Computing μ-Bases of Rational Curves and Surfaces Using Polynomial Matrix Factorization

Jiansong Deng Falai Chen Liyong Shen
Department of Mathematics
University of Science and Technology of China
Hefei, Anhui 230026, P. R. of China
dengjs@ustc.edu.cn,chenfl@ustc.edu.cn

ABSTRACT

The μ-bases of rational curves/surfaces are newly developed tools which play an important role in connecting parametric forms and implicit forms of the rational curves/surfaces. They provide efficient algorithms to implicitize rational curves/surfaces as well as algorithms to compute singular points of rational curves and to reparametrize rational ruled surfaces. In this paper, we present an efficient algorithm to compute the μ-basis of a rational curve/surface by using polynomial matrix factorization followed by a technique similar to Gaussian elimination. The algorithm is shown superior than previous algorithms to compute the μ-basis of a rational curve, and it is the only known algorithm that can rigorously compute the μ-basis of a general rational surface. We present some examples to illustrate the algorithm.

Categories and Subject Descriptors

I.1.2 [**Symbolic and Algebraic Manipulation**]: Algorithms—*Algebraic algorithms*; I.3.5 [**Computer Graphics**]: Computational Geometry and Object Modeling—*Curve, surface, solid, and object representations*

General Terms

Algorithms

Keywords

μ-basis, syzygy module, implicitization, primitive factorization algorithm, Hermite form, GCD extraction algorithm

1. INTRODUCTION

The μ-basis was first introduced in [9] to provide a compact representation for the implicit equation of a rational parametric curve. Then it was generalized by one of the present authors to general rational surfaces [1, 5, 6]. The μ-basis can be used not only to recover the parametric equation of a rational curve/surface but also to derive the implicit equation of the rational curve/surface. Thus it provides a connection between the parametric form and the implicit form of a curve/surface. Furthermore, the μ-basis was successfully applied in reparametrizing a rational ruled surface [4], in computing the singular points of a rational curve [7] and in finding more compact representation for the implicit equation of a rational curve with high order of singularities [2].

There are several methods to compute the μ-basis of a rational curve. The first method is based on undetermined coefficients by solving linear system of equations [14]. This method needs $O(n^3)$ arithmetic operations, where n is the degree of the curve, and it is a trial-and-error approach. The second method was developed by Zheng and Sederberg [18], and it is similar to the Buchberger's algorithm for computing the Gröbner basis of a module. The computational cost of the method is about $\frac{81}{4}n^2 + O(n)$ multiplications in generic case. In [3], Chen and Wang applied vector elimination technique to improve the efficiency of the second algorithm by a factor of two.

For a rational ruled surface, an efficient algorithm similar to curve case was developed to compute the μ-basis [1]. However, we do not have a rigorous algorithm to compute the μ-basis of a general rational surface so far. Currently, we use the Gröbner basis technique to compute a generator for the syzygy module of the rational surface, and then try to find the μ-basis by forming linear combinations of the elements in the generator. This is totally a non-automatic approach and fails in most circumstances.

In this paper we apply the theory of polynomial matrices developed by researchers in linear systems [11, 12, 13] to the computation of a μ-basis. Using some polynomial matrix operations, such as primitive factorization and GCD extraction, we are able to compute a μ-basis of a rational curve/surface rigorously. The computed μ-basis is further simplified by lowering its degree using vector elimination technique [3]. For curve case, a μ-basis can be computed in $\frac{33}{4}n^2 + O(n)$ operations, which is superior than any existing algorithms.

The organization of the paper is as follows. In Section 2, some preliminary knowledge about the μ-basis of a rational curve or surface is introduced. In Section 3, some basic concepts and results in the theory of polynomial matrices are reviewed, including the primitive factorization algorithm, Hermite form, and GCD extraction algorithm. Sections 4 and 5 apply the results of Section 3 to the computation of the μ-basis of a rational curve and surface respectively. Some examples are illustrated to demonstrate the detailed process of the algorithm. We end the paper with some conclusions and future works in Section 6.

2. μ-BASES OF RATIONAL CURVES AND SURFACES

Throughout the paper, we work over the field K of real numbers or rational numbers. $K[x_1, \ldots, x_k] = K[\mathbf{x}]$ and $K(\mathbf{x})$ are the polynomial ring and the rational function field, respectively, in variables $\mathbf{x} = (x_1, \ldots, x_k)$ with coefficients in K. $K^{m\times l}[\mathbf{x}]$ denotes the set of $m \times l$ matrices with entries in $K[\mathbf{x}]$. If $m = 1$, we write it in $K^l[\mathbf{x}]$ for short.

For any $F := (\mathbf{f}_1, \ldots, \mathbf{f}_l) \in K^{m\times l}[\mathbf{x}]$, the set

$$\mathrm{Syz}(F) := \left\{(h_1, \ldots, h_l) \in K^l[\mathbf{x}] \,\Big|\, \sum_{i=1}^{l} h_i \mathbf{f}_i \equiv \mathbf{0}\right\}$$

is a module over $K[\mathbf{x}]$, called a *syzygy module* [8]. If we can find a generating set $\{\mathbf{b}_1, \ldots, \mathbf{b}_m\}$, $\mathbf{b}_i \in K^l[\mathbf{x}]$, of a syzygy module, then the matrix $M = (\mathbf{b}_1, \ldots, \mathbf{b}_m)$ is called the *generating matrix* of the syzygy module. It follows that $FM = \mathbf{0}$.

A generating set of a module over $K[\mathbf{x}]$ is called a *basis* if the elements in the generating set are $K[\mathbf{x}]$-linearly independent. If a module has a basis, then it is called a *free module*. Conditions for a syzygy module being free will be given in the next section. We just mention that, if $k = 1$ or 2, i.e., we are working with univariate or bivariate polynomials, then the syzygy module is free.

Now we review the definitions of μ-bases of a planar rational curve [3] and a rational surface [6]. Consistent with the notation in [6, 3, 5, 1, 9], we use t and s, t as the variable names for univariate and bivariate cases, respectively.

Definition 1 ([9]). *Given a planar rational curve of degree n in homogeneous form:*

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

where $\max(\deg_t a, \deg_t b, \deg_t c) = n$ *and* $\gcd(a, b, c) = 1$. *The syzygy module* $\mathrm{Syz}(a, b, c)$ *has a basis* $\{\mathbf{p}(t), \mathbf{q}(t)\} \subset K^3[t]$ *with degree μ and $n - \mu$ respectively, where* $\mu \leqslant \frac{n}{2}$. $\{\mathbf{p}(t), \mathbf{q}(t)\}$ *is called a μ-basis of the rational curve* $\mathbf{P}(t)$.

Remark 1 A μ-basis has the following properties [3]:

(1) The μ-basis has the lowest possible degree among all the bases of the syzygy module $\mathrm{Syz}(a, b, c)$.

(2) The parametric equation of $\mathbf{P}(t)$ can be recovered from a μ-basis. In fact, for any basis $\mathbf{p}, \mathbf{q}$ of $\mathrm{Syz}(a, b, c)$, we have

$$[\mathbf{p}, \mathbf{q}] = \kappa(a, b, c)$$

for some nonzero constant κ in K.

(3) A basis $\{\mathbf{p}(t), \mathbf{q}(t)\}$ of $\mathrm{Syz}(a, b, c)$ is a μ-basis if and only if $\deg_t(\mathbf{p}(t)) + \deg_t(\mathbf{q}(t)) = n$, and if and only if $\mathrm{LCV}(\mathbf{p}(t))$ and $\mathrm{LCV}(\mathbf{q}(t))$ are linearly independent. Here $\mathrm{LCV}(\mathbf{p}(t))$ is the leading coefficient vector of vector polynomial $\mathbf{p}(t)$ which is defined by $\mathrm{LCV}(\mathbf{p}(t)) := (p_{1\mu}, p_{2\mu}, p_{3\mu})$ if we write $\mathbf{p}(t) = (p_{1\mu}, p_{2\mu}, p_{3\mu})t^\mu + \ldots + (p_{10}, p_{20}, p_{30})$. $\mathrm{LCV}(\mathbf{q}(t))$ is defined similarly.

(4) The implicit equation of $\mathbf{P}(t)$ can be obtained by taking the resultant of $\mathbf{p} \cdot \mathbf{v}$ and $\mathbf{q} \cdot \mathbf{v}$ with respect to t, where $\mathbf{v} = (x, y, 1)$.

Definition 2. *Given a rational parametric surface in homogeneous form:*

$$\mathbf{P}(s, t) := (a(s, t), b(s, t), c(s, t), d(s, t)) \in K^4[s, t],$$

where a, b, c, d are relatively prime. A basis $\{\mathbf{p}(s, t),\ \mathbf{q}(s, t),\ \mathbf{r}(s, t)\} \subset K^4[t]$ *of the syzygy module* $\mathrm{Syz}(a, b, c, d)$ *is called a μ-basis of the surface* $\mathbf{P}(s, t)$. *If in addition,* $\mathbf{p}$, $\mathbf{q}$, $\mathbf{r}$ *satisfy*

1. *among all the bases of* $\mathrm{Syz}(a, b, c, d)$, $\deg_t \mathbf{p} + \deg_t \mathbf{q} + \deg_t \mathbf{r}$ *is smallest, and*
2. *among all the bases of* $\mathrm{Syz}(a, b, c, d)$ *which satisfy item 1,* $\deg_s \mathbf{p} + \deg_s \mathbf{q} + \deg_s \mathbf{r}$ *is smallest,*

then $\{\mathbf{p},\ \mathbf{q},\ \mathbf{r}\}$ *is called a minimal μ-basis of* $\mathbf{P}(s, t)$.

Remark 2 The existence of μ-basis of a rational surface was proved in [6]. It can be also seen from Corollary 3.2 in the next section. However, except for parametrizations with no base points, standard computational methods only give generating sets for the syzygy module. The main task of the current paper is to describe how to compute a basis of this module, i.e., a μ-basis.

Remark 3 From [6], the parametric equation of a rational surface can be recovered by the outer-product of a μ-basis, i.e.,

$$[\mathbf{p}, \mathbf{q}, \mathbf{r}] = \kappa(a, b, c, d)$$

for some nonzero constant κ in K. Here

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

On the other hand, the implicit equation of a rational surface can be obtained by computing the Gröbner basis for the ideal $\langle \mathbf{p}\cdot\mathbf{v}, \mathbf{q}\cdot\mathbf{v}, \mathbf{r}\cdot\mathbf{v}\rangle : g^N$, where $\mathbf{v} = (x, y, z, 1)$, $g \in K[s]$ is defined by $\langle a, b, c, d\rangle \cap K[s] = \langle g\rangle$ and N is a sufficiently large integer. Though it is relatively more efficient than the method by direct computation of Gröbner basis of the ideal $\langle dx - a, dy - b, dz - c, dw - 1\rangle \cap K[x, y, z, s, t]$, finding more efficient method to derive the implicit representation from a μ-basis is a problem worthy of further investigation.

3. PRELIMINARY RESULTS IN THE THEORY OF POLYNOMIAL MATRICES

Given a matrix M in $K^{m\times m}[\mathbf{x}]$, its determinant $\det M$ is a polynomial in $K[\mathbf{x}]$. If the polynomial is nonzero, the matrix M is nonsingular, otherwise it is singular. If the determinant $\det M$ is a nonzero constant in K, then we called M a *unimodular matrix*.

A matrix $M \in K^{m\times l}[\mathbf{x}]$ is of rank r if there exists at least one minor of order r being nonzero polynomial, and all the minors of order $r+1$ being zero polynomials. We use $\mathrm{rank}\, M$ to denote the rank of M. If $\mathrm{rank}\, M = \min(l, m)$, we call the matrix full-rank.

For a nonsingular matrix $M \in K^{m\times m}[\mathbf{x}]$, we can calculate its inverse matrix, whose entries are in $K(\mathbf{x})$. The inverse matrix is also in $K^{m\times m}[\mathbf{x}]$ if and only if M is unimodular.

Definition 3. *Let $F \in K^{m\times l}[\mathbf{x}]$ with $m \leqslant l$. Then F is said to be :*

1. *minor left prime (MLP) if all $m \times m$ minors of F are coprime.*
2. *factor left prime (FLP) if any polynomial decomposition $F = F_1 F_2$ in which F_1 is square, then F_1 is a unimodular matrix, i.e.,* $\det F_1 = k_0 \in K\backslash\{0\}$.

Minor right prime (MRP) and factor right prime (FRP) can be similarly defined.

In [16], the authors proved that for $k = 1, 2$, MLP $\equiv$ FLP, MRP $\equiv$ FRP; for $k \geqslant 3$, MLP $\not\equiv$ FLP, MRP $\not\equiv$ FRP; and for all $k \geqslant 1$, MLP $\Rightarrow$ FLP, MRP $\Rightarrow$ FRP. Here k is the number of variables.

Definition 4. *Given two polynomial matrices A, B with the same number of rows (columns), where entries are in $K[\mathbf{x}]$, we call them to be left (right) coprime if whenever there are two matrices $\tilde{A}$, $\tilde{B}$ and a square polynomial matrix C, where entries of all the three matrices are in $K[\mathbf{x}]$ such that*

$$A = C\tilde{A},\ B = C\tilde{B} \qquad (A = \tilde{A}C,\ B = \tilde{B}C),$$

then C is a unimodular matrix.

Definition 5. *Given two polynomial matrices A, B with the same number of rows (columns), where entries are in $K[\mathbf{x}]$, a square polynomial matrix D is their greatest common left (right) divisor (GCL(R)D) if there exist two left (right) coprime polynomial matrices $\tilde{A}, \tilde{B}$ such that*

$$A = D\tilde{A},\ B = D\tilde{B} \qquad (A = \tilde{A}D,\ B = \tilde{B}D).$$

The following theorem due to Lin [12] describes when a syzygy module is free, i.e., it has a basis.

Theorem 3.1. *[12] Let $F = [-\tilde{N}, \tilde{D}] \in K^{m\times l}[\mathbf{x}]$ be of rank m, with $l > m$, $\tilde{D} \in K^{m\times m}[\mathbf{x}]$ being nonsingular, and $r = l - m$. Then* $\mathrm{Syz}(F)$ *has a generating matrix of dimension $l \times r$ (i.e.,* $\mathrm{Syz}(F)$ *is free) if and only if there exists an MRP matrix $H \in K^{l\times r}[\mathbf{x}]$ such that $FH = \mathbf{0}_{m\times r}$. Furthermore, H is the generating matrix.*

Based on Theorem 3.1, Lin derived the following corollary, the proof of which is constructive. We copy its proof to help the reader to more easily understand the algorithm in Sections 4 and 5.

Corollary 3.2. *Let $F = [-\tilde{N}, \tilde{D}] \in K^{m\times l}[s,t]$ be of rank m, with $l > m$, $\tilde{D} \in K^{m\times m}[\mathbf{x}]$ being nonsingular, and $r = l - m$. Then, there exists a generating matrix $H \in K^{l\times r}[s,t]$ of* $\mathrm{Syz}(F)$.

Proof. Associate F with a rational matrix $P = \tilde{D}^{-1}\tilde{N}$. By a well-known result in bivariate polynomial matrix theory [11, 13], P has a right matrix fraction description (MFD) $P = ND^{-1}$, where N and D, whose entries are in $K[s,t]$, are right coprime. Let $H = (D^T, N^T)^T \in K^{l\times r}[s,t]$, which is FRP, hence MRP. Clearly, $P = \tilde{D}^{-1}\tilde{N} = ND^{-1}$ gives rise to $FH = 0$. By Theorem 3.1, H is a generating matrix of $\mathrm{Syz}(F)$. $\square$

According to the proof of Corollary 3.2, to find a basis of $\mathrm{Syz}(F)$, we need to get the MFD of a rational matrix. For any rational matrix M, it is easy to write it into $M = AB^{-1}$, where A, B are polynomial matrices. Hence it is important on how to extract GCRDs from A and B. The approach consists of some important algorithms in the theory of bivariate polynomial matrices, including primitive factorization, Hermite form, and GCD extraction. We will review them in the following subsections.

3.1 Primitive factorization algorithm

For a bivariate polynomial $a(s,t) \in K[s][t]$, we write it into the following form:

$$a(s,t) = \sum_{i=0}^{n} a_i(s) t^i,$$

where $a_i(s) \in K[s]$. The *content* of $a(s,t)$ with respect to $K[s][t]$ is the gcd of the a_i's.

Suppose $p(s)$ is irreducible in $K[s]$. Then

$$a(s,t) \pmod{p(s)} = 0$$

(i.e., $p(s) | a_i(s)$, $i = 0, \ldots, n$), or

$$a(s,t) \pmod{p(s)} = \sum_{i=0}^{n_1} \alpha_i(s) t^i,$$

where $\alpha_i(s) \in K[s]$ with $\deg_s \alpha_i(s) < \deg_s p(s)$, $n_1 \leqslant n$, and $\alpha_{n_1}(s) \not\equiv 0$. The α_i's can be obtained by means of the Euclidean division algorithm.

In [13] a primitive factorization (PF) algorithm of bivariate polynomial matrices is proposed, which extracts the content of a full-rank matrix with entries in the ring $K[s,t]$ of bivariate polynomials over some algebraically closed field K. [11] eliminates the restriction on K, such that we can do the factorization over the real field or even the field of rational numbers, provided the coefficients start out in the same field. We describe the PF algorithm as follows. Further details can be found in [11].

Algorithm 1 (PF Algorithm).

Input F: an $m\times l$ full-rank matrix with entries in $K[s,t]$, $m \leqslant l$.

Output L, R: $m \times m$ and $m \times l$ matrices, respectively, with entries in $K[s,t]$, such that $F = LR$ and $\det L = g(s)$, where $g(s) \in K[s]$ is the content of the greatest common divisor (GCD) of the set of $m \times m$ minors of F.

Step

1. Calculate the GCD of the set of $m \times m$ minors of F. $g(s)$ is its content as a polynomial in t.
2. Let L be an identity matrix of order m, and $R = F$. Factorize $g(s)$ into a list of irreducible factors in $K[s]$. For every factor $p(s)$ do the following steps:
   (a) Set the current row and column indices i, j to be 1. $\bar{R} = R \pmod{p(s)}$.
   (b) Among rows from i to m in $\bar{R}$, if there exists a row with all entries zeros, say row i_0, then

   $$D_0 = \mathrm{diag}(1, \ldots, 1, \overset{i_0}{p(s)}, 1, \ldots, 1)$$

   is a left divisor of F, and we let $L \leftarrow LD_0$, and $R \leftarrow D_0^{-1}R$. Continue Step 2 for the next factor. If no row of $\bar{R}$ from rows i to m is zero, then go to the next sub-step.

(c) From columns j to l, find the first column (say column j_0) with at least one nonzero entry from rows i to m. Set $j \leftarrow j_0$.

(d) In the column j, from rows i to m, find the entry with the smallest degree of t, say i_1. Interchange row i and i_1 of $\bar{R}$. This is equivalent to premultiplying $\bar{R}$ with matrix D_1, where D_1 comes from I_m by interchanging rows i and i_0. Let $L \leftarrow LD_1$, $R \leftarrow D_1^{-1}R = D_1 R$.

(e) Suppose the entries in column j to be

$$\big(*, \ldots, *, a_i(s,t), \ldots, a_m(s,t)\big)^T.$$

The leading coefficients of $a_i(s,t), \ldots, a_m(s,t)$ in t are $b_i(s), \ldots, b_m(s)$. Since $b_i(s)$ and $p(s)$ are relatively prime, by Euclidean algorithm we can find $x(s)$ and $y(s)$ in $K[s]$ such that

$$x(s)b_i(s) = 1 - y(s)p(s).$$

Let $a_i^*(s,t) = x(z)a_i(s,t) \pmod{p(s)}$.[1] There exist $q_k(s,t)$ and $r_k(s,t)$ in $K[s,t]$ such that

$$a_k(s,t) = q_k(s,t)a_i^*(s,t) + r_k(s,t),$$

$k = i+1, \ldots, m$, where

$$\deg_t r_k(s,t) < \deg_t a_i^*(s,t), \text{ or } r_k(s,t) \equiv 0.$$

Then for $k = i+1, \ldots, m$, we add to row k with row i multiplied by $-x(s)q_k(s,t)$. This is equivalents to premultiplying $\bar{R}$ with the matrix $D_3 = \operatorname{diag}(I_{i-1}, E)$, where

$$E = \begin{pmatrix} 1 & & & & \\ -xq_{i+1} & 1 & & & \\ -xq_{i+2} & & 1 & & \\ \vdots & & & \ddots & \\ -xq_m & & & & 1 \end{pmatrix}.$$

Let $L \leftarrow LD_3^{-1}$, $R \leftarrow D_3 R$. Then the j column of $\bar{R}$ is with the form

$$\big(*, \ldots, *, a_i(s,t), r_{i+1}(s,t), \ldots, r_m(s,t)\big)^T.$$

Let $\bar{R} \leftarrow \bar{R} \bmod p(z)$.

If $r_{i+1}(s,t) \equiv \cdots \equiv r_m(s,t) \equiv 0$, then $j \leftarrow j+1$, $i \leftarrow i+1$, and go to sub-step (b). Otherwise, repeat the current sub-step (e).

□

Remark 4 There is of course a similar primitive factorization algorithm for $m \geqslant l$, where an $l \times l$ matrix is extracted on the right. We denote these two algorithms as the LPF and RPF algorithms with respect to $K[s][t]$, respectively.

Remark 5 The LPF and RPF algorithms terminate after finitely many steps. In fact, the complexity is predictable after given the degree of polynomials in F. For a given F, the factorization is unique up to a unimodular matrix.

3.2 Hermite form

Given a univariate or bivariate $m \times l$ full-rank polynomial matrix F, $m \geqslant l$, we are interested in finding its Hermite form with respect to $K[t]$ or $K[s][t]$. The Hermite form [10, 13] is a matrix $(a_{ij}(t))$ or $(a_{ij}(s,t))$ with $a_{ij} \equiv 0$, $j < i$, and $\deg_t a_{jj} > \deg_t a_{ij}$, $j > i$.

[10] and [13] presented algorithms to compute the Hermite form of a full-rank matrix in univariate case and bivariate case respectively. For univariate case, based on Gaussian elimination technique and Euclid division algorithm, one can find a unimodular matrix U such that $H = UF$ is the Hermite form of F. For bivariate case, the algorithm consists of two steps. First, we work over $K(s)[t]$ to find U with entries in $K(s)[t]$ such that $\tilde{H} = \tilde{U}F$ is a Hermite form with respect to $K(s)[t]$, where $\det \tilde{U} \in K(s)$. Second, let $p_i(s,t)$ be the least common multiple of the denominators in row i of $\tilde{U}$, and $D = \operatorname{diag}(p_1(s,t), \ldots, p_m(s,t))$, $H = D\tilde{H}$ and $U = D\tilde{U}$. Then it follows that $H = UF \in K[s,t]$ is the Hermite form of F with respect to $K[s][t]$, and $\det U \in K[s]$. It is obvious that the two steps can be merged into one by using the pseudo division algorithm for two polynomials.

3.3 GCD extraction algorithm

In [13], a GCD extraction algorithm of bivariate polynomial matrices is presented. We describe it as follows.

Algorithm 2 (GCRD extraction algorithm).

Input A, B: two bivariate polynomial matrices $A(s,t)$ and $B(s,t)$ with the same number of columns, such that (A^T, B^T) is of full rank.

Output D: GCRD of A and B.

Step

1. Use the RPF algorithm with respect to $K[s][t]$ on the right side of $(A^T, B^T)^T$, i.e., find $\bar{A}$, $\bar{B}$ and R_0 such that
$$\begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} \bar{A} \\ \bar{B} \end{pmatrix} R_0,$$
where $\det R_0 \in K[s]$.

2. Find U with entries in $K[s,t]$ and $\det U \in K[s]$ to get the Hermite form of $(\bar{A}^T, \bar{B}^T)^T$, i.e.,
$$U \begin{pmatrix} \bar{A} \\ \bar{B} \end{pmatrix} = \begin{pmatrix} R \\ 0 \end{pmatrix}.$$

3. Use the LPF algorithm to R,
$$R = \bar{R}R^*.$$

Then $D = R^* R_0$ is the GCRD of A and B. □

Remark 6 To save some unnecessary primitive factorization in Step 3, we make a little modification to the above algorithm. In the computation of the Hermite form of a bivariate polynomial matrix, after we get $\tilde{H}$ and $\tilde{U}$, let $q_i(s,t)$ be the least common multiple of the denominators in row i of $\tilde{H}$, then $q_i(s,t)$ is a factor of $p_i(s,t)$. Let $\bar{D} = \operatorname{diag}(q_1(s,t), \ldots, q_m(s,t))$ and $\bar{H} = \bar{D}\tilde{H}$, and take $\bar{H}$ in place of H in Step 3 of the GCD extraction algorithm.

4. COMPUTING μ-BASES OF A RATIONAL CURVE

Suppose we are given a planar rational curve

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

where $a, b, c \in K[t]$ and $\gcd(a,b,c) = 1$. Computing a μ-basis of $\mathbf{P}(t)$ is equivalent to computing a basis of the

[1] Note that $a_i^*(s,t)$ is monic and $\deg_t a_i^*(s,t) = \deg_t a_i(s,t)$.

syzygy module $\mathrm{Syz}(a,b,c)$ with lowest possible degree. We first compute a basis of $\mathrm{Syz}(a,b,c)$ based on the proof of Corollary 3.2.

Set $\tilde{D}=(c)$, $\tilde{N}=(-a,-b)$. Construct a matrix P and compute its MFD:

$$P=\tilde{D}^{-1}\tilde{N}=AB^{-1}.$$

where $A=(-a,-b)$ and $B=\mathrm{diag}(c,c)$. To compute a generating matrix of $\mathrm{Syz}(a,b,c)$, we need to find the GCRD of A and B.

The GCRD extraction algorithm in Section 3.3 is described for bivariate polynomial matrices, but it works also for univariate case with minor modifications. In the univariate case, we do not need to do the primitive factorization in Steps 1 and 3 of Algorithm 2. The key step is to find the Hermite form of matrix

$$\begin{pmatrix} A \\ B \end{pmatrix}=\begin{pmatrix} -a & -b \\ c & 0 \\ 0 & c \end{pmatrix}.$$

Suppose $\gcd(-a,c)=d$, then there exist $\lambda_1,\lambda_2\in K[t]$ such that $\lambda_1(-a)+\lambda_2 c=d$. Assume $\gcd(-bc/d,c)=e$, then there exist $\mu_1,\mu_2\in K[t]$ such that $\mu_1(-bc/d)+\mu_2 c=e$. Finally suppose the quotient and remainder of $\lambda_1 b$ divided by e are k and r. Denote the following matrix as D,

$$\begin{pmatrix} 1 & -k & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & \mu_1 & \mu_2 \\ 0 & c/e & bc/(de) \end{pmatrix}\begin{pmatrix} \lambda_1 & \lambda_2 & 0 \\ c/d & a/d & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Then

$$D\begin{pmatrix} -a & -b \\ c & 0 \\ 0 & c \end{pmatrix}=\begin{pmatrix} d & r \\ 0 & e \\ 0 & 0 \end{pmatrix}$$

is the Hermite form. Hence the GCRD of A and B is

$$R=\begin{pmatrix} d & r \\ 0 & e \end{pmatrix},$$

and the generating matrix of $\mathrm{Syz}(a,b,c)$ is

$$M=\begin{pmatrix} B \\ A \end{pmatrix}R^{-1}=\begin{pmatrix} e & -r \\ 0 & d \\ -a/d & (ar-bd)/c \end{pmatrix}, \quad (1)$$

since $c=de$. The two columns $\tilde{\mathbf{p}}(t),\tilde{\mathbf{q}}(t)$ of matrix M are a basis of the syzygy module $\mathrm{Syz}(a,b,c)$.

Note that the basis obtained so far is possibly of higher degree than a μ-basis. To get the μ-basis, we need reduce the degree of $\tilde{\mathbf{p}}(t),\tilde{\mathbf{q}}(t)$. Suppose $n_2:=\deg(\tilde{\mathbf{q}}(t))\geq n_1:=\deg(\tilde{\mathbf{p}}(t))$ and $n_1+n_2>n$. Then $\mathrm{LCV}(\tilde{\mathbf{p}}(t))$ and $\mathrm{LCV}(\tilde{\mathbf{q}}(t))$ must be linearly dependent (otherwise $\tilde{\mathbf{p}}(t)\times\tilde{\mathbf{q}}(t)\neq k(a,b,c)$), that is, there exists some constant α such that $\mathrm{LCV}(\tilde{\mathbf{q}}(t))=\alpha\,\mathrm{LCV}(\tilde{\mathbf{p}}(t))$. Update $\tilde{\mathbf{q}}(t)$ by $\tilde{\mathbf{q}}(t):=\tilde{\mathbf{q}}(t)-\alpha t^{n_2-n_1}\tilde{\mathbf{p}}(t)$. This process can be continued until $\deg(\tilde{\mathbf{p}}(t))+\deg(\tilde{\mathbf{q}}(t))=n$, i.e., $\tilde{\mathbf{p}(t)},\tilde{\mathbf{q}(t)}$ are a μ-basis. Let us use an example to illustrate the process.

Example 1 Suppose a rational curve is parametrized by

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

Then

$$\lambda_1(t)=1, \qquad \lambda_2(t)=2, \qquad d=1,$$
$$e(t)=t^2+2t+3, \qquad r(t)=5(t+1),$$

and

$$M=\begin{pmatrix} t^2+2t+3 & -5(t+1) \\ 0 & 1 \\ -2t^2-4t-5 & 10t+7 \end{pmatrix}.$$

The column-reduced form of M is

$$M'=\begin{pmatrix} 5(t+3) & -5(t+1) \\ t & 1 \\ -13t-25 & 10t+7 \end{pmatrix}.$$

The two columns of M' are a μ-basis of the rational curve $(a(t),b(t),c(t))$. □

The main computational costs of the μ-basis algorithm lie in computing GCDs of univariate polynomials using Euclidean algorithm and column-reduction of matrix M. One can easily prove that the computational complexity is less than $\frac{33}{4}n^2+O(n)$ multiplications, which is faster than fastest known algorithm [3].

5. COMPUTING μ-BASES OF A RATIONAL SURFACE

To compute a μ-basis of a rational surface, we just follow what we did to compute a μ-basis of a rational curve. Here the main computational complexity comes from the GCRD extraction algorithm. However, since Steps 1 and 3 of Algorithm 2 can't be omitted, it is difficult to write down the generating matrix of the syzygy module explicitly.

Given a rational parametric surface in homogeneous form

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

where $a,b,c,d\in K[s,t]$ and $\gcd(a,b,c,d)=1$. A μ-basis of rational surface $\mathbf{P}(s,t)$ is a basis of the syzygy module $\mathrm{Syz}(a,b,c,d)$.

Set $\tilde{D}=(d)$, $\tilde{N}=(-a,-b,-c)$. Construct a matrix P and compute its MFD:

$$P=\tilde{D}^{-1}\tilde{N}=(-a/d,-b/d,-c/d)=AB^{-1},$$

where $A=(-a,-b,-c)$ and $B=\mathrm{diag}(d,d,d)$. Suppose the GCRD of A and B is G, i.e., there exist $\bar{A},\bar{B}\in K[s,t]$ such that

$$A=\bar{A}G, \quad B=\bar{B}G,$$

where $\bar{A}$ and $\bar{B}$ are right coprime. Then $(\bar{B}^T,\bar{A}^T)^T$ is the generating matrix of $\mathrm{Syz}(a,b,c,d)$, and the three columns $\mathbf{p},\mathbf{q},\mathbf{r}$ of the generating matrix are a μ-basis of the rational surface $\mathbf{P}(s,t)$.

Similar to curve case, the μ-basis obtained may not be a minimal μ-basis. To lower the degree, we proceed as follows.

Rewrite the μ-basis as

$$\mathbf{p}=\sum_{i=0}^{d_p}\mathbf{p}_i(s)t^i,\mathbf{q}=\sum_{i=0}^{d_q}\mathbf{q}_i(s)t^i,\mathbf{r}=\sum_{i=0}^{d_r}\mathbf{r}_i(s)t^i,$$

where $\mathbf{p}_i(s)$, $\mathbf{q}_i(s)$ and $\mathbf{r}_i(s)$ in $K^4[s]$. Without loss of generality, we assume $d_p\geqslant d_q\geqslant d_r$.

Let $\mathbf{m}_p$, $\mathbf{m}_q$, $\mathbf{m}_r\in K^4[s]$ be the leading coefficient vectors of $\mathbf{p}$, $\mathbf{q}$ and $\mathbf{r}$ with respect to t, respectively, i.e., $\mathbf{m}_p(s)=\mathbf{p}_{d_p}(s)$, etc. From the recovery equation of **Remark 3** in Section 2, it is easy to see that $d_p+d_q+d_r=\deg_t(\mathbf{P}(s,t))$ if and only if $\mathbf{m}_p$, $\mathbf{m}_q$ and $\mathbf{m}_r$ are $K[s]$-linearly independent.

Now if $\mathbf{m}_p$, $\mathbf{m}_q$ and $\mathbf{m}_r$ are $K[s]$-linearly independent, then $d_p+d_q+d_r$ reaches minimum and the process is terminated. Otherwise, consider the syzygy module $\mathrm{Syz}(\mathbf{m}_p$, $\mathbf{m}_q$,

$\mathbf{m}_r$), the basis of which can be found based on the results in [12]. Find a vector $\alpha := (\alpha_p, \alpha_q, \alpha_r)$ in the basis of the syzygy module $\mathrm{Syz}(\mathbf{m}_p, \mathbf{m}_q, \mathbf{m}_r)$ such that one of $\alpha_p, \alpha_q, \alpha_r$ is a non-zero constant, if possible. If not, terminate the process. Set $\beta_p = \alpha_p$, $\beta_q = \alpha_q s^{d_p - d_q}$, $\beta_r = \alpha_r s^{d_p - d_r}$ and $\mathbf{u} = \beta_p \mathbf{p} + \beta_q \mathbf{q} + \beta_r \mathbf{r}$. If α_p is a non-zero constant and $\deg_s(\mathbf{u}) < \deg_s(\mathbf{p})$, update $\mathbf{p}$ by $\mathbf{u}$. Otherwise if α_q is a non-zero constant, and $d_p = d_q$ and $\deg_s(\mathbf{u}) < \deg_s(\mathbf{q})$, update $\mathbf{q}$ by $\mathbf{u}$. Otherwise if α_r is a non-zero constant, and $d_p = d_q = d_r$ and $\deg_s(\mathbf{u}) < \deg_s(\mathbf{r})$, update $\mathbf{r}$ by $\mathbf{u}$. This process can be continued until $d_p + d_q + d_r = \deg_t(\mathbf{P}(s,t))$ or one of the above conditions fails to hold.

The next step is to reduce the degree of $\mathbf{p}, \mathbf{q},$ and $\mathbf{r}$ with respect to s while keeping the degree of $\mathbf{p}, \mathbf{q},$ and $\mathbf{r}$ with respect to t unchanged. This can be done by applying the vector elimination technique in [3] to $\mathbf{p}, \mathbf{q},$ and $\mathbf{r}$.

We should note that, while the above process generally reduces the degree of a μ-basis, it doesn't necessarily produce a minimal μ-basis.

Now we present some examples to demonstrate the detailed process of the algorithm.

Example 2 The Steiner surface is defined by $(a, b, c, d) = (2st, 2t, 2s, s^2 + t^2 + 1)$. The matrices A and B are then

$$\begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} -2st & -2t & -2s \\ s^2+t^2+1 & 0 & 0 \\ 0 & s^2+t^2+1 & 0 \\ 0 & 0 & s^2+t^2+1 \end{pmatrix}.$$

The content of the GCD of all the minors of order 3 with respect to $K[s][t]$ is 1, so we skip Step 1 in the GCRD extraction algorithm, i.e., $R_0 = I_3$.

In Step 2 of the GCRD extraction algorithm, we make use of the discussion in Remark 6 of Section 3.3, and obtain

$$R = \begin{pmatrix} (s^2+1)s & s^2+1 & -st \\ 0 & s^2+t^2+1 & 0 \\ 0 & 0 & s^2+t^2+1 \end{pmatrix},$$
$$U = \begin{pmatrix} t/2 & s & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ \frac{s^2+t^2+1}{2s} & t & \frac{t}{s} & 1 \end{pmatrix}.$$

Here $U \in K(s,t)$, but $\notin K[s,t]$. Since $\det(R) = (s^2+1)s(s^2+t^2+1)^2$, its irreducible factor list of the content with respect to t is s^2+1, s. Applying the LPF algorithm in Algorithm 1, we get

$$\bar{R}^{-1} = \begin{pmatrix} -\frac{t^2+1}{s} & \frac{1}{s} & 0 \\ 1 & 0 & 0 \\ -\frac{st}{s^2+1} & 0 & \frac{1}{s^2+1} \end{pmatrix},$$
$$R^* = \begin{pmatrix} -(t^2+1)(s^2+1) & -st^2 & t(t^2+1) \\ (s^2+1)s & s^2+1 & -st \\ -s^2t & -st & t^2+1 \end{pmatrix}.$$

Then the GCRD of A and B is $R^* R_0 = R^*$. Therefore the generating matrix of $\mathrm{Syz}(a,b,c,d)$ is

$$M = \begin{pmatrix} B \\ A \end{pmatrix} (R^*)^{-1} = \begin{pmatrix} -1 & 0 & t \\ s & t^2+1 & 0 \\ 0 & st & s^2+1 \\ 0 & -2t & -2s \end{pmatrix}.$$

The three columns of M gives a μ-basis of the Steiner surface. One can show that it is a minimal μ-basis.

Example 3 Given a bi-quadratic surface defined by

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

The content of the GCD of all the major minors of

$$\begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} -a & -b & -c \\ d & 0 & 0 \\ 0 & d & 0 \\ 0 & 0 & d \end{pmatrix}$$

with respect to $K[s][t]$ is s^2. Then the irreducible factor list is $\{s, s\}$.

In Step 1 of GCRD extraction algorithm, one can compute

$$\begin{aligned} R_0 &= \begin{pmatrix} 1 & 1 & -1 \\ 0 & s & 0 \\ 0 & 0 & s \end{pmatrix}, \\ \bar{A} &= \begin{pmatrix} 2s^2t - 2s^2 - st - t^2 \\ -t(2st + s + t + 1) \\ 2st^2 + 3st - 4s - 2t^2 - 2t \end{pmatrix}^T, \\ \bar{B} &= t(st + 2s + 2t - 2) \begin{pmatrix} -s & 1 & -1 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}. \end{aligned}$$

After Step 2, it follows that

$$R = \begin{pmatrix} 2s(3s^4 + 5s^3 + s^2 - 2s + 2) & \alpha(s,t) & \beta(s,t) \\ 0 & \gamma(s,t) & 0 \\ 0 & 0 & \gamma(s,t) \end{pmatrix},$$

where

$$\begin{aligned} \alpha(s,t) &= -(s+2)(3s^2 - 5s - 4)st, \\ \beta(s,t) &= 12s^4 + 20s^3 + 4s^2 - 8s + 8 \\ &\quad + 5s^4t + 4s^3t - 4s^2t + 12st - 8t, \\ \gamma(s,t) &= t(2s + st + 2t - 2). \end{aligned}$$

The results of the rest steps are omitted since they are a little clumsy to write down. Finally, we obtain a μ-basis for the biquadratic surface as follows:
$\mathbf{p} = \frac{1}{35412} \cdot$

$$\begin{pmatrix} 30440\,ts^4 + 36528\,s^4 + 56037\,s^3t + 98902\,s^3 + 16316\,s^2t \\ \quad + 93930\,s^2 + 52004\,st + 9410\,s + 35412 \\ -35412, \\ -2\,s\left(18264\,s^3 + 49451\,s^2 + 46965\,s + 4705\right), \\ 12176\,s^4 + 18762\,s^3 + 30440\,s^2t - 11887\,s^2 - 4843\,st \\ \quad + 35412\,s + 26002\,t + 17706 \end{pmatrix}$$

$\mathbf{q} = \frac{1}{256176}\cdot$

$$\begin{pmatrix} -46308\,st - 74337\,t^2s^4 - 96066\,ts^4 - 216726\,s^2t \\ \quad - 209666\,s^3t + 59836\,s^2t^2 - 40826\,s^3t^2 - 311720\,st^2 \\ \quad + 92216\,s + 100316\,t - 36272 + 21680\,s^2 - 54752\,s^3 \\ \quad - 22872\,s^4, \\ 4\left(-4534 + 6993\,s + 9703\,s^2 + 2859\,s^3\right) \\ \quad (2\,s + st + 2\,t - 2)\,, \\ 32022\,t\left(3\,s^4 + 5\,s^3 + s^2 - 2\,s + 2\right), \\ -20586\,ts^4 + 22872\,s^4 + 55203\,s^3t + 73812\,s^3 \\ \quad - 74337\,s^2t^2 + 226126\,s^2t + 11240\,s^2 + 107848\,st^2 \\ \quad - 68094\,st - 118252\,s - 155860\,t^2 - 82180\,t - 18136 \end{pmatrix}$$

$$\mathbf{r} = \frac{1}{6}\begin{pmatrix} \left(6\,s^4 + 10\,s^3 + 2\,s^2 - 4\,s + 4 + 5\,ts^4 + 4\,ts^3 \right. \\ \quad \left. -4\,ts^2 + 12\,ts - 8\,t\right)s, \\ 0, \\ -2\,s\left(3\,s^4 + 5\,s^3 + s^2 - 2\,s + 2\right), \\ 2\,s^5 + s^4 + 5\,s^3t - 4\,s^3 - 6\,s^2t \\ \quad + 10\,s^2 + 8\,st - 4\,t \end{pmatrix}$$

Now we apply degree reduction algorithm to reduce the degree of the μ-basis. The new μ-basis is shown below.

$\mathbf{p}' = \frac{1}{236661622380753}\cdot$

$$\begin{pmatrix} -300729067167523\,st + 56467802265703\,s^2t \\ \quad + 203543640533634\,s + 228386226979701\,t \\ \quad - 196295646522670\,s^2 - 140869867499516, \\ -279870932485122\,s + 90277583448339\,st \\ \quad - 125135373778758\,t + 140869867499516 \\ \quad + 48465134115412\,s^2 - 97142080550445\,s^2t, \\ -58285248330267\,s^2t + 81366332623128\,st \\ \quad + 103250853200943\,t + 147830512407258\,s^2 \\ \quad + 76327291951488\,s, \\ -40462746679845\,st - 77713664440356\,s^2t \\ \quad - 207436107658841\,s - 105225741859592\,t \\ \quad - 811703353674\,s^2 - 70434933749758 \end{pmatrix}$$

$\mathbf{q}' = \frac{1}{56167843795}\cdot$

$$\begin{pmatrix} 326160947200 + 162042688768\,s^2t + 770629365248\,s^2 \\ \quad + 324085377536\,st - 323344102656\,s, \\ -326160947200 - 360111336704\,s^2 + 487462361088\,s, \\ -410518028544\,s^2 - 164118258432\,s, \\ 163080473600 - 223271993856\,s^2 \\ \quad + 82429766656\,s + 162042688768\,t \end{pmatrix}$$

$\mathbf{r}' = \frac{1}{2039538}\cdot$

$$\begin{pmatrix} 23600164 - 47200328\,s^3 + 64900451\,s^2 - 23600164\,s, \\ -23600164 + 47200328\,s + 29500205\,s^3 - 35400246\,s^2, \\ 17700123\,s^3 - 29500205\,s^2 - 23600164\,s, \\ 11800082 + 23600164\,s^3 + 5900041\,s^2 \end{pmatrix}$$

Example 4 Consider the surface parameterized by

$$a(s,t) = -3s^2t^2 + 5s^2t - 5t^2 - 4st + 5,$$
$$b(s,t) = -3s^2t^2 + 3s^2t + s^2 + st^2 - s - 2t^2 - 5st + 1,$$
$$c(s,t) = -5s^2t^2 + 6s^2t + 2st - t^2 - t - 5,$$
$$d(s,t) = -4s^2t^2 + 3s^2t - st + 6t^2 - t + 1.$$

If we use the computer algebra system Singular or the package CASA in Maple to compute a generator of syzygy module $\mathrm{Syz}(a,b,c,d)$, then we get four or five vector polynomials (depending on different orderings), and it is very difficult to find proper combinations of them to form a μ-basis.

By our algorithm, we can easily compute a μ-basis. The result is omitted.

6. CONCLUSION AND FUTURE WORKS

In this paper, we apply the theory of polynomial matrices to compute μ-bases of rational curves and surfaces. The algorithm is based on several important techniques in the theory of polynomial matrices, such as primitive factorization, Hermite form and GCD extraction. This is the only known algorithm to compute the μ-bases of general rational surfaces, and it is superior than any existing algorithms for computing the μ-bases of rational curves.

In the future, μ-bases of a spatial rational parametric curve will be considered. It is expected that the implicit equation of a space curve can be computed from a μ-bases. On the other hand, finding an efficient method to compute a minimal μ-basis of a rational surface and the complexity analyzing of the algorithm are problems worthy of further research.

7. ACKNOWLEDGMENTS

The authors are support by the Outstanding Youth Grant of NSF of China (No. 60225002), NSF of China (10201030 and 60473132), a National Key Basic Research Project of China (2004CB318000), the TRAPOYT in Higher Education Institute of MOE of China, and SRF for ROCS, SEM. Special thanks go to Dr. Zhiping Lin from Nanyang Technological University, Singapore, for his novel results in the paper [12] and for the helpful discussions with him.

8. REFERENCES

[1] Falai Chen, Jianmin Zheng, and T. W. Sederberg, The μ-basis of a rational ruled surface, Computer Aided Geometric Design, Vol.18, 2001, 61–72.

[2] Falai Chen and Thomas W. Sederberg, A new implicit representation of a planar rational curve with high order of singularity, Comput. Aided Geom. Design, vol.19, 2002, 151–167.

[3] Falai Chen and Wenping Wang, The μ-basis of a planar rational curve — properties and computation, Graphical Models, Vol.64, 2003, 368–381.

[4] Falai Chen, Reparameterization of a rational ruled surface by μ-basis, Computer Aided Geometric Design, Vol.20, 2003, 11–17.

[5] Falai Chen and Wenping Wang, Revisiting the μ-basis of a rational ruled surface, Journal of Symbolic Computation, Vol.36, 2003, 699–716.

[6] Falai Chen, David Cox, and Yang Liu, The μ-basis of a rational parametric surface, Journal of Symbolic Computation, Vol.39, 2005, 689–706.

[7] Falai Chen and Wenping Wang, Computing the singular points of a planar rational curve using the μ-basis, preprint, 2004.

[8] David Cox, John Little, and Donal O'Shea, Using Algebraic Geometry, New York, Springer-Verlag, 1998.

[9] David Cox, T. W. Sederberg, and Falai Chen, The moving line ideal basis of planar rational curves, Computer Aided Geometric Design, Vol.15, 1998, 803–827.

[10] F. R. Gantmacher, Theory of Matrices, New York: Chelsea Publishing Co., 1959.

[11] John P. Guiver and N. K. Bose, Polynomial matrix primitive factorization over arbitrary coefficient filed and related results, IEEE Transactions on Circuits and Systems, Vol.CAS-29, No.10, 1982, 649–657.

[12] Zhiping Lin, On syzygy modules for polynomial matrices, Linear Algebra and Its Application, Vol.298, 1999, 73–86.

[13] Martin Morf, Bernard C. Lévy, and Sun-Yuan Kung, New results in 2-D system theory, Part I: 2-D polynomial matrices, factorization, and coprimeness, Proceedings of the IEEE, Vol.65, No.6, 1977, 861–872.

[14] T. W. Sederberg and Falai Chen, Implicitization using moving curves and surfaces, Computer Graphics Proceedings, Annual Conference Series, Vol.2, 1995, 301–308.

[15] T. W. Sederberg, T. Saito, D. Qi, and K. Klimaszewski, Curve implicitization using moving lines, Computer Aided Geometric Design, Vol.11, 1994, 687–706.

[16] D. C. Youla and G. Gnavi, Notes on n dimensional systems, IEEE Transaction on Circuits and System, Vol.26, 1979, 105–111.

[17] Fangling Zeng and Falai Chen, Degree reduction of rational curves by μ-basis, Computer Mathematics, Proceedings of the Sixth Asian Symposium (ASCM'2003), Lecture Notes Series on Computing, Vol.10, ed. Ziming Li and William Sit, World Scientific, 2003, 265–275.

[18] Jianmin Zheng and T. W. Sederberg, A direct approach to computing the μ-basis of planar rational curves, Journal of Symbolic Computation, Vol.31, 2001, 619–629.