Implicitization of rational ruled surfaces with μ-bases

Marc Dohm

Implicitization of rational ruled surfaces with μ-bases

Marc Dohm

June 5, 2007

Abstract

Chen, Sederberg, and Zheng introduced the notion of a μ-basis for a rational ruled surface in Chen et al. (2001) and showed that its resultant is the implicit equation of the surface, if the parametrization is generically injective. We generalize this result to the case of an arbitrary parametrization of a rational ruled surface. We also give a new proof for the corresponding theorem in the curve case and treat the reparametrization problem for curves and ruled surfaces. In particular, we propose a partial solution to the problem of computing a proper reparametrization for a rational ruled surface.

Introduction

Implicitization is a fundamental problem in Computer Aided Geometric Design and there are numerous applications related to it, e.g. the computation of the intersection of two ruled surfaces, see Fioravanti et al. (2005). The method of μ-bases (also known as "moving lines" or "moving surfaces") constitutes an efficient solution to the implicitization problem. Introduced in 1998 by Cox, Sederberg, and Chen for rational curves in Cox et al. (1998), it was generalized to ruled surfaces in Chen et al. (2001) and Chen and Wang (2003b). Whereas the curve case is very well understood and we know that the resultant of a μ-basis is the implicit equation to the power d, where d is the degree of the rational map induced by the parametrization, this result is still to be shown in its full generality (i.e. for arbitrary d) for ruled surfaces. We fill this gap by giving a proof, which relies on a geometric idea that reduces the ruled surface case to the curve case. From a computional point of view, μ-bases are in general more efficient than other resultant-based methods such as the ones introduced in Busé and Chardin (2005) or in Khetan (2003), since they are well adapted to the geometry of ruled surfaces.

1 μ-bases of rational planar curves

As we will need them later on, we will start with some known results about the μ-basis of a rational parametric planar curve $\mathcal{C}$ over an algebraically closed field $\mathbb{K}$ of arbitrary characteristic, i.e. one given by a parametrization map

$$\begin{array}{rccc} \Phi_{\mathcal{C}}: & \mathbb{P}^1 & \dashrightarrow & \mathbb{P}^2 \\ & (s:\bar{s}) & \mapsto & (f_0(s,\bar{s}):f_1(s,\bar{s}):f_2(s,\bar{s})) \end{array}$$

where each $f_i \in \mathbb{K}[s,\bar{s}] =: R$ is homogeneous of degree $n > 0$ and $g := gcd(f_0,f_1,f_2)$ is of degree strictly less than n. The first syzygy module of f_0, f_1, f_2 is defined as

$$Syz(f_0,f_1,f_2) = \{P \in R[x,y,z] \mid deg(P) \leq 1, P(f_0,f_1,f_2) = 0\} \subseteq R[x,y,z]$$

Then we have the following well-known result.

Theorem 1 *There exists an isomorphism of graded R-modules*

$$Syz(f_0,f_1,f_2) \cong R(-\mu_1) \oplus R(-\mu_2)$$

where $\mu_i \in \mathbb{N}$, $\mu_1 \leq \mu_2$ and

$$\mu_1 + \mu_2 = n - deg(g) = deg(\Phi_{\mathcal{C}}) \cdot deg(\mathcal{C}) =: d$$

The isomorphism in the above theorem is a direct consequence of the Hilbert-Burch Theorem (see Eisenbud (1995)[Th. 20.15]) applied to the exact sequence

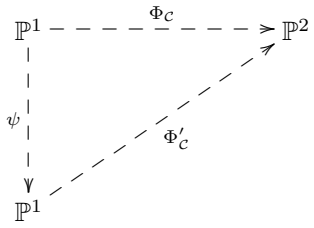
$$0 \to Syz(f_0,f_1,f_2)(-n) \to R^3(-n) \to R \to R/I \to 0$$

and the degree property can easily be checked by computing the Hilbert polynomials of this sequence.

A basis (p,q) of $Syz(f_0,f_1,f_2)$ with minimal degrees $deg(p) = \mu_1$ and $deg(q) = \mu_2$ in s and $\bar{s}$ is called a μ-basis of the parametrization $\Phi_{\mathcal{C}}$. One interesting feature of μ-bases is that the resultant of its elements is a power of the implicit equation of $\mathcal{C}$, as was proved in (Cox et al., 1998, Sect. 4, Th. 1). We propose an alternative proof which relies on the idea that we can reduce the problem to the generically injective case. The essential tool for this reduction is the existence of a proper reparametrization, which is a consequence of Lüroth's Theorem, a proof of which can be found for example in (van der Waerden, 1970, Section 5.4). In the following lemma we deduce a reparametrization with an additional property.

Lemma 2 *There exists $\psi : \mathbb{P}^1 \dashrightarrow \mathbb{P}^1$ parametrized by two coprime homogeneous polynomials h_0 and h_1 of degree $deg(\Phi_{\mathcal{C}})$ and a parametrization Φ' of $\mathcal{C}$*

defined by homogeneous polynomials $f'_0(s,\bar{s})$, $f'_1(s,\bar{s})$ *and* $f'_2(s,\bar{s})$ *such that the following diagram commutes:*



It follows that $\Phi'_{\mathcal{C}}$ *is a proper (i.e. generically injective) parametrization of* $\mathcal{C}$*, in other words* $deg(\Phi'_{\mathcal{C}}) = 1$*. Moreover, if* $gcd(f_0, f_2) = gcd(f_1, f_2) = 1$*, we can choose* $\Phi'_{\mathcal{C}}$ *such that* $f_i = f'_i(h_0, h_1)$ *for* $i \in \{0, 1, 2\}$*.*

Proof: First, we treat the case $gcd(f_0, f_2) = gcd(f_1, f_2) = 1$. Then we can dehomogenize $\frac{f_0}{f_2}$ and $\frac{f_1}{f_2}$ by setting $\bar{s} = 1$ without changing the degree as rational functions and decompose them by means of Lüroth's Theorem (van der Waerden, 1970, Section 5.4)) in the following way

$$\frac{f_0}{f_2} = \frac{f'_0}{f'_2} \circ \frac{h_0}{h_1} \qquad\qquad \frac{f_1}{f_2} = \frac{f'_1}{f'_2} \circ \frac{h_0}{h_1}$$

with $gcd(h_0, h_1) = gcd(f'_0, f'_2) = gcd(f'_1, \tilde{f}'_2) = 1$ and $deg(h_0) = deg(h_1) = deg(\Phi_{\mathcal{C}})$ after having rehomogenized them with respect to $\bar{s}$. By multiplying the fractions with a suitable power of h_1 we can consider the f'_i as bivariate homogeneous polynomials

$$\frac{f_0}{f_2} = \frac{f'_0(h_0,h_1)}{f'_2(h_0,h_1)} \qquad\qquad \frac{f_1}{f_2} = \frac{f'_1(h_0,h_1)}{f'_2(h_0,h_1)}$$

Then the numerators and denominators are all coprime, which for the right hand sides follows from (Zippel, 1991, Prop. 6) and we deduce the term-by-term equalities $f_i = f'_i(h_0, h_1)$ for $i \in \{0, 1, 2\}$.
In the general case, we divide the polynomials of the parametrization by their greatest common divisor and perform a generic coordinate change in order to pass to another parametrization of $\mathcal{C}$ which fulfills $gcd(f_0, f_2) = gcd(f_1, f_2) = 1$ and whose polynomial decomposition completes the commutative diagram of rational maps. □

Now we are ready to proceed to the main theorem of this section, for which we give a new proof that establishes a link between the μ-basis of $\Phi_{\mathcal{C}}$ and a μ-basis of a proper reparametrization of the curve.

Theorem 3 *Let* (p, q) *be a* μ*-basis of the parametrization* $\Phi_{\mathcal{C}} : \mathbb{P}^1 \dashrightarrow \mathbb{P}^2$*. Then*

$$Res(p, q) = F_{\mathcal{C}}^{deg(\Phi_{\mathcal{C}})}$$

where $F_{\mathcal{C}}$ is an implicit equation of the curve $\mathcal{C}$ defined by $\Phi_{\mathcal{C}}$ and $Res(p,q) \in \mathbb{K}[x,y,z]$ is the homogeneous resultant with respect to the indeterminates s and $\bar{s}$.

Proof: First of all, we may assume that $gcd(f_0, f_2) = gcd(f_1, f_2) = 1$ (if necessary, we divide by $gcd(f_0, f_1, f_2)$ and perform a generic coordinate change, both of which do not affect the result). So by Lemma 2 there exist $f_0', f_1', f_2' \in R$ and homogeneous, coprime $h_0, h_1 \in R$ of degree $deg(\Phi_{\mathcal{C}})$, such that

$$\begin{aligned} f_0 &= f_0'(h_0, h_1) \\ f_1 &= f_1'(h_0, h_1) \\ f_2 &= f_2'(h_0, h_1) \end{aligned}$$

Let (p', q') be a μ-basis of the proper reparametrization $\Phi_{\mathcal{C}}'$ of $\mathcal{C}$ defined by the f_i'. Then $p'(h_0, h_1)$ and $q'(h_0, h_1)$ are linearly independent syzygies (i.e. we substitute h_0 for s and h_1 for $\bar{s}$). It is easy to see that they form a μ-basis by verifying the degree property and if $\mu_1 < \mu_2$, they are related to our original μ-basis (p, q) by

$$\begin{aligned} p'(h_0, h_1) &= \lambda p \\ q'(h_0, h_1) &= ap + q \end{aligned}$$

for some constant $\lambda \neq 0$ and a homogeneous $a \in R$ of degree $deg(q) - deg(p)$. (If $\mu_1 = \mu_2$, we have $p' \circ h = \alpha_1 p + \alpha_2 q$ and $q' \circ h = \beta_1 p + \beta_2 q$ for some constants α_i and β_i (see (Chen and Wang, 2003a, Th. 2)), which leads to computations that are analogous to the ones that follow).
Now we can apply elementary properties of resultants to calculate

$$\begin{aligned} Res(p,q) &= \lambda^{-\mu_2} \cdot Res(\lambda p, ap + q) \\ &= \lambda^{-\mu_2} \cdot Res(p'(h_0, h_1), q'(h_0, h_1)) \\ &= \lambda^{-\mu_2} \cdot Res(h_0, h_1)^{deg(p')deg(q')} \cdot Res(p', q')^{deg(h_0)} \\ &= c \cdot Res(p', q')^{deg(\Phi_{\mathcal{C}})} \qquad (c \in \mathbb{K}^*) \quad (1) \end{aligned}$$

where $c = \lambda^{-\mu_2} \cdot Res(h_0, h_1)$ is a constant (since the h_i do not depend on x, y, z) and non-zero (because $gcd(h_0, h_1) = 1$). The third identity is a well-known base change formula for resultants, which is proved in (Jouanolou, 1991, 5.12), and in the last identity we used $deg(h_0) = deg(\Phi_{\mathcal{C}})$.
So by (1) we have reduced the theorem to the special case where the parametrization has degree 1, and it remains to show:

$$\begin{aligned} &a) \quad Res(p', q') \neq 0 \\ &b) \quad F_{\mathcal{C}} \mid Res(p', q') \\ &c) \quad deg_{x,y,z}(Res(p', q')) \leq deg(\mathcal{C}) \end{aligned}$$

a) Suppose $p = G \cdot H$ were reducible into non-constant $G, H \in R[x, y, z]$, then one of the two, say G, would be independent of x, y, z, because p is linear in those variables and H would define a syzygy with lower degree than p which

contradicts the definition of a μ-basis. So p is irreducible in $R[x, y, z]$ and $Res(p, q) = 0$ would mean that $q = r \cdot p$ with $r \in R$, which is impossible, for p and q are linearly independent over R. Hence $Res(p, q) \neq 0$ and by (1) also $Res(p', q') \neq 0$.

b) By construction p and q vanish for all points in $Im(\Phi_{\mathcal{C}})$. So for any $X = (x_1 : x_2 : x_3) \in Im(\Phi_{\mathcal{C}})$ we have that $p(X) = q(X) = 0$ which rests true after setting $\bar{s} = 1$, so the two univariate polynomials have a common zero and therefore $Res(p(X), q(X)) = (Res(p, q))(X) = 0$. Again, by (1) we have $(Res(p', q'))(X) = 0$ as well and it follows that the implicit equation $F_{\mathcal{C}}$ divides $Res(p', q')$.

c) All the coefficients of p and q are of degree ≤ 1 in x, y, z, so we can give an upper bound for the degree of the resultant in x, y, z:

$$deg_{x,y,z}(Res(p, q)) \leq deg(p) + deg(q) = d = deg(\Phi_{\mathcal{C}})deg(\mathcal{C})$$

Once again we look at (1) to deduce that $deg_{x,y,z}(Res(p', q')) \leq deg(\mathcal{C})$ which concludes the proof. □

2 Implicitization of rational ruled surfaces with μ-bases

Chen, Sederberg, and Zheng introduced the notion of a μ-basis for rational ruled surfaces in Chen et al. (2001), and it was further developed in Chen and Wang (2003b). However, they worked with the restrictive assumption that the parametrization is generically injective. In this section, we will give a proof for the ruled surface version of Theorem 3 in its general form and explain to what extent the ruled surface case can be reduced to the curve case.
In this paper, a rational ruled surface $\mathcal{S}$ is meant to be a surface given by a rational map

$$\begin{array}{rccc} \Phi_{\mathcal{S}} : & \mathbb{P}^1 \times \mathbb{P}^1 & \dashrightarrow & \mathbb{P}^3 \\ & ((s : \bar{s}), (t : \bar{t})) & \mapsto & (f_0(s, \bar{s}, t, \bar{t}) : \ldots : f_3(s, \bar{s}, t, \bar{t})) \end{array}$$

where the $f_i \in \mathbb{K}[s, \bar{s}, t, \bar{t}]$ are bihomogeneous of degree $(n, 1)$, by which we mean that they are homogeneous of degree $n + 1$ and that $deg_{s,\bar{s}}(f_i) = n$ and $deg_{t,\bar{t}}(f_i) = 1$ for all $i = 0, \ldots, 3$. We assume that $gcd(f_0, \ldots, f_3) = 1$ and that we can rewrite

$$f_i = \bar{t}\bar{s}^{n_1 - n_0} f_{i0} + t f_{i1} \tag{2}$$

where $f_{i0}, f_{i1} \in \mathbb{K}[s, \bar{s}]$ and $n_0 := max(deg_s(f_{i0}))$ and $n_1 := max(deg_s(f_{i1}))$, and where we have assumed that $n_1 \geq n_0$ (otherwise we may reparametrize (2) by exchanging t and $\bar{t}$) and $n_1 = n$ (otherwise, we may divide the f_i by a suitable power of $\bar{s}$). Finally, we need to make the assumption that $(f_{00}, \ldots, f_{30})$ and $(f_{01}, \ldots, f_{31})$ are R-linearly independent to exclude the degenerate case where $\Phi_{\mathcal{S}}$ does not parametrize a surface.

Let us fix some notation first: The R-module of syzygies on $f_0, \ldots, f_3$ depending only on s and $\bar{s}$ is defined as

$$Syz_R(f_0, \ldots, f_3) = \{P \in R[x, y, z, w] \mid deg(P) = 1, P(f_0, f_1, f_2, f_3) = 0\}$$

Then the structure of this module is well known; see Chen et al. (2001) for a proof of the following

Theorem 4 *There exists an isomorphism of graded R-modules*

$$Syz_R(f_0, \ldots, f_3) \cong R(-\mu_1) \oplus R(-\mu_2)$$

where $\mu_i \in \mathbb{N}$, $\mu_1 \leq \mu_2$ and $\mu_1 + \mu_2 = deg(\Phi_{\mathcal{S}}) \cdot deg(\mathcal{S})$.

A basis (q_1, q_2) of $Syz_R(f_0, f_1, f_2, f_3)$ where q_1 and q_2 are homogeneous of minimal degrees $deg(q_1) = \mu_1$ and $deg(q_2) = \mu_2$ in s and $\bar{s}$ is called a μ-basis of the parametrization $\Phi_{\mathcal{S}}$. As we can see, the syzygy module of the surface $\mathcal{S}$ resembles the one of a curve, which leads to the following question: is there a curve with the same syzygy module which can be defined by means of the surface parametrization? The answer to this question is positive and according to an idea due to Busé et al. (2007), we define the curve $\mathcal{C}$ associated to $\mathcal{S}$ by

$$\begin{array}{rccc} \Phi_{\mathcal{C}}: & \mathbb{P}^1 & \dashrightarrow & \mathbb{P}^2 \\ & (s:\bar{s}) & \mapsto & (p_{03}(s,\bar{s}) : p_{13}(s,\bar{s}) : p_{23}(s,\bar{s})) \end{array}$$

where $p_{ij} := f_{i0}f_{j1} - f_{i1}f_{j0} \in R$ are the Plücker coordinates, which are homogeneous of degree $n_1 + n_0$. Let us denote $g := gcd(p_{03}, p_{13}, p_{23})$.
The geometric idea behind this definition is that for almost all parameter values $(s : \bar{s}) \in \mathbb{P}^1$ the image of the map

$$\begin{array}{rccc} \Phi_{\mathcal{S}}((s:\bar{s}),-): & \mathbb{P}^1 & \dashrightarrow & \mathbb{P}^3 \\ & (t:\bar{t}) & \mapsto & (f_0(s,\bar{s},t,\bar{t}) : \ldots : f_3(s,\bar{s},t,\bar{t})) \end{array}$$

is a line $L_{(s:\bar{s})}$ in $\mathbb{P}^3$, hence the surface $\mathcal{S}$ can be viewed as the closure of the union of these lines. The curve defined by all the Plücker coordinates

$$\begin{array}{rccc} \Psi: & \mathbb{P}^1 & \dashrightarrow & \mathbb{P}^5 \\ & (s:\bar{s}) & \mapsto & (p_{ij})_{i,j\in\{0,\ldots,3\},\, i<j} \end{array}$$

is contained in a quadric parametrizing the lines in $\mathbb{P}^3$, more precisely there is a one-to-one correspondance between the points $\Psi((s : \bar{s}))$ on the Plücker curve and the lines $L_{(s:\bar{s})}$ on the ruled surface $\mathcal{S}$, which will allow us to carry over the results about curves to the ruled surface case. However, it is more convenient to work with the curve $\Phi_{\mathcal{C}}$, which is a projection of Ψ to $\mathbb{P}^2$. As we will see, we need to make sure that this projection does not add any base points, which is the statement of the following lemma.

Lemma 5 *If* $gcd(f_{30}, f_{31}) = 1$ *then*

$$gcd(p_{03}, p_{13}, p_{23}) = gcd(p_{03}, p_{13}, p_{23}, p_{01}, p_{02}, p_{12})$$

Proof: Let us suppose $q = gcd(p_{03}, p_{13}, p_{23}) \neq 1$; the case $q = 1$ is trivial. We need to show that q divides the other Plücker coordinates as well. Euclidean division of the f_{ij} by q yields

$$f_{ij} = q \cdot \tilde{f}_{ij} + a_{ij}$$

We have the congruences

$$p_{ij} \equiv f_{i0}f_{j1} - f_{i1}f_{j0} \equiv a_{i0}a_{j1} - a_{i1}a_{j0} \qquad (mod\, q)$$

The other cases being analogous, we only show $p_{12} \equiv 0 \pmod{q}$, i.e. that $a_{10}a_{21} - a_{11}a_{20}$ is divisible by q. Since p_{13} and p_{23} are divisible by q, we can write $a_{10}a_{31} - a_{11}a_{30} = qr_1$ and $a_{20}a_{31} - a_{21}a_{30} = qr_2$, or equivalently $a_{21}a_{30} = a_{20}a_{31} - qr_2$ and $a_{11}a_{30} = a_{10}a_{31} - qr_1$. As $gcd(f_{30}, f_{31}) = 1$ it follows that not both f_{30} and f_{31} are divisible by q, so we may assume that one of the rests of the Euclidean division, say a_{30}, is non-zero. We have

$$a_{30}(a_{10}a_{21} - a_{11}a_{20}) = a_{10}(a_{20}a_{31} - qr_2) - a_{20}(a_{10}a_{31} - qr_1) = q \cdot (r_1 - r_2)$$

and as a_{30} is non-zero and prime to q, we conclude that $a_{10}a_{21} - a_{11}a_{20}$ is divisible by q. □

Later on, we will see in another context why the condition $gcd(f_{30}, f_{31}) = 1$ is necessary. We should note that it is non-restrictive, since it can always be achieved by a generic coordinate change. Next, we state a useful degree formula, which we will use to study the relationship between a ruled surface and its associated curve in more detail.

Proposition 6 (Degree Formula) *With the same notation and hypotheses as before the equality*

$$deg(\mathcal{S})deg(\Phi_{\mathcal{S}}) = n_1 + n_0 - deg(g)$$

holds.

Proof: This formula is an adaptation of the general result

$$deg(\mathcal{S})deg(\Phi_{\mathcal{S}}) = 2n - \sum_{p \in V(f_0,\ldots,f_3)} m_p$$

(see (Fulton, 1984, Prop. 4.4) for a proof, m_p is the multiplicity of p). Our formula follows by counting the base points $\sum_{p \in V(I)} m_p = deg(g) + (n_1 - n_0)$, where $n_1 - n_0$ is the trivial multiplicity of the base point $(\infty, 0) := ((1:0), (0:1))$ and where the other base points (including additional multiplicities of $(\infty, 0)$)

can be identified with the roots of g by elementary calculations. $\square$

Note that for characteristic zero $deg(\Phi_{\mathcal{S}})$ - and thus also $deg(\mathcal{S})$ - can be computed by means of gcd and resultant computations, see Pérez-Díaz and Sendra (2006).

Next, we proceed to relate $Syz_R(f_0, \ldots, f_3)$ to the syzygy module of the associated curve, given as

$$Syz(p_{03}, p_{13}, p_{23}) = \{P \in R[x, y, z] \mid deg(P) = 1, P(p_{03}, p_{13}, p_{23}) = 0\}$$

Proposition 7 *If $gcd(f_{30}, f_{31}) = 1$, then there exists a canonical isomorphism of graded R-modules*

$$Syz_R(f_0, \ldots, f_3) \cong Syz(p_{03}, p_{13}, p_{23})$$

and $deg(\Phi_{\mathcal{S}}) \cdot deg(\mathcal{S}) = deg(\Phi_{\mathcal{C}}) \cdot deg(\mathcal{C})$.

Proof: As a direct consequence of Theorem 1 and the degree formula, we obtain

$$deg(\Phi_{\mathcal{C}}) \cdot deg(\mathcal{C}) = n_1 + n_0 - deg(g) = deg(\Phi_{\mathcal{S}}) \cdot deg(\mathcal{S})$$

and it remains to construct an isomorphism of degree zero between the syzygy modules. Let $h_0x + h_1y + h_2z + h_3w \in Syz_R(f_0, \ldots, f_3)$. As it does not depend on t and $\bar{t}$, we can deduce from (2) that

$$\begin{array}{rcl} h_0f_{00} + h_1f_{10} + h_2f_{20} + h_3f_{30} & = & 0 \\ h_0f_{01} + h_1f_{11} + h_2f_{21} + h_3f_{31} & = & 0 \end{array}$$

By multiplying the first equation by f_{31} and the second one by f_{30} and by substracting the second from the first we get

$$h_0p_{03} + h_1p_{13} + h_2p_{23} = 0 \tag{3}$$

which is a syzygy on the p_{i3}. Hence, by setting $w = 0$ we obtain a well-defined morphism

$$\begin{array}{rccc} \varphi: & Syz_R(f_0, \ldots, f_3) & \rightarrow & Syz(p_{03}, p_{13}, p_{23}) \\ & h_0x + h_1y + h_2z + h_3w & \mapsto & h_0x + h_1y + h_2z \end{array}$$

which has obviously degree zero. Now φ is injective, because if $h_0 = h_1 = h_2 = 0$ for a syzygy on the f_i, then $h_3 = 0$ as well (as f_{30} and f_{31} are coprime and hence non-zero). To see why it is also surjective, let $h_0x+h_1y+h_2z \in Syz(p_{03}, p_{13}, p_{23})$ and by rewriting (3) we have

$$(h_0f_{00} + h_1f_{10} + h_2f_{20})f_{31} = (h_0f_{01} + h_1f_{11} + h_2f_{21})f_{30}$$

The assumption that f_{30} and f_{31} are coprime implies that there is a polynomial $h \in K[s, \bar{s}]$ such that

$$hf_{30} = h_0 f_{00} + h_1 f_{10} + h_2 f_{20} \tag{4}$$

and by substituting this in the above equation also $hf_{31} = h_0 f_{01} + h_1 f_{11} + h_2 f_{21}$. These two relations show that $h_0 x + h_1 y + h_2 z - hw \in Syz_R(f_0, \ldots, f_m)$ is a preimage of $h_0 x + h_1 y + h_2 z$, hence φ is surjective and the proof is complete. □

Corollary 8 *If we perform a generic coordinate change beforehand, we also have $deg(\mathcal{S}) = deg(\mathcal{C})$ and $deg(\Phi_{\mathcal{S}}) = deg(\Phi_{\mathcal{C}})$ in the situation of the preceding Proposition 7.*

Proof: As we have seen in the proof of the proposition, the associated curve is obtained by intersecting the surface with the plane $w = 0$ and the isomorphism of the syzygy modules is induced by the projection map. If this plane is generic, the theorem of Bézout ensures that this intersection preserves the degree. □

An important remark is that the inverse of φ in the proof of Proposition 7 can be described explicitly as

$$\begin{array}{rccl} \varphi^{-1}: & Syz(p_{03}, p_{13}, p_{23}) & \to & Syz_R(f_0, \ldots, f_3) \\ & h_0 x + h_1 y + h_2 z & \mapsto & h_0 x + h_1 y + h_2 z - \dfrac{h_0 f_{00} + h_1 f_{10} + h_2 f_{20}}{f_{30}} w \end{array} \tag{5}$$

by using equation (4).It is of degree 0 and hence preserves degrees, so it takes μ-bases to μ-bases. This leads to an efficient method for the computation of the μ-basis of the surface: One computes the μ-basis of the associated curve and takes its image under φ^{-1}. See Section 3 for an explicit description of this algorithm.

One can regard the results in Theorem 4 as a corollary of Theorem 1 and Proposition 7. Let us also note that Theorem 1 and Theorem 4 can easily be generalized to higher dimension and the proofs are completely analogous to the ones given here. For example, the μ-basis of a curve in $\mathbb{P}^m$ consists of $m-1$ syzygies whose degrees in s and $\bar{s}$ sum up to d. We are now ready to show our main result.

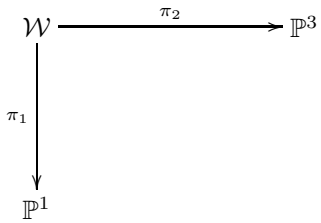
Theorem 9 *Let (q_1, q_2) be a μ-basis of the parametrization $\Phi_{\mathcal{S}} : \mathbb{P}^1 \times \mathbb{P}^1 \dashrightarrow \mathbb{P}^3$. Then*

$$Res(q_1, q_2) = F_{\mathcal{S}}^{deg(\Phi_{\mathcal{S}})}$$

where $F_{\mathcal{S}}$ is an implicit equation of the ruled surface $\mathcal{S}$ and where the resultant is taken with respect to s and $\bar{s}$.

Proof: First, we can ensure that the hypotheses of Proposition 7 are fulfilled by performing a generic linear coordinate change in $\mathbb{P}^1 \times \mathbb{P}^1$, which leaves both the implicit equation and the resultant unchanged (up to multiplication by a constant). We will show that $Res(q_1, q_2)$ is the power of an irreducible polynomial, i.e. that it defines an irreducible hypersurface in $\mathbb{P}^3$. Let

us consider the incidence variety $\mathcal{W} := \{(\ (s_0 : \bar{s_0}), (x_0 : y_0 : z_0 : w_0)) \in \mathbb{P}^1 \times \mathbb{P}^3 \mid q_i(s_0, \bar{s_0}, x_0, y_0, z_0, w_0) = 0\ \}$ then we have the following diagram



where π_1 and π_2 are the canonical projections. $\mathcal{W}$ is a vector bundle over $\mathbb{P}^1$, as the q_i are linear in x, y, z, and w, and for any parameter $(s_0 : \bar{s_0})$ the fiber is a $\mathbb{K}$-vector space of codimension 2 (because $q_1(s_0, \bar{s_0})$ and $q_2(s_0, \bar{s_0})$ are linearly independent, as was proved in (Chen and Wang, 2003b, Sect. 2, Prop. 3)). As $\mathbb{P}^1$ is irreducible, it follows that $\mathcal{W}$ is irreducible too (see (Shafarevich, 1977, Ch.6, Th.8)), hence so is $Im(\pi_2)$. (If $Im(\pi_2) = A \cup B$ for two closed sets A and B, $\mathcal{W} = \pi_2^{-1}(A) \cup \pi_2^{-1}(B)$, which implies $\mathcal{W} = \pi_2^{-1}(A)$ or $\mathcal{W} = \pi_2^{-1}(B)$, since $\mathcal{W}$ is irreducible and, consequently, $Im(\pi_2) = A$ or $Im(\pi_2) = B$). Now the points of $Im(\pi_2)$ are exactly those for which the q_i have a common zero in s and $\bar{s}$, so by definition of the resultant they are the zeros of $Res(q_1, q_2)$. In other words, we have shown that $V(Res(q_1, q_2)) = Im(\pi_2)$ is irreducible, so $Res(q_1, q_2)$ is the power of an irreducible polynomial.

By definition, the syzygies of $\Phi_{\mathcal{S}}$ vanish on all of $Im(\Phi_{\mathcal{S}})$ and hence on all of $\mathcal{S}$, so $F_{\mathcal{S}} \mid Res(q_1, q_2)$. This implies that $Res(q_1, q_2)$ is a power of $F_{\mathcal{S}}$ and it remains to verify that it has the correct degree $deg(\Phi_{\mathcal{S}}) \cdot deg(\mathcal{S})$.

In the proof of Theorem 7, we have seen the isomorphism of R-modules

$$\begin{array}{rccc} \varphi : & Syz_R(f_0, f_1, f_2, f_3) & \rightarrow & Syz(p_{03}, p_{13}, p_{23}) \\ & h_0 x + h_1 y + h_2 z + h_3 w & \mapsto & h_0 x + h_1 y + h_2 z \end{array}$$

between the syzygies of the parametrization $\Phi_{\mathcal{S}}$ and of the parametrization $\Phi_{\mathcal{C}}$ of its associated curve $\mathcal{C}$. By abuse of notation, we will not differentiate between φ and its extension to the morphism of R-algebras $\varphi : R[x, y, z, w] \rightarrow R[x, y, z]$ defined by $\varphi(x) = x$, $\varphi(y) = y$, $\varphi(z) = z$, and $\varphi(w) = 0$.

As remarked earlier on, φ takes μ-bases to μ-bases, so $(\varphi(q_1), \varphi(q_2))$ is a μ-basis of $\Phi_{\mathcal{C}}$. Applying Theorem 3 yields

$$\begin{array}{rcl} F_{\mathcal{C}}^{deg(\Phi_{\mathcal{C}})} & = & Res(\varphi(q_1), \varphi(q_2)) \\ & = & \varphi(Res(q_1, q_2)) \end{array}$$

where the last equality is true, because φ is the specialisation $w = 0$ and as such commutes with the resultant. Finally, we have $deg(\varphi(Res(q_1, q_2))) = deg(Res(q_1, q_2))$, as $Res(q_1, q_2)$ is homogeneous, which shows that

$$deg(Res(q_1, q_2)) = deg(\Phi_{\mathcal{C}}) \cdot deg(\mathcal{C}) = deg(\Phi_{\mathcal{S}}) \cdot deg(\mathcal{S})$$

so $Res(q_1, q_2)$ has indeed the correct degree, which concludes the proof. □

3 Algorithm and example

In this section, we give a detailed description of a new algorithm to compute a μ-basis of a rational ruled surface based on the one-to-one correspondence between the syzygies of a ruled surface and its associated curve: As we have remarked, a μ-basis of the ruled surface can be obtained by computing a μ-basis of its associated curve (e.g. with the algorithm presented in Chen and Wang (2003a)) and taking its image under the isomorphism (5) in the proof of Proposition 7. In particular, this method has the same computational complexity as the curve algorithm that is used (since all the other steps in the algorithm are immediate), which makes it very efficient.

While it is convenient to work in the homogeneous setting for theoretical considerations, actual computations should be done after dehomogenizing, i.e. setting $\bar{s} = 1$ and $\bar{t} = 1$ in the parametrization (2). In other words, we switch to the affine parametrization

$$\begin{array}{rccc} \Phi_{\mathcal{S}}^{\mathtt{aff}}: & \mathbb{K}^2 & \dashrightarrow & \mathbb{K}^3 \\ & (s,t) & \mapsto & (\frac{f_0(s,t)}{f_3(s,t)}, \frac{f_1(s,t)}{f_3(s,t)}, \frac{f_2(s,t)}{f_3(s,t)}) \end{array}$$

where $f_i = f_{i0}(s) + t f_{i1}(s) \in \mathbb{K}[s,t]$. We remark that bihomogeneous polynomials of a fixed degree are in one-to-one correspondence to their dehomogenized counterparts and that this correspondence commutes with syzygy computations, resultants, etc. As a consequence, all the results in this paper are equally valid in the affine setting, so the μ-basis and the implicit equation can be obtained by computing their affine analogues and then rehomogenizing them.

ALGORITHM (μ-basis of a ruled surface)

INPUT: $f_i \in \mathbb{K}[s,t]$ for $i = 0,1,2,3$

1. Check whether $deg_t(f_i) = 1$ for all i. If yes, set $f_{i0}(s) = f_i(s,0)$ and $f_{i1}(s) = \frac{d}{dt} f_i(s,t)$ for all i. If not, return an error message.

2. Check whether $max(deg_s(f_{i1})) \geq max(deg_s(f_{i0}))$. If not, interchange f_{i1} and f_{i0} for all $i = 0,1,2,3$.

3. Check whether $gcd(f_{30}, f_{31}) = 1$. If not, check if there is $i \in \{0,1,2\}$ such that $gcd(f_{i0}, f_{i1}) = 1$.
   - If there is such an i, interchange f_i and f_3.
   - If not, replace f_3 by $\alpha f_0 + \beta f_1 + \gamma f_2 + f_3$ for generic $\alpha, \beta, \gamma \in \mathbb{K}$.

4. Set $p_{i3} = f_{i0} f_{31} - f_{i1} f_{30}$ for $i = 0,1,2$.

5. Calculate a μ-basis $(\tilde{q}_1, \tilde{q}_2) = (q_{11}x + q_{12}y + q_{13}z, q_{21}x + q_{22}y + q_{23}z)$ of the curve defined by p_{03}, p_{13}, and p_{23} with an algorithm for planar curves.

6. Set $q_j = q_{j1}x + q_{j2}y + q_{j3}z - \frac{q_{j1}f_{00}+q_{j2}f_{10}+q_{j3}f_{20}}{f_{30}}$ for $j = 1, 2$.

OUTPUT: A μ-basis (q_1, q_2) of the parametrization $\Phi_{\mathcal{S}}^{\mathtt{aff}}$

Note that the second step of the algorithm may lead to a denser polynomial f_3 if a coordinate change is necessary, because the support of f_3 after such a change becomes the union of the supports of the f_i. However, f_0, f_1 and f_2 are not changed, as we only have to ensure the (relatively weak) condition $gcd(f_{30}, f_{31}) = 1$ and do not need "full" genericity.

Throughout the paper, we have considered a ruled surface to be given by a parametrization which has degree one in t. However, such a surface can also be defined by a parametrization of higher degree in t, so it would be interesting to give a criterion for when a given parametrization corresponds to a ruled surface and in this case to be able to replace it by another one which is linear in t.

Illustrative example

Let us consider the ruled surface $\mathcal{S}$ defined by the polynomials $\tilde{f}_0 = s^2+t(s^2-1)$, $\tilde{f}_1 = 1 + t(-s^2 + 1)$, $\tilde{f}_2 = 1 + t(-s^6 + 1)$, and $\tilde{f}_3 = t(-s^6 - 2s^2)$. As $\tilde{f}_{30} = 0$ and $\tilde{f}_3 = s^2$ are not coprime, we interchange $\tilde{f}_3$ and $\tilde{f}_0$ and consider the new parametrization of $\mathcal{S}$

$$\begin{aligned} f_0 &= t(-s^6 - 2s^2) \\ f_1 &= 1 + t(-s^2 + 1) \\ f_2 &= 1 + t(-s^6 + 1) \\ f_3 &= s^2 + t(s^2 - 1) \end{aligned}$$

where $gcd(f_{30}, f_{31}) = 1$.
Then its associated curve $\mathcal{C}$ is parametrized by the Plücker coordinates

$$p_{03} = s^8 + 2s^4 \qquad p_{13} = s^4 - 1 \qquad p_{23} = s^8 - 1$$

and we have $deg(\Phi_{\mathcal{C}}) \cdot deg(\mathcal{C}) = deg(\Phi_{\mathcal{S}}) \cdot deg(\mathcal{S}) = 8$ which follows from the degree formulae. Next we compute the following μ-basis for $\Phi_{\mathcal{C}}$ with a suitable algorithm:

$$\begin{aligned} \tilde{q}_1 &= (s^4 + 1)y - z \\ \tilde{q}_2 &= (-s^4 + 1)x - y + (s^4 + 1)z \end{aligned}$$

Applying the isomorphism φ^{-1} yields the following μ-basis for $\Phi_{\mathcal{S}}$

$$\begin{aligned} q_1 &= (s^4 + 1)y - z - s^2 \\ q_2 &= (-s^4 + 1)x - y + (s^4 + 1)z - s^2 \end{aligned}$$

and we obtain

$$\begin{aligned} Res(q_1, q_2) &= (4x^2y^2 - 4xy^3 + y^4 - 4x^2yz + 2xy^2z + x^2z^2 + 4xyz^2 \\ &\quad -2y^2z^2 - 2xz^3 + z^4 - x^2 + xy + 2y^2 - xz - 4yz + 2z^2)^2 \end{aligned}$$

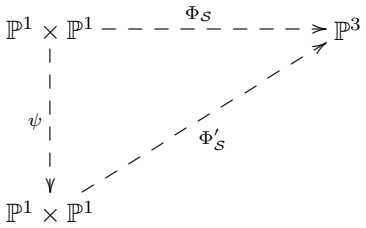
which is the square of an implicit equation $F_{\mathcal{S}}$ of $\mathcal{S}$.

We have seen and used the equality $deg(\Phi_{\mathcal{C}}) \cdot deg(\mathcal{C}) = deg(\Phi_{\mathcal{S}}) \cdot deg(\mathcal{S})$ between the surface $\mathcal{S}$ and its associated curve $\mathcal{C}$. It is natural to ask whether $deg(\mathcal{C}) = deg(\mathcal{S})$ also holds. However, this is not true in our example: we have $deg(\mathcal{C}) = 2$, but $deg(\mathcal{S}) = 4$. According, to the corollary to Proposition 7, we would have had to perform a generic coordinate change in order to ensure the equality of the degrees.

Let us compare the μ-basis method to some others. In our example, $F_{\mathcal{S}}^2$ is obtained as a determinant of a 8×8-matrix, the Sylvester matrix of q_1 and q_2. After dehomogenizing our surface and homogenizing back to $\mathbb{P}^2$ we can use approximation complexes to implicitize, as in Busé and Chardin (2005), and we obtain $F_{\mathcal{S}}^2$ as the quotient of a 28×28-determinant by a 12×12-determinant and an additional term that arises because we add a non-complete-intersection base point when passing from $\mathbb{P}^1 \times \mathbb{P}^1$ to $\mathbb{P}^2$, which is by far not as efficient. Another possibility is to use the classical formula $F_{\mathcal{S}}^2(w = 1) = Res(f_0 - xf_3, f_1 - yf_3, f_2 - zf_3)$ combined with an efficient method to calculate the resultant such as Khetan (2003). $F_{\mathcal{S}}^2$ is obtained as the determinant of 10×10-matrix, which is larger than our Sylvester matrix and whose entries are themselves determinants of smaller matrices.

4 Remark on the reparametrization problem for ruled surfaces

In the proof of Theorem 3 about the implicit equation of a planar curve, we reduced the general case to the proper case by reparametrizing the curve. If the field $\mathbb{K}$ is of characteristic zero, we know by the theorem of Castelnuovo that there exists a proper reparametrization for any rational surface, i.e. there exists a commutative diagram



where $\psi = (\sigma, \tau)$ is of degree $deg(\mathcal{S})$ and $\Phi'_{\mathcal{S}}$ is a proper reparametrization of $\mathcal{S}$.

As far as we know, this problem is yet to be solved algorithmically. However, Pérez-Díaz (2006) gives a criterion for the existence of a reparametrization of a rational surface such that $\sigma = \sigma(s, \bar{s})$ depends only on s and $\bar{s}$ and $\tau = \tau(t, \bar{t})$ depends only on t and $\bar{t}$ and proposes an algorithm for its computation if it exists. If we restrict our attention to ruled surfaces we can also treat the case where $\tau = (\bar{t}\alpha + t\beta, \bar{t}\gamma + t\delta)$ with $\alpha, \beta, \gamma, \delta \in \mathbb{K}[s, \bar{s}]$ such that $\alpha\delta - \beta\gamma \neq 0$ by using the associated curve. So let us suppose that there exists a reparametrization such that we can write

$$f_i = \bar{t}(\alpha f'_{i0}(\sigma) + \gamma f'_{i1}(\sigma)) + t(\beta f'_{i0}(\sigma) + \delta f'_{i1}(\sigma)) \tag{6}$$

for $i = 0, \ldots, 3$, where the f'_{ij} define a proper parametrization $\Phi'_{\mathcal{S}}$ of $\mathcal{S}$. We can deduce that $deg(\psi) = deg(\sigma) = deg(\Phi_{\mathcal{S}})$, because τ is a homography with respect to t. We have the following identity

$$p_i = \begin{vmatrix} f_{i0} & f_{i1} \\ f_{30} & f_{31} \end{vmatrix} = \begin{vmatrix} \alpha f'_{i0}(\sigma) + \gamma f'_{i1}(\sigma) & \beta f'_{i0}(\sigma) + \delta f'_{i1}(\sigma) \\ \alpha f'_{30}(\sigma) + \gamma f'_{31}(\sigma) & \beta f'_{30}(\sigma) + \delta f'_{31}(\sigma) \end{vmatrix} = (\alpha\delta - \beta\gamma) p'_i(\sigma)$$

from which we conclude that σ yields a proper reparametrization of the associated curve in the generic case $deg(\Phi_{\mathcal{S}}) = deg(\Phi_{\mathcal{C}})$. On the other hand, any $\lambda(s, \bar{s})$ defining a proper reparametrization $p_i = p''_i(\lambda)$ of $\mathcal{C}$ differs from σ only by a homography, so we can assume $\lambda = \sigma$, which provides us with a (naive) method for calculating the reparametrization: We compute σ with a reparametrization algorithm for curves such as in Pérez-Díaz (2006) and consider (6) as a linear system of equations by comparing the coefficients of the left hand side and the right hand side, where we leave the coefficients of $\alpha, \beta, \gamma, \delta$ and the f'_{ij} undetermined. Then any solution of this system defines a proper reparametrization of the ruled surface. However, the systems are generally too large and further research is needed to develop an efficient algorithmic solution to the reparametrization problem.

5 Acknowledgements

The author was partially supported by the French ANR "Gecko" and the European project ACS nr. IST FET open 6413.

References

Busé, L., Chardin, M., 2005. Implicitizing rational hypersurfaces using approximation complexes. J. Symbolic Comput. 40 (4-5), 1150–1168.

Busé, L., Elkadi, M., and Galligo, A., 2007. A computational study of ruled surfaces, accepted to appear in *J. Symbolic Comput.*

Chen, F., Wang, W., 2003a. The μ-basis of a planar rational curve - properties and computation. Graphical Models 64, 368–381.

Chen, F., Wang, W., 2003b. Revisiting the μ-basis of a rational ruled surface. J. Symbolic Comput. 36 (5), 699–716.

Chen, F., Zheng, J., Sederberg, T. W., 2001. The mu-basis of a rational ruled surface. Comput. Aided Geom. Design 18 (1), 61–72.

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

Eisenbud, D., 1995. Commutative algebra with a view toward algebraic geometry. Vol. 150 of Graduate Texts in Mathematics. Springer-Verlag, New York.

Fioravanti, M., Gonzalez-Vega, L., Necula, I., 2005. Computing the intersection of two ruled surfaces. In: Proc. of Algorithmic Algebra and Logic. Conference in Honor of the 60 th. Birthday of Volker Weispfenning. pp. 187–194.

Fulton, W., 1984. Intersection Theory. Springer Verlag.

Jouanolou, J.-P., 1991. Le formalisme du résultant. Adv. Math. 90, 117–263.

Khetan, A., 2003. The resultant of an unmixed bivariate system. J. Symbolic Comput. 36 (3-4), 425–442, international Symposium on Symbolic and Algebraic Computation (ISSAC'2002) (Lille).

Pérez-Díaz, S., 2006. On the problem of proper reparametrization for rational curves and surfaces. Comput. Aided Geom. Design 23 (4), 307–323.

Pérez-Díaz, S. and Sendra, J.R., 2004. Computation of the degree of rational surface parametrizations. J. Pure Appl. Algebra 193, 99–121.

Shafarevich, I. R., 1977. Basic algebraic geometry, study Edition. Springer-Verlag, Berlin, translated from the Russian by K. A. Hirsch, Revised printing of Grundlehren der mathematischen Wissenschaften, Vol. 213, 1974.

van der Waerden, B. L., 1970. Algebra. Vol 1. Translated by Fred Blum and John R. Schulenberger. Frederick Ungar Publishing Co., New York.

Zippel, R., 1991. Rational function decomposition. In: Proceedings of the 1991 international symposium on symbolic and algebraic computation. Bonn, Germany, pp. 1–6.