J Syst Sci Complex (2010) 23: 804–814

IMPLICITIZATION USING UNIVARIATE RESULTANTS*

Liyong SHEN · Chunming YUAN

DOI: 10.1007/s11424-010-7218-6
Received: 1 November 2007 / Revised: 18 June 2008

Abstract Among several implicitization methods, the method based on resultant computation is a simple and direct one, but it often brings extraneous factors which are difficult to remove. This paper studies a class of rational space curves and rational surfaces by implicitization with univariate resultant computations. This method is more efficient than the other algorithms in finding implicit equations for this class of rational curves and surfaces.

Key words Implicitization, rational space curves, rational surfaces, resultants.

1 Introduction

Implicit and parametric expressions are classic representations of curves and surfaces in CG (Computer Graphics) and CAGD (Computer Aided Geometry Design). Both implicit and parametric representations have their advantages in solid modeling: The parametric form is best suited for generating points along a curve, whereas the implicit representation is most convenient for determining whether a given point lies on a specific curve or surface. This motivates the search for a means of converting from one representation to the other. In industry of art and solid modeling, the originally designed curves and surfaces are often in parametric forms. Thus, it is necessary to find their implicit forms, this procedure is called implicitization.

A complete implicitization method using Gröbner bases is presented in [1–2]. However, the computation complexity of the Gröbner basis technique is exponential, it is seldom used in practice when the degree of the parametrization is not low enough. Another implicitization method is based on the characteristic set method[3−4]. But it often involves some low dimensional redundant branches. Li[5] and Gao[6] provided some techniques to improve the method. However, how to simplify a complicated polynomial sets to a simple implicit variety is a fussy problem. Recently, Sederberg and Chen[7] proposed a new implicitization method using moving curves and moving surfaces, and improved it to the μ-basis method[8−9]. The μ-basis method has been implemented efficiently on planar curves and ruled surfaces. But this method needs to be studied further.

Liyong SHEN
School of Mathematical Sciences, Graduate University, Chinese Academy of Sciences, Beijing 100049, *China.*
Email: shenly@amss.ac.cn.
Chunming YUAN
Key Laboratory of Mathematics Mechanization, Institute of Systems Science, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, *China.*
Email: cmyuan@mmrc.iss.ac.cn.
*This project is supported by the Natural Science Foundation of China under Grant No. 10901163 and the Knowledge Innovation Program of the Chinese Academy of Sciences.

In 1908, Dixon[10] introduced the resultant method to eliminate variables from polynomials, which leads to a method for implicitization. However, the computation of resultants on multivariate is not easy[11]. When the surfaces have base points, the general resultant formula will be identical to zero. An alternative method is to select the biggest non-zero minor determinant as the resultant, but it often involves extraneous factor which is difficult to remove[12]. It is still an open problem to find the exact resultant formula. Although the resultant method is not a complete method, it has at least two advantages. First, it is efficient and known better than the Gröbner basis method and the characteristic set method. Second, the resultant method can be applied in numerical computations, while the other three methods cannot be used to do this task. That is why we develop implicitization using the resultant this paper.

Space curves are widely used in art design, cartoon movies, and industry modeling. In the first part of the paper, we study the implicitization problem of space curves, then give the implicit variety by univariate resultant computation. In the second part, we discuss the rational surfaces which can be implicitized using resultant method. Combining the re-parametrization method with the uni-multivariate decomposition and birational transformation, we get the rational surfaces which can be projected as planar curves and then obtain the implicit formula by the successive resultant computations.

2 Rational Space Curves

A rational space curve is defined as

$$(x, y, z) = \boldsymbol{P}(t) = \left(\frac{P_1(t)}{Q_1(t)}, \frac{P_2(t)}{Q_2(t)}, \frac{P_3(t)}{Q_3(t)}\right), \tag{1}$$

where $P_i, Q_i \in \mathbb{C}[t]$ and $\gcd(P_i, Q_i) = 1, i = 1, 2, 3$. Assume that the curve does not degenerate to a planar curve. Let $p = Q_1 x - P_1,\ q = Q_2 y - P_2$, and $r = Q_3 z - P_3$. Then $I = \langle p, q, r\rangle$ is the corresponding ideal of the curve $\boldsymbol{P}(t)$. So $I' = I \cap \mathbb{C}[x, y, z]$ is the elimination ideal of $\boldsymbol{P}(t)$. In [2], we have the following elimination property.

Lemma 1 *Let $\boldsymbol{P}(t)$ be a space curve of the form (1). Let I' be the elimination ideal of $P(t)$ and $\boldsymbol{V}(I')$ be the common zero set of I'. Then $\boldsymbol{V}(I')$ is the smallest affine variety including $\boldsymbol{P}(t)$.*

2.1 Resultant Method

Let us recall some properties of resultants in [2].

Consider two polynomials $f = a_0 t^s + \cdots + a_s$ and $g = b_0 t^l + \cdots + b_l$ in $\mathbb{C}[t, x, y, z]$ where $a_i, b_i \in \mathbb{C}[x, y, z]$. The Sylvester matrix of f and g with respect to t is defined to be

$$\mathrm{Syl}(f, g, t) = \begin{pmatrix} a_0 & & & b_0 & & \\ a_1 & \ddots & & b_1 & \ddots & \\ & \ddots & a_0 & & \ddots & b_0 \\ \vdots & & a_1 & \vdots & & b_1 \\ a_s & & \vdots & b_l & & \vdots \\ & \ddots & & & \ddots & \\ & & a_s & & & b_l \end{pmatrix}.$$

The resultant of f and g with respect to t, denoted by $\mathrm{Res}(f, g, t)$, is the determinant of the above Sylvester matrix:

$$\mathrm{Res}(f, g, t) = \det(\mathrm{Syl}(f, g, t)).$$

Then we have the following lemma.

Lemma 2 1) $\mathrm{Res}(f,g,t)$ *is in the elimination ideal of* $\langle f,g\rangle$ *in* $\mathbb{C}[x,y,z]$.

2) *For any* $X_0=(x_0,y_0,z_0)$, $\mathrm{Res}(f,g,t)$ *is zero at* X_0 *if and only if either* f *and* g *decrease the degrees of* t *at* X_0*, or* f *and* g *has a common solution for* t *at* X_0.

2.2 Compute Varieties with Univariate Resultants

Consider the ideal $I=\langle p,q,r\rangle$ of $\boldsymbol{P}(t)$. Then the resultant system[11] can be used to compute the elimination ideal, but the resultant systems often contain many redundant elements. We now consider a direct method, that is, finding the variety of the parametric curve by the resultant computations of any two polynomials in I.

For a rational space curve $\boldsymbol{P}(t)$ of the form (1), consider the resultants

$$f=\mathrm{Res}(p,q,t),\quad g=\mathrm{Res}(p,r,t),\quad h=\mathrm{Res}(q,r,t)\in\mathbb{C}[x,y,z].$$

Then $\langle f,g,h\rangle\subset I'$ and $\boldsymbol{V}(I')\subset\boldsymbol{V}(\langle f,g,h\rangle)$. However, the inverse inclusion

$$\boldsymbol{V}(I')\supset\boldsymbol{V}(\langle f,g,h\rangle) \tag{2}$$

is not true in general, as illustrated by the following counterexample.

Example 1 Let $\boldsymbol{P}(t)$ be the cubic space curve

$$(t^2\,(t-2)\,,(t-1)^2\,(t+1)\,,t\,(t-1)\,(t-2)).$$

One can verify that the point $(-1,1,0)$ is in $\boldsymbol{V}(\langle f,g,h\rangle)$ but not in $\boldsymbol{V}(I')$.

We now study the situation for (2). Note that $p=Q_1x-P_1$ is linear in x. Then

$$p=(Q_1,0,0,-P_1)\cdot(x,y,z,1),$$

where $\cdot$ denotes the inner product of two vectors. Set $\boldsymbol{p}=(Q_1,0,0,-P_1)$ and $\deg(\boldsymbol{p})=\deg_t(p)$. Similarly, $\boldsymbol{q}=(0,Q_2,0,-P_2)$ for q and $\boldsymbol{r}=(0,0,Q_3,-P_3)$ for r. Then

$$[\boldsymbol{p},\boldsymbol{q},\boldsymbol{r}]=Q_1Q_2Q_3\left(\frac{P_1(t)}{Q_1(t)},\frac{P_2(t)}{Q_2(t)},\frac{P_3(t)}{Q_3(t)},1\right), \tag{3}$$

where $[\boldsymbol{p},\boldsymbol{q},\boldsymbol{r}]$ is the exterior product of $\boldsymbol{p},\boldsymbol{q}$, and $\boldsymbol{r}$.

Denote by $\mathrm{Lcv}(\cdot)$ the leading coefficient vector with respect to t. The following lemma is a generalization of Theorem 1 of [8].

Lemma 3 *Let* X_0 *be a point in* $\boldsymbol{V}(\langle f,g,h\rangle)$. *Then* X_0 *belongs to* $\boldsymbol{V}(I')$ *if one of the following conditions is satisfied*

i) *p, q and r decrease the degrees of t at X_0, and,* $\mathrm{Lcv}(\boldsymbol{p})$, $\mathrm{Lcv}(\boldsymbol{q})$ *and* $\mathrm{Lcv}(\boldsymbol{r})$ *are linearly independent.*

ii) *the polynomials p,q and r have a common solution for t at X_0.*

Proof Note that for convenience we can regard p as its vector form $\boldsymbol{p}$ when needed.

i) Let $X_0=(x_0,y_0,z_0)$. Suppose that p, q, and r decrease the degrees of t. This means that the leading terms of p,q and r become zeros at X_0, i.e.,

$$(x_0,y_0,z_0,1)\cdot\mathrm{Lcv}(\boldsymbol{p})=(x_0,y_0,z_0,1)\cdot\mathrm{Lcv}(\boldsymbol{q})=(x_0,y_0,z_0,1)\cdot\mathrm{Lcv}(\boldsymbol{r})=0,$$

where $\mathrm{Lcv}(\boldsymbol{p})=(q_{1n},0,0,-p_{1n}),\mathrm{Lcv}(\boldsymbol{q})=(0,q_{2n},0,-p_{2n})$ and $\mathrm{Lcv}(\boldsymbol{r})=(0,0,q_{3n},-p_{3n})$.

By the assumption, $\mathrm{Lcv}(\boldsymbol{p})$, $\mathrm{Lcv}(\boldsymbol{q})$ and $\mathrm{Lcv}(\boldsymbol{r})$ are linearly independent. Then $(x_0, y_0, z_0, 1)$ must be a nonzero scalar multiple of their exterior product

$$[\mathrm{Lcv}(\boldsymbol{p}), \mathrm{Lcv}(\boldsymbol{q}), \mathrm{Lcv}(\boldsymbol{r})] = q_{1n}q_{2n}q_{3n}\left(\frac{p_{1n}}{q_{1n}}, \frac{p_{2n}}{q_{2n}}, \frac{p_{3n}}{q_{3n}}, 1\right).$$

Writing in affine form, we have $(x_0, y_0, z_0) = (\frac{p_{1n}}{q_{1n}}, \frac{p_{2n}}{q_{2n}}, \frac{p_{3n}}{q_{3n}})$.

On the other hand, from (3) and $\mathrm{Lcv}([\boldsymbol{p}, \boldsymbol{q}, \boldsymbol{r}]) = [\mathrm{Lcv}(\boldsymbol{p}),\ \mathrm{Lcv}(\boldsymbol{q}),\ \mathrm{Lcv}(\boldsymbol{r})]$, we have that $(\frac{p_{1n}}{q_{1n}}, \frac{p_{2n}}{q_{2n}}, \frac{p_{3n}}{q_{3n}})$ is a point on $\boldsymbol{P}(t)$ corresponding to $t = \infty$. So $(x_0, y_0, z_0) \in \boldsymbol{V}(I')$.

ii) Suppose p, q, and r have a common solution at X_0. Then

$$(x_0, y_0, z_0, t_0) \in \boldsymbol{V}(\langle p, q, r\rangle) = \boldsymbol{V}(I).$$

By the elimination theory, we have $(x_0, y_0, z_0) \in \boldsymbol{V}(I')$. ∎

Now, we are ready to give the implicit varieties for space curves by resultant computation. Actually, except the element t, here $p(x,t), q(y,t)$, and $r(z,t)$ involve only x, y and z respectively.

Theorem 1 *Let $\boldsymbol{P}(t)$ be a rational space curve of the form* (1). *If $\deg(P_i/Q_i) = 1$ for some i, then $\boldsymbol{P}(t)$ is an intersection curve of two surfaces.*

Proof Without loss of the generality, we assume $\deg(P_3/Q_3) = 1$. We will show that $\boldsymbol{V}(I') = \boldsymbol{V}(\langle g, h\rangle)$.

Given a point $(x_0, y_0, z_0) \in \boldsymbol{V}(\langle g, h\rangle)$, we have $g(x_0, z_0) = h(y_0, z_0) = 0$. By Lemma 2, g is zero if and only if either p and r decrease the degrees of t, or, p and r have a common solution. Similarly, h is zero if and only if either q and r decrease the degrees of t, or, q and r have a common solution.

Let $\mathcal{S} = \{i \mid \deg(Q_i) < \deg(P_i), i = 1, 2, 3\}$ and the cardinality of $\mathcal{S}$ be $\#\mathcal{S}$.

If $\#\mathcal{S} \geq 2$, then at least two polynomials of $\{p, q, r\}$ cannot decrease the degrees of t at X_0. Moreover, $\deg_t r(z_0, t) \leq 1$, so we can find a solution of the system $\{p = q = r = 0\}$ at X_0. According to Lemma 3, $X_0 \in \boldsymbol{V}(I')$.

If $\#\mathcal{S} \leq 1$, then $\mathrm{Lcv}(\boldsymbol{p}), \mathrm{Lcv}(\boldsymbol{q})$ and $\mathrm{Lcv}(\boldsymbol{r})$ are linearly independent. We consider the following two cases.

Case 1: The polynomials p, q and r decrease the degrees of t at X_0. Then $X_0 \in \boldsymbol{V}(I')$ by Lemma 3.

Case 2: $\{p = r = 0\}$ has a solution and $\{q = r = 0\}$ has a solution. Since $r(z_0, t) = 0$ is a linear equation, $\{p = q = r = 0\}$ has a solution at X_0. By Lemma 3, $X_0 \in \boldsymbol{V}(I')$.

Finally, we show no other cases happen. Otherwise, we must have $\deg_t r(z_0, t) = 0$ and $r(z_0, t) = 0$. Therefore, $Q_3 z_0 - P_3$ is identical to zero, a contradiction to $\gcd(P_3, Q_3) = 1$. ∎

Example 2 For the twist curve $\boldsymbol{P}(t) = (t^3, t^2, t)$, we can get its variety

$$\boldsymbol{V}(\langle x - z^3, y - z^2\rangle)$$

by computing the resultants between p, q, and r, respectively.

3 Rational Surfaces

A rational surface is defined as

$$(x, y, z) = \boldsymbol{P}(s, t) = \left(\frac{P_1(s,t)}{Q_1(s,t)}, \frac{P_2(s,t)}{Q_2(s,t)}, \frac{P_3(s,t)}{Q_3(s,t)}\right), \tag{4}$$

where $P_i, Q_i \in \mathbb{C}[s, t]$ and $\gcd(P_i, Q_i) = 1$ for $i = 1, 2, 3$.

As introduced, one can implicitize the above rational surface by Gröbner basis method theoretically which cannot be really implemented in practice. Another way is based on the multivariate resultant computation, which is incomplete.

In this section, we will consider the rational surfaces which can be projected as planar curves.

We first give some preliminary results. For the implicitization of planar curves, we have the following lemma.

Lemma 4[13] *Let* $\boldsymbol{P}(t)=\left(\frac{P_1(t)}{Q_1(t)},\frac{P_2(t)}{Q_2(t)}\right)$ *be the parametrization of a planar curve in reduced form and* $f(x,y)$ *be its defining polynomial. Then* $f(x,y)^{\mathrm{index}(\boldsymbol{P})}$ *is equal to* $\mathrm{Res}(Q_1(t)x-P_1(t),Q_2(t)y-P_2(t),t)$ *up to multiplication by nonzero constants.*

In Lemma 4, $\mathrm{index}(\boldsymbol{P})$ is defined to be the number of parameters corresponding to a generic point of $f(x,y)$ and called the improper index of $\boldsymbol{P}(t)$. The improper index of a rational surface is defined similarly[14]. A rational parametrization is proper if and only if its improper index is equal to one[13−14].

We now consider the rational surfaces of the following form:

$$(x,y,z)=\boldsymbol{P}(s,t)=\left(\frac{P_1(s,t)}{Q_1(s,t)},\frac{P_2(s,t)}{Q_2(s,t)},\frac{P_3(s)}{Q_3(s)}\right). \tag{5}$$

Obviously, the surface (5) can be regarded as a planar curve on $\mathbb{C}(s)^2$:

$$(x,y)=\boldsymbol{P}_s(t)=\left(\frac{P_1(s;t)}{Q_1(s;t)},\frac{P_2(s;t)}{Q_2(s;t)}\right). \tag{6}$$

Clearly, we can write

$$\mathrm{Res}(Q_1(t)x-P_1(t),Q_2(t)y-P_2(t),t)=l(s)L(x,y,s),$$

where $l(s)\in\mathbb{C}[s]$ is the content of the resultant with respect to parameters x,y. Hence, $L(x,y,s)$ is the primitive part of the resultant. Then $l(s)L(x,y,s)$ is not zero since $\gcd(P_i,Q_i)=1$ and $\deg(P_i/Q_i)\geq 1$ for $i=1,2$. Let $f(x,y;s)\in\mathbb{C}[x,y,s]$ be the irreducible defining polynomial of (6). By Lemma 4, we have

$$L(x,y,s)=f(x,y,s)^{\mathrm{index}(\boldsymbol{P}_s)}. \tag{7}$$

If $\deg_s(L)=0$, then the surface (5) is exactly a cylinder over the xy plane and $f(x,y)=0$ is its irreducible implicit equation. Since it is not difficult to determine whether a rational surface is a cylinder over a coordinate plane or not, it suffices to consider the non-degenerate case with $\deg_s(L)\geq 1$. Before the implicit theorem, we give a preparative lemma.

Lemma 5 *Let* $M(z,s)$ *and* $N(s)$ *be two irreducible polynomials in* $R[z,s]$*, where* R *is a unique factorization domain. Suppose that* $\mathrm{Res}(M(z,s),N(s),s)=a*g(z)^k$*, where* $a\in R$*,* g *is irreducible and* $k\in\mathbb{N}$*. If* $M(z,\beta)$ *is square-free for every root* β *of* $N(s)$ *and* z_0 *is a generic zero of* g*, then* k *is the degree of* $GCD(M(z_0,s),N(s))$.

Proof Let b be the initial of $N(s)$ and $d_1=\deg(M,s),d_2=\deg(N,s)$. Then

$$a*g(z)^k=\mathrm{Res}(M(z,s),N(s),s)M(z,\bar{s})=b^{d_1}\prod_{i=1}^{d_2}M(z,s_i),$$

where $s_i,i=1,2,\cdots,d_2$ is the conjugate roots of $N(s)$. Let z_0 be a generic zero of g, then the multiplicity of zero z_0 at both sides of the above equation is k. Note that $M(z,s_i)$ is square-free for every s_i. If z_0 is the root of $M(z,s_i)$, then the multiplicity of z_0 in $M(z,s_i)$ is one.

Hence, there exist $i_1, i_2, \cdots, i_k$ among $1, 2, \cdots, d_2$, such that $M(z_0, s_{i_j}) = 0$ and $M(z_0, s_l) \neq 0$ for $l \notin \{i_1, i_2, \cdots, i_k\}$. So $M(z_0, s)$ and $N(s)$ have exactly k common roots. The conclusion follows. ∎

Theorem 2 *Let $\boldsymbol{P}(s,t)$ be a rational surface of the form* (5) *and its defining polynomial be $F(x,y,z) \notin \mathbb{C}[x,y]$. Then up to multiplication by nonzero constants,*

$$F(x,y,z)^{\mathrm{index}(\boldsymbol{P})} = \mathrm{Res}\Big(Q_3(s)z - P_3(s), L(x,y,s), s\Big). \tag{8}$$

Proof Consider the resultant,

$$\mathrm{Res}\Big(Q_3(s)z - P_3(s), L(x,y,s), s\Big) = \widetilde{F}(x,y,z).$$

First, we show that $\widetilde{F}(x,y,z)$ is some power of $F(x,y,z)$ up to multiplication by nonzero constants. Since $F(x,y,z) \notin \mathbb{C}[x,y]$, we have $\deg_s(L) \geq 1$. And since $\deg_s(r) \geq 1$ and $\gcd(P_3, Q_3) = 1$, we know that $\widetilde{F}(x,y,z)$ is not identical to zero. Let (x_0, y_0, z_0) be a generic point on $\widetilde{F}(x,y,z)$. By Lemma 2, $\widetilde{F}(x_0,y_0,z_0) = 0$ if and only if there exists $s_0 \in \mathbb{C}$ such that

$$L(x_0, y_0, s_0) = 0 \quad \text{and} \quad Q_3(s_0)z_0 = P_3(s_0).$$

Then $z_0 = P_3(s_0)/Q_3(s_0)$ because $\gcd(Q_3, P_3) = 1$. Here, since (x_0, y_0, z_0) is generically chosen, the degree reduction cannot occur in Lemma 2. Similarly, $L(x_0, y_0, s_0) = 0$ if and only if there exists t_0 such that

$$Q_1(s_0,t_0)x_0 - P_1(s_0,t_0) = 0 \quad \text{and} \quad Q_2(s_0,t_0)y_0 - P_2(s_0,t_0) = 0.$$

Assume that (s_0, t_0) is a base point. Then $l(s_0)$ must be zero. Otherwise, $L(x,y,s) \equiv 0$ because x_0, y_0 are generic, a contradiction. But $l(s)$ is removed as the content, this case cannot happen. Therefore, (s_0, t_0) is not a base point. Hence,

$$x_0 = \frac{P_1(s_0,t_0)}{Q_1(s_0,t_0)}, \quad y_0 = \frac{P_2(s_0,t_0)}{Q_2(s_0,t_0)}, \quad \text{and} \quad z_0 = \frac{P_3(s_0)}{Q_3(s_0)}.$$

So far, we have proved that a generic point on $\widetilde{F}$ corresponds to the pair (s_0, t_0) in the rational parametrization $\boldsymbol{P}(s,t)$ whose irreducible implicit polynomial is $F(x,y,z)$. That means there exits an integer $h \geq 1$ such that $\widetilde{F}(x,y,z) = F(x,y,z)^h$ up to multiplication by nonzero constants. Next, we show that h is exactly the improper index of $\boldsymbol{P}(s,t)$.

By the properties of resultants, we have

$$\begin{aligned} F(x,y,z)^h &= \mathrm{Res}\Big(Q_3(s)z - P_3(s), L(x,y,s), s\Big) \\ &= \mathrm{Res}\Big(Q_3(s)z - P_3(s), f(x,y,s), s\Big)^{\mathrm{index}(\boldsymbol{p}_s)}. \end{aligned}$$

We choose (x_0, y_0, z_0) as a generic point of $F(x,y,z)$. By Lemma 5, the number of s corresponding to (x_0, y_0, z_0) is

$$\ell := \deg\Big(\gcd\Big(\mathrm{Res}\Big(Q_3(s)z_0 - P_3(s), f(x_0,y_0,s), s\Big)\Big)\Big) = \frac{h}{\mathrm{index}(\boldsymbol{P}_s)}.$$

Suppose that they are s_i, $i = 1, 2, \cdots, \ell$. Then for each i, the number of t corresponding to (x_0, y_0, s_i) is $\mathrm{index}(\boldsymbol{P}_s)$. Hence, for a generic point (x_0, y_0, z_0) of $F(x,y,z)$, the number of points (s_i, t_i) corresponding to the generic zero is $\mathrm{index}(\boldsymbol{P}_s) \cdot \frac{h}{\mathrm{index}(\boldsymbol{p}_s)} = h$. So $\mathrm{index}(\boldsymbol{P}) = h$. The conclusion follows. ∎

By Theorem 2, we can implicitize a rational surface of the form (5) rapidly, since only successive univariate resultants with two steps need to be computed.

3.1 Birational Transformation and Rational Decomposition

In this subsection, we will study the rational surfaces which can be transformed to the form (5). The decomposition method for rational functions[15] will be used and more specifically, we only concern about uni-multivariate decomposition.

Let $f, h \in \mathbb{C}(s,t)$, and g be a univariate polynomial over $\mathbb{C}$ such that $f = g(h)$. We call (g, h) a uni-multivariate decomposition of f, and h a decomposition factor.

Lemma 6 *A rational function $f \in \mathbb{C}(s,t)$ can be transformed to $g(S)$ birationally if and only if f has the decomposition (g, h) and there exists a rational function $\widetilde{h}$ such that $\mathbb{C}(h, \widetilde{h}) = \mathbb{C}(s,t)$.*

Proof If the uni-multivariate decomposition is $g(h(s,t))$ and there exists an associated rational function $\widetilde{h}(s,t)$ such that $\mathbb{C}(h, \widetilde{h}) = \mathbb{C}(s,t)$, then the transformation $S = h, T = \widetilde{h}$ is birational.

Conversely, suppose that $S = S(s,t), T = T(s,t)$ is a birational transformation such that the reparametrization is $g(S)$. Then $g(S,T) = g(S)$ is a uni-multivariate decomposition of f. ∎

Consider the fractional linear transformations in the following.

Lemma 7 *Let $\boldsymbol{P}(s,t)$ be a rational surface of the form (4). Then a reparametrization $\boldsymbol{P}(S,T)$ by the parameter transformations*

$$\begin{cases} S = s \\ T = \dfrac{T_1(s)t + T_2(s)}{T_3(s)t + T_4(s)} \end{cases} \quad \textit{and} \quad \begin{cases} S = \dfrac{S_1(t)s + S_2(t)}{S_3(t)s + S_4(t)} \\ T = t \end{cases}$$

is an equivalent parametrization of $\boldsymbol{P}(s,t)$, where $T_i(s) \in \mathbb{C}[s], S_i(t) \in \mathbb{C}[t]$ and $T_1T_4 - T_2T_3 \neq 0, S_1S_4 - S_2S_3 \neq 0$.

Proof The lemma follows from the fact that the two parameter transformations are birational. ∎

If there exits i such that $P_i(s,t)/Q_i(s,t)$ has the form $P_i(S)/Q_i(S)$ or $P_i(T)/Q_i(T)$, by a birational transformation in Lemma 7, then we reparameterize the rational surface and compute its implicit equation by Theorem 2.

A question then arises on how to determine whether $P_i(s,t)/Q_i(s,t)$ can be rewritten in the form following Lemma 7. In other words, by Lemma 6, we need to find if there exists a decomposition factor $h = \frac{T_1(s)t+T_2(s)}{T_3(s)t+T_4(s)}$ or $h = \frac{S_1(t)s+S_2(t)}{S_3(t)s+S_4(t)}$. That is, $\min\{\deg_s(h), \deg_t(h)\} = 1$ and we call such h as quasi-linear. Fortunately, we can use the uni-multivariate rational decomposition method[15] to solve this problem.

We modify the algorithm 2.1 in [15] to find quasi-linear decomposition factors.

Algorithm 1 Input: $f = \frac{f_n(s,t)}{f_d(s,t)} \in \mathbb{C}(s,t)$.

Output: the quasi-linear decomposition factor if it exists, and "no quasi-linear decomposition" otherwise.

A) Factor the symmetric polynomial $P = f_n(s,t)f_d(u,v) - f_d(s,t)f_n(u,v)$.

B) Let H be a divisor of P with $\min\{\deg_s(H), \deg_t(H)\} = 1$.

C) If H is a symmetric near-separated polynomial, that is, there exist N and D in $\mathbb{C}[s,t]$ such that $H = N(s,t)D(u,v) - D(s,t)H(u,v)$, then return $N(s,t)/D(s,t)$.

D) If all divisors are not symmetric near-separated polynomial, then return "no quasi-linear decomposition".

For a rational surface (4), we can find its quasi-linear decomposition factor by Algorithm 1 if it has. Indeed, Algorithm 1 finds all rational surfaces which can be reparameterized to the form of (5) by a birational transformation.

Example 3 Let $(x,y,z)=\boldsymbol{P}(s,t)$ be a rational surface defined by

$$\left(\frac{1-t^2-2\,s^2t}{1+t^2},\frac{2\,t+s^2\,(1-t)}{1+t^2},\frac{s^2t^4+4\,st^2+1+s^2t^2-4\,s^2t+4\,s^2-4\,st+t^2}{(3\,st^2+3+st-2\,s+t)\,(st^2+1)}\right).$$

It is not of the form (5), but by Algorithm 1, z has a quasi-linear decomposition

$$\frac{s^2t^4+4\,st^2+1+s^2t^2-4\,s^2t+4\,s^2-4\,st+t^2}{(3\,st^2+3+st-2\,s+t)\,(st^2+1)}=\frac{S^2+1}{S+3},$$

where the birational transformation corresponding the decomposition factor is

$$S=\frac{s\,(t-2)+t}{st^2+1},\quad T=t.$$

We can get a reparameterization $\boldsymbol{P}(S,T)$ to be the following:

$$\left(-\frac{-T^4S^2+2\,ST^3-8\,ST^2+3\,T^2+4\,T-4+T^6S^2-2\,T^5S+4\,T^4S+T^4-2\,T^3+2\,TS^2}{(ST^2-T+2)^2\,(1+T^2)},\right.$$

$$\left.\frac{2\,T^5S^2-4\,T^4S+8\,ST^3+T^3-7\,T^2+8\,T+S^2-TS^2-2\,ST+2\,ST^2}{(ST^2-T+2)^2\,(1+T^2)},\frac{1+S^2}{3+S}\right),$$

which can be implicitized using Theorem 2. Here, we omit the implicit equation with degree 18 since it has a long expression.

Obviously, $\widetilde{h}$ is easy to find such that $\mathbb{C}(h,\widetilde{h})=\mathbb{C}(s,t)$ for a quasi-linear decomposition h. However, it is difficult to determine whether there exist $\widetilde{h}$ for a general h, we will focus on this problem in further work.

3.2 Some Applications

Based on the methods presented above, let us do the implicitization for two classes of rational surfaces that are frequently occurred in CAGD.

3.2.1 Rational Ruled Surfaces

The rational ruled surfaces appear in many applications. The developable surfaces, a particular class of ruled surfaces, are widely used in architecture. A ruled surface in affine form is defined as

$$(x,y,z)=\boldsymbol{P}(s,t)=\left(\frac{a_0(s)+a_1(s)t}{d_1(s)},\frac{b_0(s)+b_1(s)t}{d_2(s)},\frac{c_0(s)+c_1(s)t}{d_3(s)}\right),\tag{9}$$

where $a_i,b_i,c_i,i=0,1$; $d_j,j=1,2,3$, are nonzero polynomials in $\mathbb{C}[s]$. We also assume that the parametric equations are irreducible fractions, for instance, $\gcd(a_0,a_1,d_1)=1$.

Obviously, we can transform the ruled surface (9) to the form of (5) by Lemma 7, precisely, we can write the ruled surface as

$$\boldsymbol{P}(s,t)=\left(\frac{a_0(s)+a_1(s)t}{d_1(s)},\frac{b_0(s)+b_1(s)t}{d_2(s)},t\right),\tag{10}$$

where $a_i,b_i,c_i\in\mathbb{C}[s]$ for $i=1,2$ and $0\neq d_j\in\mathbb{C}[s]$ for $j=1,2,3$.

After the reparametrization, we can implicitize the ruled surface only by a univariate resultant computation.

Corollary 8 *Let $\boldsymbol{P}(s,t)$ be a rational ruled surface of the form* (10) *and its defining polynomial be $f(x,y,z)$. Then*

$$f(x,y,z)^{\mathrm{index}(\boldsymbol{P})} = pp_{x,y}(\mathrm{Res}(d_1x-(a_0+a_1t), d_2y-(b_0+b_1t), s))|_{t=z},$$

where $pp_{x,y}$ takes the primitive part with respect to x and y.

Example 4 Let $(x,y,z)=\boldsymbol{P}(s,t)$ be a ruled surface defined by

$$\left(\frac{1-s^2-2\,ts}{1+s^2}, \frac{2\,s+t(1-s^2)}{1+s^2}, t\right).$$

Since the surface is of the form (10), we do not need reparametrization. The resultant for a projected planar curve can be found

$$R(x,y;t)=4\,y^2+4\,t^2x^2+4\,t^2y^2-8\,t^2-4\,t^4+4\,x^2-4.$$

Removing the content $(4\,t^2+4)$, one can get the primitive part as $-t^2+y^2-1+x^2$. Then the implicit equation of the ruled surface is

$$-z^2+y^2-1+x^2=0.$$

For the same ruled surface, Fioravanti, et al.[16] computed three resultants and their gcd to get the implicit equation.

3.2.2 Rational Revolution Surfaces

Another class of rational surfaces that are frequently used in porcelain modeling is revolution surfaces. A rational revolution surface is generated by a space curve circumrotating around the z-axis. We assume that it has the following form:

$$\boldsymbol{P}(s,t)=\left(\frac{P_1(s)}{Q_1(s)}\frac{2t}{1+t^2}, \frac{P_2(s)}{Q_2(s)}\frac{1-t^2}{1+t^2}, \frac{P_3(s)}{Q_3(s)}\right),$$

where $P_1/Q_1=P_2/Q_2$. Since it is exactly of the form (5), so we can apply our method directly. We consider a torus surface as an example. Let

$$(x,y,z)=\boldsymbol{P}(s,t)=\left(\frac{4\left(1+\,s^2+\,s\right)t}{(1+s^2)\,(1+t^2)}, \frac{2\left(1+\,s^2+\,s\right)\left(1-t^2\right)}{(1+s^2)\,(1+t^2)}, \frac{1-s^2}{1+s^2}\right).$$

By successive resultant computation, we can compute its implicit equation

$$9-10\,x^2-10\,y^2+2\,z^2x^2+2\,z^2y^2+6\,z^2+x^4+y^4+2\,x^2y^2+z^4=0.$$

4 Experiments and Conclusions

To illustrate the efficiency of our method, we give two time costing tables. On each row of Table 1, we list the average computation time of ten examples of same degree but with some random integer coefficients in $[-10,10]$. The examples are implemented in Maple 10 with IBM corporation, CPU Intel Pentium 3.0G, RAM 256M. Times of our method and that of Gröbner bases are given in seconds of CPU.

Table 1 Time Costing: Implicitization of space curves

$(\deg_t x, \deg_t y, \deg_t z)$	Resultants	Gröbner Bases
(1,2,2)	~ 0.0	0.141
(1,3,5)	~ 0.0	3.081
(1,5,6)	0.073	29.78
(1,7,8)	0.126	401.4

Recently, Pérez-Diáz and Sendra[17] gave an implicitization method based on univariate resultant computations for general rational surfaces. The method brought auxiliary parameters which increases the complexity of computations. For the class of rational surfaces mentioned in our paper, our algorithm is more efficient than theirs. Using our method, one can quickly implicitize fourteen of sixteen examples in their paper. On the above computer, the implicitization of these examples can be computed quickly using our method but can not be done within ten minutes using the algorithm in [17]. After switching to a HP workstation xw4600 with CPU (Dual intel 2.4G) and 4 GB of RAM, we obtain the following time costing of 11 examples in Appendix of [16] using our method (Time I) and their method (Time II), respectively.

Table 2 Time Costing: Implicitization of rational surfaces

$\boldsymbol{P}(s,t)$	Time I	Time II	tdeg(F)	Terms of F
$\boldsymbol{P}_2(s,t)$	0.359	7.828	16	111
$\boldsymbol{P}_3(s,t)$	0.563	89.593	48	10
$\boldsymbol{P}_4(s,t)$	0.844	>1000	24	148
$\boldsymbol{P}_5(s,t)$	0.687	>1000	11	1027
$\boldsymbol{P}_6(s,t)$	0.249	>1000	9	164
$\boldsymbol{P}_7(s,t)$	1.375	>1000	17	206
$\boldsymbol{P}_8(s,t)$	7.453	>1000	42	1321
$\boldsymbol{P}_9(s,t)$	3.719	>1000	60	1645
$\boldsymbol{P}_{10}(s,t)$	0.157	0.782	36	156
$\boldsymbol{P}_{11}(s,t)$	7.563	>1000	23	418
$\boldsymbol{P}_{12}(s,t)$	2.906	>1000	26	367

where

$$
\begin{aligned}
\boldsymbol{P}_2 &= \left(-\frac{(s^2-1)^3 t}{s^4-2\,s^2}, \frac{t^4}{s^2-1}, -\frac{ts^2(s^2-2)}{s^2-1}\right),\\
\boldsymbol{P}_3 &= \left(\frac{t^4}{s^2-1}, \frac{(s^2-1)^3}{t^4}, s^6\left(s^2+1\right)^3+t\right),\\
\boldsymbol{P}_4 &= \left(\frac{s^6}{2\,s^4+3\,s^2+2\,st-8\,s+t^2-8\,t+19}, \left(2\,s^2+2\,st-8\,s\right)^2, t^3\right),\\
\boldsymbol{P}_5 &= \left(\frac{-6+2\,s^3+6\,t^2-10\,s}{-5+4\,t^2+9\,st}, 12-32\,st+3\,s+3\,s^2-6\,t-4\,s^3, s^2t+1\right),\\
\boldsymbol{P}_6 &= \left(t-(s-t+3)^3, t^3-4\,s^2-5\,s, s^2-t+4\right),\\
\boldsymbol{P}_7 &= \left(\frac{7-2\,st^2-4\,st}{1-4\,s^2+2\,t}, \frac{st}{st+1-3\,s^2}, -54-6\,s^4t-4\,s-26\,s^2\right),\\
\boldsymbol{P}_8 &= \left(t^2+\left(s^4-1\right)^{-1}, st-1+t^{-2}, s^{-7}\right),\\
\boldsymbol{P}_9 &= \left(\frac{t^4}{s^2-1}, \left(\left(s^2-1\right)^2 t^4+2\right)^{-1}, s^6\left(s^2+1\right)^3+t\right),\\
\boldsymbol{P}_{10} &= \left(t^6\left(t^2+1\right)^3, s^{-2}, \frac{4t}{1+s}+\frac{t}{s}\right),\\
\boldsymbol{P}_{11} &= \left(\frac{5\left(t^2+1\right)^3}{t^6}, \frac{t(st+t+1)}{4(1+s)}, \frac{t}{s^2}+1\right),\\
\boldsymbol{P}_{12} &= \left(\frac{5s^2}{s^{10}+s^3t+t}, \frac{s+t}{s+5\,st+s^5}, 5\,s^2+t+st+4\right).
\end{aligned}
$$

For further work, we will find the elimination ideal $\sqrt{I'}$ of space curves with efficient computation. In addition, we hope to determine a rational function $\widetilde{h}$ associated to h such that $\mathbb{C}(h,\widetilde{h}) = \mathbb{C}(s,t)$. This will be very helpful for birational transformation and implicitization of rational surfaces.

Acknowledgments

We thank the anonymous referees and their comments encourage us replace the Section 3 with this version. Thank Dr. Min Wu for her kind help on revising our paper.

References

[1] B. Buchberger, Gröbner bases, An algorithmic method in polynomial ideal theory, in *Multidimensional Systems Theory*, N. K. Bose (Ed.), D. Reidel Publishing Company, 1985, 184–232.
[2] D. Cox, J. Little, and D. O'shea, *Ideals, Varieties, and Algorithms*, Springer-Verlag, 1992.
[3] W. T. Wu, On a projection theorem of quasi-varieties in elimination theory, *Chin. Ann. Math.* (*Ser.B*), 1990, **11**(2): 220–226.
[4] F. J. Chai, X. S. Gao, and C. M. Yuan, A characteristic set method for solving Boolean equations and application in cryptanalysis of stream ciphers, *Journal of Systems Science* & *Complexity*, 2008, **21**(2): 191–208.
[5] Z. M. Li, Automatic implicitization of parametric objects, *Math. Mech. Res. Preprints*, 1989, **4**: 54–62.
[6] X. S. Gao and S. C. Chou, Implicitization of rational parametric equations, *Journal of Symbolic Computation*, 1992, **14**(5): 459–470.
[7] T. W. Sederberg and F. Chen, Implicitization using moving curves and surfaces, *Proceeding of Siggraph'*1995, ACM Press, 1995, 301–308.
[8] D. Cox, T. W. Sederberg, and F. Chen, The moving line ideal basis of planar rational curves, *Comput. Aided Geom. Des.*, 1998, **15**(8): 803–827.
[9] F. Chen and W. Wang, The μ-basis of a planar rational curve–properties and computation, *Graphical Models*, 2002, **64**(6): 368–381.
[10] A. L. Dixon, The eliminant of three quantics in two independent variables, *Proc. London Math. Soc.*, 1909, **7**(1): 49–69, 473–492.
[11] B. L. Van der Waerden, *Modern Algebra II*, Frederick Ungar Pub., New York, 1953.
[12] D. Manocha and J. F. Canny, Algorithm for implicitizing rational parametric surfaces, *Comput. Aided Geom. Des.*, 1992, **9**(1): 25–50.
[13] J. R. Sendra and F. Winkler, Tracing index of rational curve parametrizations, *Computer Aided Geometric Design*, 2001, **18**(8): 771–795.
[14] S. Pérez-Diaz, J. R. Sendra, and J. Schicho, Properness and inversion of rational parametrizations of surfaces, *Applicable Algebra in Engineering, Communication, and Computing*, 2002, **13**(1): 29–51.
[15] J. Gutierrez, R. Rubio, and D. Sevilla, On multivariate rational function decomposition, *Journal of Symbolic Computation*, 2002, **33**(5): 545–562.
[16] M. Fioravanti, L. Gonzalez-Vega, and I. Necula, Computing the intersection of two ruled surfaces by using a new algebraic approach, *Journal of Symbolic Computation*, 2006, **41**(1): 1187–1205.
[17] S. Pérez-Diáz and J. R. Sendra, A univariate resultant-based implicitization algorithm for surfaces, *Journal of Symbolic Computation*, 2008, **43**(2): 118–139.