Matrix-based Implicit Representations of Rational Algebraic Curves and Applications

Laurent Busé, Thang Luu Ba

Matrix-based Implicit Representations of Rational Algebraic Curves and Applications

Laurent Busé[a], Thang Luu Ba[a,b]

[a] *INRIA, Galaad, 2004 route des Lucioles, 06902 Sophia Antipolis, France*
[b] *Laboratoire J.A. Dieudonné, Université de Nice, Parc Valrose, 06108 Nice Cedex 02, France*

Abstract

Given a parameterization of an algebraic rational curve in a projective space of arbitrary dimension, we introduce and study a new implicit representation of this curve which consists in the locus where the rank of a single matrix drops. Then, we illustrate the advantages of this representation by addressing several important problems of Computer Aided Geometric Design: The point-on-curve and inversion problems, the computation of singularities and the calculation of the intersection between two rational curves.

1. Introduction

Algebraic curves that are used in Computer Aided Geometric Design (CAGD) are often given in parametric form. Such curves form a particular class of algebraic curves that are called *rational*. For many applications it is helpful to turn a parametric representation into an implicit representation, so that implicitization of algebraic curves has been and is always an active research topic.

The case of plane curves can be considered as well understood. Indeed, the implicitization problem can be solved by a simple resultant computation and an implicit equation is obtained as the determinant of a square matrix. The case of rational curves in a space of higher dimension is much more involved. One of the main reason of this fact is that a single equation can not serve as an implicit representation, several equations are necessary. The determination of these equations in good shape and in small number is a difficult problem (see for instance [11], [21] and [15]). The aim of this paper is to propose new implicit representations of rational curves which are based on a matrix formulation and which have the advantage to be given by a *single* matrix, whatever the dimension of the space the curve is embedded in. This representation can be seen as an extension of the Sylvester matrix whose determinant provides an implicit equation in the case of a plane rational curve. It uses the notion of a μ-basis of a parameterization of a rational curve that we will recall in Section 2. The new matrix-based representations of rational curves which we propose will be exposed in Section 3.

In the rest of this paper, we will show how to use matrix-based implicit representations of rational curves to solve some important problems in CAGD, namely the point-on-curve and inversion problems in Section 4, the detection of singularities in Section 5 and the computation of the intersection locus between two rational curves in Section 6 and Section 7. All these problems have been considered recently in [21], [23] and [15] with methods based on a set of equations that are built from a μ-basis of the parameterization. We will show in this paper how the use of matrix-based representations allow to remove the limitations of the above methods in terms of the degree of the curve and the multiplicities of singular points.

The paper ends with Section 8 where a construction of matrix-based representations of rational curves that does not require the computation of a μ-basis is given. As we will see, the price to pay to avoid this computation is to get matrices of significantly bigger size, but on the other hand, these matrix-based representations can be implemented in a programming environment where exact linear algebra routines are not available.

Throughout this paper, we will assume that $\mathbb{K}$ is an algebraically closed field for simplicity. However, most of the results in this paper, notably the matrix-based representations of curves we will introduce could be given over an infinite field.

2. The defining ideal of a rational curve and μ-bases

Let $f_0, f_1, \ldots, f_n$ be $n+1$ homogeneous polynomials in $\mathbb{K}[s,t]$ of the same degree $d \geq 1$ such that their greatest common divisor (GCD) is a non-zero constant in $\mathbb{K}$. Consider the regular map

$$\begin{array}{rcl} \mathbb{P}^1_{\mathbb{K}} & \stackrel{\phi}{\rightarrow} & \mathbb{P}^n_{\mathbb{K}} \\ (s:t) & \mapsto & (f_0 : f_1 : \cdots : f_n)(s,t). \end{array}$$

The image of ϕ is an algebraic curve C in $\mathbb{P}^n_{\mathbb{K}}$ which is called a *rational* curve. The degree of C is the number of intersection points counted properly between C and any hyperplane in $\mathbb{P}^n_{\mathbb{K}}$ not containing C. By a well known formula, it is related to the degree of the f_i's and the degree of the map ϕ co-restricted to C through the equation

$$\deg(C)\deg(\phi) = d.$$

Recall that $\deg(\phi)$ is, by definition, the degree of the canonical field extension induced by ϕ, namely

$$\deg(\phi) = [\mathbb{K}(s) : \mathbb{K}(f_0(s,1), \ldots, f_n(s,1))] = [\mathbb{K}(t) : \mathbb{K}(f_0(1,t), \ldots, f_n(1,t))].$$

Roughly speaking, $\deg(\phi)$ is the number of pre-images of a generic point on C via ϕ.

2.1. The defining ideal of a rational curve

The parameterization ϕ is a very practical representation of C and it is widely used in CAGD. However, for many problems it is useful to have an implicit representation of C, that is to say a representation in terms of the coordinates of $\mathbb{P}^n_{\mathbb{K}}$; hereafter we will denote these coordinates by $(x_0 : \cdots : x_n)$. One of the most commonly used implicit representation of C in $\mathbb{P}^n_{\mathbb{K}}$ is the *defining ideal* of C, that we will denote by $\mathfrak{I}_C$. By definition, it is the kernel of the ring morphism

$$\begin{array}{rcl} h : \mathbb{K}[x_0, \ldots, x_n] & \rightarrow & \mathbb{K}[s,t] \\ x_i & \mapsto & f_i(s,t) \quad i = 0, \ldots, n. \end{array}$$

In other terms, $\mathfrak{I}_C$ is the set of polynomials $P \in \mathbb{K}[x_0, \ldots, x_n]$ that satisfy to the equality $P(f_0, \ldots, f_n) = 0$. It is a graded ideal of $\mathbb{K}[x_0, \ldots, x_n]$ which is moreover prime (hence radical) because $\mathbb{K}[s,t]$ is a domain. It is finitely generated and any collection of generators of $\mathfrak{I}_C$ provides a representation of C since we have, in terms of algebraic varieties

$$V(\mathfrak{I}_C) = \{(x_0 : \cdots : x_n) \in \mathbb{P}^n_{\mathbb{K}} \ : \ P(x_0, \ldots, x_n) = 0 \text{ for all } P \in \mathfrak{I}_C\} = C.$$

Such a representation can be hard to compute and is not easy to handle for applications in CAGD; see for instance [12, 11] and the references therein for the case of space curves (i.e. $n = 3$).

2.2. μ-basis of a rational curve

The concept of a μ-basis has been introduced in [8]. It can be seen as a bridge between the parametric representation ϕ of C and its implicit representation $\mathfrak{I}_C$. We recall here briefly its definition and main properties that all follow from a classical structure theorem of commutative algebra called the Hilbert-Burch Theorem (see for instance [9, §20.4]).

Consider the set of syzygies of $\mathbf{f} := (f_0, \ldots, f_n)$, that is to say the set

$$\mathrm{Syz}(\mathbf{f}) = \left\{ (g_0(s,t), \ldots, g_n(s,t)) \ : \ \sum_{i=0}^{n} g_i(s,t) f_i(s,t) = 0 \right\} \subset \bigoplus_{i=0}^{n} \mathbb{K}[s,t]$$

It is known to be a free and graded $\mathbb{K}[s,t]$-module of rank n. Moreover, there exist non-negative integers $\mu_1, \ldots, \mu_n$ and n vectors of polynomials

$$(u_{i,0}(s,t), u_{i,1}(s,t), \ldots, u_{i,n}(s,t)) \in \mathrm{Syz}(\mathbf{f}) \subset \mathbb{K}[s,t]^{n+1} \quad (i = 1, \ldots, n) \tag{1}$$

such that

- for all $i \in \{1, \dots, n\}$, $j \in \{0, \dots, n\}$, $u_{i,j}(s,t)$ is a homogeneous polynomial in $\mathbb{K}[s,t]$ of degree $\mu_i \geq 0$,
- the n vectors in (1) form a $\mathbb{K}[s,t]$-basis of $\mathrm{Syz}(\mathbf{f})$,
- $\sum_{i=1}^{n} \mu_i = d$,
- For all $j \in \{0, \dots, n\}$, the determinant of the matrix obtained by deleting the column $(u_{i,j})_{i=1,\dots,n}$ from the matrix

$$M(s,t) := \begin{pmatrix} u_{1,0}(s,t) & u_{1,1}(s,t) & \dots & u_{1,n}(s,t) \\ u_{2,0}(s,t) & u_{2,1}(s,t) & \dots & u_{2,n}(s,t) \\ \dots & \dots & \dots & \dots \\ u_{n,0}(s,t) & u_{n,1}(s,t) & \dots & u_{n,n}(s,t) \end{pmatrix} \tag{2}$$

  is equal to $(-1)^j c\, f_j(s,t) \in \mathbb{K}[s,t]$ where $c \in \mathbb{K} \setminus \{0\}$.

A collection of vectors as in (1) that satisfy the above properties is called a μ-basis of the parameterization ϕ. It is important to notice that a μ-basis is far from being unique, but the collection of integers $(\mu_1, \mu_2, \dots, \mu_n)$ is unique if we order it. Therefore, in the sequel we will always assume that a μ-basis is ordered so that $0 \leq \mu_1 \leq \mu_2 \leq \dots \leq \mu_n$. We refer the interested reader to [21] for more details on the topic of μ-basis.

2.3. Projection of the graph of ϕ

Here is an important property of a μ-basis as a tool for the representation of the curve C. Recall that $M(s,t)$ denotes the matrix (2) built from a μ-basis of ϕ.

Lemma 1. *For any point $(s_0 : t_0) \in \mathbb{P}^1_{\mathbb{K}}$, the kernel of $M(s_0, t_0)$ is $\mathbb{K}$-generated by the nonzero vector*

$$< f_0(s_0,t_0), f_1(s_0,t_0), \dots, f_n(s_0,t_0) >$$

so that it has dimension exactly one. In particular, $M(s_0,t_0)$ is full rank for any point $(s_0 : t_0) \in \mathbb{P}^1_{\mathbb{K}}$.

Proof. Straightforward from the properties of a μ-basis and the classical Cramer's rules. □

For all $i = 1, \dots, n$ set

$$u_i(s,t,x_0,x_1,\dots,x_n) = \sum_{j=0}^{n} u_{i,j}(s,t)x_j \in \mathbb{K}[s,t,x_0,\dots,x_n]. \tag{3}$$

An immediate consequence of Lemma 1 is that the algebraic variety W defined by the zero locus of the μ-basis, i.e.

$$W := \{(s:t) \times (x_0 : \dots : x_n) \ : \ u_1 = u_2 = \dots = u_n = 0\} \subset \mathbb{P}^1_{\mathbb{K}} \times \mathbb{P}^n_{\mathbb{K}},$$

is nothing but the graph of the parameterization ϕ. Therefore, the canonical projection

$$\pi : \mathbb{P}^1_{\mathbb{K}} \times \mathbb{P}^n_{\mathbb{K}} \to \mathbb{P}^n_{\mathbb{K}} : (s:t) \times (x_0 : \dots : x_n) \mapsto (x_0 : \dots : x_n)$$

sends W on C; we have $\pi(W) = C$. But the situation is actually even nicer: this equality is not only true at the level of algebraic varieties, but also at the level of ideals. To be more precise we need some additional notation.

Define the polynomial ring $A := \mathbb{K}[x_0, \dots, x_n]$, so that $\mathbb{K}[s,t,x_0,\dots,x_n] = A[s,t]$, the ideal $I := (u_1, \dots, u_n)$ of $A[s,t]$ and consider its *resultant ideal* (also called the projective elimination ideal in [7, Chapter 8, §5]) $\mathfrak{A}$ with respect to the ideal $\mathfrak{m} = (s,t)$ of $A[s,t]$. By definition, we have

$$\mathfrak{A} = \{P \in A \text{ such that } \exists\, \nu \in \mathbb{N} \ : \ (s,t)^\nu P \subset I\} \subset A.$$

Proposition 2 ([5, Corollary 3.8])**.** *With the above notation, we have $\mathfrak{A} = \mathfrak{I}_C$ as ideals of A.*

In the next section, we will take advantage of this proposition to produce a matrix-based representation of C. For that purpose, we will need a property that relates resultant ideals with certain annihilators. Define the quotient $B := A[s,t]/I$ and recall that it inherits of a structure of graded ring from the canonical grading of $C := A[s,t]$ and the homogeneous ideal I: $\deg(s) = \deg(t) = 1$ and $\deg(a) = 0$ for all $a \in A$. Set $\mathfrak{m} := (s,t) \subset C$ and for any integer $\nu \in \mathbb{N}$ consider

$$\operatorname{ann}_A(B_\nu) = \{P \in A \text{ such that } P.B_\nu = 0\} \subset A.$$

Corollary 3. *For all integer $\nu \geq \mu_n + \mu_{n-1} - 1$ we have $\operatorname{ann}_A(B_\nu) = \mathfrak{A} = \mathfrak{I}_C$.*

Proof. Since $\mathfrak{A} = \mathfrak{I}_C$, we will explain why $\operatorname{ann}_A(B_\nu) = \mathfrak{A}$ for all $\nu \geq \mu_n + \mu_{n-1} - 1$. First, define

$$H^0_{\mathfrak{m}}(B) := \bigcup_{k=0}^{\infty}(0 :_B \mathfrak{m}^k) = \{s \in B : \exists k \in \mathbb{N} \text{ such that } \mathfrak{m}^k s = 0\}.$$

It is a graded C-module and it is clear that $\mathfrak{A} = H^0_{\mathfrak{m}}(B) \cap A = H^0_{\mathfrak{m}}(B)_0$. Moreover, for any $\eta \in \mathbb{N}$ such that $H^0_{\mathfrak{m}}(B)_\eta = 0$, we have $\mathfrak{A} = \operatorname{ann}_A(B_\eta)$; see for instance [2, Proposition 1.2].

Now, for any point $(s_0 : t_0) \in \mathbb{P}^1_{\mathbb{K}}$ the variety $V(u_1(s_0,t_0), \ldots, u_n(s_0,t_0))$ is of codimension n in $\mathbb{P}^n_{\mathbb{K}}$ by Lemma 1. Therefore, the polynomials $u_1, \ldots, u_n$ form a regular sequence in $A[s,t]$ outside $V(\mathfrak{m})$. It follows that we can apply the techniques developed in [16, §2.10] and deduce that $H^0_{\mathfrak{m}}(B)_\nu = 0$ for all $\nu \geq \mu_n + \mu_{n-1} - 1$ (recall that we have assumed that $0 \leq \mu_1 \leq \cdots \leq \mu_{n-1} \leq \mu_n$). □

3. Matrix-based implicit representations of a rational curve

The aim of this section is to produce a matrix-based representation of C which is geometrically faithful to the parameterization ϕ. In this order, we will exhibit ideals that are good approximations (in a sense that we will make precise hereafter) of the ideal $\mathfrak{I}_C$. In view of Corollary 3, certain Fitting ideals associated to a μ-basis of ϕ are natural candidates for that purpose.

3.1. The initial Fitting ideal of a μ-basis

Taking again the notation of the previous section, the quotient ring B is, by definition, equal to the cokernel of the following graded map:

$$\oplus_{i=1}^n C(-\mu_i) \xrightarrow{u_1,\ldots,u_n} C : (g_1, \ldots, g_n) \mapsto \sum_{i=1}^n u_i g_i. \tag{4}$$

Recall that we consider the grading of C given by $\deg(s) = \deg(t) = 1$ and $\deg(a) = 0$ for all $a \in A$. Recall also that, given an integer $\nu \in \mathbb{N}$, the notation C_ν stands for the set (actually a A-module) of homogeneous elements of degree ν in C, so that $C = \oplus_{i \geq 0} C_\nu$. Finally, the notation $C(k)$, $k \in \mathbb{Z}$, denotes the graded ring such that $C(k)_\nu = C_{k+\nu}$ for all $\nu \in \mathbb{Z}$.

By taking graded parts in (4), we deduce that for all $\nu \in \mathbb{N}$ the cokernel of the A-linear map

$$\oplus_{i=1}^n C_{\nu-\mu_i} \xrightarrow{u_1,\ldots,u_n} C_\nu : (g_1, \ldots, g_n) \mapsto \sum_{i=1}^n u_i g_i \tag{5}$$

is exactly the A-module B_ν. From here, a well known result of commutative algebra allows to approximate the ideal $\operatorname{ann}_A(B_\nu)$ with the *initial Fitting ideal* of B_ν, denoted $\mathfrak{F}(B_\nu)$, which is the ideal of A generated by the $(\nu+1)$-minors of a matrix of (5). Indeed, it is well known that (see for instance [9, Proposition 20.7] or [20, Theorem 5, Chapter 3])

$$\operatorname{ann}_A(B_\nu)^{\nu+1} \subset \mathfrak{F}(B_\nu) \subset \operatorname{ann}_A(B_\nu). \tag{6}$$

In particular, $V(\mathfrak{F}(B_\nu)) = V(\operatorname{ann}_A(B_\nu)) \subset \mathbb{P}^{n-1}_{\mathbb{K}}$. Therefore, we deduce the following

Theorem 4. *For all integer $\nu \geq \mu_n + \mu_{n-1} - 1$, we have $V(\mathfrak{F}(B_\nu)) = C$.*

Proof. Straightforward from the Corollary 3 and (6). □

For all integer $\nu \geq \mu_n + \mu_{n-1} - 1$ denote by $\mathtt{M}(\phi)_\nu$ a matrix of the A-linear map (5). Observe that $\mathtt{M}(\phi)_\nu$ depends on the choice of the μ-basis of ϕ and the choices of the A-basis of C_ν and $C_{\nu-\mu_i}$, $i = 1, \ldots, n$ (monomial basis, Bernstein basis, etc). Theorem 4 shows that a point $P \in \mathbb{P}^n$ belongs to the curve C if and only if all the $(\nu+1)$-minors of $\mathtt{M}(\phi)_\nu$ (which form a set of generators of the ideal $\mathfrak{F}(B_\nu)$) vanish at this point, and hence if and only if the rank of the matrix $\mathtt{M}(\phi)_\nu$ evaluated at P is not equal to $\nu+1$ (its maximal possible value). So we deduce that we have a collection of matrices indexed by ν with the property that for all $\nu \geq \mu_n + \mu_{n-1} - 1$

(i) $\mathtt{M}(\phi)_\nu$ is generically full rank, that is to say generically of rank $\nu+1$,

(ii) the rank of $\mathtt{M}(\phi)_\nu$ drops exactly on the curve C.

These properties suggest that any matrix $\mathtt{M}(\phi)_\nu$, $\nu \geq \mu_n + \mu_{n-1} - 1$, can be seen as an *implicit representation* of the curve C. Set-theoretically, the implicit representation of C as the simultaneous vanishing locus of several polynomial equations (e.g. generators of the defining ideal of C) is replaced by a drop of rank of a single matrix.

Definition 5. For any $\nu \geq \mu_n + \mu_{n-1} - 1$, we will call a matrix $\mathtt{M}(\phi)_\nu$ a representation matrix of the curve C, or more rigorously a representation matrix of ϕ.

Before moving on, let us justify the fact that a representation matrix really depends on ϕ, and not only on the curve C. Given an integer $\nu \geq \mu_n + \mu_{n-1} - 1$, the ideal $\mathfrak{F}(B_\nu)$ is not equal to the defining ideal $\mathfrak{I}_C$ of the rational curve C in general (see Example 7). However, $\mathfrak{F}(B_\nu)$ is almost everywhere algebraically faithful to the parameterization ϕ in the following sense.

Theorem 6. *For all integer $\nu \geq \mu_n + \mu_{n-1} - 1$, we have the following equality of ideals in the ring $A_{\mathfrak{I}_C}$ which denotes the localization of A by the prime ideal $\mathfrak{I}_C$:*

$$\mathfrak{F}(B_\nu)_{\mathfrak{I}_C} = {\mathfrak{I}_C}^{\deg(\phi)} A_{\mathfrak{I}_C}.$$

In other words, the ideals $\mathfrak{F}(B_\nu)$ and ${\mathfrak{I}_C}^{\deg(\phi)}$ are equal at all points of C except a finite number (possibly zero) of them.

Proof. Since $\mathfrak{I}_C = \mathfrak{A} = \operatorname{ann}_A(B_\nu)$, B_ν has a canonical structure of $A/\mathfrak{A}A$-module. Moreover, since $\mathfrak{A}$ is a prime ideal, we get that $(B_\nu)_\mathfrak{A}$ is a $A_\mathfrak{A}/\mathfrak{A}A_\mathfrak{A}$-vector space. Therefore, we only need to prove that $\dim_{A_\mathfrak{A}/\mathfrak{A}A_\mathfrak{A}}(B_\nu)_\mathfrak{A} = \deg\phi$. This result is a consequence of the equality (12) in the proof of Theorem 2.5 in [5] (see also the proof of Theorem 5.2 in loc. cit.).

Now, we have that $(B_\nu)_\mathfrak{A} \simeq (A/\mathfrak{A}A)^{\deg(\phi)}_\mathfrak{A}$. Using classical properties of Fitting ideals (see for instance [20, §3.1]) we deduce that

$$\mathfrak{F}(B_\nu)_\mathfrak{A} \simeq \mathfrak{F}((A/\mathfrak{A}A)^{\deg\phi}_\mathfrak{A}) = \mathfrak{A}^{\deg\phi} A_\mathfrak{A}$$

as claimed. □

This theorem shows that the ideal $\mathfrak{F}(B_\nu)$ is equal to ${\mathfrak{I}_C}^{\deg(\phi)}$ plus a finite number (possibly zero) of embedded isolated points on C. We illustrate this property with the following example.

Notice that in the rest of this paper, when dealing with parameterized curves in $\mathbb{P}^3_\mathbb{K}$ we will often adopt the more commonly used notation (x, y, z, w) and (p, q, r) for the homogeneous coordinates of $\mathbb{P}^3_\mathbb{K}$ and a μ-basis instead of the notation (x_0, x_1, x_2, x_3) and (u_1, u_2, u_3).

Example 7. Let C be the rational space curve parameterized by

$$\begin{array}{ccc} \mathbb{P}^1_\mathbb{K} & \xrightarrow{\phi} & \mathbb{P}^3_\mathbb{K} \\ (s:t) & \mapsto & (s^4 : s^3t : s^2t^2 : t^4). \end{array}$$

A μ-basis of C is given by

$$\begin{aligned} p &= -tx + sy \\ q &= -ty + sz, \\ r &= -t^2z + s^2w. \end{aligned}$$

We have $\mu_1 = \mu_2 = 1, \mu_3 = 2$ and hence $\mu_3 + \mu_2 - 1 = 2$. Therefore, we obtain the following representation matrix of ϕ:

$$\mathtt{M}(\phi)_2 = \begin{pmatrix} y & 0 & z & 0 & w \\ -x & y & -y & z & 0 \\ 0 & -x & 0 & -y & -z \end{pmatrix}.$$

Using the computer algebra system `Macaulay2` [13], we get that $\mathfrak{I}_C = (z^2 - xw, y^2 - xz)$ and that

$$\mathfrak{F}(B_2) = \mathfrak{I}_C \cap (x, y^2, z^3, yz^2) \cap (w, x, z^3, yz^2, y^2z, y^3).$$

This computation shows that ϕ is birational onto C by Theorem 6 and also that $\mathfrak{F}(B_2)$ has an embedded component supported at the point $(0 : 0 : 0 : 1) \in C$. Therefore, $\mathfrak{F}(B_\nu) \neq \mathfrak{I}_C$ (notice that the third component in the decomposition of $\mathfrak{F}(B_\nu)$ is (x, y, z, w)-primary).

3.2. Computational aspects

We start by giving an algorithm to compute a representation matrix of a parameterized curve.

Algorithm 1: Matrix representation of a rational curve

Input: A parameterization ϕ of a rational curve which is defined by the polynomials $f_0(s,t), f_1(s,t), ..., f_n(s,t) \in \mathbb{K}[s,t]$.

Output: The smallest possible matrix representation of C among the ones given in Definition 5.

1. *Compute a μ-basis as* (1) *of $f_0(s,t), f_1(s,t), ..., f_n(s,t)$.*
2. *Build the polynomials $u_i(s,t)$, $i = 1, 2, ..., n$, as in* (3).
3. *Compute the degree μ_i, $i = 1, \ldots, n$, of the μ-basis.*
4. *Build the matrix $\mathtt{M}(\phi)_\delta$ where $\delta := \max\{\mu_i + \mu_j - 1 : 1 \leq i \neq j \leq n\}$.*

Observe that only the first step in this algorithm requires a computation which is the computation of a μ-basis. An efficient algorithm to compute such a μ-basis, which is mainly based on Gaussian elimination, is given in [21].

The step 4 consists in the building of a matrix whose entries are the coefficients of the polynomials $u_i(s,t)$, $i = 1, \ldots, n$. It requires the choice of basis for the A-modules C_k, $k \in \mathbb{N}$. For the sake of simplicity we choose hereafter the usual monomial basis, but we could choose any other basis, for instance the Bernstein basis that are widely used in CAGD and for which there exists a dedicated algorithm to compute a μ-basis (see [4]) so that Algorithm 1 can be run entirely in these basis.

For all integer $i = 1, \ldots, n$ and all integer $\nu \in \mathbb{N}$, consider the matrix $\mathrm{Sylv}_\nu(u_i)$ that satisfies to the identity

$$\left[s^\nu \; s^{\nu-1}t \; \cdots \; st^{\nu-1} \; t^\nu\right] \times \mathrm{Sylv}_\nu(u_i) = \left[s^{\nu-\mu_i}u_i \; s^{\nu-\mu_i-1}tu_i \; \cdots \; st^{\nu-\mu_i-1}u_i \; t^{\nu-\mu_i}u_i\right].$$

It is a $(\nu + 1) \times (\nu - \mu_i + 1)$-matrix which usually appears as a building block in well known Sylvester matrices. It follows that the matrix

$$\mathrm{Sylv}_\nu(u_1, \ldots, u_n) = \left(\begin{array}{c|c|c|c} \mathrm{Sylv}_\nu(u_1) & \mathrm{Sylv}_\nu(u_2) & \cdots & \mathrm{Sylv}_\nu(u_n) \end{array} \right)$$

is a matrix of the map (5). It has $\nu + 1$ rows and $n(\nu + 1) - d$ columns. Its entries are *linear forms* in $\mathbb{K}[x_0, \ldots, x_n]$; in particular, it can be evaluated at any point $(x_0 : \cdots : x_n) \in \mathbb{P}^n_{\mathbb{K}}$ and yields a matrix with coefficients in $\mathbb{K}$.

From the results we proved above, for all $\nu \geq \mu_n + \mu_{n-1} - 1$ the matrix $\mathrm{Sylv}_\nu(u_1, \ldots, u_n)$ is a *matrix-based representation* of the curve C. Of course, in practice the most useful matrix is the smallest one, that is to say $\mathrm{Sylv}_{\mu_n+\mu_{n-1}-1}(u_1, \ldots, u_n)$. We will illustrate in the next sections how one can take advantage of such a representation to perform important operations of CAGD as the point-on-curve and inversion problems, the computation of singularities and the calculation of the intersection between two rational curves.

3.3. Rational curves contained in a plane

Matrix representations of plane rational curves have been widely studied in the literature, so for the sake of completeness we briefly mention it and show how the results presented in the previous sections encapsulate it.

Assume that $n = 2$. Then C is a plane curve and $\mathfrak{I}_C$ is a principal ideal. It follows that C is the zero locus of a single polynomial equation called an implicit equation (this property never happens again if $n > 2$). A μ-basis is made of two elements u_1 u_2 such that $\mu_2 + \mu_1 = d$ and it is well known that the Sylvester matrix of u_1 and u_2 is a square matrix whose determinant is an implicit equation of C raised to the power $\deg(\phi)$. With the notation of the previous sections, this Sylvester matrix is nothing but the representation matrix $\mathtt{M}(\phi)_{d-1}$. The particularity in the case $n = 2$ is that this matrix is square, which rarely happens (even in the case $n = 2$ since $\mathtt{M}(\phi)_\nu$ is non square for $\nu \geq d$). Also, Theorem 6 contains the fact the $\det(\mathtt{M}(\phi)_{d-1})$ is equal to an implicit equation of C raised to the power $\deg(\phi)$. Here again, the particularity is that $\mathfrak{F}(B_{d-1}) = \mathfrak{I}^{\deg(\phi)}$ since $\mathfrak{F}(B_{d-1})$ is a principal ideal and hence cannot have embedded components.

Another interesting situation is the case of a curve C in $\mathbb{P}^n$ which is contained in a plane. By a linear change of coordinates, we can assume that the parameterization is of the form

$$\begin{array}{ccc} \mathbb{P}^1_{\mathbb{K}} & \xrightarrow{\phi} & \mathbb{P}^n_{\mathbb{K}} \\ (s:t) & \mapsto & (f_0(s,t) : f_1(s,t) : f_2(s,t) : 0 : \cdots : 0) \end{array}$$

so that C is included in the plane of equation $x_3 = x_4 = \ldots = x_n = 0$. Therefore a μ-basis is given by $u_i = x_i$, $i = 3, \ldots, n$ and u_1, u_2 is a μ-basis of the plane curve parameterized by

$$\mathbb{P}^1_{\mathbb{K}} \xrightarrow{\overline{\phi}} \mathbb{P}^2_{\mathbb{K}} : (s:t) \mapsto (f_0(s,t) : f_1(s,t) : f_2(s,t)).$$

Then it is not hard to see that the representation matrix $\mathtt{M}(\phi)_{d-1}$ (notice that $\mu_1 + \mu_2 = d - 1$) is of the form

$$\left(\begin{array}{c|ccc|c|ccc} & x_3 & & 0 & & x_n & & 0 \\ \mathtt{M}\left(\overline{\phi}\right)_{d-1} & & \ddots & & \cdots & & \ddots & \\ & 0 & & x_3 & & 0 & & x_n \end{array}\right).$$

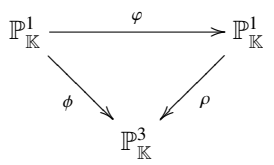
Let us end this paragraph with a last particular case: a line in $\mathbb{P}^3$ (we restrict ourselves to $\mathbb{P}^3$ for simplicity). Such a case occurs when $\mu_1 = \mu_2 = 0$. By a linear change of coordinates, we can suppose that $u_1 = x$, $u_2 = y$ and $u_3 = p(s,t)z + q(s,t)w$. Notice that necessarily $\mu_3 = d$. In other words, the curve C is parameterized by

$$\begin{array}{ccc} \mathbb{P}^1_{\mathbb{K}} & \xrightarrow{\phi} & \mathbb{P}^3_{\mathbb{K}} \\ (s:t) & \mapsto & (0:0:f_2:f_3)(s,t). \end{array}$$

We obtain the following matrix representation of ϕ where, notably, f_2 and f_3 does not appear (because $C_{-1} = \emptyset$):

$$\mathtt{M}(\phi)_{d-1} = \left(\begin{array}{cccc|cccc} x & 0 & \ldots & 0 & y & 0 & \ldots & 0 \\ 0 & x & \ldots & 0 & 0 & y & \ldots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \ldots & x & 0 & 0 & \ldots & y \end{array}\right).$$

It is a $d \times 2d$-matrix from we see easily find that $\mathfrak{F}(B_{d-1}) = (x,y)^d$. It turns out that d is actually equal to $\deg(\phi)$ from we get easily that $\mathfrak{F}(B_\nu) = {I_C}^{\deg(\phi)}$ in this case. This last property follows from Luröth Theorem (see for instance [17]). Indeed, this theorem implies that there exists a commutative diagram



where

$$\begin{array}{ccc} \mathbb{P}^1_{\mathbb{K}} & \xrightarrow{\rho} & \mathbb{P}^3_{\mathbb{K}} \\ (x:y) & \mapsto & (0:0:x:y)(s,t), \end{array}$$

$$\begin{array}{ccc} \mathbb{P}^1_{\mathbb{K}} & \xrightarrow{\varphi} & \mathbb{P}^1_{\mathbb{K}} \\ (t:s) & \mapsto & (f_2:f_3)(s,t), \end{array}$$

and $\deg(\phi) = \deg(\rho)\deg(\varphi)$, $\deg\rho = 1$ and $\deg\varphi = d$. Therefore, $\deg\phi = d$.

4. Point-on-curve and inversion problems

In this section we will show how to utilize matrix representations of rational curves to solve two basic problems for rational space curves: point-on-curve problem, that is to say determining if a point lies on a curve, and inversion problem, that is to say finding the parameter of a point on a curve given by its homogeneous coordinates.

These problems have been treated previously in the literature by means of a GCD computation of the μ-basis in [21], and also by describing the curve C as the intersection of three surfaces in [15], although this latter method is limited to some particular types of curves. Using the results we got in the previous sections, we propose the following new approach to the point-on-curve problem.

Suppose given a parameterization ϕ of a rational curve C and a point P in $\mathbb{P}^3$. Denote by $\mathtt{M}(\phi)_\nu$ a matrix representation of ϕ for some integer $\nu \geq \delta := \mu_n + \mu_{n-1} - 1$. Since its entries are linear forms in the variables $x_0, \ldots, x_n$, one can evaluate $\mathtt{M}(\phi)_\nu$ at P and get a matrix with coefficients in the ground field $\mathbb{K}$. Then, we have that

$$\operatorname{rank}\left(\mathtt{M}(\phi)_\nu(P)\right) < \nu + 1 \text{ if and only if } P \in C.$$

This property answers the point-on-curve problem.

Example 8. Suppose that the parameterization ϕ is given by

$$\begin{aligned} f_0(s,t) &= 3s^4t^2 - 9s^3t^3 - 3s^2t^4 + 12st^5 + 6t^6, \\ f_1(s,t) &= -3s^6 + 18s^5t - 27s^4t^2 - 12s^3t^3 + 33s^2t^4 + 6st^5 - 6t^6, \\ f_2(s,t) &= s^6 - 6s^5t + 13s^4t^2 - 16s^3t^3 + 9s^2t^4 + 14st^5 - 6t^6, \\ f_3(s,t) &= -2s^4t^2 + 8s^3t^3 - 14s^2t^4 + 20st^5 - 6t^6. \end{aligned}$$

A μ-basis for C is

$$\begin{aligned} p &= (s^2 - 3st + t^2)x + t^2y \\ q &= (s^2 - st + 3t^2)y + (3s^2 - 3st - 3t^2)z, \\ r &= 2t^2z + (s^2 - 2st - 2t^2)w. \end{aligned}$$

From $\deg(p) = \deg(q) = \deg(r) = 2$, we have $\mu_n + \mu_{n-1} - 1 = 3$ and hence a matrix representation of C is given by

$$\mathtt{M}(\phi)_3 = \begin{pmatrix} x+y & 0 & 3y-3z & 0 & 2z-2w & 0 \\ -3x & x+y & -y-3z & 3y-3z & -2w & 2z-2w \\ x & -3x & y+3z & -y-3z & w & -2w \\ 0 & x & 0 & y+3z & 0 & w \end{pmatrix}.$$

Let $P = (1:1:1:1) \in \mathbb{P}^3$. Evaluating $\mathtt{M}(\phi)_3$ at P we find that

$$\mathtt{M}(\phi)_3 = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 \\ -3 & 2 & -4 & 0 & -2 & 0 \\ 1 & -3 & 4 & -4 & 1 & -2 \\ 0 & 1 & 0 & 4 & 0 & 1 \end{pmatrix}$$

is of rank 4 so that P does not lie on C.

This example is taken from [15, Example 3.7]. There, the authors' approach is to represent the curve C as the intersection of three surfaces, namely

$$\mathrm{Res}(p,q) = \det\begin{pmatrix} x+y & 0 & 3y-3z & 0 \\ -3x & x+y & -y-3z & 3y-3z \\ x & -3x & y+3z & -y-3z \\ 0 & x & 0 & y+3z \end{pmatrix} = 0,$$

$$\mathrm{Res}(p,r) = \det\begin{pmatrix} x+y & 0 & 2z-2w & 0 \\ -3x & x+y & -2w & 2z-2w \\ x & -3x & w & -2w \\ 0 & x & 0 & w \end{pmatrix} = 0,$$

$$\mathrm{Res}(r,q) = \det\begin{pmatrix} 3y-3z & 0 & 2z-2w & 0 \\ -y-3z & 3y-3z & -2w & 2z-2w \\ y+3z & -y-3z & w & -2w \\ 0 & y+3z & 0 & w \end{pmatrix} = 0.$$

It turns out that P belongs to the intersection of these three surfaces, but does not belong to the curve C. It is interesting to notice how the rank condition on the matrix $\mathtt{M}(\phi)_3$, which is a kind of join of the three above matrix, corrects this default.

Another classical problem is the inversion problem. In [21] this problem is treated through a GCD computation of a μ-basis. Using a matrix representation of the curve, we propose another approach which is based on the computation of the kernel of a matrix with coefficients in the ground field $\mathbb{K}$.

Suppose given a point in homogeneous coordinates P and let $\mathtt{M}(\phi)_\nu$ be a representation matrix of ϕ for a given integer $\nu \geq \mu_n + \mu_{n-1} - 1$. If $\operatorname{rank}\mathtt{M}(\phi)_\nu(P) = \operatorname{rank}\mathtt{M}(\phi)_\nu - 1 = \nu$ then P has a unique pre-image $(s_0 : t_0)$ by ϕ and moreover, this pre-image can be recovered from the computation of a generator, say $W_P = (w_0, \ldots, w_\nu) \in \mathbb{K}^{\nu+1}$, of the kernel of the transpose of $\mathtt{M}(\phi)_\nu(P)$. Indeed, if $b_0(s,t), \ldots, b_\nu(s,t)$ is the basis of C_ν that has been chosen to build $\mathtt{M}(\phi)_\nu$, then there exists $\lambda \in \mathbb{K} \setminus \{0\}$ such that

$$W_P = \lambda\,(b_0(s_0,t_0), \ldots, b_\nu(s_0,t_0))\,.$$

For instance, suppose that $b_i(s,t) = s^i t^{\nu-i}$, $i = 0, \ldots, \nu$ (the usual monomial basis), then $(s_0 : t_0) = (w_1 : w_0)$ if $w_0 \neq 0$, otherwise $(s_0 : t_0) = (1 : 0)$.

We point out that the points $P \in C$ such that $\operatorname{rank}\mathtt{M}(\phi)_\nu(P) = \operatorname{rank}\mathtt{M}(\phi)_\nu - 1 = \nu$ are precisely the regular points on C, that is to say that all the points that do not verify this property are singular points on C. We will come back again on this property and on the treatment of the singular points on C in the next section. We close this section with an illustrative example.

Example 9. Take again Example 8. Evaluating the matrix $\mathtt{M}(\phi)_3$ at the point $P = (9 : 9 : 9 : 6) \in \mathbb{P}^3$ we obtain the matrix

$$\mathtt{M}(\phi)_3(P) = \begin{pmatrix} 18 & 0 & 0 & 0 & 6 & 0 \\ -27 & 18 & -36 & 0 & -12 & 6 \\ 9 & -27 & 36 & -36 & 6 & -12 \\ 0 & 9 & 0 & 36 & 0 & 6 \end{pmatrix}.$$

which has rank 3. Therefore, P is a smooth point on the curve C. Moreover, the computation of the kernel of the transpose of $\mathtt{M}(\phi)_3(P)$ returns the vector $(1, 1, 1, 1)$. Thus, we deduce that $P = \phi(1 : 1)$.

5. Computing the singular points of a rational curve

This section is devoted to the computation of the singular points of a rational curve. Hereafter, we will restrict ourselves to the case of rational space curves for simplicity, and also to emphasize our new methods in a case which is of particular interest in CAGD. However, all our results can be easily extended to a rational curve in a projective space of arbitrary dimension.

In [23], the authors derive correspondences between the singularities of rational space curves and a μ-basis. They also show how to employ μ-bases to compute all the singularities of rational space curves of low degree. We propose another approach to compute the singularities of rational space curves which is based on the matrix representations introduced in Section 3. It can be seen as an extension of what is called *singular factors* for the case of rational plane curves in [6]; see also [3].

5.1. Rank of a representation matrix at a singular point

Let C be a rational space curve of degree $d \geq 1$ parameterized by the regular map

$$\begin{array}{ccc} \mathbb{P}^1_{\mathbb{K}} & \stackrel{\phi}{\rightarrow} & \mathbb{P}^3_{\mathbb{K}} \\ (s:t) & \mapsto & (f_0 : f_1 : f_2 : f_3)(s,t). \end{array}$$

where f_0, f_1, f_2, f_3 are four homogeneous polynomials in $\mathbb{K}[s,t]$ of the same degree d such that their GCD is a nonzero element in $\mathbb{K}$.

Let P be a point on C. There exists at least one point $(s_1 : t_1) \in \mathbb{P}^1$ such that $P = \phi(s_1 : t_1)$. Now, let $\mathcal{H}$ be a plane in $\mathbb{P}^3$ passing through P, not containing C and denote by $H(x,y,z,w)$ an equation (a linear form in $\mathbb{K}[x,y,z,w]$) of $\mathcal{H}$. We have the following degree d homogeneous polynomial in $\mathbb{K}[s,t]$

$$H(f_0(s,t), f_1(s,t), f_2(s,t), f_3(s,t)) = \prod_{i=1}^{d} (t_i s - s_i t) \tag{7}$$

where the points $(s_i : t_i) \in \mathbb{P}^1$, $i = 1, \ldots, d$ are not necessarily distinct. We define the intersection multiplicity of C with $\mathcal{H}$ at the point P, denoted $i_P(C, \mathcal{H})$, as the number of points $(s_i : t_i)_{i=1,\ldots,d}$ such that $\phi(s_i : t_i) = P$.

Definition 10. The multiplicity $m_P(C)$ of the point P on C is defined as the minimum of the intersection multiplicity $i_P(C, \mathcal{H})$ where $\mathcal{H}$ runs over all the hyperplanes not containing C and passing through the point $P \in C$, minimum which is reached with a sufficiently generic such $\mathcal{H}$.

Definition 11. An *inversion formula* of the point P on C is a homogeneous polynomial $h_P(s,t) \in \mathbb{K}[s,t]$ of degree $m_p(C)$ such that h_P divides (7) for any hyperplane $\mathcal{H}$ going through P. It is uniquely defined up to multiplication by a nonzero element in $\mathbb{K}$.

Given a μ-basis of the parameterization ϕ, say

$$\begin{aligned} p(s,t;x,y,z,w) &= p_0(s,t)x + p_1(s,t)y + p_2(s,t)z + p_3(s,t)w, \\ q(s,t;x,y,z,w) &= q_0(s,t)x + q_1(s,t)y + q_2(s,t)z + q_3(s,t)w, \\ r(s,t;x,y,z,w) &= r_0(s,t)x + r_1(s,t)y + r_2(s,t)z + r_3(s,t)w, \end{aligned}$$

where p, q, r are of degree $m \geq n \geq l$ respectively, on can extract an inversion formula of a given point in $\mathbb{P}^3$ with the following result that appears in [23] (we provide here a short proof for the sake of completeness).

Lemma 12. *Let P be a point on C. Then the GCD of the three homogeneous polynomials $p(s,t;P)$, $q(s,t;P)$, $r(s,t;P)$ in $\mathbb{K}[s,t]$ is an inversion formula of P.*

Proof. By a linear change of coordinates in $\mathbb{P}^3$, one can assume without loss of generality that $P = (0 : 0 : 0 : 1)$, because μ-bases have the expected property under linear change of coordinates. It follows that $p(s,t;P) = p_3(s,t)$, $q(s,t;P) = q_3(s,t)$ and $r(s,t;P) = r_3(s,t)$. Set $K(s,t) := \gcd(p_3, q_3, r_3)$.

From the definition of inversion formula we immediately deduce that $h_P(s,t) := \gcd(f_0, f_1, f_2)$. So we have to prove that K and h_P are equal up to multiplication by a nonzero element in $\mathbb{K}$.

From the properties of the μ-basis there exists $c \in \mathbb{K} \setminus \{0\}$ such that

$$cf_0 = \begin{vmatrix} p_1 & p_2 & p_3 \\ q_1 & q_2 & q_3 \\ r_1 & r_2 & r_3 \end{vmatrix}, \quad cf_1 = -\begin{vmatrix} p_0 & p_2 & p_3 \\ q_0 & q_2 & q_3 \\ r_0 & r_2 & r_3 \end{vmatrix}, \quad cf_2 = \begin{vmatrix} p_0 & p_1 & p_3 \\ q_0 & q_1 & q_3 \\ r_0 & r_1 & r_3 \end{vmatrix}.$$

Therefore, it is clear that K divides h_P.

Now, since

$$p_0(s,t)f_0(s,t) + p_1(s,t)f_1(s,t) + p_2(s,t)f_2(s,t) = -p_3(s,t)f_3(s,t)$$

we deduce that h_P divides $p_3 f_3$. But f_0, f_1, f_2 all vanish at the roots of h_P so h_P and f_3 cannot share a common root because ϕ is regular. It follows that h_P divides p_3. With the same argument, we get that h_P divides q_3 and r_3 as well. Therefore, h_P divides K. □

Taking again the notation of Section 3, for all integer $\nu \geq m + n - 1$ we have a representation matrix $\mathtt{M}(\phi)_\nu$ of the curve C which is built from the μ-basis p, q, r. Its entries are linear forms in $\mathbb{K}[x, y, z, w]$ so that it makes sense to evaluate $\mathtt{M}(\phi)_\nu$ at a point in $\mathbb{P}^3$ to get a matrix $\mathtt{M}(\phi)_\nu(P)$ with entries in $\mathbb{K}$.

Theorem 13. *Given a point P in $\mathbb{P}^3$, for all integer $\nu \geq m + n - 1$ we have*

$$\operatorname{rank} \mathtt{M}(\phi)_\nu(P) = \nu + 1 - m_P(C),$$

or equivalently $\operatorname{corank} \mathtt{M}(\phi)_\nu(P) = m_P(C)$.

Proof. From Lemma 12, we have that $h_P(s,t) = \gcd(p(s,t;P), q(s,t;P), r(s,t;P))$ is a homogeneous polynomial in $R := \mathbb{K}[s,t]$ of degree $m_P(C)$. From Section 3, we recall that $\mathtt{M}(\phi)_\nu(P)$ is a matrix of the map

$$R(-m)_\nu \oplus R(-n)_\nu \oplus R(-l)_\nu \xrightarrow{(p(s,t;P),q(s,t;P),r(s,t;P))} R_\nu$$

so that $\operatorname{corank} \mathtt{M}(\phi)_\nu = \dim_{\mathbb{K}}(R/I)_\nu$ for all integer ν, where I stands for the ideal of $\mathbb{K}[s,t]$ generated by the polynomials $p(s,t;P)$, $q(s,t;P)$ and $r(s,t;P)$.

Now, the homogeneous polynomials $p(s,t;P)/h_P, q(s,t;P)/h_P, r(s,t;P)/h_P$ are relatively prime other $\mathbb{K}[s,t]$ so it follows that the saturation of the homogeneous ideal $J = (p(s,t;P)/h_P, q(s,t;P)/h_P, r(s,t;P)/h_P) \subset \mathbb{K}[s,t]$ with respect to the ideal $\mathfrak{m} = (s,t)$ is equal to $\mathfrak{m}$. Therefore, we get the following result that we already used: $J_\nu = \mathfrak{m}_\nu$ for all $\nu \geq m + n - 2m_P(C) - 1$. But then, multiplying this equality by the homogeneous polynomial h_P we obtain

$$I_{\nu+m_P(C)} = h_P\,(p(s,t;P)/h_P, q(s,t;P)/h_P, r(s,t;P)/h_P)_\nu = (s,t)_\nu = (h_P)_{\nu+m_P(C)}$$

for all $\nu \geq m + n - 1 - 2m_P(C)$. We conclude that

$$\operatorname{corank} \mathtt{M}(\phi)_\nu(P) = \dim_{\mathbb{K}}(R/(h_P))_\nu = \nu + 1 - (\nu - m_P(C) + 1) = m_P(C)$$

for all $\nu \geq m + n - 1 - m_P(C)$, which finishes the proof since $m_P(C) \geq 0$ for any $P \in \mathbb{P}^3$. □

This result provides a stratification of the points in $\mathbb{P}^3$ with respect to the curve C. Indeed, we have that

- if P is such that $\operatorname{rank} \mathtt{M}(\phi)_\nu(P) = \nu + 1$ then $P \notin C$,
- if P is such that $\operatorname{rank} \mathtt{M}(\phi)_\nu(P) = \nu$ then P is a regular point (i.e. of multiplicity 1) on C,
- if P is such that $\operatorname{rank} \mathtt{M}(\phi)_\nu(P) = \nu - 1$ then P is singular point of multiplicity 2 on C,

- and so on.

Moreover, an immediate consequence of this theorem and Lemma 12 is that if P is a singular point on C then necessarily

$$2 \leq m_P(C) \leq n \text{ or } m_P(C) = m. \tag{8}$$

We refer the reader to [23] for more results of this kind about the possible singularities on C with respect to a μ-basis of its parameterization ϕ.

5.2. Singular factors

Theorem 13 suggests to introduce the *singular factors* of a representation, similarly to what has been done in [6], then in [3], for the case of plane curves. Although we are not able to get results similar to those proved in [3] for plane curves, because the geometry of space curves is much less constrained than the one of plane curves, we will nevertheless see that these singular factors allow to compute all the singularities of a rational space curve.

As above, suppose given an integer $\nu \geq m + n - 1$ and a representation matrix $\mathtt{M}(\phi)_\nu$ of the curve C which is built from the μ-basis p, q, r of degree $m \geq n \geq l$ respectively. We denote by $\mathtt{M}(\phi)_\nu(s,t)$ the matrix $\mathtt{M}(\phi)_\nu$ where we substitute x, y, z, w by $f_0(s,t), f_1(s,t), f_2(s,t), f_3(s,t)$ respectively. It is then clear that $\operatorname{rank} \mathtt{M}(\phi)_\nu(s,t) < \nu + 1$ for any point $(s:t) \in \mathbb{P}^1$.

Definition 14. A collection of homogeneous polynomials $d_1(s,t), \ldots, d_{\nu+1}(s,t)$ in $\mathbb{K}[s,t]$ such that for all integer $i = 1, \ldots, \nu + 1$ the product

$$d_{\nu+1}(s,t)^{\nu+1-i+1} d_\nu(s,t)^{\nu+1-i} \cdots d_{i+1}(s,t)^2 d_i(s,t)$$

is equal to the GCD of all the $(\nu + 2 - i)$-minors of $\mathtt{M}(\phi)_\nu(s,t)$ is called a collection of singular factors of the parameterization ϕ.

Notice that these singular factors are defined up to multiplication by a nonzero element in $\mathbb{K}$. Moreover, their existence is guaranteed because the ground variety is $\mathbb{P}^1_{\mathbb{K}}$, or in other words by homogenizing with some care the invariant factors of the matrix $\mathtt{M}(\phi)_\nu(s,1)$, $\mathbb{K}[s]$ being a principal ideal domain.

Theorem 15. *We have $d_{\nu+1}(s,t) = d_\nu(s,t) = \cdots = d_{m+1}(s,t) = 1$ and $d_1(s,t) = 0$. Moreover, for any singular point $P \in C$, the inversion formula $h_P(s,t)$ divides $d_{m_P(C)}(s,t)$ and is coprime with $d_k(s,t)$ for all $k > m_P(C)$.*

Proof. The entries of the matrix $\mathtt{M}(\phi)_\nu$ are linear forms in $\mathbb{K}[x,y,z,w]$. Therefore, its determinantal ideals, denoted $I_k(-)$ and which correspond to the ideals generated by all the k-minors of $\mathtt{M}(\phi)_\nu$, $k = 1, \ldots, \nu + 1$, are homogeneous ideals in $\mathbb{K}[x,y,z,w]$.

Then, by using Lemma 12 we deduce that

$$V(I_k(\mathtt{M}(\phi)_\nu)) = \emptyset \subset \mathbb{P}^3$$

for all $k = 1, \ldots, \nu + 1 - m$, as there cannot be any common factor of degree more than m of the three element of the μ-basis after specialization at a given point. It follows then that

$$V(I_k(\mathtt{M}(\phi)_\nu(s,t))) = \emptyset \subset \mathbb{P}^1$$

for all $k = 1, \ldots, \nu + 1 - m$, and this implies $d_k(s,t) = 1$ for all $k > m$.

Now, assume for simplicity that $P = (0:0:0:1)$. As we did above, we have $P \notin V(I_k(\mathtt{M}(\phi)_\nu))$ for all $k = 1, \ldots, \nu + 1 - m_P(C)$ which implies that $h_P(s,t)$ and $d_k(s,t)$ are relatively prime polynomials for all $k > m_P(C)$. On the other hand, $P \in V(I_{\nu+1-m_P(C)+1}(\mathtt{M}(\phi)_\nu))$, that is $I_{\nu+1-m_P(C)+1}(\mathtt{M}(\phi)_\nu) \subset (x_0, x_1, x_2)$, and hence

$$I_{\nu+1-m_P(C)+1}(\mathtt{M}(\phi)_\nu(s,t)) \subset (f_0(s,t), f_1(s,t), f_2(s,t)) \subset (h_P(s,t)) \subset \mathbb{K}[s,t].$$

It follows that $h_P(s,t)$ divides

$$d_{\nu+1}(s,t)^{\nu+1-m_P(C)+1} \cdots d_{m_P(C)+1}(s,t)^2 d_{m_P(C)}(s,t)$$

and therefore that $h_P(s,t)$ divides $d_{m_P(C)}(s,t)$. □

Here are two consequences of this theorem that allows to characterize the multiplicity of a singular point and to compute the singular points.

Corollary 16. *Let $P = \phi(s_0 : t_0)$ be a point on C, then $d_{m_P(C)}(s_0 : t_0) = 0$ and $d_k(s_0 : t_0) \neq 0$ for all $k > m_P(C)$. In particular, the multiplicity of P is the highest integer k such that $d_k(s_0 : t_0) = 0$.*

Corollary 17. *For any integer k such that $2 \leq k \leq m$, the product*

$$\prod_{P \in C \,:\, m_P(C)=k} h_p(s,t)$$

that runs over all the singular points on C of multiplicity k, divides the singular factor $d_k(s,t)$.

5.3. Computational aspects

The computation of the singular factors can be done through Smith form computations. Indeed, the matrix $\mathtt{M}(\phi)_\nu(s,1)$ is a matrix with entries in the principal ideal domain $\mathbb{K}[s]$. Therefore it is equivalent to the diagonal matrix

$$\begin{pmatrix} d_{\nu+1}(s,1) & & & & & & \\ & d_{\nu+1}d_\nu(s,1) & & & & & \\ & & d_{\nu+1}d_\nu d_{\nu-1}(s,1) & & & & \\ & & & \ddots & & & \\ & & & & d_{\nu+1}\cdots d_3(s,1) & & \\ & & & & & d_{\nu+1}\cdots d_3 d_2(s,1) & \\ & & & & & & 0 \end{pmatrix}.$$

So, the computation of this Smith form (or equivalently its invariant factors) yields the dehomogenized singular factors where t is set to 1. It follows that if the point $P = \phi(1 : 0)$ is not a singular point, then the singularities of the curve C can be recovered after a single Smith form computation. If not, it is necessary to either perform the same computation for the matrix $\mathtt{M}(\phi)_\nu(1,t)$ to get the dehomogenized singular factors where now s is set to 1, or either obtain directly the information on the possible singular point $\phi(1 : 0)$ by performing the GCD computation from Lemma 12.

We conclude this section with two illustrative examples.

Example 18 ([23, Example 7.6])**.** Let C be the rational space curve parameterized by

$$\phi : \mathbb{P}^1_{\mathbb{K}} \to \mathbb{P}^3_{\mathbb{K}} : (s : t) \mapsto (s^5 : s^3t^2 : s^2t^3 : t^5).$$

A μ-basis for C is given by

$$\begin{aligned} p &= ty - sz \\ q &= t^2x - s^2y, \\ r &= t^2z - s^2w. \end{aligned}$$

Since $\deg(q) = \deg(r) = 2$, we can choose $\nu = 3$, then a matrix representation of C is given by

$$\mathtt{M}(\phi)_3 = \begin{pmatrix} y & 0 & 0 & x & 0 & z & 0 \\ -z & y & 0 & 0 & x & 0 & z \\ x & -z & y & -y & 0 & -w & 0 \\ 0 & 0 & -z & 0 & -y & 0 & -w \end{pmatrix}.$$

Substituting $x = s^5, y = s^3t^2, z = s^2t^3, w = t^5$, we obtain

$$\mathtt{M}(\phi)_3(s,t) = \begin{pmatrix} s^3t^2 & 0 & 0 & s^5 & 0 & s^2t^3 & 0 \\ -s^2t^3 & s^3t^2 & 0 & 0 & s^5 & 0 & s^2t^3 \\ 0 & -s^2t^3 & s^3t^2 & -s^3t^2 & 0 & -t^5 & 0 \\ 0 & 0 & -s^2t^3 & 0 & -s^3t^2 & 0 & -t^5 \end{pmatrix}.$$

Now, the Smith form of $M(s,1)$ and $M(1,t)$ are respectively

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & s^2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & t^2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Therefore, the singular factors of C are $d_4(s,t) = 1, d_3(s,t) = 1, d_2(s,t) = s^2t^2$. Thus, C has only two singular points of multiplicity 2, the points $A = (0:0:0:1)$ and $B = (1:0:0:0)$ that correspond to the parameters $(0:1)$ and $(1:0)$ respectively.

Example 19. Let C be the classical rational twisted cubic which is parameterized by

$$\phi : \mathbb{P}^1_{\mathbb{K}} \to \mathbb{P}^3_{\mathbb{K}} : (s:t) \mapsto (s^3 : s^2t : st^2 : t^3).$$

A μ-basis for C is given by

$$\begin{aligned} p &= -tx + sy \\ q &= -ty + sz, \\ r &= -tz + sw. \end{aligned}$$

Since $\deg(q) = \deg(r) = 1$, we can choose $\nu = 1$ and then a matrix representation of C is

$$\mathtt{M}(\phi)_1 = \begin{pmatrix} -x & -y & -z \\ y & z & w \end{pmatrix}.$$

Substituting $x = s^3, y = s^2t, z = st^2, w = t^3$, we obtain

$$\mathtt{M}(\phi)_1(s,t) = \begin{pmatrix} -s^3 & -s^2t & -st^2 \\ s^2t & st^2 & t^3 \end{pmatrix}.$$

The Smith forms of $M(s,1)$ and $M(1,t)$ are respectively:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

It follows that the singular factors of C are $d_3(s,t) = 1, d_2(s,t) = 1$: we recover the well known fact that C has no singular point.

6. Intersection problem

In this section, we deal with the problem of computing the intersection between two algebraic curves given by parameterizations. The approach which we develop below is based on the use of a representation matrix of one of the two curves. With such a matrix, we show that the intersection problem become completely similar to the intersection between a curve and a surface when a representation matrix is used for the surface, as treated for instance in [19, 1, 18].

6.1. Matrix representations and curve/curve intersection

Suppose given two rational curves, say C_1 parameterized by

$$\mathbb{P}^1 \xrightarrow{\phi_1} \mathbb{P}^n : (s:t) \mapsto (f_0 : \cdots : f_n)(s,t) \tag{9}$$

and C_2 parameterized by the regular map

$$\mathbb{P}^1 \xrightarrow{\phi_2} \mathbb{P}^n : (s:t) \mapsto (g_0 : \cdots : g_n)(s,t). \tag{10}$$

Let $\mathtt{M}(\phi_1)_\nu$ be a representation matrix of C_1 for a suitable integer ν, as described in Section 3. The substitution in $\mathtt{M}(\phi_1)_\nu$ of the variables x, y, z, w by the homogeneous parameterization of C_2 yields the matrix

$$\mathtt{M}_\nu(\phi_1, \phi_2)(s, t) := \mathtt{M}(\phi_1)_\nu(g_0(s, t), \ldots, g_n(s, t))$$

As a consequence of the properties of a representation matrix, we have the following easy property.

Lemma 20. *Let* $(s_0 : t_0) \in \mathbb{P}^1$*, then* $\operatorname{rank} \mathtt{M}_\nu(\phi_1, \phi_2)(s_0, t_0) < \nu + 1$ *if and only if the point* $\phi_2(s_0, t_0)$ *belongs to the intersection locus* $C_1 \cap C_2$*.*

The set $C_1 \cap C_2$ is in correspondence with the points of $\mathbb{P}^1$ where the rank of $\mathtt{M}_\nu(\phi_1, \phi_2)(s, t)$ drops. By setting $t = 1$, the determination of the values of s such that the rank of $\mathtt{M}_\nu(\phi_1, \phi_2)(s, 1)$ can be treated at the level of matrices (that is to say without any symbolic computation and in particular without any determinant computations) by using linearization techniques and generalized eigenvalues computations. These techniques are quite classical for square matrices but representation matrices are rarely square (except for plane curves where the smallest representation matrix is always a square matrix). Recently, they have been extended for non-square matrices in [18]. In the rest of this section we will briefly reproduce them for the convenience of the reader and give an illustrative example. We refer to [18] for more details.

Before moving on, mention that we use linearization techniques, but we could also compute a Smith form of $\mathtt{M}_\nu(\phi_1, \phi_2)$. We chose this option because linearization techniques are powerful tools from linear algebra that are very efficient and stable and that are widely available in softwares. In comparison, the computation of a Smith form requires exact computations and the more efficient algorithms, for instance the one given in [22], are tricky and not easily available in softwares. Moreover, point out that the study of theoretical complexity seems to be in favor of linearization techniques (the complexity of linearization techniques is given in [18] and the one of Smith form computation in [22]), although these algorithms are not really comparable because they are not computing the same outputs and they are not using the same arithmetics. In practice, linearization techniques had always shown to be faster than Smith form computations in our context.

6.2. Linearization of a polynomial matrix

We begin with some notation. Let A and B be two matrices of size $m \times n$ with coefficients in $\mathbb{K}$. We will call a generalized eigenvalue of A and B a value in the set

$$\lambda(A, B) := \{t \in \mathbb{K} : \operatorname{rank}(A - tB) < \min\{m, n\}\}.$$

In the case $m = n$, the matrices A and B have n generalized eigenvalues if and only if $\operatorname{rank}(B) = n$. If $\operatorname{rank}(B) < n$, then $\lambda(A, B)$ can be finite, empty or infinite. Moreover, if B is invertible then $\lambda(A, B) = \lambda(AB^{-1}, I)$, which is the ordinary spectrum of the matrix AB^{-1}.

Suppose given an $m \times n$-matrix $M(t) = (a_{i,j}(t))$ with polynomial entries $a_{i,j}(t) \in \mathbb{K}[t]$. It can be equivalently written as a polynomial in t with coefficients $m \times n$-matrices with entries in $\mathbb{K}$: if $d = \max_{i,j}\{\deg(a_{i,j}(t))\}$ then

$$M(t) = M_d t^d + M_{d-1} t^{d-1} + \ldots + M_0$$

where $M_i \in \mathbb{K}^{m \times n}$.

Definition 21. The generalized companion matrices A, B of the matrix $M(t)$ are the matrices with coefficients in $\mathbb{K}$ of size $((d-1)m + n) \times dm$ that are given by

$$A = \begin{pmatrix} 0 & I & \ldots & \ldots & 0 \\ 0 & 0 & I & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & \ldots & I \\ M_0^t & M_1^t & \ldots & \ldots & M_{d-1}^t \end{pmatrix}$$

$$B = \begin{pmatrix} I & 0 & \dots & \dots & 0 \\ 0 & I & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & I & 0 \\ 0 & 0 & \dots & \dots & -M_d^t \end{pmatrix}$$

where I stands for the identity matrix and M_i^t stands for the transpose of the matrix M_i.

Theorem 22. *With the above notations, the following equivalence holds:*

$$\operatorname{rank} M(t) \textit{ drops} \Leftrightarrow \operatorname{rank}(A - tB) \textit{ drops}.$$

6.3. Extracting the regular part of a non square pencil of matrices

We start with a pencil $A - tB$ where A, B are constant matrices of size $p \times q$ with coefficients in a field $\mathbb{K}$. Set $\rho = \operatorname{rank} B$. In the following algorithm, all computational steps are easily realized via the classical LU-decomposition.

Step 1 Transform B into its column echelon form; that amounts to determine unitary matrices P_0 and Q_0 such that

$$B_1 = P_0 B Q_0 = [\underbrace{B_{1,1}}_{\rho} \mid \underbrace{0}_{q-\rho}]$$

where $B_{1,1}$ is an echelon matrix. Then, compute

$$A_1 = P_0 A Q_0 = [\underbrace{A_{1,2}}_{\rho} \mid \underbrace{A_{1,2}}_{q-\rho}]$$

Step 2 Transform $A_{1,2}$ into its row echelon form; that amounts to determine unitary matrices P_1 and Q_1 such that

$$P_1 A_{1,2} Q_1 = \begin{pmatrix} A'_{1,2} \\ \hline 0 \end{pmatrix}$$

where $A'_{1,2}$ has full row rank while keeping $B_{1,1}$ in echelon form.

At the end of step 2, matrices A and B are represented under the form

$$A'_1 = \left(\begin{array}{c|c} A'_{1,1} & A'_{1,2} \\ \hline A_2 & 0 \end{array}\right) \quad B'_1 = \left(\begin{array}{c|c} B'_{1,1} & 0 \\ \hline B_2 & 0 \end{array}\right)$$

where

- $A'_{1,2}$ has full row rank,
- $\begin{pmatrix} B'_{1,1} \\ \hline B_2 \end{pmatrix}$ has full column rank,
- $\begin{pmatrix} B'_{1,1} \\ \hline B_2 \end{pmatrix}$ and B_2 are in echelon form.

After steps 1 and 2, we obtain a new pencil of matrices, namely $A_2 - tB_2$.

Step 3 Starting from $j = 2$, repeat the above steps 1 and 2 for the pencil $A_j - tB_j$ until the $p_j \times q_j$ matrix B_j has full column rank, that is to say until $\operatorname{rank} B_j = q_j$.

Step 4 If B_j is not a square matrix, then we repeat the above procedure with the transposed pencil $A_j^t - tB_j^t$.

At last, we obtain the regular pencil $A' - tB'$ where A', B' are two square matrices and B' is invertible. Moreover, we have the

Theorem 23. *With the above notation, the following equivalence holds:*

$$\text{rank}(A - tB) \textit{ drops} \Leftrightarrow \text{rank}(A' - tB') \textit{ drops}.$$

We are now ready to state our algorithm for solving the curve/curve intersection problem:

Algorithm 2: Intersection of two parameterized curves

Input: Two parameterized curves C_1 and C_2 given by (9) and (10).
Output: The intersection points of C_1 and C_2.
1. *Compute the matrix representation* $\mathtt{M}(\phi_1)_\nu$ *of* C_1 *for a suitable* ν.
2. *Compute the generalized companion matrices* A *and* B *of* $\mathtt{M}_\nu(\phi_1, \phi_2)$.
3. *Compute the companion regular matrices* A' *and* B'.
4. *Compute the eigenvalues of* (A', B').
5. *For each eigenvalue* t_0, $\phi_2(t_0 : 1)$ *is an intersection point.*

Before illustrating the above algorithm with two examples, we would like to make two comments. First, it should be noticed that this algorithm returns all the points in $C_1 \cap C_2$ except possibly the point $\phi(1 : 0)$. However, this is not a limitation because this latter point can be treated independently. Second, the eigenvalues of (A', B') in the step 4 of Algorithm 2 comes with their multiplicities (as eigenvalues). These multiplicities are definitely in relation with the intersection multiplicities of the intersection points of C_1 and C_2. We already noticed such a link in our study of the curve/surface intersection problem in [18]. However, the situation here appears much more complicated, especially when the point is already a singular point on C_1, or on C_2, or on both C_1 and C_2.

Example 24. Let C_1 be the rational space curve given by the parameterization

$$\begin{aligned}
f_0(s,t) &= 3s^4t^2 - 9s^3t^3 - 3s^2t^4 + 12st^5 + 6t^6,\\
f_1(s,t) &= -3s^6 + 18s^5t - 27s^4t^2 - 12s^3t^3 + 33s^2t^4 + 6st^5 - 6t^6,\\
f_2(s,t) &= s^6 - 6s^5t + 13s^4t^2 - 16s^3t^3 + 9s^2t^4 + 14st^5 - 6t^6,\\
f_3(s,t) &= -2s^4t^2 + 8s^3t^3 - 14s^2t^4 + 20st^5 - 6t^6.
\end{aligned}$$

We want to compute the intersection of C_1 with the twisted cubic C_2 which is parameterized by

$$g_0(s,t) = s^3, g_1(s,t) = s^2t, g_2(s,t) = st^2, g_3(s,t) = t^3.$$

First, we compute a representation matrix of C_1:

$$\mathtt{M}(\phi_1)_3 = \begin{pmatrix}
x+y & 0 & 3y-3z & 0 & 2z-2w & 0\\
-3x & x+y & -y-3z & 3y-3z & -2w & 2z-2w\\
x & -3x & y+3z & -y-3z & w & -2w\\
0 & x & 0 & y+3z & 0 & w
\end{pmatrix}.$$

A point P at finite distance belongs to the intersection locus of C_1 and C_2 if and only if $P = (1 : t : t^2 : t^3)$ and t is one of the generalized eigenvalues of the matrix

$$M(t) := \mathtt{M}_3(\phi_1, \phi_2) = \begin{pmatrix}
1+t & 0 & 3t-3t^2 & 0 & 2t^2-2t^3 & 0\\
-3 & 1+t & -t-3t^2 & 3t-3t^2 & -2t^3 & 2t^2-2t^3\\
1 & -3 & t+3t^2 & -t-3t^2 & t^3 & -2t^3\\
0 & 1 & 0 & t+3t^2 & 0 & t^3
\end{pmatrix},$$

We have $M(t) = M_3t^3 + M_2t^2 + M_1t + M_0$ and the generalized companion matrices of $M(t)$ are

$$A = \begin{pmatrix}
0 & I & 0\\
0 & 0 & I\\
M_0^t & M_1^t & M_2^t
\end{pmatrix}, B = \begin{pmatrix}
I & 0 & 0\\
0 & I & 0\\
0 & 0 & -M_3^t
\end{pmatrix}$$

Applying Algorithm 2, we find that the regular part of the pencil $A - tB$ is the pencil $A' - tB'$ where A', B' are given by

$$A' = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, B' = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Therefore, the computation yields a single eigenvalues $t = 0$, and thus C_1 intersect C_2 at the only point $P = (1 : 0 : 0 : 0)$.

We can also determine the parameter(s) corresponding to P through the parameterization ϕ_1 of C_1. For that purpose, we first evaluate the rank of the matrix $\mathtt{M}_3(\phi_1, \phi_2)(P)$. It is equal to 2. Therefore, P is a singular point of multiplicity 2. It follows that it is not possible to apply the inversion method given in Section 4, but rather the method for computing the singular points of C_1 given in Section 5. We get that P is obtained through the two parameters $(1 : \frac{1}{2}(3 + \sqrt{5}))$ and $(1 : \frac{1}{2}(3 - \sqrt{5}))$ via ϕ_1.

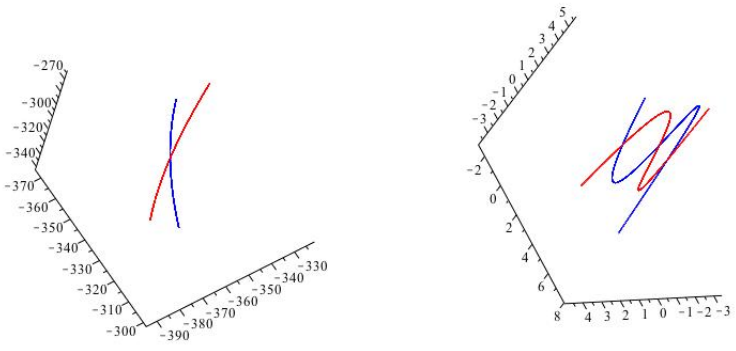
Example 25. We have implemented Algorithm 2 in the software `Maple`. The corresponding files are available at `http://www-sop.inria.fr/members/Luu.Ba_Thang/`. Consider the two curves parameterized, in affine coordinate, by

$$\begin{aligned} f_0(t) &= -33 + \frac{115}{2}\,t - \frac{49}{2}\,t^2 + t^4, \\ f_1(t) &= -36 + 61\,t - 25\,t^2 + t^4, \\ f_2(t) &= -8 + \frac{27}{2}\,t - 13/2\,t^2 + t^3, \\ f_3(t) &= 1. \end{aligned}$$

and

$$\begin{aligned} g_0(t) &= -3 + 17/2\,t - 11/2\,t^2 + t^3, \\ g_1(t) &= -6 + 12\,t - 6\,t^2 + t^3, \\ g_2(t) &= -38 + \frac{125}{2}\,t - \frac{51}{2}\,t^2 + t^4, \\ g_3(t) &= 1. \end{aligned}$$

Running our algorithm, we find 4 values of the parameter t that corresponds to an intersection point, namely $t = -5, 1, 2, 3$. These four intersection points, of coordinates $(1, 0, 0), (1, 2, 3), (0, 1, 1)$ and $(-308, -341, -363)$ can be visualized in the following pictures.



7. Line intersection of two ruled surfaces

The aim of this section is to show that curves in a projective space of higher dimension than 3 can be useful for applications in CAGD. Hereafter, we consider the problem of computing line intersections between two ruled

surfaces. As we will see, this can be done by computing the intersection of two rational curves in a $\mathbb{P}^5$, a problem that can be solved by using the techniques we have presented in the previous section.

It is worth mentioning that the computation of the intersection lines between two ruled surfaces is interesting because it corresponds to the singular case in the methods given in [14] and [10] to compute the complete intersection locus between two ruled surfaces.

Rational ruled surfaces. A rational ruled surface $\mathbb{S}$ is meant to be a surface given by a rational map

$$\begin{array}{rcl} \Phi_{\mathbb{S}} : \mathbb{P}^1_{\mathbb{K}} \times \mathbb{P}^1_{\mathbb{K}} & \to & \mathbb{P}^3_{\mathbb{K}} \\ (s : \bar{s}) \times (t : \bar{t}) & \mapsto & (f_0(s, \bar{s}, t, \bar{t}) : \cdots : f_3(s, \bar{s}, t, \bar{t})) \end{array} \tag{11}$$

where $f_i \in \mathbb{K}[s, \bar{s}; t, \bar{t}]$ are bi-homogeneous polynomials of degree $(n, 1)$, by which we mean that they are homogeneous polynomials of degree $n + 1$ and that $\deg_{s,\bar{s}}(f_i) = n$ and $\deg_{t,\bar{t}}(f_i) = 1$ for all $i = 0, 1, 2, 3$. We assume that $\gcd(f_0, f_1, f_2, f_3) = 1$ so that we can rewrite

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

where $f_{i0}, f_{i1} \in \mathbb{K}[s, \bar{s}], n_0 = \max \deg_s(f_{i0}), n_1 = \max \deg_s(f_{i1})$ and where we assume that $n_1 \geq n_0$ (otherwise we can re-parameterize $\Phi_{\mathbb{S}}$ by exchanging t and $\bar{t}$). Therefore, $n_1 = n$. We also assume that $(f_{00}, ..., f_{30})$ and $(f_{01}, ..., f_{31})$ are $\mathbb{K}[s, \bar{s}]$-linearly independent to exclude the degenerate case where $\Phi_{\mathbb{S}}$ does not parameterize a surface.

For almost all parameter $(s : \bar{s}) \in \mathbb{P}^1_{\mathbb{K}}$, the image of map

$$\begin{array}{rcl} L^{\mathbb{S}}_{(s:\bar{s})} : \mathbb{P}^1_{\mathbb{K}} & \to & \mathbb{P}^3_{\mathbb{K}} \\ (t : \bar{t}) & \mapsto & (f_0(s, \bar{s}, t, \bar{t}) : \cdots : f_3(s, \bar{s}, t, \bar{t})) \end{array}$$

is the line passing through the two distinct points $(f_{00}(s : \bar{s}), ..., f_{30}(s : \bar{s}))$ and $(f_{01}(s : \bar{s}), ..., f_{31}(s : \bar{s}))$ in $\mathbb{P}^3_{\mathbb{K}}$. The ruled surface $\mathbb{S}$ can be considered as the closure of the union of these lines.

Plücker coordinates. Let L be a line in the projective space $\mathbb{P}^3$. Given two distinct points A, B on L with homogeneous coordinates $(a_0 : a_1 : a_2 : a_3)$, $(b_0 : b_1 : b_2 : b_3)$ respectively, we define the Plücker coordinates of L as the point $(p_{01} : p_{02} : p_{03} : p_{23} : p_{31} : p_{12}) \in \mathbb{P}^5$ where

$$p_{ij} := \det \begin{pmatrix} a_i & b_i \\ a_j & b_j \end{pmatrix} = a_i b_j - a_j b_i.$$

It is not hard to see that the Plücker coordinates of L are well defined (it does not depend on the choice of the points $A, B \in L$) and satisfy to the quadratic relation $p_{01}p_{23} + p_{02}p_{31} + p_{03}p_{12} = 0$, that is to say belongs to the Klein quadric

$$\mathfrak{S} = \{(x_0 : x_1 : x_2 : x_3 : x_4 : x_5) \in \mathbb{P}^5 : x_0x_3 + x_1x_4 + x_2x_5 = 0\}.$$

Conversely, to any point in $\mathfrak{S}$ one can associate a line in $\mathbb{P}^3$ and hence we see that Plücker coordinates give a bijective correspondence between lines in $\mathbb{P}^3$ and points in $\mathfrak{S} \subset \mathbb{P}^5$.

Plücker curves. Now, returning to the ruled surface (11), we define the Plücker curve as the image of the rational map

$$\begin{array}{rcl} \Psi_{\mathbb{S}} : \mathbb{P}^1 & \to & \mathbb{P}^5 \\ (s : \bar{s}) & \mapsto & (p_{01} : p_{02} : p_{03} : p_{23} : p_{31} : p_{12}) \end{array}$$

where $p_{ij} = f_{i0}f_{j1} - f_{i1}f_{j0}$ are the Plücker coordinates of the line in $\mathbb{P}^3$ defined by the two points $(f_{00}(s : \bar{s}), ..., f_{30}(s : \bar{s}))$ and $(f_{01}(s : \bar{s}), ..., f_{31}(s : \bar{s}))$. Since there is a one to one correspondence between the points $\Psi_{\mathbb{S}}(s : \bar{s})$ on the Plücker curve and the associated line $L_{(s:\bar{s})}$ on the ruled surface $\mathbb{S}$, we obtain the following algorithm to compute intersection lines between two ruled surfaces.

Algorithm 3: Intersection lines between two ruled surfaces

Input: Two rational ruled surfaces $\mathbb{S}_1$ and $\mathbb{S}_2$.

Output: The intersection lines of $\mathbb{S}_1$ and $\mathbb{S}_2$.

1. *Compute the Plücker curves C_1 and C_2 associated to the ruled surfaces $\mathbb{S}_1$ and $\mathbb{S}_2$ respectively.*
2. *Compute the intersection points of C_1 and C_2 using Algorithm 2.*
3. *Each intersection point is obtained as a value $(s : \bar{s}) \in \mathbb{P}^1$ that corresponds to the intersection line $L^{\mathbb{S}_1}_{(s:\bar{s})}$.*

8. Complement: matrix representations without μ-bases

In Section 3 we defined matrix representations of a rational curve. To build such a matrix it is necessary to first compute a μ-basis of the parameterization of the curve. There exist efficient algorithms to compute μ-basis (see [24, 21]), but they all require the use of *exact* linear algebra routines. Therefore, in order to make matrix representations accessible to any programming environment having linear algebra routines (but not necessarily exact), we provide a new family of matrix representations that does not require symbolic computations to be built. As we will see, the price to pay for this property is that the matrices we obtain are of bigger size than the ones obtained from a μ-basis.

Take again the notation of Section 3 and set

$$\Delta_{i,j} = \begin{vmatrix} f_i(s,t) & f_j(s,t) \\ x_i & x_j \end{vmatrix}$$

for all $0 \leq i < j \leq n$. The $\Delta_{i,j}$'s are the 2-minors of the matrix

$$\begin{pmatrix} f_0(s,t) & f_1(s,t) & \cdots & f_{n-1}(s,t) & f_n(s,t) \\ x_0 & x_1 & \cdots & x_{n-1} & x_n \end{pmatrix}.$$

They are homogeneous polynomial in $\mathbb{K}[s,t;x_0,\ldots,x_n]$. More precisely they are linear forms in the homogeneous variables $x_0,\ldots,x_n$ and homogeneous polynomials of degree d in the homogeneous variables s,t.

As in Section 3, set $A = \mathbb{K}[x_0,\ldots,x_n]$, $C = A[s,t]$ and consider the grading of C such that $\deg(s) = \deg(t) = 1$ and $\deg(a) = 0$ for all $a \in A$. Now, consider the graded map

$$\bigoplus_{0\leq i<j\leq n} C(-d) \xrightarrow{(\ldots,\Delta_{i,j},\ldots)} C : (\cdots : g_{i,j} : \cdots) \mapsto \sum_{0\leq i<j\leq n} g_{i,j}\Delta_{i,j} \tag{12}$$

and denote by $\overline{B}$ its cokernel.

Proposition 26. *For all integer $\nu \geq 2d-1$, we have $B_\nu = \overline{B}_\nu$.*

Proof. Consider the Koszul complex associated to the sequence $(f_0,\ldots,f_n)$ over the ring C. It is of the form

$$\cdots \to \bigoplus_{0\leq i<j\leq n} C(-2d) \xrightarrow{\partial_2} \bigoplus_{0\leq i<j\leq n} C(-d) \xrightarrow{\partial_1} C.$$

Observe then that the kernel of ∂_1 is exactly the ideal generated by a μ-basis of ϕ and that the image of ∂_2 is in correspondence with the syzygies of the f_i's that are of the form given by the $\Delta_{i,j}$'s. Therefore, the difference between B and $\overline{B}$ is controlled by the first homology group H_1 of this Koszul complex.

Now, by a classical property of Koszul complexes, H_1 is annihilated by the ideal $(f_0,\ldots,f_n)$. Since ϕ is a regular map, we deduce that $B_\nu = \overline{B}_\nu$ for $\nu >> 0$. Now, a classical spectral sequence (see for instance [16]) shows that we have a graded isomorphism, for all $\nu \in \mathbb{Z}$,

$$(H_1)_\nu \simeq H^2_{\mathfrak{m}}(C(-3d))_\nu.$$

Therefore, we deduce that $(H_1)_\nu = 0$ for all $\nu \geq 3d-1$ and the result follows by noting that H_1 is embedded in the twisted graded ring $C(-d)$. □

By taking graded parts (12), for all integer $\nu \in \mathbb{N}$ we obtain the A-linear map

$$\bigoplus_{0\leq i<j\leq n} C_{\nu-d} \xrightarrow{(\ldots,\Delta_{i,j},\ldots)} C_\nu.$$

Denote by $\overline{\mathtt{M}(\phi)}_\nu$ a matrix of this map. Then, by Proposition 26, we have

Corollary 27. *For all integer $\nu \geq 2d-1$, the matrix $\overline{\mathtt{M}(\phi)}_\nu$ is a representation matrix of C.*

The matrices $\overline{\mathtt{M}(\phi)}_\nu$ have exactly the same properties as the matrices $\mathtt{M}(\phi)_\nu$ that are built from a μ-basis. On the one hand, they do not require symbolic computations, but on the other hand their sizes are much bigger. For instance, the matrix $\overline{\mathtt{M}(\phi)}_{2d-1}$ (the smallest one) is of size $(2d) \times \binom{n+1}{2} d$ whereas the matrix $\mathtt{M}(\phi)_{d-1}$ (the smallest one) is of size $d \times (n-1)d$.

Example 28. Let C be the classical rational twisted cubic which is parameterized by

$$\phi : \mathbb{P}^1_{\mathbb{K}} \to \mathbb{P}^3_{\mathbb{K}} : (s,t) \mapsto (s^3 : s^2t : st^2 : t^3).$$

We have $\{\Delta_{i,j} : 0 \le i < j \le 4\} = \{s^3y - s^2tx, s^3z - st^2x, s^3w - t^3x, s^2tz - st^2y, s^2tw - t^3y, st^2w - t^3z\}$. Choosing $\nu = 5$ and the usual monomial basis, we obtain the following matrix representation of C:

$$\overline{\mathtt{M}(\phi)}_5 = \begin{pmatrix} y & 0 & 0 & z & 0 & 0 & w & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -x & y & 0 & 0 & z & 0 & 0 & w & 0 & z & 0 & 0 & w & 0 & 0 & 0 & 0 & 0 \\ 0 & -x & y & -x & 0 & z & 0 & 0 & w & -y & z & 0 & 0 & w & 0 & w & 0 & 0 \\ 0 & 0 & -x & 0 & -x & 0 & -x & 0 & 0 & 0 & -y & z & -y & 0 & w & -z & w & 0 \\ 0 & 0 & 0 & 0 & 0 & -x & 0 & -x & 0 & 0 & 0 & -y & 0 & -y & 0 & 0 & -z & w \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -x & 0 & 0 & 0 & 0 & 0 & -y & 0 & 0 & -z \end{pmatrix}.$$

References

[1] Aruliah, D.A., Corless, R.M., Gonzalez-Vega, L., Shakoori, A., 2007. Geometric applications of the bezout matrix in the lagrange basis, in: Proceedings of the 2007 international workshop on Symbolic-numeric computation, ACM, London, Ontario, Canada. pp. 55–64.

[2] Busé, L., 2006. Elimination theory in codimension one and applications. Notes of lectures given at the CIMPA-UNESCO-IRAN school in Zanjan, Iran, July 9-22 2005.

[3] Busé, L., D'Andrea, C., 2009. Singular factors of rational plane curves. Preprint arXiv:0912.2723.

[4] Busé, L., Goldman, R., 2008. Division algorithms for Bernstein polynomials. Comput. Aided Geom. Design 25, 850–865.

[5] Busé, L., Jouanolou, J.P., 2003. On the closed image of a rational map and the implicitization problem. J. Algebra 265, 312–357.

[6] Chen, F., Wang, W., Liu, Y., 2008. Computing singular points of plane rational curves. J. Symbolic Comput. 43, 92–117.

[7] Cox, D., Little, J., O'Shea, D., 1997. Ideals, varieties, and algorithms. Undergraduate Texts in Mathematics, Springer-Verlag, New York. second edition. An introduction to computational algebraic geometry and commutative algebra.

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

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

[10] Fioravanti, M., Gonzalez-Vega, L., Necula, I., 2006. Computing the intersection of two ruled surfaces by using a new algebraic approach. Journal of Symbolic Computation 41, 1187 – 1205. Special Issue on the Occasion of Volker Weispfenning's 60th Birthday, Special Issue on the Occasion of Volker Weispfenning's 60th Birthday.

[11] Fortuna, E., Gianni, P., Trager, B., 2009. Generators of the ideal of an algebraic space curve. J. Symbolic Comput. 44, 1234–1254.

[12] Garrity, T., Warren, J., 1989. On computing the intersection of a pair of algebraic surfaces. Comput. Aided Geom. Design 6, 137–153.

[13] Grayson, D.R., Stillman, M.E., . Macaulay2, a software system for research in algebraic geometry. Available at http://www.math.uiuc.edu/Macaulay2/.

[14] Heo, H.S., Kim, M.S., Elber, G., 1999. The intersection of two ruled surfaces. Computer-Aided Design 31, 33 – 50.

[15] Jia, X., Wang, H., Goldman, R., 2010. Set-theoretic generators of rational space curves. Journal of Symbolic Computation 45, 414 – 433.

[16] Jouanolou, J.P., 1980. Idéaux résultants. Adv. in Math. 37, 212–238.

[17] Kunz, E., 2005. Introduction to plane algebraic curves. Translated from the original German by Richard G. Belshoff .

[18] Luu Ba, T., Busé, L., Mourrain, B., 2009. Curve/surface intersection problem by means of matrix representations, in: SNC '09: Proceedings of the 2009 conference on Symbolic numeric computation, ACM, New York, NY, USA. pp. 71–78.

[19] Manocha, D., Canny, J., 1991. A new approach for surface intersection, in: Proceedings of the first ACM symposium on Solid modeling foundations and CAD/CAM applications, ACM, Austin, Texas, United States. pp. 209–219.

[20] Northcott, D.G., 1976. Finite free resolutions. Cambridge University Press, Cambridge. Cambridge Tracts in Mathematics, No. 71.

[21] Song, N., Goldman, R., 2009. μ-bases for polynomial systems in one variable. Comput. Aided Geom. Design 26, 217–230.

[22] Storjohann, A., Labahn, G., 1997. A fast las vegas algorithm for computing the smith normal form of a polynomial matrix. Linear Algebra and its Applications 253, 155 – 173.

[23] Wang, H., Jia, X., Goldman, R., 2009. Axial moving planes and singularities of rational space curves. Comput. Aided Geom. Design 26, 300–316.

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