, \ldots, f_k)$ is a free module.

A finitely generated R-module M is said to be *projective* if there is another finitely generated R-module N such that there is an R-module isomorphism

$$M \oplus N \simeq R^s, \qquad \text{for some } s \geq 1.$$

See Cox et al. (1998a, p. 230) and Eisenbud (1995, p. 615) for more background on projective modules.

The Quillen–Suslin Theorem asserts every projective module over a polynomial ring is free. This result was conjectured by Serre in 1955 and, in the case of two variables considered here, was proved by Seshadri in 1958. Quillen and Suslin independently showed that Serre's conjecture is true for n variables in 1976 see Cox et al. (1998a, p. 231).

Hence it suffices to prove that $\mathrm{syz}(f_1, \ldots, f_k)$ is projective. For this, we need to discuss local rings. Given a point $p \in F^2$, the *local ring* of R at p is defined by

$$R_p = \left\{ \frac{f}{g} \,\middle|\, f, g \in R,\ g(p) \neq 0 \right\}.$$

Then define the *local syzygy module* by

$$\mathrm{syz}_p(f_1, \ldots, f_k) = \{(h_1, \ldots, h_k) \in R_p^k \mid h_1 f_1 + \cdots + h_k f_k = 0\}.$$

This is now a submodule of R_p^k. By Eisenbud (1995, Ex. 4.11 on p. 136), $\mathrm{syz}(f_1, \ldots, f_k)$ is projective if and only if $\mathrm{syz}_p(f_1, \ldots, f_k)$ is free for all $p \in F^2$. (In general, given an R-module M, one can define its *localization* M_p. Then one says that M is *locally free* if all of its localizations are free. The above exercise from Eisenbud asserts that if M is finitely generated, then M locally free if and only if it is projective.)

It follows that we need only prove that $\mathrm{syz}_p(f_1, \ldots, f_k)$ is free for all $p \in F^2$. For this, we use the ideal

$$I_p = \langle f_1, \ldots, f_k \rangle = \{h_1 f_1 + \cdots + h_k f_k \mid h_1, \ldots, h_k \in R_p\} \subset R_p.$$

We first dispose of two easy cases:

- If $I_p = \{0\}$, then every $f_i = 0$, in which case $\mathrm{syz}_p(f_1, \ldots, f_k) = R_p^k$ is free.
- If $I_p = R_p$, then Cox et al. (1998a, Ex. 6(b) on p. 231) implies that $\mathrm{syz}_p(f_1, \ldots, f_k)$ is projective. But over a local ring, every projective module is free by Cox et al. (1998a, Theorem (4.13) on p. 231).

Hence we may assume that $\{0\} \neq I_p \neq R_p$.

Every finitely generated R_p-module M_p has a minimal free resolution

$$\cdots \to R_p^c \to R_p^b \to R_p^a \to M_p \to 0.$$

Minimal means that the map $R_p^a \to M_p$ is determined by a minimal set of generators of M_p, the map $R_p^b \to R_p^a$ is determined by a minimal set of generators of the syzygies on the minimal generators, and so on. Free resolutions are discussed in Cox et al. (1998a, Chapter 6, Section 1), and minimal free resolutions over local rings are discussed in Eisenbud (1995, Lemma 19.4 on p. 473).

Suppose for the moment that the R_p-module R_p/I_p has a minimal resolution of the form

$$0 \to R_p^c \to R_p^b \to R_p \to R_p/I_p \to 0. \tag{5.1}$$

Here, the map $R_p \to R_p/I_p$ uses the minimal generator of R_p/I_p given by the coset of 1 in R_p/I_p, $R_p^b \to R_p$ comes from minimal generators of I_p, and $R_p^c \to R_p^b$ comes from minimal generators on the syzygies on the minimal generators of I_p. The fact that the resolution ends at R^c means that the syzygies on the minimal generators of I_p are free. By Cox et al. (1998a, Ex. 6(a) on p. 231), it follows that the syzygies on any set of generators of I_p are projective and hence free since we are working over a local ring. Thus $\mathrm{syz}_p(f_1, \ldots, f_k)$ is free provided we can prove the existence of a free resolution of the form (5.1).

We will prove this using the *Auslander–Buchsbaum formula*, which computes the number of free modules in the minimal free resolution. If the free resolution has N nonzero free modules, then we say that its *projective dimension* is $N - 1$. For example, in (5.1), we have $N = 3$ if $R_p^c \neq \{0\}$, and $N \leq 3$ in any case. In this language, proving (5.1) means showing that R_p/I_p has projective dimension ≤ 2.

According to Eisenbud (1995, Theorem 19.9 on p. 475), the Auslander–Buchsbaum formula for the projective dimension of R_p/I_p is

$$\text{projective dimension} = \mathrm{depth}(\mathfrak{m}_p, R_p) - \mathrm{depth}(\mathfrak{m}_p, R_p/I_p), \tag{5.2}$$

where

$$\mathfrak{m}_p = \{h \in R_p \mid h(p) = 0\}$$

is the unique maximal ideal of R_p.

In general, depth is a sophisticated concept, but for a Cohen–Macaulay ring, depth is the same as codimension by Eisenbud (1995, p. 452), and by Eisenbud (1995, Proposition 18.9 on p. 452), every polynomial ring is Cohen–Macaulay. Then

$$\mathrm{depth}(\mathfrak{m}_p, R_p)\mathrm{codim}(\mathfrak{m}_p, R_p) = 2, \tag{5.3}$$

where the last equality follows since $\mathfrak{m}_p$ defines the point p and R_p is a two-dimensional local ring (since $Rk[s, t]$ has two variables).

Combining (5.2) and (5.3), we obtain

$$\begin{aligned} \text{projective dimension} &= \mathrm{depth}(\mathfrak{m}_p, R_p) - \mathrm{depth}(\mathfrak{m}_p, R_p/I_p) \\ &\leq \mathrm{depth}(\mathfrak{m}_p, R_p) \\ &= \mathrm{codim}(\mathfrak{m}_p, R_p) = 2. \end{aligned}$$

As noted above, this proves the existence of (5.1) and completes the proof of the theorem. □

Finally, we should remark that Proposition 2.1 is false in three variables. If $R = F[s, t, u]$, then it is easy to show that the syzygy module

$$\mathrm{syz}(s, t, u) \subset R^3$$

has minimal generators given by

$$(t, -s, 0),\ (u, 0, -s),\ (0, u, -t).$$

If the syzygy module were free, then there would be no nontrivial syzygies on the minimal generators. Thus

$$u(t, -s, 0) - t(u, 0, -s) + s(0, u, -t) = (0, 0, 0)$$

proves that $\mathrm{syz}(s, t, u)$ is not free over $R = k[s, t, u]$.

References

Busé, L., Cox, D., D'Andrea, C., 2003. Implicitization of surfaces in $\mathbb{P}^2$ in the presence of base points. J. Algebra Appl. 2, 189–214.

Bruns, W., Herzog, J., 1993. Cohen–Macaulay Rings. Cambridge University Press, Cambridge.

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

Chen, F., Sederberg, T.W., 2002. A new implicit representation of a planar rational curve with high order singularity. Comput. Aided Geom. Design 19, 151–167.

Chen, F., 2003. Reparametrization of a rational ruled surface using the μ-basis. Comput. Aided Geom. Design 20, 11–17.

Chen, F., Wang, W., 2003a. Revisiting the μ-basis of a rational ruled surface. J. Symbolic Comput. 36, 699–716.

Chen, F., Wang, W., 2003b. The μ-basis of a planar rational curve-properties and computation. Graphical Models 65, 368–381.

Chen, F., Wang, W., 2003c. Computing the singular points of a planar rational curve using the μ-basis, preprint.

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.

Cox, D., Goldman, R., Zhang, M., 2000. On the validity of implicitization by moving quadrics for rational surfaces with no base points. J. Symbolic Comput. 29, 419–440.

Cox, D., 2004. Curves, surfaces and syzygies. In: Algebraic Geometry and Geometric Modeling. In: Contemporary Mathematics, AMS, Providence, RI, pp. 131–150.

Eisenbud, D., 1995. Commutative Algebra, with a View Toward Algebraic Geometry. Springer-Verlag, New York.

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

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., Goldman, R., Du, H., 1997. Implicitizing rational curves by the method of moving algebraic curves. J. Symbolic Comput. 23, 153–175.

Zhang, M., Chionh, E., Goldman, R., 1999. On a relationship between the moving line and moving conic coefficient matrices. Comput. Aided Geom. Design 16, 517–527.

Zheng, J., Sederberg, T.W., 2001. A direct approach to computing the μ-basis of planar rational curves. J. Symbolic Comput. 31, 619–629.