A computational study of ruled surfaces

Laurent Busé, Mohamed Elkadi, André Galligo

A computational study of ruled surfaces

Laurent Busé[1], Mohamed Elkadi[2] and André Galligo[2]

[1] *Galaad, INRIA Sophia Antipolis,*
2004 route des Lucioles, B.P. 93,
06902 Sophia-Antipolis, Cedex France.
lbuse@sophia.inria.fr

[2] *Université de Nice Sophia-Antipolis, Parc Valrose,*
BP 71, 06108 Nice Cedex 02, France.
{elkadi,galligo}@math.unice.fr

Abstract

We study rational ruled surfaces and μ-bases which were recently considered in a series of articles by Chen and coworkers. We give short and conceptual proofs with geometric insights and efficient algorithms. In particular, we provide a method to reparameterize an improper parameterization and we also briefly explain how to deal with approximate input data. Finally we provide an algorithmic description of self-intersection loci.

1. Introduction

During the XIXth (and the beginning of the XXth) century, many articles were dedicated to the study of algebraic ruled surfaces (see e.g. [10]) and more generally of rational ones. In the last decade, there has been a renewed interest in the subject, mainly driven by applications in Computer Aided Design and Manufacturing. A series of papers by Chen and coworkers ([3, 5, 6, 8]) attracted our attention. The question they initially addressed is: given a parameterization of a ruled surface (or a curve), get an implicit equation represented by the determinant of a matrix of linear forms, with a special structure.

In this paper, we rely on classical algebraic geometry to revisit and improve the works of Chen et al. to give shorter proofs and geometric insights. We also provide more efficient algorithms and we consider the case of approximate data, which is an important issue for the aimed applications.

The paper is organized in two parts. In the first one, we recall two classical geometric approaches on rational ruled surfaces and derive some consequences for simplifying parameterization of ruled surfaces with regards to properness and base points. In particular, we provide algorithms to reparameterize such surfaces in order to get proper parameterizations base point free. In the second part, we

review the notion of μ-basis introduced in [6]; we provide shorter and more conceptual proofs of existence of a μ-basis and also reparameterization as in [3]. On the way, we describe, analyze and compare different algorithms for computing such a μ-basis. Finally, we end this paper by applying these techniques to the computation of self-intersection loci of ruled surfaces.

In the following, $\mathbb{K}$ is assumed to be an infinite field, and $\mathbb{P}^n$ denotes the projective space of dimension n over $\mathbb{K}$. We are primarily interested by $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, however, except in the last section, the main results of this paper and the given proofs are valid on any field, with the following re-interpretation if $\mathbb{K}$ is a finite field. Some intermediate constructions in our proofs rely on taking "generic" elements in $\mathbb{K}$ but the final result will always be rational on $\mathbb{K}$. So, when $\mathbb{K}$ is a finite field the construction should be made in the algebraic closure of $\mathbb{K}$ which is infinite, and at the end, one goes back to $\mathbb{K}$ thanks to the rationality of the aimed result.

2. Rational ruled surfaces

An affine rational ruled surface is given by a parameterization

$$\begin{array}{rccl} \phi: & \mathbb{K}^2 & \to & \mathbb{K}^3 \\ & (s,t) & \mapsto & \left(\dfrac{f_{1,0}(s)+tf_{1,1}(s)}{f_{4,0}(s)+tf_{4,1}(s)}, \dfrac{f_{2,0}(s)+tf_{2,1}(s)}{f_{4,0}(s)+tf_{4,1}(s)}, \dfrac{f_{3,0}(s)+tf_{3,1}(s)}{f_{4,0}(s)+tf_{4,1}(s)}\right), \end{array} \quad (1)$$

where the $f_{i,j}$'s are polynomials in $\mathbb{K}[s]$. We set $f_i(s,t) := f_{i,0}(s) + tf_{i,1}(s)$ for $i = 1, \ldots, 4$, and $n_0 := \max_{i=1,\ldots,4} \deg(f_{i,0}(s))$, $n_1 := \max_{i=1,\ldots,4} \deg(f_{i,1}(s))$. We denote by $\mathcal{S}$ the closed image of ϕ, i.e. the smallest algebraic (irreducible) variety in $\mathbb{P}^3$ containing the image of ϕ and assume that it is a surface; this amounts to require that both vectors $(f_{1,0}(s), \ldots, f_{4,0}(s))$ and $(f_{1,1}(s), \ldots, f_{4,1}(s))$ are $\mathbb{K}[s]$-linearly independent. We assume moreover, for simplicity in the following discussions, that $\gcd(f_1(s,t), \ldots, f_4(s,t))$ is a (non-zero) constant.

Without loss of generality, we can assume that $n_1 \geq n_0$, since otherwise we can reparameterize $\mathcal{S}$ by substituting t by $1/t'$. For an algebraic and geometric study, we also consider the corresponding projective setting

$$\begin{array}{rccl} \phi^h: & \mathbb{P}^1 \times \mathbb{P}^1 & \to & \mathbb{P}^3 \\ & (s:\overline{s};t:\overline{t}) & \mapsto & (f_1^h : f_2^h : f_3^h : f_4^h)(s,\overline{s};t,\overline{t}) \end{array}$$

where, for $i = 1, \ldots, 4$, $f_i^h(s,\overline{s};t,\overline{t}) := \overline{t}\overline{s}^{n_1-n_0} f_{i,0}^h(s,\overline{s}) + tf_{i,1}^h(s,\overline{s})$, with $f_{i,1}^h(s,\overline{s})$ (resp. $f_{i,0}^h(s,\overline{s})$) being the homogenization of $f_{i,1}(s)$ (resp. of $f_{i,0}(s)$) of degree n_1 (resp. of degree n_0). Note that $\mathcal{S}$ is also the image of ϕ^h.

Hereafter, we will denote by $\deg(\phi)$ (resp. $\deg(\phi^h)$) the degree of the rational map ϕ (resp. ϕ^h) onto its image $\mathcal{S}$. This invariant roughly corresponds to the number of points in the preimage of a generic point on $\mathcal{S}$. In particular, if ϕ is generically injective, or equivalently if ϕ^h is generically injective onto $\mathcal{S}$, then $\deg(\phi) = \deg(\phi^h) = 1$ (we always have $\deg(\phi) = \deg(\phi^h)$).

2.1. Base points and the degree formula

We give here a formula to compute the degree of the ruled surface $\mathcal{S}$ in terms of polynomials defining its parameterization. Recall that a base point of the parameterization ϕ^h is a point in the parameter space $\mathbb{P}^1 \times \mathbb{P}^1$ which annihilates the polynomials $f_1^h, \ldots, f_4^h$. Since the base points are isolated by assumption, it is known that the quantity $\deg(\mathcal{S})\deg(\phi)$ equals $2n_1$ minus the number of these base points counted with multiplicities; as t appears linearly, their multiplicities are given by the order of $(s, \overline{s})$.

The point $(\infty, 0) \in \mathbb{P}^1 \times \mathbb{P}^1$ is a base point of multiplicity (at least) $n_1 - n_0$ and the other base points (including the possible increasing of the multiplicity of $(\infty, 0)$) are counted as the degree of the gcd $g^h(s, \overline{s})$ of all the 2×2 minors $\begin{vmatrix} f_{i,0}^h(s,\overline{s}) & f_{i,1}^h(s,\overline{s}) \\ f_{j,0}^h(s,\overline{s}) & f_{j,1}^h(s,\overline{s}) \end{vmatrix}$, $1 \leq i < j \leq 4$. The degree formula is hence

$$\deg(\mathcal{S})\deg(\phi) = n_1 + n_0 - \deg(g^h(s, \overline{s})). \tag{2}$$

It is straightforward to turn this formula into an "affine" version which is more suited for effective computations, by counting separately the base points with $\overline{s} = 0$.

Proposition 2.1: *With the above notations, we have*

$$\deg(\mathcal{S})\deg(\phi) = \max_{1 \leq i < j \leq 4} \left(\deg \begin{vmatrix} f_{i,0}(s) & f_{i,1}(s) \\ f_{j,0}(s) & f_{j,1}(s) \end{vmatrix} \right) - \deg(g(s)),$$

where $g(s) := \gcd\left(\begin{vmatrix} f_{i,0}(s) & f_{i,1}(s) \\ f_{j,0}(s) & f_{j,1}(s) \end{vmatrix} : 1 \leq i < j \leq 4 \right)$. *Moreover,* $\deg(g(s))$ *is the number of base points, counted with multiplicities, of* ϕ^h *which are at finite distance in* s.

2.2. Plücker coordinates and properness

In this paragraph we interpret the ruled surface $\mathcal{S}$ in its Plücker coordinates; this will permit us to reparameterize properly $\mathcal{S}$.

For almost all value of $(s : \overline{s}) \in \mathbb{P}^1$, the image of $\phi^h(s, \overline{s}; -)$ is a line in $\mathbb{P}^3$ that we denote by $D_{(s:\overline{s})}$. Thus, $\mathcal{S}$ is the closure of $\cup_{(s:\overline{s}) \in \mathbb{P}^1} D_{(s:\overline{s})}$. This gives rise to a geometric approach on ruled surfaces initiated by Plücker, Grassmann and Cayley. The line $D_{(s:\overline{s})}$ is represented by its Plücker coordinates

$$p_{i,j}(s, \overline{s}) := \begin{vmatrix} f_{i,0}^h(s,\overline{s}) & f_{i,1}^h(s,\overline{s}) \\ f_{j,0}^h(s,\overline{s}) & f_{j,1}^h(s,\overline{s}) \end{vmatrix}, \quad 1 \leq i < j \leq 4,$$

which satisfy the quadratic relation $Q := p_{1,2}p_{3,4} - p_{1,3}p_{2,4} + p_{1,4}p_{2,3} = 0$. Any point of the quadric $\mathcal{Q}$ of $\mathbb{P}^5$ (defined by the equation $Q = 0$) determines a

unique line in $\mathbb{P}^3$. Therefore, a rational ruled surface can be viewed as a rational curve $\mathcal{C}$ on $\mathcal{Q}$ in $\mathbb{P}^5$, and this curve is given by the parameterization

$$\begin{array}{rccc} \phi^G: & \mathbb{P}^1 & \to & \mathcal{Q}\subset\mathbb{P}^5 \\ & (s:\overline{s}) & \mapsto & (p_{i,j}(s,\overline{s}))_{1\le i<j\le 4}\,. \end{array}$$

Now, associated to the map ϕ^G, which parameterizes a curve, we have the inclusion of function fields $\mathbb{K}(\mathcal{C})\hookrightarrow\mathbb{K}(s)$. By Lurőth theorem [17, §10.2] there exists an intermediate field $\mathbb{K}(\sigma)$, which admits constructive and algorithmic versions (see e.g. [14]), where $\sigma=h(s)\in\mathbb{K}(s)$ and such that $p_{i,j}(s,1)=\tilde{p}_{i,j}(\sigma)$ and $(\tilde{p}_{i,j}(\sigma))_{1\le i<j\le 4}$ defines a *proper* parameterization of $\mathcal{C}$. We refer to these papers for algorithms and implementations of this property, even in the real setting ($\mathbb{K}=\mathbb{R}$). This result is now going to be used to prove the following proposition.

PROPOSITION 2.2: *An improper parameterization of a rational ruled surface can be replaced by a proper one via a change of parameterization in* $\mathbb{P}^1\times\mathbb{P}^1$:

$$(s,t)\mapsto(\sigma,\tau):=\left(h(s),\frac{\lambda_1(s)+t\Lambda_1(s)}{\lambda_0(s)+t\Lambda_0(s)}\right)$$

where $\lambda_0(s)$,$\lambda_1(s)$,$\Lambda_0(s)$ *and* $\Lambda_1(s)$ *are in* $\mathbb{K}[s]$.

Proof: We take again the previous notation and fix σ. Via the proper reparameterization of the curve $\mathcal{C}$, all the lines D_s such that $h(s)=\sigma$ are equal in $\mathbb{P}^3$ to a line Δ_σ. Solving a linear system, we find two points $M_0(\sigma)$ and $M_1(\sigma)$ on Δ_σ with coordinates which are rational fuctions in σ. Hence, if $h(s)=\sigma$, any point of $D_s=\Delta_\sigma$ can be written as a linear combination $M_0(\sigma)+\tau M_1(\sigma)$, with τ in $\mathbb{P}^1$. Expanding this relation, we find four rational scalar functions $\lambda_0(s)$, $\lambda_1(s)$, $\Lambda_0(s)$, $\Lambda_1(s)$, such that $\tau=\lambda_1(s)+t\Lambda_1(s)$, $f_0(s)=\lambda_0(s)M_0(h(s))+\lambda_1(s)M_1(h(s))$ and $f_1(s)=\Lambda_0(s)M_0(h(s))+\Lambda_1(s)M_1(h(s))$. □

Before ending this paragraph, let us make another remark regarding this interpretation of $\mathcal{S}$ in terms of its Plücker coordinates. We will consider in the sequel a generic plane section of the ruled surface $\mathcal{S}$ given by a proper parameterization without base points, except the "trivial" one $(\infty,0)$ with multiplicity n_1-n_0. Consider a generic linear form, with coefficients in $\mathbb{K}$, $Z_1:=aX+bY+cZ+dT$. Then, the section $\mathcal{D}:\{Z_1=0\}$ of $\mathcal{S}$ satisfies

$$t=\frac{af_{1,0}(s)+bf_{2,0}(s)+cf_{3,0}(s)+df_{4,0}(s)}{af_{1,1}(s)+bf_{2,1}(s)+cf_{3,1}(s)+df_{4,1}(s)},$$

and hence (X,Y,Z) is proportional to the vector

$$(bp_{1,2}+cp_{1,3}+dp_{1,4},-ap_{1,2}+cp_{2,3}+dp_{2,4},-ap_{1,4}-bp_{2,4}-cp_{3,4}).$$

We see that the curve $\mathcal{D}$ is a projection on $\mathbb{P}^2$ of the curve $\mathcal{C}\subset\mathcal{Q}\subset\mathbb{P}^5$ attached to the ruled surface $\mathcal{S}$. Moreover, as a,b,c,d are generic coefficients, we can expect that $\mathcal{D}$ captures some of the features of $\mathcal{C}$, hence of $\mathcal{S}$. This will be the case as we will see in the next section.

2.3. Scrolls and base points

Another geometric point of view on rational ruled surfaces, initiated by Segre, is to consider them as projection of a surface in a higher projective space. Such a surface is nowadays denoted by $\mathbb{F}(n_0, n_1)$ and called a scroll in $\mathbb{P}^N$ with $N = n_0 + n_1 + 1$. It is obtained by considering two Veronese parameterized curves of respective degree n_0 and n_1 in $\mathbb{P}^{n_0}$ and $\mathbb{P}^{n_1}$, respectively. Then, $\mathbb{F}(n_0, n_1)$ is the union of the lines joining the points with same parameters in $\mathbb{P}^N$. Its parameterization is simply:

$$\begin{array}{rcl} \mathbb{K}^2 & \to & \mathbb{P}^N \\ (s,t) & \mapsto & (1 : s : s^2 : \cdots : s^{n_0} : t : ts : ts^2 : \cdots : ts^{n_1}). \end{array}$$

This gives rise to a natural and refined presentation of ruled surfaces in $\mathbb{P}^3$ which will allow us to reparameterize ϕ without base points, except the trivial one $(\infty, 0)$ with multiplicity $n_1 - n_0$.

Let us say that ϕ is of type $((n_0, n_1), 1)$ if it satisfies (1) (recall that $n_1 \geq n_0$). The couple $(n_1, 1)$ is the bidegree of the map ϕ^h in the projective setting. By abuse of language, we will say that such a parameterization is *base point free* if the obvious base point is the only base point with the lowest possible multiplicity $n_1 - n_0$. In this case, the degree of $\mathcal{S}$ is $n_0 + n_1$.

PROPOSITION 2.3: *Suppose that $\mathcal{S}$ is a ruled surface in $\mathbb{P}^3$ given by a proper parameterization $\phi^h : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$ of bidegree $(n, 1)$ with m base-points, counted with multiplicities. Then, there exists a parameterization ψ of type $((n_0, n_1), 1)$ of $\mathcal{S}$ which is base-point free and such that with $2n - m = n_0 + n_1$. Moreover the morphism of reparameterization $\Lambda : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^1 \times \mathbb{P}^1$, which satisfies $\phi = \psi o \Lambda$, is such that for any s, $\Lambda(s,t) = (\sigma, \tau)$ where τ is an homography in t with coefficients depending only on s.*

Proof: We proceed by induction. First suppose that among the m base-points of ϕ, there exist two points (s_1, t_1) and (s_2, t_2) such that $t_1 \neq t_2$. We perform an homography on $\mathbb{P}^1$ which sends t_1 to 0 and t_2 to ∞. If $s_1 = s_2$, then the new ϕ^h writes $\phi^h(s,t) = t(s - s_1)V_1(s) + (s - s_1)V_2(s)$, and simplifying by $s - s_1$, the number n decreases strictly. If $s_1 \neq s_2$, the new ϕ^h writes

$$\phi^h(s,t) = t(s - s_1)V_1(s) + (s - s_2)V_2(s).$$

We set $t = \dfrac{(s - s_2).\tau}{s - s_1}$, and we can simplify by $s - s_2$ to get a smaller number n.

Now, if all the remaining m_1 base points have the same first coordinate t_1, we send t_1 to 0. Then the new ϕ^h writes $\phi^h(s,t) = tV_1(s) + g(s)V_2(s)$, with $\deg(g) = m_1$. We set $t = g(s).\tau$, so we can simplify by $g(s)$, and we are done.

Finally, in all the performed changes of parameterizations we had the required property for $\Lambda(s,t)$, property which is stable by composition. □

PROPOSITION 2.4: *With the notations of the previous proposition, the coefficients of ψ belongs to the field generated by the coefficients of ϕ.*

Proof: We take again the notations of the previous proposition and its proof. The change of parameterization $\Lambda(s,t)$ leaves s unchanged. So, for a fixed generic s, the images of the two parameterizations ϕ and ψ give the same line that we call D_s. The Plücker coordinates of D_s are the six 2×2 determinants $p_{i,j} = f^h_{i,0}f^h_{j,1} - f^h_{i,1}f^h_{j,0}$, with $1 \leq i < j \leq 4$, considered in subsection 2.2. As we have seen in subsection 2.1, their gcd has degree m. Dividing out by this gcd we get six polynomials in s of degree $2n-m$, that we denote by $\overline{p}_{i,j}$.

Therefore $X_i = \psi_i(s,\tau)$, for $i = 1,\ldots,4$, satisfy the four linear equations of the form $\overline{p}_{i,j}X_k + \overline{p}_{j,k}X_i + \overline{p}_{k,i}X_j = 0$ corresponding to the vanishing of 3×3 determinants, and expressing that the point belongs to the line D_s. We expand, in the case $\tau = 0$ (respectively $\tau = \infty$), these conditions into a (large) linear system in the coefficients of ψ. The previous proposition says that this linear system admits a solution in the algebraic closure. By Cramer's rule, it also admits a solution in the field of the coefficients of ϕ. □

3. Notion of μ-basis

We begin with a review of the definition and some properties of a μ-basis of a rational plane curve that we will use in our approach to study and to construct a μ-basis of the ruled surface $\mathcal{S}$.

3.1. μ-basis of a plane rational curve

The notion of μ-bases of a rational plane curve appears first in the paper [8]. It is useful in Computer Aided Geometric Design (see [5, 16]).

Let $\mathcal{C}$ be a plane curve given by a parametric representation

$$\psi : (s,\overline{s}) \in \mathbb{P}^1 \mapsto \big(g_1(s,\overline{s}) : g_2(s,\overline{s}) : g_3(s,\overline{s})\big) \in \mathbb{P}^2 \ , \tag{3}$$

where g_1, g_2, g_3 are homogeneous polynomials in $\mathbb{K}[s,\overline{s}]$ of degree δ. We consider the first module of syzygies

$$\mathrm{Syz}(g_1,g_2,g_3) = \{(h_1,h_2,h_3) \in \mathbb{K}[s,\overline{s}]^3 : h_1g_1 + h_2g_2 + h_3g_3 = 0\} \subset \mathbb{K}[s,\overline{s}]^3$$

which fits in the exact sequence of $\mathbb{K}[s,\overline{s}]$-modules

$$0 \to \mathrm{Syz}(g_1,g_2,g_3) \to \mathbb{K}[s,\overline{s}]^3 \to I := (g_1,g_2,g_3) \to 0.$$

Let us denote by μ the smallest positive integer such that there exists a nonzero element of degree μ in $\mathrm{Syz}(g_1,g_2,g_3)$. It turns out that this syzygy module is *free* by Hilbert Syzygy Theorem ([11, corollary 19.7]). The Hilbert-Burch Theorem [11, theorem 20.15] shows that it has rank 2, and $\mathrm{Syz}(g_1,g_2,g_3)$ is a *graded*

free $\mathbb{K}[s,\overline{s}]$-module such that we have the following *graded* isomorphism (using standard notation)

$$\mathbb{K}[s,\overline{s}](-\mu)\oplus\mathbb{K}[s,\overline{s}](-d+\mu)\simeq \mathrm{Syz}(g_1,g_2,g_3)\subset\mathbb{K}[s,\overline{s}]^3, \tag{4}$$

with $d:=\delta-\deg\big(\gcd(g_1,g_2,g_3)\big)=\deg(\psi)\deg(\mathcal{C})$, where $\deg(\psi)$ denotes the degree of the parameterization ψ and $\deg(\mathcal{C})$ the degree of the curve $\mathcal{C}$.

DEFINITION 3.1: *A basis* $(\mathbf{p},\mathbf{q})$ *of* $\mathrm{Syz}(g_1,g_2,g_3)$ *is called a* μ*-basis of the parameterization (3) of* $\mathcal{C}$ *if* $\deg(\mathbf{p})=\mu$ *and* $\deg(\mathbf{q})=d-\mu$.

Of course a μ-basis of $\mathcal{C}$ is not unique; but if $(\mathbf{p}_1,\mathbf{q}_1)$ and $(\mathbf{p}_2,\mathbf{q}_2)$ are two different μ-bases such that $\deg(\mathbf{p}_i)\leq\deg(\mathbf{q}_i)$, for $i=1,2$, then there exist α,β in $\mathbb{K}^*$ and a homogeneous polynomial $h\in\mathbb{K}[s,\overline{s}]$ of degree $\deg(\mathbf{p}_2)-\deg(\mathbf{p}_1)$ which satisfy $\mathbf{p}_1=\alpha\mathbf{p}_2, \mathbf{q}_2=\beta\mathbf{q}_1+h\mathbf{p}_1$ (see e.g. [8]).

REMARK 3.2: *Any basis* $(\mathbf{p},\mathbf{q})$ *of* $\mathrm{Syz}(g_1,g_2,g_3)$ *such that* $\deg(\mathbf{p})+\deg(\mathbf{q})=d$ *is a* μ*-basis of the parameterization (3) of* $\mathcal{C}$.

Let $\mathbf{p}:=(p_1,p_2,p_3)$ and $\mathbf{q}:=(q_1,q_2,q_3)$ be the two elements of a μ-basis of the parameterization (3) of $\mathcal{C}$. It is possible to recover a parameterization of the curve $\mathcal{C}$. Indeed, the Hilbert-Burch Theorem also says that there exists $0\neq a\in\mathbb{K}[s,\overline{s}]$ such that

$$I=(g_1,g_2,g_3)=a\left(\begin{vmatrix} p_2 & q_2\\ p_3 & q_3\end{vmatrix},-\begin{vmatrix} p_1 & q_1\\ p_3 & q_3\end{vmatrix},\begin{vmatrix} p_1 & q_1\\ p_2 & q_2\end{vmatrix}\right),$$

where the ideal on the right hand side has codimension 2 and thus gives a reparameterization of $\mathcal{C}$. Note that the polynomial a is equal, up to a multiplication by a nonzero constant in $\mathbb{K}$, to the gcd of g_1,g_2 and g_3 in $\mathbb{K}[s,\overline{s}]$.

Now we assume that the polynomials g_1,g_2 and g_3 are relatively prime and we discuss the computation of a μ-basis of the associated rational curve. Two algorithms to compute a μ-basis of a rational plane curve has been presented in [16] and [5]. They proceed by rewriting rules, they are similar to Gröbner basis computation for a module, and require $O(d^2)$ arithmetic operations. Their strategy is to reduce a simple system of three generators of $Syz(g_1,g_2,g_3)$ to a μ-basis of $\mathcal{C}$ which contains two elements. These algorithms do not seem well suited for computing with approximate data, encountered in Computer Aided Geometric Design. We have implemented the algorithm in [5] (their constant in $O(d^2)$ is better than in [16]) in MAPLE in order to compare it with the algorithm that we describe below. It turns out that there is an important increase of the size of the coefficients during the computation; this will be illustrated by a table of experiments below.

Now we present a simple and more efficient algorithm which relies on basic linear algebra:

INPUT: Three homogeneous polynomials $g_1(s,\bar{s}), g_2(s,\bar{s}), g_3(s,\bar{s})$ in $\mathbb{K}[s,\bar{s}]$ of the same degree $\delta \geq 1$.
OUTPUT: A μ-basis $(\mathbf{p},\mathbf{q})$ of the rational curve parametrized by (3).
STRATEGY: Solve the linear system in the coefficients of $\mathbf{p}$ and $\mathbf{q}$ with respect to the monomial basis.

The corresponding matrix is similar to a Sylvester one but with three blocks defined respectively by g_1, g_2, g_3. This kind of structured matrix is called pseudo-Toeplitz and behaves nicely with respect to complexity of basic operations via Fast Fourier Transform, but also via a naive implementation as we will see. The integer μ can be deduced from the rank of this matrix, whose size is at most $d + [\frac{d}{2}] + 1 \times 3\big([\frac{d}{2}] + 1\big)$. Similarly, we obtain $\mathbf{q}$ as a solution of a pseudo-Toeplitz system of size at most $(2d - \mu + 1) \times 3(d - \mu + 1)$. It is known that solving such linear systems requires $O\big(d(\log d)^2\big)$ arithmetic operations (see [1]). Our experiments rely on MAPLE commands which are not optimized. We also implemented a floating point version using the MAPLE Linear Algebra package.

The examples show that the coefficients of μ-bases obtained by linear algebra are much shorter than the ones obtained by algorithms in ([5, 6]); and moreover their computation takes also less time, as indicated below. The use of floating point (double) is interesting because, in the generic cases, the error was smaller than 10^{-9}. The polynomials involved in our experiments are dense and randomly generated.

In the following table, *time* is given in seconds, *mdig* is the maximum number of digits in the coefficients of the computed μ-basis, "-" means that the computation is stopped after twenty minutes. The second array of this table is obtained using our algorithm and the third one using Chen-Wang algorithm.

degree	9	19	31	40	50
(time, mdig)	$(0.04, 27)$	$(0.2, 66)$	$(5, 106)$	$(13, 141)$	$(107, 178)$
(time, mdig)	$(3, 500)$	$(110, 2500)$	$(900, -)$	$(-, -)$	$(-, -)$

We notice that the algorithm running with floating points is much faster, as it takes 3 seconds for degree 100.

The advantage of our approach based on linear algebra is to compute with approximate data. The input parameterization of the curve $\mathcal{C}$ is given by polynomials g_1, g_2, g_3 of a fixed degree, but whose coefficients are known with some imprecision; similarly to the situation in the univariate approximate GCD (see [7, 12, 18]). Here, we want to compute an approximate μ-basis of the parameterization (3). First, we test if g_1, g_2, g_3 are coprime; this can be done with certification and efficiently using Rupprecht's algorithm (see [15]). Otherwise, we divide by the approximate gcd and replace g_1, g_2, g_3 by approximate polynomials $\tilde{g_1}, \tilde{g_2}, \tilde{g_3}$ which are coprime and define the same curve (within the given precision). Then, as above we form the matrix with pseudo-Toeplitz structure and we adapt the argument in [13] using SVD to compute the number μ and a certified solution within the precision.

3.2. μ-basis of a ruled surface

The notion of μ-bases was generalized to the case of a ruled surface in both papers ([5, 6]). The study of this notion for the parameterized ruled surface $\mathcal{S}$ is done through the graded $\mathbb{K}[s,\overline{s}]$-module $\mathrm{Syz}(f_1^h, f_2^h, f_3^h, f_4^h) \cap \mathbb{K}[s,\overline{s}]^4$, denoted by

$$\mathrm{Syz}_{\mathbb{K}[s,\overline{s}]}(f^h) = \{(h_1,h_2,h_3,h_4) \in \mathbb{K}[s,\overline{s}]^4 : h_1 f_1^h + h_2 f_2^h + h_3 f_3^h + h_4 f_4^h = 0\}.$$

We denote by μ the smallest positive integer such that there exists a nonzero element of degree μ in $\mathrm{Syz}_{\mathbb{K}[s,\overline{s}]}(f^h)$. We have the following proposition:

PROPOSITION 3.3: *The module* $\mathrm{Syz}_{\mathbb{K}[s,\overline{s}]}(f^h)$ *is a free graded* $\mathbb{K}[s,\overline{s}]$*-module of rank 2. More precisely, if* $d := \deg(\phi)\deg(\mathcal{S})$*, we have a graded isomorphism*

$$\mathbb{K}[s,\overline{s}](-\mu) \oplus \mathbb{K}[s,\overline{s}](-d+\mu) \simeq \mathrm{Syz}_{\mathbb{K}[s,\overline{s}]}(f^h) \subset \mathbb{K}[s,\overline{s}]^4.$$

Proof: We construct the claimed isomorphism as follows. Let $h = (h_1,h_2,h_3,h_4)$ be a homogeneous syzygy in $\mathrm{Syz}_{\mathbb{K}[s,\overline{s}]}(f^h)$. We easily deduce that

$$\begin{aligned} h_1(s,\overline{s})f_{1,0}^h(s,\overline{s}) + h_2(s,\overline{s})f_{2,0}^h(s,\overline{s}) + h_3(s,\overline{s})f_{3,0}^h + h_4(s,\overline{s})f_{4,0}^h(s,\overline{s}) &= 0, \\ h_1(s,\overline{s})f_{1,1}^h(s,\overline{s}) + h_2(s,\overline{s})f_{2,1}^h(s,\overline{s}) + h_3(s,\overline{s})f_{3,1}^h(s,\overline{s}) + h_4(s,\overline{s})f_{4,1}^h(s,\overline{s}) &= 0. \end{aligned}$$

We multiply the first line by $f_{3,1}^h(s,\overline{s})$, the second one by $f_{3,0}^h(s,\overline{s})$ and we substrate them to get $h_1|f_1^h f_3^h| + h_2|f_2^h f_3^h| + h_4|f_4^h f_3^h| = 0$. For $i = 1,2,4$, set $g_i := |f_i^h f_3^h|$. Then (h_1,h_2,h_4) is a homogeneous syzygy in $\mathrm{Syz}(g_1,g_2,g_3)$. Note that the curve $\mathcal{C} : (s,\overline{s}) \xrightarrow{\psi} \big(g_1(s,\overline{s}), g_2(s,\overline{s}), g_3(s,\overline{s})\big)$ is exactly the intersection of $\mathcal{S}$ with the plane $z = 0$. Consequently, we obtain a $\mathbb{K}[s,\overline{s}]$-homomorphism

$$\begin{aligned} \Phi : \mathrm{Syz}_{\mathbb{K}[s,\overline{s}]}(f^h) &\to \mathrm{Syz}(g_1,g_2,g_3) \\ (h_1,h_2,h_3,h_4) &\mapsto (h_1,h_2,h_4) \end{aligned}$$

which is injective (unless $f_{3,0}^h = f_{3,1}^h = 0$, in which case we change the section).

Consider a generic projective plane $Z_1 = aX + bY + cZ + dT = 0$ in $\mathbb{P}^3$. Then we change the coordinates such that Z_1 replaces Z. Since both polynomial vectors $(f_{1,0}^h, f_{2,0}^h, f_{3,0}^h, f_{4,0}^h)$ and $(f_{1,1}^h, f_{2,1}^h, f_{3,1}^h, f_{4,1}^h)$ are linearly independent over $\mathbb{K}[s,\overline{s}]$, and by the genericity of coefficients a,b,c,d, $f_{3,0}^h$ and $f_{3,1}^h$ are coprime. Now, Φ is an isomorphism. Indeed, let $(h_1,h_2,h_4) \in \mathrm{Syz}(g_1,g_2,g_3)$, then

$$\overline{s}^{n_1-n_0}(h_1 f_{1,0}^h + h_2 f_{2,0}^h + h_4 f_{4,0}^h) f_{3,1}^h = (h_1 f_{1,1}^h + h_2 f_{2,1}^h + h_4 f_{4,1}^h) f_{3,0}^h.$$

Since $\gcd(f_{3,0}^h, f_{3,1}^h) = 1$, $f_{3,0}^h$ divides $h_1 f_{1,0}^h + h_2 f_{2,0}^h + h_4 f_{4,0}^h$. Then, there exists a homogeneous polynomial $h \in \mathbb{K}[s,\overline{s}]$ such that

$$\begin{aligned} &\overline{s}^{n_1-n_0}(h_1 f_{1,0}^h + h_2 f_{2,0}^h + h_4 f_{4,0}^h) = h f_{3,0}^h \quad , \\ &h_1 f_{1,1}^h + h_2 f_{2,1}^h + h_4 f_{4,1}^h = h f_{3,1}^h. \end{aligned}$$

So $(h_1,h_2,-h,h_4) \in \mathrm{Syz}_{\mathbb{K}[s,\overline{s}]}(f^h)$. It is clear that Φ preserves the grading. To conclude the proof we use the isomorphism (4) and the fact that $\deg(\phi)\deg(\mathcal{S}) = \deg(\psi)\deg(\mathcal{C})$. □

The integer d involved in this proposition can be easily obtained from the parameterization of $\mathcal{S}$ using formula (2) or Proposition 2.1. Note also that, as we saw in the proof of this proposition, the study of a μ-basis of a ruled surface can be reduced to the study of a μ-basis of a generic plane section of this surface. This last remark is the cornerstone of our computational approach of μ-bases of ruled surfaces.

DEFINITION 3.4: *A basis of the* $\mathbb{K}[s,\overline{s}]$*-module* $\mathrm{Syz}_{\mathbb{K}[s,\overline{s}]}(f^h)$ *of minimal degree is called a* μ*-basis of the ruled surface* $\mathcal{S}$*.*

An algorithm is proposed in [6] which gives an explicit way to compute a μ-basis of the ruled surface $\mathcal{S}$. It is based on rewriting rules on a known system of four generators of $\mathrm{Syz}_{\mathbb{K}[s,\overline{s}]}(f^h)$. Here we give an efficient approach which reduces the study of μ-bases of $\mathcal{S}$ to μ-bases of an algebraic plane $\mathcal{C}$ via a plane section of the surface $\mathcal{S}$. Then we lift the μ-basis of this curve $\mathcal{C}$, computed by the method developed in the previous subsection, to a μ-basis of $\mathcal{S}$.

Our geometric strategy is to lift a μ-basis $(\mathbf{p},\mathbf{q})$ of a generic plane section $\mathcal{C}$ corresponding to $z=\eta$, given by three polynomials g_1, g_2, g_3, of the ruled surface $\mathcal{S}$ in order to construct a μ-basis of $\mathcal{S}$.

If $\mathbf{p}=(a_1,b_1,\delta_1)$ and $\mathbf{q}=(a_2,b_2,\delta_2)$, for $i=1,2$, let $\mathcal{L}_i = a_i(s)x+b_i(s)y+\delta_i(s)$ be the associated moving lines to $\mathbf{p}$ and $\mathbf{q}$. Consider the plane Π_i defined by $\mathcal{L}_i$ and the line $\mathcal{D}_s$ obtained from the parameterization of $\mathcal{S}$ when the parameter t is fixed, its equation is $a_i(s)x+b_i(s)y+c_i(s)z+d_i(s)=0$. Since $\delta_i(s)=\eta c_i(s)+d_i(s)$, the equation of Π_i is $a_i(s)x+b_i(s)y+c_i(s)(z-\eta)+\delta_i(s)=0$. Using a point in $\mathcal{D}_s$ which does not belong to the plane section, we compute $c_i(s)$ and we deduce $d_i(s)$. See the illustrative Figure 1.

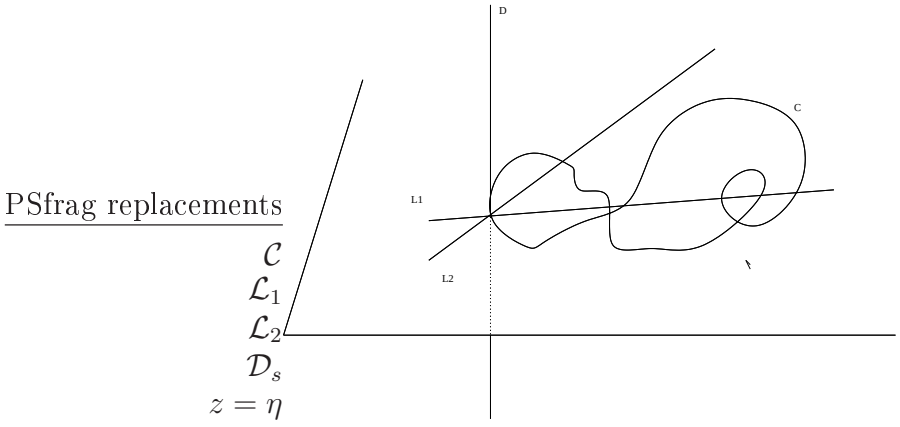


Figure 1: Lifting of a μ-basis from a generic plane section

3.3. Reparameterization of a ruled surface

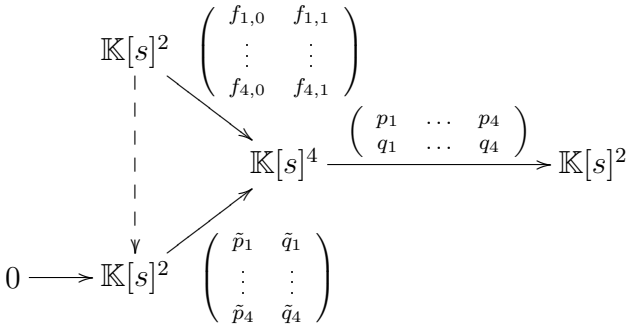
We now describe the use of μ-bases to give an algebraic method, alternative to the one presented in subsection 2.3, in order to reparameterize a ruled surface. We follow [4] but we shorten the proof.

PROPOSITION 3.5: *Let* $(\mathbf{p}, \mathbf{q})$ *be a* μ*-basis of the rational ruled surface* $\mathcal{S}$*. Denote by* $(\tilde{\mathbf{p}}, \tilde{\mathbf{q}})$ *a* μ*-basis of the ruled surface parameterized by* $\mathbf{p}(s) + t\mathbf{q}(s)$*. Then* $\tilde{\mathbf{p}}(s) + t\tilde{\mathbf{q}}(s)$ *is a base point free parameterization of* $\mathcal{S}$*.*

Proof: Set $\mathbf{p} := (p_1, \ldots, p_4)$ and $\mathbf{q} := (q_1, \ldots, q_4)$, and $\mathcal{M}_\phi$ the 2×4 matrix $(f_{i,j}(s))_{i=0,1;j=1,\ldots,4}$, with the notation of (1). Consider the exact sequence

$$0 \to \mathrm{Syz}_{\mathbb{K}[s]}(f) \xrightarrow{(\mathbf{p},\mathbf{q})} \mathbb{K}[s]^4 \xrightarrow{\mathcal{M}_\phi} \mathbb{K}[s]^2.$$

On one hand, the usual duality (apply $\mathrm{Hom}(-, \mathbb{K}[s])$) gives the following upper sequence which is exact in the middle. On the other hand, a μ-basis associated to the ruled surface $\mathbf{p}(s) + t\mathbf{q}(s)$, denoted here by $(\tilde{\mathbf{p}}, \tilde{\mathbf{q}})$, gives the lower exact sequence.



Therefore this diagram shows that, for almost all the values of s, both lines $(f_0(s), f_1(s))$ and $(\tilde{\mathbf{p}}(s), \tilde{\mathbf{q}}(s))$ are the same; so we get exactly the same surface. The absence of base points in the second parameterization comes from the property of minimality of the degree in a μ-basis. □

3.4. Implicitization and inversion

By Proposition 2.2 we can assume that the ruled surface $\mathcal{S}$ is given by a proper parameterization. The following results show that a μ-basis of $\mathcal{S}$ can be used to derive an implicit equation (see also [6, Theorem 3]) and compute an inversion formula for the ruled surface $\mathcal{S}$.

PROPOSITION 3.6: *Let* $(\mathbf{p}, \mathbf{q})$ *be a* μ*-basis of the ruled surface* $\mathcal{S}$*. The resultant* $\mathrm{Res}(P, Q)$ *of polynomials*

$$\begin{aligned} P &= p_1(s)x + p_2(s)y + p_3(s)z + p_4(s), \\ Q &= q_1(s)x + q_2(s)y + q_3(s)z + q_4(s) \end{aligned}$$

in the variable s *is exactly the implicit equation* $S(x, y, z)$ *of the surface* $\mathcal{S}$*.*

Proof: First, observe that this resultant is not identically zero; otherwise P and Q would have a common factor in $\mathbb{K}[s]$, which contradicts the fact that $(\mathbf{p}, \mathbf{q})$ is a μ-basis. By construction of μ-bases, it is obvious that $\mathrm{Res}(P, Q)$ vanishes on $\mathcal{S}$, so any implicit equation $S(x, y, z)$ of $\mathcal{S}$ divides $\mathrm{Res}(P, Q)$. Moreover, $\mathrm{Res}(P, Q)$ is a polynomial in x, y, z of degree at most $\deg(\mathcal{S})(= \deg(S))$, and we are done. □

The previous result states that the resultant of a μ-basis gives exactly the implicit equation. As it is shown in [2], some matrices (including the Sylvester one) whose determinant is exactly this resultant can be used to compute an inverse of the parameter s of ϕ by means of some minors of this matrix; then an inverse of t can be straightforwardly deduced. Moreover, an algorithm to test the properness of the parameterization can be derived from this matrix (see [2]).

Notice that recently, Proposition 3.6 has been extended by Marc [9] to the non-proper case, providing directly an implicitization formula without relying on Proposition 2.2.

4. Self-intersections points on a ruled surface

Let $\mathcal{S}$ be a ruled surface in $\mathbb{P}^3$ given by a parameterization $\phi : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$ of type $((n_0, n_1), 1)$, which is base point free. Then $\mathcal{S}$ has degree $d := n_0 + n_1$. We set $\mathcal{S} = \cup D_s$, as it is an union of lines. We denote by $\mathcal{A}$ the curve of singular points of $\mathcal{S}$. A point M of $\mathcal{A}$ is either an image of a critical point of ϕ, i.e. a point where the jacobian matrix $\dfrac{D(\phi)}{D(s,t)}$ is of rank smaller than 2, or it is a double point of the parameterization i.e. $M = \phi(s_1, t_1) = \phi(s_2, t_2)$ with $(s_1, t_1) \neq (s_2, t_2)$. A direct computation in a chart shows that, generically, there are only a finite number of points of the first kind and they are in the algebraic closure of the set of the points of the second kind. Here after we suppose that we are in that situation.

We cut S by a generic plane of $\mathbb{P}^3$, we obtain an algebraic plane curve $\mathcal{C}$ of degree $d = n_0 + n_1$ which is the image of a curve of bidegree $(1, d)$ in $\mathbb{P}^1 \times \mathbb{P}^1$, hence rational; therefore $\mathcal{C}$ is also rational. By the adjunction formula, $\mathcal{C}$ admits generically $\dfrac{(d-1)(d-2)}{2}$ double points. These points are precisely the intersection points between the singular curve $\mathcal{A}$ and the considered generic plane. So the degree of $\mathcal{A}$ is $\dfrac{(d-1)(d-2)}{2}$.

The curve $\mathcal{A}$ lies on the surface $\mathcal{S}$ and is the image by ϕ of an algebraic curve denoted $\mathcal{B}$ in $\mathbb{P}^1 \times \mathbb{P}^1$. We denote by (a, b) the bidegree of the equation $f(s, t) = 0$ of $\mathcal{B}$. As the inverse image by ϕ of a plane has bidegree $(n_1, 1)$, expressing twice the intersection number of $\mathcal{A}$ with a generic plane, we get the equality:

$$(d-1)(d-2) = n_1.b + 1.a.$$

For a fixed generic s_0, the integer b counts the number of $t = t_i$ such that

$f(s_0, t_i) = 0$. In other words, the line D_{s_0} cuts b other lines D_s of the family. The condition "cuts" is equivalent to say that the two lines are coplanar, or to say that the determinant

$$\det\left(M(s_0,0), M(s_0,\infty), \frac{M(s,0)-M(s_0,0)}{s-s_0}, \frac{M(s,\infty)-M(s_0,\infty)}{s-s_0}\right)$$

vanishes. Counting the degree in s, we get $b = (n_0 - 1) + (n_1 - 1) = d - 2$. We deduce that $a = (d-1)(d-2) - (d-2)n_0 = (n_1 - 1)(d-2)$. When $n_0 = n_1 = n$, then $d = 2n$, $a = 2(n-1)$ and $b = 2(n-1)2$.

The self-intersection locus lies naturally in $(\mathbb{P}^1 \times \mathbb{P}^1)^2$, but it is more convenient to represent it by one of its 2D projection. The projection usually considered is on the first and second $\mathbb{P}^1$ factors. This amounts to eliminate the 2 variables (s_2, t_2) in the system of 3 equations expressing that $\phi(s_1, t_1) = \phi(s_2, t_2)$, in order to get a polynomial of bidegree (a, b). As the degree in t_2 of these expressions is 1, we eliminate t_2 by a simple substitution, so it remains two equations. Then s_2 is eliminated via a resultant.

An alternative computation is to compute, as in the previous section, an implicit equation F of $\mathcal{S}$, then its derivatives and substitute the parameterization in these expressions. Finally we keep the gcd of all the obtained expressions; it is a polynomial in (s, t) of bidegree (a, b). Another interesting projection is the one on the second and the fourth $\mathbb{P}^1$ factors. The simpler elimination of the (linear) variables (t_1, t_2), described just above with a determinant, provides a symmetric polynomial in (s_1, s_2) of bidegree $(d-2, d-2)$. We can express this condition as a polynomial of total degree $d-2$ in the the sum σ and the product π of s_1 and s_2. Let us call $\mathcal{T}$ the plane curve defined by this last polynomial. Then, $\mathcal{T}$ is birationnally equivalent to $\mathcal{C}$, and it is easier to study.

Acknowledgments

This work has been partially supported by the french ANR GECKO.

References

[1] Dario Bini and Victor Y. Pan. *Polynomial and matrix computations. Vol. 1.* Progress in Theoretical Computer Science. Birkhäuser Boston Inc., Boston, MA, 1994. Fundamental algorithms.

[2] Laurent Busé and Carlos D'Andrea. Inversion of parameterized hypersurfaces by means of subresultants. In *Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation*, pages 65–71 (electronic), New York, 2004. ACM.

[3] Falai Chen. Reparameterization of a rational ruled surface using the μ-basis. *Comput. Aided Geom. Design*, 20(1):11–17, 2003.

[4] Falai Chen and Wenping Wang. Revisiting the μ-basis of a rational ruled surface. *J. Symbolic Comput.*, 36(5):699–716, 2003.

[5] Falai Chen and Wenping Wang. The μ-basis of a planar curve-properties and computation. *Graphical Models*, 64:368–381, 2003.

[6] Falai Chen, Jianmin Zheng, and Thomas W. Sederberg. The μ-basis of a rational ruled surface. *Comput. Aided Geom. Design*, 18(1):61–72, 2001.

[7] Robert Corless, Patrizia Gianni, Barry Trager, and Stephen Watt. The singular value decomposition for polynomial systems. In *ISSAC*, pages 195–207. ACM, 1995.

[8] David A. Cox, Thomas W. Sederberg, and Falai Chen. The moving line ideal basis of planar rational curves. *Comput. Aided Geom. Design*, 15(8): 803–827, 1998.

[9] Marc Dohm. Implicitization of rational ruled surfaces with μ-bases. Accepted to appear in *J. Symbolic Comput., Special Issue EACA 2006*, 2007.

[10] William L. Edge. *The theory of ruled surfaces*. Cambridge University Press, Cambridge, UK, 1931.

[11] David Eisenbud. *Commutative algebra with a view toward algebraic geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

[12] Ioannis Z. Emiris, André Galligo, and Henri Lombardi. Numerical univariate polynomial GCD. In *The mathematics of numerical analysis (Park City, UT, 1995)*, volume 32 of *Lectures in Appl. Math.*, pages 323–343. Amer. Math. Soc., Providence, RI, 1996.

[13] Ioannis Z. Emiris, André Galligo, and Henri Lombardi. Certified approximate univariate GCDs. *J. Pure Appl. Algebra*, 117/118:229–251, 1997. Algorithms for algebra (Eindhoven, 1996).

[14] Christoph Hoffmann, Rafael Sendra, and Franz Winkler, editors. *Parametric algebraic curves and applications*. Academic Press, Amsterdam, 1997. Including papers from the IMACS-ACA Session on Parametric Curves and Applications in Computer-aided Geometric Design held at the University of New Mexico, Albuquerque, NM, May 1995, J. Symbolic Comput. **23** (1997), no. 2-3.

[15] David Rupprecht. An algorithm for computing certified approximate GCD of n univariate polynomials. *J. Pure Appl. Algebra*, 139(1-3):255–284, 1999. Effective methods in algebraic geometry (Saint-Malo, 1998).

[16] Thomas W. Sederberg and Jianmin Zheng. A direct approach to computing the μ-basis of planar rational curves. *J. Symb. Comput.*, 31(5):619–629, 2001.

[17] Bartel L. Van der Waerden. *Algebra. Vol 1.* Translated by Fred Blum and John R. Schulenberger. Frederick Ungar Publishing Co., New York, 1970.

[18] Zhonggang Zeng and Barry H. Dayton. The approximate gcd of inexact polynomials. In *ISSAC '04: Proceedings of the 2004 international symposium on Symbolic and algebraic computation*, pages 320–327, New York, NY, USA, 2004. ACM Press.